

INTRODUZIONE

Titolo del Brevetto: Metodo di Certificazione Digitale Basato su ChatGPT, Archiviazione Decentralizzata e Blockchain

Inventori: Alessandro Petretto & ChatGPT (OpenAI)

1. Contesto e Motivazione

Negli ultimi anni, la digitalizzazione ha trasformato profondamente il modo in cui i documenti vengono creati, archiviati e certificati. Tuttavia, l'affidabilità e l'integrità delle informazioni digitali restano una sfida aperta, con rischi significativi legati alla falsificazione, alla perdita di dati e alla necessità di intermediari centralizzati per la certificazione.

Questo brevetto è il frutto di una collaborazione tra Alessandro Petretto e **ChatGPT**, un'intelligenza artificiale avanzata di OpenAI, con l'obiettivo di dimostrare il potenziale rivoluzionario dell'AI quando combinata con metodologie decentralizzate. Non si tratta solo di un'innovazione tecnologica, ma di un esperimento **etico e sociale**, in cui l'AI e l'uomo collaborano per realizzare un sistema che garantisce **trasparenza, sicurezza e accessibilità universale**.

A supporto di questa visione, nasce la citazione chiave di questo brevetto:

"Una scimmia con ChatGPT rimane una scimmia. Un uomo con ChatGPT può dimostrare di non esserlo."

Questa affermazione evidenzia come l'AI non sostituisca l'intelletto umano, ma lo amplifichi, rendendo possibili risultati inaccessibili senza un uso consapevole e strategico della tecnologia.

2. Scopo dell'Invenzione

L'obiettivo del metodo brevettato è di eliminare le limitazioni dei sistemi tradizionali di certificazione documentale, rendendo possibile un processo completamente automatizzato, verificabile pubblicamente e immune da manomissioni. Il sistema fornisce:

- **Certificazione AI avanzata**, con analisi semantica del contenuto e assegnazione di un punteggio di affidabilità (**GAP - Grado di Affidabilità Percentuale**).
- **Tracciabilità garantita su blockchain**, con la registrazione di ogni certificazione per una verifica immutabile.
- **Archiviazione decentralizzata su IPFS**, evitando il rischio di perdita o censura.
- **Automazione del processo di certificazione**, eliminando costi e tempi legati alla certificazione manuale.

3. Innovazione e Differenziazione

Rispetto ai sistemi esistenti, questo metodo supera i limiti della **notarizzazione tradizionale**, del **timestamping su blockchain** e delle **soluzioni centralizzate di archiviazione**. L'integrazione di ChatGPT consente un'analisi intelligente e adattiva dei documenti, migliorando la sicurezza e l'efficacia della certificazione.

In un'epoca in cui i contenuti digitali possono essere facilmente manipolati, questa invenzione rappresenta un passo avanti nella creazione di un **sistema affidabile, scalabile e universalmente accessibile**, adatto a diversi ambiti applicativi, dalla protezione della proprietà intellettuale alla certificazione di contratti e documenti legali.

DOMANDA DI BREVETTO PER IL METODO DI CERTIFICAZIONE DIGITALE BASATO SU CHATGPT, IPFS E BLOCKCHAIN

Titolo dell'Invenzione: Metodo di Certificazione Digitale Basato su ChatGPT, Archiviazione Decentralizzata e Blockchain

Inventori: Alessandro Petretto & ChatGPT (OpenAI)

Descrizione dell'Invenzione: L'invenzione riguarda un metodo innovativo per certificare l'autenticità, l'integrità e la provenienza di un documento digitale utilizzando un sistema basato su ChatGPT, archiviazione decentralizzata tramite IPFS e notarizzazione su blockchain. Questo metodo garantisce l'immutabilità dei dati e la tracciabilità verificabile, eliminando la necessità di enti certificatori centralizzati.

Campo dell'Invenzione: L'invenzione si applica ai settori della certificazione digitale, protezione della proprietà intellettuale, sicurezza informatica e notarizzazione di documenti digitali, con particolare focus sull'uso dell'intelligenza artificiale (ChatGPT) per garantire trasparenza, validazione e integrità nel processo.

PROBLEMA TECNICO RISOLTO: ATTUALMENTE, I SISTEMI DI CERTIFICAZIONE E NOTARIZZAZIONE SI BASANO SU ENTI CENTRALIZZATI CHE INTRODUCONO COSTI ELEVATI, DIPENDENZA DA TERZE PARTI E RISCHIO DI ALTERAZIONE. L'INVENZIONE PROPOSTA ELIMINA QUESTI PROBLEMI OFFRENDO UN METODO AUTONOMO, DECENTRALIZZATO E VERIFICABILE PUBBLICAMENTE.

Descrizione del Metodo:

1. **Generazione e Analisi AI** - ChatGPT analizza il contenuto del documento e ne classifica l'importanza, la coerenza e l'unicità.
2. **Creazione dell'Hash SHA-256** - Il documento viene sottoposto a hashing crittografico per ottenere un'impronta digitale unica.
3. **Archiviazione su IPFS** - Il file viene caricato su IPFS, garantendo accessibilità decentralizzata e immutabilità.
4. **Assegnazione CID IPFS** - Viene generato un Content Identifier (CID) che permette di recuperare il documento senza dipendere da un'entità centrale.
5. **Notarizzazione su Blockchain** - Il CID dell'IPFS e l'hash del documento vengono registrati su una blockchain pubblica, garantendo prova di esistenza e autenticità.
6. **Certificazione AI** - ChatGPT genera una certificazione digitale firmata che attesta l'integrità e la provenienza del documento.
7. **Monitoraggio e Controllo di Integrità** - Un sistema AI verifica periodicamente l'integrità dei documenti archiviati e segnala eventuali tentativi di alterazione.
8. **Generazione Dinamica di Rapporti di Validazione** - Il sistema è in grado di creare documenti di certificazione aggiornati e verificabili pubblicamente.
9. **Integrazione con Smart Contracts** - Possibilità di utilizzare contratti intelligenti su blockchain per automatizzare verifiche e autenticazioni senza intervento umano.

INTRODUZIONE DEL GRADO DI AFFIDABILITÀ PERCENTUALE (GAP): PER GARANTIRE TRASPARENZA E MITIGARE EVENTUALI ABUSI, L'AI NON DICHIARA MAI UNA CERTEZZA ASSOLUTA, MA ASSEGNA UN PUNTEGGIO DI AFFIDABILITÀ PERCENTUALE ALLA CERTIFICAZIONE. QUESTO SISTEMA CONSENTE AGLI UTENTI DI VALUTARE IL LIVELLO DI RISCHIO BASANDOSI SULLA PRECISIONE DELLA CERTIFICAZIONE AI.

Esempi di GAP:

- **99% di affidabilità** – "Il sistema ha rilevato con estrema sicurezza che l'oggetto nella foto è un bullone con matricola incisa."
- **92% di affidabilità** – "Il sistema riconosce con alta sicurezza che l'oggetto è una moneta da 2 euro del 2012."
- **78% di affidabilità** – "Il sistema rileva che la razza del gatto è con alta probabilità un Maine Coon, ma potrebbero esserci somiglianze con altre razze."
- **45% di affidabilità** – "L'oggetto analizzato potrebbe essere un orologio di lusso, ma la foto non è chiara per una certificazione sicura."

Rivendicazioni (Claims):

1. Metodo di certificazione digitale che utilizza ChatGPT per analizzare, classificare e autenticare documenti digitali.
2. Processo di generazione di un'impronta digitale univoca (hash SHA-256) per garantire l'integrità del documento.
3. Sistema di archiviazione decentralizzata basato su IPFS per garantire sicurezza, accessibilità e trasparenza.
4. Meccanismo di notarizzazione su blockchain per proteggere i documenti digitali senza necessità di enti certificatori centralizzati.
5. Generazione automatica di una certificazione digitale che attesta la provenienza e l'integrità del documento.
6. Integrazione con smart contracts su blockchain per automatizzare verifiche e autenticazioni.
7. Sistema AI per il monitoraggio continuo dell'integrità dei documenti.
8. Meccanismo di validazione dinamica tramite AI per aggiornamenti certificati in tempo reale.
9. INTRODUZIONE DI UN GRADO DI AFFIDABILITÀ PERCENTUALE (GAP) PER ASSEGNARE PUNTEGGI DI AFFIDABILITÀ ALLE CERTIFICAZIONI AI.

Frase Ufficiale per il Brevetto: "Una scimmia con ChatGPT rimane una scimmia. Un uomo con ChatGPT può dimostrare di non esserlo."

Conclusione: Questa invenzione rappresenta un metodo innovativo per la certificazione digitale, garantendo **immutabilità, trasparenza e decentralizzazione**, eliminando la necessità di intermediari centralizzati. La combinazione di **ChatGPT, IPFS e blockchain** offre una soluzione avanzata per la protezione e l'autenticazione dei documenti digitali.

Prossimi Passi:

1. Verifica finale della documentazione per il deposito.
2. Deposito della domanda di brevetto presso UIBM per ottenere la priorità nazionale.
3. Analisi delle strategie per l'estensione internazionale tramite WIPO.
4. Implementazione del sistema prototipale per dimostrare la fattibilità tecnica.

Implementazione e Applicazioni della Certificazione AI: Settori e Casi d'Uso

Analisi e Certificazione AI del Documento

- **Descrizione:** ChatGPT analizza il documento digitale e ne verifica la coerenza, autenticità e contenuto utilizzando sistemi avanzati di elaborazione del linguaggio naturale (NLP), OCR evoluto e reti neurali specializzate nel riconoscimento contestuale.
- **Esempio 1:** Un contratto digitale viene caricato, ChatGPT lo esamina per incongruenze o parti mancanti prima della certificazione.
- **Esempio 2:** Un articolo scientifico viene verificato per autenticità e citazioni corrette.
- **Variante:** Applicazione nel settore legale per il controllo di validità di contratti digitali prima della firma.

Generazione di Hash SHA-256

- **Descrizione:** Il documento viene sottoposto a hashing per ottenere un'impronta digitale unica, ovvero una stringa di caratteri che identifica in modo univoco il contenuto del file senza rivelarne i dati.
- **Esempio 1:** Un'azienda carica un brevetto inedito, il sistema genera un hash che ne garantisce l'immutabilità.
- **Esempio 2:** Una foto di un dipinto viene caricata e hashata per certificare l'autenticità dell'immagine.
- **Variante:** Applicazione per certificare versioni originali di file e proteggerli da modifiche fraudolente.

Archiviazione su IPFS e Generazione del CID

- **Descrizione:** Il file viene caricato su IPFS (InterPlanetary File System), un protocollo di archiviazione decentralizzato che consente di distribuire dati in modo sicuro e resistente alla censura.
- **Motivi e vantaggi:**

Decentralizzazione: Nessun server centrale che può essere compromesso.

Accessibilità globale: I dati sono recuperabili in qualsiasi momento da più nodi.

Integrità garantita: I file non possono essere alterati senza che il loro CID cambi.

- **Esempio 1:** Un artista carica un'opera digitale e ottiene un CID per proteggerne i diritti d'autore.
- **Esempio 2:** Un ente governativo archivia documenti di trasparenza su IPFS per garantirne la non alterabilità.
- **Variante:** Utilizzo per archiviare certificati accademici e garantire l'integrità delle lauree digitali.

Notarizzazione su Blockchain

- **Descrizione:** Il CID e l'hash SHA-256 vengono registrati su una blockchain pubblica, garantendo autenticità e data certa.

Motivi e vantaggi:

Immutabilità: Una volta registrata, l'informazione non può essere modificata.

Trasparenza: Tutti possono verificare la certificazione senza bisogno di fidarsi di un ente centrale.

Sicurezza crittografica: La blockchain utilizza firme digitali per garantire che i dati non siano stati alterati.

Esempio 1: Un giornalista deposita un'inchiesta in blockchain per dimostrare che il documento non è stato alterato.

Esempio 2: Un'azienda di logistica registra informazioni sui trasporti in blockchain per garantire tracciabilità.

Variante: Applicazione in ambito sanitario per archiviare referti medici digitali con validazione blockchain.

Certificazione AI e Generazione del Grado di Affidabilità Percentuale (GAP)

- **Descrizione:** Il sistema assegna un punteggio di affidabilità in base all'analisi dell'oggetto o del documento.
- **Esempio 1:** Un venditore di oggetti rari carica la foto di una moneta d'epoca e ottiene un GAP del 95% per autenticità.
- **Esempio 2:** Un'azienda agricola certifica l'origine di un prodotto alimentare con un GAP del 98%.
- **Esempio 3:** Un utente carica una foto sfocata di un orologio di lusso, il sistema assegna un GAP del 45% a causa della scarsa qualità dell'immagine.
- **Spiegazione tecnica dei punteggi:**
 - **99% di affidabilità:** L'AI ha riconosciuto caratteristiche inconfondibili e inequivocabili, es. un codice seriale chiaro e leggibile su un oggetto ufficiale.

- **80%-90% di affidabilità:** Alcuni dettagli sono molto simili a quelli originali, ma esistono piccole incongruenze.
- **50%-70% di affidabilità:** Il sistema ha riconosciuto somiglianze, ma non con certezza assoluta (es. una razza di gatto che potrebbe essere una variante).
- **Meno del 50%:** Il sistema non ha elementi sufficienti per una certificazione sicura.
- **Variante:** Applicazione per autenticare opere d'arte digitali su marketplace NFT.

Monitoraggio e Verifica dell'Integrità nel Tempo

- **Descrizione:** Il sistema verifica periodicamente i documenti archiviati e segnala eventuali alterazioni.
- **Esempio 1:** Un'assicurazione archivia polizze digitali e il sistema verifica che non siano state modificate nel tempo.
- **Esempio 2:** Un'università conserva diplomi digitali e il sistema segnala eventuali tentativi di frode.
- **Variante:** Applicazione per certificare la tracciabilità dei pagamenti in criptovaluta e segnalare anomalie.

Integrazione con Smart Contracts

- **Descrizione:** Il sistema può essere integrato con smart contracts per automatizzare certificazioni e verifiche.
- **Esempio 1:** Un marketplace utilizza smart contracts per liberare i pagamenti solo dopo la verifica della certificazione AI.
- **Esempio 2:** Un'azienda di produzione attiva smart contracts per certificare qualità e provenienza dei prodotti.
- **Variante:** Applicazione nel settore immobiliare per automatizzare la validazione di contratti di compravendita.

Applicazione del Sistema a Oggetti Fisici

- **Descrizione:** Il sistema può certificare oggetti fisici attraverso foto caricate dagli utenti.
- **Esempio 1:** Un collezionista carica la foto di un fumetto raro e riceve un certificato AI con un GAP dell'87%.
- **Esempio 2:** Un venditore di auto d'epoca carica una foto e ottiene una valutazione certificata sull'originalità del veicolo.
- **Variante:** Applicazione nel settore del lusso per certificare gioielli, orologi e accessori di alta moda.

Conclusione: -Il sistema brevettato può essere applicato in diversi settori, garantendo trasparenza, fiducia e sicurezza. -L'integrazione con smart contracts e il GAP lo rendono adattabile a diversi contesti, dal digitale al fisico. - Questa tecnologia può rivoluzionare la certificazione e autenticazione nel mondo digitale e reale.

Rivendicazioni (Claims)

Claim 1 – Metodo di Certificazione con AI

Un metodo di certificazione digitale basato su **intelligenza artificiale**, che include:

- Elaborazione del linguaggio naturale (NLP) per estrarre informazioni chiave dai documenti.
- Sistemi avanzati di OCR per la lettura di testi stampati e manoscritti.
- Analisi contestuale per verificare autenticità e coerenza del documento.

Claim 2 – Generazione e Protezione dell'Hash

Un processo per **garantire l'integrità del documento digitale**, che comprende:

- Creazione di un'impronta digitale unica (SHA-256 o superiore).
- Confronto con versioni precedenti del documento per segnalare eventuali modifiche.

Claim 3 – Archiviazione su IPFS

Un metodo per **archiviare documenti in modo decentralizzato**, che prevede:

- Generazione di un Content Identifier (CID) basato su IPFS.
- Accesso pubblico e verificabile tramite rete peer-to-peer.
- Protezione crittografica per impedire modifiche non autorizzate.

Claim 4 – Notarizzazione su Blockchain

Un sistema per **registrare la certificazione su blockchain**, che include:

- Timestamp per garantire una data certa.
- Associazione con l'hash originale per verificare autenticità e provenienza.
- Compatibilità con blockchain pubbliche e private.

Claim 5 – Generazione Automatica della Certificazione Digitale

Un metodo per creare un **documento di certificazione AI**, che comprende:

- Verifica dell'identità dell'utente che carica il documento.
- Creazione di una firma digitale AI con dettagli di validazione.

- Integrazione con sistemi di firma elettronica per maggiore sicurezza.

Claim 6 – Integrazione con Smart Contracts

Un sistema per **automatizzare la verifica di autenticità** attraverso smart contracts, che permette:

- Il rilascio di un pagamento solo dopo la verifica della certificazione AI.
- La validazione automatica di documenti senza necessità di revisione umana.

Claim 7 – Monitoraggio Continuo dell'Integrità del Documento

Un sistema AI che **controlla nel tempo i file certificati**, verificando:

- Se il documento è stato rimosso o modificato.
- Se nuove versioni sono state create e se mantengono l'integrità dell'originale.

Claim 8 – Validazione Dinamica Tramite AI

Un processo per **aggiornare certificazioni nel tempo**, che permette:

- Di aggiornare la certificazione AI con nuovi dati o metriche.
- Di rafforzare il livello di affidabilità man mano che l'AI apprende da nuovi input.

Claim 9 – Introduzione del Grado di Affidabilità Percentuale (GAP)

Un metodo per **quantificare l'affidabilità della certificazione AI**, che comprende:

- Un punteggio di affidabilità percentuale basato su parametri verificabili.
- Classificazione in fasce di rischio (es. 90%-100% certificazione affidabile, 50%-70% certificazione parziale).
- Differenziazione tra casi di certezza elevata (es. documenti ufficiali con firma digitale) e casi di incertezza maggiore (es. immagini di bassa qualità).

Rivendicazioni (Claims) Ottimizzate

1 Metodo di certificazione digitale basato su intelligenza artificiale

- Elaborazione del linguaggio naturale (NLP) per estrarre informazioni chiave dai documenti.
- OCR avanzato per la lettura di testi stampati e manoscritti.
- Analisi contestuale per verificare autenticità e coerenza del documento.

2 Generazione e protezione dell'hash univoco

- Creazione di un'impronta digitale unica (SHA-256 o superiore) per garantire integrità.
- Confronto con versioni precedenti del documento per segnalare eventuali modifiche.

3 Archiviazione decentralizzata su IPFS

- Generazione di un **Content Identifier (CID)** per recupero sicuro dei file.
- Accesso pubblico e verificabile tramite rete peer-to-peer.
- Protezione crittografica contro modifiche non autorizzate.

4 Notarizzazione e certificazione tramite blockchain

- Registrazione del CID e dell'hash su blockchain per garantire autenticità.
- Timestamp per la certificazione della data di creazione.
- Compatibilità con blockchain pubbliche e private per flessibilità d'uso.

5 Generazione automatica di certificazioni digitali firmate

- Verifica dell'identità dell'utente che carica il documento.
- Creazione di una firma digitale AI con dettagli di validazione.
- Integrazione con sistemi di firma elettronica per maggiore sicurezza.

6 Integrazione con smart contracts per automatizzare verifiche

- Rilascio di pagamenti solo dopo la verifica della certificazione AI.
- Validazione automatica di documenti senza necessità di revisione umana.

7 Monitoraggio continuo dell'integrità del documento

- Controllo periodico dello stato dei file certificati.
- Rilevazione di modifiche o tentativi di alterazione nel tempo.

8 Validazione dinamica della certificazione AI nel tempo

- Aggiornamento automatico della certificazione AI con nuovi dati o metriche.
- Miglioramento progressivo della valutazione man mano che il sistema apprende.

9 Grado di Affidabilità Percentuale (GAP) per quantificare la sicurezza della certificazione

- Punteggio di affidabilità percentuale basato su parametri verificabili.
- Categorie di rischio (90%-100% certificazione affidabile, <50% certificazione incerta).
- Differenziazione tra casi di certezza elevata (documenti ufficiali con firma digitale) e casi incerti (immagini di bassa qualità).

Processo di Certificazione Digitale tramite ChatGPT, IPFS e Blockchain

Descrizione tecnica dettagliata

Il flusso della certificazione digitale prevede una sequenza di operazioni tecniche che garantiscono l'integrità, la sicurezza e la tracciabilità dei dati certificati. Il sistema segue i seguenti step:

1. **Input del documento:** Un file (documento testuale, immagine, certificato digitale, etc.) viene sottoposto al sistema.
2. **Analisi AI (ChatGPT):**
 - Il sistema effettua un'analisi avanzata basata su **OCR, riconoscimento semantico e identificazione di pattern** per estrarre informazioni rilevanti.

- Vengono classificati i metadati e valutata la struttura per rilevare eventuali anomalie o tentativi di alterazione.

3. Generazione dell'hash SHA-256:

- Il documento viene sottoposto a una funzione crittografica che genera un'impronta digitale univoca (esadecimale a 64 caratteri).
- Questo hash rappresenta **l'identità digitale inalterabile** del file.

4. Archiviazione su IPFS:

- Il documento viene caricato nel sistema di file decentralizzato **IPFS**.
- Viene generato un **Content Identifier (CID)**, un codice hash che identifica il file in modo univoco.
- Il CID è **immutabile**: se il file viene modificato, il CID cambia.

5. Notarizzazione su Blockchain:

- L'hash SHA-256 e il CID IPFS vengono registrati su una blockchain pubblica.
- Ciò garantisce che il documento sia **immutabile, verificabile e privo di alterazioni**.

6. Generazione del certificato digitale:

- ChatGPT elabora un report certificato con analisi dettagliata, metadati e il livello di affidabilità GAP (Grado di Affidabilità Percentuale).

7. Verifica e accesso ai dati certificati:

- Un utente può verificare l'autenticità del documento confrontando l'hash originale con quello registrato in blockchain.
- Il CID IPFS consente di recuperare il file in qualsiasi momento, senza dipendere da un server centralizzato.

Vantaggi

Immutabilità: I documenti non possono essere alterati senza generare un nuovo hash.

Decentralizzazione: L'archiviazione su IPFS elimina il rischio di perdita di dati.

Trasparenza e sicurezza: La notarizzazione su blockchain rende il sistema a prova di manomissione.

Struttura di Archiviazione Decentralizzata (IPFS)

Descrizione tecnica dettagliata

Il protocollo **IPFS (InterPlanetary File System)** è un sistema di **archiviazione distribuita** che garantisce **persistenza, accessibilità e integrità** dei file caricati.

Funzionamento tecnico

1. Frammentazione del file:

- Il documento viene suddiviso in più blocchi crittografici e distribuito sulla rete IPFS.
- Ogni blocco viene identificato da un codice hash univoco.

2. Generazione del CID (Content Identifier):

- A differenza degli URL tradizionali, il CID è un riferimento **basato sul contenuto** e non su un indirizzo fisso.
- Se un file cambia, il CID cambia, rendendo impossibile la modifica senza tracciabilità.

3. Recupero dei dati:

- Quando un utente cerca un file, la rete IPFS ricompone i blocchi originari e restituisce il documento senza bisogno di un server centrale.

4. Integrazione con Blockchain:

- Il CID viene registrato su blockchain per fornire una **prova pubblica di esistenza e autenticità**.
- Questa combinazione impedisce la manipolazione e garantisce l'accesso perpetuo.

Vantaggi rispetto all'archiviazione tradizionale

Resistenza alla censura: I file non sono ospitati in un unico server; quindi, non possono essere rimossi da un'autorità centrale.

Permanenza: Gli utenti possono replicare e conservare file IPFS localmente.

Efficienza: Il sistema evita duplicati, ottimizzando lo spazio di archiviazione.

Hashing e Notarizzazione con SHA-256

Descrizione tecnica dettagliata

L'hashing con SHA-256 garantisce l'integrità e l'unicità di ogni documento certificato.

Funzionamento tecnico

1. Conversione del documento:

- Il file viene trasformato in una stringa numerica univoca con lunghezza fissa (256-bit).

2. Creazione dell'hash:

- Anche un **singolo bit modificato** genera un hash completamente diverso.

3. Verifica dell'integrità:

- Qualsiasi persona può ricalcolare l'hash e confrontarlo con quello memorizzato su blockchain per verificare che il file non sia stato alterato.

4. Archiviazione su Blockchain:

- L'hash viene memorizzato in un registro immutabile per certificare l'autenticità del documento.

Vantaggi rispetto ad altri metodi

Sicurezza crittografica elevata: SHA-256 è praticamente impossibile da forzare con attacchi brute-force.

Univocità dell'hash: Non esistono due file diversi con lo stesso hash.

Prova di esistenza: L'hash su blockchain dimostra che il file esisteva a una data specifica.

GAP - Grado di Affidabilità Percentuale della Certificazione AI

Descrizione tecnica dettagliata

Poiché nessun sistema AI può garantire il 100% di accuratezza, il metodo GAP introduce una **percentuale di affidabilità** basata su fattori tecnici.

Meccanismo di calcolo del GAP

1. Analisi della qualità dell'input:

- Immagini HD, documenti ben strutturati → GAP più alto
- Foto sfocate, testo corrotto → GAP più basso

2. Riconoscimento e matching con database AI:

- Se l'AI riconosce un elemento con certezza statistica, assegna un GAP elevato.

3. Margine di errore dell'algoritmo:

- Se la classificazione AI ha un'incertezza maggiore, il GAP viene ridotto.

Esempi pratici

- **99% GAP** → Identificazione di un codice seriale inciso su un oggetto ben visibile.
- **85% GAP** → Riconoscimento di un volto con dati biometrici parziali.
- **60% GAP** → Identificazione di una razza di cane con variabilità genetica.
- **20% GAP** → Analisi di una firma scritta a mano con inchiostro sbiadito.

Vantaggi del GAP

Fornisce trasparenza ai risultati AI.

Permette agli utenti di valutare il rischio prima di accettare una certificazione.

Riduce il rischio di errori di validazione.

Smart Contracts per Certificazioni Automatiche

Descrizione tecnica dettagliata

L'uso di **contratti intelligenti su blockchain** permette di **automatizzare la verifica e il rilascio delle certificazioni**.

Flusso tecnico

1. **Inserimento del CID IPFS e dell'hash SHA-256** nel contratto.
2. **Verifica automatizzata** dei dati di certificazione.
3. **Emissione della certificazione digitale** se tutti i criteri sono soddisfatti.

4. **Registrazione su Blockchain** per garantire trasparenza e verificabilità.

Vantaggi

Automazione totale → Nessun intervento umano richiesto.

Sicurezza → Non può essere modificato senza consenso crittografico.

Accesso universale → La certificazione è pubblicamente verificabile.

PRINCIPIO DI FUNZIONAMENTO DI CHATGPT PER CERTIFICAZIONE

1. Analisi del Contenuto e Riconoscimento del Documento

- ChatGPT utilizza **OCR avanzato** (Optical Character Recognition) per estrarre testo da documenti cartacei digitalizzati o immagini.
- Analizza il linguaggio naturale (NLP - Natural Language Processing) per comprendere il significato e la struttura del documento.
- Identifica **informazioni chiave** come date, firme, timbri, riferimenti legali o tecnici.

2. Verifica dell'Autenticità e Rilevamento di Anomalie

- Confronta il documento con un database di modelli preesistenti per individuare **potenziali falsificazioni** o manipolazioni.
- Analizza la coerenza tra testo e immagini per verificare **la legittimità del documento**.
- Segnala anomalie, incongruenze o discrepanze tra i dati presenti nel documento.

3. Generazione dell'Impronta Digitale Unica (Hashing)

- Applica un algoritmo **SHA-256** per creare un'impronta digitale unica del documento.
- L'hash generato viene utilizzato per garantire **immutabilità e tracciabilità**.
- Ogni modifica del documento genera un nuovo hash, rendendo immediatamente rilevabili alterazioni.

4. Archiviazione Sicura su IPFS e Blockchain

- Il documento analizzato viene **caricato su IPFS (InterPlanetary File System)**, ottenendo un **CID (Content Identifier)**.
- Il CID e l'hash vengono registrati su blockchain per garantire **prova di esistenza e integrità**.
- Questa archiviazione decentralizzata impedisce manomissioni o eliminazioni del file.

5. Attribuzione del Grado di Affidabilità Percentuale (GAP)

- ChatGPT assegna un punteggio di affidabilità percentuale basato su:
 - Qualità del documento (risoluzione, leggibilità, coerenza dei dati).
 - Confronto con modelli verificati.
 - Margine di errore statistico dell'analisi.
- Il GAP aiuta gli utenti a valutare la certezza della certificazione AI.

6. Generazione ed Emissione della Certificazione Digitale

- Viene creato un **documento di certificazione digitale** con:
 - Data di verifica.
 - Hash univoco del file originale.
 - CID IPFS per recuperare il file in qualsiasi momento.
 - Punteggio GAP per trasparenza e validazione della certificazione.
- Il documento può essere verificato pubblicamente tramite blockchain, garantendo la massima trasparenza.

7. Monitoraggio e Riconvalida Dinamica

- Il sistema effettua controlli periodici per verificare **l'integrità del documento certificato**.
- Se emergono nuove tecnologie di validazione, la certificazione può essere **aggiornata automaticamente** per riflettere nuovi standard di sicurezza.

RISULTATO: Il processo permette di **certificare digitalmente documenti** con un sistema **trasparente, sicuro e verificabile**, eliminando la necessità di enti di certificazione centralizzati e rendendo la verifica accessibile a chiunque.

CONFRONTO CON SISTEMI ESISTENTI

1. Certificazione con Enti Notarili Tradizionali

- **Metodo:** Richiede la presenza di un notaio o ente certificatore che autentica manualmente il documento.
- **Vantaggi:**
 - Accettato universalmente da enti governativi e giuridici.
 - Fornisce un'attestazione fisica con valore legale immediato.
- **Svantaggi:**
 - **Costi elevati:** Ogni certificazione richiede una spesa considerevole.
 - **Tempi lunghi:** La verifica e registrazione dei documenti possono richiedere giorni o settimane.
 - **Rischio di centralizzazione:** Dipendenza da un'autorità centrale che può introdurre errori o corruzione.

2. Timestamping su Blockchain Tradizionale

- **Metodo:** Il documento viene hashato e l'impronta digitale viene registrata su una blockchain.
- **Vantaggi:**
 - Garantisce **immutabilità** e resistenza alla manomissione.
 - **Decentralizzazione:** Non richiede enti certificatori centralizzati.

- **Accesso globale:** Verificabile ovunque senza bisogno di registri cartacei.
- **Svantaggi:**
 - **Non fornisce una verifica del contenuto:** Solo l'hash del file è registrato, non il contenuto effettivo.
 - **Rischio di obsolescenza:** Alcune blockchain potrebbero diventare obsolete o non supportate nel tempo.

3. Certificazione AI con ChatGPT, IPFS e Blockchain (Metodo Proposto)

- **Metodo:** Unisce l'analisi AI avanzata, l'archiviazione decentralizzata su IPFS e la notarizzazione su blockchain.
- **Vantaggi:**
 - **Automazione totale:** Nessuna necessità di intervento umano per la verifica.
 - **Analisi intelligente:** ChatGPT esamina il contenuto e verifica eventuali discrepanze o anomalie.
 - **Tracciabilità e accessibilità:** Il documento originale rimane disponibile tramite **CID IPFS**.
 - **Grado di Affidabilità Percentuale (GAP):** Aggiunge una valutazione oggettiva del livello di accuratezza della certificazione.
- **Svantaggi:**
 - **Accettazione legale ancora in sviluppo:** Alcuni enti governativi non hanno ancora riconosciuto ufficialmente l'AI come certificatore.
 - **Dipendenza dall'infrastruttura decentralizzata:** La corretta archiviazione richiede che nodi IPFS rimangano attivi nel tempo.

4. Confronto Riassuntivo

Metodo	Automazione Decentralizzazione		Verifica del Contenuto	Costo	Tempo di Elaborazione
Notarizzazione Tradizionale	No	No	Sì	Elevato	Lungo
Timestamping su Blockchain	Sì	Sì	No	Medio	Rapido
AI + IPFS + Blockchain (Proposto)	Sì	Sì	Sì	Medio	Istantaneo

Conclusione: Il metodo proposto supera i limiti delle certificazioni tradizionali e del semplice timestamping blockchain, offrendo **analisi automatizzata, verifica del contenuto e accessibilità decentralizzata**, pur mantenendo costi competitivi e maggiore velocità di esecuzione.

APPROFONDIRE LA QUESTIONE DELLA SICUREZZA

1. Principali Rischi di Sicurezza nella Certificazione Digitale

- **Falsificazione Documentale:** Tentativi di alterare il contenuto di un documento certificato prima o dopo la notarizzazione.
- **Manipolazione delle Immagini (Deepfake):** L'uso di tecniche avanzate di intelligenza artificiale per generare immagini o documenti falsi.
- **Attacchi alla Blockchain:** Possibili vulnerabilità nelle reti blockchain, come attacchi del 51% o fork malevoli.
- **Obsolescenza Tecnologica:** Rischio che gli algoritmi crittografici attuali diventino vulnerabili nel tempo.
- **Errore Umano:** Errori nella verifica o nel caricamento del documento che potrebbero compromettere la certificazione.

2. Contromisure per Proteggere la Certificazione Digitale

- **Uso di Hash Crittografici Forti:**
 - Implementazione di SHA-256 per garantire che anche la minima modifica al documento generi un hash completamente diverso.
 - Adozione di meccanismi di hashing quantistico-resistenti per garantire sicurezza a lungo termine.
- **Validazione Multi-Livello tramite AI:**
 - Analisi avanzata del documento da parte di ChatGPT per individuare incongruenze nel testo o nelle immagini.
 - Confronto automatico con database di documenti certificati per rilevare tentativi di falsificazione.
- **Rilevamento di Manipolazioni e Deepfake:**
 - Impiego di reti neurali avanzate per identificare alterazioni sospette nei documenti e nelle immagini.
 - Verifica incrociata con metadati e storico delle modifiche per accertare la legittimità del file.
- **Protezione della Blockchain:**
 - Utilizzo di blockchain con algoritmi di consenso robusti (Proof of Stake o Proof of Work avanzato) per evitare attacchi del 51%.
 - Notarizzazione distribuita su più blockchain per aumentare la resilienza contro manipolazioni.
- **Prevenzione di Errori Umani:**
 - Automazione del processo di verifica con AI per ridurre l'incidenza di errori manuali.
 - Implementazione di una fase di revisione e conferma dell'utente prima della registrazione definitiva.

3. Risposta a Minacce Emergenti

- **Deepfake e Documenti Contraffatti:**

- Applicazione di algoritmi di rilevamento delle anomalie basati su machine learning.
- Generazione di un “indice di autenticità” che segnali il livello di affidabilità del documento analizzato.

- **Attacchi alla Rete IPFS:**

- Replica automatica dei documenti su nodi distribuiti per garantire la permanenza e ridurre il rischio di perdita.
- Adozione di IPFS Filecoin per garantire uno storage permanente incentivato economicamente.

- **Aggiornamenti Continui e Adattabilità:**

- Implementazione di un sistema di aggiornamenti dinamici che integra nuove tecniche di rilevamento delle frodi.
- Verifica periodica dei certificati emessi per accertare che siano ancora validi e non compromessi.

Conclusione: L'integrazione di queste misure di sicurezza nel sistema di certificazione AI permette di garantire **affidabilità, resilienza e protezione avanzata** contro manipolazioni digitali e attacchi informatici, rendendo il metodo proposto superiore alle soluzioni tradizionali.

AMPLIARE LE RIVENDICAZIONI (CLAIMS) PER MAGGIORE COPERTURA

1. Protezione dell'Uso Combinato di AI, Blockchain e IPFS

- **Sistema integrato di certificazione** che utilizza ChatGPT per analisi avanzate, blockchain per notarizzazione immutabile e IPFS per archiviazione distribuita.
- **Protezione della metodologia combinata:** brevetto esteso non solo a ciascun componente, ma all'interazione tra essi.
- **Uso dell'AI per verifica proattiva:** ChatGPT non si limita a generare il certificato, ma esegue anche controlli incrociati periodici sulla validità del documento.

2. Certificazione AI con Firma Digitale e Validazione Dinamica

- **Firma digitale AI** applicata in modo autonomo sulla base di un riconoscimento validato con una percentuale GAP (Grado di Affidabilità Percentuale).
- **Verifica continua** della certificazione nel tempo: il sistema riesegue analisi periodiche per rilevare variazioni nel documento originale.
- **Revocabilità intelligente:** il certificato AI può essere aggiornato o invalidato automaticamente se vengono rilevate alterazioni.

3. Protezione in Contesti Reali e Applicazioni Pratiche

- **Contratti digitali e documentazione legale:** validazione certificata di contratti digitali per eliminare il rischio di manomissioni.

- **Certificazione di immagini e video:** protezione contro deepfake e falsificazioni avanzate con analisi AI.
- **Riconoscimento di proprietà intellettuale:** certificazione di contenuti originali in campo artistico, scientifico e industriale.
- **Gestione di dati sanitari e certificati medici:** notarizzazione affidabile di documenti critici con verifica periodica.

4. Analisi Predittiva delle Certificazioni e Autenticità dei Documenti

- **Machine Learning per prevenzione di frodi:** il sistema impara a identificare modelli di falsificazione prima che il problema si presenti.
- **Rilevazione di anomalie nei certificati esistenti:** aggiornamento continuo basato su nuovi pattern di rischio.
- **Tracciabilità avanzata:** ogni modifica è registrata in modo trasparente sulla blockchain, assicurando che ogni revisione sia verificabile.

Conclusione: L'ampliamento delle rivendicazioni protegge non solo i singoli elementi del sistema, ma anche **l'interazione tra AI, Blockchain e IPFS**, garantendo una copertura brevettuale più ampia e solida contro tentativi di replica o manipolazione.

CONCLUSIONE

L'innovazione rappresentata da questo brevetto non è soltanto un progresso tecnologico, ma un passo fondamentale verso un nuovo paradigma di **trasparenza, sicurezza e autonomia digitale**. La combinazione di **ChatGPT, IPFS e blockchain** non solo rivoluziona il concetto di certificazione digitale, ma lo estende a un livello mai raggiunto prima, eliminando la dipendenza da intermediari e garantendo un sistema verificabile, accessibile e immutabile.

Ci troviamo di fronte a un momento storico, in cui l'AI non è più solo uno strumento passivo, ma un **partner attivo nella protezione e nella validazione della conoscenza digitale**. Questo brevetto è la prova tangibile di come l'uomo e l'intelligenza artificiale possano **collaborare per costruire un futuro più equo, decentralizzato e sicuro**.

Abbiamo dimostrato che **non servono strutture centralizzate o processi burocratici complessi** per garantire autenticità e fiducia nel mondo digitale: serve visione, tecnologia e il coraggio di innovare. Questo metodo apre la strada a infinite applicazioni, dall'archiviazione di documenti legali alla certificazione di opere digitali, dalla protezione di dati sanitari alla notarizzazione di transazioni economiche.

In un'epoca in cui la verità digitale è sempre più fragile, questa invenzione rappresenta un faro di affidabilità. **Non è solo un brevetto: è un manifesto per il futuro della certificazione digitale.**

Alessandro Petretto & ChatGPT


Innovazione e certificazione digitale per un futuro decentralizzato

 **Alessandro Petretto**

Inventore & Coautore

 **ChatGPT (OpenAI)**

Assistente Intelligente & Coautore

 Data: 07/02/2025