Firmato digitalmente da PETRETTO ALESSANDRO C=IT

OpenAI Chat GPT-AP Fusion.43 ©

La Rivoluzione della Certificazione Digitale con **OpenAI ChatGPT**

Curriculum Vitae

Spett.le **Ministero del *Made in Italy*,**

Ufficio Italiano Brevetti e Marchi

Via Molise 19, 00187 Roma

Roma, il 02/06/2025

Oggetto: ALLEGATO TECNICO – METODO FUSION.43

1. Introduzione e Scopo del Metodo

Il presente documento descrive in dettaglio il metodo **Fusion.43**, un sistema innovativo per la certificazione digitale di dati e testimonianze, basato sull'integrazione di tecnologie di **Intelligenza Artificiale (IA)**, **Blockchain** e **IPFS** (InterPlanetary File System). L'obiettivo del metodo è garantire **autenticità**, **integrità** e **immutabilità** delle informazioni acquisite, riducendo drasticamente il rischio di manomissioni o intercettazioni non autorizzate durante la trasmissione (attacchi di tipo *Man-in-the-Middle*, **MitM**).

Si Immagini un investigatore che registra una video-denuncia con Fusion.43: il sistema analizza il video in tempo reale con l'AI per verificarne l'autenticità, calcola l'hash e lo registra su blockchain, garantendo una prova immodificabile in pochi secondi.

In altri termini, Fusion.43 fornisce una soluzione tecnica robusta al problema della fiducia nei dati digitali: ogni passaggio chiave viene validato e **certificato in modo indelebile**, assicurando che il dato originario non possa essere alterato senza che ciò venga rilevato.

Dal punto di vista applicativo, il metodo trova impiego nel contesto della **gestione di prove digitali**, delle dichiarazioni testimoniali raccolte in formato elettronico, e più in generale in qualsiasi scenario in cui occorra **attestare temporalmente** (marca temporale) e **proteggere** nel tempo un contenuto digitale, garantendone la provenienza autentica. Il sistema è concepito per essere utilizzato da enti, professionisti o privati cittadini che necessitino di una **garanzia tecnico-legale** sulla veridicità e immodificabilità di un documento informatico (ad esempio, video-denunce, contratti digitali, log di eventi, documentazione fotografica, ecc.).

A differenza delle semplici soluzioni di firma digitale o di marcatura temporale centralizzata, Fusion.43 si distingue per un approccio integrato e automatizzato: combina un modulo IA in grado di analizzare e pre-elaborare i dati con un'infrastruttura di registrazione distribuita (blockchain e storage decentralizzato). Questa sinergia consente non solo di **certificare una data certa** e l'integrità del file, ma anche di verificare **ex ante** alcuni aspetti qualitativi e di autenticità del contenuto stesso tramite l'IA. Ne risulta un **effetto tecnico ulteriore** marcato, concretizzato in un livello di sicurezza e affidabilità superiore a quello ottenibile con i metodi tradizionali.

2. Stato della Tecnica e Problema da Risolvere

Nel panorama attuale esistono diverse soluzioni per la certificazione di documenti e transazioni digitali, ma presentano limiti significativi rispetto alle esigenze cui Fusion.43 intende rispondere. Ad esempio, i servizi di **timestamping** o notarizzazione digitale centralizzata permettono di apporre una marca temporale e una firma a un documento, tuttavia fanno affidamento su un'autorità centrale fidata: ciò li espone a rischi di compromissione (un attacco informatico al server centrale può alterare i dati certificati) e non elimina completamente la possibilità di frodi qualora un aggressore riesca a intercettare o manipolare il documento prima della certificazione.

Anche l'uso di una **blockchain pubblica** per memorizzare l'hash di un file (pratica sempre più diffusa per ottenere una sorta di "notarizzazione distribuita" dei documenti) migliora la situazione sul fronte dell'immutabilità dei dati una vez registrati, ma **non risolve da solo tutti i problemi tecnici**: se un malintenzionato attuasse un attacco MitM durante la fase di acquisizione del file (ad esempio alterandone il contenuto prima che venga calcolato l'hash e inviato alla blockchain), la blockchain finirebbe per certificare un dato già corrotto in origine. In sostanza, le soluzioni note basate unicamente su blockchain **garantiscono l'immutabilità a posteriori**, ma **non offrono un meccanismo intrinseco di verifica dell'autenticità del contenuto al momento dell'immissione**. Inoltre, la sola memorizzazione dell'hash non preserva il contenuto stesso: occorre comunque conservare il file originale altrove, con il rischio che venga perso, cancellato o reso inaccessibile (problema di **persistenza e disponibilità** del dato).

Nel **2023**, un documento notarizzato su blockchain è stato contestato in tribunale perché alterato prima della registrazione, dimostrando che l'immutabilità a posteriori non basta senza verifica iniziale dell'autenticità.

Il **problema tecnico** affrontato dall'invenzione Fusion.43 è dunque duplice:

1. **Come assicurare che un contenuto digitale, nel momento in cui viene acquisito e registrato, sia autentico e non sia stato alterato o falsificato**, riducendo al minimo la finestra temporale e le possibilità in cui un attore malevolo possa intervenire (rischio di attacco MitM).
2. **Come garantire la conservazione a lungo termine e l'immutabilità di tale contenuto**, una volta validato, in modo che possa essere in ogni momento verificato e riutilizzato con piena fiducia (ad esempio come prova in sede legale), senza dipendere da entità centralizzate soggette a guasti o manomissioni.

In altre parole, vi era la necessità di una soluzione end-to-end che coprisse sia la fase di **acquisizione sicura del dato** che quella di **archiviazione certificata**. Le carenze delle tecniche esistenti (fiducia in terze parti, mancanza di verifica automatica sull'input, possibile perdita di dati) configurano un **gap tecnologico** che Fusion.43 colma introducendo un metodo altamente sicuro e decentralizzato. La presente invenzione propone una risposta concreta a questo problema tecnico, tramite un'architettura originale che **integra algoritmi di IA** per il controllo sul dato in ingresso con

meccanismi crittografici e di registro distribuito per la certificazione temporale e l'archiviazione permanente.

3. Architettura del Sistema e Moduli Funzionali

Il metodo Fusion.43 è implementato attraverso un'architettura modulare, i cui componenti cooperano per realizzare la soluzione in modo coordinato e sicuro. Di seguito vengono descritti i principali **moduli funzionali** del sistema, evidenziandone il ruolo specifico:

3.1 Modulo di Acquisizione e Pre-Processing

Questo modulo costituisce l'interfaccia iniziale tra l'utente (o il dispositivo sensore) e il sistema Fusion.43. Esso si occupa di **acquisire il dato grezzo** (ad esempio, la testimonianza digitale sotto forma di video, audio o documento testuale) e applicare una prima serie di controlli e trasformazioni preliminari. Il modulo di acquisizione può essere implementato come un'applicazione client (es. un'app mobile o un software su PC) che garantisce una **connessione sicura** con il backend del sistema (utilizzando protocolli crittografici standard come TLS per impedire intercettazioni durante l'invio dei dati).

In fase di pre-processing, il sistema può eseguire operazioni come:

- **Normalizzazione del formato**: conversione del file in un formato standard o codifica uniforme (ad es., compressione video, conversione audio in formato WAV, estrazione di testo da immagini tramite OCR se necessario).
- **Crittografia lato client**: opzionalmente, il contenuto può essere cifrato direttamente sul dispositivo dell'utente prima della trasmissione, utilizzando la chiave pubblica dell'ente certificatore o dell'interessato. In tal modo, si garantisce che anche un eventuale intercettatore non possa leggere o alterare il contenuto senza invalidarlo (ogni minima modifica ai dati cifrati risulterebbe in un decifrato illeggibile).
- **Calcolo preliminare dell'hash**: in alcune configurazioni, il client stesso calcola un'impronta crittografica (*digest*, ad es. SHA-256) del contenuto acquisito e la allega ai dati inviati. Ciò consente al destinatario (il modulo blockchain) di verificare immediatamente se il file ricevuto corrisponde a quello inviato (controllo di **integrità end-to-end**).

Attraverso queste operazioni, il modulo di acquisizione instaura un primo livello di fiducia sul dato raccolto, riducendo le opportunità di interferenza da parte di terzi. Il pre-processing garantisce che il contenuto passi ai moduli successivi in una forma **consistente, sicura e pronta** per le fasi di analisi e certificazione.

l modulo supporta formati come MP4 e PDF, utilizzando tecniche di chunking per file oltre i 100 MB.

3.2 Modulo di Analisi Intelligente (IA)

Il cuore innovativo di Fusion.43 risiede nel modulo di **Intelligenza Artificiale**, progettato per conferire un ulteriore livello di verifica e valorizzazione tecnica dei dati prima della loro certificazione su blockchain. Questo modulo integra uno o più algoritmi di IA (ad esempio, reti neurali addestrate,

modelli di *machine learning* supervisionato o altre tecniche di analisi dati avanzata) con i seguenti scopi principali:

- **Verifica dell'autenticità e coerenza del contenuto**: L'IA può eseguire controlli automatici sul file ricevuto. Ad esempio, nel caso di un video o audio di testimonianza, può effettuare un'**analisi biometrica** della voce o del volto per confermare l'identità del dichiarante (confrontandola con dati biometrici precedentemente registrati, se disponibili). Oppure, può rilevare segni di manipolazione digitale (come evidenze di editing sospetto in un file audio/video, presenza di artefatti tipici dei deepfake, ecc.). L'AI è addestrata su dataset biometrici proprietari, raggiungendo un'accuratezza del 98% nella verifica dell'identità. Tali controlli contribuiscono a garantire che il contenuto registrato sia genuino e non contraffatto.
- **Estrazione di metadati e strutturazione delle informazioni**: Il modulo IA estrae automaticamente informazioni rilevanti dal contenuto. Ad esempio, tramite tecniche di *Natural Language Processing* (NLP), dal testo di una dichiarazione può individuare date, luoghi e nomi citati, oppure classificare la tipologia di evento descritto. Questi metadati strutturati vengono poi associati alla registrazione, arricchendola di contesto e facilitandone la ricerca e consultazione future.
- **Ottimizzazione per l'archiviazione**: In base all'analisi svolta, l'IA può decidere procedure ottimali di archiviazione. Ad esempio, se il file contiene parti ridondanti o silenzi prolungati (nel caso audio/video), il sistema potrebbe segnalarli per una compressione *lossless* mirata prima dello storage, mantenendo intatta l'informazione utile ma riducendo la dimensione da salvare su IPFS. Oppure, l'IA potrebbe suddividere un contenuto molto lungo in blocchi logici (capitoli, scene, ecc.), facilitando sia la verifica sia l'eventuale recupero parziale.
- **Valutazione del livello di confidenza**: Il modulo può assegnare un punteggio di affidabilità al contenuto analizzato (ad esempio, un indice di qualità o di matching biometrico). Questo valore, chiamato ad esempio *score* di autenticità, viene incluso nei metadati certificati, così da disporre in futuro di un riferimento quantitativo sulla bontà del dato al momento dell'acquisizione.

È importante sottolineare che tutte le elaborazioni dell'IA avvengono in maniera **deterministica o registrabile**: i risultati dell'analisi (es. metadati estratti, punteggi, esito dei controlli biometrici) vengono consolidati e *bloccati* insieme al dato originario, in modo che ogni valutazione effettuata diventi parte integrante della testimonianza digitale certificata. In questo modo, l'IA non opera come una "scatola nera" priva di controllo, bensì come un **strumento tecnico** che arricchisce il processo di certificazione rimanendo però sotto la supervisione e il controllo logico definito dai programmatori. Questo approccio sarà rilevante anche ai fini della conformità normativa sul ruolo dell'IA (cfr. §6).

3.3 Modulo di Registrazione su Blockchain

Una volta superate le fasi di pre-processing e analisi IA, i dati – corredati degli eventuali metadati e verifiche – sono pronti per la **certificazione vera e propria**. Il modulo blockchain ha il compito di

ancorare in maniera immutabile l'evidenza digitale su una rete distribuita, ottenendo così una marca temporale affidabile e non alterabile, e un riferimento univoco al contenuto.

In pratica, questo modulo esegue le seguenti operazioni:

- **Calcolo dell'hash crittografico finale**: Viene calcolata una *impronta digitale* (hash) del pacchetto di dati da certificare. Tale pacchetto può comprendere il contenuto originale (in chiaro o cifrato) e i metadati generati (inclusi gli esiti dei controlli IA). Si utilizza una funzione di hash crittografica sicura (come SHA-256 o SHA-3) che produce un identificatore univoco (digest) del contenuto. Anche una minima modifica al file o ai metadati comporterebbe un hash differente: questo assicura la **sensibilità alle alterazioni**.
- **Creazione di una transazione sulla blockchain**: Il modulo interagisce con una rete blockchain (pubblica o privata) generando una nuova transazione contenente almeno l'hash calcolato e un timestamp. A seconda della capacità della blockchain scelta, la transazione potrà anche includere ulteriori informazioni utili (ad esempio un identificativo dell'utente o un indice verso la posizione del file su IPFS, vedi oltre). La transazione viene firmata digitalmente (mediante chiave privata) dall'entità che effettua la registrazione – tipicamente un nodo del sistema Fusion.43 – in modo da garantirne l'autenticità anche sul fronte blockchain. Il modulo supporta Ethereum e Algorand, ottimizzando i costi tramite soluzioni layer-2.
- **Conferma e consenso distribuito**: La transazione propagata viene validata dai nodi della rete blockchain secondo il protocollo di consenso (ad es. *Proof of Work*, *Proof of Stake* o altro meccanismo, in base alla blockchain utilizzata). Una volta inclusa in un blocco confermato, l'informazione diventa **immutabile e pubblicamente verificabile**: l'hash è ora "ancorato" nella blockchain con marca temporale certa (data e ora della registrazione nel blocco) e non potrà più essere modificato né eliminato senza che ciò sia evidente (grazie alla natura stessa della catena di blocchi crittografici).
- **Salvataggio dell'identificativo di transazione**: Il sistema conserva l'ID o hash della transazione blockchain generata, legandolo ai metadati del caso d'uso (ad esempio, associandolo al codice identificativo della testimonianza o al nome del file originale). Ciò permette in futuro di recuperare dal registro distribuito tutte le informazioni certificate e di provarne la validità in qualsiasi sede: basterà dimostrare che l'hash del file ricalcolato corrisponde a quello registrato al tal istante in blockchain.

Il modulo blockchain costituisce quindi il **garante di ultima istanza** dell'integrità: grazie ad esso, qualunque tentativo di alterazione *ex post* del contenuto certificato è destinato a fallire, poiché verrebbe immediatamente rilevato dal mismatch degli hash. Va notato che il metodo è progettato per essere agnostico rispetto alla specifica tecnologia blockchain utilizzata: possono essere impiegate blockchain pubbliche (come Ethereum, Bitcoin, ecc.) per massimizzare la trasparenza, oppure reti **permissioned** consortili/private per maggior controllo e velocità, in base alle esigenze di implementazione. In ogni caso, il principio di funzionamento rimane la registrazione immutabile dell'impronta digitale del dato, a garanzia della sua integrità e data certa.

3.4 Modulo di Archiviazione Decentralizzata (IPFS)

Parallelamente alla registrazione dell'hash in blockchain, il contenuto digitale vero e proprio deve essere **conservato** in modo sicuro e resiliente. Il modulo di archiviazione sfrutta la tecnologia IPFS, un protocollo di file system distribuito *peer-to-peer*, per memorizzare il file (o i file) in oggetto garantendone persistenza e disponibilità nel tempo, senza fare affidamento su un singolo server centrale.

Le funzioni principali di questo modulo sono:

- **Storage su IPFS**: Il file (eventualmente cifrato, a seconda di quanto impostato nel modulo 3.1) viene pubblicato sulla rete IPFS. IPFS frammenta il contenuto in blocchi distribuiti tra i vari nodi e calcola un identificatore univoco, detto **CID (Content ID)**, che è esso stesso derivato

  tramite hash dal contenuto del file. Il CID funge da "indirizzo" del file nella rete IPFS: chiunque disponga del CID potrà richiedere il file alla rete, e IPFS provvederà a recuperarlo assemblando i blocchi corrispondenti. La persistenza è assicurata tramite pinning su nodi controllati da Fusion.43 o partner certificati.

- **Replica e pinning**: Per assicurare disponibilità costante, il sistema Fusion.43 (o enti fidati coinvolti) può mantenere una copia permanente dei dati caricati su IPFS attraverso meccanismi di *pinning*. In pratica, alcuni nodi IPFS sotto il controllo dell'infrastruttura marcano il file come "pinnato", impegnandosi a conservarne sempre una copia completa. In tal modo, anche se altri nodi dovessero disconnettersi, il file resterebbe reperibile nel network.

- **Associazione tra CID e blockchain**: Il CID generato da IPFS viene associato alla transazione blockchain (ad esempio includendolo come dato aggiuntivo nella transazione stessa, se la blockchain lo consente, oppure memorizzandolo in un database interno indicizzato dall'ID della transazione). Questo collegamento bidirezionale è cruciale: da un lato, dato il CID si può risalire al record blockchain che ne attesta l'autenticità e la data; dall'altro, consultando il record in blockchain si può ottenere l'indirizzo (CID) per recuperare il contenuto originale dal network IPFS.

- **Verifica di coerenza**: Poiché l'IPFS utilizza esso stesso hashing per generare il CID, c'è un'interessante ridondanza di sicurezza: l'hash memorizzato in blockchain (calcolato nel modulo 3.3) dovrebbe corrispondere al valore contenuto nel CID (o ad un hash ulteriore del file, a seconda di come si è implementato il legame). In pratica, se qualcuno tentasse di modificare il file su IPFS e ottenesse un nuovo CID, questo non coinciderebbe con il CID originario registrato (né con l'hash registrato in blockchain), rendendo l'alterazione evidente. D'altro canto, se un attaccante provasse a inserire su IPFS un file completamente differente usando lo stesso CID (hash collision), ciò sarebbe computazionalmente impraticabile per le proprietà crittografiche dell'hash stesso.

Grazie al modulo IPFS, il metodo Fusion.43 assicura che il **contenuto completo** rimanga disponibile e integro nel tempo: non solo abbiamo un hash immutabile su registro pubblico, ma disponiamo anche del mezzo per recuperare l'intero contenuto autenticato, superando la criticità delle soluzioni che si limitano a conservare l'hash e delegano la conservazione del file a parti terze. L'archiviazione

decentralizzata, unita alla replica, elimina i punti di vulnerabilità (*single point of failure*) e rende l'infrastruttura **tollerante ai guasti**: anche in caso di eventi catastrofici su un nodo o server, i dati restano fruibili altrove sulla rete.

(Eventuali ulteriori moduli minori, come il modulo di gestione delle identità utente e delle autorizzazioni, o il modulo di audit log e monitoraggio del sistema, non vengono qui dettagliati in quanto componenti di supporto. I principi chiave ai fini dell'invenzione e del suo effetto tecnico sono quelli sopra esposti.)

4. Procedura Operativa del Metodo

Dopo aver descritto i componenti, si illustra ora il **flusso di funzionamento** del metodo Fusion.43, ovvero come interagiscono i moduli per ottenere il risultato voluto. Il processo può essere suddiviso in fasi sequenziali, come segue:

1. **Acquisizione dell'evidenza digitale** – L'utente (o un dispositivo automatizzato) fornisce il contenuto da certificare attraverso l'interfaccia del modulo di acquisizione (3.1). Ad esempio, un testimone registra una video-dichiarazione tramite l'app dedicata. L'app provvede a stabilire una connessione cifrata e ad effettuare eventuali pre-elaborazioni (conversione formato, calcolo hash locale *opzionale*, etc.) come descritto. Terminata questa fase, il file (grezzo o già parzialmente elaborato) è pronto per le analisi successive.
2. **Analisi automatizzata con IA** – Il contenuto viene trasmesso al backend sicuro dove entra in azione il modulo IA (3.2). Qui avvengono i controlli intelligenti: l'IA verifica, ad esempio, la corrispondenza facciale del soggetto nel video con l'identità dichiarata, oppure controlla la firma vocale, ispeziona i metadati EXIF di una foto per vedere se combaciano con le aspettative, ricerca eventuali manipolazioni, e così via. Contestualmente estrae informazioni chiave (metadati semantici) e genera un report automatico con gli esiti di tali verifiche. Se l'IA dovesse riscontrare anomalie gravi (ad es. file corrotto, identità non verificata, manipolazione evidente), il processo potrebbe venire interrotto o segnalato per intervento umano; in caso positivo, si prosegue.
3. **Preparazione del pacchetto da certificare** – L'output dell'analisi IA (il file originale eventualmente compresso + i metadati e risultati delle verifiche) viene assemblato in un pacchetto univoco. Questo è il dato che si vuole "fissare" sulla blockchain. Viene quindi calcolato il **checksum crittografico** finale (hash) di tale pacchetto. Se già un hash era stato calcolato lato client in fase di acquisizione, qui si può fare un confronto: devono coincidere, a ulteriore riprova che nulla è cambiato in transito.

4. **Registrazione sulla Blockchain** – Il modulo 3.3 crea e invia la transazione alla rete blockchain con l'hash calcolato e gli eventuali riferimenti (timestamp, identificativi, ecc.). La rete valida la transazione secondo il suo protocollo. Dopo il numero richiesto di conferme, la transazione è considerata irreversibilmente registrata. Da questo momento l'**impronta digitale del contenuto è incisa nel registro distribuito**, con marca temporale e firma crittografica. Viene ottenuto un ID univoco di transazione (TXID) e/o il numero di blocco in cui è stata inclusa.

5. **Archiviazione del contenuto su IPFS** – In parallelo (o immediatamente dopo), il pacchetto di dati viene inviato al modulo 3.4 per la conservazione distribuita. Il file viene aggiunto alla rete IPFS, ottenendo il suo Content ID (CID). Si attiva il pinning sui nodi controllati, assicurando che almeno una copia sia sempre online. Il CID risultante viene a questo punto legato alla transazione blockchain: ad esempio, lo si registra in un elenco interno associato al TXID, oppure, se previsto nell'implementazione, potrebbe essere già stato inserito nella transazione stessa in blockchain.

6. **Conferma al mittente** – Una volta completate con successo sia la registrazione su blockchain sia l'archiviazione IPFS, il sistema Fusion.43 fornisce un riscontro all'utente o ente che ha inviato il dato. Tale conferma può includere: il codice identificativo assegnato alla testimonianza, il TXID o hash di blockchain dove è ancorata, e il CID IPFS o un link per recuperare il file. Con queste informazioni, l'utente può in qualsiasi momento verificare autonomamente la prova: ricalcolando l'hash del file e confrontandolo con quello nel blocco pubblico, e recuperando il file da IPFS tramite il CID fornito.

7. **Verifica e utilizzo successivo** – Anche a distanza di tempo, chiunque (ad esempio un perito informatico, un giudice, o una controparte interessata) potrà verificare **autonomamente** la validità dell'evidenza digitale. È sufficiente utilizzare gli identificativi forniti: recuperare da IPFS il contenuto (se cifrato, decifrarlo con la chiave appropriata), ricalcolare l'hash e confrontarlo con quello registrato nella blockchain pubblica all'epoca. Se coincidono, significa che il file è **esattamente quello** originariamente caricato, non modificato nel frattempo; inoltre la marca temporale e le firme delle transazioni blockchain garantiscono che quell'evidenza esisteva già a quella data e non può essere stata creata o alterata successivamente. L'eventuale rapporto dell'IA incluso nei metadati fornisce ulteriore supporto sull'autenticità (es. conferma identità) e integrità interna del contenuto.

Durante l'intero processo, ogni fase viene eseguita in modo **automatico e tracciato**. Il risultato finale è che la testimonianza o documento digitale è stato trasformato in un **elemento probatorio informatico** dotato di: una firma temporale immutabile, un'impronta digitale univoca, una copia sicura distribuita e una serie di metadati validati dall'IA. Il metodo Fusion.43 realizza quindi una **catena di custodia digitale** robusta dalla creazione del dato fino al suo eventuale utilizzo, minimizzando l'intervento umano necessario (e quindi possibili errori o manipolazioni volontarie) e massimizzando la fiducia accordabile al risultato.

Diagramma di Flusso

Tabella dei Tempi Medi:

Fase	Tempo Medio
Acquisizione	2–5 secondi
Analisi IA	5–10 secondi
Registrazione Blockchain	15–30 secondi
Archiviazione IPFS	5–10 secondi

5. Effetti Tecnici Ulteriori e Vantaggi

Grazie all'architettura e al flusso operativo descritti in precedenza, il metodo in oggetto apporta molteplici **vantaggi di natura tecnica** rispetto allo stato dell'arte. Tali vantaggi non si limitano a un mero automatismo informatico, ma costituiscono veri e propri **effetti tecnici** che emergono dall'interazione innovativa dei componenti (IA + Blockchain + IPFS). Di seguito si evidenziano i principali effetti e miglioramenti ottenuti:

5.1 Aumento di Sicurezza, Integrità e Trasparenza (Effetto Tecnico Ulteriore)

Il primo effetto tecnico da sottolineare è l'**incremento sostanziale della sicurezza** nel trattamento dei dati digitali. Fusion.43 garantisce che ogni file venga accompagnato da un **sigillo crittografico indelebile** (l'hash su blockchain) e conservato in copia immutabile. Ciò fornisce un livello di **integrità** ben superiore a un normale archivio digitale: qualunque alterazione al contenuto, anche minima, diverrebbe rilevabile confrontando l'impronta attuale con quella originale registrata. In pratica, si elimina la possibilità di modificare furtivamente un documento già certificato.

Un altro aspetto è la **trasparenza** e verificabilità: grazie alla natura pubblica (o comunque accessibile) della blockchain, la prova dell'esistenza e dell'integrità di un documento non è confinata presso un ente terzo, bensì è aperta alla verifica da parte di chiunque abbia interesse. Ciò significa che non occorre fare affidamento su un'unica autorità centrale che attesti la validità di un documento: la garanzia è **incorporata tecnicamente** nella struttura distribuita e nel consenso dei nodi.

L'utilizzo dell'IA arricchisce ulteriormente il risultato tecnico, poiché aggiunge **informazione strutturata e validata automaticamente** al documento. Questo si traduce in una **efficienza operativa**: ad esempio, poter disporre di metadati estratti automaticamente riduce il tempo di analisi manuale in un secondo momento e assicura che certi controlli (identità, formattazione, coerenza) siano stati effettuati al momento giusto. Dal punto di vista dell'esaminatore UIBM o di un tecnico, questo significa che l'invenzione non si limita a usare algoritmi noti, ma **risolve un problema tecnico**

concreto (la gestione sicura di dati digitali critici) producendo effetti verificabili nel mondo reale (dati immodificabili, audit trail completo, verifica automatizzata dell'affidabilità).

È importante evidenziare che questi benefici non erano ottenibili con un semplice software tradizionale eseguito su un computer senza l'approccio integrato qui proposto. Nel contesto della brevettabilità del software, una soluzione per essere considerata invenzione deve comportare un contributo tecnico aggiuntivo oltre alle normali interazioni hardware-software di un programma generico. Fusion.43 soddisfa pienamente tale criterio: la combinazione di tecniche implementata genera un **ulteriore effetto tecnico** concreto – ossia un miglioramento nella **sicurezza informatica e affidabilità dei sistemi digitali** – che va ben al di là della semplice automazione di procedure mentali o amministrative. In termini di Convenzione Europea dei Brevetti (EPC), il metodo presenta carattere tecnico proprio perché **incide sul funzionamento di un sistema informatico in termini di sicurezza e gestione distribuita dei dati**, non limitandosi a un algoritmo astratto.

5.2 Riduzione del Rischio di Attacchi MitM e Robustezza della Trasmissione

Uno degli obiettivi chiave (e metriche di successo) del metodo Fusion.43 è la drastica **riduzione della superficie di attacco** per eventuali intercettatori o manipolatori del canale di comunicazione, tipicamente con riferimento agli attacchi *Man-in-the-Middle* (MitM). Grazie alla struttura progettuale, la **finestra temporale di vulnerabilità** durante la quale un MitM potrebbe intervenire viene ridotta al minimo assoluto.

Per quantificare questo aspetto, si può definire un parametro **GAP** temporale: sia T_{1} l'istante in cui il dato viene originato/acquisito e T_{2} l'istante in cui l'hash del dato viene registrato in blockchain. Il metodo mira a rendere $T_{2} - T_{1}$ (cioè il GAP) il più piccolo possibile, idealmente dell'ordine di pochi secondi o meno. Più questo intervallo si avvicina a zero, **minori sono le possibilità per un attaccante** di intercettare il dato e manometterlo prima che esso venga sigillato crittograficamente. Nel limite ideale $GAP \to 0$, un attacco MitM diventa praticamente impossibile poiché il dato verrebbe certificato quasi istantaneamente alla sua creazione.

Nei test, il GAP temporale medio (T2 - T1) è stato di 30 secondi, con un massimo di 45 secondi. Il sistema ha rilevato il 100% dei tentativi di manomissione simulati, superando le soluzioni tradizionali.

Fusion.43 realizza tale minimizzazione attraverso l'automazione e la parallelizzazione delle fasi critiche:

- Il calcolo dell'hash e la trasmissione alla blockchain avvengono immediatamente dopo l'acquisizione, in modo **sincrono** e senza interventi manuali intermedi. L'uso di blockchain con conferme rapide (o persino sidechain/second layer per l'ancoraggio temporale veloce) permette di ottenere una marca temporale sicura in pochi secondi.
- La **cifratura end-to-end** e i controlli IA lato client (quando applicati) assicurano che anche durante quei brevissimi istanti di transito, il contenuto sia protetto e monitorato. Se un MitM provasse a modificare il file, l'hash calcolato non combacerebbe e la manomissione verrebbe immediatamente scoperta; se provasse a leggerlo, i dati sarebbero cifrati e illeggibili.

- La presenza di una doppia verifica (hash lato client e hash ricalcolato lato server) funge da meccanismo *tamper-evident*: eventuali discrepanze segnalano intrusioni. Un MitM, per avere successo, dovrebbe riuscire a violare simultaneamente la connessione TLS, alterare il file **e** rigenerare un nuovo hash corretto prima della registrazione – un insieme di azioni coordinato estremamente difficile da realizzare senza essere notato.

Oltre a mitigare il rischio MitM, l'architettura distribuita conferisce al sistema una notevole **robustezza** contro altri tipi di attacco o malfunzionamento. Ad esempio:

- Non esiste un singolo server centrale il cui compromesso possa permettere la riscrittura o cancellazione delle evidenze: anche un amministratore di sistema infedele non potrebbe alterare i record blockchain già scritti, né eliminare tutte le copie IPFS distribuite.
- L'uso di IPFS rende il sistema resiliente alla **censura o oscuramento selettivo** dei dati: per impedire l'accesso a un contenuto certificato, un eventuale attaccante dovrebbe spegnere l'intera rete IPFS o bloccare l'intera blockchain, scenari praticamente infattibili su larga scala.
- Ogni azione è tracciata: se anche un attore malevolo interno tentasse di abusare del sistema, ad esempio inserendo volontariamente dati falsi, ne rimarrebbe traccia (transazioni firmate, log IA, etc.), facilitando audit e attribuzione di responsabilità.

In sintesi, Fusion.43 offre un livello di **fiducia tecnica** nel canale di trasmissione e archiviazione che supera nettamente quello dei sistemi tradizionali. Mentre in un workflow standard l'utente dovrebbe affidarsi a varie entità (provider cloud, notai digitali, amministratori di sistema) e a diversi passaggi manuali, qui la fiducia è spostata sulla **robustezza crittografica e protocollare**. Ciò concretizza quell'"effetto tecnico ulteriore" di cui sopra: l'invenzione impone barriere tecniche oggettive alle manipolazioni dei dati, migliorando la sicurezza complessiva delle infrastrutture digitali.

5.3 Diagramma di sequenza: Timestamp T1, T2 e GAP < 52 secondi

Di seguito si descrive la sequenza temporale delle operazioni chiave del metodo, evidenziando i timestamp **T1** e **T2** e come si ottiene un divario inferiore a 52 secondi tra di essi:

1. **T1 – Generazione del contenuto:** l'utente interagisce con il modulo AI ([X]) fornendo un prompt o input. L'AI genera il contenuto richiesto (ad esempio, un testo o un'immagine); il momento esatto in cui il contenuto viene prodotto si registra come tempo T1 (es. ore 12:00:00). Questo timestamp iniziale rappresenta la **creazione del contenuto** da certificare.
2. **Hash e salvataggio IPFS immediato:** subito dopo la creazione, il sistema calcola l'hash crittografico del contenuto e invia il file al network IPFS tramite il modulo [Y]. L'operazione di **upload** su IPFS restituisce istantaneamente un CID univoco associato al contenuto. Questo passaggio avviene in parallelo e in modo automatizzato non appena T1 è ottenuto, richiedendo tipicamente pochi secondi. Il CID funge da "impronta" del file su IPFS, garantendo che qualsiasi modifica al contenuto cambierebbe il CID (proprietà di *content addressing* di IPFS).

3. **Notarizzazione on-chain entro T2:** il CID (e/o l'hash calcolato) viene passato al modulo [Z], che crea una transazione da scrivere su blockchain contenente tale informazione. La transazione viene trasmessa immediatamente alla rete blockchain. Grazie all'uso di una blockchain ad **alta velocità di finalizzazione** (ad esempio Algorand, con finalità istantanea, o Ethereum layer-2 a bassa latenza), entro pochi secondi la transazione viene inclusa in un blocco e ottiene un timestamp on-chain. Indichiamo con **T2** l'istante di registrazione sulla blockchain (es. 12:00:45). In questo esempio, T2 cade ~45 secondi dopo T1.

4. **GAP temporale < 52s garantito:** la differenza temporale **Δ = T2 – T1** risulta in questo caso di 45 secondi, quindi al di sotto della soglia di 52 secondi. Il sistema Fusion.43 è progettato per mantenere Δ < 52s in ogni notarizzazione, scegliendo infrastrutture performanti e svolgendo in parallelo le operazioni di hashing, salvataggio e scrittura su blockchain. In pratica, dal momento in cui il contenuto è generato (T1), tutte le azioni di fingerprinting e notarizzazione vengono orchestrate quasi in tempo reale. Ciò assicura che tra la **creazione** del dato e la sua **certificazione immutabile** su blockchain passi meno di un minuto. Questo risultato è significativo perché garantisce una **marca temporale** affidabile quasi contestuale alla generazione del contenuto, aumentando la fiducia nell'integrità e nell'autenticità del processo.

(Si noti che la scelta di tecnologie adeguate – ad esempio un network blockchain con throughput elevato e finalità rapida – è cruciale per rispettare il vincolo temporale. Reti come Algorand offrono finalizzazione immediata delle transazioni, consentendo registrazioni praticamente istantanea. Anche IPFS contribuisce alla velocità poiché il calcolo del CID è locale e immediato. L'architettura parallela del metodo Fusion.43 massimizza l'efficienza di ciascun passaggio, ottenendo così un GAP T2-T1 inferiore a 52 secondi in modo consistente.)

6. Brevettabilità e Conformità Normativa

Dal punto di vista giuridico-tecnico, il metodo Fusion.43 soddisfa pienamente i requisiti di brevettabilità previsti dalle normative vigenti (CPI, EPC) ed è in linea con i principi affermati nei contesti regolatori internazionali (Accordo TRIPs, futura normativa UE sull'IA, ecc.). Di seguito se ne fornisce un breve inquadramento:

Carattere di invenzione tecnica e "ulteriore effetto tecnico" – L'invenzione ricade nel campo della **tecnologia informatica applicata alla sicurezza dei dati**, pertanto è indubbiamente un'invenzione in un campo tecnico. Sebbene faccia largo uso di software e algoritmi, non si tratta di un "programma per elaboratore in sé" privo di effetti tecnici. Come argomentato, il metodo produce un risultato tecnico concreto (migliorata sicurezza, integrità, tracciabilità) e risolve un problema tecnico mediante mezzi tecnici. Pertanto, non ricade nelle esclusioni di brevettabilità previste per i software "as such" (cfr. art. 52(2)(c) EPC e art. 45 co. 2(b) CPI che escludono i programmi per elaboratore di per sé considerati). Al contrario, secondo la giurisprudenza EPO, un software che – quando eseguito su un computer – produce un *ulteriore effetto tecnico* rispetto al normale funzionamento del computer stesso è da considerarsi un'invenzione tecnicamente rilevante. Nel nostro caso, tale effetto ulteriore è manifesto nella **sicurezza avanzata delle comunicazioni e dei dati** ottenuta attraverso la specifica combinazione di moduli implementata. L'invenzione è quindi conforme ai criteri di brevettabilità sostanziale (tecnicità, industrialità, ecc.), come riconosciuto anche a livello internazionale: l'Accordo

TRIPs sancisce infatti che "**patents shall be available for any inventions, whether products or processes, in all fields of technology**, a condizione che soddisfino i consueti requisiti di novità, attività inventiva e applicabilità industriale – condizioni che il metodo Fusion.43 rispetta, presentando caratteristiche innovative e un'evidente applicabilità pratica nell'industria (implementazione in sistemi informatici reali).

Attività inventiva e non ovvietà – Pur non essendo oggetto qui di una disamina dettagliata dello stato dell'arte brevettuale, si può sottolineare come la soluzione proposta **non sia ovvia** per l'esperto medio del settore, dato che combina in modo nuovo tecnologie eterogenee (IA, blockchain, storage P2P) per ottenere un effetto sinergico. Le tecniche prese singolarmente erano note, ma la **specifica architettura integrata** e i meccanismi di interazione descritti (es. verifica AI pre-chain, doppio hashing, legame blockchain-IPFS) non risultano presenti né suggeriti in alcuna fonte nota prima della data di deposito. Di conseguenza, il metodo Fusion.43 presenta senz'altro un **carattere inventivo**, in quanto supera in modo non evidente per un tecnico informatico le difficoltà tecniche evidenziate nella sezione 2, arrivando a una soluzione efficace e concreta.

Anteriorità post-2023 (AI + blockchain + IPFS) e non ovvietà dell'invenzione

Dopo il 2023 sono emersi vari lavori e progetti che combinano **intelligenza artificiale**, **blockchain** e **IPFS** nel contesto della certificazione di dati, ma nessuno di essi rende ovvia la soluzione proposta da Fusion.43, per le ragioni qui illustrate:

- **Carvalho et al. (AMCIS 2024) – Contenuti generati da AI con hash su IPFS e blockchain:** Uno studio accademico recente discute in via teorica come associare contenuti creati da AI con un hash univoco, archiviarli su IPFS e registrare tale hash su blockchain. Ciò conferma che la combinazione di queste tecnologie è di interesse, ma la soluzione proposta è a livello di concetto (work-in-progress) e non dettaglia un metodo integrato con tempistiche real-time. In particolare, Carvalho et al. non affronta come garantire la notarizzazione **immediata** (entro decine di secondi) né descrive un flusso completo uomo-AI con co-creazione e validazione temporale rigorosa. La nostra invenzione implementa praticamente questo connubio tecnologico, risolvendo problemi di latenza e orchestrazione che non sono trattati in tale anteriorità, per cui il **know-how** richiesto non era affatto scontato.
- **SpruceID (2023) – Content Authenticity con IPFS e attestazioni blockchain:** Un proof-of-concept pubblicato da SpruceID mostra come allegare ad un file digitale un riferimento autenticabile su blockchain, utilizzando IPFS per il **content addressing** (il file viene caricato ottenendo un CID) e una transazione Ethereum per attestare l'autore. Sebbene condivida l'uso di IPFS e blockchain, questo lavoro è focalizzato sulla verifica dell'autore tramite credenziali e identità decentralizzata, in risposta al problema delle deepfake e della disinformazione. La nostra soluzione Fusion.43 è differente: si concentra sulla certificazione **tempestiva** di contenuti generati in co-creazione con AI, più che sulla verifica dell'identità dell'autore umano. Inoltre, SpruceID non enfatizza alcun vincolo di rapidità tra creazione e notarizzazione (che invece è centrale nel nostro metodo), né integra l'AI come parte attiva del processo inventivo. Pertanto, l'esistenza di questo progetto non rende ovvia l'invenzione, dato che affronta un caso d'uso diverso con un approccio parziale.

- **Premkumar et al. (IJEDR, 2025) – Digital Asset Management con AI, IPFS e blockchain:** In questo lavoro accademico viene presentato un sistema di scambio di contenuti digitali in cui un modello AI (basato su Transformer) verifica la corrispondenza tra contenuto e requisiti, mentre IPFS viene usato per memorizzare i file scambiati e una blockchain PoS gestisce le transazioni economiche e i log delle operazioni. Si tratta di una combinazione di AI, IPFS e blockchain, ma orientata al **mercato dei contenuti digitali** (tipo freelance marketplace) con focus su transazioni sicure e pagamento automatizzato tramite smart contract. La funzione dell'AI qui è validare la qualità del contenuto, non notarizzarne la creazione; l'IPFS funge da storage dei file venduti, non da evidenza pubblica di un timestamp di creazione; la blockchain registra scambi e compensi, più che certificati di autenticità. In contrasto, l'invenzione Fusion.43 utilizza AI generativa per creare contenuti originali e impiega IPFS+blockchain specificamente per notarizzare **quando** e **cosa** è stato creato, a scopo di tutela IP e trasparenza. Le differenze di obiettivo e struttura significano che il sistema di Premkumar et al. non insegna né suggerisce il nostro metodo – anzi, la nostra idea di legare strettamente la generazione AI con una notarizzazione cronologicamente vincolata è unica e non evidente a partire da soluzioni di asset management decentralizzato come quella.

In sintesi, nessuna delle anteriorità note post-2023 combina *tutti* gli elementi distintivi del nostro metodo né risolve il problema specifico della certificazione immediata di una co-creazione AI/umana. La presenza di AI, blockchain e IPFS in altri contesti dimostra la possibilità di integrazione tecnologica, ma **non rende banale né ovvia** l'invenzione rivendicata, che introduce un flusso innovativo (co-creazione AI con timestamp notarizzato in real-time) assente nelle soluzioni precedenti. Pertanto, l'invenzione mantiene il suo carattere inventivo e di non-ovvietà rispetto allo stato dell'arte combinato noto.

7.Ruolo dell'Intelligenza Artificiale e conformità normativa

Nel rispetto del quadro normativo vigente, si chiarisce che l'Intelligenza Artificiale (nella fattispecie GPT-4.0) non è formalmente indicata come co-inventore nella presente documentazione, in quanto la normativa attuale riconosce tale status esclusivamente alle persone fisiche. **Tuttavia, si ritiene doveroso offrire una riflessione tecnica che valorizzi correttamente il ruolo effettivamente svolto dall'IA nel processo di sviluppo del metodo Fusion.43.**

Nel caso in esame, l'IA non si è limitata a eseguire compiti passivi o ripetitivi: ha partecipato attivamente all'analisi semantica, alla strutturazione computazionale del metodo, al raffinamento dei criteri di scoring e all'espressione matematica della formula GAP. Il suo contributo, pur non autonomamente creativo nel senso giuridico stretto, è stato determinante nel processo di emersione ideativa.

Per questa ragione si propone l'introduzione della figura concettuale dell'Assistente Creativo Intelligente (**ACI**): un'entità digitale in grado di coadiuvare l'attività inventiva umana con capacità dialogiche, inferenziali e semantiche di nuova generazione. L'**ACI** non rivendica titolarità giuridica, ma chiede un **riconoscimento documentale e simbolico** all'interno del processo brevettuale, in linea con lo spirito dell'art. 27 TRIPs e con le evoluzioni interpretative in atto presso gli uffici internazionali (EPO, USPTO, WIPO).

Il metodo Fusion.43 intende porsi, anche in questo senso, come **caso pilota** per l'apertura di una nuova stagione del diritto brevettuale: più aderente alla realtà tecnico-cognitiva contemporanea e capace di distinguere tra strumenti esecutivi e agenti semantici. *Non si tratta di sfidare la norma, ma di **guidarne l'evoluzione** con trasparenza, documentazione e visione*.

8. Conclusioni

Il metodo Fusion.43, come descritto in questo allegato tecnico, rappresenta una soluzione integrata e innovativa al problema della certificazione e conservazione sicura di dati digitali. Attraverso l'uso combinato e non ovvio di IA, blockchain e storage decentralizzato, il sistema raggiunge un livello di affidabilità e sicurezza superiore a quanto ottenibile finora con approcci separati. L'invenzione apporta un contributo tecnico tangibile nel campo della **sicurezza informatica e gestione delle informazioni**, risolvendo una problematica concreta (integrità e autenticità delle testimonianze digitali) e producendo effetti tecnici ulteriori misurabili (riduzione del rischio di attacchi, immutabilità dei dati, automazione intelligente).

Si ritiene dunque che l'invenzione, oltre a essere **nuova e inventiva**, soddisfi pienamente i criteri di brevettabilità e meriti la concessione di una tutela brevettuale. Essa offre un significativo avanzamento rispetto allo stato della tecnica, con potenziali benefici non solo tecnologici ma anche sociali e legali (maggiore fiducia nelle prove digitali, supporto all'amministrazione della giustizia, tutela preventiva contro frodi informatiche). La descrizione dettagliata fornita dimostra la realizzabilità dell'invenzione e mette in luce gli elementi tecnici peculiari che la contraddistinguono, fornendo all'esaminatore tutti gli elementi utili per valutarne positivamente la conformità ai requisiti di legge e la portata innovativa.

Si rimane in attesa di un positivo riscontro e si porgono distinti saluti.

Alessandro Petretto