DESCRIZIONE del brevetto per invenzione industriale dal titolo: “Sistema e metodo per la creazione di un legame fisico-digitale per l'autenticazione di beni di lusso”. Richiedente ed inventore Stefano PEZZI di nazionalità italiana.

Campo tecnico

La presente invenzione si colloca nel campo dei sistemi di sicurezza e anticontraffazione per beni di lusso. Più specificamente, l'invenzione riguarda un sistema e un metodo per l'autenticazione e la tracciabilità di orologi di alta gamma, sebbene la sua applicazione possa essere estesa ad altri beni di valore che richiedono una prova di autenticità certa e un legame univoco tra l'oggetto fisico e la sua rappresentazione digitale. La soluzione tecnologica si basa sull'integrazione sinergica di una funzione fisica non clonabile (Physical Unclonable Function, PUF) di tipo ottico, un chip per la comunicazione in prossimità (Near Field Communication, NFC) dotato di un elemento sicuro (Secure Element), e una piattaforma di registro distribuito (Distributed Ledger Technology, DLT), comunemente nota come blockchain.

Stato dell’arte

Lo stato dell'arte nel campo dell'autenticazione di beni di lusso, e in particolare degli orologi di alta gamma, si basa su una varietà di approcci che, tuttavia, presentano significative limitazioni in termini di sicurezza, affidabilità e resistenza alla contraffazione. I metodi tradizionali includono l'uso di certificati di autenticità cartacei, l'incisione di numeri di serie univoci sulla cassa o sul movimento dell'orologio, e l'apposizione di ologrammi o altri

segni distintivi. Tali metodi sono intrinsecamente vulnerabili alla falsificazione, alla duplicazione e alla manomissione. I certificati cartacei possono essere riprodotti con relativa facilità, i numeri di serie possono essere incisi su orologi contraffatti e gli ologrammi possono essere imitati.

Con l'avvento delle tecnologie digitali, sono state introdotte soluzioni più sofisticate. L'uso di codici a risposta rapida (QR code) o di etichette a radiofrequenza (RFID) e NFC è diventato comune. Sebbene questi metodi offrano un livello di sicurezza superiore rispetto a quelli tradizionali, non sono esenti da vulnerabilità. Un QR code può essere facilmente copiato e associato a un prodotto contraffatto. I chip RFID/NFC standard, privi di adeguate contromisure di sicurezza, possono essere clonati (un attacco noto come "skimming") o letti senza autorizzazione, compromettendo l'integrità del sistema di autenticazione. Documenti come "NFC anti-counterfeiting framework for ID verification and image protection" [Lee, W. H., Chou, C. M., & Wang, S. W. (2016); An NFC anti-counterfeiting framework for ID verification and image protection; *Mobile Networks and Applications*, 21(4), pp. 721-733] e "Lightweight authentication protocol for NFC based anti-counterfeiting system in IoT infrastructure" [Alzahrani, B. A., Mahmood, K., & Kumari, S. (2020); Lightweight authentication protocol for NFC based anti-counterfeiting system in IoT infrastructure; *IEEE Access*, 8, pp. 90752-90765] descrivono architetture che tentano di mitigare questi rischi, ma spesso si basano su protocolli che non garantiscono un legame inscindibile con l'oggetto fisico.

L'introduzione della tecnologia blockchain ha aperto nuove prospettive per la tracciabilità e l'autenticazione. La capacità di creare un registro immutabile e decentralizzato degli eventi legati a un prodotto offre una soluzione promettente per combattere la contraffazione. Diverse iniziative hanno esplorato l'uso di token non fungibili (NFT) per rappresentare la proprietà e l'autenticità di beni fisici, come discusso in "Combining NFC Authenticated Tags with NFTs to Spot Counterfeit Luxury Products Using Solana Blockchain" [Zocca, M., & Jahankhani, H. (2023); Combining NFC Authenticated Tags with NFTs to Spot Counterfeit Luxury Products Using Solana Blockchain; *Wireless Networks: Cyber Security Threats and Solutions* (pp. 123-136)]. Tuttavia, la sfida principale rimane quella di stabilire un "ancoraggio" sicuro e affidabile tra l'oggetto fisico e la sua controparte digitale (il cosiddetto "digital twin"). Senza un legame fisico-digitale robusto, la sola registrazione su blockchain non può impedire che un certificato digitale autentico venga associato a un prodotto fisico contraffatto. Questo limite è evidenziato in articoli critici come "Why Blockchain Is Not A Great Solution For Tracking, Tracing Or Authenticating Physical Items" [Forbes Business Council; (2023, May 16); Why Blockchain Is Not A Great Solution For Tracking, Tracing Or Authenticating Physical Items; *Forbes*.].

Per superare questa limitazione, la ricerca si è orientata verso le Physical Unclonable Functions (PUF). Una PUF è una caratteristica fisica di un oggetto che è il risultato di un processo stocastico di fabbricazione e che è facile da misurare ma praticamente impossibile da duplicare, anche per il

produttore originale. Le PUF sono state proposte come "impronte digitali" per oggetti fisici. Esistono vari tipi di PUF, tra cui quelle elettroniche (es. SRAM PUF) e quelle ottiche. Le PUF ottiche, che sfruttano le proprietà uniche di un materiale di interagire con la luce (ad esempio, attraverso scattering, riflessione o assorbimento), sono particolarmente promettenti per l'autenticazione di oggetti. La letteratura scientifica, come "Authentication of Optical Physical Unclonable Functions Based on Single-Pixel Detection" [Wang, P., et al. (2021); Authentication of Optical Physical Unclonable Functions Based on Single-Pixel Detection; *Physical Review Applied*, 16(5), 054025] e "Spectral physical unclonable functions" [Sandomirskii, M., et al. (2025); Spectral physical unclonable functions: downscaling randomness with multi-resonant hybrid particles; *Nature Communications*, 16(1), 5097], descrive diverse realizzazioni di PUF ottiche. Alcuni studi, come "Enabling IC traceability via blockchain pegged to embedded PUF" [Bhargava, M., & Gu, C. (2019); Enabling IC traceability via blockchain pegged to embedded PUF; *Proceedings of the 2019 on Great Lakes Symposium on VLSI;* (pp. 323-328)], hanno anche proposto di combinare le PUF con la blockchain per la tracciabilità dei circuiti integrati.

Nonostante questi progressi, lo stato dell'arte attuale non presenta una soluzione integrata che combini sinergicamente una PUF ottica robusta, un sistema NFC sicuro e una piattaforma blockchain per creare un sistema di autenticazione completo e affidabile specificamente progettato per le problematiche peculiari poste dagli orologi di lusso.

Le soluzioni esistenti o si concentrano su singoli aspetti del problema (ad esempio, solo NFC, solo blockchain, o solo PUF) o non affrontano la necessità di un legame fisico-digitale basato su una caratteristica intrinseca, unica e non modificabile dell'oggetto stesso, come la microstruttura del suo movimento meccanico. Vi è quindi la necessità di un sistema che superi le limitazioni descritte, fornendo una soluzione olistica che garantisca non clonabilità, integrità, tracciabilità e privacy per l'intero ciclo di vita di un bene di lusso.

Esposizione sintetica dell'invenzione

I succitati obiettivi ed altri scopi sono raggiunti mediante un sistema e metodo per la creazione di un legame fisico-digitale per l'autenticazione di beni di lusso secondo le annesse rivendicazioni principali di sistema e metodo. Alcune forme vantaggiose di attuazione sono rappresentate nelle rivendicazioni dipendenti.

La presente invenzione si prefigge di superare le limitazioni dello stato dell'arte fornendo un sistema e un metodo per l'autenticazione e la tracciabilità di beni di lusso, in particolare orologi di alta gamma, che stabilisce un legame fisico-digitale univoco, sicuro e non clonabile. L'invenzione risolve il problema tecnico di garantire l'autenticità di un bene di valore in modo robusto, impedendo la contraffazione, la sostituzione di parti e la duplicazione del certificato di autenticità, assicurando al contempo la privacy del proprietario e la tracciabilità immutabile del bene nel tempo.

La soluzione proposta si basa sull'integrazione sinergica e innovativa di tre elementi tecnologici

chiave:

- Una Funzione Fisica Non Clonabile (PUF) di tipo ottico e tridimensionale (3D), che genera un'impronta digitale (fingerprint) unica e irripetibile basata sulla micro-geometria intrinseca di una componente interna dell'orologio, preferibilmente il movimento o calibro. Questa impronta digitale è ottenuta tramite una scansione 3D ad alta risoluzione e l'applicazione di algoritmi di estrazione di caratteristiche che catturano le imperfezioni stocastiche e uniche della superficie del componente. Questo approccio rende il legame con l'oggetto fisico intrinseco e virtualmente impossibile da replicare.
- Un chip per la Comunicazione in Prossimità (NFC) dotato di un Elemento Sicuro (Secure Element), integrato in modo non invasivo nell'orologio. Questo chip non agisce come un semplice contenitore di dati, ma come un microcomputer sicuro. L'Elemento Sicuro custodisce in modo protetto un token digitale, contenente il fingerprint PUF cifrato e altri metadati rilevanti. Esso gestisce le operazioni crittografiche e implementa contromisure hardware contro attacchi fisici, clonazione e manomissione, garantendo che l'accesso e la decifratura del token avvengano solo in un ambiente controllato e autorizzato.
- Una piattaforma di Registro Distribuito (blockchain), di tipo permissioned e nella fattispecie Hyperledger Fabric, che assicura l'immutabilità, la trasparenza e la tracciabilità della storia dell'orologio. Su tale registro non vengono memorizzati dati sensibili, ma unicamente

un hash crittografico del token digitale cifrato. Questo hash agisce come un sigillo digitale, un'ancora immutabile che permette di verificare l'integrità e l'autenticità del token memorizzato nel chip NFC in qualsiasi momento, senza compromettere la privacy. La gestione dei trasferimenti di proprietà e di altri eventi del ciclo di vita dell'orologio è affidata a smart contract (chaincode).

L'invenzione prevede inoltre un metodo (workflow) operativo completo che inizia nella fase di produzione dell'orologio e si estende per tutto il suo ciclo di vita. Durante la produzione, viene generato il fingerprint PUF, creato e cifrato il token digitale, programmato il chip NFC e registrato l'hash sulla blockchain. Successivamente, per la verifica, un utente autorizzato, con il proprio sistema di backend, effettua una scansione del calibro tramite scanner 3D e confronta il PUF appena letto con quello contenuto nel chip NFC. Inoltre l'applicazione avvia un protocollo di autenticazione che decifra, in un ambiente sicuro, il token registrato sul chip NFC e ne confronta l'hash calcolato con quello registrato sulla blockchain. La corrispondenza tra i due PUF, unita alla corrispondenza tra i due hash, prova in modo inconfutabile l'autenticità dell'orologio in tutte le sue parti.

Un ulteriore aspetto innovativo dell'invenzione è un meccanismo di aggiornamento incrementale del modello di fingerprint, che permette al sistema di adattarsi a piccole variazioni naturali della superficie del calibro dovute a usura o accumulo di polvere nel tempo, senza compromettere la sicurezza. Questo garantisce la

robustezza e l'affidabilità del sistema a lungo termine, un requisito fondamentale per beni durevoli come gli orologi di lusso.

Gli effetti vantaggiosi dell'invenzione sono molteplici. In primo luogo, si ottiene un livello di sicurezza anti-contraffazione senza precedenti, basato su una caratteristica fisica unica dell'oggetto. In secondo luogo, si crea un legame indissolubile tra l'orologio fisico e il suo certificato digitale, eliminando il rischio di dissociazione. In terzo luogo, si garantisce la privacy dell'utente, poiché i dati sensibili rimangono off-chain e protetti da crittografia. Infine, si fornisce uno strumento potente per la gestione del mercato secondario, consentendo trasferimenti di proprietà sicuri e tracciabili, aumentando la fiducia e il valore per collezionisti e consumatori.

Modo migliore per attuare l’invenzione

La modalità preferita per la realizzazione dell'invenzione verrà ora descritta in dettaglio, facendo riferimento alle tecnologie e ai processi che ne consentono l'attuazione ottimale. Questa descrizione ha lo scopo di fornire a un tecnico del settore tutte le informazioni necessarie per riprodurre e utilizzare l'invenzione, senza per questo limitarne la portata. La realizzazione del sistema si articola in diverse fasi e componenti logiche, che verranno analizzate singolarmente.

1. Generazione del Fingerprint Fisico mediante PUF Ottica 3D: Il cuore dell'invenzione risiede nella capacità di generare un'impronta digitale (fingerprint) unica e irripetibile dall'oggetto fisico

stesso. La scelta del componente da cui estrarre il fingerprint (PUF) è cruciale. Nella modalità preferita ma non esclusiva, si utilizza il movimento o calibro dell'orologio, in quanto è un componente di alto valore, complesso e interno, la cui sostituzione, anche parziale di un solo componente è un evento raro e tracciabile. La sua superficie, anche se prodotta con le massime tolleranze, presenta a livello microscopico delle imperfezioni stocastiche (micro-graffi, variazioni di texture, inclusioni minime nel materiale) che sono uniche per ogni singolo pezzo. Queste imperfezioni costituiscono la base della nostra PUF ottica. Detta prima fase comprende le seguenti attività:

1.1. Acquisizione dell'Immagine 3D: Per catturare queste caratteristiche, si impiega uno scanner 3D ottico ad alta risoluzione. Le tecnologie preferite per questa fase sono la scansione a luce strutturata o la scansione laser confocale. Questi sistemi proiettano un pattern di luce (nel caso della luce strutturata) o un punto laser (nel caso della scansione confocale) sulla superficie del calibro e ne acquisiscono la deformazione o il riflesso tramite una o più telecamere ad alta sensibilità. Il risultato di questa scansione è una nuvola di punti (point cloud) tridimensionale ad alta densità, che rappresenta una mappa topografica dettagliata della superficie del calibro con una precisione micrometrica o sub-micrometrica. In questo contesto è fondamentale che la fase di acquisizione avvenga in un ambiente controllato per garantire la ripetibilità e la qualità della scansione. Ciò include un sistema di fissaggio stabile per il calibro, un'illuminazione controllata per minimizzare riflessi

e ombre (ad esempio, utilizzando luce polarizzata o diffusa), e una calibrazione accurata dello scanner.

1.2. Pre-elaborazione della Nuvola di Punti: La nuvola di punti grezza ottenuta dalla scansione richiede una fase di pre-elaborazione per essere utilizzabile. Questa fase comprende:

- Filtraggio del Rumore: Vengono applicati filtri statistici (es. Statistical Outlier Removal) per eliminare i punti isolati (outlier) che non appartengono alla superficie reale, ma sono dovuti a rumore del sensore o a riflessi spuri.
- Allineamento e Normalizzazione: La nuvola di punti viene allineata a un sistema di coordinate di riferimento e normalizzata in scala e orientamento. Questo passaggio è essenziale per garantire che le scansioni successive dello stesso oggetto siano confrontabili, indipendentemente da piccole variazioni nel suo posizionamento durante la scansione.
- Stima delle Normali: Per ogni punto della nuvola, viene calcolata la normale alla superficie locale. Questa informazione è fondamentale per gli algoritmi di estrazione delle caratteristiche.

1.3. Estrazione delle Caratteristiche (Feature Extraction): Una volta pulita e normalizzata la nuvola di punti, si procede all'estrazione delle caratteristiche che costituiranno il fingerprint. Questo non si basa sull'intera nuvola di punti (che sarebbe troppo pesante da gestire), ma su un insieme di descrittori locali calcolati in punti di interesse (keypoints). Detti keyoints essendo collegati alle seguenti attività:

- Identificazione dei Keypoints: Vengono utilizzati

algoritmi come l'Intrinsic Shape Signatures (ISS) per identificare punti geometricamente salienti e stabili sulla superficie, come angoli, spigoli o punti ad alta curvatura. Questi punti sono meno suscettibili a essere alterati da piccole variazioni o rumore.

- Calcolo dei Descrittori Locali: Attorno a ciascun keypoint, viene calcolato un descrittore locale che ne codifica la geometria circostante. Un descrittore particolarmente efficace per questo scopo è il Fast Point Feature Histogram (FPFH). L'FPFH crea un istogramma multidimensionale che rappresenta le relazioni geometriche tra il keypoint e i suoi vicini, risultando robusto a rumore e a piccole deformazioni. Altri descrittori validi includono SHOT (Signature of Histograms of OrienTations) o Spin Images.

1.4. Generazione del Fingerprint Binario: L'insieme dei descrittori FPFH calcolati per tutti i keypoints costituisce una rappresentazione ricca ma ancora troppo complessa. Per ottenere un fingerprint compatto, efficiente e facilmente confrontabile, si procede a una fase di binarizzazione.

- Aggregazione: I vettori dei descrittori vengono aggregati in un'unica grande matrice di caratteristiche.
- Hashing Sensibile alla Località (Locality-Sensitive Hashing, LSH): Questa matrice viene processata tramite un algoritmo di LSH. L'LSH ha la proprietà di mappare punti dati simili (in questo caso, descrittori geometrici simili) allo stesso "bucket" con alta probabilità, mentre mappa punti dati dissimili a bucket diversi. Applicando

una serie di funzioni LSH, si ottiene un codice hash binario (una stringa di 0 e 1) di lunghezza fissa (es. 256 o 512 bit). Questo codice binario è il fingerprint finale: una rappresentazione compatta e robusta della micro-geometria unica del calibro.

Il succitato processo, dalla scansione alla generazione del fingerprint binario, viene eseguito preferibilmente utilizzando librerie software specializzate nell'elaborazione di dati 3D, come Open3D, e per l'hashing, come datasketch.

2. Creazione e Gestione del Token Digitale: Il fingerprint binario generato è il nucleo del token digitale, che funge da certificato di autenticità elettronico. Detta seconda fase comprende in una attuazione vantaggiosa le seguenti attività:

2.1. Composizione del Token: Il token digitale è un pacchetto di dati strutturato, preferibilmente in formato JSON (JavaScript Object Notation), che include ad esemepio:

- puf_fingerprint: Il fingerprint binario a 256 o 512 bit.
- metadata: Un insieme di metadati essenziali sull'orologio, come:
    - brand: Marca
    - model: Modello
    - serial_number: Numero di serie univoco dell'orologio
    - production_year: Anno di produzione
    - movement_caliber: Numero o nome del calibro.
    - lista dei proprietari (attuale e precedenti).
    - interventi e manutenzioni eseguite

sull’orologio
- ulteriori ed eventuali

- timestamp: Una marcatura temporale che indica la data e l'ora di creazione del token.

2.2. Crittografia del Token: Per garantire la riservatezza e l'integrità del token, questo viene cifrato prima di essere memorizzato o trasmesso. La modalità di cifratura preferita è l'algoritmo simmetrico AES (Advanced Encryption Standard) con una chiave a 256 bit, operante in modalità GCM (Galois/Counter Mode). La modalità GCM è scelta perché, oltre a garantire la confidenzialità (cifratura), fornisce anche l'autenticazione dei dati (integrità), proteggendo il token da modifiche non autorizzate.

La chiave di cifratura (K_device) è unica per ogni orologio. Essa non viene generata casualmente, ma derivata da una chiave master (K_master) custodita in un ambiente ultra-sicuro (HSM, come descritto più avanti) tramite una Funzione di Derivazione di Chiave basata su HMAC (HKDF). L'input per l'HKDF è la K_master e un "sale" (salt) unico per ogni dispositivo, che nella modalità preferita è l'identificativo univoco (UID) del chip NFC. Questo lega crittograficamente la chiave al componente hardware, aggiungendo un ulteriore livello di sicurezza.

3. Integrazione con il Chip NFC e il Secure Element: Il token digitale cifrato viene memorizzato nel chip NFC integrato nell'orologio. La scelta del chip è fondamentale per la sicurezza del sistema. Detta terza fase comprende in una attuazione vantaggiosa le seguenti attività:

3.1. Scelta del Chip NFC: Preferibilmente ma non

necessariamente si selezionerà un chip NFC passivo (non richiede alimentazione propria, ma viene attivato dal campo magnetico del lettore) che incorpora un Secure Element (SE). Esempi di tali chip includono la serie NXP NTAG 5, la serie STMicroelectronics ST54J o la serie Infineon SLE. Un Secure Element è un microprocessore a prova di manomissione (tamper-resistant) con una propria memoria sicura e un proprio sistema operativo, certificato secondo standard di sicurezza come Common Criteria EAL5+ o superiori. Esso è progettato per resistere ad attacchi fisici (es. micro-sonde, attacchi a canale laterale, fault injection) e logici.

3.2. Provisioning del Chip: Durante la fase di produzione, il token digitale cifrato viene scritto nella memoria sicura del Secure Element. I dati sono incapsulati in un formato standard NFC, come il NDEF (NFC Data Exchange Format). Una volta scritto, il chip viene configurato in modo da bloccare ulteriori scritture non autorizzate. Le policy di accesso del Secure Element vengono impostate per permettere la lettura del token cifrato, ma per impedire in modo assoluto l'accesso in chiaro alla chiave di decifratura (K_device), che viene anch'essa caricata in modo sicuro nel SE e mai esposta all'esterno. Tutte le operazioni di decifratura per la verifica avverranno all'interno del perimetro sicuro del SE.

4. Registrazione su Blockchain: Per garantire l'immutabilità e la verificabilità pubblica (o consortile) dell'autenticità, si utilizza una piattaforma blockchain. Detta quarta fase comprende in una attuazione vantaggiosa le seguenti attività:

4.1. Scelta della Blockchain: La modalità preferita impiega una blockchain di tipo permissioned (autorizzata), come Hyperledger Fabric. Questo tipo di blockchain è preferibile a una pubblica (come Ethereum) per applicazioni aziendali, in quanto offre maggiore controllo sugli accessi, scalabilità, privacy e finalità delle transazioni. I partecipanti alla rete (nodi) sono entità note e autorizzate (es. il produttore, i centri di assistenza, i rivenditori autorizzati).

4.2. Registrazione dell'Hash: Per massimizzare la privacy e l'efficienza, sulla blockchain non viene registrato l'intero token digitale, ma solo un suo hash crittografico. Il processo è il seguente:

- Si calcola un hash del token digitale già cifrato utilizzando un algoritmo robusto come SHA-256 o SHA3-256.
- Questo hash, una stringa di 64 caratteri esadecimali, viene registrato sulla blockchain all'interno di uno smart contract (chiamato "chaincode" in Hyperledger Fabric).

La registrazione dell'hash di un dato cifrato garantisce che i dati originali (fingerprint e metadati) non siano mai esposti pubblicamente, ma fornisce un'ancora immutabile per la verifica. Qualsiasi minima alterazione del token cifrato produrrebbe un hash completamente diverso, rendendo la manomissione immediatamente rilevabile.

Lo smart contract gestisce la logica di business, inclusa la creazione di un asset digitale (simile a un NFT) che rappresenta l'orologio, associando l'hash al numero di serie e registrando il proprietario iniziale. Lo stesso smart contract gestirà i futuri trasferimenti

di proprietà.

5. Procedura di Verifica dell'Autenticità: Un operatore, con le dovute autorizzazioni, può verificare l'autenticità dell'orologio utilizzando un dispositivo di backend rappresentato da un comune personal computer al quale è collegato, via USB, uno scanner ottico 3D e un dispositivo di lettura/scrittura per chip NFC.

La prima fase consiste nella lettura del calibro (eventualmente anche del quadrante se così è previsto dal produttore) tramite scanner ottico 3D e si ottiene il fingerprint PUF della lettura (Ft).

La seconda fase consiste nel leggere e decriptare il fingerprint PUF depositato sul chip NFC poiché il sistema di backend dispone delle chiavi crittografiche (vedi punto 7.) quindi estrae il relativo fingerprint PUF di riferimento (Fm).

Si effettua poi il matching (autenticazione) fra i fingerprint PUF (Fm) e (Ft).

Si fissa una soglia di matching (θmatch) corrispondente al valore massimo di distanza accettabile tra il fingerprint PUF acquisito (Ft) e quello di riferimento (Fm) affinchè il matching sia valido. Tipico valore: 0,12-0,18 in termini di distanza normalizzata (ad es. Hamming o Euclidea su vettori binari).

Definizione pratica: Se, ad esempio, la distanza di Hamming tra i due hash binari è <= 0,15 (15%) la verifica è considerata positiva. Il valore preciso dipende dalla dimensione del fingerprint: per hash su 256 bit, ciò equivale a ~ 38 bit diversi permessi.

Se questo primo controllo restituisce esito positivo il sistema effettua le seguenti operazioni:

- Lettura NFC: L'operatore avvicina il dispositivo di lettura/scrittura NFC all'orologio. Il lettore

NFC attiva il chip passivo e legge il record NDEF contenente il token digitale cifrato.

- Invio al Backend (o Elaborazione Locale Sicura): L'applicazione invia il token cifrato a un backend sicuro gestito dal produttore. In un'implementazione alternativa ad altissima sicurezza, la decifratura potrebbe avvenire tramite un applet sicuro direttamente sul Secure Element del dispositivo di lettura/scrittura, se disponibile.
- Decifratura e Calcolo Hash: Il backend utilizza la chiave K_device appropriata (recuperata in modo sicuro dal suo sistema di gestione chiavi) per decifrare il token. Una volta ottenuto il token in chiaro, il backend ricalcola l'hash SHA-256 del token cifrato originale.
- Verifica su Blockchain: Il backend interroga la blockchain (tramite un nodo autorizzato) per recuperare l'hash di riferimento associato al numero di serie dell'orologio.
- Confronto e Risultato: Il backend confronta l'hash appena calcolato con l'hash recuperato dalla blockchain. In queste circostanze:
    - Se i due hash corrispondono, l'autenticità è confermata. L'applicazione mostra un esito positivo, visualizzando i metadati dell'orologio (marca, modello, ecc.) per un'ulteriore conferma visiva da parte dell'utente.
    - Se i due hash non corrispondono, il sistema segnala un'anomalia, indicando una possibile contraffazione o manomissione.

In conclusione, se il PUF appena letto risulta coerente

con il PUF estratto dal chip NFC e se l'hash del chip NFC corrisponde con l'hash salvato su blockchain l'orologio, in tutte le sue parti, è autentico.

6. Gestione delle Variazioni nel Tempo (Aggiornamento del Modello): Per garantire che il sistema rimanga robusto nel tempo, è previsto un meccanismo per gestire le piccole variazioni fisiologiche del fingerprint PUF (dovute a titolo esemplificativo e non limitativo a usura, polvere, ecc.).

Durante una verifica periodica (es. in un centro assistenza), viene eseguita una nuova scansione 3D e generato un nuovo fingerprint PUF. Questo nuovo fingerprint PUF viene confrontato con il fingerprint PUF di riferimento memorizzato nel token. La metrica di confronto è la distanza di Hamming tra i due codici binari (ovvero il numero di bit differenti) e in particolare:

- Se la distanza di Hamming è al di sotto di una soglia di matching (es. 15%), l'orologio è considerato autentico.
- Se la distanza è al di sotto di una soglia più restrittiva, detta soglia di aggiornamento (es. 10%), il sistema può aggiornare il modello di riferimento. L'aggiornamento non consiste in una sostituzione, ma in una media pesata con parametro α (ad esempio $\alpha=0,1$) tra il vecchio fingerprint PUF e quello nuovo, per adattarsi lentamente alle variazioni senza consentire cambiamenti drastici che potrebbero nascondere una manomissione.
- Se la distanza supera la soglia di matching, o se il "drift" cumulativo rispetto al fingerprint PUF originale supera una soglia di allarme, viene generata una segnalazione per un'ispezione

manuale.

Questo meccanismo di aggiornamento adattivo è una caratteristica chiave per la longevità e l'affidabilità del sistema.

7. Infrastruttura di Sicurezza (HSM e Gestione Chiavi): Tutta l'architettura di sicurezza si basa su una gestione rigorosa delle chiavi crittografiche. La chiave master (K_master) da cui tutte le chiavi dei dispositivi sono derivate, è generata e custodita all'interno di un Hardware Security Module (HSM). Un HSM è un apparato fisico dedicato, ultra-sicuro, che protegge le chiavi da qualsiasi accesso esterno. Le operazioni che coinvolgono la chiave master (come la derivazione delle K_device) avvengono all'interno dell'HSM stesso, senza che la chiave master venga mai esposta. Questo approccio centralizzato e ultra-sicuro alla gestione delle chiavi è fondamentale per l'integrità dell'intero sistema.

Applicabilità industriale

Il L'invenzione descritta trova la sua applicazione industriale primaria nel settore dei beni di lusso, e più specificamente nell'industria orologiera di alta gamma. La sua utilità industriale è manifesta e risponde a un'esigenza critica e crescente di questo mercato: la lotta alla contraffazione, la garanzia di autenticità e la tracciabilità del prodotto lungo tutto il suo ciclo di vita. L'applicabilità industriale può essere descritta sotto diversi profili. a. Produzione e Integrazione nella Catena di Montaggio: Il metodo descritto può essere integrato direttamente nel processo di produzione degli orologi. La fase di

generazione del fingerprint PUF tramite scansione 3D può essere inserita come una stazione di controllo qualità e registrazione alla fine della linea di assemblaggio del movimento o dell'orologio completo. Le stazioni di scansione e di provisioning del chip NFC possono essere automatizzate per gestire alti volumi di produzione. I produttori di orologi possono quindi offrire un prodotto che ha un certificato di autenticità digitale, intrinseco e non falsificabile, incorporato fin dall'origine. Questo aumenta il valore percepito del bene e rafforza la fiducia del consumatore nel marchio.

b. Gestione della Catena di Fornitura e Distribuzione: Il sistema offre uno strumento potente per la tracciabilità lungo la catena di fornitura. Ogni passaggio dell'orologio, dal produttore al distributore, al rivenditore autorizzato, può essere registrato sulla blockchain tramite la scansione del chip NFC. Questo crea una cronologia completa e immutabile del percorso del prodotto, aiutando a combattere il mercato grigio (vendite non autorizzate) e a garantire che i prodotti venduti attraverso i canali ufficiali siano autentici.

c. Mercato Secondario e Servizi Post-Vendita: L'invenzione ha un impatto industriale significativo sul mercato secondario (pre-owned). La possibilità di verificare in modo semplice e sicuro l'autenticità di un orologio facilita le transazioni tra privati e attraverso piattaforme di vendita specializzate, aumentando la liquidità e la sicurezza del mercato. I trasferimenti di proprietà possono essere gestiti tramite gli smart contract sulla blockchain, creando un registro di provenienza ufficiale e affidabile.

Inoltre, i centri di assistenza autorizzati possono utilizzare il sistema per registrare gli interventi di manutenzione, creando uno storico di servizio completo e verificabile, che contribuisce a mantenere il valore dell'orologio nel tempo.

d. Estensione ad Altri Settori Industriali: Sebbene la modalità preferita di attuazione sia descritta per gli orologi, il principio industriale è direttamente trasferibile ad altri settori che producono beni di alto valore e sono afflitti dal problema della contraffazione. Esempi includono:

- Gioielleria: Autenticazione di pietre preziose uniche (basandosi su inclusioni interne come PUF) o di gioielli di design.
- Arte: Creazione di un legame fisico-digitale per opere d'arte, utilizzando la micro-texture della pennellata o della superficie della scultura come PUF.
- Moda di Lusso: Autenticazione di borse, accessori o capi di alta moda, utilizzando le caratteristiche uniche del materiale (es. la grana della pelle) come base per il fingerprint.
- Vini e Distillati Pregiati: Autenticazione delle bottiglie, utilizzando le imperfezioni del vetro o del tappo come PUF per combattere la contraffazione e il rabbocco.
- Componenti Critici (Aeronautica, Automotive): Tracciabilità e autenticazione di componenti meccanici critici per garantirne l'origine e l'integrità, prevenendo l'uso di parti contraffatte o non conformi.

In sintesi, l'invenzione è suscettibile di un'applicazione industriale su larga scala, in quanto

fornisce una soluzione tecnologica robusta a un problema economico pervasivo. Il sistema può essere prodotto e utilizzato in un contesto industriale per creare, verificare e tracciare l'identità unica di oggetti fisici, generando valore per i produttori, sicurezza per i consumatori e trasparenza per l'intero mercato.

Mentre l'invenzione sopra descritta è suscettibile di varie modifiche e costruzioni alternative, alcune forme di realizzazione preferite sono state mostrate nell'esempio di realizzazione precedentemente illustrato.

Si deve intendere, comunque, che non vi è alcuna intenzione di limitare l'invenzione alla specifica forma di realizzazione illustrata, ma, al contrario, essa intende coprire tutte le modifiche, costruzioni alternative, ed equivalenti che ricadano nell'ambito dell'invenzione come definito nelle rivendicazioni allegate.

L'uso di "ad esempio", "ecc.", "oppure" indica alternative non esclusive senza limitazione a meno che non altrimenti indicato.

L'uso di "include" significa "include, ma non limitato a" a meno che non altrimenti indicato.

In particolare, il trovato potrà essere realizzato con equivalenti tecnici, con materiali o accorgimenti integrativi adatti allo scopo e all'ambito applicativo.

Conformazione e dimensionamento delle parti costituenti e dei prodotti realizzati potranno variare in maniera idonea, ma coerente con la soluzione proposta.

Le eventuali modifiche all'esemplare di realizzazione proposto, inclusive di regolazioni e

dimensionamento adeguati a specifiche ed ulteriori applicazioni, saranno facilmente deducibili da un tecnico del ramo adeguatamente istruito e senza uscire dall'ambito di protezione del brevetto rivendicato. Questo senza inficiare o eludere il nucleo inventivo dell'invenzione.

Stefano PEZZI
(Richiedente)