MINISTERO DELLO SVILUPPO ECONOMICO
DIREZIONE GENERALE PER LA LOTTA ALLA CONTRAFFAZIONE
UFFICIO ITALIANO BREVETTI E MARCHI

DOMANDA DI INVENZIONE NUMERO	**102018000010379**
Data Deposito	**16/11/2018**
Data Pubblicazione	**16/05/2020**

Classifiche IPC

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
H	04	L	9	32

Titolo

BLOCKCHAIN NEURALE

Descrizione Domanda di Brevetto Italiano avente per titolo: BLOCKCHAIN NEURALE

A nome: ABCD TECHNOLOGY SARL-Svizzera (CH)

* * * * * *

A28698 IM

La presente invenzione è relativa a un sistema implementato tramite computer e a un metodo implementato tramite computer per la archiviazione e il trasferimento sicuri di dati digitali di transazioni tra utenti di una rete per condivisione di dati.

Oggigiorno, per la registrazione sicura di transazioni tra due o più soggetti (ad esempio tra un venditore e un acquirente, tra un cittadino e un ufficio governativo o una banca, ecc.) vengono impiegati database distribuiti basati sui protocolli blockchain (d'ora in avanti denominati semplicemente "blockchain"). Le tecnologie basate su blockchain sono ben note nel settore (si veda ad esempio "Mastering Bitcoin. Unlocking Digital Crypto-Currencies", Andreas M. Antonopoulos, O'Reilly Media, 2014); in breve, esse possono essere definite come elenchi in continua crescita di record di dati (blocchi), collegati cronologicamente e resi sicuri tramite l'uso della crittografia; tipicamente, i dati registrati sono

transazioni. Blockchain della tecnica sono gestite da una rete peer-to-peer di dispositivi di elaborazione finali di utenti (nodi) che aderiscono a un protocollo per una comunicazione inter-nodo: l'aggiunta di nuovi blocchi di dati nella blockchain è controllata con il consenso tra la maggioranza dei nodi. L'integrità e la legittimità della blockchain è tipicamente garantita rendendo l'aggiunta di blocchi ingannevoli troppo costosa, da un punto di vista monetario o temporale. La blockchain della tecnologia maggiormente prevalente (blockchain della criptovaluta Bitcoin) registra tutte le informazioni relative a una transazione nei suoi blocchi, in modo inalterabile: un blocco viene aggiunto alla blockchain soltanto se autorizzato dalla maggioranza dei nodi della rete e l'autenticità del blocco aggiunto è garantita dalle funzioni crittografiche (funzioni hash unidirezionali); il calcolo della funzione è costoso, ma la verifica è rapida e computazionalmente facile (ad esempio, nella criptovaluta Bitcoin essa è implementata dalla rete di verifica non controllata dei miner).

I protocolli blockchain hanno due inconvenienti principali: in primo luogo, la rete

di verifica (rete dei miner) delle blockchain è altamente esigente in termini energetici (oggi, il consumo per verificare e gestire 1/1000° delle transazioni bancarie per i bitcoin richiede il bilancio energetico dell'Irlanda); in secondo luogo, tutti possono iscriversi, senza una certificazione che convalidi l'identità di un utente: potenzialmente, un numero enorme di account potrebbe essere generato e controllato dallo stesso utente, portando così a problemi di sicurezza.

La presente invenzione mira a risolvere i problemi di cui sopra per mezzo di un sistema implementato tramite computer e un metodo implementato tramite computer per la archiviazione di dati e la condivisione di dati sicure, impiegando un nuovo concetto di blockchain, denominato nella presente "blockchain neurale" e descritto in dettaglio di seguito.

L'invenzione fornisce inoltre una maggiore sicurezza per la archiviazione dei dati e la condivisione di dati, superando i limiti ben noti dei sistemi di autenticazione basati su nomi utente (username) e password, come ad esempio, tra gli altri, la necessità di un numero enorme di password diverse e complesse per aumentare la sicurezza di

informazioni (personali) e il rischio che password copiate o crackate diano accesso a una quantità enorme di dette informazioni.

Inoltre, la presente invenzione consente di includere oggetti come utenti di una rete di condivisione di dati. Gli oggetti fisici sono già usati per generare, archiviare e trasferire dati e in futuro si formeranno sempre più connessioni tra oggetti e con i loro dati (Internet delle cose, IoT, o Internet del tutto); tuttavia, i sistemi attuali per la condivisione sicura di dati non possono essere gestiti autonomamente da oggetti a causa della mancanza di un'identità affidabile e certificata automaticamente di detti oggetti e a causa della mancanza di capacità di detti oggetti di interagire in modo diverso a ogni diversa transazione. La presente invenzione è quindi mirata a risolvere anche questo problema.

La presente invenzione è relativa a un sistema implementato tramite computer per la archiviazione e il trasferimento sicuri di dati digitali tra utenti di una rete per condivisione di dati, comprendente:

(a) una pluralità di dispositivi di elaborazione per l'accesso degli utenti a una rete

per la condivisione di dati;

(b) un'identità digitale associata a ogni utente della rete e comprendente un mezzo di autenticazione configurato per generare automaticamente (ossia senza intervento umano) un nuovo codice di autenticazione in risposta a ogni nuova interrogazione per la verifica di identità;

(c) almeno un ente di certificazione in grado di autenticare l'identità digitale degli utenti della rete;

(d) almeno una transazione tra due o più utenti della rete, comprendente informazioni digitali che sono generate, possedute e/o condivise da almeno uno di detti due o più utenti, preferibilmente comprendente inoltre un contratto intelligente (smart contract) che definisce doveri e diritti di detti due o più utenti sulle informazioni digitali; in cui la transazione è autorizzata soltanto se le identità digitali di detti due o più utenti sono convalidate dall'almeno un ente di certificazione;

(e) almeno un repository digitale che archivia le informazioni digitali della transazione e che comprende un gateway per condividere dette informazioni digitali, in cui l'accesso a dette

informazioni digitali è reso sicuro dall'identità digitale dei due o più utenti coinvolti nella transazione: preferibilmente soltanto detti utenti possono avere accesso alle (ad almeno una parte delle) informazioni digitali, preferibilmente come definito in uno smart contract che è parte della transazione;

(f) un libro mastro (database ledger) personale basato su un protocollo simil-blockchain, associato a ciascun utente della rete, preferibilmente archiviato nel o connesso digitalmente al dispositivo di elaborazione dell'utente,

e strutturato in modo tale che, quando viene autorizzata una transazione tra due o più utenti, venga aggiunto un nuovo blocco ai database ledger personali associati a ciascuno di detti due o più utenti, in cui detto nuovo blocco registra soltanto gli indirizzi digitali di (collegamenti ipertestuali a) un repository digitale (repository digitali) che archivia (archiviano) le informazioni digitali della transazione. Pertanto, i blocchi del database ledger personale non registrano le informazioni digitali della transazione, che sono archiviate soltanto negli uno o più repository

digitali. Il database ledger personale di un utente comprende quindi un elenco dei repository digitali che archiviano informazioni digitali di tutte le transazioni che coinvolgono detto utente, ma non le informazioni digitali stesse.

L'invenzione è relativa inoltre a un metodo implementato tramite computer per la archiviazione e il trasferimento sicuri di dati digitali tra utenti di una rete per condivisione di dati, basato sul sistema implementato tramite computer dell'invenzione, il metodo comprendendo:

a) accesso di utenti, tramite un dispositivo di elaborazione, alla rete per la condivisione di dati;

b) trasmissione, a un ente di certificazione, di una transazione tra due o più utenti della rete;

c) autenticazione, da parte dell'ente di certificazione, delle identità digitali di detti utenti coinvolti nella transazione ed emissione di un certificato elettronico ai dispositivi di elaborazione dell'utente (degli utenti) di cui viene convalidata l'identità digitale;

d) autorizzazione della transazione;

e) esecuzione della transazione e archiviazione delle informazioni digitali della

transazione in uno o più repository digitali;

f) aggiunta di un nuovo blocco ai database ledger personali associati a ciascuno degli utenti coinvolti nella transazione, detto nuovo blocco registrando gli indirizzi digitali degli uno o più repository digitali in cui le informazioni digitali della transazione sono archiviate.

Forme di realizzazione preferite della presente invenzione verranno ora descritte con riferimento ai disegni allegati, in cui:

la figura 1 (Fig. 1) è una vista generale degli elementi del sistema implementato tramite computer (100) secondo l'invenzione e delle loro connessioni;

la figura 2 (Fig. 2) è una vista generale di elementi del sistema implementato tramite computer che interagiscono nel metodo dell'invenzione, in cui: (Fig. 2A) una transazione tra due utenti (103-1 e 103-2) è inviata alla rete (101) da un primo utente di detti due utenti (103-1) e una richiesta di autorizzazione della transazione è inviata a un ente di certificazione (105), l'ente di certificazione (105) interrogando quindi i mezzi di autenticazione (114-1 e 114-2) di detti due utenti; (Fig. 2B) la transazione è autorizzata

dall'autenticazione dell'identità digitale dei due utenti (104-1 e 104-2) da parte dell'ente di certificazione (105), attraverso i loro mezzi di autenticazione (114-1 e 114-2), e un certificato elettronico (113-1 e 113-2) è emesso a ciascun dispositivo di elaborazione (103) degli utenti validati (102'-1 e 102'-2);

la figura 3 (Fig. 3) è una vista generale di elementi del sistema implementato tramite computer che interagiscono nel metodo dell'invenzione, in cui nuovi blocchi (118), aggiunti ai database ledger personali (108-1 e 108-2) di un primo e un secondo utente validato (102'-1 e 102'-2) coinvolti in una transazione (106-1), comprendono entrambi un collegamento (ad esempio un collegamento ipertestuale) (109) al repository digitale (107-1) che archivia le informazioni digitali di detta transazione (106-1); il database ledger personale (108-2) del secondo utente è mostrato in modo da includere anche un blocco cronologicamente precedente che comprende un secondo collegamento (109') a un secondo repository digitale (106-2) che archivia le informazioni digitali di una seconda transazione (106-2) tra detto secondo utente (102'-2) e un terzo utente (non mostrato); lo stesso

secondo collegamento ipertestuale (109') essendo così registrato in un blocco del database ledger personale (108-3) di detto terzo utente;

la figura 4 (Fig. 4) mostra una forma di realizzazione preferita dell'invenzione in cui un repository digitale (107-1) che archivia le informazioni digitali di una transazione (106-1) è anche un utente validato (102'-5) della rete, che ha una propria identità digitale (104-5) ed è il seme per un nuovo database ledger personale (108-5), che registra transazioni che coinvolgono detto repository digitale (107-1);

la figura 5 (Fig. 5) mostra database ledger personali esemplificativi secondo l'invenzione, aventi (A) una struttura lineare quando i blocchi sono collegati cronologicamente o (B) una struttura ad albero in cui i blocchi sono collegati (anche) semanticamente, e che è ramificata, ad esempio sulla base di user-case diversi, o di diversi avatar degli utenti;

la figura 6 (Fig. 6) mostra un mezzo di autenticazione del tipo a impronta digitale (fingerprint), secondo una forma di realizzazione preferita dell'invenzione: il fingerprint può avere forme diverse visibili a occhio nudo (A), quando

illuminato con un dispositivo di misurazione ottica a lunghezze d'onda diverse (B), o quando analizzato a risoluzioni diverse (C), o può fornire valori diversi in corrispondenza degli stessi punti quando misurato con dispositivi di misurazione diversi (D).

Secondo l'invenzione, la rete per condivisione di dati (101) può avere una qualsiasi topologia e/o disposizione di rete di comunicazione; preferibilmente la rete è Internet.

Gli elementi del sistema implementato tramite computer (100) sono connessi tra loro attraverso qualsiasi mezzo cablato e/o senza fili adatto, in grado di comunicare e inviare dati digitali tra loro e nella rete; preferibilmente, gli elementi del sistema (100) sono connessi tramite mezzi senza fili.

Un "utente" come definito nella presente è un soggetto che accede alla rete per condivisione di dati (101) attraverso un dispositivo di elaborazione (103). Ad esempio, un utente può essere una persona che usa un dispositivo di elaborazione, o può essere un oggetto che comprende un dispositivo di elaborazione (connesso a o incorporato in detto oggetto). In forme di

realizzazione preferite dell'invenzione, almeno uno degli utenti della rete è un oggetto che comprende un dispositivo di elaborazione, preferibilmente un oggetto con intelligenza artificiale.

Secondo l'invenzione, ogni utente della rete ha un'identità fisica e una digitale (104), tramite cui detto utente è identificabile univocamente; secondo l'invenzione, ogni utente è pertanto associato biunivocamente a un'identità digitale, che è specifica di ogni utente.

Il termine "biunivocamente" significa che si verifica una corrispondenza uno a uno; ad esempio, quando riferito ad un utente e alla sua identità digitale, si intende che per detto utente esiste una e una sola identità digitale e che ogni specifica identità digitale identifica uno e un solo utente.

L'"identità digitale" (104) di un utente è caratterizzata dal fatto di comprendere un mezzo di autenticazione (114) per autenticare univocamente l'identità dell'utente.

Il "mezzo di autenticazione" (114) è un qualsiasi mezzo in grado di generare e trasmettere un codice di autenticazione (come ad esempio, senza limitazioni, una chiave o una password) da

verificare per validare l'identità dell'utente.

Il mezzo di autenticazione (114) può essere un archivio di valori digitali e/o analogici, e il codice di autenticazione può essere composto di una stringa casuale di un sottoinsieme di detti valori digitali e/o analogici. Secondo l'invenzione, detto codice di autenticazione è verificato da un ente di certificazione (105): in risposta a ogni nuova interrogazione da parte dell'ente di certificazione (105), un nuovo codice di autenticazione (diverso da qualsiasi codice di autenticazione precedente generato dal mezzo di autenticazione) viene generato dal mezzo di autenticazione (114).

Preferibilmente, l'identità digitale (104) di un utente (102) include uno username pubblico.

Opzionalmente, l'identità digitale (104) di un utente (102) comprende uno o più avatar, tutti collegati allo stesso mezzo di autenticazione. Un "avatar" per un dato utente può essere ad esempio uno username secondario, usato per un certo tipo di transazione, che consente la certificazione attraverso il mezzo di autenticazione (114), dell'identità digitale, garantendo la privacy.

Quando il codice di autenticazione generato da un mezzo di autenticazione (114) è autenticato

(validato) da un ente di certificazione (105), l'identità digitale dell'utente è confermata e viene emesso un certificato elettronico (113) (si veda la Fig. 2); l'utente è quindi un "utente validato", la cui identità (validata e certificata) è fidata.

Una "transazione" (106) tra due o più utenti (102) della rete (101) comprende le informazioni digitali generate, possedute e/o condivise da almeno uno dei due o più utenti.

Ad esempio, una transazione comprende la o consiste nella condivisione di dette informazioni digitali tra due o più utenti.

"Informazioni digitali" nel contesto della presente invenzione possono essere dati (grezzi o elaborati), un programma software, uno smart contract, o un modo per esprimere/rappresentare valori (come ad esempio bitcoin o altre criptovalute, senza essere esaustivi).

Secondo la presente invenzione, una transazione (106) è autorizzata soltanto se le identità digitali (104) di detti due o più utenti (102) sono validate.

Pertanto, diversamente dai database basati su protocolli blockchain della tecnica, in cui una

transazione è autorizzata tramite il consenso della rete di verifica (ad es. il metodo proof-of-work per gli scambi di criptovaluta Bitcoin), le transazioni (106) nel sistema implementato tramite computer (100) dell'invenzione sono autorizzate tramite la verifica delle identità digitali (104) degli utenti (102) coinvolti nella transazione, attraverso l'autenticazione del mezzo di autenticazione (114) della loro identità digitale da parte di un ente di certificazione (105). Preferibilmente, l'autorizzazione di una transazione è trasmessa alla rete.

Come semplice esempio, un ente di certificazione (105) può essere una banca o un governo che autorizza una transazione (106) tra due utenti validati (102'), in cui un bene viene venduto/acquistato.

Preferibilmente, il sistema implementato tramite computer (100) comprende vari enti di certificazione (105), in cui ogni ente di certificazione è configurato per autorizzare un tipo specifico di transazione.

Opzionalmente, l'ente di certificazione (105) può essere esso stesso un utente (102) della rete (101), coinvolto in una data transazione (106): ad

esempio, quando una transazione (106-1) include la vendita/l'acquisto di un bene tra due utenti (102-1 e 102-2), l'ente di certificazione (105-1) che autorizza detta transazione (106-1) può essere esso stesso coinvolto in un'ulteriore transazione (106-2) con detti due utenti, ad esempio per il pagamento di tasse sulla vendita/l'acquisto di detto bene o di altro bene: in questo caso, un ulteriore ente di certificazione (105-2) può autenticare l'identità digitale (104-1) del primo ente di certificazione (105-1) coinvolto nell'ulteriore transazione (106-2) come utente.

Secondo l'invenzione, le informazioni digitali di una transazione (106) sono archiviate in almeno un repository digitale (107) (si veda la Fig. 3).

Un "repository digitale" (107) è un qualsiasi supporto o sistema digitale in grado di archiviare informazioni digitali. Esempi di repository digitale adatti sono: un disco rigido, un cloud, un fog, una chiave USB, ecc. Un repository digitale può essere connesso ad altri repository digitali attraverso la rete per condivisione di dati, ad esempio Internet.

In una forma di realizzazione preferita, il repository digitale (107) che archivia informazioni

digitali di una transazione tra due o più utenti (102) è reso sicuro dalle identità digitale (104) di detti due o più utenti (102), cosicché soltanto utenti validati (102') coinvolti nella transazione (106) possono accedere agli uno o più repository digitali (107) che archiviano le informazioni digitali di detta transazione (106).

Avendo accesso alle informazioni digitali archiviate in uno o più repository digitali (107), gli utenti validati (102') coinvolti in una transazione (106) sono in grado di leggere dette informazioni; preferibilmente gli utenti validati (102') non possono modificare le informazioni digitali.

Preferibilmente, l'ente di certificazione (105) che autentica un'identità digitale di un utente, e che non è un utente della transazione, non ha alcun accesso alle informazioni digitali generate, possedute o condivise da detto utente.

Opzionalmente, le informazioni digitali di una transazione possono essere archiviate in un database su fog (ad es. invece che in un database su cloud o un supporto di memoria locale), cosicché parti diverse delle informazioni digitali sono archiviate in repository digitali diversi.

Preferibilmente, le informazioni digitali di una transazione sono distribuite in vari repository digitali, potenzialmente un repository diverso per ogni utente coinvolto nella transazione.

Opzionalmente, la transazione comprende o consiste in uno smart contract, che definisce diritti e doveri degli utenti coinvolti sulle informazioni digitali della transazione. Ad esempio, uno smart contract può definire quale utente ha accesso a quali informazioni digitali della transazione. L'utente (102) della transazione (106) può quindi avere accesso soltanto a uno o più repository digitali (107) che archiviano le informazioni digitali, ma non a tutti, avendo così accesso soltanto a una porzione di dette informazioni digitali, come definito nello smart contract.

L'accesso alle informazioni digitali può essere pubblico o privato come definito ad esempio nello smart contract.

Gli indirizzi digitali dei repository digitali (107) che archiviano almeno parte delle informazioni di una transazione (106) sono registrati nei blocchi dei database ledger personali (108) associati a ogni utente della

transazione (si veda la fig. 3), preferibilmente in forma di un collegamento ipertestuale o in qualsiasi altra forma adatta in grado di creare una connessione al repository digitale.

I database ledger personali (108) del sistema implementato tramite computer (100) dell'invenzione si basano su un protocollo "simil-blockchain", dato che condividono alcune delle, ma non tutte le, caratteristiche tipiche di una blockchain: i database ledger personali (108) secondo l'invenzione sono infatti un elenco crescente di blocchi che includono una chiave crittografica (ad es. una funzione di hash), che collega ogni nuovo blocco al precedente, e un timestamp. Tuttavia, differiscono dalle tipiche blockchain della tecnica almeno per il fatto che i blocchi non registrano le informazioni digitali di una transazione (106), ma soltanto l'indirizzo dei repository (107) che archiviano dette informazioni, e per il fatto che l'aggiunta di nuovi blocchi (118) non è gestita da una rete paritetica di nodi, ma dalla validazione delle identità digitali (104) degli utenti da parte di un ente di certificazione (105), come descritto sopra.

Opzionalmente, i blocchi di un database ledger

personale (108) possono (anche) essere collegati semanticamente quando contengono uno stesso hashtag o parola chiave, opzionalmente gestiti da un avatar dedicato. Ad esempio, tutti i blocchi di un database ledger personale (108), degli stessi utenti o di utenti diversi (102), relativi a transazioni bancarie possono essere collegati da un hashtag comune (ad esempio #banca), essendo così tutti ricercabili con questo hashtag comune. I database ledger personali (108) di uno stesso utente (102) possono quindi avere una forma lineare (si veda nella Fig. 5A), quando i blocchi sono collegati soltanto cronologicamente, o possono avere una forma ad albero (si veda la Fig. 5B), quando i blocchi sono collegati (anche) semanticamente.

Preferibilmente, i database ledger personali sono pubblici o accessibili da utenti non coinvolti nella transazione, ma le informazioni digitali di una transazione archiviata nel repository digitale il cui indirizzo è registrato nel database ledger personale sono private e accessibili soltanto da almeno uno degli utenti validati coinvolti nella transazione.

In una forma di realizzazione preferita, una

transazione (106) comprende uno smart contract che include un modulo (form) che riporta i dati di utenti coinvolti nella transazione, e il sistema implementato tramite computer (100) è configurato in modo tale che, quando detta transazione (106) viene autorizzata, un hashtag che identifica il tipo di transazione è generato automaticamente nei blockchain personali (108) di detti utenti coinvolti.

Quando un utente è un oggetto, gli enti di certificazione preferiti possono essere, senza limitazioni, il produttore dell'oggetto e/o il proprietario dell'oggetto.

Secondo forme di realizzazione preferite dell'invenzione, i repository digitali (107) e gli stessi enti di certificazione (105) possono anche essere utenti della rete (101). Preferibilmente, quando un repository digitale (107-1), che archivia le informazioni digitali di una prima transazione (106-1), è un utente validato (102'-5) di una ulteriore transazione, un (primo o nuovo) blocco può essere generato in un database ledger personale (108-5) associato al repository digitale (si veda la Fig. 4).

Quando un utente della rete (101) è un

repository digitale (107) per la archiviazione remota di informazioni digitali, come ad esempio un server cloud, l'ente di certificazione (105) può essere, senza limitazioni, il fornitore (provider) di detto repository digitale.

Un repository digitale (107) secondo l'invenzione può anche agire da ente di certificazione (105), in grado di autenticare l'identità digitale di un utente.

Un'identità digitale può essere attribuita anche ai file archiviati in un repository: ad esempio, l'identità digitale di un file può comprendere il nome del file e il mezzo di autenticazione dell'identità digitale del repository che archivia il file.

Secondo forme di realizzazione preferite, il mezzo di autenticazione (114) del sistema implementato tramite computer (100) dell'invenzione è un token hardware o una funzione fisica non clonabile (PUF, Physical Unclonable Function). Nella maggior parte delle forme di realizzazione preferite, il mezzo di autenticazione è un fingerprint che comprende una pluralità di punti aventi proprietà materiali misurabili, e che comprende inoltre un processore in grado di

eseguire un protocollo che genera il codice di autenticazione cifrando valori ottenuti misurando almeno una di dette proprietà materiali misurabili in corrispondenza di uno o più punti del fingerprint per mezzo di un dispositivo di misurazione.

Una "proprietà materiale misurabile" è una qualsiasi proprietà analogica misurabile, come ad esempio una qualsiasi proprietà fisica o chimica, e la cui misurazione restituisce un valore. Ad esempio, le proprietà materiali misurabili di un fingerprint possono essere proprietà ottiche, elettriche, topografiche, meccaniche, termiche, magnetiche, chimiche, e loro combinazioni.

Il fingerprint, secondo forme di realizzazione preferite dell'invenzione, è quindi un archivio di valori ottenibili misurando una o più delle sue proprietà materiali in corrispondenza di uno o più punti del fingerprint; il fingerprint può generare codici di autenticazione composti da una stringa casuale di detti valori. Il codice di autenticazione può quindi essere generato misurando proprietà materiali di un sottoinsieme di punti, ottenendo valori, combinando casualmente una stringa di detti valori e trasponendola in un

codice tramite un algoritmo.

Preferibilmente, detto fingerprint ha fino a circa 10^6 punti per mm^2 aventi proprietà materiali misurabili diverse.

WO2015140731 descrive film sottili (etichette) ottenuti tramite deposizione chimica da vapore a fascio (CBVD, Chemical Beam Vapor Deposition), adatti come mezzo di autenticazione a fingerprint secondo la presente invenzione. Detti film sottili possono essere modellati simultaneamente e letti a scale diverse per fornire un'ampia gamma di proprietà materiali diverse (pattern con risoluzione da nanometrica a (sub)millimetrica, si veda ad esempio la Fig. 7); il processo di produzione descritto in WO2015140731 consente di ottenere più di 10^{20} configurazioni diverse nello stesso processo di deposizione, portando così potenzialmente a più di 10^{20} identità digitali diverse comprendenti detti film sottili come mezzo di autenticazione. Con una quantità così enorme di valori complessi incorporati nel film, il fingerprint fornisce un'identità elettronica non clonabile agli utenti, in quanto è impossibile da falsificare, anche con ingenti investimenti, senza conoscere l'esatta configurazione

dell'apparecchiatura e tutti i parametri di processo usati per la crescita dei film sottili. Questo rende impossibile contraffare il film tramite reverse engineering. Misurando e combinando un numero così elevato di proprietà materiali misurabili, è possibile generare un numero enorme di codici di autenticazione diversi con un singolo fingerprint. I codici di autenticazione generati dal fingerprint, un codice nuovo a ogni interrogazione, possono essere inseriti in un gateway per impedire un accesso remoto indesiderato ad esempio a un repository digitale.

La variabilità delle proprietà materiali in funzione degli stimoli, algoritmi matematici (firmware variabile usato come codice di cifratura), o i diversi dispositivi di misurazione usati, forniscono un numero molto elevato di valori e combinazioni dei valori possibili ottenibili con lo stesso fingerprint. L'interrogazione da parte dell'ente di certificazione può variare qualsiasi parametro con un numero infinito di possibili risposte che vanno oltre ciò che potrebbe essere memorizzato in un database software binario. Il fingerprint può in questo modo generare un nuovo codice in risposta ad ogni interrogazione, detto

codice essendo impossibile da predire. Ogni transazione può quindi essere autenticata e certificata univocamente.

Preferibilmente, il fingerprint dell'invenzione è un film ottenuto tramite deposizione chimica da vapore a fascio (CBVD). È noto che gli ossidi, che possono essere depositati tramite il processo CBVD, possiedono proprietà multifunzionali (ossia proprietà diverse simultanee) che vengono facilmente regolate tramite piccole modifiche della composizione materiale e del processo di deposizione. Ossidi preferiti impiegati nel processo CBVD di produzione del film comprendono TiO_2 (ossido di titanio), HfO_2 (ossido di afnio), ZrO_2 (ossido di zirconio), Al_2O_3 (ossido di alluminio), Si (silice), ZnO (ossido di zinco), Ta_2O_5 (pentossido di tantalio), ossidi di vanadio, Nb_2O_5 (pentossido di niobio), $LiNbO_3$ (niobato di litio), $LiTaO_3$ (niobato di tantalio).

Preferibilmente, nel sistema di computer dell'invenzione, l'identità digitale associata biunivocamente a ogni utente comprende un fingerprint unico.

"Unico" riferito a un fingerprint significa che il fingerprint associato a un dato utente è

diverso dal fingerprint dell'identità digitale associata a un altro utente; ad esempio, un fingerprint è unico quando differisce da altri fingerprint in almeno una delle sue proprietà materiali misurabili, e/o in almeno uno dei valori ottenuti misurando una o più delle sue proprietà materiali misurabili in corrispondenza di un dato punto. Ad esempio, in corrispondenza di un dato punto di coordinate *x, y* è possibile misurare una o più proprietà materiali ottenendo un valore specifico che è unico per detto punto/detta proprietà per un dato fingerprint. Inoltre, la combinazione di detti valori può fornire una stringa di valori unica per ogni fingerprint.

Preferibilmente, il sistema di computer comprende inoltre almeno un fingerprint gemello associato a ogni fingerprint. Un "fingerprint gemello" è una copia identica del fingerprint, le cui proprietà materiali misurabili sono identiche in ogni punto a quelle del fingerprint a cui il fingerprint gemello è associato. Preferibilmente, il sistema implementato tramite computer dell'invenzione comprende un singolo fingerprint gemello per ciascun fingerprint di ciascun utente; opzionalmente, il sistema di computer

dell'invenzione comprende due o più copie di un fingerprint gemello.

Il fingerprint gemello, secondo forme di realizzazione preferite dell'invenzione, comprende un processore in grado di comunicare con il fingerprint a cui è associato e di decifrare il codice di autenticazione generato dal fingerprint dell'utente. Ogni fingerprint gemello è preferibilmente in grado di comunicare con il fingerprint a cui è associato con un linguaggio unico, in base alla cifratura unica di valori specifici per ogni fingerprint e alla decifratura tramite il fingerprint gemello.

Preferibilmente, il sistema implementato tramite computer dell'invenzione comprende molteplici fingerprint gemelli per ogni fingerprint, per avere un backup e/o aumentare resilienza e accuratezza nella lettura/misurazione delle proprietà del fingerprint, o evitare l'esposizione eccessiva di un singolo server a un numero enorme di interrogazioni.

In forme di realizzazione preferite dell'invenzione, l'ente di certificazione (105) è un repository di tipo hardware centrale remoto, connesso digitalmente ai mezzi di autenticazione a

fingerprint delle identità digitali degli utenti; più preferibilmente, esso archivia i fingerprint gemelli associati a detto fingerprint; opzionalmente, una o più copie di un fingerprint gemello sono archiviate in repository di tipo hardware centrali diversi. Opzionalmente, un ente di certificazione, che archivia un fingerprint gemello e in grado di emettere un certificato elettronico di autenticazione alla convalida di un fingerprint, può comunicare digitalmente con altri enti di certificazione e trasferire il certificato a detti altri enti di certificazione.

L'ente di certificazione è configurato preferibilmente per eseguire un protocollo di autenticazione per autenticare il fingerprint che include: interrogare il fingerprint ottenendo un codice di autenticazione, decifrare detto codice di autenticazione per mezzo del fingerprint gemello, confermare l'autenticazione del fingerprint ed emettere un certificato di autenticazione.

Il fingerprint e il suo fingerprint gemello possono inoltre essere usati in un metodo di criptazione simil-cifrario, sulla base dell'archivio di proprietà materiali del fingerprint, in cui due (o più) fingerprint

identici (il fingerprint dell'utente e l'uno o più fingerprint gemelli) sono usati come chiavi di cifratura "puramente hardware".

In forme di realizzazione preferite, i fingerprint sono impacchettati con (sistema su chip) o fatti crescere monoliticamente su un dispositivo di misurazione in grado di misurare detta almeno una proprietà materiale misurabile.

I fingerprint secondo forme di realizzazione preferite dell'invenzione possono essere inoltre in grado di cifrare e decifrare informazioni. Ad esempio, un fingerprint di un'identità digitale di utente può essere usato come mezzo crittografico che consente la cifratura delle informazioni digitali archiviate nel repository digitale, la cui decifratura può essere eseguita soltanto tramite il fingerprint gemello.

Gli utenti validati (102') coinvolti in una data transazione (106), i repository digitali (107) che archiviano le informazioni di detta transazione (106), i blocchi dei ledger personali (108) degli utenti che registrano gli indirizzi digitali di detti repository digitali (107), sono tutti collegati tra loro nel sistema implementato tramite computer dell'invenzione. In particolare, i

database ledger personali (108) del sistema implementato tramite computer (100) dell'invenzione sono collegati tramite ciò che qui viene denominato "collegamenti neurali": i blocchi di ledger personali (108) di utenti diversi, che registrano lo stesso collegamento ipertestuale su almeno un repository digitale (107) che archivia le informazioni digitali di una data transazione (106) tra detti utenti diversi, sono collegati tra loro tramite ciò che qui viene denominato "collegamento neurale esterno" (109, Fig. 3). Inoltre, secondo forme di realizzazione preferite dell'invenzione, i blocchi di database ledger personali degli stessi utenti o di utenti diversi possono essere collegati semanticamente tramite un "collegamento neurale interno" (110) (si veda la Fig. 5B).

I collegamenti neurali (interni e/o esterni) che connettono i blocchi dei database ledger personali del sistema di computer dell'invenzione formano ciò che nella presente viene denominata "blockchain neurale".

L'interconnessione dei database ledger personali del sistema di computer connette inoltre tutti gli utenti che accedono alla rete per condivisione di dati la cui identità sia

certificata. Infatti, ogni nuovo collegamento neurale è creato soltanto dopo l'autorizzazione di una transazione, quindi dopo l'autenticazione delle identità digitali degli utenti della transazione. In questo modo, ogni collegamento neurale contribuisce a rafforzare il protocollo di autenticazione degli utenti coinvolti e la Fiducia (Trust) della blockchain di ogni utente che può essere resa quantitativa.

L'autenticazione di identità digitali di utenti, secondo l'invenzione, crea relazioni di fiducia indipendenti tra gruppi di utenti della rete coinvolti in una transazione; tanto maggiore è il numero di transazioni tra utenti della rete (e di conseguenza il numero di utenti validati), quanto più cresce la rete di utenti fidati (validati).

Il livello di Fiducia (Trust) può anche essere estrapolato da sottocategorie (approccio semantico) in funzione del numero di collegamenti neurali che supportano un utente in tale sottocategoria.

Il sistema di computer dell'invenzione consente di connettere verticali diverse e crea una rete di terza generazione, il cui contenuto è completamente tracciabile e certificato dai propri

utenti senza alcuna governance (governo) fornita da un numero limitato di autorità di certificazione di controllo (gli enti di certificazione).

Inoltre, i database ledger personali dell'invenzione forniscono un record di transazioni che richiede molto meno spazio di memoria rispetto alle blockchain tipiche, dato che registrano soltanto gli indirizzi dei repository digitali che archiviano effettivamente le informazioni digitali. Preferibilmente, i repository digitali sono generati in un numero ridotto, principalmente a scopo di backup.

Esempi non limitativi del metodo e del sistema implementato tramite computer, secondo forme di realizzazione preferite dell'invenzione, sono forniti di seguito.

ESEMPIO 1

In una forma di realizzazione esemplificativa dell'invenzione, l'identità digitale (104) di un primo utente (102-1) comprende un mezzo di autenticazione a fingerprint (114) avente, tra le altre, proprietà materiali ottiche.

Detto fingerprint (114) è fatto crescere monoliticamente direttamente su un sensore CMOS (ASIC) che agisce da dispositivo di misurazione.

Quando illuminato da LED di lunghezze d'onda diverse, il fingerprint fornisce colori iridescenti con diversa riflettività. Il sensore CMOS legge i dati dal fingerprint illuminato a lunghezze d'onda di luce diverse e associa le misurazioni a valori in una tabella alfa. Dal fingerprint è estratta casualmente una stringa di almeno 10-12 valori, fornendo così un codice di autenticazione, validabile da un ente di certificazione.

ESEMPIO 2

Una transazione (106) tra due utenti (102) è inviata alla rete (101) per condivisione di dati attraverso i dispositivi di elaborazione (103) di detti utenti. L'identità digitale (104) dei due utenti è verificata da un ente di certificazione (105) che confronta i codici di autenticazione generati dai fingerprint di detti due utenti con il codice di autenticazione fornito dai rispettivi fingerprint gemelli archiviati dall'ente di certificazione, letti nello stesso modo. Con la affermata autenticazione dei fingerprint, viene emesso un certificato elettronico (113) al dispositivo di elaborazione (103) di ogni utente validato (102') e la transazione è autorizzata ed eseguita. Le informazioni digitali relative alla

transazione sono quindi archiviate in almeno un repository digitale (107), mentre un nuovo blocco (118) viene aggiunto ai database ledger personali (108) di ciascuno dei due utenti validati (102'), registrando l'indirizzo digitale di detto almeno un repository digitale (107).

Vengono così creati collegamenti neurali (109) tra il repository digitale (107) e i database ledger personali (108) dei due utenti.

Le informazioni digitali della transazione archiviate sono accessibili soltanto a detti due utenti dopo la validazione delle loro identità digitali a ogni nuova connessione al repository digitale (107).

ESEMPIO 3

Un fingerprint di un utente e il suo fingerprint gemello, secondo forme di realizzazione preferite dell'invenzione, sono usati in un metodo simil-cifrario di criptazione di informazioni, come segue. Il fingerprint dell'utente è interrogato per l'autenticazione illuminando lo stesso con una prima lunghezza d'onda w1 in corrispondenza di un dato punto del fingerprint alle coordinate *x*, *y*. L'intensità di luce emessa dal fingerprint in corrispondenza di detta posizione viene misurata da

un dispositivo di misurazione e viene ottenuto un valore (*x*, *y*, I1); associando a detto valore un carattere alfanumerico, viene cifrato un messaggio (*x*, *y*, #). Una seconda lunghezza d'onda w2 viene usata per illuminare lo stesso fingerprint sulla stessa posizione e viene misurato un secondo valore di intensità di luce (*x*, *y*, I2) ottenendo un codice di autenticazione (*x*, *y*, I2). Il codice di autenticazione è trasferito al processore di un repository di tipo hardware che archivia il fingerprint gemello. La lunghezza d'onda w2 è usata per illuminare il fingerprint gemello sulla stessa posizione (*x*, *y*), autenticando il codice di autenticazione (*x*, *y*, I2), quindi la prima lunghezza d'onda w1 viene usata per illuminare il fingerprint gemello in corrispondenza della posizione (*x*, *y*), ottenendo il valore (*x*, *y*, I1) e decifrando il messaggio (*x*, *y*, #).

È possibile ottenere un effetto simile illuminando con una singola lunghezza d'onda due fingerprint nello stesso punto, modificando al contempo le loro proprietà materiali applicando una stimolazione esterna (ossia un campo elettrico per materiali optoelettrici).

Un effetto simile può anche essere ottenuto

applicando stimoli (elettrici, magnetici, ecc.) in condizioni diverse per conseguire una risposta diversa da parte del fingerprint.

RIVENDICAZIONI

1. Sistema implementato tramite computer (100) per la archiviazione e il trasferimento sicuri di dati digitali tra utenti (102) di una rete (101) per condivisione di dati, comprendente:

(a) una pluralità di dispositivi di elaborazione (103) di utenti per l'accesso a una rete (101) per condivisione di dati;

(b) un'identità digitale (104) associata a ciascun utente (102) della rete (101) e comprendente un mezzo di autenticazione (114), detto mezzo di autenticazione (114) comprendendo un processore in grado di generare automaticamente un codice di autenticazione in risposta a un'interrogazione per convalidare l'identità digitale (104) di un utente (102), in cui viene generato un nuovo codice di autenticazione in risposta a ogni nuova interrogazione;

(c) almeno un ente di certificazione (105) in comunicazione con il mezzo di autenticazione (114) e i dispositivi di elaborazione (103) del sistema (100) e comprendente un processore in grado di convalidare un'identità digitale (104) di un utente interrogando il mezzo di autenticazione (114) e verificando il codice di autenticazione generato

dal mezzo di autenticazione in risposta all'interrogazione, e configurato per emettere un certificato elettronico (113) ai dispositivi di elaborazione (103) di utenti validati (102') dei quali è validata l'identità digitale (104);

(d) almeno una transazione (106) che coinvolge due o più utenti (102) autorizzata dalla convalida delle identità digitali (104) di detti due o più utenti dall'almeno un ente di certificazione (105), ogni transazione (106) comprendendo informazioni digitali che sono generate, possedute e/o condivise da almeno uno di detti due o più utenti validati (102'), dette informazioni digitali comprendendo preferibilmente uno smart contract che definisce diritti e doveri di detti due o più utenti validati (102') su dette informazioni digitali;

(e) almeno un repository digitale (107) avente un indirizzo digitale e che archivia almeno parte delle informazioni digitali di una transazione autorizzata (106), detto repository digitale (107) comprendendo un gateway configurato per condividere le informazioni digitali soltanto con i dispositivi di elaborazione (103) di uno o più degli utenti validati (102') coinvolti nella transazione (106);

(f) un database ledger personale (108)

associato a ciascun utente (102) della rete (101), archiviato nel o in comunicazione con il dispositivo di elaborazione (103) degli utenti, ogni database ledger personale (108) comprendendo blocchi collegati da una chiave crittografica, ed essendo strutturato in modo tale che, quando viene autorizzata una transazione (106) tra due o più utenti validati (102'), sia aggiunto un nuovo blocco (118) ai database personali (108) associati a ciascuno di detti due o più utenti validati (102'), in cui detto nuovo blocco (118) registra gli indirizzi digitali dell'almeno un repository digitale (107) che archivia almeno parte delle informazioni digitali di detta transazione (106).

2. Sistema implementato tramite computer (100) secondo la rivendicazione 1, in cui il mezzo di autenticazione (114) di un'identità digitale (104) è un fingerprint che comprende una pluralità di punti aventi una o più proprietà materiali misurabili, il fingerprint comprendendo inoltre un processore in grado di generare codici di autenticazione cifrando valori ottenuti misurando in modo casuale almeno una di dette proprietà materiali misurabili in corrispondenza di punti diversi del fingerprint per mezzo di un dispositivo

di misurazione.

3. Sistema implementato tramite computer (100) secondo la rivendicazione 2, comprendente inoltre almeno un fingerprint gemello associato a ciascun fingerprint (114), detto fingerprint gemello essendo una copia identica del fingerprint (114), in cui: il fingerprint gemello comprende un processore in grado di comunicare con il fingerprint (114) e di decifrare il codice di autenticazione generato dal fingerprint (114); in cui l'almeno un ente di certificazione (105) è un repository di tipo hardware in comunicazione con i fingerprint (114) e che archivia i fingerprint gemelli, e che è configurato per eseguire un protocollo di autenticazione per validare l'identità digitale (104) di un utente che include: interrogare il fingerprint (114) di un utente (102) ottenendo un codice di autenticazione, decifrare detto codice di autenticazione per mezzo del fingerprint gemello, confermare l'autenticità del fingerprint (114), validare l'identità digitale (104) dell'utente, emettere un certificato elettronico (113) al dispositivo di elaborazione (103) dell'utente validato (102').

4. Sistema implementato tramite computer (100)

secondo le rivendicazioni da 2 a 3, in cui il fingerprint (114) è o un sistema su chip impacchettato con o fatto crescere monoliticamente su un dispositivo di misurazione in grado di misurare detta almeno una proprietà materiale misurabile.

5. Sistema implementato tramite computer (100) secondo le rivendicazioni da 2 a 4 in cui l'almeno una proprietà materiale misurabile del fingerprint (114) è una proprietà fisica e/o chimica; preferibilmente, è una proprietà ottica, elettrica, topografica, meccanica, termica, magnetica, chimica, e loro combinazioni.

6. Sistema implementato tramite computer (100) secondo le rivendicazioni da 2 a 5, in cui il fingerprint è in grado inoltre di cifrare e decifrare informazioni, preferibilmente tramite protocolli di algoritmi matematici, più preferibilmente misurando almeno una delle pluralità di proprietà materiali misurabili in corrispondenza di punti diversi casuali, ottenendo valori, e trasformando tramite un algoritmo la stringa di valori ottenuta in un codice crittografico.

7. Sistema implementato tramite computer (100)

secondo le rivendicazioni da 1 a 6 in cui il mezzo di autenticazione (114) è un film sottile, preferibilmente in cui detto film ha fino a 10^6 punti aventi proprietà materiali misurabili diverse per mm^2.

8. Sistema implementato tramite computer (100) secondo le rivendicazioni da 1 a 7, in cui almeno un utente (102) della rete (101) è un oggetto comprendente un dispositivo di elaborazione (103).

9. Sistema implementato tramite computer (100) secondo le rivendicazioni da 1 a 8, in cui almeno un repository digitale (107) e/o almeno un ente di certificazione (105) è anche un utente (102) della rete, avente la propria identità digitale (104).

10. Sistema implementato tramite computer secondo la rivendicazione 1, in cui almeno un repository digitale (107) o il provider dell'almeno un repository digitale (107) è anche un ente di certificazione (105).

11. Metodo implementato tramite computer per la archiviazione e il trasferimento sicuri di informazioni digitali tra utenti di una rete per condivisione di dati basato sul sistema di computer (100) secondo la rivendicazione 1, il metodo comprendendo:

i) accesso di almeno due utenti (102) alla rete (101) per condivisione di dati, per mezzo di dispositivi di elaborazione (103);

ii) trasmissione di una transazione (106) tra detti almeno due utenti (102) a un ente di certificazione (105), detta transazione (106) comprendendo informazioni digitali;

c) autenticazione delle identità digitali (104) di detti almeno due utenti (102) da parte dell'almeno un ente di certificazione (105), ottenendo almeno due utenti validati dei quali è confermata l'identità digitale (104);

d) emissione di un certificato elettronico (113) agli utenti validati (102');

e) autorizzazione della transazione (106);

f) archiviazione delle informazioni digitali della transazione autorizzata (106) in almeno un repository digitale (107) avente un indirizzo digitale;

g) registrazione dell'indirizzo digitale dell'almeno un repository digitale (107) che archivia le informazioni digitali della transazione in nuovi blocchi (118) dei database ledger personali (108) associati a ciascuno di detti utenti validati (102').

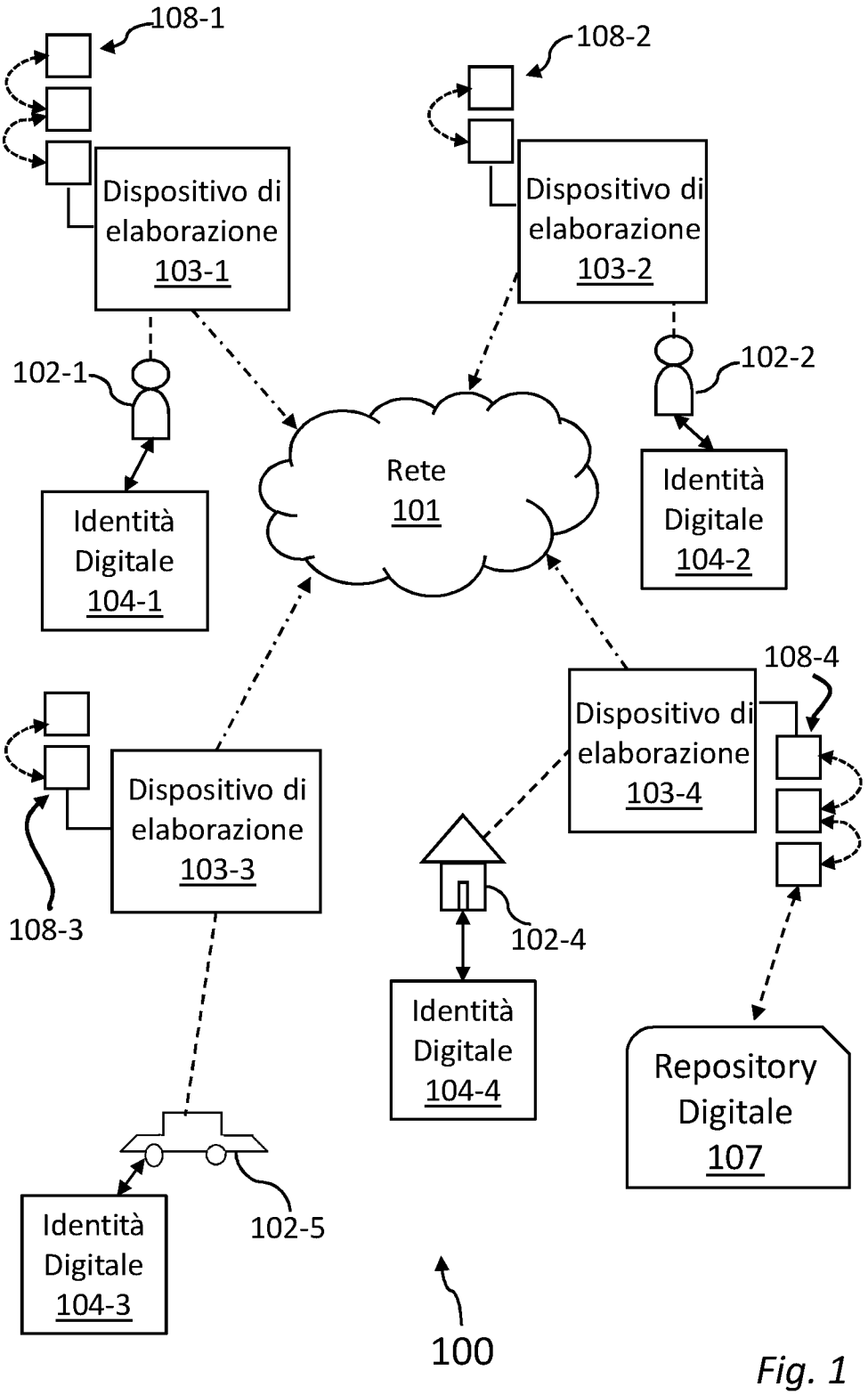
108-1
Dispositivo di elaborazione 103-1
108-2
Dispositivo di elaborazione 103-2
102-1
Identità Digitale 104-1
Rete 101
102-2
Identità Digitale 104-2
108-4
Dispositivo di elaborazione 103-4
Dispositivo di elaborazione 103-3
108-3
102-4
Identità Digitale 104-4
Repository Digitale 107
Identità Digitale 104-3
102-5
100

Fig. 1

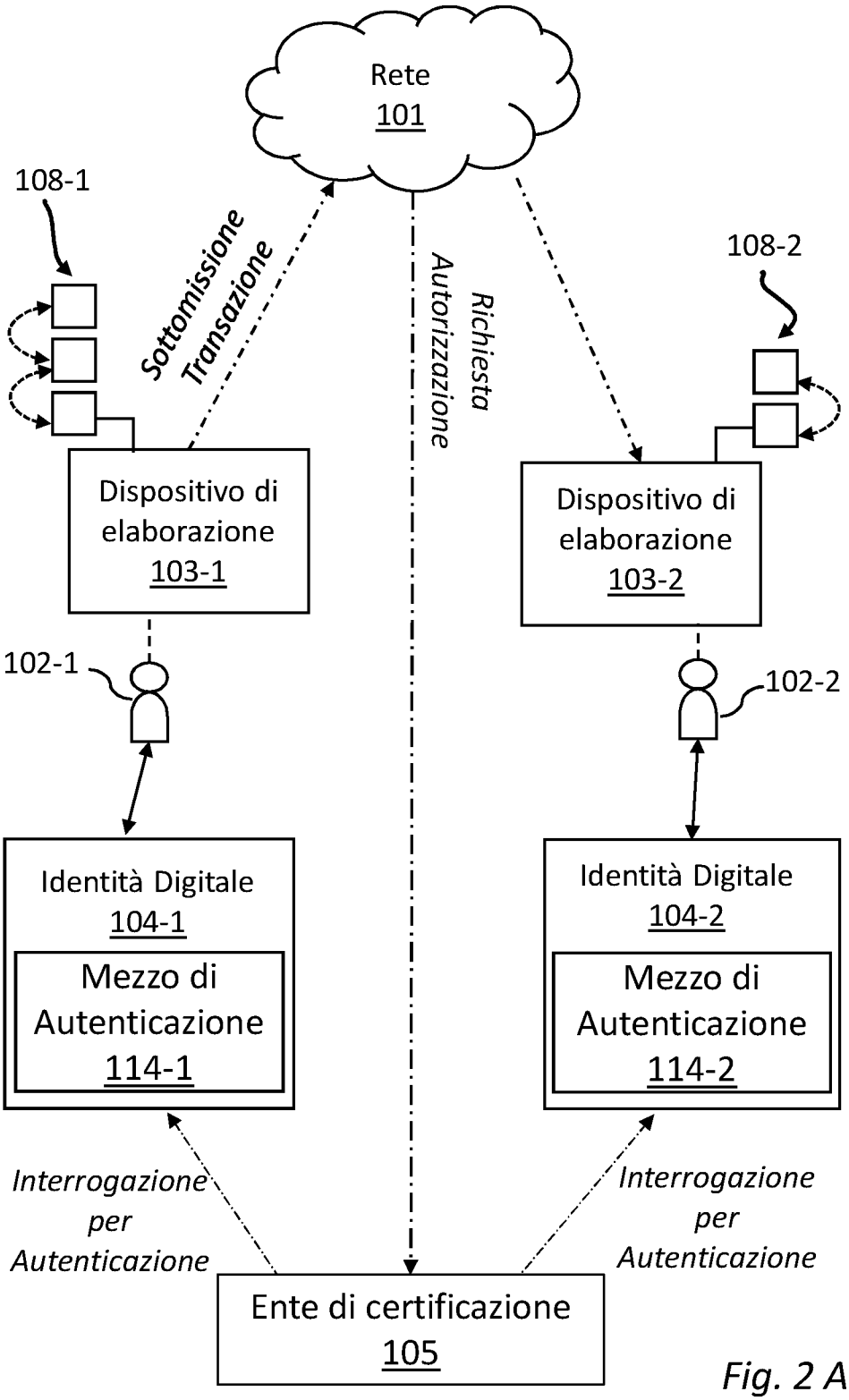
Rete
101
108-1
108-2
Sottomissione Transazione
Richiesta Autorizzazione
Dispositivo di elaborazione 103-1
Dispositivo di elaborazione 103-2
102-1
102-2
Identità Digitale 104-1
Mezzo di Autenticazione 114-1
Identità Digitale 104-2
Mezzo di Autenticazione 114-2
Interrogazione per Autenticazione
Interrogazione per Autenticazione
Ente di certificazione 105

Fig. 2 A

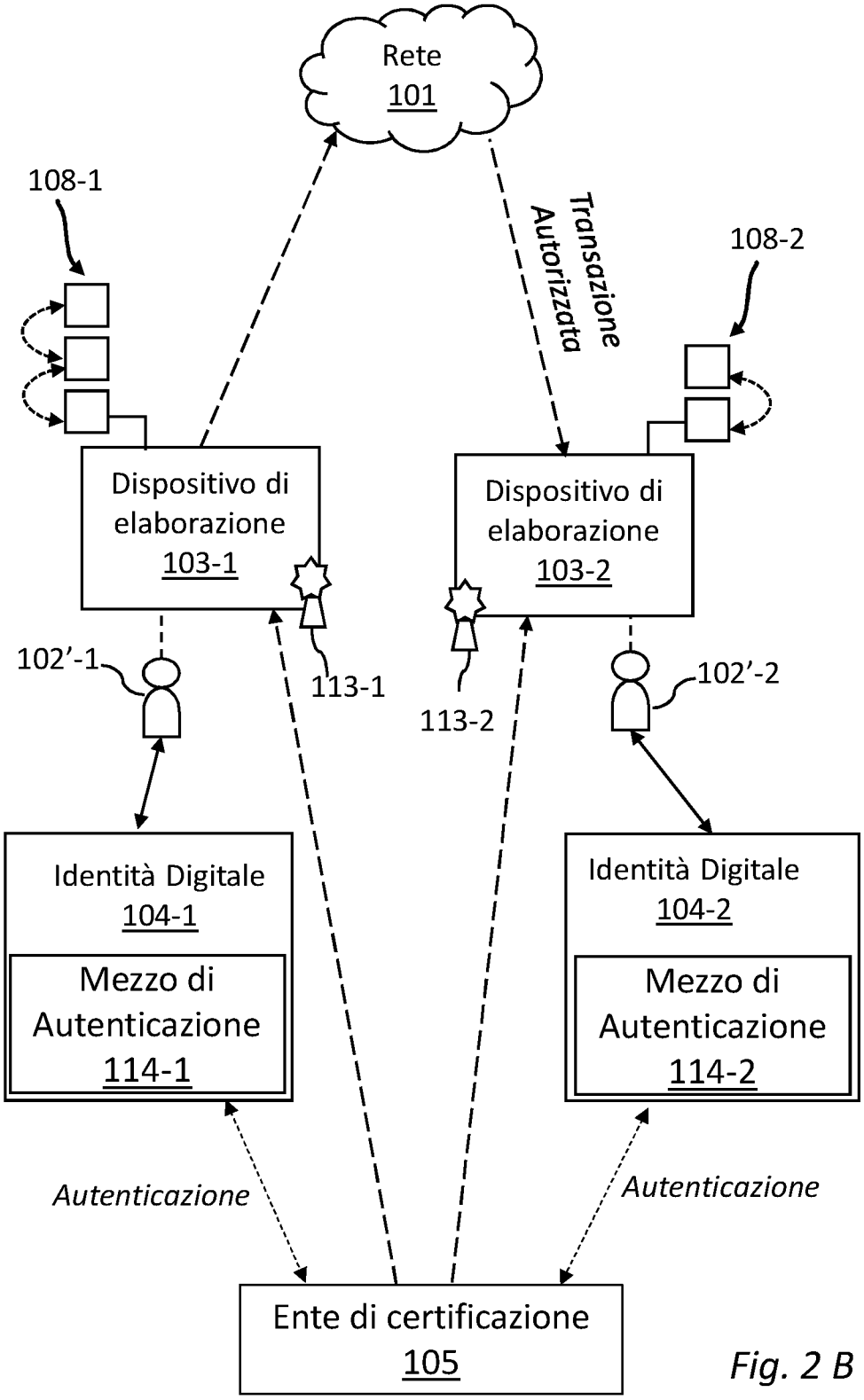
Rete
101
108-1
Transazione
Autorizzata
108-2
Dispositivo di
elaborazione
103-1
Dispositivo di
elaborazione
103-2
102'-1
113-1
113-2
102'-2
Identità Digitale
104-1
Mezzo di
Autenticazione
114-1
Identità Digitale
104-2
Mezzo di
Autenticazione
114-2
Autenticazione
Autenticazione
Ente di certificazione
105

Fig. 2 B

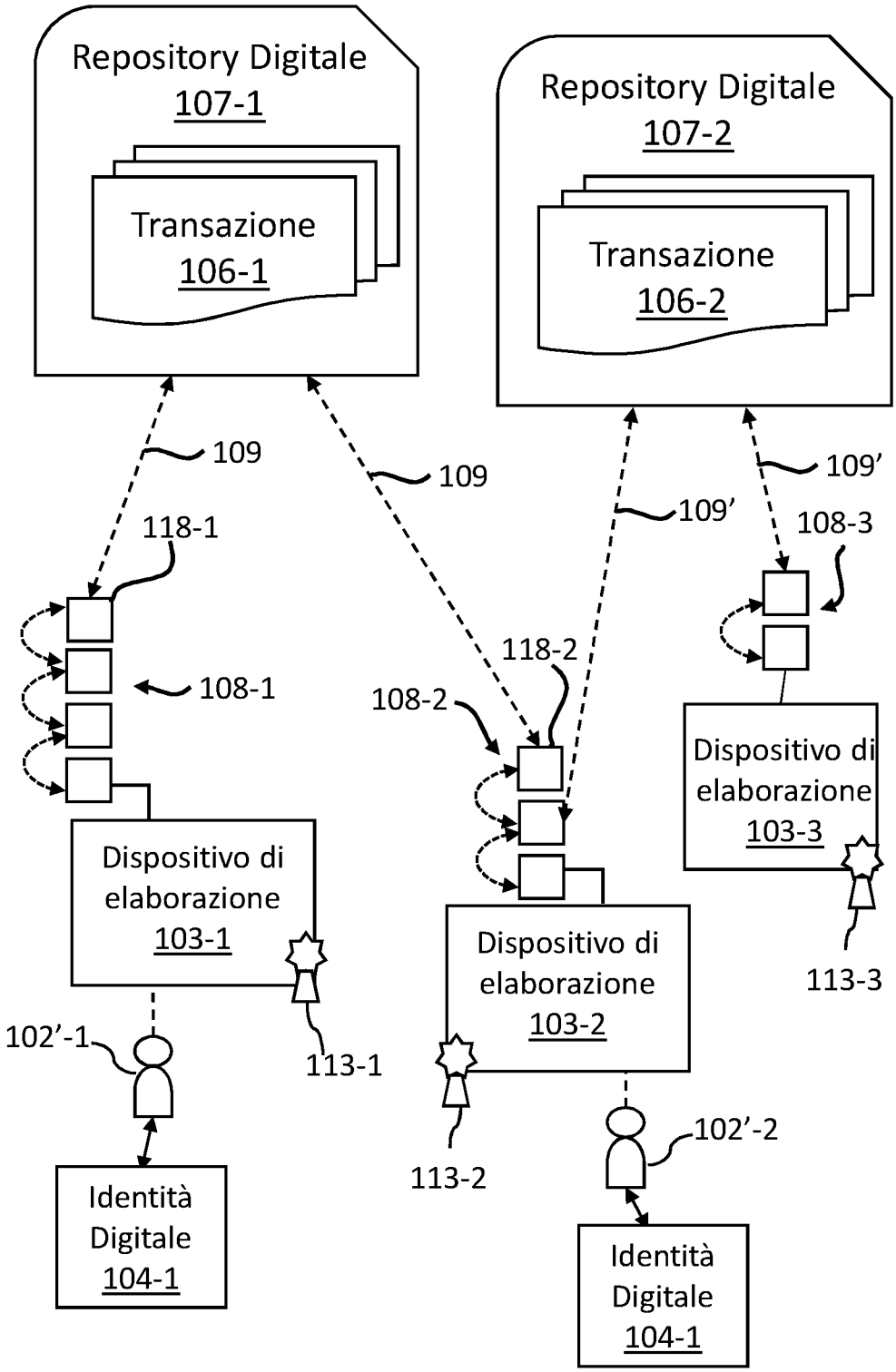
Repository Digitale
107-1
Transazione
106-1
Repository Digitale
107-2
Transazione
106-2
109
109
109'
109'
118-1
118-2
108-1
108-2
108-3
Dispositivo di elaborazione
103-1
Dispositivo di elaborazione
103-2
Dispositivo di elaborazione
103-3
102'-1
102'-2
113-1
113-2
113-3
Identità Digitale
104-1
Identità Digitale
104-1

Fig. 3

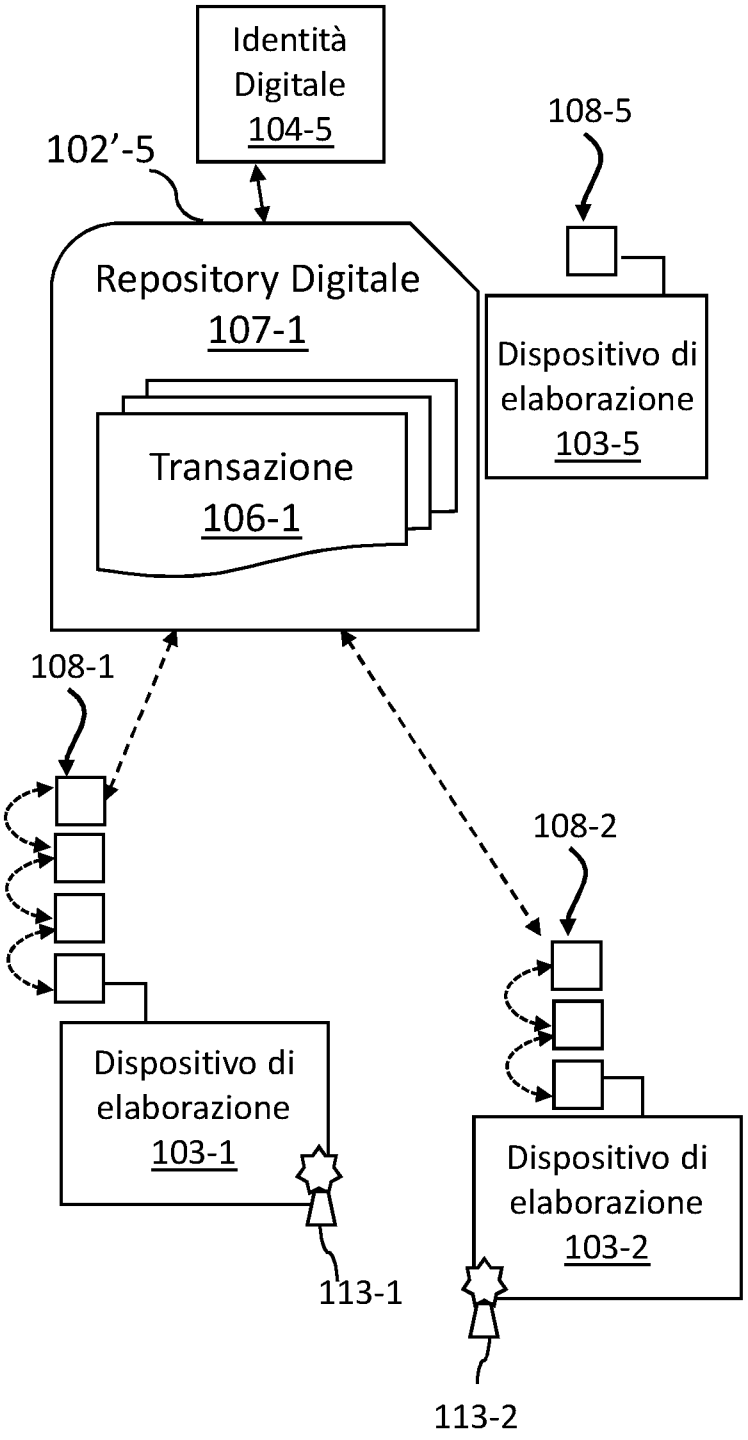
Identità
Digitale
104-5
102'-5
108-5
Repository Digitale
107-1
Dispositivo di
elaborazione
103-5
Transazione
106-1
108-1
108-2
Dispositivo di
elaborazione
103-1
Dispositivo di
elaborazione
103-2
113-1
113-2

Fig. 4

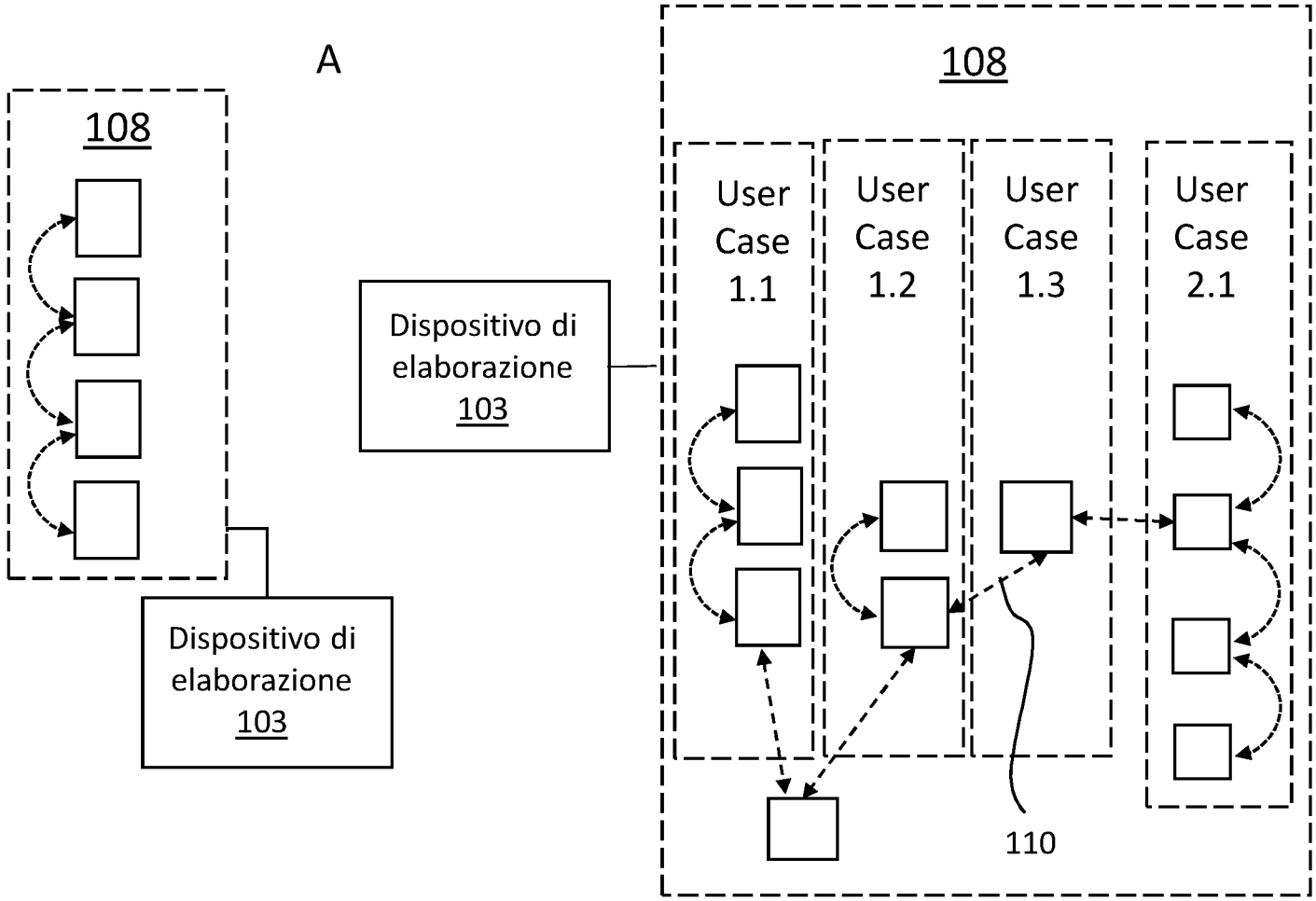
A
108
Dispositivo di elaborazione 103
B
108
User Case 1.1
User Case 1.2
User Case 1.3
User Case 2.1
Dispositivo di elaborazione 103
110

Fig. 5

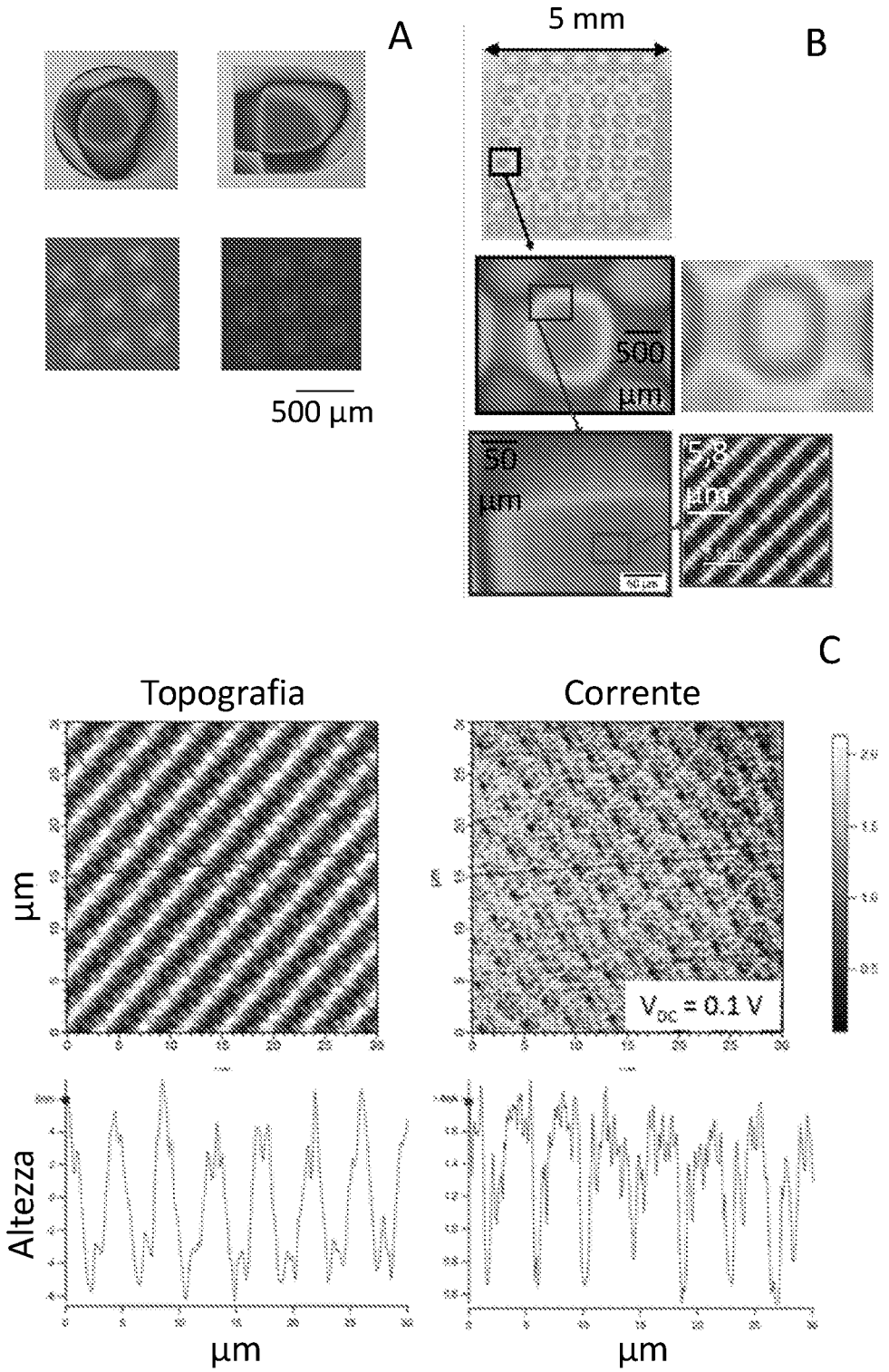
A
5 mm
B
500 µm
500 µm
50 µm
C
Topografia
Corrente
µm
V_{DC} = 0.1 V
Altezza
µm
µm

Fig. 6