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

UIBM

DOMANDA DI INVENZIONE NUMERO	**102021000021920**
Data Deposito	**16/08/2021**
Data Pubblicazione	**16/02/2023**

Classifiche IPC

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	F	21	62

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
H	04	L	9	32

Titolo

Metodo di gestione per l?archiviazione e la condivisione di informazioni personali

Metodo di gestione per l'archiviazione e la condivisione di informazioni personali

Descrizione

La presente invenzione ha come oggetto un metodo di gestione implementato via computer, generalmente noto come *computer implemented method* (CI *method*), per l'archiviazione e la condivisione di informazioni personali, ovvero di un insieme di dati personali protetti che un utente implementa mediante aggiunta, modifica o cancellazione di dati, categorie di dati, elenchi di dati, e così via.

Ogni utente di sistemi informatici in rete utilizza più App, giochi, siti web, piattaforme social, e ha bisogno di archiviare una grande quantità informazioni che risultano così sparse su centinaia di differenti database associati a questi sistemi, senza che l'utente ne abbia alcun controllo.

A tale proposito si definisce un insieme di dati personali protetti come una raccolta, riferita a un utente, di informazioni personali, alcune delle quali possono essere rese anonime togliendo ogni collegamento con l'identità dell'utente, e altre invece definiscono l'identità dell'utente. Le prime sono definite come informazioni a libero accesso, ammesso che siano state svincolate dall'utente, e possono essere utilizzate, nel loro insieme, in particolare a fini statistici. Le seconde sono definite come informazioni private, perché permettono di risalire all'identità e/o a un recapito fisico o digitale dell'utente.

La maggior parte dei software destinati a utenze private, inclusi App e piattaforme social,

raccolgono ed elaborano le informazioni personali che un utente, più o meno consapevolmente, condivide nei server a cui questi software fanno capo.

Gli operatori di questi software spesso sfruttano e trattano le informazioni personali degli utenti, in generale sulla base di un generico consenso degli utenti attraverso l'accettazione dei termini e delle condizioni d'uso, principalmente per i propri interessi commerciali, come l'identificazione di prodotti, servizi o contenuti da offrire ai propri utenti, o anche condividendo queste informazioni con altri partner commerciali, sebbene queste condivisioni debbano essere specificatamente autorizzate.

La situazione attuale lascia agli utenti un labile controllo sulla portabilità delle proprie informazioni personali archiviate in tali sistemi. Spesso, gli utenti devono ricreare le proprie informazioni personali tra diversi operatori di piattaforme e App per utilizzare funzionalità non disponibili su una piattaforma, ma disponibili su un'altra piattaforma.

Inoltre, il modo in cui questi sistemi conservano e accedono alle informazioni personali di un utente generalmente fornisce una scarsa e insufficiente trasparenza su come vengono mantenuti i dati, e ciò conduce a una serie di inconvenienti, tra cui il fatto che gli utenti potrebbero non essere invogliati a condividere dati con i sistemi informatici in rete, o l'impossibilità di disporre di una tracciabilità delle modifiche apportate, sia dall'utente sia dal sistema, alle informazioni personali.

In questo contesto, gli utenti sentono una forte esigenza di poter avere accesso a una tecnologia diretta verso un sistema per mantenere le informazioni personali dell'utente che sia affidabile, trasparente e tracciabile, e che fornisca all'utente il controllo sulle modifiche e la condivisione delle proprie informazioni personali.

Sono noti esempi di sistemi mirati alla tutela dell'identità e delle informazioni riservate di un utente, come nei brevetti USA No. 10,572,684 B2, 10,621,376 B2, 9,635,000 B1 e nella domanda di brevetto Usa No. 2019/020,5563 A1.

I processi e le strutture informatiche descritte però sembrano in generale orientate quasi esclusivamente alla tutela delle informazioni personali, combinata eventualmente con un rigoroso controllo dell'identità degli utenti, e non a una maggiore sicurezza nella loro condivisione.

Il problema tecnico che è alla base della presente invenzione è di fornire un metodo di gestione, implementato via computer, per l'archiviazione e la condivisione di informazioni personali che consenta di ovviare all'inconveniente menzionato con riferimento alla tecnica nota, soddisfacendo allo stesso tempo l'esigenza sopra delineata.

Tale problema viene risolto da un metodo di gestione come sopra specificato, che si caratterizza per il fatto di comprendere le fasi definite nell'annessa rivendicazione 1.

In generale, l'invenzione qui descritta è quindi mirata a creare un ambiente che favorisca l'accesso

degli utenti alle più disparate applicazioni e siti web, come per esempio software e siti web bancari, assicurativi e per transazioni finanziarie, software di carattere sanitario, messaggistica elettronica, software aziendali, software e siti web per la compravendita di oggetti e servizi, ma anche applicazioni più orientate all'intrattenimento e al tempo libero, come *social network*, videogiochi multiutente, giochi di ruolo, siti di incontri, siti di viaggio e così via, laddove notoriamente la distinzione tra queste diverse tipologie di applicazione è sempre più labile e sfumata.

L'archiviazione e la condivisione di informazioni personali prevede, nel metodo di gestione che verrà descritto di seguito, che un gestore principale fornisca, attraverso un qualsiasi punto di accesso che potrà essere per esempio un sito web e/o una app, una struttura informatica che comprende almeno un processore e almeno un server condiviso, capaci di collegarsi a una rete di connessione, tipicamente Internet, per il collegamento, attraverso tale rete di connessione, con una pluralità di dispositivi client che sono associati a rispettivi utenti che desiderano archiviare e condividere le proprie informazioni personali presso uno o più sistemi informatici.

Qui e nel seguito, per sistemi informatici si intendono software e siti web di terze parti, rappresentate quindi da rispettivi gestori dei sistemi informatici decentralizzati.

Questi sistemi informatici, nella comune prassi, hanno bisogno che i loro utenti condividano con essi informazioni personali per assicurare agli utenti un

loro corretto funzionamento, ma in questo modo devono essere aggravati dall'onere di gestire queste informazioni personali, alcune estremamente sensibili e private, altre più di carattere ludico, assicurando comunque a tutte un certo livello di tutela.

Uno scopo della presente invenzione è eliminare questo aggravio, offrendo ai gestori dei sistemi informatici la possibilità di sfruttare le informazioni, che gli utenti vogliono condividere con essi, grazie a un sistema di archivio decentralizzato, con differenti livelli di accesso in base al tipo di informazioni personali archiviate.

Pertanto, il metodo di gestione secondo la presente invenzione comprende una fase di iscrizione, in cui un utente si registra presso la struttura informatica, e per fare ciò l'utente deve usare, e quindi generare nel caso non la possieda, una chiave crittografica asimmetrica pubblica/privata, eventualmente accoppiata a una *password* sicura, scelta dall'utente stesso.

Si intende che la chiave crittografica privata dovra' essere custodita dall'utente stesso e mai condivisa con chiunque, la sua chiave pubblica potrà eventualmente essere invece fornita ad altre strutture informatiche.

In questa fase, l'utente potrà scegliere una o più identità alternative, alter-ego o avatar, con cui egli verrà identificato, se permesso dalle regole vigenti, nei sistemi informatici nei quali egli opererà, come per esempio videogiochi multiruolo.

Parallelamente, viene prevista una fase di accredito, concettualmente simile alla precedente, in cui un gestore di sistemi informatici acquisisce una chiave crittografica pubblica e registra, presso detta struttura informatica, uno o più sistemi informatici atti a interagire con l'utente.

In questo caso, la chiave crittografica pubblica può essere acquisita, eventualmente dietro compenso, dalla struttura informatica.

Questa fase di accredito ha lo scopo di permettere l'interazione reciproca tra struttura informatica e i sistemi informatici che fanno capo ai loro gestori, per lo scambio, a determinate condizioni, delle informazioni personali fornite dagli utenti attraverso detti sistemi informatici, che in ogni caso non vengono conservate dai gestori dei sistemi informatici.

Affinché ciò avvenga, viene prevista una fase di permesso, in cui la struttura informatica riceve dall'utente la richiesta di impiegare per esempio un sistema informatico, essendo un utente registrato presso la struttura informatica stessa, e a tale proposito egli fornisce, usando la struttura informatica come mediatore, le informazioni personali che sono richieste dal sistema informatico.

Altrimenti, la stessa interazione tra utente e sistema informatico produce informazioni personali che vengono raccolte da detta struttura informatica, come punteggi, accrediti, preferenze, livelli acquisiti e così via.

In questa fase, queste informazioni vengono

suddivise in due categorie principali: informazioni di libero accesso, che non sono vincolate all'identità dell'utente, e informazioni private, che definiscono l'identità dell'utente e che devono essere trattate con maggiore riservatezza.

All'interno di ciascuna categoria principale, le informazioni possono essere ulteriormente categorizzate in liste, ciascuna fornita di un marcatore.

Inoltre, sempre in questa fase, le informazioni personali fornite dall'utente potranno essere collegate a un suo alter-ego o avatar.

Le informazioni personali fornite dall'utente, ciascuna nelle rispettive categorie e liste, vengono registrate in almeno un registro pubblico distribuito secondo la tecnologia blockchain, in un'apposita fase di caricamento del metodo di gestione qui descritto. Inoltre sul medesimo registro blockchain verranno anche registrate le autorizzazioni che l'utente emette tramite transazione crittografica, per permettere a strutture informatiche terze di acccedervi, tali autorizzazioni possono sempre essere modificate o revocate dall'utente stesso lasciandogli un completo controllo sui propri dati.

Una volta caricate, queste informazioni personali possono essere lette, aggiornate o cancellate, e ne possono anche essere aggiunte di nuove.

A tale proposito, il metodo di gestione comprende una fase di accesso alle informazioni private, in cui il gestore di sistemi informatici richiede all'utente, attraverso la mediazione della struttura

informatica, un'autorizzazione ad accedere alle informazioni informazioni personali che sono state categorizzate come informazioni private, e l'utente concede, se vuole, l'autorizzazione all'accesso impiegando la sua chiave crittografica privata e/o la sua password per emettere la transazione crittografica di autorizzazione. Ogni informazione registrata sulla blockchain sara' protetta da crittografia forte che permette la lettura solo ai detentori della chiave privata di accesso, tali informazioni se condivise verrano quindi crittografate utilizzando sia la chiave pubblica dell'utente, sia la chiave pubblica della struttura informatica autorizzata dall'utente stesso alla lettura del dato.

Queste informazioni private non possono comunque essere modificate dai sistemi informatici.

Inoltre, il metodo di gestione comprende una fase di accesso alle informazioni di libero accesso, in cui detto gestore di sistemi informatici richiede a detta struttura informatica, impiegando la sua chiave crittografica, di accedere alle informazioni di libero accesso, ed eventualmente aggiungerne di nuove, o di modificare quelle presenti sulla base dell'interazione tra utente e sistema informatico. Qualsiasi transazione di accesso a tali dati verra' quindi registrata nella blockchain per mantenere un registro delle richeiste di accesso che l'utente potra' sempre controllare in qualsiasi momento.

Infine, il metodo di gestione comprende un'eventuale fase di modifica, in cui detta struttura informatica riceve dall'utente la richiesta di impiegare detti uno o più sistemi informatici come utente registrato

presso detta struttura informatica, aggiungendo, modificando o cancellando, attraverso detta struttura informatica, informazioni personali che vengono suddivise in informazioni di libero accesso e in informazioni private.

Il metodo di gestione sopra delineato e il sistema informatico che lo implementa forniscono quindi un modo per archiviare un insieme di informazioni personali protette in un archivio crittografico sicuro, sfruttando la blockchain, per scrivere i dati crittografati e dare loro accesso a chiunque ne faccia richiesta purché con l'approvazione dell'utente mediato attraverso un gestore. Ciò consente agli utenti di avere il controllo sui propri dati, con un approccio che può essere eventualmente ludicizzato attraverso un sistema di ricompense.

In una versione preferita del metodo di gestione secondo la presente invenzione, esso comprende anche una fase di ricompensa in cui l'utente, in occasione di una fase di permesso e/o modifica, riceve un compenso di natura digitale, come ad esempio un gettone (*token*) digitale, spendibile presso la struttura informatica, o presso gli stessi sistemi informatici, per acquisire, servizi, priorità o altri vantaggi.

La presente invenzione verrà qui di seguito descritta secondo un suo esempio di realizzazione preferita, fornito a scopo esemplificativo e non limitativo con riferimento ai disegni annessi in cui:

*

a figura 1 mostra un primo diagramma che illustra un

insieme di informazioni personali protette riferite a un utente (*actor*) anonimizzato attraverso un alter-ego o avatar, che definisce un'identità alternativa dell'utente;

* a figura 2 mostra un secondo diagramma schematico che illustra l'interazione tra utenti e le società responsabili di sistemi informatici attraverso un database distribuito gestito da un gestore; e

* a figura 3 mostra un terzo diagramma schematico che illustra le principali fasi del metodo di gestione secondo la presente invenzione.

La presente descrizione deve essere considerata come una esemplificazione dell'invenzione e non intende limitare l'invenzione alle forme di realizzazione specifiche illustrate dalle figure o dalla descrizione di seguito.

Questa descrizione si riferisce generalmente alla gestione di informazioni e dati personali che possono essere di carattere privato, in quanto relativi a dati sensibili relativi alla persona, alla sua identità, ai suoi recapiti digitali e fisici, allo stato della sua salute, alla sua situazione finanziaria e così via, o possono avere invece un carattere pubblico in quanto dati da condividere attraverso sistemi informatici di terzi come software, app, siti web, piattaforme social e così via; tali informazioni possono, ad esempio, essere archiviati in una tecnologia di archiviazione criptata e distribuita (DLT), come una *blockchain*, che le possono anonimizzare.

Le espressioni "*Distributed Ledger Technology*", "DLT", "registro pubblico distribuito" sono in generale utilizzate per fare riferimento a un elemento di archiviazione dei dati che comprende, ad esempio, un consenso di dati digitali replicati, condivisi e/o sincronizzati che possono essere distribuiti geograficamente su più siti, paesi o istituzioni. In un DLT, in genere non esiste un amministratore centrale o un archivio dati centralizzato. Esempi dell'uso di DLT includono: *blockchain*, criptovalute, contratti intelligenti e archiviazione decentralizzata di file in rete.

In generale, *blockchain* è un database distribuito che mantiene un elenco in continua crescita di record di dati. Ogni record di dati è protetto contro manomissioni e revisioni. Le *blockchain* vengono utilizzate con registri pubblici delle transazioni, in cui al record viene applicata una crittografia, cosa che consente alle transazioni di essere private crittografando il contenuto della transazione, e così solo gli utenti o le entità che possiedono la chiave della transazione possono visualizzarla.

I termini "a", "un" e "il" intendono includere anche le forme plurali, a meno che il contesto non indichi chiaramente un intento differente.

I termini "comprende" e/o "comprendente", ed equivalenti, quando utilizzati in questa descrizione, specificano la presenza di fasi, caratteristiche, passaggi, operazioni, elementi e/o componenti dichiarati, ma non precludono la presenza o l'aggiunta di una o più altre fasi, caratteristiche, numeri interi, passaggi, operazioni, elementi, componenti e/o gruppi di essi.

Nel contesto della presente invenzione, il termine "registro pubblico" consiste specificatamente in un elenco accessibile al pubblico di transazioni per il database distribuito o *blockchain*.

Nella descrizione che segue, il termine "*blockchain*" indica generalmente un database distribuito che contiene un registro o un elenco di record, chiamati blocchi, protetti da manomissioni e revisioni tipicamente mediante un codice univoco di *hash* crittografico.

Le *blockchain* costituiscono un "libro mastro" (*ledger*) aperto e distribuito, in grado di registrare insiemi di informazioni personali protette, riferibili a un utente, in modo efficiente, verificabile e permanente. Il consenso all'impiego di questa metodologia di codifica garantisce che i registri condivisi siano copie esatte, e riduce il rischio di transazioni fraudolente, poiché la manomissione potrebbe dover verificarsi in molti luoghi esattamente nello stesso momento.

Al suo interno, un sistema informatico *blockchain* può anche registrare l'ordine cronologico degli input, attribuendo loro una rispettiva marcatura temporale (*timestamp*), con tutti i nodi del sistema che accettano la validità dell'input utilizzando il modello di consenso scelto. Il risultato consiste in un'identificazione irreversibile e accettata da tutti i partner del sistema informatico.

Una chiave crittografica privata è una stringa alfanumerica codificata in formati diversi a seconda della metodologia di generazione utilizzata. In

questo contesto, essa può essere generata dall'utente e la cui parte pubblica puo' essere registrata o liberamente utilizzata presso un ente certificato, o eventualmente alla medesima struttura informatica che presiede al metodo di gestione qui descritto.

Una chiave crittografica pubblica consiste anch'essa in una stringa di lettere e numeri, generalmente da 26 a 34 caratteri, generata dalla chiave privata.

Nei sistemi a crittografia asimmetrica, impiegati nelle *blockchain*, ogni coppia di chiavi privata e pubblica è formata in modo tale che ciò che viene cifrato con una, può essere decifrato solo con l'altra. Le due chiavi sono, a priori, perfettamente interscambiabili, ma generalmente una delle due viene definita "pubblica" e una "privata", cosicché una delle due, appunto la chiave pubblica, può essere scambiata anche su un canale non sicuro come e-mail, key server, su una pagina e così via l'importante è sapere che una chiave pubblica è di per sé associata a una chiave privata, e può anche essere associata a un utente in genere con l'impiego di un certificato digitale.

La combinazione tra le chiavi pubbliche e private viene utilizzata per effettuare transazioni irreversibili garantite da firme matematiche legate ad ogni transazione.

Il metodo di gestione per l'archiviazione e la condivisione di informazioni personali è realizzato in una piattaforma informatica che comprende in generale una struttura informatica, indicata nel suo complesso con 100.

Commentato [1]: Che significa indicata con 100???

Un esempio illustrativo di alcuni dei componenti fisici che possono realizzare una piattaforma informatica che comprende la struttura informatica 100 per la gestione di informazioni personali utilizzando una *blockchain*, identificata in breve come struttura, configurati per facilitare il trasferimento di dati e informazioni personali tra uno o più punti di accesso, ovvero tra utenti 1 e i rispettivi dispositivi client 2 e almeno un server 3 su una rete di dati.

Ogni dispositivo client 2 può inviare dati e ricevere dati dalla rete dati tramite una connessione di rete con un punto di accesso. Un archivio dati accessibile dal server 2 può contenere uno o più database. I dati possono comprendere qualsiasi informazione personale pertinente a uno o più utenti, comprese informazioni che descrivono uno o più utenti, *timestamp*, informazioni di carattere pubblico, eventualmente da uno o più sistemi informatici impiegati dall'utente e riferite a esso, e un eventuale *nonce*, ovvero un numero, generalmente casuale o pseudo-casuale, che ha un utilizzo unico.

I dispositivi client 2 possono essere dispositivi mobili, come laptop, tablet, assistenti digitali personali, smartphone e simili, dotati di un'interfaccia di rete wireless in grado di inviare dati a uno o più server con accesso a uno o più archivi dati su una rete come una rete locale senza fili (WLAN). Inoltre, i dispositivi client 2 possono essere dispositivi fissi, come desktop, workstation e simili, dotati di un'interfaccia di rete wireless o cablata in grado di inviare dati a uno o più server con accesso a uno o più archivi dati tramite una

rete wireless o rete locale cablata.

La presente invenzione può essere implementata su almeno un dispositivo client 2 e/o server 3 programmato per eseguire una o più delle fasi qui descritte. In alcune forme di realizzazione, è possibile utilizzare più di un dispositivo client 2 e/o server 3, ciascuno programmato per eseguire una o più fasi di un metodo o processo qui descritto.

Il dispositivo client 2 può essere un dispositivo digitale che, in termini di architettura hardware, generalmente include un processore, interfacce di input/output (I/O), una radio, un archivio dati e una memoria.

Il server 3 può essere un computer digitale che, in termini di architettura *hardware*, generalmente include un processore, interfacce di input / output (I/O), un'interfaccia di rete, un archivio dati e una memoria.

In generale, il processore di server o dispositivo client è un dispositivo *hardware* per eseguire le istruzioni del *software*. Il processore può essere qualsiasi processore personalizzato o disponibile in commercio, un'unità di elaborazione centrale (CPU), un processore ausiliario tra diversi processori associati al dispositivo, un microprocessore basato su semiconduttori (sotto forma di un microchip o un set di chip) o in generale qualsiasi dispositivo per eseguire le istruzioni del *software*. Quando il server e il dispositivo client sono in funzione, il processore è configurato per eseguire il *software* archiviato nella memoria, per comunicare dati da e verso la memoria e per controllare in generale le

operazioni del server secondo le istruzioni del software. Le interfacce I/O possono essere utilizzate per ricevere l'input dell'utente da e/o per fornire l'output del sistema a uno o più dispositivi o componenti.

L'input dell'utente può essere fornito tramite, ad esempio, una tastiera, un touch pad e/o un mouse. L'output di sistema può essere fornito tramite un dispositivo di visualizzazione e una stampante (non mostrata). Le interfacce I/O possono includere, ad esempio, una porta seriale, una porta parallela, un'interfaccia SCSI (Small Computer System Interface), un ATA seriale (SATA), un *Fibre Channel*, iSCSI, un'interfaccia PCI Express (PCI-x), un'interfaccia a infrarossi (IR), un'interfaccia a radiofrequenza (RF) e/o un'interfaccia USB (Universal Serial Bus) e sue evoluzioni, e in generale qualsiasi altra interfaccia per la trasmissione di dati digitali.

L'interfaccia di rete può essere utilizzata per consentire al server di comunicare su una rete, come Internet, una rete geografica (WAN), una rete locale (LAN) e simili, ecc. L'interfaccia di rete può includere, per esempio, una scheda o un adattatore Ethernet o una scheda o un adattatore di rete locale wireless (ad esempio, 802.11a/b/g/n). L'interfaccia di rete può includere indirizzi, controllo e/o connessioni dati per abilitare comunicazioni appropriate sulla rete. È possibile utilizzare un archivio dati per archiviare i dati. L'archivio dati può includere qualsiasi elemento di memoria volatile (ad esempio, memoria ad accesso casuale (RAM, come DRAM, SRAM, SDRAM e simili)), elementi di memoria

non volatile (ad esempio, ROM, disco rigido, nastro, CDROM e simili) e loro combinazioni. Inoltre, l'archivio dati può incorporare supporti di memorizzazione elettronici, magnetici, ottici e/o di altro tipo. In un esempio, l'archivio dati può trovarsi all'interno del server come, ad esempio, un disco rigido interno connesso all'interfaccia locale nel server. Inoltre, in un'altra forma di realizzazione, l'archivio dati può essere posizionato all'esterno del server come, ad esempio, un disco rigido esterno collegato alle interfacce I/O. In un'ulteriore forma di realizzazione, l'archivio dati può essere connesso al server attraverso una rete, come, ad esempio, un file server collegato alla rete.

Si noti che la memoria può avere un'architettura distribuita, altrimenti detta *cloud*, in cui vari componenti sono situati in remoto l'uno dall'altro, ma possono essere raggiunti dal processore. Il software in memoria può includere uno o più programmi software, ciascuno dei quali include un elenco ordinato di istruzioni eseguibili per l'implementazione di funzioni logiche. Il software in memoria include un sistema operativo adatto (O/S) e uno o più programmi. Il sistema operativo controlla essenzialmente l'esecuzione di altri programmi per computer, come uno o più programmi, e fornisce pianificazione, controllo input-output, gestione di file e dati, gestione della memoria e controllo della comunicazione e servizi correlati. L'uno o più programmi possono essere configurati per implementare i vari processi, algoritmi, metodi, tecniche, ecc. qui descritti.

La struttura informatica 100 comprende una connessione a una rete *blockchain*, avente uno o più nodi, che possono essere in comunicazione con uno o più server 2 e/o dispositivi client 3 della struttura 100. Un nodo può essere costituito da un server, un dispositivo client o qualsiasi altra appropriata piattaforma di elaborazione in rete. La rete *blockchain* può gestire un database *blockchain* 101 distribuito contenente i dati registrati dal sistema. Questi dati possono essere mantenuti come un registro pubblico distribuito, che possono essere indicati come blocchi, protetti da manomissioni e revisioni.

Con riferimento alle figure 2 e 3, la struttura informatica 100 è preposta all'archiviazione e alla condivisione di un insieme di informazioni personali 102 e, a tale proposito, essa fornisce a un generico utente un qualsiasi punto di accesso che potrà essere per esempio un sito web e/o una app; una pluralità di dispositivi client 2 sono associati a rispettivi utenti 1 che desiderano archiviare e condividere le proprie informazioni personali presso uno o più sistemi informatici, indicati nel loro complesso con 103, i quali fanno capo a rispettivi gestori di sistemi informatici 104 che interagiscono con detta struttura principale 100.

L'utente 1 ottiene quindi sul suo client, per esempio il proprio *smartphone*, l'app che costituisce detto punto di accesso e, collegandosi alla struttura informatica 100, genera all'interno dell'app la sua chiave crittografica pubblica 4, per esempio utilizzando l'algoritmo secp256k1, e sceglie anche una password 5 per proteggerla.

L'algoritmo secp256k1 si riferisce ai parametri di una particolare curva ellittica utilizzata nella crittografia a chiave pubblica, definita negli *Standards for Efficient Cryptography* (SEC), costruita in uno speciale modo non casuale che consente un calcolo particolarmente efficiente.

La generazione di chiave pubblica 4 e password 5 realizza una fase di iscrizione dell'utente, che può comprendere anche una fase di generazione di un'identità alternativa 6, definita come alter-ego o avatar, che può comprende per esempio un *nickname*, una descrizione, una o più immagini associate.

Con la fase d'accesso, l'utente 1 sottoscrive un contratto *blockchain* per gestire il suo insieme di informazioni personali protetti 102. Se l'utente 1 possiede già una chiave secp256k1, visto che per esempio *Bitcoin* ed *Ethereum Wallet* utilizzano lo stesso algoritmo, egli può importare la sua chiave 4.

Successivamente, l'utente 1 può accedere a una fase di permesso, in cui la struttura informatica 100 riceve dall'utente 1 la richiesta di impiegare per esempio un sistema informatico 103, scelto tra quelli disponibili, cioè tra quelli che aderiscono a questo servizio.

In questo modo, l'utente può fornire al sistema informatico scelto, usando la struttura informatica come mediatore, le informazioni personali che sono richieste. Si noti inoltre che questa opzione apre un canale bidirezionale, perché anche il sistema informatico 103 potrà generare informazioni personali appartenenti all'insieme 102, che saranno

comunque gestite e conservate dalla struttura informatica 100. Queste informazioni personali potranno essere per esempio punteggi, accrediti, preferenze, livelli acquisiti e così via.

In questa fase, queste informazioni 102 vengono suddivise in due categorie principali: informazioni di libero accesso 7, che non sono vincolate all'identità dell'utente, e informazioni private 8, che definiscono l'identità dell'utente e che devono essere trattate con maggiore riservatezza.

All'interno di ciascuna categoria principale 7, 8, le informazioni possono essere ulteriormente categorizzate in liste 10, ciascuna fornita di un marcatore 11.

Inoltre, sempre in questa fase, le informazioni personali 102 fornite dall'utente potranno essere collegate a un suo alter-ego o avatar 6 (figura 1).

Le informazioni personali 102 fornite dall'utente 1, ciascuna nelle rispettive categorie 7, 8 e liste 10, vengono registrate in almeno un registro pubblico distribuito 101 secondo una crittografia 106 basata su tecnologia blockchain, in una fase di caricamento del metodo di gestione qui descritto (figura 3).

Una volta caricate, queste informazioni personali possono essere lette, aggiornate o cancellate, e ne possono anche essere aggiunte di nuove.

Nel presente metodo, viene prevista un'impostazione per mantenere le informazioni personali sono presso il server 3 della struttura informatica 100, il che comporta che esse devono essere recuperate ogni volta che il sistema informatico 103 viene impiegato, ma anche che le informazioni personali

102 sono conservate qualunque cosa possa succedere al dispositivo client 2. Ad ogni accesso, può essere prevista la richiesta, per maggiore semplicità, della password 5.

In questo modo, l'utente 1 può vedere i suoi dati e gestire le autorizzazioni per consentire a terzi di accedere ai suoi dati e in quale momento. L'app sul suo dispositivo client 2 scaricherà tutte le notifiche di "richiesta di autorizzazione" e consentirà all'utente di approvarle, modificarle o negarle utilizzando la propria chiave pubblica 4 come funzionalità di firma.

Il metodo di gestione prevede anche una fase di accredito, concettualmente simile alla precedente, in cui un gestore 104 di sistemi informatici 103 acquisisce una chiave crittografica privata 9 destinata a essere accoppiata con detta chiave pubblica 4. Attraverso questo processo, un sistema informatico 103 viene registrato presso detta struttura informatica 100, e da quel momento l'utente 1 può interagire con esso.

Questa fase di accredito ha lo scopo di permettere l'interazione reciproca tra struttura informatica e i sistemi informatici che fanno capo ai loro gestori, per lo scambio, a determinate condizioni, delle informazioni personali fornite dagli utenti attraverso detti sistemi informatici, che in ogni caso non vengono conservate dai gestori dei sistemi informatici.

A tale proposito, il gestore 104 di ogni sistema informatico 103 è così in grado di vedere le informazioni personali 102 disponibili per ogni

utente 1, ma non è consentito conoscere i valori al loro interno, e può solo inviare una richiesta per accedervi con una transazione firmata con la propria chiave privata 9. La richiesta avviene attraverso una crittografia blockchain 106, così da ottenere una marcatura temporale

L'utente 1, a cui viene inoltrata questa richiesta, può scegliere se dare il suo consenso al gestore del servizio informatico, indicando, se lo ritiene adeguato, anche un intervallo di tempo, con un'ora di inizio e un'ora di fine, per eseguire la richiesta: al di fuori dell'intervallo di tempo concesso dall'utente 1, il sistema informatico 103 non potrà scaricare alcuna informazione personale.

La struttura informatica 100, che è mediatrice nella gestione di questa richiesta, potrà così controllare la marcatura temporale della *query* con la quale il sistema informatico 103 interrogherà registro pubblico distribuito 101, e rilasciare il permesso di accesso se la marcatura ricade nell'intervallo di tempo concesso dall'utente 1.

In questa fase di accesso alle informazioni private, in cui il gestore 104 di sistemi informatici richiede quindi all'utente 1, attraverso la mediazione della struttura informatica 100, un'autorizzazione all'accesso alle informazioni personali che sono state categorizzate come informazioni private 8, e l'utente concede, se vuole, l'autorizzazione all'accesso impiegando la sua chiave crittografica pubblica 4 e/o la sua password 5 (figura 3).

Queste informazioni private 8 non possono comunque essere modificate dai sistemi informatici 103.

Il metodo di gestione comprende un'eventuale fase di modifica 107, in cui detta struttura informatica 100 riceve dall'utente 1 la richiesta di impiegare detti uno o più sistemi informatici 103 per un'operazione di modifica, aggiunta, cancellazione di qualunque tipo di informazione personale, che quindi vengono di nuovo suddivise in informazioni di libero accesso 7 e in informazioni private 8.

Tutti i dati vengono salvati in un formato adatto all'interscambio di dati fra applicazioni client/server, per esempio un formato json, per evitare formattazioni.

Infine, il metodo di gestione comprende una fase di accesso alle informazioni di libero accesso, in cui un gestore 104 di sistemi informatici 103 richiede alla struttura informatica 100, impiegando la sua chiave crittografica, di accedere alle informazioni di libero accesso, ed eventualmente aggiungerne di nuove, o di modificare quelle presenti sulla base dell'interazione tra utente e sistema informatico.

Ogni sistema informatico 103 può avere un permesso speciale, come per esempio una funzione aggiornamento della scheda di un utente, a cui corrisponde, sempre a titolo esemplificativo, un personaggio in un videogioco multiruolo.

L'utente può quindi consentire a un gestore 104 di aggiornare la propria scheda ogni volta che lo desidera, eventualmente in un intervallo temporale predefinito.

In una versione preferita del metodo di gestione, l'accesso alle informazioni di libero accesso 107 è invece libero per tutti, trattandosi di dati

anonimizzati.

In una versione preferita del metodo di gestione, può essere previsto un sistema di ricompensa che si basa su gettoni crittografici virtuali generati nella blockchain; essi possono essere utilizzati per coinvolgere gli utenti o premiarli con servizi dalle app associate, questi gettoni potrebbero essere convertiti quindi in funzionalità e risorse di app di terze parti o anche scambiati tra tutti gli utenti.

Inoltre, anche in occasione di una fase di permesso e/o modifica, l'utente 1 può ricevere un compenso di natura digitale, come ad esempio un gettone crittografico virtuale (*token*), spendibile presso la struttura informatica, o presso gli stessi sistemi informatici, per acquisire, servizi, priorità o altri vantaggi.

Si noti che, per poter interagire come utente 1, non sono previsti permessi, basta generare la propria chiave asimmetrica pubblica/privata 4 e richiamare una funzione di iscrizione nel punto di accesso prescelto. Invece, per interagire come gestore 104 di sistemi informatici 103, è necessario superare un processo di approvazione per valutare la duplicazione dei dati e le interazioni delle statistiche delle informazioni personali che il gestore richiede alla struttura 100.

Il gestore 104 di ogni app affiliata può utilizzare le statistiche ottenibili dalle informazioni di libero accesso 7 per creare qualche elemento unico nell'app stessa. Ad esempio, in un gioco può fornire un oggetto specifico o un'arma specifica, o un luogo, in base alle statistiche dell'Insieme di dati personali protetti.

Una qualsiasi app potrebbe, ulteriormente, utilizzare le informazioni di libero accesso 7 come un modo per coinvolgere gli utenti in un percorso di ludicizzazione.

Casi d'uso

1. Il caso d'uso finanziario

Una app di gestione di materie finanziarie offre all'utente uno strumento finanziario che lo aiuta a generare un piano finanziario di natura pensionistica, consentendo anche all'utente di calcolarne la fattibilità. La app utilizza già una blockchain privata per archiviare i piani utente e tutte le loro revisioni: la struttura informatica potrà così essere impiegata per salvare tutti i piani in un archivio privato, così da consentire all'utente di decidere se e quando condividere questi dati con qualsiasi istituto finanziario. Una società di terze parti (assicurazione, banca o investimento) potrebbe chiedere all'utente di esaminare la propria pianificazione finanziaria per generare un sistema di punteggio finanziario, in modo che una richiesta di accesso, ad esempio un'assicurazione, possa essere più agevole, poiché la compagnia assicurativa potrebbe richiedere l'accesso ai propri dati (nome indirizzo ecc.), dati

privati (ID documento) e dati finanziari. L'utente ha il controllo completo su cosa condividere con l'azienda, e quando, e fino a quando, potendo così non condividere automaticamente nessun aggiornamento sulla propria situazione finanziaria. <Le sole informazioni di libero accesso potrebbero anche essere condivisi in forma anonimaad aziende interessate ad analisi di mercato o raccolta dati, generando un sistema di ricompensa in cui un utente potrebbe essere ripagato in denaro o in gettoni virtuali, o in premi per la condivisione di queste informazioni, anche con le istituzioni pubbliche (vedi agenzie di statistica nazionali o università a scopo di ricerca), mantenendo sempre il controllo completo su cosa condividere e quando. La app cambierà anche le statistiche relative alle informazioni personali protette, ad esempio per un utente che cambia il suo piano molto spesso, attribuendo un profilo di rischio più alto o più basso.

2. Il caso d'uso dell'utilità

Un'azienda di gestione dell'energia utilizza la blockchain e la crittografia per creare comunità energetiche, centrali elettriche virtuali e/o un nuovo tipo di mercato energetico in cui l'utente può gestire meglio il proprio livello di servizio, vendere la propria energia prodotta in modo rinnovabile, ed essere parte di una comunità energetica per una migliore gestione dell'energia e una migliore consapevolezza sull'utilizzo dell'energia verde. La struttura informatica 100 può, in questo caso, memorizzare i dati di misurazione aggregati, suddivisi in periodi, per

poterli condividere con le aziende che richiedono ricerche sul consumo di energia in una determinata area, nazione o tipo di utente, condividere con TSO (organizzazione di servizi di trasporto) per gestire la rete energetica e trovare equilibri migliori, e l'utente può essere ricompensato grazie alla sua quota.

L'azienda di gestione dell'energia influenza le statistiche risultanti dalle informazioni di libero accesso rilasciate dagli utenti, ovvero in base all'impronta energetica dell'utente, così da migliorare le proprie performance nella gestione delle risorse energetiche.

3. Il caso d'uso dello stadio intelligente

Un'azienda che si occupa di intrattenimento, per esempio di eventi sportivi, emette *smart ticket*, ovvero soluzioni di pagamento intelligenti per sedi di eventi, impiegando la tecnologia blockchain per gestire i pagamenti e gli asset digitali ma generando anche molti dati sul locale a cui sta accedendo l'utente che vi si registra attraverso la struttura informatica 100: quando, come paga, cosa compra e come si comporta. Questi dati possono essere archiviati come informazioni di libero accesso per essere condivisi con società di marketing che li richiedono in forma anonima, generando valori per l'utente e mantenendo il controllo completo su cosa viene condiviso, quando e per quanto tempo.

Anche l'incentivazione mediante ambiente competitivo è una parte molto importante per questo tipo di aziende, e la scheda di un personaggio di giochi di ruolo potrebbe essere sfruttata per creare sistemi

di gioco che coinvolgono l'utente e lo spingano ad accedere a un locale per ottenere maggiori ricompense, o per essere più caratterizzato.

4. Il caso d'uso della salute

La struttura informatica sopra descritta può essere particolarmente utile nella gestione dei dati sanitari, in quanto questi tipi di dati sono molto sensibili e dovrebbero essere, per legge, di proprietà dell'utente piuttosto che degli enti sanitari.

Soprattutto in periodi di emergenze sanitarie, ma anche in generale, il problema della forte dispersione di informazioni, che si verifica quando un utente cambia ospedale o medico, è molto sentito. L'archiviazione dei dati sanitari nella struttura informatica consentirebbe all'utente di condividere la propria storia medica con qualsiasi medico che potrebbe richiederlo. Il più delle volte esistono anche correlazioni sconosciute che, per motivi statistici, non vengono divulgate perché raramente correlate: avere un unico luogo dove poter archiviare tutti i propri dati medici, i farmaci utilizzati, le analisi specifiche e così via, permetterebbe all'utente di condividere tutti i propri dati con qualsiasi medico che potrebbe richiederlo, mantenendo il controllo completo su cosa e quando condividere a chi, ma permetterebbe anche di ottenere molti più risultati da studi statistici di carattere clinico condotti sulle informazioni personali, se anonimizzate come informazioni di libero accesso.

5. Il caso d'uso dei videogiochi

L'industria del gioco può sfruttare in modo molto interessante l'impiego di una struttura informatica come descritta in precedenza, consentendo ai videogiochi di condividere risorse digitali e informazioni per generare valori specifici dell'utente che possono essere utilizzati all'interno dei giochi. Un videogioco può sfruttare la blockchain per la raccolta e la commerciabilità di asset digitali, e ha un meccanismo strategico applicato al gioco stesso, ma sfrutta anche il sistema in modo tale che ogni giocatore abbia le proprie informazioni personali protetti.

* * *

In conclusione, il metodo di gestione sopra descritto permette agli utenti di app, siti web e qualsiasi altra applicazione che interagisce attraverso la rete di essere i proprietari dei propri dati, e avere il controllo totale su di essi. Inoltre, il possesso di un'identità alternativa gestita attraverso un algoritmo crittografico consente loro di archiviare in modo sicuro le proprie informazioni ma anche di condividerle a chi vogliono, ottenendo in cambio una ricompensa in una logica di ludicizzazione della gestione delle proprie informazioni personali.

Si noti come questa logica possa insegnare all'utente il valore della privacy attraverso un compenso che corrisponde a comportamenti virtuosi in tema di tutela dei dati personali, e senza incorrere in alcuna spesa.

Nel descrivere la presente invenzione, sono state descritte tecniche e fasi che comportano specifici

vantaggi. Di conseguenza, per motivi di chiarezza, si eviterà di ripetere ogni possibile combinazione delle singole fasi in modo ridondante. Tuttavia, la descrizione e le rivendicazioni dovrebbero essere lette con la consapevolezza che tali combinazioni rientrano interamente nell'ambito dell'invenzione e delle rivendicazioni.

Inoltre, nella presente descrizione sono stati discussi nuovi sistemi e metodi implementati dal computer per l'elaborazione di dati, di diritti e di transazioni inerenti a contenuti digitali…. Nella descrizione che segue, a scopo di spiegazione, vengono riportati numerosi dettagli specifici allo scopo di fornire una comprensione completa della presente invenzione. Risulterà evidente, tuttavia, all'esperto del ramo che la presente invenzione può essere messa in pratica senza questi dettagli specifici.

Al sopra descritto metodo di gestione… un tecnico del ramo, allo scopo di soddisfare ulteriori e contingenti esigenze, potrà apportare numerose ulteriori modifiche e varianti, tutte peraltro comprese nell'ambito di protezione della presente invenzione, quale definito dalle rivendicazioni allegate.

Metodo di gestione per l'archiviazione e la condivisione di informazioni personali

RIVENDICAZIONI

1. Metodo di gestione per l'archiviazione e la condivisione di informazioni personali (102) in una struttura informatica (100) che comprende almeno un processore e almeno un server condiviso (3), una rete di connessione a cui detto server (3) condiviso è atto a connettersi con una pluralità di dispositivi client (2) attraverso detta rete di connessione, detti dispositivi client (2) essendo associati a rispettivi utenti (1), che comprende:

- una fase di iscrizione (opzionale), in cui un utente (1) si registra presso detta struttura informatica (100) impiegando una chiave crittografica pubblica (4), nel caso di iscrizione libera (quindi senza registrazione) qualsiasi utente potra' registrare le proprie informazioni nella struttura (100) senza richiederne un accesso specifico;
- una fase di accredito, in cui un gestore (104) di sistemi informatici (103) acquisisce una chiave crittografica privata (9) e registra, presso detta struttura informatica (100), uno o più sistemi informatici (103) atti a interagire con l'utente (1);
- una fase di permesso, in cui detta struttura informatica (100) riceve dall'utente (1) la richiesta di impiegare detti uno o più sistemi informatici (103) come utente registrato presso detta struttura informatica (100), fornendo, attraverso detta struttura informatica (103),

informazioni personali (102) che vengono suddivise in informazioni di libero accesso (7), non vincolate all'identità dell'utente, e in informazioni private (8), che definiscono l'identità dell'utente;

- una fase di caricamento, in cui dette informazioni personali (102) sono registrate in almeno un registro pubblico distribuito (101) secondo la tecnologia *blockchain*;
- una fase di accesso alle informazioni private, in cui detto gestore (104) di sistemi informatici richiede all'utente (1), attraverso detta struttura informatica (100), un'autorizzazione ad accedere a dette informazioni private (8), e l'utente (1) concede l'autorizzazione impiegando la sua chiave crittografica pubblica (4);
- una fase di accesso alle informazioni di libero accesso (7), in cui detto gestore di sistemi informatici richiede a detta struttura informatica (100), impiegando la sua chiave crittografica (9), di accedere alle informazioni di libero accesso; e
- un'eventuale fase di modifica, in cui detta struttura informatica (100) riceve dall'utente (1) la richiesta di impiegare detti uno o più sistemi informatici (103) come utente registrato presso detta struttura informatica (100), aggiungendo, modificando o cancellando, attraverso detta struttura informatica (100), informazioni personali (102) che vengono suddivise in informazioni di libero accesso (7) e in informazioni private (8).

2. Metodo di gestione secondo la rivendicazione 1,

che comprende una fase di ricompensa in cui l'utente (1), in occasione di una fase di permesso e/o modifica, riceve un compenso di natura digitale.

3. Metodo di gestione secondo la rivendicazione 1, in cui detta struttura informatica (100) fornisce un punto di accesso agli utenti (1), come un sito web e/o una app, accessibile da un dispositivo client (2).

4. Metodo di gestione secondo la rivendicazione 1, in cui le chiave crittografiche pubblica (4) e privata (9) sono fornite dalla stessa struttura informatica (100).

5. Metodo di gestione secondo la rivendicazione 1, in cui, nella fase di scrizione, l'utente (1) sceglie una o più identità alternative (6), alter-ego o avatar, con cui verrà identificato, se permesso dalle regole vigenti, nei sistemi informatici (103) nei quali egli opererà.

6. Struttura informatica (100) in cui è implementato il metodo di gestione per l'archiviazione e la condivisione di informazioni personali di una delle rivendicazioni precedenti, che è connesso a una rete *blockchain* che fa riferimento a un registro pubblico distribuito.

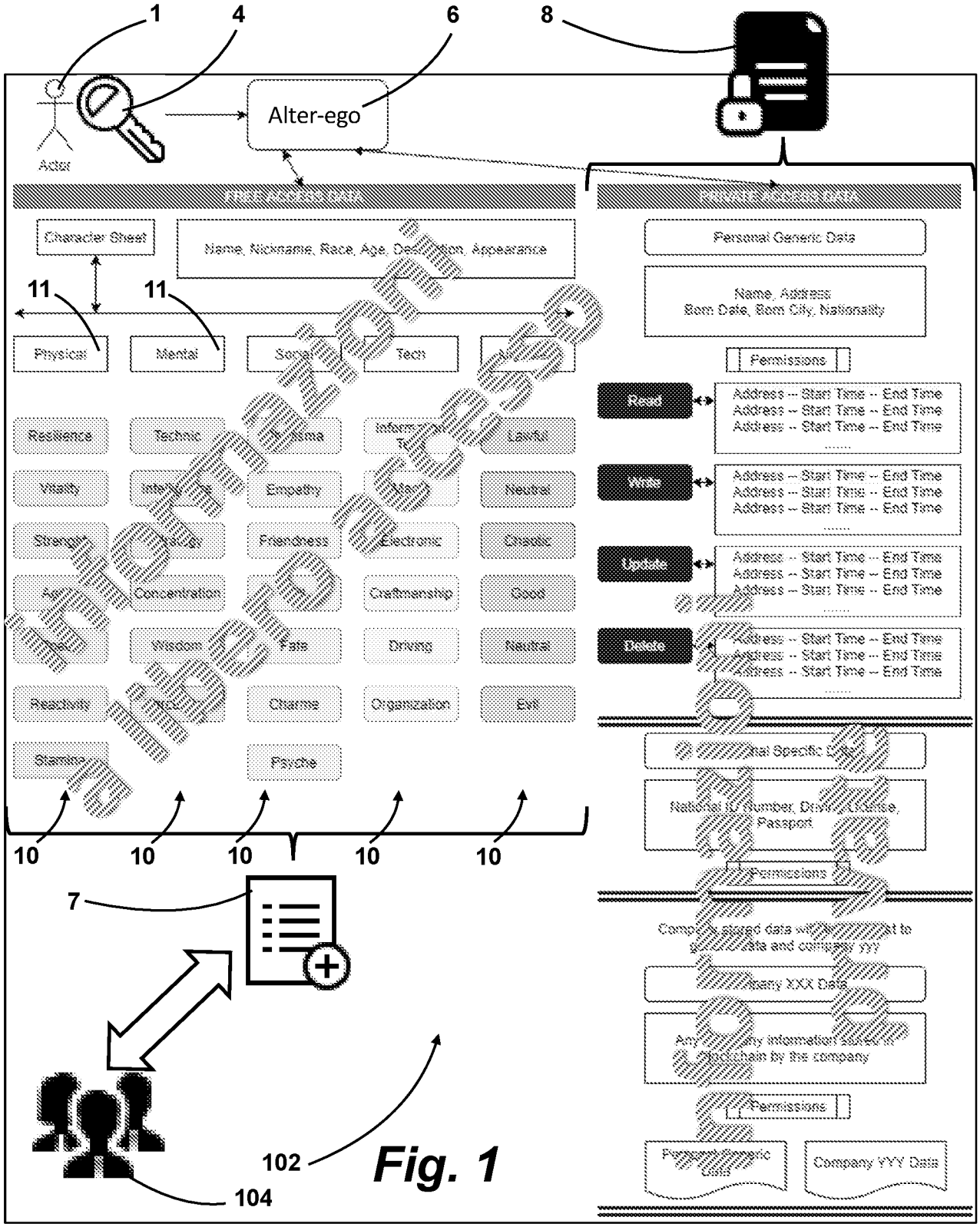

Fig. 1

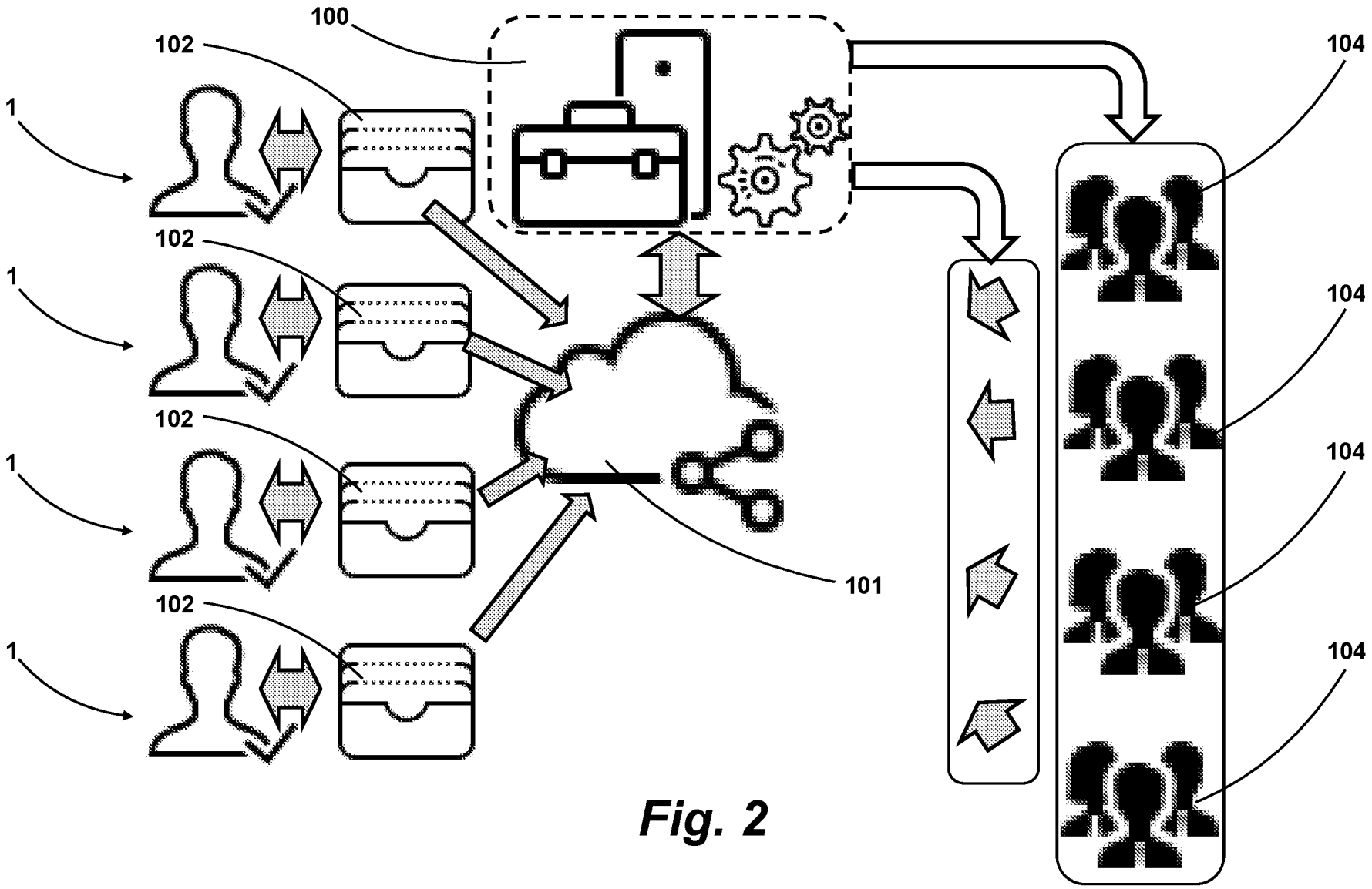

Fig. 2

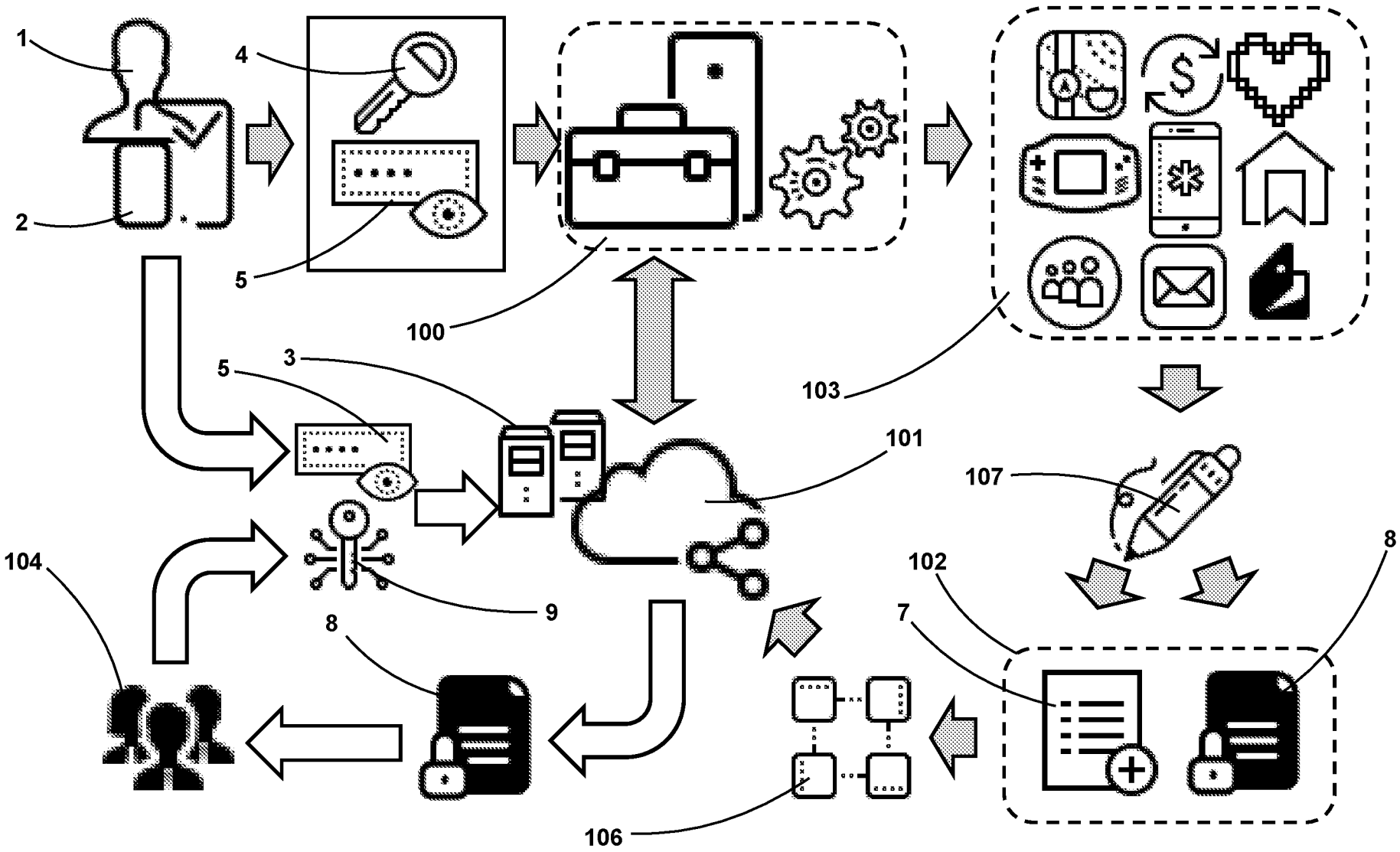

Fig. 3