WEB DESIGN

treccani.it/enciclopedia/web-design_(XXI-Secolo)

di Giovanni Anceschi, Davide Fornari - XXI Secolo (2010)

Web design

Il *web design* è un settore ibrido per eccellenza, per vari motivi: intreccia differenti discipline, ma soprattutto si evidenzia come una pratica di scrittura e, allo stesso tempo, come un'attività di configurazione. Si parla normalmente di *web-architecture*, per es., e tutta la terminologia è allora intrisa di portali e piazze elettroniche, per non parlare della nozione stessa di sito. Anche l'interfaccia ha a che vedere con l'idea di facciata. E questo quando del web si vogliano cogliere i caratteri strutturali, diremmo statici, e distributivi; ma nell'immaginario del web è molto presente anche la terminologia della mobilità, che ci parla di processi soggettivi, progressivi e dinamici: vi si trovano termini come *navigator*, *explorer* e simili. Spazio ma anche tempo. Il web design assume però contemporaneamente un carattere 'terzo', di disciplina trasversale – diciamo così – di servizio: si occupa infatti di come fare affiorare e di come porgere contenuti prodotti da altri e informazioni da data-base, e li presenta graficamente. Non solo graficamente, ma, come vedremo, in versione multimediale. In altre parole, se il design di interfacce consisteva in prima istanza nel dare forma alla metaforica membrana osmotica che ha luogo fra oggetto e utilizzatore, successivamente il web design si è concentrato su come mostrare informazioni di provenienza anche lontanissima e svariata sullo schermo del nostro personal computer.

Oggi il web design sta però vivendo una profonda trasformazione, legata ai cambiamenti tecnologici che hanno investito gli strumenti informatici, con il trasferimento delle tecnologie digitali e ICT (*Information and Communication Technologies*) nel campo, per non dire addirittura nel corpo, degli oggetti tecnici e degli oggetti d'uso. A questo punto, per es., risulta sempre più difficile – si pensi al *wearable computing* – anche solo isolare la membrana osmotica di cui parlavamo, senza vederla intrecciata e distribuita nella rete degli oggetti che costituiscono l'ambiente in cui viviamo.

Non sarà forse che nel giro di qualche lustro, così come è nato e si è sviluppato, il web design è giunto oggi alla propria estinzione?

Una definizione

Con web design si intende la progettazione di artefatti comunicativi – o, se usiamo una terminologia informatica – di applicativi fruiti da utenti finali sul *world wide web*, per mezzo di un *browser* o di un altro software basato su tecnologie web. Questo tipo di progettazione – che ha per oggetto pagine, siti e applicazioni web – è per sua natura multimodale, in quanto manipola i diversi ingredienti che vanno a costituire le tecnologie mediali (per es., font e calligrafie, e poi filmati, foto, disegni, illustrazioni, schemi e *icons*; ma anche: parlato, musica, canto, rumori ed *earcons*; o perfino: dinamismi, cinetismi, gestualità e mimiche), coinvolgendo così una gamma di attività operative appartenenti a diverse branche della comunicazione, quali il design grafico, l'immagine coordinata, l'architettura delle informazioni o *infodesign*, la tipografia, la fotografia, l'animazione, la *human-computer in-teraction*, e molte altre (Anceschi, Botta, Garito 2006).

A sua volta, il web design può essere considerato un vero e proprio sottoinsieme dell'*interaction design*, e questo sia da un punto di vista concettuale sia per il fatto che, nel nostro equipaggiamento di artefatti, si vanno sempre più diffondendo le applicazioni delle ICT che impiegano sistemi basati sul web. L'impatto di queste tecnologie ha avuto una ricaduta fondamentale sulla configurazione stessa degli oggetti d'uso e degli artefatti comunicativi. Le loro modalità di progettazione ne sono state profondamente trasformate: da un sistema cronologicamente stringente, strettamente vincolato alla sequenzialità di ciò che sta prima e ciò che sta dopo e basato sull'"impaginato', si è passati a una logica esperienziale e immersiva, coreografica e registica, basata sulla 'messa in scena'.

I contenuti web possono essere statici – quando vengono progettati e realizzati una volta e richiedono per ogni modifica l'intervento di un operatore – oppure dinamici: quando sono capaci in altre parole di integrare in maniera automatica contenuti o formattazioni, sia come risultato delle attività dell'utente oppure del gestore del sito sia come manifestarsi dell'approvvigionamento di informazioni da data-base.

Il primo 'sistema' web, realizzato nel 1991 dall'allora ricercatore presso il CERN (*Conseil Européen pour la Recherche Nucléaire*) di Ginevra Sir Timothy Berners-Lee, combinava due tecnologie già esistenti da decenni: la rete (o web) creata a fini militari nel secondo dopoguerra per lo scambio di informazioni in tempo reale, in un 'ambiente' informatico controllato ma soprattutto non monocentrico; e l'ipertesto, un sistema di organizzazione delle informazioni testuali scritto in HTML (*Hyper Text Mark-up Language*). Questo primo esempio di sito web di fatto univa alla gerarchia del testo, formattato e distinto in paragrafi, la possibilità di creare connessioni – link – al suo interno e all'esterno, garantendo così la navigabilità fra pagine.

Nel tempo il sistema HTML si è evoluto, permettendo di integrare immagini e tabelle nelle pagine web. In particolare, la costruzione di tabelle – per la presentazione di informazioni in forma di tabulati – è stata piegata alla progettazione dei siti web, fornendo quell'ossatura modulare della pagina che nella progettazione editoriale chiameremmo gabbia.

L'avvento dei CSS (*Cascading Style Sheets*), o fogli di stile, ha permesso un'operazione importante: i CSS consentono, sempre utilizzando il sistema HTML nella progettazione web, di trattare i contenuti separati dalla loro presentazione formale (formattazione del testo, colori, sfondi, stili).

La progettazione di siti web viene generalmente considerata affine alla progettazione editoriale, quando in realtà se ne discosta in maniera significativa. Mentre l'insieme di saperi coinvolti nel processo progettuale è molto simile – al punto che potremmo parlare di una sorta di baricentro disciplinare comune – a essere ben diverse sono le capacità redazionali che definiscono la gerarchia e la gestione delle informazioni. Nella progettazione di siti web, per quanto dinamici nella variazione e nell'adattamento dei contenuti, la pianificazione iniziale, cioè la redazione di contenuti con un taglio e un linguaggio adatti alla lettura a schermo, la gerarchizzazione delle informazioni, la progettazione della navigazione e infine il presupposto che il web va inteso come servizio, sono passaggi preliminari e indispensabili, specifici della disciplina nel senso che garantiscono o meno l'efficacia e il successo dell'artefatto. Solo a questo punto e fatte salve queste condizioni preliminari, un sito web (e in generale un'applicazione testuale informatica) diventa un artefatto per la presentazione di informazioni, che funziona in maniera non troppo differente da un libro composto da testo e immagini, di cui rappresenta

l'evoluzione tecnologica (Bolter 20012). La differenza principale consiste nel fatto che ora testi e immagini possiedono una potenzialità in più: quella che potremmo chiamare profondità temporale grazie alla quale 'cliccando' si può procedere nella specificazione percettiva e concettuale di termini e figure.

Dal web 1.0 al 2.0

Nel 1999 venne coniata la locuzione *web* 2.0 come prefigurazione del web futuro, rispetto alla sua condizione, ritenuta in quel momento embrionale: il web sarebbe diventato un «meccanismo di trasporto, l'etere attraverso cui si sarebbe realizzata l'interattività» (D. DiNucci, *Fragmented future*, «Print», 1999, 4, p. 32), cioè il canale, più che il supporto, di ogni futura interazione con gli artefatti fisici e con il loro carico di informazioni. Web 1.0 è quindi un retronimo con cui si indica lo stato del web e del web design precedentemente all'esplosione dei domini '.com' – siti web di proprietà commerciale – avvenuta nel 2001.

Ai tempi del web 1.0, le connessioni a Internet attraverso *modem dial-up*, cioè a chiamata, rendevano l'esperienza di fruizione dei siti web lenta e frustrante, soprattutto in presenza di contenuti non testuali (immagini, video, audio). Le pagine web inoltre, erano statiche, ospitate in server remoti, e non rendevano possibili commentare i contenuti.

Il passaggio dal web 1.0 al 2.0 può quindi essere visto come il risultato di una serie di concause, tra cui le innovazioni tecnologiche, come la diffusione della banda larga, il miglioramento dei browser, la diffusione di piattaforme con applicazioni Flash e lo sviluppo di massa della 'widgetizazzione'. Un *widget* è una parte di un codice HTML – per es., una pagina web – che aggiunge un contenuto non statico al codice stesso, prendendo spesso la forma di un'applicazione a pieno schermo in grado di fornire informazioni generalmente di contesto: sul clima, l'andamento del mercato, il tempo. Molte piattaforme di condivisione di contenuti che hanno segnato il passaggio al web 2.0 fanno ampio uso di codici widget per la gestione dei contenuti in maniera dinamica.

Fondamentale in questo passaggio è stato anche il cambiamento nei comportamenti degli utenti del *world wide web*. Rispetto a una prima fase pionieristica della progettazione di interfacce web, e alla nascita della figura professionale del web designer, il web 2.0 ha visto un'ampia

diffusione sia della fruizione della rete sia delle conoscenze pratiche necessarie a immettere e gestire contenuti, oltre alla diffusione in tutto il pianeta dell'hardware: i personal computer o altri prodotti incorporanti ICT per la fruizione del web (computer palmari, telefoni cellulari, reti *wireless*) sono onnipresenti nei Paesi del cosiddetto primo mondo, e si stanno diffondendo anche nei Paesi in via di sviluppo per sopperire alla mancanza di altre infrastrutture per la comunicazione, come le reti di telefonia fissa. In altre parole si è trattato complessivamente del passaggio da un tipo di *medium* gerarchico, a comunicazione unidirezionale, a un sistema bidirezionale, oltre che multimodale. Il web design integrava già, pur con alcuni limiti tecnici, i *media* classici come il cinema, la televisione e la radio, oltre al 'testo scrittorio'. Ma con l'avvento del web 2.0 la comunicazione fra gli utenti del web – per es., sito e fruitore – è divenuta sempre più paritetica o colloquiale: si osservi in tal senso la diffusione di strumenti di scambio di informazioni sia in differita (i forum) sia in tempo reale (le chat, i servizi di telefonia Internet, le videoconferenze).

Oggi i blog – abbreviazione di *weblog* – e i *social networks* sono generati in maniera dinamica: permettono agli utenti commenti sui *post*. I post sono le immissioni di contenuti che caratterizzano quei siti o portali in cui uno o più utenti inseriscono contenuti multimediali. A questo tipo di utenti, che fruisce e al tempo stesso produce contenuti web, ci si riferisce con il termine di *prosumer* – neologismo risultato della crasi fra *producer* e *consumer* –, diffuso anche nell'ambito del design. Si è trattato quindi di un passaggio dalla pubblicazione alla partecipazione, dai contenuti web intesi come risultato di un investimento individuale a un processo dinamico e interattivo di natura sociale se non addirittura collettiva, e dai sistemi centralizzati di *content management* ai link basati sulla pratica del *tagging* (*folksonomy*, o in italiano folksonomia: cfr. Flew 20083).

Folksonomy (crasi di *folk* e *taxonomy*) è un neologismo che indica la pratica collettiva di attribuzione di un significato ai contenuti web: un'attribuzione – diciamo così – dal basso. Questa si realizza conferendo una specifica categoria a testi, immagini, video, audio attraverso l'utilizzo di parole chiave (*tags*) che funzionano da didascalie ai contenuti immessi nel web. Questo tipo di collaborazione spontanea contiene nell'etimo di *folk* un tradimento della 'tassonomica' classica, a indicare la spontaneità, la non rigorosità disciplinare che si sviluppa spesso nei social network o nei siti di condivisione dei contenuti. Il tagging è diventato sia una forma

euristica – è possibile ricercare i contenuti di un sito o di un blog scegliendo i tag come chiavi di ricerca – sia uno strumento di costruzione delle pagine web. Ma esiste addirittura un uso improprio e provocatorio del tagging: si è diffusa nei social network la pratica di 'taggare' in una fotografia i volti dei partecipanti al gruppo ritratto, ma allo stesso tempo è invalso l'uso di taggare dentro a una qualsiasi immagine i nomi di tutte le persone che ci si vuole garantire vedano l'immagine in questione.

Il web 2.0 si riferisce nel suo insieme a questa seconda generazione dello sviluppo e della progettazione di siti web, caratterizzata da forme di comunicazione facilitata, dalla condivisione di informazioni e dalla collaborazione fra utenti.

Una nuova prospettiva progettuale

Le innovazioni tecnologiche e i cambiamenti sociali – l'estendersi cioè delle comunità di utenti e il modificarsi delle modalità di fruizione del web – hanno portato a una trasformazione radicale del web design. Non si tratta più infatti di progettare siti web intesi come singoli artefatti, e nemmeno come portali che danno accesso a un insieme di servizi che poi, come effetto dell'applicazione di un progetto di immagine coordinata, sono costituiti di pagine fra loro coerenti. Nel web 2.0 l'artefatto 'sito' non è più al centro del progetto, mentre le piattaforme, i motori di ricerca, le interfacce, intese come sistemi di significazione, diventano di primaria importanza. Anche nella progettazione dei siti web si tende quindi a prescindere da una logica di artefatto. Non si progetta più un sito come un manufatto da usare o abitare, ma si preferisce un approccio 'teatrale' o 'coreutico'. Si tratta, insomma, di progettare una 'scena' per l'azione del fruitore e, contemporaneamente, gli 'attrezzi di scena', per es., in forma di widget, che ognuno può montare o utilizzare come vuole. Si tratta quindi di configurare le condizioni affinché l'attività di scambio fra uomo e macchina avvenga fluidamente: progettare interazioni non solo attraverso la creazione di apposite interfacce, ma soprattutto attraverso l'adozione di altre forme di interfacciamento, come il linguaggio naturale o il movimento gestuale, alla ricerca di una scioltezza comportamentale totale. In questo senso il nucleo e il campo di lavoro del web designer saranno sempre più centrati sull'interazione fra utente e apparato informatico, piuttosto che sul design delle interfacce web, in quanto i *media* attraverso cui i sistemi informatici e tecnologici sono destinati, appunto, a interfacciarsi con le comunità di utenti sono diversi e numerosi. Non si tratta quindi nemmeno

più di immaginare la varietà delle coreografie per un unico supporto (design esperienziale), ma di prevedere, accogliere e gestire la varietà delle possibili interazioni nella loro spontaneità (design evenemenziale).

La diffusione della piattaforma multimediale Flash – inizialmente prodotta da Macromedia e poi da Adobe, che l'ha integrata con altri strumenti per il *publishing* appartenenti alla Creative suite – a partire dal 1996 ha profondamente influenzato il dibattito disciplinare sul web design. Flash divenne – in un panorama di siti realizzati in HTML e quindi statici e 'tabellari' – lo strumento per aggiungere attrattiva ai siti web. Il software omonimo permette infatti di realizzare animazioni e di innestare nelle pagine componenti dotate di motilità, ma anche di inserire contenuti video, consentendo di manipolare contenuti *raster* – cioè composti da pixel – o anche vettoriali, ossia scalabili all'infinito senza perdere in definizione. Per determinare questi contenuti, che si sviluppano in uno spazio chiamato *stage*, proprio come il palco teatrale, Flash utilizza un sistema di notazione denominato ActionScript. Per la visualizzazione di contenuti Flash, i browser devono disporre di un componente specifico (il cosiddetto *plug-in* Flash). La grande innovazione del software Flash per la creazione di animazioni è stata la presenza di una *timeline* che assimila il programma a un sistema di montaggio video, con la possibilità di inserire contenuti multimediali: immagini, video, tipografia e così via. ActionScript permette di creare, oltre alle animazioni, intere applicazioni, come video interattivi e videogiochi.

La diffusione di animazioni Flash, segnatamente come 'intro' alle *home pages* dei siti del web 1.0, ha suscitato, a suo tempo, un dibattito disciplinare sull'usabilità dei siti che le incorporano, come sostenuto da Jakob Nielsen (2000). L'anatema di Nielsen – che però, diventato in seguito consulente di Flash, ha modificato la sua posizione – suonava così: i contenuti artistoidi prodotti in Flash non sono editabili, né selezionabili, né copiabili, né modificabili e, soprattutto, rallentano l'accesso degli utenti ai contenuti del sito (in quel periodo vi era anche scarsa diffusione di connessioni veloci). La creazione di contenuti animati che, in quella fase iniziale di abuso creativista del software, erano di inevitabile fruizione, riavvicinava il web design a un altro *medium*, la televisione, da cui si distingueva chiaramente e sempre più per l'interattività e per la comunicazione biunivoca (*one-to-one*) invece che strettamente gerarchica (*one-to-many*). Inoltre, la personalizzazione degli elementi di interfaccia

dei siti abbassava il livello di standardizzazione del web in un momento in cui la sua diffusione come *ipermedium* di comunicazione di massa richiedeva uno sforzo di uniformazione (Nielsen, Loranger 2006).

In questo senso, lo sviluppo del web design è andato di pari passo con la definizione della *graphic user interface* (GUI). La denominazione GUI è legata allo sviluppo di interfacce per personal computer, quando il sistema grafico, non più verbocentrico ma 'per oggetti', sviluppato dalla Xerox Palo Alto research unit venne proposto come alternativa al sistema di interfacciamento legato alla riga di comando, rigidamente scrittoria e lineare, impiegato, per es., sui personal computer MS-DOS fino alla diffusione dell'ambiente Windows. Le GUI permettono all'utente di agire direttamente, attraverso un puntatore (tipicamente, il mouse), su icone, finestre e menu, elementi da cui deriva l'acronimo WIMP (*Window, Icon, Menu, Point-ing device*). Nella massima parte dei personal computer e dei loro sistemi operativi, gli elementi della GUI risultano modellizzati attraverso la metafora della scrivania. Anzi sarebbe forse meglio parlare di allegoria, cioè di metafora prolungata e articolata, che crea un ambiente di lavoro concettualmente e graficamente coerente (Botta 2006).

La diffusione di tecnologie aptiche (tattili) nei prodotti elettronici di consumo e il continuo investimento nei sistemi *multi-touch* hanno portato alla diffusione di schermi tattili: l'esempio più famoso è quello di iPhone della Apple, ma schermi aptici erano già ampiamente diffusi in apparecchiature automatiche come gli sportelli bancari automatici o le macchine emettitrici di biglietti. Le interfacce tattili presentano una situazione di grande interesse in quanto il monitor o la superficie di interazione diventano lo strumento su cui l'utente agisce con la sua mano (punta, ruota, sposta), e integrano ogni altra componente hardware tradizionale che compare o scompare a seconda delle necessità: tastiera, visore per camera e videocamera, pannello di controllo audio e così via. Le GUI infatti permettono un numero limitato di operazioni rispetto a quelle che un utente può effettuare agendo direttamente attraverso la gestualità tattile: un esempio molto chiaro è dato dalle operazioni manuali che possiamo compiere con immediatezza su un iPhone, e che richiederebbero invece diversi passaggi in un ambiente bidimensionale e l'ausilio di un puntatore.

Nel tempo il web design e il design di interfacce hanno visto i rispettivi campi d'azione sempre più sfumati e sovrapposti: si sono diffuse piattaforme 'proprietarie' – cioè determinate da logiche commerciali – che offrono non solo contenuti ma anche applicativi. Il caso lampante è quello di Google: nato come motore di ricerca, presenta oggi una vasta offerta di servizi, come caselle di posta elettronica, mappe multimediali, condivisione di documenti, vendita di merci, ricerca su testi scientifici, consultazione di opere cartacee digitalizzate. Un servizio-locomotiva che trascina con sé un intero, stratificato, portale di servizi. In questo senso, non risulta più possibile distinguere fra web design e design delle interfacce: quanto avviene attualmente sul monitor, il flusso di informazioni e significazioni che vi transita, ci pone di fronte a interrogativi radicali rispetto al ruolo del designer. Questi non si occupa più soltanto di presentare informazioni prodotte da terzi in una logica di servizio, ma è impegnato a costruire sistemi di semiotica visiva che creano abitudini e fidelizzano gli utenti nell'accesso ai contenuti e ai significati del web. Google sta cercando di definire una serie di interfacce standard per i propri prodotti: non si tratta più e soltanto di *corporate image* applicata alla GUI, ma di mediazione dell'accesso ai contenuti del *world wide web* e quindi, di conseguenza, dei significati stessi (C. Vandi, *La strategia di Google. Abiti e pratiche*, e, su posizioni diverse, C. Gianelli, *Progettare l'interazione attraverso l'azione. Le interfacce open source*, in *Il discorso sul design*, «E/C», 2009, 3, 4 pp. 163-72 e 173-82).

Progettare comunità

Un fattore di profonda innovazione per il web design è costituito dalla diffusione di tecnologie per la gestione dei contenuti, ovvero i CMS (*Content Management Systems*). Si tratta generalmente di applicazioni web che permettono la gestione di contenuti HTML anche a utenti non specializzati e consentono il controllo e l'operabilità di pagine dinamiche comprendenti testo, immagine e altri elementi, come video o musica, che possono essere incorporati nelle pagine attraverso l'inserimento di un codice fornito dalla piattaforma in cui i contenuti risiedono, come nel caso dei video presenti su YouTube.

Generalmente un applicativo per web CMS fornisce gli strumenti per creare e gestire contenuti da parte di utenti senza conoscenza di linguaggi di programmazione. Questi applicativi utilizzano dei data-base per archiviare dati a essi relativi, e impiegano interfacce interne ai browser: si

evidenzia così nuovamente la sovrapposizione fra web design e design delle interfacce. Mentre l'utente di un CMS ha nessuna o poca esperienza nella gestione di un sito, l'autore del sistema CMS deve essere un ingegnere informatico o un designer, in modo da poter rendere il mantenimento dei siti web un'operazione relativamente semplice per amministratori non tecnici.

Il PHP (*Personal Home Page*) è un linguaggio di programmazione per produrre pagine web dinamiche, creato nel 1995 e diffuso in forma libera, poi diventato una modalità standard della programmazione di pagine HTML. Questo linguaggio agisce principalmente come filtro su una serie di contenuti, eseguendo delle operazioni che producono come output una pagina HTML, cioè visibile sul web. Alcuni siti web di particolare interesse sono scritti in linguaggio PHP, come, per es., Facebook, Wikipedia, Wordpress, YouTube e diversi altri.

In questo senso, gli applicativi CMS e il linguaggio PHP hanno contribuito a disfare la logica che connetteva i designer al design di siti web, intesi come artefatti. La diffusione di portali, di siti basati su sistemi di gestione dei contenuti e di comunità on-line ha annullato le distanze progettuali fra utente e web. Il design dei siti web diventa sempre più costruzione di 'infrastrutture' informatiche, cui provvedono ingegneri e programmatori, lasciando le scelte formali agli utenti finali. Queste interfacce, in cui la variabilità è rappresentata dalla definizione dei CSS, sono espressione di «una diffusa riluttanza alla figuratività, probabilmente sintomo di una serie di pregiudizi verso la questione della forma, che ancora è intesa come un vezzo progettuale, mentre la progettazione di sistemi comunicativi informatizzati avviene utilizzando approcci e metodi di tipo funzionalista, un funzionalismo di ritorno che è poi puro formalismo» (Botta 2006, pp. 249-50). In altre parole, accanto agli ingegneri e programmatori sarebbero auspicabili figure di designer che padroneggino la tecnologia, molto simili all'antico industrial designer o al designer sistemico delle comunicazioni – in un ruolo che potrebbe essere quello di rappresentante degli utenti finali – al tavolo delle trattative del progetto web e informatico.

La diffusione di pratiche comunitarie sul web è stata possibile proprio grazie a queste innovazioni nella gestione tecnologica dei sistemi comunicativi. Minimizzando le competenze necessarie alla gestione dei siti, i sistemi CMS hanno reso fattibile l'accesso al web per gli utenti meno esperti. Un primo approccio si è concentrato specialmente sui contenuti

testuali, come è avvenuto per i primi weblog o blog, siti web gestiti secondo una logica diaristica. L'autore-gestore del sito scrive liberamente dei post – ma oltre al testo formattato, è possibile inserire immagini, audio e video, in un ambiente grafico governato da CSS, modificabile e implementabile – di cui può autorizzare e filtrare i commenti. La pratica di commento ha reso possibile lo sviluppo di comunità: in ogni blog figurano gli amici dell'autore, sotto forma di link a blog del medesimo portale o di avatar (parola di origine sanscrita che si riferisce alla discesa in terra di una divinità, in forma umana, animale o fantastica e che nell'uso corrente indica l'icona che rappresenta l'utente all'interno di un software di gioco o in un social network on-line). Questa comunità globale basata sul web ha preso il nome di *blogosphere*, o blogosfera, ossia un network sociale interconnesso virtualmente – e anche fattualmente – attraverso link, commenti, post e blog collettivi che, per livello di specializzazione, assumono in certi casi il ruolo di 'riviste' tematiche e diventano spesso le fonti dei *mass media* tradizionali. Le pratiche del tagging dei contenuti e la folksonomia rendono possibile la ricerca dei contenuti per analogia: una pratica fondamentale per la costruzione di queste comunità virtuali.

Tali comunità esistevano ovviamente anche prima della diffusione dei blog, in forma di gruppi di partecipanti a forum virtuali che lasciavano messaggi e commenti in differita su piattaforme web condivise. I primi blog erano pagine web statiche modificate manualmente dagli autori: in questo senso la disponibilità di CMS e di portali di blog ha reso possibile la diffusione indiscriminata dei blog e delle relative comunità di blogger.

La programmazione di un blog può avvenire in maniera autonoma, utilizzando una base Wordpress, uno dei fornitori più attenti alla qualità grafica dei format di blog, usando PHP e un sistema di gestione di data-base. Ma l'apparente semplicità di progettazione è tale soltanto se l'utente si accontenta di uno dei temi o generi grafici disponibili. In alternativa, è necessaria una buona conoscenza di CSS e PHP (Budd, Collison, Davis et al. 2006). L'impiego di un linguaggio di programmazione di apprendimento non immediato sposta nuovamente il focus delle competenze necessarie al web designer – sempre più informatico e sempre meno grafico – oppure scinde la progettazione di siti in competenze strutturali-funzionali e formali-estetiche.

Mentre i blog e gli applicativi necessari al loro funzionamento possono essere implementati nei siti web degli utenti, la diffusione di comunità on-line basate, per es., su un interesse degli utenti per un *medium* specifico ha stabilito nuovi confini nel web design. I siti destinati agli appassionati di fotografia – quali Fotolog e Flickr – permettono, per es., di raccogliere immagini, creare didascalie e tag, stabilire pratiche di gestio-ne dei diritti in un ambiente comunitario, destinato sia a individui sia a gruppi. Generalmente, le pagine di gruppi raccolgono immagini che sono state prodotte nelle pagine di individui. La ricerca nel data-base di questi siti permette anche agli utenti non registrati di visualizzare risultati per analogia sulla base di tag e didascalie. Selezioni di immagini provenienti dai siti hanno anche prodotto pubblicazioni (*Fotolog.book*, 2006) o mostre virtuali, come nel caso di Jpeggy. Ciò che conta è che questo tipo di siti non ha ragione d'essere come oggetto commisurato alle esigenze di un utente specifico: il progetto grafico del sito è già un progetto di comunità, di una serie di pagine standard che si dipanano a partire dalla home page e che sono riempite da contenuti gestiti in maniera semplificata dagli utenti registrati. La personalizzazione di questi 'palcoscenici individuali' è limitata alla definizione delle dimensioni delle immagini, alla loro scelta, alla loro classificazione.

Un'altra comunità significativa è quella di Last.fm: un sito che permette di importare il contenuto audio presente sul proprio personal computer e di renderlo disponibile all'ascolto sulla propria pagina personale. Di nuovo, è l'analogia a costruire connessioni dinamiche fra utenti secondo la logica: «se ti piace il cantante *x*, dovrebbe piacerti anche il gruppo *y*». Questo tipo di interazione automatizzata e resa possibile da filtri e algoritmi, costruisce relazioni, contenuti e sistemi sulla base di informazioni altrimenti 'residenti' su macchine individuali e non interconnesse.

Il sito YouTube è nato come piattaforma di condivisione di contenuti video attraverso tecnologie Flash. Le pagine personali prendono in questo caso il nome di *canali*. Prima del lancio del sito nel 2005, esistevano pochi metodi per condividere contenuti video sul web: per es., caricando file video su un server e rendendoli visibili attraverso opportuni *plug-in*, con difficoltà di caricamento per connessioni lente alla rete. L'interfaccia utente del sito ha reso possibile il caricamento e la conversione dei video per la loro condivisione. Inoltre, è possibile incorporare i video depositati in YouTube all'interno di altri siti, semplicemente copiando una sequenza di codice

HTML. E ciò perché non esiste un metodo consentito per scaricare i video destinati a essere fruiti soltanto attraverso l'interfaccia di YouTube o tramite altri siti in cui vengono incorporati, che raramente sono 'canali individuali' per la fruizione diretta. YouTube ha diffuso sia la pratica del tagging sia la fruizione *random*, resa celebre dall'uso di altri prodotti, come iPod mini di Apple, un lettore di file audio MP3 che non incorporava un visore e proponeva quindi l'ascolto di musica in ordine casuale. Nel caso di YouTube, la folksonomia e il tagging sono i criteri principali che regolano l'ordinamento dei contenuti in un sito che possiamo considerare un deposito o un magazzino di contenuti – per così dire – immateriali.

Due siti, infine, hanno stabilito nuovi standard nella definizione grafica del web: Second life e Facebook, non a caso esempi ibridi di applicazioni web, siti e software allo stesso tempo, con componenti informatiche scaricabili o fruibili sul web. Second life è un ambiente-mondo virtuale lanciato nel 2003, accessibile attraverso un applicativo gratuito e la rete Internet. Gli utenti, chiamati residenti, possono interagire con l'ambiente e fra loro attraverso degli avatar. All'arrivo nel 'mondo' di Second life, ogni utente 'rinasce', e sceglie il proprio sesso e il proprio aspetto, attraverso un processo generativo per tappe che rappresenta uno dei momenti di maggiore interesse (Gerosa 2007). Questo genere di vita virtuale e mediata da un avatar era stato sperimentato dai MMOG (*Massive Multiplaying Online Games*), per es., EverQuest, che attualizzava il regno virtuale di Norrath, dove 'vivevano' più di 500.000 giocatori iscritti, o il coreano Lineage, con 8 milioni di 'abitanti'.

Il concetto di avatar era stato reso popolare nella narrativa fantascientifica, in particolare in quel filone definito *cyberpunk*, nel quale si postulava una pronta diffusione della realtà virtuale immersiva, profezia che si è invece scontrata con la difficoltà di produrre ambienti virtuali tridimensionali con velocità di *refresh* per ottenere, come avviene nell'ambito del cinema, che l'occhio umano non riesca a registrare la frammentazione del movimento.

In Second life si realizza una situazione ibrida di reale e virtuale: l'evoluzione delle ICT applicate al web permette di fatto un'autorappresentazione identitaria digitale, dinamica e interagente: siti e ambienti web vengono a sovrapporsi al reale in scala 1:1. I residenti di Second life esplorano un mondo definito *grid*, dove incontrano altri residenti, partecipano ad attività ricreative o commerciali – è possibile acquistare a un cambio variabile una valuta chiamata Linden dollar, dal

nome del produttore del software di Second life – costruiscono oggetti grafici tridimensionali virtualmente fruibili, abitabili, a seconda dei desideri. Queste realizzazioni, cui si possono aggiungere funzionalità attraverso un linguaggio di programmazione, sono prodotte attraverso strumenti semplici. In Second life sono presenti, oltre agli utenti individuali, organizzazioni e istituzioni che si occupano di scopi non-profit, come università e musei che offrono attività didattiche o culturali in un ambiente tridimensionale, il cui aspetto figurale e grafico è il risultato sistemico della collaborazione fra utenti e sviluppatori, in una logica di *prosuming*.

Alla luce dell'esperienza di Second life, Facebook è un'enorme raccolta di avatar in senso lato. Non si tratta di repliche dell'utente o di personaggi mossi da lui sulla scena tridimensionale del grid come una marionetta. Sono rappresentanti virtuali dell'utente su una scena sociale artificiale. E sono rappresentanti in gran parte 'mimetici'. In altre parole, generalmente, ritraggono più o meno fedelmente l'utente, o comunque l'utente li considera rappresentativi di sé. Il nome stesso del sito tradisce un progetto di raccolta dei volti degli utenti. Le loro facce associate ai loro dati personali e attraversate dagli strumenti di ricerca garantiscono un'esperienza di interazione rafforzata e rassicurata dalla promessa veridittiva del volto, generalmente quello reale, ridotto a immagine fotografica, bidimensionale e statica (*Il fenomeno Facebook*, 2008). Si può pensare a Facebook come a un campo di gioco: in fondo il designer/ingegnere informatico – o, in altre parole, Facebook in quanto intrapresa – è l'ideatore e il costruttore del 'tavoliere di gioco' e delle regole per giocare. Il partecipante ha tutte le libertà, se resta dentro le regole. E, come avviene con il gioco delle bambole o con quello della guerra, Facebook insegna comportamenti: per es., le regole della *netiquette* (come accogliere o rifiutare amicizie nell'elenco della posta dentro al gioco esibizionista/voyeurista delle proprie conoscenze galanti o importanti, perché visibili a tutti gli altri utenti), ma insegna anche direttamente delle abilità, per es., a comunicare in sincronia (in chat) o in differita (sul wall). Facebook è il luogo di un'evasione – è infatti, anche, un gigantesco *surprise party* – ma un'evasione confinata, come un quartiere protetto, da regole precise e dall'impunità del virtuale; è infine un luogo ibrido reale/virtuale, una versione virtuale del mondo reale. È costitutivo

dell'esperienza Facebook il piacere/fastidio derivante dalla presenza discreta di tutti gli altri utenti accettati come amici, come amici degli amici e così via.

Facebook – dal nome degli annuari americani, che riportano volti e nomi degli studenti – è un vero e proprio mondo a parte, con regole proprie rispetto al diritto d'autore e al copyright: ogni elemento – testo, immagini, audio e video – diventa proprietà dell'ospite Facebook, che in cambio di un'interfaccia grafica coerente entra in possesso di contenuti e dati personali degli utenti con evidenti problemi di privacy. Gli utenti possono così organizzare il proprio network, oltre che ricercando nomi e indirizzi e-mail dei propri amici, operando ricerche sui tag personali: città di nascita e residenza, scuole frequentate, posti di lavoro e così via. Facebook ha integrato molte delle funzioni particolari svolte da altri siti che sono stati oggetto di analisi, per es., la condivisione di blog e microblogging – cioè scrittura in tempo reale di poche righe di testo –, di immagini organizzate in gallerie e di video, incorporati da YouTube. Con il risultato di raggiungere una carica di contenuti multimediali che offre un aggiornamento – in tempo reale – per tutto il network sulle attività degli utenti, in un ambiente grafico ordinato e prestabilito, in cui l'utente può controllare la disposizione di widget presentati nella sua pagina personale. Facebook si basa inoltre su tassonomie proposte dal sito, permettendo, attraverso algoritmi che costituiscono un segreto industriale della piattaforma, l'accrescimento del proprio network e l'affiliazione a gruppi di utenti, che rappresentano prodotti, persone, pratiche comuni. Gli utenti possono, anzi sono – per così dire – 'sospinti' a comunicare attraverso un sistema di posta elettronica interno al sito, attraverso forum o mediante conversazioni in diretta (chat). Si tratta di un sito gratuito, destinato all'intrattenimento, che produce profitti sulla base della vendita di spazi pubblicitari, personalizzati sugli utenti, venduti con la stessa logica dei *media* tradizionali (pubblicità tabellare), ma in collaborazione esclusiva con un'azienda di computer come Microsoft.

L'interfaccia grafica di Facebook è fortemente normalizzata: è sensibilmente diversa da quella, per es., di MySpace, un sito che permette una maggiore personalizzazione delle pagine dei membri attraverso HTML e CSS. Facebook ammette il caricamento di contenuti eterogenei, rendendo personalizzabili informazioni di pubblico dominio, ma non permette una modifica dell'aspetto delle pagine personali. Per sviluppare applicazioni in

Facebook, come, per es., versioni elettroniche degli scacchi o di Scarabeo, esiste un *Facebook mark-up language*, che ha permesso la diffusione del sito nelle sue versioni per telefoni cellulari.

Scenari aperti

Abbiamo già evidenziato come il web design abbia visto il proprio campo di applicazione estendersi e sovrapporsi con quello delle interfacce. Ma di fronte alla nascita dell'*interaction design*, la stessa progettazione dei siti web diventa una delle regioni di quest'ambito progettuale. Soprattutto in uno scenario che vede sempre più frequente l'incorporazione di tecnologie digitali e ICT dentro gli oggetti d'uso. Si tratterà sempre meno di progettare interfacce interattive e sempre più di immaginare interazioni tattili, vocali, coreutiche. In particolare, l'*ubiquitous computing* – ossia il diffondersi di tecnologie distribuite nell'ambiente e il trasformarsi dell'intero ambiente in un 'ambiente sensibile' – in prospettiva tenderà a ridurre in gran parte il lavoro del web designer. Non solo, ma, come abbiamo visto, il sito web è sempre meno oggetto di progettazione da parte del singolo designer, ed è sempre più il riflesso di un progetto di ampia portata, che fornisce gli strumenti di gestione di una o più pagine a utenti con conoscenze solo elementari di design, realizzato da ingegneri e programmatori, e forse *neodesigners*.

Il web è divenuto un ambiente performativo, l'ambiente in cui si gioca una partita esistenziale: ognuno propone e produce i propri contenuti, ed è nell'interazione fra utenti che si realizza un'ulteriore diffusione e rielaborazione. Peraltro, di fronte a queste nuove prospettive di design delle 'infrastrutture' della comunicazione e di design degli 'attrezzi di scena', i *media* classici rischiano di dissolversi: libri e giornali rischiano di diventare un modello di diffusione delle informazioni e della cultura non sostenibile per diversi motivi – ambientali, ecologici, economici – e in questo senso, ossia nella migrazione da libri e riviste cartacei a *media* elettronici, il (web) designer ha ancora molto da fare. La progettazione grafica esecutiva di libri e riviste è passata dalle mani dei tecnici tipografici direttamente a quelle dei grafici attraverso l'uso di applicativi di impaginazione e gestione di immagini, vettori e tipografia – è il caso di Adobe indesign o di QuarkXPress – che nel tempo hanno iniziato a costituire la base 'registica' di un'ulteriore serie di applicativi che, a loro volta, implementano soluzioni web, come HTML: è possibile cioè inserire rimandi interni ed esterni a un testo che viene impaginato con i medesimi

applicativi destinati ai *media* 'cartacei'. È quindi possibile implementare funzioni web dentro un file PDF (*Portable Data Format*), il formato più conosciuto, che per essere visualizzato richiede un *plug-in* di diffusione ormai globale. Questo apre nuove prospettive nel campo della progettazione di siti web, che forse vedranno nuovamente all'opera il grafico inteso come progettista di artefatti comunicativi, ora elettronici, aggiornabili, cliccabili che, per il momento, sono alla ricerca dei propri e specifici canali di fruizione. Amazon – un sito che vende principalmente libri, ma anche altre merci – ha sviluppato, per es., una piattaforma software e hardware per diffondere la pratica dell'e-book: libri in formato elettronico, quindi immateriali, acquistabili sul proprio sito web e visualizzabili su una periferica – il Kindle – che permette di stivare e leggere testi in bianco e nero. La migrazione digitale dei testi è un processo inarrestabile, che offre nuove possibilità al design per definire il comfort, i metodi e le configurazioni degli ipertesti del futuro (*Questione di leggibilità*, 20082).

Web design: la fine o un nuovo inizio

Alla domanda iniziale, relativa alla possibile estinzione di questa specializzazione disciplinare, nel corso dei veloci sviluppi che vivono ora tanto il web quanto il design, non si può francamente rispondere che il web design è estinto. Finché ci saranno entità organizzate che intendono presentarsi autonomamente sulla rete, ci saranno siti, e quindi ci saranno progettisti di siti: siti che informano l'utente (per es., che propongono un'immagine istituzionale o presentano un catalogo di prodotti e servizi) e altri che gli consentono di compiere operazioni a distanza (telecertificazione, teleacquisto e così via). Ma la stragrande maggioranza del traffico che passa in rete non è ormai più strutturato secondo un modello di comunicazione gerarchica: un'entità forte che parla a molti destinatari. Il web è diventato un ambiente della socializzazione.

Chi naviga nel web si muove nei corridoi di un immenso e onnivoro archivio/galleria/biblioteca, e questo nella prospettiva di cercare e/o offrire un particolare contenuto e in quello di frequentare i suoi analogici dintorni (come ci insegnano, in modi diversi, Google, Wikipedia o YouTube). Chi esplora e passeggia sul web si muove lungo i *passages* di un immenso *mall*: il luogo del mercato, dove scambiare beni e servizi (come E-bay e Amazon). Chi soggiorna sul web frequenta oggi una sorta di

immenso parco di divertimento, un ambiente unificato del *loisir* e del tempo libero (come i MMOG, Facebook, e tutti i siti dedicati all'erotismo e alla pornografia).

Transito è la parola chiave. Chi progetta il web oggi progetta, insomma, i flussi del transito degli utenti e dentro e intorno a essi. Crea *main streets* e piazze: in altre parole disegna le infrastrutture di un grande sistema della mobilità virtuale. Si tratta, in questa prospettiva, di creare movimento, fornire opportunità, generare occasioni, costruire canali, attorno ai quali si dipana la vita sociale, si mettono in atto la fruizione e il consumo culturale e si sviluppano il mercato, il consumo e il profitto. Dentro a questo, che è solo parzialmente un progetto consapevole ma è soprattutto un grandioso andamento socioculturale, il problema dell'estensione se non dell'universalizzazione dell'accesso, diventa fondamentale (e ci riferiamo all'accesso materiale, non solo attraverso l'aggiornamento continuo delle tecnologie dell'informazione e della comunicazione, ma pensiamo anche alla disponibilità dell'hard-ware necessario a fruire i contenuti da parte di tutti i 'mondi', come nel caso del *laptop* XO, nato come personal computer a basso costo per i Paesi poveri da un'idea di Nicholas Negroponte). Ma soprattutto si tratta di accesso cognitivo e concettuale. Di un sapere e saper fare diffuso e condiviso. In fondo l'intera storia dell'informatizzazione non è che la storia di un tumultuoso avanzare tecnologico (con la svolta cruciale di Silicon Valley), ma anche la storia della massimizzazione del numero degli utenti. Una massificazione che è anche articolazione sempre più sfumata delle specializzazioni e degli interessi. Ma è allo stesso tempo la storia dello sforzo per superare le difficoltà dell'accesso appianandole, rendendole amichevoli, mascherandole e nascondendole. È la storia dello sforzo di rendere accessibili a un pubblico di non esperti le cose che la tecnologia ci consente di fare. E sarà sempre più la storia del passaggio dai criptici *commands* del sistema operativo MS-DOS, che passo per passo prescrivevano al computer cosa fare, al gesto sintetico del mouse, della cloche della *playstation*, del puntatore di Wii, per cui il computer ci deve capire a cenni, come un buon animale ammaestrato.

Il ruolo del designer informatico – e massimamente del web designer – è diventato, e diventerà sempre più, quello di facilitare lo scambio di informazioni. Il designer informatico è prima di tutto il progettista delle infrastrutture ed è poi l'orchestratore dell'interazione e dell'interfaccia percorribile che rendono il web fruibile, comprensibile, gestibile, piacevole.

Bibliografia

J. Nielsen, *Designing web usability. The practice of simplicity*, Indianapolis 2000 (trad. it. *Web usability*, Milano 2000).

J.D. Bolter, *Writing space. Computers, hypertext, and the remediation of print*, Nahawah (N.J.) 20012 (trad. it. Milano 2002).

G. Anceschi, M. Botta, M.A. Garito, *L'ambiente dell'apprendimento. Web design e processi cognitivi*, Milano 2006.

M. Botta, *Design dell'informazione. Tassonomie per la progettazione di sistemi grafici auto-nomatici*, Trento 2006.

A. Budd, S. Collison, Ch.J. Davis et al., *Blog design solutions*, Berkeley (Cal.) 2006.

J. Nielsen, H. Loranger, *Prioritizing web usability*, Berkeley (Cal.) 2006 (trad. it. *Web usability* 2.0. *L'usabilità che conta*, Milano 2006).

Fotolog.book. A global snapshot for the digital age, ed. A. Long, N. Currie, London 2006.

M. Gerosa, *Second life*, Roma 2007.

T. Flew, *New media. An introduction*, Oxford 20083.

Il fenomeno Facebook. La più grande comunità in rete e il successo dei social network, «nova24» - «Il Sole 24 ore», Milano 2008.

Questione di leggibilità. Se non riesco a leggere non è solo colpa dei miei occhi, a cura di L. Baracco, E. Cunico, F. Fogarolo, Venezia 20082.

Il discorso del design. Pratiche di progetto e saper-fare semiotico, a cura di D. Mangano, A. Mattozzi, «E/C», 2009, 3-4, n. monografico.

Vocabolario

design
design ‹diʃàin› s. ingl. [propr. «disegno, progetto», dal fr. dessein, che a sua volta è dall'ital. disegno] (pl. designs ‹diʃàinʃ›), usato in ital. al masch. – Nella produzione industriale, progettazione (detta più precisamente industrial design…

web tax
(Web tax) s. f. inv. Insieme di norme volte a regolare la tassazione sui guadagni delle grandi aziende che operano sul web, che hanno sedi all'estero ma vendono in Italia. ◆ [tit.] Rinvio per la web tax. [testo] La web tax, la norma introdotta...

nuovi media

Lessico del XXI Secolo (2013)

nuòvi mèdia (o <... *mìdia*>) locuz. sost. m. pl. – Espressione entrata a far parte del lessico degli studi sulla comunicazione verso la fine del 20° sec., che indica i mezzi di comunicazione informatizzati. Oltre che all'informatica, la novità dei media si sostanzia nell'interattività, nella partecipazione creativa e nella formazione di comunità di utenti intorno ai contenuti digitali. In senso strettamente tecnico i n. m. coincidono con lo sviluppo dell'informatica di massa e del personal computer. La rapida diffusione ed evoluzione delle tecnologie digitali ha dato luogo a un processo di convergenza con i mezzi di comunicazione tradizionali, come la telefonia mobile e la televisione, estendendo a questi le qualità reticolari e interattive associate all'informatica. Sono considerati n. m. anche i videogames, oltre a tutto il complesso di applicazioni nate su Internet – dalla posta elettronica alle chat room, dal web ai forum, dai blog ai social network – e ai dispositivi utilizzati per accedere alla rete, quali i palmari, gli smartphone, i tablet. Il concetto di n. m. si qualifica soprattutto per l'implicito riferimento a questioni artistiche, culturali e politiche che contiene, prima tra tutte la promessa di democratizzare la produzione, la distribuzione e l'accesso a informazioni e conoscenze artistiche e culturali. Una delle caratteristiche salienti dei n. m. è infatti la versatilità, che permette loro di rispondere meglio nel tempo ai bisogni del proprio utilizzatore, dando vita al paradigma dell'*on demand*, che si sostanzia nella possibilità, oltre che nella sempre più stringente aspettativa, di poter accedere ai contenuti di proprio interesse in qualsiasi momento, da qualsiasi luogo, utilizzando un qualunque dispositivo digitale.

Il linguaggio dei nuovi media. – Secondo lo studioso Lev Manovich, i n. m. sono caratterizzati da modularità, variabilità e automazione. Un contenuto digitale è composto da diverse parti, o moduli. La continuità è data da un insieme di oggetti uniti da una stringa di informazioni ma separabili a piacimento, senza che la struttura complessiva ne venga danneggiata. Queste parti rendono il prodotto flessibile, dato che può essere scomposto, modificato e ricomposto in continuazione, in modo da creare prodotti differenti. Tutti i contenuti cognitivi dei n. m. possono essere ridotti a dati

digitali che sono trasformati e manipolati da software. Così, una pagina web può essere composta da testi, immagini, filmati, file musicali, senza coincidere singolarmente con nessuno di questi oggetti, né con l'insieme degli oggetti stessi: lo stesso insieme di oggetti potrebbe essere utilizzato per costruire una pagina web totalmente diversa. I n. m. possono anche dar vita a diverse versioni dello stesso oggetto: per es., un'immagine può essere manipolata e modificata con l'uso di specifici algoritmi, al fine di invertirne i colori, di modificarne la definizione e di intervenire sull'apparenza e sulle forme in questa rappresentati. Infine, la flessibilità e la potenza dei processori permette di rendere automatici molti processi: per es., creare interfacce personalizzate, recuperare file e documenti da fonti diverse, estrarre dati significativi da grandi basi di dati (v. data mining).

I nuovi media come ambiente. – I n. m. sono il risultato dell'integrazione e dell'ibridazione dei media precedenti, in un costante processo di ri-mediazione dove si intrecciano relazioni, funzioni e prassi di tutta la tastiera mediale disponibile (dalla stampa alla televisione): un ambiente comunicativo pienamente multimediale, in grado di integrare formati e domini della comunicazione originariamente distinti e distanti. Strumenti di accesso e di espressione di rete, i n. m. ricalcano l'architettura reticolare: semplice, flessibile e decentrata, articolata in nodi autonomi tendenzialmente paritari e disposti alla cooperazione e allo scambio di risorse cognitive. Alle caratteristiche intrinseche dei n. m. come oggetto tecnologico fa riscontro una nuova concezione dei mezzi di comunicazione, dove l'oggetto tecnologico agisce come elemento catalizzatore di un ambiente formato da attori sociali e dinamiche culturali e materiali. In quanto processi di mediazione col mondo, i n. m. favoriscono la formazione e la condivisione delle esperienze. Un luogo virtuale che consente di sperimentare il processo di costruzione del sé, attraversato da flussi identitari mobili, messo costantemente alla prova nelle interazioni comunicative. La ricchezza lessicale, sintattica e relazionale dei n. m. li ha posti al centro di un'utopia di emancipazione fondata sulla libera cooperazione degli individui, in opposizione ai rigidi modelli gerarchici dei mezzi di comunicazione di massa. Secondo Jay D. Bolter e Richard Grusin, «ogni nuovo *medium* trova una sua legittimazione perché riempie un vuoto o corregge un errore compiuto dal suo predecessore, perché realizza una promessa non mantenuta del *medium* che lo ha preceduto» (*Remediation. Understanding new media*, 1999). Un'utopia non diversa

da quella associata, quasi un secolo prima, all'avvento della radio e alla sua promessa di eliminare spazio e tempo come limiti alla comunicazione umana.

I nuovi media come comportamento. – I n. m. rompono la secca alternativa tra mezzi di comunicazione fondati su rapporti uno a uno, come le comunicazioni postali e quelle telefoniche, e uno a molti, come la stampa, la radio e la televisione, creando un ambiente nuovo e in perpetuo cambiamento. Strumenti come Internet, la posta elettronica, il web, la telefonia cellulare, rappresentano tutti modelli che combinano rapporti uno a uno e molti a molti. La separazione tra autore e pubblico sfuma al pari di quella tra produttore e consumatore (v. prosumer): ciascun nodo della rete può essere l'uno o l'altro in un processo di diffusa cooperazione. La cooperazione in rete ha alimentato movimenti artistici e culturali, dando vita a prodotti innovativi: dal software open source, alle enciclopedie online, dalla ricerca scientifica (v. scienza 2.0) alla realizzazione in rete di prodotti e servizi per conto di enti e imprese (v. crowdsourcing).

I nuovi media come disintermediazione. – Uno degli effetti delle possibilità abilitanti dei n. m. è la generale democratizzazione delle forme artistiche e culturali, in termini sia di possibilità creative sia di accesso, visibilità e distribuzione di opere. L'utilizzo di software per la composizione di testi, per il ritocco delle immagini, per la manipolazione dei filmati, per il mixaggio di musica è profondamente diffuso in tutti gli ambienti sociali, favorendo l'irruzione di nuovi e inattesi talenti nella sfera ufficiale delle produzioni artistiche. La democratizzazione delle vie d'accesso all'arte non avviene senza frizioni tra il mondo consolidato dell'arte e della cultura da una parte e la miriade di artisti che emergono nelle reti digitali e nei social network dall'altra. L'affermazione di piattaforme di condivisione di fotografie, filmati, testi e opinioni o di reti sociali che combinano le funzioni di condivisione permette a molti artisti, prima sconosciuti, di conquistarsi un pubblico e una notorietà, senza dover passare per i tradizionali meccanismi di accesso al mondo professionale consolidato (v. disintermediazione). Allo stesso modo, l'affermazione di blogger competenti e dall'ampio seguito rappresenta una sfida al mondo del giornalismo. Ne consegue una profonda crisi dei tradizionali meccanismi di accesso alla sfera pubblica (esami di stato, appartenenza a ordini e corporazioni, colli di bottiglia di natura economica),

accompagnata da una continua ridefinizione dei confini tra cultura alta e cultura popolare, tra lavoro e tempo libero, tra attività professionali e attività amatoriali.

Vocabolario

new media
new media ‹niùu mìidië› locuz. ingl. (propr. «nuovi media»), usata in ital. come s. new media pl. – Il complesso dei nuovi mezzi di comunicazione (Internet, tv digitale, telefonia cellulare, ecc.) frutto delle più recenti e avanzate tecnologie:...

mèdia
mèdia s. f. [femm. sostantivato dell'agg. medio, sottint. misura, quantità, ecc.]. – 1. In matematica e nelle sue applicazioni, media di un insieme di valori, o media aritmetica, o assol. media, il valore dato dalla somma algebrica degli elementi...

New Media

Alberto Abruzzese

Esiste una vasta letteratura sulla dimensione dei new media. Ma manca lo sforzo di rendere espliciti i poteri che si contendono i territori dell'esperienza. Manca la volontà di chiarire la natura del processo oltre gli schieramenti in cui sino a oggi siamo stati irretiti. La riflessione teorica sui nuovi media – emblematica quella di Pierre Lévy – assai spesso sembra dimenticare che tutte le promesse dell'innovazione digitale e telematica possono venire meno se non si delinea la forza di una soggettività sino a oggi repressa ma proprio per questo in grado di spezzare la continuità del Moderno e di ingoiarlo. In Italia, intellettuali di spicco come Umberto Eco o Furio Colombo hanno fatto la loro scelta: parlano dei new media a nome dei vecchi soggetti, cioè del "soggetto storico" di quel *modo di sapere* che essi credono o vogliono credere indifferente all'innovazione. In loro continua ad albergare il *principio di continuità*. Offrono la loro intelligenza per divorare il diverso e non per esserne divorati, per consegnarsi al banchetto. Si riconoscono l'un l'altro come custodi e non come *padroni* o *traditori*.

Resta in ombra la scelta opposta: evidenziare quanto più possibile la differenza tra i linguaggi della riproducibilità tecnica e quelli digitali. Tra una tecnologia industriale che opera sui testi e sul loro mercato distributivo e una tecnologia post-industriale, che opera direttamente sulla percezione e sul desiderio. Bisogna mettere al centro delle metamorfosi del presente una soggettività che non può più essere quella del patto sociale tra scrittori e lettori. In questo patto storico, nella sua lunga durata, si dispiegano non solo tutte le strategie che hanno caratterizzato il processo di socializzazione della civiltà moderna; non solo lo sviluppo della scrittura come matrice dei lin-

guaggi audiovisivi (di cui si è garantita il controllo attraverso il dispositivo della *sceneggiatura*). Ma vi si dispiegano anche le forme dell'arte, i rapporti tra artista e pubblico, tra pubblico e critica, tra critica e mercato.

Già la neotelevisione – cioè la fase estrema della TV generalista – ha lasciato emergere per la prima volta corpi quasi in tutto estranei al patto sociale tra scrittura e lettura: gente che non aveva i tratti socio-antropologici né dello spettatore dell'industria culturale di massa né del cittadino della civiltà metropolitana, tantomeno quindi del soggetto della politica moderna, quello delle classi, dei movimenti, del lavoro, delle istituzioni, dei partiti, dell'identità collettiva nazionale. Il mondo della scrittura e della critica – della stampa e della cultura – ha subito assegnato a questa gente gli attributi del *barbaro*, le qualità del disordine e della destabilizzazione. I sorveglianti della tradizione sono insorti in difesa dei vecchi produttori e dei vecchi consumatori, senza domandarsi (o dire) che cosa potesse significare l'invasione barbarica della scena televisiva nazionale. Essendo *incolti*, questi soggetti sono reputati *cattivi* e, essendo senza memoria istituzionale, sono definiti i*ncivili*, senza cittadinanza, senza coscienza politica. Subendo il paradigma dominante nelle élite sociali (con poche correzioni dilagato nell'opinione pubblica a mezzo della stampa, fattasi "élite di massa"), questi nuovi soggetti hanno ricevuto attenzioni soltanto strumentali: demagogiche o repressive o sprezzanti. Abbiamo così assistito al paradosso per cui un'esigua contro-élite, essendo in grado di interagire con questi nuovi pubblici e dunque di abitare intelligentemente lo spazio televisivo, è stata messa al bando dalle élite storiche, sino al giorno prima assai convinte del mandato divulgativo e popolare dell'intellettuale quanto della sua funzione scandalosa.

Al contempo il principe – attratto da una democrazia diretta televisivamente governabile al pari di quella rappresentativa – ha cominciato, seppure con discrezione e spesso sottobanco, a servirsi sempre più dei mediatori te-

levisivi dell'audience piuttosto che dei mediatori culturali. A loro volta, alcuni persuasori professionisti hanno imparato sin troppo bene a intrattenersi con il principe, a destreggiarsi nel gioco tra informazione e potere, senz'altro possibile referente che se stessi in quanto venditori. La povertà comunicativa – quindi conoscitiva e politica – delle vecchie élite intellettuali è stata così forte ed evidente da lasciare interamente il campo alla qualità di un sistema di potere tanto complesso quanto fatalmente incollato alla brutalità o rozzezza delle proprie regole. Il reiterato – quasi rituale – dibattito sul rapporto tra cultura e TV è divenuto il segno più emblematico della connivenza tra i limiti endemici del ceto intellettuale e i limiti altrettanto endemici del ceto politico e istituzionale.

Ora, tra il dominio della TV, che *fa vedere*, e lo spazio del pubblico e della società civile, che *guarda*, si è intromesso il computer, che *dialoga*. La sua capacità interattiva si contrappone alla tendenziale asimmetria dei media generalisti e della società dello spettacolo. L'interrogazione dominante è sul destino di questo nascente conflitto: integrazione con la società di massa o sua radicale negazione? *Mass computer* o *personal computer*? L'avvento del computer costituisce la punta estrema delle tecnologie, dunque dei poteri che ne hanno prodotto la fattibilità sociale corrispondendo a un insieme di fattori disomogenei: la guerra, le scienze pure e applicate, il mercato dei giochi.

Proprio in quanto attrezzatura estremamente duttile, adatta a corrispondere a ogni bisogno e a ogni forma d'uso, la comunicazione digitale ha la qualità di poter aprire accessi sociali di natura globale quanto locale, previsti quanto imprevisti, amichevoli quanto aggressivi. Non ha la rigidità delle macchine industriali, che sono commisurate alla determinata funzione che assolvono, alla modellistica sociale che servono, ai valori che diffondono. Dunque i nuovi media possono non rendere altrettanto semplice o quantomeno ripetibile l'operare dei sorveglianti. Nati come massima necessità di controllo e di simulazio-

ne, introducono tuttavia nuovi livelli conflittuali, nuovi fattori di squilibrio.

Il computer è (può essere) uno spazio aperto e malleabile, non rigido come oggi risulta il televisore. Il televisore nasconde o maschera i vertici che lo governano e mette in luce la piazza che lo consuma; il computer, per quanto sia ancora – o sembri essere – una strategia élitaria, tecnoscientifica, mette in gioco qualcosa che è sentito dalla corporeità diffusa dei consumatori, che già c'è, che attende da molto tempo: qualcosa che – dopo un intero lungo ciclo di artificializzazioni del corpo e di progressivi esoneri delle sue membra – riemerge tra noi. Qualcosa che, grazie ai linguaggi digitali, può finalmente esprimersi *fuori della nostra mente*: un aumento prodigioso delle simulazioni, al di là di ogni tradizionale analogia con la realtà, con le sue costruzioni sociali e con le sue immagini schermiche. Questo qualcosa è la possibilità di agire il tempo e lo spazio *mediante la corporeità delle cose*: soggetti, oggetti, relazioni, territori, memorie. I confini relativamente ancora circoscritti delle nostre protesi corporali si stanno aprendo a una dimensione inconcepibile per l'economia politica della riproducibilità tecnica.

Siamo agli albori. Tuttavia la qualità principale delle nuove tecnologie è la rapidità con cui il mercato abbassa i loro costi e facilita la loro interfaccia con l'utente. Il computer è un eccezionale traduttore – divulgatore – di se stesso; lo è in quanto dispositivo capace di rapide metamorfosi e non in quanto inerte diffusore, puro veicolo di sodalizzazione. Si trasforma a misura delle aspettative che può soddisfare: le insegue e anticipa. È un attrezzo integralmente culturale: non solo spazio ma anche tempo, non solo immagini audiovisive ma anche insieme di oggetti e strumenti di lavoro o di piacere, non solo produzione ma anche consumo, non solo agire sociale ma anche memoria e progetto. Ed è quest'attrezzo che entra nello stesso potenziale di sviluppo universale di mezzi familiari e personali come la cucina, il frigorifero, l'auto, il

telefono e il televisore. La generalità che esso deve arrivare a soddisfare – offrendo sempre più facili interfacce – riguarda trasporti, comunicazione, mercato, relazioni pubbliche e private, servizi, prestazioni, divertimento. Quanto più il computer, per essere usato, si emanciperà dal sapere della scrittura, dal suo potere di comando, tanto più si potrà approssimare alla corporeità illetterata del consumatore, alle sue risorse palesi e latenti, all'estro dei suoi desideri. Questo è il delicato transito socioantropologico che ci è di fronte.

Si tratta quindi di servirsi del computer non come antidoto della TV in quanto barbarie, disordine e destabilizzazione, ma al contrario come rilancio di questi dirompenti valori in una rete comunicativa che ne sappia esprimere il senso riposto, la soggettività reclusa, il non-detto. Si tratta di usare il computer per recuperare il nostro corpo e la nostra esperienza, quella parte di noi e quella parte di territori che la civiltà della stampa e dell'immagine ha oscurato per consentire lo splendore di una trasparenza collettiva altrimenti impossibile (e tanto necessaria allo sviluppo della società di massa).

Se ci si colloca dentro questa nuova soggettività *analfabeta*, allora ogni tradizione artistica moderna perde terreno e memoria, sprofonda nella persona. Nel cyberspace – che della persona è *il luogo senza luogo* – l'artista si fa *nessuno*, cioè finalmente uno e tutti. L'opera si fa incursione e arbitrio del desiderio: è il consumatore a farsi *creatore* e *critico*. Per un aspetto, la comunicazione digitale si apre al fenomeno – dal punto di vista estetico così irritante o quantomeno inqualificabile – dei tanti poeti, scrittori o pittori che si definiscono artisti trovando la loro legittimazione soltanto nel proprio desiderio di esserlo. Per altro aspetto, crea le condizioni atte a cancellare il carattere provinciale del protagonismo artistico e a dissolverlo in una condizione poietica generale.

The EDRi papers

EDITION 03

COME FUNZIONA INTERNET

Una guida per "policy-makers"

EUROPEAN DIGITAL RIGHTS

Per la versione italiana:

Centro Nexa su Internet & Società
Politecnico di Torino

Questo documento mette a disposizione
di tutti una guida introduttiva ad alcune
delle tecnologie che costituiscono il cuore di Internet.
Speriamo che questo testo rappresenti un utile
strumento di riferimento in grado di illustrare in
maniera accessibile il funzionamento di Internet,
la Rete globale la cui apertura è alla base di così
tanti diritti civili e di così tante attività economiche.

CONTENUTI:

Documento scritto da:
Joe McNamee, Advocacy Coordinator
Kirsten Fiedler & Marie Humeau, Advocacy Managers e Sophie Maisuradze, Intern

Design: CtrlSPATIE

La European Digital Rights (EDRi) è un gruppo di 32 associazioni sulla privacy e sui diritti civili digitali attive in 20 paesi

European Digital Rights
39 Rue Montoyer
B-1000 Brussels
tel: + 32 (0)2 550 4112
brussels@edri.org

Traduzione italiana a cura del:

Centro Nexa su Internet & Società
Politecnico di Torino

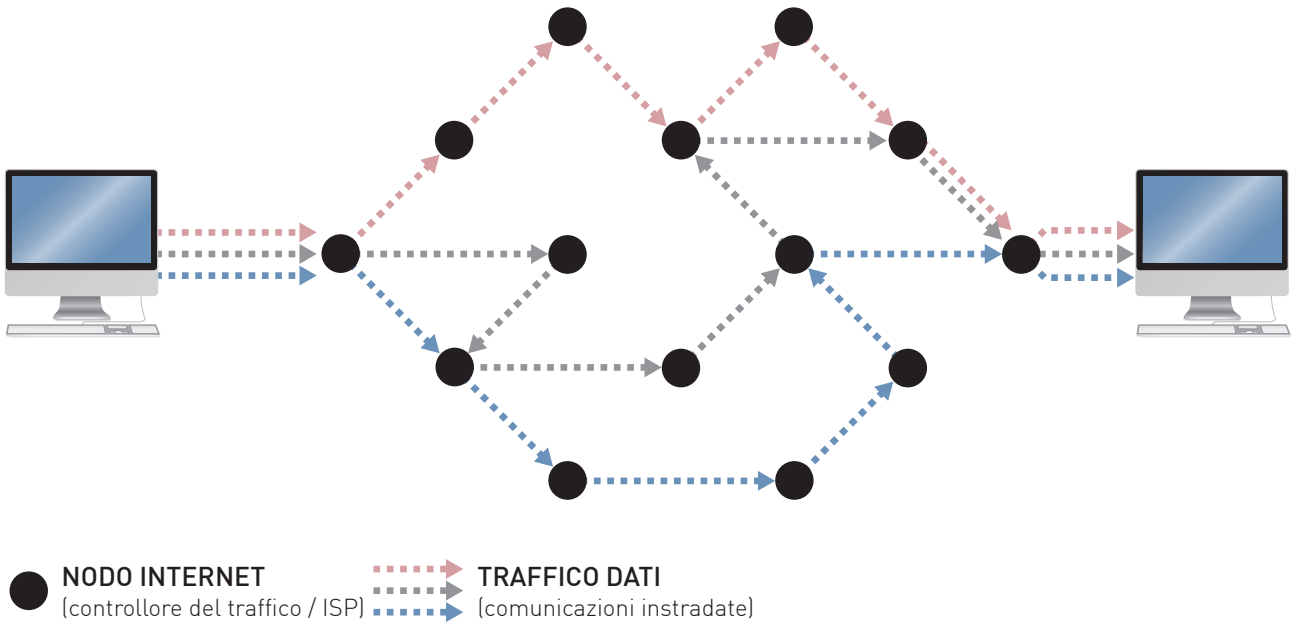
http://nexa.polito.it/ - Dip. Automatica e Informatica

Coordinatore: Juan Carlos De Martin.
Hanno contribuito: Elena Atzeni, Alberto Bellan, Fabio Chiusi, Arturo Di Corinto, Giuseppe Futia, Giovanni Battista Gallus, Raimondo Iemma, Luca Leschiutta, Luca Nicotra, Margherita Salvadori, Claudia Sarrocco, Valentin Vitkov. Si ringraziano i Fellow del Centro Nexa.

Versione 1.0 (9 maggio 2012)

INTERNET

UNA RETE DI RETI DI COMPUTER



Internet è un sistema globale di reti di computer interconnesse.

Quando due o più dispositivi elettronici vengono connessi per permettere la comunicazione reciproca, essi formano una rete. Internet è costituita dall'interconnessione su scala mondiale di reti di questo tipo, ciascuna appartenente ad aziende, governi o individui, col risultato di permettere a tutti i dispositivi connessi a tale rete di reti di comunicare tra di loro.

Per comunicare i computer devono essere in grado di comprendersi a vicenda. Su Internet la comunicazione è possibile perché tutti i dispositivi parlano la stessa "lingua" o protocollo, ovvero, il Protocollo Internet (in inglese, Internet Protocol, in sigla IP), un "mercato unico" senza barriere fisiche, tecniche o nazionali. Il protocollo IP costituisce la base di tutti gli altri sistemi di comunicazione su Internet.

Trasmettere una qualsiasi comunicazione su Internet usando il protocollo IP è come inviare le pagine di un libro per posta usando moltissime buste differenti. Tutte le buste usano lo stesso indirizzo mittente e lo stesso indirizzo di destinazione.

Anche se alcune buste viaggiano via nave e altre via aereo, alla fine tutte arrivano a destinazione ed il libro può essere ricomposto.

Su Internet il contenuto della busta (chiamata tecnicamente "pacchetto") dipende da protocolli, ossia, da convenzioni che definiscono il formato dei dati e le procedure di connessione per i diversi tipi di comunicazione. Esempi di queste convenzioni costruite sopra il protocollo IP sono:

- SMTP per spedire la posta elettronica;
- HTTP per accedere a siti web;
- BitTorrent per la condivisione di file in modalità peer-to-peer (P2P), ovvero tra pari (una modalità per condividere file di dati all'interno di gruppi di persone anche molto ampi).

Chiunque è libero di creare il proprio protocollo e usarlo su Internet, a patto che si basi sul protocollo IP.

In altre parole, il solo limite è l'immaginazione, la sola regola è che l'indirizzo sulla busta sia nel formato standard richiesto dal protocollo IP. L'apertura del sistema è ciò che ha reso Internet un fenomeno globale.

Qualsiasi restrizione dell'apertura di Internet riduce il suo potenziale di sviluppo futuro.

L'uso universale di un singolo protocollo di base per tutte le forme di comunicazione ha importanti vantaggi.

I dispositivi che sono responsabili per il trasporto dei dati su Internet (chiamati "routers", che in italiano potremmo tradurre come "instradatori") non hanno bisogno di essere programmati differentemente per trattare diversi tipi di dati. Anzi, non hanno alcun bisogno di sapere nulla dei dati che smistano, a patto che tali dati usino il protocollo IP.

Come il postino che consegna la posta tradizionale, i "router" devono solo guardare all'esterno della busta per essere in grado di consegnare il messaggio. Non importa se la busta contiene una bolletta o una lettera d'amore (tranne che per il ricevente, naturalmente).

Ciò implica:

- Possibilità di innovazione illimitata in termini di nuovi protocolli e nuove applicazioni, purchè costruite sopra il protocollo IP;
- Non c'è alcun bisogno di sapere nulla in merito al contenuto di qualsiasi comunicazione: "privacy by design"; [1]
- Flussi dati flessibili e veloci.

Essenzialmente, Internet offre un solo, flessibile servizio: trasportare dati da un dispositivo ad un altro a prescindere dalla natura dei dispositivi usati, da come e dove essi sono connessi a Internet e dalla natura o dal contenuto dei dati stessi.

"L'apertura e la flessibilità di Internet sono le ragioni primarie dei successi economici, d'innovazione e democratici resi possibili dalla Rete"

1 Con tale espressione si fa riferimento alla concezione secondo cui le tecnologie devono essere strutturate in maniera da assicurare una protezione dei dati intrinseca, di tipo tecnico-procedurale.

L'INDIRIZZO IP

UN INDIRIZZO DIGITALE

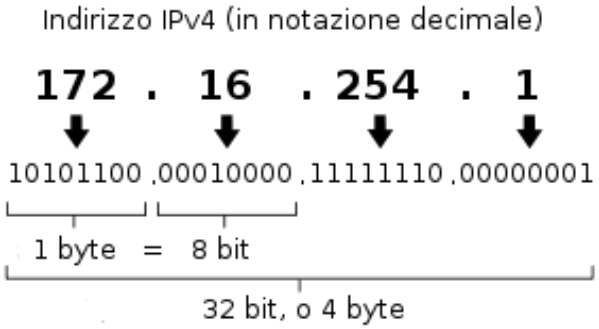
Un indirizzo IP è un indirizzo numerico che viene assegnato ad ogni dispositivo collegato ad Internet.[2]

In molti casi gli indirizzi IP possono essere utilizzati per identificare un'organizzazione o un individuo che usino un Internet Service Provider per collegare ad Internet uno o più apparecchi.

In altri casi, in particolare nelle reti aziendali, nelle connessioni wireless pubbliche o non protette e nelle connessioni mobili ad Internet, l'indirizzo IP non sempre identifica la persona che ha compiuto un atto tracciabile digitalmente.

Poiché un router casalingo o aziendale spesso mostrerà solo un indirizzo IP per tutte le persone connesse ad esso, l'indirizzo IP identificherà un gruppo di persone piuttosto che un singolo individuo. Di conseguenza, spesso è difficile, se non impossibile, essere sicuri di chi ha fatto cosa sulla base del solo indirizzo IP.

D'altra parte, gli indirizzi IP sono molto spesso associabili a specifiche persone, e perciò devono essere trattati come "dato personale" tranne nel caso in cui venga inequivocabilmente stabilito che non lo siano.



"L'indirizzo IP non sempre identifica la persona che ha compiuto un atto tracciabile digitalmente"

2 A causa della scarsità nell'attuale generazione di indirizzi IP, è sempre più comune, particolarmente nelle reti aziendali, che gli indirizzi IP vengano condivisi da tutti i computer, per esempio, di un ufficio. Questa scarsità è in via di soluzione con l'adozione dell'indirizzamento IPv6.

CRITTOGRAFIA

RISERVATEZZA IN UNA RETE PUBBLICA

Una lettera può essere aperta, letta e chiusa senza lasciare traccia. Una telefonata può essere intercettata. Come può un utente inviare un messaggio sensibile in modo che rimanga al riparo da occhi indiscreti?

Grazie alle tecnologie informatiche nel ventesimo secolo abbiamo assistito a una rapida evoluzione della crittografia. I computer hanno reso possibile non solo la cifratura rapida dei messaggi elettronici, ma anche la violazione molto più rapida delle chiavi di cifratura usate finora.

Va detto che la crittografia non è una soluzione infallibile e non garantisce una completa riservatezza. Una tecnica frequente per aggirare la crittografia è catturare il messaggio prima ancora che venga cifrato – per esempio, ad opera di un programma installato di nascosto sul computer (o sul telefono cellulare) dell'utente, programma che registra quali tasti vengano premuti sulla tastiera (i cosiddetti programmi "cavallo di Troia registra-tasti", o in inglese "Trojan keylogger").

Un altro elemento al quale bisogna porre attenzione cifrando un messaggio è la sua integrità (cioè la completezza del file), altrimenti il messaggio può essere manipolato anche senza conoscere la chiave di cifratura. I migliori strumenti crittografici verificano automaticamente l'integrità dei file cifrati.

L'immagine qui sopra mostra le fasi di una importante tecnica di crittografia chiamata crittografia a chiave pubblica ('public key encryption'), che funziona sulla base di una coppia di chiavi, una pubblica e una privata:

1. Il mittente richiede una copia della chiave pubblica del destinatario;

2. Usando un software appropriato, il mittente cifra il messaggio usando la chiave pubblica del destinatario;

3. Il messaggio viene inviato;

4. Il destinatario decifra il messaggio usando sia la sua chiave pubblica sia quella privata.

IL DOMAIN NAME SYSTEM (DNS)

L'ELENCO TELEFONICO DI INTERNET

Un sito web su Internet è raggiungibile tramite l'indirizzo IP numerico del server che lo ospita (nel momento in cui scriviamo, per esempio, l'indirizzo di EDRi.org è 217.72.179.7). Gli indirizzi IP non sono facili da ricordare per gli esseri umani. Usarli per identificare risorse online, inoltre, non è pratico, dato che i servizi su Internet devono di tanto in tanto migrare su un nuovo indirizzo IP (se cambiano Internet Service Provider, per esempio).

Dato che l'uso di indirizzi IP per siti web non è né pratico né 'user friendly', sono stati creati i 'domain names' (cioè i nomi a dominio, come edri.org). Il Domain Name System globale funziona un po' come una rubrica telefonica per Internet.

Se conoscete il nome a dominio del sito web che volete visitare, il Domain Name System è utilizzato – in modo invisibile e automatico – per reperire l'indirizzo IP corrispondente al web server presso cui si trova il sito. Perciò, quando digitate http://edri.org, il vostro computer è in grado di identificarlo come se fosse 217.72.179.7 e invia una richiesta specifica per quel sito.

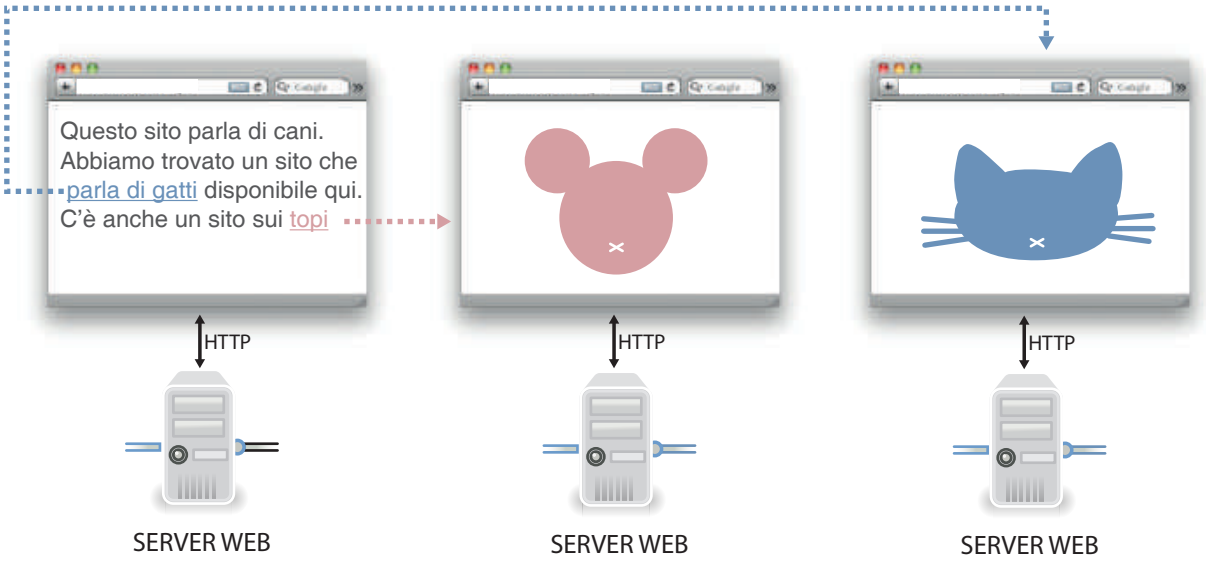
Il sistema per cercare un nome a dominio funziona in maniera gerarchica. Quando digitate http://edri.org, il vostro computer innanzitutto si connette a un server DNS per chiederne l'indirizzo.[3] Il server DNS predefinito di norma è gestito dal vostro Internet provider, ma è possibile utilizzarne uno diverso.

Se qualcuno ha effettuato l'accesso di recente a http://edri.org, il server DNS ne 'ricorderà' i dettagli e vi fornirà l'indirizzo IP corretto. In caso contrario, affiderà la richiesta a un livello più alto di autorità, dove viene seguita la stessa procedura. Al massimo livello di autorità ci sono 13 'root server' che in sostanza mettono insieme i server DNS. I 13 root server sono molto solidi e hanno un'enorme potenza di calcolo. Ne hanno talmente tanta che hanno continuato a funzionare in modo efficiente perfino quando sono stati vittima di attacchi imponenti (i cosiddetti attacchi 'distributed denial of service').

3 Se il vostro computer ha effettuato un accesso a http://edri.org di recente, allora è già a conoscenza dell'indirizzo e non ha bisogno di verificarlo con il service provider.

IL WORLD WIDE WEB

CONNETTENDO LA SOCIETÀ DELL'INFORMAZIONE



Il World Wide Web si basa sull'HTTP, un protocollo (un linguaggio di comunicazione), relativamente giovane, che a sua volta si basa sul protocollo IP. HTTP è l'acronimo del HyperText Transfert Protocol (protocollo di trasferimento dell'ipertesto), ed è stato creato per scaricare i documenti ipertestuali (cioè le pagine web) e per spedire alcune informazioni essenziali al server.

Le pagine Web possono essere create utilizzando il linguaggio HTML – HyperText Markup Language (linguaggio di marcatura dell'ipertesto). Le regole di questo linguaggio sono stabilite dal World Wide Web Consortium (W3C), e specificano marcatori speciali che indicano le proprietà tipografiche e di impaginazione del testo. Per esempio, il carattere in grassetto sarà preceduto dal segno **e sarà seguito dal segno** .

Queste specifiche tecniche hanno subito delle evoluzioni nel tempo (una delle ultime versioni è il linguaggio HTML5), perché il processo di sviluppo del linguaggio HTML è continuo nonché aperto alla partecipazione di tutti. Una volta che lo standard è stato definito, il suo uso non è soggetto ad alcuna licenza o pagamento di royalties. Il vantaggio è che tutti i computer leggono le istruzioni scritte nel linguaggio HTLM esattamente allo stesso modo, quindi chiunque può usarlo, gratis, ed essere certo che ogni apparecchio visualizzerà la pagina Web nello stesso modo. Il Web (e tutto sommato anche il mondo) sarebbe molto più povero se le persone dovessero pagare per scrivere le pagine nei linguaggi richiesti da tutti i diversi tipi di computer.

Tali caratteristiche di apertura e libertà del linguaggio HTML sono essenziali al fine di assicurare la compatibilità di tutte le pagine Web per ogni tipo di apparecchio: computer fissi, telefoni cellulari, lettori digitali, computer

portatili ed ogni altro dispositivo. La corretta applicazione delle specifiche del linguaggio HTML per il formato delle pagine Web assicura anche la libertà di accesso a tutte le persone che hanno difficoltà visive, altrimenti i sistemi di lettura dei testi non sarebbero in grado di comprendere le pagine alle quali gli utenti accedono.

Le pagine Web sono pubblicate su macchine note come Web server. Un web server è un computer che può essere individuato attraverso il suo specifico indirizzo IP (come abbiamo spiegato a pagina 5). Normalmente molti nomi a dominio (come ad esempio www.edri.org e www.bitsoffreedom.nl) possono trovarsi allo stesso indirizzo IP perché sono ospitati ("hosted") dallo stesso server. Per questo un singolo Web server con un unico indirizzo IP può ospitare numerosi siti Web. Nel caso delle società commerciali che vendono spazio ad altri siti web, sullo stesso server vengono ospitati centinaia di siti web, che non hanno alcuna relazione fra loro. Per questo eventuali tentativi di bloccare singoli siti Web in base al loro indirizzo IP hanno sempre avuto conseguenze disastrose anche per le altre pagine ospitate sullo stesso server.

Il protocollo HTTP ha una variante sicura, chiamata HTTPS. HTTP non è cifrato: di conseguenza chiunque abbia accesso ai cavi della rete o a una delle connessioni che collegano il computer dell'utente al server web può accedere a tutte le informazioni che l'utente invia al server e viceversa.

HTTPS invece cifra queste connessioni in modo che (teoricamente) solo gli utenti e il server web possono decifrare le informazioni che si scambiano. Tutto ciò è basato sulla fiducia: colui che pubblica le pagine Web chiede a un'autorità affidabile di dargli un certificato strettamente personale, una sorta di firma digitale che identifica colui che pubblica; un meccanismo simile al sigillo in ceralacca che nei secoli passati era utilizzato per chiudere i documenti.

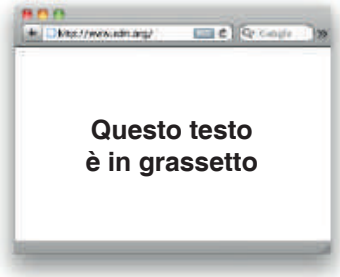
Quando un utilizzatore acquista un nuovo computer o installa un nuovo browser Web, questo contiene una lista di autorità di certificazione affidabili, cioè il riferimento ad enti il cui mestiere consiste nell'emettere certificati di sicurezza. Il computer dell'utente, collegandosi a siti web il cui certificato è stato rilasciato da uno degli enti menzionati, segnalerà all'utente che la connessione è sicura. La fragilità di questo sistema deriva da questa lista che contiene dozzine di enti. Se uno di questi enti diventa inaffidabile, i servizi che certificava diventano insicuri ma gli utenti non se ne accorgono.

LINGUAGGIO SVILUPPATO DAL WORLD WIDE WEB CONSORTIUM

W3C®

Questo testo è in grassetto

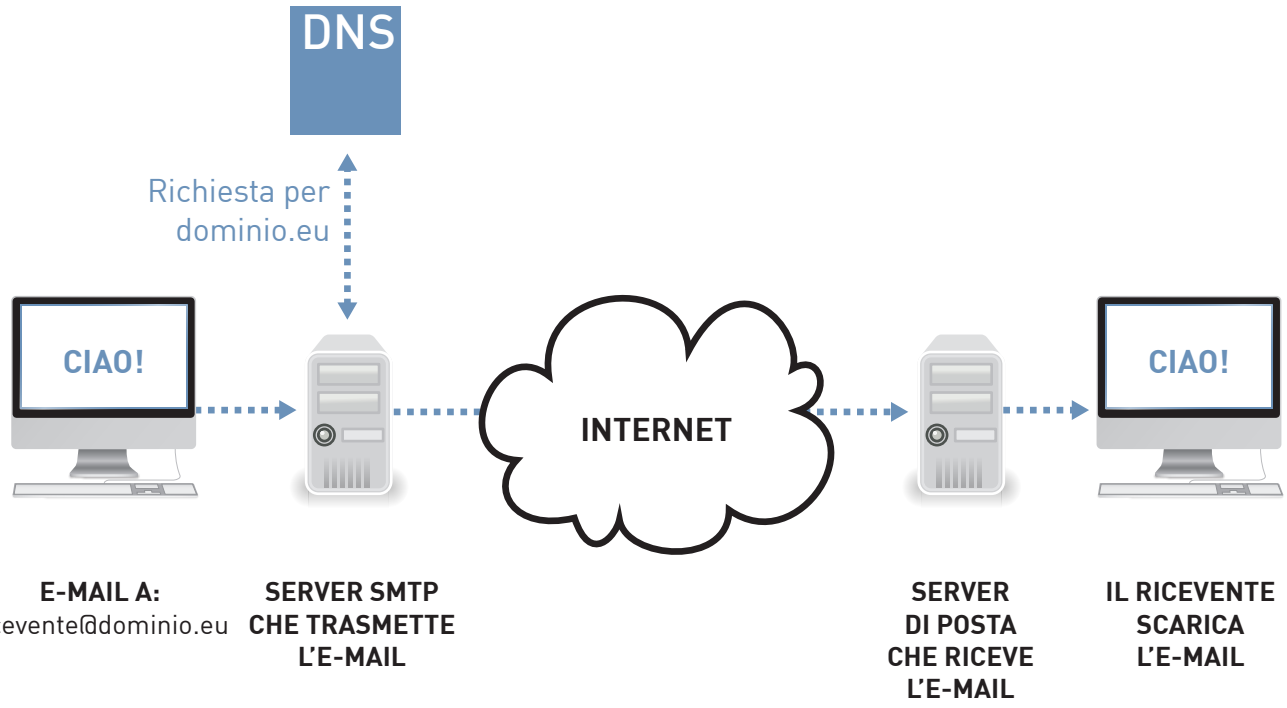
COSA SCRIVE UN PROGRAMMATORE



COSA VEDI COL BROWSER

L'E-MAIL E LA SICUREZZA

LA POSTA NEL MONDO DIGITALE



I messaggi di posta elettronica, o e-mail, sono messaggi inviati da un mittente a uno o più destinatari. L'invio di questi messaggi è gestito tramite il protocollo SMTP (Simple Mail Transfer Protocol - Protocollo semplice di invio della posta) che, come l'HTTP, è anch'esso basato sul protocollo IP.

Dopo aver composto una e-mail mediante un sito webmail o un programma di posta elettronica, essa è trasferita a un server SMTP in uscita. Viene poi trasferita da un server e-mail all'altro, sempre usando SMTP, fino a che non raggiunge il server di destinazione finale.

I server e-mail ricavano le informazioni necessarie all'invio interrogando le informazioni del Domain Name System (DNS) descritto a pagina 7. Il DNS contiene anche le informazioni relative a quali server siano deputati alla gestione delle e-mail per ogni dominio. Il dominio può essere ricavato dalla porzione dell'e-mail del destinatario successiva al segno @.

Dopo che il messaggio arriva al server e-mail che gestisce tutte le e-mail del destinatario, vi rimane fintanto che quest'ultimo non lo cancelli. Alcuni programmi di posta eseguono quest'operazione automaticamente una volta che l'utente ha scaricato la posta dal proprio PC o smartphone.

Sicurezza delle e-mail Le e-mail possono essere intercettate da terzi quando transitano da un server all'altro. Ci sono due modi per evitare che

ciò succeda: rendere sicura la comunicazione tra i server e-mail, oppure cifrare il contenuto delle stesse e-mail. La comunicazione tra server e-mail può essere resa sicura nello stesso modo in cui il protocollo HTTPS rende sicure le comunicazioni HTTP (nel modo descritto in precedenza).

Nel caso dell'e-mail vi è però una debolezza, in quanto il nostro computer non comunica direttamente con il server di destinazione finale. Ciò comporta il fatto che se anche uno solo dei server e-mail intermedi non usa la cifratura per inoltrare il messaggio, esso può essere intercettato durante questa fase del transito.

A causa di questa vulnerabilità, è preferibile cifrare il messaggio stesso. Per cifrare le e-mail si può usare un sistema diffuso e liberamente disponibile, quale ad esempio PGP (Pretty Good Privacy), anche disponibile come OpenPGP e GPG.

DEEP PACKET INSPECTION

SBIRCIANDO NEL VOSTRO TRAFFICO INTERNET

I dati su Internet sono trasmessi in "pacchetti", ovvero piccoli blocchi di dati. Ogni pacchetto ha un'intestazione che descrive la sua origine e la sua destinazione (è come una busta su cui siano scritti gli indirizzi del mittente e del destinatario). Tali informazioni permettono alle apparecchiature di rete di determinare il miglior percorso per trasmettere un pacchetto in un dato momento.

Storicamente le apparecchiature di rete si limitavano a esaminare solamente le informazioni di origine e destinazione. Tuttavia, con il rapido incremento di attività malevole, i gestori delle reti hanno deciso di dover esaminare un maggior numero di dettagli di ogni pacchetto per distinguere i pacchetti "sicuri" da pacchetti generati da intrusioni informatiche o da attacchi finalizzati a bloccare un servizio (noti in inglese come "denial of service attacks").

Ad esempio, i programmi per la sicurezza di rete [firewalls] inizialmente bloccavano solamente pacchetti che partivano da un'origine specifica ed erano indirizzati verso una destinazione specifica e uno specifico servizio. Usando tali criteri si possono bloccare tutte le richieste di servizi verso la rete di un'azienda provenienti dall'esterno, perché, per esempio, non si vogliono rendere disponibili al pubblico i propri servizi (per esempio, non si vuole che un estraneo stampi sulle nostre stampanti di rete). Allo stesso tempo, non bloccando le richieste di servizi originati dalla rete della propria azienda, si possono tranquillamente fruire di tutti i servizi disponibili su Internet.

Ad un certo punto si potrebbe decidere di attivare un server web sulla propria rete per pubblicare dei documenti. In tal caso sarebbe necessario modificare le impostazioni del proprio firewall per permettere l'accesso a richieste provenienti dall'esterno e dirette al servizio web. Tuttavia, ci sono numerosi attacchi contro server web che appaiono inoffensivi dal punto di vista degli algoritmi usati dal firewall. In altre parole, è impossibile distinguere tra pacchetti legittimi e pacchetti dannosi basandosi unicamente sui dettagli di origine e destinazione.

Gli ingegneri di rete hanno compreso velocemente che sarebbe stato più semplice individuare gli attacchi se le apparecchiature di rete avessero esaminato un po' più in profondità i pacchetti. In teoria, tale operazione è tecnicamente semplice - le intestazioni di un pacchetto non sono separate dal pacchetto se non in base a una definizione logica dei confini delle intestazioni. Si tratta solamente di analizzare pochi altri bytes rispetto a quelli che vengono normalmente analizzati, ad esempio per effettuare l'instradamento. Oppure andare ancora più in fondo e guardare l'intero contenuto

del pacchetto.

I dispositivi predisposti a fare ciò sono stati inizialmente chiamati "Sistemi di prevenzione delle intrusioni" (Intrusion Prevention Systems, IPS). Successivamente tali caratteristiche sono state introdotte nella maggior parte dei dispositivi di rete. Quando questi dispositivi venivano usati solo per bloccare attacchi informatici, ciò non causava controversie.

Tuttavia, nel corso del tempo, i governi, i fornitori di contenuti e gli operatori di rete hanno iniziato a rendersi conto che la tecnica - generalmente denominata Deep Packet Inspection (DPI) - offre loro un controllo ben maggiore sui contenuti trasmessi tramite Internet rispetto a prima.

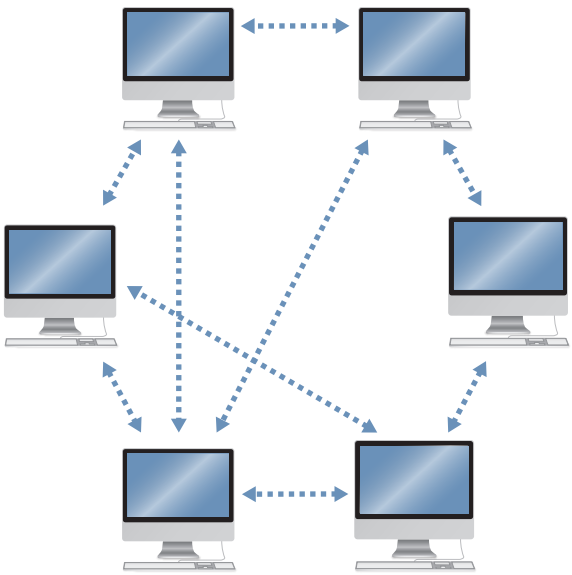
Le tecniche di Deep Packet Inspection sono già in uso per fini di giustizia (sorveglianza, blocco, ecc.), profilazione per fini di marketing, pubblicità mirata, per far rispettare livelli contrattuali di servizio, e vengono proposte come mezzo per la tutela dei diritti d'autore.

Tuttavia la DPI può costituire una pratica lesiva di diritti fondamentali quali la riservatezza ed inviolabilità delle comunicazioni e la protezione dei dati personali.

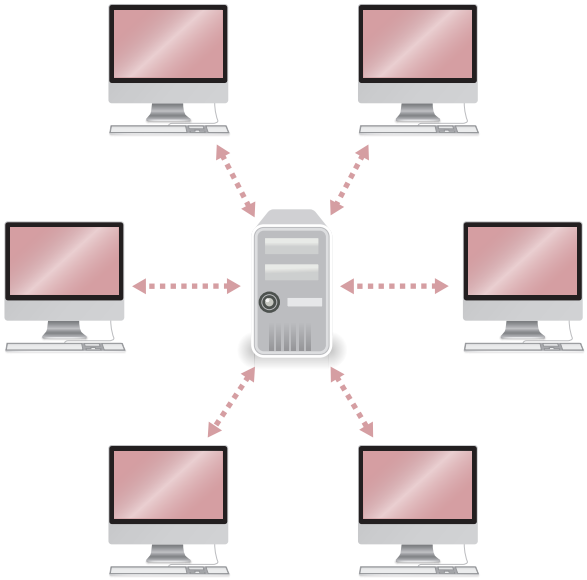
Dal punto di vista dell'utente, le tecniche di Deep Packet Inspection possono essere contrastate usando la crittografia: il contenuto "profondo" di un pacchetto crittografato, infatti, è totalmente opaco per l'operatore.

PEER-TO-PEER

DA ME A TE, CON NESSUNO IN MEZZO



PEER-TO-PEER
SISTEMA DI NODI SENZA INFRASTRUTTURA CENTRALIZZATA



CENTRALIZZATO
MODELLO DI SERVIZIO BASATO SU SERVER (NON PEER-TO-PEER)

Le reti peer-to-peer sono costituite da dispositivi (web server o computer di utenti) che comunicano su un piano paritario. Ogni "peer" (ossia ogni dispositivo) può comunicare con gli altri "peer" e non sussiste alcuna distinzione tra produttori e consumatori, client e server, ecc. Si tratta semplicemente di un certo numero di dispositivi che comunicano con altri dispositivi.

Questo modello si differenzia da quello client-server o uno-a-molti, nel quale un computer soddisfa le richieste di numerosi client - per esempio un sito web che fornisca contenuti rivolti a molti utenti (un dispositivo che comunica con molti dispositivi).

Su Internet le applicazioni peer-to-peer utilizzano protocolli peer-to-peer che sono basati - come è inevitabile che sia - sul protocollo IP.

Le reti peer-to-peer presentano un numero di particolari vantaggi:

- Non presentano i problemi legati al "punto singolo di fallimento" ("single point of failure") in quanto non ci sono entità centralizzate. In una rete uno-a-molti, se il dispositivo "uno" presenta

un problema, viene di conseguenza influenzato l'intero sistema. In una rete basata sul modello molti-a-molti, anche nel caso in cui si verificasse un guasto ad uno dei dispositivi, ciò produrrebbe un danno minimo da un punto di vista generale;

- Queste reti possono crescere agevolmente, in quanto ogni partecipante che si aggiunge porta anche risorse addizionali (capacità di traffico, memoria, potenza di calcolo) alla rete stessa;

- Non c'è nessun amministratore perché non c'è un'autorità centrale;

- I guasti hanno un impatto minimo perché non ci sono risorse centralizzate e c'è un livello di duplicazione delle risorse intrinsecamente elevato;

- Garantiscono libertà agli utenti. Non solo i dispositivi che partecipano si trovano su un piano di uguaglianza, ma anche gli stessi utenti lo sono.

Uno dei compiti importanti di un'applicazione peer-to-peer è di organizzare e individuare le risorse nella rete.

In una certa misura, i server di posta elettronica rappresentano un primo esempio di applicazioni peer-to-peer. Usando il protocollo SMTP, qualsiasi server può inviare un'email a qualsiasi altro server. Il DNS (Domain Name System) può anche elencare molteplici server in grado di gestire e-mail in entrata per un determinato dominio, aumentando l'affidabilità del sistema.

Gli utenti "peer" in una rete di condivisione file non conoscono immediatamente l'indirizzo IP degli altri utenti che partecipano alla rete e non sanno quali utenti hanno quali file (o parte di essi). Questo è tipicamente gestito mediante un processo nel quale gli utenti condividono informazioni riguardo ai contenuti di cui dispongono altri utenti. I file sono identificati usando chiavi "hash", le quali sono fondamentalmente impronte digitali che permettono a singoli file di essere identificati in modo inequivocabile. I DHT (Distributed Hash Tables) permetto ai "peer" di scoprire quali utenti mettono a disposizione una parte o la totalità di un determinato file.

Gli utenti di reti peer-to-peer hanno bisogno di un modo per ottenere le impronte "hash" dei file desiderati. Alcune di esse sono pubblicate su siti web, ad esempio quelli per scaricare versioni del sistema operativo Ubuntu. Ci sono dizionari che mappano le descrizioni leggibili dei file in impronte "hash", in modo da rendere possibile la ricerca di file in reti peer-to-peer.

Siti web quali thepiratebay.org e mininova.org mettono a disposizione questi dizionari. In ogni caso, queste impronte digitali possono essere distribuite anche tramite e-mail, chat e per mezzo dei social network - ovvero, non esiste alcun sistema centralizzato.

Esistono anche reti peer-to-peer che garantiscono l'anonimato degli utenti che vi partecipano.

PUBBLICITÀ COMPORTAMENTALE

PERSONALIZZANDO

La pubblicità comportamentale (in gergo anche "targeting comportamentale") è una tecnica che si basa sul tracciamento delle attività degli utenti su Internet. È utilizzata per costruire profili di utenti Internet, in modo da veicolare messaggi pubblicitari che, se il profilo è corretto, saranno per loro più rilevanti, e quindi più efficaci.

La pubblicità comportamentale sfrutta un principio facile da comprendere: se un utente visita un sito web dedicato, ad esempio, al calcio, il browser web (ad esempio Internet Explorer, Firefox o Chrome) memorizzerà sul computer un piccolo file, detto "cookie". Un sito web è di regola composto da contenuti provenienti da diverse fonti. Ad esempio, il testo e le immagini possono provenire dal sito digitato nel browser dell'utente, mentre altri contenuti aggiuntivi, come i messaggi pubblicitari, sono scaricati da altri indirizzi (addirittura da sorgenti senza legami con il sito web). Ogni volta che un contenuto viene scaricato, la richiesta al server può includere anche dati contenuti nei cookie ospitati sul computer dell'utente.

Per i fini della pubblicità comportamentale, i cookie contengono, di regola, un numero di identificazione. Se successivamente l'utente legge un articolo sulle automobili, le società pubblicitarie saranno in grado di fare ipotesi su chi legge articoli sia sulle auto sia sul calcio. Nel nostro esempio, un'ipotesi semplice potrebbe essere che l'utente sia qualcuno di potenzialmente sensibile a pubblicità di birra.

La pubblicità comportamentale è concepita anche per non presentare ad un utente pubblicità non pertinenti rispetto al suo profilo di consumatore.

Quanti più siti che fanno parte della stessa rete di tracciamento utilizzata per i servizi di pubblicità comportamentale (come gran parte dei siti web dei giornali e molti altri) vengono visitati dall'utente, tanti più dati relativi al suo profilo vengono raccolti. Analizzando in un arco di tempo relativamente breve le abitudini online di una persona è possibile sviluppare un profilo molto dettagliato – e "l'identificabilità" dei dati aumenta, anche se in teoria sono dati anonimi.

Grandi quantità di dati relativi ai comportamenti online possono ridurre la dimensione del gruppo di persone al quale appartiene un utente, fino ad arrivare a un numero molto esiguo di individui che possano corrispondere al suo profilo. Molti anni fa, il gestore di un motore di ricerca ha pubblicato una grande quantità di dati "anonimi" relativi alle ricerche fatte. Il risultato è stato che, analizzando tali dati "anonimi", alcuni giornalisti sono stati in grado di identificare persone specifiche, dimostrando che i dati "anonimi" alla

fine anonimi non sono.

Non è dato sapere se dati aggiuntivi, provenienti da altre fonti, vengano utilizzati per i servizi di pubblicità comportamentale. Molte società attive nel settore del targeting comportamentale, come Google e Yahoo!, forniscono anche altri servizi online, oltre alla ricerca. L'aggregazione di dati provenienti da diverse fonti rende possibile l'identificazione di singoli individui.

Si sostiene che la pubblicità comportamentale sia uno dei fattori di sviluppo dei successi economici dell'industria della pubblicità online negli ultimi anni. La tecnica è utilizzata su base sperimentale anche per fornire altri contenuti agli utenti di Internet, come ad esempio le notizie.

I fornitori di servizi ed i pubblicitari argomentano che tale tipo di tracciamento è essenziale ed è di fatto svolto nell'interesse dell'utente, in quanto permette loro di offrire molti servizi gratuiti e di proporre unicamente messaggi pubblicitari rilevanti e mirati. Coscienti peraltro dei problemi di privacy, sostengono l'adozione di procedure di "opt-out" secondo cui la profilazione per scopi legittimi è ammissibile a meno che l'utente non abbia esplicitamente dichiarato di opporsi.

A seguito della modifica apportata alle direttive europee sulla privacy nel 2009, che richiede per alcuni tipi di cookies il consenso preventivo dell'utente, tale procedura di opt-out rischia però di esser insufficiente e non aderente al dettato normativo.

Per contro, la richiesta di un consenso informato preventivo per l'utilizzo di ogni singolo cookies potrebbe rendere pressoché impossibile la navigazione.

Una soluzione di compromesso, adottata in alcuni stati membri dell'Unione e ipotizzata nella stessa normativa europea, potrebbe essere individuata nel consenso dell'utente espresso preventivamente mediante le impostazioni del browser o l'uso di applicativi quali "do not track".

Rimane il problema che molti utenti di Internet non sanno dell'esistenza dei cookies, né tantomeno cambiano le impostazioni dei loro browser.

Inoltre, i browser moderni e le loro estensioni (i cosiddetti plug-in, come ad esempio Flash) offrono molti altri modi per salvare e richiamare dati, che si aggiungono ai cookies tradizionali. Tali dati aggiuntivi sono difficilmente gestibili dall'utente medio e non sono sempre contemplati nelle preferenze dei browser relative ai cookies.

A tutt'oggi, il rapporto tra la tutela dei dati personali e la pubblicità comportamentale deve in rete ancora trovare il giusto equilibrio: molti stati membri dell'Unione Europea, tra cui l'Italia, non hanno infatti ancora recepito le modifiche alle direttive privacy in tema di cookies e molte sono le questioni tecniche e giuridiche aperte.

I MOTORI DI RICERCA

UN INDICE DI INTERNET

La navigazione sul World Wide Web avviene attraverso hyperlink (testi o immagini che, una volta cliccati, aprono altri siti o risorse).

Ogni utente può creare dei link che indirizzano a contenuti presenti sul web. Attraverso l'attività di linking, gli utenti di Internet contribuiscono all'organizzazione delle informazioni on-line in una rete di risorse connesse tra loro.

È importante sottolineare che non esiste un indice ufficiale di tutti i contenuti disponibili in rete: i motori di ricerca forniscono quindi un servizio essenziale, permettendo agli utenti di navigare su Internet in modo più efficiente.

Ci sono diversi tipi di motori di ricerca. Il più importante è il motore di ricerca detto "crawler based".

Questo tipo di motore di ricerca utilizza dei programmi (detti "crawlers" o "spiders" ovvero "striscianti" o "ragni") per ricercare le informazioni disponibili in rete, indicizzandole in modo sistematico. La complessità e l'efficienza del crawler influenza le dimensioni e il livello di aggiornamento dell'indice, entrambi elementi fondamentali per la qualità del servizio offerto da un motore di ricerca. Semplificando, lo spider/crawler segue i link contenuti su una pagina e indicizza le pagine alle quali questi link fanno riferimento, poi segue i link contenuti su queste ultime e nuovamente indicizza le pagine "linkate", e avanti così di seguito.

L'attività più importante dei motori di ricerca è stabilire una relazione tra la ricerca dell'utente e le informazioni contenute nell'indice. Il risultato di questa attività è solitamente una lista di riferimenti presentati sotto forma di classifica. In particolare, i riferimenti sono costituiti da titoli, informazioni sommarie e hyperlink che il motore di ricerca ritiene rilevanti.

A fianco dei 'risultati naturali' (i risultati selezionati dal motore di ricerca) i motori di ricerca commerciali fanno comparire risultati sponsorizzati scelti in base a un'asta di parole chiave precedentemente svolta tra diversi soggetti interessati a promuovere la propria attività. Il procedimento attraverso cui vengono individuati i risultati naturali è particolarmente complesso e i motori di ricerca commerciali proteggono come segreti industriali gli algoritmi in base ai quali individuano tali risultati. L'algoritmo PageRank di Google è uno degli algoritmi di ricerca Web più famosi. PageRank stabilisce la rilevanza dei siti presenti all'interno dell'indice sulla base della struttura dei link che vi fanno riferimento (per esempio, tenendo conto della tipologia di siti che puntano a una determinata pagina).

Altre tecniche importanti per combinare in modo efficiente le richieste degli utenti con le informazioni contenute nell'indice sono l'analisi del contenuto dei siti e l'analisi dei dati dell'utente. A quest'ultimo riguardo, i motori

di ricerca commerciali utilizzano i cookies per memorizzare le ricerche degli utenti, i link di preferenza e altri tipi di informazioni in sezioni personalizzate dei loro database, anche per un lungo periodo di tempo.

Un motore di ricerca "verticale" o "specializzato" è un servizio dedicato alla ricerca di informazioni su un determinato argomento come i viaggi, lo shopping, gli articoli accademici, le notizie o la musica. I grandi motori di ricerca "crawler based" possono fornire, come servizio aggiuntivo, anche motori di ricerca specializzati. Un "meta motore di ricerca" è un motore di ricerca che non dispone di un proprio indice e non fornisce risultati propri, ma usa i risultati di uno o più motori di ricerca diversi. Una "directory" è un insieme di link classificati in diverse categorie. Esempi celebri sono la directory Yahoo! e l'Open Directory Project.

CLOUD COMPUTING

INTERNET DIVENTA IL TUO COMPUTER

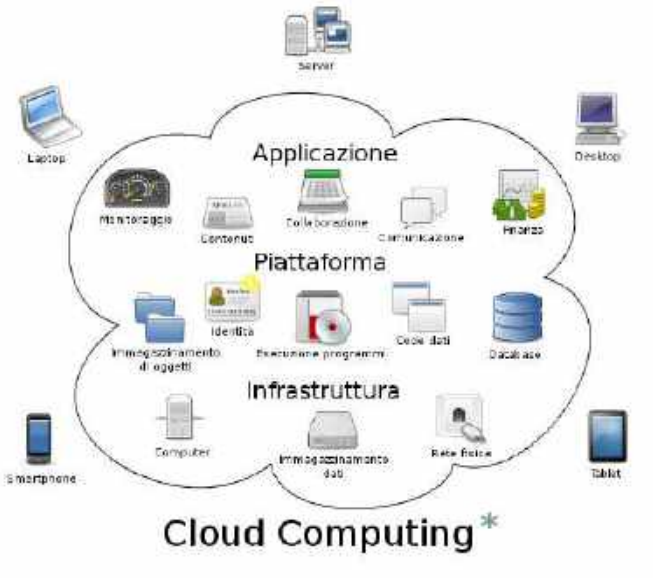
"Cloud computing" è diventato di recente un neologismo alla moda ad uso del marketing. Il concetto, di per sé, è tutt'altro che nuovo, sebbene il numero di applicazioni realizzate secondo questo paradigma stia crescendo enormemente.

Nei diagrammi che descrivono le reti di comunicazione, la nuvola ("cloud") viene usata per rappresentare la rete che sta al di fuori della rete di un utente. Cloud computing si riferisce dunque a qualsiasi servizio di elaborazione realizzato nella rete invece che all'interno del computer dell'utilizzatore.

Uno dei primi esempi di cloud computing è la versione web dell'e-mail ("webmail"). Gli utenti di una webmail possono accedere alla loro casella di posta elettronica da qualsiasi dispositivo collegato a Internet, piuttosto che da un apparecchio soltanto. I servizi di webmail più noti e usati includono Yahoo! Mail, Hotmail e Gmail.

Con il costante aumento della velocità delle connessioni a Internet, la gamma di servizi che possono essere offerti via cloud computing è molto cresciuta negli ultimi anni. Oggi, ad esempio, è possibile conservare considerevoli quantità di dati nella "cloud" facendo uso di hard disk virtuali, come quello fornito da Microsoft Live o Dropbox.

Analogamente suite per ufficio, ad esempio per la videoscrittura, e strumenti per la gestione dei database, vengono offerti online in misura



crescente.

Il progetto di sistema operativo sviluppato da Google (Google Chrome OS) è un ulteriore passo nella transizione verso sistemi di elaborazione in cloud (o "cloud-based computing"). Utilizzando il browser Google Chrome come base, il sistema operativo mira a incorporare in via automatica tecnologie cloud, così da rendere minima la quantità di software utilizzata nel proprio computer, con un forte affidamento ai servizi disponibili online - secondo un approccio che, per molti versi, è opposto a quello dell'elaborazione tradizionale, che prevede un utilizzo di software installati nel proprio computer preponderante rispetto al ridotto (o assente) utilizzo di software nella cloud.

* Immagine originale di Sam Johnston: http://commons.wikimedia.org/wiki/File:Cloud_computing.svg?uselang=de

SOCIAL MEDIA

DOVE CI INCONTRIAMO

I social media sono applicazioni Internet che consentono la creazione e lo scambio di contenuti generati dagli utenti (c.d. "User Generated Content").

I social media si differenziano dai mezzi di comunicazione ordinari poiché non si limitano a trasmettere informazioni, ma consentono all'utente di interagire con le informazioni stesse. L'interazione può consistere semplicemente nella possibilità di lasciare commenti, di votare per un articolo o di esprimere il proprio apprezzamento per una qualsiasi azione di altri utenti (il ben noto "mi piace"). Ogni utente dunque non è più un semplice spettatore, ma diventa parte del mezzo, poiché altri utenti possono leggere i suoi commenti o recensioni.

Oggi gli utenti si stanno abituando ad avere la possibilità di reagire alle informazioni ricevute e a esprimere il proprio punto di vista. Ciò incrementa la partecipazione collettiva ai dibattiti in corso. Il numero di utenti dei social media è in continua crescita, e di conseguenza cresce anche la loro forza e influenza.

Qualsiasi sito web che invita i visitatori ad interagire col sito e con gli altri visitatori può essere considerato un "social media". Questi ultimi possono essere divisi a grandi linee in sei diverse tipologie:

1. Progetti collaborativi (es. Wikipedia), nei quali gli utenti interagiscono aggiungendo articoli e modificando testi esistenti;

2. Blog e microblog (es. Twitter);

3. Aggregatori di contenuti (es. YouTube, Flickr), nei quali gli utilizzatori interagiscono condividendo e commentando foto e video;

4. Reti sociali (es. Facebook, Myspace, Hi5, Google+), nelle quali gli utenti interagiscono aggiungendo amici, commentando i profili di altri utenti, aggregandosi in gruppi e partecipando a discussioni e scambi di opinioni;

5. Giochi di ruolo virtuali (es. World of Warcraft);

6. Realtà sociali virtuali (es. Second Life).

Un aspetto importante e delicato quando si parla di social media è la tutela degli utenti - in particolare la tutela del diritto alla riservatezza (privacy). Difatti, sebbene gli utenti possano in genere scegliere quali informazioni personali condividere o nascondere, le impostazioni di base e le ulteriori forme di tutela per i bambini sono oggetto di molte controversie. In aggiunta, alcuni siti, come Facebook, hanno già in più occasioni modificato unilateralmente le impostazioni sulla privacy dei propri utenti.

INTERNET GOVERNANCE

DEMOCRAZIA DIGITALE

Il primo tentativo di definire l'espressione "Internet Governance" ebbe luogo durante le riunioni preparatorie del Summit mondiale sulla società dell'informazione (World Summit on Information Society, WSIS) delle Nazioni Unite.

Una prima definizione comunemente accettata fu prodotta dal "Working Group on Internet Governance", un gruppo multi-stakeholder (governi, privati, società civile e comunità tecniche) creato dal Segretario Generale delle Nazioni Unite, definizione poi inclusa nell'Agenda di Tunisi per la società dell'informazione:

"Lo sviluppo e l'applicazione da parte dei governi, del settore privato e della società civile, nei loro rispettivi ruoli, di principi condivisi, standard, regole, procedure decisionali e programmi sui quali si basi l'evoluzione e l'uso di Internet."

Questa definizione sottolinea l'approccio multilaterale alla discussione di politiche relative a Internet che, stante l'impatto sulla comunità, deve avvenire in modo aperto, trasparente e responsabile.

È proprio per raggiungere tale obiettivo che è stato creato l'Internet Governance Forum, un forum multi-stakeholder per la discussione e il confronto di politiche pubbliche relative ad elementi chiave dell'Internet governance. Il forum, che è già arrivato alla sua sesta edizione (dal 2006 al 2011), ha ispirato l'organizzazione di incontri simili a livello nazionale e regionale (e.g. EuroDIG – il dialogo pan-europeo sulla governance di Internet). Nonostante l'importanza di tali luoghi di discussione e confronto, è necessario evidenziare che questi meeting non funzionano come organismi decisionali, ma cionondimeno influenzano le politiche relative a Internet.

Quali temi include l'Internet Governance?

- Infrastrutture e standardizzazione;
- Questioni tecniche relative al funzionamento di Internet: infrastrutture di telecomunicazioni, standard e servizi (es. Internet Protocol, Domain Name System), standard relativi a contenuti e applicazioni (es. HyperText Markup Language);
- Questioni relative alla salvaguardia del funzionamento sicuro e stabile di Internet: cybersecurity, crittografia, spam;
- Questioni giuridiche: legislazione e regolamentazione a livello nazionale e internazionale applicabile a Internet (es. diritto d'autore, privacy e protezione dei dati, criminalità informatica);
- Questioni economiche: e-commerce, tassazione, firma elettronica, pagamenti elettronici;
- Sviluppo: digital divide, accesso universale a

Internet;

- Questioni socio-culturali: diritti umani (libertà di espressione, diritto di cercare, ricevere e fornire informazioni), politiche per l'utilizzo dei contenuti, privacy e protezione dati, multilinguismo e diversità culturali, educazione, tutela dei minori online.

Chi partecipa all'Internet Governance?

- Governi: elaborano e danno attuazione alle politiche e norme pubbliche relative a Internet;

- Settore privato: i fornitori di servizi Internet (ISPs), i gestori della rete, le società che gestiscono l'anagrafe dei nomi a dominio ("registries" in inglese), quelle che forniscono i nomi a dominio a cittadini e imprese ("registrars" in inglese), società di software, società che producono contenuti;

- Società civile: organizzazioni non governative che rappresentano gli utenti Internet;

- Organizzazioni internazionali: l'Unione Internazionale delle Telecomunicazioni (ITU), UNESCO, United Nations Development Programme (UNDP);

- Comunità tecnica: Internet Society (ISOC), Internet Engineering Task Force (IETF), Internet Architecture Board (IAB), Internet Corporation for Assigned Names and Numbers (ICANN).

Per maggiori informazioni:

Jovan Kurbalija, An Introduction to Internet Governance, Diplo Foundation, 2010

EDRI.ORG/PAPERS

Per la versione italiana:

Centro Nexa su Internet & Società
Politecnico di Torino

nexa.polito.it/publications

Il Centro Nexa è un centro di ricerca del Dipartimento di Automatica e Informatica del Politecnico di Torino.

Con il supporto finanziario del Programma per i Diritti Fondamentali e la Cittadinanza dell'Unione Europea (solo per la versione inglese).

BLOCKCHAIN

Unchaining business through the Blockchain.

ENGINEERING

DI COSA PARLIAMO?

AUTORI

Massimo Canducci

Chief Innovation Officer, Engineering

massimo.canducci@eng.it

Massimo Canducci

Con oltre 25 anni di esperienza nei settori dell'Innovazione e della Trasformazione Digitale, in Engineering Massimo guida un team di oltre 200 innovatori per diffondere l'innovazione, raccogliendo le esigenze di tutta l'organizzazione e proponendo attività di innovazione sul mercato.

Mauro Isaja

Research Area Manager

mauro.isaja@eng.it

Mauro Isaja

Dopo aver ricoperto ruoli di primo piano nella progettazione e nella fornitura di soluzioni software di medie e grandi dimensioni per clienti bancari internazionali, dal 2012 Mauro lavora nel dipartimento Ricerca e Sviluppo di Engineering, dove è responsabile dell'area di ricerca su Distributed Ledger & Fintech.

Adriana Carotenuto

Ph.D Student and Business Analyst at Nexen (Engineering Group)

adriana.carotenuto@eng.it

Adriana Carotenuto

Laureata in Economia Aziendale e International Management, Adriana si occupa di ricerca in ambito Blockchain e Digital Banking. Collabora con Engineering all'interno della Divisione Finanza dal 2018. Partecipa a progetti e conferenze di respiro internazionale sul tema della Trasformazione Digitale.

Giuseppe Idone

Innovation Advisor - Engineering

giuseppe.idone@eng.it

Giuseppe Idone

Dopo gli studi in Management dell'Innovazione presso l'Università Bocconi, l'Università di Trento e la Scuola Superiore Sant'Anna, Giuseppe si è specializzato nello studio della radical e open innovation, pubblicando i suoi studi in un libro di management. Oggi in Engineering lavora come Innovation Advisor.

Edward Abbiati

Chief Marketing Officer, Engineering

edward.abbiati@eng.it

Edward Abbiati

Con oltre 24 anni di esperienza nel settore IT, Edward ha ricoperto ruoli di Consulting, Advisory, Sales e Management in varie multinazionali IT, nel Regno Unito, in Australia e in Europa. Edward ha l'incarico strategico di potenziare e sviluppare la value proposition e il Portfolio del Gruppo e dal 2021 ha l'incarico di gestire col suo team la comunicazione del gruppo Engineering.

Umberto Tarantino

CSolution Developer Senior

umberto.tarantino@eng.it

Umberto Tarantino

Con il ruolo di Solution Developer, dal 2015 si occupa in Engineering di sviluppo software front-end in progetti per la Pubblica Amministrazione Centrale. Sin dal 2014 Umberto è anche co-founder del Blockchain Education Network Italia, associazione non-profit dedita alla divulgazione scientifica in materia di Blockchain e criptovalute.

Vincenzo Croce

Senior Researcher, Engineering

vincenzo.croce@eng.it

Vincenzo Croce

Vincenzo coordina un gruppo di ricercatori che lavorano in iniziative inerenti a Multimedia and Digital Contents. Da diversi anni si occupa di Blockchain con sperimentazioni in diversi ambiti, dal Finance all'Energetico, fino ai contenuti digitali per i quali è autore di numerosi articoli scientifici discussi in importanti conferenze internazionali.

Michele Russo

Head of Consultancy & Services at Engineering S.p.A. BlockChain Unit

michele.russo@eng.it

Michele Russo

Da 25 anni nel settore IT Michele ha maturato grande esperienza nello sviluppo e nella gestione di soluzioni Enterprise per alcune tra le maggiori istituzioni finanziarie italiane e su progetti di integrazione di soluzioni informatiche multi-tenant. Oggi è nella Direzione Generale Tecnica, Ricerca e Innovazione di Engineering.

IN BREVE

Nell'attuale era della Trasformazione Digitale, la maggior parte delle tecnologie abilitanti ha già vissuto la sua giusta dose di clamore per poi entrare nella "maggiore età", dove ha trovato applicazioni "mature" impiegandole al meglio.

Più di altre la Blockchain porta su di sé il peso di aspettative enormi sia in termini di applicabilità che in termini di crescita dei ricavi ed efficienza dei costi. A differenza di altre enabling technology, però, questa tecnologia non ha ancora raggiunto la sua maturità.

Come già avvenuto per altre tecnologie di frontiera, infatti, la Blockchain non solo sta lottando per trovare la sua strada, ma ha anche generato opinioni e definizioni diverse.

È comprensibile che le tecnologie "giovani" creino clamore e, allo stesso tempo, confusione, perché nonostante molti settori siano interessati a integrarle nei loro processi aziendali, mancano ancora risposte a domande su un loro utilizzo significativo ed efficace. Man mano che le sperimentazioni procedono, le nuove tecnologie suscitano aspettative che si trasformano rapidamente in hype, ma poi pretese irrealistiche rispetto alle loro applicazioni generano insoddisfazione e disillusione con una conseguente diminuzione delle sperimentazioni. Ed è proprio questo il momento in cui il clamore iniziale diminuisce e vengono gettate le basi per una piena maturità della tecnologia.

La Blockchain sta vivendo proprio questa fase: superato l'hype iniziale, oggi è coinvolta in una sperimentazione meno diffusa ma più focalizzata, che le consentirà di raggiungere la sua piena età adulta.

Come raccontiamo in questo Paper, oggi in molti settori la maggior parte delle applicazioni Blockchain sono ferme a un livello sperimentale. Nello stesso momento, però, si stanno sviluppando velocemente idee nuove su come applicare questa tecnologia e all'interno della vasta comunità Blockchain è in corso un dibattito su quali direzioni potrebbe prendere e quale impatto potrebbe avere sulla società, sull'industria, sul commercio e sui governi.

La Blockchain promette immutabilità, affidabilità, completa trasparenza e sicurezza di transazioni: tutto all'interno di ecosistemi decentralizzati. Questo significa garantire in qualsiasi momento la certezza e l'integrità del dato per tutti quelli che fanno parte di quell'ecosistema. Ed è questa l'idea vincente, perché in un mondo che fa sempre più affidamento sui dati e sulla capacità di operare prendendo decisioni in tempo reale, garantire la sicurezza e l'integrità delle informazioni è fondamentale.

In ogni caso, il dibattito è ancora aperto e ci si chiede se questa tecnologia sarà veramente rivoluzionaria o se invece il suo impatto sarà limitato.

Oggi noi di Engineering ne stiamo esplorando le frontiere, avviando nuovi confronti, workshop, progetti di ricerca. Stiamo inoltre fornendo tecnologie e laboratori per co-progettare, insieme ai nostri clienti, soluzioni di business efficaci.

Siamo convinti infatti che all'orizzonte ci sono molte e interessanti applicazioni aziendali, che puntano sulla Blockchain e che daranno un importante contributo per migliorare il nostro mondo.

Nelle prossime pagine daremo la nostra definizione di Blockchain e spiegheremo come stiamo lavorando con i nostri clienti e partner nella scoperta e nella progettazione di casi d'uso reali. Infine, racconteremo il nostro punto di vista sulla sua evoluzione.

1

COS'È LA BLOCKCHAIN?

BLOCKCHAIN

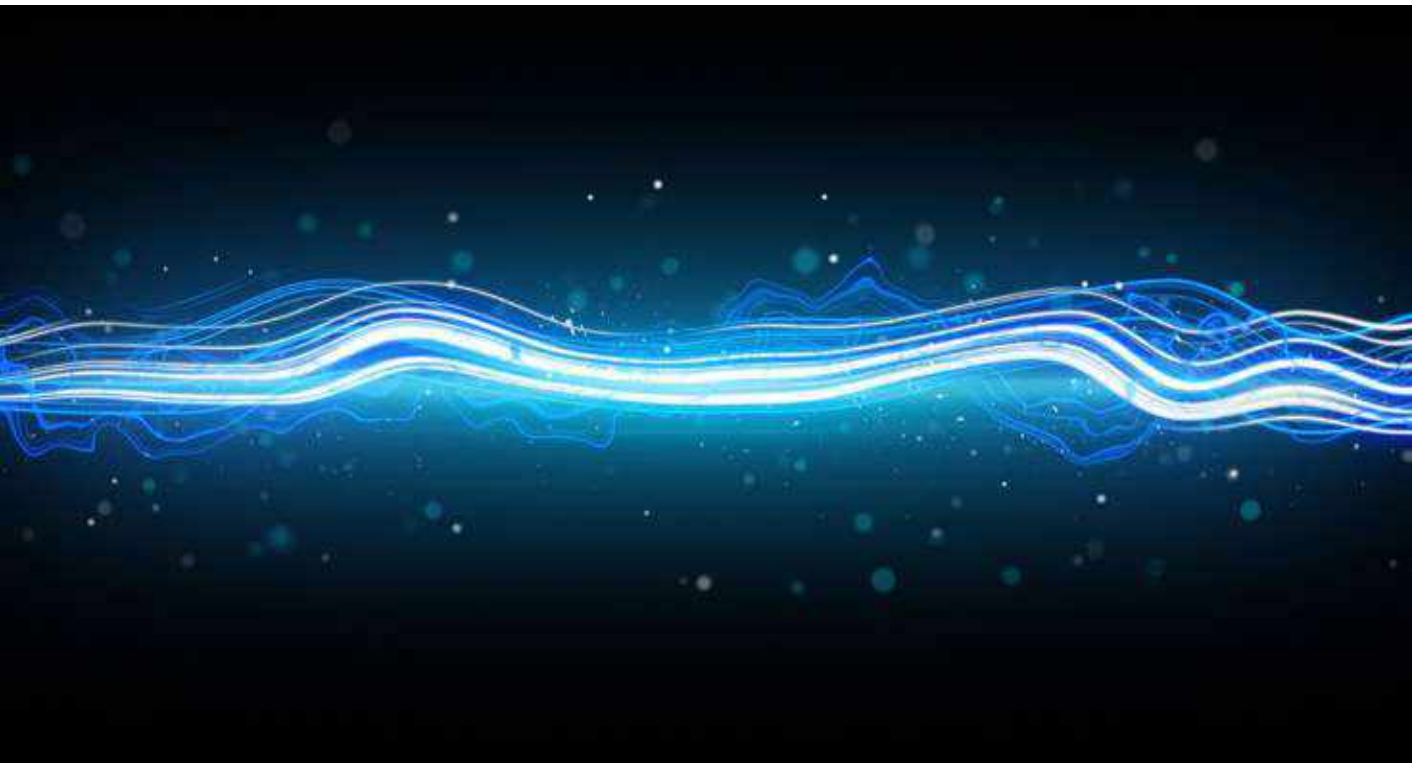
Esistono molte definizioni di Blockchain: alcune derivano da punti di vista diversi, mentre altre, sfruttando il clamore del momento, generano solo confusione. Dal 2014 stiamo svolgendo attività di ricerca su questi temi e, sviluppandoli, abbiamo costruito la nostra visione e definizione di questa tecnologia.

Quindi, cos'è una Blockchain? Da un punto di vista tecnico, è un **registro distribuito, decentralizzato, pubblico (o privato)** di blocchi di transazioni crittografati e irrevocabili, condivisi da tutti i partecipanti ad un ecosistema.

Il motivo dell'interesse per la Blockchain sono le sue caratteristiche di base, che garantiscono la sicurezza, l'integrità e l'immutabilità dei dati, ma anche un certo livello di anonimato, senza terze parti che controllino le transazioni di dati e informazioni. Questo crea interessanti campi di ricerca, stimolando l'esplorazione non solo delle applicazioni di business del nuovo paradigma, ma anche i confini delle sue frontiere tecnologiche.

La Blockchain è una soluzione caratterizzata da database distribuiti, che conservano registri di dati in crescita costante, resistenti ad alterazioni e a revisioni, anche se modificati dagli stessi nodi su cui risiedono, e che a loro volta sono confermati dagli altri nodi che partecipano alla rete.

Una copia dell'elenco dei record è archiviata su tutti i nodi della rete ed è sempre conservata in sicurezza anche in presenza di partecipanti inaffidabili. I record memorizzati in questi database possono essere di due tipi: le transazioni (per esempio i dati effettivi) e i blocchi, registri che annotano l'ordine con cui le transazioni sono state inserite in modo indelebile nel database.



In queste poche linee e concetti si trova un universo di grandi opportunità di business. Per la prima volta nella storia umana, diversi attori aziendali, che agiscono all'interno di un ecosistema complesso, sono in grado di condividere informazioni, valori, contenuti e responsabilità, mentre delegano direttamente alla tecnologia aspetti altamente complessi, come la fiducia, il consenso e l'immutabilità.

Funzionalità molto simili possono essere trovate anche in diverse architetture, che non andremo a considerare come Blockchain, ma che chiameremo Distributed Ledger Technologies (DLT): sono simili alle Blockchain e possono sicuramente essere utilizzate con successo in diverse applicazioni aziendali.

La Blockchain è solo un tipo di DLT: una Distributed Ledger, infatti, non deve necessariamente essere costituita da una sequenza di blocchi, la Blockchain ne rappresenta quindi soltanto un sottoinsieme.
In generale, **la Distributed Ledger Technology può essere definita usando lo stesso concetto di Blockchain**, ma mentre tutte le Blockchain sono Distributed Ledger, non tutte le Distributed Ledger sono Blockchain.

Per chiarire questa distinzione, sottile ma importante, ci affidiamo a uno dei documenti più autorevoli in materia, pubblicato dall'Organizzazione internazionale per la standardizzazione (ISO / CD 23257.2), che afferma: "una piattaforma Blockchain è una piattaforma DLT in cui la tecnologia utilizzata è la Blockchain".

DLT e Blockchain condividono alcune funzionalità di base: sono entrambi registri distribuiti con crittografia a chiave asimmetrica, con un protocollo di consenso per la convalida delle transazioni, basato su una rete P2P per la propagazione dei dati.

Blockchain e Distributed Ledger Technologies (DLT)

	Blockchain	DLT
Definizione	Appartiene alla categoria dei DLT, in cui ogni singolo nodo contiene una copia del Ledger (libro mastro): ogni volta che qualcuno aggiunge una transazione ne crea una copia nuova.	La DLT consiste in un database decentralizzato su più computer o nodi. Ogni nodo contiene il Distributed Ledger e ciascuno di essi è autorizzato ad aggiornare gli altri Distributed Ledger in modo indipendente, ma sotto il controllo consensuale degli altri nodi.
Struttura	Dati e informazioni rappresentano una catena di blocchi. Questa struttura non è la vera struttura dei Distributed Ledger.	È un database distribuito su più nodi. I dati sono rappresentati in modo diverso sui diversi Ledger.
Sequenza di Blocchi	I blocchi seguono una sequenza definita.	Non è necessario seguire la sequenza di dati che caratterizza la Blockchain.
Consenso	C'è un largo uso di meccanismi di proof-of-work nella Blockchain.	Non c'è bisogno di un particolare tipo di consenso e sono relativamente più scalabili della Blockchain.
Implementazione in casi reali	Molte aziende e start-up utilizzano già la Blockchain.	I progetti che utilizzano la DLT sono ancora in fase di sviluppo. Non ha molte implementazioni nella vita reale.
Token	Molte piattaforme Blockchain si basano sull'utilizzo dei token.	Non è necessario disporre di token o di qualsiasi tipo di valuta sulla rete.

Per capire quali tipi di scenario può abilitare la Blockchain, si può partire dalla sua applicazione più famosa: il Bitcoin, la prima e più importante criptovaluta al mondo. Si tratta di un asset digitale condivisibile tra diversi player utilizzando una Blockchain, l'infrastruttura tecnica nativa del Bitcoin, a cui è delegata la garanzia che le transazioni siano corrette, che si evitino casi di doppia spesa e che si mantenga l'immutabilità delle informazioni archiviate nella catena.

Partendo dall'idea iniziale di sistema peer-to-peer per lo scambio di Bitcoin, il concetto di Blockchain si è evoluto, trasformandosi in una "multipurpose technology", che consente casi d'uso che vanno oltre le funzionalità delle criptovalute.

Grazie all'impatto di questa prima applicazione, oggi abbiamo a disposizione altre **diverse tecnologie Blockchain con varie proprietà tecniche e funzioni per gli utenti**, che possono essere utilizzate per progettare e realizzare diversi nuovi casi d'uso aziendali.

Le tecnologie Blockchain e DLT permettono di effettuare transazioni con la garanzia di una completa trasparenza, perché visibili a tutti. Assicurano inoltre una completa sicurezza poiché questi blocchi non possono essere modificati, assicurando l'integrità dei dati nel tempo. La Blockchain potrà rivoluzionare il modo in cui interagiamo e facciamo affari attraverso i nuovi ecosistemi abilitati dalle piattaforme digitali, potendo garantire informazioni complete, trasparenti e sicure sulle transazioni.

Gli attuali sistemi basati sull'architettura DLT possono essere classificati in tre tipologie: pubblica, privata e consortile.

Architettura DLT

Proprietà	Pubblica	Privata	Consortile
Consenso	Tutti i "miners"	Organizzazione centralizzata	Un set di nodi
Permesso	Pubblico	Pubblico o riservato	Pubblico o riservato
Immutabilità	Quasi impossibile da manomettere	Può essere manomessa	Può essere manomessa
Efficienza	Bassa	Alta	Alta
Processo per il consenso	Senza autorizzazione	Con autorizzazione	Con autorizzazione

Le **DLT pubbliche** corrispondono a sistemi in cui chiunque può accedere alla rete. Sono sistemi "zero-trust" dove i nodi sono pseudo-anonimi e la conformità alle regole è imposta da incentivi e da un processo competitivo, come ad esempio uno schema matematico "puzzle-solving", noto anche come "Proof of Work".
Le **DLT private** consentono l'accesso a seguito di un'autorizzazione specifica, si basano su controparti fidate e su identità digitali forti, mentre la conformità alle regole è imposta da diverse autorità in collaborazione ed è accettata da tutti i partecipanti alla rete.

La **Blockchain Consortile** è governata invece da un gruppo di nodi ristretto e non da un unico nodo centrale, come per le private. Questa sua composizione ne garantisce la decentralizzazione, un elemento che contraddistingue la Blockchain e che rende tutti i nodi indipendenti l'uno dall'altro, ma soggetti a un controllo reciproco.

DLT permission-less o permissioned: le DLT "permission-less" (senza autorizzazione) sono sistemi in cui chiunque può operare, senza autenticazione e senza autorizzazioni di alcun tipo. Nelle DLT "permissioned" (con autorizzazione) si può operare solo se si è autorizzati.

Le **Distributed Ledger Technologies** possono essere classificate utilizzando diverse dimensioni di analisi:

- Chi può accedere alla Distributed Ledger?
- Quale tipo di autorizzazioni sono necessarie per operare?
- Quale tipo di crittografia viene utilizzata?
- Quale tipo di consenso viene utilizzato?
- Qual è la forma della rete (centralizzata, distribuita, decentralizzata)?
- Chi può decidere la priorità nella chiusura dei blocchi?
- Chi paga per i costi di infrastruttura e di calcolo?
- Quali algoritmi sono utilizzati e che tipo di comportamento hanno?

Combinando le prime due dimensioni otterremo:

1. **DLT pubblica e permission-less:** tutti possono accedere a questi sistemi, leggere e scrivere informazioni, senza la necessità di un'autorizzazione per eseguire operazioni, compresa la partecipazione ai meccanismi di consenso e alla verifica delle transazioni (esempi di questi sistemi sono Bitcoin ed Ethereum). Secondo alcuni esperti, questi sistemi sono gli unici a poter davvero essere chiamati Blockchain perché hanno le quattro caratteristiche universalmente riconosciute per queste architetture: sicurezza, trasparenza, decentralizzazione e immutabilità.

2 **DLT pubblica e permissioned:** tutti possono accedere al sistema e leggere le informazioni memorizzate nei blocchi, ma sono necessari permessi e autorizzazioni per eseguire altre operazioni, come l'aggiunta di una nuova transazione al sistema. Un esempio di caso d'uso per questi sistemi è il monitoraggio della catena alimentare: il consumatore può leggere e verificare in modo indipendente l'origine e il percorso intrapreso da un prodotto alimentare, ma solo gli utenti qualificati, come gli operatori della supply chain, possono immettere nuove informazioni sul sistema (ad esempio, un cambio di stato in un lotto di merci).

3 **DLT privata e permission-less:** le operazioni sono limitate a determinati gruppi di utenti, ma non sono richieste autorizzazioni speciali per eseguirle. La limitazione si verifica in genere isolando "geograficamente" la rete in modo da non fornire un accesso pubblico ma all'interno di un'organizzazione.

4 **DLT privata e permissioned:** l'accesso è limitato a gruppi specifici di utenti e sono necessari permessi e requisiti speciali per eseguire operazioni sul sistema. Un esempio di questo tipo di DLT è la piattaforma HyperLedger Fabric.

A volte usare una Blockchain pubblica e permission-less può essere conveniente, specialmente quando l'ecosistema è aperto e l'infrastruttura deve essere utilizzata da utenti non prevedibili. In altre condizioni, invece, è consigliabile impiegare una Distributed Ledger privata e permissioned, soprattutto quando è necessario condividere valori e informazioni tra utenti precedentemente circoscritti in un ecosistema chiuso.

In entrambi i casi, gli ecosistemi possono trarre vantaggio da una Blockchain o da un'infrastruttura DLT, perché delegano loro ogni aspetto relativo alla fiducia e all'immutabilità e questo apre nuove opportunità sia in campo commerciale che industriale.

In Engineering non stiamo solo studiando l'evoluzione delle tecnologie DLT e Blockchain, ma stiamo contribuendo attivamente al loro avanzamento attraverso la partecipazione ai più importanti gruppi di lavoro internazionali su DLT e Blockchain, come il Focus Group on Application of Distributed Ledger Technology promosso al livello delle Nazioni Unite e il gruppo di lavoro Blockchain and Distributed Ledger technologies promosso dal comitato tecnico ISO / TC 307. Questi gruppi di rilevanza globale sono incentrati sulla progettazione e lo sviluppo della migliore strategia Blockchain a tutti i livelli.

2

COME FUNZIONA?

BLOCKCHAIN

Come suggerisce il nome, una Blockchain è una catena di blocchi di informazioni. Ogni blocco è un'unità di archiviazione approvata (ne parleremo più avanti) contenente una sequenza di transazioni, che a loro volta sono record singoli che dispongono di un certo ammontare di informazioni. Ogni blocco ha un timestamp e un collegamento di riferimento al precedente blocco che deve essere confermato e crittografato: ciò garantisce l'**immutabilità** e la **tracciabilità completa** della catena.

Grazie alle sue caratteristiche di immutabilità, trasparenza, verificabilità, crittografia dei dati e resilienza operativa, la Blockchain può permettere un continuo miglioramento delle tecniche di difesa informatica, prevenendo attività fraudolente attraverso meccanismi di consenso e rilevando la manomissione dei dati. È chiaro, ovviamente, che nessun sistema di cyber-difesa può essere considerato sicuro al 100%.

Quando viene creato, un nuovo blocco è collegato all'ultimo della catena, in modo che la sequenza risultante rappresenti **il libro mastro storico** di tutte le transazioni avvenute nel sistema dal giorno zero.

Nella maggior parte dei sistemi ogni blocco ha una capacità limitata: per esempio, nella Blockchain utilizzata per i Bitcoin viene incluso un nuovo blocco nella catena ogni 10 minuti circa, le transazioni sono aggregate in blocchi e devono essere verificate dai miners.

Le informazioni sulla Blockchain non vengono archiviate in un'unica posizione: ogni partecipante possiede una copia completa automaticamente sincronizzata con tutte le altre, in modo tale che le informazioni siano **sempre accessibili e non corruttibili**.

La tecnologia Blockchain è stata creata per raggiungere un consenso sulle azioni condotte nei sistemi di archiviazione dei dati, così da creare una coerenza che contribuisca alla verifica, all'atomicità, alla durata e all'integrità delle informazioni. A differenza dei tradizionali sistemi di archiviazione dei dati, le **Blockchain offrono la possibilità di scegliere diversi modi per raggiungere il consenso**. La metafora della "catena" è usata per sottolineare il concetto che la Distributed Ledger è immutabile: una volta che un blocco è stato scritto, non può poi essere modificato o cancellato. Per applicare questo vincolo di integrità, le piattaforme Blockchain utilizzano due tecniche: algoritmi crittografici per sigillare il contenuto; la replica dell'intera Distributed Ledger per tutti i membri del sistema distribuito. Quest'ultimo consente alla catena di blocchi di essere memorizzata più volte da più utenti, aumentandone l'affidabilità e l'integrità. Poiché quindi ogni blocco contiene informazioni che fanno riferimento a quelle appartenenti al blocco precedente nella catena, per modificarne uno è necessario modificare anche tutti i successivi. È inoltre necessario farlo per ogni partecipante alla catena, dal momento che tutti hanno una copia completa delle informazioni, sincronizzate automaticamente con le altre copie.

In teoria, da un punto di vista tecnico è possibile modificare le informazioni memorizzate su una Blockchain. In pratica, però, è sostanzialmente impossibile nella maggior parte delle Blockchain pubbliche (ad esempio quelle che ospitano criptovalute) per due motivi principali:

- **Consenso:** ogni nodo della rete può rilevare in modo indipendente qualsiasi violazione dei sigilli digitali
- **Potenza di calcolo:** la quantità di risorse necessarie per modificare tutti i nodi e i blocchi in tutte le Blockchain interessate sarebbe quasi impossibile da ottenere.

Questi sono i motivi per cui riteniamo che le informazioni inserite nella Blockchain siano sempre accessibili ma non corruttibili.

La vera differenza rispetto alle architetture più tradizionali consiste nel fatto che i nodi di una rete Blockchain devono essere posseduti e gestiti da entità diverse e autonome che, pur cooperando come pari su un insieme comune di obiettivi, sono vincolati da un conflitto di interessi e non dalla buona volontà e/o da vincoli gerarchici. In altre parole, tutte le parti interessate concordano su alcune regole comuni, ma allo stesso tempo ognuna è vigile contro le violazioni, perché andrebbero a beneficio dell'autore e a spese degli altri.

Questo tratto fondamentale della tecnologia Blockchain non viene messo in evidenza al pari delle sue altre peculiarità più ovvie, come la condivisione di informazioni, l'immutabilità e la resilienza, ma potrebbe e dovrebbe essere un'area da esplorare per sviluppare casi d'uso più maturi.

Come sistema di archiviazione che abbraccia più organizzazioni, la Blockchain è solo l'applicazione più basilare di un paradigma pionieristico. In scenari più avanzati, i diversi nodi di una rete Blockchain non solo collaborano per proteggere la Distributed Ledger, ma applicano anche **regole di convalida delle singole transazioni**, rifiutando il blocco che le contiene se non è conforme. Questo processo è a prova di manomissione come la stessa Distributed Ledger, perché la decisione finale sulla sua validità è raggiunta per consenso: tutti i nodi possono fornire un parere e la maggioranza vince, affinché nodi malfunzionanti o dannosi non possano corrompere il processo. Quando il set di regole è scritto nel software, viene definito "smart contract". **Con gli smart contract la tecnologia Blockchain può davvero consentire una nuova era di interazioni sicure ma decentralizzate**.

Combinando inoltre la sua immutabilità all'applicazione di un timestamp specifico (data e ora) su ciascun blocco della catena, la Blockchain garantisce l'esistenza delle informazioni dall'istante in cui il timestamp è applicato al blocco che le contiene.

Che tipo di risorse vogliamo "notarizzare" su un sistema DLT?

La Blockchain assume il ruolo di "notaio dei dati" e ne salvaguarda soltanto l'accuratezza dei dati, fungendo da sigillo digitale.

Risorse digitali: un documento digitale o un insieme di dati possono essere crittografati in modo sicuro e l'HASH risultante può essere facilmente pubblicato su un sistema DLT. In questo modo, la loro esistenza alla data di pubblicazione e la loro immutabilità è garantita nel tempo.

Beni fisici unici, riprodotti da rappresentazioni digitali uniche: un esempio può essere una fotografia ad alta definizione di un'opera d'arte, da considerare la sua rappresentazione digitale unica. In questo caso è possibile notarizzare la rappresentazione digitale, tornando, di fatto, al caso precedente di notarizzazione di un bene digitale.

3

COSA FA?

Fiducia e responsabilità

Uno degli aspetti più importanti nelle relazioni commerciali e nelle partnership è il concetto di fiducia tra i diversi attori di un ecosistema globale. La sua gestione è un costo e rappresenta un ostacolo culturale alla costruzione di relazioni commerciali positive. All'interno degli ecosistemi digitali le organizzazioni fanno fatica a definire l'equilibrio tra tecnologia, processo e persone, ma devono decidere come affrontare il problema ed evolvere il livello di fiducia tra le controparti. Poter condurre interazioni affidabili, garantire l'integrità e accessibilità dei dati e l'operatività del sistema potrebbe rivelarsi cruciale per il successo di qualsiasi ecosistema aziendale.

I trend digitali stanno cambiando le aspettative degli stakeholder I trend digitali stanno cambiando le aspettative degli stakeholder e l'uso della tecnologia sta influenzando il modo in cui le organizzazioni vengono valutate. Ci si aspetta che quest'ultime agiscano in modo sempre affidabile, ma anche quando soddisfano questo requisito, non sempre tutte le parti interessate concedono la loro fiducia. Ogni stakeholder, all'interno di un determinato dominio e nel corso delle sue attività, deve infatti garantire regolarmente l'integrità dei dati e l'operatività del sistema, per assicurarne l'efficacia del processo.

Con la Blockchain non è necessario che terze parti certifichino la responsabilità degli stakeholders, perché tutti quelli che appartengono allo stesso ecosistema possono svolgere le loro attività e allo stesso tempo verificare quelle svolte dagli altri. Qualsiasi violazione può essere rilevata dagli altri partecipanti alla rete, che hanno quindi la possibilità di decidere di non convalidare il lavoro di attori inaffidabili o dannosi, perché tutte le operazioni avvengono in modo trasparente e sono visibili a tutti, seguendo un algoritmo di consenso o regole comuni precedentemente stabilite. In questo scenario il concetto di fiducia è intrinseco, non è necessario che la convalida provenga da terze parti.

Alta disponibilità e flessibilità

Il consenso sull'accuratezza e l'immutabilità dei dati garantisce la resilienza del sistema, progettato per resistere a qualsiasi tipo di attacco in vari contesti. Le tecnologie informatiche consolidate da decenni, come la crittografia e gli algoritmi HASH, sono inclusi nella tecnologia Blockchain e assicurano che il network possa essere immune da attacchi di qualsiasi tipo, inclusi corruzione e manomissione dei dati.

Questa **elevata resilienza** determina naturalmente la grande disponibilità dei dati su Blockchain e sui sistemi basati su DLT. Qualsiasi tentativo di manomissione è inibito di default e i dati danneggiati vengono ripristinati grazie alla ridondanza della rete. Ciò ne garantisce l'integrità e la continuità dei processi basati su di essi.

Unico punto di verità

Determinare un Single Point of Truth è uno dei fattori fondamentali per garantire la coerenza dei dati nelle aziende. Realizzarlo tramite DLT o Blockchain è più facile perché entrambe consentono di avere un **database distribuito**, i cui dati sono conservati in modo ridondante attraverso i nodi che partecipano alla rete. Attraverso questa moltitudine di nodi sincronizzati, che costituisce un unico punto di verità, si preserva l'integrità dei dati e qualsiasi aggiornamento legittimo proveniente da un nodo viene automaticamente ricevuto dagli altri partecipanti alla rete.

What does it do?

Fiducia e responsabilità

Garantire la reciproca responsabilità tra le parti interessate

Alta disponibilità e flessibilità

Assicurare continuità ai processi critici anche in ambiente ostile

Unico punto di verità

Mantenere le istanze multiple dello stesso processo in sincrono

Cosa sono e come funzionano gli NFT

Gli NFT, acronimo di non-fungible token, sono gli asset digitali più popolari del momento insieme alle criptovalute. Diversi NFT sono stati venduti online a cifre incredibili e sono in continuo aumento coloro che desiderano entrare in possesso di questi particolari token. In questo approfondimento vedremo cosa sono gli NFT, come funzionano e quali sono le loro possibili applicazioni, compreso il loro utilizzo nel Metaverso.

Cosa sono gli NFT: la definizione

Gli NFT sono dei token crittografici che certificano la proprietà, l'unicità e l'autenticità di un bene digitale. Questi token non sono fungibili, questo significa che non sono reciprocamente intercambiabili. Dato che ogni token non convertibile è identificabile in modo univoco, gli NFT differiscono dalle criptovalute, che sono invece fungibili. Acquistando un NFT si acquisterà dunque un'immagine, un video, una canzone o qualsiasi altro asset digitale, la cui proprietà, unicità e autenticità è certificata. I casi d'uso più comuni degli NFT sono l'arte, la musica, i film e i videogiochi. Tecnicamente, gli NFT sono unità di dati memorizzati su una blockchain. Non tutti i dati vengono però memorizzati sulla blockchain, di solito un tipico NFT è diviso in due entità separate, il contratto 'smart' memorizzato sulla blockchain e l'asset digitale stesso. Nel momento in cui un NFT viene creato, ogni vendita di quello specifico NFT viene registrata su una blockchain. Si crea perciò un libro mastro con le informazioni sulla proprietà e la storia dei prezzi dell'NFT. Questa registrazione è nota come "provenance" (provenienza). La provenienza di un NFT è molto importante in quanto influisce sul suo valore. La provenienza identifica i beni digitali, fornendo prove circostanziali e contestuali della loro creazione e della loro storia. Anche nel mondo dell'arte vero e proprio, la provenienza può stabilire che un bene non è un falso, un furto o una riproduzione, influenzando così il suo valore. È bene notare che gli NFT non trasmettono la proprietà intellettuale o il copyright dei file digitali. L'NFT attesta la prova della proprietà che è però separata dal copyright. Il contratto smart associato all'NFT può però essere scritto in modo tale da includere i diritti d'autore. La criticità maggiore degli NFT riguarda proprio la mancanza di una specifica regolamentazione sul piano giuridico atta a preservare l'originalità dell'opera.

Come funzionano i Non-fungible Token?

La creazione di un NFT viene definita 'minting', e consiste nella trasformazione sulla blockchain di un file digitale in un asset digitale. Il modo più comune per coniare un NFT è farlo su un marketplace NFT. Esistono molti marketplace su cui un NFT può essere creato, scambiato, verificato o distrutto. Una delle piattaforme più note è OpenSea, ma ce ne sono molte altre. Per creare NFT, è necessario possedere un wallet (portafoglio). I wallet sono le applicazioni che vengono utilizzate per memorizzare e custodire criptovalute e NFT. Il proprio wallet deve essere compatibile con la blockchain su cui viene creato l'NFT. Trust Wallet, Coinbase Wallet e MetaMask sono tre portafogli molto popolari ma ce ne sono anche altri. In pratica, il creatore carica un file sulla piattaforma, gli assegna un titolo e un sottotitolo, aggiunge una descrizione, imposta le royalties e mette in vendita l'NFT. Le royalties sono sempre stabilite nel momento in cui l'NFT viene creato e danno diritto al creatore a una percentuale delle vendite successive. Una volta che l'NFT è stato creato, il token viene trasferito al portafoglio. Questo processo ha dunque trasformato il file digitale in un asset crittografico che può essere scambiato su un mercato digitale. Agli NFT vengono poi associate delle commissioni di transazione. Quando gli utenti creano un NFT, pagano commissioni di "minting", chiamate anche "gas fees". Su molte piattaforme, gli utenti pagano solo le commissioni di minting e solo una volta le gas fees. Coloro che desiderano acquistare NFT dovranno dunque scegliere una piattaforma NFT.

- Piattaforme a tema aperto: in cui tutti possono creare NFT. Le più conosciute sono OpenSea e Rarible.

- Piattaforme a tema aperto più esclusive: in cui serve un'approvazione per diventare creator. Le più note sono Foundation e Nifty Gateway.
- Piattaforme esclusive e con un determinato tema: in queste piattaforme i creatori sono integrati con i proprietari della piattaforma e solo le collezioni pre-approvate possono essere scambiate. Alcuni esempi noti sono Larva Labs e Dapper Labs.

Gli acquirenti potranno scegliere la piattaforma che meglio si adatta alle loro esigenze, come ad esempio una piattaforma che permetta di acquistare NFT con moneta fiat piuttosto che una che consenta di pagare solo tramite crypto.

Per cosa vengono utilizzati oggi gli NFT

Come anticipato, gli NFT vengono utilizzati per acquistare o vendere beni digitali, questi asset digitali generalmente sono: immagini, video, GIF, tweet, canzoni, film, carte da gioco virtuali, skin per videogiochi, beni immobili virtuali, ecc. Gli NFT vengono spesso acquistati dagli utenti per essere rivenduti ad un prezzo maggiore o per il mero desiderio di possedere qualcosa di unico. Questi token trovano infatti applicazione in davvero tantissimi ambiti, ecco qui di seguito i casi d'uso più noti:

- Arte: gli NFT raffiguranti le opere d'arte sono tra i più ricercati ed acquistati sul mercato. Il più noto tra gli NFT artistici è indubbiamente " Everydays – The First 5000 Days", un collage composto da cinquemila opere digitali, realizzate una al giorno per cinquemila giorni, ad opera di Mike Winkelmann (in arte Beeple).
- Metaverso: gli NFT vengono utilizzati nelle piattaforme Metaverso, come ad esempio Decentraland. Su Decentraland gli NFT definiscono la proprietà di terreni digitali che rappresentano dunque il patrimonio immobiliare digitale dell'utente. Nel mondo della realtà aumentata gli NFT possono essere potenzialmente utilizzati non solo per i terreni ma anche per i vestiti del proprio avatar o per qualsiasi altro oggetto digitale.
- Gaming: nel mondo dei videogiochi gli NFT vengono utilizzati per ricompensare l'utente. Il sistema "giocare per guadagnare" funziona molto bene all'interno di questo settore.
- Social: gli NFT trovano ampia applicazione anche nel mondo di Twitter. Basti pensare che Elon Musk ha rifiutato circa 1 milione di dollari per l'acquisto di un suo tweet.
- Sport: anche lo sport è un caso d'uso per gli NFT. Ad esempio, sulla piattaforma NBA Top Shot, gli utenti acquistano video NFT legati all'NBA.

Web3: il web *stateful*

Se assumiamo che il WWW abbia rivoluzionato le informazioni e che il Web2 abbia rivoluzionato le interazioni, il Web3 ha il potenziale per rivoluzionare gli accordi e lo scambio di valore.

Il Web3 modifica le strutture dei dati nel backend di Internet, introducendo un livello di stato universale, spesso incentivando gli attori della rete con un token. La spina dorsale di questo Web3 è rappresentata da una serie di reti blockchain o ledger distribuiti simili.

L'Internet che abbiamo oggi è *guasto*. Non controlliamo i nostri dati, né disponiamo di un livello di regolazione del valore nativo. A trent'anni dall'adozione di massa di Internet, le nostre architetture di dati si basano ancora sul concetto di computer autonomo, in cui i dati vengono archiviati e gestiti centralmente su un server e inviati o recuperati da un client. Ogni volta che interagiamo su Internet, copie dei nostri dati vengono inviate al server di un fornitore di servizi e ogni volta che ciò accade, perdiamo il controllo sui nostri dati. Di conseguenza, e anche se viviamo in un mondo sempre più connesso, i nostri dati sono per lo più archiviati centralmente: su server locali o remoti, sui nostri personal computer, dispositivi mobili, hard disk esterni e sempre più anche sui nostri orologi, automobili, TV, o frigoriferi. Tutto ciò solleva problemi di fiducia. Posso fidarmi di quelle persone e istituzioni che archiviano e gestiscono i miei dati contro qualsiasi forma di corruzione, internamente o esternamente, intenzionalmente o accidentalmente? Le strutture dati centralizzate non solo sollevano problemi di sicurezza, privacy e controllo dei dati personali, ma producono anche molte inefficienze lungo la catena di fornitura di beni e servizi.

Le radici di questi problemi risalgono a prima ancora dell'avvento di Internet. Agli albori dei personal computer non si potevano inviare file da un computer all'altro. Dovevi salvare un file su un floppy disc, andare dalla persona che aveva bisogno del file e copiarlo sul suo computer perché potesse usarlo. Se quella persona era in un altro paese, bisognava spedirle il floppy disc via posta.

L'emergere del protocollo Internet (IP) ha posto fine a questi passaggi, collegando tutti quei computer stand-alone con un protocollo di trasmissione che ha reso il trasferimento dei dati più veloce e ha ridotto i costi di transazione dello scambio di informazioni. Tuttavia, l'Internet che utilizziamo oggi è ancora prevalentemente basata sull'idea del computer autonomo, in cui la maggior parte dei dati viene archiviata e gestita centralmente sui server di istituzioni affidabili. I dati memorizzati su questi server sono protetti da firewall e sono necessari amministratori di sistema che ne gestiscano la sicurezza.

L'emergere del WWW all'inizio degli anni '90 ha aumentato l'usabilità di Internet con siti web visivamente accattivanti e facili da navigare. Dieci anni dopo, Internet è diventato più maturo e programmabile. Abbiamo assistito all'ascesa del cosiddetto Web2, che ci ha portato social media, e-commerce e piattaforme di apprendimento. Il Web2 ha rivoluzionato le interazioni sociali, avvicinando produttori e consumatori di informazioni,

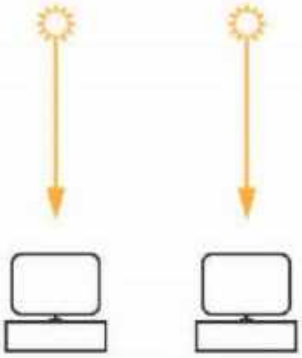
beni e servizi. Il Web2 ci ha permesso di godere di interazioni peer-to-peer (P2P) su scala globale, ma sempre con un intermediario: una piattaforma che funge da intermediario fidato tra due persone che non si conoscono o non si fidano l'una dell'altra. Sebbene queste piattaforme Internet abbiano svolto un lavoro fantastico nel creare un'economia P2P, dettano anche tutte le regole e controllano i dati dei loro utenti.

In questo contesto, le reti blockchain sembrano essere una forza trainante dell'Internet di prossima generazione, quello che alcuni chiamano Web3. Esse reinventano il modo in cui i dati vengono archiviati e gestiti su Internet, fornendo un set di dati univoco, un livello di stato universale, che viene gestito collettivamente da tutti i nodi della rete. Questo livello di stato unico, per la prima volta, fornisce un livello di regolazione del valore nativo per Internet in assenza di intermediari. Consente transazioni P2P reali e tutto è iniziato con l'emergere di Bitcoin.

Mentre Web2 è stata una rivoluzione front-end, Web3 è una rivoluzione backend. Il Web3 reinventa il modo in cui Internet è cablato nel backend, combinando le funzioni di sistema di Internet con le funzioni di sistema dei computer. Tuttavia, per l'utente medio non cambierà molto sul front-end di Internet. Il Web3 rappresenta un insieme di protocolli, con i ledger distribuiti come spina dorsale. I dati sono gestiti in modo collaborativo da una rete di computer P2P. Le regole di gestione sono formalizzate nel protocollo e garantite dal consenso di maggioranza di tutti i partecipanti alla rete, che sono incentivati con un token di rete per le loro attività. Il protocollo formalizza le regole di governance della rete e garantisce che le persone che non si conoscono o non si fidano l'una dell'altra raggiungano e concludano accordi sul Web. Mentre il tentativo di manipolare i dati su un server somiglia a un'irruzione in una casa, dove la sicurezza è garantita da una recinzione e un sistema di allarme, il Web3 è progettato in modo tale da dover entrare in più case contemporaneamente in tutto il mondo, ognuna dotata della propria recinzione e sistema di allarme. Questo è possibile ma proibitivo.

Storia del Web

Economia dell'Informazione

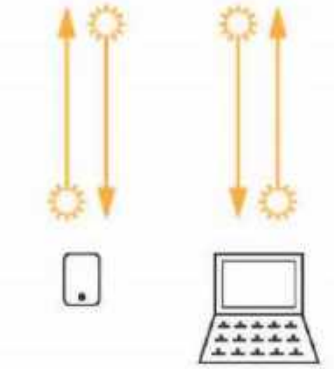


Benvenuta Internet (Hello World)

Tim Berners Lee introduce un nuovo standard che permette di creare pagine web visivamente accattivanti con poche righe di codice, e di navigare in Internet tramite link ipertestuali anzichè usando interfacce a linea di comando. Internet diventa più usabile. Ora chiunque può usare Internet come una "Autostrada per dati e informazioni"

Applicazioni: Web browsers, motori di ricerca.

Economia delle Piattaforme

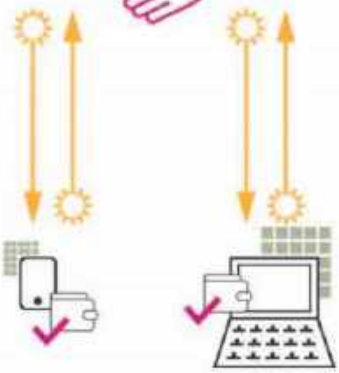


Rivoluzione del front-end

Internet diventa più matura, Le applicazioni possono essere usate sia per leggere sia per scrivere. Questo rivoluziona le interazioni sociali ed economiche, avvicinando tra loro i produttori e i consumatori di informazioni, beni e servizi. Ma sempre con un intermediario: una piattaforma fidata tra due persone che non si conoscono e non hanno quindi fiducia l'uno nell'altro.

Applicazioni: Wikipedia, social media, e-commerce.

Economia dei Token



Rivoluzione del Back-end

Il front-end rimane invariato, ma cambiano le strutture dei dati nel back-end. Chiunque può partecipare alla verifica delle transazioni ed essere ricompensato per il suo contributo con un token della rete. Le parti possono prendere accordi al volo e in modalilità P2P tramite protocolli detti smart contract. Le applicazioni Web3 necessitano di una connessione ad un ledger distribuito, gestita tramite una applicazione speciale chiamata "wallet" (portafogli)

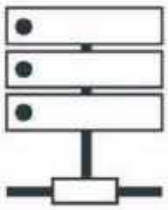
Applicazioni: Token

Internet Client-Server

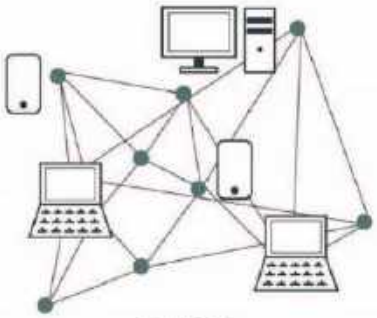
Server

Client

Monopolio dei Dati vs. Sovranità dei Dati

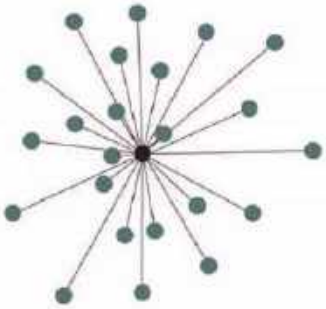


Server

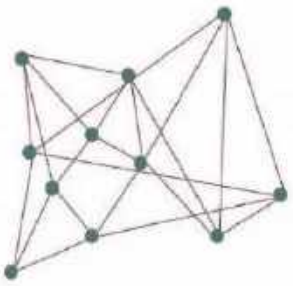


Reti P2P

Centralizzato vs. Distribuito



Punto Unico
di Guasto



Nessun Punto Unico di Guasto
=> maggiore sicurezza

Blockchain: Un protocollo *stateful*

L'Internet che utilizziamo oggi è "stateless". Non ha un meccanismo nativo per trasferire ciò che l'informatica chiama "stato". Lo stato si riferisce alle informazioni o allo stato di "Chi è chi?", "Chi possiede cosa?" e "Chi ha il diritto di fare cosa?" in una rete. La capacità di trasferire facilmente valore e P2P è essenziale per mercati efficienti e lo "stato" è una proprietà chiave per la gestione e il trasferimento di valori. Nel Web3 i valori sono rappresentati da token protetti crittograficamente.

Se non puoi mantenere lo stato su Internet, non puoi trasferire valore senza istituzioni centralizzate che agiscono come entità di compensazione. Sebbene l'Internet di oggi abbia accelerato il trasferimento di informazioni di diversi ordini di grandezza rispetto a prima, abbiamo ancora bisogno di istituzioni affidabili, come i fornitori di piattaforme Internet, per negoziare le nostre azioni come soluzione alternativa a questa mancanza di stato. I protocolli apolidi, come l'attuale Web, gestiscono solo il trasferimento di informazioni, laddove il mittente o il destinatario di tali informazioni non è a conoscenza dello stato dell'altro. Questa mancanza di stato si basa sulla semplicità dei protocolli su cui è costruito il Web, come TCP / IP, SMTP o HTTP. Questa famiglia di protocolli regola la trasmissione dei dati, non il modo in cui i dati vengono archiviati. I dati possono essere archiviati centralmente o in modo decentralizzato. Per molte ragioni, l'archiviazione centralizzata dei dati è diventata la forma principale di archiviazione e gestione dei dati.

L'introduzione di cookie di sessione e fornitori di servizi centralizzati ha offerto soluzioni alternative a questo Web senza stato. I cookie di sessione sono stati inventati in modo che le applicazioni basate sul Web potessero preservare lo stato sui dispositivi locali. Prima dei cookie di sessione, nei primi giorni del WWW, non avevamo la cronologia di navigazione, i siti preferiti salvati e il completamento automatico, il che significava che dovevamo inviare nuovamente le nostre informazioni utente ogni volta che stavamo utilizzando un sito web. Sebbene i cookie di sessione forniscano una migliore usabilità, questi cookie sono creati e controllati da un fornitore di servizi, come Google, Amazon, Facebook, la tua banca, la tua università, ecc., il cui ruolo è quello di fornire e gestire lo stato dell'utente.

Le piattaforme Web2 hanno introdotto molti servizi vantaggiosi e creato un notevole valore sociale ed economico nel corso degli anni. Tuttavia, la ricchezza è stata accumulata principalmente dalle società che offrono i servizi e meno dal pubblico in generale che contribuisce con contenuto e valore a tali servizi. Invece di decentralizzare il mondo, le piattaforme Web2 hanno contribuito a una ri-centralizzazione del processo decisionale economico, del processo decisionale di ricerca e sviluppo e, successivamente, a un'enorme concentrazione di potere attorno a questi fornitori di piattaforme. Inoltre, poiché il primo Internet è stato creato attorno all'idea di informazioni gratuite, i clienti spesso non erano disposti a pagare per i contenuti online con una quota di abbonamento ricorrente e nella maggior parte dei casi i micropagamenti non sono ancora fattibili. Pertanto, molte di queste piattaforme Web2 avevano bisogno di trovare modi alternativi per trarre profitto dai servizi gratuiti che fornivano e questa alternativa era la pubblicità. Ciò che è seguito è stata una pubblicità mirata basata sul comportamento degli utenti e sulla mercificazione

dei dati privati. I modelli di business si sono quindi sviluppati intorno alla pubblicità mirata che si basa sui set di dati raccolti, che forniscono lo "stato" per queste piattaforme. Di conseguenza, gli utenti pagano i servizi con i loro dati privati.

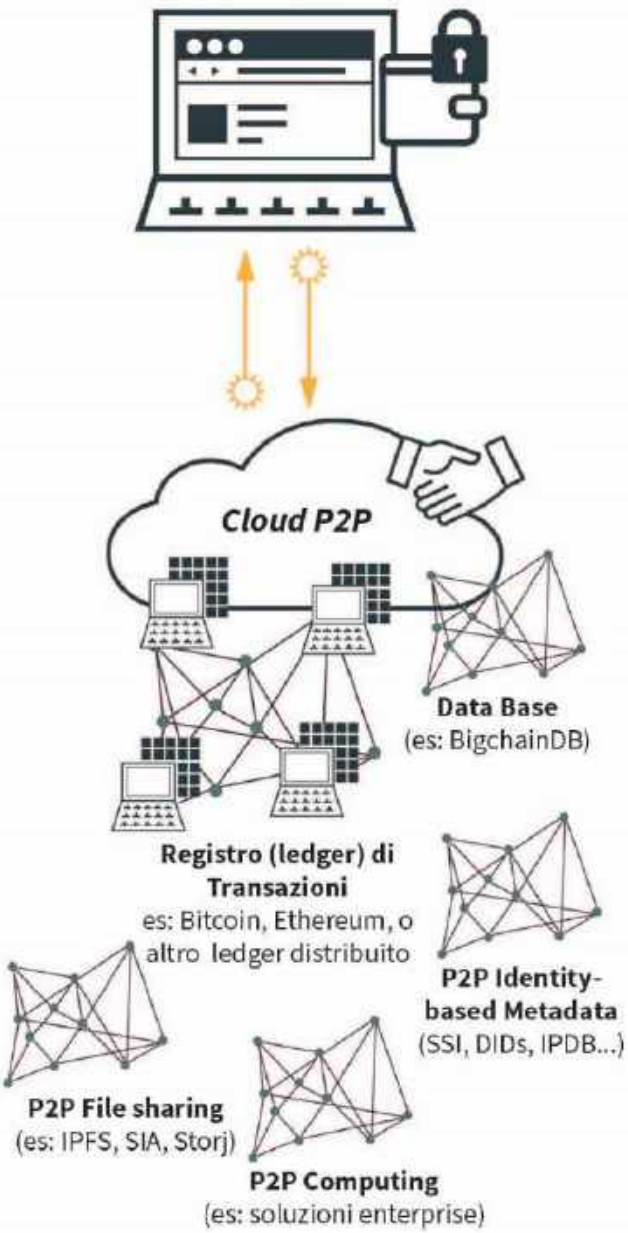
La rete Bitcoin ha introdotto un meccanismo per ogni nodo in una rete per inviare e ricevere token e registrare lo stato dei token, in un formato nativo digitale. Il protocollo di consenso della rete Bitcoin è progettato in modo che la rete possa ricordare collettivamente eventi precedenti o interazioni degli utenti, risolvendo il problema della “doppia spesa” fornendo un'unica fonte di riferimento per chi ha ricevuto cosa e quando. Il protocollo Bitcoin può, quindi, essere visto come un punto di svolta, che apre la strada a un Web più decentralizzato. Il white paper Bitcoin del 2008 ha avviato una nuova forma di infrastruttura pubblica, in cui lo stato di tutti i bitcoin viene mantenuto collettivamente.

Le reti blockchain, come la rete Bitcoin, sono solo la spina dorsale e il punto di partenza, ma non l'unico mattone in questo nuovo Web decentralizzato. L'architettura del Web3 sfrutta lo stato universale gestito collettivamente per l'elaborazione decentralizzata. Le applicazioni decentralizzate possono gestire alcuni o tutti i loro contenuti e logica tramite una rete blockchain o un altro registro distribuito. Ma sono necessari anche altri protocolli. Molti sviluppatori hanno iniziato a creare reti blockchain alternative, oltre a protocolli complementari per il Web3.

Applicazioni Web2 vs. Applicazioni Web3

L'applicazione Web2 (client) comunica con i server

L'applicazione Web3 (client), denominata "wallet", comunica con una rete blockchain



Le applicazioni **Web2** vengono eseguite su una combinazione di server di proprietà di diverse organizzazioni, svolgendo diverse operazioni di backend. La sicurezza è fornita dall'amministratore di sistema che lavora presso quelle società, che fungono da intermediario fidato. Gestiscono tutte le identità e credenziali (combinazioni di user ID e password) e i dati personali ad esse collegati.

Le applicazioni **Web3** vengono eseguite su una combinazione di reti pubbliche e/o private, svolgendo diverse operazioni di backend. Il ledger distribuito funge da spina dorsale per le altre reti Web3 che sono gestite collettivamente e sono spesso incentivate utilizzando un token. La sicurezza è fornita da una rete P2P che valida le transazioni utilizzando tecniche di consenso a maggioranza distribuito

Applicazioni decentralizzate nel Web3

A differenza delle applicazioni centralizzate che vengono eseguite su un singolo computer, le applicazioni decentralizzate vengono eseguite su una rete P2P di computer. Esistono sin dall'avvento delle reti P2P e non devono necessariamente funzionare su una rete blockchain. "Tor", "BitTorrent", "Popcorn Time" e "BitMessage" sono tutti esempi di applicazioni decentralizzate che vengono eseguite su una rete P2P, ma non su una rete blockchain, che è un tipo specifico di rete P2P (per approfondire: Appendice – Origini del Bitcoin e del Web3).

Le applicazioni tradizionali utilizzano HTML, CSS o javascript per eseguire il rendering di una pagina Web o di un'app mobile. Il front-end di una pagina Web o di un'applicazione mobile interagisce con uno o più database centralizzati. Quando utilizzi un servizio come Twitter, Facebook, Amazon o Airbnb, ad esempio, la pagina web chiamerà un'API per elaborare i tuoi dati personali e altre informazioni necessarie archiviate sui loro server, per visualizzarli sul front-end. Per l'identificazione e l'autenticazione vengono utilizzati l'ID utente e le password, con bassi livelli di sicurezza, poiché i dati personalizzati sono memorizzati sul server del fornitore di servizi.

Le applicazioni decentralizzate non hanno un aspetto diverso dai siti Web o dalle app mobili attuali. Il front-end rappresenta ciò che si vede, e il backend di un'applicazione decentralizzata rappresenta l'intera logica aziendale. Un'applicazione decentralizzata è un client blockchain chiamato "wallet". Utilizza le stesse tecnologie per il rendering di una pagina web o di un'app mobile (come HTML, CSS, Javascript) ma comunica con una rete blockchain invece che con un server e, nel caso delle reti smart contract, anche gli smart contract (per approfondire: Parte 2 – Smart Contract). Il portafoglio gestisce anche la coppia di chiavi pubblica-privata e l'indirizzo blockchain, per fornire un'identità univoca per i nodi di rete in modo che possano interagire in modo sicuro con la rete (per approfondire: Parte 1 – Sicurezza dei token e Identità user-centriche). Gli smart contract rappresentano la logica di core business dell'applicazione decentralizzata ed elaborano feed di dati dall'interno e dall'esterno della rete per gestire lo stato di tutti gli attori della rete (per approfondire: Parte 1 – Smart Contract). Se il client blockchain è un full-node, gestirà anche lo stato completo del ledger (per approfondire: Parte 1 – Bitcoin, Blockchain e altri registri distributi). In questo caso, il client blockchain esegue le funzioni di un client HTTP e di un server, poiché tutti i dati sono archiviati lato client. I dati front-end, inclusi file audio o video e altri documenti, potrebbero essere archiviati e gestiti collettivamente da reti di archiviazione decentralizzate come "Swarm" o "IPFS". Al momento della stesura di questo libro tali dati sono ancora, per la maggior parte, archiviati e gestiti da server.

Per l'utente medio, le applicazioni decentralizzate devono avere lo stesso aspetto delle applicazioni esistenti, il che significa che devono essere facili e intuitive da usare se devono essere adottate su scala più ampia. Attualmente, il software wallet e la gestione delle chiavi sono difficili, il che potrebbe essere un collo di bottiglia per l'adozione di massa delle applicazioni Web3. Inoltre, l'adozione su larga scala può avvenire solo se la sfiducia nelle

soluzioni centralizzate è sufficientemente elevata da giustificare gli attuali compromessi nell'usabilità.

Riassunto del capitolo

L'Internet che abbiamo oggi è rotto. Non controlliamo i nostri dati, né abbiamo un livello di liquidazione del valore nativo. Ogni volta che interagiamo su Internet, copie dei nostri dati vengono inviate al server di un fornitore di servizi e ogni volta che ciò accade, perdiamo il controllo sui nostri dati. Tutto ciò genera problemi di fiducia.

L'Internet che utilizziamo oggi archivia e gestisce i dati sui server di istituzioni affidabili. Nel Web3 i dati sono archiviati in più copie di una rete P2P, e le regole di gestione sono formalizzate nel protocollo, e garantite dal consenso di maggioranza di tutti i partecipanti alla rete, spesso (ma non sempre) incentivati con un token di rete per le loro attività.

Nel Web3 lo stato della rete (rappresentato dal registro) viene mantenuto collettivamente.

Mentre il Web2 è stata una rivoluzione del front-end, il Web3 è una rivoluzione del backend, che introduce un livello di stato universale. È un insieme di protocolli guidati da una rete blockchain o da un registro distribuito simile, che intende reinventare il modo in cui Internet è cablato nel back-end. Il Web3 combina le funzioni di sistema di Internet con le funzioni di sistema dei computer.

A differenza delle applicazioni centralizzate che vengono eseguite su un singolo computer, le applicazioni decentralizzate vengono eseguite su una rete P2P di computer. Esistono dall'avvento delle reti P2P. Le applicazioni decentralizzate non devono necessariamente essere eseguite su una rete blockchain.