QUADERNI DI ALAI ITALIA

3

QUADERNI DI ALAI ITALIA

In the series "Quaderni di ALAI Italia", the Italian branch of the Association Littéraire et Artistique Internationale intends to offer an overview of the current issues in the field of copyright, also in a comparative and international perspective, in particular through the publication of the proceedings of ALAI's Meetings and Congresses.

The series is open to contributions from the community of scholars and practitioners involved in Copyright studies and research.

ALAI Italia applies transparency rules in the selection of the contributions, which may be in Italian or English. The Scientific Committee is in charge of the selection of the essays that are published and has the responsibility of the editorial guidelines. They are oriented in particular to the analysis and evaluation of the effects of technology on the creation and production of intellectual works, on their dissemination and economic exploitation and on the attitudes of the final users. The interactions between copyright and the development of the cultural industry are among the matters the series is focused on.

Il Gruppo italiano dell'Association Littéraire et Artistique Internationale (ALAI) è stato attivo fin dagli anni Venti del secolo scorso e si è formalmente costituito come ALAI Italia il 5 marzo 2015, con l'obiettivo di analizzare e diffondere i principi giuridici che assicurano la protezione nazionale, comunitaria ed internazionale del diritto d'autore e dei diritti connessi.

Inaugurando la collana "Quaderni di ALAI Italia", l'associazione intende offrire, in particolare attraverso la pubblicazione degli atti di incontri e congressi internazionali di ALAI, una panoramica dei temi più attuali in materia di diritto d'autore, anche in una prospettiva comparatistica e internazionale.

La collana è aperta ai contributi della comunità di studiosi della materia, con regole di trasparenza nella selezione dei contributi stessi, che possono essere in lingua italiana o inglese. Il comitato scientifico ha il ruolo di garantire le procedure selettive delle pubblicazioni proposte e il rispetto della linea editoriale, che dedica una particolare attenzione ad analisi e approfondimenti riguardanti gli effetti della tecnologia sulla creazione e sulla produzione delle opere dell'ingegno, sul loro sfruttamento economico e sulle modalità della loro fruizione. Saranno esplorate anche le interazioni tra diritto d'autore e sviluppo dell'industria culturale.

La tecnologia blockchain e il diritto d'autore: miraggio o realtà?

Atti del Convegno Roma, 19 giugno 2019

a cura di
Valeria Coltellacci

Valeria Coltellacci
Deborah De Angelis
Pedro De Miguel Asensio
Stefania Ercolani
Matteo Fedeli
Daniel Gervais
Laura Ricci
Stephanie Rotelli
Angela Saltarelli

Aracne editrice

ISBN 978-88-255-3773-4

I edizione: **Roma**, maggio 2021

Indice

La tecnologia blockchain e il diritto d'autore: miraggio o realtà?
ISBN 978-88-255-3773-4
DOI 10.4399/97888255377341
pag. 9–12 (maggio 2021)

Introduzione

Valeria Coltellacci*

Con questo terzo Quaderno si pubblicano gli Atti del Convegno *"La tecnologia blockchain e il diritto d'autore: miraggio o realtà?"* organizzato da ALAI Italia a Roma il 19 giugno 2019 presso la Sala Spadolini del Ministero per i Beni e le Attività Culturali.

Gli atti che qui si presentano sono il portato dei contributi degli illustri studiosi partecipanti al Convegno, nel comune intento di delineare, ciascuno dal proprio ambito, i cambiamenti che la nuova tecnologia blockchain sta apportando in diversi settori del diritto d'autore.

Purtroppo, la situazione emergenziale di questi ultimi mesi, derivata dalla pandemia da Covid-19, ha rallentato la pubblicazione degli atti che si realizza contemporaneamente a quella di un importante studio condotto dall'Osservatorio e Forum dell'Unione Europea sulla blockchain[1]„ che rappresenta un consolidamento del lavoro svolto dall'osservatorio da febbraio 2017 a maggio 2020[2].

L'emergere e lo sviluppo di diversi progetti basati sull'uso delle tecnologie blockchain e *smart contract*, infatti, sono stati accolti con grande interesse a livello europeo, tanto che, la Commissione Europea, attraverso specifici gruppi di lavoro, ha pubblicato una serie di report tematici su aspetti specifici legati alla blockchain con l'obiettivo di fornire una visione d'insieme e una trattazione concisa di ogni tema. In esito a questo studio, è emerso

* Giurista esperta in Diritto della Proprietà Intellettuale, della Concorrenza e del Mercato. È autrice di diversi articoli presso riviste giuridiche specializzate in tema di Diritto d'Autore. In qualità di membro del gruppo italiano di ALAI, partecipa assiduamente agli incontri periodici organizzati dall'associazione a livello nazionale e internazionale. Dal 2007 lavora presso la Società Italiana degli Autori ed Editori.

1. L'impegno assunto a livello europeo con i diversi soggetti interessati coinvolti nel settore della blockchain emerge in particolare con la creazione da parte della Commissione Europea di un Osservatorio e Forum dell'U.E. sulla blockchain (https://www.eublockchainforum.eu). A questi ultimi, è demandato lo studio degli sviluppi più importanti di tale tecnologia, nonchè la promozione dei protagonisti europei. Le istituzioni europee mirano ad accelerare l'innovazione e lo sviluppo della blockchain all'interno dell'U.E., contribuendo così a consolidare la posizione dell'Europa come leader globale in questa nuova tecnologia di trasformazione.

2. Il report completo è stato pubblicato il 25 giugno 2020 ed è disponibile al seguente link: https://www.eublockchainforum.eu/reports/.

come questa tecnologia possa sostenere il mercato unico digitale e persino giocare un ruolo significativo nella lotta contro il Covid-19.

In Europa, d'altronde, si sta assistendo a un aumento significativo del numero di aziende che aderiscono ai consorzi di blockchain in settori come quello alimentare, farmaceutico, energetico, dei beni di lusso o della finanza, che forniscono servizi e creano valore, e in alcuni casi introducono modelli di business innovativi.

Sul fronte della regolamentazione si è ancora nelle prime fasi[3]. L'Unione Europea ha promosso e reso possibile la blockchain come parte del quadro giuridico del mercato unico digitale, ad esempio attraverso la recente consultazione pubblica sui beni digitali. Si sta inoltre esaminando la normativa sui servizi digitali, che si concentra sull'e-commerce, per vedere come sostenere il riconoscimento reciproco di *smart contract* ed evitare la frammentazione della regolamentazione dei stessi tra gli Stati membri.

Possiamo aspettarci che questo slancio continui man mano che la strategia europea diventi sempre più ben definita. La Commissione Europea, ha detto Pēteris Zilgalvis[4], pubblicherà presto la sua prima strategia Blockchain, vale a dire una comunicazione della Commissione al Parlamento Europeo e al Consiglio su come portare avanti la blockchain nell'ambito del prossimo budget.

Tali circostanze impongono di interrogarsi anche sul possibile uso dei nuovi strumenti digitali per la gestione e la protezione della proprietà intellettuale e, in particolare, del diritto d'autore.

Oggi, nell'era del digitale, si assiste a nuove forme di generazione e condivisione di contenuti on-line che espongono il diritto d'autore a nuove sfide per garantire una remunerazione adeguata ai titolari dei diritti e, al contempo, per informare gli utilizzatori in merito al regime giuridico sotto il quale una determinata opera circoli in rete. Un passo in tale direzione è già stato fatto, da qualche decennio, sia a livello internazionale che comunitario con la tutela giuridica delle misure tecnologiche anticopia ed antiaccesso alle opere protette che consentono la gestione automatizzati dei diritti, i c.d. sistemi di *Digital Rights Management* (DRM)[5].

3. Cfr. anche la *"Risoluzione del Parlamento europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione (2017/2772(RSP)"* disponibile su http://www.europarl.europa.eu/doceo/document/TA-8-2018-0373_IT.pdf

4. Head of Unit, Digital Innovation and Blockchain, Digital Single Market, DG CONNECT and Co-Chair of the EC's FinTech Task Force.

5. Trattasi di protezioni tecnologiche che, nel normale corso del loro funzionamento, impediscono il compimento di atti sull'opera non autorizzati dal titolare dei diritti e forniscono le informazioni elettroniche sui diritti dell'opera, impresse sulla medesima dai relativi titolari. Il riconoscimento giuridico, a livello internazionale, delle misure tecnologiche di protezione delle opere protette risale ai trattati WIPO sul diritto d'autore e sui diritti connessi del 1996 e al *Digital Millennium Copyright Act (DMCA)* del 1998 che ha modificato il Copyright Act americano (per un'analisi approfondita si veda P.

In tale contesto, le potenzialità della tecnologia blockchain, basata su registri distribuiti e contratti *smart*, potrebbero essere lo strumento utile per la creazione di nuovi modelli di gestione digitale dei diritti che, salvaguardando i vari interessi in gioco, rispondano ad alcune necessità emerse con la digitalizzazione dei contenuti protetti, tra cui l'esigenza di conoscere i diritti di proprietà sulle opere e di arginare la pirateria on-line.

Facendo uso della crittografia, la blockchain permette di gestire in maniera decentralizzata un registro pubblico condiviso nel quale vengono memorizzate tutte le transazioni dell'asset che si vuole gestire. Questo permette agli stakeholder di costruire e partecipare a piattaforme che non sono controllate da un'unica entità, ma che sono piuttosto condivise.

Ma ciò che rende particolarmente utile questa tecnologia a superare alcuni problemi legati agli asset proprietari tipici della proprietà intellettuale sembrerebbe essere la trasparenza e la fiducia nei dati inseriti in un sistema basato su blockchain. Tali sistemi infatti garantiscono che i dati, una volta immessi nella "catena" non possano essere successivamente alterati o replicati o, quantomeno, che i tentativi di manipolazione di essi siano facilmente riconoscibili. Ogni dato viene memorizzato in modo da includere una quota di informazioni che fanno capo alle informazioni precedenti. Tale connessione rende impossibile l'alterazione senza che venga immediatamente pregiudicata l'integrità di tutta la catena.Per esempio, mediante la creazione di un "*hash*", ovvero un'impronta digitale temporalmente marcata di una determinata opera, è possibile tracciarne indelebilmente la provenienza, la titolarità dei diritti di privativa e la storia di utilizzo dell'opera stessa, fornendo alti livelli di trasparenza e verificabilità dei dati.

Queste caratteristiche rendono tale tecnologia impiegabile in diversi settori[6], specie in quelli in cui la fiducia sulla provenienza e la validità dei dati assume particolare rilevanza, come accade nel nell'ambito dell'intermediazione dei diritti d'autore. La possibilità, infatti, di verificare facilmente chi abbia operato con i dati lungo la catena potrebbe consentire alle organizzazioni di gestione collettiva dei diritti di autore di verificare le effettive utilizzazioni di un'opera su una piattaforma digitale, superando gli attuali problemi di audit nei confronti dei *Digital Service Provider* e fornendo alti livelli di trasparenza e verificabilità dei dati ai titolari dei diritti da esse rappresentate.

MARZANO, *Sistemi anticopiaggio, tatuaggi elettronici e responsabilità on-line: il diritto d'autore risponde alle sfide di Internet*, in *Dir. aut*., Milano, Giuffrè, 1998, p.149 e ss.). Il legislatore europeo ha operato un riconoscimento giuridico di tali misure con la Dir. 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione e, prima ancora, con la Dir. 91/250/CEE, del 14 maggio 1991, relativa alla tutela giuridica dei programmi per elaboratore che prevedeva una protezione dei meccanismi anticopia legati ai programmi per elaboratore.

6. Per un'indagine approfondita v. report tematici pubblicati dall'Osservatorio e Forum dell'U.E. sulla blockchain, disponibili su https://www.eublockchainforum.eu/reports.

Tuttavia, nel corso dei vari interventi dei partecipanti si è altresì osservato che si sta trattando di una tecnologia che in ragione della sua immaturità presenta ancora dei rischi di utilizzo. Tra questi rilevano in particolare gli elevanti costi di gestione applicati dalle piattaforme on-line per consentire la c.d. tokenizzazione, vale a dire quel processo di conversione di un diritto su un bene in un *token*, un'informazione digitale che poi viene inserita su una piattaforma blockchain (nella quale il bene reale e il *token* sono collegati da uno *smart contract*) per il relativo scambio fra gli utenti. Oltre a ciò, la tokenizzazione potrebbe creare alcune problematiche in futuro anche con riguardo alla mancanza di controllo sull'offerta dei *token*, all'autenticità e all'attribuzione delle opere, in caso di furto o deterioramento delle opere di cui si è frazionata la proprietà o nel caso di fallimento della società che emette i *token*.

Un altro aspetto da considerare è che la sola tecnologia blockchain non è sufficiente a impedire la realizzazione *off-chain* di copie contraffatte di materiali protetti e, se non correttamente implementata, potrebbe consentire l'indelebile registrazione di dati erronei concernenti l'autore o il titolare o i diritti di utilizzazione economica di un'opera o un bene immateriale (c.d. *"garbage in, garbage out"*).

Emerge, dunque, la necessità che la tecnologia blockchain, affinché possa essere considerata un valido mezzo di attuazione on-line dei diritti di proprietà intellettuale, aprendo le porte a nuovi modelli di business, sia dotata di regole standard di governo ed efficaci misure di *enforcement* ulteriori che consentano la correzione di errori o impediscano la realizzazione di atti fraudolenti.

Il Convegno ha costituito, quindi, una occasione propizia per sviluppare un interessante dibattito e confronto sulle suddette tematiche mediante la partecipazione di relatori esperti, ai quali si rivolge un sentito ringraziamento per aver magistralmente condiviso le proprie esperienze e le proprie conoscenze, rendendo questa opportunità un'esperienza di reciproco apprendimento.

La tecnologia blockchain e il diritto d'autore: miraggio o realtà?
ISBN 978-88-255-3773-4
DOI 10.4399/97888255377342
pag. 13–?? (maggio 2021)

Blockchain: aspetti tecnologici e casi d'uso

Laura Ricci*

In questo capitolo descriveremo la transizione in atto, da alcuni anni, dai sistemi centralizzati a sistemi distribuiti, ci focalizzeremo quindi sulla tecnologia delle blockchain e presenteremo una tassonomia delle blockchain esistenti.

1. Dai sistemi centralizzati ai sistemi distribuiti

La tecnologia delle blockchain, che ha conosciuto un'enorme diffusione negli ultimi anni, si inquadra nell'ambito di una transizione, in atto ormai da diversi anni, dei sistemi informativi da una struttura fortemente centralizzata verso una architettura sempre più distribuita.

Un sistema informativo centralizzato è caratterizzato dal modello *client-server,* in cui i servizi forniti dal sistema sono offerti da uno o più server appartenenti ad un unico dominio amministrativo, mentre gli utenti, tramite un programma (il programma client) accedono ai servizi da remoto.

La struttura di un sistema centralizzato viene mostrata nella parte sinistra della Figura 1. Il nodo centrale, rappresentato da un cerchio, corrisponde ad un server centralizzato, ad esempio gestito da un ente pubblico, che eroga i servizi a utenti generici, quali industrie, banche, pubblica amministrazione. Il gestore del server centralizzato può decidere chi ha il diritto di accedere ai servizi offerti, memorizza tutte le informazioni necessarie per erogarli, risponde alle richieste di tutti gli utenti. Il gestore può quindi disporre di tutti i dati raccolti dagli utenti. I fruitori del servizio devono riporre fiducia nell'ente che eroga il servizio, confidando nella correttezza della gestione e della elaborazione dei dati, rispettando le politiche di privacy degli utenti del servizio.

* Professoressa Associata, insegna P2P and Blockchain presso il Dipartimento di Informatica dell'Università degli Studi di Pisa e membro del gruppo di esperti blockchain presso il Ministero dello Sviluppo Economico.

Il recente scandalo di Cambridge Analytica, la società di consulenza britannica divenuta celebre per aver utilizzato i dati ottenuti da Facebook per influenzare diverse campagne elettorali, costituisce un esempio dei problemi che possono sorgere quando una entità centralizzata gestisce una così grande mole di dati. In seguito ad episodi come questo, accaduti anche in tempi meno recenti, negli ultimi anni si è assistito ad una spinta sempre più decisa verso la transizione a sistemi in cui il controllo del sistema stesso sia distribuito tra molteplici entità.

Un sistema informativo distribuito è caratterizzato da un insieme di nodi collegati da una rete informatica che cooperano, in modo autonomo, per mantenere le informazioni rilevanti per una certa applicazione. Ogni nodo può quindi elaborarle, senza l'ausilio di un server centralizzato che ne coordini il comportamento. Le informazioni gestite possono essere di interesse per un insieme di entità amministrative, ad esempio un consorzio di Enti pubblici e/o enti/industrie private. In alternativa, le informazioni possono essere condivise su scala globale, ad esempio nel caso delle criptomonete.

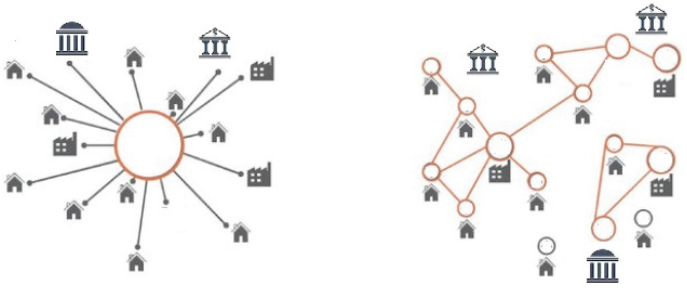

Figura 1. Struttura di sistemi informatici centralizzati e distribuiti.

Nella parte destra della Figura 1, è mostrata la struttura di un sistema distribuito. Come è facile notare, i nodi corrispondenti ai diversi utenti del sistema cooperano al mantenimento del suo stato senza la presenza di un'unica entità centralizzata. Questo implica che ogni nodo deve avere capacità di auto-organizzazione. L'idea della distribuzione del controllo del sistema è alla base della tecnologia delle blockchain, che rappresentano uno dei modi possibili per realizzare questo tipo di sistemi.

2. Le blockchain: concetti di base

La tecnologia alla base delle blockchain è complessa ed affascinante allo stesso tempo. Per introdurne i principi, ricorreremo quindi ad un esempio

che fa riferimento ad uno scenario realistico, anche se molto semplificato rispetto alla realtà.

Consideriamo quindi il caso in cui istituti bancari internazionali indipendenti e con sedi in paesi diversi, ad esempio *Barclays*, *Santander*, *UBS*, interagiscano per trasferire tra di loro diversi tipi di asset. Ogni istituto può utilizzare sistemi informatici propri basati su tecnologie diverse, spesso proprietarie. Spesso un ente terzo si occupa di offrire un protocollo per l'interscambio.

Semplificando la situazione reale, immaginiamo che ogni istituto registri in un proprio *libro mastro* o *"ledger"* tutte le operazioni di trasferimento verso gli altri istituti. Ad esempio, in Fig.2 viene mostrato il trasferimento di una somma di 500 $, da Barclays a USB, e la rispettiva registrazione nel libro mastro privato di USB.

JOURNAL -ID	DATESTAMP	FROM	TO	CURRENCY	AMOUNT
1	03/01/2020	Barclays	USB	$	500

Figura 2. Trasferimenti di Asset.

La stessa transazione comparirà in diversi "libri mastri", ad esempio la transazione mostrate in Figura 2 sarà registrata simmetricamente anche nel libro mastro di Barclays. Un requisito essenziale per il corretto funzionamento del sistema è quello della *consistenza* tra le informazioni registrate dai diversi istituti: chi assicura che una transazione sia registrata in modo coerente nei diversi ledger? Una soluzione che preveda audit da parte di terze parti, presenta almeno due problemi: la presenza di una terza parte di cui le parti si devono necessariamente fidare e la difficoltà del processo di auditing, dovuta alla necessità di accedere a sistemi informativi realizzati con tecnologie diverse. Un ulteriore problema riguarda la lentezza dei processi: nei sistemi attuali, se gli istituti bancari non aderiscono ad uno stesso protocollo di trasferimento, il processo può richiedere anche alcuni giorni.

Vediamo ora come la tecnologia delle blockchain contribuisca a superare questi problemi.

Immaginiamo di fondere i ledger dei diversi istituti in un unico ledger in cui ogni transazione compaia una sola volta, identificata in modo univoco. Il ledger risultante è mostrato nella parte alta della Figura 3.

A questo punto, supponiamo di distribuire le transazioni contenute nell'unico ledger in un insieme di blocchi, come mostrato nella parte bassa

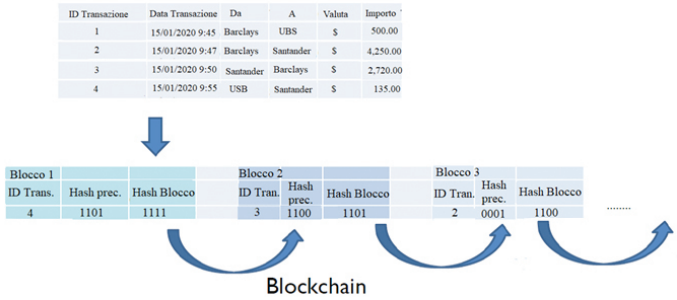

Figura 3. Distribuzione delle transazioni in blocchi.

della Figura 3. È importante notare che la figura presenta uno scenario semplificato, in cui ogni blocco contiene una sola transazione, mentre, nel caso più generale, più transazioni fanno parte di un blocco. I blocchi risultanti vengono collegati tra di loro mediante collegamento, che tecnicamente viene indicato come puntatore hash, la sua funzione verrà discussa più in dettaglio nel paragrafo successivo. La catena di blocchi viene detta *blockchain*.

A questo punto esiste un unico ledger, memorizzato in una blockchain. Il passo successivo consiste nel far in modo che tutti gli istituti abbiano una copia *replicata* e *consistente* della blockchain. Tutte le copie vengono mantenute uguali, in maniera automatica, mediante l'esecuzione di algoritmi distribuiti. La situazione risultante è mostrata in Figura 4.

La blockchain replicata gode di alcune proprietà, che elenchiamo:

— *Append-only*: i blocchi vengono aggiunti alla struttura, uno alla volta ed ogni blocco può essere aggiunto solo dopo il blocco precedentemente inserito. Nell'esempio, l'ultimo blocco inserito nella struttura è quello con identificatore 3, corrispondente all'ultima transazione inserita nel ledger. Non è possibile, ad esempio, inserire un blocco a metà del ledger, o in qualsiasi altra posizione. Per questa ragione la struttura viene detta *"append only"*, intendendo con questo termine che non è possibile aggiungere blocchi in un punto qualsiasi della struttura, ma solo aggiungere blocchi a quelli memorizzati in precedenza.
— *Tamper-freeness*: una volta che i blocchi vengono inseriti, essi non possono essere successivamente modificati, risultando così *immutabili*
— *Consistenza:* tutti i nodi della rete possiedono esattamente la stessa copia della blockchain, che è quindi replicata identica su ogni nodo. Per garantire questa proprietà occorre che un blocco venga aggiunto alla blockchain solo quando tutti i nodi hanno acconsentito al suo inserimento nella blockchain. Questo viene garantito da un *algoritmo*

di consenso, che garantisce che tutti i nodi posseggano la stessa copia della blockchain. È importante notare che questa proprietà può essere garantita se e solo se la maggioranza di nodi seguono correttamente le regole che governano il sistema e non si comportano quindi in modo "malizioso".

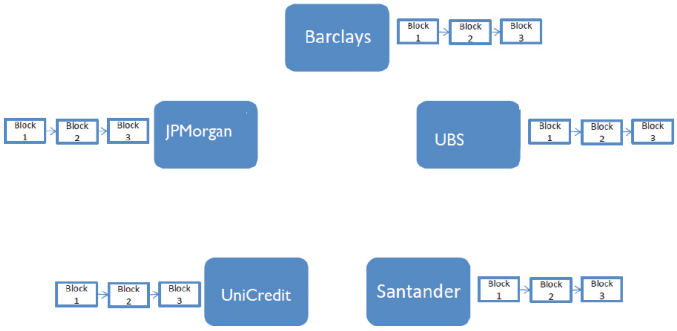

Figura 4. La Blockchain.

3. Blockchain: tecnologia di base

In questo paragrafo approfondiamo le tecnologie necessarie per definire una struttura che garantisca le proprietà introdotte nel paragrafo precedente.

3.1. *Tamper Freeness*

Per garantire questa proprietà si sfruttano le *funzioni hash*, ovvero particolari funzioni matematiche. Ricordiamo che una funzione matematica è una corrispondenza tra valori tale che, per ogni valore in ingresso, restituisce uno ed un solo valore in uscita. Una funzione hash è una funzione matematica che calcola un *fingerprint*, ovvero una *"impronta digitale"* dei dati e gode delle seguenti proprietà:

— ogni *fingerprint ha la stessa lunghezza*, indipendentemente dalla lunghezza del dato di cui si vuol calcolare il fingerprint. Infatti, la funzione restituisce sempre in uscita una sequenza di caratteri di lunghezza fissa. Ad esempio, il fingerprint dell'intera Divina Commedia e quello del nome di una città italiana sono sequenza di caratteri della stessa lunghezza.

Esistono diversi tipi di funzioni hash, ad esempio lo SHA-256, in cui il valore in uscita è una sequenza di caratteri esadecimali di 256 caratteri, qualsiasi sia il valore in ingresso.

— il *fingerprint è unico*. Supponiamo di applicare la funzione hash a due immagini che differiscono solo per un dettaglio. Si consideri, ad esempio, la Fig. 5.: nella parte sinistra viene mostrata l'immagine di un cane, in formato jpg, nella parte destra la stessa immagine a cui è stata apportata solo una piccola modifica: è stato tolto un baffo al cane. Si può notare come questo minimo cambiamento generi un valore del fingerprint completamente diverso.
— *non invertibilità*: è molto difficile risalire dal valore del fingerprint, (A3FX56748 in Fig.5) al valore in ingresso, (l'immagine del cane). Questo significa che risolvere questo problema, cioè risalire all'immagine dal suo hash, richiederebbe l'uso di risorse computazionali elevate e, comunque, molto grande, con i computer attuali.

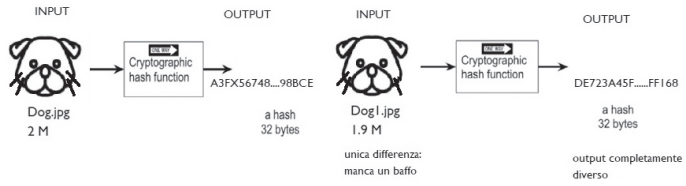

Figura 5. Fingerprinting mediante hash.

Le funzioni hash sono la base per garantire la proprietà di tamper freeness della blockchain. Consideriamo di nuovo la blockchain mostrata in Figura 3. Per ogni blocco della blockchain si calcola il rispettivo hash, che in figura viene rappresentato come una sequenza di cifre binarie: si considerano tutte le transazioni appartenenti ad un blocco, se ne calcola l'hash e si ricava un fingerprint del blocco. È importante notare che in ogni blocco della blockchain viene memorizzato anche l'hash del blocco precedente: ad esempio nel blocco con identificatore 4 viene memorizzata il valore 1101, che è proprio l'hash del blocco che lo precede nella blockchain.

Immaginiamo ora che un utente malintenzionato tenti di modificare il contenuto di un qualsiasi blocco della blockchain ed analizziamo come questa modifica risulterebbe facilmente rilevabile. Abbiamo visto che l'hash del blocco cambia completamente in seguito anche a piccole modifiche del contenuto del blocco. Poiché l'hash di un blocco è memorizzato nel blocco successivo della blockchain, la modifica può essere immediatamente

rilevata confrontando i valori dei due hash. Ovviamente l'attaccante potrebbe ricalcolare anche l'hash del blocco successivo, inserendo nel blocco il valore modificato dell'hash del blocco precedente e così via. In generale, per oscurare completamente la modifica effettuata in un blocco della blockchain, sarebbe necessario ricalcolare l'hash per tutti i blocchi che seguono il blocco modificato. Inoltre, ogni blocco dovrebbe essere di nuovo approvato dagli altri nodi appartenenti alla rete, mediante l'algoritmo di consenso. Questo risulta non realistico, in quanto comporterebbe un costo computazionale molto alto.

3.2. *Consenso*

Il processo con cui i nodi (computer) della rete mantengono la consistenza della blockchain viene indicato come *consenso*. Per spiegare tale processo, consideriamo la figura 6. Immaginiamo che tutti i nodi della rete posseggano una blockchain consistente (a sinistra in Fig. 6), cioè replicata in modo esattamente uguale in ogni nodo. Ogni nuova transazione viene inviata a tutti gli altri nodi nella rete, che tuttavia non la inseriscono direttamente nella blockchain, ma la memorizzano temporaneamente in un contenitore. Le transazioni in attesa di validazione sono quelle mostrate nella "nuvola" nella parte destra della figura 6.

Prima di inserire la transazione nella blockchain (come abbiamo visto l'inserimento è un'azione irreversibile) è necessario che la transazione sia approvata da tutti i nodi della rete, mediante un procedimento indicato come *consenso*. Un *algoritmo di* consenso è una procedura eseguita da tutti i nodi della rete per prendere una decisione comune e condivisa circa quali transazioni inserire nella blockchain ed in quale ordine inserirle.

Ogni blockchain è caratterizzata da un proprio algoritmo di consenso. La forma più nota di consenso è quella proposta originariamente per Bitcoin che prevede che i nodi partecipino ad una "lotteria". Il vincitore della lotteria decide quale transazione deve essere inserita nella blockchain. Nel caso di Bitcoin, la lotteria viene realizzata con il meccanismo della Proof of Work (PoW). In pratica, i nodi devono risolvere un problema molto difficile, dal punto di vista computazionale, ed il primo nodo che riesce a risolverlo è il vincitore della lotteria e decide quale transazione inserire nella blockchain. Il consenso basato su PoW, viene indicato come *mining*. Meccanismi di questo tipo sono utilizzati generalmente in blockchain permissionless (vedi paragrafo successivo), quali quelle di Bitcoin o di Ethereum. Blockchain di tipo permissioned, come HypeLedger, utilizzano invece meccanismi basati su *votazione esplicita*, come algoritmi basati su Byzantine Fault Tolerance.

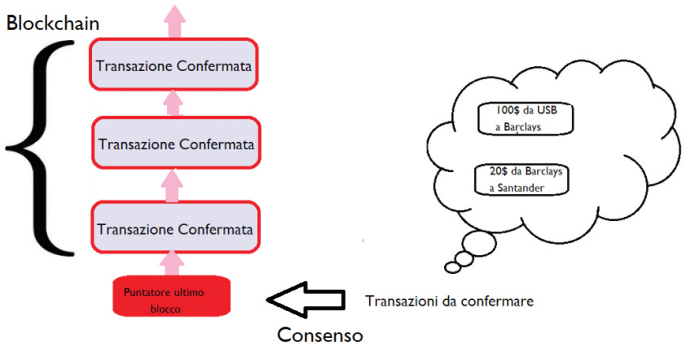

Figura 6. Conferma di transazioni tramite consenso.

4. Blockchain: una tassonomia delle proposte esistenti

Anche se la tecnologia delle blockchain è molto recente, negli ultimi anni è stata declinata in modi diversi per la realizzazione di sistemi che presentano requisiti diversi. Tutte le blockchain proposte sono comunque basate sui principi generali illustrati nel paragrafo precedente.

A partire da Bitcoin, l'applicazione che per prima ha realizzato una criptovaluta basata su blockchain, sono stati successivamente considerati scenari applicativi diversi, il cui denominatore comune è quello di offrire un servizio in cui transazioni di tipo diverso possono essere notarizzate sulla blockchain, in un ambiente in cui i diversi attori operano senza poter contare su una terza parte fidata e senza alcuna garanzia di fiducia reciproca.

Se pur ancora oggetto di dibattito, i sistemi basati su blockchain sono stati classificati sulla base del sul livello di accessibilità dei dati memorizzati sulla blockchain (blockchain *pubbliche* e *private*), e sulla autorizzazione necessaria per aggiungere dati alla blockchain (blockchain *permissioned* o *permissionless*).

In particolare, la tassonomia si basa sulle regole con cui si permette l'accesso alle operazioni che un utente può effettuare su una blockchain, queste operazioni sono:

— *leggere* i dati memorizzati sulla blockchain
— *sottomettere transazioni*, che successivamente devono essere approvate dall'algoritmo di consenso, per essere quindi memorizzate sulla blockchain
— *aggiornare lo stato della* blockchain inserendo nuove transazioni, partecipando alla procedura di consenso distribuito.