

# Blockchain: aspetti giuridici tra dati, numeri e algoritmi

Fernanda Faini

Università Telematica Internazionale Uninettuno

**Abstract.** Nell'affascinante rapporto che lega tecnologia e diritto, il contributo intende affrontare il fenomeno della blockchain sotto la lente giuridica. A tal fine l'analisi, dopo aver esaminato le caratteristiche che connotano tale tecnologia, tratta gli aspetti giuridici e il contesto normativo europeo e nazionale di riferimento. Il contributo si concentra su alcuni profili particolarmente complessi di interazione della tecnologia blockchain con principi e norme esistenti a tutela dei diritti e dei valori dei nostri ordinamenti, in specifico la disciplina in materia di data protection.

**Keywords.** diritto; blockchain; distributed ledger technology; smart contract; data protection

## Introduzione

Il contributo intende esaminare il rapporto che lega blockchain e diritto, mettendo in luce il quadro normativo di riferimento ed analizzando alcuni profili particolarmente significativi di tale tecnologia, che sollevano problematiche nell'interazione con normative già esistenti a tutela dei diritti, in specifico la disciplina in materia di data protection. Al fine di esaminare la relazione tra scienza giuridica e tecnologia blockchain è necessaria una premessa: in tal caso, come negli altri in cui si confronta con la tecnologia, il diritto è chiamato a dialogare con altri insiemi di regole, in particolare la *lex informatica* o *digitalis*, ossia le regole informatiche; il codice giuridico deve interagire con quello algoritmico per poter essere efficace.

Le regole informatiche, infatti, condizionano i comportamenti umani, dal momento che abilitano azioni e interazioni, collegano effetti, determinano quali informazioni fornire all'utente: la *lex informatica* è capace di condizionare ogni altra forma di regolazione, compresa quella giuridica. Di conseguenza il diritto è chiamato a intervenire sulla tecnologia: ciò che è giuridicamente legittimo deve essere un sottoinsieme del tecnologicamente possibile, al fine di rispettare i principi dell'ordinamento e tutelare i diritti. A tal fine il diritto può decidere di avvalersi della stessa tecnologia, prevedendo misure tecniche capaci di disabilitare azioni illecite.

Pertanto, nel complesso rapporto tra blockchain e diritto, il giurista deve muoversi come un abile equilibrista: la tecnologia non deve prevalere sul diritto, ma il diritto non deve limitare le potenzialità della tecnologia, non solo perché in tal modo non svolgerebbe in modo adeguato la funzione di regolazione, ma anche perché rischierebbe di votarsi all'inefficacia e al mancato rispetto (Finocchiaro 2012; Sartor 2010).

## **1. Tecnologia e diritto**

### **1.1 Aspetti tecnologici**

Alla luce di quanto espresso in premessa, l'analisi giuridica della blockchain deve necessariamente muovere dall'oggetto della regolazione, da ciò che si vuole regolare e, pertanto, dalle caratteristiche della tecnologia blockchain. L'osservazione della tecnologia è necessaria perché proprio nelle sue caratteristiche, come sarà più avanti esaminato, emergono alcune criticità per il diritto.

Seppur con una inevitabile dose di semplificazione, le tecnologie basate su registri distribuiti (distributed ledger technologies o DLT) e la blockchain, species del genus DLT che impiega una catena di blocchi, si caratterizzano principalmente per i seguenti aspetti: disintermediazione, decentralizzazione e distribuzione; immodificabilità, inalterabilità e persistenza dei dati; meccanismo peer-to-peer alternativo di fiducia, consenso e incentivazione; trasparenza, tracciabilità e sicurezza; funzioni di hash, crittografia asimmetrica e validazione temporale (Giuliano 2018).

Tali caratteristiche si attecchiano in maniera diversa nelle diverse tipologie di blockchain, a seconda che si tratti di blockchain permissionless, che si distinguono per essere aperte e liberamente accessibili a chiunque senza autorizzazioni (es. Bitcoin), oppure blockchain permissioned, che hanno la caratteristica di essere chiuse e non accessibili pubblicamente, dal momento che le autorizzazioni sono gestite da un'autorità centrale, oppure, ancora, blockchain ibride, dette anche consorzi, che sono parzialmente decentrate, dal momento che esiste un controllo sul meccanismo di consenso da parte di alcuni nodi preselezionati, che hanno maggiore influenza degli altri (Gambino et al. 2019; Giuliano 2018; Sarzana et al. 2018).

### **1.2 Profili normativi**

Passando dagli aspetti tecnologici ai profili giuridici, le caratteristiche e gli obiettivi che la blockchain permette di perseguire emergono negli atti di riferimento europei e nazionali. A livello sovranazionale, rileva la risoluzione del Parlamento europeo del 3 ottobre 2018 sulle «tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione». Secondo la risoluzione, tali tecnologie sono in grado di migliorare l'efficienza dei costi delle transazioni, oltre ad aumentarne la trasparenza; tale paradigma informatico può democratizzare i dati e rafforzare la fiducia, fornendo un percorso sicuro ed efficace per l'esecuzione delle transazioni. L'Unione europea però chiarisce esplicitamente che i rischi e i problemi di tale tecnologia non sono ancora completamente noti.

A livello europeo rileva, altresì, l'istituzione da parte della Commissione europea del EU Blockchain Observatory and Forum nel febbraio 2018 e dell'European Blockchain Partnership nell'aprile 2018.

A livello nazionale, l'art. 8-ter del d.l. 135/2018, convertito dalla legge 12/2019, si occupa di definire le tecnologie basate su registri distribuiti e lo smart contract. Le «tecnologie basate su registri distribuiti» (DLT), tra le quali rientra la blockchain, sono definite dalla norma, che riprende le caratteristiche tecnologiche sopra esaminate, come «le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, repli-

cabile, accessibile simultaneamente, architetturealmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili».

La disposizione chiarisce che la memorizzazione di un documento informatico attraverso l'uso di DLT produce gli effetti giuridici della validazione temporale elettronica di cui all'art. 41 del regolamento UE n. 910/2014. Ai fini della produzione di tali effetti le DLT devono possedere gli standard tecnici individuati dall'Agenzia per l'Italia digitale (AgID). Il secondo comma dell'art. 8-ter definisce lo "smart contract", significativa applicazione della blockchain, come «un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse».

Anche in tal caso, come per le DLT, la norma collega gli effetti giuridici, specificando che lo smart contract soddisfa il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'AgID con linee guida (Bomprezzi 2019).

Nelle caratteristiche che normativamente definiscono lo smart contract si scorge un'evoluzione del contratto automatico (es. il distributore automatico di bevande): in tal caso si aggiunge la piena disintermediazione umana e la qualificazione normativa oscilla tra software e documento informatico. Il fatto che lo smart contract configuri un documento informatico comporta la necessità del rispetto delle norme europee e nazionali di riferimento, ossia in particolare il regolamento eIDAS n. 910/2014, il codice civile, il d.lgs. 82/2005 (Codice dell'Amministrazione Digitale) e le relative regole tecniche.

A livello strategico, in Italia è stato nominato dal Ministero dello Sviluppo Economico un gruppo di esperti, formato da 30 profili multidisciplinari, con l'obiettivo di elaborare una strategia nazionale in materia di tecnologie basate su registri distribuiti e blockchain.

## 2. Blockchain e data protection

Per quanto riguarda l'impiego della blockchain, uno dei profili di maggiore criticità è costituito dal rispetto della disciplina in materia di data protection, di cui al regolamento UE 2016/679 e alla normativa italiana (d.lgs. 196/2003 come modificato dal d.lgs. 101/2018). In premessa è opportuno rilevare che nella blockchain la funzione di hash può essere fatta rientrare in un'operazione di pseudonimizzazione, di cui all'art. 4, par. 1, n. 5, del regolamento UE 2016/679, che come tale comporta l'applicazione della normativa in materia di protezione dei dati personali.

Di conseguenza, in caso di utilizzo della blockchain, laddove siano presenti dati personali, è necessario il rispetto dei principi applicabili al trattamento previsti dalla normativa, in specifico dall'art. 5 del regolamento UE 2016/679, tra i quali rilevano ai fini di tale analisi la minimizzazione dei dati (i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati) e la limitazione della conservazione (i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le

quali sono trattati).

In considerazione delle esaminate caratteristiche tecniche, la blockchain configge con il rispetto di tali principi: sotto il profilo della minimizzazione dei dati, la difficoltà sta nel fatto che la blockchain per il suo funzionamento replica i dati nei vari nodi e, sotto il principio della conservazione, come precisato anche nella norma italiana, i dati nella blockchain sono «non alterabili e non modificabili». Tali aspetti costituiscono indubbiamente punti di forza di tale tecnologia, ma rischiano di trasformarsi in aspetti di debolezza capaci di creare complesse problematiche al cospetto dei principi in materia di data protection (Gambino et al. 2019).

La normativa in materia di protezione dei dati personali individua alcuni soggetti di riferimento della disciplina: in particolare, accanto all'interessato a cui i dati personali si riferiscono, il titolare, ossia la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, che, singolarmente o insieme ad altri titolari, determina le finalità e i mezzi del trattamento, e il responsabile, eventualmente preposto dal titolare (art. 4, reg. UE 2016/679). L'individuazione di tali figure è fondamentale nella disciplina, dal momento che a tali soggetti si applicano obblighi necessari a garantire la tutela della persona e dei suoi dati, come il principio di responsabilizzazione, secondo cui il titolare è competente per il rispetto dei principi e deve essere in grado di provarlo (art. 5, par. 2, reg. UE 2016/679).

In tal caso rileva la tipologia di blockchain, dal momento che nelle permissioned è individuabile il titolare e nel caso dei consorzi si può fare leva sulla norma relativa alla contitolarità (art. 26, reg. UE 2016/679), ma nelle permissionless diventa complesso individuare tali figure: tutti i nodi devono essere considerati contitolari? Non è presente nessun titolare? In tal caso come trova applicazione la disciplina? (Gambino et al. 2019; Giuliano 2018).

Insieme al necessario rispetto dei principi e all'individuazione delle figure di riferimento, è necessario garantire i diritti dell'interessato, che spaziano nel regolamento europeo 2016/679 dall'accesso (art. 15) alla rettifica (art. 16), dalla cancellazione (art. 17) alla limitazione di trattamento (art. 18), dall'opposizione (art. 21) al non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (art. 22). In considerazione delle richiamate caratteristiche di immutabilità, inalterabilità e persistenza dei dati, nella tecnologia blockchain diventano difficili la modifica, la rettifica, l'opposizione e la cancellazione dei dati stessi e, di conseguenza, il rispetto di tali diritti dell'interessato (Paladino 2019).

### 3. Conclusioni

In considerazione degli ambiti presi in considerazione emergono alcune complesse criticità nel rapporto tra blockchain e diritto. Per quanto attiene all'aspetto documentale e agli smart contracts, risulta necessario un maggiore coordinamento tra la norma italiana dedicata alla blockchain e il quadro di regolazione europea e nazionale in materia di documenti informatici. Sotto tale profilo, particolare rilevanza assumono le linee guida e gli standard tecnici cui è chiamata l'AgID per dare contenuto ai principi posti dalla norma.

Sotto il profilo della data protection, al fine di superare le problematiche esaminate, una direzione è individuabile nell'approccio sistematico, preventivo, proattivo e tecnico, previ-

sto dal regolamento UE 2016/679, che si traduce nell'incorporazione dei principi e delle norme nella tecnica, facendo assolvere al diritto la funzione preventiva che gli spetta: la regolazione giuridica può servirsi della tecnologia, adattandola al fine di garantire il suo rispetto.

La blockchain mostra sicuramente sfide inedite per il diritto, che è necessario affrontare per far esplodere il valore che tale tecnologia è in grado di esprimere. I nodi aperti e la necessità di rispettare i principi e i valori giuridici di riferimento evidenziano l'importanza della capacità umana di orientare la tecnologia: qualunque evoluzione tecnologica da sola non è sufficiente se non è accompagnata anche dallo strumento del diritto, che da sempre costituisce il mezzo con cui l'uomo regola la società.

### Riferimenti bibliografici

Bomprezzi C. (2019), Commento in materia di Blockchain e Smart contract alla luce del nuovo Decreto Semplificazioni, in *Diritto, mercato, tecnologia*, pp. 1-7.

Finocchiaro G. (2012), Riflessioni su diritto e tecnica, in *Il diritto dell'informazione e dell'informatica* (4-5), pp. 831-840.

Gambino A.M., Bomprezzi C. (2019), Blockchain e protezione dei dati personali, in *Il diritto dell'informazione e dell'informatica* (3), p. 619 ss.

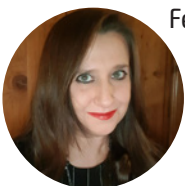
Giuliano M. (2018), La blockchain e gli smart contracts nell'innovazione del diritto nel terzo millennio, in *Il diritto dell'informazione e dell'informatica* (6), p. 989 ss.

Palladino A. (2019), L'equilibrio perduto della blockchain tra platform revolution e GDPR compliance, in *Rivista di diritto dei media* (2), pp. 144-158.

Sartor G. (2010), *L'informatica giuridica e le tecnologie dell'informazione. Corso di informatica giuridica*, II ed., Giappichelli, Torino.

Sarzana di S. Ippolito F., Nicotra M. (2018), *Diritto della blockchain, intelligenza artificiale e IoT*, Wolters Kluwer - Ipsoa, Milano.

### Autrice



**Fernanda Faini** - [fernandafaini@gmail.com](mailto:fernandafaini@gmail.com)

Docente di "Diritto e nuove tecnologie" presso l'Università Telematica Internazionale Uninettuno. Responsabile dell'assistenza giuridica in materia di amministrazione digitale, innovazione tecnologica e informatica giuridica presso la Regione Toscana. PhD in diritto e nuove tecnologie presso l'Università di Bologna, collabora nell'insegnamento di Informatica giuridica presso l'Università degli Studi di Firenze, dove è membro dello Steering Committee dell'Unità di ricerca "Babel – Blockchains and Artificial Intelligence for Business, Economics and Law". Membro del Gruppo di esperti in materia di tecnologie basate su registri distribuiti e blockchain del Ministero dello Sviluppo Economico.