

TECNOLOGIA E LEGGE

La blockchain è ancora in cerca di un passaporto giuridico

La validità giuridica della blockchain, inizialmente prevista nello schema del decreto legge Semplificazioni, è stata sfilata dal testo approvato la scorsa settimana (Dl 135/2018). La norma, che potrà essere "recuperata" più avanti, conteneva la definizione delle

tecnologie basate su registri condivisi e precisava gli effetti giuridici della marca temporale (*timestamp*) delle transazioni. Ma la tecnologia della "catena dei blocchi" richiede una riflessione sul quadro giuridico e normativo in generale.

Aquaro e Capaccioli — a pagina 5

Tecnologie e legge

Smart contract, identità digitale certa, criptovalute: occorre dare uno status giuridico qualificato ai «registri condivisi», ma per ora si è perso il treno del Dl semplificazioni

La blockchain cerca il passaporto legale

Dario Aquaro

La validità giuridica della blockchain, inizialmente prevista nello schema del Dl Semplificazioni, è stata spinta più in là. Sfilata dal decreto approvato la scorsa settimana dal Governo, se non verrà recuperata nel percorso parlamentare del provvedimento, o a sorpresa nella legge di Bilancio, potrà rientrare con il Ddl delega per ulteriori semplificazioni, riassetto normativi e codificazioni di settore.

La norma saltata conteneva la definizione delle tecnologie basate su registri condivisi (*distributed ledger technology*, Dlt), di cui fa parte anche la "catena dei blocchi". E precisava che la condivisione di un documento informatico via Dlt «produce gli effetti giuridici della validazione temporale elettronica» ex articolo 41 del Regolamento Ue 910/2014: una validazione "semplice", che rende giuridicamente certa la data e l'ora dei dati in forma elettronica (il *timestamp*, la marca temporale della transazione) e garantisce «l'ammissibilità come prova in procedimenti giudiziari».

Ma al di là delle definizioni e dell'accenno a uno "status", la tecnologia della blockchain – nelle sue diverse forme (aperta o chiusa, privata o pubblica) – richiede un approfondimento sul quadro giuridico e normativo generale, che tenga conto dei vari modelli applicabili. «La norma espunta non era comunque dirimente – osserva Michele Nastro, presidente di Notartel, società informatica dei notai italiani –. Certo si trattava di un'apertura verso queste tecnologie, che però venivano inserite al livello più basso, non in quello della validazione "qualificata"». Per quest'ultima,

infatti, le regole europee richiedono particolari requisiti, tra cui l'intervento di un «prestatore di servizi fiduciari qualificato», con importanti riflessi sul "peso" stesso della prova.

Gli esempi di Dlt richiamati nella relazione illustrativa allo schema di decreto spaziavano dalla gestione e archiviazione di documenti (passaporti, certificati anagrafici) o di registri (aziendali, personali, scolastici) alla riscossione delle imposte, dall'identità digitale agli *smart contract*. Mettendo così insieme applicazioni con diverse "valenze" e necessità probatorie: un conto è dimostrare la titolarità del diritto d'autore, un altro la cosiddetta "tokenizzazione" di un asset (come un immobile).

A fine settembre l'Italia, dove il ministero dello Sviluppo economico ha organizzato dei tavoli di lavoro sulla "catena dei blocchi", ha aderito all'European blockchain partnership che era stata lanciata dalla Commissione Ue ad aprile. Ma nella corsa che si sta aprendo tra le proposte dei singoli Stati (si veda l'articolo in basso) nasce anche l'esigenza di una riflessione interna *tout court* sulle regole tecniche. E in particolare sullo *smart contract*, «che rimane un atto giuridico-negoziale e non può non essere normato dallo Stato», come dice il notaio Nastro: anche se «l'intervento umano può essere sostituito solo in atti serializzati e dove l'eventuale esecuzione sbagliata sia gestibile con piccoli risarcimenti».

Dare valore legale "compiuto" ai registri distribuiti sarebbe un grande passo in avanti. «Occorre però chiarire, ad esempio, chi garantisce la certezza del dato immesso, che diventa immutabile – spiega l'avvocato Stefano Loconte, esperto della materia –. La risposta può essere l'intervento di un ente certificatore terzo e indipendente, che a sua volta si avvalga di un modello decentralizzato». Una sorta di meta-

blockchain come quella che, su più livelli, sta esplorando il Notariato, che si propone anche in un ruolo di garanzia per le reti pubbliche. «Per favorire e diffondere l'adozione dei servizi di notarizzazione su blockchain *permissionless*, che

tuttora presentano dei limiti tecnici – commenta Leonardo Maria De Rossi, research fellow di Information system alla Sda Bocconi –, è però necessario innanzitutto definire uno standard di riferimento e attribuirgli validità legale».

© RIPRODUZIONE RISERVATA

LE REGOLE DEGLI ALTRI

La Francia ora fa le cose sul serio

Stefano Capaccioli

Nell'Unione europea c'è chi cerca di imbrigliare la blockchain in quadri regolamentari che diminuiscono l'incertezza per le imprese, mentre a livello di istituzioni europee prevale la necessità di approfondimenti e di informazioni, anche grazie all'iniziativa European Blockchain Observatory and Forum della DG Cnect e alla Risoluzione del Parlamento Europeo di ottobre. Tali attività rischiano di portare alla frammentazione del quadro giuridico in Europa, in assenza di una strategia comune e in previsione dell'uscita del Regno Unito, che potrebbe scatenare la concorrenza normativa tra Paesi membri, con particolare fermento in Francia e a Malta.

Parigi sta lavorando alacremente sul lato normativo dell'innovazione delle criptoattività e sulle potenzialità derivanti dai sistemi blockchain. France Stratégie, l'istituzione di supporto al Primo ministro per gli indirizzi strategici, ha avviato il progetto con la costituzione nel maggio 2017 di un gruppo di lavoro che ha svolto numerose riunioni ed audizioni. Tale lavoro ha coinvolto istituzioni pubbliche e private, in uno sforzo collettivo iniziato nel 2014 con il primo rapporto del Senato sulle valute virtuali e che sta producendo interpretazioni e proposte di riforma che contemperino le esigenze pubbliche con quelle private. Lo scorso giugno Camera e Senato hanno pubblicato un rapporto sulle "Sfide tecnologiche della blockchain" ed è in corso di completamento la riforma per un quadro giuridico sulle Ico.

Le istituzioni di Malta hanno approvato poco più di un mese fa tre nuovi provvedimenti per poter creare sull'isola un centro di attrazione di eccellenza. I provvedimenti comprendono il "Virtual Currencies Act", per regolamentare le Ico soggette ad autorizzazione e i token che, in base al Financial Instruments Test, sono da considerarsi strumenti finanziari, e il "Technology Arrangement Bill", teso a creare una riconoscibilità giuridica alle soluzioni tecnologiche innovative e alla creazione della "Malta Digital Innovation Authority", principale responsabile dell'impulso di tutte le politiche che promuovono Malta come centro di eccellenza per l'innovazione tecnologica.

In assenza di una strategia definita che può basarsi esclusivamente su un'analisi che coinvolga tutti gli attori, l'Italia rischia di rimanere indietro: azioni e approfondimenti di qualche organo dello Stato rischiano di restare isolate e infeconde in assenza di un disegno complessivo.

© RIPRODUZIONE RISERVATA

COME FUNZIONA LA BLOCKCHAIN

La catena

Tecnologia di registri condivisi

- La blockchain è un database decentralizzato, strutturato in blocchi e distribuito in un network.
- La rete dei dispositivi interconnessi (nodi) forma un registro digitale condiviso (ledger), riprodotto su tutti i dispositivi-nodi

I blocchi

Sequenza di numeri certificata

- Ogni blocco è identificato da un hash (un numero composto da 256 bit), generato da un algoritmo sulla base delle regole del network
- Il blocco contiene l'intestazione, il riferimento all'hash del blocco precedente e un gruppo di transazioni

L'algoritmo

Validazione per poter fare l'aggiunta

- I blocchi devono essere validati per poter essere aggiunti alla catena (da ogni nodo)
- La validazione dei blocchi è fatta da miner (minatori) tramite complessi algoritmi matematici, per giungere alla certezza di immutabilità dei dati inseriti

La sicurezza

Rifiutati tutti i dati irregolari

- Ogni blocco validato, con marca temporale (timestamp), è aggregato agli altri in una catena lineare e aggiornata
- Se un hacker cerca di aggiungere un blocco contraffatto gli altri nodi della rete registrano le modifiche e rifiutano l'hash irregolare



L'Italia ha aderito a fine settembre alla recente European blockchain partnership lanciata dalla Ue

LE POTENZIALI APPLICAZIONI (E I LIMITI)

1 IDENTITÀ DIGITALE

Realizzare un sistema di identità digitale su blockchain significa consentire a una serie di soggetti autorizzati di agire da validatori dei documenti d'identità: non solo lo Stato (con Spid, anagrafe, eccetera), ma anche banche o assicurazioni. La categorizzazione di diverse tipologie di dati personali, inoltre, permette al

cittadino di conoscere sempre l'entità delle informazioni condivise con enti terzi e tracciarne i successivi utilizzi. Il sistema consente l'implementazione di servizi accessori come il voto digitale, garantendo trasparenza e sicurezza. Il principale limite sta nella mancanza di sistemi di riconoscimento biometrico completamente affidabili.

Malta ha approvato circa un mese fa tre provvedimenti per creare un centro di attrazione «dedicato»

2 SERVIZI DI «NOTARIZZAZIONE»

Nelle blockchain pubbliche e aperte, all'interno di una micro-transazione si può salvare l'hash di un documento (l'impronta digitale crittografata, immutabile e trasparente). Chiunque può verificare che l'hash corrisponda al documento sottoposto alla marcatura temporale (o timestamping). Un tale servizio di notarizzazione può essere

usato nei registri centralizzati che richiedono elevati livelli di affidabilità e trasparenza (come il procurement della Pa). Tuttavia, il timestamping di per sé non garantisce la correttezza del documento: se l'auditing non avviene in real-time, è possibile inserire in seguito hash di documenti diversi ma salvati allo stesso tempo dell'originale.

3 SERVIZI BANCARI DECENTRALIZZATI

Le criptovalute abilitano due processi: l'invio e la ricezione di transazioni di unità di valore in maniera peer-to-peer fra gli utenti di uno stesso network. La diversa combinazione può dare vita a diverse soluzioni finanziarie: ad esempio, per le "rimesse" internazionali (spesso ignorate dal mondo bancario

tradizionale) e le piattaforme di prestito P2P (associando direttamente mutuatari e prestatori privati, con un sistema di credit scoring). I servizi realizzati finora hanno però patito le stesse limitazioni delle criptovalute su cui si basano, in termini di alta volatilità e mancanza di regolamentazione.

Schede a cura di **Leonardo Maria De Rossi** e **Nico Abbatemarco**, Sda Bocconi (School of management)