Associazione Blockchain Italia

Francesco Rampone
Presidente Associazione Blockchain Italia

25 dicembre 2019

Ecologia delle parole e blockchain

Hype e falsi miti

Sulla blockchain c'è molto, troppo entusiasmo, e l'entusiasmo non è buon viatico per chi vuole studiare il fenomeno con rigore scientifico. Il rischio è di perdere tempo in inutile ricerca. La certezza è di fare pessima informazione.

I falsi miti generati da questo approccio fideistico e markettaro producono progetti fallimentari in cui anche grandi imprese hanno investito e dei quali, a parte un po' di pubblicità (non a buon mercato), è rimasto ben poco.

Per prendere le distanze da tutto questo, e per riconquistare un più sobrio approccio laico, vorrei fare un po' di ecologia delle parole (e dei concetti) restituendo ad esse il corretto significato e l'ambito che meritano.

Autenticazione e certificazione.

Autenticare, certificare, validare, verificare, sono verbi utilizzati in modo promiscuo quando si vuole spiegare cosa fa una blockchain. Questo conduce a fraintendimenti sulle capacità di una blockchain e sui vantaggi che essa offre.

A dispetto di un'idea ricorrente, una blockchain in sé non autentica né certifica alcunché.

Autenticare un dato, vuol dire attribuire ad esso una specifica provenienza o fonte (un determinato ente o persona). Certificare un dato vuol dire attribuirgli status di verità per *decreto* emesso da un'autorità riconosciuta (pubblica o privata).

Ebbene, quanto all'autenticazione va detto che essa è già compiuta assai efficacemente con le firme digitali o con altro tipo di firma elettronica qualificata o avanzata (o altro processo avente i requisiti fissati dall'AgID *ex* art. 20 CAD, comma 1-*bis*); quindi, non serve affatto la blockchain[1]. Peraltro, la blockchain nasce soprattutto come soluzione anonima di scambio di

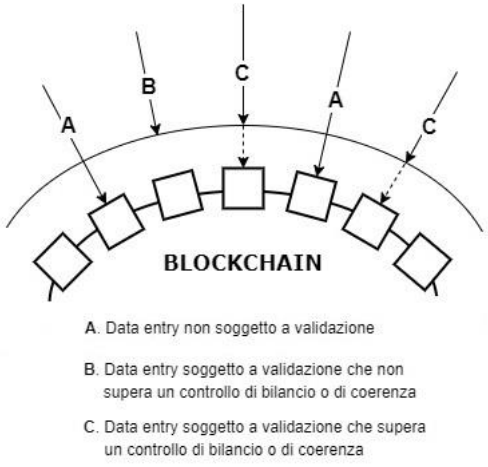
[1] Peraltro la firma digitale consente anche l'immodificabilità del testo sottoscritto, altra caratteristica erroneamente attribuita in via esclusiva alla blockchain.

rapporti di debito-credito. Il fatto che i bitcoin per circolare ricorrano ad una soluzione criptografica a chiave asimmetrica, anche utilizzata per le firme digitali, non significa che essi non siano anonimi. Sarebbe come dire che poiché le banconote hanno un numero di serie, allora non sono anonime. In entrambi i casi – bitcoin e banconote fisiche – vale il principio del *possesso vale titolo*. Nulla di più lontano dall'autenticazione.

Quanto alla *certificazione*, riconoscere questa proprietà alla blockchain vuol dire tradire lo spirito criptoanarchico alle sue origini. La vocazione peer-to-peer della blockchain rifugge dall'attribuzione di verità conferita da una autorità. La "verità" è invece ottenuta per validazione, ovvero attraverso lo sfruttamento della capacità del network di abilitare in ambiente informatico protocolli decisori a consenso distribuito.

(*Segue*) Validazione e verifica.

Validare un dato vuol dire verificarne la correttezza per effetto di mere operazioni matematiche o di riscontro per equivalenza, coerenza o congruità con altri dati[2]. Verificare un dato vuol dire sottoporlo a scrutinio diretto per accertarne lo status di verità; se con la *certificazione* ci affidiamo ad un terzo, con la verifica ci affidiamo al nostro giudizio.



Tenendo presenti le due definizioni precedenti, la peculiarità della blockchain sembra essere proprio quella di consentire al tempo stesso la validazione dei dati in ingresso e la possibilità di verificare quelli in uscita poiché gli algoritmi a cui sono sottoposti e i relativi output sono immodificabili e osservabili da chiunque. In altri termini, i dati che superano l'*orizzonte* della validazione "precipitano" nella blockchain e non ne escono più, possono così essere oggetto di smart contract in successive operazioni soggette a verifica[3].

Di converso, se i dati caricati in blockchain non sono soggetti a validazione o verifica, se cioè essi sono caricati sulla base di una mera attività di (auto)certificazione e la loro elaborazione non è trasparente (attraverso smart contract *on-chain*), che senso ha allora fare ricorso alla blockchain?

---

[2] Nel protocollo Bitcoin, per esempio, i dati sono sottoposti ad un controllo di bilancio contabile (il saldo di transazione, al netto del resto, deve essere zero). In altri protocolli si può ricorre a diversi tipi di bilancio, come quello di materia nel settore agroalimentare. Si tratta in entrambi i casi di validazioni all'ingresso dei dati. Ma la validazione può anche essere differita, cioè compiuta su dati già entrati in blockchain, ma sottoposti con degli smart contract ad un controllo di coerenza con altri dati, precedenti o successivi, che affidano loro un indice di attendibilità o attivano altre risposte al fine di garantire il rispetto del disciplinare. Ad esempio, il dato di produzione di un campo di grano deve essere coerente a monte con il dato di fattura dei fitofarmaci impiegati o con i dati meteo che vanno dalla semina al raccolto e, a valle, con i dati di logistica del vettore e di vendita del GDO. In caso di incoerenza, potrebbero scattare controlli o richieste di spiegazione da parte del consorzio titolare del marchio di qualità.

[3] La possibilità di verificare la correttezza delle operazioni compiute sui dati è un punto centrale. È stato messo bene a fuoco e definito «*Open Execution*» da E. DAMIANI *et al.*, *Open Execution—The Blockchain Model*, in *IEEE Blockchain Technical Briefs* (2018).

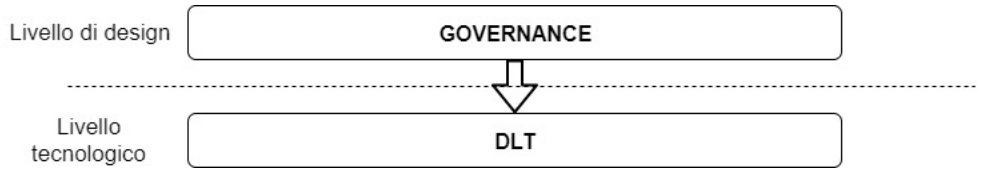
Non mi stupisce che, ignorando questa banale verità, molti progetti di tracciabilità su piattaforma blockchain si siano rivelati fasulli (ciò tuttavia non toglie che alcuni protocolli blockchain debbano correttamente fare uso di *data entry* di tipo A).

Blockchain vs DLT.

Blockchain è un termine che nasce dopo la pubblicazione del paper di Satoshi Nakamoto del 2008. Ma *blockchain* non è solo il design di Bitcoin, altrimenti non dovrebbe essere definita, ma solo descritta. Essa ha invece assunto un significato ampio di sottoclasse di DLT realizzate attraverso l'impiego di blocchi di dati concatenati gli uni agli altri attraverso soluzioni criptografiche[4]. La blockchain, pertanto, è innanzi tutto un registro che si aggiorna secondo un *protocollo distribuito*, e cioè attraverso un meccanismo di consenso peer-to-peer la cui esecuzione è verificabile da chiunque e i cui risultati sono pressoché immutabili[5].

Alla luce di ciò, non comprendo che senso abbiano altre dispute definitorie che vorrebbero distinguere tra DLT e blockchain, se non per mere ragioni tassonomiche.

Infatti, più che parlare dello strato tecnologico (DLT o blockchain), la vera distinzione attende alle condotte abilitate dalla tecnologia. L'attenzione, insomma, dovrebbe essere rivolta anziché alla sottostante tecnologia, allo strato superiore della *governance*. Con tale termine non intendo le regole di governo, mantenimento e sviluppo del network e remunerazione dei nodi (che potremmo semmai definire *corporate governance*, come per esempio la *corporate governance* di Libra), bensì i protocolli di consenso di uno specifico progetto blockchain e, con essi, il ruolo, i task e i livelli di accesso dei vari nodi e dei soggetti partecipanti.



Poiché la blockchain abilita l'esecuzione di specifiche condotte in rete (la partecipazione di nodi alla computazione di un algoritmo di consenso, nonché la possibilità degli utenti di verificare il risultato della computazione), allorché intendiamo adottare una soluzione *blockchain based*, più che porci la domanda «blockchain o DLT» (Ethereum o Hyperledger), dovremmo chiederci se vogliamo fare le cose in modo diverso, condividendo le informazioni e assoggettandoci a reciproco controllo in ossequio ad una verità non calata dall'alto, ma generata dalla partecipazione più ampia possibile e paritetica degli *stakeholder*. Se non vogliamo cambiare la *governance*, o se addirittura non ci siamo neanche posti il problema, è inutile parlare di sottili e sterili distinzioni tecnologiche e tanto vale continuare ad utilizzare soluzioni tradizionali[6].

---

[4] Vedi definizione 3.6, in *Blockchain and distributed ledger technologies — Terminology* (ISO/DIS 22739), aggiornato al 21 dicembre 2019 (*draft*).

[5] La definizione di blockchain non è pacifica. Quella qui fornita è una sintesi, senz'altro perfettibile, delle proprietà che la Blockchain di Satoshi Nakamoto ha dimostrato di possedere.

[6] Al *Tavolo Filiera Agroalimentare* costituito presso l'Associazione Blockchain Italia stiamo svolgendo profonde riflessioni su quali elementi di governance dovrebbero giustificare l'adozione di una soluzione DLT nel comparto

Token.

In senso improprio[7], in ambito blockchain, un token è un'unità informativa che rappresenta o simula un bene.

Il concetto di bene ha un connotato innanzi tutto giuridico: «*le cose che possono formare oggetto di diritti*» (art. 810 c.c.). Le cose non sono solo i *beni materiali* (una casa, una pinacoteca, ecc.), ma anche i *beni immateriali* (opere dell'ingegno, partecipazioni in società di capitali, ecc.), oppure un mix dei due (un'azienda, un'eredità, ecc.).

Un token, inoltre, può anche rappresentare un diritto, reale (diritto di proprietà di una casa) o personale (diritto a ricevere una certa prestazione), una qualità (certificato identità), uno status (diritto di voto), un diritto di credito (criptovaluta), ecc.

A fronte di tale varietà di token, la tradizionale bipartizione tra *security token* e *utility token* pare un po' riduttiva.

Tuttavia, per quanto la natura o le funzioni di un token siano varie, mi pare che una caratteristica comune a tutti, da un punto di vista tecnico ma non solo, sia il fatto che esso è una stringa invariabile destinata a circolare in blockchain e univocamente connessa ad un'altra, per mezzo di una funzione hash o RSA, destinata a circolare nel mondo fisico *embedded* in un bene o a disposizione, a vario titolo giuridico, di uno o più soggetti. L'effetto di tale connessione univoca è che se nel mondo fisico circola la chiave privata o il digest del token, allora si traccia il bene o si trasferisce il diritto, il rapporto, il credito, lo status o la qualità (almeno fino a querela di falso).

Mi pare insomma che per avere un token che effettivamente svolga una funzione di rappresentazione di un bene, di un diritto, di una qualità o di uno status, occorra sempre che siano in gioco due codici accoppiati in modo che ciò che accade ad uno abbia effetti sull'altro. Una sorta di *entaglement* tra token e bene rappresentato, o tra token e soggetto a cui è conferito il titolo, di tal ché le sorti del bene o del diritto tokenizzato siano in qualche modo riflesse nel corrispondente token virtuale in modo isomorfo.

Creare un entanglement è operazione assai complessa che non può prescindere da una solida base concettuale che tenga conto di cosa voglia dire *identificare* un bene o un diritto e cosa comporti davvero creare un *digital twining*.

Sottovalutare tutto questo, e pensare semplicisticamente ad un token come la virtualizzazione di un oggetto reale (come le monete o i titoli azionari) non solo è riduttivo, ma ontologicamente errato, e fonte di innumerevoli errori di design che ostacolano l'effettivo sviluppo di un progetto blockchain.

Rinvio ad un mio prossimo contributo un'analisi più approfondita su cosa voglia dire tokenizzare un bene e quali necessari step occorra seguire per una effettiva tokenizzazione.

---

agroalimentare e soprattutto che genere di controlli dovrebbero essere adottati. Molte delle riflessioni espresse in questo capitolo sono frutto di quelle lunghe e utili discussioni.

[7] In informatica, un token è un set invariabile di dati (un'unità informativa in forma di stringa) a cui è attribuito un particolare significato. In tale dominio, la tokenizzazione è il processo che converte un testo in una sequenza di token.

Permissionless vs. permissioned.

Qualcuno sostiene che la vera blockchain è solo quella pubblica, cioè permissionless. Non capisco il senso di questa affermazione, anche perché permissionless non è sinonimo di pubblica, né permissioned è sinonimo di privata.

Come ci ricorda un gruppo di lavoro della University of Southampton in un recente lavoro[8], per fare le giuste distinzioni occorre innanzi tutto categorizzare i possibili ruoli dei partecipanti ad una blockchain:

- **read**, accesso ai dati in blockchain;
- **write**, sottoporre transazioni alla blockchain;
- **commit**, eseguire un protocollo di consenso e aggiornare lo stato della blockchain con l'aggiunta di un nuovo blocco.

A questo punto, possiamo utilmente distinguere le blockchain in funzione delle operazioni di tipo *read*:

- **blockchain pubbliche**, nessuna restrizione per eseguire operazioni di tipo *read*;
- **blockchain private**, solo una lista predefinita di soggetti ha il permesso di eseguire operazioni di tipo *read*;

Poi si possono distinguere le bockchain in funzione delle operazioni di tipo *write* e *commit*:

- **blockchain permissionless**, nessuna restrizione per eseguire le operazioni di tipo *write* e *commit*;
- **blockchain permissioned**, solo una lista predefinita di soggetti ha il permesso di eseguire operazioni di tipo *write* e *commit*.

	read	write	commit
public permissionless	anyone	anyone	anyone
public permissioned	anyone	authorised participants	all or subset of authorised participants
private permissioned	restricted to a subset of authorised participants	authorised participants	all or subset of authorised participants

Le blockchain pubbliche si possono combinare con le blockchain permissionless e permissionled. Le private si possono combinare solo con le blockchain permissioned (non avrebbe infatti senso che solo alcuni possano leggere, ma tutti possano scrivere ed eseguire smart contract). Esistono quindi tre tipi di blockchain, il tutto come riassunto nello schema qui accanto[9].

Ora, i tre tipi sopra individuati rispondo l'uno meglio dell'altro a seconda delle circostanze ed esigenze che devono soddisfare. Bitcoin senz'altro deve essere pubblica-permissionless. Un progetto di filiera agroalimentare si adatta bene ad una DLT di tipo pubblica-permissioned (o quasi pubblica). la spunta interbancaria su Corda del consorzio R3, deve senz'altro essere eseguita su una piattaforma privata-permissioned.

La blockchain, insomma, è una tecnologia, come tale non può essere ricondotta a categorie valoriali in quanto il suo fine è quello di risolvere un problema. Non può essere né vera né falsa, ma solo più o meno utile allo scopo.

---

[8] S. DE ANGELIS, G. ZANFINO, L. ANIELLO, F. LOMBARDI, V. SASSONE, *Blockchain and cybersecurity: a taxonomic approach*, (Oct. 2019), p.3. Gli autori rinviano a G. HILEMAN, M. RAUCHS, *2017 Global blockchain benchmarking study* (2017); BITFURY GROUP, J. GARZIK, *Public versus private blockchains (part 1 and 2)*, (Oct. 2015).

[9] *Ibid*. p.4.

Privacy.

Una parola largamente abusata a proposito di blockchain è *privacy*. A molti pare che i digest delle funzioni hash e soprattutto le chiavi pubbliche siano dati personali, con tutti i doveri e i vincoli che ciò importa, sicché o si modifica il GDPR o si rinuncia alla tecnologia blockchain. In proposito ho espresso chiaramente la mia posizione in un recente post (qui) e in altre innumerevoli occasioni. Voglio solo ribadire con fermezza che il GDPR non è un ostacolo allo sviluppo di progetti blockchain, nemmeno di quelli pubblici e permissionless, poiché l'impiego di impronte hash, di soluzioni RSA o altre stringhe frutto di tecniche di pseudonimizzazione – ancorché utilizzate con riferimento a dati identificativi – non costituisce di per sé trattamento di dati personali[10].

Smart contract.

La vulgata vuole che gli smart contract siano dei contratti. Del resto il nome può ragionevolmente indurre in errore più che scusabile. Il problema sorge allorché anche alcuni incauti giuristi cadono in questa trappola lessicale (anche loro sempre vittime evidentemente dell'entusiasmo!).

Ebbene, mi sia concesso dirlo (scriverlo) in termini perentori: gli smart contract **non sono contratti e mai lo saranno!**

Sono programmi per elaboratore e, come tali, sono innanzi tutto delle istruzioni ad una macchina (singola, network o virtuale), non messaggi di un dialogo tra le parti di un contratto[11].

Infatti, un contratto è un accordo tra due o più parti per costituire, regolare o estinguere una situazione giuridica soggettiva. Esso è, insomma, un *incontro di volontà* che per lo più assume forma orale (concludo un contatto con l'edicolante anche quando la mattina compro il giornale), raramente scritta.

Uno smart contract, pertanto, costituisce tutt'al più un attributo di un contratto (la forma scritta); un contratto, peraltro, che per esser tale necessiterebbe innanzi tutto che le parti leggendolo ne **comprendessero il significato** e ne **accettassero l'esecuzione** in un determinato ecosistema informatico. Insomma, non basta che vi sia un documento scritto perché vi sia contratto, occorre che tale documento sia intellegibile e voluto dalle parti; cosa che non accade mai negli smart contract (se non in casi marginali e rare ipotesi di DAO che non possono senz'altro essere generalizzati[12]).

Concludendo, nella prospettiva del diritto gli smart contract sono innanzi tutto dei documenti (in formato elettronico), ovvero elementi di prova di un atto o di un fatto. Al ricorre di certe

---

[10] Più diffusamente, ho argomentato in *I dati personali in ambiente blockchain tra anonimato e pseudonimato*, in *Ciberspazio e diritto*, vol. 19, n. 61 (3-2018), pp. 457-478 (anche su SSRN). Le conclusioni qui espresse, sono recentemente condivise anche dalla *Agencia Española Protectión Datos* (AEPD) e dalla *European Data protection Supervisor* (EDPS) nel lavoro congiunto *Introduction to the Hash Function as a Personal Data Pseudonymisation Technique* (2019), §§ VI e VII a pag. 22.

[11] Rinvio per una approfondita analisi ad un mio contributo di prossima pubblicazione, *Smart contract: né smart né contract*, in *Riv. Dir. Civ.* I, 2020.

[12] Peraltro, il noto caso *the DAO* costituisce piena prova del fatto che gli smart contract, al di là del falso mito «*the code is law*», non sono affatto un contratto (e tanto meno sono law!). Allorché qualcuno eseguendo il codice sottrasse alla comunità qualche milione di dollari, fu accusato di aver tradito il vero accordo associativo esistente tra i partecipanti e la sua condotta, benché conforme alle regole espresse dal protocollo, fu considerata furto.

condizioni possono semmai diventare un'opera dell'ingegno o un'invenzione industriale, ma mai sono un contratto[13].

Sovranità monetaria.

Anche su questa locuzione mi sono ampiamente speso criticando l'atteggiamento scomposto e complottista di esponenti delle istituzioni e accademici vari (qui) che, all'indomani dell'annuncio di Libra, hanno nuovamente evocato scenari apocalittici (come nel dicembre 2017 quando i Bitcoin sfiorarono quota 20.000 Euro), invocando un presunto **diritto unico di battere moneta** spettante agli stati sovrani.

In realtà, non esiste alcun diritto unico di battere moneta. Chiunque può farlo. Né i Bitcoin né Libra costituiscono una minaccia per gli stati sovrani. Semmai, l'unica minaccia per questi ultimi sono le politiche di impiego a dir poco sconsiderate adottate da politici ignoranti e arruffapopoli (se non addirittura mascalzoni). Tutti bravi a millantare soluzioni economiche miracolose, ma subito pronti a far debito a danno delle generazioni future per sostenere le loro propagandistiche promesse elettorali.

Invero, il denaro nasce come *registro contabile centralizzato* di rapporti di debito-credito. Diventa via via decentralizzato con l'introduzione di monete e banconote a libera circolazione. Prosegue il suo cammino di decentralizzazione con la nascita delle banche private e poi di quelle centrali. Oggi il denaro aspira ad essere più che decentralizzato: *distribuito*, grazie all'impiego della tecnologia blockchain[14].

Concludo quindi sostenendo che le criptovalute sono denaro a tutti gli effetti[15].

---

[13] Altra vulgata sugli smart contract, che non merita altro che una nota in questo articolo, è quella che li vuole immutabili e irreversibili. Ebbene, a costo di essere banale e scontato, evidenzio che gli smart contract sono soggetti a mutazione con fork (poco importando che nel ramo superstite sopravviva la formula originaria, senza contare la predisposizione nel codice di specifici trigger di tipo *kill*) e sono reversibili con esecuzione di un nuovo smart contract avente effetti uguali e contrari o con esecuzione di misure *off chain* disposte da un giudice.

[14] Il D.Lgs. 231/2007 (in recepimento della recente V Direttiva antiriciclaggio n. 2018/843), fornisce la definizione di criptovaluta: «*una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata ad una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche o giuridiche come mezzo di scambio e può essere trasferita, memorizzata o scambiata elettronicamente*». Quando una definizione è troppo lunga, si declina in termini negativi («non è… non è… non possiede…»), fa elenchi di proprietà, attributi e funzioni, ed esprime possibilità («può essere…»), mi viene il sospetto che chi la scrive non abbia affatto le idee chiare.

[15] Per approfondire su natura del denaro e delle criptovalute, rinvio ad un mio recente lavoro (qui)