diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

Bitcoin e Blockchain: democrazia valutaria algoritmica o colonizzazione dei margini dell'attività umana?

Autore: Biamonte Alessandro
In: Diritto civile e commerciale

1. Front running, proof of work. Velocità e colonizzazione del margine

Gli algoritmi stanno colonizzando i margini dell'attività umana e anche l'attuale trasformazione della finanza globale sta progressivamente orientando la sua evoluzione verso forme di arbitraggio tra due universi temporali sempre più veloci: quello della immissione di un ordine e della sua esecuzione.
E' la frenesia del front running in un sistema di continui riposizionamenti fondati sulla soluzione di problemi di proof of work (dimostrazione di lavoro), in cui l'astrazione centrale del capitalismo è a sua volta astratta nel calcolo: un aggiornamento al codice macchina che introduce un nuovo strato fondamentale di valore (è il ruolo del blockchain – di cui diremo più approfonditamente di seguito – nella creazione di criptovaluta).
Scott Mc Cloud (1)parla di gutter («margine») alludendo a quello spazio extradiagenetico, il vuoto tra le vignette, che salda le immagini statiche in una narrazione animata: il luogo dove si deducono eventi e azioni cui vi è una semplice allusione nel discorso di narrazione, allo stesso modo in cui la coscienza costruisce la narrazione dal margine inaccessibile della cognizione; la creazione di una storia personale che muove da inferenze e frammenti di percezioni sensoriali.
Allo stesso modo, oggi, gli algoritmi generano miliardi di profitti per i loro detentori, sfruttando una peculiare conoscenza della latenza della rete (il ritardo tra quando un segnale ha origine partendo da un nodo e arrivando a un altro).
Questa forma di arbitraggio temporale ha implicato la rinegoziazione del valore anche in termini finanziari: il tempo è denaro, misurato in millisecondi moltiplicato su milioni di server. Come Diderot e d'Alambert con l'Encyclopédie, in termini epistemologici, rivoluzionarono la conoscenza comprimendola in senso temporale, gli argomenti interconnessi cui hanno concorso gli algoritmi di Page Rank creati da Larry Page e Sergej Brin agli albori di Google (nel 1996), hanno formato il sostrato di AdSense.
Page Rank crea l'indice di base per la circolazione delle idee – valutazione essenziale nell'economia dell'attenzione – per poi consentire ad AdSense di monetizzare l'attenzione su basi inimmaginabili. La funzionalità di AdSense è fondata su di un arbitraggio HFT (High Frequency Trading): ogni volta che un

Diritto & Diritti ISSN 1127-8579

utente naviga verso un sito che diffonde pubblicità per il tramite della rete di Google, viene effettuata una rapida asta tra i committenti e le offerte più alte pubblicano i propri annunci. Le transazioni trasformano in merce la lunga scia di dati che ognuno lascia dietro di sé: profili dettagliati di consumatori creati da cronologia degli acquisti, delle ricerche, dei dati. AdSense è una forma di arbitraggio temporale alla medesima stregua dei sistemi finanziari HFT, che estraggono profitti in un millisecondo; un vero e proprio livello di astrazione in termini computazionali, che crea una sovrastruttura sulla stessa informazione(2).
Il ruolo della velocità nell'arbitraggio (inteso come capitalizzazione della differenza temporale tra il punto A e il punto B) costituisce il percorso logico di un ingrediente passaggio da un sistema analogico a uno digitale in cui il valore crescente delle informazioni e del denaro è al centro di un'astrasione algoritmica. Il futurologo Peter Schwartz, nel 1997, sulla rivista «Wired», preconizza – tra le varie previsioni – un nuovo tipo di arbitraggio computazionale per il capitalismo, che libera il commercio dalle tradizionali e pesanti vestigia della burocrazia, dei contanti e del controllo dall'alto; la moneta elettronica diviene il fulcro dell'economia della rete globale di intrinseca natura postmateriale. Sin dagli albori, i primi imprenditori delle valute digitali riconoscono il valore delle informazioni e cercano di creare un'astrazione algoritmica dal denaro alle informazioni.
La relazione tra **velocità, massa monetaria, livello generale dei prezzi e volume delle transazioni** aveva già formato il nucleo essenziale della riflessione – agli inizi del XX secolo – della teoria quantitativa della moneta: la nota «equazione dello scambio» di Fisher (M'V+M'V'=PT)(3) esprime gli effetti dell'incremento di una variazione autonoma della quantità di moneta (e della sua velocità di circolazione) sul livello generale dei prezzi. Nella relazione i due termini V e V' individuano il numero degli atti di scambio in cui l'unità di moneta interviene nell'unità di tempo considerata (si considera il numero totale delle transazioni effettuate nell'unità di tempo e la velocità di circolazione, intesa in "termini di transazione", è data dal rapporto tra volume delle transazioni complessive e quantità complessiva del circolante e dei depositi). L'analisi fisheriana, però, muoveva da una differente concezione della moneta e del suo valore, e si fondava su di un'astrazione, presupponendo che la sua velocità di circolazione fosse pressoché costante (in quanto legata a consuetudini o a forme di interventi istituzionali lentamente modificabili) e, di lì a poco, la rivoluzione keynesiana concentrerà l'attenzione su altri fattori, quali le decisioni di spesa relative al consumo e all'investimento globali e l'interdipendenza tra redditi e spesa: mentre i teorici quantitativi consideravano la moneta nella sua funzione di strumento di scambio, Keynes ne richiamava, invece, la sua natura di riserva di valore.
Ma la dicotomia tra economia reale ed economia monetaria non esiste: «La moneta – precisa Schumpeter – entra nel quadro solo come espediente tecnico o come strumento che è estato adottato per rendere più agevoli le transazioni… l'analisi monetaria introduce l'elemento "moneta" nella base stessa della nostra struttura analitica ed esclude che tutti i lineamenti essenziali della vita economica possano essere rappresentati da uno schema di economia di baratto»(4) .
L'avvento dei bitcoin desta attenzione come risposta libertaria, o addirittura anarcoide, alle restrizioni sul commercio e sulla valuta imposte da attori finanziari e politici tradizionali: un nuovo modello di arbitraggio algoritmico che inverte l'equazione descritta sinora, spingendosi a sfruttare la vivacità del commercio, il rapporto tra pubblico e privato, tra comunità e identità, sino a invertire la relazione tra azione individuale e costruzione di valore. Il termine, comparso per la prima volta in un articolo del 2008 a firma del matematico Satoshi Nakamoto, sintetizza il rivoluzionario programma quasi ideologico: «Un

Diritto & Diritti ISSN 1127-8579

sistema di pagamento elettronico basato su dimostrazioni crittografiche anziché sulla fiducia, che consente a due parti consenzienti di negoziare direttamente tra loro senza la necessità di una terza parte fidata»(5) . In breve un sistema per lo scambio di valuta fondato esclusivamente sulla potenza di calcolo dell'algoritmo, senza alcuna dipendenza da un'autorità emittente o da una banca centrale, o subordinati a standard di fiducia eterodiretti tipici delle valute tradizionali.

2. Trasparenza, decentralizzazione e l'elaborazione collettiva della riserva di valore. I bitcoin

Il bitcoin, in un'economia sinora dominata da **«scatole nere» impenetrabili**, vuole fondare sulla «trasparenza» il suo programma, una vera e propria scatola di vetro le cui funzioni, essendo completamente trasparenti, rendono il sistema a prova di manomissione. Al pari delle altre piattaforme open source, la logica sottesa individua il punto nodale della sicurezza nel permettere a chiunque di ispezionare il suo codice e suggerire miglioramenti additivi.
Poiché ogni sistema di sicurezza può esporsi a una vulnerabile compromissione, affidarsi a una qualunque autorità esterna o terza parte, ancorché fidata, per condividere informazioni potrebbe introdurre elementi di vulnerabilità, oltre a implicare l'esposizione a un groviglio finanziario, normativo ed elettronico suscettibile di manipolazione. Ecco, dunque, l'inversione dei termini nella relazione tra azione individuale e costruzione di valore, passando per accessibilità collettiva al suo codice.
La sfida rivoluzionaria è affidata a due soluzioni algoritmiche.
La prima di esse è l'utilizzo di algoritmi di crittografia asimmetrica, che si basano su funzioni unidirezionali (calcoli facili da eseguire, ma difficili da invertire per risalire ai termini essenziali; un esempio è quello dell'algoritmo RSA: è facile moltiplicare due numeri primi per risalire a un numero enorme, ma è più difficile scomporre un numero enorme nei due numeri primi che ne sono i fattori. Seguendo il meccanismo dei numeri primi, la chiave «privata» potrebbe essere costituita dai due fattori primi e usata per firmare digitalmente i dati che l'utente desidera mantenere protetti; a cascata si può utilizzare una chiave «pubblica» - derivata dal numero enorme – per verificare quei dati, assicurandosi che per firmarli sia stata utilizzata effettivamente quella chiave privata.
Fermandosi, tuttavia, a questo sistema dinamico, il bitcoin finirebbe con il configurarsi come l'ennesimo metodo di pagamento che si affida a una autorità centrale per consentire la tracciatura della chiave pubblica e dunque validare il pagamento, scongiurando il problema della doppia spesa.
La peculiarità, invece, risiede nella seconda delle soluzioni, l'introduzione di una forma collettiva di arbitraggio computazionale guidato all'unanimità dalla collettività: il meccanismo della blockchain (catena di blocchi). Si tratta del vero e proprio cuore del sistema, il libro che riporta tutte le transazioni bitcoin nella storia della valuta; il resoconto dettagliato di ciascuna di esse da quando esiste la moneta; un file che ha superato la dimensione di 20 gigabyte e che deve essere scaricato localmente da ogni client. Ogni unità incrementale di bitcoin viene tracciata per mezzo della blockchain, cosicché ogni transazione è legata a una o più identità di acquirente e venditore (identità che consistono in stringhe alfanumeriche derivate da un protocollo di crittografia asimmetrica).

Diritto & Diritti ISSN 1127-8579

La radicalità del bitcoin risiede non tanto e non solo nella **natura decentralizzata della valuta**, ma nella sua autorità fondata sull'elaborazione collettiva come forma intrinseca di valore. Poiché la rete bitcoin non ha un'autorità centrale, chiunque pervenga alla conclusione della transazione lo annuncia per mezzo di una rete peer to peer. Gli annunci vengono raggruppati in blocchi di transazioni dai cosiddetti miners (veri e propri minatori) che sono in competizione nell'attività di convalida delle transazioni in coda alla preesistente storia della valuta. Il risultato è un nuovo blocco della blockchain e così via all'infinito. Per farlo, tuttavia, occorre risolvere un problema matematico molto complesso e il minatore che per primo correttamente lo risolve «vince» quel blocco. La ricompensa è questa: la prima transazione in ogni nuovo blocco diventa «transazione di generazione», che crea una certa quantità di bitcoin – che decresce gradualmente nel tempo –. Il minatore riceve anche una ricompensa secondaria, riscuotendo una commissione sulle transazioni come corrispettivo per avere elaborato le varie operazioni computazionali (commissione che cresce gradualmente con il passare del tempo). Il software è calibrato sulla generazione di un blocco ogni 10 minuti, prevedendosi la riduzione della ricompensa per il completamento di nuovi bitcoin fino a zero quando si raggiungerà la creazione di 21 milioni di bitcoin; a quel punto l'incentivo all'aggiornamento indefinito della blockchain sarà costituito solo dalle commissioni sulle transazioni.
Un assetto in cui l'elaborazione collettiva crea valore e ne plasma la sua forma intrinseca, offuscando l'astrazione del valore di scambio dalle altre misure di valore indotto dall'alienazione teorizzata dal pensiero marxiano.

3. Libertà, fiducia e controllo del sistema monetario

Qualsiasi sistema di pagamento – centralizzato o decentralizzato, formalizzato da una convenzione o garantito da un assetto di riferimento – si fonda sulla fiducia; il denaro è la risultante di un paradigma simbolico in cui è immessa fiducia per antonomasia nella misura in cui viene accettato come mezzo di pagamento. Sinora le valute statali e le banche centrali hanno aggiunto all'equazione un livello di fiducia insito nella gestione diretta, garantendo il valore della moneta con l'autorità dello Stato (il Full Faith and Credit – piena fede e credito –). Gli ordinamenti hanno individuato molteplici ragioni giustificatrici e modalità di attuazione. Nell'ordinamento costituzionale italiano, il riconoscimento e la salvaguardia di risparmio e credito effettuati in maniera espressa dall'**art. 47 Cost.** sono funzionali a garantire un terzo bene – la moneta – che in sede di elaborazione della Carta fondamentale si è ritenuto di non menzionare in via diretta (implicitamente tutelata dal rapporto tra risparmio e credito, tutela qualificata di «rilevante interesse pubblico», cfr. Corte Cost. n. 52/2010, associata al correlato bene della stabilità dei mercati finanziari, in un sistema affidato a un controllo penetrante della Banca d'Italia, oltre che a Consob, Istituto che, dismessa la veste pubblicistica, riveste la forma di Società per Azioni), non lesinando l'esigenza dell'intervento legislativo allorquando la «spiccata aleatorietà delle negoziazioni aventi ad oggetto gli strumenti finanziari in esame [qui ci si riferisce alla finanza derivata degli enti locali, n.d.r.], all'evidente scopo di evitare che possa essere messa in pericolo la disponibilità delle risorse finanziarie pubbliche utilizzabili dagli enti stessi per il raggiungimento di finalità di carattere, appunto, pubblico e, dunque, di generale interesse per la collettività» (punto 12.1 della sentenza n. 52/2010 cit.). Finalità ancora più

Diritto & Diritti ISSN 1127-8579

esplicite – a margine dell'attività del Sistema Europeo delle Banche Centrali – alla luce dell'**art. 127 del Trattato di Funzionamento dell'Unione Europea**, per il quale **«sviluppo armonioso,** equilibrato e sostenibile delle attività economiche, un elevato livello di occupazione e di protezione sociale, la parità tra uomini e donne, una crescita sostenibile e non inflazionistica, un alto grado di competitività e di convergenza dei risultati economici, un elevato livello di protezione dell'ambiente ed il miglioramento della qualità di quest'ultimo, il miglioramento del tenore e della qualità della vita, la coesione economica e sociale e la solidarietà tra Stati membri» devono essere perseguiti tramite una politica monetaria che in primo luogo garantisca il mantenimento della stabilità dei prezzi (profili ampiamente enucleati in termini di **incidenza eurounitaria della politica monetaria del Sistema Europeo delle Banche Centrali dalla Corte di Giustizia con la Sentenza CGEU 16 giugno 2015, causa C-62/14**).

4. Oltre l'orizzonte della fiducia. Democrazia algoritmica o traslazione del valore finanziario?

Nei casi appena indicati il sistema valutario non dipende direttamente dalla fiducia collettiva – o di una specifica comunità – che ne sostiene la circolazione, ma da una sovrastruttura che si interseca in nome di un interesse superiore istituzionalizzato.
Mentre le normali transazioni finanziarie sono sostenute da attori statali, il bitcoin utilizza l'elaborazione che si spinge oltre il meccanismo ordinario della fiducia, laddove la blockchain si basa su di una norma computazionale che premiano i minatori che la potenziano al calcolo di ogni nuovo blocco con la soluzione di problemi di proof of work: l'astrazione del capitalismo che a sua volta è astratta nel calcolo.
Il sistema dei bitcoin per raggiungere un efficace livello di affidabilità postula due tipologie di fiducia: la fiducia nell'algoritmo (e specificamente nella **trasparenza della blockchain**) e, in secondo luogo, quella nella creazione di collettivi di calcolo, che danno vita a una comunità condivisa intenta nell'elaborazione delle soluzioni. In definitiva, al di là delle aspirazioni democratiche, è un sistema elitario che inserisce il valore computazionale nelle basi capitalistiche della moneta, traslando il valore finanziario nel primo. Si potrebbe addirittura pervenire all'ipotesi di un paradosso: se le monete virtuali vedessero incrementare in modo esponenziale gli utilizzatori, si ingenererebbe un meccanismo a catena, per cui chi ancora si affida alle valute tradizionali finirebbe con l'accollarsi oneri fiscali crescenti per sostenenere l'infrastruttura statale; nel contempo, la sostituzione dei sistemi di pagamento con i bitcoin darebbe origine al un sistema fiscale a supporto di una rete di cicli di calcolo finalizzati all'estrazione del prossimo blocco della catena.
L'esternalità del valore computazionale dei bitcoin alimentato dal processo additivo della blockchain (che, fondandosi sul calcolo, si differenzia da quello mnestico umano caratterizzato dalla elaborazione dell'idea) reca in sé la sua natura di denaro «programmabile», ma anche di simbolo allegorico verso l'affermazione di un sistema fondato sulla cultura programmabile in cui la produzione di valore è frutto dell'iterazione e figlia della velocità.
Per Sartre è osceno il corpo privo di referenza, che non è orientato, poiché non è in azione o in situazione; teoria che può applicarsi al corpo sociale e ai suoi processi quando vengono spogliati di narratività, di senso e orientamento per essere assorbiti dalla iperacelerazione: «il movimento non scompare tanto

Diritto & Diritti ISSN 1127-8579

nell'immobilità, quanto nella velocità e nell'accelerazione, nel più mobile del movimento, se così si può dire, e che lo conduce all'estremo mentre lo spoglia di senso»(6) .
Nel caso delle criptovalute, se è pur vero che le aspirazioni utopiche che le animano costituiscono una tensione verso una riappropriazione dei processi, su di un altro piano non può negarsi l'astrazione e la perdita di senso, attratta nel vortice computazionale che attribuisce valore proprio al sistema di calcolo in sé inteso, estrema sintesi di una società che perde narratività a favore di un processo additivo-quantitativo..
In Hegel il pensiero è animato da negatività che, facendogli attraversare le esperienze, lo trasformano. La negatività del rendersi-altro è dunque essenza costitutiva del pensiero, aprendo le porte alla conoscenza, quell'unica conoscenza che può porre in discussione in già esistente e trasformarlo.
E' su questo fronte che si gioca il nostro futuro.

Volume consigliato

NOTE

(1)McCloud Scott, Undestanding Comics: The Invisible Art, William Morrow Paperbacks, New York, 1996, trad it., Capire il fumetto, L'arte invisible, Pavesio, Torino, 1996

(2)Liu Alan, The Laws of Cool: Knowledge Work and the Culture of Information, University of Chicago, 2004, p. 181.

(3)Fisher Irving, The Purchasing Power of Money, New York, 1911. Trad. It. Torino, 1975.

(4)Schumpeter Joseph Alois, History of Economic Analisys, New York, 1954, trad. it., Storia dell'analisi economica, I, Torino, 1959, pp. 329-338.

(5)Nakamoto Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, in «The Cryptography mailing list», metzdowd.com. https://bitcoin.org/bitcoin.pdf

(6)Baudrillard Jean, Le strategie fatali, trad. it. di D'Alessandro S., Feltrinelli, Milano, 2007.

https://www.diritto.it/bitcoin-blockchain-democrazia-valutaria-algoritmica-colonizzazione-dei-margini-della ttivita-umana/

Diritto & Diritti ISSN 1127-8579