MICHAEL J. CASEY, PAUL VIGNA

LA MACCHINA DELLA VERITÀ

LA BLOCKCHAIN E IL FUTURO DI OGNI COSA

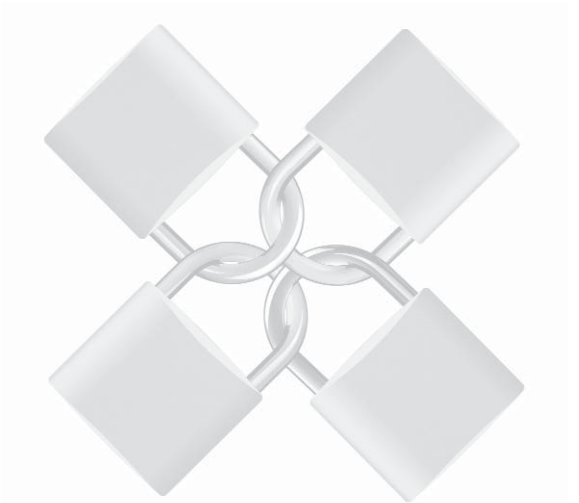
FRANCOANGELI

Informazioni per il lettore

Questo file PDF è una versione gratuita di sole 20 pagine ed è leggibile con

La versione completa dell'e-book (a pagamento) è leggibile con Adobe Digital Editions. Per tutte le informazioni sulle condizioni dei nostri e-book (con quali dispositivi leggerli e quali funzioni sono consentite) consulta cliccando qui le nostre F.A.Q.

Tracce
I nuovi passaggi della contemporaneità



"Con una serie di analisi documentate e ben ponderate, *La macchina della verità* vi propone una storia delle criptovalute e delle blockchain che apre a un percorso verso un'economia distribuita, con maggiori opportunità e possibilità di accesso per tutti".

Andreas M. Antonopoulos, autore di *Mastering Bitcoin* e della serie *The Internet of Money*

"*La macchina della verità* è una guida brillante e ben scritta alla rivoluzione della blockchain, che sta ridefinendo il concetto di fiducia per il nostro mondo sempre più globalizzato".

Hernando de Soto, presidente dell'Institute for Liberty and Democracy e autore di *Il mistero del capitale*

"Le opinioni sul bitcoin sono discordi, ma pochi dubitano del potenziale trasformativo della tecnologia blockchain. *La macchina della verità* è il miglior libro apparso finora su questo argomento, sia per come ricostruisce il passato, sia per come riflette sul futuro. Dovrebbe interessare a chiunque abbia a cuore il futuro della nostra economia".

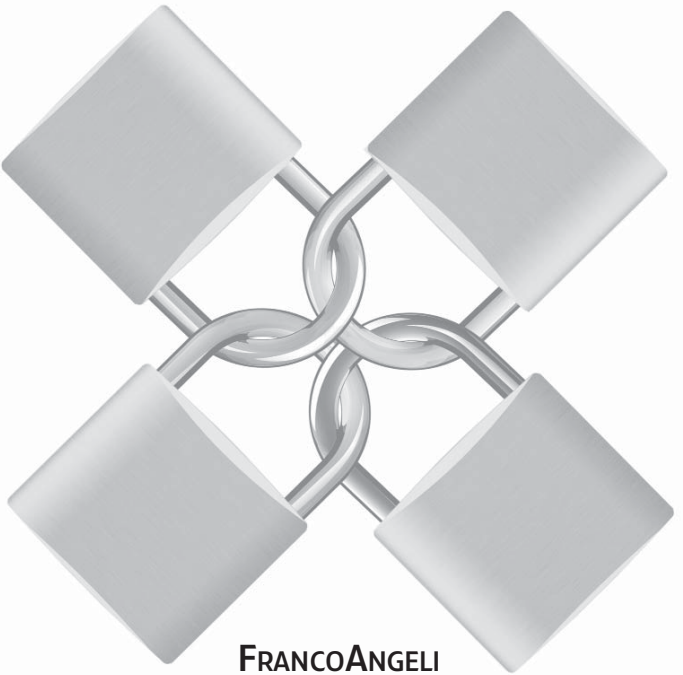
Lawrence H. Summers, Charles W. Eliot University Professor e Presidente Emerito di Harvard ed ex Segretario del Tesoro degli Stati Uniti

MICHAEL J. CASEY, PAUL VIGNA

LA MACCHINA DELLA VERITÀ

LA BLOCKCHAIN E IL FUTURO DI OGNI COSA

EDIZIONE ITALIANA A CURA DI ALESSANDRO GIAUME



FRANCOANGELI

Progetto grafico della copertina: Elena Pellegrini

Titolo originale: *The Truth Machine. The Blockchain and the Future of Everything*

Originally published by St. Martin's Press

Traduzione dall'inglese di Stefano Ballerio

Per Liz, Jenny, Sarah e Di
M.C.

Per mamma e papà
P.V.

Indice

Prefazione

In *The Age of Cryptocurrency* abbiamo esplorato la moneta digitale bitcoin e la sua promessa di un sistema globale dei pagamenti più equo, che funzioni senza banche o altri intermediari finanziari. Quando il libro stava per andare in stampa, le più vaste applicazioni del sistema Bitcoin[1] – in che modo il nucleo del suo sistema operativo possa aiutare a risolvere i problemi di fiducia che insorgono tra individui e aziende quando scambiano risorse, stipulano contratti, rivendicano diritti di proprietà o condividono informazioni sensibili e di valore – vennero in piena luce. Aziende, governi e media furono attraversati da un'ondata di interesse, che dipendeva anche da una buona dose di promozione, per la tecnologia che sarebbe divenuta nota come "blockchain".

Con la sua promessa di risolvere i più annosi problemi di fiducia e di consentire alle comunità di tracciare le proprie transazioni senza affidare la gestione del registro a un intermediario, l'idea della blockchain si presentava come un modo per aggirare i molteplici guardiani che controllano gli scambi economici all'interno della società. Per esempio, la tecnologia blockchain potrebbe consentire a un gruppo di prosumer di quartiere – nuclei familiari che consumino energia e che insieme la producano con dei pannelli solari installati sui tetti delle proprie case – di scambiare quell'energia all'interno del gruppo come un mercato distribuito e senza un'azienda orientata al profitto a stabilire le tariffe. Analogamente, i proprietari di immobili, gli

acquirenti e i soggetti che erogano i mutui non dovrebbero ricorrere necessariamente al registro inaffidabile di una pubblica amministrazione come all'unica fonte di documentazione su precedenti e relazioni, perché un altro e più affidabile registro potrebbe essere costruito a partire da un database inalterabile gestito da una rete distribuita e meno esposto a rischi di manomissioni, errori umani o furti. E queste sono solo alcune delle numerose, nuove applicazioni che hanno attratto su quest'idea innovativa l'attenzione delle persone.

Lo *Zeitgeist* di questa diffusa attenzione del pubblico ha avuto due conseguenze sulle nostre vite. La prima è stata che uno di noi – Michael Casey – si è entusiasmato per le potenzialità di cambiare il mondo della tecnologia blockchain al punto da lasciare una carriera ventennale nel giornalismo per dedicarsi a questo tema a tempo pieno. Meno di sei mesi dopo la pubblicazione di *The Age of Cryptocurrency*, Mike lasciò il *Wall Street Journal* per il Media Lab del MIT. Il frenetico direttore del laboratorio, Joichi Ito – comunemente noto come Joi –, aveva colto dei parallelismi tra l'ascesa del sistema Bitcoin e l'evoluzione del software a cui aveva assistito nei primi tempi di Internet. Percependo un entusiasmo analogo per questa nuova architettura distribuita, Ito concepì un piano per concentrare ingenti risorse accademiche e finanziarie con lo scopo prioritario di sviluppare questa nascente tecnologia. Il risultato fu la Digital Currency Initiative del MIT, un centro presso il quale i migliori ricercatori e studenti nei campi della crittografia, dell'ingegneria e della finanza avrebbero collaborato con strateghi delle *Fortune 500*, startup innovative, filantropi e funzionari governativi per progettare l'architettura digitale di una nuova Internet del valore. Quando ricevette l'invito a unirsi al progetto, Mike sentì che gli veniva offerta l'occasione straordinaria di partecipare alla fondazione di una rivoluzione economica.

La seconda conseguenza è il libro che state leggendo. In *The Age of Cryptocurrency* ci concentravamo specificamente

su una singola applicazione della tecnologia Bitcoin essenziale e sulle sue potenzialità di sovvertire il sistema delle valute e dei pagamenti. Da allora, però, abbiamo imparato che scrivere di tecnologia comporta un rischio: la tecnologia cambia, mentre le parole, una volta stampate, non cambiano più. E in questi tre anni, in effetti, sono cambiate così tante cose che ci siamo trovati costretti a scrivere un nuovo libro. *La macchina della verità* allarga il discorso che avevamo iniziato nel 2015 e lo porta a un livello superiore, per esplorare in quali modi la tecnologia Bitcoin e le sue diverse propaggini, proponendo una molteplicità di applicazioni alternative, agiscano per un ripensamento generale delle organizzazioni sociali.

Nell'economia di oggi, controllare l'informazione significa controllare il mondo. Lo vediamo nel crescente potere di Moloch della tecnologia quali Google o Facebook, che accumulano senza sosta dati su chi siamo e come interagiamo. In questa economia del XXI secolo, il potere è di chiunque abbia l'autorità di raccogliere, conservare e condividere i dati. Attualmente, questa autorità è concentrata nelle mani di un ristretto gruppo di giganti della tecnologia. E, se vi state chiedendo perché ciò sia problematico, pensate solo all'influenza che l'algoritmo nascosto di Facebook, la cui priorità è il modello di business dell'azienda, ha avuto sulla nostra politica. Incentivando la creazione e la condivisione di informazioni spesso incerte ma buone per favorire il rilascio di dopamina entro reti sociali di persone con idee simili, l'algoritmo ha svolto un ruolo strumentale nel determinare il risultato dirompente delle elezioni americane del 2016.

Le idee alla base della blockchain[2] hanno innescato una lotta per sovvertire questa concentrazione di potere e per capire in che modo la capacità di controllare e gestire l'informazione potrebbe passare a un sistema distribuito che non sia controllato da *nessuno*. Possiamo immaginare un mondo liberato dal dominio di Google e di Facebook – o da quello dell'NSA, se preferite – e nel quale siamo noi, le per-

sone, i componenti essenziali della società globale, a dire come debbano essere gestiti i nostri dati.

Sentivamo che questo messaggio fosse importante. *La macchina della verità* è il nostro tentativo di farlo passare.

Note

[1] Nel corso del libro, come vedrete, distingueremo tra "bitcoin", con la [b] minuscola, e "Bitcoin", con la [B] maiuscola. Con "bitcoin" ci riferiremo alla valuta, mentre con "Bitcoin" ci riferiremo al sistema complessivo e al protocollo soggiacenti alla valuta, nonché ad altri usi del registro basato sulla blockchain del sistema Bitcoin.

[2] Nel tentativo di risolvere le ambiguità degli usi linguistici comuni, abbiamo scelto di impiegare la parola "blockchain" in tre modi diversi: con "la blockchain" ci riferiamo al registro distribuito originale del sistema Bitcoin; con "una blockchain" o "delle blockchain", ai più recenti registri distribuiti che condividono la struttura a catena di blocchi del sistema Bitcoin; e con "tecnologia blockchain", infine, a ciò che in generale sfrutta un registro distribuito di questo tipo, a catena di blocchi. Useremo anche l'espressione "tecnologia a registri distribuiti" per comprendere sia le tecnologie a registri distribuiti che usano una blockchain, sia quelle che non ne usano. Inoltre, concepiamo una blockchain, e in generale un registro distribuito, come una cosa distinta e particolare, o identificabile, e non, come spesso avviene nell'uso comune, come un processo. Il titolo del libro usa l'articolo determinativo per rendere conto di come la blockchain originale del sistema Bitcoin abbia svolto un ruolo di catalizzatore nel lanciare questo nuovo campo.

Introduzione.
Uno strumento di sviluppo sociale

Sessanta miglia a est di Amman, su una superficie arida e rocciosa di 14,5 chilometri quadrati nel deserto della Giordania, sorge il campo di Azraq dell'Alto commissariato delle Nazioni Unite per i rifugiati (UNHCR). Il campo di Azraq brulica di una popolazione di 32.000 siriani disperati, alloggiati in rifugi prefabbricati – file e file di cabine bianche di acciaio ondulato, disposte a griglia in stile militare –, e presenta tutte le complessità logistiche di una piccola città. Ma l'UNHCR e le altre agenzie che forniscono ai rifugiati cibo, riparo e un minimo di speranza non possono contare sulle istituzioni e sulle infrastrutture che di norma le città possono usare per garantire ordine, sicurezza e funzionalità ai propri abitanti.

Tutti i campi profughi, per definizione, sono a corto di quello che i politologi chiamano "capitale sociale", quelle reti di relazioni e di legami di fiducia consolidatisi nel tempo che consentono alle comunità di funzionare e di animare scambi e interazioni sociali. Azraq, tuttavia, sembra esserne privo in misura particolare. Ad Azraq ci sono dei funzionari di polizia, ma sono giordani. Non sono membri della popolazione residente, non fanno parte della comunità. E, sebbene i tassi di criminalità di Azraq siano inferiori a quelli del vicino campo di Zaatari, dove 130.000 siriani vivono in condizioni che un report delle Nazioni Unite ha descritto come "al di fuori di qualsiasi legalità", questo luogo assolato, arido e petroso è decisamente inospitale. Quando Azraq fu allestito come alternativa al caos di Zaatari, nel 2014, i rifugiati si

lamentarono del fatto che fosse un luogo privo di vita. L'elettricità era intermittente e questo impediva di ricaricare i telefoni cellulari, cosicché i rifugiati si trovavano isolati dalle proprie famiglie e dagli amici. L'assenza di una comunità funzionante e in cui avere fiducia, inoltre, acuiva la paura dei rifugiati di essere rapiti dagli estremisti dello Stato Islamico. All'inizio, molti rifiutarono di trasferirsi ad Azraq e, sebbene di recente i numeri siano aumentati, il campo resta ancora molto al di sotto della capacità di 130.000 residenti per la quale era stato costruito.

Non è sorprendente, quindi, che questa città spuntata dal nulla, con il suo estremo bisogno di un capitale sociale funzionante, sia divenuta il teatro di una sperimentazione radicale di nuovi modelli di governance comunitaria, di sviluppo istituzionale e di gestione delle risorse. Alla base di questo sforzo c'è la tecnologia blockchain, il sistema distribuito di gestione di registri sul quale è fondata la valuta digitale bitcoin e che promette di costituire un metodo più affidabile e immediato per tracciare le transazioni. Il Programma alimentare mondiale (o World Food Programme: WFP), un'agenzia delle Nazioni Unite che provvede all'alimentazione di 80 milioni di persone in tutto il mondo, ha coinvolto 10.000 rifugiati di Azraq in un esperimento pilota che usa questo sistema per coordinare al meglio la distribuzione del cibo. In questo modo, il WFP spera di affrontare con successo una sfida gestionale enorme: quella di garantire, in un ambiente dove i furti sono continui e poche persone hanno con sé dei documenti di riconoscimento, che ciascuno riceva la propria giusta razione di cibo.

Tra i partecipanti al progetto c'era la quarantatreenne Najah Saleh Al-Mheimed, una degli oltre cinque milioni di siriani costretti a fuggire dalle proprie case dalle devastazioni di una guerra civile brutale e senza fine. All'inizio di giugno del 2015, con il cibo che scarseggiava sempre più e con il moltiplicarsi dei casi di ragazze rapite da miliziani nei villaggi vicini, Najah e suo marito presero la drastica decisione di lasciare il proprio paese natale di Hasaka, dove le

loro famiglie vivevano da generazioni. "È stata una disgrazia che prego Dio che nessun altro essere umano debba mai conoscere di nuovo", ha detto Najah nel corso di un'intervista condotta per noi da funzionari del WFP che lavoravano nel campo di Azraq[1].

Nel lasciarsi alle spalle la propria casa, i propri beni, la propria cerchia di familiari e conoscenti e i propri legami con quella che un tempo era stata una nazione siriana più unita, Najah stava anche rinunciando a qualcosa di estremamente potente, che la maggior parte di noi dà per scontata: un sistema sociale di fiducia, identità e conservazione della memoria che lega il nostro passato al nostro presente, ci garantisce un ancoraggio in quanto esseri umani e ci consente di partecipare alla società. Storicamente, l'amalgama di informazioni che complessivamente provano che possiamo essere ritenuti dei membri affidabili della nostra società è stato controllato da istituzioni che registrano e certificano gli eventi della nostra vita e le nostre credenziali – conti in banca, certificati di nascita, cambi di indirizzo, risultati scolastici, patenti di guida e così via – e che tengono traccia delle nostre transazioni finanziarie. Perdere tutto ciò, come accade spesso ai rifugiati nel momento in cui si trovano privi di uno Stato, significa essere gettati in una posizione di estrema vulnerabilità, che le peggiori organizzazioni criminali e terroristiche del pianeta possono sfruttare facilmente. Se non siete in grado di provare la vostra identità, siete alla mercé di qualsiasi sconosciuto. Nel complesso del lavoro svolto dalle agenzie come l'UNHCR e il WFP, questa funzione essenziale – di creazione di istituzioni sociali sostitutive – non è meno importante di quella di procurare il cibo. Operando in polverose tendopoli affollate di profughi di tutto il mondo, queste agenzie umanitarie devono incaricarsi del difficile compito di ricreare dei sistemi di fiducia sociale. Devono ricostruire delle società, riedificarle da capo. E la tecnologia blockchain, a quanto pare, può essere uno strumento per fare proprio questo.

È in queste situazioni, quando cioè gli esseri umani han-

no bisogno di istituzioni affidabili che tengano traccia delle loro interazioni sociali e forniscano prove della validità delle loro rivendicazioni, che la tecnologia blockchain può funzionare al meglio. Con questo sistema non dovremo più affidarci a delle istituzioni perché mantengano dei registri delle nostre transazioni e garantiscano per noi, perché i sistemi basati sulla tecnologia blockchain presentano un complesso insieme di caratteristiche che producono qualcosa che non era mai esistito prima: un registro delle transazioni visibile a tutti e che può essere verificato in qualsiasi momento, ma che non è controllato da nessuna autorità centrale. Questo implica due cose: che nessuno possa alterare i dati per i propri fini e che tutti abbiano un controllo maggiore sui propri dati. Non è difficile intuire in che modo tutto questo potrebbe avere un effetto di empowerment per quei milioni di siriani che vivono una vita da terra bruciata.

Così come il registro distribuito della blockchain viene usato per garantire ai possessori di bitcoin che nessun altro stia spendendo le loro riserve di valuta – in altre parole, per prevenire quella che altrimenti diventerebbe una contraffazione valutaria digitale su larga scala – il progetto pilota basato sulla tecnologia blockchain di Azraq garantisce che nessuno stia usando due volte i propri titoli rispetto alle forniture di cibo. In un campo profughi, dove i rifornimenti sono limitati e dove è noto che gruppi criminali si organizzano per rubare e accumulare cibo a scopo di lucro, si tratta di un'esigenza piuttosto rilevante. E significa che i rifugiati come Najah saranno sempre in grado di provare la legittimità dei propri titoli. Sarebbe la fine di quelle interruzioni ricorrenti e allarmanti dei rifornimenti che molti hanno vissuto con il sistema dei buoni. In questo sistema, qualsiasi irregolarità tende a mettere in sospetto gli amministratori, che spesso si sentono in dovere di interrompere l'accesso al cibo della persona interessata fino a che l'irregolarità non sia sanata.

In questo nuovo progetto pilota, tutto ciò che serve per consentire un pagamento a un rivenditore di cibo è una

scansione dell'iride del rifugiato. Di fatto, l'occhio diventa una specie di portafogli digitale e questo consente di ovviare al bisogno di contanti, buoni, carte di debito o smartphone, riducendo il pericolo di furti (la scansione dell'iride può suscitare delle perplessità sul rispetto della privacy: ci arriveremo). Per il WFP, digitalizzare questi pagamenti significa risparmiare milioni di dollari di commissioni, poiché consente di tagliare fuori intermediari, come le agenzie di trasferimento di denaro e le banche, che in precedenza controllavano il funzionamento del sistema dei pagamenti.

Ogni volta che un rifugiato spende una parte del suo "denaro" digitale per comprare della farina o altro, quindi, la transazione eseguita viene trascritta automaticamente in un registro trasparente che non può essere manomesso. Questo modello di registrazione sempre attiva, sempre aggiornata e massimamente affidabile implica che gli amministratori del WFP possano avere in qualsiasi momento una visione completa del flusso delle transazioni, nonostante il fatto che il WFP non abbia un proprio registro centralizzato. L'organizzazione può abilitare un sistema di pagamenti all'interno del campo senza per questo dovere assumere il ruolo di una banca o di un gestore dei pagamenti.

Al contrario, il programma per l'identità dell'UNHCR, che è stato integrato nella soluzione basata su tecnologia blockchain del WFP, viene supportato da un database centralizzato. Ciò ha suscitato qualche preoccupazione e qualche critica. I sistemi di questo tipo sono più soggetti a manomissioni, perché, accumulando grandi quantità di dati in un'unica, grande "cassaforte", offrono agli attacchi quello che usualmente viene descritto come un singolo vettore. In teoria, ciò significa che questo gruppo di esseri umani particolarmente vulnerabile si troverebbe ulteriormente a rischio – è facile intuire che cosa potrebbe accadere se un database di identificatori biometrici dovesse cadere nelle mani di un gruppo incline alla pulizia etnica come l'ISIS. Le persone che operano nel mondo delle blockchain sono spesso degli accesi difensori del diritto alla riservatezza e