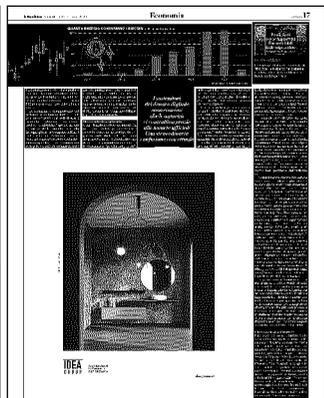


## Se le criptovalute alimentano l'economia illegale

di **Tito Boeri**  
e **Roberto Perotti**

**I**n un articolo precedente abbiamo sostenuto che le criptovalute non svolgono alcuna funzione sociale positiva. Sono, al più, uno strumento di investimento rischiosissimo e speculativo.

● alle pagine 16 e 17 |



L'inchiesta

# Bitcoin & Co. le antimonete liberano solo i criminali

Le cripto, nate come alternativa al sistema finanziario, non mostrano alcuna funzione sociale. E la loro segretezza piace solo all'economia nera

di **Tito Boeri e Roberto Perotti**

L'impatto ambientale delle valute virtuali è pesantissimo: per crearne una si consuma l'energia utilizzata in 13 anni da una famiglia media

**I**n un articolo precedente abbiamo sostenuto che le criptovalute non svolgono alcuna funzione sociale positiva. Sono, al più, uno strumento di investimento rischiosissimo e puramente speculativo. Per rendersene veramente conto, è importate capire come funzionano. Come esempio prenderemo ancora una volta la criptovaluta più diffusa, i bitcoin.

## Blockchain e minatori: come funzionano i bitcoin

Nonostante la retorica imperante, l'impalcatura tecnologica dei bitcoin non ha alcuna ratio economica. Questo è difficile da cogliere perché quasi nessuno sa esattamente

come funziona una blockchain, ma poiché tutti ne parlano deve essere per forza una tecnologia intelligente e utile (tanto da essere inclusa persino nel programma elettorale del Pd...).

Come l'oro, un bitcoin va "estratto", o guadagnato; lo si estrae registrando per primi un "blocco" di transazioni. Un "miner" (un proprietario di computer con forte potenza di calcolo) propone un blocco di transazioni da registrare e aggiungere alla catena, o blockchain. Quel blocco serve come input in una funzione che genera un numero ("hash") tra miliardi di possibili combinazioni. Si pensi a un dado con miliardi di facce: ogni lancio del dado genera un hash. Il primo miner che ottiene un hash inferiore ad una soglia (basata sul numero di miner che interagiscono nella rete) registra il blocco e ottiene il premio (attualmente 6,25 bitcoin).

Quindi ogni volta che un miner propone un nuovo blocco si scatena una gara tra computer per essere il primo a generare un hash sotto la soglia minima. Le possibili combinazioni sono così tante che in media ci vogliono decine di trilioni di tentativi da tutti i computer partecipanti prima che qualcuno registri un blocco. E più sono i miner più la difficoltà aumenta e con questa i tempi di calcolo.

## Un enorme utilizzo di energia, ma per cosa?

Con questi numeri, anche se i computer moderni ci mettono una frazione di millisecondo per generare un hash, è facile capire come nel maggio 2021 estrarre un bitcoin richiedesse 13 anni di consumi energetici di una famiglia media; in un anno, il sistema bitcoin consumava quanto un paese come l'Olanda. Oggi forse un po' meno, ma stiamo parlando sempre di consumi pazzeschi. E la cifra si riferisce solo ai bitcoin, poi ci sono tutte le altre criptovalute.

Perché questo enorme spreco di energia? Essenzialmente per due motivi: creare gli incentivi per registrare i blocchi di transazioni in modo decentrato, cioè accessibile a tutti; e allo stesso tempo garantire che la registrazione non sia manipolabile. Per esempio, poiché ogni blocco include i dati dei precedenti, per cambiare il quartultimo blocco dovrei ri-estrarre tutti i quattro blocchi dal quartultimo all'attuale. La probabilità che lo stesso nodo (computer) registri quattro blocchi di fila è probabilmente nell'ordine di trilionesimi di trilionesimi, nessuno ha interesse a provarci.

Entrambe le motivazioni, decentralizzazione e non manipolabilità, sono però inutili in pratica nel contesto della moneta. Prendiamo la decentralizzazione, le transazioni sono in ogni caso anonime, con il software giusto posso interrogare la blockchain (quanti lo faranno mai davvero?), ma non saprò mai

chi ha fatto quella particolare transazione. A cosa mi serve? Anche oggi so per certo che la mia banca il 13 gennaio ha processato migliaia di bonifici, ma se non so chi sono pagante e beneficiario, cosa me ne faccio (e anche se sapessi, cosa mi interessa)?

Per ovvi motivi Amazon Web Services è forse l'organizzazione al mondo con più proposte di progetti che usano la tecnologia blockchain. Tim Bray, a lungo a capo del team che si occupava di valutare questi progetti incredibilmente sofisticati, ha scritto recentemente: «Uno dei miei colleghi ingegneri pose la domanda: "di tutti questi vostri sistemi, ce n'è uno che non funzionerebbe senza blockchain?" Il tizio (il capo della tecnologia dell'azienda che proponeva il progetto) non esitò un attimo: "no, veramente no"».

## “La tecnologia delle criptovalute non è manipolabile”

Il secondo presunto vantaggio del blockchain applicato alle criptovalute è che le renderebbe non manipolabili.

Secondo Caroline Ellison, l'amministratrice del fondo Alameda Research collegato a Ftx (che si è dichiarata colpevole per 7 accuse inclusa la frode e rischia fino a 110 anni di prigione): «La moneta decentralizzata non custodita sembra essere un fondamento delle libertà civiche ... E se i governi autoritari sono una seria minaccia alla civiltà, il che sembra non totalmente insensato, potrebbe finire per essere importante». Dietro la straordinaria confusione concettuale e sintattica (doppiamente preoccupante in chi gestiva almeno 10 miliardi) si intravede una generica protesta libertaria, anti-sistema, anti-governi, anti-tutto, diffusissima tra i sostenitori delle criptovalute. Ma a cosa ci si riferisce quando si accusano banche centrali e governi di manipolare la moneta?

Per alcuni, i più sofisticati, la manipolazione consiste nel signoraggio, la possibilità di pagare la spesa pubblica con l'emissione di moneta a costo zero. Ma il signoraggio è minimo nei paesi avanzati, nessun governo fa affidamento su di esso per finanziare la spesa pubblica. Il signoraggio può essere significativo quando l'inflazione è molto alta (molto più del livello attuale). Di qui l'accusa alle banche centrali di manipolare scientemente il valore

della moneta, cioè di creare inflazione. In realtà, a parte l'ultimo anno (e per motivi ovviamente indipendenti da governi e banche centrali) l'inflazione è stata bassissima negli ultimi 40 anni, il che basta per confutare questa tesi assurda.

Ed è paradossale che si sia parlato di manipolazione del valore dell'euro quando l'inflazione era all'1 per cento, mentre i bitcoin perdevano l'80 per cento del loro valore in un anno.

La stragrande maggioranza dei sostenitori in buona fede dei bitcoin non è però così sofisticata: è convinta che governi e banche centrali ci “controllino” grazie all'uso esclusivo della moneta ufficiale. Ma ogni giorno avvengono miliardi di transazioni: governi e banche centrali sono interessate esclusivamente a quelle che potrebbero essere legate ad attività criminali. Ed è ancora paradossale che si parli di controllo da parte delle banche centrali, quando comprando criptovalute affidiamo agli intermediari, spesso senza alcuna regolamentazione né controllo, una miriade di dati personali che vengono utilizzati per fini commerciali.

## Un mondo di criptovalute

Come funzionerebbe un mondo in cui le criptovalute private venissero usate come moneta al posto degli euro e dei dollari? Pochi ci hanno pensato, ma se i bitcoin devono davvero rappresentare una moneta alternativa, “gestita dal popolo”, la loro architettura è semplicemente folle: una quantità fissa, 21 milioni di bitcoin, di cui oltre 19 milioni già “estratti”. Gli ultimi saranno estratti nel 2040.

Perché il mitico (e probabilmente mai esistito) fondatore dei bitcoin abbia fatto questa scelta è un mistero. Le versioni più accreditate sono due: che la quantità fissa avrebbe dato valore ai bitcoin, e che l'avrebbe sottratta alle “manipolazioni” delle banche centrali. Ma il fatto che metta in vendita una quantità fissa di aria fritta non le dà più valore, a meno che la gente non la compri solo perché pensa di poterla rivendere a un prezzo più alto: la definizione di una bolla, uno strumento senza alcuna funzione sociale. E come abbiamo visto la nozione che le banche centrali “manipolino” le monete è frutto di una profonda ignoranza di una economia monetaria moderna.

Il mondo si è disfatto del gold standard, in cui l'offerta di moneta

era legata, anche se non in modo meccanico, alla quantità di oro esistente nel mondo, proprio per liberare uno strumento fondamentale: la politica monetaria. Con i bitcoin sarebbe peggio di un ritorno al passato: sarebbe un mondo in cui la quantità di moneta è letteralmente fissa mentre produzione e scambi di beni e servizi aumentano. Questo significa depressione dell'economia e deflazione, cioè prezzi costantemente in diminuzione, un disastro ben peggiore dell'inflazione.

Naturalmente niente impedisce di aggiungere altre criptovalute, e lo si sta già facendo (attualmente si stima che ce ne siano circa 20.000). Ma questo porterebbe ad avere tante monete contemporaneamente, con un tasso di cambio tra ogni paio di criptovalute all'interno dello stesso paese che cambia letteralmente ogni minuto: un incubo senza fine. Immaginate un negozio che deve esporre e continuamente aggiornare ogni prezzo in Bitcoin, Ethereum, etc. Su una scala molto inferiore, negli Stati Uniti nell'ottocento una miriade di banche private emetteva dollari. Il dollaro emesso dalla banca X non valeva quanto un dollaro emesso dalla banca Y. E naturalmente i fallimenti delle banche che avevano emesso più dollari di quanti potessero “ripagare” erano all'ordine del giorno, con i clienti che si facevano prendere dal panico e ritiravano i depositi. Chi arrivava dopo gli altri perdeva tutti i risparmi. Ogni somiglianza con la vicenda Ftx non è da ritenersi del tutto casuale.

La posizione vagamente libertaria di quasi tutti i sostenitori delle criptovalute è ispirata a una profonda e ingiustificata sfiducia, ma anche a una visione semplicistica e ingenua del ruolo delle banche centrali. Che non è più quello esclusivo di coniare monete e stampare biglietti, ma molto più complesso, e fondamentale per il funzionamento delle economie moderne. Ma se si parte dall'assunto che il sistema finanziario è tutto da buttare e possiamo tornare all'età della pietra...

## Che conclusioni trarre?

Due cose. Se avete comprato bitcoin all'inizio, avete ancora fatto un sacco di soldi. Ma non perché le criptovalute abbiano svolto una funzione sociale; semplicemente perché, per intuito o per fortuna, avete anticipato la bolla. Secondo:

come ha scritto l'economista di Harvard Ken Rogoff, investire in criptovalute significa essenzialmente scommettere sull'economia sommersa, quando va bene, o sulla criminalità organizzata. Come abbiamo visto, la vera funzione della tecnologia blockchain finora è nella sua segretezza e anonimato. Non ci vuole molto a capire chi se ne avvantaggia. © RIPRODUZIONE RISERVATA



Su Repubblica

La prima puntata dell'inchiesta di Tito Boeri e Roberto Perotti sulle criptovalute è stata pubblicata lo scorso 30 gennaio

*I sostenitori del denaro digitale sono convinti che le autorità ci controllino grazie alle monete ufficiali. Una straordinaria confusione concettuale*

## Come funzionano le criptomonete

### IL BITCOIN

Lanciata nel 2009, è la prima criptovaluta al mondo per diffusione. È un valore digitale che due persone possono scambiarsi in Rete senza bisogno di intermediari.

### IL MINING

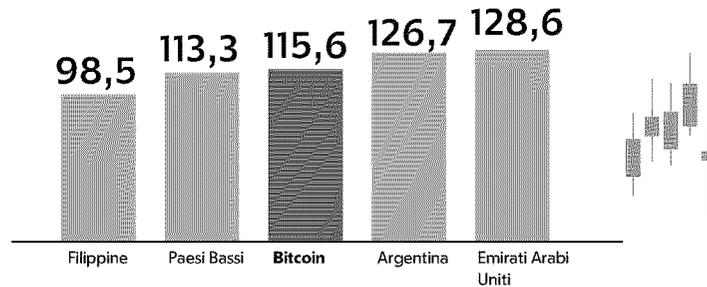
È "l'estrazione" delle monete virtuali. Il processo fa compiere a dei computer una serie di complessi calcoli matematici che validano e registrano le transazioni.

### LA BLOCKCHAIN

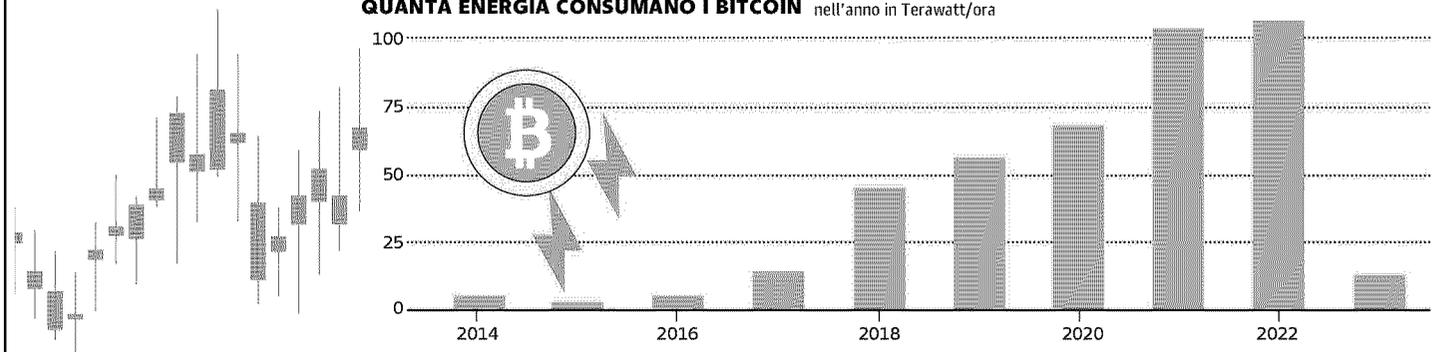
La "catena di blocchi" è il registro contabile immutabile su cui una dopo l'altra vengono archiviate le transazioni in criptomonete.

## IL CONFRONTO CON I PAESI

Se il bitcoin fosse uno Stato, il suo consumo di energia sarebbe al 33esimo posto mondiale (Terawatt/ora nell'anno 2022)



## QUANTA ENERGIA CONSUMANO I BITCOIN nell'anno in Terawatt/ora



INFOGRAFICA DI ROBERTO TRINCHIERI