

Bitcoin: valuta del futuro o minaccia per l'ambiente?

Stefano Porciello

I Bitcoin sono la criptovaluta più famosa al mondo, ma la conosciamo davvero? Dopo che il suo valore è esploso e poi crollato nei primi mesi del 2018, sono ancora in molti a credere che si tratti della “moneta del futuro”, ma pochi sanno spiegare cosa sia una blockchain o come funzioni Bitcoin. Si tratta davvero di una “bolla”? Perché i Bitcoin sono accusati di consumare tanta energia elettrica?

Subito dopo il suo decimo compleanno, tra il 14 e il 26 novembre 2018, Bitcoin ha bruciato quasi il 40% del suo valore, scendendo al di sotto della soglia dei 4000 dollari. Mentre si aspetta un possibile rimbalzo, si è momentaneamente perso circa un quinto della potenza di calcolo necessaria al funzionamento del suo network. Ma anche se naviga in acque tempestose, Bitcoin non ha perso nulla del suo fascino né – per ora – del suo potenziale.

Come funziona Bitcoin e per come mai è così famoso? Ha davvero un impatto ambientale insostenibile? Prima di cercare una risposta a queste domande, facciamo un passo indietro. Perché proprio un anno fa eravamo alla vigilia di una storia incredibile, che non solo ha fatto molto discutere il mondo intero, ma ha anche contribuito al mito, ai pregiudizi e alle speranze esagerate riposte in questa “moneta digitale”. Il 17 novembre 2017 un Bitcoin valeva 7.844,02 dollari. Un mese dopo, la stessa moneta veniva scambiata per 19.497,5\$. Rispetto alla quotazione di novembre, il suo valore era triplicato e la capitalizzazione totale sul mercato aveva raggiunto e superato i 326,5 miliardi, segnando un +2.003% da inizio anno. Solo 40 giorni dopo, però, tutto sembrava finito. Il 5 febbraio 2018, un Bitcoin tornava a valere 7.489\$ e la sua capitalizzazione crollava al di sotto dei 130 miliardi, dopo averne bruciati 200 in poco più di un mese. Matt O'Brien, sulle pagine del *The Washington Post*, l'aveva già definita la “più perfetta delle bolle possibili”.

Si è molto parlato di Bitcoin negli ultimi anni – come di una bolla finanziaria e di un consumatore esagerato di energia, ma anche come di una speranza e di una ri-

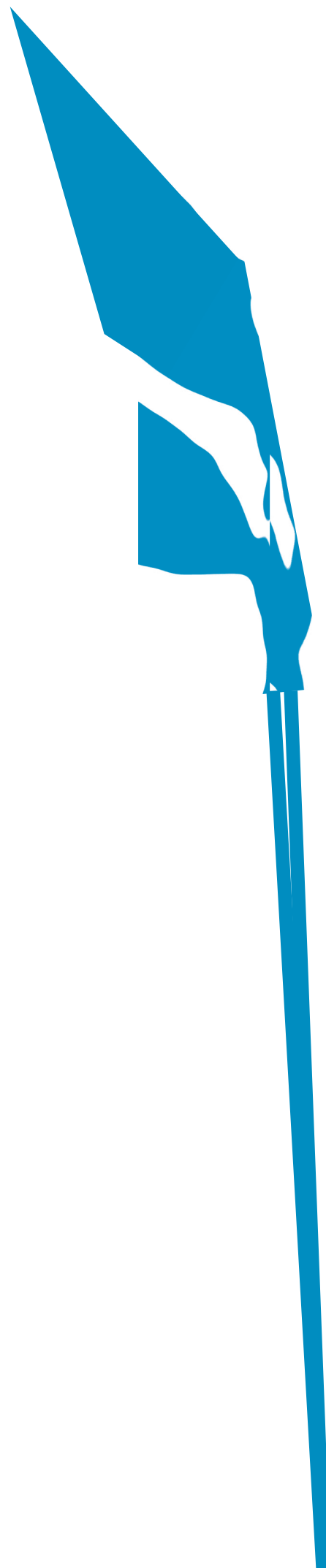
voluzione nel mondo del denaro – senza che si sia creata una vera e propria conoscenza condivisa sull'argomento. Cercare di capire il mondo di Bitcoin e delle molte altre criptovalute che sono nate sulla sua scia, è decisamente complicato. Ad oggi esistono migliaia di criptovalute di ogni tipo che funzionano in modi diversi e attorno a cui si sono aggregate speranze, interessi e capitali. Nel momento in cui scriviamo, secondo *Coin Market Cap*, sono ben 9 le criptovalute con una capitalizzazione oltre il miliardo di dollari (erano 16 soltanto poche settimane fa). Bitcoin domina su tutte coprendo, da solo, più della metà del mercato. Per quanto sia difficile destreggiarsi tra termini e fatti poco conosciuti a cavallo della cronaca, dell'informatica e dell'economia, proviamo a fare il punto su cosa è una *blockchain*, come funziona Bitcoin e a capire perché si discute del suo consumo energetico (che equivale, secondo diverse stime, a quello di un paese di medie dimensioni). La stampa internazionale non è mai stata particolarmente “morbida” nei confronti di Bitcoin, e ne ha giustamente evidenziato le criticità. *The Economist*, uno dei giornali più autorevoli al mondo in economia e finanza, ha dedicato il suo *Technology Quarterly* di settembre 2018 proprio alle criptovalute. Tim Cross è arrivato a scrivere: «Bitcoin ha fallito nel suo obiettivo dichiarato: diventare una valuta utilizzabile. La sicurezza è scarsa [...] la sua natura decentralizzata lo rende inevitabilmente lento; non c'è protezione del consumatore; e il prezzo è così volatile che non molte persone vorrebbero usarlo come mezzo di scambio di beni e servizi». Sullo stesso numero Tim Swanson, fondatore di *Post Oak Labs*, dichiarava: «Ad essere



onesti, la maggior parte delle persone compra [criptovalute] perché spera che il prezzo aumenti, piuttosto che per qualsiasi grande ragione filosofica». Il 30 agosto, sempre *The Economist* rilanciava online un articolo dal titolo decisamente esplicito: *Bitcoin and other cryptocurrencies are useless*. Inutili. Augustín Carsens, General Manager della Banca dei Regolamenti Internazionali (BIS), è stato una delle voci più critiche sull'argomento. «Una nuova tecnologia non è una tecnologia migliore, o una migliore economia», ha detto durante una lezione alla Goethe University di Francoforte il 6 febbraio 2018. «Questo è chiaramente il caso di Bitcoin: sebbene fosse inteso come un sistema di pagamento alternativo senza coinvolgimento del governo, è diventato una combinazione di una bolla, uno schema di Ponzi [cioè una truffa, ndr] e un disastro ambientale». E ancora, in un'intervista rilasciata alla CNBC, Carsens ha difeso la sua posizione, affermando che le criptovalute – in realtà – non sono monete, ma *asset*, beni. Ai microfoni di *Radio3 Scienza*, il professor Ferdinando Ametrano ha dichiarato che considerare Bitcoin uno schema di Ponzi sia

Ad oggi, esistono migliaia di criptovalute che funzionano in modi diversi, attorno a cui si sono aggregate speranze, interessi e capitali

impreciso, se non addirittura sbagliato, ha definito Bitcoin come un “esperimento ardito” e ha giustamente relativizzato l'importanza del consumo energetico del network se confrontato con altre attività economiche con un grande impatto ambientale. Per quanto forte, tuttavia, quanto evidenziato da Carsens non è da liquidare troppo in fretta: principalmente a causa della loro estrema volatilità – e cioè il continuo, repentino e incontrollato cambio di prezzo – le criptovalute non riescono a svolgere nessuna delle funzioni tipiche di una moneta. Non sono cioè ancora riuscite ad affermarsi né come misura né come riserva di valore, e per di più non possono essere scambiate facilmente con beni e servizi. Non sono vere monete, quindi, ma qualcos'altro. Che Bitcoin e la tecnologia su cui si fonda – l'ormai celebre *blockchain* – siano stati delle innovazioni totali c'è poco da discutere. Per la prima volta nella storia di internet, è stato risolto grazie a un algoritmo il problema fondamentale del



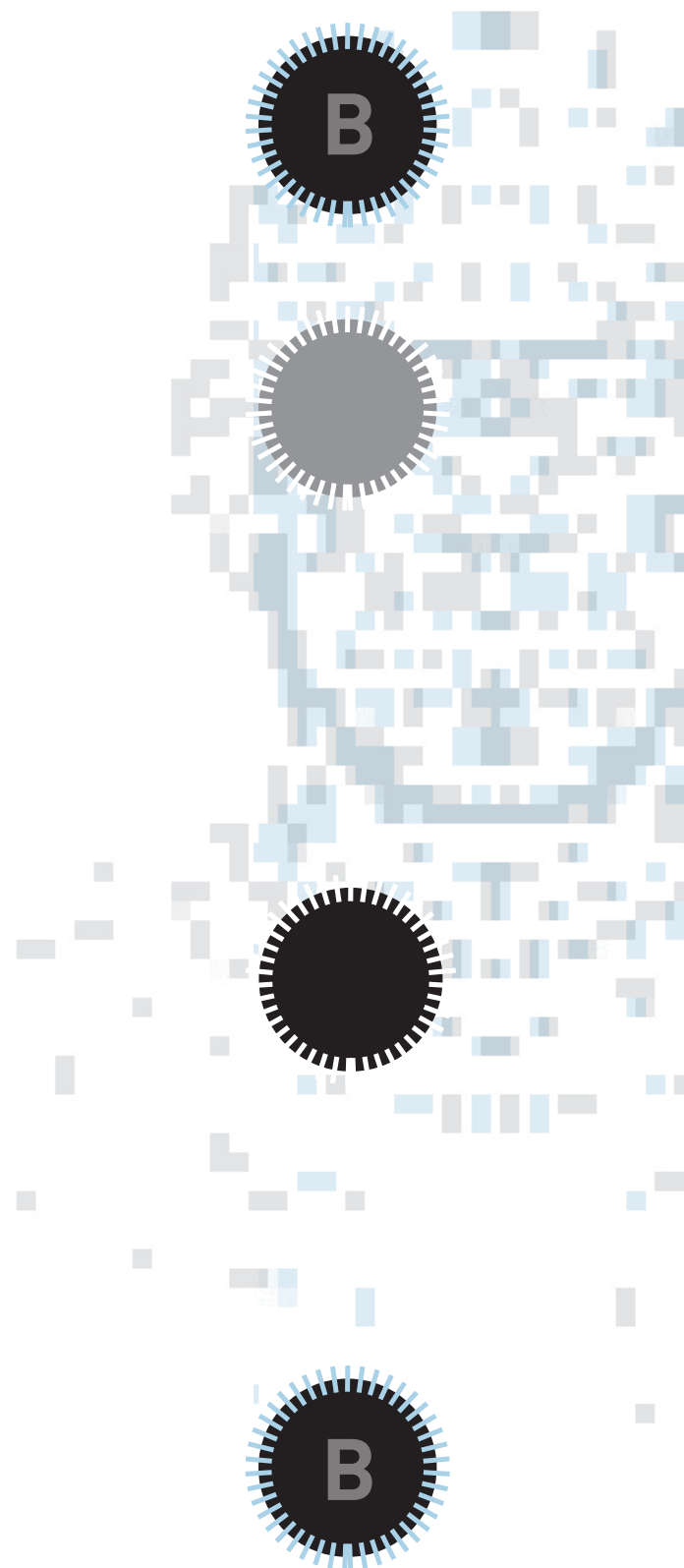
double spending. In altre parole, si è data una risposta credibile alla domanda: come faccio a sapere che una certa moneta virtuale non venga copiata o spesa due volte, senza che un intermediario, o un'autorità, garantisca e controlli tutte le transazioni? Lo ha fatto attraverso la *blockchain*, una tecnologia *open source* e *peer-to-peer* che attraverso l'uso della crittografia e l'offerta di incentivi economici a chi investe tempo, soldi ed energia perché il network funzioni, fa sì che le informazioni registrate nella "catena dei blocchi" siano inalterabili (o quasi). Questo design consente agli utilizzatori di affidare la sicurezza del loro denaro alla matematica di un algoritmo piuttosto che alla credibilità di un'istituzione. Per di più, l'uso di *blockchain* permette di abbattere i costi legati alla registrazione delle transazioni ed evita che chi normalmente si occupa di garantirle (un operatore o un intermediario come la banca o la compagnia della vostra carta di credito) acquisti qualche tipo di potere di mercato. Bitcoin è stato disegnato per essere una moneta il più possibile decentrata, "democratica" e sicura. Ogni nodo del network possiede una copia del libro mastro di tutte le transazioni effettuate dal 2009 ad oggi e contribuisce ad aggiornarlo attraverso un'attività chiamata *mining*, o estrazione. Ogni volta che un utente chiede di svolgere una transazione, questa dev'essere verificata dalla maggior parte degli utenti: la transazione viene inserita in un blocco e tutti i minatori gareggiano per aggiungerlo alla catena. Come? Attraverso un sistema chiamato *Proof-of-Work*: i computer dei minatori cercano di risolvere di forza bruta un puzzle matematico, e se ci riescono per primi indovinando casualmente la soluzione del problema, aggiungono il blocco alla *blockchain*. Questo avviene circa ogni 10 minuti, e in palio ci sono 12,5 Bitcoin: ai prezzi correnti significa guadagnare più o meno 50.000 dollari. L'8 novembre scorso erano ben 81.000, mentre intorno a Natale 2017, nel bel mezzo della frenesia per l'acquisto di Bitcoin, si trattava di oltre 170.000\$. Incentivi di questa portata hanno spinto molti a tentare la sorte e diventare *miners*, minatori, aggiungendo potenza di calcolo al network e, di conseguenza, diminuendo le pro-

babilità per i minatori più piccoli di vincere questa "lotteria matematica". Se nel 2009 bastava un PC per avere qualche probabilità di estrarre Bitcoin, oggi il *mining* avviene principalmente attraverso *data center* specializzati: vere e proprie fabbriche dove computer dedicati svolgono calcoli ininterrottamente, 24 ore al giorno. I *miners* possono affittare una certa potenza di calcolo, pagando la loro quota di energia elettrica, e ricevendo in cambio una parte dei Bitcoin estratti proporzionale al loro contributo.

Da un punto di vista "filosofico", Bitcoin è ciò che è grazie al fatto che «non ci sono intermediari di fiducia, chiunque può diventare un "miner" o aggiungere transazioni legittime, nessuno può bloccare le transazioni di un altro partecipante», spiegano Catilini e Gans in *Some Simple Economics of the Blockchain*. «Mentre questo rende Bitcoin estremamente resiliente agli attacchi e alla censura, lo rende anche meno efficiente, nella sua forma attuale, rispetto alle reti di pagamento centralizzate», scrivono. Al momento, Bitcoin non può processare più di sette transazioni al secondo: una performance sicuramente inadeguata per una piattaforma che vuole essere globale. Tuttavia, per riuscire a truffare il sistema di Bitcoin o a modificare una transazione già registrata una certa entità dovrebbe avere – almeno momentaneamente – il controllo di oltre la metà della capacità computazionale di tutti gli altri *miners*. Dovrebbe quindi bruciare, da solo, almeno la metà dell'energia di tutto il sistema. Questo rende un attacco informatico talmente costoso che, ad oggi, Bitcoin non è mai stato "bucato". «In altre parole, è proprio la difficoltà computazionale del *mining* che rende le *blockchain* pubbliche difficili da attaccare da parte degli avversari», ha dichiarato Arvind Narayanan, professore associato di *Computer Science* a Princeton. Più energia viene "sprecata" dal network, più il network stesso sarà impenetrabile agli attacchi.

Mentre le criptovalute (come Bitcoin) sono monete digitali che hanno un certo valore, funzionano tramite un particolare algoritmo e vengono scambiate tra attori economici, la *blockchain* è la tecnologia su cui sono costruite e attraverso cui sono scambiate.

Sebbene non esista al momento una definizione condivisa di *blockchain*, possiamo dire che è un metodo per conservare delle informazioni digitali: le informazioni vengono raccolte in blocchi che vengono aggiunti uno alla volta, in modo permanente, a una “catena di blocchi”. La catena dei blocchi è una specie di libro mastro di tutti i dati – o transazioni, nel caso delle criptovalute – che viene conservato collettivamente, in numerose copie, dai diversi “nodi” che compongono la rete. Come ben spiegato dall’articolo di *The Verge* “Blockchain is meaningless”, non è vero che una *blockchain* sia per sua natura immutabile e non sottoposta a censure: lo è solo fintanto che chi si occupa di mantenere il network (siano questi gli sviluppatori, i minatori, o qualcun altro) così vorrà. La sicurezza e l’immutabilità di una *blockchain* dipendono dalle regole comuni su cui si fonda il network, dalla crittografia che viene usata per aggiungere i blocchi alla catena e dal tipo di accesso permesso a ogni utilizzatore. Le grandi aspettative che ruotano intorno alle applicazioni della *blockchain* al mondo delle transazioni e dell’industria hanno in realtà molto trasformato la sua prima e più originale applicazione che ha dato origine a Bitcoin. Mentre infatti la tecnologia blockchain è ancora a tre-cinque anni dalla maturità, spiega un’analisi di *McKinsey&Company* dal titolo *Blockchain beyond the hype*, «il modello commerciale che ha più probabilità di successo a breve termine non è la *blockchain* pubblica, ma quella privata». Catene, quindi, che si basano sull’aggiunta di informazioni in blocchi a dei database distribuiti, ma che sono gestiti da organizzazioni (non da chiunque voglia far parte del network) e caratterizzati dalla presenza di diritti e autorizzazioni d’accesso e di modifica. Per questo, come ha fatto notare il Professor Narayanan, *private blockchain* rischia di essere solo un nuovo modo confusionario di chiamare un database condiviso. Che sia privata o pubblica, comunque, una *blockchain* può avere moltissime applicazioni: dal controllo delle emissioni di carbonio ai trasferimenti internazionali di capitali, dalla logistica dei trasporti all’identità digitale delle persone, fino allo sviluppo di contratti che si attivano automaticamente date certe condizioni e molto altro ancora. Con un impatto ambientale, bisogna dirlo, che può essere assolutamente trascurabile: la *blockchain* non ha bisogno di consumare inutilmente energia per poter funzionare. Alcune criptovalute, invece,



sì. Tra queste, Bitcoin è forse il più importante divoratore di energia elettrica, principalmente a causa del suo grande successo.

Il problema deriva dal modo in cui i blocchi di transazioni vengono aggiunti alla *blockchain*. La *Proof-of-work* è una lama a doppio taglio: se da una parte permette alti livelli di sicurezza per l'intero sistema, dall'altra è un incentivo a consumare più energia possibile, così da avere più probabilità di aggiungere un blocco alla catena e aggiudicarsi le monete in palio. Per questo motivo, l'uso di computer sempre più efficienti non diminuisce la quantità di energia consumata dal sistema. A parità di costi, ai *miners* conviene aggiungere capacità di calcolo, piuttosto che consumare (e spendere) meno. Sono state fatte numerose stime sul consumo elettrico di Bitcoin, ma tra le più interessanti c'è proprio quella del Professor Narayanan, nella sua testimonianza davanti alla Commissione energia e risorse naturali del Senato americano il 21 agosto 2018. Considerando che tutti i *miners* usino la tecnologia più efficiente presente sul mercato, ha stimato che l'estrazione di Bitcoin consumi una quantità di energia «leggermente inferiore all'1% del consumo mondiale di elettricità, o leggermente superiore al consumo di elettricità dello stato dell'Ohio o dello stato di New York. Anche altre *blockchain* pubbliche consumano una quantità considerevole, anche se molto più bassa, di energia». Online, tra i difensori di Bitcoin viene talvolta argomentato che il sistema bancario mondiale – che la criptovaluta potrebbe potenzialmente rendere obsoleto – consuma molta più energia della loro *blockchain*, e che il dibattito sul consumo energetico di Bitcoin sia stato preso dal verso sbagliato: l'attenzione dovrebbe essere su chi produce energia, non su chi la consuma. Semplificando il dibattito, si dice: «Se il *mining* consuma energia rinnovabile, perché porsi il problema?». In realtà, il consumo di energia ottenuta dalle rinnovabili non giustifica il dispendio energetico della *Proof-of-Work*: si tratta comunque di bruciare energia che potrebbe essere dedicata ad altro. Tuttavia, soprattutto negli ultimi tempi, alcuni paesi hanno attirato più di altri imprese dedicate

al *mining*. Tra questi, l'Islanda è un caso esemplare, non solo perché quasi la totalità dell'energia prodotta proviene da fonti rinnovabili, ma anche perché il clima molto freddo consente di risparmiare sul raffreddamento dei “rig”, cioè dei computer che svolgono, effettivamente, il *mining*. Johann Snorri Sigurbergsson, un impiegato della compagnia HS Orka, già citato da diversi media internazionali come *AP* e *The Guardian*, ha calcolato che nel corso del 2018 l'energia richiesta dai *data center* islandesi dedicati al *mining* potrebbe superare il consumo domestico di tutte le abitazioni del Paese. Non solo: se tutti i progetti per nuovi *data center* dovessero essere accettati, l'Islanda non produrrebbe abbastanza elettricità per soddisfare la domanda, riporta la BBC. Ci sarà da capire se queste previsioni finiranno per realizzarsi nei fatti, considerato che il recente crollo di valore di Bitcoin sembra aver portato, tra il 4 e il 27 novembre 2018, a una riduzione dell'attività di estrazione a livello globale di circa il 20%. «La questione fondamentale è: da dove arriva tutta questa energia?» ci dice Gary Cook, che dirige le campagne di Greenpeace per incoraggiare le grandi aziende di internet e i grandi produttori di elettronica a rendere i loro servizi e i loro prodotti più sostenibili, e ad alimentarsi attraverso fonti rinnovabili. Cook ci racconta che i giganti di internet come Google o Facebook «stanno costruendo *data center* molto grandi [...] ma stanno anche firmando contratti



Bitcoin è stato disegnato per essere una moneta il più possibile decentrata, “democratica” e sicura

importanti e stanno facendo grandi investimenti in energie rinnovabili. Questo sta aggiungendo nuova energia rinnovabile alla rete. E così stanno creando la domanda, ma stanno anche creando un'offerta di energia [verde] molto più grande». Il problema di Bitcoin e delle altre criptovalute che utilizzano la *Proof-of-Work* è che non esiste un signor Zuckerberg a cui chiedere di investire in energia pulita; è la co-

munità di *miners* a doversi organizzare per mantenere un certo livello di sostenibilità della piattaforma. Ma d'altra parte, proprio perché gran parte dei costi di estrazione delle criptovalute se ne va in bollette dell'elettricità, c'è forse più interesse nel cercare energia a buon mercato piuttosto che nell'investire in rinnovabili. Così, se a volte l'energia più economica è quella derivata dal carbone cinese, altre volte è il geotermico islandese. «Ad oggi», ci dice Cook «non li vedi guidare una nuova fornitura di energia rinnovabile capace di soddisfare la loro domanda nello stesso modo in cui vediamo fare dalle più grandi aziende di internet globali».

C'è speranza, quindi, che il *mining* non solo si trasformi per sprecare meno energia, ma sia sempre più alimentato attraverso le rinnovabili? «Penso che la realtà del cambiamento climatico e la necessità di una transizione verso una piattaforma più sostenibile finiranno per prevalere», dice Cook. «E quindi le criptovalute che saranno in grado di farlo più velocemente e con maggiore successo dovrebbero trovarsi in una posizione molto migliore per poter continuare ad attrarre investimenti e accettabilità [sociale] come valute, col passare del tempo». Per il momento, purtroppo, questa è solo una speranza. Bitcoin, come altre criptovalute basate sulla *Proof-of-Work*, sta consumando un mare di energia. Abbandonare il *mining* significherebbe perdere – in una certa misura – indipendenza, democraticità e sicurezza. E, forse, valore. Non è detto che *miners*, sviluppatori e utilizzatori siano disposti ad accettarlo. Così come non è detto che l'utilizzo di energia rinnovabile per l'estrazione di Bitcoin finirà per prevalere.