Bitcoin e criptovalute: mondi contrapposti

Cos'è Bitcoin, come funziona
e perché il mondo delle altcoin
ne rappresenta l'antitesi

Febbraio 2022

Federico Rivi

Indice

Introduzione: nani sulle spalle del gigante		4
Capitolo 1	**Esigenze e innovazioni**	**6**
	Economia del dono e baratto	6
	Dalle merci all'oro	6
	Banconote e sistema finanziario	7
	La risposta alla crisi del 2008	8
Capitolo 2	**Come funziona Bitcoin?**	**9**
	Cos'è Bitcoin	9
	Blockchain	10
	Mining	12
	Halving	14
Capitolo 3	**A cosa serve Bitcoin?**	**16**
	Riserva di valore	16
	Emancipazione finanziaria	17
	Difesa della privacy e diritti umani	19
	Transizione energetica	20
Capitolo 4	**Critpovalute, un altro paradigma**	**22**
	Il Trilemma e la decentralizzazione	22
	Proof-of-Work vs Proof-of-Stake	24
	Ethereum e governance	25
Conclusioni		27
Fonti		28

“Una delle cose belle di Bitcoin è che costringe le persone a farsi domande sui fondamenti del denaro”.

Andreas M. Antonopoulos

Introduzione
Nani sulle spalle del gigante

Questo documento nasce dall'esigenza di distinguere due concetti che vengono comunemente accostati, talvolta utilizzati come sinonimi, ma che in realtà sottendono tecnologie, ideologie e casi d'uso completamente diversi: Bitcoin e criptovalute.

Criptovaluta è la traduzione italiana di *cryptocurrency*, che a sua volta deriva da *cryptography* e *currency*: crittografia e valuta[1]. Il termine intende la rappresentazione digitale di un valore basata sulla crittografia. Dal punto di vista strettamente etimologico, dunque, qualunque tipo di valore scambiabile digitalmente tramite il coinvolgimento di qualche forma di crittografia può essere definito criptovaluta. I pagamenti elettronici con carta di credito, per esempio, sono crittografati. Per assurdo, quando non vengono scambiate tramite contante, le valute fiat - le monete a corso legale come l'euro e il dollaro - possono essere definite criptovalute.

L'intento di questo documento è mostrare come il mondo delle cosiddette *altcoin* - ossia tutte le criptovalute al di fuori di Bitcoin - sia in gran parte molto più affine al sistema finanziario tradizionale - fatto da Stati, banche centrali, banche commerciali e mercati azionari - che a Bitcoin.

La nascita di Bitcoin nel 2009 e il progressivo aumento della sua popolarità hanno portato alla proliferazione di migliaia di nuove *cripto* - a febbraio 2022 se ne contano più di 17.000[2] - che con il protocollo introdotto da Satoshi Nakamoto[3] hanno ben poco a che vedere. La maggior parte di queste millantano varie forme di decentralizzazione basate su solamente una parte del protocollo Bitcoin che in tanti considerano la vera innovazione: la *blockchain*.

Nelle prossime pagine verrà argomentato come una vera e autentica blockchain conservi le sue proprietà originali solamente all'interno del sistema Bitcoin e non in altri protocolli pseudo-decentralizzati. Peraltro, nel white

---

[1] La traduzione italiana grammaticalmente corretta sarebbe *crittovaluta*, ma ormai è ampiamente diffuso il termine *criptovaluta*.
[2] Coinmarketcap.com
[3] Satoshi Nakamoto è lo pseudonimo dietro il quale si cela il creatore di Bitcoin. Non si è mai scoperto se si tratti di un uomo, una donna o di un gruppo di persone.

paper[4] pubblicato il 31 ottobre 2008 non si fa mai riferimento ad alcuna *blockchain*, bensì si parla di *proof-of-work chain*, il cui significato verrà approfondito.

Le caratteristiche che contraddistinguono Bitcoin - cioè il suo essere libero, distribuito, incensurabile e senza confini - sono inimitabili nel loro insieme da qualunque altcoin. Questo non fa della creazione di Satoshi Nakamoto un sistema perfetto: dal 2009 ad oggi sono state eseguite delle implementazioni al codice - *Taproot* è l'ultima in ordine di tempo - e altre ancora ne verranno effettuate. Il mercato, tuttavia, ne riconosce la leadership incontrastata: l'intera economia delle criptovalute a inizio febbraio 2022 vale 1.777 miliardi di dollari, di cui 735 miliardi rappresentati dal solo Bitcoin, il 41%[5].

Per comprendere che cosa contraddistingua Bitcoin dalle altre criptovalute è utile - senza pretesa di esaustività tecnica - farsi un'idea generale del suo funzionamento e del perché sia comparso apparentemente dal nulla 13 anni fa. A quali esigenze c'era bisogno di rispondere? Le altcoin soddisfano istanze simili o invece, come sostengo, rispondono in buona parte alle stesse priorità delle monete tradizionali?

[4] Il documento con cui Satoshi Nakamoto ha presentato per la prima volta Bitcoin: https://bitcoin.org/bitcoin.pdf
[5] Messari

1. Esigenze e innovazioni

- *Economia del dono e baratto*

Parallelamente alla sua evoluzione l'uomo ha sempre sviluppato nuovi metodi per scambiare valore.
In antichità, quando ancora non esisteva il concetto di moneta, era diffusa l'economia del dono: il modo più frequente per scambiarsi beni era, per l'appunto, regalarli. Naturalmente un simile sistema non poteva essere concepito per economie di larga scala, funzionava per lo più in piccole comunità autosufficienti in cui persistesse un legame affettivo o di fiducia reciproca.

Il baratto era già più evoluto: i diretti interessati attribuivano un valore analogo a beni differenti a seconda delle esigenze di ognuno. Questo tipo di scambio richiedeva una negoziazione che il dono non contemplava e divenne infatti il primo esempio di mercato in cui anche degli sconosciuti potevano far incontrare domanda e offerta: la sola cosa che importava per i soggetti coinvolti era il valore che loro stessi assegnavano agli oggetti scambiati. Una forma di commercio, tuttavia, ancora estremamente limitante: beni diversi tra loro raramente hanno lo stesso valore.
Per usare le parole dell'economista americano Gene Epstein: "Ci si rese conto che se io ho delle uova e tu hai una mucca, potrebbe servirci un mezzo di scambio per permettere a te di comprare le mie uova o a me di comprare la tua mucca".[6]

- *Dalle merci all'oro*

Dall'esigenza di scambiare merci in modo più efficiente e su più larga scala nacque una nuova forma di linguaggio per comunicare valore: la moneta. Dapprima svolsero questa funzione le merci, poi arrivarono i metalli.

A seconda delle caratteristiche di ogni società nel corso dei secoli sono state utilizzate innumerevoli tipologie di merci come moneta di scambio: sale, fave di cacao, animali, conchiglie, pietre e molto altro. Si diffusero perché avevano caratteristiche che le rendevano efficaci unità di conto per le popolazioni che le adoperavano: godevano - seppur in misura molto varia - di un certo livello di scarsità, divisibilità, fungibilità e trasportabilità. Qualunque bene avesse

[6] Bitcoin - The End of Money As We Know It

queste caratteristiche e fosse riconosciuto da un ampio numero di persone poteva essere utilizzato come mezzo di scambio e dunque come moneta.

Il valore delle merci però non è duraturo. Quando si vende qualcosa ottenendo in cambio una moneta è necessario che il valore di quest'ultima sia durevole affinché possa essere utilizzata per comprare altri beni in futuro: con merci e animali questo non è possibile.

E' per rispondere a questa necessità che sono nate le monete metalliche: dal bronzo, al rame, all'argento e fino all'oro, la forma di moneta più longeva e che ha fatto prosperare l'uomo più a lungo. L'oro, al contrario di come qualcuno potrebbe pensare, non deve il suo successo al fatto che è da sempre utilizzato per produrre gioielli ma al fatto che supera tutti gli altri metalli in fatto di fungibilità, divisibilità (1 kg d'oro solido ha lo stesso valore di 1 kg d'oro fuso) e, soprattutto, scarsità.
E' un bene raro che implica importanti investimenti infrastrutturali per essere ottenuto e si stima che il 90% di tutto l'oro presente sulla superficie terrestre sia già stato estratto[7]. Per questi motivi è stato per secoli la miglior riserva di valore e il miglior mezzo di scambio possibile. Tuttavia presenta anch'esso dei limiti: è difficilmente trasportabile.

- *Banconote e sistema finanziario*

Per consentire in comodità lo spostamento di grandi quantità di valore emersero le banche e, con loro, le banconote. I clienti degli istituti bancari iniziarono così a depositare nei caveau i propri metalli preziosi ottenendo in cambio cartamoneta che, facilmente trasportabile, rappresentava le ricchezze detenute.

Il valore del dollaro americano dal 1900 al 1914 - l'epoca del cosiddetto *Gold Standard* - è stato legato direttamente all'oro detenuto dagli Stati Uniti, che possiedono ancora oggi oltre la metà delle riserve auree globali[8], le più ampie in assoluto. Grazie a questo legame il dollaro non poteva essere emesso in modo incontrollato e non subiva l'inflazione che invece caratterizzava molte altre valute sovrane: divenne così la moneta più stabile al mondo e per questo venne acquistata da altri paesi come riserva di valore, trasformandosi in un riferimento globale.

[7] Oregold - Tutto l'oro del mondo
[8] Bitcoin - The End of Money As We Know It

La piena convertibilità del dollaro in oro venne abolita, come detto, nel 1914. Successivamente, nel 1971, il presidente Richard Nixon eliminò completamente la conversione e da allora il dollaro, come tutte le altre valute nazionali, è garantito solamente dalla fiducia nello Stato e nelle istituzioni finanziarie.

- *La risposta alla crisi del 2008*

Il sistema post-Nixon ha retto senza forti scossoni fino al recente 2008, quando la crisi dei mutui subprime ha innescato la più grande recessione economica globale degli ultimi novant'anni.
Come scrive il giornalista economico del *New York Times* Andrew Ross Sorkin fin dal titolo del suo bestseller *Too big to fail*, si pensava che Wall Street e il sistema finanziario statunitense fossero troppo grandi, troppo affermati per poter davvero crollare.

Dal 2008 la fiducia - unico valore fondamentale di quel sistema composto da Tesoro americano, Federal Reserve, Wall Street e grandi banche commerciali - è quindi iniziata a scemare. E' emersa l'esigenza di scambiarsi valore al di fuori del sistema oligopolistico della moneta di Stato, di poter conservare privatamente i propri risparmi senza doversi fidare di una banca, di fare transazioni con i propri soldi senza dover chiedere il permesso a qualcuno.

In risposta a questa esigenza il 31 ottobre 2008 è stato pubblicato online il white paper di Bitcoin: *A Peer-to-Peer Electronic Cash System.*

2. Come funziona Bitcoin?

“Il cancelliere sull'orlo del secondo salvataggio delle banche”
The Times, 3 Gen 2009

A far intuire che Bitcoin sarebbe potuto diventare una vera e propria alternativa al sistema finanziario tradizionale è stato lo stesso Satoshi Nakamoto. Il giorno della nascita della criptovaluta - il 3 gennaio 2009 - all’interno del primo blocco della blockchain di Bitcoin - anche noto come *Genesis block* - Nakamoto ha inserito un messaggio: *“Il cancelliere sull'orlo del secondo salvataggio delle banche”.* Era l’apertura del quotidiano londinese *The Times* di quel giorno. Gli istituti di credito avevano fallito nella gestione dei risparmi dei propri clienti e gli Stati erano costretti a enormi interventi pubblici per salvarli. Bitcoin era la nuova tecnologia che avrebbe permesso di escludere le banche dall’equazione dell’economia.

- *Cos’è Bitcoin*

Definire una tecnologia in continuo sviluppo è già di per sé complesso. Lo è ancora di più nel caso di Bitcoin, uno strumento che non ha solamente implicazioni economiche ma ne ha anche a livello politico, geopolitico, sociale, energetico. A 13 anni dalla sua nascita ancora nessuno può dire con certezza di aver compreso del tutto cosa potrà diventare Bitcoin e fino a dove potrà arrivare. Per cui, senza pretesa di esaustività, mi limiterò a riportare alcuni aspetti utili allo scopo di questo documento.

Innanzitutto Bitcoin è il primo bene digitale che risolve il problema della doppia spesa senza la presenza di una figura garante: duplicare un file sul computer è estremamente semplice, ma il sistema Bitcoin introduce la non-riproducibilità e la scarsità in ambito digitale. Così come una singola banconota non può essere copiata in più esemplari e può essere spesa da un individuo una e una sola volta, lo stesso accade con i bitcoin[9] (o le loro frazioni, chiamate *Satoshi*[10]). Proprio come le banconote, controllate da chi le possiede fisicamente, i bitcoin sono uno strumento al portatore: sono in mano a chi detiene le chiavi private che li controllano[11]. A differenza delle

[9] Bitcoin, con lettera maiuscola, indica il protocollo. Se scritto invece con lettera minuscola, “bitcoin” indica la moneta utilizzata all’interno del protocollo.
[10] Un bitcoin è composto da 100.000.000 di Satoshi.
[11] Chiave privata: stringa di caratteri alfanumerici, come una password, indispensabile per poter inviare una transazione in bitcoin.

banconote, però, il valore non può essere inflazionato in modo arbitrario e dipende unicamente dal rapporto tra domanda e offerta.

Il protocollo Bitcoin non è altro che un insieme di regole pubbliche[12] che permettono a un sistema di funzionare. Così come l'Internet Protocol (IP) - il principale della famiglia dei protocolli Internet e quindi di vitale importanza per lo scambio di messaggi in rete - ha permesso la distribuzione delle informazioni, il protocollo Bitcoin è stato ideato per consentire la distribuzione di un sistema monetario e forse, in futuro, di molte altre cose.

Perché è così importante? Perché per sua natura è:

- Libero: non è governato da alcun ente centrale. A controllarlo sono gli utenti;
- Distribuito: è una rete peer-to-peer aperta a chiunque;
- Incensurabile: disincentiva economicamente i tentativi di modifica o censura del codice o delle transazioni;
- Finito: non esisteranno mai più di 21 milioni di bitcoin;
- Senza confini: i bitcoin possono essere inviati ovunque, senza limiti e in tempi molto brevi;
- Antifragile: non ha un punto singolo di vulnerabilità, elemento che lo rende estremamente resistente a qualunque tipo di attacco.

Come vengono riunite tali caratteristiche in un unico protocollo? Scopriamolo con alcuni concetti chiave della struttura Bitcoin.

- *Blockchain*

Quando si effettua un bonifico è la banca che, da intermediario, garantisce la correttezza della transazione: verifica che il pagante abbia sufficiente disponibilità di denaro e si cura di aggiornare i saldi dei conti correnti interessati. Come avviene la verifica in un sistema privo di intermediari come Bitcoin?

Tra le sue varie funzioni, la blockchain mantiene l'archivio di tutte le transazioni avvenute fin dall'avvio del network a oggi e continua ad aggiornarsi costantemente. Ogni membro della rete[13] Bitcoin detiene una copia della blockchain e, di conseguenza, conosce lo storico delle transazioni globali.

[12] Per i lettori più tecnici, il codice di Bitcoin è consultabile al link: https://github.com/bitcoin/bitcoin
[13] Per membro della rete si intende un nodo: ovvero un hardware su cui sia installato un client Bitcoin funzionante. Il più diffuso è Bitcoin Core: https://bitcoin.org/it/scarica

Questo fa sì che chiunque sia in grado di verificare in ogni momento la correttezza di una transazione: essendo in possesso dell'archivio si può facilmente ricostruire il saldo di un portafoglio e stabilire quindi se abbia sufficienti fondi per effettuare un pagamento. Le transazioni vengono costantemente verificate da tutti i nodi della rete che quindi non hanno bisogno di fidarsi di un intermediario, ma eseguono i controlli in modo indipendente l'uno dall'altro per convergere sulla correttezza di tutte le operazioni: questo meccanismo è conosciuto come *Nakamoto consensus*.

La blockchain è pubblica e può essere consultata anche da chi non fa parte del network[14]: ciò non significa che tutti siano in grado di conoscere l'identità di chiunque abbia mai fatto una transazione insieme al suo saldo e al suo storico di pagamenti, perché sulla blockchain non compaiono nomi e cognomi ma stringhe alfanumeriche.

Come è costituita la blockchain di Bitcoin? Si configura, come spiega la parola stessa, in una catena di blocchi che viene aggiornata ogni circa 10 minuti e include due tipi di dati:

- Le transazioni in forma estesa avvenute nei minuti trascorsi dall'approvazione dell'ultimo blocco[15];
- L'intestazione: contiene un riferimento che collega il blocco a quello precedente della catena (funzione di hash), informazioni relative al mining (approfondito in seguito) e una struttura che riassume le transazioni contenute nel blocco (merkle tree root).

A differenza di come molti credono la blockchain di Bitcoin non ha solamente la funzione di registro globale delle transazioni - per quella basterebbe un archivio condiviso - ma, come detto, collega anche tutti i blocchi l'uno con l'altro tramite la funzione crittografica di hash.

All'interno dell'intestazione di ogni blocco è contenuto l'hash del blocco precedente: questo significa che l'hash di ogni blocco è in parte costituito dall'hash del blocco precedente. Perciò per modificare l'hash di un blocco è necessario cambiare l'hash del blocco successivo, che per essere modificato

[14] Esistono più siti per consultare la blockchain. Uno dei più affidabili è Blockstream Bitcoin Explorer.
[15] Non necessariamente un blocco contiene tutte quante le transazioni degli ultimi 10 minuti. Quelle che per motivi di spazio non stanno all'interno del blocco restano in un *limbo* chiamato mempool in attesa di essere inserite in uno dei blocchi successivi. La priorità viene data in base alle commissioni. Più è alta la commissione pagata per una transazione, prima quest'ultima verrà inclusa in un blocco ed entrerà quindi a far parte dell'immutabile registro globale.

richiede il cambiamento dell'hash del blocco seguente e così via. Insomma, per violare un blocco della blockchain di Bitcoin bisognerebbe ricalcolare tutti i blocchi che lo seguono fino all'ultimo della catena.

Grazie all'algoritmo di *proof-of-work* (approfondito in seguito) serve molta potenza computazionale per calcolare l'hash di un blocco e, di conseguenza, la potenza di calcolo necessaria per violarlo cresce esponenzialmente all'aumentare del numero di blocchi che lo seguono. Di fatto Satoshi Nakamoto ha reso antieconomici i tentativi di attacchi al network. Per convenzione si considera praticamente inviolabile un blocco che ne abbia altri 6 davanti, perciò a un'ora dall'approvazione di un blocco (10 minuti moltiplicati per 6) il suo contenuto diviene scolpito nella storia di Bitcoin.
E' per questo motivo che una blockchain non regolata dalla proof-of-work (come nel caso della grande maggioranza delle altcoin) è infinitamente meno sicura - gli attacchi non richiedono così tanta potenza computazionale e non sono quindi antieconomici - e perciò perde la sua funzione principale: quella di rendere un network distribuito inviolabile.

Per comprendere come viene aggiunto un nuovo blocco alla blockchain è il momento di introdurre il concetto di mining.

- *Mining*

Non di rado si legge che il mining è quel meccanismo utile a "estrarre" nuovi bitcoin. Questo tipo di lettura è sbagliato in partenza. Il network di Bitcoin è messo in sicurezza dalla potenza computazionale: più capacità di calcolo coinvolge, più diventa complesso attaccarlo. L'obiettivo del mining è quello di blindare la sicurezza della rete in modo decentralizzato, mettendo a disposizione più potenza di calcolo possibile da ogni parte del mondo. Chi guadagna il diritto di aggiungere il nuovo blocco alla blockchain ottiene come ricompensa nuovi bitcoin, che sono a tutti gli effetti l'incentivo economico che spinge i miner a svolgere l'attività di guardiani del network.

L'algoritmo che regola tale processo è detto di *proof-of-work* (prova di lavoro): il suo principio fondamentale consiste nel dover dimostrare di aver svolto una certa quantità di lavoro - e aver quindi speso delle risorse - per poter essere ricompensati economicamente. Per questo motivo Satoshi Nakamoto nel white paper di Bitcoin non parla di blockchain ma di *proof-of-work chain*. Un sistema in netto contrasto con quello delle valute fiat che possono essere emesse a costo zero e a discrezione delle banche centrali.

Per poter scrivere un nuovo blocco nella blockchain - e ottenere quindi i nuovi bitcoin - è necessario risolvere prima di tutti gli altri un complesso calcolo matematico, troppo avanzato per la mente umana. A processarlo sono macchine specializzate chiamate ASIC (Application Specific Integrated Circuit) che eseguono migliaia di miliardi di operazioni al secondo provando tutte le soluzioni possibili fino a quando non trovano quella corretta.

Si tratta di una vera e propria competizione globale: chi nella rete trova per primo la soluzione scrive il blocco e, se questo risulta coerente con le informazioni del resto del network (se quindi combacia con il consenso distribuito), riceve in cambio i bitcoin di ricompensa più tutte le commissioni delle transazioni incluse nel blocco.
Di fatto, più si dispone di potenza computazionale, maggiori sono le entrate, perché sono più alte le probabilità di trovare la soluzione prima di chi possiede minor potenza di calcolo. I partecipanti a tale competizione sono chiamati *miner*, minatori. Ma anziché vestire casco e tuta antinfortunistica, gestiscono macchine specializzate.

La competizione in un mercato molto remunerativo ha creato negli anni grandi aziende che gestiscono le cosiddette *mining farm*: strutture con migliaia di macchine che simultaneamente calcolano 24 ore al giorno. Alle mining farm si sono poi aggiunte le *mining pool*, ovvero “squadre” di miner che uniscono la loro potenza computazionale da ogni parte del mondo. Quando la *pool* vince la competizione e ottiene i nuovi bitcoin, questi vengono distribuiti tra i partecipanti in proporzione al contributo che hanno portato in termini di potenza di calcolo.

Cosa accadrebbe se un miner inserisse una transazione scorretta, ad esempio di *double spending*[16], in un blocco? In base alle regole sopracitate del *consenso*, i nodi della rete inizierebbero a marcare l’operazione come invalida scartando il blocco e il miner perderebbe la sua ricompensa in bitcoin, dopo aver comunque speso risorse energetiche per calcolare la soluzione matematica. I miner sono quindi incentivati economicamente a comportarsi onestamente.

Per far approvare una transazione irregolare bisognerebbe controllare la maggioranza assoluta della rete Bitcoin, in modo da far combaciare il consenso della rete con la propria volontà: tuttavia, date le dimensioni del

[16] Double spending: doppia spesa, ovvero il tentativo di spendere due volte lo stesso titolo.

network, si tratta già oggi di un'eventualità estremamente remota e più la rete cresce, più diminuiscono le possibilità di successo di un attacco.

Il protocollo Bitcoin è dotato di una funzione che gli permette di modellarsi in base alla variazione di potenza computazionale presente nella rete. Per semplificare la comprensione supponiamo che esistano 100 macchine Asic in tutto il mondo e che con la loro potenza di calcolo siano in grado di risolvere l'indovinello crittografico in media ogni 10 minuti. Con un mercato profittevole, la concorrenza attrarrebbe nuovi investitori che acquisterebbero altri Asic, portando a 200 il numero totale di macchine: se la difficoltà dell'indovinello fosse sempre identica, la soluzione non impiegherebbe più 10 minuti per essere trovata ma solamente 5 per via della potenza di calcolo raddoppiata. Così facendo la quantità di bitcoin emessi verrebbe duplicata (ogni 5 minuti anziché 10) e il mercato si inflazionerebbe in modo eccessivo. Per risolvere questo problema il protocollo Bitcoin utilizza il *difficulty adjustment*, che ogni 2016 blocchi - all'incirca due settimane - adegua la difficoltà del calcolo in base alla potenza computazionale presente nel network per fare in modo che la media temporale di scrittura di nuovi blocchi sia sempre 10 minuti.

- *Halving*

Bitcoin ha una politica monetaria decisamente drastica. Come anticipato, si tratta di un asset scarso che in futuro sarà finito. Non è possibile produrre più bitcoin del numero prestabilito, 21 milioni[17].

In precedenza è stato chiarito che alla scrittura di ogni blocco vengono emessi nuovi bitcoin: ma quanti? La quantità varia in base al momento storico. Ogni 210.000 blocchi, che corrispondono approssimativamente a 4 anni, ha luogo l'*halving*, evento che dimezza il numero di bitcoin emessi per ogni blocco per i successivi 210.000 blocchi.

Nello specifico:

- Dal 3 gennaio 2009 al 28 novembre 2012: 50 bitcoin ogni 10 minuti;
- Dal 28 novembre 2012 al 9 luglio 2016: 25 bitcoin ogni 10 minuti;
- Dal 9 luglio 2016 all'11 maggio 2020: 12,5 bitcoin ogni 10 minuti;
- Dal 11 maggio 2020: 6,25 bitcoin ogni 10 minuti.

[17] Essendo open-source, è possibile in realtà creare un "nuovo Bitcoin" copiando il codice e modificando solamente i dati che stabiliscono il circolante totale a 21 milioni. Si tratterebbe a tutti gli effetti di una nuova criptovaluta e il suo valore dipenderebbe da domanda e offerta. I tentativi ci sono stati ma il vero Bitcoin ha sempre retto senza particolari problemi.

Tale processo proseguirà fino al 2140, quando verrà minata l'ultima frazione di bitcoin. Da quel momento in poi si suppone che i miner potranno sostentarsi con le sole commissioni di transazione. A febbraio 2022 è già stato emesso il 90% dei 21 milioni di bitcoin totali.

E' dunque possibile conoscere con precisione il ritmo di emissione di nuova valuta del network Bitcoin: l'informazione è di dominio pubblico. L'offerta è nota e ciò significa che l'unica variabile a influenzare il prezzo dell'asset è la domanda.

3. A cosa serve Bitcoin?

Come detto è ancora presto per cucire un vestito adatto attorno a Bitcoin e stabilire quale sia la sua miglior funzione. Riserva di valore, moneta di scambio, strumento di difesa dei diritti umani: Bitcoin è stato definito in tanti modi ma la risposta migliore a chi si chiede a cosa serva davvero è “dipende”. Dipende dal contesto e dalle esigenze di chi lo utilizza. Può essere tutto quanto appena elencato e può essere molto di più. In questo capitolo mi limiterò a osservare le sue caratteristiche più evidenti fino a oggi.

- *Riserva di valore*

La scarsità e la progressiva diminuzione dell’emissione hanno reso bitcoin la miglior riserva di valore dell’ultimo decennio, periodo in cui il tasso di crescita annuo composto (Cagr) del prezzo è stato del 196,7%[18], un dato ineguagliato nella storia della finanza. Dopo la prima parte della pandemia di Covid-19 diversi grandi fondi hanno inserito bitcoin nel proprio portafogli e l’asset è stato sdoganato anche a livello istituzionale: l’authority statunitense *Office of the comptroller of the currency*[19] nel 2020, per esempio, ha consentito alle banche Usa di offrire servizi di custodia di bitcoin.

Se molti esperti lo affermavano già da tempo[20], specialmente negli ultimi anni a bitcoin è stata riconosciuta l’etichetta di *oro digitale* anche da parte della narrativa mainstream. Rick Rieder, capo investimenti di Blackrock - la più grande società di investimento al mondo -, si è spinto oltre: ha dichiarato a novembre 2020 che «il bitcoin è destinato a durare a lungo e potrebbe un giorno rimpiazzare l'oro»[21].

Come ha spiegato l’economista Saifedan Ammous “l’oro e il bitcoin sono diversi da materie prime di consumo come rame, zinco, nichel, ottone perché entrambi hanno un alto rapporto *Stock-to-Flow*[22]. [...] I bitcoin circolanti nel 2017 valevano circa 25 volte quelli prodotti nello stesso anno: un rapporto

---

[18] Case Bitcoin
[19] Organismo di vigilanza e regolamentazione delle banche statunitensi.
[20] In Italia è presente il centro di ricerca e sviluppo Digital Gold Institute, fondato dal prof. Ferdinando M. Ametrano.
[21] Intervista a SquawkCNBC.
[22] Il rapporto *Stock-to-Flow* è la quantità circolante di una risorsa divisa per la sua quantità prodotta annualmente. I beni scarsi come oro e bitcoin hanno un alto rapporto Stock-to-Flow perché anche se la domanda cresce in modo significativo, l’offerta non può aumentare proporzionalmente.

comunque molto inferiore a quello dell'oro, che verrà superato nel presente ciclo di halving"[23].

C'è tuttavia ancora molta strada da fare in termini di adozione per rimpiazzare l'oro come principale riserva di valore mondiale. Nel 2021 le criptovalute - non solo Bitcoin - contavano approssimativamente 500 milioni di utenti, gli stessi che aveva internet nel 1997. Mantenendo il tasso di crescita attuale si stima che potrebbero diventare un miliardo nel 2024[24]. Il dato si riflette anche nella capitalizzazione di mercato di Bitcoin, che a febbraio 2022 corrisponde al 6,4% di quella dell'oro e al 25,8% di quella di Apple[25].

- *Emancipazione finanziaria*

Nel mondo occidentale pensare di ricevere lo stipendio o pagare piccole spese quotidiane in bitcoin, anche se tecnicamente possibile, è ancora visto con scetticismo per il semplice fatto che ad ora il valore della criptovaluta è più volatile di quello di monete fiat come euro e dollaro.

Una buona moneta per poter svolgere la funzione di unità di conto deve garantire un prezzo il più possibile stabile per permettere all'uomo di pianificare la propria vita nel medio e lungo termine: risparmiare, investire, contrarre debiti o concedere prestiti può essere fatto in modo efficiente quando il valore del mezzo di scambio in un dato momento del tempo è simile al suo valore nel futuro.

Non tutto il mondo però vive di euro e dollari. In molti paesi l'inflazione erode i risparmi della popolazione con tassi inimmaginabili nell'Eurozona o negli Stati Uniti. In alcuni casi bitcoin è una moneta molto meno volatile rispetto a quella di Stato ed è quindi più efficiente.

E' il caso del Venezuela, dove tra il 2016 e il 2019 la valuta locale, il bolivar, ha subito un'inflazione del 10.000.000%[26]. Il Paese sudamericano, non a caso, è il settimo al mondo per utilizzo di bitcoin. Per Chainalysis "diversi Stati nei mercati emergenti tra cui Kenya, Nigeria e Vietnam sono ai primi posti dell'indice d'adozione, in gran parte perché hanno enormi volumi di

[23] The Bitcoin Standard, Saifedan Ammous, 2018
[24] Measuring Global Crypto Users, Crypto.com, 2021
[25] Infinite Market Cap
[26] Venezuela hyperinflation hits 10 million percent, CNBC

transazioni se rapportati al Pil pro capite e alla popolazione che utilizza Internet"[27].

E' proprio Internet che insieme a Bitcoin sta offrendo un'opportunità di emancipazione senza precedenti a una grossa fetta di popolazione mondiale. L'accesso al sistema finanziario tradizionale, contrariamente a quanto si potrebbe pensare, non è cosa scontata. Nel 2017 erano 1,7 miliardi le persone adulte prive di un conto in banca; 1,5 miliardi quelle con un conto ma nessun accesso al credito[28]. Si tratta di più di 3 miliardi di persone su 7,9 totali[29] escluse del tutto o in parte dal sistema economico.
Al contrario, il 59,5% della popolazione globale ha accesso a Internet[30], con cui è possibile utilizzare Bitcoin e dunque risparmiare, ricevere e inviare denaro in forma digitale, ovunque nel mondo.

Non sorprende che un Paese in via di sviluppo come El Salvador, dove il 70% della popolazione non ha un conto in banca[31], sia stato il primo in assoluto - e per ora l'unico - a rendere Bitcoin valuta a corso legale con una legge entrata in vigore nel settembre del 2021. Il Pil di El Salvador conta per il 23% - circa 6 miliardi di dollari - sulle rimesse dei cittadini emigrati che inviano denaro alle proprie famiglie rimaste nel Paese d'origine. I servizi locali di money transfer come Western Union o Money Gram applicano commissioni sulle transazioni che vanno dal 10% al 50%. Bitcoin, solamente evitando il passaggio dall'intermediario ed eliminando le commissioni potrebbe portare nelle tasche dei cittadini salvadoregni un valore aggiunto di 400 milioni di dollari all'anno.

El Salvador è inoltre un Paese dollarizzato: in fatto di politica monetaria è dunque incapace di prendere decisioni autonome ed è dipendente dalla Federal Reserve, la banca centrale statunitense. Nel testo della legge[32] che ha reso Bitcoin valuta a corso legale c'è un chiaro riferimento al fatto che l'emancipazione monetaria non riguarda solo gli individui, ma interi Stati che dipendono da valute di cui non hanno il controllo:

"*Per favorire la crescita economica della nazione è necessario autorizzare la circolazione di una moneta digitale il cui valore risponda esclusivamente a criteri di libero mercato, al fine di aumentare la ricchezza nazionale a beneficio del maggior numero di abitanti*".

---

[27] The 2021 Global Crypto Adoption Index, Chainalysis
[28] Global Findex Database
[29] Worldometer
[30] Global digital population, Statista
[31] Share of adult population with a bank or mobile money service account in El Salvador, Statista
[32] Asamblea Legislativa de El Salvador: Ley Bitcoin

- *Difesa della privacy e diritti umani*

“La privacy è necessaria per una società aperta nell'era digitale. La privacy non è segretezza. Una questione privata è qualcosa che non si vuole che il mondo intero sappia, una questione segreta è qualcosa che non si vuole che nessuno sappia. La privacy è il potere di rivelarsi selettivamente al mondo”.

Eric Hughes è un programmatore e attivista della privacy ed è considerato uno dei fondatori del movimento cypherpunk. Le righe qui riportate sono state scritte da lui nel 1993 in un documento dal titolo: *A Cypherpunk’s Manifesto*[33].

Con il termine cypherpunk si indica un movimento, attivo soprattutto tra gli anni ’80 e ’90, composto principalmente da studenti ed esperti di informatica che lottavano per preservare diritti come quello d’associazione o quello di comunicare privatamente nel mondo digitale. Il loro lavoro era guidato dall’ambizione di sviluppare strumenti che non potessero essere fermati da alcun censore, come spiegato anche da un altro membro del movimento, Wen Dai:

“*Non è mai esistito un governo che, presto o tardi, non abbia provato a ridurre le libertà dei propri cittadini e ad aumentare il controllo su di loro. Forse non ce ne sarà mai uno. Quindi, anziché convincere il nostro governo a non provarci, svilupperemo la tecnologia per impedirglielo*”.

Bitcoin è il risultato di 40 anni di ricerca e sviluppo, in gran parte portati avanti dal movimento cypherpunk, per provare a separare Stato e moneta e consegnare all’individuo il completo controllo del suo denaro. I dati dicono che ci sta riuscendo.
In Cina, per esempio, vige il Sistema di Credito Sociale, meccanismo più volte accostato ai peggiori scenari orwelliani che prevede l’assegnazione di punteggi alla popolazione in base a comportamenti e abitudini e la conseguente concessione di agevolazioni o imposizione di restrizioni in base ai punti di ognuno. Il monitoraggio include anche le informazioni più private come la situazione patrimoniale, la puntualità nei pagamenti o le eventuali insolvenze. Tale tipologia di sorveglianza sta diventando mano a mano sempre più accurata con la diffusione dello yuan digitale, la valuta di Stato emessa solamente in forma elettronica e in quanto tale programmabile e

[33] A Cypherpunk’s Manifesto

gestibile dal regime. I soldi, in tale forma, sono a tutti gli effetti un bene in comodato d'uso, non di proprietà.

Non sorprende che il governo di Pechino abbia provato a bandire Bitcoin in varie forme quasi dieci volte negli ultimi 9 anni[34]. Nonostante ciò, la Cina è il tredicesimo Paese al mondo per adozione di Bitcoin[35]: un dato sinonimo del fatto che chi vuole difendersi dalla sorveglianza di massa sta trovando uno strumento per farlo, così come chi vuole difendersi dalle persecuzioni politiche come, ad esempio, Alexei Navalny e Julian Assange.

La Fondazione Anticorruzione (Fbk) del dissidente russo Navalny è considerata dal governo di Mosca "estremista". In quanto tale i conti dell'organizzazione sono congelati ma la Fbk continua a fare vaste campagne di comunicazione grazie ai 666 bitcoin ricevuti in donazioni dal 2016 ad oggi[36]: quelli sì, inconfiscabili.
WikiLeaks, organizzazione fondata nel 2006 da Julian Assange, che, tra le altre cose, ha rivelato crimini di guerra compiuti in Afghanistan e secretati dal governo americano, ha ricevuto in donazioni 4077 bitcoin.

- *Transizione energetica*

Il tema delle emissioni è uno dei più controversi e dibattuti degli ultimi anni. Bitcoin è sotto l'attacco di istituzioni e stampa generalista da tempi non sospetti per l'utilizzo di energia sempre crescente richiesto dall'algoritmo di proof-of-work e dall'aggiustamento della difficoltà: più il network cresce, più potenza di calcolo viene coinvolta, maggiore è l'energia richiesta in assenza di soluzioni di efficientamento. Già nel gennaio 2018 il World Economic Forum scriveva che "il costo nascosto di Bitcoin" è "l'ambiente"[37].

Anche volendo tralasciare il fatto che il sistema bancario impieghi ogni anno oltre 250 terawattora[38] (ad oggi quasi il doppio di Bitcoin), le critiche omettono quasi sempre di spiegare che consumo energetico ed emissioni di CO_2 sono cose ben diverse: la quantità di inquinamento prodotta dipende in gran parte dalle fonti energetiche utilizzate. Secondo la stima più recente il 58,5%[39] del fabbisogno energetico dei miner in tutto il mondo è alimentato da fonti rinnovabili. Il dato è destinato a salire perché - come evidenziato dalla ricerca

[34] Tweet Jameson Lopp
[35] The 2021 Global Crypto Adoption Index, Chainalysis
[36] Indirizzo Bitcoin Fbk, Blockchain Explorer
[37] Tweet World Economic Forum
[38] Galaxy Digital
[39] Global Mining Data Review - Bitcoin Mining Council

di Square, azienda guidata dal fondatore di Twitter Jack Dorsey, *Bitcoin is key to an abundant, clean energy, future*[40] - le fonti rinnovabili, con il progredire della tecnologia, diventeranno via via sempre più economiche rispetto a quelle fossili e il prezzo dell'elettricità per un miner è un costo, non un ricavo: il mining rappresenta quindi un incentivo all'investimento in ricerca e sviluppo per arrivare a nuove tecnologie che possano produrre energia pulita in modo sempre più efficiente.

Non solo, Bitcoin è anche una soluzione ideale per eliminare gli sprechi energetici: uno dei grandi limiti dell'elettricità, infatti, è il costo del suo stoccaggio. A differenza di altre risorse, non è affatto semplice produrre elettricità e conservarla a lungo: in ogni istante deve esserci equilibrio tra consumo e produzione di energia. Questo diventa ancor più problematico nel caso di fonti rinnovabili come il solare, l'idroelettrico e l'eolico in cui la produzione varia frequentemente a seconda delle condizioni e del tempo. Bitcoin, tramite il mining, consente di destinare i surplus energetici - che altrimenti verrebbero dispersi - alla creazione di valore spendibile digitalmente.

Per questi motivi Bitcoin svolgerà nei prossimi decenni un ruolo da protagonista nella transizione energetica globale verso le fonti rinnovabili.

[40] Square: Bitcoin is key to an abundant, clean energy, future

4. Criptovalute, un altro paradigma

- *Il Trilemma e la decentralizzazione*

Trade-off: se ne sente parlare spesso in economia ma è un concetto che fa parte della vita di tutti i giorni. E' quella situazione in cui migliorando un aspetto di qualcosa si finisce inevitabilmente per peggiorarne un altro.
Quando la Bce immette liquidità nei mercati tramite il Quantitative Easing[41], per esempio, lo fa per stimolare la crescita economica e la dinamicità dei mercati ma la stessa azione comporta anche un aumento dei debiti pubblici e, di conseguenza, la possibile adozione di politiche conservative da parte dei governi.

Nel mondo delle criptovalute il trade-off più conosciuto è noto come *Il Trilemma* perché coinvolge tre concetti: decentralizzazione, sicurezza, scalabilità.
In una rete distribuita che scambia informazioni non si può raggiungere il massimo livello in tutti e tre gli aspetti perché il miglioramento di uno implica direttamente il peggioramento di un altro. Serve dunque stabilire delle priorità e decidere quali aspetti siano più e meno importanti: è qui la differenza chiave che traccia una profondissima linea di demarcazione tra Bitcoin e le altcoin.

Bitcoin non è una tecnologia nata dal nulla. Prima del white paper di Satoshi Nakamoto altri progetti, tutti strettamente connessi tra loro, hanno provato a creare una moneta nativa di Internet: Digicash (1989), E-Gold (1996), BitGold (1998), B-money (1998), RPow (2004). Questi tentativi, nonostante siano risultati determinanti per lo sviluppo di Bitcoin, non sono sopravvissuti alla prova del tempo per diversi motivi ma, in particolare, per una caratteristica che ne accomunava alcuni: la centralizzazione.

E' per questo motivo che Bitcoin aspira al massimo della decentralizzazione - il white paper parla persino di "distribuzione" - e della sicurezza possibili e perde dunque in scalabilità: non a caso il livello base della tecnologia, la sua blockchain, ospita circa 280.000 transazioni al giorno, troppo poche per una rete pensata per diffondersi su scala globale. Mastercard e Visa, che sono aziende e in quanto tali completamente centralizzate, processano ogni giorno rispettivamente 366 milioni e 597 milioni di transazioni[42].

---

[41] Quantitative Easing: acquisto di titoli di debito sovrano tramite il quale la Bce immette nuova liquidità nelle casse dei paesi.
[42] Bitcoin network overtakes PayPal in quarterly volume, The Independent

La decentralizzazione deve essere mantenuta con il massimo degli sforzi dalla comunità Bitcoin perché rappresenta l'essenza stessa della tecnologia ed è ciò che le conferisce valore e la rende inattaccabile. Se il network fosse centralizzato, chi lo gestirebbe potrebbe essere ricattabile (un'azienda, con un amministratore delegato e un cda, può essere messa alle strette dal proprio governo). Insomma, se qualcuno controllasse Bitcoin potrebbe arbitrariamente modificarne le caratteristiche. Non sarebbe, in poche parole, nulla di diverso rispetto a ciò che già esiste.

Una rete sicura e distribuita che possa essere utilizzata dal mondo intero non può però permettersi di consentire solamente poche centinaia di migliaia di transazioni quotidiane. E' per questo che nel 2015 è nato Lightning Network, un protocollo costruito sopra alla blockchain di Bitcoin - e per questo noto anche come *layer 2* - meno decentralizzato e sicuro rispetto al layer 1 ma in grado di consentire un numero potenzialmente infinito di transazioni istantanee in bitcoin. Idealmente il Lightning Network è pensato come un portafoglio utile per le consuete transazioni quotidiane di piccola e media entità, la blockchain è invece la cassaforte in cui conservare i risparmi o con cui effettuare pagamenti più significativi come l'acquisto di un'auto, di una casa o il trasferimento di un'eredità.

Bitcoin, in breve, è la rete più distribuita attualmente esistente. Tutte le altre criptovalute, anche se in misure diverse tra loro, sono più centralizzate e meno sicure. La natura centralizzata o semi-centralizzata del settore *cripto* rappresenta quindi un mare magnum di nuovi strumenti per scambiare valore che fa però parte di un paradigma non diverso da quello esistito finora: quello in cui il successo delle operazioni all'interno della rete è garantito e dipende da un singolo o da pochi attori. In parole più semplici, non è più la singola banca a processare la transazione ma sono i pochi soggetti coinvolti nella gestione della rete.

Le altcoin non sono rivali del settore bancario-assicurativo, ne rappresentano l'evoluzione: potranno innovare i sistemi di pagamento, di investimento, di trading, forse di risparmio, ma sempre e comunque con il requisito della fiducia in uno o più organi, pubblici o privati che siano. Bitcoin, al contrario, è ciò che può permettere di creare un vero e proprio sistema finanziario alternativo con una concreta eliminazione dell'intermediario: settore cripto e finanza tradizionale rappresentano ciò che Bitcoin vuole cambiare.

Prendiamo il caso di Ethereum, l'asset più capitalizzato del settore dopo Bitcoin e network sul quale vengono sviluppati numerosi token. In futuro l'invenzione di Vitalik Buterin - già il fatto che il creatore di Ethereum sia conosciuto e goda di significativa influenza sullo sviluppo del network rappresenta un punto di fragilità - affronterà dei cambiamenti che puntano dritti verso un accentramento di potere, così come ammesso da Buterin stesso: "C'è un'alta probabilità che la produzione di blocchi[43] finisca per essere centralizzata".[44] E' proprio la futura transizione che ci porta all'origine tecnologica della differenza tra Bitcoin e buona parte delle altcoin: *proof-of-work* contro *proof-of-stake.*

- *Proof-of-Work vs Proof-of-Stake*

Con proof-of-work e proof-of-stake si indicano due sistemi che regolano la scrittura dei blocchi in una blockchain. Se il primo conserva più efficacemente la decentralizzazione tramite l'utilizzo di potenza computazionale, il secondo è più efficiente dal punto di vista energetico ma tende alla centralizzazione nel medio-lungo periodo. Come anticipato nel secondo capitolo Bitcoin si affida alla proof-of-work e così fa anche Ethereum, la cui roadmap prevede però il passaggio alla proof-of-stake.

Se nella proof-of-work, come spiegato nel secondo capitolo, viene premiato chi dimostra di aver compiuto una certa quantità di lavoro spendendo risorse, nella proof-of-stake viene invece premiato chi dimostra di detenere una data quantità di capitale investito nell'asset. A stabilire chi ha diritto a scrivere il nuovo blocco della blockchain è una vera e propria lotteria, dove per poter partecipare è necessario depositare una quantità minima di denaro.

Nel caso di Ethereum 2.0 serviranno almeno 32 Ether[45]. Le chances di scrivere il blocco, e guadagnare quindi la ricompensa, aumentano proporzionalmente al crescere della somma *in stake*, cioè investita e bloccata. Di fatto più denaro si deposita, maggiore è la possibilità di riceverne e, di conseguenza, aumenta anche la disponibilità di denaro da depositare, che a sua volta si traduce in ancor più chances di scrivere il blocco successivo: un ciclo senza fine. E' per questo che Buterin ha parlato di produzione dei blocchi centralizzata: si tratta di un sistema in cui nel medio-lungo termine i ricchi

[43] Così come in Bitcoin, in Ethereum la produzione dei blocchi porta alla remunerazione di chi ha scritto il blocco con nuova moneta (Ether). Se la produzione dei blocchi tende alla centralizzazione, la nuova moneta finirà per arricchire solo i pochi destinati a tale attività.
[44] Endgame, Vitalik Buterin
[45] Ether: moneta della rete Ethereum

diventeranno sempre più ricchi e dove il numero di miner tenderà a ridursi sempre più creando a tutti gli effetti un oligopolio.

- *Ethereum e governance*

Del fondatore di Bitcoin, come detto, si conosce solamente lo pseudonimo e il suo ultimo contributo alla comunità risale al 2010: da allora non vi è più traccia di Satoshi Nakamoto. L'assenza di una leadership riconosciuta è fondamentale per l'autentica decentralizzazione di un network perché l'influenza del fondatore non può risultare neutra nello sviluppo della tecnologia.

Quella di Bitcoin è però una caratteristica unica e tutte le altre criptovalute hanno uno o più creatori che le controllano direttamente o indirettamente oppure, ottimisticamente, hanno un ascendente non trascurabile sulla community. E' il caso di Ethereum, il cui fondatore Vitalik Buterin non solo è noto ma è anche molto attivo nelle discussioni relative allo sviluppo della sua creatura e ha una forte voce in capitolo all'interno dell'Ethereum Foundation. Esatto, esiste anche una fondazione le cui indicazioni risultano spesso determinanti quando arriva il momento di prendere decisioni strategiche. E' vero che Buterin e la Ethereum Foundation non possono cambiare il corso della piattaforma con un click, ma è indubbio che l'approvazione finale dei più importanti aggiornamenti alla rete passi soprattutto dal loro consenso. Non è un caso se la politica monetaria di Bitcoin ha conservato la sua immutabilità negli anni, mentre quella di Ethereum è cambiata più e più volte.

La minor distribuzione di Ethereum è data anche dalla struttura dei nodi: attivarne uno - entrare quindi a far attivamente parte del network globale e contribuire alla sua decentralizzazione - è più costoso e meno accessibile rispetto all'attivazione di un nodo Bitcoin. Se per utilizzare un full-node[46] Bitcoin bastano ad oggi circa 400 GB di memoria su hard disk, 2 GB di RAM e una buona connessione Internet, installare un nodo completo Ethereum richiede 6 TB di memoria SSD, 16 GB di RAM e una connessione di 2,5 MB/s in download. Di fatto Ethereum è una tecnologia meno accessibile rispetto a Bitcoin: lo dimostra il numero dei nodi che ospitano i protocolli: si stima che in tutto il mondo siano attivi circa 50.000 nodi Bitcoin[47] e 5.000 nodi Ethereum[48].

[46] Esistono vari tipi di nodi, ma il nodo più completo è il full-node: è ciò che permette di mantenere copia di tutti i dati necessari per non doversi fidare di nessun altro membro della rete e godere quindi di completa autonomia.
[47] Bitcoin Node Branches
[48] Ethernodes.org

Il risultato è che buona parte degli utenti senza un nodo a casa si affida a servizi centralizzati come Infura che permettono comunque l'utilizzo del protocollo affidandosi a loro volta all'hosting via cloud. Oggi quasi il 70% dei nodi Ethereum è ospitato da cloud privati[49] e il 40% di questi è gestito da Amazon Web Services: cosa significa? Che circa il 25% di tutto il carico di lavoro del protocollo a livello globale è eseguito su Amazon Web Services[50].

[49] Ethereum Mainnet Statistics
[50] Blockchain in Aws

Conclusioni

Le caratteristiche di Bitcoin lo rendono una singolarità nella storia dello scambio di valore: le sue proprietà non possono essere replicate. Bitcoin è la scoperta dell'assoluta scarsità digitale e l'unico modo per proteggere tale autenticità è difendere ad ogni costo la decentralizzazione, l'incensurabilità e l'immutabilità del protocollo.

Le altcoin - come spiegato anche dall'autore della newsletter *Bitcoin Tech Talk,* Jimmy Song - sono "decentralizzate solo di nome"[51] e la loro governance è accentrata in tutto ciò che conta. Questo significa che comportano rischi rilevanti sia interni (appropriazione indebita, inflazione, censura) che esterni (regolamenti, acquisizioni forzate, tasse). In altre parole, si tratta di progetti vulnerabili.

"*Se hai intenzione di investire in qualcosa di centralizzato, dovresti investire in un sistema finanziario che ha alle spalle centinaia di anni di storia istituzionale, non in sistemi che fingono di essere decentralizzati o in nuove nozioni di governance del signore delle mosche*"[52].

Nick Szabo

Scarsità e indipendenza da ogni forma di controllo centrale rendono Bitcoin la tecnologia adatta a creare la moneta del libero mercato per eccellenza. Bitcoin è la realizzazione del sogno cypherpunk, ciò che rompe il monopolio statale dell'emissione di denaro, la separazione tra Stato e moneta. Per questo motivo è spesso associato alle teorie liberali della scuola economica austriaca. Uno dei suoi massimi esponenti, Friedrich von Hayek, ha scritto di come la storia sia in gran parte costituita da una serie di fenomeni inflazionistici creati intenzionalmente dai governi[53]. Perciò, ha detto in un'intervista nel 1984, "non credo che avremo mai più una moneta solida prima di eliminare il monopolio del governo. Non possiamo eliminarlo violentemente. Tutto ciò che possiamo fare è introdurre qualcosa che non possano fermare"[54]. Un qualcosa che è nato il 3 gennaio 2009.

---

[51] Altcoins are DINOs (Decentralized in Name Only), Jimmy Song
[52] Tweet Nick Szabo
[53] La denazionalizzazione della moneta, Friedrich von Hayek,
[54] Friedrich von Hayek, estratto da una video intervista del 1984 all'università di Friburgo.

Fonti

1. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008
2. Bitcoin - The End of Money As We Know It, 2020
3. Nick Szabo, Shelling Out: The origins of Money, Nakamoto Institute, 2002
4. Oregold - Tutto l'oro del mondo
5. Messari
6. Bitcoin Core
7. Blockstream Bitcoin Explorer
8. Case Bitcoin
9. SquawkCNBC, intervista a Rick Rieder
10. Modello Stock to Flow, Plan B
11. The Bitcoin Standard, Saifedan Ammous, 2018
12. Measuring Global Crypto Users, Crypto.com, 2021
13. Infinite Market Cap
14. Venezuela hyperinflation hits 10 million percent, CNBC
15. The 2021 Global Crypto Adoption Index, Chainalysis
16. Global Findex Database
17. Worldometer
18. Global digital population, Statista
19. Share of adult population with a bank or mobile money service account in El Salvador, Statista
20. Asamblea Legislativa de El Salvador: Ley Bitcoin
21. A Cypherpunk's Manifesto
22. Tweet Jameson Lopp
23. Indirizzo Bitcoin Fbk, Blockchain Explorer
24. Tweet World Economic Forum
25. Galaxy Digital
26. Global Mining Data Review - Bitcoin Mining Council
27. Square: Bitcoin is key to an abundant, clean energy, future
28. Bitcoin Mining Council: Global Bitcoin Mining Data Rewiew
29. Bitcoin network overtakes PayPal in quarterly volume, The Independent
30. Bitcoin Node Branches
31. Ethernodes.org
32. Ethereum Mainnet Statistics
33. Blockchain in Aws
34. Altcoins are DINOs (Decentralized in Name Only), Jimmy Song
35. Tweet Nick Szabo
36. La denazionalizzazione della moneta, Friedrich von Hayek,
37. Friedrich von Hayek, estratto da una video intervista del 1984 all'università di Friburgo