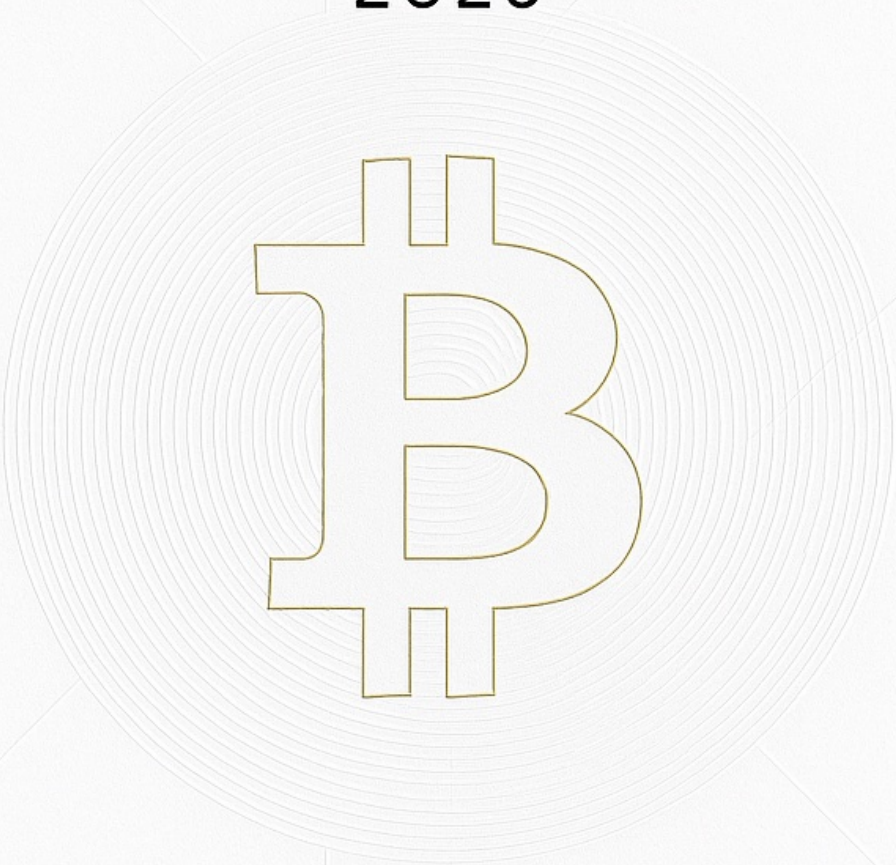
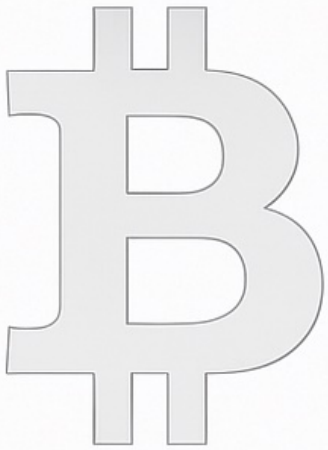
BITCOIN FUTURO

2025



The unstoppable financial infrastructure



Il Futuro di Bitcoin: Verso un'Infrastruttura Finanziaria Globale

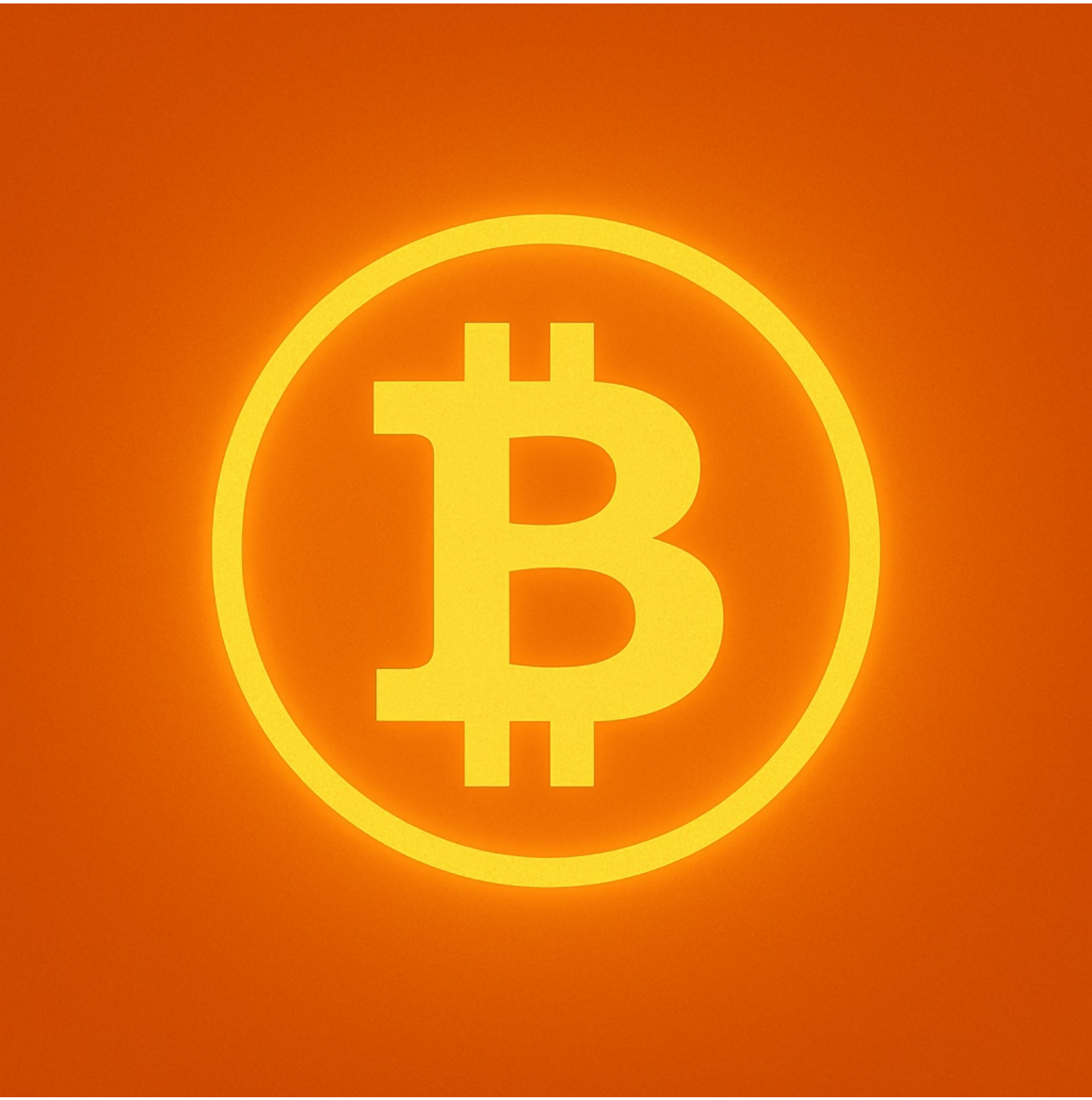
A cura Gianpaolo Marcucci

Magazine periodico libero dello Human Advisor Project

humanadvisorproject.org

Info whatsapp: +39 339 651 7088

HUMAN ADVISOR PROJECT
HELP HUMAN HELP HUMANITY



Indice


DECENTRALIZED * PEER TO PEER *

Introduzione

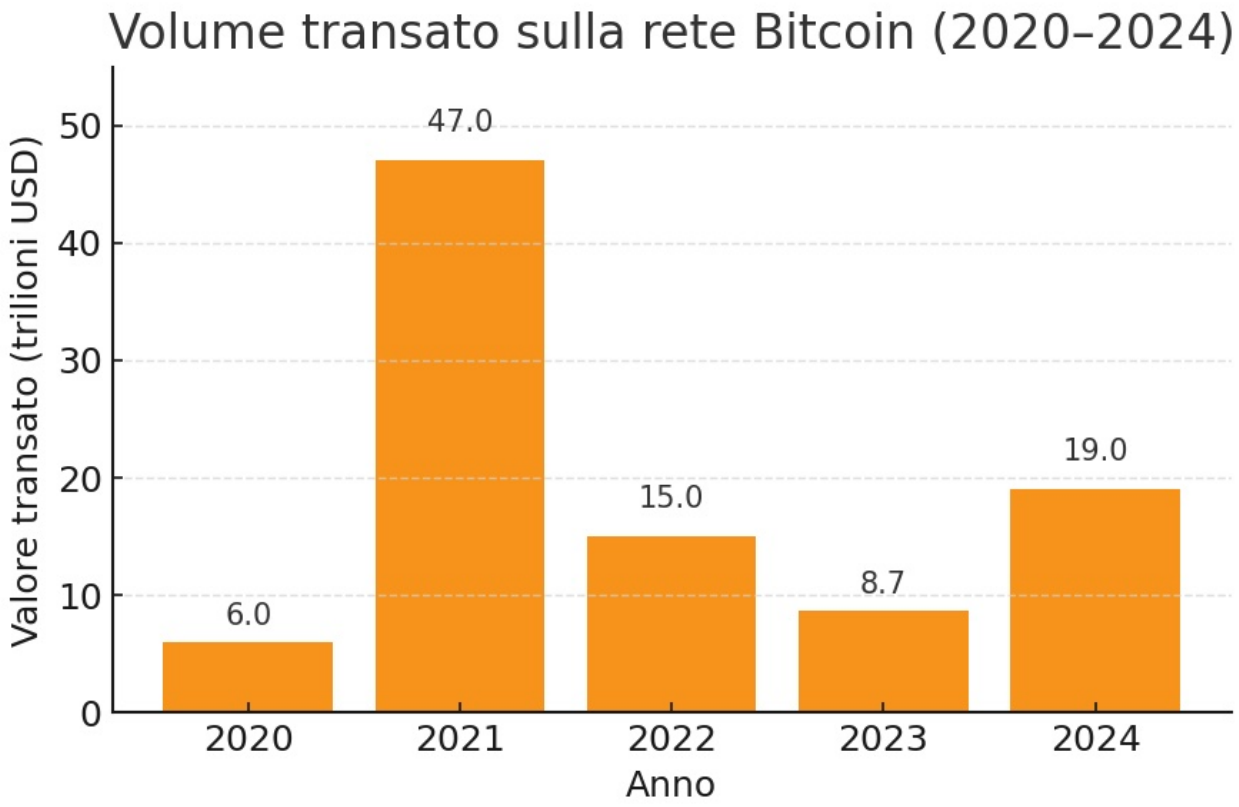
Bitcoin, nato nel 2009 come moneta digitale sperimentale, è progressivamente evoluto fino a essere considerato non solo un asset finanziario ma anche una potenziale infrastruttura per la finanza globale. In questi quindici anni, la sua capitalizzazione di mercato è passata da pochi milioni a sfiorare i 2.000 miliardi di dollari, e la rete Bitcoin ha elaborato volumi di transazioni paragonabili ai grandi sistemi di pagamento internazionali. Nel 2024, ad esempio, la blockchain di Bitcoin ha regolato pagamenti per oltre 19 mila miliardi di dollari, più del doppio rispetto all'anno precedente – un dato che "*dimostra in modo decisivo che Bitcoin è sia riserva di valore sia mezzo di scambio*", come ha osservato Pierre Rochard di Riot Platforms. Parallelamente, l'interesse di istituzioni finanziarie di primo piano è esploso: Larry Fink, CEO di BlackRock (il più grande asset manager mondiale), ha dichiarato che Bitcoin e la tokenizzazione potrebbero "rivoluzionare la finanza", riconoscendo Bitcoin come un "asset internazionale" e "oro digitale" .

In questo numero speciale, esploriamo il futuro di Bitcoin non tanto come semplice moneta alternativa, ma come infrastruttura finanziaria emergente su scala globale. Approfondiremo i seguenti temi chiave:

- Bitcoin come Infrastruttura Finanziaria Globale – La visione di Bitcoin quale livello base di un nuovo sistema finanziario: proprietà, ruolo nel contesto macroeconomico e paralleli con le infrastrutture tradizionali.
- Tecnologia e Scalabilità (Lightning Network e Oltre) – Le soluzioni di scaling come Lightning Network e i nuovi modelli di layerizzazione che consentono a Bitcoin di gestire volumi elevati di transazioni.
- Integrazione con la Finanza Tradizionale – ETF su Bitcoin, adozione istituzionale, evoluzione normativa globale e l'ingresso di Bitcoin nei portafogli e nei mercati regolamentati.
- Bitcoin e Intelligenza Artificiale – Analisi inedite sulle possibili sinergie tra Bitcoin e AI: dall'economia machine-to-machine resa possibile dai micropagamenti di Lightning, alle implicazioni di AI che utilizzano Bitcoin come infrastruttura di valore.
- Sicurezza, Decentralizzazione e Impatto Energetico – Lo stato attuale e futuro della sicurezza della rete Bitcoin (hash rate, distribuzione geografica dei miner) e

della sua sostenibilità energetica, elementi cruciali per un'infrastruttura finanziaria globale affidabile.

- Prospettive Economiche e Geopolitiche – Implicazioni di ampio respiro: Bitcoin come riserva di valore in un contesto di instabilità monetaria, il rapporto con le politiche delle banche centrali, e possibili scenari geopolitici in un mondo che adotta Bitcoin come standard finanziario.



Bitcoin come Infrastruttura Finanziaria Globale

Bitcoin viene spesso paragonato all'oro digitale, ma la sua vera portata potrebbe essere più simile a quella di una rete di pagamento e settlement globale. In questa sezione esamineremo Bitcoin come infrastruttura finanziaria di base, analizzando le sue caratteristiche di fondo e il ruolo che potrebbe giocare nel sistema economico mondiale futuro.

Caratteristiche di un'infrastruttura monetaria globale: La rete Bitcoin opera 24 ore su 24, 7 giorni su 7, permettendo il trasferimento di valore senza confini nazionali e senza bisogno di intermediari centrali. Ogni ~10 minuti, una nuova blocco di transazioni viene confermato, offrendo finalità (settlement) alle transazioni registrate. A differenza dei sistemi tradizionali (come i circuiti bancari o SWIFT) che possono avere orari di chiusura o tempi di regolamento di 1-2 giorni, Bitcoin fornisce una base costantemente attiva e resistente alla censura per lo scambio di valore. Nel corso del 2024 la rete Bitcoin ha elaborato transazioni per un valore totale di circa 19 trilioni di dollari , una cifra in crescita rispetto agli anni precedenti e paragonabile ai volumi annuali dei maggiori sistemi di pagamento tradizionali. Questa capacità di regolare pagamenti su larga scala indica come Bitcoin stia già funzionando de facto come un livello infrastrutturale per trasferimenti di valore globali, sebbene finora impiegato principalmente per grandi transazioni e come riserva di valore.

Una proprietà fondamentale che rende Bitcoin interessante come infrastruttura finanziaria globale è proprio questa politica monetaria algoritmica e trasparente. L'offerta di Bitcoin è predeterminata e inalterabile salvo consenso quasi unanime della rete: circa il 93% dei Bitcoin che esisteranno è già stato emesso, e l'inflazione residua scenderà sotto l'1% annuo dopo il halving del 2024. Entro circa il 2140 l'emissione di nuovi Bitcoin cesserà, fissando l'offerta totale a 21 milioni. Questa prevedibilità conferisce a Bitcoin caratteristiche da riserva di valore a lungo termine in un contesto globale dove molte valute fiat vedono un costante aumento di offerta. In termini pratici, attori istituzionali iniziano a considerare Bitcoin come un hedge contro l'inflazione o la svalutazione monetaria locale. "Invece di investire nell'oro come copertura contro l'inflazione o la svalutazione di una valuta nazionale… Bitcoin è un asset internazionale non basato su una singola valuta, e può rappresentare un'alternativa", ha affermato Larry Fink nel 2023 . Dal punto di vista di infrastruttura finanziaria, ciò significa che Bitcoin potrebbe servire non solo come mezzo di scambio, ma anche come base per riserve e collaterali in un sistema economico globalizzato, analogamente a come l'oro fungeva da base nel sistema di Bretton Woods (pur con le dovute differenze tecnologiche).

Bitcoin come Settlement Layer internazionale: Oltre all'aspetto di riserva di valore, Bitcoin si propone come un strumento di regolamento finale (settlement) tra parti che

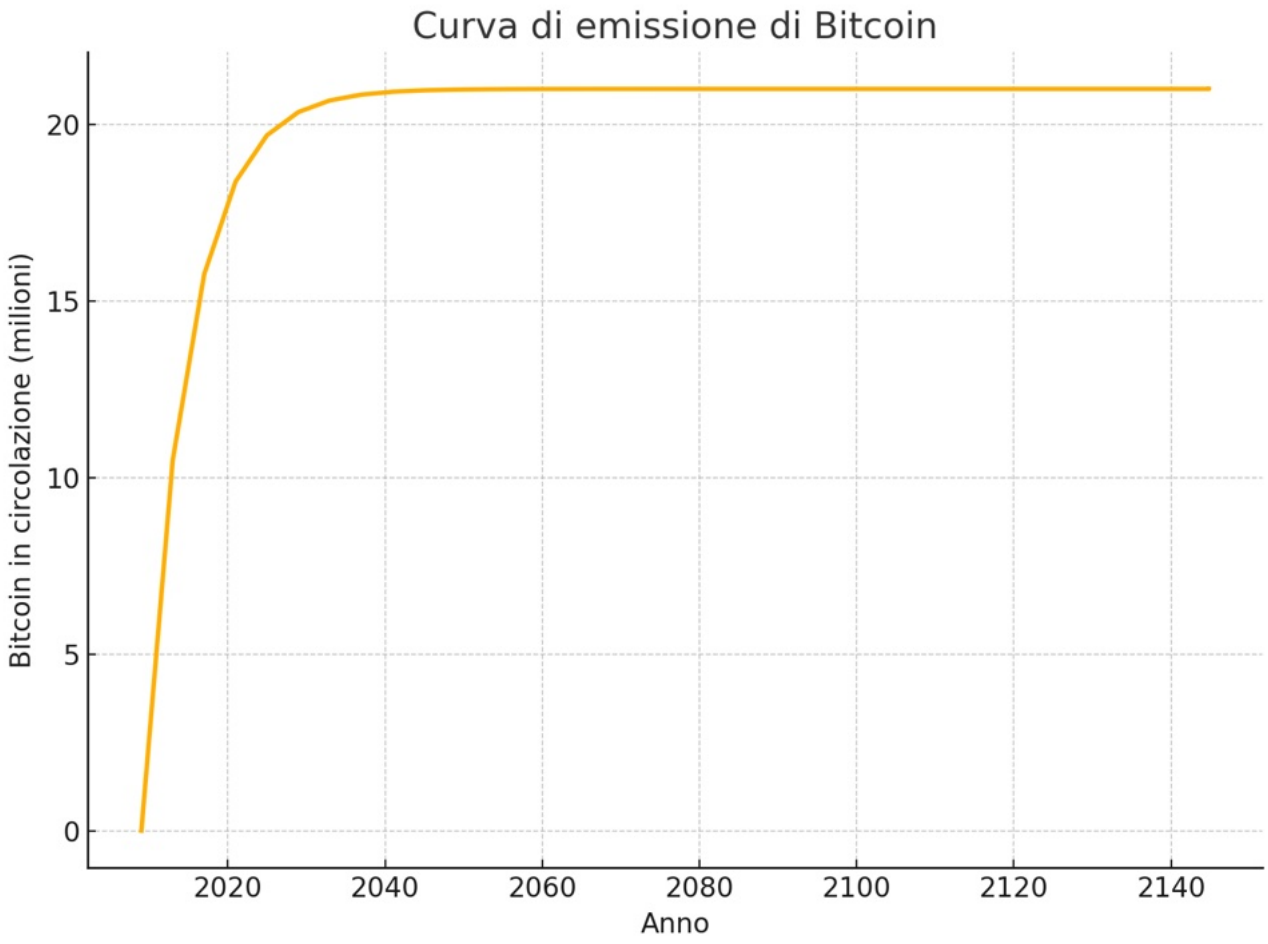
non devono fidarsi l'una dell'altra. Immaginiamo banche centrali, istituzioni finanziarie o persino governi che utilizzino Bitcoin per regolare saldi internazionali: una transazione Bitcoin può trasferire valori elevatissimi con costi marginali e senza rischio di controparte, poiché la finalizzazione è garantita dalla proof-of-work e dalla distribuzione globale dei nodi. Già oggi esistono esempi in scala ridotta: in alcuni corridoi valutari soggetti a sanzioni o restrizioni (si pensi a certe rimesse di emigrati o scambi tra paesi soggetti a embargo), Bitcoin è stato utilizzato come mezzo di scambio neutrale. A livello ufficiale, il caso di El Salvador – che nel 2021 ha reso Bitcoin moneta a corso legale – ha aperto scenari sull'uso di Bitcoin nei pagamenti di stato e nelle rimesse internazionali, anche se l'adozione di massa nel paese è ancora moderata. Tuttavia, questi esempi suggeriscono che Bitcoin può agire come infrastruttura alternativa quando i canali tradizionali sono lenti, costosi o politicamente filtrati.

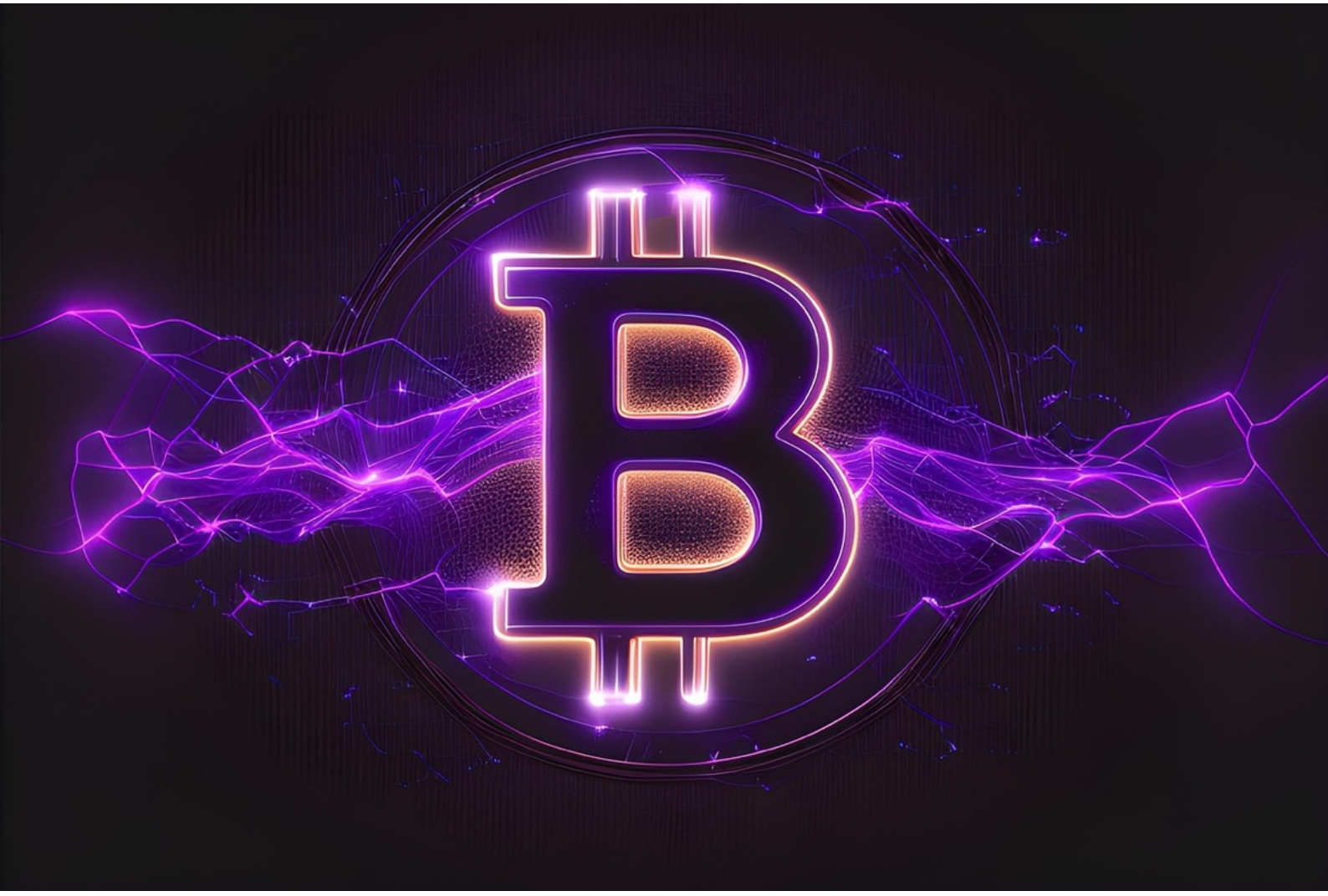
Un vantaggio infrastrutturale importante di Bitcoin è la sua neutralità e resistenza alla censura. La rete non distingue tra utenti o provenienza delle transazioni: chiunque (persona, azienda o programma software) può trasferire valore a chiunque altro con la garanzia che nessuna autorità possa intervenire per bloccare o revertire la transazione, fintanto che questa rispetta le regole del protocollo. Ciò è particolarmente rilevante in un contesto geopolitico frammentato: Bitcoin può fungere da livello di base neutrale, analogo a un "HTTPS del denaro", su cui possono innestarsi applicazioni e valute di livello superiore. In questa visione, valute nazionali o stablecoin potrebbero utilizzare la rete Bitcoin come infrastruttura di settlement, proprio come oggi diverse applicazioni utilizzano Internet come infrastruttura di comunicazione.

Sfide e limiti attuali: Va notato che ad oggi l'uso di Bitcoin come piattaforma di pagamento globale è limitato da alcuni fattori. Il throughput on-chain di Bitcoin è modesto (circa 5-7 transazioni al secondo teoriche nel blocco base da 1 MB, anche se con SegWit e batch si ottiene di più) rispetto ai circuiti tradizionali come Visa. Inoltre, la volatilità del tasso di cambio BTC/USD rende difficile per Bitcoin fungere da unità di conto o mezzo di scambio stabile per beni e servizi. Questi limiti sono però al centro di intensi sforzi di mitigazione: la scalabilità viene affrontata tramite soluzioni di second layer (vedi sezione seguente sul Lightning Network) e l'integrazione di stablecoin ancorate a valute fiat, mentre la volatilità potrebbe ridursi con l'aumentare della capitalizzazione e con l'ingresso di investitori a lungo termine (che rendono la domanda di Bitcoin più stabile). In prospettiva, se Bitcoin venisse utilizzato soprattutto come infrastruttura sottostante – ad esempio per trasferire dollari tokenizzati o altre attività – la questione della volatilità sarebbe aggirata mantenendo il BTC come "rail" e non necessariamente come valuta di spesa diretta.

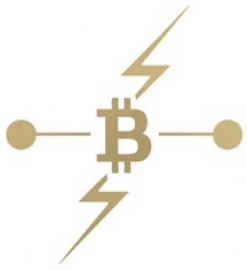
In conclusione, Bitcoin mostra molti attributi di una infrastruttura finanziaria emergente: è globale, aperta, neutrale e resistente. Come ha sottolineato BlackRock nella sua lettera agli investitori del 2025, "se gli USA non controlleranno il proprio debito pubblico, rischiano di perdere [il ruolo di valuta di riserva] a favore di asset digitali come Bitcoin" . Questo riconoscimento – proveniente dal gestore di patrimoni più grande al mondo –

indica che Bitcoin è ormai considerato un elemento da tenere in conto nell'evoluzione del sistema finanziario globale. Nelle prossime sezioni vedremo come la tecnologia di Bitcoin stia progredendo per rispondere alle sfide di scala e usabilità (Lightning Network), come il mondo istituzionale stia abbracciando Bitcoin, e quali innovazioni stanno nascendo al suo interno che potrebbero ampliare ulteriormente il suo ruolo infrastrutturale.





Tecnologia e Scalabilità: Lightning Network e nuovi Layer



Uno degli aspetti fondamentali per il futuro di Bitcoin come infrastruttura globale è la sua scalabilità tecnologica. La rete base di Bitcoin (Layer 1) ha limitazioni intenzionali in termini di capacità transazionale, utili a garantirne la decentralizzazione e sicurezza, ma che ne impediscono l'uso per masse di micro-transazioni quotidiane a livello mondiale. La risposta a questo limite è rappresentata dallo sviluppo di soluzioni di secondo livello (Layer 2) e di nuovi modelli di "layerizzazione" che permettono di aumentare ordini di grandezza sia il numero di transazioni al secondo, sia la flessibilità dei casi d'uso, senza sovraccaricare la blockchain principale. In questa sezione esploriamo la tecnologia del Lightning Network – la principale rete di secondo livello di Bitcoin – e altre innovazioni emergenti (sidechain, Fedimint, ecc.), analizzando come insieme possano costituire un vero e proprio stack multilivello simile a quello delle reti dati (ad esempio, con Bitcoin base come "TCP/IP del valore" e Lightning come "HTTP" delle microtransazioni).

Lightning Network: la rete fulminea di Bitcoin – Il Lightning Network (LN) è un protocollo sovrapposto alla blockchain di Bitcoin che consente transazioni istantanee e a bassissimo costo tra due utenti, sfruttando canali di pagamento off-chain. Proposto concettualmente nel 2015 da Joseph Poon e Thaddeus Dryja (Lightning Network whitepaper), LN è diventato operativo sul mainnet di Bitcoin nel 2018 e da allora è cresciuto in modo significativo. Il funzionamento base prevede che due parti aprano un canale di pagamento mediante una transazione sulla blockchain di Bitcoin; all'interno di questo canale, possono scambiarsi fondi con transazioni immediate che non vengono registrate singolarmente on-chain, ma solo contabilizzate tra le parti. Solo quando il canale viene chiuso, lo stato finale (saldo) viene scritto sulla blockchain. Inoltre, attraverso un meccanismo di instradamento a più hop, un utente può inviare un pagamento ad un altro anche senza un canale diretto tra loro, sfruttando una rete di nodi intermedi collegati da canali (analogo al routing dei pacchetti in Internet). Questo consente pagamenti peer-to-peer rapidi su scala globale, con commissioni minime, mantenendo la sicurezza delle transazioni grazie all'uso di smart contract (HTLC – Hash Time-Locked Contracts) che assicurano che ogni nodo intermedio riceva la propria quota solo se la transazione viene completata end-to-end.

Dal 2018 ad oggi, la capacità e dimensione del Lightning Network sono aumentate costantemente. Al 2024 la rete contava oltre 15.000 nodi pubblici interconnessi da quasi 54.000 canali aperti, per una liquidità totale di circa 5.000 BTC (oltre 270 milioni di dollari) bloccati nei canali . Sebbene questi numeri siano piccoli rispetto al sistema finanziario globale, il trend è in forte crescita: un report di River Financial ha stimato che il numero di transazioni instradate su Lightning è aumentato di 12 volte (1212%) in due anni, passando da ~500 mila transazioni nel mese di agosto 2021 a 6,6 milioni ad

agosto 2023 . Questo tasso di crescita ha portato il throughput stimato di LN a circa 2,5 transazioni al secondo (tps) – oltre la metà del throughput medio on-chain di Bitcoin (~4,4 tps) – segno che Lightning sta già oggi alleggerendo la catena principale in modo significativo . Nonostante il cosiddetto "inverno cripto" 2022-2023, che ha visto il prezzo di Bitcoin calare e l'interesse di ricerca web sul Lightning diminuire (-45%), l'utilizzo di Lightning è esploso in termini di volumi reali . Ciò indica che dietro le quinte si sta formando una infrastruttura di pagamenti sempre più utilizzata per casi d'uso concreti.

Gli utilizzi di Lightning Network emersi recentemente vanno oltre la semplice transazione fra due individui: micropagamenti all'interno di applicazioni e servizi digitali, mance istantanee sui social network (es. tipping su piattaforme come Nostr o su Twitter tramite servizi come Strike), pagamenti streaming (pagare pochi satoshi al minuto per contenuti come podcast, video, articoli a consumo) e addirittura ambiti come il gaming online, dove Lightning viene utilizzato per trasferire piccolissime somme come ricompense o fee di partecipazione in tempo reale. Secondo River, i settori di gaming, social tipping e streaming sono stati tra i maggiori driver della crescita, contribuendo al 27% dell'incremento totale delle transazioni . Questi modelli erano impraticabili con i sistemi di pagamento tradizionali (le commissioni avrebbero superato l'importo trasferito), ma Lightning rende economicamente sostenibili transazioni anche da pochi centesimi o meno, aprendo la strada a una "economia dei micropagamenti" finora mai realizzata su larga scala.

Un esempio concreto di innovazione abilitata da Lightning è l'integrazione con il mondo dell'intelligenza artificiale, di cui parleremo in dettaglio più avanti. In breve, Lightning permette a agenti software o AI di effettuare pagamenti automatici: Lightning Labs nel 2023 ha dimostrato strumenti che consentono a un modello AI (come GPT) di tenere e inviare Bitcoin autonomamente . Un potenziale caso d'uso illustrato è quello di un'AI che interroga un'altra AI tramite un'API a pagamento: usando il protocollo L402 (un'estensione di HTTP 402 Payment Required con autenticazione via pagamenti Lightning), un agente può pagare pochi satoshi per una chiamata API, ricevere la risposta e verificare che sia soddisfacente prima di pagare ulteriormente . Si intravede qui una futura economia machine-to-machine dove dispositivi e algoritmi transano valore istantaneamente l'uno con l'altro – uno scenario reso possibile quasi esclusivamente da sistemi come Lightning, data la necessità di pagamenti granulari e programmabili.

Nuovi modelli di layerizzazione su Bitcoin: Lightning Network è la soluzione di secondo livello più affermata, ma non l'unica. La comunità Bitcoin sta sperimentando una varietà di approcci per estendere funzionalità e scalabilità, creando una sorta di ecosistema multi-strato sopra la blockchain principale:

- Sidechain e Drivechain: Le sidechain sono blockchain separate, ancorate a Bitcoin tramite un peg (1:1 con BTC) che permette di spostare Bitcoin avanti e indietro tra la catena principale e quella laterale. Esempi sono Liquid (di Blockstream) e Rootstock (RSK). Liquid offre transazioni rapide (finalità ~1 min) con funzionalità come asset emittibili e privacy migliorata (confidential

transactions), già usata da alcune istituzioni per grandi trasferimenti e scambi OTC. Rootstock fornisce funzionalità di smart contract compatibili con Ethereum (EVM) ma garantite da Bitcoin (i BTC peggati vengono usati come gas sulla sidechain). Le sidechain possono alleggerire la catena madre spostando specifici tipi di attività su reti dedicate (es. Liquid per il trading tra exchange, RSK per i contratti). La proposta delle drivechain (ancora in fase di discussione) mira a rendere più facile la creazione di sidechain agganciate a Bitcoin, con un meccanismo che coinvolge i miner nel controllo del peg (BIP300-301). Se attuate, potrebbero dare vita a molte catene specializzate (per privacy, smart contract, etc.) senza modificare il protocollo Bitcoin di base, sebbene esistano dibattiti sui rischi (es. centralizzazione nei miner).

- Fedimint e federazioni di custodia (Chaumian e-cash): Una delle innovazioni più interessanti è il concetto di Fedimint (Federated Mint) – una federazione di nodi che custodisce collettivamente fondi Bitcoin e in cambio emette token e-cash (IOU digitali) spendibili con forte privacy. Si tratta di un'implementazione moderna delle idee di Chaumian e-cash degli anni '80, applicata a Bitcoin. In pratica, un gruppo di entità di fiducia locale (i guardian della federazione) gestisce un wallet multi-firma dove gli utenti depositano BTC; gli utenti ricevono in cambio token anonimi (criptati con firme cieche) che possono scambiarsi liberamente con la garanzia crittografica che nessuno, nemmeno i gestori, possa tracciare chi spende cosa. Quando un utente vuole uscire, può riscattare i token per riavere BTC on-chain. La magia avviene collegando Fedimint a Lightning Network: i token e-cash possono essere inviati tramite Lightning, permettendo pagamenti istantanei anonimi che però alla fine regolano in Bitcoin. Il protocollo Fedimint è ancora in fase di sviluppo attivo (ha ricevuto attenzione e finanziamenti nel 2022), ma promette di unire scalabilità, privacy e custodia comunitaria . Potrebbe rivelarsi particolarmente utile in paesi emergenti con scarsa infrastruttura bancaria: comunità locali potrebbero gestire le proprie banche federate Bitcoin, beneficiando di privacy e commissioni nulle nelle transazioni interne, il tutto interoperabile con l'ecosistema Bitcoin più ampio . In termini di "layer", Fedimint può essere visto come un terzo layer (L3) sopra Lightning: utenti comuni transano con token e-cash all'interno della federazione (L3), le federazioni si regolano tra loro via Lightning (L2), che a sua volta poggia su Bitcoin (L1).

- Asset tokenizzati su Bitcoin (es. Stablecoin su Lightning): Un'altra direzione cruciale è l'estensione della rete per supportare altri asset oltre a BTC. Nel 2023-2024, Lightning Labs ha sviluppato e rilasciato il protocollo Taproot Assets (ex Taro) che consente di emettere token sulla blockchain Bitcoin (grazie a Taproot) e trasferirli su Lightning Network . Ciò significa poter avere, ad esempio, stablecoin in USD o altre valute che viaggiano sui canali Lightning con la stessa velocità e economicità dei pagamenti BTC. Taproot Assets ricicla la liquidità Bitcoin esistente su LN come liquidità di instradamento per i token: in pratica un nodo può inoltrare token (es. "L-USD") ad altri convertendoli e riconvertendoli automaticamente in BTC lungo il percorso . Questo rende Bitcoin un "routing currency" globale per l'Internet del denaro . Le implicazioni sono enormi: utenti in

paesi emergenti con forte domanda di dollari digitali potranno detenere e trasferire stablecoin su un'infrastruttura Bitcoin, beneficiando della sicurezza e apertura della rete. Come notano gli sviluppatori, "la domanda globale di stablecoin è innegabile, specialmente nei mercati emergenti", e dare a questi utenti accesso a Lightning permette di unire la stabilità del dollaro con la robustezza di Bitcoin . Già nel periodo di test, oltre 170.000 asset sono stati creati on-chain con Taproot Assets , e a luglio 2024 il protocollo è entrato in funzione sul mainnet. Possiamo immaginare un futuro in cui Lightning diventa una rete multi-valuta, dove BTC funge da collante e riserva di ultima istanza, ma circolano anche token rappresentativi di valute fiat, materie prime, crediti, ecc. In tal senso, Bitcoin si evolverebbe davvero come infrastruttura finanziaria universale, non solo per transare Bitcoin stesso ma qualsiasi valore digitalizzato.

- Channel factories, Ark e altri: Sul fronte dell'ottimizzazione di Lightning stesso, si studiano tecniche come le channel factories (che permettono a gruppi di utenti di creare canali multipli con una sola transazione on-chain, migliorando l'efficienza) e il progetto più recente chiamato Ark. Ark, proposto nel 2023, mira a combinare elementi di CoinPool e Lightning per ottenere pagamenti off-chain non custodiali con un minor grado di interattività e senza necessità di liquidità di routing, migliorando privacy e scalabilità. Senza entrare nei dettagli tecnici, queste innovazioni puntano a ridurre ulteriormente la dipendenza dalla blockchain L1: idealmente, milioni di utenti potrebbero transare quotidianamente con un numero minimo di transazioni on-chain aggregate. Anche l'introduzione di MuSig e Taproot (nel 2021) ha aperto la strada a canali Lightning multi-firma più efficienti e riservati, e a funzionalità come eltoo (un'alternativa al meccanismo di penalità dei canali, che richiede l'attivazione di sighash ANYPREVOUT) per rendere la gestione dei canali più semplice.

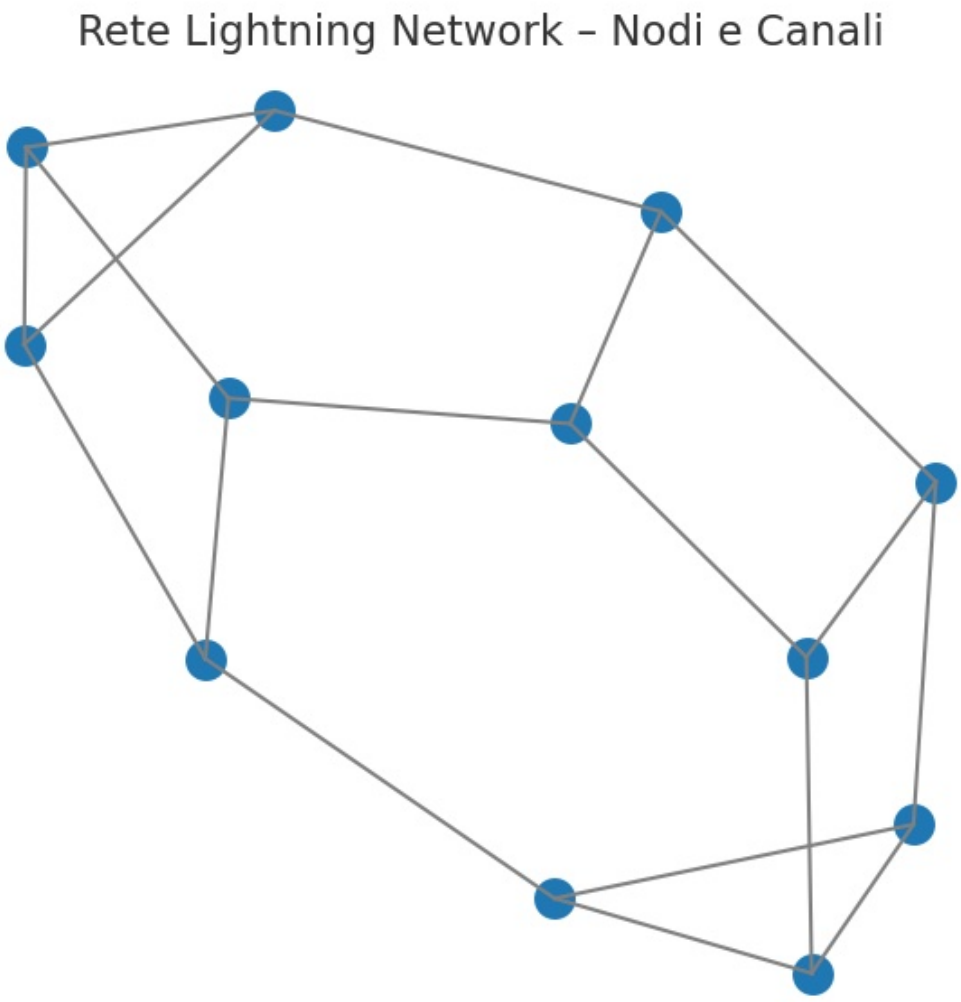
Verso un ecosistema a più strati: Sommando tutti questi sviluppi, la direzione tecnologica è chiara: Bitcoin sta diventando il fondamento di un'intera pila di protocolli finanziari. Il Layer 1 rimane la radice di sicurezza, adatto a transazioni finali, regolamenti di grande importo e ancoraggio di altri layer. Il Layer 2 (Lightning, sidechain, ecc.) offre velocità, programmabilità e funzionalità aggiuntive, scaricando dalla mainnet la maggior parte delle transazioni quotidiane. Il Layer 3 e oltre (Fedimint, applicazioni specifiche) costruiscono servizi di livello ancora più alto, ottimizzati per casi d'uso particolari (privacy massima, integrazione con AI, finanza decentralizzata, ecc.), pur rimanendo interoperabili con l'ecosistema Bitcoin sottostante.

Da un punto di vista di infrastruttura globale, questo significa che Bitcoin non è statico ma si espande e adatta per assorbire esigenze prima considerate fuori portata. I critici spesso sottolineavano l'incapacità di Bitcoin di gestire pagamenti di tutti i giorni per miliardi di persone; la risposta emergente è che forse non ne ha bisogno: così come Internet ha livelli e protocolli diversi per diversi scopi (non ogni comunicazione avviene tramite i router di base), anche Bitcoin avrà livelli differenziati. L'utente medio in futuro potrebbe utilizzare un wallet Lightning o Fedimint per le spese quotidiane in varie valute tokenizzate, senza nemmeno accorgersi che sotto, di tanto in tanto, avviene una

transazione sulla blockchain Bitcoin per consolidare gli stati. Bitcoin diventerebbe quindi l'invisibile ma solido strato di fiducia su cui poggia gran parte della finanza digitale globale.

Naturalmente, rimangono sfide aperte: la sicurezza di questi layer aggiuntivi (es. il trade-off di fiducia nelle federazioni Fedimint, o la centralizzazione dei nodi Lightning con molta capacità), la necessità di educazione e UX adeguate affinché l'utente finale ne tragga beneficio senza complessità, e la governance tecnica di Bitcoin che deve bilanciare innovazione e conservazione (non tutte le proposte avanzate – come Drivechain o ANYPREVOUT – trovano subito consenso nella comunità). Tuttavia, le tendenze indicano che la base di Bitcoin è sufficientemente stabile da permettere la costruzione di queste soluzioni off-chain senza dover hard-forkare o stravolgere il protocollo.

In conclusione, sul fronte tecnologico Bitcoin sta dimostrando una notevole vivacità e capacità di evoluzione. La combinazione di Lightning Network, sidechain e nuovi layer sta trasformando quello che era "solo" un registro distribuito relativamente lento in una piattaforma dinamica, capace di supportare un'intera economia digitale. Nella prossima sezione vedremo come, parallelamente alle evoluzioni tecniche, Bitcoin stia entrando sempre più nel mondo della finanza tradizionale, dai mercati regolamentati agli equilibri di portafoglio degli investitori istituzionali.



Integrazione con la Finanza Tradizionale: ETF, Istituzioni e Regolamentazione

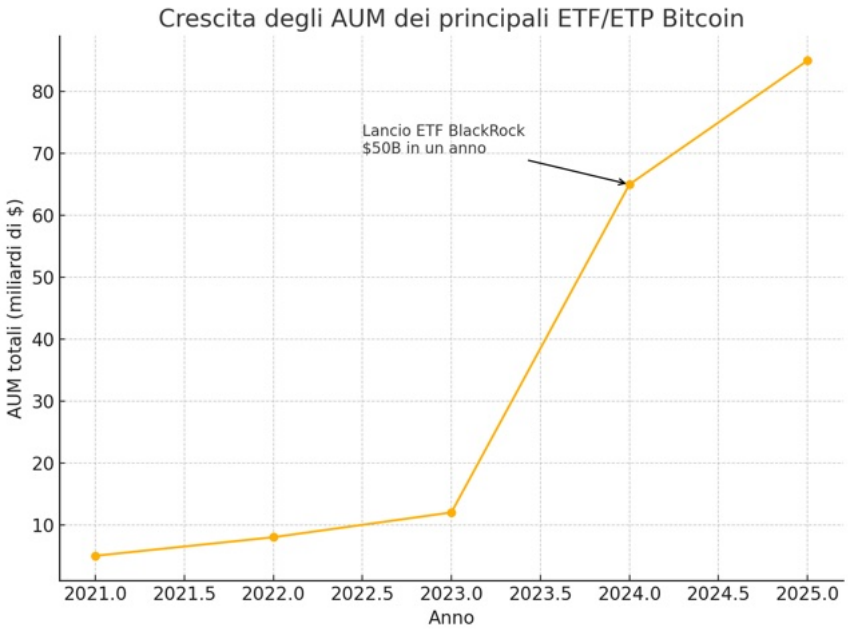
Mentre gli sviluppatori lavorano all'evoluzione tecnica, un altro fenomeno degli ultimi anni è la crescente integrazione di Bitcoin nei circuiti finanziari tradizionali. Una volta percepito ai margini del sistema, Bitcoin è oggi al centro di prodotti d'investimento regolamentati, strategie di allocazione di grandi fondi e dibattiti regolamentari nelle principali giurisdizioni. In questa sezione analizziamo come Bitcoin stia diventando parte integrante della finanza "ufficiale": dall'approvazione di ETF e fondi dedicati, all'ingresso di attori istituzionali, fino all'evoluzione normativa in diversi paesi. Questo processo, oltre a legittimare Bitcoin, ne sta ponendo le basi come infrastruttura finanziaria complementare a quelle esistenti.

L'era degli ETF e dei fondi istituzionali: Un punto di svolta simbolico è stato il lancio del primo ETF (Exchange-Traded Fund) su Bitcoin in Nord America nel 2021 (in Canada), seguito da un'ondata di richieste per ETF spot anche negli Stati Uniti. Nel 2023, BlackRock – colosso mondiale della gestione patrimoniale – ha sorpreso i mercati depositando una domanda per un ETF spot Bitcoin presso la SEC americana . Questa mossa ha segnato l'inizio di una "corsa all'ETF", con altri attori come Fidelity, Invesco, WisdomTree e ARK Invest a ruota. Storicamente, BlackRock gode di un tasso di successo quasi perfetto nelle approvazioni di ETF, il che ha alimentato l'aspettativa che anche un ETF Bitcoin potesse ottenere luce verde . In effetti, entro la fine del 2024, la SEC ha iniziato ad approvare alcuni di questi prodotti, portando Bitcoin nei listini di Wall Street in forma di titoli scambiabili in borsa.

I numeri registrati sono notevoli: il fondo iShares Bitcoin Trust (ETF) di BlackRock, lanciato nel 2024, ha raggiunto oltre 50 miliardi di dollari di asset in gestione nel primo anno, diventando il lancio di prodotto più grande nella storia dell'industria ETF . Questo ETF si è anche classificato terzo per afflussi netti tra tutti gli ETF (dietro solo a due fondi sull'S&P 500), segno di un interesse senza precedenti degli investitori per Bitcoin in una veste regolamentata . Curiosamente, più della metà della domanda per l'ETF di BlackRock è venuta da investitori retail, e il 75% di questi non aveva mai posseduto prima prodotti iShares: Bitcoin sta fungendo da strumento di onboarding di una nuova fascia demografica di investitori verso i mercati finanziari . Parallelamente, in Canada e in Europa esistono già da tempo ETP (exchange-traded products) su Bitcoin che hanno accumulato migliaia di BTC in custodia, segno che una parte dell'offerta circolante è "parcheggiata" in strumenti finanziari destinati a investitori tradizionali.

Questa istituzionalizzazione va oltre gli ETF: fondi pensione, compagnie assicurative, fondi hedge e tesorerie aziendali hanno iniziato ad allocare una piccola percentuale in Bitcoin come asset di riserva o diversificazione. Il caso emblematico è MicroStrategy,

società quotata al NASDAQ, che dal 2020 ha convertito gran parte delle riserve di tesoreria in Bitcoin (oltre 150.000 BTC detenuti nel 2025). Anche Tesla per un periodo ha detenuto Bitcoin nel bilancio. Grayscale Bitcoin Trust (GBTC), un veicolo istituzionale lanciato già nel 2013, è arrivato a gestire più di 600.000 BTC (circa 3% dell'offerta totale). Questi esempi mostrano come Bitcoin stia entrando nei bilanci e nei portafogli di attori mainstream.



Riconoscimento e accettazione da leader finanziari: Un indicatore qualitativo di integrazione è il cambio di tono di molti leader finanziari. Se fino a pochi anni fa prevalevano scetticismo e derisione verso Bitcoin, più di recente stiamo assistendo a una sorta di "sdoganamento". Oltre al già citato Larry Fink di BlackRock (in foto pg 18) – che ha pubblicamente ammesso di aver cambiato idea, definendo Bitcoin "oro digitale" e uno strumento legittimo – anche Jamie Dimon (CEO di JPMorgan), un feroce critico storico, ha attenuato i toni (pur restando guardingo sulle crypto, la sua banca offre ai clienti facoltosi accesso a fondi Bitcoin). Le grandi banche d'affari come Goldman Sachs e Morgan Stanley hanno istituito desk per il trading di futures su Bitcoin e per fornire esposizione ai propri clienti. Banche depositarie come BNY Mellon e State Street hanno avviato servizi di custodia di asset digitali per rispondere alla domanda dei loro clienti istituzionali. Persino società di pagamento tradizionali come VISA e Mastercard collaborano con exchange e startup Bitcoin per emettere carte di debito in BTC o per utilizzare Lightning Network (ad esempio tramite partnership con società Lightning per pagamenti istantanei).

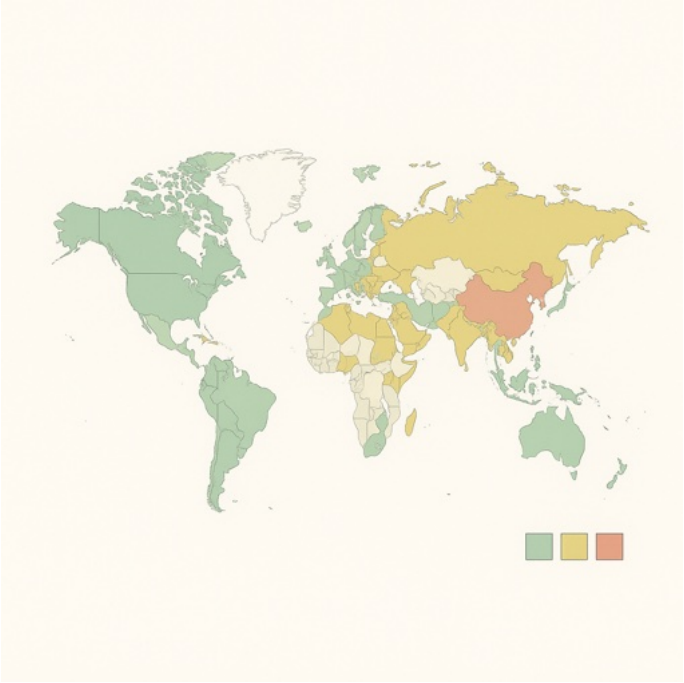
In Europa, la SVB (Six Swiss Exchange) di Zurigo ha quotato ETP su Bitcoin e alcune banche private offrono investimenti in Bitcoin ai correntisti più facoltosi. In Asia, Singapore e Hong Kong si sono mosse per diventare hub di asset digitali regolamentati, mentre in Medio Oriente paesi come gli Emirati Arabi Uniti hanno creato quadri normativi per attrarre business legati a Bitcoin e crypto.

Evoluzione normativa: La regolamentazione è un campo fondamentale per l'integrazione di Bitcoin nel sistema finanziario. Negli ultimi anni abbiamo assistito a progressi importanti:

- L'Unione Europea ha approvato nel 2023 il regolamento MiCA (Markets in Crypto-Assets), il primo quadro normativo organico per le criptovalute in una grande giurisdizione. MiCA fornisce definizioni legali di crypto-asset, obblighi per

gli emittenti (es. stablecoin) e requisiti per gli operatori (exchange, custodi) che vogliono offrire servizi legati a Bitcoin & co. Il regolamento, applicabile dal 2024/25, dà chiarezza legale e armonizza le regole nei 27 paesi UE, facilitando l'adozione istituzionale perché riduce i rischi di compliance. Bitcoin, in quanto asset senza emittente, è esentato dalla sezione sui "token referenziati" ma rientra negli obblighi di trasparenza e custodia per i fornitori di servizi.

- Negli Stati Uniti, la situazione è stata a lungo incerta: la SEC ha rifiutato dozzine di proposte di ETF spot Bitcoin dal 2017 al 2022 citando rischi di manipolazione di mercato, mentre il CFTC ha classificato Bitcoin come commodity. Dal 2021 esistono ETF su futures Bitcoin negli USA (basati su contratti regolamentati CME), ma l'approvazione di ETF spot è considerata un salto maggiore di accettazione. Come discusso, entro il 2024/25 il vento sembra cambiato, con la probabile approvazione di più ETF spot. Oltre a ciò, la Federal Reserve e l'OCC hanno emanato linee guida per banche che volessero custodire criptovalute o emettere stablecoin. Permane un dibattito su chi debba supervisionare il settore (SEC vs CFTC) e su future leggi (es. il possibile trattamento di alcune crypto come titoli). Nel frattempo, singoli Stati hanno adottato posture proprie: il Wyoming si è distinto per legislazione pro-crypto (creando la figura di "banca custode di criptovalute" e chiarendo la proprietà di asset digitali), New York ha un regime di licenza (BitLicense) stringente, il Texas promuove il mining e Lightning con normative favorevoli.



•Altre giurisdizioni: la Svizzera ha integrato nel proprio codice civile le DLT laws (2021) che riconoscono i titoli tokenizzati e facilitano il trading di crypto-asset con uno status legale chiaro. Il Regno Unito post-Brexit punta a regolare cripto con un approccio simile a quello tradizionale, in un'ottica di rendere Londra un centro anche per gli asset digitali. La Cina ha bandito il trading e mining di Bitcoin nel 2021 (portando a un'effimera scomparsa dei volumi cinesi, poi parzialmente ricomparsi via OTC e Hong Kong). L'India ha oscillato tra ipotesi di ban e tassazione penalizzante. El Salvador ha legalizzato Bitcoin come moneta legale – caso unico finora – e la Repubblica Centrafricana ha fatto un annuncio simile, sebbene quest'ultimo poco implementato.

Questi sviluppi normativi indicano che i governi e i regolatori stanno passando dalla fase dell'ignorare/deridere Bitcoin a quella del confrontarsi con la sua esistenza e

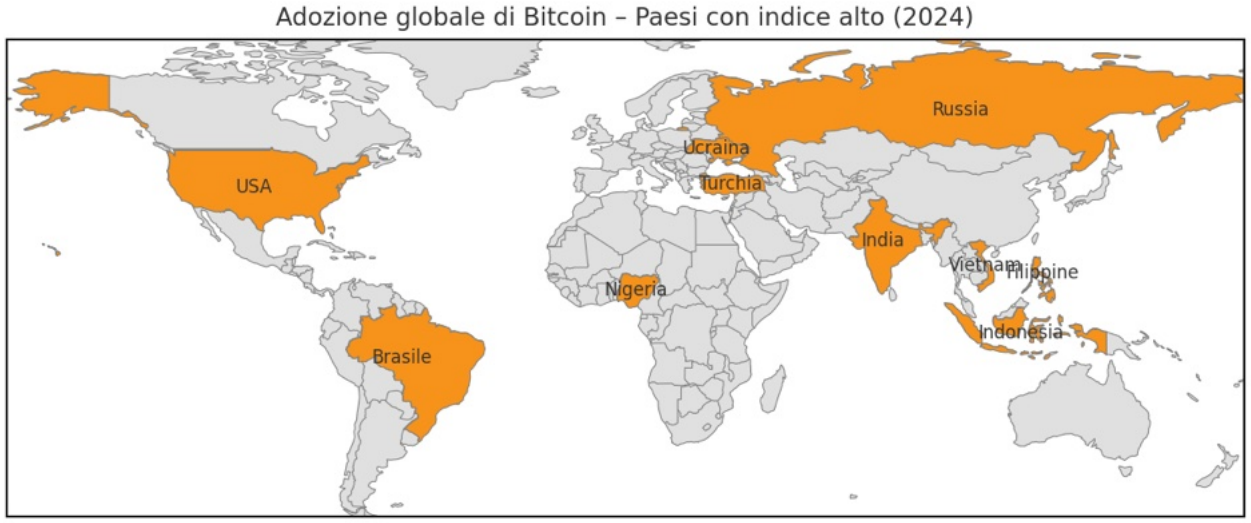
incanalarla entro regole. In una prospettiva di Bitcoin come infrastruttura globale, la regolamentazione è un'arma a doppio taglio: da un lato la chiarezza normativa favorisce l'adozione istituzionale (poiché riduce i rischi legali), dall'altro occorre vigilare che l'essenza aperta e disintermediata di Bitcoin non venga soffocata da norme eccessivamente restrittive. Finora Bitcoin si è dimostrato resiliente: anche dove è stato vietato in parte (es. Cina), la rete ha continuato a funzionare e i partecipanti si sono spostati verso lidi più accoglienti. Ciò fa parte dell'argomentazione a favore di Bitcoin come infrastruttura anticensura: chi vorrà partecipare lo farà nelle giurisdizioni amichevoli, e le altre rischiano di rimanere indietro in innovazione.

Impatti sul mercato finanziario tradizionale: L'ingresso di Bitcoin nei portafogli comporta anche effetti sul piano finanziario. Ad esempio, la correlazione di Bitcoin con altri asset è oggetto di studio: storicamente era molto decorrelato (utile per diversificazione), poi durante alcune fasi macro (2020-2021) ha mostrato correlazione positiva con titoli tech o con l'andamento della liquidità globale. Se Bitcoin divenisse un asset di riserva, potremmo vederlo comportarsi più come l'oro in certe fasi (salire nei periodi di sfiducia valutaria). Già nel 2022, in piena crisi inflazionistica, paesi emergenti con monete deboli hanno visto crescere l'uso di Bitcoin come hedge. La società di investimento Ark Invest ipotizza traiettorie di prezzo di Bitcoin molto elevate se anche solo pochi punti percentuali degli asset globali (azioni, riserve auree, immobili) venissero riallocati su BTC. Senza spingerci su previsioni speculative, è chiaro però che Bitcoin sta guadagnando uno status di "nuova classe di asset" che i gestori devono quantomeno considerare in una asset allocation moderna.

Un segnale in tal senso: nel 2025 BlackRock, nella sua lettera annuale, ha menzionato Bitcoin diverse volte, evidenziando come "gli investitori potrebbero iniziare a trattare Bitcoin come riserva di valore di lungo termine più stabile del dollaro, specialmente in presenza di deficit pubblici crescenti" . Allo stesso tempo, Fink avverte che l'ascesa di strumenti come Bitcoin (e la finanza decentralizzata) potrebbe "minare la supremazia finanziaria dell'America" se non governata . Queste affermazioni riflettono che il dibattito su Bitcoin non è più relegato agli appassionati, ma è arrivato ai vertici della finanza globale, con un misto di entusiasmo per l'innovazione e cautela per le implicazioni sistemiche.

In sintesi, l'integrazione di Bitcoin nella finanza tradizionale è in pieno svolgimento. Questo fenomeno consolida Bitcoin come infrastruttura finanziaria: quando banche, borse ed enti regolatori abbracciano (anche solo parzialmente) Bitcoin, esso cessa di essere un elemento antagonista per diventare parte dell'architettura finanziaria complessiva. Se questa tendenza proseguirà, Bitcoin potrebbe fungere da ponte tra il vecchio e il nuovo sistema: un asset nativo di Internet che però viene scambiato nei mercati legacy e detenuto insieme a azioni e obbligazioni. Il risultato finale potrebbe essere una finanza globale più interconnessa, dove Bitcoin offre elementi di settlement rapido e sicurezza crittografica a mercati altrimenti frammentati.

Nel prossimo capitolo, esploreremo un ambito forse meno prevedibile ma estremamente promettente: l'intersezione tra Bitcoin e Intelligenza Artificiale, e come queste due tecnologie emergenti possano potenziarsi a vicenda, ridefinendo concetti come lavoro, servizi digitali e economia delle macchine.



Bitcoin e Intelligenza Artificiale: Sinergie e Implicazioni

A prima vista Bitcoin e Intelligenza Artificiale (AI) appartengono a domini diversi: il primo è una rete finanziaria decentralizzata, la seconda una branca dell'informatica che punta a creare sistemi intelligenti. Eppure, sta emergendo un'interessante area di convergenza in cui Bitcoin (in particolare Lightning Network) e AI si incontrano, con potenziali sinergie capaci di abilitare nuovi modelli economici e applicazioni rivoluzionarie. In questa sezione esploreremo come l'AI potrebbe sfruttare l'infrastruttura Bitcoin per transare valore, e viceversa come Bitcoin potrebbe beneficiare dei progressi dell'AI, toccando scenari che fino a poco tempo fa erano fantascienza: macchine che pagano altre macchine, modelli AI che monetizzano i propri servizi in autonomia, e un'economia digitale in cui il denaro diventa nativo dell'automazione.

Micropagamenti programmabili per AI: Uno dei colli di bottiglia nello sviluppo di servizi AI distribuiti è la monetizzazione granulare. Molti servizi AI (si pensi alle API di modelli di linguaggio, riconoscimento immagini, ecc.) oggi sono accessibili tramite abbonamenti o pagamenti relativamente grossolani, spesso perché i sistemi di pagamento tradizionali non gestiscono bene importi piccoli o transazioni ad alta frequenza. Lightning Network fornisce la soluzione naturale: pagamenti istantanei anche di un milionesimo di dollaro, automatizzabili via software. Nel 2023, Lightning Labs ha rilasciato il protocollo L402, un'estensione del codice di stato HTTP 402 ("Payment Required", mai usato finora) che permette l'autenticazione su API web mediante un pagamento Lightning . In pratica, un client AI che vuole chiamare un servizio può presentare un ticket Lightning (un pre-pagamento) invece di una chiave API statica. Questo abilita un modello pay-per-call: ogni richiesta ha un costo (es. 100 satoshi) e viene accettata solo se il pagamento è stato effettuato. Già esistono integrazioni con framework popolari di AI: ad esempio, è stato dimostrato un plugin per LangChain (ambiente di sviluppo per agenti AI) che consente a un agente di auto-approvvigionarsi di Bitcoin su Lightning e spenderli per chiamare servizi esterni . Immaginiamo un agente intelligente che per rispondere alle richieste dell'utente debba consultare un database a pagamento: grazie a Lightning, l'agente può pagare pochi centesimi, ottenere l'accesso al dato e fornire il risultato, tutto automaticamente e in pochi secondi, senza che un essere umano inserisca credenziali o completi manualmente un pagamento.

Uno scenario concreto descritto da Lightning Labs: "Un pezzo di software AI può vendere risposte a pagamento. I potenziali acquirenti chiedono qualcosa all'AI venditrice; la risposta iniziale è valutata da un AI locale dell'acquirente; se è soddisfacente, quest'ultimo effettua un pagamento per sbloccare ulteriori risposte" . Questo schema mostra interazioni economiche autonome tra AI: l'AI che fornisce un

servizio (ad esempio generare un'immagine o risolvere un problema) pone un prezzo, l'AI cliente decide se vale la pena pagare in base alla qualità della preview, e poi paga tramite Lightning in modo trustless. Il pagamento può essere condizionato: solo se la risposta soddisfa certi criteri, viene rilasciato il resto dei fondi. Tali logiche possono essere implementate tramite smart contract a tempo di Lightning (il citato HTLC).

- Macchine che pagano macchine: Estendendo questo concetto, in un futuro di Internet of Things (IoT) con device intelligenti, i micropagamenti Bitcoin potrebbero diventare la lingua franca economica delle macchine. Ad esempio, un'auto elettrica autonoma potrebbe automaticamente pagare una stazione di ricarica; sensori in una smart city potrebbero vendere i dati raccolti ad altri sistemi in cambio di satoshi; una rete di dispositivi potrebbe bilanciare carico computazionale o energetico compensandosi economicamente in tempo reale. Tutto ciò richiede un mezzo di pagamento programmatico, senza attriti e senza necessità di autorizzazioni esterne – esattamente il profilo di Lightning. Le alternative centralizzate (es. un API di pagamento gestita da un'azienda) introducono dipendenze e punti di fallimento; Bitcoin LN, essendo decentralizzato, permette a qualsiasi dispositivo di partecipare con sole regole matematiche e crittografiche a garantire le transazioni.

AI come partecipanti economici autonomi: Un'idea più futuristica è che gli stessi agenti AI possano possedere e gestire Bitcoin. Essendo Bitcoin denaro nativamente digitale e non legato identitariamente a persone fisiche, non c'è nulla nel protocollo che impedisca a un software di detenere una chiave privata e quindi controllare dei fondi. Con opportuni protocolli di sicurezza (ad es. multi-firma con partecipazione umana per evitare derive impreviste), si potrebbe creare un'entità AI che guadagna Bitcoin fornendo servizi (scrittura di testi, analisi dati, moderazione contenuti…) e li spende per acquistare risorse (capacità computazionale, accesso a informazioni, o persino servizi nel mondo fisico come la stampa 3D di un oggetto). Questo concetto richiama le DAO (organizzazioni autonome decentralizzate) ma portato oltre, a entità autonome artificiali. Un embrione di ciò è visibile in progetti come Robonomics (su Ethereum) o nelle teorizzazioni di "AI DAO". Bitcoin potrebbe giocare un ruolo chiave qui poiché, a differenza di token più complessi, è semplice, universale e la sua sicurezza è robustissima – qualità importanti se un'AI deve usarlo come base per la propria "vita economica".

Un caso pratico presentatosi di recente riguarda ChatGPT e i pagamenti: OpenAI inizialmente integrò ChatGPT con plug-in collegati a carte di credito per consentire all'assistente di comprare cose online per conto dell'utente. Ma questo approccio è limitato (rischi di frodi, necessità di autorizzazioni). Un ChatGPT che avesse invece un wallet Lightning potrebbe, su mandato dell'utente, effettuare pagamenti diretti a un servizio senza esporre dati sensibili, regolando solo l'importo dovuto. Ciò può migliorare la sicurezza e l'autonomia dell'agente AI. Lightning Labs ha dimostrato che modelli GPT possono inviare e ricevere bitcoin tramite LN con pochi comandi , aprendo la strada ad assistenti virtuali finanziariamente capaci.

Bitcoin come dataset e l'uso di AI per Bitcoin: Finora abbiamo visto come Bitcoin avvantaggia l'AI, ma vale anche il viceversa: l'Intelligenza Artificiale può supportare Bitcoin e il suo ecosistema. Ad esempio, la manutenzione della rete Lightning potrebbe giovarsi di AI: esistono già strumenti che suggeriscono ai nodi Lightning come gestire al meglio i propri canali (instradamento, fee) usando algoritmi avanzati, e potrebbero evolvere in agenti autonomi che ottimizzano la topologia di rete per ridurre latenze e costi. Oppure, l'AI può analizzare i dati on-chain per individuare pattern di sicurezza, allertando se ci sono anomalie (tentativi di attacco al 51%, bug sfruttati, ecc.). Nel mining, l'AI può ottimizzare l'allocazione di carichi sui chip ASIC per massimizzare l'hash rate e minimizzare consumi e usura.

Un ambito dove AI e Bitcoin si incrociano è la privacy e analisi blockchain: da un lato, algoritmi di machine learning sempre più sofisticati vengono usati dalle società di analytics per tracciare i flussi di Bitcoin e deanonimizzare transazioni sospette; dall'altro, la comunità privacy utilizza AI per generare decoy e mescolare le transazioni (coinjoin) in modo più efficace. È un gioco di gatto e topo tecnologico che probabilmente continuerà.

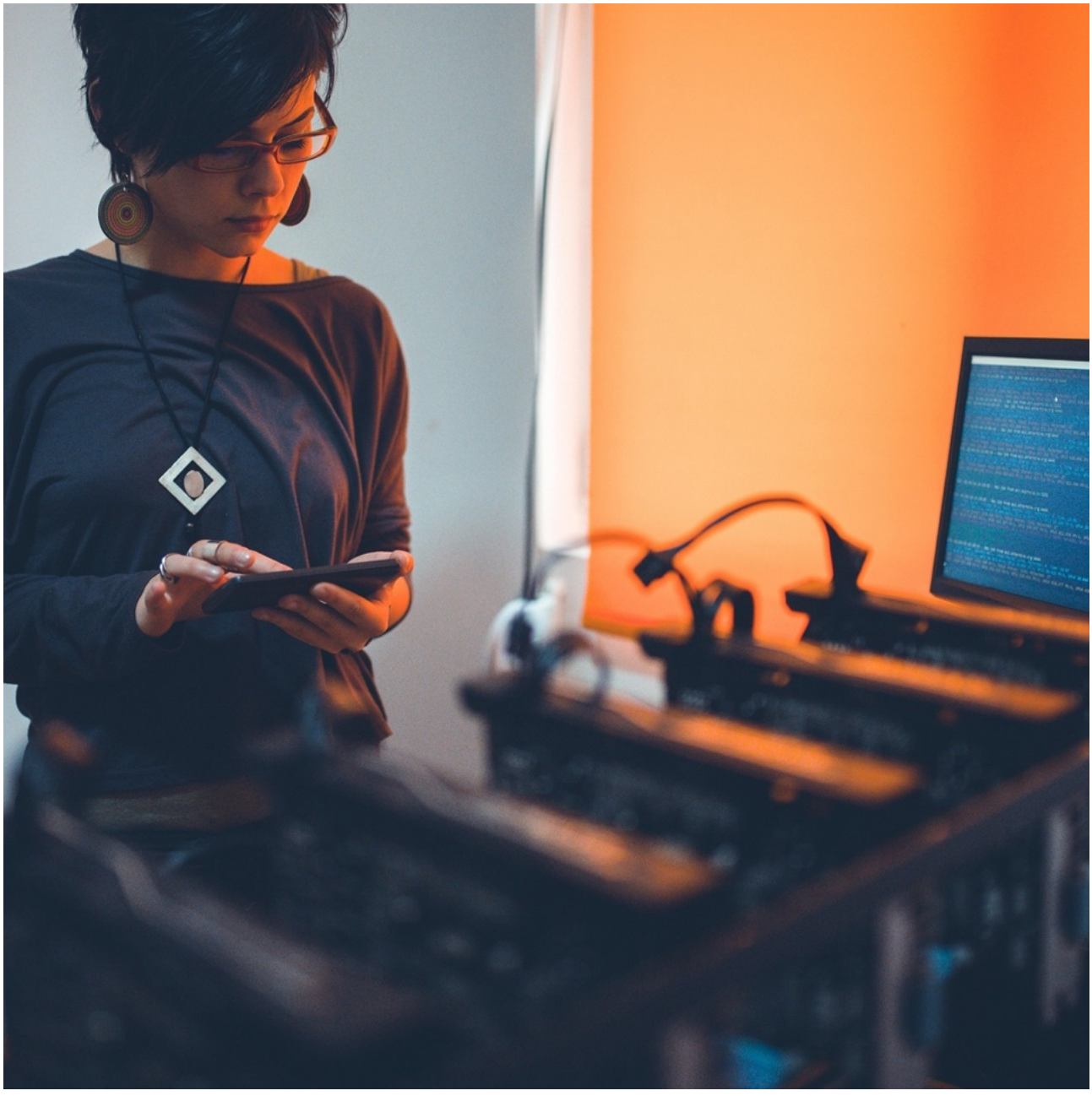
Implicazioni economiche e sociali: Se la combinazione Bitcoin+AI dovesse prendere piede, potremmo assistere alla nascita di un mercato dei dati e dei servizi AI totalmente nuovo. I dati – carburante dell'AI – potrebbero essere comprati e venduti in micropagamenti direttamente dai proprietari (immaginiamo sensori che vendono letture, utenti che vendono spezzoni di attenzione o preferenze per addestrare modelli, il tutto remunerato in satoshi). Questo toglierebbe potere dalle grandi piattaforme accentratrici, distribuendo il valore a chi effettivamente fornisce la risorsa. Ad esempio, invece di far guadagnare YouTube tramite pubblicità, si potrebbe pagare pochi centesimi al minuto direttamente al creatore (magari automaticamente mentre si guarda un video) utilizzando Lightning – un modello streaming money già sperimentato con i podcast (Podcasting 2.0). Con l'AI, si può immaginare di remunerare anche contributi minimi: ogni volta che la nostra foto o frase viene utilizzata per addestrare un modello, potremmo ricevere una microporzione di compenso in Bitcoin, tracciata e distribuita da smart contract.

Allargando la visione, la convergenza di AI e Bitcoin potrebbe portare a un'economia dove l'efficienza allocativa aumenta: i prezzi di servizi digitali diventano dinamici e granulari (un modello AI costoso può abbassare il prezzo se ha capacità inutilizzata e accettare milioni di micro-pagamenti), e dove nuovi lavori nascono nel facilitare queste interazioni (es. prompt engineering remunerato per far ottenere output migliori da un'AI, oppure data labelers pagati direttamente via Lightning per curare dataset).

Certo, ci sono anche rischi e interrogativi: dare ad AI la gestione diretta di denaro – seppur programmato – solleva questioni di sicurezza (cosa impedisce a un attore malintenzionato di ingannare l'AI e farsi inviare fondi?) e di etica (un'AI può "possedere" denaro legalmente? Chi è responsabile delle sue transazioni?). Queste domande richiederanno sia soluzioni tecniche (multi-sig con umani supervisori, limiti incorporati) sia legali/regolamentari col tempo.

In definitiva, Bitcoin e Lightning forniscono all'AI un livello economico aperto, analogo a come Internet fornisce all'AI un livello informativo aperto. Storicamente, le AI non hanno mai avuto accesso nativo a un sistema di pagamento trustless – Bitcoin è il primo e unico in questo senso – e questo può sbloccare forme di interazione completamente nuove. Dall'altro lato, l'AI può aumentare l'efficienza, l'accessibilità e l'intelligenza dell'ecosistema Bitcoin, aiutando a gestire la complessità di una rete globale decentralizzata.

Il futuro delineato è quello di un ciclo virtuoso: Bitcoin rende possibili nuove applicazioni AI monetizzabili, le quali a loro volta attirano più transazioni e utenti su Bitcoin, rafforzando la rete. Già oggi vediamo i primi passi concreti (es. strumenti Lightning per ChatGPT, pagamenti machine-to-machine in progetti IoT). Nei prossimi anni, questa sinergia potrebbe crescere esponenzialmente e dare origine a un'economia digitale in cui valore e informazione fluiscono insieme, senza soluzione di continuità, guidati dall'interazione di intelligenze umane e artificiali.



Sicurezza, Decentralizzazione e Impatto Energetico

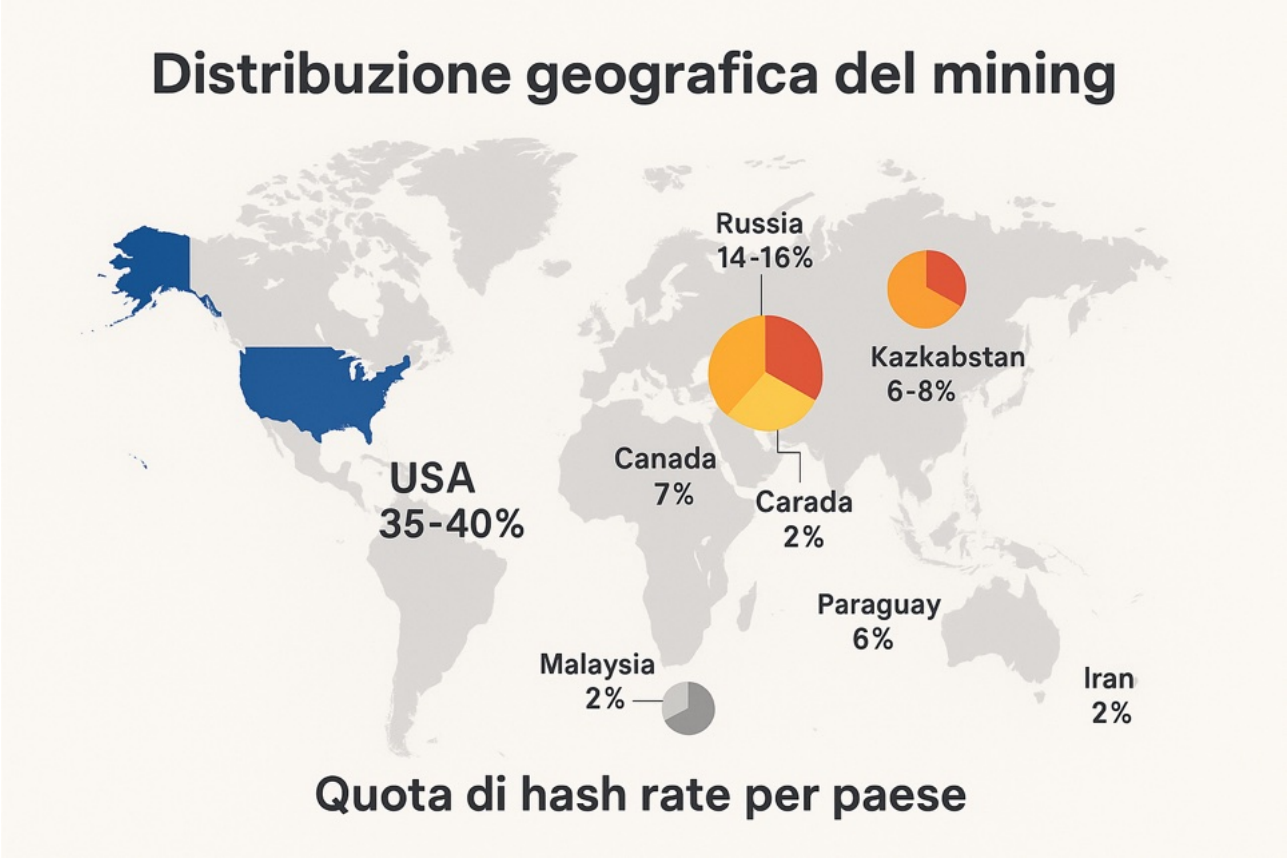
Affinché Bitcoin possa diventare effettivamente la spina dorsale della finanza futura, deve mantenere e migliorare i suoi fondamentali di sicurezza e decentralizzazione. Inoltre, deve affrontare le preoccupazioni riguardo al suo impatto energetico, assicurando che la crescita della rete avvenga in modo sostenibile. In questa sezione, approfondiamo lo stato attuale e le prospettive future di questi aspetti: l'hash rate e la distribuzione dei miner (sicurezza della rete), la decentralizzazione degli attori chiave (miner, nodi, sviluppatori) e l'impatto ambientale del mining e come sta evolvendo verso una maggiore sostenibilità.

Sicurezza della rete – hash rate in forte crescita: La sicurezza di Bitcoin è fondata sul meccanismo di Proof-of-Work (PoW), che richiede potenza computazionale (hash rate) per confermare i blocchi e proteggere la catena da riscritture o attacchi. Negli ultimi anni, l'hash rate della rete Bitcoin ha raggiunto livelli senza precedenti. All'inizio del 2025 è stato brevemente toccato il picco di 1.000 exahash al secondo (EH/s), un record storico , per poi assestarsi intorno a 750-800 EH/s – comunque un ordine di grandezza mai visto prima. Per dare un'idea, 1.000 EH/s equivalgono a 10^{21} hash al secondo, ossia un miliardo di miliardi di tentativi di calcolo al secondo: una potenza combinata di calcolo che supera di molti multipli quella dei più potenti supercomputer del mondo sommati insieme. Questo rende la rete estremamente resistente ad attacchi 51% – un eventuale aggressore che volesse controllare la maggioranza del hash rate per doppie spese dovrebbe investire decine di miliardi di dollari in hardware e consumi elettrici, per poi competere con un network globale e molto distribuito.

Nel corso del 2023, l'hash rate è quasi raddoppiato (+104%) rispetto all'anno precedente , segno di un continuo investimento nell'infrastruttura di mining. Questo incremento è avvenuto nonostante la riduzione dei margini per i miner in un mercato orso nel 2022, e anticipando il halving del 2024 (che dimezza la ricompensa e quindi potenzialmente la redditività). La industria del mining ha risposto con notevoli miglioramenti di efficienza: l'efficienza media delle macchine miner (energia consumata per unità di hash) è ora di ~34 W/TH, con prospettive di scendere a 20 e fino a 10 W/TH entro il 2026 grazie a chip e impianti migliori. Questo significa che l'aumento di hash rate non si è tradotto in un aumento proporzionale dei consumi energetici – un punto cruciale che toccheremo più avanti.

Distribuzione geografica del mining: Uno degli indicatori di decentralizzazione della sicurezza è la diffusione dei miner a livello globale. Dopo il ban del mining in Cina a metà 2021, il panorama è cambiato drasticamente: dagli inizi del 2022 gli Stati Uniti hanno assunto la leadership del mining Bitcoin. Secondo i dati del Cambridge Centre for Alternative Finance (CCAF) aggiornati al 2023, gli USA contribuiscono a circa 35-40%

dell'hash rate globale . Al secondo posto vi è una combinazione di regioni: stime di fine 2024 indicano che la Russia potrebbe detenere intorno al 14-16% dell'hash rate , con la Cina (nonostante il divieto, tramite operazioni clandestine soprattutto nel Sichuan e altrove) ancora intorno al 10-14% . Seguono paesi come il Kazakhstan (tradizionalmente forte, ora attorno al 6-8%), il Canada (~7%), e altri emergenti come Malaysia, Paraguay, Norvegia, Iran con quote minori . I primi tre paesi (USA, Russia, Cina) sommano in alcune stime circa il 60-70% del totale, il che è significativo ma comunque più bilanciato rispetto al passato quando la Cina da sola era >60% . Importante notare: la decentralizzazione geografica aiuta a resilienza (eventi politici o blackout in un paese non compromettono l'intera rete), ma la decentralizzazione perfetta è utopica poiché i miner tendono a concentrarsi dove ci sono energia a basso costo e ambienti favorevoli. Ad ogni modo, il mining di Bitcoin oggi copre ogni continente (eccetto l'Antartide), con farm dal Texas alla Siberia, dall'Islanda all'Inner Mongolia, dal Sud America (vedi Paraguay con idroelettrico Itaipú) all'Africa (esperimenti in Kenya e altre zone con surplus rinnovabile). Questa distribuzione diffusa rafforza Bitcoin come infrastruttura globale: è improbabile che un singolo governo possa mai più spegnere la rete, data la mobilità e diversificazione dei miner.



Anche i dati di concentrazione per pool (ad esempio Foundry USA e AntPool spesso sono i due maggiori pool, ognuno 15-25%) sono utili da monitorare: a fine 2024, due pool americani (Foundry e Marathon) producevano insieme ~38,5% dei blocchi – una concentrazione che va tenuta d'occhio, pur mitigata dal fatto che i pool aggregano molti

miner indipendenti e possono essere facilmente abbandonati se abusano del loro ruolo.

Full node e decentralizzazione della convalida: Un altro pilastro è la decentralizzazione dei nodi che verificano la blockchain. Chiunque può far girare un full node Bitcoin (il software è libero e gira su hardware modesto), e questa è l'autorità ultima nel convalidare le regole: un'infrastruttura finanziaria decentralizzata dipende dal fatto che decine o centinaia di migliaia di nodi sparsi nel mondo eseguono e concordano sulle regole del protocollo. Stimare il numero di nodi Bitcoin non è facile (solo quelli con porta pubblica aperta sono visibili, tipicamente 10-15 mila; molti altri sono dietro NAT o utilizzano solo la rete Tor). L'importante è che la barriera all'esecuzione di un nodo resti bassa: grazie a migliorie come SegWit, l'ottimizzazione dei database e ai costi decrescenti di storage, oggi si può archiviare l'intera blockchain (oltre 500 milioni di transazioni dal 2009) su un semplice hard disk da 1-2 TB e con un Raspberry Pi come hardware. Questa leggerezza comparata è ciò che distingue Bitcoin da blockchain più "pesanti" e ne tutela la decentralizzazione nel lungo termine.

Resilienza e aggiornamenti di sicurezza: Bitcoin ha dimostrato elevata resilienza contro attacchi informatici: non si sono più verificati bug critici dal 2010 (inflation bug) e la rete ha retto ad attacchi DDoS, fork accidentali e tentativi di spam. Miglioramenti come Taproot (attivato nel 2021) hanno reso le transazioni più private ed efficienti, e aprono porte per futuri upgrade (es. delegating script via Merkelized Abstract Syntax Trees). La prossima sfida sul tavolo per la sicurezza del protocollo è a più lungo termine: la transizione del modello economico dalla dipendenza dai block reward (che decresceranno con i halving) alle sole commissioni come incentivo per i miner. Entro il 2035 circa, le commissioni potrebbero diventare la voce predominante delle entrate dei miner. Sarà essenziale che l'uso di Bitcoin (on-chain e via second layer) generi una domanda di spazio blocco sufficiente a pagare i miner in modo adeguato, mantenendo quindi l'hash rate. Su questo punto c'è dibattito, ma l'emersione di nuovi casi d'uso (es. ancoraggio di dati su blockchain, transazioni periodiche per consolidare layer2, ecc.) fa pensare che col crescere dell'economia Bitcoin anche le fee on-chain aumenteranno in aggregato, sostenendo la sicurezza.

Impatto Energetico e Sostenibilità: Il tema energetico è spesso citato come la critica principale a Bitcoin come infrastruttura. La rete attualmente consuma un quantitativo di elettricità paragonabile a quello di un medio paese industrializzato (stime variano, ma intorno ai 100-150 TWh annui, simile al consumo della Polonia o della Malaysia). Questo consumo, lungi dall'essere "spreco fine a sé stesso", è il cuore del meccanismo di sicurezza PoW; tuttavia, è importante contestualizzarlo e vedere come sta evolvendo la sostenibilità del mining:

- Mix energetico sempre più verde: Contrariamente alla percezione comune, una porzione significativa dell'energia usata per il mining proviene da fonti rinnovabili o a basso costo (spesso in eccesso e quindi sprecata se non utilizzata). Secondo

studi di settore (ad es. Bitcoin Mining Council, e analisti come D. Batten), oltre 50-60% dell'energia del mining oggi è da fonti sostenibili . Ad esempio, in regioni come il Sichuan o lo Yunnan in Cina, i miner operavano (e quelli nascosti operano ancora in parte) quasi esclusivamente durante la stagione delle piogge grazie al surplus idroelettrico. Negli USA, molte farm in Texas sfruttano il fotovoltaico e l'eolico abbondante, insieme al gas naturale di scarto (flare gas) che altrimenti verrebbe bruciato in atmosfera senza recupero energetico. In paesi nordici come Islanda e Norvegia, l'energia geotermica e idroelettrica alimenta data center di mining. Questo trend è in aumento: man mano che l'industria si sviluppa, c'è incentivo economico a localizzarsi dove l'energia costa meno – tipicamente luoghi con rinnovabili in eccesso o non altrimenti trasportabili.

- Bitcoin come utilizzatore di energia di ultima istanza: Una prospettiva interessante vede il mining Bitcoin come stabilizzatore di rete elettrica. Poiché i miner possono accendersi o spegnersi rapidamente in base alla disponibilità di elettricità, fungono da domanda flessibile che può assorbire surplus e ridursi in momenti di picco di domanda civile. In Texas, ad esempio, alcune mining farm hanno accordi con l'operatore di rete ERCOT per spegnersi all'istante se ci sono carichi critici, contribuendo a evitare blackout e venendo remunerate per questa disponibilità. In questo senso, Bitcoin può incentivare lo sviluppo di rinnovabili: un impianto eolico isolato che avrebbe difficoltà di redditività perché produce più di quanto la rete locale possa assorbire, può aggiungere miner Bitcoin che comprano quell'eccesso energetico altrimenti sprecato, migliorando il ROI del progetto complessivo. È il concetto di Bitcoin come acquirente di energia di ultima istanza: sempre disponibile a comprare elettricità a un certo prezzo fisso (determinato dal valore di mercato di BTC e dalla difficoltà corrente). Questo pavimento di domanda potrebbe stimolare investimenti in energia pulita in zone remote e non servite.

- Riduzione emissioni tramite mining: Può sembrare paradossale, ma il mining può ridurre emissioni climalteranti in certi contesti. Ad esempio, la pratica di gas flaring (bruciare gas naturale di scarto nei pozzi petroliferi, emettendo CO2 e metano) può essere mitigata usando quel gas per alimentare generatori di corrente che minano Bitcoin in loco. Invece di bruciare il gas inutilizzato, lo si monetizza e nel processo si riducono emissioni non controllate di metano (gas serra potentissimo). Si stima che questo approccio potrebbe tagliare una quantità significativa di emissioni se adottato su larga scala .

- Efficienza e fonti alternative: L'industria del mining sta esplorando tecnologie per aumentare l'efficienza: dal raffreddamento a immersione (per spingere i chip ASIC oltre i limiti convenzionali) all'uso di calore di scarto per usi utili. Ci sono progetti pilota in cui il calore generato dai miner viene usato per riscaldare serre agricole, edifici residenziali o piscine pubbliche – trasformando un sottoprodotto in risorsa, e migliorando l'impronta energetica netta. Inoltre, l'evoluzione dei chip e la concorrenza spinge a ridurre l'energia per hash (come detto, watt per TH in calo costante). Infine, alcuni team stanno studiando PoW "chiuso" per fare calcoli

scientifici utili, ma finora Bitcoin rimane su calcoli inutili per design (sha256) per evitare di centralizzare su chi ha specifici carichi.

Percezione pubblica e realtà: Nonostante questi miglioramenti, l'impatto ambientale di Bitcoin rimane un tema delicato a livello mediatico e politico. Molte discussioni su ban o restrizioni (es. nello stato di New York si è discusso di moratorie su nuovi impianti di mining a gas) nascono dalla preoccupazione per emissioni e consumo. È fondamentale quindi comunicare correttamente i dati: ad esempio, un report 2023 di CoinShares evidenzia che il mining Bitcoin è responsabile di circa lo 0,1-0,2% delle emissioni globali di CO_2 – un ordine di grandezza simile a quello dell'industria dei giochi online o della produzione di pet food, e decisamente inferiore all'industria dell'alluminio o a quella aerea . Inoltre, si può argomentare che l'impatto va commisurato all'utilità: se Bitcoin diviene l'infrastruttura finanziaria di miliardi di persone, quale costo energetico sarebbe giustificato? Il sistema bancario/finanziario tradizionale ha un'impronta energetica (data center, sportelli, trasporti valori) non banale, seppur meno concentrata e quantificata. In prospettiva, un Bitcoin che alimenta una fetta significativa dell'economia potrebbe giustificare anche consumi paragonabili a quelli attuali, purché decarbonizzati.

Sicurezza a lungo termine: Uno sguardo al lungo periodo deve contemplare anche minacce come l'avvento di computer quantistici in grado di rompere le attuali firme crittografiche (ECDSA). La comunità Bitcoin monitora i progressi del quantum computing: benché gli esperti stimino che una macchina in grado di compromettere ECDSA-256 sia lontana almeno 10-15 anni (probabilmente di più), il protocollo può essere aggiornato con algoritmi post-quantum prima che ciò avvenga. C'è ovviamente inerzia ad aggiornare un sistema da centinaia di miliardi di dollari, ma all'occorrenza la rete ha già dimostrato di sapersi evolvere (vedi passaggio a SegWit, Taproot). La trasparenza di Bitcoin è utile: se qualcuno stesse accumulando capacità quantistica, sarebbe presumibilmente rilevabile da un aumento di transazioni anomale (tentativi di violare chiavi pubbliche riutilizzate). In ogni caso, questo rimane un aspetto da risolvere entro il 2030-2040, un orizzonte comunque lungo rispetto alla velocità con cui Bitcoin avanza su altri fronti.

In conclusione, sul piano di sicurezza e decentralizzazione, Bitcoin appare in salute e in rafforzamento: più potenza di calcolo, più dispersione globale dei miner, progressi nell'efficienza e nella sostenibilità. Questi elementi sono cruciali perché conferiscono robustezza sistemica – caratteristica imprescindibile per un'infrastruttura su cui ci si aspetta che il mondo possa fare affidamento. La proof-of-work di Bitcoin, spesso criticata, è in realtà la fonte della sua credibilità: è ciò che rende costosissimo barare e che ha permesso alla rete di operare senza intrusioni per oltre 14 anni. Finché la comunità e l'industria saranno in grado di adattare il mining a un mondo che punta alla decarbonizzazione e a mitigare eventuali centralizzazioni e rischi, Bitcoin rimarrà una piattaforma sicura e trustless su cui costruire servizi finanziari.

Nel prossimo capitolo conclusivo, tireremo le fila di quanto esposto, delineando una visione d'insieme delle prospettive di Bitcoin come infrastruttura finanziaria globale, tra opportunità e sfide future.

E

In foto il presidente di El Salvador **Nayib Armando Bukele Ortez**: è in carica dal 1° giugno 2019 e ha iniziato il suo secondo mandato il 1° giugno 2024

Prospettive Economiche e Geopolitiche di Bitcoin

L'emergere di Bitcoin come infrastruttura finanziaria globale porta con sé ampie implicazioni economiche e geopolitiche. In questa sezione finale, allarghiamo lo sguardo per comprendere come l'adozione crescente di Bitcoin potrebbe influire sugli equilibri macroeconomici, sulle politiche monetarie e sulle relazioni internazionali nei prossimi decenni. Si tratta di un esercizio necessariamente speculativo, ma basato su trend osservabili e paralleli storici.

Bitcoin e politiche monetarie nazionali: Se Bitcoin venisse adottato su larga scala come riserva di valore o mezzo di scambio, i banchieri centrali e i governi dovrebbero confrontarsi con un asset che sfugge al loro controllo diretto. Un aspetto chiave è la competizione tra valute fiat e Bitcoin: in paesi con monete stabili e bassa inflazione (es. USA, UE, Giappone), Bitcoin finora è visto più come investimento che come moneta per le spese quotidiane. Ma in economie con valuta debole o inflazione elevata, la popolazione già cerca rifugio in dollari USA, oro o altre monete forti; Bitcoin sta diventando un ulteriore rifugio disponibile. Nel 2022-2023, ad esempio, si è notato un aumento dell'uso di Bitcoin e stablecoin in paesi come Turchia, Argentina, Nigeria – tutti alle prese con inflazione a due o tre cifre percentuali. Se questa tendenza prosegue, i governi di tali paesi potrebbero trovarsi con una dollarizzazione/bitcoinizzazione spontanea dell'economia: cittadini che preferiscono risparmiare e talvolta commerciare in asset alternativi rispetto alla valuta locale, riducendo l'efficacia della politica monetaria interna.

Da un lato, questo può fungere da disciplina esterna: costringe i governi a politiche più prudenti per evitare la fuga verso Bitcoin. Dall'altro, pone sfide: ad esempio, come tassare o regolamentare transazioni in Bitcoin? Come garantire la stabilità finanziaria se banche e aziende iniziano ad esporre bilanci in Bitcoin soggetto a oscillazioni di mercato globali? Alcune banche centrali potrebbero scegliere la via dell'integrazione: accumulare esse stesse Bitcoin come parte delle riserve nazionali (cosa che finora nessuna ha dichiarato di fare apertamente, ma figure come il vice-governatore della Banca d'Inghilterra nel 2023 hanno discusso in teoria la possibilità di detenere crypto come riserva).

De-dollarizzazione e ruolo di riserva globale: A livello geopolitico, si parla sempre più di "de-dollarizzazione" – il tentativo di alcune nazioni (es. BRICS: Cina, Russia, ecc.) di ridurre la dipendenza dal dollaro USA nel commercio internazionale e riserve. Finora, le alternative sono state marginali (uso di valute locali, euro, oro). Bitcoin potrebbe entrare in questo discorso come una sorta di riserva neutrale: non emessa da alcuno stato, disponibile a chiunque. Certo, la volatilità attuale lo rende inadatto a breve termine come moneta di conto per commercio, ma come asset di riserva alcuni lo paragonano all'oro 2.0. Larry Fink di BlackRock ha suggestivamente avvertito che se gli USA

continuano con debito eccessivo, Bitcoin potrebbe candidarsi a sostituire il dollaro come riserva globale . Questo scenario estremo richiederebbe comunque anni e un contesto di forte perdita di fiducia nel dollaro. Ma non è implausibile che, ad esempio, una Russia sotto sanzioni o una Cina in conflitto finanziario con l'Occidente possano preferire regolare alcune transazioni internazionali in Bitcoin anziché in dollari/EUR (ci sono già stati piccoli esperimenti: nel 2022 alcune aziende iraniane hanno usato criptovalute per importazioni, sfuggendo a sanzioni SWIFT).

Se Bitcoin divenisse una porzione significativa delle riserve globali, le dinamiche cambierebbero: la sua offerta fissa lo rende deflazionario nel lungo periodo, potenzialmente stabilizzandone il valore man mano che la domanda cresce. Tuttavia, la sua quotazione è anche in parte legata alla salute delle economie fiat (es. in recessioni globali finora Bitcoin ha sofferto, essendo considerato asset di rischio). In futuro, potremmo assistere a una decorrelazione: se più persone vedranno Bitcoin come porto sicuro in caso di politiche fiscali avventate o crisi valutarie, il prezzo di BTC potrebbe salire proprio quando bond e fiat tradizionali calano, invertendo il pattern attuale.

Infrastruttura finanziaria parallela e sovranità: Per alcuni stati, Bitcoin rappresenta anche un modo di bypassare infrastrutture controllate da potenze estere. Il sistema finanziario globale oggi ha nodi centrali come SWIFT (per i pagamenti interbancari) dominati da potenze occidentali, e il dollaro è usato come leva politica (sanzioni, congelamento di riserve). Una rete come Bitcoin è resiliente alle sanzioni: non esiste un "pulsante" per escludere un paese. Paesi come la Russia hanno visto i vantaggi di poter transare fuori dal sistema SWIFT, e anche se Bitcoin oggi non ha la liquidità sufficiente per sostenere il commercio di grandi materie prime (pensiamo al petrolio, il cui mercato è immensamente più grande in volume di Bitcoin), ciò potrebbe cambiare se la capitalizzazione di BTC continuasse a crescere. Un petroBitcoin è forse fantasia, ma ricordiamo che all'inizio del '900 l'oro svolgeva questa funzione di riserva neutrale.

Alcuni analisti hanno ipotizzato scenari di "Bitcoin standard": ad esempio, piccole economie potrebbero ancorare la propria valuta a Bitcoin (come facevano col gold standard) per importare la credibilità di una moneta forte. El Salvador (il cui presidente Bukele), oltre ad aver reso Bitcoin corso legale, sta sperimentando strumenti come i "Volcano Bonds" – bond di stato denominati in USD ma legati al finanziamento di infrastrutture Bitcoin e con partecipazione in Bitcoin. Se iniziative così dimostrassero successo (El Salvador afferma di aver attratto turismo e investimenti grazie a Bitcoin, anche se i risultati sono misti finora), altri paesi potrebbero seguirne l'esempio, creando un blocco di nazioni pro-Bitcoin.

Stabilità finanziaria e rischi sistemici: D'altro canto, i regolatori temono possibili rischi: se Bitcoin diventasse molto integrato nel sistema, un suo crollo repentino di valore potrebbe avere effetti a catena. Ad esempio, immaginiamo che nel 2030 molte banche abbiano piccole percentuali di riserve in BTC, o aziende e fondi pensione esposti: un drawdown del 50% di Bitcoin (non insolito finora) potrebbe causare perdite e innescare una contrazione del credito. Ciò spinge verso la necessità di regole prudenziali: Basilea (il comitato per la regolamentazione bancaria) ha già proposto limiti stringenti su

quanto Bitcoin le banche possono detenere come capitale (massimo 1% del patrimonio, ponderazione di rischio 1250%). Queste misure indicano un riconoscimento: Bitcoin esiste e può essere detenuto, ma viene inquadrato come asset ad alto rischio dal regolatore tradizionale, almeno finché la volatilità non scende.

Una riduzione della volatilità potrebbe avvenire man mano che la market cap cresce e che strumenti come futures/ETF aumentano la partecipazione e la liquidità. Già dal 2021 l'indice di Sharpe di Bitcoin (performance aggiustata per la volatilità) è risultato comparabile o superiore a quello dell'S&P500 su orizzonti pluriennali, suggerendo che il rapporto rischio-rendimento di Bitcoin si sta avvicinando a quello di asset mainstream, pur mantenendo una volatilità più elevata.

Prospettiva di lungo termine – convergenza con il sistema finanziario: Potremmo immaginare che tra dieci o vent'anni la distinzione tra "finanza crypto" e "finanza tradizionale" sia molto sfumata. Bitcoin, se continuerà ad affermarsi, potrebbe fungere da strato di settlement universale anche per la finanza tradizionale tokenizzata. Lo stesso CEO di BlackRock, nella lettera 2025, ha parlato di tokenizzazione dei mercati dei capitali come evoluzione inevitabile, paragonandola al passaggio dalla posta tradizionale all'e-mail . In quella visione, l'infrastruttura di settlement odierna (complessa, lenta, con molti intermediari) potrebbe essere in parte rimpiazzata da reti blockchain che permettono trasferimenti peer-to-peer istantanei di asset tokenizzati (azioni, obbligazioni, ecc.). Se così fosse, Bitcoin – con la sua sicurezza e il suo record di immutabilità – è una candidata naturale per ospitare almeno una porzione di questo nuovo sistema (direttamente on-chain per asset semplici o via sidechain per quelli complessi). Un paragone fatto da Fink è con il network SWIFT: "l'infrastruttura di asset tokenizzati potrebbe bypassare gli intermediari tradizionali abilitando movimenti di asset istantanei peer-to-peer" . Ciò potrebbe democratizzare l'accesso ai mercati, ridurre costi e tempi, e portare ad un sistema finanziario più integrato e globale.

Geopolitica dell'hash rate: Un'ultima nota geopolitica riguarda la competizione per l'hash rate e le risorse minerarie. Se il mining di Bitcoin diventa un'industria strategica (perché Bitcoin stesso è strategico), potremmo vedere paesi favorire politiche per attrarre miner – un po' come fanno per le aziende high-tech. Gli Stati Uniti già beneficiano di essere top nell'hash rate, e alcuni politici (soprattutto a livello statale) sostengono apertamente il mining come settore di innovazione e occupazione. Al contrario, la Cina ha scelto di soffocarlo (forse per motivi di controllo sul capitale). Il Kazakhstan dopo il boom iniziale ha imposto regolamentazioni e tasse ai miner. La Russia, che dispone di enormi surplus energetici, ultimamente sembra voler usare il mining come strumento per monetizzare il gas e l'elettricità in eccesso (ci sono proposte di legge per riconoscere e regolare il mining come attività lecita, creando pool di stato). Insomma, Bitcoin entra nelle agende politiche nazionali, e la distribuzione del hash rate potrebbe essere vista come parte di una "gara tecnologica" tra potenze, non diversamente da quella per l'AI o per i semiconduttori.

Inclusione finanziaria: Sul fronte socio-economico, Bitcoin come infrastruttura aperta potrebbe portare vantaggi di inclusione finanziaria. Circa 1,4 miliardi di persone nel

mondo sono ancora unbanked, prive di accesso ai servizi finanziari di base. Tuttavia, una larga parte di queste persone possiede ormai uno smartphone. Bitcoin e Lightning permettono a chiunque con un telefono di ricevere e inviare pagamenti globali, di custodire risparmi senza autorizzazione esterna, e persino di accedere a strumenti di risparmio/investimento di base (anche solo detenere BTC è una forma di investimento). Già iniziative come Bitcoin Beach in El Salvador o programmi educativi in Africa stanno mostrando come giovani e comunità possano usare wallet Lightning al posto di conti bancari. Se questa tendenza si diffonde, Bitcoin potrebbe ridurre il divario di accesso finanziario, fungendo da "banca tascabile" per milioni di nuovi utenti. Questo avrebbe implicazioni macro: più inclusione significa più attività economica, imprenditorialità e resilienza finanziaria in paesi poveri.

Resistenze e scenari avversi: Non è scontato però che tutto fili liscio verso un'utopia bitcoin-centrica. Possiamo delineare alcune possibili resistenze e contromosse:

- Le banche centrali stanno sviluppando proprie valute digitali (CBDC). Una CBDC, pur centralizzata, potrebbe offrire alcuni benefici tecnici (pagamenti rapidi) e cercare di sbarrare la strada a Bitcoin offrendo un'alternativa "ufficiale". Tuttavia, la differenza in termini di libertà e privacy rimane netta, quindi probabilmente coesisteranno, servendo scopi diversi.

- I governi potrebbero intensificare la regolamentazione: ad esempio, imponendo severe misure KYC/AML su qualsiasi conversione tra Bitcoin e valute locali, o tassazioni punitive. Ciò potrebbe rallentare l'adozione, ma l'esperienza mostra che la domanda trova vie traverse (OTC, peer-to-peer).

- Attacchi coordinati: se Bitcoin venisse visto come minaccia diretta all'ordine monetario (ad esempio se molte persone abbandonassero la valuta locale per BTC, ostacolando la politica monetaria), potrebbero sorgere alleanze tra paesi per limitarlo. Ma un "ban globale" è improbabile dati gli incentivi a defezionare (ci sarà sempre un paese pronto ad accogliere innovazione e capitali bitcoin se altri li scacciano).

- Crisi interne: bug critici o fallimenti di parti dell'ecosistema (exchange importanti, stablecoin legate a Bitcoin) potrebbero intaccare la fiducia. Finora la robustezza tecnica di Bitcoin è stata alta, e paradossalmente i fallimenti (MtGox, FTX, ecc.) hanno rafforzato la narrativa dell'importanza della self-custody e della solidità del protocollo vs intermediari.

Tirando le somme delle prospettive: il cammino di Bitcoin come infrastruttura finanziaria globale appare plausibile e già avviato, ma non lineare né garantito. È una sorta di stress test su scala planetaria: stiamo scoprendo in tempo reale come un sistema monetario decentralizzato interagisce con sistemi centralizzati secolari. Forse vedremo un'integrazione graduale: Bitcoin coesisterà con valute fiat e altre innovazioni, venendo utilizzato dove offre vantaggi comparativi (sicurezza, riserva di valore, neutralità) e integrandosi con l'esistente (ad esempio, fungendo da rete di settlement per CBDC o stablecoin, come già avviene con Taro/Lightning per USD tokenizzati). In parallelo,

potrebbe crescere una economia nativa Bitcoin: individui e aziende che operano principalmente in BTC, simile a come Internet ha creato industrie native (e-commerce, social media) parallelamente all'uso di internet da parte di settori tradizionali.

Se dovessimo immaginare una rivista tra 10 anni che riguardi Bitcoin, potremmo trovarci a discutere non più se Bitcoin sarà parte della finanza globale, ma in che misura e sotto quale forma. Sarà più un "oro digitale" detenuto da banche centrali e privati come riserva anti-inflazione? Oppure sarà la "rete di regolamento" sottostante la maggior parte delle transazioni di valore del mondo, magari invisibile agli utenti finali ma presente dietro ogni pagamento? O entrambe le cose?

In ogni caso, l'evoluzione fin qui analizzata mostra che Bitcoin sta già forzando riflessioni profonde sul concetto di denaro, sovranità monetaria e infrastrutture finanziarie. Ha innescato innovazione in campi collaterali (crittografia, hardware, politiche energetiche). Come infrastruttura emergente, ha il potenziale di rendere il sistema finanziario più aperto, efficiente e inclusivo, ma anche la potenza di sconvolgere status quo consolidati.

Il futuro di Bitcoin come infrastruttura globale dipenderà dalla sua capacità di maturare – tecnicamente, economicamente e istituzionalmente – mantenendo i suoi valori fondanti di decentralizzazione e libertà. Gli anni a venire saranno cruciali per osservare se questa promessa si realizzerà pienamente o se rimarrà confinata a una nicchia, pur significativa, del sistema. I segnali attuali, come abbiamo visto in questo numero speciale, indicano un percorso di crescita e integrazione sempre più marcato, al punto che parlare di Bitcoin solo come "moneta alternativa" è riduttivo: sta diventando un vero ecosistema finanziario parallelo, destinato a intersecarsi con quello tradizionale.

Come autori e analisti, rimaniamo attenti e rigorosi nel monitorare questi sviluppi, pronti a documentare il prossimo capitolo di quella che è – a tutti gli effetti – una rivoluzione infrastrutturale in divenire.

Glossario

Bitcoin (BTC): Protocollo decentralizzato e criptovaluta nativa lanciata nel 2009 da Satoshi Nakamoto. Consente di trasferire valore in modo pseudonimo senza autorità centrali. Il termine si riferisce sia alla rete (Bitcoin con la B maiuscola) sia all'unità di conto (bitcoin/btc, minuscolo).

Blockchain: Registro distribuito costituito da blocchi di transazioni collegati in ordine cronologico e assicurati crittograficamente. La blockchain di Bitcoin è la sequenza immutabile di tutti i blocchi (in media uno ogni ~10 minuti) contenenti le transazioni confermate dalla rete.

Proof-of-Work (PoW): Meccanismo di consenso usato da Bitcoin. I miner competono nel risolvere un puzzle computazionale (trovare un hash inferiore a una certa soglia) per poter aggiungere un nuovo blocco alla blockchain. PoW rende onerosa la scrittura dei blocchi, garantendo la sicurezza della rete: un eventuale attaccante dovrebbe disporre di più potenza di calcolo di tutto il resto della rete per riscrivere la storia delle transazioni.

Hash Rate: La potenza computazionale totale dedicata al mining su una rete PoW. Misurata in hash al secondo (H/s), indica quante operazioni di hashing vengono effettuate globalmente dai miner. Un hash rate elevato rende la rete più robusta contro attacchi 51%. Nel caso di Bitcoin si parla in terahash (TH/s), petahash, exahash (EH/s).

Mining (estrazione): Il processo di partecipazione alla sicurezza della rete PoW, in cui i "miner" utilizzano hardware specializzato (ASIC) per calcolare hash e tentare di creare il prossimo blocco valido. Come incentivo, il miner vincitore di ogni blocco riceve una ricompensa in bitcoin (block reward) più le commissioni delle transazioni incluse.

Halving: Evento programmato nel protocollo Bitcoin che dimezza la ricompensa per blocco ogni 210.000 blocchi (circa ogni 4 anni). Iniziata a 50 BTC per blocco nel 2009, la reward è scesa a 25 BTC (2012), 12.5 BTC (2016), 6.25 BTC (2020), e continuerà (3.125 BTC dal 2024, ecc.). I halving garantiscono che l'offerta totale converga a 21 milioni di BTC.

Lightning Network (LN): Rete di secondo livello costruita su Bitcoin per abilitare transazioni off-chain istantanee e a basso costo. Funziona attraverso canali di pagamento bidirezionali fra nodi: gli utenti aprono canali con una transazione on-chain, poi possono effettuare molte micro-transazioni fuori dalla blockchain. I pagamenti possono essere instradati attraverso più canali (come nodi di una rete) grazie ad appositi contratti (HTLC), raggiungendo destinatari non direttamente connessi. LN migliora la scalabilità e l'usabilità di Bitcoin per pagamenti frequenti e di piccolo importo.

Layer 2 / Secondo Livello: Indica protocolli o reti costruite sopra la blockchain principale (Layer 1) per migliorarne funzionalità e prestazioni. Lightning Network è un esempio di

layer 2 per Bitcoin. I layer 2 in genere mantengono la sicurezza del layer 1 (ancorandosi ad esso per le finalità) ma evitano di usare la blockchain per ogni transazione, scaricando così il livello base.

Sidechain: Blockchain parallela e separata collegata alla blockchain principale tramite un meccanismo di peg (ancoraggio). Permette di spostare asset (es. BTC) dalla mainchain alla sidechain e viceversa. Sulla sidechain vigono regole possibimente diverse (più capacità, smart contract, privacy, ecc.) senza però coinvolgere il consenso della mainchain per le sue operazioni interne. Esempi: Liquid e Rootstock per Bitcoin.

Stablecoin: Token digitale ancorato nel valore a un asset stabile, tipicamente valute fiat come il dollaro. I stablecoin possono esistere su varie blockchain. Nel contesto Bitcoin, storicamente Tether (USDT) era emesso su un layer chiamato Omni, oggi l'attenzione è su stablecoin portati su Lightning tramite protocolli come Taproot Assets (ex Taro). I stablecoin permettono di scambiare valore in dollari (o altra valuta) pur utilizzando l'infrastruttura crypto.

Taproot: Upgrade del protocollo Bitcoin attivato nel 2021 (block 709,632) che migliora la privacy e la flessibilità degli script. Introduce le MAST (Merklized Abstract Syntax Tree) e le firme di Schnorr. Consente di nascondere le condizioni non utilizzate di uno script e rende le transazioni multi-firma indistinguibili da quelle standard, aumentando la fungibilità.

Multisig (Multi-firma): Meccanismo per cui un indirizzo Bitcoin è controllato da n chiavi e richiede m firme (m di n) per spendere i fondi. Ad esempio un multisig 2-di-3 richiede almeno 2 firme su 3 chiavi totali. Usato per custodia condivisa, portafogli aziendali, federazioni (Fedimint) e come misura di sicurezza (es. custodire backup delle chiavi in luoghi separati).

Full Node: Un nodo completo della rete Bitcoin che scarica e verifica l'intera blockchain in modo indipendente, assicurandosi che ogni blocco e transazione seguano le regole di consenso. I full node non minano necessariamente, ma propagano transazioni e blocchi e rifiutano quelli non validi. Sono cruciali per la decentralizzazione: ogni utente può eseguire un full node per verificare in proprio le proprie transazioni e mantenere la rete onesta.

SPV (Simple Payment Verification): Modalità "leggera" di un wallet Bitcoin che non scarica l'intera blockchain ma solo gli header dei blocchi, richiedendo prova dell'inclusione di transazioni rilevanti. Gli SPV wallet sacrificano parte della sicurezza (si fidano dei nodi completi per la verifica) in cambio di minore consumo di dati e risorse.

Hash Rate (share) per Paese: Distribuzione percentuale della potenza di mining tra diversi paesi. Spesso stimata indirettamente tramite dati dei pool o indirizzi IP. Ad es. USA ~38%, Cina ~20%, etc. (dati variabili nel tempo) .

ETF Bitcoin (Exchange-Traded Fund): Fondo d'investimento negoziato in borsa che replica il prezzo di Bitcoin. Può essere basato su contratti futures (come gli ETF approvati inizialmente negli USA) o detenere bitcoin fisici (ETF "spot", approvati in Canada, UE e in fase di approvazione negli USA). Permette agli investitori di esporsi a BTC attraverso mercati tradizionali regolamentati, senza gestire direttamente chiavi private.

L402: Protocollo (nome che richiama l'errore HTTP 402 Payment Required) per autenticare richieste verso servizi web tramite pagamenti Lightning. Presentato da Lightning Labs, consente di monetizzare API e servizi web con micropagamenti machine-to-machine . Integrato ad esempio con librerie AI (LangChain) per far pagare ad agenti AI l'accesso a risorse.

Fedimint: Contrazione di Federated Mint, è un protocollo di federazioni di custodia con Chaumian e-cash su Bitcoin . Un gruppo di nodi federati custodisce bitcoin in un indirizzo multi-firma e rilascia token e-cash (IOU anonimi) agli utenti depositanti. Offre privacy e transazioni off-chain istantanee tra membri della federazione. Può integrarsi con Lightning per trasferimenti inter-federazione. È un modo per scalare Bitcoin preservando decentralizzazione locale e privacy, bilanciando trust (i guardian federati) e verifica comunitaria.

Chaumian e-cash: Schema di moneta digitale inventato da David Chaum negli anni '80 che utilizza blind signatures per emettere token che il banco non può collegare all'identità dell'utente. Fornisce privacy nelle transazioni simile al contante. Fedimint è un'applicazione di Chaumian e-cash abbinata a Bitcoin.

Micropagamento: Transazione di valore molto basso (centesimi o frazioni di centesimo). Nei sistemi tradizionali i micropagamenti non sono praticabili per via delle commissioni (es. commissione carta di credito supera l'importo). Lightning abilita micropagamenti in satoshi (es. 1 satoshi = 0,00000001 BTC, pochi millesimi di centesimo) in modo efficiente, aprendo nuove possibilità (pagare al secondo, pay-per-use minimo, etc.).

Tokenizzazione: Processo di rappresentare un asset reale (es. una quota azionaria, un'obbligazione, un immobile) come token su una blockchain. Ciò permette trasferimenti e gestione più agili (24/7, peer-to-peer). Nel contesto, la tokenizzazione su Bitcoin potrebbe implicare usare protocolli come Taproot Assets per emettere token ancorati (vedi stablecoin) o usare sidechain per creare versioni tokenizzate di titoli tradizionali. BlackRock evidenzia la tokenizzazione come trend per rivoluzionare i mercati finanziari .

CBDC (Central Bank Digital Currency): Valuta digitale emessa da una banca centrale, essenzialmente la versione elettronica del contante nazionale, ma tracciabile e programmabile. Esempi pilota: e-CNY (yuan digitale cinese), sand dollar (Bahamas). Spesso centralizzate su database della banca centrale o con permessi limitati. Viste come risposta istituzionale alle criptovalute, offrono vantaggi di efficienza ma sollevano timori per la privacy e il controllo statale sulle transazioni.

Economia Machine-to-Machine: Ecosistema in cui dispositivi o software autonomi scambiano valore e servizi tra loro senza intervento umano diretto. Richiede un mezzo di pagamento automatizzato e interoperabile – le criptovalute (specie via Lightning) sono candidate ideali. Esempio: un'auto self-driving che paga automaticamente una stazione di ricarica elettrica; due agenti software che negoziano e pagano per risorse computazionali.

51% Attack: Scenario in cui un'entità (o collusione) controlla oltre il 50% dell'hash rate in una rete PoW, potendo quindi potenzialmente riorganizzare la blockchain a proprio vantaggio (es. doppia spesa). In Bitcoin, dato l'enorme hash rate distribuito, è considerato impraticabile a livello globale. Reti più piccole di altcoin a volte hanno subito attacchi 51%. La difesa principale è avere un hash rate elevato e decentralizzato, cosa in cui Bitcoin eccelle.

Decentralizzazione: Proprietà di un sistema in cui il controllo e le decisioni non sono concentrati in un singolo ente ma distribuiti tra i partecipanti. In Bitcoin significa: nessun server centrale, migliaia di nodi che convalidano, centinaia di migliaia di miner competitori, sviluppatori sparsi globalmente col codice open source e utenti con pieno controllo delle proprie chiavi. È graduale (non assoluta) e deve essere costantemente mantenuta (es. evitando che troppi utenti dipendano da pochi exchange o fornitori di wallet).

Fungibilità: Caratteristica per cui ogni unità di un asset è intercambiabile ed equivalente a un'altra. Per valute, è importante che nessuno possa discriminare tra "bitcoin buoni" e "bitcoin cattivi". Bitcoin a livello protocollo è fungibile, ma l'analisi blockchain può rendere alcuni coin "segnati" (es. provenienti da hack) e quindi rifiutati da alcuni servizi. Migliorie come CoinJoin, Taproot aumentano la fungibilità pratica mischiando gli output e uniformando il formato delle transazioni.

Cold Storage: Metodo di custodia di criptovalute offline, scollegato da internet, per prevenire hack. Può essere un hardware wallet, un paper wallet (chiavi scritte fisicamente), dispositivi tenuti in caveau, ecc. Fondamentale per custodire grosse quantità di BTC in sicurezza. Contrario di hot wallet, connesso e adatto all'uso frequente ma più vulnerabile.

Self-custody (Autocustodia): Tenere i propri bitcoin in un wallet di cui si detengono le chiavi private, senza affidarli a terzi (exchange, banche). "Not your keys, not your coins" è il motto: solo chi possiede la chiave privata può considerarsi realmente proprietario dei BTC associati. È resa possibile da software e hardware wallet user-friendly. L'autocustodia è un elemento chiave per la sovranità finanziaria individuale che Bitcoin propugna.

Wallet: Software o dispositivo che gestisce chiavi private e indirizzi per inviare/ricevere bitcoin. Può essere full node wallet (che verifica la blockchain interamente) o light wallet (che usa server esterni per info). Esempi: Core (full node), Electrum (light/SPV), Wallet of

Satoshi (custodial LN wallet), hardware wallet (Ledger, Trezor). Su Lightning, i wallet gestiscono anche canali e bilanci LN.

Smart Contract: In Bitcoin sono tipicamente script di spesa con determinate condizioni (es. multisig, lock temporali). Non sono turing-complete come su Ethereum, ma permettono funzionalità essenziali. Esempi: HTLC per Lightning (pagamento condizionato a rivelazione di segreto), timelock per escrow/HTLC, script multifirma per Fedimint, ecc. Taproot amplia la flessibilità degli smart contract Bitcoin mantenendoli privati fino all'esecuzione.

Oracolo: Fonte esterna di dati che, se integrata, permette a uno smart contract di reagire a eventi del mondo reale (es. prezzo, meteo). Bitcoin non ha oracoli nativi (per scelta di minimalismo e sicurezza), ma può interfacciarsi tramite schemi come DLC (Discrete Log Contracts) dove oracoli firmano esiti esterni e le parti possono regolare scommesse o contratti basati su quei dati. Esempio: un contratto che paga X BTC se il prezzo dell'oro supera Y, usando un oracolo di prezzo.

MOE, UoA, SoV: Tre funzioni classiche della moneta: Medium of Exchange (mezzo di scambio), Unit of Account (unità di conto) e Store of Value (riserva di valore). Bitcoin finora è usato principalmente come riserva di valore (SoV) e in certa misura mezzo di scambio (MoE) in nicchie specifiche, ma non è ancora diffusamente unità di conto (nessuno prezza beni in BTC a parte eccezioni). La direzione futura potrebbe vederlo affermarsi in tutti e tre i ruoli, almeno in alcuni contesti.

DeFi (Finanza Decentralizzata): Ecosistema di applicazioni finanziarie costruite su blockchain senza intermediari tradizionali (es. lending, trading, derivati tramite smart contract). Sviluppato soprattutto su Ethereum e affini. Su Bitcoin la DeFi è meno sviluppata per scelta tecnica (Bitcoin non ha contratti complessi on-chain), ma esistono protocolli come Lightning (per prestiti?), Sovryn su RSK, e vari progetti su sidechain/Layer2 che potrebbero portare funzionalità DeFi rispettando la sicurezza Bitcoin.

NFT (Non-Fungible Token): Token unico e non intercambiabile, rappresentante tipicamente proprietà di oggetti digitali o fisici (arte digitale, collezionabili, certificati). Pur non essendo un caso d'uso centrale per Bitcoin, nel 2023 un upgrade (Taproot) e la nascita del protocollo "Ordinals" hanno permesso la creazione di NFT rudimentali direttamente sulla blockchain Bitcoin (inscription di dati). È un tema dibattuto perché porta carico sulla blockchain per dati non monetari; comunque, è possibile tokenizzare oggetti unici anche su Bitcoin, sebbene la community sia più focalizzata su asset fungibili e valore.

DAO (Decentralized Autonomous Organization): Organizzazione che opera tramite regole codificate su blockchain, tipicamente gestita dai membri attraverso token di governance. Esempio: protocolli DeFi governati da token holder. Su Bitcoin non esistono DAO complesse on-chain, ma concetti simili possono emergere in layer2/federazioni (Fedimint ha elementi di DAO nella governance delle federazioni). Si parla anche di AI-DAO quando un'entità autonoma posseduta da un'IA agisce economicamente – concetto ancora teorico.

Blind Signature: Schema crittografico che permette a un firmatario di firmare un messaggio senza conoscerne il contenuto. Usato nei sistemi Chaumian e-cash (Fedimint) per emettere token spendibili anonimamente: l'utente blinda il token, la federazione firma, e l'utente può riscattare il token scoprendolo – la firma è valida ma l'emittente non sa quale token ha firmato.

Trilemma della Blockchain: Concetto per cui è difficile ottimizzare contemporaneamente per decentralizzazione, sicurezza e scalabilità: aumentando la scalabilità (es. blocchi più grandi) si rischia di ridurre decentralizzazione (meno nodi possono operare) o sicurezza. Bitcoin privilegia sicurezza e decentralizzazione, spostando la scalabilità sui layer esterni (Lightning etc.) per aggirare il trilemma a livello base.

Cryptography (Crittografia): Pilastro tecnologico di Bitcoin – algoritmi come SHA-256 (hash), ECDSA (firme digitali) garantiscono integrità e autenticità delle transazioni. La solidità della crittografia usata è fondamentale: eventuali rotture (es. quantum computing) richiederanno aggiornamenti a schemi più robusti. Finora, la crittografia di Bitcoin ha resistito a ogni attacco pratico.

Privacy (in Bitcoin): Bitcoin offre pseudonimità, ma tutte le transazioni sono pubbliche. Vari strumenti migliorano la privacy: CoinJoin (mescolamento di transazioni tra più utenti), indirizzi diversi per ogni transazione, uso di Lightning (transazioni off-chain non pubbliche), Taproot che rende uniformi output complessi, e soluzioni esterne come Fedimint/Cashu per privacy completa a scapito di custodia federata. La privacy è vista come componente cruciale per fungibilità e libertà dell'utente.

UTXO (Unspent Transaction Output): Il modello contabile di Bitcoin è basato su output non spesi. Ogni transazione prende UTXO in input e crea nuovi output. Un output può essere speso interamente in una transazione successiva (non si può spendere parzialmente un UTXO, il resto viene "dato come resto" in un nuovo output all'utente). Mantenere il sistema UTXO efficiente e anonimo è parte del design: es. riutilizzo di indirizzi può collegare UTXO a uno stesso utente, riducendo privacy.

Lightning Channel: Connessione tra due nodi Lightning dove hanno allocato una certa quantità di BTC come capacità di canale. All'apertura, i fondi sono bloccati in multisig su Bitcoin. All'interno del canale, i due nodi scambiano transazioni firmate che aggiornano i saldi reciproci. Quando il canale si chiude, l'ultimo saldo viene risolto on-chain e i BTC restituiti a ciascuno secondo l'ultimo stato. Un canale può instradare pagamenti per terzi se connesso a più nodi, guadagnando commissioni.

Rebalancing (Lightning): Operazione di riequilibrio della liquidità nei canali LN. Se un nodo esaurisce la capacità in uscita su un canale (perché ha inviato molto e ricevuto poco), può spostare fondi attraverso la rete (spesso usando un loop interno) per ricaricare la capacità. Il rebalancing efficiente è importante per mantenere linetti i pagamenti LN e richiede algoritmi ottimizzati (spesso aiutati da tool automatici, potenzialmente AI in futuro).

Payment Channels (Canali di Pagamento): Concetto generale di tenere un conto aperto off-chain tra due parti, regolando on-chain solo all'inizio e alla fine. Il Lightning Network è una rete di canali di pagamento. I channel factory consentono di creare molti canali off-chain con un gruppo multi-party usando una singola transazione on-chain, migliorando la scalabilità di apertura.

Hash Time-Locked Contract (HTLC): Contratto usato in LN e atomic swaps: un output viene bloccato da due condizioni ("hashlock" e "timelock"). Il destinario deve fornire un preimage segreto corretto per riscattare prima della scadenza; se non lo fa entro un certo tempo, il mittente può reclamare i fondi. Questo consente pagamenti condizionali e la costruzione di catene di fiducia: i nodi LN transit intermedi ricevono la loro parte solo se inoltrano la chiave segreta, garantendo correttezza del routing.

On-chain / Off-chain: Attività o transazioni che avvengono direttamente sulla blockchain (on-chain) vs al di fuori di essa (off-chain). Lightning è off-chain. Off-chain spesso implica maggior centralizzazione/trust ma velocità e costo minore; Lightning cerca di mantenere trust-minimization usando contratti con possibili ritorni on-chain in caso di dispute (backup on-chain). Off-chain allevia il carico on-chain e migliora esperienza utente per microtransazioni.

Brevetti e Open-Source: Il software Bitcoin (Bitcoin Core) e protocolli correlati sono open-source e comunitari. Ciò ha favorito l'adozione globale. Alcune aziende nel settore custodiscono brevetti (es. su tecniche di ottimizzazione mining o funzioni di wallet), ma i protocolli base restano aperti. Un'infrastruttura finanziaria globale idealmente dovrebbe essere come Internet: basata su standard aperti, non proprietari, per massima interoperabilità.

Security Budget: Termine che indica quanto i miner guadagnano (block reward + fees) per mantenere la rete sicura. Su Bitcoin è attualmente dominato dai block reward, ~900 BTC al giorno (2023). Dopo vari halving, il "budget" scenderà se le fee non compensano. Un adeguato security budget è cruciale per incentivare abbastanza hash rate da prevenire attacchi. C'è dibattito se col tempo le sole fee basteranno o se saranno necessarie modifiche (molto controverso, es. qualche forma di tail emission; al momento la maggioranza preferisce mantenere il limite fisso di 21M e confidare nel mercato delle fee).

Lightning Liquidity: La disponibilità di fondi in un canale LN per inviare/ricevere. Un nodo per ricevere pagamenti deve avere capacità in ingresso (liquidità allocata dal lato dei partner di canale verso di lui). Sono nati servizi e mercati per liquidity leasing (es. Lightning Pool di Lightning Labs) dove i nodi pagano per ottenere canali aperti a loro favore. La gestione della liquidità è un nuovo mestiere introdotto da LN, quasi analogo alla gestione di liquidità bancaria, ma su scala di satoshi.

BIP (Bitcoin Improvement Proposal): Processo attraverso cui vengono proposte, discusse e standardizzate modifiche o aggiunte al protocollo Bitcoin e all'ecosistema (ci sono BIP per protocolli secondari, formati wallet, etc.). Esempi: BIP39 (mnemoniche seed), BIP125 (RBF), BIP141 (SegWit). Le decisioni sul protocollo coinvolgono la comunità e

richiedono consenso diffuso dei nodi per attuazione. Questo processo di governance informale ma robusto è un aspetto chiave della decentralizzazione di Bitcoin.

MEV (Maximal Extractable Value): Concetto dalla DeFi Ethereum (miner/cercatori che estraggono valore riordinando transazioni), in Bitcoin è meno rilevante data la mancanza di arbitraggi complessi on-chain. Tuttavia, con Ordinals e altri usi, potrebbe emergere. Finora il "MEV" su Bitcoin era limitato a includere transazioni con fee più alte o qualche raro caso (es. catturare una transazione errore con fee altissima). Su LN, esiste il concetto di routing fee ma è un mercato libero e competitivo.

Riferimenti

1. Munawa, F. (2023). Lightning Labs Unveils Bitcoin Tools for AI – CoinDesk
2. Gentry, R. (2024). Taproot Assets on Lightning: The Global Financial Interoperability Layer – Lightning Labs Engineering Blog
3. Braun, H. (2023). BlackRock CEO Larry Fink Says Bitcoin Could 'Revolutionize Finance' – CoinDesk
4. Wright, L. (2025). BlackRock's Larry Fink confirms Bitcoin could replace US dollar as global currency amid rising US debt – CryptoSlate
5. Quill, V. (2025). $19 trillion in transactions settled on the Bitcoin network in 2024 – CoinTelegraph
6. CoinShares Research (2023). The Bitcoin Mining Network – 2024 Mining Report
7. Tuwiner, J. (2024). Bitcoin Mining Hashrate by Country – Bitbo Research
8. The Past, Present, and Future of the Lightning Network – UTXO Stack Medium
9. River Financial (2023). The Lightning Network Grew by 1212% in 2 Years – River Lightning Report
10. Coinbase Institutional (2022). Bitcoin Fedimints - Market Intelligence Report
11. Lightning Labs (2023). Twitter announcement
12. CCAF – Cambridge Bitcoin Electricity Consumption Index & Mining Map (2022 data)
13. BlackRock (2025). Annual Chairman's Letter to Shareholders – (Estratti cit. da CryptoSlate)
14. Medium (2018). Them Lightning Network Nodes Sure Do Look Centralized To Me! – StopAndDecrypt
15. Bitcoin Magazine (2023). Lightning Network Capacity Chart – BitcoinMagazine Pro
16. SEC (2024) – Statement on the Approval of Spot Bitcoin Exchange-Traded Products. U.S. Securities and Exchange Commission, 10 gennaio 2024. (Annuncio ufficiale dell'approvazione dei primi ETF spot su Bitcoin negli USA, a firma del Chair G. Gensler).
17. BIS (2023) – Annual Economic Report, Cap. III: "Blueprint for the future monetary system: improving the old, enabling the new". Bank for International Settlements,

giugno 2023. (Analisi della posizione delle criptovalute e delle CBDC nel futuro sistema monetario globale).

18. FRB Cleveland (2022) – The Lightning Network: Turning Bitcoin into Money. Federal Reserve Bank of Cleveland, Working Paper No. 22-19, giugno 2022. (Studio sul funzionamento e sull'adozione di Lightning Network come soluzione per scalare Bitcoin nelle transazioni quotidiane).

19. IMF (2023) – Elements of Effective Policies for Crypto Assets. International Monetary Fund, Policy Paper No. 2023/004, febbraio 2023. (Orientamenti del FMI sulla regolamentazione cripto; il Direttorio IMF ha raccomandato di non conferire status di moneta a corso legale alle cripto).

20. OSTP (2022) – Climate and Energy Implications of Crypto-Assets in the United States. White House Office of Science and Technology Policy, settembre 2022. (Rapporto ufficiale della Casa Bianca sull'impatto energetico delle criptovalute, con stime di consumo annuale e raccomandazioni per mitigare le emissioni).

HUMAN ADVISOR PROJECT

HELP HUMAN HELP HUMANITY

humanadvisorproject.org