Debunking delle più comuni critiche a Bitcoin

L’autore di questo pezzo è Pindol, che si è ispirato all’articolo pubblicato in inglese da SafeHodl su Github e qui largamente espanso attingendo da numerose fonti. Dopo una revisione da parte di vari amici (fra cui Marco Amadori, David Coen, Francesco Simoncelli, Luca Venturini) è stato infine riadattato da Alberto De Luigi nella versione che segue.

Nonostante i detrattori da anni dichiarino Bitcoin morto, capitalizzazione di mercato, hashrate e quantità di nodi della rete continuano a crescere. Ogni giorno sempre più sviluppatori, ricercatori, investitori e sostenitori entrano in quell’incredibile cammino di iniziazione che è la conoscenza di Bitcoin, del mondo che gli gravita attorno e del suo potenziale dirompente.

Una maggiore adozione attrae inevitabilmente anche le attenzioni degli haters, che fantasticano sugli scenari più disparati in cui Bitcoin, per una ragione o per l’altra, è destinato a fallire. Per fugare ogni dubbio ai neofiti, in questo articolo si elencano alcune delle più comuni critiche rivolte a Bitcoin, mettendone a nudo l’inconsistenza.

INDICE

- La sorveglianza e la regolamentazione renderanno inutile Bitcoin

2. **La tecnologia Bitcoin è destinata al fallimento!**

- Un crash di internet fermerà Bitcoin
- Bitcoin non può scalare, le transazioni sono troppo lente e costose
- L'informatica quantistica romperà la crittografia usata in Bitcoin
- Un bug in Bitcoin potrebbe consentire agli hacker di rubare bitcoin o interrompere la funzionalità della rete.

3. **Un ecosistema Bitcoin decentralizzato non può durare!**

- Chi controlla o colpisce le mining pool più grandi ha il potere di censurare o interrompere tutte le transazioni
- Un pesante calo dei prezzi o il termine dell'emissione di nuovi bitcoin nel 2140 potrebbero indurre i miners a spegnere le macchine, paralizzando la rete
- Bitcoin è troppo complesso per essere detenuto in sicurezza dalle persone comuni, quindi i servizi di custodia finiranno per "corrompere" il sistema e potranno essere attaccati dai governi

4. **Bitcoin non è una riserva di valore!**

- La scarsità può essere modificata dagli sviluppatori a differenza di altre riserve di valore come l'oro
- Il prezzo di bitcoin è troppo alto, perciò gli investitori preferiranno crypto che costano meno
- Il Bitcoin può essere **forkato** all'infinito, il che diluisce il valore
- Bitcoin non ha valore intrinseco
- Bitcoin è uno schema Ponzi
- Bitcoin è una bolla come quella dei tulipani
- Bitcoin non ha rendimento, non è un investimento, quindi non ha valore

- Bitcoin non può essere garantito, a differenza dei depositi bancari
- Il bitcoin è troppo volatile per essere riserva di valore o in un portafoglio di investimenti
- Il prezzo di Bitcoin è manipolato dalla stablecoin Tether
- Le valute digitali della banca centrale (CBDC) supereranno Bitcoin

5. **Le nuove criptovalute supereranno Bitcoin!**

- Il codice di Bitcoin si può copiare e riprodurre in una versione migliore
- La tecnologia di Bitcoin è obsoleta
- Il mondo degli smart contracts e finanza decentralizzata è alternativo a Bitcoin e più attrattivo per gli investitori
- La Proof-of-Stake è il futuro

6. **I bitcoiner sono una setta di idioti e criminali!**

- La blockchain è la vera rivoluzione non Bitcoin
- Bitcoin permette di evadere le tasse
- I terroristi, criminali e narcotrafficanti usano Bitcoin
- Le valute legali hanno successo perché sono imposte con l'uso della forza (militarmente) e sono l'unico modo per pagare le tasse, Bitcoin non è supportato da nulla
- Bitcoin non ha reali casi d'uso in cui può essere superiore alle valute tradizionali
- La distribuzione di Bitcoin nella popolazione è socialmente iniqua e la rendita derivata premia i possessori in modo immeritato
- Una moneta deflazionistica rallenta l'economia, per cui l'adozione di Bitcoin è deleteria
- Bitcoin non è adottato dai commercianti e ha fallito come moneta
- Bitcoin è soggettivo, immaginario, un'illusione di massa
- Bitcoin è un culto, le persone che ci credono sono

ideologi e massimalisti
- Bitcoin usa troppa energia, fa male all’ambiente

1. Bitcoin verrà bloccato dai governi!

I governi vieteranno la proprietà di Bitcoin o fermeranno il network di nodi

- Tutti i Paesi hanno confini che possono essere attraversati più o meno facilmente da cose e persone. Bitcoin, essendo immateriale, attraversa i confini con la stessa facilità con cui lo può fare qualsiasi tipo di informazione. Le transazioni Bitcoin (o i seed e le chiavi private) possono essere nascosti in messaggi di testo, immagini o anche emoji su qualsiasi supporto digitale o fisico, e quindi inviati tramite diversi mezzi di comunicazione: via internet, tramite satellite, reti mesh, trasmettitori radio o – se proprio si volesse – anche coi piccioni viaggiatori.
- Bitcoin è pura informazione che può essere persino memorizzata (brainwallet) senza alcuna necessità di un supporto fisico. Qualsiasi altra risorsa è quindi più facile da confiscare o tassare: immobili, metalli preziosi, azioni, conti correnti. In casi estremi, come quello della confisca dell’oro avvenuta nel 1933 negli Stati Uniti, si è notato come molti cittadini abbiano nascosto con successo i loro averi in oro, nonostante la fisicità di quest’ultimo. Una confisca dei wallet casa per casa è tecnicamente impossibile anche per uno stato totalitario.
- Precursori di Bitcoin come E-Gold o Liberty Reserve furono facilmente bloccati dai governi principalmente a causa della loro centralizzazione. Al contrario, la rete

Bitcoin è peer to peer. Protocolli di rete come BitTorrent o Gnutella non possono essere fermati: fin dagli albori i governi hanno tentato di chiuderli ed ostacolarli senza avere successo.

- Sarebbe estremamente improbabile per un governo o una coalizione di governi fermare i nodi Bitcoin in tutti i Paesi del mondo. Finché un solo nodo è in esecuzione da qualche parte nel mondo, Bitcoin può continuare a convalidare le transazioni. Anche se uno stato obbligasse gli ISP operanti sul proprio territorio a bloccare i nodi Bitcoin, questa restrizione può essere facilmente aggirata attraverso VPN o Tor. La maggior parte dei software di gestione di nodi Bitcoin (come ad esempio MyNode o Umbrel) integrano Tor abilitato di default, tutte le connessioni in entrata e in uscita sono sotto rete onion, sul "dark web".
- In molti paesi difficilmente si trovano i presupposti giuridici per poter censurare Bitcoin, poiché possedere bitcoin è in ultima istanza possedere informazione, quindi vietarlo sarebbe simile a proibire la conoscenza e la divulgazione del sapere umano. Le leggi e costituzioni vigenti, come anche l'approccio tenuto finora da governi ed enti governativi, possono costituire precedente giuridico. Due esempi negli Stati Uniti:

    1. In US ci sono sentenze che stabiliscono che il codice sorgente del software è considerato un diritto di parola protetto dal primo emendamento della costituzione. Questo significa che la distribuzione del software open source come Bitcoin è, dal punto di vista giuridico, una libertà fondamentale assimilabile alla libertà di parola.
    2. Uno degli enti governativi degli Stati Uniti (FBI) ha messo all'asta migliaia di bitcoin sequestrati dagli account del mercato del dark web "Silk

Road”. Eventi analoghi sono accaduti altrove: Germania, Francia, Inghilterra, Lituania. Questo ha di fatto creato un precedente giuridico per cui Bitcoin non è considerato illegale, dal momento che i beni illegali sequestrati – come le droghe – non possono essere rivenduti, ma solo distrutti.

- Infine, di quali governi stiamo parlando? In El Salvador, bitcoin è diventato a giugno 2021 moneta a corso legale e altri stati (Paraguay, Colombia) sembrano intenzionati a fare la stessa cosa. La reazione a Bitcoin è decisamente diversa da paese a paese. I paesi competono tra loro vogliono attrarre investimenti e tecnologia, e può essere nel loro interesse farlo anche con Bitcoin. Alcuni governi e amministrazioni hanno vantaggio ad attrarre bitcoin e le industrie ad esso collegate, piuttosto che rischiare di farle fuggire. Nel corso della storia, sono sempre sorte giurisdizioni che vogliono catturare l’innovazione finanziaria incentivando la stessa con bassa tassazione e burocrazia più snella. Dove c’è forte competizione (es. Cina vs US), i Paesi tendono ad accumulare beni di riserva come l’oro, non potendo escludere che gli Stati concorrenti adottino politiche monetarie espansive, svalutando così le proprie riserve di valuta estera. Inoltre, i Paesi a cui sono state imposte sanzioni internazionali hanno interesse ad usare bitcoin per aggirarle.

Tutti i principali intermediari, fondi e servizi che si occupano di Bitcoin possono essere bloccati dai governi

- Fondi Pensione, fondi di investimento, compagnie di assicurazione, aziende, grandi istituzioni finanziarie, servizi di custodia ed exchange quotati in borsa possiedono bitcoin. I governi che hanno permesso a queste istituzioni di possedere bitcoin non saranno

sempre in grado di renderlo illegale senza impoverire la loro base di potenziali elettori.

- Il numero di coloro che possiede bitcoin è in continua crescita ed include anche politici, membri del governo e gruppi di interesse in grado di fare pressioni sullo stesso. Con una maggiore e più capillare diffusione di Bitcoin nel tempo, aumenta la probabilità che gli interessi in gioco siano troppo alti perché i governi siano intenzionati a remare contro Bitcoin.
- Ogni Paese che ha tentato di chiudere gli Exchange ha visto l'emergere delle alternative peer-to-peer diretti da persona a persona (es. Bitcoin per contanti tramite exchange decentralizzati) che possono sfruttare qualsiasi rete di pagamento esistente. Vi sono esempi come Bisq o HodlHodl.
- I governi non possono controllare a loro piacimento la domanda di mercato. Quando uno stato mette in atto politiche protezionistiche nascono spontaneamente mercati neri, ne sono un esempio quelli della cocaina, della cannabis o degli alcolici, che riescono ad espandersi e sopravvivere nonostante le enormi difficoltà di produzione, trasporto e distribuzione insiti in ogni bene fisico. I mercati neri prosperano anche sotto i regimi più oppressivi, come ad esempio la Corea del Nord. Bitcoin essendo immateriale è enormemente più facile da spostare e più difficile da rilevare rispetto a qualsiasi sostanza stupefacente.
- I governi hanno convenienza a trattare il mercato dei bitcoin come qualsiasi altra risorsa, ovvero tassandoli piuttosto che farli fuggire oltre confine. Nella maggior parte dei Paesi gli exchange di bitcoin operano legalmente seguendo le normative KYC e AML e i governi hanno convenienza economica al fiorire di queste aziende piuttosto che combattere il mercato nero o gli exchange decentralizzati.

La blockchain si può fermare localizzando i minatori tramite il consumo energetico e tagliando loro l'energia

- I minatori sono distribuiti a livello globale e utilizzano vari tipi di energia. Possono utilizzare l'energia semplicemente collegandosi alla rete elettrica, lavorando direttamente con i fornitori di energia (per prevenire il Renewable Curtailment), o autoprodurla (solare, eolico, micro-idroelettrico). Non c'è entità che possa trovarli e fermarli tutti.
- Anche se un gran numero di miners non potesse più utilizzare fonti energetiche e ciò provocasse un calo dell'hashpower (come peraltro è già accaduto) Bitcoin continuerebbe a funzionare. Nel caso in cui l'hashpower calasse repentinamente, per un breve periodo gli utenti attenderanno più a lungo per le conferme delle loro transazioni. Dopo 2016 blocchi la difficoltà della PoW si adegua riportando la distanza tra un blocco e l'altro vicina alla media dei 10 minuti, permettendo alla rete di continuare a funzionare come prima. In exrema ratio, se i tempi per la produzione di 2016 blocchi fossero troppo lunghi, la community può ridurli accordando un hard fork che modifichi i criteri di aggiustamento della difficoltà (come fatto ad esempio per Bitcoin Cash).

La sorveglianza e la regolamentazione di KYC / AML renderanno inutile Bitcoin

- I regolamenti interessano alcuni utenti in alcuni Paesi, ma non hanno alcun effetto sulla rete Bitcoin stessa. La creazione di indirizzi e transazioni non è censurabile.
- Aggiornamenti al protocollo bitcoin (Taproot e Schnorr Signatures), second layer come Lightning Network, tecnologie come Coinjoin, incrementano esponenzialmente il livello di privacy e fungibilità di bitcoin, scambi peer-to-peer (per cash ad esempio) e scambi tra

giurisdizioni che non condividono le informazioni non possono essere facilmente monitorati o sorvegliati.

- Per quegli individui che applicano alcuni basilari accorgimenti di privacy finanziaria, specialmente nell'uso del proprio wallet Bitcoin (ricambio degli indirizzi, coinjoin, lightning network, etc.) la sorveglianza tramite blockchain analysis non solo diventa incredibilmente costosa, ma anche tecnicamente inapplicabile.

2. La tecnologia Bitcoin è destinata al fallimento!

Un crash di internet fermerà Bitcoin

- Interruzioni di Internet per cause naturali – come eruzioni solari – potrebbero interrompere gran parte dell'infrastruttura di internet, ma Bitcoin continuerebbe a funzionare su quella rimanente: fintanto che un singolo nodo è online, la rete Bitcoin sopravvive.
- Se la comunicazione via internet è lenta o interrotta via internet fra alcune parti del mondo, è possibile "aggirarla" integrando in quella tratta geografica altre modalità di comunicazione. I ritardi nella trasmissione fra i nodi comporterebbe soltanto una maggiore attesa per la finalizzazione delle transazioni.
- Bitcoin può funzionare anche senza internet: i satelliti Bitcoin , le reti mesh e i trasmettitori radio possono continuare a trasmettere blocchi e transazioni bitcoin tra Paesi anche se Internet non funzionasse. Il singolo individuo non ha bisogno della rete internet per detenere bitcoin, creare transazioni e trasmetterle attraverso altri protocolli di comunicazione, o pagare tramite Lightning Network (se si possiede un canale

diretto con la controparte).

- Internet ormai è parte integrante della nostra società e anche se si verificasse un down generale della rete, sarebbe una priorità di tutta la società ripristinarla il più presto possibile. Se Internet smettesse del tutto di funzionare, in primis sarebbero le economie e i governi a subirne l'impatto.

Bitcoin non può scalare, le transazioni sono troppo lente e costose

- I bitcoin, tramite teoria dei giochi e crittografia avanzata, possono essere scambiati , senza che effettivamente avvenga un trasferimento su blockchain. Si dice in questo caso che i bitcoin vengono scambiati su un "layer" (strato) superiore alla blockchain, poiché vengono trasferite direttamente da wallet a wallet le informazioni necessarie a transare su blockchain, senza effettivamente farlo. La rete che realizza questo layer è nota come "Lightning Network" e chiunque può aderirvi senza doversi affidare ad alcun custodian o terza parte (è cioè detta "trustless"). Questo permette a Bitcoin di scalare, poiché, a fronte di uno spazio occupato minimo su blockchain (una singola transazione per l'apertura dello smart contract) è possibile effettuare potenzialmente migliaia di miliardi di transazioni all'anno, sufficienti a soddisfare il fabbisogno dell'intero pianeta (Visa a paragone ne processa 55 miliardi/anno).
- Metodi di pagamento che integrano bitcoin, pensiamo alle ricaricabili di Visa, Mastercard, payment processor come Paypal o app come Strike possono supportare un numero virtualmente infinito di transazioni, visto che non necessitano di usare il layer base di bitcoin per operare, tranne che per le macro operazioni di compensazione.
- Gli scambi di bitcoin si possono realizzare e ritenere

compiuti anche secondo modalità differenti rispetto a quanto normalmente previsto, ovvero attendendo un numero arbitrario di conferme sulla Blockchain (1, 3 o 6 blocchi). Si possono infatti rilassare o modificare i requisiti di "fiducia" in base alle circostanze in cui si effettua la transazione. Si possono per esempio accettare pagamenti a zero conferme da persone fidate (amici, parenti, clienti con KYC ecc.) che pagano fee basse. Se tali pagamenti non venissero mai inclusi in un blocco della blockchain, è possibile ottenere una conferma per un gruppo di transazioni tramite child-pays-for-parent

- I tempi di transazione sul layer base di Bitcoin possono sembrare elevati rispetto ad alternative di pagamento (ad esempio una transazione di carta di credito o paypal) perché si tratta in realtà di transazioni con settlement definitivo. Se si vuole transare istantaneamente con bitcoin, si può utilizzare Lightning Network o accettare zero conferme. Anche le transazioni con carta di credito non sono "confermate" istantaneamente e richiedono in realtà tempi di settlement molto più lunghi (anche settimane), motivo per cui vi sono così tante frodi. Paragonare dunque Bitcoin a Visa, Mastercard o simili è insensato.
- A parità di sicurezza sulla immutabilità delle transazioni (normalmente attribuita a transazioni con un minimo di 6 conferme), Bitcoin è più veloce di qualsiasi altra crittovaluta.

L'informatica quantistica romperà la crittografia usata nel protocollo Bitcoin

- L'informatica quantistica potrebbe non rompere mai l'attuale crittografia. Sebbene gli algoritmi quantistici possano in teoria rompere l'ECDSA, in pratica potrebbe essere impossibile ridurre il rumore di un computer quantistico per avere qubit sufficienti per

eseguire l’algoritmo.

- L’aggiunta di indirizzi resistenti al quantum computing a Bitcoin può essere ottenuta tramite un soft fork (un semplice upgrade al protocollo, come ce ne sono già stati vari nella storia di Bitcoin). Il lavoro sulla crittografia a prova di computer quantistici sta avanzando molto più velocemente degli stessi computer quantistici, poiché la matematica è molto più facile da eseguire per i ricercatori rispetto alla fisica sperimentale.
- Anche se ci sono progressi sorprendenti nei computer quantistici, questi non possono rompere la crittografia SHA256 che utilizza Bitcoin a protezione dei bitcoin negli indirizzi che non hanno rivelato la loro chiave pubblica. Se però viene ri-utilizzata una seconda volta la stessa chiave per un altro pagamento, potrebbe esserci una vulnerabilità ai computer quantistici. In quel caso, un soft fork può permettere la creazione di indirizzi resistenti al quantum computing consentendo ai proprietari di chiavi private di firmare transazioni senza rivelare la loro chiave pubblica. Ad oggi ci sono solo 4 milioni su 21 milioni di bitcoin in indirizzi potenzialmente “attaccabili” da un computer quantistico. I proprietari di questi bitcoin possono comunque in qualunque momento trasferire i loro averi su nuovi indirizzi “quantum resistance”.
- I primi computer quantistici saranno di proprietà di grandi aziende o governi. È improbabile che tali entità rivelino la supremazia quantistica attaccando prima Bitcoin rispetto ad utilizzarli per scopi decisamente più utili. Anche se rubassero dei bitcoin, è nell’interesse personale degli aggressori farlo lentamente e segretamente per il massimo profitto piuttosto che rischiare di far crollare il prezzo di bitcoin.

Un bug potrebbe consentire agli hacker di rubare bitcoin o interrompere la funzionalità della rete.

- Bitcoin è costantemente sotto attacco da un decennio, visto che la ricompensa per chiunque riesca a scoprire una falla critica sarebbe enorme, al limite dell'intera capitalizzazione di bitcoin.
- In passato (specialmente nei primi anni) diversi bug sono stati risolti in poche ore dagli sviluppatori Bitcoin (come quello del 2010 che ha permesso la creazione di 184 milioni di bitcoin o bug più recenti come quello del 2018) e di fatto ad oggi la rete Bitcoin è in UpTime con una percentuale del 99,98% del tempo.
- Fino ad oggi i bug hanno coinvolto una specifica versione di software del nodo e non tutti i nodi della rete. Il fatto che vi siano software full node diversi, ad esempio versioni di Bitcoin Core meno recenti dell'ultimo rilascio, o nodi sviluppati in altri linguaggi e mantenuti da team e contributori diversi, conferisce maggiore resilienza alla rete
- In casi estremi, Bitcoin può sempre eseguire un fork per correggere bug critici.

3. Un ecosistema Bitcoin decentralizzato non può durare!

Chi controlla o colpisce le mining pool più grandi ha il potere di censurare o interrompere tutte le transazioni

- I miners hanno ingenti investimenti in Bitcoin e nell'hardware che ha l'unico scopo di produrre Bitcoin (gli ASIC), quindi sono incentivati □□a mantenere l'integrità della rete.
- Le mining pool sono gruppi coordinati di miners che

aggregano la loro potenza di calcolo per avere maggiori chance di scoprire il blocco successivo. Gli amministratori delle pool potrebbero avere un potere decisionale sui blocchi creati, come la censura di transazioni o la segnalazione di upgrade del protocollo, ma gli utenti miner possono passare facilmente da una pool all'altra. I protocolli come Stratum V2 consentono ai miners nella pool di creare autonomamente i blocchi, impedendo all'amministratore della pool di gestire la potenza di calcolo a suo piacimento, ad esempio censurando transazioni o promuovendo fork del protocollo indesiderati al resto della rete

- Un goffissimo tentativo di censura delle transazioni si è avuto nel maggio 2021, quando la pool statunitense "Mara Pool" (gestita da Marathon Digital Holdings), ha creato un blocco "OFAC compliant", escludendo cioè tutte le transazioni provenienti da indirizzi segnalati in blacklist dal Dipartimento del Tesoro Americano. Poiché quelle transazioni sono state confermate da chi ha minato i blocchi immediatamente successivi, l'esito conseguito da Mara Pool è stato soltanto quello di aver perso le relative commissioni di transazione, lasciandole ad altri miners. Oltretutto, per farsi beffe di Mara Pool, qualche simpatico utente della community Bitcoin ha inviato dei bitcoin da un mixer (coinjoin) all'indirizzo in cui Mara Pool ha ricevuto i bitcoin generati dal blocco OFAC compliant, così da marcarlo come non compliant e finire esso stesso in blacklist. Infine, la community ha creato in meno di 24 ore dall'evento un sito che monitora il comportamento delle mining pool, per promuovere dei boycott di quelle che tentano di imporre la compliance di qualche governo.
- I miners sono troppo distribuiti per essere tutti attaccati, poiché ricercano le fonti energetiche a minor costo in tutto il mondo, spesso in aree remote. Ad Aprile 2021 un blackout nella regione dello Xinjiang ha causato un calo dell'hashrate nell'ordine del 20-25%:

circa l’80% dei miners cinesi sono stati interessati da questo blackout, un dato che ha permesso di stimare la quantità di hashrate presente sul territorio cinese: attorno al 32-40%. Sarebbe la prova che la Cina non detenga una potenza di calcolo in grado di tentare un 51% attack alla rete Bitcoin. Eventuali attacchi sarebbero un incentivo ad aumentare ancor di più la decentralizzazione.

- Assumendo per assurdo la possibilità, per un attaccante, di detenere la maggioranza dell’hashpower, la community Bitcoin potrebbe di concerto eseguire un fork upgrade del protocollo di Bitcoin, sfruttando un nuovo algoritmo di mining che gli ASIC utilizzati fino a quel momento non sono in grado di elaborare, rendendo di fatto inutile l’hardware utilizzato dall’aggressore. L’attacco quindi non solo non avrebbe successo, ma avrebbe comportato un impressionante esborso economico da parte dell’attaccante nel tentativo di ottenere la maggioranza di hashpower.
- Pe perpetrare tale attacco non è sufficiente “dirottare” ingenti quantità di energia che servono attualmente per tenere in piedi il sistema economico (industria, agricoltura, terziario) o attingere a nuovi fonti energetiche, ma anche impiegarla nel modo più efficiente per aumentare l’hashrate, cioè acquistando un enorme quantitativo di ASIC. La fattibilità pratica di un simile attacco e le sue chance di successo sono minime, a fronte di costi insostenibili.
- Anche in caso di “attacco 51%”, nessun bitcoin può essere rubato, quindi nessuno spenderebbe centinaia di miliardi di dollari semplicemente per censurare le transazioni bitcoin o tentare double-spending dei propri fondi.

Un pesante calo dei prezzi o il termine

dell’emissione di nuovi bitcoin nel 2140 potrebbero indurre i miners a spegnere le macchine, paralizzando la rete

- Il prezzo di bitcoin non dipende dall’hashrate, anche se l’hashrate è correlato al prezzo, in quanto all’aumentare del prezzo diventa più conveniente produrre Bitcoin, quindi nuova energie e nuove macchine vengono utilizzate a quello scopo, aumentando l’hashrate.
- Anche se il prezzo fosse un’invariante, l’hashrate tenderebbe al rialzo per via del progresso tecnologico: man mano che i chip di mining migliorano diventano più potenti ed efficienti e i minatori riescono a rifornirsi di energia più a buon mercato.
- Se l’hashrate diminuisse rallentando la catena, la frequenza media di 1 blocco ogni 10 minuti verrà ripristinata al cambio di difficoltà dopo 2016 blocchi. In casi estremi, un fork può riportare la difficoltà nello standard.

- Il mining non è sostenuto solo dall’emissione di nuovi bitcoin (coinbase transaction) ma anche dalle commissioni di transazione. Più il tempo passa, più queste costituiscono una quota percentuale maggiore rispetto al totale di bitcoin che i miners ottengono come remunerazione dalla creazione dei blocchi.
- Le ricompense per i miners, espresse in bitcoin diminuiscono ogni 4 anni (halving) fino al 2140 (33 cicli di halving), quindi in un intervallo di tempo ampio e con la gradualità necessaria a dare all’economia e all’ecosistema Bitcoin il tempo sufficiente per adattarsi in modo non traumatico ai cambiamenti degli incentivi per il mining, inclusa – nello scenario più pessimista – un’eventuale diminuzione dell’hashrate e dismissione delle macchine.

Bitcoin è troppo complesso per essere detenuto in sicurezza dalle persone comuni, quindi i servizi di custodia finiranno per centralizzare il sistema costituendo dei single point of failure

- La user experience dei numerosi wallet a disposizione sta migliorando giorno dopo giorno e, col crescere dell'adozione di Bitcoin, sempre più sviluppatori lavorano ai software. Allo stesso modo, Internet in passato era usato solamente da persone con buone abilità informatiche, mentre oggi è usato da quasi la totalità della popolazione mondiale.
- La maggior parte dei bitcoin ad oggi in circolazione è già tenuta in sicurezza dagli stessi utenti, con metodologie diverse in base alla loro preparazione (hardware wallet, paper wallet, software wallet, custodian ecc).
- La community Bitcoin è sostenuta da ideali forti di autonomia e decentralizzazione che vengono promossi con insistenza dagli utenti, incentivando i nuovi arrivati alle best practices per la detenzione in sicurezza dei bitcoin: "not your keys, not your coins".
- I servizi di custodia possono de-localizzarsi in più giurisdizioni, rendendo più difficile la confisca da parte di autorità o regolatori.
- Grazie alla natura digitale di Bitcoin, gli utenti possono utilizzare meccanismi per cui il servizio di custodia non avrà pieno possesso dei bitcoin in esso depositati, come i wallet multifirma

4. Bitcoin non può funzionare come riserva di valore!

La scarsità può essere modificata dagli sviluppatori a differenza di altre riserve di valore come l'oro

- Pur essendo possibile per chiunque operare un fork di Bitcoin, per introdurre un upgrade che modifichi l'offerta monetaria totale di Bitcoin deve esserci un accordo (esplicito o implicito, tramite meccaniche di mercato) tra i principali attori che gravitano attorno alla governance di Bitcoin, fra cui: miners, sviluppatori, principali servizi e compagnie, traders e comuni utenti.
- La modifica della total supply di bitcoin richiede un hard fork, creando due catene in cui gli utenti possiederanno bitcoin su entrambe (come già avvenuto con Bitcoin Cash). Il mercato quindi deciderà quale dei due Bitcoin sarà il Bitcoin originale: quello con supply aumentata o quello originale con supply a 21 milioni. Non ci sono incentivi per i principali attori nel mercato a scegliere un fork con supply aumentato, poiché comporterebbe soltanto una svalutazione dei loro risparmi.

Il prezzo di bitcoin è troppo alto, perciò gli investitori preferiranno crypto che costano meno

- La capitalizzazione di mercato di bitcoin è ancora molto piccola rispetto ad esempio all'oro. Se bitcoin viene percepito come "oro digitale" da una massa critica della popolazione, il suo valore è destinato ancora a crescere enormemente.
- È possibile acquistare una frazione di Bitcoin anziché 1 BTC intero: l'unità più piccola di onchain è il satoshi ovvero 0,00000001 bitcoin (1 centomilionesimo), mentre su Lightning Network si utilizza solitamente il

millisatoshi (0,001 satoshi). Un futuro softfork potrebbe aumentare i decimali onchain in caso di necessità, ovvero qualora il satoshi si apprezzasse al punto da non costituire una misura adeguata ai micro-pagamenti.

- Il protocollo Bitcoin prevede che l'offerta di btc emessi si dimezzi ogni 4 anni circa (halving). Dopo ogni dimezzamento il prezzo tende ad aumentare: infatti, assumendo una curva della domanda stabile, dato che la quantità di bitcoin prodotta diminuisce il prezzo necessariamente aumenta, per via della legge della domanda e dell'offerta.
- Man mano che bitcoin diventa più facile da usare e con maggiore liquidità nei mercati di scambio, nuovi utenti (privati ed istituzionali) possono usarlo come metodo di investimento alternativo. La curva di adozione di qualsiasi tecnologia utile all'umanità tende ad essere esponenziale.

Bitcoin può essere forkato all'infinito, il che ne diluisce il valore

- Un fork del codice di Bitcoin con creazione di una nuova altcoin partendo con un nuovo genesis block (vedi Litecoin o Aurora Coin), non inflaziona bitcoin
- Un fork operato da una parte della community (come Bitcoin Cash o Bitcoin SV) non diluisce il valore che un utente detiene in bitcoin perché si ottengono pari numero di bitcoin anche sulla catena forkata. L'utente a quel punto potrà decidere se conservare o vendere la nuova versione di bitcoin. Il prezzo – e di conseguenza l'hashrate – sulla blockchain che viene preferita dagli utenti tende a salire e in questo modo il mercato decreta qual è il "vero" bitcoin.
- I fork di Bitcoin sono una "feature", non un bug. I fork con "split" della catena in due valute diverse rappresentano un esperimento evolutivo in cui il mercato

sceglie quale sia il “bitcoin” migliore..

- Dopo tutti i fork di Bitcoin (105 al momento della stesura di questo articolo), il mercato gravita verso un unico protocollo come riserva di valore, ovvero il Bitcoin originale.

Bitcoin non ha valore intrinseco

- Nessun bene o servizio ha di per sé un “valore intrinseco”, il valore è sempre stabilito soggettivamente da chi utilizza quel determinato bene o servizio.
- Bitcoin ha le migliori “caratteristiche intrinseche” per essere qualificato come moneta: è facilmente trasferibile, verificabile, è fungibile, divisibile, non è deperibile e può essere messo in sicurezza facilmente, celato ad attaccanti o occhi indiscreti. Infine, è presente in quantità limitata (non arbitrariamente modificabile secondo logiche politiche), garantendo così che – a parità di domanda – non perda valore nel tempo.
- Bitcoin ha alle spalle un industria di mining che ha investito un valore pari a miliardi di dollari per funzionare e milioni di ore di sviluppo del protocollo Bitcoin.
- Un bene monetario non deve necessariamente avere un uso industriale per essere definito moneta. Ad esempio, per millenni l’oro, al di là dell’uso monetario, è stato usato soltanto per scopi decorativi, ornamentali ed estetici. Solo negli ultimi secoli ha visto un utilizzo di tipo industriale, ad esempio come conduttore. Ancora oggi, tale utilizzo è minimo rispetto al ruolo centrale di riserva di valore nella forma di lingotti o monete nei caveau di tutto il mondo. Ad ogni modo, anche Bitcoin ha un suo uso industriale: può essere utilizzato ad esempio per fare timestamp di informazioni sul database distribuito più sicuro del mondo. Questa funzionalità ha potenziali applicazioni in qualunque

settore di business e può agevolmente rimpiazzare i più comuni servizi di notarizzazione di tutto il pianeta.

Bitcoin è uno schema Ponzi

- Gli schemi Ponzi si basano su promesse di reddito che richiedono sempre più partecipanti per essere realizzate: una sorta di “codice amico” incentivato da guadagni personali. Bitcoin non è uno schema ponzi perché non esiste alcun meccanismo che arricchisca direttamente chi ha investito in precedenza nell’asset rispetto ai nuovi investitori, se non il naturale apprezzamento di mercato che l’asset ottiene quando aumenta la sua domanda rispetto all’offerta.

Bitcoin è una bolla come quella dei tulipani

- Storicamente, Bitcoin ha sempre raggiunto dei nuovi massimi dopo che ogni ”bolla” del prezzo è scoppiata. Le bolle possono verificarsi in tutte le attività, comprese le valute legali, le materie prime, gli immobili e le azioni. Il singolare grafico a “bolle” di Bitcoin è dovuto al meccanismo di halving, che provoca uno shock della supply (dimezzamento improvviso dell’offerta monetaria ogni 4 anni), e di conseguenza ad un nuovo processo naturale di aggiustamento del prezzo (discovery price). Tale aggiustamento vede forti ondate speculative, poiché gli attori presenti nel mercato hanno informazioni imperfette e non sempre si comportano in maniera razionale. Possiamo notare come un processo simile si verifichi nella discovery price fra oro e moneta fiat: l’elevata inflazione delle monete fiat rende il loro valore molto volatile nel corso dei decenni rispetto all’oro e a un paniere di beni tradizionali, portando alla formazione di bolle ripetute nel tempo (anche se più dilatate nel tempo).
- Ciò che rende bitcoin diverso dai tulipani sono le sue proprietà monetarie – divisibilità, scarsità,

fungibilità, portabilità, non deperibilità etc. – che lo rendono un buon veicolo di risparmio, più simile all'oro che ai tulipani.

Bitcoin non ha rendimento, non è un investimento, quindi non ha valore

- Il valore è deciso dalla domanda e dall'offerta di mercato, non dal rendimento. Se soltanto un asset che presenta dei rendimenti può essere considerato un asset di valore, allora beni di consumo comuni, metalli preziosi, l'arte o oggetti collezionabili e ornamentali non avrebbero alcun valore.
- Bitcoin è uno strumento che permette ai risparmiatori di conservare valore al riparo dall'inflazione. La continua svalutazione delle valute fiat modifica le "preferenze temporali" degli individui, incentivando i consumi immediati e disincentivando il risparmio, che è alla base dell'investimento e – quindi – della crescita economica. Il denaro arbitrariamente manipolato da un'istituzione politica tende a incentivare in modo perverso l'allocazione errata delle risorse economiche scarse. L'effetto di lungo periodo è un impoverimento della civiltà, in conseguenza di continui cicli di boom & bust, come brillantemente illustrato nella teoria austriaca dei cicli economici (es. vedi Moneta, Credito Bancario e Cicli Economici di Huerta De Soto, The Austrian Theory of the Trade Cycle and Other Essays di Richard Ebeling, Austrian Macroeconomics e Time and Money di Roger Garrison, Monetary Theory and the Trade Cycle e Price and Production di Friedrich Hayek, Economic Depressions: Their Cause and Cure di Murray Rothbard).

Bitcoin non può essere garantito, a differenza dei depositi bancari

- Esistono moltissimi servizi di custodia dei bitcoin

(anche in Italia) coperti da polizze assicurative private.
- Il fondo interbancario di tutela depositi (FITD) copre a malapena lo 0.022% dei fondi nei conti correnti italiani, quindi non si può nemmeno dire che i depositi bancari stessi siano davvero assicurati.

Il bitcoin è troppo volatile per essere riserva di valore o in un portafoglio di investimenti

- Per gli investitori con un lungo orizzonte temporale la volatilità non è un problema, il prezzo minimo di bitcoin tende a raddoppiare in media ogni anno.
- Diversi studi evidenziano come una piccola percentuale di bitcoin in un portafoglio di investimento diminuisca il rischio e la volatilità dello stesso, essendo bitcoin decorrelato rispetto agli altri strumenti finanziari.
- Usando strategie di investimento come il PAC (piano di accumulo capitale) la volatilità di bitcoin può essere mitigata.
- Man mano che i volumi e la capitalizzazione di mercato crescono, bitcoin diventa meno volatile poiché è necessario spostare molti più capitali per modificarne sensibilmente il prezzo.

Il prezzo di Bitcoin è manipolato dalla stablecoin Tether

- Tether è solo una delle tante possibilità che consentono agli utenti di acquistare bitcoin.Tether è nato per soddisfare i bisogni di un gran numero di exchange in tutto il mondo, avendo un dollaro digitale più facile da spostare senza dover necessariamente aspettare i lunghi tempi dettati dai protocolli bancari.
- Ad oggi non ci sono prove che dimostrino frodi da parte di Bitfinex nell’emissione di Tether, come attestato anche dal recente accordo extragiudiziale (febbraio 2021) fra Tether e la procura generale di NewYork.

Il valore di Bitcoin è dettato da un’illusione di massa

- I prezzi di qualsiasi bene o servizio esistente, sono la sintesi di un processo in cui gli attori di mercato (acquirenti e venditori) tramite la legge della domanda/offerta determinano il valore e di conseguenza il prezzo. Bitcoin non rompe alcuna legge universale della domanda e offerta.
- L’ecosistema Bitcoin è, oltre che puro codice digitale, anche una vera e propria rete fisica di computer e infrastrutture per un costo pari a miliardi di dollari e milioni di ore di contributi da parte di ingegneri, crittografi, matematici e pensatori di tutto il mondo.

Le valute digitali della banca centrale (CBDC) supereranno Bitcoin

- Bitcoin ha una supply scarsa, è incensurabile, inconfiscabile e può essere custodito e transato in completa autonomia senza alcuna licenza (anche prodotto, se si possiedono risorse sufficienti per qualificarsi come miner). Le “Central Bank Digital Currency” (CBCD) emesse dalle banche centrali non hanno nessuna di queste caratteristiche, non possono essere quindi paragonate a Bitcoin.
- Il passaggio alla valuta digitale della banca centrale non modifica le proprietà monetarie della valuta fiat, che viene regolata da logiche politiche del tutto arbitrarie. La “tokenizzazione” della moneta legale sarebbe soltanto un passo verso la sorveglianza centralizzata e l’eliminazione del contante per i cittadini.

5. Le nuove criptovalute supereranno Bitcoin!

Il codice di Bitcoin si può copiare e riprodurre in una versione migliore

- La rete Bitcoin è messa in sicurezza da molti milioni di TeraHash, corrispondenti a una quantità di energia enorme, che rende Bitcoin la cryptovaluta più sicura. I volumi di scambio e lo sviluppo dell'ecosistema danno a Bitcoin un vantaggio comparato in termini di effetto network e lo sviluppo attrae i migliori tecnici. Ad oggi, la blockchain Bitcoin è l'unica ad aver sviluppato una rete di smart contract (lightning network) effettivamente funzionante che permette pagamenti offchain, superando così anche i limiti di scalabilità intrinseci alla tecnologia blockchain.
- Per effetto network, il mercato tende a convergere naturalmente verso lo standard più utilizzato, scegliendo spontaneamente come schelling point la soluzione più ovvia. Di conseguenza, intorno a tale soluzione si raccolgono i migliori sviluppatori e fiorisce un ecosistema che risulta vincolato al protocollo sottostante. Questo meccanismo costituisce interessi sempre più consolidati al mantenimento di quella architettura di base, che comunque viene aggiornata per rimanere al passo con l'evoluzione tecnologica.

La tecnologia di Bitcoin è obsoleta

- La narrativa di chi sponsorizza le altcoin si focalizza attorno al concetto di come quella specifica coin svolga un compito migliore rispetto ad un'altra (la altcoin X è

più veloce della Y, la Y ha maggiore privacy rispetto alla Z ecc). Tuttavia, queste presunte “migliorie” vanno inevitabilmente a sacrificare uno dei tre punti cardine del “trilemma della blockchain”, ovvero: scalabilità, sicurezza e decentralizzazione. Solo in Bitcoin queste tre caratteristiche sono ben bilanciate e gli attori che giocano un ruolo chiave nella governance della blockchain sono incentivati economicamente (teoria dei giochi) a garantire che questo sistema rimanga in equilibrio, incensurabile e inattaccabile.

- Molte delle cryptovalute alternative a Bitcoin sono nate come copie di Bitcoin che implementano tecnologie apparentemente “nuove”, che in realtà sono soltanto scarti di lavorazione degli sviluppatori Bitcoin. Quando una nuova tecnologia veramente valida è implementata nell’ecosistema crypto e testata a sufficienza a garanzia di sicurezza, il protocollo Bitcoin viene aggiornato. Ad oggi sono stati effettuati 18 consensus fork per aggiornare Bitcoin, l’ultimo nell’agosto 2017. Il prossimo upgrade è già pronto nella più recente versione di Bitcoin Core (con Schnorr, MAST e Taproot), in attesa di attivazione da parte della community.

Il mondo degli smart contracts e finanza decentralizzata è alternativo a Bitcoin e più attrattivo per gli investitori

- La maggior parte delle cryptovalute non è utilizzata come riserva di valore o mezzo di pagamento, ma ha un fine puramente intrattenitivo in quanto rappresenta una mera scommessa su cui puntare, come in un gioco d’azzardo, dove generalmente risulta vincente (nel breve periodo) il token che ha un team di marketing più efficace alle spalle. Ether è il principale veicolo del trading speculativo, fungendo da gas per le transazioni di arbitraggio fra smart contract che permettono di speculare sui prezzi di queste cryptovalute. Un mercato

di questo tipo può durare e attrarre speculatori, ma non ha la stessa carica rivoluzionaria di un asset che, ponendosi come alternativa alle monete fiat tradizionali, da oltre 10 anni taglia un traguardo dopo l'altro.

- Bitcoin è progettato per essere oro digitale, ed il suo protocollo è studiato per garantire la massima sicurezza. Supportare la programmazione generica come avviene su altre cryptovalute turing complete apre possibili problemi di sicurezza, come avviene su altcoin come Ethereum. Inoltre, i second layer costruiti su Bitcoin, ed alcuni dei miglioramenti allo stesso protocollo di base, possono fornire strumenti utili alla "programmabilità", pensiamo ad esempio a progetti come RGB, Liquid, Mintlayer o future implementazioni al protocollo come Taproot.

> Come shilla De Luigi neanche Big Luca international! Occhio alla public sale a breve!

- La maggior parte delle altre valute ha perso un valore significativo rispetto a Bitcoin nel tempo. Generalmente dopo uno "spike" iniziale, tutte le altcoin tendono a perdere terreno rispetto alla crescita del prezzo di Bitcoin, come si evince dal grafico:

La Proof-of-Stake è il futuro

- Moltre cryptovalute sbandierano il sistema Proof-of-Stake come innovativo e sostitutivo della "vecchia" Proof-of-Work di Bitcoin. Tuttavia, non esiste ad oggi un modello PoS comprovatamente sicuro. Infatti, il principale problema dei PoS è che se nel passato

qualcuno ha avuto una quantità maggioritaria di coin in stake, può usarli per attaccare la rete in un qualunque momento nel futuro, anche dopo essersene sbarazzato. Se ad esempio al blocco 0 di una certa cryptovaluta il suo creatore avesse il 100% dello stake, potrebbe riscrivere (tecnicamente "riorganizzare") l'intera blockchain anche fra molti anni, pur avendo preventivamente venduto tutti i propri token. Questo significa avere il totale controllo sulla blockchain e nessun rischio finanziario associato all'attacco.
I checkpoint, ovvero un meccanismo che previene tale "riorganizzazione" nei PoS, è deciso arbitrariamente da un ente centrale, oppure delegato ai singoli nodi. Questo però porta con sé ulteriori problemi:

1. un nodo di nuova installazione non è in grado di determinare i checkpoint, deve fidarsi dei nodi a cui si collega (potenzialmente malevoli),
2. se il checkpoint è troppo indietro nel tempo i tempi di conferma per essere certi di un pagamento si allungano perché di fatto il checkpoint è l'unica cosa che tiene in sicurezza la rete PoS
3. se il checkpoint è troppo vicino c'è una certa probabilità che si generino biforcazioni e quindi "nascano" blockchain parallele con storie diverse, rendendo più aleatorie le conferme di transazione
4. Qualora vi fosse un fork della catena perché alcuni nodi sono isolati, in caso di PoW i nodi si ri-organizzeranno automaticamente non appena scoperta la catena con maggiore hashrate (ad esempio, quando si ristabilisce la connessione fra due aree geografiche), mentre in caso di PoS può esserci uno split permanente. Infatti in genere i protocolli PoS (es. Casper) rendono impossibile recuperare una catena alternativa il cui fork è avvenuto troppo tempo addietro, anche se è in realtà quella valida

5. Nella PoW chi detiene la maggioranza dell'hashpower può tentare un attacco di double spending o censurare delle transazioni, ma non può riscrivere la blockchain se non con costi enormi ed esponenziali. Nella PoS invece, chi detiene la quota di maggioranza ha un potere illimitato. Oltre al "double spending" e alla censura delle tx senza è possibile anche:
   – riscrivere la cronologia, se il protocollo non ha checkpoint
   – causare divisioni di catena inconciliabili, se il protocollo ha checkpoint.

6. I bitcoiner sono una setta di idioti e criminali!

La blockchain è la vera rivoluzione, non Bitcoin

- La blockchain è un database incrementale ridondante e distribuito, database di questo tipo si studiano dall'inizio degli anni '70, con l'arrivo delle prime reti di computer (Arpanet). Nel 1991 il matematico Stuart Haber e il fisico Scott Stornetta crearono un primo prototipo di blockchain usando la sezione oggetti smarriti del New York Times (come fonte esterna "affidabile") per fare timestamping dell'hash del database di "Absolute Proof". Nel 2008, con il white paper "Bitcoin: A Peer-to-Peer Electronic Cash System", Satoshi Nakamoto prese spunto dall'idea di Haber e Stornetta (un db incrementale crittografato con funzioni di hash) unendola al concetto di rete distribuita peer-to-peer, attingendo sapientemente da idee e tecnologie

già esistenti come: crittografia asimmetrica (1977), HashCash di Adam Back (1997), B-Money di Wei Dai (1998), Bit Gold di Nick Szabo (1998), Reusable Proof of Work di Hal Finney (2004). Nakamoto risolse così un problema di consenso insito nei sistemi distribuiti, noto come il problema dei generali Bizantini, realizzando per la prima volta un sistema che converge al consenso senza richiedere fiducia fra i suoi partecipanti (trustless). L'intero meccanismo funziona solo grazie a un token sottostante (Bitcoin) che ricompensa gli attori coinvolti nella messa in sicurezza della blockchain stessa.

- La blockchain può essere usata per fare un timestamping di qualsiasi cosa possa essere digitalizzata (documenti, brevetti, attestati, etichette ecc), tuttavia non può (e non potrà mai) garantire la veridicità delle informazioni provenienti dall'esterno ed inserite in essa. Usare la blockchain per applicazioni come il tracciamento della filiera produttiva, il voto elettronico, il catasto o il pubblico registro automobilistico necessita di un ente terzo certificatore che garantisca la validità dei documenti inseriti essa. In questo caso viene meno la caratteristica principale della blockchain, ovvero essere un sistema trustless.

Bitcoin permette di evadere le tasse

- La maggior parte dei Paesi tratta bitcoin e le plusvalenze generate su Bitcoin proprio come qualsiasi altra attività finanziaria, quindi chi intendesse pagare le tasse può continuare a farlo anche con Bitcoin.
- Pagare le tasse può non essere stupido, nella misura in cui facendolo ci si protegge dall'aggressione di una forza a cui difficilmente si riesce a far fronte. Tuttavia, condannare una tecnologia solo perché offre una scappatoia in più a chi intende liberarsi dalla violenza statale, è completamente insensato. Le imposte

costituiscono un meccanismo involutivo e parassitario della presente civiltà e i falsi miti alla giustificazione della tassazione sono frutto di ideologie perverse come il collettivismo di matrice fascista, socialista, nazionalista, statalista, europeista etc.

I terroristi, criminali e narcotrafficanti usano Bitcoin

- La stragrande maggioranza dei bitcoin viene utilizzata da persone comuni che vogliono salvaguardare i propri risparmi o speculare.
- I terroristi usano le automobili per le autobombe, gli aerei per abbattere grattacieli, telefoni cellulari e internet per organizzare attentati, denaro contante per finanziarsi nell'ombra, banche compiacenti per riciclare denaro. Non per questo tali strumenti sono vietati. Bitcoin non è un'arma speciale che rende impossibile fermare i terroristi.
- Secondo un recente report gli utilizzi "illegali" di bitcoin sono in netto calo, ed analizzando i dati si nota come la percentuale più cospicua venga guidata da truffe, schemi ponzi, ransomware e acquisti sul darknet. L'uso di bitcoin per finanziare il terrorismo o pedopornografia è praticamente inesistente. Spesso poi, il concetto di "illegale" non coincide con quello di "morale". Un attivista per la libertà in Iran o a Hong Kong può essere considerato illegale e Bitcoin costituirebbe un'ancora di salvezza. Lo strumento è neutro, il male o il bene dipendono dall'uso che se ne fa.

Le valute legali hanno successo perché sono imposte con l'uso della forza (militarmente) e sono l'unico modo per pagare le tasse, invece

Bitcoin non è supportato da nulla

- Molti Paesi hanno sperimentato iperinflazione o grandi svalutazioni delle loro valute nonostante ognuno di loro avesse a disposizione “armi e tasse”.
- L’oro e le pietre preziose hanno avuto valore per migliaia di anni nonostante non fossero supportati da alcun ente pubblico. L’oro è la riserva di valore della maggior parte delle banche centrali e Bitcoin può svolgere una funzione simile.
- Bitcoin è supportato dalle sue proprietà monetarie imposte da un protocollo tenuto in piedi da una massiccia rete p2p a governance decentralizzata.
- Gli stati possono aumentare la domanda di una valuta sotto forma di pagamenti di tributi e tasse, ma il commercio e la politica monetaria sono fattori più importanti nel determinare il valore della valuta.

Bitcoin non ha reali casi d’uso in cui può essere superiore alle valute tradizionali

- Bitcoin è una rete di pagamenti digitale che non ha barriere d’ingresso, tutti possono usare Bitcoin senza dover chiedere il permesso a nessuno. Si stima che circa un quinto della popolazione mondiale sia “unbanked” e Bitcoin potrebbe consentire a chi non ha accesso alla finanza tradizionale di ricevere e inviare pagamenti digitalmente con costi prossimi allo zero (usando il layer 2 di bitcoin, Lightning Network).
- Le valute tradizionali per poter essere utilizzate in forma digitale necessitano di una parte terza fiduciaria che può essere corrotta o forzata a censurare alcuni tipi di transazione. Storicamente vi sono vari esempi di censura e restrizioni che sono state scavalcate tramite l’adozione di Bitcoin per ricevere pagamenti: Wikileaks, l’oppositore di Putin in Russia Navalny, i gruppi di protesta in Nigeria contro la SARS (Special Anti-Robbery

Squad), i dissidenti in Cina, Bielorussia, Myanmar.

- Gli intermediari finanziari possono decidere di bloccare le transazioni anche senza un obbligo da parte di un'istituzione o un'autorità giudiziaria, ne è un esempio il caso di PornHub a cui è stata preclusa la possibilità di ricevere pagamenti dai due maggiori circuiti di pagamento (VISA e Mastercard). Pornhub ha di conseguenza deciso di accettare cryptovalute.
- Nessuno può prelevare, bloccare, congelare o razionare i risparmi in Bitcoin: in Grecia, in occasione della crisi di liquidità, nel 2015 i privati cittadini potevano ritirare al massimo 60€ al giorno presso i bancomat, mentre a Cipro nel 2013 il limite fu imposto a 100€ al giorno, in accoppiata con un prelievo forzoso (bail-out) sui conti correnti, che avvenne anche in Italia nel 1992, sotto il governo Amato (prelievo del 6 per mille su ogni conto corrente e ogni deposito, anche dai conti intestati ai minori).

La distribuzione di Bitcoin nella popolazione è socialmente iniqua e la rendita derivata dal suo apprezzamento premia i possessori in modo immeritato

- Bitcoin è un bene monetario distribuito in tutto il mondo in modo non violento, ovvero quasi esclusivamente tramite contratti volontari di acquisto e vendita. Al contrario, l'attuale redistribuzione della ricchezza nel mondo misurabile in terra, oro, pietre preziose e moneta fiat è in larga parte legata ad atti di violenza nella misura in cui individui o popolazioni sono stati soggiogati, uccisi e schiavizzati.
- Recenti studi dimostrano come la concentrazione di ricchezza in bitcoin non sia affatto elevata rispetto agli asset finanziari tradizionali (video ita)
- Chi per primo investe tempo o denaro in un'attività finanziaria o imprenditoriale si accolla il rischio

morale e materiale di credere ed investire in quel progetto. Se l'idea ha successo, questi individui godranno meritatamente dei frutti delle loro decisioni. Il profitto è infatti il mezzo mediante cui una civiltà riconosce i meriti a coloro che più contribuiscono all'evoluzione e al progresso.

- Bitcoin non distribuisce dividendi o interessi, quindi nel tempo i grandi possessori di Bitcoin che non forniscono nessun bene o servizio agli altri, saranno costretti a spendere i propri bitcoin per vivere.

Una moneta deflazionistica rallenta l'economia, per cui l'adozione di Bitcoin è deleteria

- Il 1800 è stato un secolo di continua deflazione per gli USA, dovuta principalmente alle continue innovazioni in ambito industriale, che hanno permesso una enorme efficientamento della produzione. Gli unici anni inflattivi furono i periodi di guerra (Anglo-americana del 1812–1815 e Civile 1861–1865). Nella seconda metà dell'800 gli USA quintuplicarono il loro PIL e diventarono la prima potenza mondiale superando la Gran Bretagna.
- Esistono tutt'oggi mercati deflattivi e di grande successo, pensiamo ad esempio al mercato tecnologico, caratterizzato da continue innovazioni e nuovi modelli (hardware, smartphone, accessori) che subiscono una forte svalutazione dei prezzi (deflazione) anche solo pochi mesi dopo il lancio. Nonostante i prodotti si svalutino in breve tempo (anche pesantemente), la domanda e il consumo non ne risentono negativamente.
- Le crisi e i cicli economici sono causati da un'errata allocazione delle risorse economiche scarse (lavoro, beni capitali, materie prime ecc) causate da un sistema bancario centralizzato e dalle distorsioni introdotte da regolatori e autorità, fra cui le politiche monetarie inflattive, che incentivano l'indebitamento. Oggi

l’economia mondiale ha sviluppato una totale dipendenza dalle Banche Centrali attraverso le politiche di tassi a zero e il Quantitative Easing, senza il quale imploderebbe su se stessa.

- L’inflazione mitiga il rischio di default da debito, poiché diminuisce il valore reale del debito, essendo questo nominato in moneta fiat. Questo fatto garantisce agli Stati la possibilità di continuare a sottrarre potere d’acquisto alla popolazione creando altro debito, che permette alla classe parassitica (chi non lavora o dipende dal Pubblico) di vivere alle spalle di chi produce. Le fasce produttive (soprattutto coloro che non hanno investito almeno una parte dei loro risparmi in riserve di valore) di fatto si ritrovano in tasca una moneta che vale sempre meno con il passare degli anni.

Bitcoin non è adottato dai commercianti e ha fallito come moneta

- Storicamente ogni tipo di hard money come Bitcoin usato nella storia (perline, sale, conchiglie, oro e in generale qualsiasi “moneta di scambio” la cui offerta non è arbitrariamente modificabile da un’entità centrale, ad esempio tramite le politiche moentarie), prima di diventare moneta passa attraverso le 4 fasi dell’evoluzione del denaro, nell’ordine: 1) bene collezionabile, 2) riserva di valore, 3) mezzo di scambio, 4) unità di conto. Si tratta di un processo lungo che richiede un adattamento della società nei comportamenti abitudinari degli individui che la compongono.
- Le persone preferiscono (a parità di prezzo del bene/servizio che si vuole acquistare) spendere easy money (valute fiat), visto che tende a svalutarsi nel tempo, piuttosto che spendere hard money. Per questo motivo nei commerci è utilizzato principalmente l’euro o il dollaro piuttosto che Bitcoin. Questo fatto però non

va a discapito di Bitcoin, bensì lo qualifica come la “moneta buona” che è scacciata (dalle piazze di scambio) dalla “moneta cattiva” (per la nota legge di Gresham). Chi ad esempio ha Bitcoin ed Euro, preferisce tenersi in tasca i primi e spendere i secondi.

- I commercianti saranno via via più spinti all’adozione e promozione di Bitcoin una volta che non vorranno più accettare le loro valute locali (legge di Thiers) come è successo con il Venezuela e il dollaro USA .
- Sempre più commercianti stanno accettando Bitcoin, in particolare perché i nuovi metodi di pagamento come Lightning e Strike hanno reso più facile riceverli e spenderli. Questa tendenza continuerà ad aumentare man mano che la conoscenza dello strumento e la user experience miglioreranno, proprio come avvenuto con qualsiasi altra tecnologia. Analogamente, alla metà degli anni 90 solo alcuni pionieri utilizzavano Internet, ma con il migliorare della user experience (sistemi operativi con GUI ed intuitivi) e la maggior alfabetizzazione informatica, l’adozione di internet negli ultimi venti anni è diventata esponenziale, fino a raggiungere la quasi totalità della popolazione mondiale.

Bitcoin è un culto, le persone che ci credono sono ideologi e massimalisti

- Tutti gli sforzi umani su larga scala, comprese le società e i governi, hanno contributi ideologici.
- I sostenitori di Bitcoin coprono un’ampia gamma di attivisti per i diritti umani, economisti austriaci, crittografi, cripto-anarchici, tecnologi, futuristi e trader alla ricerca della pura speculazione: se è una religione, non si tratta certo di una religione dogmatica.

Bitcoin usa troppa energia, fa male all’ambiente

- L’energia consumata dalla rete Bitcoin serve anche a mettere in sicurezza la stessa, visto che un attaccante che volesse provare a distruggere Bitcoin dovrebbe usare (quindi acquistare o produrre) una quantità superiore di energia rispetto a quella utilizzata dalla rete Bitcoin.
- L’energia sprecata da tutti i dispositivi elettrici in standby (quindi inutilizzati) nei soli Stati Uniti d’America, potrebbe alimentare la rete Bitcoin per 2 anni. Televisori, i giochi per computer, i server su cui poggia il sistema bancario, post e tweet inutili, i video di tik-tok, gli aerei, le luci di natale, la plastica, ecc. Richiedono energia per essere prodotti ed utilizzati. Qual è la quantità di energia considerata “troppa” per produrli? Bitcoin, in quanto “hard money” digitale che si pone come alternativa alle distorsioni degli attuali regimi monetari, non costituisce forse un obiettivo sufficientemente nobile per consumare energia?
- Un miner per essere competitivo e sopravvivere nel mercato è costretto a rifornirsi di energia al più basso costo possibile e l’energia a costi più convenienti è tipicamente quella prodotta in eccesso, che altrimenti non verrebbe sfruttata e letteralmente sprecata. Ogni spreco energetico può essere visto come un’opportunità di profitto per il miner. Prima del ban cinese, molti minatori si concentravano presso le grosse centrali idroelettriche (come nella regione di Yunnan in Cina) dove i livelli di surplus di produzione sono enormi e possono così spuntare prezzi dell’energia molto bassi. Basti pensare che nel 2017 a fronte di 250twh prodotti dalle dighe ne sono stati utilizzati 155twh (95twh sono stati sprecati, per via dei costi eccessivi e anti-economici di stoccaggio).
- Recenti studi evidenziano come il mining di bitcoin sia alimentato – con una certa variabilità stagionale – da un’elevatissima percentuale di energia prodotta da fonti

rinnovabili (solare, idroelettrico, eolico, geotermico) ed, in minima parte, da energia prodotta utilizzando combustibili fossili.

- Bitcoin può aiutare l'efficientamento dell'industria energetica, ad esempio a prevenire il "Renewable Curtailment" (come avviene nelle mining farm Texane) oltre a rendere redditizia la cattura del gas flaring, incentivando così i produttori a ridurre le emissioni di carbonio. I progetti energetici a basse emissioni di carbonio come l'idroelettrico, il nucleare o le rinnovabili possono essere resi redditizi vendendo l'energia prodotta in eccesso a chi la utilizzi per l'estrazione di Bitcoin.
- A fine anni 90 i mass media si scagliavano contro internet e il mondo dei pc per l'elevato consumo energetico, ora è il turno di Bitcoin. Per quanto la risonanza mediatica di queste tematiche impressioni le masse, raramente le teorie di giornalisti e dei più popolari opinion leaders rispecchia un metodo scientifico ed oggettivo nell'approciare l'argomento.
- L'estrazione dell'oro è estremamente energivora ed ecologicamente meno sostenibile rispetto al mining di bitcoin. A titolo esemplificativo, si tenga conto che la miniera d'oro canadese di Yellowknife, chiusa nel 2004, contiene oltre 230.000 tonnellate di polvere di triossido di arsenico derivante dai processi chimici utilizzati per separare l'oro dalle rocce. Sono sufficienti 120mg di arsenico perché sia fatale all'essere umano, perciò il trattamento di questi rifiuti altamente tossici – letali se inflitrassero le falde acquifere! – è estremamente costoso. Una soluzione potrebbe essere il congelamento, che nel caso specifico di Yellowknife richiederebbe un esborso di 900 milioni di dollari (e 2 milioni di dollari all'anno) per il mantenimento del sistema di raffreddamento.

Link utili per approfondimenti

- 7 idee sbagliate su Bitcoin
- Gradualmente, poi all’improvviso
- Bitcoin is Venice
- Glossario Bitcoin