FALSITÀ SU BITCOIN

@anilsaidso

Questa argomentazione è stata confutata!

Traduzione a cura di @loop_btc

"Bitcoin rappresenta una rottura radicale con il passato, quindi la comprensione del sistema monetario tradizionale non aiuta a capire Bitcoin. Semmai ne ostacola la comprensione.

Le persone che capiscono meno Bitcoin sono gli esperti di economia monetaria. Non riescono a capacitarsene."

—Andreas M. Antonopoulos

"dovrebbe essere messo al bando."

—Joseph Stiglitz

"La volatilità di Bitcoin lo rende poco attraente per la maggior parte delle aziende che lo detengono come riserva di liquidità."

—Steve Hanke

"Bitcoin è arrivato a 1.000 miliardi di dollari di capitalizzazione di mercato: un rendimento che ricorda quello da falsificazione del denaro."

—Jeffrey Sachs

@anilsaidso

3 SECCHIATE DI CRITICHE

SPECULATIVO/INIQUO

- BOLLA
- TROPPO VOLATILE
- SENZA SOTTOSTANTE
- ACCAPARRAMENTO
- POSSESSO CONCENTRATO

DISPENDIOSO/INUTILE

- OBSOLETO
- ENERGIVORO
- TRANSAZIONI LENTE
- COMMISSIONI COSTOSE
- INTERNET-DIPENDENTE

PERICOLOSO/TRUFFA

- UTILIZZO CRIMINALE
- PONZI/SCHEMA PIRAMIDALE
- DIVIETO DEL GOVERNO
- BUG DELL'INFLAZIONE
- DUPLICABILE

È UNA BOLLA

Bitcoin è stato ripetutamente definito come una bolla, da molte persone e per molti anni. Sebbene il prezzo di bitcoin abbia subìto svariati pesanti ribassi che potrebbero giustificare tale etichetta, l'andamento complessivo è stato in spettacolare crescita.

I critici che proclamano la *morte* di Bitcoin dopo ogni ciclo di mercato stanno fortunatamente esaurendo le analogie e si stanno rivelando per quello che sono: **dei falsi**.

@anilsaidso

La volatilità è soggettiva. Aspettarsi che il prezzo di bitcoin si mantenga all'interno di un intervallo predefinito non ha alcun fondamento.

Bitcoin viene scambiato 24 ore su 24, 7 giorni su 7, 365 giorni all'anno in quasi tutti i Paesi del mondo. Non ci sono obblighi di registrazione, festività, interruzioni o salvataggi bancari. È un mercato veramente libero. Qualsiasi volatilità è il frutto dell'accordo tra acquirenti e venditori in tempo reale, senza l'intervento governativo.

Bitcoin si avvia a diventare la principale riserva di valore globale dell'era dell'informazione. Partendo da zero, l'idea che una tale traiettoria possa avvenire linearmente è assurda.

Con l'aumento dell'adozione, bitcoin diventa sempre meno rischioso, il potenziale rialzo diminuisce e si riduce la volatilità.

@anilsaidso

SENZA SOTTOSTANTE

Il concetto di *denaro garantito* è un ossimoro, dal momento che, in tal caso, sarebbe il *sottostante* ad essere considerato come il *vero denaro*.

Il denaro deriva parte del suo valore dalla scarsità. Bitcoin non richiede un altro bene scarso come sottostante perché già di per sé è assolutamente scarso. Bitcoin è completamente privo di rischio di controparte in quanto verificabile e controllabile in modo indipendente. Non c'è bisogno di fidarsi di una terza parte per immagazzinare e mettere al sicuro una certa quantità di merci o beni. Semmai, in futuro sarà probabilmente Bitcoin a fare da sottostante.

"In fondo, Bitcoin è garantito da qualcosa, ed è l'unica cosa che sostiene qualsiasi tipo di denaro: la veridicità delle sue ***proprietà monetarie****."*
—Parker Lewis

DIVENTERÀ OBSOLETO

Bitcoin rappresenta la più singolare scoperta dell'assoluta scarsità. Si tratta di un evento irripetibile, come la scoperta del fuoco, dell'elettricità o della matematica. Competere con Bitcoin in questa dimensione è illogico e impossibile. Non esiste un livello di scarsità superiore a quello della scarsità *assoluta*.

Le critiche ai limiti o agli svantaggi attualmente percepiti in Bitcoin partono dal pregiudizio che non esistano compromessi tra la sicurezza e il meccanismo degli incentivi e non tengono conto degli immensi benefici che la struttura attuale di Bitcoin fornisce già a milioni di partecipanti.

In quanto rete *permissionless* in crescita esponenziale con un funzionamento continuo del 99,98% per oltre un decennio, che transa trilioni di dollari di valore e che è protetta da miliardi di dollari di hardware, pensare di sostituire Bitcoin come rete monetaria digitale dominante è, a questo punto, improbabile.

"Non c'è mai stato un esempio di un'enorme rete digitale da 100 miliardi di dollari che sia stata sconfitta, una volta raggiunta la posizione dominante."
—Michael Saylor

ECCESSIVO CONSUMO DI ENERGIA

Bitcoin è una moneta sonante accessibile a livello globale e resistente alla censura grazie al meccanismo di *Proof of Work* (prova di lavoro).

Si stima che quattro miliardi di persone attualmente vivano sotto una qualche forma di autoritarismo. Bitcoin offre a tutti la libertà di inviare, ricevere, salvare e trasportare ricchezza.
Provate a chiedervi: qual'è la giusta quantità di energia che una rete monetaria di questo tipo dovrebbe consumare? E soprattutto, perché proprio voi dovreste essere nella posizione migliore per giudicare questo aspetto?

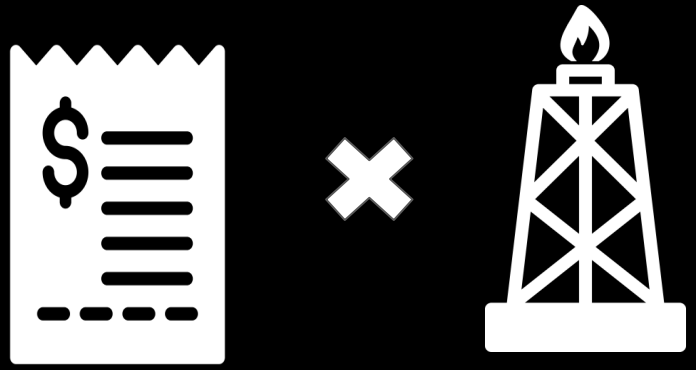
"Immaginate una mappa topografica del mondo, ma con i costi dell'elettricità locale come variabile che determina i picchi e le depressioni. Introdurre Bitcoin in questo scenario equivale a versare un bicchiere d'acqua su una mappa tridimensionale: si deposita nelle depressioni, appianandole. Bitcoin è un acquirente globale di energia a prezzo fisso".

—Nic Carter

CASO D'USO

MONETIZZAZIONE DI ENERGIA INUTILIZZATA

Il mining di bitcoin offre una soluzione altamente portatile per le risorse energetiche situate in regioni dove non esiste una domanda locale né la convenienza di generarle per trasportarle altrove. Attraverso l'uso in loco di apparecchiature per la generazione di *hash* è possibile minare bitcoin, che potranno essere conservati nell'ottica di un loro futuro apprezzamento o venduti in un mercato libero altamente liquido e accessibile a livello globale.



"Portare il mercato al livello della molecola è molto potente".
—Marty Bent

INTERNET-DIPENDENTE

Il rischio di perdere l'accesso a Internet a causa di malfunzionamenti delle infrastrutture, disastri naturali o interruzioni intenzionali è una preoccupazione legittima. Fortunatamente esistono diversi metodi per effettuare transazioni bitcoin offline e tramite altre reti di telecomunicazione.

Nel caso dell'invio di bitcoin *on-chain*, una transazione firmata deve raggiungere un solo nodo per essere trasmessa alla rete e inclusa dai minatori in un futuro blocco. Alcuni dei diversi metodi che si possono utilizzare per ottenere questo risultato sono, ad esempio, la trasmissione tramite SMS delle transazioni ad un dispositivo connesso a Internet, il passaggio di wallet fisici contenenti una chiave privata monouso a prova di manomissione o persino la ricezione degli ultimi blocchi via satellite.

@anilsaidso

TRANSARE BITCOIN OFFLINE

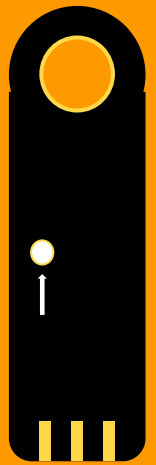
SATELLITE (BLOCKSTREAM)

RADIO A ONDE CORTE

SMS

RETI MESH

STRUMENTI FISICI AL PORTATORE

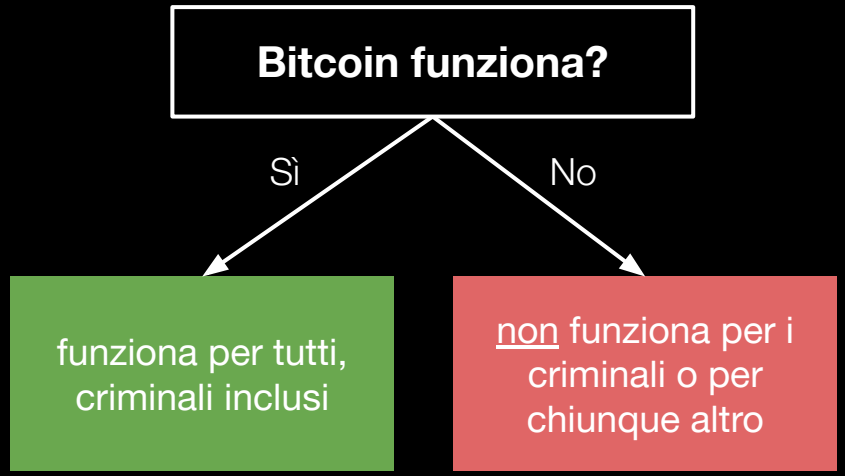


Traduzione a cura di @loop_btc

FACILITA IL CRIMINE

Bitcoin è uno strumento neutrale per trasmettere valore. Non ha alcun credo, opinione o significato intrinseco. Le persone danno un significato a Bitcoin attraverso l'uso che ne fanno.

L'argomentazione secondo cui le proprietà di Bitcoin hanno portato ad un aumento dell'attività criminale nel suo complesso non regge di fronte ad un'analisi approfondita. La criminalità non deriva dall'accesso ad alcuni strumenti, ma piuttosto dalle circostanze individuali.



fonte: Bitcoin Is Not For Criminals (2019)

"Non c'è nulla di intrinseco negli strumenti utilizzati per facilitare i crimini che li renda di per sé criminali. Nonostante abbiano un uso criminale, nessuno chiede la messa al bando delle strade, di Internet, della posta, ecc."

—Parker Lewis

@anilsaidso

Traduzione a cura di @loop_btc

SCHEMA PONZI

Affermare che Bitcoin è uno schema Ponzi significa non conoscere tanto Bitcoin quanto la definizione di schema Ponzi. Un elemento chiave di un ponzi richiede che ci sia una qualche promessa di **guadagni superiori al mercato** per gli investitori.

Essendo una rete *permissionless* (NdT: aperta a tutti, senza bisogno di autorizzazioni), Bitcoin non ha un'autorità centrale in grado di fare promesse di questo tipo. Essenzialmente, Bitcoin non è uno schema di investimento, ma è a tutti gli effetti denaro. Inoltre, a differenza delle opportunità di investimento opache promosse ad un individuo inconsapevole, il codice di Bitcoin è *open-source* e la sua *supply* (offerta) è verificabile in modo indipendente in qualsiasi momento.

L E N T O

Concludere una transazione di bitcoin sulla catena principale non è come usare la carta di credito per pagare un panino. Anche in questo caso, sebbene il pagamento possa sembrare istantaneo, in realtà passa attraverso diverse controparti ed il deposito sul conto bancario del commerciante avviene solo dopo diversi giorni di lavorazione. Con Bitcoin, non state inviando un “pagherò”. Si sta inviando denaro forte **direttamente** al destinatario, senza intermediari, senza rischi di censura e con la garanzia di un regolare esito finale una volta che la transazione è stata confermata. Sei blocchi non sembrano poi un tempo così lungo.

"Il confronto corretto sarebbe tra Bitcoin e la Fed come emittente di valuta e come meccanismo per lo scambio delle informazioni di pagamento."
—Parker Lewis

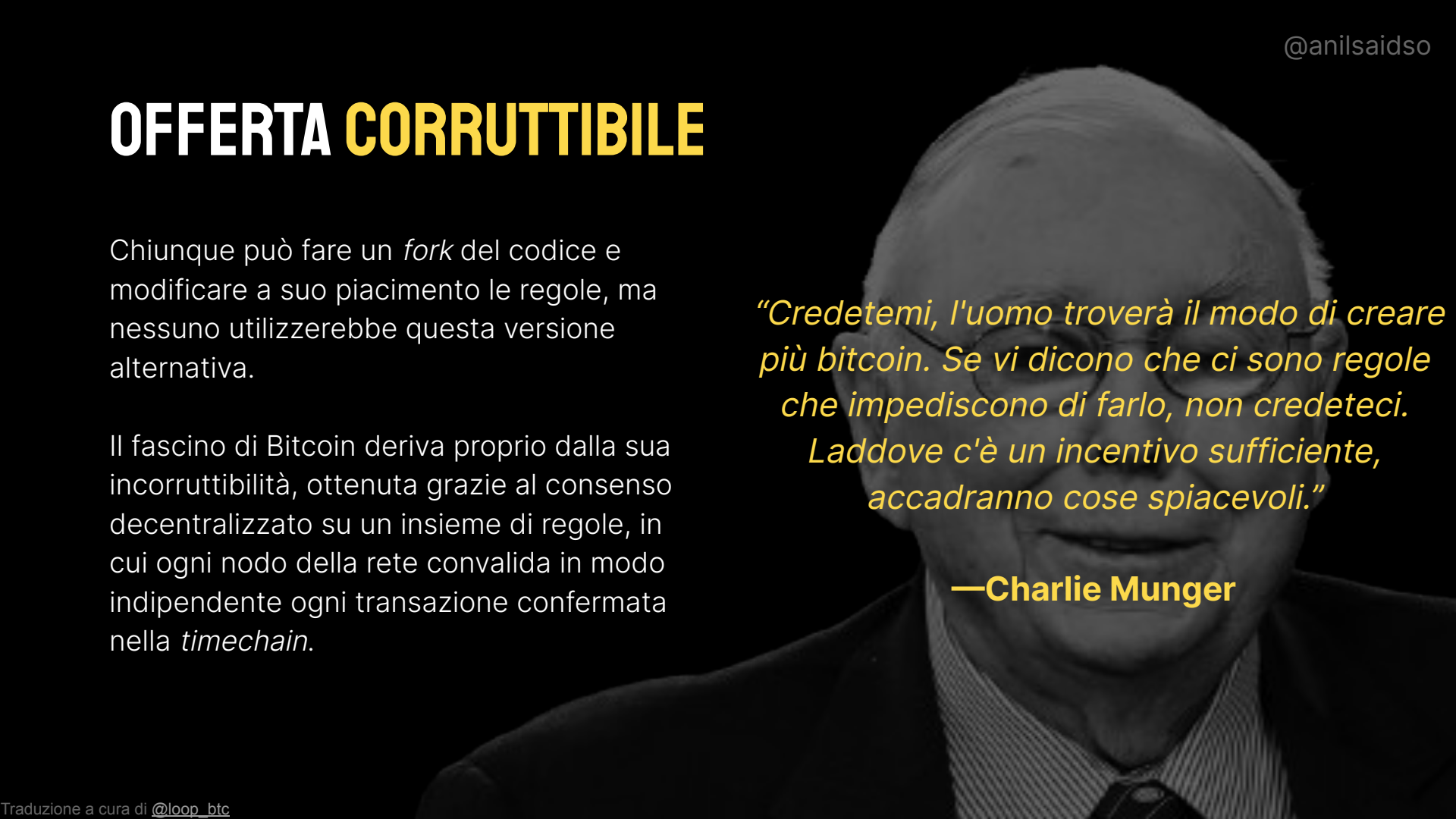
"Usare bitcoin per gli acquisti al consumo è come guidare un Concorde per andare a fare la spesa: uno spreco ridicolmente costoso di uno strumento sorprendente."
—Saifedean Ammous

@anilsaidso

OFFERTA CORRUTTIBILE

Chiunque può fare un *fork* del codice e modificare a suo piacimento le regole, ma nessuno utilizzerebbe questa versione alternativa.

Il fascino di Bitcoin deriva proprio dalla sua incorruttibilità, ottenuta grazie al consenso decentralizzato su un insieme di regole, in cui ogni nodo della rete convalida in modo indipendente ogni transazione confermata nella *timechain*.

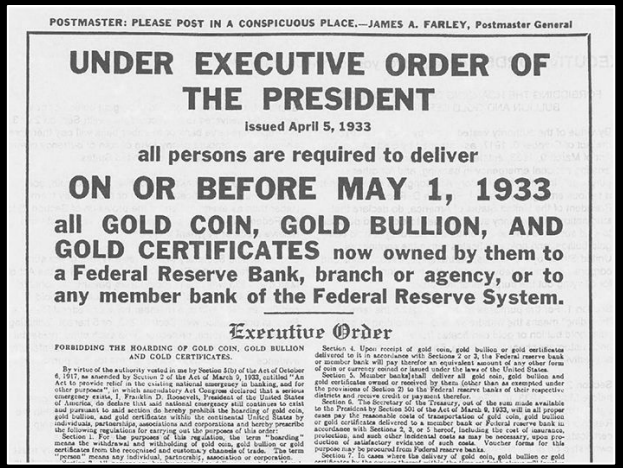


“Credetemi, l'uomo troverà il modo di creare più bitcoin. Se vi dicono che ci sono regole che impediscono di farlo, non credeteci. Laddove c'è un incentivo sufficiente, accadranno cose spiacevoli.”

—Charlie Munger

@anilsaidso

VERRÀ VIETATO



POSTMASTER: PLEASE POST IN A CONSPICUOUS PLACE.—JAMES A. FARLEY, Postmaster General

UNDER EXECUTIVE ORDER OF THE PRESIDENT

issued April 5, 1933

all persons are required to deliver

ON OR BEFORE MAY 1, 1933

all GOLD COIN, GOLD BULLION, AND GOLD CERTIFICATES now owned by them to a Federal Reserve Bank, branch or agency, or to any member bank of the Federal Reserve System.

Executive Order

FORBIDDING THE HOARDING OF GOLD COIN, GOLD BULLION AND GOLD CERTIFICATES.

By virtue of the authority vested in me by Section 5(b) of the Act of October 6, 1917, as amended by Section 2 of the Act of March 9, 1933, entitled "An Act to provide relief in the existing national emergency in banking, and for other purposes", in which emergency Act Congress declared that a serious emergency exists, I, Franklin D. Roosevelt, President of the United States of America, do declare that said national emergency still continues to exist and pursuant to said section do hereby prohibit the hoarding of gold coin, gold bullion, and gold certificates within the continental United States by individuals, partnerships, associations and corporations and hereby prescribe the following regulations for carrying out the purposes of this order:

Section 1. For the purposes of this regulation, the term "hoarding" means the withdrawal and withholding of gold coin, gold bullion or gold certificates from the recognized and customary channels of trade. The term "person" means any individual, partnership, association or corporation.

Section 4. Upon receipt of gold coin, gold bullion or gold certificates delivered to it in accordance with Sections 2 or 3, the Federal reserve bank or member bank will pay therefor an equivalent amount of any other form of coin or currency coined or issued under the laws of the United States.

Section 5. Member banks shall deliver all gold coin, gold bullion and gold certificates owned or received by them (other than as exempted under the provisions of Section 2) to the Federal reserve banks of their respective districts and receive credit or payment therefor.

Section 6. The Secretary of the Treasury, out of the sum made available to the President by Section 501 of the Act of March 9, 1933, will in all proper cases pay the reasonable costs of transportation of gold coin, gold bullion or gold certificates delivered to a member bank or Federal reserve bank in accordance with Sections 2, 3, or 5 hereof, including the cost of insurance, protection, and such other incidental costs as may be necessary, upon production of satisfactory evidence of such costs. Voucher forms for this purpose may be procured from Federal reserve banks.

Section 7. In cases where the delivery of gold coin, gold bullion or gold

In tutta onestà, Bitcoin *può* essere vietato. È l'applicazione del divieto che è una causa persa. Questo perché Bitcoin ha trasformato il denaro in pura informazione (una chiave privata è semplicemente un numero casuale a 256 bit). Vietare Bitcoin equivarrebbe a impedire la generazione di numeri casuali... buona fortuna!

Se le transazioni Bitcoin sono ben visibili sulla *timechain*, la localizzazione delle chiavi private che ne controllano l'accesso rimane perlopiù non rilevabile. Inoltre l'infrastruttura necessaria per accedere alla rete Bitcoin al fine di verificare in modo affidabile le transazioni è banale, a condizione che sia reperibile un hardware di base.

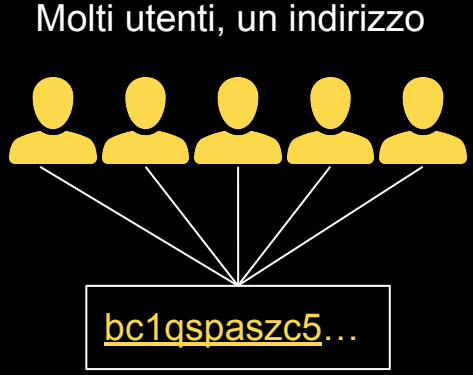
"Vietare Bitcoin non è diverso dal cercare di vietare la matematica. Dimostrerà solo la sua utilità e spingerà più persone verso di esso."
—Saifedean Ammous

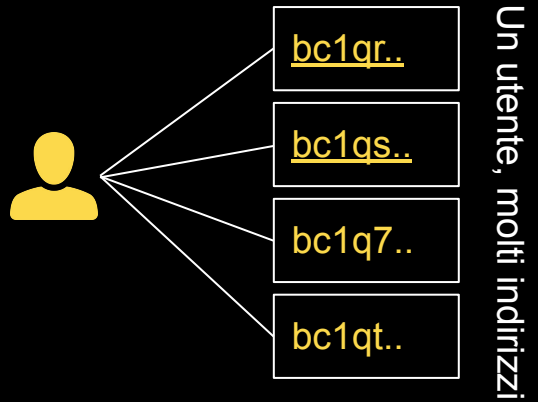
POSSESSO CONCENTRATO

Quante volte avete sentito dire: "***una manciata di wallet detiene la maggior parte di tutti i bitcoin!***".

È vero, ma manca una precisazione fondamentale. In genere si tratta di wallet di operatori di cambio (exchange), ognuno dei quali ha milioni di clienti. In un mondo ideale, le persone non lascerebbero i propri bitcoin in un exchange, ma questo è un argomento per un altro giorno.

Un singolo indirizzo bitcoin può contenere bitcoin appartenenti a molti utenti e un singolo utente può controllare più wallet. In effetti, per mantenere la privacy si consiglia di evitare il riutilizzo degli indirizzi, il che significa che viene generato un nuovo indirizzo per ogni transazione ricevuta.



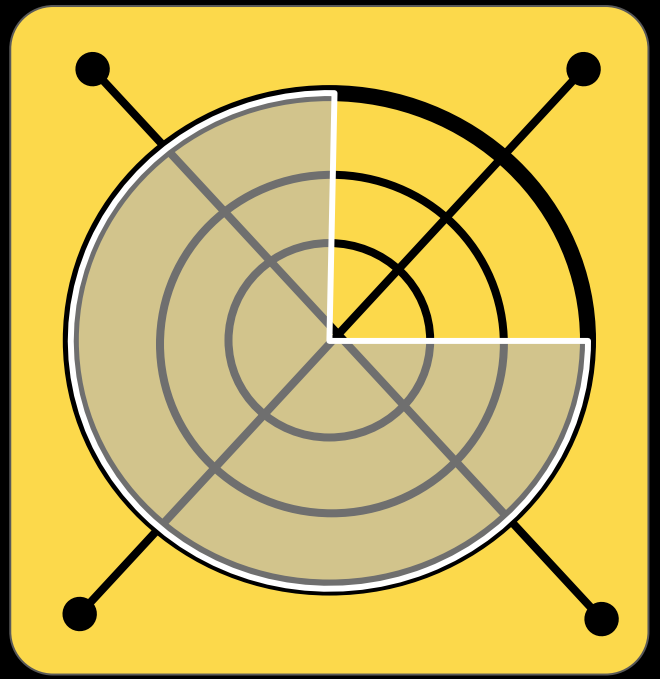


@anilsaidso

MINING CENTRALIZZATO

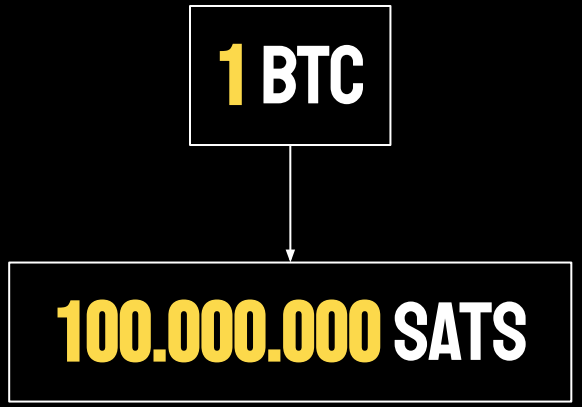
Il rischio che i *pool* di minatori si accordino tra loro per interrompere in qualche modo la rete, censurando le transazioni o effettuando una doppia spesa in bitcoin, deriva dalla mancanza di comprensione degli incentivi per i minatori e del loro controllo sulla rete e sulla *timechain*.

"La maggioranza del potere di hashing ***non può****:*
- privarti dei bitcoin in tuo possesso;
- cambiare le regole di Bitcoin;
- danneggiare te senza danneggiare loro stessi."
—Jimmy Song



TROPPO COSTOSO

Il confronto tra il prezzo unitario di bitcoin e il prezzo unitario di altri asset (ad esempio, 1 bitcoin e 1 oncia d'oro) dimostra una **distorsione delle unità**. È più accurato confrontare l'intera capitalizzazione di mercato di bitcoin con quella di altre *asset class*. Inoltre, un singolo bitcoin è divisibile in **100 milioni di unità più piccole** (*satoshi o sats*). Come dice il detto massimalista: "*puoi comprare una frazione di bitcoin!*".



COSTI DI TRANSAZIONE PROIBITIVI

Le transazioni confermate sul livello principale di Bitcoin forniscono un livello di certezza della loro finalizzazione che non può essere eguagliato nel sistema finanziario tradizionale. Pertanto, anche se le commissioni possono aumentare di tanto in tanto a causa della capacità limitata di ogni blocco, la rete Bitcoin rappresenta un metodo di *settlement* (regolamento) degli scambi incredibilmente efficiente e affidabile per le transazioni di valore elevato. Le transazioni più piccole (microtransazioni incluse) continuano a migrare verso livelli secondari (ad esempio, *Lightning Network*, *Liquid* o altre *side-chain* federate), dove le commissioni sono di un ordine di grandezza inferiore a quanto può permettersi una banca commerciale.

*"Tra l'ottobre 2010 e il luglio 2021, le commissioni medie giornaliere per le transazioni si sono attestate intorno allo **0,02%** del loro valore."*

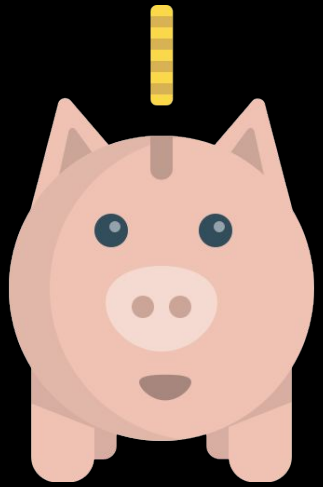
—Saifedean Ammous

(The Fiat Standard)

SARÀ ACCAPARRATO

Un'argomentazione che ha visto una recrudescenza in un'epoca di debito a basso costo è che una moneta a offerta fissa incentiva l'*hoarding* (accaparramento), per cui i possessori non spenderanno i loro bitcoin nel sistema economico, ma se ne staranno semplicemente con le mani in mano a guardare il loro valore aumentare.

Questa logica presenta alcuni problemi, soprattutto perché demonizza un'attività più comunemente nota come *risparmio* (l'eccesso di reddito rispetto alla spesa). Ribattezzare il risparmio come accaparramento significa sostenere la necessità di vivere di stipendio in stipendio. Qualsiasi investimento significativo richiede prima di tutto un risparmio di capitale da impiegare (almeno questa era la logica prima che le banche creassero denaro attraverso i prestiti).



"Le persone detengono denaro per proteggersi dall'incertezza futura.

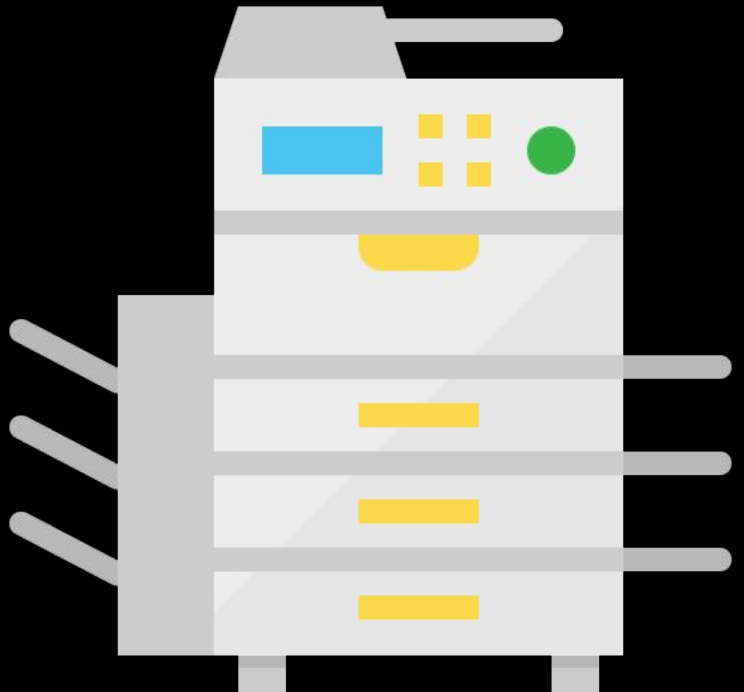
Sì, detenere bitcoin significa usare bitcoin. Tutti i bitcoin sono sempre detenuti da qualcuno, i pagamenti cambiano solo chi li detiene."
—Pierre Rochard

PUÒ ESSERE DUPLICATO

CRITICA: "***Bitcoin non è scarso perché ci sono migliaia di altre criptovalute in circolazione e inoltre chiunque può copiare il codice e creare la propria versione.***"

Bitcoin è un protocollo *open source* per il trasferimento di valore. È vero, chiunque può creare un *fork* o tentare di lanciare la propria versione. Ma non può portarsi dietro tutti gli sviluppatori, i minatori e la potenza di *hash*, gli utenti, gli operatori dei nodi o la suite di prodotti e servizi.
Bitcoin attrae persone e risorse proprio per la sua trasparenza e il suo rigoroso processo di sviluppo.

"L'open source è di fatto una meritocrazia. È una mente collettiva che costruisce soluzioni. I molteplici controlli si traducono in una maggiore sicurezza. Bitcoin Core è probabilmente uno dei software più controllati al mondo."
—@BTCSchellingPt

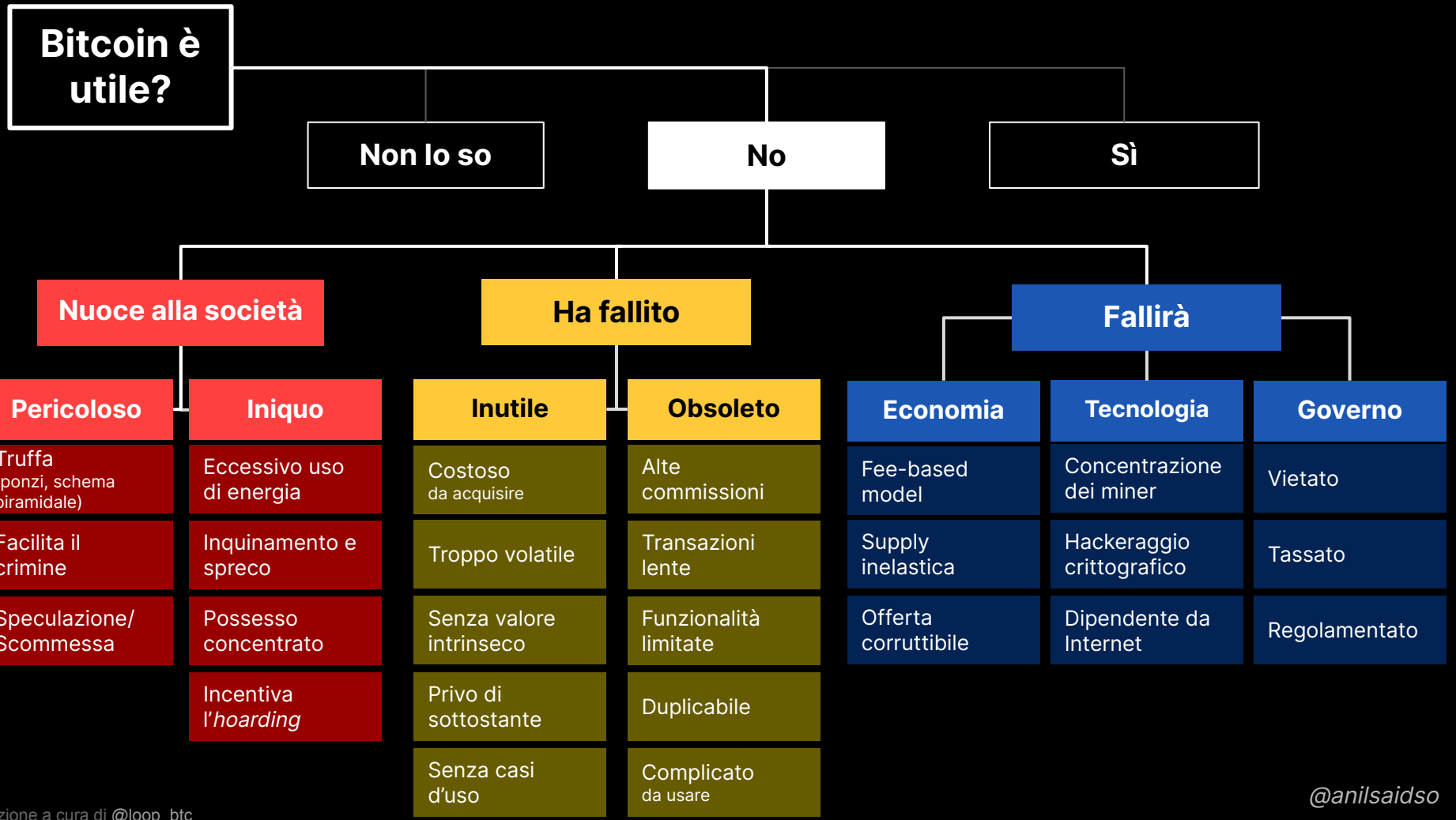


IL VIAGGIO DI UN BITCOINER

Ci vuole poco talento per trovare **100 motivi** per cui Bitcoin fallirà.

Ma ci vuole una genuina curiosità per sfatare in modo indipendente e sistematico queste ragioni, una per una, partendo da princìpi elementari.

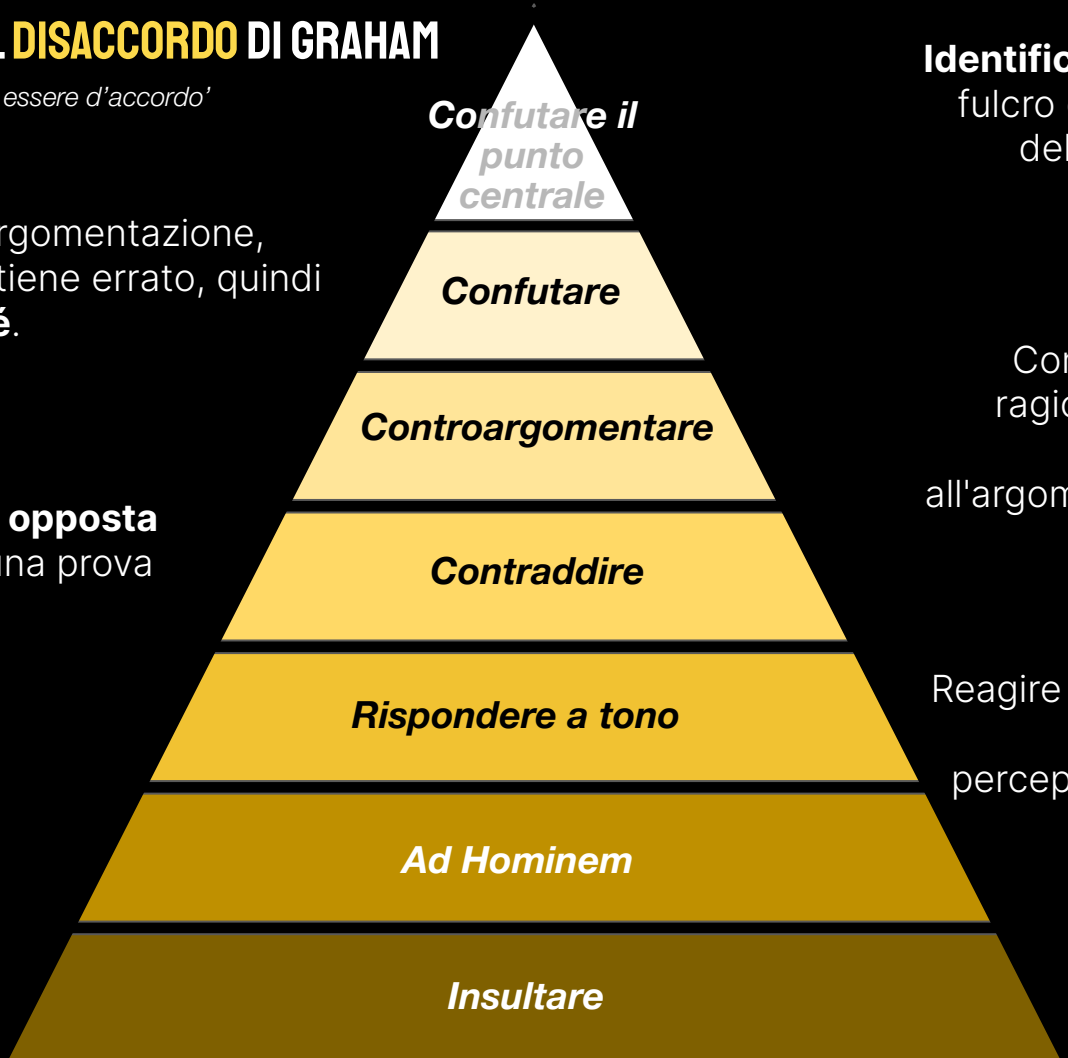
È così che si **plasma** un bitcoiner.



Traduzione a cura di @loop_btc

LA GERARCHIA DEL DISACCORDO DI GRAHAM

Adattato da 'Imparare a non essere d'accordo' di Paul Graham (2008)



Identificare correttamente il fulcro dell'argomentazione dell'avversario prima di controbattere.

Individuare, in un'argomentazione, l'elemento che si ritiene errato, quindi spiegarne il **perché**.

Controargomentare **più** ragionamento e/o prove. Puntando dritto all'argomentazione originale.

Dichiarare una tesi **opposta** con poche o nessuna prova a sostegno.

Reagire con **irritazione** a un tono che gli altri percepiscono come neutro

Attaccare **personalmente** l'avversario

La forma più **meschina** di disaccordo.

@anilsaidso

Traduzione a cura di @loop_btc

I QUATTRO CRITICI DI BITCOIN

Secondo **Alex Gladstein**

"Potresti essere un'eccezione, ma in pratica tutti i critici di Bitcoin rientrano in una di queste 4 categorie:"

L'odiatore acido

"Hai sentito parlare di Bitcoin anni fa, ma non l'hai comprato, e ora sei diventato acido"

Lo statista disperato

"Credi che il denaro possa essere creato solo dallo Stato, quindi Bitcoin demolisce la tua visione del mondo"

L'intellettuale disonesto

"Non hai fatto il lavoro necessario per capire Bitcoin e quindi vorresti che sparisse."

Il prigioniero delle perdite

"Hai investito in altcoin e senti il bisogno di criticare Bitcoin per difendere la tua scelta di vita."

@anilsaidso

Grazie per aver letto!

Lascia una recensione su Gumroad e contribuisci a ridurre la FUD (*NdT*: da Fear, Uncertainty, and Doubt - Paura, incertezza e dubbio) su Bitcoin aiutando altre persone a trovare queste slide.

**Puoi utilizzare queste slide per scopi educativi non a scopo di lucro.*