Marco Dal Prà (m_dalpra)

# BITCOIN: PERCHÉ SONO A FAVORE DEI BLOCCHI PICCOLI

30 August 2020

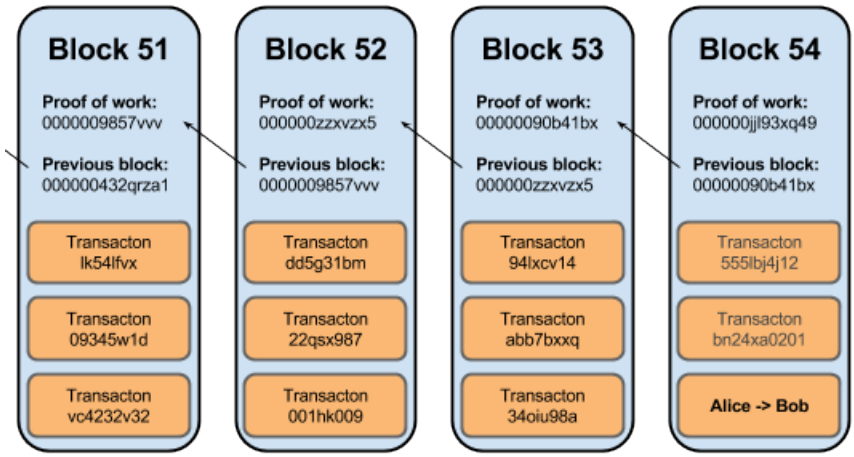
Uno dei problemi che assilla la comunità dei sostenitori di Bitcoin, è la dimensione dei blocchi. Questa tematica ha già causato scissioni tra gli sviluppatori che hanno portato allo sviluppo di progetti alternativi somiglianti ma comunque diversi. La storia è presto detta: alcuni credono che i blocchi, dove sono memorizzate le operazioni di pagamento, debbano essere più piccoli possibili, mentre altri ritengono che la dimensione dei blocchi non deve avere dei limiti. Vediamo vantaggi e svantaggi delle proposte e perché sono favorevole ad una delle due.

**Cosa sono i Blocchi**

Bitcoin è praticamente una banca diffusa tra i correntisti. una banca dotata di una propria moneta. Chiunque può conservare nel proprio PC l'archivio di tutte le operazioni di pagamento dal 2009 ad oggi, la blockchain, soltanto che per mantenerla aggiornata deve tenerlo acceso 24 ore su 24.

La blockchain oggi occupa **circa 300GB**, uno spazio sostenibile da qualsiasi PC domestico, soltanto che non è un numero fisso, ma aumenta di circa 1,3 MB ogni 10 minuti. Questo perché, come abbiamo detto, la blockchain è il database che contiene tutti gli scambi "monetari" che avvengono tra gli utenti, e ne avvengono in continuazione, 24 ore su 24.
Ricordo inoltre che bitcoin, seppure si possa ritenere un "esperimento" privato, è una moneta che non conosce confini geografici né fusi orari o festività, pertanto funziona 24 ore su 24.

Il sistema è quindi sempre online ed elabora ordini di pagamento in qualsiasi momento, senza interruzione alcuna, dal gennaio 2009 ad oggi.
Generalmente in un blocco si riescono a far stare circa 2500 operazioni di pagamento, e contando che un blocco viene chiuso ogni 10 minuti, significano circa 5 operazioni al secondo, un numero bassissimo (se non ridicolo) se confrontato con i circuiti delle maggiori carte di credito come VISA o Mastercard, che posso processare **oltre 30.000 operazioni al secondo**!




*blockchain_Blocks.png*

**Sembra un problema irrisolvibile**

Il limite prestazionale del protocollo Bitcoin, detto anche limite di scalabilità, è risaputo ed stato affrontato fin dai primi anni, senza che sia mai stata trovata una soluzione vera e propria.
Di conseguenza negli anni sono nate molte altre criptovalute - che ricordo, oggi sono centinaia - ognuna con la propria ricetta per risolvere il problema di scalabilità di Bitcoin, come ad esempio Litecoin, che processa circa 20 operazioni al secondo. Sono comunque ancora tutte lontanissime dai livelli prestazionali dei sistemi di pagamento tradizionali, tranne alcune altre proposte che vedremo a breve.

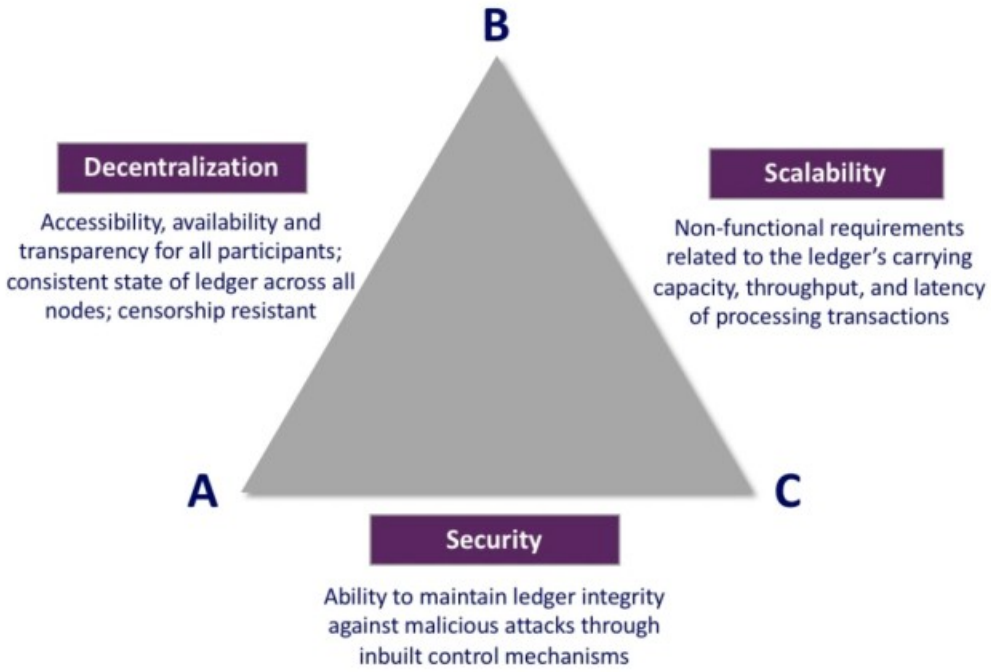
**Il Trilemma di Vitalik Buterin**

Vitalik Buterin è un giovane programmatore canadese molto famoso perché è l'autore di una piattaforma per l'esecuzione di Smart Contract decentralizzati dotata di una criptovaluta denominata Ethereum.
Ebbene Buterin ha fatto notare che le criptovalute (ma forse tutti i sistemi monetari) sono afflitte da un problema che lui stesso ha chiamato **Il Trilemma della Scalabilità** e che si potrebbe sintetizzare in una sorta di "non puoi avere tutto". In pratica ad oggi risulta impossibile raggiungere tutti e tre questi obiettivi:

- Decentralizzazione,
- Sicurezza,
- Scalabilità

Per chi non conosce il settore, la prima significa incensurabilità, la seconda significa impossibilità di falsificazione, la terza significa potenza di elaborare un elevato numero di transazioni a servizio un grande numero di utenti.
Le banche ed i sistemi di pagamento ordinari, generalmente assicurano Sicurezza e Scalabilità, ma sono censurabili, come accaduto ad esempio a Julian Assange con Wikileaks, che non può ricevere

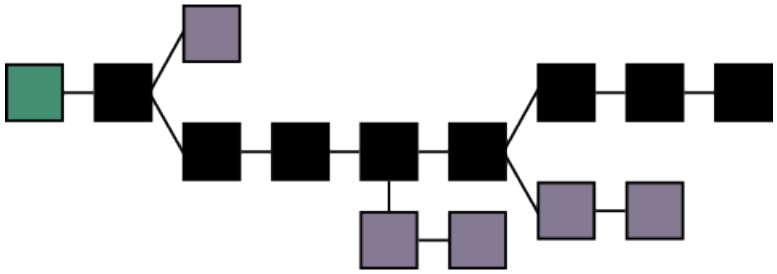
donazioni con le carte di credito. Bitcoin invece raggiunge le prime due ma non è scalabile, in quanto il protocollo non prevede la possibilità di aumentare il numero di operazioni al secondo (limitate dallo spazio concesso per inserire dentro ogni blocco).




*Scalability Trilemma*

**Le biforcazioni**

Come per tutte le cose del mondo, anche nelle criptovalute ci sono conflitti di opinione tanto da portare ad accadimenti che definirei un tantino "bizzarri". Non sto parlando di interessi di tipo economico, ma di veri e propri scontri ideologici sul futuro degli algoritmi di governo delle criptovalute.
Ad esempio nel 2017 un gruppo programmatori ha elaborato dei nuovi codici sorgenti per Bitcoin con un protocollo, denominato Bitcoin Cash, nel quale il limite di riempimento per i blocchi veniva aveva aumentato da 1 a 8 MB, con la possibilità in futuro di allargarlo ulteriormente.
Ma nel mondo ognuno è libero di fare le proprie scelte, cosè solo una piccola parete dei nodi della rete ha accettato questa modifica (circa 1000 nodi) mentre la restante parte ha preferito rimanere con il vecchio software (circa 10.000 nodi), così la blockchain ha subito una biforcazione (nel gergo "fork"), tra i nodi con il nuovo software (**e quindi una nuova moneta**) ed altri nodi con quello "tradizionale". Ma non contenti, anche all'interno della comunità Bitcoin Cash si sono creati degli attriti, tanto che nel Novembre 2018 si è arrivati ad una ulteriore scissone. Oggi abbiamo quindi una nuova criptovaluta, che prevede blocchi fino a 128 MB e che si chiama Bitcoin SV.
Queste due nuove criptovalute permettono quindi di aumentare il numero di operazioni elaborate ogni secondo, ma hanno per contraltare il fatto che mettono a rischio la decentralizzazione: vediamo perché.



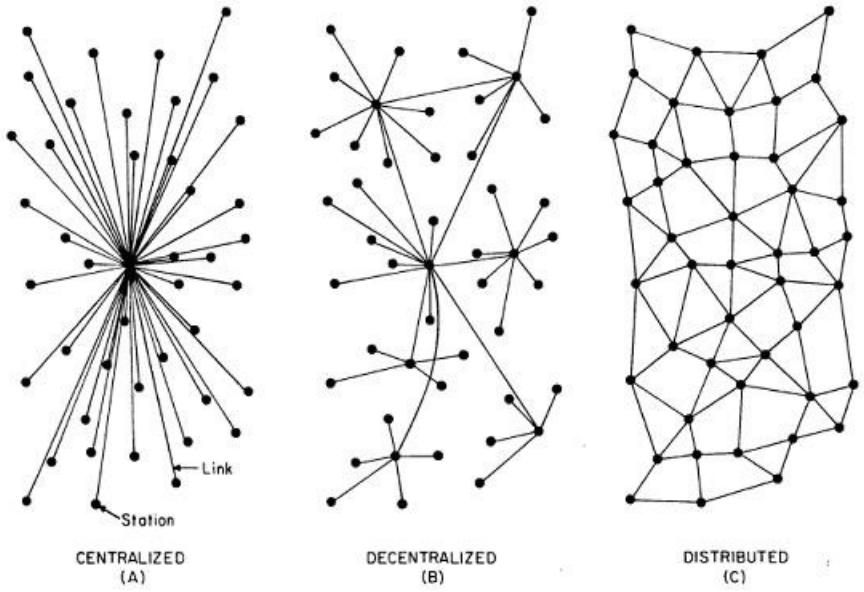
*Blockchain "Fork"*

**La decentralizzazione**

Per chi non lo conoscesse, Bitcoin è nato nel 2008 a pochi giorni dal fallimento della banca americana Lehman Brothers, quella che a causa dei mutui subprime ha lasciato in mezzo alla strada migliaia di persone. Lo scopo di Bitcoin, di contestare l'alchimia finanziaria che operava con la complicità dei governi è del tutto evidente.
Come rendere un sistema monetario indipendente ed inattaccabile ad eventuali "nemici"? Come evitare di essere chiusi da eventuali governi che operano contro l'interesse i cittadini (come appunto successo nel 2008 negli USA)?
La soluzione prospettata è quella che hanno preso Bitcoin e tutte le altre criptovalute: una rete **senza un centro**.
Per una rete "informatica", semplificando al massimo, decentralizzazione significa:

- accessibilità da qualunque parte del mondo,
- elevatissima disponibilità (e quindi affidabilità)
- trasparenza per tutti i partecipanti (tanti nodi non riescono a mettersi d'accordo per "imbrogliare")
- resistenza alla censura (se le autorità di uno stato più o meno democratico decidono di chiudere quella specifica rete, non hanno qualcuno a cui rivolgersi per spegnarla, ed anche "chiudendo" qualche nodo, il resto della rete continua a funzionare).

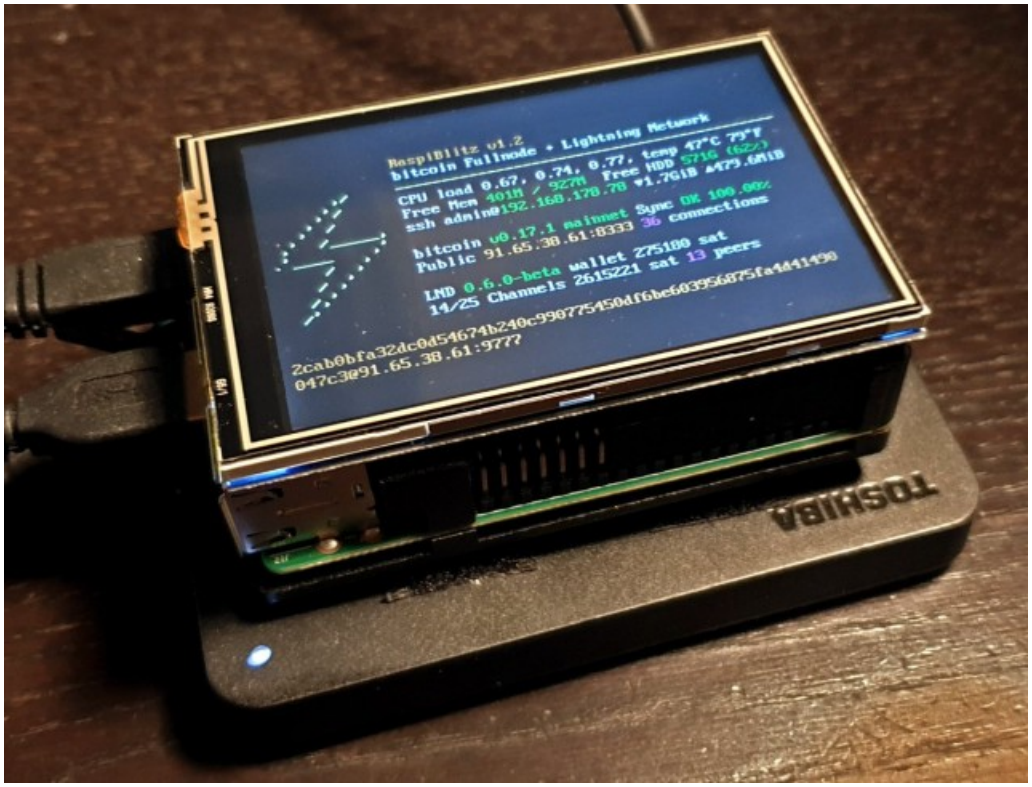
Questa prerogativa delle reti decentralizzate o meglio distribuite, è stata ampiamente dimostrata dalla rete Edonkey o Emule oppure al più recente protocollo **BitTorrent**, che infatti non si possono fermare.




*Networks.png*

**Cos'è un Nodo?**

Un ultimo concetto da chiarire nelle criptovalute è quello del Nodo, o meglio del **Full Node**.
Un nodo è solitamente un PC connesso alla rete "H24" nel quale c'è una copia integrale della blockchain e nel quale il software controlla se i nuovi movimenti della criptovaluta sono corretti oppure no. Il nodo quindi aggiunge nuovi blocchi alla blockchain solamente se rispondono alle regole del protocollo e, ad esempio, non sono stati "illecitamente" duplicati i contenuti di un qualsiasi conto.
Per fare un nodo sulla rete Bitcoin è sufficiente un processore Raspberry, un Hard Disk esterno da 1TB e poco altro, cioè una spesa inferiore a 130€; questo l'altro è un dispositivo dal consumo bassissimo, dissipazione termica e rumorosità quasi zero: si può tenere anche nel soggiorno di casa. Che succederebbe se le risorse hardware per realizzare un nodo diventassero molto più impegnative?




*Rasberry PI + HD 1TB: Bitcoin Full Node*

**Cosa c'entra la dimensione dei blocchi?**

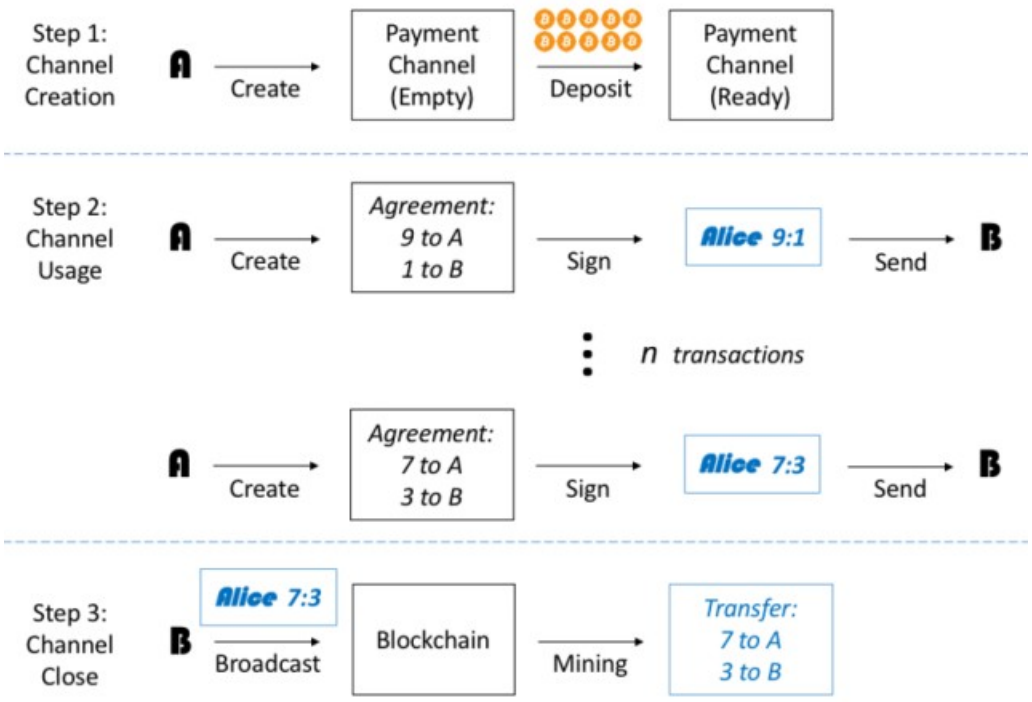
Bene, dopo queste premesse, torniamo alla problematica della scalabilità di Bitcoin.
Che succede se, per aumentare il numero di operazioni al secondo (per raggiungere le prestazioni del "tradizionale" mondo dei pagamenti), **aumentiamo la dimensione dei blocchi?**
Semplice: i nostri nodi dovranno avere una potenzialità di archiviazione maggiore ma soprattutto, per validare un numero molto maggiore di operazioni nello stesso tempo, dovranno avere una potenzialità di calcolo enormemente maggiore.
La realizzazione del nodo quindi **non sarebbe più alla portata di tutti** ma richiederebbe risorse hardware ed economiche molto maggiori, ed un maggiore utilizzo di spazio, di energia elettrica. Tralasciamo poi i problemi di rumorosità, la dissipazione termica ed i periodici interventi per aggiungere Hard Disk.
Oggi la rete Bitcoin conta circa 10000 nodi: quanti ne resteranno se per gestirli è necessario un armadio Rack invece di 130€ **sono necessarie risorse per oltre 10.000€ ?** Saranno 1000, saranno 500 o saranno meno di 100?
Saranno in mano a privati, come ora o saranno prevalentemente in mano ad aziende?
Il problema è importantissimo, perché pochi nodi, in gestione a poche aziende (magari anche ben conosciute) sono rapidamente localizzabili e "spegnibili". La criptovalute finirebbe rapidamente, senza aspettare l'intervento della autorità.
In poche parole... una follia!

**La Storia Insegna**

Forse non tutti avete seguito la storia di Libra, la criptovaluta ideata da Facebook e per la quale è stata creata una fondazione composta da aziende prestigiose e famose. Bene, il progetto ora si è notevolmente ridimensionato perché ministri, funzionari e deputati di varie nazioni hanno sollevato un "polverone" di polemiche tanto da causarne la defezione di alcuni membri importanti del calibro di Paypal, Visa, Mastercard e Vodafone.
Non è quindi servita nessuna azione legale: le aziende, solo per questioni di prestigio, legittimazione e rischio di richiesta danni, si sono di loro spontanea volontà tolte dal progetto, nonostante ancora da definire. Come si può pensare di destinare il portafoglio di alcuni privati ad una banca che potrebbe venir chiusa in quattro e quattr'otto dalla rinuncia di chi detiene i server?

**Conclusione**

Le criptovalute sono monete sorte dall'ordine spontaneo, con la libera iniziativa della comunità Open Source. Trasformarle in sistemi di pagamento che richiedono enormi risorse economiche e tecnologiche, significherebbe praticamente tornare al sistema tradizionale cioè al sistema bancario.
Hanno provato già due volte a modificare il protocollo, ma la maggioranza ha deciso altrimenti, ecco perché Bitcoin Cash e Bitcoin SV occupano posizioni di nicchia, una situazione che mette a rischio la sicurezza delle loro stesse blockchain, per l'esiguo numero di nodi che le compone.
Poi a ben vedere il problema della scalabilità di Bitcoin è un falso problema. Non è infatti necessario cercare di risolvere il Trilemma della Scalabilità, perché la soluzione c'è già, senza scomodare la modifica del protocollo Bitcoin e senza rischiare le strade impervie degli sviluppatori di Bitcoin Cash e SV: si chiama **Lightning Network**.
Questa non è una modifica al protocollo Bitcoin, ma è l'implementazione di **un secondo Layer** sopra il protocollo Bitcoin, proprio come lo stack dei livelli ISO/OSI del protocollo TCP/IP.
Per semplificare il concetto, è come se Bitcoin fosse il conto corrente bancario mentre Lightning Network fosse la carta di credito "ricaricabile", una soluzione rende superflui tutti gli sforzi per scalare il protocollo Bitcoin.




*Transazioni su Lightning Network*

E' vero, ligthning network **richiede dei software differenti** per la gestione dei propri fondi rispetto ai tradizionali Wallet per le criptovalute che si installano nei cellulari o nei PC, ma risolve il problema di scalabilità sia nel tempo che nello spazio. LN, questa è la sigla del protocollo, non ha limiti "quantitativi" sul numero di operazioni che gestisce (è uno scambio di firme digitali, non ci sono blocchi da riempire), e non ha limiti "temporali" in quanto i pagamenti si risolvono istantaneamente (non ci sono da attendere i 10 minuti della conferma del blocco che ha Bitcoin).
Ecco quindi che con Lightning Network, accettando il compromesso di utilizzare un secondo software, tutti gli incubi che affliggevano gli sviluppatori delle criptovalute da circa 10 anni sono superati, nonostante quelli che ancora tirano fuori la questione della scalabilità o della dimensione dei blocchi.
Sopra il protocollo TCP/IP viaggiano i protocolli POP3 o SMTP o HTTP; allo stesso modo sopra Bitcoin c'è Lightning Network: è il giusto approccio di risolvere i problemi, per livelli, per strati, per competenze.
Del resto, non si può fare tutto con Bitcoin, ne va della sua caratteristica più importante, finora mai scalfita:
**la sicurezza**.

**Disclaimer**

Seguo per passione gli aspetti tecnologici delle criptovalute e dei loro risvolti culturali.
Preciso che sono un tecnico elettronico e non sono un operatore "finanziario": non vendo niente e

soprattutto... non faccio previsioni sui prezzi!
Non nascondo di essere favorevole alle criptovalute come Bitcoin perché penso siano tecnologicamente superiori alle monete emesse dalle banche centrali, nonostante siano benedette dai governi.
Sono di questa opinione persone del del calibro di Robert Kiyosaki o Nassim Taleb, Raoul Pal, Andreas Antonopoulos, e tanti altri. Persino il responsabile della ricerca di **Deutsche Bank**, Jim Reid, è arrivato a dire che l'era della Fiat Money volge al termine.
Cosa la sostituirà non lo sappiamo, ma le criptovalute sono dei candidati.

**LINK UTILI**

Lightning Network - Spiegazione di Emanuele Pagliari https://cryptonomist.ch/2019/06/09/lightning-network-bitcoin-come-funziona/

Lo spazio occupato dalla Blockchain di Bitcoin https://www.blockchain.com/charts/blocks-size

Esempio di contenuto di un blocco Bitcoin https://www.blockchain.com/btc/block/000000000000000000009fb1d318c4a494001f5345a0326fc0f4d9b93dcdd6727

Il numero di nodi in in tempo reale, cioè PC che eseguono il software ed hanno una copia della blockchain:

- [Bitcoin] https://bitnodes.io/
- [Bitcoin Cash] https://cash.coin.dance/nodes
- [Bitcoin SV] https://sv.coin.dance/nodes

**Foto di Copertina**

Un "full node" bitcoin inserito in un vecchio televisore anni '80, realizzato con un Raspberry Pi e con un Hard Disk USB, dallo sviluppatore americano Lukas Nuzzi https://medium.com/@LucasNuzzi

Estratto da "https://www.electroyou.it/mediawiki/index.php?title=UsersPages:M_dalpra:bitcoin-perch-sono-a-favore-dei-blocchi-piccoli"