Cosa sta succedendo al Bitcoin: tutte le spiegazioni

di Alberto De Luigi

25 Marzo 2017

Indice dei contenuti:

PREMESSA: COSA STA SUCCEDENDO NEL MONDO BITCOIN

In base al protocollo Bitcoin ogni dieci minuti circa si aggiunge alla blockchain un nuovo blocco dalla capacità di 1 megabyte, nel quale vengono registrate le transazioni eseguite dagli utenti e non convalidate nel blocco precedente. Il successo del Bitcoin ha fatto affluire nuovi utenti nella rete, che si è saturata: il numero di transazioni effettuate ogni secondo ha raggiunto il limite di capacità del blocco. I miners si occupano della creazione del blocco, registrando le transazioni degli utenti e guadagnando in cambio una

commissione su ogni transazione. Ora che 1mb non basta più, gli utenti sono costretti ad aumentare le commissioni ai miners per avere le proprie transazioni confermate, pena l'attesa di molte ore o giorni.

L'ALTO COSTO DELLA TRANSAZIONE

Le commissioni si pagano in proporzione al peso in bytes della transazione (mediamente poco più di 200 bytes ogni transazione), a prescindere dal fatto che spostino un valore di miliardi di euro o pochi centesimi. Per questo motivo, non è assolutamente conveniente fare transazioni di basso importo in bitcoin: ad esempio un caffé pagato in bitcoin costerebbe circa il doppio.
Dunque se fino a qualche mese fa il Bitcoin poteva essere utilizzato quotidianamente per l'acquisto di beni di consumo, come un cappuccino o una ricarica telefonica, oggi è solo una valida riseva di valore e strumento di investimento (almeno finché il trend del prezzo è positivo). Utenti che fino a non molto tempo fa erano abituati a fare molte transazioni e acquisti di tutti i tipi, sono rimasti delusi. Sostituire Purse ad Amazon rimane veramente conveniente solo per acquisti di un importo medio-alto, mentre in precedenza, chi conosceva e utilizzava il servizio non ne poteva fare a meno. Gli alti costi di transazione non sono solo un problema per gli utenti, ma anche per quelle aziende che vogliono fare business in bitcoin: qualsiasi e-commerce che venda al dettaglio oggetti dal costo relativamente basso (o servizi come ricariche telefoniche) è praticamente tagliato fuori dal mercato. Se il Bitcoin fallisce come mezzo di pagamento, anche solo momentaneamente, fallisce l'obiettivo per cui è stato creato. Le prime quattro parole del white paper di Nakamoto sono "Commerce on the internet", non certo "Invest in digital assets", e questo è un fatto che non si può ignorare.
C'è chi ancora vanta di vivere in Bitcoin, anche in Italia, ed effettivamente percepisce uno stipendio esclusivamenete in bitcoin. Ma con transazioni così alte, vivere di soli bitcoin

è economicamente del tutto sconveniente. Chi afferma di utilizzare solo bitcoin, in realtà quando spende paga in euro: utilizza infatti delle carte prepagate che vengono solo caricate in bitcoin (cambiandoli in euro), ma si appoggiano a un circuito di pagamento tradizionale in moneta fiat. Se per utilizzare il Bitcoin si è costretti a fare transazioni nel circuito Visa, è chiaro che qualcosa non va: Bitcoin dovrebbe essere una soluzione del tutto indipendente, disintermediata e untrusted, mentre in questo caso è obbligato il passaggio al circuito tradizionale, attraverso un intermediario (che fra l'altro chiede commissioni aggiuntive) di cui ci si deve fidare.

AUMENTARE IL BLOCCO PER RISOLVERE I COSTI DI TRANSAZIONE

Una soluzione al problema è aumentare la dimensione del blocco. Un aumento da 1 megabyte a 2, 3 o 30 è, tecnicamente, una banalità da eseguire. Chiunque potrebbe fare una modifica di questo tipo al protocollo Bitcoin e proporla al resto della rete. Un blocco più grande permetterebbe di decongestionare la rete, così che gli utenti ottengano con facilità le proprie transazioni convalidate nel primo blocco. Data la maggiore capacità, gli utenti non competerebbero come oggi per avere una conferma delle transazioni alzando le commissioni per i miner, perciò anche il costo per transazione rimarrebbe basso. La usability della moneta ne trarrebbe un enorme vantaggio. Ma non tutto è così semplice: c'è infatti un trade-off fra usability e sicurezza.

IL PROBLEMA DI SICUREZZA DELLA RETE CON L'AUMENTO DEL BLOCCO

Bitcoin è un sistema di pagamento che può funzionare in modo completamente decentralizzato. Tuttavia, nella pratica funziona in modo solo parzialmente decentralizzato. Questo perché esistono nodi "pieni" (full nodes) e nodi "leggeri" (lightweight o "lite" nodes), in base al software che l'utente utilizza sul proprio device per collegarsi alla rete Bitcoin. L'utente che ha scaricato un wallet come Electrum sul proprio

smartphone, col quale inviare e ricevere bitcoin, rappresenta un lite node. L'utente che invece utilizza il software Bitcoin Core e scarica l'intera Blockchain sul proprio device, rappresenta un full node, perché è in grado di controllare sulla blockchain che le informazioni trasmesse nella rete si attengano strettamente al protocollo Bitcoin. I full nodes sono la spina dorsale della rete peer-to-peer di bitcoin, poiché tutti i lite nodes devono rivolgersi ad essi per interrogare la blockchain, così da poter accettare una transazione e riconoscerla come valida. Inoltre, i full nodes spediscono le transazioni ai miners, affinché le registrino sulla blockchain. Maggiore è il numero di full nodes attivi, più la rete è sicura.

Essere un lite node ha un fondamentale vantaggio e uno svantaggio:
– PRO: non è necessario scaricare l'intera blockchain. Questo permette a chiunque di utilizzare i bitcoin in pochi minuti, semplicemente scaricando un'app sullo smartphone
– CONTRO: si è costretti a collegarsi con un full node per confermare qualsiasi transazione

Dato che la blockchain pesa oggi più di 105gb e sono necessarie molte ore per scaricarla, la maggior parte degli utenti non utilizza client come Bitcoin Core, ma semplici wallet che costituiscono nodi lite. Se il numero di full nodes calasse drasticamente, questo rappresenterebbe un rischio. Un attacco hacker DDoS verso i pochi full nodes rimasti potrebbe sovraccaricarli di richieste, invalidando la capacità di comunicare con gli altri nodi, bloccando così l'intera rete Bitcoin.

IL PESO DELLA BLOCKCHAIN CRESCE TROPPO VELOCEMENTE

Oggi (marzo 2017) un comune computer può ancora scaricare l'intera blockchain e costituire un full node, ma col passare del tempo, la blockchain diventa pesante e i costi economici da sostenere per conservare i dati crescono. Dato un blocco di

max 1mb ogni 10 minuti, se ogni blocco è costantemente saturo di transazioni, la Blockchain aumenta di oltre 50gb annui. Raddoppiando o triplicando la dimensione del blocco, risultano 100gb o 150gb in più ogni anno. Se la tecnologia hardware non cresce proporzionalmente (abbattendo i costi per il data storage), questo aumento significa una progressiva diminuzione di full nodes, fino a compromettere la sicurezza del sistema.
Il tema non è limitato esclusivamente alla memoria dati, ma anche alla larghezza della banda. Più il blocco è grande, più dati vengono trasmessi fra i full nodes, e non tutti potrebbero avere sufficiente capacità di banda per sostenere l'aumento del blocco.

Se il Bitcoin continuasse ad avere successo, la rete è destinata a crescere a dismisura. Se solo le transazioni raggiungessero la frequenza di utilizzo di Paypal o Visa, la blockchain crescerebbe esponenzialmente, rimanendo prerogativa di pochi o pochissimi full nodes. Per molti sostenitori di Bitcoin, l'ambizione è quella di rimpiazzare le monete nazionali: prima che come una tecnologia innovativa, vedono il Bitcoin come uno strumento di liberazione sociale, un nuovo paradigma rivoluzionario di matrice libertaria. Se il Bitcoin dovesse rimpiazzare anche l'utilizzo del contante, necessiteremmo di enormi datacenter per memorizzare la blockchain. Per abbattere la rete sarebbe sufficiente colpire pochi centri non difficilmente identificabili.

UNA SOLUZIONE DEFINITIVA AL PROBLEMA DI SCALABILITÀ: IL TRIBUNALE DELLE TRANSAZIONI

La soluzione definitiva al problema di scalabilità del Bitcoin non può essere l'aumento del blocco, questo è un assunto che in pochi mettono in discussione. Chi lo ritiene una soluzione definitiva, sostiene necessariamente una visione del Bitcoin che rispecchia uno di questi due scenari:
A) il Bitcoin non può davvero sostituire i mezzi di pagamento tradizionali, è piuttosto uno strumento destinato esclusivamente ad una piccola nicchia di utenti che non

crescerà mai al punto da costituire una vera forza rivoluzionaria.
oppure
B) il Bitcoin è una tecnologia scalabile, ma che per il suo funzionamento si affida ad alcune (poche) precise entità che custodiscono e aggiornano la blockchain: il sistema non è quindi decentralizzato, o lo è in senso molto limitato.

Per chi non condivide questa visione del Bitcoin, l'alternativa 'attualmente proposta' è solo una: scalare off-chain con la tecnologia Lightning Network. Se LN fosse implementato, la blockchain non sarebbe più utilizzata come registro di tutte le transazioni, piuttosto come un tribunale, cui si ricorre esclusivamente in caso di frode, ovvero quando un utente tenta di registrare sulla blockchain la proprietà di bitcoin che non gli spettano. Le transazioni effettuate saranno ridotte all'essenziale e la blockchain potrà rimanere alla portata di chiunque.

COS'È LIGHTNING NETWORK

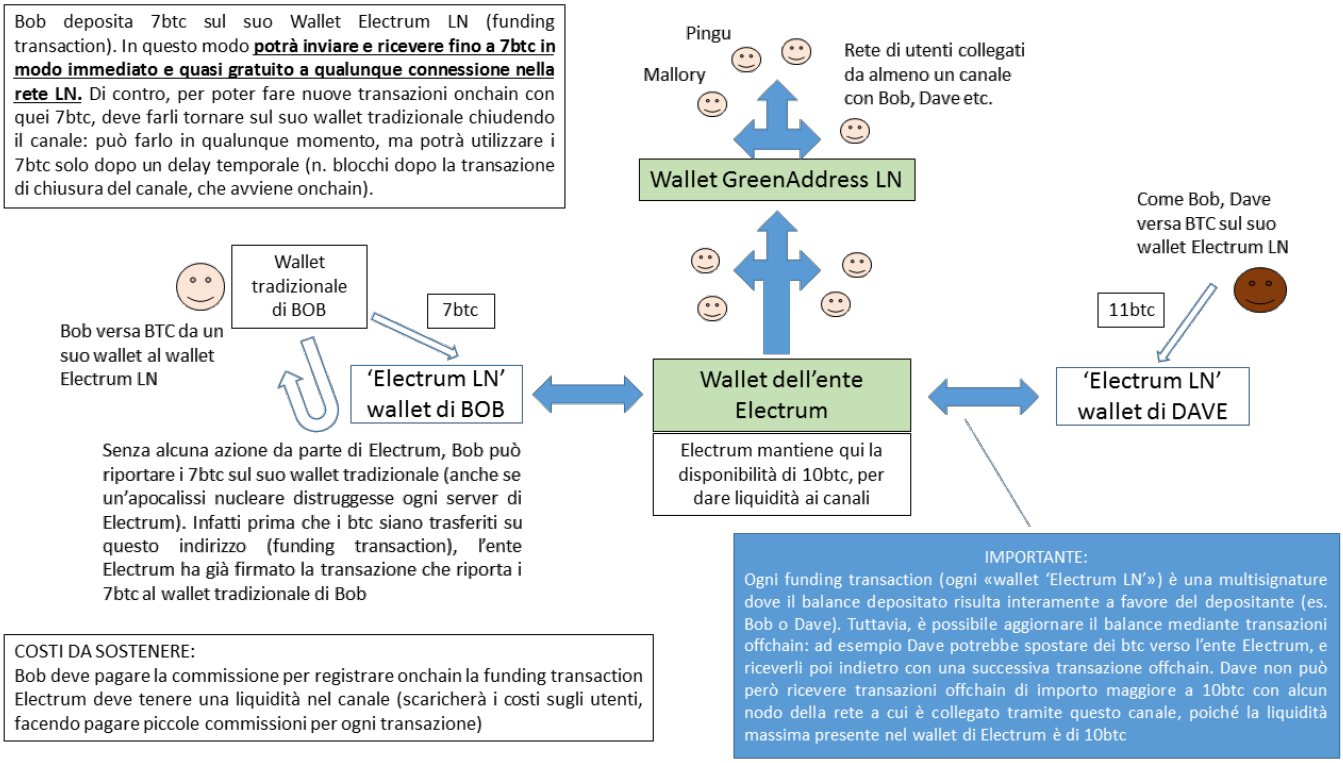
La tecnologia LN è spiegata dettagliatamente nella **sezione dedicata del blog**, disponibile sia in italiano che in inglese:
Per gli utenti meno tecnici, basti leggere il seguente esempio semplificato del funzionamento.

L'utente Bob carica i propri bitcoin su un determinato wallet che supporta la tecnologia LN, che chiamiamo "Electrum LN" (un'ipotetica evoluzione di Electrum). Per farlo si effetta una "funding transaction" multisignature che viene registrata sulla blockchain (onchain), pagando regolarmente le commissioni e attendendo la creazione del blocco dai miner. Questa transazione comporta l'apertura di un "canale" fra Bob ed Electrum LN. Questo "Electrum LN" più che un wallet rappresenta un output non speso (l'output della funding transaction), ma lo possiamo pensare come un wallet perché effettivamente nell'ecosistema LN avrebbe una funzione simile a quello che sono i wallet oggi. Dal momento dell'apertura del

canale, Bob potrà effettuare (offchain) in modo ‘istantaneo’ e ‘quasi gratuito’, qualsiasi altra transazione da e verso quel “wallet” a un altro wallet ad esso collegato, direttamente o indirettamente, attraverso una rete di canali.
Poniamo ad esempio che sia Bob che Dave abbiano Electrum LN. Mallory invece ha il wallet “GreenAddress LN”, che anch’esso supporta la tecnologia Lightning Network. Dato che Electrum LN ha un canale aperto sia con Dave che con Bob, può far fluire i pagamenti da uno all’altro istantaneamente. Essendo sia Electrum che GreenAddress due wallet conosciuti, ovviamente ci sarà un canale stabilito anche fra di essi (entrambi i wallet providers hanno convenienza ad aprire un canale, per fare rete). Perciò per Bob o Dave sarà possibile scambiare in modo istantaneo bitcoin anche con Mallory. L’utente Pingu potrebbe aprire un canale direttamente con Mallory, e finché questo canale rimane aperto (ovvero non viene chiuso con una transazione onchain) potrà effettuare transazioni con tutti gli altri utenti in modo istantaneo.
Gli utenti non devono fidarsi né di Electrum né GreenAddress, né di Mallory. Se una bomba nucleare dovesse farli sparire, ogni utente potrà ritirare i propri bitcoin dal canale, con l’unico inconveniente di dover aspettare un delay temporale prima di poterli riutilizzare (l’entità del delay temporale viene decisa ex ante: ad esempio qualche minuto, o un giorno). Se invece un utente tenta la frode, è possibile per l’utente frodato non solo riappropriarsi immediatamente dei propri bitcoin, ma anche di tutti quelli che l’impostore ha depositato nella funding transaction. Per questo motivo c’è un enorme disincentivo a tentare una frode.

La transazione è istantanea, ma probabilmente sarà solo ‘quasi’ gratuita (anziché gratuita), poiché:
1) il software del wallet deve chiudere il canale qualora uno degli utenti, ad esempio Mallory, provi a barare trasmettendo on chain tutti i bitcoin presenti nel canale (e non solo quelli a lei spettanti). Non è detto che il software esegua questo servizio in modo gratuito.

2) Per evitare che ogni utente debba aprire centinaia di canali con altri utenti per raggiungere potenzialmente ogni nodo della rete, i wallet svolgerebbero la funzione di nodi intermediari per i pagamenti. Per farlo però devono tenere dei bitcoin “bloccati” nei canali e, per svolgere questa funzione di garante della liquidità nel sistema, potrebbero richiedere una retribuzione. Ovviamente, nello stabilire il costo della commissione tali nodi non sono solo in concorrenza l’un l’altro, ma devono essere più economici del costo della transazione onchain.



La tecnologia LN nella teoria è pronta, rimangono da eseguire i test pratici e lo sviluppo di un software (come l’ipotetico wallet Electrum LN) per la chiusura automatica del canale qualora un utente tenti la frode. Tale software non è strettamente necessario, poiché l’utente potrebbe eseguire i controlli e la chiusura in autonomia, ma ovviamente non tutti hanno sempre la prontezza o le capacità tecniche per farlo, né possono costantemente monitorare la blockchain.

COME ATTIVARE LIGHTNING NETWORK: SEGWIT

Affinché si attivi Lightning Network, è necessaria una soft-fork, ovvero un aggiornamento del protocollo bitcoin, chiamato SegWit (Segregated Witness). In passato ci sono state varie soft-fork, che si distinguono da una hard fork poiché non costituiscono una scissione con l'attuale protocollo, ma sono compatibili retroattivamente. Tuttavia è necessario che la stragrande maggioranza dei miners adotti SegWit perché possa funzionare. L'upgrade deve essere, per così dire, plebiscitario.
SegWit non solo permette LN, ma riduce il peso in bytes delle transazioni, aumentando quindi la capacità della rete di sostenere transazioni al secondo. Questo effetto si ottiene in modo assolutamente efficiente, senza che la blockchain venga appesantita, poiché il blocco rimane fisso a 1 megabyte. Secondo alcune stime, l'adozione di SegWit comporterebbe un aumento della capacità del blocco analoga a quella che si avrebbe se il blocco venisse aumentato a 1.7mb. Un puro efficientamento di questo tipo del protocllo potrebbe dare un agio immediato alla rete ora saturata, permettendo transazioni più veloci e commissioni più basse, e avere tempo di preparare il terreno alla tecnologia Lightning Network.

ECCO PERCHE I MINERS NON ADOTTANO SEGWIT

I miners non hanno alcun incentivo economico di breve periodo ad adottare SegWit. Infatti nel blocco di 1mb potranno essere inserite più transazioni, ma la capacità del blocco rimane 1mb e i miners vengono pagati in BTC/byte. Il fatto che in un blocco sia possibile inserire più transazioni significa che gli utenti, a parità di numero di transazioni effettuate, dovranno competere meno l'uno con l'altro per avere una transazione convalidata nel blocco il prima possibile. Per la legge della domanda e dell'offerta, a parità di domanda, maggiore è l'offerta di spazio, minore è il costo. Il che si traduce in una commissione al miner inferiore. Si può vedere il problema da un altro punto di vista: se prima gli utenti pagavano i miner anche per caricare nella blockchain la parte

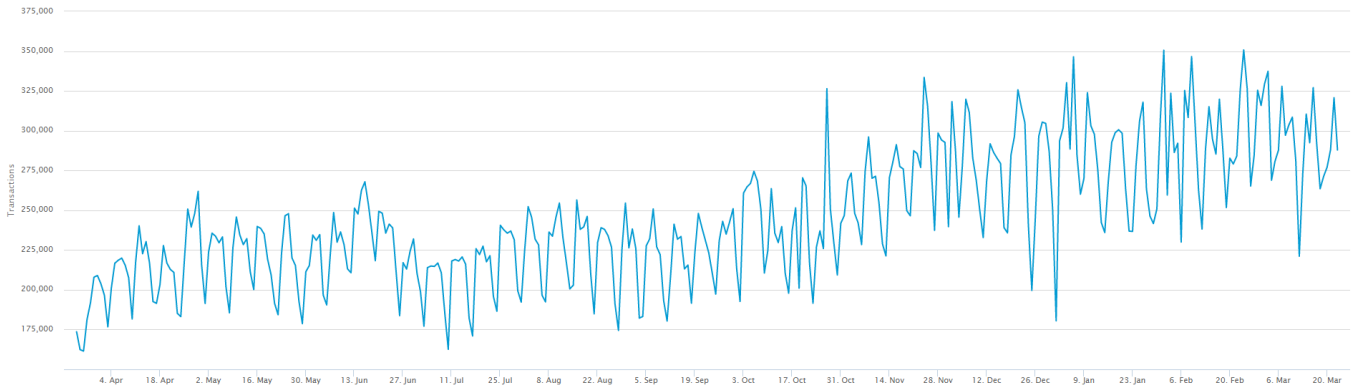
della firma, ora con la firma separata (Segregated Witness appunto) l'utente si libera di quel costo. Oggi quando un miner crea/scopre un blocco guadagna una parte fissa, cioè i 12,5 bitcoin nuovi di pacca, più una parte variabile dovuta alle commissioni sulle transazioni, che potremmo arrotondare grossolanamente a 2 bitcoin. SegWit andrebbe a erodere proprio questa variabile del guadagno del miner.
Non solo, i miners potrebbero anche essere spaventati da Lightning Network, che con SegWit potrà finalmente essere implementato. Potenzialmente, grazie a LN un utente effettua infinite transazioni con l'apertura di un canale, per la quale è richiesta una singola transazione onchain (e un'altra per chiuderlo). Aumentare del 70% la capacità del blocco con SegWit ed aggiungere LN, anche se solo in fase di startup, potrebbe comportare una drastica caduta della parte variabile del miner. Questo spiegherebbe perché SegWit è stata votata solo dal 30% dei miners.

TRATTATI POLITICI: PERCHÈ NON HA SENSO PROPORRE IL "COMPROMESSO" SEGWIT + 2MB DI BLOCCO

Data la difficoltà all'adozione di SegWit, alcuni hanno iniziato a proporre fork che unissero a SegWit un incentivo per i miners, ad esempio un aumento del blocco a 2mb. C'è da considerare però che un aumento del blocco, anche totalmente disgiunto da SegWit, non è detto che costituisca un incentivo economico per i miners. È vero infatti che un blocco più grande permette di guadagnare commissioni da un numero maggiore di transazioni, tuttavia se il blocco è parzialmente vuoto, gli utenti non hanno motivo di tenere alte le commissioni.
Infatti sappiamo che in un anno le commissioni (misurate in bitcoin) sono quintuplicate (decuplicate se misurate in euro o dollaro, dato che il bitcoin ha raddoppiato il valore) a fronte di nemmeno un raddoppio delle transazioni effettuate.

Commissione per byte:

Numero di Transazioni per blocco:



Un aumento del 500% di commissioni a fronte di un 200% delle transazioni è spiegabile solo perché ci siamo avvicinati al tetto massimo di transazioni, riempiendo il blocco di 1mb. Questo significa che se avessimo un blocco da 4mb, riempito solo per tre quarti (3mb) probabilmente pagheremmo delle fee un quinto inferiori, come quelle di un anno fa. I miner quindi avrebbero il triplo delle transazioni da cui attingere, ma che pagano un quinto della fee. I calcoli sono estremamente semplificati, ma il concetto rimane chiaro: il miner nel breve periodo probabilmente perderà il suo guadagno variabile. L'unico caso in cui il miner vince, è quello in cui il blocco aumentato venisse riempito immediatamente, al punto da creare nuovamente quella competizione fra gli utenti che mantiene alte le commissioni.
Sospetto che se fosse approvato oggi stesso un fork con SegWit combinato ad un blocco di 2mb, i miners guadagnerebbero molto meno rispetto a ieri, poiché la capacità totale sarebbe più che triplicata (grazie a SegWit) rispetto a prima e difficilmente il nuovo spazio disponibile nel blocco verrà saturato, nel breve periodo.
Date queste considerazioni, si può concludere che non avrebbe

senso proporre ai miner SegWit combinato all'aumento del blocco, o meglio: non ha senso proporlo con l'intenzione di ingolosire i miners. In un futuro in cui il Bitcoin avrà una diffusione esponenzialmente maggiore rispetto a oggi l'aumento del blocco a 2mb sarà certamente auspicabile, anche con SegWit e LN. Secondo Charlie Lee con LN Bitcoin potrà servire 500 milioni di utenti con 1mb di blocco, anche se al momento è difficile fare qualunque tipo di stima. Non si può negare la bontà dell'upgrade (segwit + 2mb) che prima o poi, guardando speranzosi al futuro del Bitcoin, sarà necessario, ma bisogna comprenderne l'inefficacia come strumento di contrattazione nel venire incontro agli interessi economici dei miners.

ALLA RETE, MINERS COMPRESI, SEGWIT CONVIENE ECCOME

Il costo dei miner è l'hardware e l'elettricità (ed eventualmente, personale, manutenzione e tasse), mentre il ricavo è il bitcoin. SegWit non è profittevole per il miner se ragioniamo in bitcoin, se però l'unità di misura è una moneta fiat, o un paniere di beni, tutto cambia.
Infatti se il Bitcoin rimane una criptomoneta decentralizzata (e quindi il blocco non può aumentare ad libitum, salvo che il progresso tecnologico non faccia miracoli) senza SegWit il valore del Bitcoin è destinato a scontrarsi con un tetto massimo, difficilmente superabile. Quando infatti il blocco è saturo, l'utilizzo di bitcoin viene limitato al punto da escludere nuove transazioni, perché troppo lente e costose, e non attrarrà nuovi entranti nel mercato. Il Bitcoin può continuare per anni a funzionare bene come asset in cui investire e come riserva di valore, può quindi crescere il prezzo, raddoppiare o decuplicare, ma non potrà mai fare il vero salto di livello. A un certo punto le aspettative scemeranno e la tecnologia, pur rimanendo valida per certi applicativi, smetterà di attrarre per la sua forza politicamente e socialmente rivoluzionaria. Verrà smentita la promessa originaria, ovvero che Bitcoin possa essere concepito come moneta. Da quel momento non ci si può aspettare che il

valore salga, al contrario è più probabile che Bitcoin venga progressivamente abbandonato e dimenticato. Salvo che l'approvazione di un ETF o altri eventi di questo tipo portino nuova linfa, potremmo addirittura pensare che il tetto massimo l'abbiamo già toccato ai primi di marzo 2017, e quello che stiamo vedendo negli ultimissimi giorni sembrerebbe confermarlo. Possiamo spostare il "tetto" un po' più in là, con un aumento del blocco a 2, 3 o 4mb, nella speranza che la tecnologia hardware possa sostenere la crescita della blockchain. Ma se manteniamo l'assunto che Bitcoin debba rimanere una criptomoneta decentralizzata, sappiamo che non è possibile spingersi troppo oltre.

Una sola cosa può permettere al valore del Bitcoin di crescere nell'ordine del 1000% o 10.000% come accaduto dal 2009 a oggi: una soluzione definitiva al problema della scalabilità, che tuttavia mantenga la decentralizzazione della rete. SegWit e LN rappresentano questa soluzione. I miners dovrebbero capire che con SegWit i bitcoin guadagnati varrebbero molto di più, ne va della sopravvivenza stessa della moneta nel lungo periodo. Se il miner dovesse continuare a perseguire gli interessi di brevissimo periodo, rischiamo quella combinazione di eventi che Elinor Ostrom chiamerebbe Tragedy of the Commons: nel lungo periodo tutti avrebbero convenienza a "cooperare", ma l'equilibrio simultaneo nel tipico "dilemma del prigioniero" della teoria dei giochi risulta purtroppo in una reciproco "defect". Bisogna convincere i miners che, quando gli utenti si accorgeranno di poter effettuare transazioni a conferma immediata e costi molto bassi, il valore del bitcoin salirà alle stelle. I profitti dal mining di nuovi bitcoin (la coinbase) saranno infinitamente più alti di quanto possano ricavare ora con qualche commissione in più.

Attualmente, ci sono due cose che possono frenare il miner dall'adozione di SegWit:
1) La sfiducia o l'incomprensione verso la tecnologia LN, che effettivamente richiede molto studio per essere compresa, e

non è ancora stata testata.
2) La paura di perdere i propri guadagni variabili nel breve periodo e la convinzione che sia possibile scalare onchain tramite proposte alternative, come Bitcoin Unlimited.

COS'È BITCOIN UNLIMITED

Bitcoin Unlimited permette ai miners di configurare in modo indipendente il volume dei blocchi che convalidano nella blockchain. Il peso del blocco sarà quindi determinato dinamicamente, in base alla convenienza economica del miner. Un blocco troppo piccolo significa lasciare fuori troppe transazioni e quindi ottenere meno commissioni, un blocco troppo grande significa lasciare spazio a un maggior numero di transazioni (potenzialmente tutte quelle avvenute dall'ultimo blocco), che tuttavia pagheranno commissioni minori. Il miner proverà a giocare la sua strategia in modo indipendente, con qualche limite: il parametro "Excessive Block Size" (EB) permette ai nodi di scegliere la dimensione massima del blocco che possono accettare, di default impostata a 16 megabytes. Questo significa che un miner non rischierà blocchi troppo grandi, poiché potrebbero non essere accettati dagli altri miners e il suo blocco verrebbe abortito (perdendo tutto il guadagno generato da nuovi bitcoin e commissioni). C'è comunque un altro parametro, "Excessive Acceptance Depth" (AD), che permette di accettare retroattivamente dei blocchi più grandi di quanto impostato in EB, a patto che una maggioranza di altri miners abbia accettato quei blocchi.
I miners che stanno segnalando di utilizzare Bitcoin Unlimited e hanno scoperto dei blocchi, per il momento stanno continuando a creare blocchi di dimensioni standard 1mb, così che siano accettati da tutti. Nel momento in cui un miner dovesse rischiare un blocco di dimensione maggiore e fosse seguito da altri, si darebbe vita ad una hard fork e due monete diverse, Bitcoin e Bitcoin Unlimited. Gli utenti raddoppieranno i loro Bitcoin, che si troveranno su due diverse fork (due blockchain che hanno una storia in comune),

ma non potranno da quel momento inviare e ricevere bitcoin in modo trasversale fra nuovi blocchi creati in una delle due catene. Se lo facessero non vedrebbero mai la transazione confermata, poiché non accettata dai miners che lavorano in quel ramo. I bitcoin presenti nei blocchi precedenti il fork invece potranno essere inviati in entrambe le catene. I client e wallet si adopereranno per semplificare l'esperienza utente nell'effettuare transazioni, così che l'utente non invii bitcoin da una catena all'altra (la transazione rimarrebbe pending e mai confermata). Il valore misurato in dollari o euro del BTC sommato a BU sarà inferiore a quello del Bitcoin oggi, sia per l'effetto network minore, sia per il panico che probabilmente si scatenerà fra gli utenti, portati a vendere e investire in altri assets (come pare stia già accadendo oggi).

COSA PUÒ SUCCEDERE DOPO IL FORK

Quanto espongo in questo paragrafo sono mere speculazioni e non sono nemmeno lo scenario più probabile. Ma se si verificasse un evento apparentemente tragico come quello qui descritto, invito a vedere le cose in questa prospettiva ottimista.
Mettiamo da parte l'ipotesi per cui si manifesterebbero problemi tecnici e bugs in BU (che non possiamo escludere in toto, visti i precedenti degli ultimi mesi), il cui esito sarebbe una caduta di BU e, forse, la fine. Se al contrario Bitcoin Unlimited tecnicamente dovesse funzionare, non avendo il limite del blocco a 1mb, vedrà probabilmente transazioni più veloci e meno care rispetto a BTC. Possiamo dunque presumere che l'utente medio valuti BU tecnicamente migliore, il quale quindi si apprezzerà rispetto alla controparte. Il prezzo del Bitcoin che affonda rispetto alla concorrenza di Unlimited potrà essere una benedizione. Il valore del Bitcoin sarà così basso che tutto l'investimento hardware ed energetico fatto dai miners non sarà sufficientemente remunerativo. Finalmente, nella disperazione dei miners, non rimarrà che adottare SegWit a plebiscito. L'adozione sarebbe

anche agevolata dal fatto che i miners scissionisti che lavoreranno per la catena Unlimited non avranno più peso nelle decisioni della blockchain Bitcoin core, dove quindi SegWit godrà già di una percentuale di sostenitori ben maggiore rispetto a oggi. Quella che sembrerà la morte del Bitcoin, in realtà sarà il momento della resurrezione. È in quel momento che dovremo comprare e holdare. La superiorità tecnica di Bitcoin non tarderà a manifestarsi, e Bitcoin non si limiterà a tornare ai massimi storici, raggiungerà traguardi mai visti.Iscriviti alla newsletter per ricevere una notifica ad ogni nuovo articolo pubblicato!**SUBSCRIBE**