La battaglia per Bitcoin: una partita a scacchi lunga 6 mesi

La notte del 22 maggio 2017 un articolo su albertodeluigi.com, in anteprima mondiale, riportava i primi rumors su un accordo storico che stava per essere scritto nelle stanze del Marriott Marquis hotel di New York. Qui i più importanti rappresentati di aziende, business e associazioni nel mondo del Bitcoin erano riuniti in occasione del ciclo di conferenze *Consensus 2017.*

Scrissi l'articolo con tono entusiastico, poiché dopo anni di dibattiti, finalmente la stragrande maggioranza di miners appariva favorevole ad effettuare subito il tanto atteso upgrade SegWit, a patto di aumentare il blocksize da 1 a 2mb per raddoppiare la capacità delle transazioni della rete. Da qui il nome della proposta: SegWit2x. Ironia vuole che un accordo abbia portato a 6 mesi di guerra anziché di pace: un

periodo eccezionale di lotte, litigi, gossip, attacchi mediatici, fanatismo, complottismo, scismi e fork.

Eppure, sono stati 6 mesi in cui la community Bitcoin ha dato prova di una grande qualità: l'ecosistema è incredibilmente attivo e ricco di idee, anche in antitesi fra loro. Gli utenti, indipendentemente da quale lato del dibattito si schierino, sono tenacemente aggrappati al proprio ideale di Bitcoin come rivoluzione sociale e liberale, combattendo affinché la tecnologia Bitcoin non si pieghi al controllo di un qualche gruppo di interesse o ideologia corrotta.

Ma per capire tutto ciò, dobbiamo fare un passo indietro, chiarendo anzitutto quali sono i termini del dibattito e se nel mondo delle cryptovalute vi siano delle "classi sociali" contrapposte.

1. IL TRADE-OFF FRA SCALABILITÀ E SICUREZZA

In linea di massima, nel mondo Bitcoin da anni vi sono due ideologie in costante lotta fra loro: big blockers e small blockers, nonostante i secondi non si siano mai definiti così, ma piuttosto come sostenitori della politica di Core. Ad ogni modo, la spaccatura è dettata da una caratteristica del protocollo Bitcoin: il trade-off fra scalabilità e sicurezza.

Se Bitcoin vuole raggiungere una vera adozione di massa, deve poter scalare a migliaia se non milioni di transazioni al secondo. Oggi Bitcoin permette poco più di 3 transazioni al secondo: una transazione pesa mediamente 500bytes e ogni 10 minuti viene creato un blocco in cui viene validato un pacchetto di 2000 transazioni circa. dal peso di 1 megabyte, che è posto come un tetto limite.

Tale limite può essere rimosso semplicemente modificando qualche riga di codice, ma il trade-off sta nel fatto che più grande è il blocco, maggiori sono i requisiti hardware del computer che fa girare un fullnode, che quindi risulta economicamente più costoso. Infatti qualsiasi fullnode deve scaricare e validare ogni blocco, operazione che impegna connessione internet, RAM e molti gigabyte di spazio sull'hard disk per conservare la blockchain (con blocchi da 1mb sono circa 50gb all'anno). Già oggi, inevitabilmente, sul totale di wallets bitcoin i fullnode sono una percentuale molto bassa, poiché sono utilizzati quasi esclusivamente da utenti esperti, appassionati, dalle aziende e dai miners.

Un maggior numero di fullnode significa maggiore decentralizzazione e sicurezza, lo capiamo con un esempio: se i miners adottassero a maggioranza una modifica al protocollo per cui le unità totali di bitcoin diventassero 210 milioni anziché 21 milioni, tutti i più comuni wallets riconoscerebbero valide le transazioni relative ai bitcoin oltre il 21 milionesimo. Solo i fullnode rifiuteranno queste modifiche e non accetteranno i "nuovi" bitcoin. In poche parole, far girare un fullnode permette di difendersi da modifiche sgradite effettuate dai miners stessi.

2. DUE "CLASSI SOCIALI" DISTINTE: MINERS E UTENTI

Come è possibile che gli utenti debbano difendersi dai miners? Si tratta di due stakeholders con interessi diversi e contrastanti? In linea di massima, entrambi guadagnano dal successo del Bitcoin. Anzi il miner ha un interesse molto più

radicato dell'utente medio, poiché ha investito molto in apparecchiature hardware, quindi è anche soggetto a un rischio di impresa.

Una differenza fra miner e utente è che il primo guadagna dalle fee pagate dal secondo, quindi ha un interesse a ottenere la reward più alta possibile dal blocco, mentre l'utente ha un interesse a pagare la fee più bassa possibile. In definitiva, ci sono tre variabili che determinano il guadagno al miner:

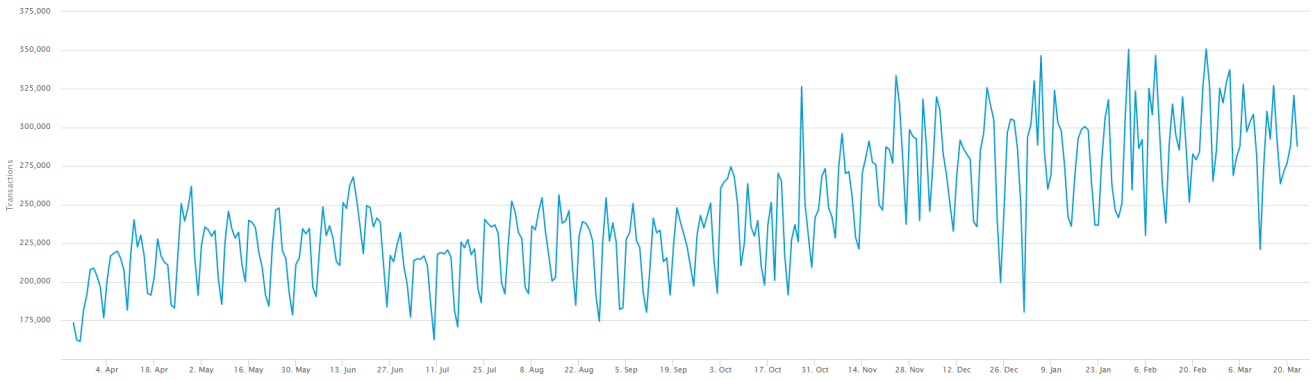
- Prezzo del bitcoin
- Numero di transazioni validate dal miner
- Fee pagata per ogni transazione

Se una di queste tre variabili cresce, a parità delle altre due, il miner ha un guadagno maggiore.

La maggioranza dei miners è da sempre favorevole a un aumento del blocksize, insomma si colloca nella fazione dei big blockers, ma per quale ragione? Avere blocchi più grandi aumenta il numero di transazioni validate (variabile 2), tuttavia abbassa il valore di fee pagata per ogni transazione (3), poiché essendoci più spazio nel blocco, gli utenti devono pagare minori fee per vedersi validate le transazioni. Quale dei due effetti è più rilevante, per cui il prodotto delle due variabili sia massimizzato? Dobbiamo andare ad analizzare il mercato delle fee per scoprirlo.

3. IL MERCATO DELLE FEE: AL MINER CONVIENE UN BLOCCO PIÙ GRANDE?

Guardando allo storico del Bitcoin, quando i blocchi ancora non erano pieni (inizi 2016) notiamo il seguente fenomeno: in un anno le commissioni (misurate in bitcoin) sono quintuplicate (decuplicate se misurate in euro o dollaro) a fronte di nemmeno un raddoppio delle transazioni effettuate (approssimativamente da 200 a 300 mila). Numero di transazioni nella rete:



Costo della transazione:

Un aumento del 500% di commissioni a fronte di un 50% di transazioni in più è spiegabile solo perché ci siamo avvicinati al tetto massimo di transazioni, riempiendo il blocco di 1mb. Questo significa che se, per ipotesi, avessimo un blocco da 4mb anziché 1mb, riempito solo per tre quarti (3mb) probabilmente pagheremmo delle fee un quinto inferiori, come quelle di inizio 2016, perché gli utenti non dovrebbero più competere allo stesso modo per ottenere una transazione validata. I miners quindi avrebbero il triplo delle transazioni da cui attingere, ma che pagano un quinto della fee. Insomma in queste circostanze il miner aumentando il blocco non ci guadagna, ma ci perde.

Tuttavia, se il blocksize venisse aumentato solo moderatamente e i blocchi venissero nuovamente riempiti cosa accadrebbe? Oltre una certa soglia, gli utenti non si spingeranno a pagare fee più alte, piuttosto utilizzeranno altri strumenti per effettuare la maggior parte di transazioni (monete fiat, altre cryptomonete) anziché Bitcoin. Di conseguenza, per ogni incremento unitario nella crescita della mempool, la crescita marginale delle fee sarà sempre progressivamente più piccola.

È probabile quindi che avere un blocco di 4mb con una mempool di pochi megabytes risulterà più conveniente per il miner piuttosto che mantenere un limite a 1mb e una mempool mediamente superiore a 100mb (numeri puramente esemplificativi). In questa nota (apri in finestra separata) ho approfondito la questione con dati e grafici.

Tuttavia, l'obiettivo dichiarato dei big blockers è quello di aumentare il blocksize quanto basti affinché i blocchi non si riempiano mai, e ad oggi è difficile immaginare che le transazioni bitcoin si moltiplichino al punto da riempire immediatamente quattro o otto volte lo spazio attuale. Perciò pensare che la presa di posizione dei miners a favore del blocksize increase sia motivata da convenienza economica è poco credibile, almeno nel breve-medio termine, specie guardando al mercato di oggi delle fee. Nel corso dell'ultimo anno, la dimensione media della mempool è stata di 13mb, con un raddoppio del blocksize si sarebbe probabilmente svuotata, abbattendo il costo delle fee e quindi diminuendo anche il guadagno variabile dei miners nel corso di quest'anno.

Se dunque il guadagno del miner dipende da queste variabili:

- Prezzo del bitcoin
- Numero di transazioni validate (blocksize increase lo aumenta)
- Fee pagata al miner per ogni transazione validata (blocksize increase la abbassa)

poiché la 2) e la 3) hanno effetti contrastanti che si annullano o compensano, il miner probabilmente è favorevole a un aumento del blocco anzitutto perché è convinto che faccia bene al network Bitcoin in generale, quindi che faccia salire il prezzo. Ma il prezzo è anche la variabile, fra le tre elencate, di cui beneficiano in generale tutti gli utenti, perciò da questo punto di vista non c'è un conflitto fra classi di interesse.

In conclusione, l’affermazione che in merito al blocksize debate i miners siano stakeholders con interessi contrastanti a quelli degli utenti non trova convincente evidenza empirica dall’analisi economica del mercato delle fee.

4. IL MINER COME POINT OF FAILURE

Se il miner non ha interessi diversi da quelli degli utenti in merito alla dimensione dei blocchi, perché preoccuparsene? In realtà ci sono altri cambiamenti del protocollo che il miner potrebbe voler implementare per sua convenienza. In generale, tecnologie di transazioni offchain come Lightning Network, possono spostare proventi dai miners ad altri attori, come exchange o wallet providers, e i miners potrebbero sentirsi minacciati e tentare di opporsi. Oppure, un esempio sempre richiamato dai supporters di Core è Asicboost: la tesi è che SegWit sarebbe stato boicottato perché incompatibile con la tecnologia Asicboost che efficienta le risorse impiegate dai miners.

Soprattutto però, i miners sono aziende identificabili e concentrate geograficamente, specialmente in Cina dove vige un regime illiberale. Se lo Stato cinese o una qualsiasi organizzazione volesse controllare o attaccare il network, potrebbe ricattare i miners, o fornire loro incentivi affinché adottino un comportamento che danneggi la rete. Uno Stato o una grossa organizzazione sovra-nazionale potrebbe tentare un 51% attack per approvare modifiche al protocollo Bitcoin, o implementare meccanismi di censura delle transazioni. In effetti, controllare la maggioranza del POW è possibile, poiché il mining è un lavoro altamente competitivo e solo le aziende che riescono a raggiungere la massima efficienza riescono a entrare nel mercato e quindi avere un certo peso “politico” nella segnalazione di upgrade. Questo porta inevitabilmente alla centralizzazione del mining nelle mani di poche aziende. Se questo è un problema, non sono certo da incolpare i miners, quanto piuttosto il protocollo Bitcoin stesso.

Seppur possa preoccupare, ritengo lo scenario di un 51% attack poco probabile. Per quanto controllare buona parte de POW sia possibile, nel momento in cui si sfrutta questa maggioranza per danneggiare il network, l'economia e il mercato si sposteranno verso una POW differente forkando, oppure passando ad un'altcoin. Il tentativo di manipolare il network risulterebbe quindi un esercizio assolutamente dispendioso e si rivelerebbe futile. Come mostrano alcune ricerce, l'energia elettrica consumata per mettere in sicurezza la rete Bitcoin è quella di uno stato di medio-piccole dimensioni e sempre in crescita. Non basta l'energia, bisogna anche sfruttarla con hardware dedicato altamente specializzato, che va acquistato, noleggiato o in alternativa sequestrato con la forza. Uno Stato potrebbe mettere a budget una spesa assolutamente ingente per questo obiettivo, col rischio di non ottenere nulla, se non il dominio su un protocollo tecnologico ormai inutilizzato, poiché gli utenti si saranno spostati altrove. Se anche uno Stato riuscisse ad abbattere una cryptomoneta, non potrebbe mai dominarle e controllarle tutte. Ormai ci sono molti POW diversi, ma anche il concetto di sistema misto di Proof of Work e Proof of Stake e persino monete come IOTA che non hanno nemmeno una blockchain da attaccare mediante Proof of Work. In ogni caso, il 51% attack è l'attacco per eccellenza che Satoshi Nakamoto stesso aveva presentato e analizzato, e Bitcoin dovrebbe funzionare proprio perché questo attacco non è conveniente, per una semplice questione di teoria dei giochi e incentivi economici.

5. DUE FAZIONI: BITCOIN COME ASSET O MONETA?

Da una parte, alcuni utenti si sentono traditi quando i miners non approvano un upgrade ritenuto benefico come SegWit, dall'altra, i miners, il cui lavoro è dedicato alla messa in sicurezza della rete tramite la POW, si sentono accusare di volere controllare Bitcoin, esattamente come farebbe un attaccante malevolo, solo perché sono favorevoli al blocksize increase. Possiamo quindi capire perché non scorra buon sangue

fra le due parti e perché i rapporti si siano esacerbati fino a raggiungere un livello di complottismo e fanatismo da sette religiose. La linea di demarcazione è labile e non esistono dei veri e propri partiti o associazioni, ma possiamo semplificare il quadro in questo modo:

Da un lato vi sono quegli utenti che vedono al momento Bitcoin come un asset (oro digitale) più che una moneta utilizzabile nel quotidiano, e sostengono la politica e la roadmap degli sviluppatori del client Bitcoin Core, molti dei quali sono anche impiegati presso l'azienda Blockstream. Questi utenti accettano di avere costi di trasferimento molto elevati e sono disposti a rimanere in una situazione del genere ancora per anni, finché non viene sviluppata una soluzione diversa rispetto allo scaling onchain. Nonostante riconoscano che sia un bene pagare fee basse, questi utenti affermano che la sicurezza del network, che è molto più importante, risentirebbe gravemente di un aumento del blocco. Perciò avversano un aumento del blocco che non sia quello potenzialmente apportato da SegWit, che una volta raggiunta la massima adozione raddoppia la capacità della blockchain. Probabilmente mantenere il limite al blocco è anche una mossa per spingere con più urgenza aziende e wallet providers ad aggiornare a SegWit, che oggi ha un'adozione di poco più del 10%.

I "Core supporters" si sono lanciati in una campagna particolarmente aggressiva contro l'upgrade SegWit2x (che voleva aumentare il blocksize a 2mb), usando canali come reddit.com/r/bitcoin e twitter (vedi esempio) facendo anche stampare gadgets e cappellini con la scritta NO2X. Il sito bitcoin.org stesso si è lanciato in una campagna selvaggia (al limite del diffamatorio) denunciando 50 aziende e firmatari del NYA, mettendo in guardia i clienti stessi delle aziende, fra cui vi sono alcune delle più grandi e importanti nel mondo Bitcoin: https://bitcoin.org/en/posts/denounce-segwit2x. Questo comportamento ha persino sollevato la reazione

indignata di Andreas Antonopoulos, generalmente vicino all'ideologia di Core, che lo ha definito come un "abuso".

Una frangia ancora più radicale di questa fazione è costituita dagli UASFers, ovvero utenti che volevano lanciare SegWit in UASF (BIP148), senza alcun meccanismo di segnalazione di upgrade e supporto dei miners. Molti degli stessi sviluppatori di Bitcoin Core vedevano UASF BIP148 come una proposta fallimentare e chi la promuovesse come un "pazzo" (vedi)

La fazione opposta invece comprende gran parte dei miners e molte aziende (fra cui i firmatari del New York Agreement) e in generale gli utenti che vedono Bitcoin come moneta digitale (e non come asset), col quale sia conveniente effettuare transazioni bitcoin per qualsiasi tipo di importo, incluso "pagare il caffè". Una frangia più radicale di questa fazione è costituita dai big blockers, i quali asseriscono che la "mania" dei Core supporters per la decentralizzazione della rete è del tutto paranoica, poiché non ci sono rischi concreti nell'aumento del blocksize e, se ci sono rischi, ad esempio un attacco da parte dei miners stessi, sarebbe comunque necessario un fork per proteggersi,e non basterebbe avere un numero elevato di fullnodes. Alcuni big blockers accusano Blockstream di voler distruggere Bitcoin boicottando un aumento del blocco, perché l'azienda è finanziata da Axa e, quindi, dal gruppo Bilderberg. Altri invece accusano Blockstream di essere interessata allo scaling offchain con lo scopo di diventare un grosso intermediario per le transazioni Lightning Network e sottrarre parte del business ai miners.

Non tutti i big blockers hanno sostenuto SegWit2x poiché molti si sono spostati su Bitcoin Cash, una versione di Bitcoin più simile all'originale sviluppato da Nakamoto, priva della tecnologia SegWit e con uno spazio per le transazioni onchain a 8mb, con la promessa di aumentarlo qualora fosse necessario. La nascita di Bitcoin Cash ha senz'altro sottratto molta propulsione al gruppo SegWit2x, poiché costituisce una rottura netta da Bitcoin, mentre il NYA era nato proprio per

conciliare i due estremi.

L’attivismo degli utenti Bitcoin, anche se un po’ guerraiolo, è senz’altro un bene. Su altre crypto si fanno hard fork e upgrade decisi prevalentemente da pochi sviluppatori (Ethereum ha persino modificato il supply) mentre Bitcoin dimostra di essere molto più resiliente: un upgrade per essere adottato senza causare uno split deve dimostrare di avere la quasi-unanimità del consenso, coinvolgendo molti stakeholders diversi: miners, aziende, exchanges, traders, developers, fullnodes economicamente rilevanti, stampa, leader di opinione etc. Tuttavia in tutta questa partecipazione c’è un lato negativo: l’emotività degli utenti prevale spesso contro la razionalità di una scelta più scientifica, come vediamo in particolare con riferimento all’upgrade SegWit2x.

6. 2MB DI BLOCKSIZE NON ACCENTRANO LA RETE

SegWit2x era probabilmente la soluzione più ragionevole per conciliare gli interessi delle due fazioni in campo. Se Bitcoin Core l’avesse appoggiata, probabilmente non avremmo avuto, al primo agosto 2017, né il caso UASF né la nascita di Bitcoin Cash. Possiamo dire che questo articolo sia di parte, poiché albertodeluigi.com era schierato a favore di S2X, ma presto uscirà su questo blog un’intervista speciale a Giacomo Zucco, per fornire anche la visione diametralmente opposta.

Fra le ragioni sollevate contro SegWit2x, si è detto che il blocksize non dovrebbe aumentare a 2mb, poiché i fullnodes necessiterebbero di un hardware più prestante per gestire blocchi del doppio della capacità, col rischio di accentrare la rete. In realtà, possiamo dire con certezza che un blocksize di 2mb non comporta affatto un accentramento della rete, motivo per cui questa ragione non è nemmeno stata sollevata dal team Bitcoin Core (eccetto Luke Dashjr). Un aumento del blocksize a 2mb, con piena adozione di SegWit (la quale si avrà probabilmente solo fra mesi, se non anni) comporta blocchi di circa 4mb. Si presti attenzione ai

requisiti che un fullnode dovrebbe quindi avere:

- Il requisito medio di bandwith per un nodo con blocchi sempre pieni a 4mb è 592kb/s. Oggi le connessioni di rete da 1gb al secondo iniziano a diffondersi in tutto il mondo. Praticamente chiunque abbia un accesso a internet è in grado di sincronizzare la blockchain.
- Un hard disk da 3 terabyte costa 100$, la blockchain con blocchi da 4mb è di 205gb all'anno. Perciò con 100 dollari un utente è in grado di conservare la blockchain per i prossimi 5 anni. E chissà che tecnologia di storage avremo fra 5 anni.
- Un Intel i7 da 2.2ghz può validare circa 4000 transazioni al secondo, mentre un blocco da 4mb contiene 8400 transazioni… ogni 10 minuti!
- I requisiti di RAM sono di circa 512mb per l'attuale blocksize, mentre uno smartphone di ultima generazione ha 6gb di RAM. Sorprendentemente, alcuni Core supporters indicano la RAM come "collo di bottiglia"… forse ignorano i requisiti RAM di un nodo Lightning Network!
- L'orphaning rate dei blocchi è un problema inventato: come dimostra il grafico, non abbiamo blocchi orfanati da giugno 2017, e guardando allo storico, aumentando il blocksize non è affatto aumentato il tasso di orphaning, anzi è diminuito (vedi fonte). Le capacità hardware dell'attuale tecnologia possono chiaramente supportare un blocksize increase moderato mantenendo una buona velocità di propagazione dei blocchi

Insomma, non si capisce perché tutti gli utenti della rete debbano pagare miliardi di fee ai miners per le proprie transazioni, solo perché si vuole garantire a utenti con computer paleolitici di far girare un fullnode, cosa che molto probabilmente non farebbero comunque. Chi avesse un pc poco adeguato potrebbe tranquillamente permettersi i soldi di un upgrade del pc solo considerando quello che risparmia in minori fee sulle transazioni.

Ci sono altre ragioni sollevate contro SegWit2x, ma vale la pena riassumere il corso degli eventi nel dettaglio, fino alla decisione di sospendere il fork.

7. L'EPOPEA SEGWIT2X

Il 24 maggio esce il **comunicato ufficiale** sull'accordo, detto "New York Agreement", firmato da 58 aziende. Successivamente alcune aziende si aggiungeranno, mentre altre si ritireranno da agosto in poi, come la mining pool F2Pool (col 10% di hashrate).

L'upgrade era pensato in due parti: approvazione di SegWit subito e l'aumento del blocksize a 2mb (il 2x) entro 6 mesi. Il blocco del fork è stato poi effettivamente minato il giorno 17 Novembre (anche se ormai l'upgrade era sospeso).

In breve tempo l'85% circa dei miners (salito al 95% a luglio) inizia a scrivere nella coinbase dei blocchi minati la sigla NYA: New York Agreement, segnalando così di essere intenzionati a perseguire l'upgrade accordato (vedi la voce di glossario: segnalazione di upgrade)

Su github viene quindi sviluppato un software di riferimento per l'upgrade: Btc1, che è un fork del client Bitcoin Core. SegWit2x prende ufficialmente vita con la Bitcoin Improvement proposal BIP91, che viene votata dai miners a luglio con maggioranza schiacciante. BIP91 prevede due passaggi:

- Adottare BIP144 (SegWit) entro agosto, forzandone la segnalazione tramite BIP91.
- Aumentare il blocksize a 2mb dal 494784esimo blocco (si è poi scoperto, dopo che SegWit2x è stato abbandonato, che il software effettuava il fork al block height 494783, poiché contando il genesis block, esso è effettivamente il 494784esimo blocco, **vedi nota**)

Fino ad agosto sembra andare tutto bene: BIP91 ottiene la quasi unanimità e SegWit, che prima dell'accordo di New York

poteva contare solo su circa il 30% del consenso (espresso in blocchi minati), viene finalmente approvato.

Nonostante questo successo, c'è chi si oppone forsennatamente a SegWit2x sin dal mese di maggio, quindi già nei primissimi giorni dalla pubblicazione della proposta e i sostenitori di S2X vengono bersagliati in modo talebano. Questo avviene nonostante il team di Bitcoin Core, pur avanzando delle riserve, non si fosse ancora schierato apertamente e unitamente contro l'upgrade. Anche il blog albertodeluigi.com è stato preso di mira da quando, il 29 maggio, a 5 giorni dalla pubblicazione della proposta del NYA, uscì questo articolo che spiegava l'accordo e perché rappresentasse un'ottima soluzione per Bitcoin (è ancora attuale, per chi lo volesse leggere). http://www.albertodeluigi.com/2017/05/29/accordo-barry-silbert-consensus-2017/

In seguito sono state chiarite le ragioni contrarie all'hard fork di novembre anche da parte degli sviluppatori di Bitcoin Core:

- L'aumento del blocksize a 2mb non è una ragione sufficiente per giustificare un hard fork non retro-compatibile col principale client fullnode del network. In caso di hard fork consensuale infatti tutti i nodi Bitcoin Core, per funzionare secondo il nuovo protocollo, avrebbero dovuto necessariamente fare l'upgrade e 6 mesi sono un preavviso troppo scarso.
- Non è accettabile implementare un upgrade proposto da una parte della community riunita senza che i principali sviluppatori di Bitcoin Core partecipassero alla discussione. In effetti, anche se invitati, i Core dev si erano rifiutati di partecipare adducendo come motivazione che le condizioni poste erano troppo restrittive. Di fatto, dato che le fee in costante aumento sono percepite come un'urgenza da risolvere per molte aziende e utenti, gli organizzatori del meeting

(Barry Silbert) avevano richiesto che i partecipanti non concludessero la riunione senza che fosse stata trovata una soluzione condivisa.

Personalmente, ritengo queste motivazioni molto deboli. Chiunque con mesi di anticipo ha tempo di effettuare l'upgrade e anche se qualche utente mancasse all'appello, non appena effettua la prima transazione non va in porto, si accorge del fork e scarica il nuovo client. Il fatto poi che Core fosse presente o meno alla riunione è poco rilevante: la parte tecnica su "come" sviluppare il client si effettua a posteriori della decisione politica, quindi non c'era nulla di tecnico da discutere il 22-24 maggio.

È stata sollevata anche una presunta ragione "tecnica" contro SegWit2x, ovvero:

- L'upgrade è fatto troppo in fretta poiché 6 mesi (da fine maggio a metà novembre) sono troppo pochi per testare ed effettuare un fork con un aumento del blocco a 2mb

Questa ragione è sempre stata molto debole, nonostante le polemiche postume sui "bug" del client Btc1. Come spiegato nella già **citata nota**, che tratta nel dettaglio le critiche mosse al client, non si può parlare di veri bug, ma solo di una grave svista sul numero del blocco del fork. Svista che, a parte la figuraccia, non avrebbe avuto alcun effetto bloccante: il fork si sarebbe fatto comunque senza problemi. È vero che Btc1 ha avuto una review scarsa e non è stato testato al meglio, ciononostante questo non dipende dal fatto di avere avuto "solo" 6 mesi per svilupparlo e testarlo: il codice era già pronto a luglio dopo poco più di un mese. In tempi molto più stretti si è svolto il fork di Bitcoin Cash: rilasciato il 1 luglio, la decisione di forkare il 1 agosto è stata presa due settimane prima. Inoltre lo split è stato fatto in una situazione molto difficile, data la scarsa potenza di calcolo a sostegno e un EDA mai testato in una situazione reale, dove

vi sono agenti economici che rischiano di incorrere in perdite spendendo in potenza di calcolo.

8. LA FINE DI SEGWIT2X

A settembre era chiaro che il fork di Bitcoin Cash avesse avuto successo e il valore non sarebbe calato a zero, nonostante la quantità di BCH dumpabili da parte degli holder di Bitcoin. Perciò il fronte dei big blockers aveva ormai un nuovo riferimento, tanto che il miner più importante della rete, Jihan Wu (Bitmain) ha iniziato a pagare i propri dipendenti con Bitcoin Cash, considerandolo "il vero Bitcoin". Anche la feroce propaganda NOS2X ha molto smorzato la forza motivazionale dietro a SegWit2x, tanto che le aziende latitavano a far sentire la propria voce a favore dell'upgrade, probabilmente anche per paura di ripercussioni sul proprio business. Un esempio su tutti è l'annuncio ambiguo di Bitwala, che tentava di imbonirsi entrambi i fronti. La denuncia di bitcoin.org da "caccia alle streghe" deve aver fatto effetto, mentre l'organizzatore del meeting di maggio, Barry Silbert, non si è più fatto sentire sull'argomento S2X, dopo un tweet in cui affermava che avrebbe preso una pausa da twitter poiché l'atmosfera era troppo ostile (i NO2X non hanno mai usato toni gentili). Insomma il fronte S2X si è fatto intimidire ed è venuta a mancare una comunicazione efficace e una leadership o un riferimento che trascinasse compatte le aziende e i miners fino all'upgrade. Senza comunicazione, nonostante la segnalazione dei miners fosse chiaramente a favore di S2X, gli utenti erano confusi e non era chiaro quali miners avrebbero mantenuto fede alla segnalazione, mentre gli exchanges principali non si sbilanciavano né da una parte né dall'altra. Su piattaforme come Bitfinex era possibile scommettere su una catena o l'altra (SegWit2x come BT2 e la legacy come BT1). I volumi erano bassi e splittare i propri bitcoin per tradare subito i futures era una pessima mossa strategica, poiché significava perdere l'occasione di poter dumpare o pumpare la catena favorita nel momento cruciale del

fork. La propaganda politica e l'esistenza di servizi come 2xdumper.com (per facilitare gli utenti a vendere i coin S2X) facevano pensare a una probabile distorsione dei prezzi in favore della legacy (il fronte pro Core), perciò non si poteva sapere quanto i futures rispecchiassero i valori reali, ma in ogni caso davano in grandissimo vantaggio la catena legacy e come "exit poll" non erano sicuramente incoraggianti per il fronte S2X.

Il colpo mortale probabilmente è arrivato da parte di ViaBTC, la quarta mining pool più grande al mondo con quasi il 15% di hashrate. Storicamente ViaBTC è un'azienda collocabile nello schieramento dei big blockers, anzi è anche stata la prima mining pool a sostenere Bitcoin Cash e a scommettere sulla sua catena sin dal primo agosto. Tuttavia il CEO Haipo Yang il primo novembre 2017 dichiara: "non abbiamo ricevuto dagli utenti richiesta di segnalare 2x. Se 2x sopravvive e gli utenti la richiedono, supporteremo entrambe le catene" (vedi fonte)

Senza ViaBTC, SegWit2x sarebbe partito con al massimo un 70% di hashrate, quindi alla legacy sarebbe rimasto oltre un 30%, abbastanza per sopravvivere.

A quel punto la situazione appariva critica e a 15 giorni dal fork intervengo io stesso nel dibattito ufficiale su SegWit2x, ovvero la mailing list su linuxfoundation, aprendo la sezione di novembre. Nella mail richiedo che per procedere all'upgrade sia necessaria una nuova dichiarazione firmata dalle aziende del New York Agreement, poiché per proseguire non solo è necessaria potenza di fuoco (l'hashrate dei miners, il sostegno delle aziende), ma anche una comunicazione efficace, altrimenti l'incertezza della situazione avrebbe potuto portare gli utenti più ingenui anche a perdere soldi.

[Bitcoin-segwit2x] Require a new Statement from NYA companies

mail at albertodeluigi.com mail at albertodeluigi.com
Wed Nov 1 23:55:37 UTC 2017

- Next message: [Bitcoin-segwit2x] Require a new Statement from NYA companies
- **Messages sorted by:** [date] [thread] [subject] [author]

In order to safeguard the community from an undesired chain split, the upgrade should be overwhelming, but it's not enough. It should also 'appear' as overwhelming. People, businesses and services needs to be certain about what is going to happen and the risks if they won't follow. My impression is that still too many speaking english people in the western world think the upgrade will be abandoned before or immediately after block 494784 is mined, thus they are going to simply ignore it. That could lead to unprepared patch up and confusion, while naïve users risk to harm themselves.
For this reason and for the sake of the Bitcoin community as a whole, we need to show again, clearly and publicly the extent of the support to SegWit2x. We also need to commit ourselves in a widespread communication campaign. I know this is not a strict technical matter, but it could help a lot avoiding technical issues in the future.

What we have to do:

First, we need a new statement from the original NYA signers and all the business, firms and individuals who joined the cause later. That statement should be slightly different from the original NYA though, and I am explaining why.
We all know that what Bitcoin is will be ultimately determined by market forces, comprehensive of all the stakeholders involved: businesses, miners, users, developers, traders, investors, holders etc. Each

Alla mia mail, che potete leggere per intero qui, segue un lungo dibattito (si veda al link: https://lists.linuxfoundation.org/pipermail/bitcoin-segwit2x/2017-November/date.html) in cui partecipano anche membri di Core e Blockstream:

Per dare un quadro della situazione, queste sono alcune delle persone partecipanti allo scambio di mail:

- Adam Back – è CEO di Blockstream e autore di Hashcash, opera citata da Satoshi Nakamoto nel White Paper di Bitcoin
- Jeff Garzik – ex Core developer e primo dev di SegWit2x, oltre che CEO di Bloq
- Mike Belshe – CEO di Bitgo.
- Charlie Shrem – cofondatore di BitInstant e passato alla storia come un simbolo nel mondo Bitcoin, poiché imprigionato per due anni negli USA per operazioni di trasmissione del denaro illecite (in bitcoin ovviamente) collegate agli affari di Silk Road (anche se il vero simbolo e "martire" della storia rimane certamente Ross Ulbricht, alias Dread Pirate Roberts).
- Luke Dashjr non è intervenuto pubblicamente, ma mi ha scritto in privato.

Come sottolineato nell'immagine, io mi impegno in vari interventi: ad esempio in **questa mail** spiego perché l'esito del fork è incerto e che la vittoria di una o l'altra catena dipende principalmente da come si comportano i traders nelle primissime ore o giorni dal blocco 494783 (teoria dei giochi spiccia).

Proprio dopo una mia ultima mail, arriva finalmente, da parte di Mike Belshe, un nuovo "statement" da parte di alcuni dei firmatari di S2X, anche se diverso da come ce lo aspettavamo: l'upgrade è sospeso. Vale la pena riportare per intero la mail (vedi sotto) di Mike Belshe, firmata da altri 5 personaggi. Anzitutto però, è bene soffermarsi sulle firme in calce, per capire come possano 6 persone sole poter sospendere l'upgrade da un giorno con l'altro.

Mike Belshe è CEO di BitGo, compagnie che offre un servizio di wallet multisignature molto diffuso, poiché fa o ha fatto da supporto a diverse aziende molto importanti, ad esempio gli exchange Kraken e Bitfinex, ora gestisce i wallet di Bitstamp, Bitbay, Okcoin, Unocoin, Genesis.

Wences Casares è CEO di Xapo, la più famosa carta di debito in Bitcoin, oltre che webwallet e "banca" per gli utenti Bitcoin. Fa anche da exchange per altre importante aziende come Bitwala che si appoggiano a Xapo.

Jihan Wu è il nome più importante della lista. Alla guida di Bitmain, azienda produttrice di Antminer, i più efficienti ASIC della rete (per ora), controlla Antpool, la più grande mining pool al mondo, nonché altre pool minori ed ha partecipazioni in importanti aziende come ViaBTC (mining pool ed exchange). Le sole mining pool di Jihan Wu controllano oltre il 30% dell'hashrate mondiale. Un suo ritiro da SegWit2x significava, in data 8 novembre, una diminuzione drastica dell'hashrate portando i "voti" a favore di SegWit2x a circa il 50%, mentre l'accordo di New York prevedeva una soglia dell'80%. Insomma gli altri miners con una soglia così bassa

non avrebbero mai osato creare uno split della rete.

Jeff Garzik è uno storico sviluppatore di Bitcoin Core. Come Gavin Andresen e Mike Hearn, ha partecipato allo sviluppo di Bitcoin sin dal 2010, scambiando anche messaggi privati con Satoshi Nakamoto stesso. Tutti e tre sono stati poi "allontanati" dal gruppo di Bitcoin Core per divergenza di vedute proprio sul tema blocksize. L'ultimo dei tre a vedere revocati i suoi committ access alle repository github di Bitcoin Core è stato proprio Garzik, dopo che ha deciso di guidare lo sviluppo di Btc1. È l'utente con la maggior parte di commitment su github per lo sviluppo del client Btc1 di SegWit2x.

Peter Smith è CEO di Blockchain Luxembourg S.A, l'azienda più semplicemente nota come Blockchain. Blockchain.com è il webwallet con più utenti al mondo (20 milioni di wallet registrati), numeri che fanno invidia persino a Coinbase (che però è anche exchange). Inoltre il sito blockchain.info è largamente il più utilizzato blockexplorer e punto informativo per tutti i bitcoiners del mondo. Insieme a coin.dance e albertodeluigi.com è senza dubbio uno dei tre siti di riferimento per la community internazionale (trovate l'intruso).

Erik Vorhees è CEO di ShapeShift, uno dei principali exchange esclusivamente fra cryptomonete (senza passaggi in fiat money)

Di seguito la mail:

"The Segwit2x effort began in May with a simple purpose: to increase the blocksize and improve Bitcoin scalability. At the time, the Bitcoin community was in crisis after nearly 3 years of heavy debate, and consensus for Segwit seemed like a distant mirage with only 30% support among miners. Segwit2x found its first success in August, as it broke the deadlock and quickly led to Segwit's successful activation. Since that time, the team shifted its efforts to phase two of the project

– a 2MB blocksize increase.

Our goal has always been a smooth upgrade for Bitcoin. Although we strongly believe in the need for a larger blocksize, there is something we believe is even more important: keeping the community together. Unfortunately, it is clear that we have not built sufficient consensus for a clean blocksize upgrade at this time. Continuing on the current path could divide the community and be a setback to Bitcoin's growth. This was never the goal of Segwit2x.

As fees rise on the blockchain, we believe it will eventually become obvious that on-chain capacity increases are necessary. When that happens, we hope the community will come together and find a solution, possibly with a blocksize increase. Until then, we are suspending our plans for the upcoming 2MB upgrade.

We want to thank everyone that contributed constructively to Segwit2x, whether you were in favor or against. Your efforts are what makes Bitcoin great. Bitcoin remains the greatest form of money mankind has ever seen, and we remain dedicated to protecting and fostering its growth worldwide.

Mike Belshe, Wences Casares, Jihan Wu, Jeff Garzik, Peter Smith and Erik Voorhees"

Parole più belle per chiudere l'articolo non ne troverei, quindi mi limito a tradurre la frase conclusiva della mail:

"Vogliamo ringraziare chiunque abbia contribuito costruttivamente a SegWit2x, sia che foste a favore o contro. Il vostro impegno è ciò che rende grande Bitcoin. Bitcoin rimane la migliore forma di denaro che l'umanità abbia mai visto, e noi rimaniamo dedicati a proteggerla e a promuovere la sua crescita in tutto il mondo".

Amen

ISCRIVITI ALLA NEWSLETTER DI ALBERTODELUIGI.COM PER RICEVERE UNA NOTIFICA AD OGNI ARTICOLO PUBBLICATO. **CLICCA QUI**