Da Nakamoto all’Hard Fork: la storia del Bitcoin, gli upgrade, la politica, gli aneddoti

scritto da Alberto De Luigi | 17 Luglio 2017

Nell’articolo si ripercorre alcuni passaggi fondamentali della storia di Bitcoin. Analizzando come avviene un upgrade del protocollo, l’articolo permette di comprendere le dinamiche sottostanti a un fork e a uno split della rete. In calce è presente un album fotografico dove sono presentati alcuni dei principali protagonisti dell’ecosistema Bitcoin citati nell’articolo

Per i lettori meno esperti: alcuni concetti o particolari potrebbero non essere di facile comprensione. Qualora si incontrino difficoltà nella lettura, o per rinfrescare i retroscena, si suggerisce di partire da questi articoli:

– Cosa sta succedendo al Bitcoin: tutte le spiegazioni (articolo del 25 marzo 2017)

– Considerazioni a caldo sull’upgrade SegWit2x (articolo del 21 giugno 2017)

Indice dei contenuti:

1) La nascita del software bitcoin

2) Blockchain fork: come avviene un upgrade del software e del protocollo bitcoin
(e come avviene uno split della rete)

3) Lo split imprevisto della rete per il fork dell’11 marzo 2013

4) Un unico software: a single point of failure

5) Segwit vs blocksize increase: la battaglia per il controllo di bitcoin?

6) Soft fork vs hard fork: quando la distinzione non vale

7) L'espressione del voto politico e delle intenzioni di upgrade

8) Threshold: la soglia di voto da raggiungere per l'upgrade

9) 1 agosto: il fallimento certo del fork bip 148 "uasf"

10) Chi sostiene uasf bip 148?

11) Nemici di bitcoin: sono i miners o chi li vuole licenziare?

12) La rete bitcoin sta passando sotto al controllo di pochi?

13) Segwit2x (btc1): la soluzione condivisa

14) Le prossime date e scadenze

15) Segnali di trading

16) I volti dei protagonisti

1) LA NASCITA DEL SOFTWARE BITCOIN

Nel 2008 inizia a circolare in rete il White Paper dell'anonimo Sataoshi Nakamoto: *Bitcoin: a peer-to-peer electronic cash system*. Presto viene pubblicata la prima release di un software, il client Bitcoin, sviluppato da Nakamoto stesso, il quale si occuperà della programmazione del software fino alla versione 0.3.19. Mentre la teoria è frutto di un lavoro privato, il software è stato sviluppato con la collaborazione della community online. Fino al 2010 il ruolo principale di developer è stato ricoperto da Satoshi stesso e

da Sirius (il finlandese Martti Malmi). Le conversazioni a margine dello sviluppo del client sono pubbliche e tutt'oggi rinvenibili sul forum *bitcointalk*, dove si possono ancora leggere i post di Nakamoto stesso. Al seguente link potete vedere l'utenza di Satoshi, registrata in data 19 novembre 2009: https://bitcointalk.org/index.php?action=profile;u=3

Sostituendo il numero in fondo all'url, troverete un altro utente. Il 3 significa che Nakamoto è il terzo membro registrato sul form, mentre il quarto è Sirius. Il primo membro è l'utenza di admin, il numero 2 non esiste più.

Presto molti altri utenti e sviluppatori si sono uniti al forum, costituendo una community internazionale particolarmente attiva. Anche dall'Italia, Franco Cimatti (nickname HostFat), ora presidente della *Bitcoin Foundation Italia*, già nel 2010 offriva il suo contributo testando il software. La prima traduzione in lingua del client Bitcoin è stata proprio l'Italiano, per cui vediamo Satoshi esultare con un post:

Dalla versione 0.3.19 del client, Nakamoto ha smesso di occuparsi del software, lasciando alla community la gestione. In modo spontaneo, si è creato un gruppo di lavoro aperto, che da allora propone nuovi aggiornamenti di quel software, il quale più tardi prenderà il nome di *Bitcoin Core* (ora alla

versione 0.14.2).

2) BLOCKCHAIN FORK: COME AVVIENE UN UPGRADE DEL SOFTWARE E DEL PROTOCOLLO BITCOIN
(e come avviene uno split della rete)

Bitcoin Core è oggi (ai primi di luglio 2017) il software usato dall'85% dei nodi. Stiamo parlando di fullnodes, ovvero i nodi che costituiscono l'ossatura della rete e scaricano l'intera blockchain. Non consideriamo quindi i più comuni wallet litenode (come quelli su smartphone) che pur permettendo di effettuare o ricevere pagamenti, devono necessariamente interfacciarsi con un fullnode per fare transazioni. Ovviamente, Bitcoin Core non è l'unico software per client full node Bitcoin. Altri software infatti seguono lo stesso protocollo, pur essendo differenti o sviluppati con un linguaggio diverso.

Un upgrade del software dei full nodes può in certi casi comportare un aggiornamento del protocollo. Alcuni miglioramenti infatti si possono fare solo cambiando le regole fondamentali che caratterizzano l'essenza del Bitcoin. Molte di queste regole sono considerate sacre e immutabili, ad esempio la quantità massima di Bitcoin esistenti al mondo, definita a quasi 21 milioni (per la precisione 20.999.999,9769 BTC), ma in realtà qualsiasi regola è potenzialmente modificabile, se c'è un consenso sufficiente da parte delle persone che compongono la rete.

Ad esempio chiunque potrebbe cambiare il protocollo aumentando il numero di Bitcoin possibili, basterebbe modificare poche righe di codice in un client Bitcoin. In Bitcoin Core:

```
CAmount nSubsidy = 50 * COIN;

If (halvings >= 64)

return 0;
```

```
nSubsidyHalvingInterval = 210000;
```

Tuttavia una modifica di questo tipo risulterà incompatibile con tutti i software utilizzati dal resto della rete. Non potrò mai inviare o ricevere il 21 milionesimo Bitcoin, perché il resto della rete non ne accetta l'esistenza. Essenzialmente, ci sono tre passaggi richiesti affinché una modifica al protocollo abbia successo.

1. Se sia Alice che Bob scaricassero il client Bitcoin Core modificato e Alice mandasse una transazione a Bob, il software di Bob la considererebbe valida, perché il suo è lo stesso client che usa Alice. Il primo passaggio, il riconoscimento da utente a utente (da nodo a nodo), avviene dunque con successo.

2. Il secondo passaggio è la registrazione di questa transazione nella blockchain, il registro pubblico di tutte le transazioni, da parte dei miners. Se i miners hanno un software non compatibile, la transazione fra Alice e Bob non sarà accettata. Tuttavia Bob (o Alice, o una terza persona) potrebbe ovviare a questo problema, installando un software per il mining modificato in modo tale che accetti il nuovo protocollo. Così, Alice e Bob potranno fare transazioni fra di loro senza problemi, vedendole convalidate nella blockchain. Anche il secondo passaggio dunque pare essere effettuato correttamente: l'inserimento della transazione nel registro pubblico blockchain.
C'è però un problema: questo registro non sarà la stessa blockchain usata come riferimento da tutto il resto della rete, bensì un suo "fork", o biforcazione, proprio perché il miner per convalidare la transazione ha usato un software modificato. La nuova blockchain registra delle transazioni (fra Alice e Bob) che tutto il resto della rete, rimasta "fedele" al protocollo originale, non riconoscerà come Bitcoin.

3. Quindi un terzo passaggio è necessario affinché una modifica al protocollo abbia effetto per l'intera rete: che il

nuovo software sia adottato da tutti (o comunque da una maggioranza). Utenti e miners devono quindi deliberatamente scaricare e installare un software che sia compatibile con quello proposto da Alice e Bob, spostandosi all'unanimità sul nuovo fork della blockchain (da questo punto di vista, il fork è sinonimo di upgrade).

Ricapitolando: una modifica del protocollo deve avere le seguenti caratteristiche:

– deve essere riconosciuta da altri nodi

– deve essere riconosciuta dai miners

– nodi e miners che la riconoscono devono essere la maggioranza

Qualora queste condizioni non si verifichino, si può ottenere uno dei seguenti scenari:

A. L'upgrade non ha effetto (una minoranza fa l'upgrade, il resto della rete non segue questa scelta, la minoranza quindi rinuncia e fa roll-back al vecchio software)

B. Si crea una nuova moneta. Nonostante l'upgrade non sia accettato dalla maggioranza, la minoranza potrebbe essere determinata a portare avanti il progetto. Questa minoranza potrà pretendere che la moneta si chiami "Bitcoin", ma il resto del mondo non la riconoscerà come tale.

C. Se la catena Legacy (quella originale) e la catena che segue il nuovo protocollo avessero entrambe un forte supporto da parte di utenti e miners, la blockchain potrebbe dividersi e il Bitcoin spaccarsi in due. Si creerebbe una situazione assolutamente confusionaria e deleteria, dove gli utenti non vedono più validate le transazioni e i meno preparati tecnicamente rischieranno di non riuscire più a recuperare i propri Bitcoin. Gli exchange avranno probabilmente una fase di stallo dove si dovrà decidere quale delle due blockchain

considerare il vero Bitcoin. Il prezzo di mercato vedrebbe un crollo, etc.

Nella situazione B e C il fork è permanente (o comunque di lungo periodo) ed è dunque la causa di uno split della blockchain, per cui la community si spacca e ci sarà chi preferirà utilizzare la blockchain legacy (quella originaria) e chi la nuova blockchain che ha effettuato il fork.

Fatta questa breve parentesi teorica, ora vedremo cosa è accaduto nella storia degli upgrade di Bitcoin, e cosa accadrà nel futuro più prossimo.

3) LO SPLIT IMPREVISTO DELLA RETE PER IL FORK DELL'11 MARZO 2013

L'upgrade dalla versione di Bitcoin Core 0.7 alla 0.8 scatenò uno split della rete il giorno 11 marzo 2013. La nuova release di Core includeva una modifica a bitcoinid, il software più utilizzato dai miners. Questa modifica doveva essere un semplice aggiornamento che migliorasse l'efficienza nei tempi di sincronizzazione della blockchain, implementando il LevelDB database. Tuttavia, ciò di cui gli sviluppatori di Core non si erano accorti è che il nuovo db introduceva accidentalmente una modifica nelle regole del protocollo. Il vecchio database BerlekelyDB della versione 0.7 infatti aveva un limite (nel numero di "locks" simultanei) non presente nella più efficiente versione 0.8. Per questa ragione, il primo blocco creato da un miner con software 0.8 che superava quel limite provocò un fork: inconsapevolmente, i miners con il vecchio software 0.7 hanno continuato a costruire la catena di blocchi partendo dall'ultimo blocco 0.7 creato, mentre la blockchain dei miners con software 0.8 prendeva un'altra direzione. Essenzialmente, si veniva a profilare un sistema monetario in cui esistono due diversi (e col tempo sempre più discordanti) database (blockchain) che registrano quanti soldi ha una determinata persona. Ovviamente la situazione richiedeva un

rimedio urgente, perciò tutti i miners, servizi ed exchange sono stati contattati chiedendo di fare un rollback alla versione 0.7, e in sole 6 ore l'ordine è stato ripristinato.

In quel breve periodo di 6 ore, c'è testimonianza di almeno una persona che sia riuscita a sfruttare il bug della release di Core: questo utente ha depositato due volte gli stessi btc sul servizio online OKpay, che gli ha accreditato quindi il doppio dei soldi. I bitcoin sono stati depositati una volta sulla catena 0.7 e una volta sulla catena 0.8. OKpay, vedendo entrambe le transazioni confermate dai miners, ha accreditato doppiamente la somma. Normalmente, i servizi come OKPay si coprono dal rischio di "double spending" attendendo 6 conferme, ovvero la creazione di 6 blocchi consecutivi sulla stessa catena, il che è eccessivamente prudente, in tempi normali. Tuttavia in questo caso (unico nella storia della blockchain) il fork è durato per ben 25 blocchi.

Questo evento storico fa riflettere su alcuni temi importanti di cui trattiamo ora.

4) UN UNICO SOFTWARE: A SINGLE POINT OF FAILURE

Uno dei rischi maggiori per la rete Bitcoin è che esista un solo software usato dalla stragrande maggioranza della rete. Al contrario, maggiore è il numero di software diversi che seguono lo stesso protocollo, meno rischi ci sono che un aggiornamento abbia conseguenze impreviste. Ad esempio, se l'ecosistema di clients Bitcoin fosse stato molto più vario nel marzo 2013, l'aggiornamento sbagliato avrebbe colpito solo i miners con software bitcoinid di Core, e di questi solo quelli che avrebbero già eseguito l'upgrade alla 0.8. Quindi nel complesso di tutti i clients esistenti nella rete, i nodi intaccati sarebbero stati una minoranza di poco conto. Meno miners coinvolti significa meno hashpower (potenza di calcolo), di conseguenza, sarebbe anche stato molto più difficile che questa minoranza avesse sufficiente potenza per

minare ben 25 blocchi in circa 6 ore.

I client Bitcoin hanno un meccanismo automatico di sincronizzazione con la catena più lunga (poiché è quella che ha più probabilità di essere quella valida, riconosciuta da tutta la rete) che si chiama "**blockchain reorganization**" (reorg): ovvero il client rifiuta blocchi che prima considerava validi e li sostituisce, facendo il download dei blocchi della catena maggioritaria. Se ci fosse un fork di una catena con poco hash power, quindi con blocchi che vengono scoperti raramente, i client riconoscerebbero presto la catena più lunga, operando un reorg e scongiurando una spaccatura della rete Bitcoin. Non si protrarrebbe insomma una situazione confusionaria con due catene di simile lunghezza dove è difficile identificare quale sia quella valida. Va precisato che il blokchain reorg non funziona sempre qualora una catena sia più lunga: i client devono anche riconoscere la catena come compatibile col protocollo. Nel caso del fork menzionato, il protocollo della 0.8 era incompatibile col software bitcoind (per il mining) della 0.7, ma non col software dei client (i wallet full nodes) degli utenti. Per questa ragione qualsiasi client poteva riconoscere l'una o l'altra catena come valida. Il reorg generalmente opera in caso di soft fork, ma non hard fork, perché un client legacy non riconoscerebbe la catena che ha fatto upgrade come valida anche se questa fosse più lunga, dal momento che non è compatibile con le regole del protocollo legacy. Se così non fosse, per assurdo la blockchain Bitcoin potrebbe essere vittima di reorg da parte della catena Litecoin, o altre monete nate come fork di Bitcoin.

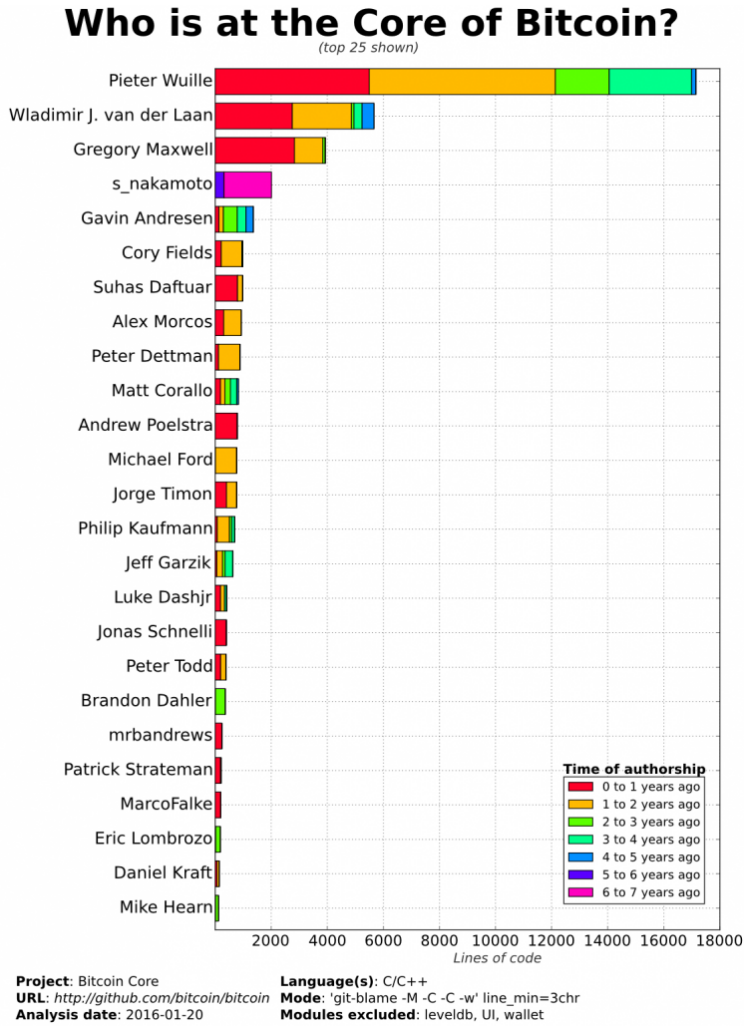
Da un certo punto di vista, potremmo pensare che avere molti software e team di sviluppo diversi possa aumentare la probabilità di incorrere in errori tecnici. Questi errori tuttavia non avrebbero impatti sistemici, poiché ogni singolo client girerebbe su una minoranza dei nodi della rete rispetto alla totalità dei nodi che usano altri client. Clients che non

seguono il protocollo verrebbero così presto individuati dalla rete e isolati. Chi facesse girare un nodo "corrotto" si renderebbe presto conto del problema, poiché non riuscirebbe a inviare e ricevere la maggior parte delle transazioni, e farebbe immediatamente un aggiornamento. Oltre a Bitcoin Core, ci sono vari software per full nodes Bitcoin, in sviluppo o in produzione: Bitcrust, Bitcore, bcoin, bitcoinj, btcd, parity-bitcoin, Bitcoin Unlimited, Bitcoin XT, Bitcoin Classic, btc1. Oggi l'85% dei nodi fa ancora girare Bitcoin Core e molte delle implementazioni alternative sono ancora in fase di test o sono delle copie di Core parzialmente modificate, ma già esistono clients scritti in un linguaggio diverso, come bcoin e bitcore (javascript), btcd (Go) o bitcoinj (java). L'ecosistema dal 2013 ai giorni nostri sta costantemente maturando e diversificandosi, garantendo sempre più una maggiore sicurezza. Quando i nodi Bitcoin Unlimited sono crashati il 15 marzo 2017, la maggior parte degli utenti bitcoin non ha nemmeno sentito nominare la notizia. Chi si è accorto dell'incidente, probabilmente è solo perché ha letto qualche sfottò da parte degli sviluppatori degli altri clients.

Bisogna poi notare che il fatto che la maggioranza di nodi usi lo stesso client non significa che la maggior parte dei flussi economici passi per un unico tipo di client. Se ad esempio i più importanti exchanges o servizi online (wallets, e-commerce) costituissero solo l'1% dei nodi, ma in questi nodi passassero moltissime transazioni, basterebbe avere una distribuzione eterogenea di clients diversi all'interno di questo 1% di nodi per avere già un ecosistema molto variegato. Per esempio, oggi Coinbase ha 27.5 milioni di wallets e Blockchain.info 15 milioni. Se dal 16 luglio in avanti solo queste due aziende passassero a btc1, il client dell'upgrade SegWit2x, potremmo affermare che un'enorme fetta dell'ecosistema Bitcoin si è spostato su un client diverso rispetto a Core, nonostante i nodi di Core rimangano circa l'85% sul totale.

Una maggiore differenziazione dei software Bitcoin significa anche decentralizzazione, poiché il software non è uno e non è mantenuto principalmetne da un unico team. Questo favorisce anche una maggiore resilienza al cambiamento del protocollo, quindi un elemento in più a garanzia di stabilità e sicurezza. Infatti, seppur Bitcoin Core sia sviluppato in peer review e chiunque in rete possa partecipare allo sviluppo, solo un team ristretto di persone ha il commit access alle repository.

Questo significa che una ristrettissima cerchia di persone potrebbe proporre alla rete un client con codice malevolo sotto al nome di prestigio Bitcoin Core, inducendo gli utenti meno esperti a installarlo sulla fiducia. Ovviamente il team di Core non avrebbe motivo per fare una cosa del genere, ma possiamo sempre ipotizzare scenari limite in cui, ad esempio, il team venisse preso in ostaggio. Inoltre, potrebbero sorgere dei conflitti di interesse, specialmente considerando che molti dei developers di Bitcoin Core sono impiegati presso un'unica azienda: Blockstream. Il grafico sotto mostra i principali autori di implementazioni e modifiche al software Bitcoin Core (ordinati per numero di righe di codice scritte, che non è un indicatore esauriente, ma comunque significativo dell'importanza dello sviluppatore). L'azienda Blockstream impiega i seguenti dev, tutti presenti nel grafico: Pieter Wuille, Gregory Maxwell, Matt Corallo, Andrew Poelstra, Luke Dashjr, Patrick Strateman. Non credo in scenari complottistici, ma ovviamente questo dettaglio fa molto discutere fra i principali stakeholders del mondo del Bitcoin. Secondo alcune fonti, pare che in Cina molti utenti (forse influenzati dai miners cinesi?) credano che l'upgrade SegWit, proposto dal team di Core, sia addirittura un tentativo delle corporations occidentali di prendere controllo del Bitcoin.



5) SEGWIT VS BLOCKSIZE INCREASE: LA BATTAGLIA PER IL CONTROLLO DI BITCOIN?

La questione su possibili conflitti di interesse del team di Core e Blockstream è spesso sollevata nella battaglia politico-ideologica che si sta combattendo sul tema sulla scalabilità: le principali mining pool nel mondo sono cinesi, e hanno un vantaggio economico a scalare onchain. Al contrario, aziende come Blockstream (statunitense), che raccolgono l'eccellenza degli sviluppatori nel mondo, propongono soluzioni di scalabilità offchain e potrebbero (ma c'è un alto grado di aleatorietà) riuscire a guadagnare grandi somme grazie all'intermediazione nel mercato offchain. Per poter scalare offchain è necessario l'upgrade SegWit, che separa la parte della firma della transazione (quella dove

usiamo la nostra chiave privata per autorizzare il trasferimento) dal resto dei dati della transazione. Questo fatto permette la creazione di una rete di payment channels, detta Lightning Network, che è attualmente l'unica soluzione conosciuta per permettere a Bitcoin di scalare, ovvero di avere un'adozione e uso di massa senza che i costi di gestione della rete e di transazione per gli utenti siano enormi. Data l'importanza di SegWit, da oltre un anno la community tenta di fare approvare l'upgrade ai miners, proponendolo in varie salse, fra cui BIP141 (l'originale SegWit), BIP148 (l'UASF del primo Agosto), BIP91 (che è parte dell'upgrade SegWit2x). Finalmente, i miners hanno confermato il sostegno a una di queste proposte, BIP91 che avverrà a fine luglio, in anticipo su BIP 148 e quindi evitando un possibile chain split. Su questo upgrade i miners avevano preso accordo a New York il 23 maggio, in seduta comune con varie aziende e alcuni sviluppatori (il team di Core non ha partecipato).

Come discusso in altri miei articoli, l'unico modo per ottenere veramente la scalabilità del Bitcoin è offchain, tuttavia anche aumentare in modo contenuto la capacità onchain può essere di notevole aiuto (e senza particolari rischi di accentramento – spiegati qui), soprattutto in queste prime fasi in cui la rete offchain Lighning Network deve ancora diffondersi. Per questo sostengo l'upgrade SegWit2x. Su scalabilità e Lightning Network ho dibattuto in altri articoli e non affronto nuovamente la questione qui.

Un altro elemento che ha fatto discutere è la scelta del team Bitcoin Core di proporre l'upgrade SegWit in soft fork, con un codice molto complesso, piuttosto che in hard fork, dove il codice sarebbe molto più semplice e quindi facilmente interpretabile anche da utenti meno tecnici. La semplicità del codice è un obiettivo importantissimo: lunghe sessioni di test possono risolvere molti problemi, ma chi si occupa di informatica sa bene che si verificano quasi sempre circostanze impreviste. Più il codice è complesso, maggiori sono le

possibilità di errore. Una maggiore complessità fa crescere la diffidenza di alcuni utenti che hanno già preconcetti negativi nei confronti del team di Core, alimentando quindi sospetti e scontri ideologici fra diverse fazioni (chi è schierato a favore di SegWit e chi a favore di un aumento del blocksize). Probabilmente, SegWit oggi è del tutto sicuro (implementato su Litecoin funziona a dovere), ma sviluppi futuri del protocollo, o comunque di applicazioni dell'ecosistema Bitcoin, dovranno scontrarsi con una sempre maggiore complessità nell'approcciare il codice. Dall'altro lato però, anche la scelta di optare per un soft fork ha un valore aggiunto ed è un obiettivo importante da perseguire. Colgo l'occasione per aprire una parentesi tecnica spiegando quale sia la differenza fra hard e soft fork.

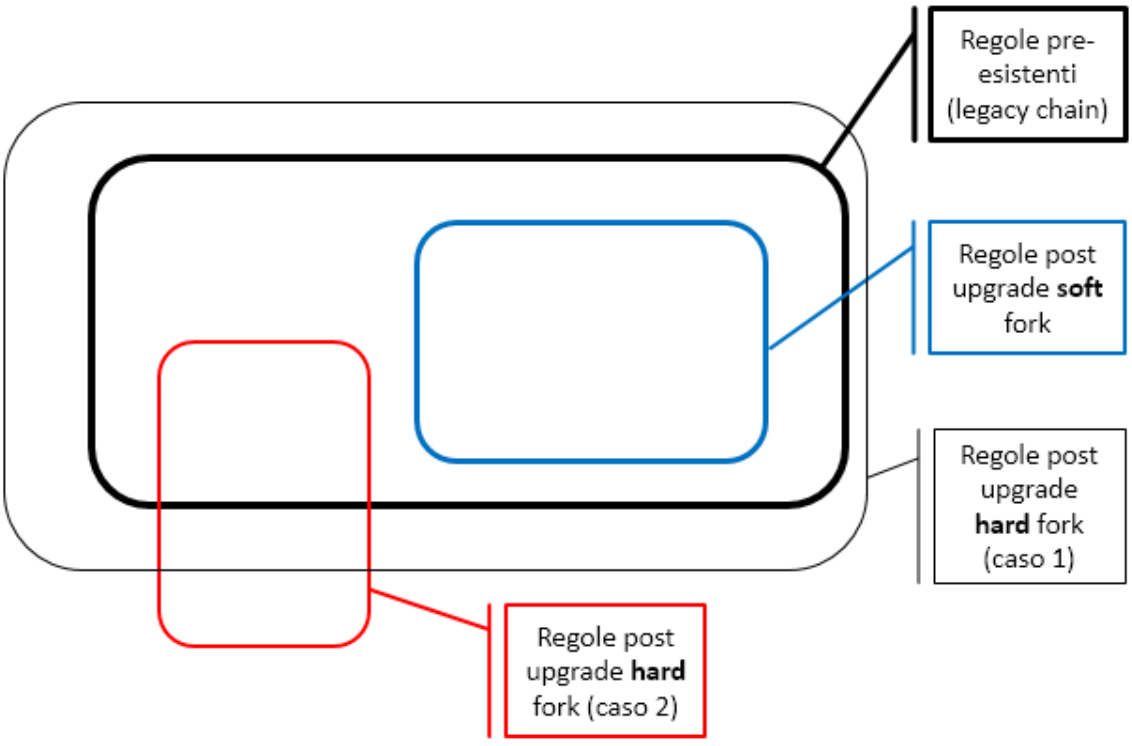
6) SOFT FORK VS HARD FORK: QUANDO LA DISTINZIONE NON VALE

Le definizioni di hard fork e soft fork sono varie e non sempre perfettamente coerenti. Entrambi sono un cambiamento del protocollo che potrebbe condurre a uno split della catena. L'unico modo per evitare lo split, è avere sufficiente consenso da parte della community sulle nuove regole del protocollo.

Un esempio di hard fork è la creazione di blocchi maggiori di 1mb (blocksize). In questo caso, il fork può essere visto come un rilassamento delle regole del protocollo (caso 1 nel grafico), poiché si allarga il protocollo ad alcune possibilità prima negate, ovvero l'esistenza di blocchi maggiori di 1mb. In altri casi che possiamo immaginare, l'hard fork potrebbe comportare allo stesso tempo una restrizione di alcune regole e un allargamento di altre (caso 2). Ad ogni modo è sicuramente vero che **l'hard fork rende validi blocchi di un certo tipo che erano prima invalidi**.

Definire un soft fork è più difficile, poiché ci sono definizioni non del tutto coerenti fra loro, come vedremo a

breve. Secondo alcune teorie, è una modifica che comporta esclusivamente un restringimento delle regole del protocollo. Un esempio è l'introduzione al limite alla dimensione del blocco (blocksize): Fino al luglio 2010 non c'erano limitazioni al peso dei blocchi, ma nella versione 0.3.1 rc1 del client Bitcoin è stato impostato un tetto massimo a 1mb, senza una particolare discussione in merito. A quei tempi le transazioni bitcoin erano ben lontane dal possibile raggiungimento di quel tetto e non si prevedeva che quella scelta sarebbe stata al centro di un terremoto politico. Ad ogni modo, tornando alla teoria diciamo che il soft fork rende invalidi blocchi che prima potevano essere validi (tutti quelli con peso superiore a 1mb), perciò restringe le possibilità permesse dal protocollo. Per tornare allo stadio precedente al soft fork, è sempre necessario un hard fork (nel caso in esame, che rimuova il limite al blocksize).



In caso di soft fork, a differenza di un hard fork, vecchie versioni del software riconoscono come validi i blocchi della chain generati col nuovo software. La ragione è mostrata nel grafico in modo semplice: i blocchi post soft fork sono un

sotto-insieme di quelli possibili nella catena originaria (o legacy). Per questo motivo, spesso si dice che il soft fork sia retro-compatibile, anche se lo è solo in senso molto stretto. Infatti, supponendo che il traffico di transazioni fosse già stato elevato nel 2010, possiamo immaginare che se alcuni miners avessero creato blocchi di oltre 1mb dopo l'upgrade, si sarebbero potute creare due blockchain, con un effettivo split. A onor di cronaca, va specificato che ai tempi della 0.3.1 la limitazione a 1mb non era stata afatto percepita come fork, poiché nessun nodo o blocco creato da un miner sarebbe stato rifiutato: il traffico di transazioni era molto limitato e non esistevano sufficienti transazioni per riempire i blocchi oltre a quella soglia.

Abbiamo (per ora) definito **soft fork** tramite queste caratteristiche:

(1) Una modifica che restringe le regole del protocollo, rendendo invalidi blocchi che prima erano validi

(2) Una modifica per cui vecchie versioni del software riconosceranno i blocchi e le transazioni generati da nuove versioni del software (retrocompatibilità)

there are "soft" rule changes and "hard" rule changes. "Soft" changes tighten up the rules– old software will accept all the blocks and transactions created by new software, but the opposite may not be true. "Soft" changes do not require the entire network of miners and merchants and users to upgrade or be left behind.

"Hard" changes modify the rules in a way that old, un-upgraded software consider illegal. At this point it is much, much more difficult (some might say impossible) to roll out "hard" changes, because they require every miner and merchant and user to upgrade.

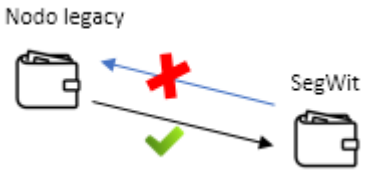
(Gavin Andresen, Bitcoin Core maintainer, 2012, vedi qui)

Tuttavia, se le definizioni date sono valide, il soft fork più famoso del momento, l'upgrade SegWit, non può essere considerato un soft fork. L'upgrade a SegWit era stato progettato come hard fork, ma con un po' di ingegno nel team di Core sono riusciti a trasformarlo in una soft fork, almeno secondo una specifica definizione di soft fork:

(3) Una soft fork è una modifica del protocollo a cui si converge nel momento in cui la maggioranza di hash power la adotta

"A softfork is defined as a consensus change that converges as long as majority of the hashrate adopts it"
(Pieter Wuille, Bitcoin Core maintainer, Blockstream co-founder, vedi qui)

SegWit non ha le stesse caratteristiche di un soft fork come quello finora descritto sulla limitazione del blocksize. Con SegWit la parte della firma non viene più inclusa nel blocco (blocksize), ma viene scambiata dai nodi a parte, in un pacchetto dati separato. A livello di transazione fra nodo e nodo, i nodi vecchi non vedono questo pacchetto dati separato, quindi non riescono a ricevere transazioni di tipo SegWit (non vedendo la parte della firma dove si aspettano di trovarla, ovvero nel blocksize). Questo invalida la definizione (2): il vecchio software non riesce a ricevere transazioni del nuovo tipo. Anche se i nuovi nodi Core sono progettati sia per effettuare transazioni a firma separata SegWit sia vecchie transazioni di tipo legacy e quindi possono inviare bitcoin anche a nodi non SegWit, non possono farlo se i bitcoin da spedire si trovano in un output di tipo SegWit (cioè ricevuti da una precedente transazione SegWit). Se si tentasse la transazione, questa restituirebbe un errore: missing witness



data.

La definizione **(2)** andrebbe quindi rivista. Non è più vero che la soft fork è:

(2.a) *Una modifica per cui vecchie versioni del software riconosceranno **le transazioni** generate da nuove versioni del software (retrocompatibilità)*

Infatti le vecchie versioni del software non riconosceranno **alcune delle possibili transazioni** generate da nuove versioni del software

Tuttavia le vecchie versioni del software riconosceranno **i blocchi** generati dai miners SegWit, anche se questi blocchi contengono output SegWit che non sono riconosciuti dai nodi legacy (suona strano, ma è così). Quindi la soft fork rimane:

(2.b) *Una modifica per cui vecchie versioni del software riconosceranno **i blocchi** generati da nuove versioni del software (retrocompatibilità)*

Questo fatto è importante, perché significa che la rete può accettare i blocchi SegWit come la propria blockchain, e non un (hard) fork incompatibile, come se fosse la blockchain di un'altra moneta, ad esempio Litecoin.

Nel merito della definizione **(2.b)**, va fatta però una precisazione:

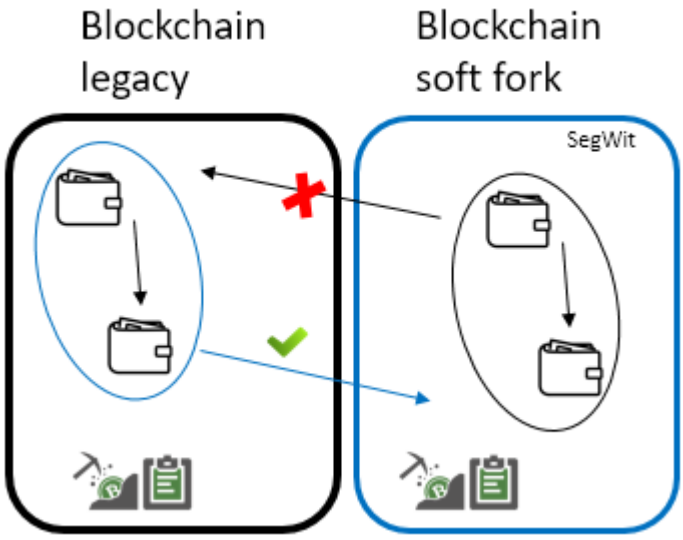
– **il software dei nodi riconoscerà i blocchi** generati da nuove versioni del software (seppur non possa accettare alcune delle transazioni provenienti da output proprio di quei blocchi: quelle provenienti da output segwit)

– **il software dei miners legacy non riconoscerà i blocchi** creati dai miners SegWit

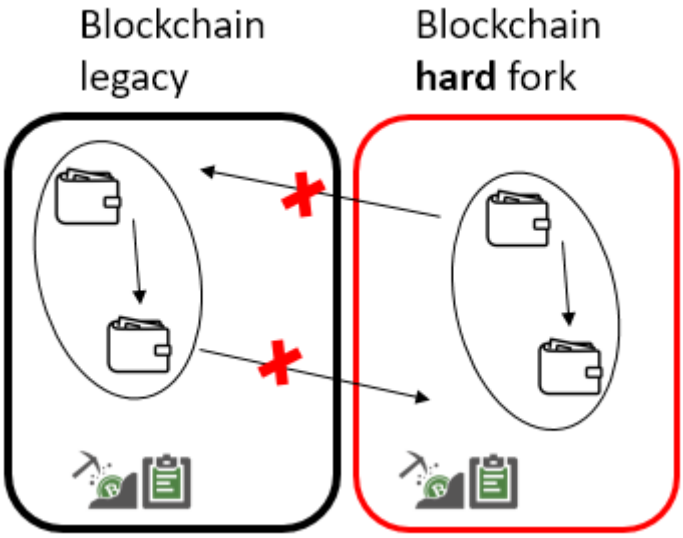
Quest'ultimo fatto è fondamentale, ed è ciò che mette a rischio di split la blockchain. Infatti, se solo una parte dei miners fa upgrade, si creano due catene inconciliabili: la catena legacy escluderà qualsiasi blocco che abbia almeno una

transazione SegWit.

Infine, dobbiamo rivedere anche la definizione **(1)**, per cui affermavamo che il soft fork rende invalidi blocchi che prima erano validi. In effetti, la catena SegWit può includere tutti i tipi di blocchi che oggi sono considerati validi nella catena legacy (vedremo perché bisogna precisare "oggi"). Qualsiasi transazione che oggi viene validata nella catena legacy potrebbe essere validata anche nella catena SegWit, mentre non vale il contrario (perché i miners legacy non ammettono transazioni SegWit).



In caso di Hard Fork la catena che fa upgrade non avrebbe



questo vantaggio:

Si tratta di vantaggio per un motivo preciso: la catena che fa upgrade può validare nella blockchain tutti i tipi di transazione, potendo così "accontentare" sia gli utenti che vogliono usare client legacy, sia gli utenti che vogliono usare client SegWit.

In definitiva, se SegWit è legittimamente un "soft fork", le definizioni **(1)** e **(2)** di soft fork sono poco precise, se non sbagliate. Conviene utilizzare la definizione di Wuille:

(3) una soft fork è una modifica del protocollo a cui si converge nel momento in cui la maggioranza di hash power la adotta (Pieter Wuille)

> A softfork is defined as a consensus change that converges as long as majority of the hashrate adopts it. Yes, a non-witness transaction spending a segwit output without signature would be valid to old nodes, but 1) they won't see that (such a transaction is nonstandard to everyone) 2) such a transaction won't be mined (same as 2) and thus 3) the majority chain will not accept such transactions. – Pieter Wuille May 16 at 17:40

Se la maggioranza dei miners accetta Segwit (scaricano un software compatibile), tutte le transazioni (legacy e SegWit) saranno approvate nella catena SegWit e i client (anche quelli legacy) faranno "reorg", riconoscendo quest'ultima come l'unica valida. Questo è il meccanismo di "blockchain reorganization" di cui trattato **sopra.** La particolarità di questa caratteristica (e che la differenzia da un generico hard fork) è che qualsiasi client, legacy o SegWit, riconoscerà come blockchain valida solo la catena SegWit, scartando l'altra, in qualunque momento la catena SegWit supererà in lunghezza quella legacy (ovvero quando avrà maggiore hashpower e lavoro da parte dei miners). In caso di reorg, nel momento in cui tutti i client della rete riconoscono SegWit come la catena valida, la catena legacy muore. Viceversa, se la catena SegWit non supererà in lunghezza la legacy, quindi non raggiungerà mai il sostegno della maggioranza di miners e hashpower, verrà probabilmente abbandonata.

Per finire, bisogna segnalare un'ultima e importante

sfaccettatura: abbiamo detto che la catena SegWit accetta blocchi con tutti i tipi di transazione che vengono effettuati oggi, anche quelli legacy, ma questo fatto *potrebbe* non essere vero in futuro. Infatti i vecchi nodi legacy non vedono la parte della firma delle transazioni SegWit, quindi vedono i bitcoin che sono output di transazioni SegWit come "di nessuno". Se dei bitcoin sono di nessuno, te ne puoi appropriare, facendo una transazione di tipo legacy (aggiungendo quindi la parte della firma) e mandandoli verso un tuo indirizzo: questa caratteristica degli output SegWit è conosciuta come "anyone can spend". La possibilità di sfruttare l'"anyone can spend" mette a rischio la catena che fa soft fork, se non ha la maggioranza dell'hashrate. Infatti una transazione legacy che sfrutti un output anyone can spend è compatibile con il protocollo legacy e può essere quindi validata dai miners all'interno dei blocchi della catena legacy, permettendo il "furto" dei bitcoin presenti in qualsiasi output SegWit. Ovviamente i miners della catena SegWit in "soft fork" non potranno mai accettare blocchi in cui compaiono transazioni che spendono a proprio piacimento i bitcoin degli utenti con client SegWit (in effetti derubandoli), di conseguenza rifiuteranno quei blocchi. In effetti quindi SegWit renderebbe invalidi dei blocchi che in base al protocollo legacy sono validi e la definizione (1) di soft fork che avevamo dato torna valida.

Su Litecoin, dove è stato approvato SegWit, nessuno ha mai sfruttato la caratteristica "anyone can spend", perché un blocco che includa una transazione di quel tipo creato da un miner verrebbe orfanato, ovvero rifiutato dalla totalità degli altri miners, che supportano le attuali regole di consenso all'unanimità (tutti hanno approvato SegWit). Nessun miner quindi spenderebbe soldi e tempo convalidando bocchi in cui ci sono transazioni che rubano soldi dagli output SegWit. Ma se non c'è un vasto supporto "politico" all'upgrade, non si possono garantire le stesse condizioni. In definitiva, suona come uno scherzo, ma se SegWit non avesse la maggioranza di

hashpower si avrebbe una situazione per cui: un nodo potrebbe accettare un blocco, ma non accettare di ricevere output da transazioni SegWit di quel blocco; output che tuttavia potrebbe tentare di spendere (rubando i bitcoin), pur rispettando il protocollo (legacy), e rimanendo quindi nell'incertezza se questa transazione verrà validata o meno dai blocchi successivi dei miners, sapendo che se venisse validata si creerebbe uno split della blockchain, che non si saprà quanto durerà e quanto catastrofico potrà essere sull'intero ecosistema.

7) L'ESPRESSIONE DEL VOTO POLITICO E DELLE INTENZIONI DI UPGRADE

Situazioni catastrofiche nel sistema Bitcoin non si sono mai verificate. Questo anche grazie ad un softisticato sistema di "voto politico", per cui viene espressa una preferenza nei confronti di un upgrade. Generalmente, solo quando una proposta è condivisa alla quasi unanimità, si procede all'upgrade. Quando in Italia siamo passati dalla Lira all'Euro, non tutti erano d'accordo con la scelta politica. Ma quando ormai era inevitabile che si sarebbe fatto il passaggio, anche i più strenui difensori dello status quo si sono dovuti rassegnare e accettare l'Euro. Se qualcuno si fosse tenuto le lire pretendendo di utilizzarle come moneta, magari sarebbe riuscito a continuare a scambiarle all'interno di una comunità ristretta, ma di certo il fenomeno non sarebbe stato un problema a livello di sistema né avrebbe potuto minare la solidità dell'Euro. Nel Bitcoin funziona allo stesso modo: immaginiamo il protocollo Bitcoin come il taglio e la stampa di una certa banconota. La banconota ha valore solo perché c'è consenso fra i cittadini (e le istituzioni che questi formano) che quella stampa rappresenti esattamente una moneta con quello specifico valore. Nel momento in cui abbiamo deciso che la Lira non valeva più niente, è diventata carta straccia, e le *consensus rules* che stanno alla base del

“protocollo” sono state modificate: “accettare solo banconote con scritto sopra Euro”.

Nel 2012 gli sviluppatori di Core hanno formulato una proposta di miglioramento di Bitcoin, il BIP 34 (Bitcoin Improvement Proposal numero 34), per cui si è stabilito un metodo sofisticato di “segnalazione” della volontà di fare l’upgrade da parte della rete. Questo metodo è stato poi perfezionato con BIP9 nel 2015.

Il funzionamento è il seguente: i miners segnalano l’intenzione di aderire a una proposta di cambiamento del protocollo tramite il blocco creato, che viene inserito nella blockchain e propagato alla rete insieme a un dettaglio importante: un messaggio inserito nel “block version”, ovvero in una stringa di 32bit. Ad esempio:

```
Version field: 00001000 00000000 00000010 00000000
                  ^      ^           ^
                  |      |           Supporto un aumento dei btc a 50 milioni
                  |      Non voglio bene a Salvini né ai gattini
                  Supporto i blocchi grandi 16mb
```

Quando si propone un particolare Bitcoin Improvement Proposal (BIP) per modificare il protocollo, si indica quale sia il bit per sostenerlo. Quando un miner crea un blocco della blockchain, dichiara che è pronto all’upgrade a quel determinato BIP indicando 1 anziché 0 nel corrispondente bit del version field.

Più un miner è ricco e potente, maggiore è la quantità di blocchi che crea rispetto ai miners concorrenti, perciò il voto non viene espresso nella modalità 1 testa = 1 voto (o 1 macchina = 1 voto), bensì con potenza di calcolo. Maggiore la potenza, maggiore influenza può avere sulle decisioni della rete.

A **questo link** vedete i risultati in tempo reale del voto dei miners

È curioso notare che i miners possano esprimersi anche a

favore di proposte non ancora concrete, ovvero in favore di idee che non hanno ancora dato vita a un software definitivo, come invece avviene nel caso dei BIP. Ad esempio, oggi il client btc1 della proposta Segwit2x è ancora in fase di testing, eppure i miners già stanno indicando l'intenzione di adottarlo, scrivendo all'interno della transazione "coinbase" le lettere: "NYA". La sigla sta per New York Agreement, il patto stretto il 23 maggio su proposta di Barry Silbert, per cui la maggioranza di miners e grosse aziende di servizi in btc concordano sull'upgrade SegWit + 2mb di blocco.

Dunque per proposte indefinite o per comunicare un qualsiasi tipo di messaggio, i miners anziché il version field del blocco possono usare la coinbase, che all'interno del nuovo blocco creato è la transazione che genera nuovi bitcoin (la ricompensa del miner per aver scoperto il blocco). Già Satoshi Nakamoto aveva inserito un messaggio nella coinbase del Genesis block (il primo blocco Bitcoin), con il famoso testo: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks". Il messaggio non solo segnava con precisione la data della nascita della blockchain Bitcoin, ma poteva già essere interpretato proprio come un messaggio politico.

8) THRESHOLD: LA SOGLIA DI VOTO DA RAGGIUNGERE PER L'UPGRADE

Un elemento fondamentale per ogni upgrade Bitcoin è la soglia di segnalazione. Generalmente un BIP specifica una percentuale di supporto che deve raggiungere la segnalazione dei miners prima che, di concerto, tutti facciano l'upgrade in una specifica data. Se la soglia non è raggiunta, l'upgrade non viene fatto da nessuno, nemmeno da chi lo ha proposto. Questo fattore è fondamentale, poiché se non si è a conoscenza del supporto verso una particolare proposta, il rischio è uno split della rete e della blockchain, con scenari anche catastrofici.

SegWit è stato proposto con BIP141 con una soglia di

attivazione del 95%. Finché non raggiunge quella soglia, l'intera community rinuncia all'upgrade. È stato presto chiaro che quella soglia non sarebbe mai stata raggiunta. La situazione di stallo fra lo schieramento pro SegWit e quello pro aumento del blocksize, se protratta ancora a lungo, avrebbe portato semplicemente alla lenta morte di Bitcoin, vittima dei progressi tecnologici effettuati da altre monete (in primis Litecoin, che ha già approvato SegWit). Anche per questa ragione si è arrivati il 23 Maggio all'accordo di New York. Da quell'accordo, è nata la proposta SegWit2x, ovvero SegWit più un moderato aumento della dimensione del blocksize. Per assicurare la riuscita del progetto, è nato BIP 91, che diminuisce la threshold dell'attivazione di SegWit all'80%. Questa soglia è stata definita proprio guardando ai miners che erano presenti all'accordo, il cui hashpower rappresenta circa l'85% della potenza computazionale dell'intera rete. In questo modo c'è sufficiente margine per assicurarsi che dal 21 luglio, giorno in cui partirà la segnalazione ufficiale, si raggiunga la threshold e SegWit venga approvato. Il 23 luglio ci sarà il probabile lockin, con attivazione al 25 luglio. Dopo 90 giorni dall'attivazione di SegWit, se tutto rimane come previsto, avverrà invece l'hard fork (la seconda parte di SegWit2x), con la rottura del limite a 1mb del blocksize. Da novembre il blocksize avrà un tetto a 2mb e il blockweight a 8mb, quindi si moltiplicherà x2 l'effetto SegWit (l'originale proposta del BIP141), che voleva un blocksize fisso a 1mb e il blockweight a 4mb. Secondo alcune stime, l'effettivo peso dei pacchetti dati scambiati ogni 10 minuti con SegWit2x sarà di circa 3.6mb, quindi circa il doppio rispetto a SegWit e in entrambi i casi superiore all'attuale 1mb.

Non tutte le proposte oggi sul mercato hanno una threshold di segnalazione. E questo è un male. La tipologia di segnalazione di voto che abbiamo visto appartiene soltanto ai miners, che sono solo una fetta della rete. Non c'è invece un sistema analogo di voto da parte degli utenti. Il tanto temuto upgrade del 1 agosto 2017, ovvero BIP 148, è un **UASF**, ovvero User

Activated Soft Fork: un upgrade attivato dagli utenti, non dai miners (altrimenti chiamato **MASF**: Miner Activated Soft Fork).

9) 1 AGOSTO: IL FALLIMENTO CERTO DEL FORK BIP 148 "UASF"

È mia opinione che i BIP che non hanno come requisito una soglia di voto, non dovrebbero nemmeno essere considerati dalla community, perché altrimenti rischiano solo di generare il panico. Non possiamo escludere che la frenata nel grafico del prezzo del Bitcoin sia dovuta all'incertezza che le voci sull'UASF del primo agosto hanno scatenato nei mercati. In realtà, guardando a BIP 148 in modo razionale e obiettivo, sappiamo che non è assolutamente un problema, per una ragione semplicissima: SegWit verrà approvato a fine luglio grazie a SegWit2x, perciò il primo agosto BIP 148 non si verificherà. O meglio, potremmo dire che si sarà già verificata, qualche giorno prima, con l'attivazione di SegWit grazie all'upgrade SegWit2x. Tutto sarà avvenuto in modo consensuale, senza alcun rischio di split.

Tempo fa, vedevo con simpatia l'idea di un UASF, e parteggiavo per Charlie Lee, creatore di Litecoin, quando minacciava di promuovere un UASF Litecoin, per costringere i miners ad approvare SegWit. Ero dell'idea che i miners cinesi a favore dei big blocks non avrebbero mai approvato SegWit e che quindi non saremmo mai riusciti a raggiungere una vera scalabilità del Bitcoin (non senza un accentramento totale della rete). L'accordo di New York invece ha cambiato le carte in tavola. Il 23 maggio i miners hanno dimostrato ragionevolezza, accordandosi su un ottimo upgrade e finalmente aprendo buone prospettive sul futuro di Bitcoin. Non poteva che essere così: i miners sono i primi a percepire sulle loro finanze le sorti negative o positive del Bitcoin, perciò hanno anche notevoli incentivi economici ad avere una rete unita e un Bitcoin tecnologicamente competitivo. Questa dopotutto era l'assunzione di partenza di Satoshi Nakamoto: è la teoria dei giochi a garantire la sopravvivenza del Bitcoin. Oggi, in

presenza di SegWit2x con oltre l’80% di hashpower a favore, cade qualsiasi ragione per minacciare un UASF. Oltretutto, la minaccia sarebbe ben poco credibile. Infatti UASF BIP 148 ha dei grossissimi limiti.

Anzitutto, si chiama User Activated Soft Fork, ma ha poco a che fare con gli utenti. Ammettiamo il caso totalmente remoto per cui SegWit2x dovesse fallire: ebbene, quello che un utente che sostiene UASF dovrà fare il primo di agosto, è semplicemente mantenere la sua versione di Bitcoin Core compatibile con SegWit. L’unico evento che farà scattare l’upgrade sarà uno spostamento di hashpower dei miners sulla catena in soft fork di BIP148. Nel momento in cui il primo miner inizia a creare blocchi con transazioni SegWit, si apre la competizione fra la catena UASF e la catena legacy. Nel mondo di Bitcoin, come era chiaro sin dal White Paper di Nakamoto, ciò che conta è l’hashpower, nessun utente può effettuare un fork. Un utente può scegliere di utilizzare un’altra cryptomoneta, e in misura aggregata gli utenti, esprimendo una preferenza per una moneta concorrenziale, potrebbero fare valere i loro i interessi, ma il peso degli utenti finisce qui. Niente miners, niente upgrade.

Secondo quanto sostenuto dai supporters di UASF, il fork sarebbe “attivato dagli utenti” poiché i miners sono costretti, stando a un calcolo razionale dei loro interessi economici, a spostarsi sulla catena UASF, perché prima o poi questa otterrà la maggioranza di hashpower e di conseguenza tutti i clients degli utenti faranno reorg, riconoscendola come l’unica vera catena.

> Ovviamente, questa teoria presuppone che la catena UASF raggiungerà un giorno la maggioranza di hashing power. Ora, sappiamo che nessun miner ha mai segnalato supporto a BIP148, se non per 1 blocco minato da Bitfury (e solo prima che l’accordo SegWit2x fosse definito), quindi l’haspower dei miner a favore di BIP148 è circa lo 0%, lontanissimo dal 51%.

Tuttavia, secondo i supporter di UASF, la maggioranza economica dei nodi effettuerà transazioni con nodi compatibili a SegWit, perciò tutta l'economia si sposterà inevitabilmente su quella catena e i miners sulla legacy non avranno altra soluzione che effettuare l'upgrade, o rimarranno a minare una catena vuota, senza transazioni e senza utenti. Secondo questa teoria, prima o poi, ed è solo questione di tempo, l'hashpower si muoverà verso la catena UASF fino a raggiungere ad un certo punto la maggioranza. Essendo quindi il destino segnato, ai miners conviene spostarsi sulla catena SegWit già dal primo momento del fork: in caso contrario, quando i client effettueranno il reorg e la catena legacy verrà orfanata, i miners perderanno tutti i bitcoin generati da tutti i blocchi legacy creati dall'inizio del fork fino al momento del reorg. In poche parole avranno speso tempo ed energia elettrica per niente. Questa teoria è fallace per varie ragioni:

1) Non c'è alcuno studio serio sulla "portata economica" dei nodi pro UASF. C'è un sistema che gli utenti hanno adottato per segnalare il supporto a UASF, per cui conosciamo il loro numero: circa 1000 nodi (il 15% dei nodi della rete, vedi fonte). Se anche fossero di più, non c'è alcun motivo di pensare che rappresentino il 15% dell'economia, figuriamoci la maggioranza economica. Come già detto, potenzialmente una piccolissima percentuale dei nodi potrebbe far transitare la maggioranza degli scambi economici: i nodi più rilevanti sono quelli degli exchange e delle grosse aziende, non di comuni utenti.

2) In presenza di split della rete, difficilmente gli utenti si arrischieranno a fare transazioni SegWit, perché tutti gli output di quelle transazioni verranno rubati e spesi sulla catena legacy, per via del meccanismo dell'anyone can spend.

3) Se anche una percentuale rilevante dei miners iniziasse a supportare la catena UASF, diciamo il 10%, la catena UASF sarà lentissima a convalidare i blocchi, perché in

concorrenza con la potenza di calcolo della catena legacy. Col 10% di hashpower ad esempio (che è forse una prospettiva fin troppo rosea per UASF), verrà generato 1 solo blocco ogni 100 minuti: gli utenti lamenteranno transazioni lentissime. I miners otterranno la ricompensa per quel blocco creato solo dopo altri 120 blocchi, quindi dopo 12.000 minuti (oltre una settimana dopo). La situazione rimarrà così fino all'aggiustamento della difficoltà sulle due catene, che avverrà circa 140 giorni dopo vedi per approfondimenti)

Considerando che:

– il valore dei bitcoin della catena BIP 148 si abbasserà a causa della sua totale lentezza e inefficienza

– probabilmente gli utenti non si arrischieranno a fare transazioni SegWit per paura di essere derubati dei loro btc sulla catena legacy

– i miners riceveranno la ricompensa in ritardo e la corrente elettrica per generare hashpower non è gratis

è decisamente più probabile che i miners non si arrischino affatto a minare sulla BIP148. Insomma, non c'è proprio speranza che con questo livello di consenso da parte della community, SegWit possa essere approvato con BIP148. Semplicemente BIP 148 non avrebbe alcun effetto, come se non fosse mai esistito. La buona notizia è che SegWit verrà approvato con BIP91 grazie a SegWit2x, i cui sviluppatori hanno oltretutto avuto il buon senso di rendere compatibile anche con UASF BIP148, così da scongiurare qualsiasi rischio remoto.

10) CHI SOSTIENE UASF BIP 148?

Nonostante ogni evidenza provi il contrario, i supporter di UASF sembrano affermare che "la maggioranza economica" (o

comunque la stragrande maggioranza di utenti), è favorevole al fork BIP148 del 1 agosto. Nel tentativo di avvalorare questa tesi, vengono presentati dati di sondaggi su Twitter: lo sviluppatore di Core e dipendente Blockstream Luke Dashjr ha persino dichiarato che si basa sui quei dati perché “le uniche metriche disponibili sono l’osservazione personale e l’attività degli utenti su twitter”.

Chiunque è libero di giudicare quale sia un upgrade consensuale e quale no, prestando attenzione alle informazioni di cui disponiamo ufficialmente:

UASF:

– Segnalazione dello 0% di hash power

– 1000 nodi circa (15%) che segnalano a supporto

SEGWIT2X:

– Segnalazione di oltre l’85% di hashpower

– 58 aziende di 22 paesi firmatarie dell’accordo, di cui:

– Oltre 20 milioni di wallets bitcoin

– Oltre 5 miliardi di dollari di transazioni effettuate mensilmente

(vedi l’accordo)

Chi sostiene UASF, se avesse avuto un minimo di fair play, anziché fare del terrorismo proponendo un fork senza voto di segnalazione (con ripercussioni sul prezzo che ci danneggiano tutti), avrebbe dovuto proporre una soft fork SegWit con soglia al 51% dell’hash power, o almeno un nuovo meccanismo di segnalazione, che contasse gli utenti che fanno girare un full node, pretendendo almeno un 51% prima dell’attivazione (ricordiamo che oggi i nodi che segnalano attivamente BIP148 sono il 15%).

Ma chi sono questi utenti pro UASF? Per lo più, sono utenti esasperati dalle attese per l'approvazione di SegWit e che sono assolutamente contrari a un qualsiasi aumento del blocksize. Ovviamente la dimensione del blocco a 1mb non è un "numero magico" che debba rimanere immutato per sempre, ma secondo alcuni UASF supporter come Luke Dashjr il blocco è fin troppo grosso e dovrebbe addirittura essere ridotto. Sembra che i pro UASF provino un rancore verso quei miners che si sono sempre schierati a favore di un aumento del blocksize e che storicamente sono stati (almeno fino a SegWit2x) contrari a SegWit. In particolare verso la più grossa mining pool del mondo "Antpool", di proprietà dell'azienda Bitmain, casa produttrice degli Antminer. Il CEO Jihan Wu è diventato il capro espiatorio in cui identificare ogni male, con teorie complottiste al di là di ogni razionalità (vedi questo articolo di Luke Dashjr).

Sembra che piuttosto che vedere approvato un upgrade sostenuto da (anche) questi miners, i più ferventi sostenitori di UASF preferiscano l'eterna l'immutabilità del protocollo. Se il protocollo non cambia però, il Bitcoin non potrà mai essere in grado di servire le masse, e presto o tardi verrà dimenticato e superato da altre altcoin.

Luke Dashjr è divenuto un po' il simbolo e portabandiera di BIP148 ed è, insieme all'italiano Giacomo Zucco, uno dei pochi ad aver proposto un'apologia di UASF formalizzata in almeno un articolo strutturato. Luke è senz'altro un bravo coder, ma in fatto di idee è quantomeno originale: non solo è complottista, pare anche sia un noto terra-piattista e fondamentalista religioso.

Non è certo questa la sede per giudicare il personaggio, ma rimanendo in argomento UASF, è interessante notare le opinioni e perplessità che direttamente i colleghi di Luke, sviluppatori di Bitcoin Core e impiegati di Blockstream, hanno sollevato nei confronti dell'UASF del 1 agosto. Pieter Wuille è co-fondatore di Blockstream e ha scritto più codice per

Bitcoin Core che tutti gli altri principali contributors messi insieme. Gregory Maxwell è co-fondatore di Blockstream e Core contributor, Matt Corallo è advisor di Blockstream e Core contributor. Tutti e tre sono nel grafico "Who is at the core of Bitcoin" postato sopra. Di seguito alcuni scambi che hanno intrattenuto con Luke Dashjr:

> **Gregory Maxwell a Luke Dashjr:** *non ho mai visto un tale supporto a BIP148 che giustifichi la tua posizione in merito. Attualmente nessun exchange o payment processor degno di nota ha dichiarato di essere per BIP148. Penso che se ce ne fossero, avresti qualche argomento valido, ma ora come ora, è difficile identificare un effettivo livello di supporto per il fork BIP148 (e ho visto anche qualche attore chiaramente malevolo che lo promuove)*
>
> **Pieter Wuille a Luke Dashjr:** *mi aspetto che qualsiasi nodo economicamente rilevante abbandoni il codice di BIP148 qualche ora dopo che l'adozione per hashpower avrà fallito*
>
> **Pieter Wuille a Luke Dashjr**: *penso che tu sia pazzo*
>
> **Pieter Wuille:** *la mia opinione è che unire BIP 148 a Bitcoin Core andrebbe contro i nostri princìpi*
>
> **Matt Corallo a Luke Dashjr**: *ti andrebbe se ti comprassi un biglietto aereo per parlare con la gente? sarei felice di farlo.. penso che tu spenda davvero troppo tempo su reddit anzichéparlando con persone reali*

(vedi conversazione originale, ed estratti)

11) NEMICI DI BITCOIN: SONO I MINERS O CHI LI VUOLE LICENZIARE?

Il titolo di questo paragrafo è deliberatamente provocatorio, ma vuole sottolineare una questione fondamentale: chi crede in UASF BIP 148, non crede che il Bitcoin come originariamente

disegnato da Nakamoto possa funzionare. Chi propone BIP148 infatti ha perso ogni fiducia nella condotta dei miners e intende effettuare un PoW change, ovvero un cambio di Proof of Work (la modalità in cui viene eseguito il lavoro dei miners). Si veda ad esempio l'articolo di Giacomo Zucco:

"l'eventualità in cui nessun miner supporti BIP148 – ma sembra estremamente improbabile – non risulterebbe comunque in un *fallimento* della proposta; piuttosto nella creazione di una nuova altcoin dalla catena BIP148, in seguito a un cambiamento di Proof of Work"

Effettuare un PoW change significa licenziare tutti i miners, poiché tutte le apparecchiature specializzate per il mining di Bitcoin (gli Asics) saranno praticamente da buttare (o in alternativa, da utilizzare su altre altcoin che abbiano la stessa proof of work, se ce ne sono). Un cambiamento di proof of work significherebbe perdere la totalità della potenza computazionale che difende il Bitcoin da attacchi esterni. Oggi, se un gigante come Google impiegasse la potenza di ogni suo datacenter per poter manovrare il Bitcoin a suo piacimento, non farebbe nemmeno il solletico alla blockchain, non raggiungendo neanche lontanamente l'1% della potenza computazionale della rete Bitcoin. La decentralizzazione in sé non ha alcun significato, poiché è un mezzo, non un fine: il fine è la sicurezza e la privacy. Ebbene, nel nome della decentralizzazione, i promotori di UASF favorevoli a un PoW change vorrebbero licenziare tutti i miners, ovvero tutta la potenza di calcolo che mette in sicurezza la rete. Più curioso sarà il metodo che proporranno per farlo: un fork che punti sulla maggioranza dell'hash power? Lo stesso hash power dei miners che vogliono licenziare?

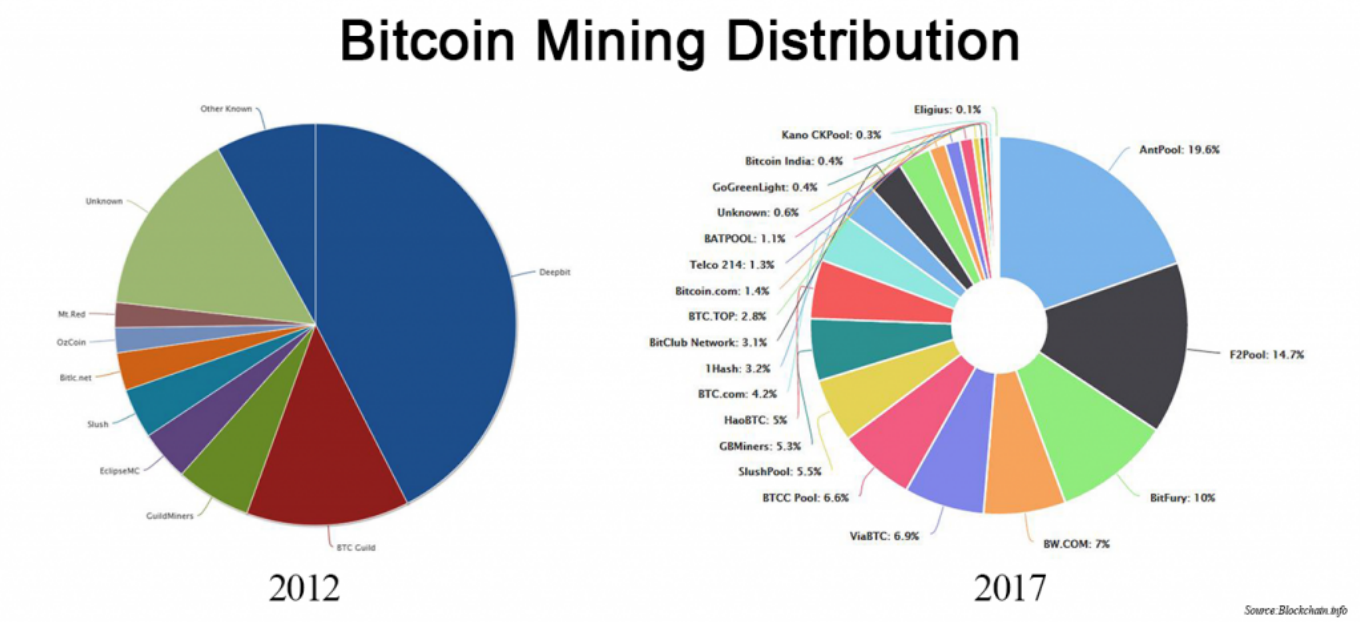
Come è evidente, i supporter di UASF credono che il meccanismo di teoria dei giochi alla base del Bitcoin come è stato inventato da Satoshi Nakamoto sia inevitabilmente fallimentare: gli incentivi e disincentivi economici dati ai miners non garantirebbero che il Bitcoin si sviluppi nel modo

migliore possible per i suoi utenti. Insomma, la blockchain Bitcoin sarebbe già sotto l'attacco del 51% immaginato da Nakamoto, ma in questo caso l'attacco sarebbe effettuato da quegli stessi miners che da anni supportano la crescita di Bitcoin e ne sono i primi investitori. A questo punto, non si capisce che senso avrebbe chiamare la moneta nata dal fork "Bitcoin". È chiaro che ciò che Zucco e Luke Dashjr vogliono non è il Bitcoin, ma un'altra cryptomoneta.

Le loro preoccupazioni possono anche essere condivisibili: crypto innovative come IOTA non si basano più sul meccanismo di PoW sottostante a una blockchain, che viene sostituita dal "Tangle". Con IOTA non solo non esistono più commissioni sulle transazioni, ma si rimedia completamente alla distinzione fra utenti e miners, quindi anche a potenziali conflitti di interesse fra le due classi. Chiedo dunque ai pro UASF: perché non concentrare le proprie energie su una tecnologia innovativa come IOTA, sicuramente da perfezionare e diffondere, piuttosto che tentare di scatenare un terremoto politico sul Bitcoin, una cryptomoneta le cui basi ormai voi considerate (esplicitamente o implicitamente) "fallite"? Se è l'attuale distribuzione della ricchezza che volete mantenere siete liberi di creare una nuova cryptomoneta mantenendo lo storico dell'attuale blockchain Bitcoin.

12) LA RETE BITCOIN STA PASSANDO SOTTO AL CONTROLLO DI POCHI?

Guardando allo storico della distribuzione del mining, non c'è particolare motivo per lamentare l'accentramento della potenza di calcolo nelle mani di pochi. La continua crescita dell'hashing power a servizio e a difesa della rete non è andata a discapito della decentralizzazione. Come vediamo nei grafici, la mining distribution è oggi migliorata rispetto ad anni fa (2012), quando Deepbit da sola controllava il 45% circa dell'hash power e con la sola BTC Guild avrebbe potuto coalizzare la maggioranza assoluta dei voti.



1% of the Bitcoin network in 2011

1% of the Bitcoin network in 2017

Ricordiamoci che tutto il terremoto inscenato da UASF è dovuto all'intransigenza di alcuni personaggi che rifiutano categoricamente un blocksize increase da 1 a 2mb, perché a loro avviso questo sarebbe il primo passo verso ulteriori aumenti successivi, e di conseguenza un inesorabile accentramento della rete. In realtà, l'incremento da 1mb a 2mb non è nel modo più assoluto un pericolo per la decentralizzazione. Infatti, dopo l'upgrade SegWit2x di fine luglio, la rete non sarà più ingolfata dalle troppe transazioni rispetto alla capacità della blockchain, e ricomincerà a funzionare senza commissioni elevate. Di conseguenza, il numero utenti, imprese, miners e fullnodes presto aumenterà, garantendo quindi maggiore (e non minore)

decentralizzazione. Il livello tecnologico attuale permette tranquillamente alle tasche di un utente medio di mantenere un fullnode casalingo, con o senza blocksize increase a 2mb.

È anche sbagliato vedere tutte le mining pool come un unico organismo con a capo una singola entità: non tutti i grossi miners sono enormi datacenter posseduti da un'unica azienda. Le pool sono aggregazioni anche di singoli utenti che minano in modo casalingo. L'accentramento della potenza di calcolo in alcune mining pool non è un male se c'è "hashrate liquidity", ovvero se gli utenti affiliati a una grossa pool sono in grado di cambiare pool nel momento in cui questa supporti un BIP ad essi sgradito. Alcune mining pool come Slushpool permettono già al singolo utente di poter decidere come segnalare. La speranza per il futuro è che ci sia sempre più consapevolezza, fra chi fa mining, delle tematiche politiche, e di conseguenza aumenti spontaneamente l'hashrate liquidity. Se si procedesse in quella direzione, il fatto di avere una rete di miners decentralizzata (con l'aggregazione in grosse mining pools) anziché distribuita (con utenti sparsi che minano singolarmente) può persino avere i suoi vantaggi: ad esempio, nel caso specifico del fork accidentale dell'11 marzo 2013, ciò che ha permesso di ripristinare l'ordine così in fretta è stata la possibilità di contattare e coordinare rapidamente tutte le mining pool.

Per concludere, diciamo che il Bitcoin sta maturando sotto molti punti di vista:

1) La blockchain è sempre più sicura da attacchi esterni, perché la potenza computazionale che la serve è sempre maggiore e, nonostante l'economia del mining sia soggetta a rendimenti di scala, non ha visto un particolare accentramento negli ultimi anni rispetto allo storico

2) I software client Bitcoin e i team di sviluppo si stanno moltiplicando e differenziando, garantendo un ecosistema più vario, adatto ad applicativi diversi, e sicuro, poiché è

sempre più difficile individuare un “single point of failure” o imporre cambiamenti non consensuali al protocollo.

3) Wallets, app per smartphone, exchanges, payment processors si stanno moltiplicando. Non c’è più il rischio di un crollo sistemico se un grosso exchange cade, come nel caso di MTGox nel 2013. Sempre più servizi e negozi accettano Bitcoin. Gli exchanges hanno talmente tante iscrizioni che non riescono a gestire la quantità di iscritti (vedasi Kraken o Coinbase – e questo vale tanto più quando i prezzi calano): tutto ciò significa una sola cosa, ovvero che c’è sempre più gente disposta a cambiare la propria moneta fiat per crypto-moneta.

4) La community si sta finalmente dimostrando compatta verso soluzioni condivise: da anni si discutevano problemi di scalabilità e possibili soluzioni, l’accordo di Hong Kong fra miners e sviluppatori si è rivelato un fallimento. Oggi c’è la svolta, grazie all’accordo di New York di SegWit2x

5) Finalmente, il Bitcoin sta per risolvere il più insormontabile problema di tutte le cryptomonete: la scalabilità. Grazie a SegWit e la rete Lightning Network, la prima soluzione tecnologia ai problemi di scalabilità può passare dall’essere teoria all’applicazione pratica, e il Bitcoin potrà essere adottato da milioni o miliardi di utenti senza che la tecnologia soffra di ingorghi, lentezza e costi insormontabili.

13) SEGWIT2X (btc1): LA SOLUZIONE CONDIVISA

SegWit2x è un upgrade in due fasi. La prima fase, che culminerà probabilmente il 28 luglio, vede l’attivazione di SegWit in soft fork. Tale attivazione è compatibile con BIP141 e BIP148 e coi nodi Bitcoin Core. Avendo ad oggi quasi il 90% della potenza computazionale a favore, la riuscita

dell’upgrade è praticamente certa.

La seconda fase prevede, a 90 giorni dall’attivazione di SegWit, un hard fork che permetta la creazione di blocchi con blocksize a 2mb. Per effettuare l’hard fork previsto a fine ottobre è stato studiato un sistema curioso. La catena SegWit2x genererà obbligatoriamente 1 blocco particolare (Blocco X), che sarà quello minato esattamente 12.960 blocchi successivi all’attivazione di SegWit. Dato che in un giorno si trovano approssimativamente 144 blocchi, significa 90 giorni dopo l’attivazione (90*144=12.960). Il blocco X dovrà presentare un blocksize necessariamente maggiore di 1mb. Se non ci dovessero essere sufficienti transazioni per la creazione di un blocco di quelle dimensioni, un qualsiasi miner potrà riempire il blocco artificialmente, effettuando transazioni fra i suoi stessi nodi o con altri metodi (per esempio la validazione nel blocco di un’unica transazione dal peso enorme, o caricando dati aggiuntivi tramite lo script OP_RETURN). Nella remota ipotesi in cui nessun miner intendesse riempire il blocco, la catena SegWit2x si fermerebbe per sempre.

L’idea di effettuare un hard fork costringendo alla creazione di un blocco maggiore di 1mb è una scelta criticata da alcuni esponenti di Blockstream come Maxwell e Luke Dashjr, secondo i quali il metodo tradizionale e più sicuro per effettuare un hard fork è quello di impostare un bit particolare nel block header, che rende il blocco incompatibile con la catena legacy. La risposta di Jeff Garzik, Core contributor e lead developer del progetto btc1 (il client di SegWit2x) fa perno su questi due aspetti:

il sistema del Blocco X assicura l’hard fork in un momento definito con assoluta precisione: da quel preciso momento o tutti accettano i blocchi più grandi o non li accettano. Non è possibile per esempio che un client accetti blocchi col bit dell’hard fork nell’header, ma al contempo non accetti blocchi che siano maggiori di 1mb. Inoltre, implementazioni di

fullnodes alternative a Core (ad esempio BitcoinJ) sono già compatibili con un hard fork come quello studiato da Garzik, mentre implementare il bit nel block header ridurrebbe tale compatibilità (altri client dovrebbero upgradare).

In fondo, se c'è consenso fra i miners e un hashpower a favore del 90% come c'è oggi (e nessun miner storicamente ha mai rotto gli accordi presi), non ci sarà alcun problema a creare un blocco maggiore di 1mb. Inoltre, se si mantiene tale consenso e una community così unita, nessuna grande pool si azzarderà a ritirare la parola data: sarebbe solo una mossa insensata, per cui ne va della reputazione (e dei soldi) della pool. Ricordiamo che le mining pool sono aziende che hanno costi e profitti, non sviluppatori che scrivono codice per passione e propongono idee politiche senza ripercussioni sui loro investimenti. Nessuno ha convenienza a creare ulteriori spaccature all'interno della comunità Bitcoin. Il dibattito sullo scaling finalmente è a una svolta.

14) LE PROSSIME DATE E SCADENZE

21 luglio: inizio segnalazione dei miners per la prima parte dell'upgrade SegWit2x (BIP91)
(nota, già oggi stanno segnalando per SegWit2x per l'89%, solo che lo stanno facendo scrivendo NYA nel codebase, passeranno presto a segnalare tramite bit con il client btc1)

25 luglio: se la segnalazione va a buon fine (se supera l'80%) avviene il lockin di SegWit (BIP91)

28 luglio: effettiva attivazione di SegWit (BIP91)
la capacità media della blockchain passerà da 1mb ogni 10 minuti a circa 1.7mb (massimo teorico: 4mb), quindi ci sarà più spazio per gli utenti per effettuare transazioni. Questo significa tempi di validazione e costi di commissione per le transazioni decisamente inferiori.

Grazie a SegWit, ci sarà la possibilità di implementare Lightning Network, la rete offchain che permette di sfruttare la blockchain non come registro, ma come giudice (o arbitro):

le transazioni offchain saranno istantanee e le commissioni più basse (in certi casi, anche nulle). Non appena la rete Lightning sarà sufficientemente diffusa, il bitcoin potrà essere adottato dalle masse (milioni o miliardi di utenti) senza alcun pericolo di futuri ingolfamenti della rete.

1 agosto: si attiva UASF (BIP148). In realtà, tutti i miners già staranno creando blocchi compatibili a UASF, grazie all'upgrade a SegWit del 28 luglio, quindi non solo non ci sarà uno split, ma nemmeno un fork (il fork sarà già avvenuto con BIP91 e in modo del tutto consensuale all'interno della community)

24 agosto: effettiva attivazione di SegWit

22 novembre (a 90gg di distanza dall'attivazione di SegWit): hard fork per aumentare il blocksize a 2mb (seconda parte dell'upgrade SegWit2x)
la capacità media della blockchain passera da circa 1.7mb a 4.6mb (massimo teorico: 8mb), quindi ci sarà ancora più margine per consentire alla rete offchain Lightning Network di svilupparsi senza che si verifichino altri ingolfamenti sulle transazioni onchain

15) SEGNALI DI TRADING

Il calo del Bitcoin di questi giorni è dovuto essenzialmente ad un aggiustamento rispetto alla bolla speculativa dei primi mesi 2017. Nel formulare ipotesi sul prezzo di fine anno, a gennaio i più coraggiosi azzardavano i 2000$: il Bitcoin ha raggiunto quasi i 3000$ a giugno. Siamo ancora a un più 50% rispetto a 3 mesi fa. È più che naturale un aggiustamento fisiologico. Una cosa è certa: l'aggiustamento è scattato con tempismo perfetto in prossimità dei fork di fine luglio/inizio

agosto. Si può dire che i timori in uno split della catena abbiano innescato la scintilla del dump, che tuttavia era già pronto a manifestarsi da tempo.

Per chi non è holder di Bitcoin sul lungo periodo, ma fa trading short term, si presti attenzione a due eventi in particolare. Qualora ci fossero aggiornamenti su entrambi, non mancherò di avvisare (iscrivetevi alla newsletter qui: **SUBSCRIBE**)

1 agosto: sarà chiaro ai mercati che non avverrà nessuno split e una volta che il panico sarà superato, il prezzo potrà tornare a crescere

22 novembere: sarà probabilmente un fork tanto consensuale quanto la prima parte di SegWit2x, per cui la segnalazione è oggi all'89% circa. Tuttavia, trattandosi di un hard fork anziché un soft fork, la semplice "semantica" del termine potrebbe spaventare maggiormente gli speculatori sui mercati. In vicinanza del fork potrebbe quindi esserci un dump del prezzo del bitcoin analogo, o peggiore, a quello verificato in questi giorni di metà luglio. La magnitudine del dump sarà probabilmente proporzionale alla crescita che ci si può aspettare dopo il primo di agosto. Generalmente d'estate i soldi si spendono, e per spendere Bitcoin oggi è ancora necessario (purtroppo) passare quasi sempre per la moneta fiat, perciò può essere che generalmente agosto rimanga un mese buono per comprare.

Note: alcuni utenti (gli attuali pro UASF BIP 148) potrebbero tentare un PoW change (o una creazione di altcoin) con un altro hard fork del Bitcoin: evento che, anche se non avesse molto seguito all'interno della community, potrebbe creare un fenomeno mediatico con ricadute sul prezzo di mercato. Anche su questo terrò aggiornati i miei lettori.

Infine lancio il solito monito: nonostante le balle d'oro che qualche mio lettore ha fatto grazie ai consigli su Litecoin

dei primi di Maggio, sappiate che non ho ancora sviluppato poteri sciamanici infallibili. Investite i vostri soldi a vostro rischio e pericolo. Se non volete rischiare, mettete degli stop loss o prestate sempre e con regolarità molta attenzione ai prezzi. Impostare allarmi sull'app per android "Bitcoin Ticker Widget" è uno dei metodi più efficaci per stare sempre sul pezzo (è un consiglio, non una pubblicità).

16) I VOLTI DEI PROTAGONISTI:

Martti Malmi

conosciuto come Sirius, è stato sviluppatore dei primissimi client Bitcoin insieme a Satoshi Nakamoto

Gavin Andresen

Informalmente designato da Satoshi Nakamoto come lead developer del client Bitcoin sin dal 2010, ha guidato il progetto per anni. Storicamente è stato a favore di soluzioni di scalabilità onchain, promuovendo fork del Bitcoin con blocksize increase.

Pieter Wuille

è il coder con più contributi al principale client Bitcoin: Bitcoin Core. È co-fondatore di Blockstream, azienda che raccoglie alcuni fra i maggiori contributors di Bitcoin Core favorevoli a soluzioni di scalabilità offchain.

Gregory Maxwell

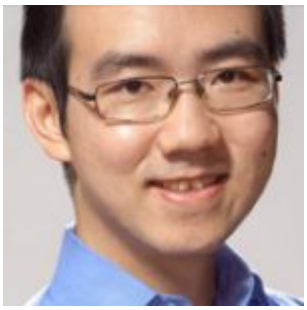
è co-fondatore di Blockstream e uno dei principali contributors di Bitcoin Core

Matthew Corallo

co-fondatore di Blockstream e uno dei principali contributors di Bitcoin Core

Luke Dashjr

è impiegato presso Blockstream e contributor di Bitcoin Core. È il primo promotore di UASF BIP148



Jihan Wu

Fra i primi a produrre hardware specializzato per il mining di Bitcoin, è a capo di Bitmain, la principale azienda produttrice di hardware per mining. Controlla Antpool, la pool più grossa del mondo, con circa il 18% di potenza computazionale di tutta la rete. Jihan è sempre stato contrario a SegWit e a favore di soluzioni di scalabilità onchain, fino all'accordo di New York del 23 Maggio, per cui Antpool ha iniziato a segnalare a favore di SegWit2x

Jeff Garzik

Contributor di Bitcoin Core, è anche il principale sviluppatore di btc1, il client di riferimento per l'upgrade SegWit2x. Storicamente favorevole a soluzioni onchain, si è poi speso per far convergere le due visioni sulla scalabilità in una soluzione condivisa

Barry Silbert

CEO di DCGco, il Digital Currency Group, grande gruppo di investimento che finanzia molte delle principali startup e aziende del mondo Bitcoin e Blockchain, fra cui Blockstream. Ha organizzato il meeting di New York, che si è finalizzato con successo nell'accordo di SegWit2x

Adam Back

CEO di Blockstream. Nel White Paper è citato direttamente da Satoshi Nakamoto per il suo paper "Hashcash" (1997). L'hashcash è un sistema anti-spam basato sulla Proof of Work, utilizzato per limitare email e attacchi DOS. Lo stesso meccanismo è alla base del mining di bitcoin inventato da Nakamoto

Franco Cimatti

Conosciuto come HostFat, è Presidente di Bitcoin Foundation Italia. Ha testato i primissimi client Bitcoin e curato la prima traduzione del software, che è stata proprio l'Italiano. Storicamente a favore di soluzioni di scalabilità onchain, come Bitcoin Unlimited.

Giacomo Zucco

CEO di Blockchainlab, ha organizzato a Milano lo Scaling Bitcoin 2016, tradizionalmente uno degli eventi più importanti dell'ecosistema Bitcoin. È uno dei supporter di UASF BIP148

Iscriviti alla newsletter per ricevere una notifica ad ogni nuovo articolo pubblicato! Clicca qui: **SUBSCRIBE**