Cosa succederà il 1 Agosto 2017 – il destino del Bitcoin

In tantissimi lo stanno chiedendo, molti in preda all'ansia dopo aver sentito rumors catastrofici: "cosa accadrà il primo agosto?

La risposta è semplicissima: niente. Il primo agosto non accadrà proprio niente.

Già prima di agosto, verrà approvato l'upgrade più importante della storia di Bitcoin, la cui effettiva attivazione avverrà nelle settimane successive. L'upgrade avverrà senza alcun pericolo, anzi risolverà moltissimi problemi di Bitcoin, abbasserà i costi di transazione e i tempi di attesa. Inoltre permetterà lo sviluppo di Lightning Network, che è la tecnologia che rende le transazioni Bitcoin istantanee.

Cosa dovete fare quindi? Comprate Bitcoin e state tranquilli. Il prezzo salirà. Parecchio.

Se siete esclusivamente interessati al destino dei vostri investimenti, vi basti quanto appena scritto.
Se non siete preparati tecnicamente, ma volete almeno avere un'idea di quello che è accaduto in questi giorni, continuate a leggere.

Si è scongiurato totalmente il pericolo di uno split della chain Bitcoin, conosciuto anche come UASF (BIP148), che sarebbe dovuto avvenire a partire dal 1 agosto.
L'UASF era un tentativo di alcuni utenti Bitcoin di creare una catena di blocchi separata (un fork), nella speranza che si mangiasse (reorg) la catena Bitcoin preesistente (la catena legacy) e diventasse la catena principale. Spiegato in pillole:

– Perché la transazione Bitcoin di un utente sia valida, deve seguire il protocollo Bitcoin. I miners convalidano le transazioni che seguono il protocollo, inserendole in un nuovo blocco della blockchain ogni 10 minuti. Per creare blocchi i miners impiegano molta potenza di calcolo. La loro potenza di calcolo aggregata protegge la rete da attacchi esterni.

– Un fork del Bitcoin è una modifica al protocollo che viene sostenuta dalla potenza di calcolo dei miners. I fork sono utilizzati normalmente per fare un upgrade a Bitcoin, oppure per creare delle criptomonete alternative.
Ad esempio, Litecoin non è altro che una modifica del protocollo Bitcoin. Nel momento in cui qualche apparecchio hardware inizia a fare mining creando la blockchain di Litecoin, la moneta "prende vita".

– Generalmente gli upgrade del Bitcoin avvengono in modo consensuale: tutti i miners sono d'accordo che l'upgrade è benefico, gli utenti anche. Molti upgrade sono stati fatti in passato. Quando gli utenti fanno l'upgrade del proprio client Bitcoin e iniziano a inviare transazioni che rispettino il protocollo modificato, i miners accettano queste transazioni e le inseriscono nella blockchain.

– Se però alcuni miners sono pro e altri contro il cambiamento, c'è il rischio che l'upgrade porti a una spaccatura: la creazione di due blockchain separate, ciascuna sostenuta dalla potenza di calcolo di un diverso gruppo di miners. Anziché modificare Bitcoin, la nuova chain crea una nuova cryptomoneta, analogamente a come è stato creato Litecoin.

– Tuttavia, mentre Litecoin era intenzionalmente e dichiaramente una moneta diversa, il problema in questo caso è che entrambe le monete pretendono di chiamarsi Bitcoin: in caso di split, alcuni exchange seguirebbero una moneta (la catena legacy) altri l'altra (la catena con upgrade), gli utenti non riuscirebbero più a vedere convalidate le proprie

transazioni, perché incompatibili con la catena gemella. Si creerebbe una confusione generale totalmente deleteria per il Bitcoin. Tutti i servizi probabilmente dovrebbero sospendere i pagamenti, i prelievi, i cambi, il network si spaccherebbe, Bitcoin verrebbe superato da altre cryptomonete.

– Ovviamente, se la catena che vuole fare upgrade non ha sostegno dei miners, non avviene nulla di ciò. A favore di UASF c'era circa il 12% dei full nodes (i nodi degli utenti), e lo 0% della potenza di calcolo dei miners. Probabilmente sarebbe stato un flop. Ad ogni modo, ogni rischio è stato scongiurato grazie ad una nuova proposta di upgrade che ha immediatamente ottenuto il consenso della stragrande maggioranza dei miners.

– Pochi giorni fa, è stato rilasciato in alpha testing il client SegWit2x, un upgrade che ha messo d'accordo tutti i miners ed è anche compatibile con la catena UASF. Ovvero, se gli utenti che avevano minacciato l'UASF (User Activated Soft Fork) dessero via al fork il primo agosto, nulla cambierebbe, poiché le modifiche portate da UASF sono già comprese nel protocollo di SegWit2x, che verrà attivato prima e le cui transazioni sono riconosciute valide dalla stragrande maggioranza di miners.

– Come vedete da **questo grafico** (aggiornato real time) Segwit2x ha raggiunto stanotte l'80% di sostegno dei miners (ovvero la soglia prevista per l'attivazione), mentre BIP148 (ovvero il Bitcoin Improvement Proposal relativo a UASF) non è nemmeno nella lista poiché non ha mai ottenuto il consenso di alcun miner (0%).

SegWit2x e BIP148 sono compatibili perché condividono una parte fondamentale del protocollo: l'upgrade a SegWit, ovvero quella modifica che, come detto a inizio articolo, abbasserà le fee e permetterà lo sviluppo di Lightning Network.
Per un ulteriore approfondimento, leggete questa breve

cronistoria con link ai miei articoli precedenti:

– Gli sviluppatori di Bitcoin Core creano l'upgrade SegWit

– Alcuni miners e utenti si oppongono a SegWit, poiché al contrario vogliono un aumento del blocksize. Si legga questo mio articolo relativamente al dibattito sullo "Scaling": SegWit vs Blocksize Increase:

http://www.albertodeluigi.com/2017/03/25/cosa-sta-succedendo-al-bitcoin-tutte-le-spiegazioni/

– Si arriva all'accordo di Hong Kong il 21 febbraio 2016 fra i big della rete (miners, sviluppatori, imprese). È un compromesso in cui i miners decidono di approvare SegWit e un aumento del blocksize da 1 a 2mb. **Leggi qui i termini dell'accordo**.

– Gli sviluppatori di Bitcoin Core (il client più utilizzato nella rete) inseriscono SegWit ma non l'upgrade a 2mb nel client (che dagli accordi era previsto per il luglio 2016), perché asseriscono che non ci sono ancora motivi tecnici per aumentare il blocco, cosa che rischierebbe invece solo di accentrare la rete. Seppur le motivazioni tecniche siano comprensibili, alcuni miners si sentono traditi.

– Dal 15 novembre 2016 è prevista l'attivazione di SegWit e i miners appoggiano l'upgrade solo al 30%, una potenza di calcolo insufficiente per raggiungere la soglia di attivazione. I motivi sono vari:
1) alcuni ritengono SegWit un upgrade non sicuro;
2) vari miners cinesi ritengono SegWit una soluzione troppo complicata, tecnicamente difficile da comprendere e che porterebbe troppa discrezionalità e potere nelle mani degli sviluppatori delle "corporations occidentali";
3) altri sostengono che l'unica via per fare upgrade sia un aumento della dimensione dei blocchi;
4) Bitmain, la casa produttrice degli antminers (e

proprietaria della mining pool più grande del mondo, Antpool) perderebbe un'ottimizzazione delle proprie macchine per il mining nel caso si facesse upgrade a SegWit.

– Nel frattempo, il successo di Bitcoin rende i blocchi sempre più intasati (molte più transazioni vengono eseguite contemporaneamente in tutto il mondo), fra gennaio e marzo 2017 i costi e la lentezza delle transazioni iniziano a diventare esasperanti, destinati solo a peggiorare.

– Charlie Lee, il creatore di Litecoin, promuove l'upgrade a SegWit su Litecoin. Alcuni miners Bitcoin contrari a SegWit tentano di sabotare l'upgrade impiegando potenza di calcolo su Litecoin, nella paura che una volta approvato SegWit su Litecoin, si riveli un protocollo sicuro e ben testato e possa condurre a un maggiore sostegno all'upgrade anche su Bitcoin

– Charlie Lee minaccia un fork di tipo UASF su Litecoin e incontra i miners a porte chiuse. Ne esce un accordo per cui all'unanimità i miners accettano l'upgrade. Il 6 maggio esce questo articolo sul mio blog, dove consiglio l'acquisto di Litecoin a palate:

http://www.albertodeluigi.com/2017/05/06/perche-acquistare-litecoin/

– Litecoin ottiene SegWit il 10 maggio. L'utilizzo e l'adozione da parte di imprese e servizi ha un'impennata, il valore di Litecoin raddoppia in un mese.

– Nel frattempo le fee su Bitcoin e i tempi di attesa sono elevatissimi. Bitcoin perde terreno nei confronti di altcoin come Ethereum e Litecoin. Il 24 maggio Barry Silbert raccoglie in meeting i principali miners, le principali imprese e servizi in Bitcoin; gli sviluppatori di Bitcoin Core sono invitati ma decidono di non partecipare. Miners e imprese arrivano a un accordo, SegWit2x. **Leggi qui i termini dell'accordo**

Su questo blog, in anteprima mondiale assoluta, avete ricevuto i primi leak relativi all'accordo: **http://www.albertodeluigi.com/2017/05/22/un-accordo-bitcoin-forse-la-svolta/**

– L'accordo su SegWit2x viene sminuito da alcuni utenti e sviluppatori, che propongono al contrario di effettuare il fork non consensuale UASF il primo agosto. In questo articolo spiego perché SegWit2x è l'upgrade giusto:

http://www.albertodeluigi.com/2017/05/29/accordo-barry-silbert-consensus-2017/

– Gli sviluppatori di SegWit2x trovano il modo di rendere compatibile il client con BIP148 (UASF), rendendo ormai inutile il tentativo di UASF, poiché già incluso in SegWit2x

– SegWit2x viene rilasciato in alpha testing il 16 giugno. Il 21 giugno (stanotte) i miners segnalano la volontà di attenersi all'accordo, la segnalazione raggiunge in un solo giorno l'80% dei consensi, ovvero la threshold prevista nell'accordo.Iscriviti alla **newsletter** per ricevere una notifica ad ogni nuovo articolo pubblicato!