Stato Avanzamento Lavori – Lightning Network: c’è speranza nel futuro più prossimo?

scritto da Alberto De Luigi | 21 Settembre 2017
Un brevissimo update sulla tecnologia Bitcoin più attesa di sempre.
Attualmente, il protocollo LN ha ancora dei grossi problemi, a detta di Rusty Russel che, per inciso, è il maggior contributor alle specifiche rfc del protocollo Lightning Network (fonte: github)

I tempi sembrano lunghi, si parla di 18 mesi secondo Lawrence Nahum di Blockstream/GreenAddress. Sappiamo poi quanto sia distante una release utilizzabile da un utente esperto rispetto a un wallet adatto alle masse e che inizi ad avere una diffusione rilevante.

I problemi irrisolti non sono affatto da poco: ironia vuole che LN, ovvero la soluzione alla scalabilità per Bitcoin… non scali! Infatti ad oggi tutti gli aggiornamenti di stato dei canali (ovvero tutte le transazioni offchain) vengono trasmesse a tutti i nodi.

La cosa è spiegata direttamente da Rusty Russel:

“There are protocol scaling issues and implementation scaling issues.
1. All channel updates are broadcast to everyone. How badly that will suck depends on how fast updates happen, but it’s likely to get painful somewhere between 10,000 and 1,000,000 channels.
2. On first connect, nodes either dump the entire topology or send nothing. That’s going to suck even faster; “catchup” sync

planned for 1.1 spec.”
(vedi fonte)

A detta di Rusty, i tre team coinvolti in tre diversi software LN stanno collaborando affinché le specifiche di ciascuno siano in compatibilità con gli altri, ma le specifiche ufficiali non possono essere ancora rilasciate per via dei problemi di cui abbiamo accennato. Rusty aggiunge che quando finalmente avranno trovato una soluzione, “i più coraggiosi inizieranno a usare LN e avremo le prime esperienze di perdita di denaro per via di bug, user experience o incidenti”. Insomma, dalla release dei primi software alfa all’utilizzo in sicurezza degli utenti, potrebbe passare davvero molto tempo.

Quindi Bitcoin è in stato di emergenza?
No, per fortuna non si scala solo tramite un layer offchain. L’upgrade a SegWit non permette solo l’applicazione di LN, quando sarà pronta, ma porta con sé anche la possibilità di utilizzare una maggiore capacità onchain. A un mese di distanza dall’attivazione, questa caratteristica non è ancora stata sfruttata molto, poiché la maggior parte di wallet e servizi non ha ancora fatto upgrade. Ma man mano che aumenta l’adozione di SegWit, la capacità onchain tende all’incirca a raddoppiarsi.
La speranza è che questo basti a non far crescere le fee nei prossimi mesi, almeno fino all’upgrade SegWit2x a fine novembre, quando la capacità onchain verrà ulteriormente raddoppiata istantaneamente, quindi senza la necessità di attendere un graduale rilascio degli aggiornamenti dei vari wallet ed exchange. Si spera che arrivando così a circa 4mb entro la fine del 2017, nei blocchi ci sia margine a sufficienza non solo per reggere l’arrivo di nuovi utenti (e quindi un aumento di transazioni), ma anche per alleggerire l’attuale costo delle commissioni. Infatti, se i blocchi non saranno interamente pieni e la mempool dovesse tornare a svuotarsi, i costi di transazione si ridurrebbero in modo più che proporzionale all’aumento della dimensione del blocco,

poiché gli utenti non dovranno più concorrere fra loro per vedersi convalidate le transazioni entro tempi ragionevoli: si potrà tornare a quei 10 o 20 centesimi che eravamo abituati a pagare fino al novembre 2016 (con rari picchi in alcuni momenti storici). Vedi il grafico.

Nell'immediato, lo scaling onchain è purtroppo l'unica soluzione efficace. Sappiamo che non è possibile esagerare con la dimensione del blocco per motivi evidenti di centralizzazione della rete (qualunque appassionato dovrebbe essere economicamente in grado di far girare un fullnode), tuttavia non ha alcun senso – dal mio punto di vista – rifiutare un upgrade che raddoppi il blocksize da 1 a 2mb (e il peso totale, o blockweight, a circa 4.2mb) come è proposto da SegWit2x.

Nelle maggiori città Italiane inizia a diffondersi la fibra a 1gb/s, quando i blocchi Bitcoin sono oggi di poco più di 1mb ogni dieci minuti e saranno circa 4mb dopo SegWit2x. Un hard disk da 3 terabyte costa 80 euro e un Intel i7 da 2.2ghz può validare circa 4000 transazioni al secondo, quando la rete Bitcoin oggi ne valida 3 o 4 al secondo. La tecnologia ci concede ogni giorno di più, non solo in occidente: quando vengono costruite nuove infrastrutture, lo si fa pressoché ovunque con la tecnologia migliore disponibile al momento.

Lo stesso Rusty Russell, impegnato nello sviluppo di LN, non ha mai nascosto simpatie per lo scaling onchain. Come vediamo sul suo blog, alla luce degli studi fatti sull'espansione della banda media disponibile, proponeva di passare a una dimensione del blocco di 3mb già nel 2016, e accrescerlo ulteriormente del 17% nel 2016. Nel luglio 2017 riprende il discorso per dichiarare che le stime fatte erano troppo pessimistiche e che la tecnologia migliora più velocemente di quanto previsto.
Non è chiaro quindi quale sarebbe il collo di bottiglia per cui l'hardware non riuscirebbe a stare dietro ad un aumento moderato del blocco. Se i supporter di Core puntano ad avere i

fullnode su smartphone, dovrebbero esplicitarlo chiaramente, allora metteremo al vaglio pro e contro di una scelta di questo tipo e il dibattito sullo scaling dovrebbe focalizzarsi sulle questioni tecniche relative.

Come i miei lettori sapranno, sono un sostenitore e divulgatore di Lightning Network della prima ora, almeno in italia (vedi le guide dedicate), ma a fronte del progresso tecnologico dell'hardware da un lato, e dei benefici che i costi di transazione possono portare a Bitcoin dall'altro, non riesco a vedere come un moderato incremento del blocco, come richiesto da SegWit2x, possa essere accusato di costituire un "attacco politico" a Bitcoin.

Non per nulla, il 94% dei miners sta ancora votando a favore di SegWit2x e dai numerosissimi firmatari del New York Agreement di maggio si è ritirata una sola azienda (l'argentina Wayniloans, che fra l'altro è di limitata rilevanza, a mio modesto parere). Non è chiarissima solo la posizione di F2pool, mining pool di Wang Chun, personaggio ambiguo e incline al trolling. I blocchi minati da F2pool in ogni caso portano ancora tutti la sigla NYA all'interno della coinbase.

La speranza è che la community metta da parte le assurde accuse di "attacchi politici" e si focalizzi sulle questioni tecniche.
Si apra la campagna elettorale dunque. albertodeluigi.com sostiene con forza SegWit2x, ma rimango aperto ad accogliere qualunque argomento sensato e ben venga se Core, o i suoi supporter, fossero in grado di convicermi del contrario.

Iscriviti alla newsletter per ricevere una notifica via email ad ogni nuovo articolo pubblicato! **CLICCA QUI**!