Bug Btc1

Btc1 è stato il client di riferimento per l'hard fork di SegWit2x pensato per novembre 2017. Il fork era stato pianificato per avvenire al blocco 494784. In realtà il blocco del fork era il 494783, come si è scoperto solo dopo che la proposta SegWit2x era stata abbandonata. Nessuno si era accorto che il programma conta i blocchi dal numero zero (il genesis block) anziché dal blocco numero 1, quindi effettivamente l'*ottantaquattresimo blocco è il numero *83. Se la proposta di fork fosse effettivamente stata portata avanti, al blocco 494782 tutti i nodi si sarebbero fermati fino alla creazione di un blocco *83 (e non *84) che avesse blocksize maggiore di 1mb. Nonostante il fork fosse annullato, il 17 novembre, quando il blocco *82 è stato minato, qualche nodo btc1 era ancora operativo, perciò ci si è accorti immediatamente dell'errore. È comunque da escludere che il fork sarebbe "fallito" per motivazioni tecniche, come sostenuto da alcuni oppositori di SegWit2x. Infatti il piano era che i nodi si sarebbero fermati al blocco del fork fino a che un miner, manualmente, non avesse creato il blocco maggiore di 1mb. Che questo blocco fosse il numero *83 o *84 è nella pratica una questione di pochi minuti di differenza. Infatti dopo essersi accorti dell'equivoco sul numero, una volta creato il primo blocco S2X, tutti i nodi forkanti avrebbero correttamente seguito quella catena.

Un'altra questione sollevata dagli oppositori di S2X è che i miners che facevano girare software btc1 non avrebbero mai potuto creare blocchi con blocksize maggiore di 1mb: il riferimento è al codice BlockAssambler del file miner.cpp, responsabile della creazione di nuovi blocchi. Qui c'è un parametro FALSE o TRUE che definisce se il maximum block weight è 4mb oppure 8mb o alternativamente, per nodi non segwit, max blocksize 1mb piuttosto che 2mb. Btc1 non definisce questo parametro, ma lascia di default in base a

quello utilizzato in precedenza. Presumibilmente, nessun miner avrebbe avuto di default il valore TRUE fino al fork, altrimenti avrebbe generato blocchi non validi prima del fork (cioè blocchi con max blockweight 8mb e max blocksize 2mb). Quindi il miner che avesse voluto creare il blocco 494783 maggiore di 1mb usando btc1, avrebbe dovuto modificare quel parametro manualmente da FALSE a TRUE solo dopo il mining del blocco 494782. Se i nodi forkanti fossero stati tutti esclusivamente client btc1, la rete avrebbe semplicemente atteso il primo miner che avesse modificato manualmente quel parametro. In realtà, poiché i principali miners fanno girare software custom e ci possono essere miners con altri software come Bitcoin Unlimited o Bitcoin Classic, quell'operazione non sarebbe nemmeno stata necessaria. In ogni caso, secondo i piani il fork sarebbe stato attivato manualmente da un miner, non automaticamente: il tema era già stato sollevato in dibattito fra Luke Dashjr e Jeff Garzik, come spiegato a Luglio 2017 in questo articolo: http://www.albertodeluigi.com/2017/07/17/storia-e-upgrade-del-bitcoin/#13 La ratio era proprio quella di garantire il la compatibilità di Btc1 con tutti i nodi della rete fino al momento del fork (quindi anche con Core) e di rimanere compatibile col maggior numero possibile di nodi dal fork in poi. Una maggiore review del codice di btc1 e un testing più approfondito avrebbero evitato l'equivoco sul numero de blocco 494784, la cui colpa è stata imputata principalmente a Jeff Garzik, primo dev di S2X.