Scoperto un bug nel codice di Bitcoin: quali sono le conseguenze

La recente scoperta di un bug nel codice Bitcoin non è un caso isolato, ma è pur sempre un evento rarissimo, che non capitava da oltre 5 anni. Certamente è un caso eclatante che fa riflettere su alcuni temi.

In passato, in tutta la storia di Bitcoin sono stati scoperti due bug critici, che hanno richiesto un fork della blockchain per essere corretti, rispettivamente il 15 agosto 2010 e l'11 marzo 2013.

I BUG "STORICI" DI BITCOIN

Il **15 agosto 2010** il blocco numero **74638** è stato creato con **184 milioni di bitcoin**, versati in 3 distinti indirizzi, di

cui due da 92 milioni di btc. Il codice che controllava la correttezza delle transazioni era buggato poiché non prevedeva un controllo per output così grandi: un po' come se volessimo controllare una transazione che trasferisce oltre 100 bitcoin, ma ogni volta che arriviamo a 99 il sistema riparte a contare da zero. Un miner ha sfruttato questa "falla" per creare bitcoin oltre la quantità prevista. Da qui, il nome con cui è conosciuto l'evento: "overflow value incident". Dopo 5 ore dal fatto, è stata sviluppata una patch e i primi miners ad installarla hanno creato un blocco 74638 alternativo, questa volta "corretto". Tecnicamente la patch rappresentava un soft fork, perciò fino al momento in cui i miners con patch non hanno superato (in potenza di calcolo) quelli con il vecchio software, la stragrande maggioranza di nodi della rete ancora riconosceva come la "vera" blockchain Bitcoin quella corrotta, con 184 milioni di bitcoin creati in un solo blocco. **I nodi aggiornati hanno prevalso soltanto al blocco 74691**, creando un numero di blocchi maggiore rispetto alla catena concorrente. In totale, dalla scoperta del bug, erano passate 8 ore e mezza prima che la situazione fosse ritornata alla normalità.
La patch era stata rilasciata direttamente da **Satoshi Nakamoto** con un post su bitcoin talk https://bitcointalk.org/index.php?topic=827.0 seguito dalla traduzione in ogni lingua (la prima, come sempre, in italiano dal nostro Franco Cimatti).

Relativamente a quell'evento del 2010 non si hanno notizie di danni economici riportati dagli utenti, anche perché a quel tempo non esisteva un'economia intorno a Bitcoin. Ricordiamo che le prime quotazioni di Bitcoin che lo davano a 0,007 dollari risalgono al marzo 2010. Nonostante il prezzo abbia avuto un incremento del 900% nel luglio dello stesso anno, passando in soli 5 giorni a circa 0,08 dollari (8 cent di dollaro), le transazioni erano estremamente rare, quindi sarebbe stato molto difficile per un attaccante sfruttare il momento di confusione del fork, per tentare di vendere i propri bitcoin (spendendoli sulla catena corrotta), e

trasferirli al contempo in un proprio wallet nella blockchain sana. Non essendoci replay protection fra i due fork, non c'è nemmeno certezza che il tentativo di frode andasse a buon fine.

Nel **2013** invece c'era già un'economia piuttosto viva intorno a Bitcoin. Il **fork dell'11 marzo** è stato risolto entro 6 ore circa dalla scoperta del problema, ne ho parlato estensivamente qui: storia-e-upgrade-del-bitcoin/#3
In quella situazione si ha notizia di un solo **caso in cui un utente abbia effettuato un double spending** (ai danni del servizio OKPay) e non fu tanto un tentativo di frode, quanto piuttosto un test da parte di quell'utente che si accorgeva in quel momento dell'anomalia.

LA SCOPERTA DEL 17 SETTEMBRE 2018

Pochi giorni fa, uno sviluppatore (sotto pseudonimo) che stava lavorando sul codice di Bitcoin Cash ha scoperto un bug critico. Inizialmente, pensava fosse soltanto un bug del software Bitcoin ABC, ovvero il full node di riferimento di Bitcoin Cash. In realtà, si è presto accorto che ABC aveva ereditato quelle linee di codice direttamente da Bitcoin Core, il principale full node di Bitcoin. Un miner malevolo quindi avrebbe potuto sfruttare il bug per tentare un attacco su Bitcoin, non soltanto su Bitcoin Cash. Fortunatamente **la notizia dell'esistenza del bug è arrivata prima agli sviluppatori che a possibili hacker malintenzionati. In una giornata la rete è stata messa in sicurezza, prima che chiunque altro potesse anche solo pensare a un attacco**.

Ma di che bug si tratta? E cosa sarebbe potuto succedere se il bug fosse stato scoperto prima da un attore malevolo? E a quel punto che contromisure avremmo dovuto prendere? Come si possono prevenire altre situazioni simili in futuro? Vediamo passo a passo la risposta a queste domande.

DAL BUG AL FIX IN 5 ORE

Alle **14.57 del 17 settembre** lo sviluppatore di Bitcoin Cash contatta alcuni dei principali dev del software Bitcoin Core (Pieter Wuille, Gregory Maxwell, Wladimir Van Der Laan) e il principale dev di Bitcoin ABC (Amauri Sechet) per comunicare la sua scoperta. Gregory Maxwell condivide il report con altri Core developers, fra cui **Matt Corallo, che aveva scritto le righe di codice incriminate**. Matt Corallo stesso si accorge che il bug è anche più grave di quanto riportato. In breve tempo viene scritta una patch che viene inviata ad una mining pool, la prima contattata (Slushpool), la quale effettua **l'upgrade alle ore 20.48**. Un'ora circa dopo (21.57) l**a patch viene resa pubblica, sia per Bitcoin Core che Bitcoin ABC**. Nel frattempo vengono contattate alcune persone chiave nell'ecosistema Bitcoin al fine di assicurarsi che tutti i principali miners o mining pools venissero a conoscenza degli eventi ed effettuassero l'upgrade al più presto. Dalla sera del giorno dopo (18 settembre) la situazione è ritenuta ormai sicura, poiché **la maggior parte dell'hashrate della rete ha aggiornato alla nuova versione del software**, e la notizia viene comunicata sui principali canali come bitcointalk e reddit, così da raggiungere un vasto pubblico di utenti. Pieter Wuille il 19 settembre scrive nella mailing list ufficiale, sollecitando a tutti l'upgrade.

IL CODICE FALLATO RISALE AL 10 NOVEMBRE 2016

Il 10 novembre 2016 è stata approvata una **modifica al codice di Bitcoin Core che ottimizza i tempi che i nodi impiegano per validare le transazioni, rimuovendo alcuni "controlli"** ridondanti (che fanno perdere al nodo circa 0.6 millisecondi durante la validazione del blocco ricevuto dal miner). Vedi: https://github.com/bitcoin/bitcoin/pull/9049
Ciò di cui nessuno si era accorto è che **questa modifica non era stata fatta compiutamente:** in particolare, non prevedeva che un miner malevolo con buone capacità di hacking avrebbe potuto modificare il proprio software bitcoin con l'intento di creare blocchi che includessero transazioni anomale. Nello

specifico, **il miner avrebbe potuto includere una propria transazione nel blocco, replicandola all'infinito, inviando a un proprio wallet più e più volte l'output (effettuando quindi double spending)**. Bisogna specificare che un qualsiasi miner bitcoin ha sempre potuto (e sempre potrà in futuro) manipolare e modificare il codice di Bitcoin, al fine di produrre un blocco in cui è presente un double spending, ma questo fatto non è certamente un bug. Il fatto che chiunque possa modificare il codice del proprio software bitcoin non è un problema finché i nodi "sani" risultano incompatibili con la modifica e quindi rifiutano le informazioni corrotte provenienti da nodi manipolati. Tuttavia, mancando dal novembre 2016 quel controllo aggiuntivo su Bitcoin Core (versione 0.14 e successive), una transazione anomala come quella descritta non viene espressamente rifiutata dai nuovi nodi Bitcoin Core.

COSA SAREBBE SUCCESSO IN CASO DI ATTACCO?

I nodi Bitcoin Core 0.14 che avessero ricevuto il nuovo blocco propagato dal miner malevolo avrebbero notato che c'era qualcosa di strano, senza però riuscire a individuare cosa, perciò **si sarebbero fermati, andando in crash**. Insomma l'attaccante sarebbe riuscito a far crashare un certo numero di nodi, inviando nella rete una sorta di "blocco velenoso". Un attacco di questo tipo è detto **Denial of Service (DOS)** poiché inabilita i nodi della rete ad operare e prestare servizio.

Bitcoin Core 0.14 non era però l'ultima release di Core, poiché circa un anno fa, **il 14 settembre 2017, è uscita la versione 0.15, in cui è stato fatto un ulteriore cambiamento al codice che permane fino alla vesione 0.16.2. Questi nodi più recenti non sarebbero affato crashati, bensì avrebbero accettato il blocco "velenoso", permettendo a tutti gli effetti una inflazione infinita.** Di questo particolare se ne è accorto Matt Corallo non appena è stato avvisato del bug. Insomma, per assurdo il protocollo di Bitcoin Core poteva

ammettere (almeno sotto particolari condizioni) una supply illimitata di Bitcoin, anziché il famoso tetto di 21 milioni che spesso si dice essere "garantito" da arcane leggi matematiche. Insomma il bug poteva essere per molti nodi ben più grave che un semplice crash temporaneo del nodo, che si risolve aggiornando il software e riavviando. Guido Dassori ha poi sfruttato il bug in testnet facendo forkare il network nell'ambiente di test, qui il suo report.

Bisogna notare che i nodi bitcoin con versioni 0.14 e successive erano, fino a pochi giorni fa, quelle presenti in maggior numero nel network Bitcoin (ad oggi la versione 0.16.3 patchata è quella preponderante), mentre le versioni del tutto immuni all'attacco (0.13 e inferiori) sono un numero decisamente minore. Ci sono altri nodi immuni, ovvero tutti quelli con implementazioni diverse da Bitcoin Core (scritte anche in altri linguaggi, ad esempio btcd, bcoin e Bitcoin Unlimited), tuttavia **si può stimare che i nodi immuni ammontassero a circa il 10% del totale, mentre il 90% della rete di full nodes era costituito da nodi Bitcoin Core con versioni fra la 0.14 e la 0.16.2** (https://coin.dance/nodes).

Ma nei fatti, come il bug avrebbe danneggiato gli utenti? **Probabilmente i danni sarebbero stati abbastanza contenuti, come nei casi visti nel 2010 e 2013. Il 10% della rete (i nodi immuni) avrebbero forkato dal network**, poiché non avrebbero riconosciuto il blocco malevolo, di conseguenza tutta la rete si sarebbe accorta dell'anomalia e **in poche ore gli sviluppatori avrebbero individuato e fixato il bug**. Il fork della blockchain costruito sul blocco malevolo, anche se inizialmente maggioritario in hashrate, sarebbe stato presto scartato e abbandonato. Tutte le transazioni oneste validate sul ramo malato della blockchain sarebbero state validate anche sul ramo sano (in assenza di replay protection, i miners attingono liberamente dalla mempool), mentre ogni transazione che coinvolgesse i bitcoin creati "dal nulla" dal miner attaccante sarebbero state definitivamente scartate dai nuovi

software aggiornati e non inserite nella blockchain sana. **Nessun utente si sarebbe dovuto preoccupare per i bitcoin custoditi al sicuro nei propri wallet**, nessun indirizzo bitcoin avrebbe potuto perdere un solo centesimo, semmai gli utenti avrebbero sperimentato un disservizio generale della rete per alcune ore, senza riuscire a effettuare transazioni o senza vedere le conferme delle transazioni effettuate. Gli unici casi a rischio sarebbero stati quegli utenti o servizi che stavano transando proprio nel momento del fork, qualora fossero coinvolti in transazioni da e verso utenti esperti e in malafede, che consci di quanto stesse accadendo tentassero di sfruttare la confusione del fork a loro beneficio. Probabilmente la maggior parte dei servizi si sarebbero fermati accorgendosi dell'anomalia, in attesa di un ripristino delle funzionalità della rete.

L'ATTACCO SAREBBE STATO CONVENIENTE?

Un attacco di questo tipo non rappresenta un guadagno diretto per il miner attaccante, quantomeno non senza tentare strategie complesse e rischiose. Ad esempio, **il miner avrebbe potuto provare a shortare bitcoin (scommettere al ribasso) sulle piattaforme di trading**, sperando in un crollo del prezzo alla notizia del fork e del crash dei nodi 0.14. Non vi è certezza però che il prezzo avrebbe seguito la notizia. In effetti, ad oggi non ci sono esempi che ci fanno pensare che il mercato presti sempre tanta attenzione a questi fattori (lo abbiamo visto anche con Verge in questo articolo). Ne è riprova anche il fatto che il prezzo di Bitcoin in questi giorni non sembra aver accusato il colpo della notizia del bug.

Un altro tentativo di attacco sarebbe potuto essere effettuato contro un servizio come un exchange: il miner avrebbe dovuto depositare i bitcoin generati sfruttando il bug e quindi venderli e ritirare dall'exchange i propri valori, il tutto prima che l'exchange bloccasse il servizio. Il guadagno non è assicurato per varie ragioni:

    1. L’exchange avrebbe potuto **bloccare ogni servizio non appena individuato il fork**

    1. Se l’exchange avesse usato **nodi 0.14**, questi **crashando avrebbero comunque negato la possibilità per il miner di depositare bitcoin** presso l’exchange

    1. Se l’exchange avesse usato **nodi 0.13 immuni al bug**, o comunque implementazioni alternative o custom rispetto a Bitcoin Core, avrebbe rifiutato la transazione del miner

1. Il miner avrebbe avuto una **finestra di tempo molto ridotta** per effettuare deposito e prelivo dall’exchange. Nel caso del deposito in bitcoin soprattutto, sono generalmente necessarie 6 conferme, le quali possono anche durare molto più di 10 minuti ciascuna in caso di fork (dato che l’hashrate cala poiché i miners spengono le macchine per aggiornare, mentre i miners con la 0.14 smettono di lavorare per via del crash). Insomma, prima della fine dell’operazione fraudolenta, l’exchange avrebbe potuto bloccare il servizio, o il network Bitcoin in generale avrebbe già rimediato al bug

Dall’altro lato, per il miner un attacco del genere costituisce **un costo chiaro e immediato**, ovvero quello di spendere soldi (hardware, energia elettrica) per la **potenza computazionale necessaria a creare il blocco malevolo**, il quale verrà chiaramente **rifiutato dalla rete, che forka sulla catena alternativa** per proteggersi dall’attacco. Il **miner rinuncia così ad almeno 12,5 bitcoin di guadagno (80,000 dollari) che avrebbe ottenuto minando un blocco sano,** sostenendo in più un costo notevole per noleggiare o acquistare hashrate. Inoltre, va calcolato anche un **costo (o tempo) non indifferente che è richiesto al fine di sviluppare la versione alternativa di software** per produrre il “blocco velenoso”. Se poi il miner malevolo fosse una mining pool, ci

sarebbe anche un **costo reputazionale** per aver lanciato l'attacco (molti utenti e "clienti" potrebbero abbandonare la pool). In generale, è **improbabile che un miner adotti strategie che possano inficiare negativamente sul prezzo di Bitcoin** in cui è presumibilmente investito.
Per farla breve, se anche il bug fosse stato di pubblica conoscenza per molti giorni prima del fix degli sviluppatori, non è detto che sarebbe mai stato tentato un attacco.

BISOGNA PREOCCUPARSI PER IL FUTURO?

La sola possibilità che, anche in futuro, vengano sfruttati dei bug di Bitcoin, dovrebbe preoccuparci? Dalle ore 2:54:25 del 3 gennaio 2009, ovvero dalla nascita del Genesis block ad oggi, **il network Bitcoin ha funzionato per il 99,992566424% del tempo in cui è ad esistenza** (vedi il counter aggiornato real time). Altri strumenti di pagamento digitali non decentralizzati non sono in grado di garantire la stessa costanza, poiché personale, server e database fondamentali per il loro funzionamento sono necessariamente localizzati in luoghi ben precisi. **Qualsiasi sistema centralizzato è meno resiliente e più soggetto a incidenti locali,** attacchi di qualsiasi tipo o ordini da parte delle autorità (per le motivazioni più disparate, dalla mancata compliance ai capricci delle amministrazioni pubbliche). Per fare un esempio, il primo gennaio di quest'anno il funzionamento di Visa ha avuto una brusca interruzione, mentre il 12 luglio di quest'anno anche Mastercard ha avuto problemi. E parliamo solo dei primi esempi relativi a quest'anno.

L'errore umano è una variabile che non si può eliminare, in qualsiasi tecnologia, anche quelle che sono ormai del tutto indispensabili ed usamo tutti i giorni, come il wifi. Nell'ottobre 2017 è stata scoperta una falla di sicurezza nel sistema WPA2 che, se sfruttata, rendeva potenzialmente accessibile buona parte dei dati che i dispositivi scambiano tra loro sulle reti wifi. Insomma ogni wifi del mondo era potenzialmente vulnerabile. Oppure, pensiamo ad altri bug

“storici” come il millenium bug, che sviluppatori, esperti e aziende di tutto il mondo non hanno saputo anticipare, nonostante l’impatto incredibilmente esteso a ogni settore e i potenziali danni. Anche se nessun sistema sarà mai perfetto, la sicurezza di Bitcoin è ineguagliata dalle alternative (pensiamo soltanto a quante carte di credito vengono clonate e le frodi bancarie), ma è ingenuo pensare che prima o poi non si riscontri un bug. I programmi sono figli degli esseri umani e come tali non sono mai perfetti.

Quindi come possiamo arginare al più possibile un problema di questo tipo nella rete Bitcoin? Anzitutto, possiamo lavorare per rendere tale problema il **meno possibile sistemico**. Se ci fossero **molte implementazioni diverse e diffuse di full nodes**, ci sarebbero anche **più bug (per un semplice fatto statistico), ma ogni bug sarebbe limitato alla singola implementazione**, con un impatto localizzato a una piccola percentuale di nodi. Parlavo proprio di questo problema in un articolo già oltre un anno fa: dei rischi ci saranno sempre, in ogni sistema creato dagli esseri umani, ciò che bisogna fare è rendere il sistema il più possibile anti-fragile e resiliente, evitando ogni “**single point of failure**“. Quindi il network di aziende, sviluppatori e appassionati dietro a Bitcoin dovrebbe impegnarsi ad aggiornare costantemente un **documento che definisce il protocollo Bitcoin**, ovvero l’insieme delle regole del consensus, che siano **distinte dall’implementazione software più diffusa (Bitcoin Core)**. Andrebbe insomma condiviso quel tipo di documento che nelle comunità scientifiche è chiamato RFC (request for comment), purtroppo ad oggi mancante. La presenza stessa di RFC condivise dall’intera community sarebbe di incoraggiamento per quegli sviluppatori che volessero implementare nuovi software fullnode, anche in linguaggi di programmazione diversi.

Segui gli aggiornamenti quotidiani sulla pagina facebook: https://www.facebook.com/albertodeluigi.news
Iscriviti alla newsletter del blog per ricevere una notifica

ad ogni nuovo articolo pubblicato