Come abbiamo visto Blockchain è una tecnologia potenzialmente ottima che può essere sfruttata in molte situazioni, ma la proof-of-woork, che al momento è la soluzione più utilizzata in larga scala per garantirne la sicurezza, è la soluzione migliore che abbiamo adesso a disposizione? I benefici offerti da blockchain devono per forza essere controbilanciati dai notevoli effetti collaterali derivati dalla sua misura di sicurezza più utilizzata?

**Attacchi 51%**

La ragione principale per adottare l’approccio della proof-of-work è per evitare I cosiddetti attacchi 51%. Un attacco 51% consiste nell’usare più del 50% della potenza dell’intera rete per modificare a proprio piacimento lo storico delle transazioni all’interno della blockchain. Ma il protocollo proof-of-work garantisce davvero l’immunità da questo tipo di attacchi? Ed è davvero il deterrente migliore per impedirli? Per provare a dare una risposta a queste domande prenderemo in analisi due casi in cui una rete blockchain, basata su algoritmo di consenso di proof-of-work, si è ritrovata esposta ad una forza che possedeva più del 50% della potenza di calcolo di quella rete.

***Attacchi 51% ethereum classic***

Il primo esempio che andiamo ad osservare è quello di un attacco 51% andato effettivamente a segno, seppure su una rete diversa da bitcoin. Il 5 gennaio del 2019 Ethereum Classic, la versione minore di Ethereum, ha subito un attacco 51% che è stato scoperto 24 ore dopo l’accaduto. Un utente è riuscito a controllare per qualche ora il 60% della potenza di mining della rete, e nel frattempo ha creato una sequenza alternativa della blockchain che ha sfruttato per eseguire il cosiddetto *double spending*. Una volta scoperto dell’attacco la moneta è stata congelata e gli scambi sospesi dai vari circuiti di trading (a causa dell’imminente crollo dovuto alla violazione dei protocolli di sicurezza della moneta), ma nel frattempo l’utente che ha effettuato l’attacco, prima che l’infrazione venisse alla luce, avrà sicuramente capitalizzato su quanto guadagnato.

È importante segnalare una cosa: la complessità della rete bitcoin al momento dell’attacco era circa 20 volte superiore a quella della rete Ethereum Classic, quindi un attacco di questo tipo su rete bitcoin sarebbe stato diversi ordini di grandezza più costoso, forse neanche remunerativo. Questo però non vuol dire che sia impossibile controllare la maggior parte della potenza di calcolo della rete. Come vedremo nel prossimo esempio, infatti, in passato è già successo.

***Ghash.io***

GHash.Io è stata una mining pool che ha operato sulla rete bitcoin, ma anche su altre altcoin, dal 2013 fino al 2016. GHash.Io consentiva ai miner al proprio interno di minare tramite hardware personale, o tramite cloud-mining collegandosi al circuito di scambio CEX.IO. È importante focalizzarsi su questa feature del cloud mining, poiché questa è una pratica che permetteva agli investitori di entrare ed uscire rapidamente dal mercato del mining senza preoccuparsi troppo di dover acquistare e mantenere a lungo termine l’hardware necessario per il mining. La facilità di ingresso e di uscita offerta dal cloud mining ha consentito alla rete GHash.IO, nel luglio del 2014, di superare da sola il 50% della potenza di calcolo dell’intera rete bitcoin. La possibilità incombente di un eventuale attacco 51% mise in discussione la sicurezza della rete, con conseguente crollo immediato del valore della moneta. Per arginare il problema in tempi rapidi, ed impedire che il valore della moneta crollasse ulteriormente, fu la mining pool stessa ad autoimporsi di non superare il limite del 40% della potenza di calcolo complessiva dell’intera rete. Inoltre, dopo essersi autolimitata, la pool stessa propose di creare una commissione che vigilasse affinché non si ripetessero situazioni simili.

I due casi precedenti ci permettono di fare due osservazioni: da un lato la proof-of-work non è una misura di sicurezza sufficiente per impedire un attacco 51% da parte di una forza esterna alla rete, e dall'altro è superflua quando l’attacco potrebbe essere invece di matrice interna, poiché sono gli stessi partecipanti della rete, anche coloro che detengono la maggior parte della potenza del network, a non volere che la trasparenza e la legittimità della rete siano a rischio.

Più nello specifico, partendo dal caso di un possibile attacco interno, il deterrente maggiore per un simile attacco non è dato tanto dal costo necessario per affittare le macchine per portare a termine un compito simile, ma dal fatto che minare la trasparenza e la sicurezza della blockchain metterebbe in discussione il valore stesso della moneta: se la moneta non è sicura il suo valore crolla, e chi ha effettuato l’attacco 51% si ritrova con un pugno di mosche in mano. Anche laddove le intenzioni non fossero malevole, come si è visto nel caso della pool Ghash.io, la minaccia di un possibile accentramento della rete porterebbe ad un’insicurezza di fondo che avrebbe come unico esito quello di abbassare il valore della moneta in quanto potenzialmente non sicura.

D’altro canto, minare la sicurezza della moneta, e quindi farne crollare il valore, può essere la ragione più valida per eseguire un attacco di matrice esterna. In questo caso, chi prende il controllo della maggior parte della potenza del network non ha interesse a mantenere la stabilità della rete: o lo fa per danneggiarla dall’esterno, con una sorta di attacco goldfinger che ha magari lo scopo di danneggiare una moneta per favorirne un’altra, o lo fa per cercare di accumulare una quantità di capitale da convertire prima che l’attacco venga scoperto e il valore della moneta scenda.

Abbiamo dunque visto che proof-of-work non è un algoritmo di consenso in grado da solo di difendere la stabilità di una blockchain, e quindi come mai continua ad essere così utilizzato, specialmente per una valuta come Bitcoin che rappresenta ad oggi il gold standard del mercato delle crypto? Non esistono soluzioni più sicure?

È difficile dare una risposta netta a queste domande: da un lato abbiamo visto che proof-of-work è un protocollo aggirabile, ma dall’altro come facciamo a dimostrare che esistano soluzioni più sicure? E soprattutto, quanto più sicure e a che costo?

Da quel che abbiamo visto proof-of-work è un protocollo che, con l’aumentare delle dimensioni della rete, scala malissimo a livello di consumi, ma fa in modo che questi consumi siano il deterrente più forte per chiunque voglia provare a forzarlo. In sostanza, l’indice di sicurezza di una blockchain basata su proof-of-work dipende da quanto è necessario spendere per ottenere la maggior parte della potenza di calcolo della suddetta rete: è una questione di costi, non di difficoltà. Non discuteremo sull'efficacia di considerare I costi di un attacco come un deterrente più sicuro rispetto all'imporre dei protocolli di difesa attivi difficili da superare su un piano tecnico, non è lo scopo di questa ricerca ed è tuttora un argomento di discussione che non ha trovato risposte chiare, perciò ci allineeremo alla filosofia vigente secondo la quale più un attacco è costoso, più esso sarà difficile da realizzare.

In questa ottica, esistono algoritmi di consenso che, per essere violati, impongano dei costi di attacco superiori a quelli richiesti da un attacco 51% su una blockchain protetta da proof-of-work?

Non solo la risposta a questa domanda è sì, ma anzi: esistono algoritmi di consenso più costosi che, oltretutto, non richiedono alcun esborso energetico di mantenimento.

**L’esempio di Ethereum: Casper**

Casper è l’algoritmo di consenso che andrà a convertire Ethereum, che attualmente si appoggia a proof-of-work (seppur diversa dal punto di vista tecnico da quella di bitcoin), in una blockchain Proof-of-Stake entro il 2020. In una blockchain proof-of-stake non esistono miners, il processo di verifica e di convalida dei blocchi di transazioni non dipende dalla risoluzione di problemi crittografici di difficoltà arbitrari, ma convalidatori di blocchi che vengono selezionati in base alla loro possibilità di mettere una posta in gioco. Il potere di voto di ogni validatore è determinato infatti non dalla potenza di calcolo a sua disposizione, ma dalla somma di ETH (la valuta di Ethereum) che può mettere in gioco per votare: maggiore sarà la posta in gioco, più alto sarà il suo potere di voto (ad esempio, se un utente mette in gioco 64ETH ed un altro ne mette 32, il voto del primo utente varrà il doppio rispetto a quello del secondo). I comitati per la validazione sono scelti di volta in volta in maniera casuale, e I membri di questi comitati vengono premiati non tramite una ricompensa generata alla validazione del blocco, ma suddividendo le tasse sulle varie transazioni all’interno del blocco. In realtà il sistema di ricompense di casper non è ancora ben definito, però possiamo comunque osservare alcune peculiarità che distinguono questo algoritmo di consenso da proof-of-work.

Dare maggiore potere di voto a chi ha più ETH può all’apparenza sembrare una misura ingiusta e antidemocratica, ma c’è una cosa di cui tenere conto: non è troppo diverso da quello che già accade su reti proof-of-work, dove i miner più potenti validano la maggior parte dei blocchi e, oltre a guadagnare di più rispetto a tutti gli altri validatori, controllano anche la maggior parte delle transazioni nella rete. Nel caso di Casper però I vantaggi sono diversi.

In primo luogo, I candidati sono scelti in modo casuale, la rete diventa automaticamente più decentralizzata perché non sono più I partecipanti più potenti del network a controllare I flussi di transazioni, e di conseguenza è molto più difficile entrare sistematicamente in tutti I sistemi di votazione (cosa che, per un utente che controlla la maggior parte della potenza di calcolo di una blockchain proof-of-work, facendo un parallelismo tecnico sarebbe invece quasi automatica).

In secondo luogo, se si considera il criterio di sicurezza definito in precedenza, un attacco su rete Casper è più costoso e più inefficiente rispetto ad un attacco su rete proof-of-work. Più costoso perché richiede l’acquisto di una quantità molto elevata di valuta: per convalidare un blocco fraudolento l’utente truffaldino deve possedere più valuta di tutti gli altri membri validatori messi insieme, e un tentativo fallito di validazione fraudolenta viene punito col sequestro della somma messa in gioco e con l’espulsione dal network. Più inefficiente perché l’utente fraudolento non può decidere arbitrariamente in quali gruppi di validazione entrare, sono scelti casualmente, e l’unico modo che ha per aumentare le sue possibilità di entrare in una commissione di convalida è quello di avere più portafogli possibili con quantità di valuta spropositate.

È chiaro che, in uno scenario simile, un attacco su una rete Proof-of-stake risulta molto più costoso e molto più improbabile rispetto ad un attacco su rete proof-of-work. Questo rende proof-of-stake completamente sicura? No, perché I comitati di validazione possono in linea teorica essere pilotati, la rete non è immune ad esempio alla corruzione (un utente fraudolento può corrompere gli altri convalidatori per farli votare a suo favore), ma per gli stessi motivi che abbiamo visto prima gli attacchi di questo tipo risultato ancora più improbabili: per eseguire un attacco è necessaria una enorme quantità di valuta, e un attacco che viene scoperto porta ad un crollo del suo valore, dunque non è nell’interesse di chi controlla molta valuta svalutarla in maniera drastica. Il discorso ovviamente è valido per un attacco di matrice interna; per un attacco esterno che ha come unico scopo quello di danneggiare la rete il discorso non può reggere, però Casper può arginare in parte anche il problema degli attacchi *blitzkrieg* (gli attacchi fulminei in cui un utente fraudolento si appropria indebitamente di più valuta possibile da vendere prima che l’attacco venga scoperto) che abbiamo visto nel caso delle reti proof-of-work, perché per un attacco su Casper serve moltissima valuta, e vendere grosse quantità di capitali, oltre ad essere difficile e sicuramente non immediato, può rappresentare un campanello d’allarme che indica la presenza di un attacco (o anche di una svalutazione della moneta).

In sostanza, per quanto riguarda la protezione dagli attacchi interni, il modello di sicurezza di proof-of-stake/Casper è un modello economico puro; lo stesso vale per gli attacchi esterni che però, a differenza di quanto accade nei sistemi proof-of-work, sono molto più costosi e meno efficienti. Se prendiamo come riferimento Il criterio di sicurezza definito in precedenza, basterebbe già questo per definire Casper un modello più sicuro rispetto a proof-of-work, ma c’è un altro aspetto a favore di Casper che non abbiamo considerato: Casper è un processo non intensivo che consuma pochissima energia elettrica e che non richiede hardware specifico.

Casper è dunque non solo un sistema più sicuro rispetto a proof-of-work, ma se applicato su larga scala risolverebbe anche completamente il problema dei consumi energetici, e del relativo inquinamento, visto finora.

**Conclusione**

Ma può Casper, o comunque un sistema basato su proof-of-stake, risolvere da solo il problema energetico generato dal mondo delle crypto? La risposta è: probabilmente no.

Proof-of-stake è un protocollo di consenso conosciuto ormai da diverso tempo, applicato da diverse blockchain con ottimi risultati, ma questo non è comunque bastato per far sì che la rete più grande, la blockchain di Bitcoin, passasse da un sistema energivoro ad un sistema nettamente più sicuro e sostenibile. Come mai? Una risposta precisa non c’è: da un lato sicuramente I miners e I produttori di hardware destinato al mining hanno enormi interessi per far sì che il sistema non cambi, ma dall’altro lato non si può neanche escludere che l’atteggiamento conservativo della rete non sia dovuto semplicemente all’indolente filosofia del “se non è rotto, non aggiustarlo”. Quel che è certo è che finché il gold standard, che per ora è bitcoin, non deciderà di spostarsi su un sistema più virtuoso e meno energivoro non c’è ragione di pensare che il problema dei consumi si possa risolvere in breve termine. Se da un lato l’introduzione da parte della seconda forza nel mercato di un algoritmo di consenso come proof-of-stake non può che essere un ottimo segnale, e lo dimostra il fatto che il solo annuncio nel 2019 ha contribuito ad aumentarne parecchio il valore, dall’altro è proprio questo aumento che potrebbe risultare un’arma a doppio taglio: finché il gold standard resta bitcoin il suo valore sale all’aumentare del prezzo delle altre crypto, ma se il suo valore sale anche l’interesse per il mining aumenta, e con esso I consumi. In definitiva, finché non si stabilisce un nuovo gold standard, o fino a quando il gold standard in vigore non decide di passare ad un sistema più virtuoso, è difficile pensare di eliminare completamente il mining e tutti I problemi da esso derivati.

Le soluzioni al problema dei consumi e dell’inquinamento delle reti blockchain non virtuose insomma esisterebbero anche, ma sta al buonsenso e alla responsabilità dei membri della rete far sì che esse vengano adottate: sviluppatori, miner, o investitori che siano. Come nel caso dell’oro e della pirite, è importante sapere come distinguere e separare i due minerali, capire cosa accomuna e cosa distingue l’oro vero da quello degli stolti per evitare di essere ingannati solo dal colore. Blockchain e le applicazioni ad essa connesse sono oro, proof-of-work è solo il colore che spesso le accomuna, non è un tratto caratterizzante. È pirite.