Storia di Bitcoin

Contents

1 Le idee che hanno portato a Bitcoin **1**

2 Satoshi Nakamoto - 2007/2011 **1**
2.1 18 agosto 2008 1
2.2 31 ottobre 2008 3

3 Gli anni della puberta' del protocollo **4**

4 Block size war **4**

1 Le idee che hanno portato a Bitcoin

Questa parte e' lasciata inizialmente vuota perche' oltre alla prima puntata del podcast vorrei aggiungere informazioni da questo talk:

https://www.youtube.com/watch?v=SDHHBJnmDVA

2 Satoshi Nakamoto - 2007/2011

Anche se la prima traccia comprovata dell'esistenza di Satoshi Nakamoto e di Bitcoin e' del 2008 ci sono diversi post pubblici in cui Satoshi commenta casualmente di aver cominciato a lavorare sul codice nel 2007, quindi possiamo gia' aspettarci che nel 2007 qualcuno, una persona o gruppo di persone stava gia' lavorando a Bitcoin. Questo e' pero' solo un claim di cui non abbiamo prove, anche se non c'e' una ragione logica per cui Satoshi abbia mentito sulla data d'inizio del suo lavoro.

2.1 18 agosto 2008

La vera e propria storia documentabile di Bitcoin nasce invece il 18 agosto 2008, quando viene registrato il dominio bitcoin.org. La storia dietro la registrazione del dominio e' molto interessante, perche' anche se sappiamo che con whois si puo' vedere il nome di chi ha registrato il dominio (con un mandato se siamo la CIA o con un po' di social engineering). Ma dalla registrazione possiamo

vedere che chi ha registrato bitcoin.org l'ha fatto usando un sistema chiamato Anonymous Speech, che permetteva di pagare per registrare il dominio che si voleva. Questa compagnia registrava a nome suo il dominio e poi cancellava l'identita' pubblica del proprio ente legale come registratore e poi trasferiva le chiavi di accesso al registrante. Era quindi in sostanza un proxy che tramite un entita' legale registrava siti. Questo sito non esiste piu' adesso, esistono pero' servizi alternativi che permettono di fare la stessa cosa, e come unico metodo di pagamento accettano proprio bitcoin. Come ha pagato quindi Satoshi Nakamoto nel 2008? Ai tempi Anonymous Speech accettava pagamento in contante inviato per posta oppure e-gold. Possiamo supporre che Satoshi abbia usato proprio quest'ultimo per effettuare il pagamento. Non abbiamo purtroppo modo di andare a chiedere ad Anonymous Speech in quanto non esiste piu' come societa', ed essendo una societa' che favoriva la privacy degli utenti immaginiamo che non l'avrebbe detto, anche se e' un informazione che immaginiamo essere in mano ai law enforcement di tutti i paesi. E' interessante notare questo serpente che si morde la coda, in quanto un sito centralizzato e' stato chiuso e confiscato, ma viene usato per registrare un dominio con cui viene promosso il suo successore decentralizzato. Questo non vuol dire che senza un sito con un dominio satoshi non avrebbe potuto lanciare Bitcoin, dato che il modo con cui l'ha lanciato e' stato principalmente tramite mailing list, e il sito e' diventato rilevante solo dopo molto altro tempo. Oltre all'uso di e-gold l'altra curiosita' legata al sito bitcoin.org e' che anche se Anonymous Speech non richiedeva per forza un nome ai clienti assegnava loro un id, da cui si vede che questo cliente ha comprato un altro dominio, cioe' netcoin.org, che ci racconta l'indecisione di Satoshi nel nome da dare al suo progetto.

L'altra domanda che ci possiamo fare e' come Satoshi pagasse l'hosting del sito. Questo non possiamo saperlo dato che Anonymous Speech non rivelava i dati dei suoi clienti, ma immaginiamo che anche questa informazione sia in mano a qualche entita' di law enforcement, anche se immaginiamo che chi si e' preso la briga di registrare bitcoin.org tramite Anonymous Speech abbia usato un servizio simile anche per usufruire di un servizio di hosting. Possiamo anche con buona certezza escludere il self-host in quanto poco sicuro, dato che caricare dei file tramite FFTP su un host di terze parti potrebbe essere un leak, invece hostare su un ip statico e' una possibilita' costante di essere attaccati.

Tramite una conversazione privata Rodolfo Andragnes, fondatore e direttore di LABITCONF (Latin America Bitcoin Conference) ha raccontato a Giacomo Zucco, Adam Back e un po' di altre persone di aver ricevuto un'offerta per il dominio bitcoin.org (dominio precedentemente in suo possesso per scopi non inerenti all moneta digitale) dalla mail di Satoshi. Rodolfo conserva ancora la mail, la cui provenienza non e' verificabile, ma ha in ogni caso raccontato che ha rifiutato l'offerta e quindi la trattativa non si e' conclusa, portando alla fine Satoshi come abbiamo appena scoperto, ad acquistare il dominio tramite Anonymous Speech.

2.2 31 ottobre 2008

Il 31 ottobre e' la data di pubblicazione effettiva del whitepaper. Il whitepaper e' la presentazione per la prima volta di come funziona Bitcoin da un punto di vista tecnico. Satoshi scrive nella mailing list cryptography, successore spirituale della mailing list cypherpunk, hostata da metzdowd.com e su cui scrivono ancora dei cypherpunk. Sul thread generale arriva quindi la mail di Satoshi, che sostanzialmente dice: "Ho lavorato a un nuovo sistema di contante elettronico, che e' completamente peer to peer, senza una terza parte fidata". Ricordiamo che in reusable proof of work di Hal Finney, in e-cash di David Chaum, e in e-gold c'era invece una terza parte fidata. Satoshi nel whitepaper indica le proprieta' principali di Bitcoin, dice infatti: "la doppia spesa e' prevenuta con una rete peer to peer, non esiste una zecca principale o un'altra parte fidata, i partecipanti possono essere anonimi. Nuovi coin sono creati da una proof of work in stile Hashcash. La prova di lavoro per la generazione di nuove monete e' anche quello che serve alla rete per evitare il double spending.". Satoshi dice che sta usando la prova di lavoro per due cose diverse, usando un'intuizione gia' accennata da Nick Szabo in Bit Gold. Ricordiamo che Wei Dai si era accorto che i nodi dovevano votare sulla finalita' di una transazione per evitare la doppia spesa, ma se votano solo i nodi e' possibile un sybil attack, con cui chiunque puo' fingersi migliaia di nodi e sovrastare qualunque votazione con una successiva, rendendo impossibile sapere quale votazione e' arrivata prima per chi si unisce dopo alla rete, dato che un utente che si aggiunge alla rete non ha una prova della cronologia, ha solo una prova di chi ha firmato, una prova di lavoro, ma non ha prova di cosa e' arrivato prima e cosa e' arrivato dopo, e di certo il fatto che uno dica di essere arrivato prima non conta niente. Allora si vota, ma se si vota senza nessun peso e' facile creare dei sybil attack. Ecco che Wei Dai ipotizzava quella che oggi viene chiamata proof of stake, dicendo che i nodi devono mettere come coefficiente del loro voto la garanzia di aver messo in palio del denaro digitale, ma poi si accorge che era circolare, quindi che la verificabilita' dell'esistenza di quella stake era data dalla sequenza transativa che era verificata dalla proof of stake, e quindi non funzionava. Allora Nick Szabo propone di pesare il voto sulla prova di lavoro. Satoshi riprende quest'idea, in modo piu' semplice di quella di Nick Szabo, dicendo che ci sono due usi per la prova di lavoro stile Hashcash: la prima e' di fare nuovi coin (questo non e' nuovo, funzionavano cosi' anche B-money e reusable proof of work di Hal Finney), la seconda invece e' di prevenire il double spending.

Nell'abstract del whitepaper, al link su bitcoin.org possiamo leggere: "Una versione completamente peer to peer di contante elettronico permetterebbe ai pagamenti online di essere mandati direttamente da una parte all'altra senza passare attraverso una istituzione finanziaria. Le firme digitali sono parte della soluzione, ma i benefici principali sono perduti se comunque dobbiamo avere una terza parte fidata per prevenire una doppia spesa. Proponiamo una soluzione alla doppia spesa usando una rete peer to peer. Il network timestampa le transazioni tramite un hash dentro una catena continuamente crescente di prove di lavoro basate su quell'hash, formando dei record che non possono essere cam-

biati senza rifare l'intera catena di prova di lavoro. La catena piu' lunga non solo serve come prova della sequenza di eventi testimoniati, ma e' anche prova del fatto che questa sequenza arriva dal piu' grande conglomerato di potenza CPU. Fintanto che la maggioranza della potenza di calcolo della CPU e' controllata da nodi che non stanno cooperando tra di loro per attaccare la rete genereranno la catena piu' lunga e supereranno gli attaccanti. La rete richiede una struttura minimale. I messaggi sono broadcastati su una base di best effort e i nodi possono aggiungersi e togliersi accettando la catena piu' lunga come prova di quello che e' accaduto mentre erano via.".

24.10

3 Gli anni della puberta' del protocollo

4 Block size war