Criticità e Idee

scritto da Alberto De Luigi | 2 Maggio 2016
< Pagina precedente

3.1 Dimensione dei blocchi

Dal momento che c'è un tetto massimo di 1mb per blocco e un nuovo blocco ogni dieci minuti, per registrare le transazioni nella blockchain sono disponibili solo 1.000.000 bytes ogni 10 minuti, che equivale a 1.666 bytes al secondo. Dato che una transazione pesa mediamente 250 bytes **la rete bitcoin può sostenere meno di 7 transazioni al secondo**. Oggi (aprile 2016) il circuito vede mediamente 1,5 transazioni al secondo e il tetto imposto dal sistema non rallenta gli scambi. Tuttavia, considerano che sono 115 le transazioni di paypal al secondo e 2000 quelle di VISA (che può arrivare a sostenerne 56.000), è chiaro che il sistema bitcoin nell'attuale situazione è lontanissimo dal poter sostituire la moneta fiat in tutte le transazioni del mondo (tantopiù se consideriamo quelle in contante).

Vi sono delle proposte per ovviare a questo problema. Per esempio quella di **aumentare la grandezza del blocco** da 1 a 32mb, oppure aumentarlo del 17% ogni anno.

Il protocollo bitcoin viene modificato per **consenso** all'interno della comunità di minatori, espresso da un voto a **maggioranza superqualificata** (ad esempio il 95% della potenza di calcolo). Chiunque è libero di non accettare l'esito della votazione e creare la propria moneta alternativa, in libera concorrenza con i bitcoin tradizionali, oppure tentare di far "deviare" la blockchain dal percorso originario, creando blocchi e compiendo transazioni che seguono un nuovo protocollo (**vedi i dettagli sulla blockchain fork in una finestra separata**). Se questa deviazione è sufficientemente consistente e appoggiata da sufficiente potenza di calcolo dei

minatori, si potrebbe creare una **hard fork** (due rami al contempo operativi della blockchain). Al contrario di una **soft fork**, l'output di una transazione che segue un protocollo non potrà essere utilizzato come input per una transazione verso un nodo che segue un protocollo differente, perciò molti utenti potrebbero trovarsi "intrappolati" in un ramo della blockchain, possessori di output (o meglio, delle relative chiavi private) che non vengono accettati come input dagli utenti sull'altro ramo della blockchain. Questo non esclude l'esistenza di un exchange che accetti di scambiare i bitcoin presenti sui due differenti rami della blockchain proprio come ora scambia euro in bitcoin e viceversa.

3.2 Consenso e sicurezza

Spesso gli utenti si chiedono se il protocollo Bitcoin sia sicuro, a prova di hacker. Non sono mai state trovate vulnerabilità né nel software originario (Bitcoin Core) né nel protocollo Bitcoin.

Il tema del consenso implicitamente garantisce la sicurezza del sistema. Infatti il valore dei bitcoin è strettamente legato al suo protocollo: gli utenti attribuiscono valore ai bitcoin perché – e solo se – seguono rigorosamente il protocollo, non perché ci sia un'autorità centrale che garantisce quel valore. Perciò, chi non segue il protocollo sta in effetti scambiando un'altra valuta, non i bitcoin. Se si riceve una transazione in modo anomalo, che non rispetta il protocollo, questa non sarà accettata dai nodi della rete e quindi non sarà inserita nella blockchain, o sarà inserita in un ramo della blockchain destinato a morire: una volta scoperta l'anomalia non sarà più considerata una transazione "valida". È possibile hackerare un software che segue un protocollo, ma non un protocollo in sé, che è una procedura. Questa o è rispettata o non lo è, e tutti i nodi della rete controllano che sia stata rispettata, scaricando la blockchain sui propri dispositivi.

Il sistema Bitcoin è una procedura che potenzialmente sopravvive anche se i principali software che gestiscono le transazioni, incluso quello degli sviluppatori originari, dovessero venire hackerati o distrutti.

I software client bitcoin stanno aumentando in numero e si stanno differenziando. Ciò che li accomuna è che fanno parte della stessa rete, perché seguono tutti lo stesso protocollo, esattamente come diversi browsers permettono di navigare su internet. Internet stesso è un protocollo che non appartiene a nessuno né esiste un'autorità centrale che lo controlli. Non è possibile «hackerare» il sistema Bitcoin esattamente come non è possibile «hackerare» internet.

Finché rimane il consenso sul protocollo e non esiste un ente dotato di una potenza di calcolo dominante, il sistema è stabile. Anche in caso di dissenso sul protocollo tale da creare un'hard fork, è possibile che vengano ad esistenza più valute figlie dei bitcoin, una in concorrenza con l'altra, e che ciascuna sopravviva in modo stabile e anzi sia possibile scambiarle tramite un exchange.

3.3 L'addio a servizi notarili, brevetti e parti fiduciarie per la verifica dei documenti

I bitcoin possono essere distrutti – o meglio – si possono creare output invalidi, cioè non riutilizzabili come input.

Se un bitcoin viene «distrutto» tramite la funzionalità OP_RETURN, si hanno a disposizione 80bytes di caratteri inseribili liberamente all'interno della transazione e che verranno quindi registrati nella blockchain e scaricati sull'hard disk di ogni nodo. Una transazione può essere anche di un solo satoshi, al lordo della commissione al miner. Il satoshi è l'ottavo decimale di un bitcoin, cioè 0,00000001

Btc.

Quanto viene scritto in quegli 80 bytes di memoria rimarrà per così dire “per l’eternità”, in quanto parte indelebile della blockchain, salvata sugli hard disk di tutti i nodi della rete.

Alcuni ritengono che questa funzione possa un giorno sostituire i servizi notarili, il deposito di contratti, brevetti e vari sistemi di verifica dei documenti. Infatti grazie alla blockchain non è più necessaria un’entità di fiducia per il «timestamping» dei propri documenti. **Un atto potrà essere pubblicato sulla blockchain con l’esatta indicazione dell’orario in cui è stato depositato. Sulla blockchain può anche essere caricato un hash del documento, così che l’atto rimanga privato** (si dimostrerà che il documento esisteva già alla data riportata nel timestamp del blocco quando verrà verificata la corrispondenza fra l’hash presente sul blocco e l’hash SHA-256 del documento).

La prova che il documento era ad esistenza in data x diviene scientifica grazie alla blockchain. Manca solo il precedente legale perché questa sia accettata nei tribunali di tutto il mondo, esattamente come è stato storicamente per la prova del DNA. Con un buon legale questa procedura potrebbe già oggi costituire una garanzia di fronte alla legge attuale.

Una delle startup italiane che si occupa della scrittura di informazioni all’interno della blockchain è proprio Eternity Wall, sul cui sito è possibile creare un hash di un proprio documento con un semplice drag & drop. Questo verrà salvato nella blockchain con una transazione di pochi satoshi. La blockchain e il metodo escrow per la firma multipla potrebbero rivoluzionare il sistema di garanzia dei contratti, oggi per lo più condotto a livello istituzionale dalle autorità centrali. Non si tratta solo di una rivoluzione del business e un efficientamento di tutte le operazioni che richiedono intermediazione, potrebbe trattarsi di un vero e proprio nuovo

paradigma socio-politico.

< Pagina precedente