Client Bitcoin – i software alternativi

scritto da Alberto De Luigi | 5 Maggio 2016

La blockchain è pubblica, perciò tutti possono vedere tutte le transazioni effettuate nel mondo. **L'anonimato** è garantito solo dal fatto che gli indirizzi per il pagamento sono generalmente diversi per ogni transazione: ovvero un utente crea una coppia di chiavi privata e pubblica per ogni transazione. Tuttavia se la stessa chiave pubblica è riutilizzata spesso, come un indirizzo statico (per esempio pubblicato su un sito o utilizzato come l'iban per le coordinate bancarie), altre persone potrebbero facilmente tracciare le quantità ricevute e spese da quell'indirizzo e quindi tutti movimenti del suo proprietario.

Con il software Bitcoin Core, la blockchain comprensiva di tutte le transazioni registrate nella storia dei bitcoin viene salvata su tutti gli hard disk presenti in ogni nodo collegato alla rete. Nell'aprile 2016 pesa circa 65gb ed è raddoppiata dall'anno precedente. Un blocco può pesare al massimo 1mb (1.000.000 bytes), una transazione generalmente 250bytes, ma è un dato variabile (in base anche al numero di input e output, la signature script ecc.). Generalmente i blocchi contengono meno di 200 transazioni, il più grande finora ne conteneva 1096.

Il software originario Bitcoin Core è **open source**. Le "consensus rules", ovvero i fatti su cui è necessario che tutti gli utilizzatori di bitcoin concordino, comprendono la composizione della block chain, non il modo di fare rete. Ci possono essere infiniti network e software alternativi a quello originale a patto che blockchain e protocollo siano gli stessi.

Sono stati sviluppati sistemi alternativi per collegarsi alla

rete Bitcoin. Il network originario è detto “public Bitcoin P2P network”, ma esiste anche il network «High-speed Bitcoin Relay Network».

Vi sono software alternativi a Bitcoin Core, come ad esempio **BitcoinJ**, che utilizzano il metodo **lightweight Simplified Payment Verificaion** (SPV), che salva soltanto l’hash finale nell’header del block (la Merkle root) e non tutte le transazioni incluse nel body. In questo modo viene risparmiato spazio sull’hard disk. Il sistema tradizionale tuttavia fornisce delle garanzie in più: se ci fosse un dato corrotto presente in uno dei nodi (un errore di trascrizione sull’hard-disk di un utente) questo nodo può confrontarsi con tutti gli altri su cui è presente l’intera blockchain, così da fare una verifica.