UNIVERSITÀ DEGLI STUDI ROMA TRE

Dipartimento di Ingegneria
Corso di Laurea Magistrale in Ingegneria Informatica

Tesi Di Laurea

Strumenti di analisi per la rete delle transazioni Bitcoin

Laureando
Claudia Romeo
Matricola 461963

Relatore
Prof. Maurizio Pizzonia

Correlatore
Dott. Valentino Di Donato

Anno Accademico 2016/2017

alla mia famiglia

Ringraziamenti

Indice

Introduzione

Negli ultimi anni, con il progresso tecnologico e con l'aumentare del coinvolgimento di Internet nella nostra quotidianità, si è arrivati a digitalizzare anche il denaro. Grazie a questa digitalizzazione, sono state create delle monete virtuali, o valute elettroniche, che possono essere utilizzate solo su Internet. La moneta elettronica che ha lanciato questa "tendenza" è una delle più famose, il Bitcoin.

Capitolo 1

Bitcoin & Blockchain

1.1 Cosa sono i Bitcoin?

Bitcoin è una valuta elettronica creata nel 2008 da Satoshi Nakamoto, uno pseudonimo dietro al quale non si sa ancora con la precisione chi si nasconde. Con il termine Bitcoin viene denotata sia la rete che consente il possesso e il trasferimento di denaro, sia la moneta. Per convenzione, Bitcoin si riferisce alla tecnologia della rete, mentre *bitcoin* alla valuta stessa.

Come ogni valuta, i bitcoin possono essere trasferiti tramite gli utenti, grazie ad un protocollo che viene rispettato all'interno della rete Internet, il quale può essere eseguito su differenti dispositivi, in modo tale da permettere la fruibilità del servizio anche attraverso gli smartphones.

I bitcoins possono essere comprati, venduti e scambiati con altre valute, tramite degli organismi specializzati nel cambio di monete virtuali. In un certo senso, Bitcoin è la forma perfetta di denaro per Internet, dal momento che è estremamente veloce, sicuro e senza limiti.

A differenza delle altre valute, i bitcoin sono esclusivamente virtuali, dietro di essi non esistono monete fisiche. Tali bitcoin vengono coinvolti in transazioni da mittente a ricevente, i quali possiedono delle chiavi crittografiche pubbliche e private che servono per trasmettere e sbloccare la spesa dei bitcoin ricevuti. Infatti, senza la chiave privata, chi riceve i bitcoin non può spenderli in nessun modo. Tali chiavi vengono conservate

all'interno di un *wallet*, letteralmente un "portafoglio". Ogni wallet è caratterizzato da un indirizzo Bitcoin il quale è univoco e ha la funzione di fare riferimento ad uno dei partecipanti alla transazione. In questo modo, quando viene effettuato uno scambio di bitcoin, vengono visualizzati solamente gli indirizzi dei wallet. Questa caratteristica permette quindi di rendere anonime le transazioni, dato che agli indirizzi non è connesso in nessun modo il nome o il cognome dell'individuo o dell'associazione che interviene nello scambio.

La rete Bitcoin, oltre ad essere completamente virtuale, è priva di un'unità centralizzata, infatti essa è costituita da un sistema distribuito peer-to-peer.
I bitcoin vengono creati tramite un processo, detto *mining*, che permette a chiunque di mettersi in competizione per trovare una soluzione ad un problema matematico. Ogni persona che partecipa alla rete bitcoin, potrebbe operare come un *miner*, ovvero colui che cerca di risolvere il problema matematico per generare bitcoin, usando le capacità del proprio computer messo a disposizione della computazione.

Quando viene effettuato uno scambio di bitcoin tra due o più wallet, viene creata una *transazione*. Ogni transazione viene conservata in una struttura dati chiamata **blocco**, il quale a sua volta va a costituire la **Blockchain**.

1.2 Cos'è la Blockchain?

La Blockchain, letteralmente *catena di blocchi*, è una base di dati distribuita, che permette la memorizzazione delle transazioni raggruppate in blocchi connessi tra loro, ognuno con il suo successivo. Ogni blocco è una struttura dati che contiene un numero variabile di transazioni, inserite dal *miner* che ha minato il blocco, fino ad un tetto massimo di 1MB per singolo blocco.

L'idea di base della Blockchain, deriva dal concetto di **libro mastro**, il registro della contabilità in cui sono riuniti tutti i conti che compongono un dato sistema contabile. In questo caso il sistema contabile sarebbe la rete Bitcoin, mentre la Blockchain sarebbe il libro mastro che contiene tutti i conti, ovvero le transazioni.

L'antico libro mastro, veniva utilizzato come fonte ufficiale per la memorizzazione degli scambi e dei passaggi di proprietà. Infatti, quando veniva fatta una compravendita tra mittente e ricevente, veniva controllato sul libro mastro se il ricevente non avesse speso precedentemente il denaro, e se il mittente non avesse già venduto la merce usata nello scambio.

Infine, se fosse andato tutto a buon fine, veniva registrata la transazione sul libro mastro, in modo da essere consultabile e pubblica per le successive transazioni.

Un principio importante di questo meccanismo è la fiducia, la quale tutti ripongono nel libro mastro: ognuno si fida del gestore della memorizzazione delle transazioni, al punto che, chi compra e chi vende, può effettuare scambi anche senza fidarsi reciprocamente. Quindi, il libro mastro è una garanzia, sia per il mittente che per il ricevente dello scambio. Inoltre, le banche possono perciò controllare gli scambi che vengono fatti e il denaro posseduto da ogni partecipante alle transazioni.

La Blockchain, come già sottolineato, è una struttura dati composta da diverse unità di base, dette blocchi. Infatti, blockchain significa letteralmente *catena di blocchi*.

Quindi, tali blocchi vengono "incatenati", ovvero collegati tra loro tramite un protocollo ben definito nella struttura del sistema bitcoin.

Ogni blocco all'interno della blockchain, è identificato da un codice hash, generato applicando l'algoritmo di crittografia SHA256 all'header del blocco. Un singolo blocco è collegato al suo predecessore, conosciuto come "blocco genitore", attraverso il campo *previous block hash* all'interno del proprio header. In altre parole, ogni blocco contiene l'hash del proprio blocco genitore all'interno dell'header. Infine, la sequenza dei vari hash genera una catena che collega tutti i blocchi all'indietro, fino al blocco numero zero.

1.2.1 Mining

Le monete bitcoin sono "coniate" durante la creazione di ciascun blocco ad un tasso fisso. Ogni blocco, generato all'incirca ogni 10 minuti, contiene nuovi bitcoin, creati da zero. Il *mining* inoltre serve per proteggere il sistema bitcoin contro transazioni fraudolente o transazioni che cercano di spendere lo stesso numero di bitcoin più di una volta, problema conosciuto con il nome di *double-spend* (doppia-spesa).

I miner validano le transazioni e le registrano sul *ledger* globale, ovvero la Blockchain, creando un nuovo blocco e inserendo le transazioni al suo interno, per poi aggiungere il blocco alla catena. Perciò, i miner raccolgono un certo numero di transazioni e cercano di inserirle all'interno di un nuovo blocco creato appositamente. Tutte le transazioni che poi risultano alla fine all'interno di tale blocco, sono considerate *confirmed* (ovvero confermate), ovvero una sorta di etichetta che permette al ricevente di tali bitcoin di spenderli successivamente.

Lo scopo dei miner è quello di guadagnare bitcoin, e possono ottenerli in due modi:

- quando un nuovo blocco viene aggiunto alla Blockchain, si ottiene un premio in bitcoin
- per ogni transazione vengono pagate le *fees* (=tasse) al miner

Al fine di ottenere il premio, i miner devono trovare la soluzione ad un problema matematico molto difficile basato su un algoritmo di crittografia. La soluzione a tale problema, chiamata **proof of work**, è inclusa all'interno del nuovo blocco, e serve come prova che il miner ha impiegato un notevole sforzo di elaborazione. La competizione tra i miner per trovare la proof of work per guadagnare bitcoin è alla base della sicurezza del sistema Bitcoin.

Il processo della generazione di nuove monete è chiamato **mining** perchè la ricompensa è progettata in modo da simulare rendimenti decrescenti, esattamente come l'estrazione di metallo prezioso. La fornitura di valuta bitcoin è creata attraverso il mining, analogamente alla procedura con cui una banca centrale crea moneta stampando banconote.

L'ammontare del premio del mining a Gennaio 2009 era di 50 bitcoin per blocco e a Novembre 2012 già si era dimezzato fino ad ottenere 25 bitcoin. Attualmente il guadagno del premio del mining risulta 12.5 bitcoin per blocco. Seguendo questo processo, il premio per il mining di un blocco, decrescerà esponenzialmente fino all'anno 2140, quando tutti i bitcoin (20.9999998 milioni) saranno emessi. All'incirca dopo il 2140 non saranno più prodotti nuovi bitcoin e il miner andrà a guadagnare solamente tramite le tasse applicate per ogni transazione.

I miners guadagnano bitcoin per ogni transazione tramite le tasse. Esse vengono calcolate come eccesso di bitcoin tra le transazioni di input e quelle di output. Infatti, il miner che riesce a creare il nuovo blocco "tiene il resto" di ogni transazione inclusa in quel blocco.
Dopo il 2140, tutti i bitcoin potranno essere guadagnati tramite tasse.

La parola "mining", ovvero minare, potrebbe avere un significato ingannevole poichè sembrerebbe indicare l'estrazione di metallo prezioso, e quindi focalizza l'attenzione sul premio che viene ottenuto dal minatore.
Sebbene il mining sia incentivato dal suo guadagno, il suo obiettivo principale non è il premio in denaro o la creazione di nuove monete.
Mining è il processo principale per la decentralizzazione del sistema, nel quale le transazioni sono validate e chiare. Rappresenta una sicurezza per il sistema e permette lo sviluppo di una rete basata sul consenso, senza l'intervento di un'autorità centrale.

1.2.2 Consenso Decentralizzato

La Blockchain non essendo creata da un'autorità centrale, è assemblata indipendentemente da ogni nodo all'interno della rete. Perciò, ogni nodo della rete, agendo sulle informazioni che vengono trasmesse attraverso delle connessioni di rete non sicure, può arrivare alla stessa conclusione e assemblare una copia della stessa blockchain, come ogni altro nodo.

La principale invenzione di Satoshi Nakamoto è il meccanismo decentralizzato del *consenso emergente*. "Emergente" perchè il consenso generale non è raggiunto esplicitamente – non esiste un'elezione o un momento prefissato quando il consenso viene espresso – è un risultato dell'interazione asincrona di migliaia di nodi indipendenti tra loro, i quali basati sulle stesse regole.

Tutte le proprietà dei bitcoin, inclusa la moneta, le transazioni, i pagamenti, il modello di sicurezza, i quali non dipendono da un'autorità centrale, derivano da questa invenzione.
Il consenso decentralizzato dei Bitcoin viene fuori dall'interazione di quattro processi che si verificano indipendentemente sui nodi attraverso la rete. Tali processi sono:

- la verifica indipendente di ogni transazione, basata su una lista globale di criteri

- l'aggregazione indipendente di tali transazioni all'interno di un nuovo blocco appena minato
- la verifica indipendente del nuovo blocco da parte di ogni nodo, e l'unione di tale blocco all'interno della chain
- la selezione indipendente, da parte di ogni nodo, della chain con la computazione che maggiormente raccoglie più transazioni e che è stata dimostrata correttamente tramite una *proof of work*

1.2.3 Blockchain Forks

Dal momento che la Blockchain è una struttura dati decentralizzata, copie differenti non sono sempre consistenti. Infatti, i blocchi possono arrivare a nodi diversi in tempi diversi, creando differenti rami all'interno della stessa blockchain.

Sebbene un blocco abbia solo un genitore, esso può avere temporaneamente un diverso numero di figli. Ogni figlio si riferisce allo stesso blocco genitore e contiene lo stesso hash del genitore nel campo *previous block hash*. Questa temporanea molteplicità di figli può causare una *fork* (letteralmente *biforcazione*), ovvero una situazione in cui blocchi differenti vengono creati quasi simultaneamente da diversi miners.

Per risolvere il problema della biforcazione, ogni nodo Bitcoin seleziona sempre e cerca di estendere la catena di blocchi che soddisfa il sistema *proof-of-work*.

Le fork avvengono come risultato di inconsistenze temporanee tra versioni della blockchain, che vengono risolte con eventuali riconvergenze, ovvero i nuovi blocchi vengono aggiunti alla catena principale della biforcazione.

Nelle figure seguenti, si può capire un esempio di una fork della blockchain. Sebbene nelle figure si nota la rete globale, in realtà la topologia della rete bitcoin non è organizzata geograficamente, piuttosto forma una rete di nodi interconnessi, che potrebbero essere geograficamente molto lontani. Nella vera rete bitcoin, la *distanza* tra i nodi è misurata in **hop** da nodo a nodo, non sulla loro distanza fisica. Un singolo hop è una porzione di percorso tra la sorgente e la destinazione.

Per scopi illustrativi, blocchi differenti sono mostrati con colori diversi, che si diffondono attraverso la rete e le connessioni attraversate vengono colorate con colori diversi.

Nel primo diagramma (*figura 1.1*), la rete appare con una singola prospettiva unificata della blockchain, con il blocco blu come estremità della catena principale.

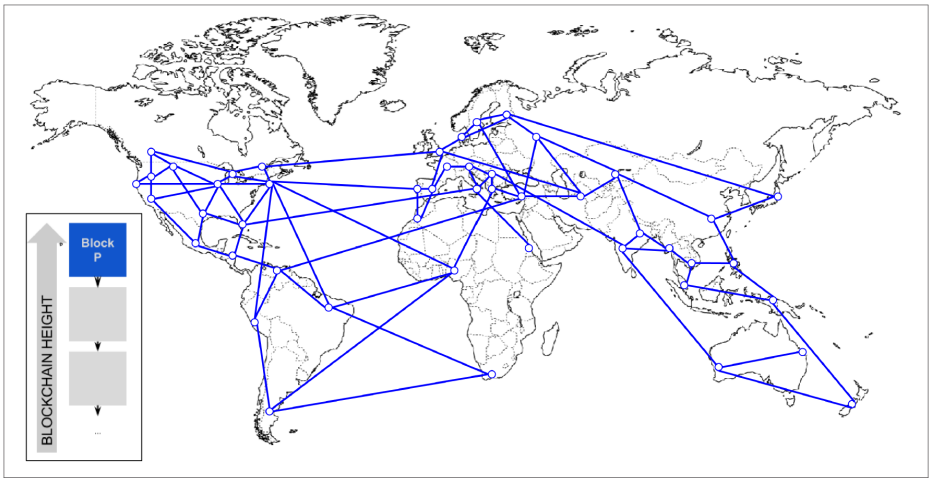

Figura 1.1: *Visualizzazione di un evento fork–prima della fork*

Un evento *fork* avviene quando ci sono due diversi blocchi che sono candidati ad essere aggiunti contemporaneamente alla Blockchain. Ciò può accadere quando due diversi miner risolvono la proof of work con uno scarto di tempo molto piccolo tra entrambi. Di conseguenza, tali miner immediatamente rivelano la loro soluzione in modo broadcast, e il nuovo blocco creato viene trasmesso tempestivamente ai loro vicini, che propagano i blocchi nuovi attraverso la rete.

Ogni nodo che riceve un blocco valido, lo incorpora all'interno della propria versione della blockchain, allungandola di un blocco. Se tale nodo si rende conto di aver ricevuto un ulteriore blocco che soddisfa le condizioni, lo aggiunge creando una catena secondaria alternativa al blocco aggiunto appena prima.

In *figura 1.2* si possono notare due miner che hanno minato due diversi blocchi quasi simultaneamente.
Entrambi i blocchi sono figli del blocco blu, ed hanno lo scopo di estendere la chain aggiungendosi sopra al blocco blu. Nella figura, un blocco è rappresentato in rosso e l'altro in verde. Per esempio, si assuma che un miner in Canada trova una soluzione proof of work per il blocco "rosso" che estende la blockchain come figlio del blocco "blu". Quasi simultaneamente, un altro miner in Australia trova un'altra soluzione

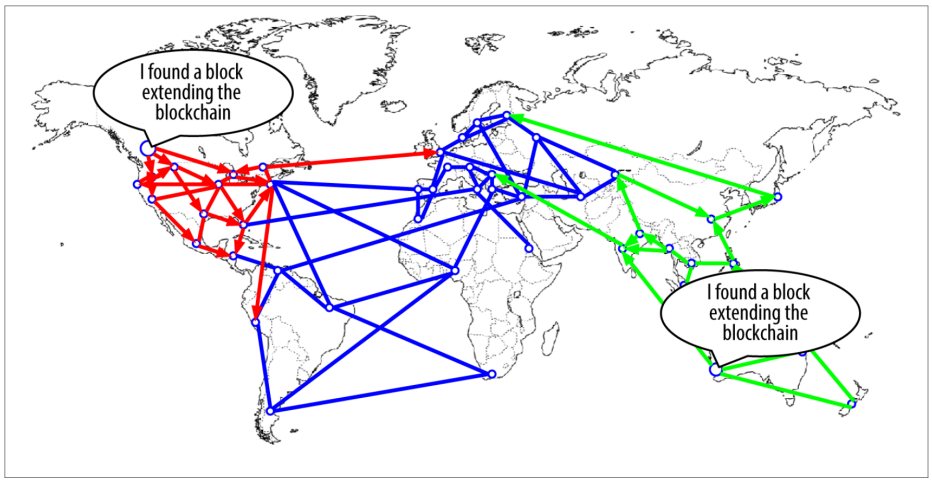

Figura 1.2: *Visualizzazione di un evento fork: due blocchi minati simultaneamente*

per il blocco "verde" al fine di estendere la blockchain. Entrambi i blocchi sono validi, entrambi contengono una soluzione valida alla proof of work, e tutti e due sono figli del blocco "blu". Inoltre, entrambi contengono quasi le stesse transazioni, con solo alcune piccole differenze.

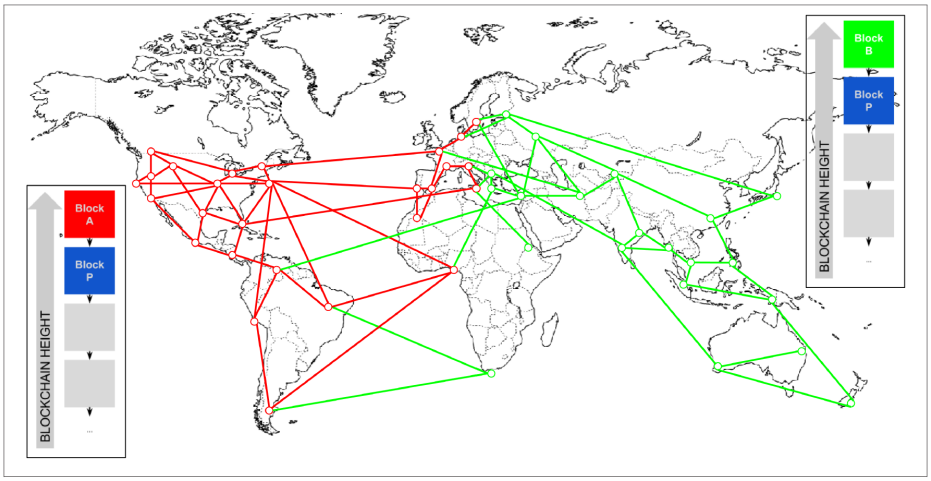

Figura 1.3: *Visualizzazione di un evento fork: due blocchi propagati, la rete biforca*

Appena i due blocchi vengono propagati, alcuni nodi ricevono il blocco "rosso" e altri il blocco "verde". Come si può vedere in *figura 1.3*, la rete si divide in due diverse prospettive della blockchain, un lato con all'estremità il blocco rosso e l'altro lato con

il blocco verde.

Da quel momento, i nodi della rete che sono più vicini al nodo del Canada, aggiungeranno anch'essi il blocco "rosso" per primo, e creeranno una nuova blockchain con il blocco "rosso" come ultimo blocco, ignorando il blocco "verde", che è arrivato un po' più tardi. Nello stesso momento, i nodi più vicini al nodo dell'Australia prenderà il blocco "verde" come vincitore e lo userà per estendere la sua versione della blockchain, aggiungendolo al blocco "blu", ignorando il blocco "rosso" che è arrivato un po' più tardi degli altri. Di conseguenza, ogni miner che vede aggiungere il blocco "rosso" in testa alla chain, immediatamente cercherà di creare altri blocchi che si aggiungeranno al blocco "rosso", ed andrà a risolvere la proof of work per tali blocchi candidati. Invece, i miners che accettano il blocco "verde" cominceranno ad estendere la porzione di chain che si andrà ad attaccare a tale blocco.

Le fork vengono quasi sempre risolte da un singolo blocco. Infatti, come parte del potere computazionale viene dedicato per aggiungere il blocco "rosso", un'altra parte della rete impiega le sue risorse per aggiungere il blocco "verde". Anche se il potere computazionale è quasi diviso in due parti, probabilmente un gruppo di miner troverà e propagherà la soluzione prima che lo faccia un altro gruppo di ulteriori miner. Per esempio, si supponga che i miner trovino un blocco "rosa" che estenda il blocco "verde", immediatamente lo propagherebbero all'intera rete (*figura 1.4*)

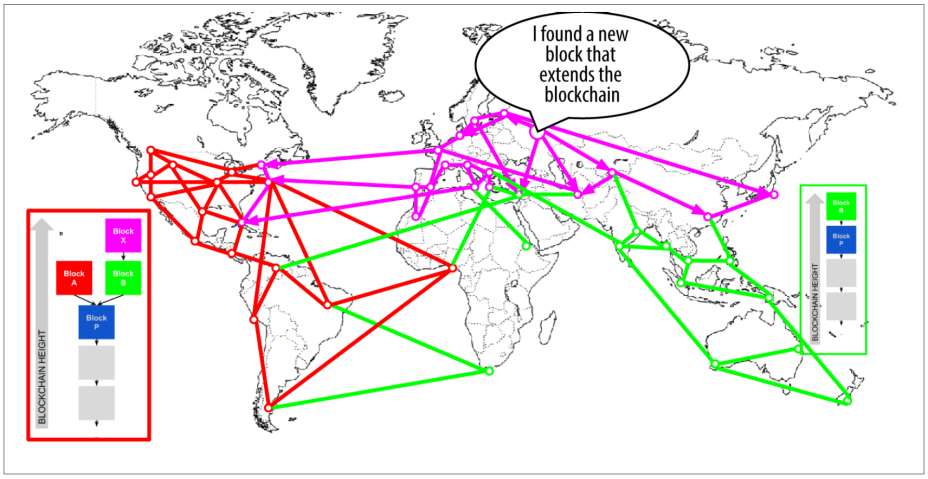

Figura 1.4: *Visualizzazione di un evento fork: un nuovo blocco estende un ramo della fork*

1.3 Le Transazioni

Come è stato detto in precedenza, una transazione è uno scambio di monete bitcoin tra due o più individui. Per esempio, se Alice vuole dare 1BTC a Bob, ha bisogno di effettuare una transazione inserendo come input l'importo da trasferire e l'indirizzo del wallet di Bob.

Nella maggior parte dei casi, la quantità di denaro che partecipa alla transazione non è quasi mai Secondo la configurazione predefinita dal protocollo, quando viene effettuata una transazione che non implica la spesa dell'intero importo contenuto nel wallet del mittente, è previsto che venga creata un ulteriore transazione con il

Una caratteristica delle transazioni è che possono partecipare più wallet contemporaneamente: ad esempio, un individuo può inviare con la stessa transazione, una quantità di bitcoin a due individui diversi, in modo da recapitare ciascuno la quantità di bitcoin desiderata.

1.4 Grafo delle transazioni

1.5 Caratteristiche del grafo

Capitolo 2

I comportamenti automatici

Questo è il capitolo 2

Capitolo 3

Analisi sul grafo delle transazioni

Questo è il capitolo 3

Capitolo 4

Approccio utilizzato

Questo è il capitolo 4

Capitolo 5

Sperimentazione & Risultati

Questo è il capitolo 5

Conclusioni e sviluppi futuri

Bibliografia