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
Ing. Valentino Di Donato

Anno Accademico 2016/2017

alla mia famiglia

Ringraziamenti

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.

Contents

Chapter 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 delle monete, che le monete stesse. 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 bitcoin che viene utilizzato tramite la rete Internet.
Il protocollo bitcoin 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 un mittente ad un ricevitore, 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 protagonisti della transazione. In questo modo, quando viene effettuato uno scambio di bitcoin, vengono visualizzati solamente gli indirizzi dei wallet. Questa caratteristica permette quindi di anonimizzare 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.

1.2.1 Caratteristiche

1.3 Le Transazioni

1.4 Grafo delle transazioni

1.5 Caratteristiche del grafo

Chapter 2

I comportamenti automatici

Questo è il capitolo 2

Chapter 3

Analisi sul grafo delle transazioni

Questo è il capitolo 3

Chapter 4

Approccio utilizzato

Questo è il capitolo 4

Chapter 5

Sperimentazione & Risultati

Questo è il capitolo 5

Conclusioni e sviluppi futuri

Bibliography