UNIVERSITÀ DEGLI STUDI DI CAGLIARI

FACOLTÀ DI SCIENZE

Corso di Laurea Triennale in Informatica

Title / Titolo

subtitle / sottotitolo

Supervisor / Relatore
Prof. Massimo Bartoletti

Candidate / Studente
Giulia Argiolas
Matr. N. 65385

ACADEMIC YEAR / ANNO ACCADEMICO 2017/2018

Mr. and Mrs. Dursley, of number four, Privet Drive, were proud to say that they were perfectly normal, thank you very much. They were the last people you'd expect to be involved in anything strange or mysterious, because they just didn't hold with such nonsense. Mr. Dursley was the director of a firm called Grunnings, which made drills. He was a big, beefy man with hardly any neck, although he did have a very large mustache. Mrs. Dursley was thin and blonde and had nearly twice the usual amount of neck, which came in very useful as she spent so much of her time craning over garden fences, spying on the neighbors. The Dursleys had a small son called Dudley and in their opinion there was no finer boy anywhere.

La tesi ha come obiettivo l'analisi della blockchain Litecoin con i presupposti di un confronto con Bitcoin. Introduce Litecoin, caratteristiche e differenze con Bitcoin, utilizzi presenti e prospettive future e contiene delle analisi svolte tramite l'estensione e l'utilizzo del tool BlockAPI, già operativo per le blockchain Bitcoin ed Ethereum, relative alla distribuzione dell'hashing power tra i mining pools, il mining di blocchi vuoti, la diffusione del merged mining e l'utilizzo dell'OP_RETURN per segnalare l'adesione a protocolli o servizi.

Indice

Capitolo 1

Introduzione

1.1 Obiettivi

L'obiettivo è lo studio della blockchain di Litecoin per effettuare una comparazione con Bitcoin. A tal fine ho svolto delle analisi riguardanti prevalentemente il lato tecnologico di essa, lo sviluppo, le applicazioni, ma anche il lato economico, tramite dati esterni, come fees, exchange rates e la loro evoluzione nel tempo.

1.2 Contributi

Per l'analisi della blockchain Litecoin ho esteso il tool BlockAPI, implementando le strutture dati e le queries necessarie a tal fine. La parte tecnica dell'estensione del tool verrà discussa nel capitolo 2.

1.3 Struttura della tesi

La tesi presenta un background tecnico iniziale necessario a capire Bitcoin e valido per tutte le criptovalute da esso derivate e mostra le caratteristiche principali per cui Litecoin differisce da Bitcoin. Segue un'introduzione delle tecnologie utilizzate e del mio contributo al tool che è stato utilizzato per l'analisi. Infine le analisi, per ciascuna delle quali viene illustrato un contesto per comprenderla, lo svolgimento di essa, il codice e le queries ed i risultati numerici e loro eventuali rappresentazioni grafiche.

1.4 Background

1.4.1 Bitcoin

Bitcoin è una criptovaluta nata nel 2009 ad opera di Satoshi Nakamoto, la cui vera identità è ancora ignota. Open source, orientata all'anonimato, decentralizzata e peer to peer, non possiede alcun server "centrale" o organismo di controllo. È una risorsa totalmente virtuale che non prevede un'unità fisica associata: i Bitcoin sono "coniati" tramite un processo, il cosiddetto mining, che comporta una competizione nel cercare le soluzioni di un problema computazionale estremamente oneroso da risolvere ma la cui soluzione sia semplicissima da verificare, detto Proof of Work. Chiunque può minare tramite la potenza di calcolo di cui dispone, ma la difficoltà del puzzle crittografico viene ricalcolata ogni 2016 blocchi -approssimativamente 2 settimane- in base alla potenza di calcolo del network affinché in media un blocco di transazioni sul network venga generato e validato ogni 10 minuti. Dunque ogni 10 minuti circa un nuovo blocco viene confermato e aggiunto alla blockchain e questo lavoro viene ricompensato con una quantità prestabilita di Bitcoin nuovi di zecca. La ricompensa per il miner si dimezza circa ogni 4 anni perché, dal momento che il protocollo Bitcoin permette l'esistenza di massimo 21 milioni di unità monetarie, la ricompensa deve essere sufficientemente elevata da incentivare il lavoro del miner ma non così tanto da deprezzare la valuta mettendo in circolazione prematuramente un numero eccessivo di Bitcoin. Attualmente la ricompensa ammonta a 12.5 BTC e nel 2020 subirà un nuovo dimezzamento. Le informazioni e lo storico di tutte le transazioni sulla rete sono immutabili e distribuiti sui nodi che la costituiscono. La struttura dati atta a garantire ciò è la Blockchain e tramite essa Bitcoin decentralizza e distribuisce sulla rete le funzioni di emissione di valuta (mining) e di compensazione (halving) eliminando la necessità di una banca centrale.

Background tecnico Per capire Bitcoin è utile chiarire cosa sia effettivamente una transazione in Bitcoin e in cosa differisca da una "ordinaria", ad esempio con carta di credito. Il concetto di transazione bancaria che conosciamo prevede una privacy ferrea e l'utilizzo della crittografia al fine di non far intercettare dati sensibili ai malintenzionati, mentre in questo caso la transazione è pubblicamente disponibile per intero in un registro pubblico immutabile e non contiene dati personali. Bitcoin ha praticamente trasformato i soldi in una struttura dati e fatto in modo che sia quasi impossibile per chiunque creare una transazione illeggittima, ma che allo stesso tempo sia facilissimo verificarne la validità. Una transazione è infatti una struttura dati che codifica e trasferisce un valore da una fonte di fondi, detta input, ad una destinazione, detta output.

Dimensione	Campo	Descrizione
4 Bytes	Versione	Specifica quali regole segue la transazione
1-9 Bytes (VarInt)	Input Counter	Quanti input sono inclusi
Variable	Inputs	Uno o più input di transazione
1-9 Bytes (VarInt)	Output Counter	Quanti output sono inclusi
Variable	Outputs	Uno o più input di transazione
4 Bytes	Locktime	Un Unix timestamp o numero del blocco

Source: Mastering Bitcoin

I componenti di una transazione sono i cosiddetti UTXO, o input di transazione non spesi, la cui aggregazione dà il "saldo" dell'utente -in Bitcoin non esiste un vero e proprio concetto di saldo- e il resto di un UTXO più grande del valore desiderato viene restituito, in modo analogo, come UTXO più piccolo (che assume il valore del resto). Ogni transazione Bitcoin contiene almeno un input e output, ad eccezione delle transazioni coinbase che contengono un solo output del valore della ricompensa per il miner, già precedentemente accennata. Tutti gli outputs ad eccezione dei cosiddetti OP_RETURN producono a loro volta bitcoin spendibili e sono composti da un importo in bitcoin e un "locking script" che ha la funzione di verifica: solo chi soddisfa le condizioni poste dallo script può riscattare l'output. La transazione viene firmata tramite la chiave privata del proprietario e può essere sbloccata solo dall'indirizzo del destinatario legittimo. Chiunque voglia ricevere un pagamento, o effettuarne uno, necessita di una copia pubKey:privateKey.Ogni partecipante al network crea tramite il client una privateKey di 256 bit che occorrerà per firmare la transazione. Da questa chiave si genera successivamente la pubKey di 512 bit, tramite l'algoritmo ECDSA su curva ellittica secp256k1. Tale chiave verrà usata per la verifica dell'autenticità della firma digitale del mittente. Per sicurezza e praticità si esegue un doppio hash: per prima cosa si calcola SHA-256(PubKey), e successivamente si esegue RIPEMD-160(SHA-256(PubKey)); per ottenere l'indirizzo si utilizza una ulteriore codifica in Base58Check per ottenere un indirizzo in formato standard.

Ogni transazione validata dal network viene inserita in un blocco di transazioni che è accodato alla blockchain. La blockchain è un registro pubblico e distribuito che tiene traccia di tutte le transazioni che sono state effettuate fin dal primo blocco. È immutabile e ciascun nodo ne contiene una copia: ai fini di questa tesi non è necessario dettagliare il sistema di consenso (la Proof of Work precedentemente citata) ma è fondamentale ricordare che l'intero sistema si basa su di esso e, soprattutto, che la versione "ufficiale" della blockchain è quella su cui il maggior numero di nodi sono d'accordo. Ciò che rende estremamente sicura la blockchain è proprio l'utilizzo della curva ellittica in associazione alle funzioni di hashing

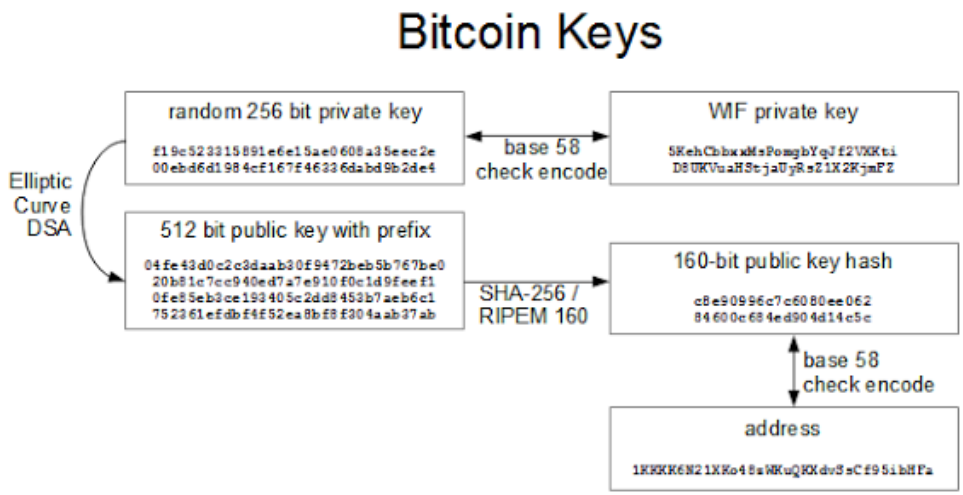

Figura 1.1

Figura 1.2

precedentemente citate, SHA-256 e RIPEMD-160, che processano l'input X producendo in output una stringa di lunghezza fissa H(X) da cui non poter ricavare l'input originario X. Inoltre, minime variazioni di X possono portare variazioni enormi in H(X) ed essa non deve contenere una pre-immagine di X.

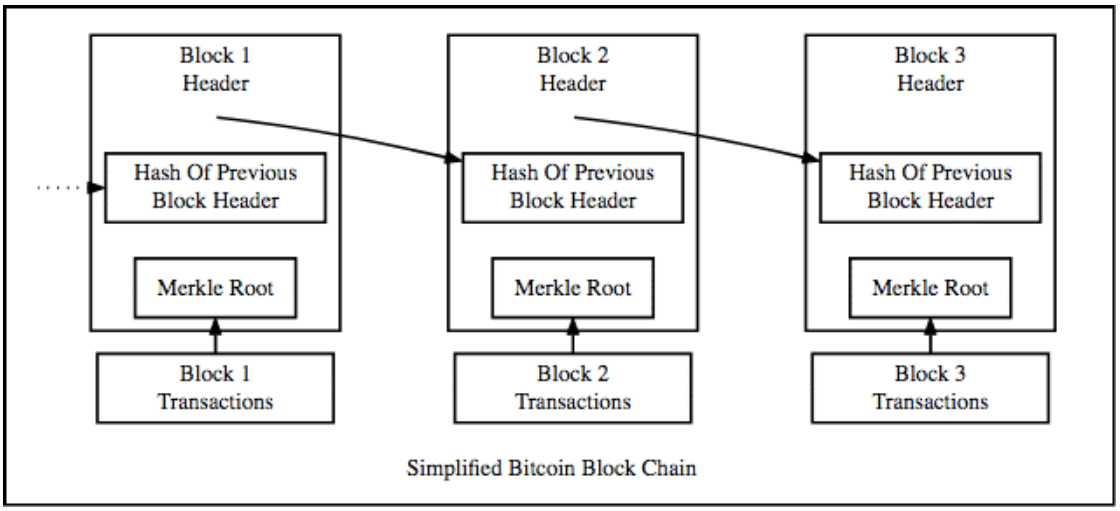

Figura 1.3

[Image courtesy of blockgeeks.com]

La blockchain è una lista concatenata che contiene dati e un hash pointer che punta al blocco precedente. Un hash pointer differisce da un normale puntatore perché invece di limitarsi a contenere l'indirizzo del blocco precedente contiene

anche l'hash dei dati del blocco che punta. Nel caso di Bitcoin, inoltre, la funzione di hashing viene applicata doppiamente nell'header in due casi In questa tabella [fonte: bitcoin.org documentazione ufficiale] possiamo osservare la struttura degli 80 Bytes dell'header di ciascun blocco. Tenendo presente quanto affermato in precedenza sulle funzioni di hashing risulta chiara la virtuale impossibilità di riuscire ad effettuare qualsivoglia modifica senza che questa abbia un impatto sull'intera blockchain.

È questo a garantire l'inalterabilità del contenuto della blockchain: oltre alla difficoltà data dalla potenza computazionale richiesta per rendere almeno fattibile l'attacco, un brute-force puro, il costo lo rende nella quasi totalità dei casi insostenibile o non profittevole. A titolo d'esempio, riporto la stima di quanto costerebbe sferrare un attacco alle principali blockchain allo stato attuale [dati crypto51.app, agosto 2018]

In breve: la blockchain è un registro pubblico immutabile contenente una serie di blocchi di transazioni validate, ognuna delle quali consiste in un trasferimento di fondi da uno o più input non spesi ad uno o più output, e tutto ciò avviene in modo decentralizzato ed è reso sicuro tramite le curve ellittiche e funzioni di hashing che garantiscono che solo i legittimi proprietari possano usufruire dei fondi.

Forks e Altcoins L'esistenza stessa di una blockchain dipende dall'aderenza alle regole dell'intero network. Blocchi che non rispettano le regole non possono essere validati. Bitcoin, essendo open source, viene mantenuto e valutato da comunità di sviluppatori che reagiscono ai problemi che emergono nel network tramite dei BIP (Bitcoin Improvement Proposal) che formalmente sono uno standard di proposta di miglioramento. Questi possono riguardare il protocollo o le regole. Una soft fork consiste infatti in un cambiamento di protocollo o di regole in modo retrocompatibile: il software continuerà a riconoscere i blocchi precedenti e i vecchi nodi non aggiornati saranno in grado di validare nuovi blocchi. Detta consensus fork, per la sua attuazione è sufficiente che la maggioranza dei miner sia d'accordo. Talvolta si hanno, tuttavia, notizie di attacchi hacker verso i nodi non aderenti (es: DDoS) per forzarne indirettamente l'adesione. Un esempio di soft fork è l'implementazione di SegWit, oggetto di un'analisi al capitolo 4. Qualora non fosse presente il consenso necessario tra i miners e la nuova versione del software non fosse retrocompatibile si verificherebbe un hard fork: quando ciò si verifica la blockchain subisce una separazione definitiva e il possessore di criptovaluta la possiede ora duplicata sulla blockchain forked. Un hard fork piuttosto noto di Bitcoin è Bitcoin Cash: differisce dal protocollo originale per la dimensione del blocco, che da 1 passa ad 8 MB. Chi possedeva X bitcoin (BTC) al momento del forking ha potuto ottenere gratuitamente X bitcoincash (BCH). Infine ci sono

le cosiddette altcoins: forks del codice sorgente di Bitcoin, blockchain totalmente separata, differenze di protocollo scarsamente compatibili. Litecoin è definibile a tutti gli effetti una altcoin.

1.4.2 Litecoin

Litecoin è una criptovaluta peer to peer che dal punto di vista tecnico condivide gran parte dell'implementazione di Bitcoin. Non è considerabile un fork di Bitcoin in senso stretto poiché non c'è stata la duplicazione della moneta, bensì una source code fork: è stato effettuato un fork del client open source Bitcoin Core e sono state effettuate delle modifiche sostanziali che si sono riflesse nella blockchain e le due valute non hanno uno storico comune. Nasce nel 2011 ad opera dell'ex ingegnere MIT Charlie Lee, con l'intento dichiarato di diventare rispetto a Bitcoin "ciò che l'argento è rispetto all'oro"; già da questa frase si può comprendere come Litecoin sia una valuta che si presta a micropagamenti e operazioni più rapide rispetto a Bitcoin. Lee sostiene di non aver concepito Litecoin come sostituto di Bitcoin, bensì come complemento per risolvere alcune criticità da lui rilevate.

Pur condividendone per la maggior parte struttura e protocollo presenta alcune differenze fondamentali:

Velocità: nel network Litecoin un blocco viene aggiunto alla Blockchain circa ogni 2.5 minuti contro i 10 di Bitcoin quadruplicando la velocità di creazione dei blocchi. Questo implica la possibilità di confermare le transazioni molto più rapidamente e a costi minori, nonché una minor congestione di rete e una riduzione del pericolo di attacchi double-spending a causa della finestra temporale utile ridotta. La proof of work utilizza l'algoritmo Scrypt: per ridurre il pericolo di centralizzazione del calcolo nei nodi che possono permettersi hashing powers enormi tramite hardware pre-esistente specializzato per il mining. Scrypt implementa alcune funzioni che fanno un largo uso di memoria per ridurre drasticamente l'efficienza dei circuiti logici tipici degli ASIC, privi di cache e ottimizzati per il mining intensivo. Trattandosi di un problema memory-hard sono privilegiate grandi quantità di RAM veloce. Questa scelta è stata fatta per evitare l'aumento esponenziale della difficoltà di mining in tempi brevi in un mercato in cui cominciavano già a prendere piede i suddetti dispositivi: Litecoin è nato oltre due anni dopo e la centralizzazione sarebbe stata un pericolo concreto. 84 milioni di unità monetarie, il quadruplo rispetto a Bitcoin.

I meccanismi di regolazione della difficoltà e di halving sono analoghi a Bitcoin ma i numeri cambiano: la difficoltà viene ricalcolata ogni 3.5 giorni -4 volte più velocemente- e l'halving è fissato ogni 840.000 blocchi -il quadruplo- in linea con la velocità e il numero di unità monetarie di Litecoin. 1.4.2.1. Qualche dato su

litecoin (?) Ad agosto 2018 risultano già minati e circolanti 57.000.000 Litecoin su un totale di 84.000.000 e il valore di un LTC fluttua intorno ai 60 euro.

Questo grafico [fonte] illustra l'andamento sul mercato di Litecoin ed evidenzia come questo segua tendenzialmente l'andamento di Bitcoin. Correntemente la ricompensa per un nuovo blocco ammonta a 25 LTC e il dimezzamento è previsto per il 6 agosto 2019. La blockchain Litecoin contiene attualmente ~1.470.000 blocchi.

$$\sum_{a}^{b} \left(\int \frac{c}{d} \right) + \begin{bmatrix} 5 & 7 \\ 9 & 8 \end{bmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix} \tag{1.1}$$

- **Bold**
- *Italic*
- Underline
- Link
- X_2
- Y^2

Capitolo 2

State of the art

2.1 Titolo section

Nel primo canto dell'Inferno, il pellegrino Dante si trova nella famigerata "selva oscura", che è simbolo esplicito di una situazione di traviamento esistenziale e spirituale che, per sua stessa ammissione, rischia di condurlo alle soglie della morte. L'aver scorto un colle rischiarato dalla luce divina non è che il primo passo del suo percorso di redenzione; le tre fiere che gli ostacolano il passo (la lonza, il leone, la lupa) lo costringono ad un lungo excursus nelle viscere infernali, durante il quale Dante sarà guidato da un altro "poeta" (v. 73), il buon Virgilio, che diverrà la sua guida morale e letteraria, subito dopo aver pronunciato la celebre profezia sul "veltro" (v. 101) che libererà il mondo terreno dal male e dal peccato [**?**].

Figura 2.1: *Just a Batman picture.*

2.1.1 Titolo subsection

Al di là dell'evidente e marcata metafora cristiana (il sacrificio e il martirio come testimonianza...), questa pellicola che ha tra i suoi protagonisti una Tilda Swinton strepitosa e sensualissima nel ruolo della malvagia strega, è visivamente seducente. Il luogo dominato da un eterno inverno, gli esseri fantastici e gli animali parlanti trasportano lo spettatore in un luogo di sogno dove anche i bambini protagonisti della pellicola in dinamiche sospese tra il gioco e l'eroismo personale 2.1.

Capitolo 3

Cuore della tesi e vari capitoli

Il gioco del trono è ambientato nei Sette Regni del Continente Occidentale, uno dei continenti del mondo fantastico creato da G. R. R. Martin, con forti richiami al Medioevo europeo. In questo continente, le stagioni durano per anni, senza cadenze precise.

```
// Hello.java
import javax.swing.JApplet;
import java.awt.Graphics;

public class Hello extends JApplet {
   public void paintComponent(Graphics g) {
      g.drawString("Hello, world!", 65, 95);
   }
}
```

Quindici anni prima dell'inizio del romanzo, i Sette Regni furono scossi da una guerra civile, nota come la "Guerra dell'Usurpatore" e la "Ribellione di Robert".

Capitolo 4

Risultati

Io ho aspettato alcuni mesi per passare dal primo volume al secondo, effetti collaterali del leggere la saga man mano che viene pubblicata. Perciò ero rimasta con Ned travolto da cavallo, e chissà quanti dettagli dimenticati.

Case	Method#1	Method#2	Method#3
1	50	837	970
2	47	877	230
3	31	25	415
4	35	144	2356
5	45	300	556

Tabella 4.1: Just a simple table

Capitolo 5

Conclusioni e sviluppi futuri

Pur essendo nato nel 2011, il network Litecoin ha recentemente guadagnato valore ed attenzione da parte di investitori e sviluppatori. La crescita è stata esponenziale soprattutto negli ultimi due anni e l'interesse allo sviluppo software per la blockchain stessa e la sua analisi si sta solo ora avvicinando a quello di Bitcoin. Le sue caratteristiche lo rendono adatto a pagamenti elettronici e correntemente, dopo un tentativo con LitePay, la fondazione Litecoin sta valutando l'adozione di una carta di debito simile ad un bancomat per pagamenti "fisici", per cui c'è da attendersi un incremento di interesse dal lato sia economico che software.

Per quanto riguarda il tool, si può pensare ad un raffinamento delle analisi tramite adeguamento delle librerie già esistenti ai nuovi protocolli e in modo analogo si possono implementare parti software per effettuare analisi simili su hard forks di Bitcoin come Bitcoin Cash. Quest'ultima seppur recente (nata il 1 agosto 2017) ha come obiettivo la riduzione delle fees e l'aumento della velocità di validazione delle transazioni sul network, ragioni per cui c'è da attendersi esiti e sviluppi simili a quelli di Litecoin.

Capitolo 6

Sviluppi futuri

Chiacchiere su profezie, sulle abitanti della città, sull'usanza delle lame che non possono essere sguainate, sui cavalieri del sangue e sui cavalieri della guardia reale. Per concludere, ennesima lite fra Dany e il fratello, con la khaleesi che decisamente non è più una bambina e non intende tollerare oltre l'idiozia di uno degli uomini peggiori che potrebbero sedere sul trono di spade.

Bibliografia

Elenco delle figure

Elenco delle tabelle

Ringraziamenti

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Praesent maximus volutpat commodo. Quisque euismod quis velit at placerat. Phasellus id nibh quis dolor pulvinar posuere. Phasellus ac nulla eget turpis tincidunt efficitur a nec nulla. In non urna finibus, suscipit sem sed, tempor turpis. Aliquam pharetra lectus sit amet mi gravida, accumsan tempor metus ullamcorper. Maecenas volutpat, felis eu euismod dignissim, arcu risus eleifend ligula, vel luctus sem neque non orci. Donec mattis arcu sed massa rutrum accumsan at nec mi. Morbi gravida risus non metus mattis tincidunt. Proin sed ipsum non erat ullamcorper ultricies. Sed quis tempus lacus, nec tincidunt dolor. Nam ornare, risus id tristique dignissim, arcu eros scelerisque ipsum, sit amet varius purus eros eu arcu. Aliquam gravida massa eget nibh tristique commodo. Suspendisse potenti. Maecenas tincidunt nisi ligula, placerat pellentesque leo malesuada vel.