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.[wik11]

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.[Ant14]

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**.

1.1.1 Bitcoin: Panoramica

Nella *figura1.1*, si può notare che il sistema bitcoin comprende: utenti con wallet che contengono chiavi, transazioni che sono propagate attraverso la rete, e miner che forniscono (attraverso una computazione competitiva) il consenso alla blockchain, la quale è il libro mastro di tutte le transazioni.

In questo paragrafo si andrà a tracciare il percorso di una singola transazione quando viene propagata attraverso la rete, e le interazioni tra ogni componente del sistema, ad alto livello.

Si prendano in considerazione per esempio, due utenti Bitcoin: Alice e Bob. Alice vorrebbe effettuare la sua transazione, comprando una tazza di caffè al bar di Bob (Bob's Cafe). Il bar di Bob, di recente ha iniziato ad accettare pagamenti in bitcoin,

Figura 1.1: *Bitcoin overview*

aggiungendo alla cassa un punto di pagamento Bitcoin. I prezzi del bar sono elencati in dollari, ma alla cassa, i clienti hanno l'opzione di pagare sia in dollari che in bitcoin.

Alice fa il suo ordine di una tazza di caffè e Bob inserisce la transazione nel registratore di cassa. Il punto di scambio di bitcoin, converte il prezzo totale dai dollari ai bitcoin secondo il tasso di mercato corrente, e mostra il prezzo nelle due valute, insieme ad un QR code contenente la *payment request* (richiesta di pagamento) per tale transazione (*figura 1.2*).

```
Total:
$1.50 USD
0.015 BTC
```

Figura 1.2: *Payment request QR code*

Se tale QR code viene scansionato, esso racchiude il seguente URL:

```
bitcoin:1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA?
amount=0.015&
label=Bob%27s%20Cafe&
message=Purchase%20at%20Bob%27s%20Cafe
```

Attraverso di esso si possono ottenere informazioni come: l'indirizzo bitcoin, l'ammontare del pagamento, un'etichetta per l'indirizzo del destinatario e una descrizione del pagamento.

A differenza di un QR code che contiene semplicemente l'indirizzo bitcoin del destinatario, un *payment request* è un QR-encoded URL che contiene un indirizzo di destinazione, il pagamento, e una descrizione generica come "Bob's Cafe". Questo permette all'applicazione del wallet di raccogliere le informazioni usate per effettuare il pagamento, al fine di mostrarle successivamente quando richieste dal proprietario del wallet. Se Bob scansiona il QR code con un'applicazione per un wallet bitcoin, oltre a ottenere il denaro, vedrà i dettagli inseriti da Alice.

Quindi, Bob dice: "Sono un dollaro e 50, oppure 15 millibitcoin"

Alice usa il suo smartphone per cansionare il codice e visualizzarlo sul display. Esso le mostra il pagamento di 0.015 BTC al Bob's Cafe e seleziona *Invia* per autorizzare il pagamento. In pochi secondi (all'incirca lo stesso tempo che ci mette una comune carta di credito), Bob potrà vedere la transazione sul registratore di cassa, conclusa.[Ant14]

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.[Ant14]

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 gli stessi 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 chain (=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* (=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.[Ant14]

Quando un blocco viene minato, ovvero viene aggiunto alla blockchain, viene etichettato con un timestamp, che rappresenta l'istante in cui viene ricevuto dal nodo bitcoin che ha la copia della blockchain.

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*

[Ant14]

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 1.3*), la rete appare con una singola prospettiva unificata della blockchain, con il blocco blu come estremità della catena principale.

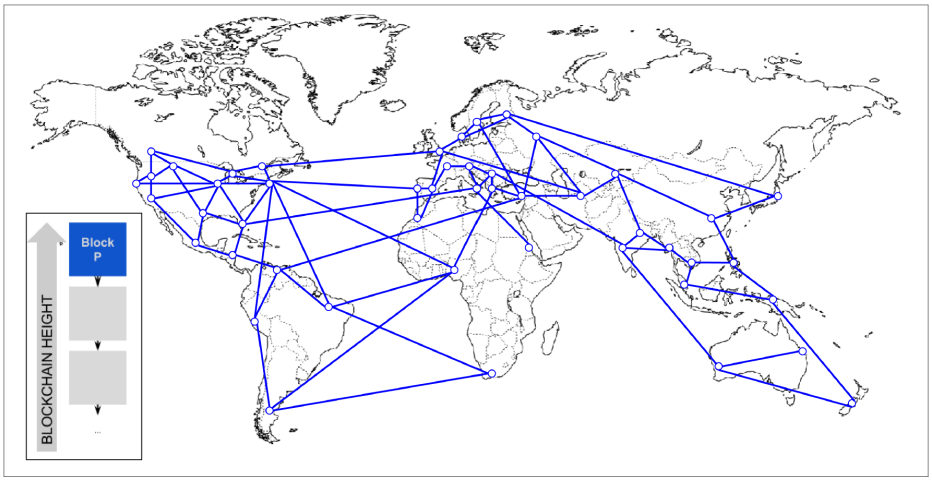

Figura 1.3: *Visualizzazione di un evento fork–prima della fork*

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 1.4* 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.

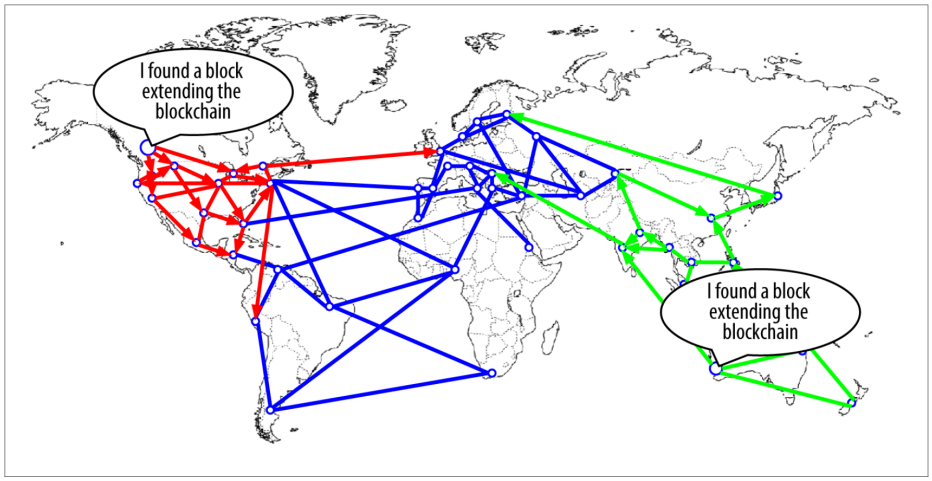

Figura 1.4: *Visualizzazione di un evento fork: due blocchi minati simultaneamente*

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 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.

Appena i due blocchi vengono propagati, alcuni nodi ricevono il blocco "rosso" e altri il blocco "verde". Come si può vedere in *figura 1.5*, 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

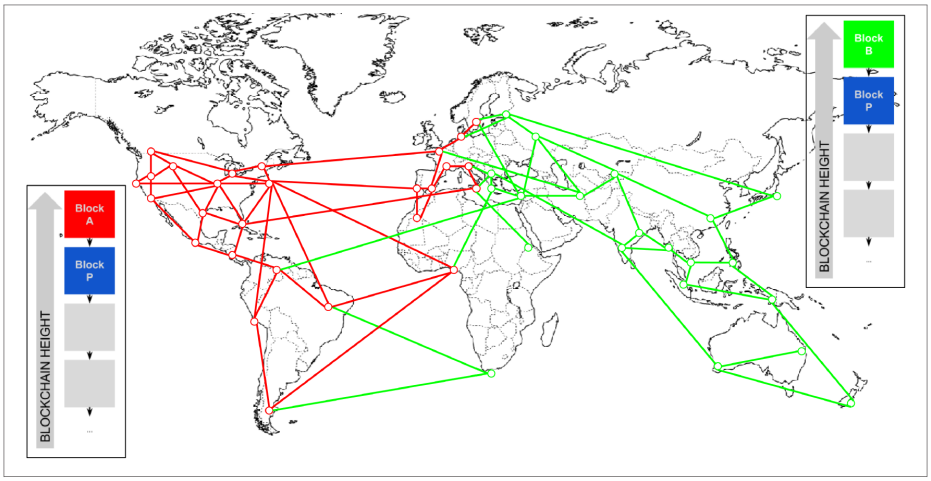

Figura 1.5: *Visualizzazione di un evento fork: due blocchi propagati, la rete biforca*

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 1.6*).

Tutti i nodi che hanno scelto il blocco "verde" come vincitore nel round precedente, estenderanno la catena di un ulteriore blocco. I nodi che hanno scelto il blocco "rosso" come vincitore, quindi, vedranno due chain: quella blu-verde-rosa e quella blu-rossa.

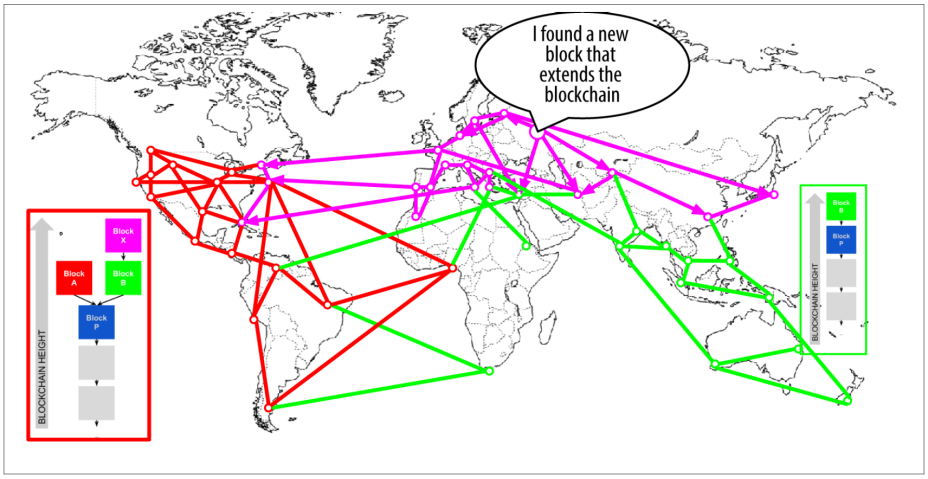

Figura 1.6: *Visualizzazione di un evento fork: un nuovo blocco estende un ramo della fork*

La chain blu-verde-rosa è la più lunga, ovvero è più difficile trovare una prook of work per essa. Inoltre, in *figura 1.7* si possono vedere i nodi che hanno scelto come catena principale la chain blu-verde-rosa e come chain secondaria quella blu-rossa.

Questo processo è detto *chain reconvergence*(letteralmente riconvergenza della catena), perchè tali nodi vengono forzati a cambiare il loro punto di vista della blockchain al fine di considerare la catena più lunga tra le due.

Ogni miner che lavora per estendere la chain blu-rossa non potrà più continuare poichè il blocco che stanno tentando di aggiungere al blocco rosso rimarrà "orfano", dato che il blocco rosso che dovrebbe fare da genitore non appartiene alla chain più lunga della blockchain.

Le transazioni che sono all'interno del blocco "rosso", vengono inserite di nuovo in coda per essere processate in un nuovo blocco, perchè, come si è già detto, il blocco a cui appartenevano non fa più parte della blockchain.

L'intera rete, quindi, riconverge la blockchain in una catena singola che fa capo ai blocchi blu-verde-rosa, con il blocco "rosa" come ultimo blocco all'estremità della catena. Tutti i miner immediatamente cominceranno a candidare nuovi blocchi che si andranno ad attaccare al blocco "rosa", al fine di estendere la catena blu-verde-rosa.

Teoricamente potrebbe essere possibile per una fork estendere due blocchi diversi,

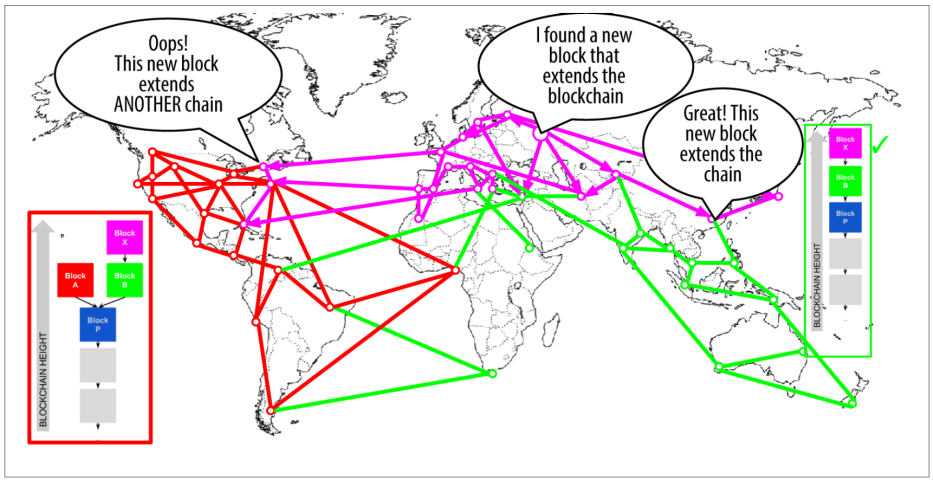

Figura 1.7: *Visualizzazione di un evento fork: la rete si riunisce in un'unica catena più lunga*

ma solamente se tali blocchi vengono creati quasi simultaneamente da miner che sono su "lati" diversi di una fork precedente. Tuttavia, la probabilità che ciò accada è molto bassa. Anche se ci fosse una fork ogni settimana, una fork a due blocchi è molto rara.

L'intervallo tra un blocco e il suo successivo è all'incirca di 10 minuti, proprio perché è stato progettato per essere un compromesso tra la velocità dei tempi di ricezione delle conferme e la probabilità di una fork. Un intervallo più ristretto da un lato potrebbe rendere le transazioni più veloci, dall'altro potrebbe causare fork più frequenti. Al contrario, un intervallo più ampio farebbe diminuire il numero delle fork ma renderebbe più lenti i pagamenti.[Ant14]

1.2.4 Merkle Tree

Ogni blocco della blockchain contiene un riepilogo di tutte le transazioni nel blocco, sotto forma di un **merkle tree**.

Un *merkle tree*, altrimenti detto *binary hash tree*, è una struttura dati usata per verificare e riepilogare efficientemente l'integrità dei dati. I merkle tree sono alberi binari composti da hash crittografici, dove ogni transazione è convertita in un hash, usando una funzione crittografica.

Il merkle tree è un albero perfettamente bilanciato, dove le foglie corrispondono

agli hash delle singole transazioni. I nodi intermedi invece, sono calcolati applicando la funzione di hash alla concatenazione dei valori dei due figli (*figura* 1.8).

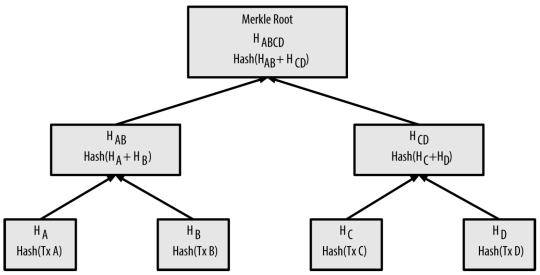

Figura 1.8: *Merkle tree*

Nella figura si può notare una porzione di un albero merkle, che prende in considerazione quattro transazioni: Tx A, Tx B, Tx C e Tx D. L'albero in questione presenta delle caratteristiche diverse se il nodo è una foglia oppure è un nodo intermedio. Esso è costruito secondo l'approccio bottom-up, prima vengono calcolati gli hash delle foglie, poi man mano si arriva al calcolo della radice.

Le foglie dell'albero, vengono calcolate come hash delle quattro transazioni, quindi si avranno le quattro foglie rispettivamente:

- H_A = Hash(Tx A)
- H_B = Hash(Tx B)
- H_C = Hash(Tx C)
- H_D = Hash(Tx D)

Successivamente si calcola il valore dei genitori delle foglie. Infatti, ogni nodo tra di essi, viene calcolato facendo l'hash della concatenazione dei valori contenuti nelle foglie. Quindi per ogni nodo intermedio si avrà:

- H_{AB} = Hash(H_A+H_B) [1]
- H_{CD} = Hash(H_C+H_D)

[1] In questo caso il simbolo + rappresenta la concatenazione

Infine, la radice si ottiene facendo lo stesso procedimento dei nodi intermedi, ossia facendo la concatenazione dei valori contenuti nei nodi figli. In questo caso si otterrà:

H_{ABCD} = Hash(H_{AB}+H_{CD})

Nell'esempio appena visto, l'albero era un albero binario, dove il numero di transazioni risultava essere un numero pari. Se ci fosse un numero dispari di transazioni da considerare nel merkle tree, l'ultima transazione verrebbe duplicata ottenendo così un numero pari di transazioni. Si otterrà quindi un albero *bilanciato*. In *figura 1.9* viene mostrata la duplicazione della transazione Tx C, e di conseguenza della foglia a cui appartiene. [Ant14]

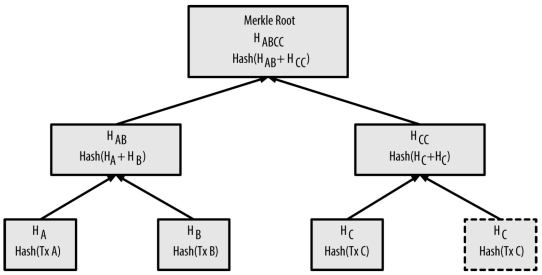

Figura 1.9: *Merkle tree con elemento duplicato*

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.

In parole semplici, la transazione dice alla rete che il proprietario di un certo numero di bitcoin, ha autorizzato il trasferimento di alcuni di tali bitcoin ad un altro individuo. Il nuovo proprietario dei bitcoin allora può spenderli creando una nuova transazione che autorizza il trasferimento degli stessi ad un altro destinatario. Tutto ciò genera una catena di proprietà di bitcoin.

Le transazioni sono come una riga in un registro di contabilità dove vengono salvati i trasferimenti. In poche parole, ogni transazione contiene uno i più input, cioè l'ad-

debito, ed uno o più output, cioè il credito aggiunto ad un altro account bitcoin. Gli input e gli output, rispettivamente l'addebito e il credito, non necessariamente devono essere la stessa cifra. Infatti, gli output aggiungono all'account destinatario una cifra leggermente minore di quella inviata negli input, la cui differenza rappresenta le *transaction fee*(ovvero le tasse di transazione), che vengono elargite al miner che ha minato il blocco nel quale andrà ad aggiungersi la transazione in corso. Nella *figura 1.10* viene mostrata una transazione come sarebbe all'interno di un registro di contabilità.

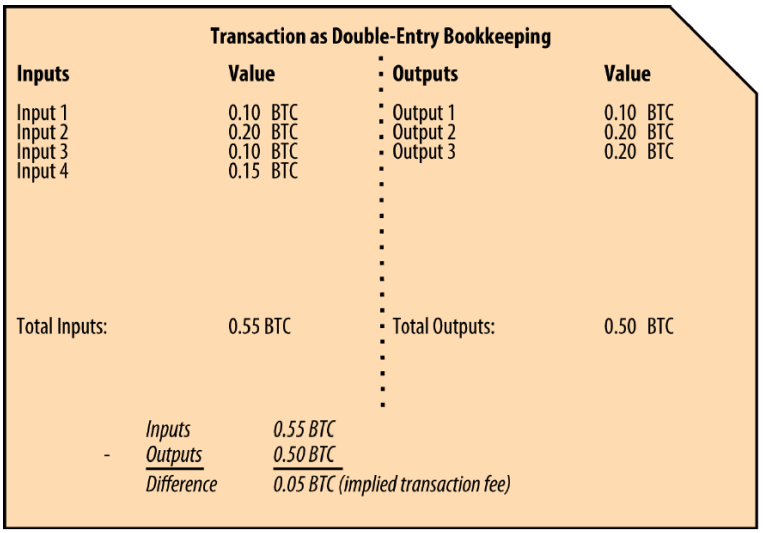

Figura 1.10: *Una transazione come una riga del registro di contabilità*

La transazione contiene anche la firma digitale del destinatario dell'importo dei bitcoin, in modo da fungere come prova di proprietà dal momento che nessun altro all'infuori del proprietario può validare la transazione e prendersi gli stessi bitcoin. In termini tecnici, "spendere" significa firmare una transazione che trasferisce il valore da una transazione effettuata in precedenza ad un nuovo proprietario identificato tramite il suo indirizzo bitcoin.

Le transazioni muovono ammontare di bitcoin da *transazioni in input* a *transazioni in output*. Un input è dove la moneta arriva da un output di una transazione effettuata in precedenza. Un output assegna un nuovo proprietario al valore scambiato, associandogli la chiave. La chiave di destinazione è chiamata *encumbrance*(letteralmente "impedimento"). Esso impone l'esigenza di avere una firma che serve a riscattare i fon-

di in transazioni future. Gli output di una transazione possono essere utilizzati come input in una nuova transazione, creando così una catena di proprietà che rappresenta il valore che si muove da indirizzo a indirizzo (*figura 1.11*).

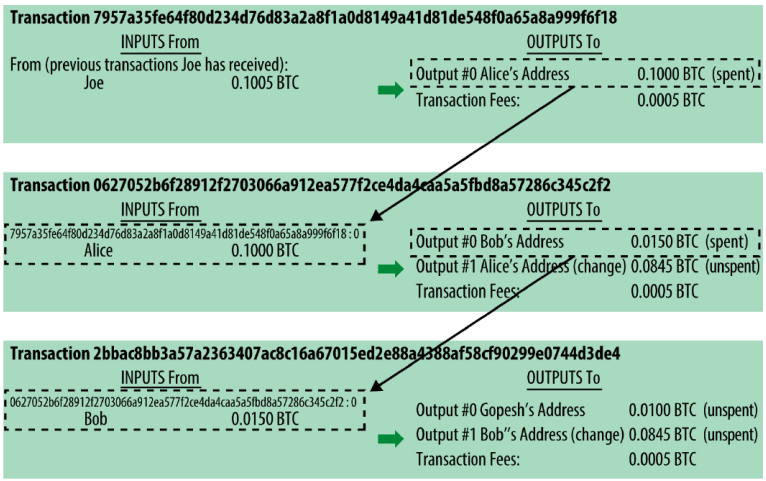

Figura 1.11: *Una catena di transazioni, dove l'output di una transazione viene utilizzato come input della transazione successiva*

Il pagamento di Alice al Bob's Cafe usa come input l'output di una precedente transazione. Infatti, prima di trasferire i suoi bitcoin a Bob, Alice li aveva ricevuti precedentemente da un suo amico Joe, che glieli aveva donati in cambio di una somma di denaro. Tale transazione ha un numero di bitcoin bloccati, che possono essere liberati solamente dalla chiave di Alice. La sua nuova transazione per pagare la tazza di caffè al bar di Bob fa riferimento come input alla transazione precedente e crea nuovi output grazie al pagamento.

Le transazioni formano una catena, dove gli input dell'ultima transazione corrispondono ad output della transazione precedente. La chiave di Alice ha la funzione di firma che sblocca gli output della transazione precedente, proprio per provare alla rete bitcoin che Alice possiede tali monete. Lei attribuisce il pagamento all'indirizzo di Bob, in tal modo bloccando l'output che poi successivamente sarà sbloccato dalla chiave di Bob. Tutto ciò rappresenta il trasferimento di bitcoin tra Alice e Bob. La catena di transazioni che parte da Joe e arriva a Bob è illustrata in *figura 1.11*.[Ant14]

1.3.1 Transaction Mining

Quando viene fatta l'operazione di mining dei blocchi, vengono inserite le transazioni all'interno del nuovo blocco. In questa sezione viene mostrato il mining dal punto di vista della transazione.

In media ogni 10 minuti, i miner generano un nuovo blocco che contiene tutte le transazioni che sono state generate dopo l'ultimo blocco inserito. Le nuove transazioni scorrono all'interno della rete dai wallet degli utenti e da altre applicazioni. Appena le transazioni incontrano la rete di nodi bitcoin, vengono aggiunte ad una struttura dati temporanea presente in ogni nodo dove vengono conservate tutte le transazioni che non sono ancora state verificate. Appena i miner generano un nuovo blocco, aggiungono le transazioni non verificate da tale struttura dati, al nuovo blocco e tentano quindi di trovare la proof of work.

Prendendo in considerazione l'esempio precedente, la transazione di Alice quindi, viene prelevata dalla rete e inclusa all'interno della struttura dati temporanea. Essa viene aggiunta ad un blocco che accetta l'importo delle tasse pagate da Alice. All'incirca cinque minuti più tardi che la transazione è stata trasmessa dal wallet di Alice, un miner riesce a minare il blocco e pubblica il blocco contenente un certo numero di transazioni compresa quella di Alice. Il miner in questione pubblica il nuovo blocco sulla rete bitcoin, dove gli altri miner lo validano e possono continuare la corsa a trovare una nuova proof of work.

Pochi minuti più tardi, un nuovo blocco viene minato da un altro miner. Dal momento che un nuovo blocco viene aggiunto come figlio del precedente, il quale contiene la transazione di Alice, tale transazione aumenta la difficoltà di computazione della soluzione, rafforzando la fiducia su tali transazioni. Il blocco che contiene la transazione di Alice è considerato come una "conferma" aggiunta alle conferme della transazione in questione. Ogni blocco minato, quindi funge come conferma addizionale ad ogni transazione che contiene.

Dal momento che i blocchi vengono impilati uno sopra l'altro, diventa esponenzialmente difficile invertire la transazione, in tal modo aumenta la fiducia della rete sulla Blockchain.

Nella *figura 1.12* si può osservare il blocco #277316 che contiene la transazione di

Alice.

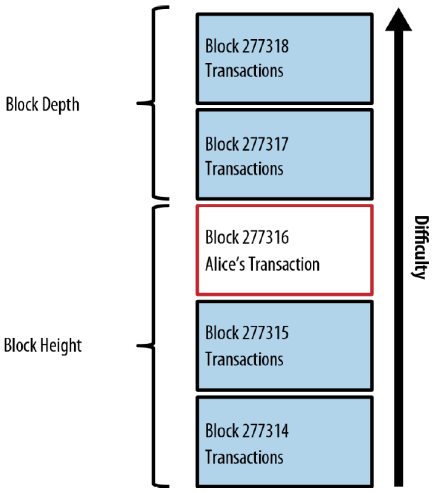

Figura 1.12: *La transazione di Alice inclusa nel blocco #277316*

Ora che la transazione di Alice è inserita all'interno della blockchain, ogni client bitcoin può verificare se la transazione è valida e spendibile. Bob allora può spendere i bitcoin che ha ricevuto da Alice, prendendo tale output e usandolo come input per una nuova transazione. Appena Bob spende tali bitcoin, allunga la catena di transazioni. Si supponga che Bob paghi il suo web designer Gopesh, per un nuovo sito web. Quindi, la catena di transazioni viene mostrata in *figura 1.13*.

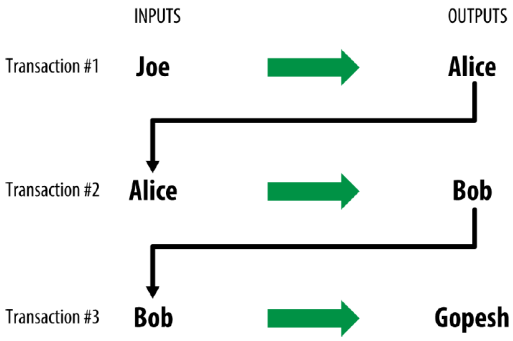

Figura 1.13: *La transazione di Alice come parte di una catena di transazioni che va da Joe a Gopesh*

1.3.2 Forma Comune delle Transazioni

La forma più comune di una transazione, è un semplice pagamento da un indirizzo ad un altro, in cui quasi sempre viene incluso il "resto" che ritorna al proprietario originale. Questo tipo di transazione ha un solo input e due output, di cui uno ha l'indirizzo pari all'indirizzo del mittente, tutto mostrato in *figura 1.14*.

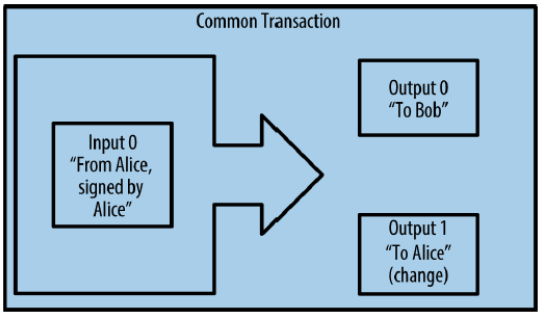

Figura 1.14: *Una comune transazione*

Un'altra forma comune è quella che aggrega molti input in un singolo output (*figura 1.15*). Questo rappresenta il reale scambio di diverse somme di denaro, in un singolo importo. Le transazioni come queste molto spesso sono generate da wallet per pulire piccoli importi che sono stati ricevuti come resto di altri pagamenti.

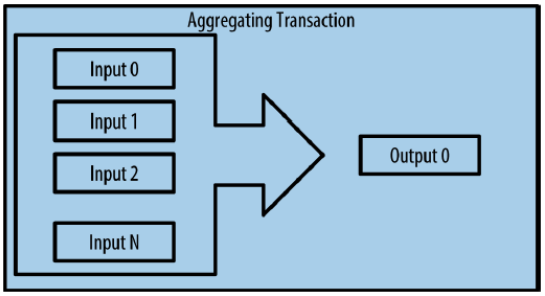

Figura 1.15: *Aggregazione*

Infine, un'altra forma può essere e quella che è il risultato di un'operazione in cui una singola transazione distribuisce il suo input su molti diversi output (*figura 1.16*). Questo tipo di transazione viene utilizzata di solito da entità commerciali per distribuire i fondi,

come quando un'azienda distribuisce il denaro come compenso ai propri dipendenti. [Ant14]

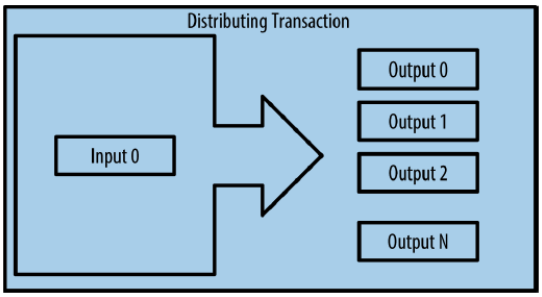

Figura 1.16: *Distribuzione*

1.3.3 Struttura di una Transazione

Una transazione è una struttura dati che racchiude un trasferimento di valori da una sorgente di fondi, chiamata *input*, ad una destinazione, chiamata *output*. Gli input e gli output non fanno riferimento ad account o ad identità. Al contrario, si potrebbe pensare ad esse come delle quantità di bitcoin – gruppi di bitcoin – che sono bloccati da una chiave crittografica. Solo il proprietario, possessore di tale chiave, può sbloccarli. Una transazione contiene dei campi di informazioni, come è mostrato nella *tabella 1.1*.

Size	Field	Description
4 bytes	Version	Specifica le regole seguite dalla transazione
1-9 byte (VarInt)	Input Counter	Numero degli input
Variable	Inputs	Transazioni in input
1-9 byte (VarInt)	Output Counter	Numero degli output
Variable	Outputs	Transazioni in output
4 bytes	Locktime	unix timestamp oppure il numero del blocco

Tabella 1.1: *La struttura di una transazione*

Il campo **Locktime** (letteralmente "tempo di chiusura") definisce il primo istante in cui una transazione può essere aggiunta alla blockchain. Quando è uguale a zero, indica l'immediata esecuzione.

Invece, se il locktime è maggiore di zero e minore di 500 milioni, è interpretato come l'altezza del blocco, ovvero significa che la transazione non è inclusa nella blockchain

prima di specificare altezza del blocco. Se è maggiore di 500 milioni, è interpretato come un timestamp di tipo Unix Epoch (il numero di secondi dal primo Gennaio 1970) e la transazione non è inclusa nella blockchain prima di quell'istante specifico.

1.3.4 Input e Output delle Transazioni

L'elemento fondamentale di una transazione bitcoin è l'**unspent transaction output** (lettralmente "output di transazione non speso"), nella forma contratta **UTXO**.

Gli UTXO sono gruppi indivisibili di monete bitcoin che possono essere sbloccati solo dall'utente proprietario. Vengono registrati nella blockchain e riconosciuti come unità monetaria dall'intera rete. La rete bitcoin ha tracciato tutti gli UTXO disponibili, e corrisponderebbero a milioni di bitcoin. Ogni volta che un utente riceve dei bitcoin, tale ammontare è registrato all'interno della blockchain sotto forma di UTXO. Quindi, un utente bitcoin potrebbe seminare migliaia di UTXO attraverso migliaia di transazioni e centinaia di blocchi. in effetti, non c'è nessun tipo di bilancio tra indirizzi bitcoin e output non spesi; ci sono solamente UTXO, che fanno capo a specifici proprietari. Il concetto di bilancio dell'utente in termini di output non spesi è un costrutto creato dall'applicazione che governa il wallet. Il wallet infatti, calcola il bilancio dell'utente scansionando la blockchain e aggregando tutti gli UTXO che appartengono a tale utente.

Un UTXO può avere un valore arbitrario che viene definito in termini di multipli di {satoshi. Come i dollari possono avere dei sottomultipli chiamati centesimi, i bitcoin possono essere divisi in satoshi. Ogni bitcoin corrispondono a 10^8 satoshi.[Ant14]

1.4 Grafo delle transazioni

Come sottolineato nelle sezioni precedenti, le transazioni sono collegate tra loro sotto forma di chain. Ogni output di ogni transazione diventa un input per la transazione successiva. In questo modo le transazioni formano catene che si possono intersecare tra di loro.

Se consideriamo ogni transazione come un nodo e il collegamento input/output come gli archi, si ottiene un grafo, dove ogni componente connessa è una chain di transazioni

connesse tra loro. Per ciò ogni catena di transazioni viene rappresentata come un gruppo di nodi-archi.

Si prenda in considerazione l'esempio visto in precedenza, della catena generata dalle transazioni di Joe, Alice, Bob e Gopesh (*figura* 1.13 di pagina 19). Alice riceve i bitcoin da Joe, poi li usa per pagare il caffè al bar di Bob, infine quest'ultimo utilizza una parte di tali bitcoin per pagare il suo web designer Gopesh.

In *figura 1.17* si può vedere come una catena di transazioni viene convertita in un grafo. In questo caso il grafo è un cammino, ovvero una sequenza di nodi collegati da archi, dove ogni nodo ha un solo predecessore ed un solo successore.

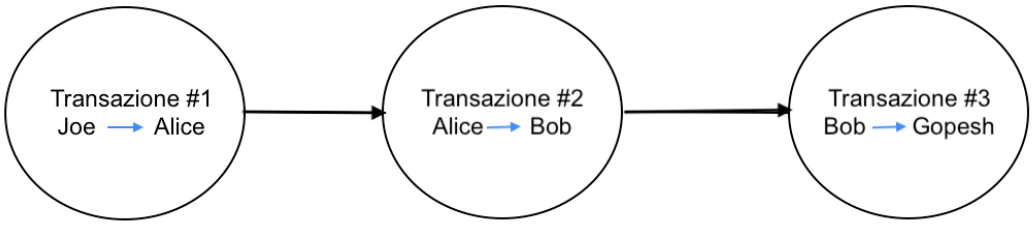

Figura 1.17: *Grafo delle transazioni*

Quindi, ogni transazione corrisponde ad un nodo, il quale è collegato agli altri nodi (alle transazioni) tramite flussi di denaro. Questi ultimi, sono gli output che vengono utilizzate come input da altre transazioni.

Per definizione, una transazione tx è caratterizzata da:

- un insieme di input $i_t^1, \cdots, i_t^h$
- un insieme di output $o_t^1, \cdots, o_t^k$

Ogni input e output sono associati ad un identificatore crittografico, chiamato *indirizzo* e un importo in bitcoin. La transazione tx trasferisce bitcoin dai suoi input ai suoi output.

Siano gli output di tx denotati con $txos$. Ad un certo istante T, ogni txo di una transazione t potrebbe essere stato speso ($stxo$) oppure no ($utxo$). L'unico modo per

spendere un certo *utxo* o_t di t, è usarlo come input $i_{t'}$ della transazione t' (con $t \neq t'$). In questo modo, come è stato già sottolineato nei paragrafi precedenti, il flusso dei bitcoin da una tx ad un'altra, crea un entità chiamata *chain of ownership* (letteralmente "catena di proprietà"). [DDP17]

Il *Transaction graph*("grafo delle transazioni") è un grafo diretto in cui i nodi sono le transazioni e viene indicato con *tx-graph*,. I nodi t e t' sono collegati tra loro dall'arco (t, t'), se l'output o_t di t è usato come input i_t di t'. Più nel dettaglio, il *tx-graph* è aciclico, poiché esse vengono generate una volta soltanto, ed è un multigrafo, dal momento che più output di t possono corrispondere a più input di t' (relazione molti-a-molti).

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

[Ant14] Andreas M Antonopoulos. *Mastering Bitcoin: unlocking digital cryptocurrencies.* " O'Reilly Media, Inc.", 2014.

[DDP17] Giuseppe Di Battista, Valentino Di Donato, and Maurizio Pizzonia. Long transaction chains and the bitcoin heartbeat. In *Workshop on Large Scale Distributed Virtual Environments (LSDVE 2017)*, 2017. To Appear.

[wik11] Bitcoin — wikipedia, l'enciclopedia libera, 2011.