LITECOIN

Litecoin (TLC) è una cripto-valuta peer-to-peer che consente di effettuare pagamenti istantanei a chiunque nel mondo. E' un software open-source rilasciato sotto licenza MIT/X11. Ispirato a Bitcoin e tecnicamente quasi identico ad esso, la creazione e il trasferimento si basa su un protocollo open-sourcee non è gestito da nessuna autorità centrale. Litecoin è nato come miglioramento di Bitcoin ed offre diverse differenze chiave rispetto ad esso. Ci sono attualmente 23 market di scambio che si occupano di Litecoin, e il più grande è BTC-E. La maggior parte degli scambi consentono solo BTC/LTC commerciali, mentre tre borse consentono anche trading LTC/USD e LTC/EUR.

Il progetto Litecoin è attualmente mantenuto da un nucleo di 6 sviluppatori software guidato dal creatore di Litecoin Charles Lee, e supportato da una grande comunità in rapida espansione.

Storia

Litecoin è stato rilasciato tramite un client open-source su GitHub il 7 ottobre 2011 da Charles Lee. Inizialmente era una fork del client BitCoin-QT, ma differisce principalmente da essa per un minor tempo di generazione di blocco, un aumento del numero massimo di monete, un diverso algoritmo di hash e una GUI leggermente modificata.

Il 25 aprile 2013 Mt.Gox ha annunciato che i trading per Litecoin erano stati ritardati a causa di un attacco DDos sul suo sito web

Nel 2013 The Economis ha citato Litecoin come la miglior alternativa a Bitcoin e i maggiori media come il Wall Steet Journal, la CNBC e il New York Times hanno battezzato i Litecoin come possibili successori di Bitcoin.

Durante novembre 2013, il valore di dei Litecoin ha visto una crescita del 100% in 24 ore. A dicembre invece ha registrato il suo maggior crollo, perdendo oltre il 50% del suo valore in 10 ore.

Versioni

Una delle ultime versione di Litecoin, la 0.8.5.1, è stata rilasciata a novembre 2013 e corregge alcune vulnerabilità e aggiunge maggiore sicurezza alla rete.

Nel dicembre 2013 il team di sviluppo ha rilasciato la versione 0.8.6.1 che offre miglioramenti della sicurezza e migliori prestazioni nel client e nella rete. Il codice sorgente e i file binari sono stati resi pubblici prima sul canale IRC #litecoin, sul

forum ufficiale e su Reddit. Solo dopo alcuni feedback dalla rete è stato aggiornato anche il sito principale. Tutto questo è stato necessario per far si che i client con la nuova versione non fossero rallentati da client con versioni precedenti.

Nel mese di aprile 2014 è stata rilasciata l'ultima versione, la 0.8.7.1, che ha risolto un grande problema di vulnerabilità e sistemato alcuni piccoli bug.

Proprietà

I Litecoin possono essere estratti efficacemente con un hardware di tipo consumer. Fornisce una conferma di transazione più veloce (circa 2.5 minuti) e prevede la produzione di 84 milioni di unità. Ogni Litecoin può essere suddiviso in 100.000.000 piccole unità, definite da 8 cifre decimali.

Uno degli scopi di Litecoin era fornire un algoritmo di mining in grado di funzionare allo stesso tempo e sullo stesso hardware utilizzato per estrarre Bitcoin. Con l'ascesa degli ASICs (Application Specific Integrated Circuits) per Bitcoin, Litecoin continua a soddisfare i suoi obiettivi.

Blocchi Litecoin e Processo di Mining

I blocchi rappresentano il modo in cui i dati sono registrati in modo permanente nella rete litecoin. Un blocco è una registrazione di alcune o di tutte le più recenti transazioni Litecoin che non sono ancora stati registrati in tutti i blocchi precedenti. Ogni blocco contiene, tra le altre cose, nel suo "block header", un record di alcune o tutte le recenti operazioni, e un riferimento al blocco che lo precede. Contiene anche una risposta a un difficile rompicapo matematico da risolvere - la cui risposta è unica per ciascun blocco. Ecco un esempio di struttura di un blocco Litecoin:

Field	Description	Size
Magic no	value always 0xD9B4BEF9, see network IDs	4 bytes
Blocksize	number of bytes following up to end of block	4 bytes
Blockheader	Contains 6 elements, see block header	80 bytes
Transaction counter	positive integer VI = VarInt	1 - 9 bytes
transactions	the (non empty) list of transactions	<Transaction counter>-many transactions

Nuovi blocchi non possono essere inoltrati alla rete senza la risposta corretta - il processo di " mining " è essenzialmente il processo di competizione per essere il primo a trovare la risposta che" risolve "il blocco attuale.

Il problema matematico in ogni blocco è difficile da risolvere, ma una volta trovata una valida soluzione è molto facile per il resto della rete confermare che la soluzione è corretta. Ci sono molteplici soluzioni valide per qualsiasi blocco.

Perché c'è una ricompensa in Litecoin per la risoluzione di ogni blocco, ognuno di essi contiene anche un record per ricevere la ricompensa. Questo record è noto come una *transazione di generazione*, o *transazione coinbase*, ed è sempre la prima operazione che appare in ogni blocco. Il numero di Litecoins generati per blocco inizia da 50 e si dimezza ogni 840.000 blocchi.

Ogni blocco contiene un riferimento al blocco precedente, quindi la raccolta di tutti i blocchi esistenti forma una catena. Tuttavia è possibile che la catena abbia spaccature temporanee - per esempio, se due *miners* arrivano a due diverse soluzioni valide per lo stesso blocco, allo stesso tempo, all'insaputa l'uno all'altro .La rete peer-to-peer è progettata per risolvere queste spaccature entro un breve periodo di tempo, in modo che solo un ramo della catena possa sopravvivere.

Non esiste un numero massimo di blocchi in Litecoin. I blocchi continuano ad essere aggiunti alla fine della catena ad un tasso medio di uno ogni 2,5 minuti.

Per la risoluzione di un blocco è possibile che un gruppo di miners mettano in comune le loro risorse in modo che possano risolvere i blocchi più velocemente. In questo caso si parla di *pool mining* e la ricompensa viene suddivisa tra i membri del pool in base alle loro contributi.

Target

Precedentemente abbiamo parlato di Difficoltà come misura di quanto sia difficile trovare un nuovo **blocco**. E 'un modo human-friendly di esprimere il Target

Il Target è un numero a 256 bit che tutti i client Litecoin condividono. Lo scrypt hash dell'header di un blocco deve essere inferiore o uguale al target corrente per essere accettato dalla rete. Più il target è basso, più è difficile generare un blocco.

Il Target viene regolato automaticamente dalla rete, in modo tale che si abbia una media di 24 blocchi all'ora da risolvere. Ogni 2.016 blocchi, tutti i client Litecoin confrontano il numero di creazioni effettive con questo obiettivo e variano il Target

La Difficoltà può essere calcolata dal Target corrente (che è un numero di 256 bit) come segue:

```
Difficoltà = 0xFFFF * 2 ** 208 / target
```

Ogni blocco memorizza una rappresentazione compressa (chiamata Bits) del suo target esadecimale. Il Target può essere derivato da esso tramite una formula predefinita. Se ad esempio il Target compresso nel blocco è 0x1b0404cb, il relativo Target esadecimale è:

```
0x0404cb * 2**(8*(0x1b - 3)) =
0x00000000000404CB000000000000000000000000000000000000000000000000
```

Si noti che il valore 0x0404cb è un valore *firmato* in questo formato. Il valore più grande possibile in questo campo è 0x7fffff. Per fare un valore più grande è necessario spostarlo in basso di un byte completo.

La difficoltà massima è approssimativamente: Target_massimo / 1 (0 poiché comporterebbe infinito), che è un numero enorme (circa 2 ^ 224)

Come già detto, La difficoltà viene regolato ogni 2016 blocchi in base al tempo impiegato per trovare i precedenti 2.016 blocchi. Al ritmo di un blocco ogni 2,5 minuti, 2.016 blocchi andrebbero creati esattamente in 3,5 giorni. Se i precedenti 2.016 blocchi sono stati creati in più di 3,5 giorni, la difficoltà è ridotta. Se hanno richiesto meno di 3,5 giorni, la difficoltà viene aumentata. La variazione in difficoltà è quindi proporzionale alla quantità di tempo sopra o meno di 3,5 giorni.

Per trovare un blocco,lo **scrypt** hash deve essere inferiore rispetto al target. Questo hash è effettivamente un numero casuale compreso tra 0 e 2 ** 256-1. L'offset per difficoltà 1 è:

```
0xffff * 2 ** 208
```

e per la difficoltà D è:

```
(0xffff * 2 ** 208) / D
```

Il numero di hash che si ha bisogno di calcolare per trovare un blocco con difficoltà D è quindi

```
D * 2**256 / (0xffff * 2**208)
```

O più semplicemente:

```
D * 2**48 / 0xffff
```

La difficoltà è settata in modo che i precedenti 2016 blocchi siano stati trovati ad un ritmo di uno ogni 2.5 al minuto, quindi sono stati calcolati (D * 2**48 / 0xffff) hash in 150 secondi. Questo significa che l'hash rate della rete era:

```
D * 2**48 / 0xffff / 150
```

Per fare un esempio, al momento della scrittura di questo documento la difficoltà è di 1169.85315079, il che significa che per la serie di 2016 blocchi trovati precedentemente l'hash rate della rete era:

```
1169.85315079 * 2**32 / 150 = circa 33 Ghashe per secondo.
```

Transazioni

Ogni transazione è registrata nel Blockchain Litecoin (un registro tenuto dalla maggior parte dei client) ed un nuovo blocco viene aggiunto alla blockchain ogni 2.5 minuti. Una transazione è considerata completa solitamente dopo 6 blocchi o dopo 16 minuti, anche se per operazioni più piccole possono essere necessari meno blocchi per un'adeguata sicurezza.

Il tasso di emissione da una serie geometrica e la riduzione del tasso di emissione ogni 4 anni (ogni 840.000 blocchi) portano a un totale di 84 milioni di Litecoin.

I pagamenti in rete Litecoin sono effettuati per indirizzi e basati su firme digitali. Esse sono stringhe di 33 caratteri alfanumerici ed iniziano sempre con la lettera 'L'.

Attualmente i Litecoin sono principalmente utilizzati per transazioni online. Operazioni reversibili (come quelle con carta di credito) non sono normalmente utilizzate per acquistarli.

Così come i Bitcoin, i prezzi dei Litecoin sono volatili e instabili subendo oscillazioni molto rapide, come il 40% in un giorno o il 1000% in un mese.

Le transazioni Litecoin sono irreversibili per contrastare il pericolo di chargeback.

Scrypt

La caratteristica principale di Litecoin è l'uso di Scrypt (una funzione di derivazione di chiave basata su password creata da Colin Percival) come protocollo proof-of work.

Un algoritmo proof-of-work è una misura economica per scoraggiare attacchi **denial of service** e altri abusi di servizio, come **spam** sulla rete, imponendo alcuni lavori dal richiedente del servizio, di solito richiedendo tempo di elaborazione di un computer. Una caratteristica chiave di questi schemi è la loro asimmetria: il lavoro deve essere moderatamente complesso (ma fattibile) dal lato richiedente ma facile da controllare per il fornitore del servizio (**service provider**). Questa idea è anche conosciuta come *funzione di costo della CPU*, *client puzzle*, *puzzle computazione* o *funzione di pricing della CPU*.

Nel caso di Litecoin, crea una sfida computazionale da risolvere al fine di "certificare" a "blocco" la transazione. In contrasto con l'SHA-256d di Bitcoin,Scrypt serve a inibire la scalabilità hardware richiedendo una notevole quantità di memoria quando si eseguono i calcoli. Questo rende l'implementazione in "special purpose" hardware meno efficiente in quanto richiede di riservare alcune zone di memoria.

Questa modifica riduce il guadagno di efficienza e gli incentivi economici per sviluppare hardware personalizzato come gli ASICs.

L'idea principale dietro Scrypt è di generare una grande quantità di numeri speudo-casuali che vengono memorizzati in RAM e sono accessibili su richiesta. L'algoritmo quindi accede a questa memoria in modo pseudo-casuale un certo numero di volte prima di ritornare il risultato.

Un'implementazione senza l'utilizzo della RAM è possibile e, in questo caso, i numeri pseudo-casuali sarebbero generati come necessario. Tuttavia, poiché la loro generazione è computazionalmente costosa ed è richiesto di accedere ad essi molte volte, un'implementazione di Scrypt in questo modo è stata considerata troppo costosa in termini di risorse computazionali.

I parametri di Scrypt possono essere modificati in modo da richiedere più o meno RAM o potenza di camcolo. Tuttavia l'implementazione di Scrypt in Litecoin è impostata in modo da richiedere solo 128KB di memoria in modo da non stressare troppo i nodi non-mining. Questo permette di implementare Litecoin negli ASICs anche se ancora in modo meno efficiente rispetto a Bitcoin: si stima che il vantaggio ASICs in Litecoin sia ridotto di un fattore 10 rispetto a Bitcoin.

Essendo Scrypt relativamente recente rispetto ad SHA-256, ha ricevuto meno controllo da parte dei crittografi e questo lo rende in un certo senso più rischioso, essendo più alta la probabilità di trovare vulnerabilità.

Bug Noti

Oltre agli indirizzi standard basati su firma singola, sulla rete BitCoin ci sono anche indirizzi multi-firma che iniziano con il numero “3”. Litecoin è stato creato prendendo lo stesso codice sorgente di Bitcoin e gli sviluppatori hanno modificato gli indirizzi a firma singola tramite l’inserimento della “L”, ma non hanno apportato modifiche agli indirizzi multi-firma. Quindi sia in Litecoin che in Bitcoin questi indirizzi iniziano con il numero “3”.

Questo può causare alcuni problemi per gli utenti alle prime armi, in quanto possono inviare Litecoin ad indirizzi Bitcoin con una irrimediabile perdita di essi, in quanto gli indiritti Bitcoin non esistono nella rete Litecoin (sono compatibili ma non esiste una chiave privata per riceverli o spenderli)

Litecoin vs Bitcoin

E' interessante sapere che la motivazione dietro la creazione di litecoin era di migliorare bitcoin.

Oggi litecoin ha la più alta capitalizzazione di mercato di qualsiasi criptovaluta, dopo bitcoin. In questi ultimi anni litecoin ha dimostrato di riuscire a tenere il passo di bitcoin ma di non avere la forza necessaria a guadagnare ulteriore terreno nonostante le caretteristiche di litecoin siano migliori di quelle di bitcoin.

Questa tabella mostra le principali differenza tra litecoin e bitcoin.

	Bitcoin	Litecoin
Limite coin	21 milioni	84 milioni
Algoritmo	Sha-256	Scrypt
Tempo medio di blocco	10 minuti	2,5 minuti
Ricompensa	Dimezzata ogni 21000 blocchi	Dimezzata ogni 840000 blocchi
Ricompensa iniziale	50 BTC	50 LTC
Blocco ricompensa corrente	25 BTC	50 LTC
Data creazione	03/01/09	07/10/11
Capitalizzazione mercato	$ 10.467.596.650.78	$ 540.274.528.26
Totale blocchi	775,48	355,18
Difficoltà	39,73	47,643,398,144

Differenze Mining

La differenza fondamentale per gli utenti finali è il tempo: 2,5 minuti per generare un blocco, 7,5 minuti in meno rispetto ai 10 minuti di Bitcoin.

Per i minatori, però, litecoin ha una differenza molto più importante rispetto Bitcoin, ossia l'algoritmo con cui lavora.

Bitcoin utilizza l'algoritmo di hashing SHA-256, che prevede un calcolo che può essere notevolmente accelerato in elaborazione parallela. Caratteristica, questa, che ha dato luogo ad un intensa gara in tecnologia ASIC e ha provocato un aumento esponenziale del livello di difficoltà di bitcoin.

Litecoin, invece, usa l'algoritmo scrypt, originariamente chiamato s-crypt, ma pronunciato 'script'. Questo algoritmo incorpora l'algoritmo SHA-256 ma i suoi calcoli sono molto più serializzati di quelli del SHA-256 di bitcoin.

Scrypt favorisce grandi quantità di RAM ad alta velocità al contrario di SHA-256 che favorisce solo potenza di elaborazione.

L'uso di scrypt porta alla conclusione che non vi è stato ancora una 'corsa agli armamenti' in litecoin (e altre valute scrypt), perché non vi è (finora) nessuna tecnologia ASIC per questo algoritmo.

Per il momento gli impianti minerari di litecoin si presentano sotto forma di PC personalizzati dotati di più schede grafiche. Questi dispositivi sono in grado di gestire i calcoli necessari per scrypt e avere accesso alla fast memory incorporata nelle proprie schede a circuiti.

C'è stato un tempo in cui si utilizzavano GPU per il mining di bitcoin, ma le tecnologie ASIC hanno portato all'inutilizzo di questi metodi.

Differenze di transazione

La differenza principale è che litecoin è in grado di confermare le transazioni in maniera più veloce di Bitcoin.

Questo implica:

- Litecoin è in grado di gestire un volume più alto di transazioni, grazie al fatto che genera blocchi più velocemente. Se bitcoin dovesse cercare di corrispondere a questo, sarebbero necessari aggiornamenti significativi per il codice attualmente in esecuzione da tutti gli utenti della rete bitcoin.
- Lo svantaggio di questo maggiore volume di blocchi è che il blockchain litecoin sarà proporzionalmente più grande di bitcoin, con blocchi più orfani.
- Il tempo di blocco veloce di litecoin riduce il rischio di attacchi doppi
- Un commerciante che ha aspettato per un minimo di due conferme avrebbe solo bisogno di attendere cinque minuti, mentre avrebbero dovuto aspettare 10 minuti per una solo conferma con bitcoin.