

Analisi di Bitcoin

Anonimato, Sicurezza e Sviluppi Futuri

Paoluzzi Matteo

Università degli Studi di Udine

Relatore:
Prof. Ivan Scagnetto

IV Sessione di Laurea AA 2012/2013, Aprile 2014

Di cosa si tratta

- È una valuta utilizzabile per scambi commerciali.
- Esiste solo in forma elettronica.
- Non ha confini geografici.
- Bitcoin indica la rete e il protocollo.
- L'unità monetaria si indica con BTC.

- Struttura completamente decentralizzata formata da nodi in un grafo casuale.
- Anonimato dell'utente.
- Indipendente da istituti centrali.
- Transazioni sicure e verificabili.

- Si usa la cifratura a chiave pubblica per creare una serie di indirizzi in cui verrà depositato il denaro.
- Ogni transazione viene firmata con la chiave privata del mittente e contiene la chiave pubblica del destinatario.
 - Solo il destinatario di una transazione può spendere il denaro trasferito come unico proprietario della chiave privata richiesta.
 - Si viene a creare una catena di transazioni legate dalle chiavi pubbliche e private di mittente e destinatario.
- Tutte le transazioni vengono rese pubbliche e confrontate tra loro in modo che nessuno possa spendere lo stesso denaro due volte.
- Le transazioni vengono fissate in blocchi che vengono concatenati tra loro.

- L'input di una transazione può solo essere l'output di una precedente transazione.
- Non è possibile spendere denaro che non è stato inviato ad un indirizzo di cui non si possiede la chiave privata.
- Le transazioni sono bloccate nel tempo da un timestamp e da un hash che le identifica in modo permanente.
- La rete verifica che uno stesso input non sia stato inviato a diversi output: un tentativo di attacco doppia-spesa.

I blocchi vengono creati risolvendo un difficile problema crittografico.

- Trovare l'hash di alcuni dati in modo che risulti un valore esadecimale inferiore ad uno specifico target.
- Il target viene ricalcolato ogni 2016 blocchi mantenendo fisso a 10 minuti il tempo medio per trovare un blocco.
- Tra i dati di cui calcolare l'hash ci sono le transazioni e l'hash del blocco precedente.
 - La modifica di un blocco richiede la modifica di tutti i blocchi successivi.
 - Concatenare blocchi rende sempre più difficile modificare un blocco vecchio.

How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES



Bob and Alice both have Bitcoin "wallets" on their computers.



Wallets are files that provide access to multiple Bitcoin addresses.



An address is a string of letters and numbers, such as 1A1izSqS2241v7PwL97Ktj9A84t9LpKt9t9.



Bob creates a new Bitcoin address for Alice to send her payment to.

CREATING A NEW ADDRESS

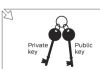


Each address has its own balance of bitcoins.

SUBMITTING A PAYMENT



Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.



Public Key Cryptography 101
When Bob creates a new address, what he's really doing is generating a "cryptographic key pair" composed of a private key and a public key. You sign a message with a private key (which only you know). It can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

It's tempting to think of addresses as bank accounts, but they work a lot differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

Gary, Gertrude, and Glenn are Bitcoin miners.



VERIFYING THE TRANSACTION

The computers bundle the transactions of the past 10 minutes into a new "transaction block."



The miners' computers are set up to calculate cryptographic hash functions.



Each new hash value contains information about all previous Bitcoin transactions.



The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.



Cryptographic Hashes

Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

Thousand of all odds	256x1000 (256 more characters)
Thousand of all odds	486C (664,160)
Thousand of all odds	1616x720 (1616x720)

The word of all odds

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.



Nonces

To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a widely different hash value.

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly mined bitcoins.



TRANSACTION VERIFIED

As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.



Creare un blocco ha molteplici scopi.

Creare un blocco ha molteplici scopi.

- Blocca le transazioni in modo permanente.
- Permette la creazione di nuova moneta.
 - Il lavoro speso per trovare il blocco viene ricompensato con BTC create “dal nulla”.
 - Il numero di BTC si dimezza nel tempo per mantenere il numero massimo di BTC a circa 21 milioni.
 - Inizialmente il premio era di 50 BTC, ora è sceso a 25 BTC.

Creare un blocco ha molteplici scopi.

- Blocca le transazioni in modo permanente.
- Permette la creazione di nuova moneta.
 - Il lavoro speso per trovare il blocco viene ricompensato con BTC create “dal nulla”.
 - Il numero di BTC si dimezza nel tempo per mantenere il numero massimo di BTC a circa 21 milioni.
 - Inizialmente il premio era di 50 BTC, ora è sceso a 25 BTC.

L'analogia è con i cercatori d'oro, che guadagnano dal ritrovamento delle pepite dopo ore di duro lavoro in miniera.

Creare un blocco ha molteplici scopi.

- Blocca le transazioni in modo permanente.
- Permette la creazione di nuova moneta.
 - Il lavoro speso per trovare il blocco viene ricompensato con BTC create “dal nulla”.
 - Il numero di BTC si dimezza nel tempo per mantenere il numero massimo di BTC a circa 21 milioni.
 - Inizialmente il premio era di 50 BTC, ora è sceso a 25 BTC.

L'analogia è con i cercatori d'oro, che guadagnano dal ritrovamento delle pepite dopo ore di duro lavoro in miniera.

Pertanto il processo di calcolo dell'hash di un nuovo blocco viene definito *mining* e il nodo *miner*.

Calcolare l'hash per un blocco è un evento casuale senza memoria che richiede elevata potenza di calcolo per essere portato a termine in tempi rapidi.

- Un computer end-user ha decisamente poche speranze di trovare un blocco e intascare la ricompensa.
- Con del costoso hardware dedicato le speranze aumentano un poco, ma restano comunque basse.

Calcolare l'hash per un blocco è un evento casuale senza memoria che richiede elevata potenza di calcolo per essere portato a termine in tempi rapidi.

- Un computer end-user ha decisamente poche speranze di trovare un blocco e intascare la ricompensa.
- Con del costoso hardware dedicato le speranze aumentano un poco, ma restano comunque basse.

La soluzione è una collaborazione tra gli utenti in quelle che vengono definite *mining pools*.

Calcolare l'hash per un blocco è un evento casuale senza memoria che richiede elevata potenza di calcolo per essere portato a termine in tempi rapidi.

- Un computer end-user ha decisamente poche speranze di trovare un blocco e intascare la ricompensa.
- Con del costoso hardware dedicato le speranze aumentano un poco, ma restano comunque basse.

La soluzione è una collaborazione tra gli utenti in quelle che vengono definite *mining pools*.

Mantenendo l'analogia con i minatori, le mining pools sono compagnie minerarie.

- Più minatori si cimentano in contemporanea nel ritrovamento di un blocco.
- Ad ogni blocco trovato la ricompensa viene divisa tra tutti coloro che hanno collaborato.
- Ogni pool ha un suo sistema di retribuzione con i suoi vantaggi e svantaggi.

Il protocollo sfrutta un linguaggio di scripting che permette di verificare le transazioni ma anche di crearne alcune non-standard che implementano situazioni diverse dal semplice pagamento.

- Sistemi di deposito temporaneo.
- Raccolte fondi con assicurazione.
- Acquisto di beni con un mediatore.

Essendo non-standard, attualmente queste transazioni vengono rifiutate dai nodi e non possono entrare a far parte della blockchain. Possono però essere usate in reti private con client ad-hoc.