

# 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.

- 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.

## 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 THULNW00KjEPeCh43BwKJLylLCWwfdDots

Each address has its own balance of bitcoins.



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 Bitcoin creates a new address, what it's really doing is generating a "cryptographic key pair" composed of a private key and a public key. If 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 bit 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.



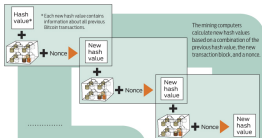
### VERIFYING THE TRANSACTION



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



Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.



## 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.

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

The root of all evil 277

0000 0000  
0000

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

The root of all evil ▶ [b0ld a1859 038a...](#)  
(56 more characters)

The root of the problem

of all full	400K, 500K, 600K...
-------------	---------------------

The root of all evil  b3db 7ee9 8392...

## None

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 wildly different hash value.

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.



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

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.

Il protocollo sfrutta un linguaggio di scripting che permette di creare transazioni non-standard.

- Bla
- BlaBla
- BlaBlaBla