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.

Criteri di progettazione

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

Implementazione

- 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.

Sicurezza: le transazioni

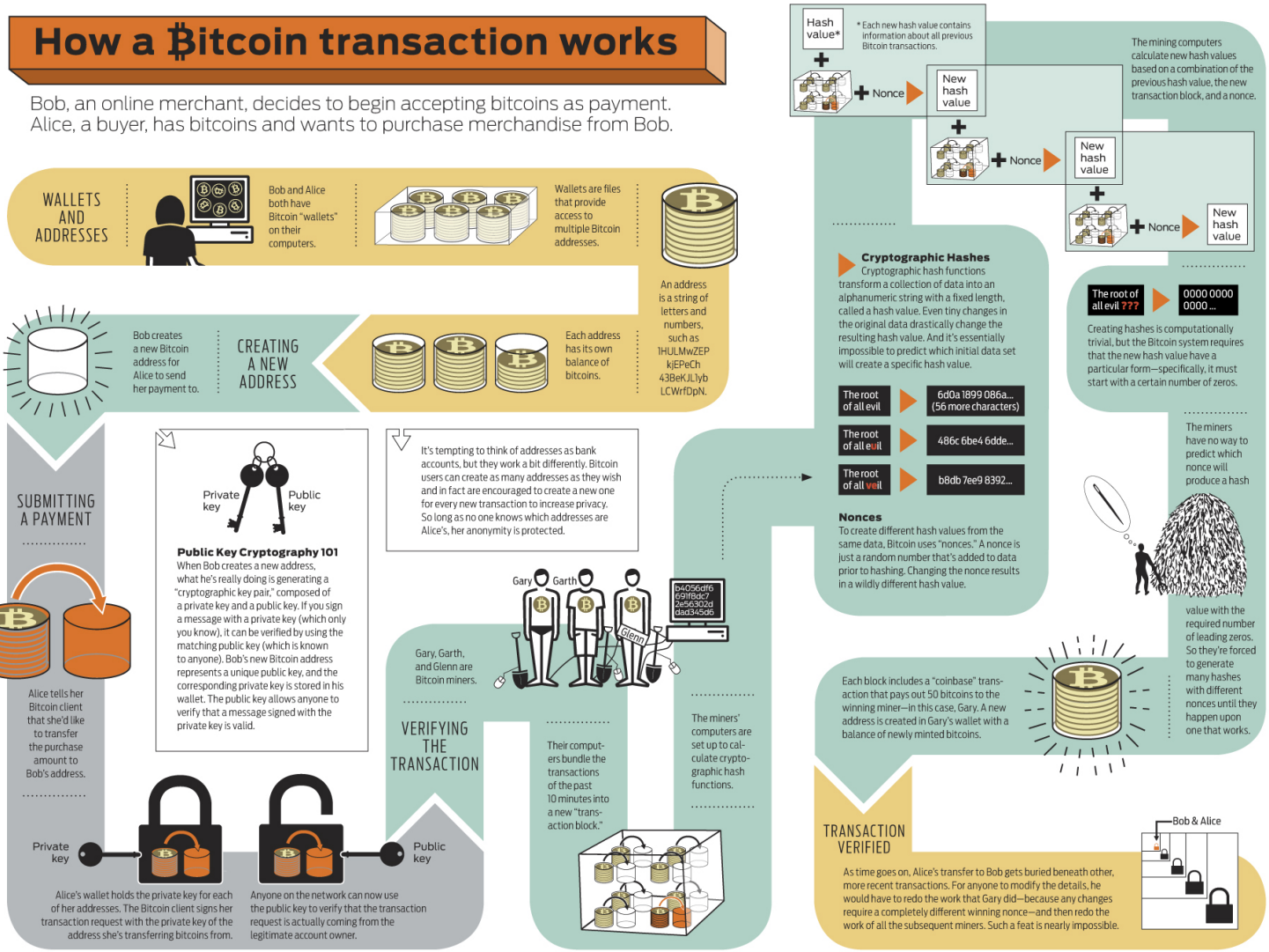
- L'input di una transazione può solo essere l'output di una precedente transazione.
- Non è possibile spendere denaro che non è stato inviato ad un indirizzo di cui non si possiede la chiave privata.
- Le transazioni sono bloccate nel tempo da un timestamp e da un hash che le identifica in modo permanente.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

Sicurezza: i blocchi

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.

Infografica



Mining

Creare un blocco ha molteplici scopi.

Mining

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.

Mining

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.

Mining

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*.

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.

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*.

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.

Scripting

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 usare in reti private con client ad-hoc.