Analisi di Bitcoin

Anonimato, Sicurezza e Sviluppi Futuri

Paoluzzi Matteo

Università degli Studi di Udine

Relatore:
Dott. Ivan Scagnetto

IV Sessione di Laurea AA 2012/2013, Aprile 2014

Di cosa si tratta

Una valuta elettronica basata su crittografia a chiave pubblica progettata per:

- Proteggere l'identità degli utenti sfruttando **indirizzi** anonimi.
- Essere indipendente da qualsiasi istituto di credito.
- Essere immune dal rischio di inflazione.
- Funzionare su base P2P in modo pubblico, sicuro e verificabile.

Indirizzi

L'anonimato dell'utente viene implementato tramite stringhe di testo note come indirizzi.

- Un indirizzo viene generato a partire da una coppia di chiavi pubbliche e private.
- Tutte le **transazioni** di BTC avvengono da e verso indirizzi, senza divulgare informazioni sull'identità delle parti coinvolte.
- Le chiavi di cifratura consentono di spendere il denaro ricevuto e impedire che il denaro inviato finisca ad un destinatario diverso da quello desiderato.
- Ogni utente è incoraggiato ad avere molteplici indirizzi, mantenendo sicure le porzioni private delle chiavi appositamente generate.

Transazioni

Contengono tutte le informazioni necessarie per effettuare un "trasferimento" di denaro.

- Sono identificate da un hash calcolato su un suo sottoinsieme di dati che ne cristallizzano le proprietà più rilevanti.
- Contengono molteplici sezioni di input e output costituite da script eseguibili che autorizzano la spesa e determinano l'invio del denaro:
  - L'input contiene un riferimento ad output di precedenti transazioni da cui prelevare denaro, e per ogni riferimento la chiave pubblica del creatore della transazione attuale e la relativa firma ECDSA che ne autorizzano il prelievo.
  - Ogni output contiene un ammontare in denaro e uno script con l'indirizzo del destinatario che autorizzerà future spese della transazione.
  - Se l'input è maggiore dell'output, il resto viene inviato ad un indirizzo scelto dal creatore della transazione.

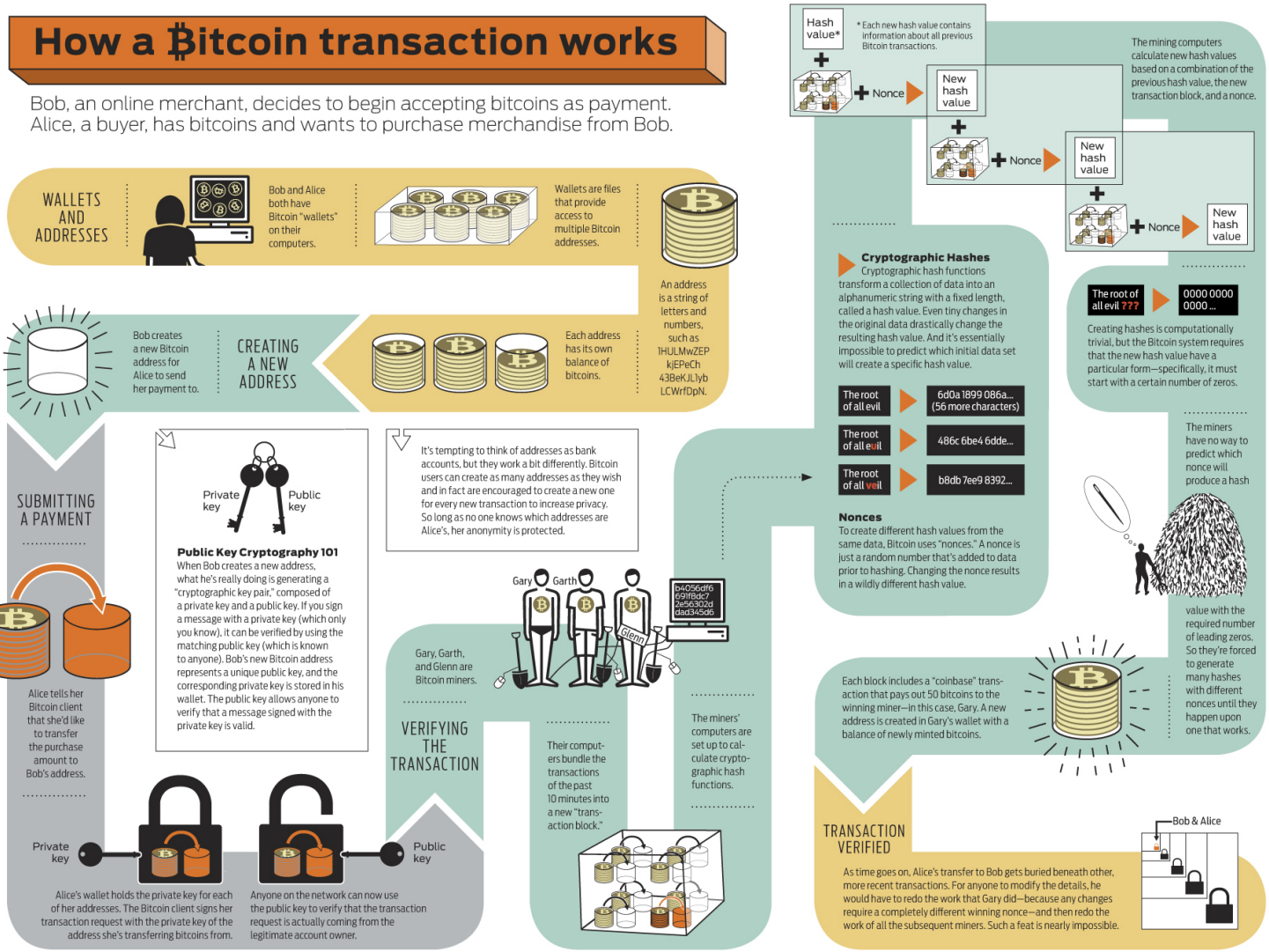
Blocchi

Le transazioni vengono raccolte in un blocco calcolando un hash il cui valore non deve superare un determinato target:

- Trovare tale hash è un lavoro computazionalmente molto difficile chiamato **mining** e viene mantenuto tale ridimensionando il target ogni 2016 blocchi in modo da generare in media un blocco ogni 10 minuti.
- Il nodo che trova il blocco viene premiato con una cifra fissa di BTC e con alcune tariffe prelevate dalle transazioni contenute nel blocco appena trovato e stabilite dal creatore delle transazioni in questione.

Dato che ogni blocco contiene l'hash del blocco precedente, nell'insieme formano una **blockchain** il cui scopo è fissare le transazioni nel tempo in modo che non possano essere arbitrariamente modificate, garantendo così la sicurezza della rete e il buon esito delle transazioni.

Infografica



Vulnerabilità: velocità di transazioni

- Un transazione non è confermata fintanto che non viene inserita in un blocco, il che richiede in media 10 minuti.
- Una transazione non confermata potrebbe non essere inserita nella blockchain e quindi risultare scartata.
- Un attacco doppia-spesa sfrutta questa debolezza per frodare un venditore poco accorto:

Vulnerabilità: velocità di transazioni

- Un transazione non è confermata fintanto che non viene inserita in un blocco, il che richiede in media 10 minuti.
- Una transazione non confermata potrebbe non essere inserita nella blockchain e quindi risultare scartata.
- Un attacco doppia-spesa sfrutta questa debolezza per frodare un venditore poco accorto:
  1. Si crea una transazione legittima e la si invia al commerciante.

Vulnerabilità: velocità di transazioni

- Un transazione non è confermata fintanto che non viene inserita in un blocco, il che richiede in media 10 minuti.
- Una transazione non confermata potrebbe non essere inserita nella blockchain e quindi risultare scartata.
- Un attacco doppia-spesa sfrutta questa debolezza per frodare un venditore poco accorto:
  1. Si crea una transazione legittima e la si invia al commerciante.
  2. Il commerciante si fida che la transazione vada bene e invia il prodotto all'attaccante.

Vulnerabilità: velocità di transazioni

- Un transazione non è confermata fintanto che non viene inserita in un blocco, il che richiede in media 10 minuti.
- Una transazione non confermata potrebbe non essere inserita nella blockchain e quindi risultare scartata.
- Un attacco doppia-spesa sfrutta questa debolezza per frodare un venditore poco accorto:
  1. Si crea una transazione legittima e la si invia al commerciante.
  2. Il commerciante si fida che la transazione vada bene e invia il prodotto all'attaccante.
  3. L'attaccante invia una seconda transazione che sovrascrive la prima inviando lo stesso denaro a se stesso, frodando il commerciante.

Vulnerabilità: velocità di transazioni

- Un transazione non è confermata fintanto che non viene inserita in un blocco, il che richiede in media 10 minuti.
- Una transazione non confermata potrebbe non essere inserita nella blockchain e quindi risultare scartata.
- Un attacco doppia-spesa sfrutta questa debolezza per frodare un venditore poco accorto:
  1. Si crea una transazione legittima e la si invia al commerciante.
  2. Il commerciante si fida che la transazione vada bene e invia il prodotto all'attaccante.
  3. L'attaccante invia una seconda transazione che sovrascrive la prima inviando lo stesso denaro a se stesso, frodando il commerciante.
  4. Se la seconda transazione viene inserita in un blocco prima della transazione legittima, l'attacco ha successo e l'attaccante ha ottenuto un bene senza pagarlo.

Vulnerabilità: velocità di transazioni

- Un transazione non è confermata fintanto che non viene inserita in un blocco, il che richiede in media 10 minuti.
- Una transazione non confermata potrebbe non essere inserita nella blockchain e quindi risultare scartata.
- Un attacco doppia-spesa sfrutta questa debolezza per frodare un venditore poco accorto:
  1. Si crea una transazione legittima e la si invia al commerciante.
  2. Il commerciante si fida che la transazione vada bene e invia il prodotto all'attaccante.
  3. L'attaccante invia una seconda transazione che sovrascrive la prima inviando lo stesso denaro a se stesso, frodando il commerciante.
  4. Se la seconda transazione viene inserita in un blocco prima della transazione legittima, l'attacco ha successo e l'attaccante ha ottenuto un bene senza pagarlo.

La prevenzione è sempre nelle mani dell'utente.

Vulnerabilità: potenza di calcolo

Se un utente riesce ad accumulare più potenza di calcolo di quella del resto della rete, potrebbe creare una nuova blockchain a sua discrezioni invalidando tutte le transazioni a partire da un momento a sua discrezione.

Vulnerabilità: potenza di calcolo

Se un utente riesce ad accumulare più potenza di calcolo di quella del resto della rete, potrebbe creare una nuova blockchain a sua discrezioni invalidando tutte le transazioni a partire da un momento a sua discrezione.

La difficoltà nel compiere tale operazione è elevata.

Vulnerabilità: potenza di calcolo

Se un utente riesce ad accumulare più potenza di calcolo di quella del resto della rete, potrebbe creare una nuova blockchain a sua discrezioni invalidando tutte le transazioni a partire da un momento a sua discrezione.

La difficoltà nel compiere tale operazione è elevata. Ma questo non vuol

dire che sia impossibile!

Privacy

Il sistema di indirizzi adottato è simile a quello dei conti bancari in Svizzera: numeri di conto non collegabili direttamente a persone.
Ma il sistema di cifratura a chiave pubblica permette di aggregare indirizzi appartenenti alla stessa persona:

- Una transazione contenente più indirizzi in input indica che tali indirizzi appartengono tutti al creatore della transazione stessa.
- Se una transazione contiene un output molto piccolo e destinato ad un indirizzo mai visto prima, probabilmente tale indirizzo è stato creato appositamente dal creatore della transazione per raccogliere il resto.

Creando un grafo delle transazioni pubblicamente disponibile e applicando le aggregazioni descritte, è possibile creare un secondo grafo approssimato rappresentante il flusso di monete tra utenti invece che tra indirizzi.
Unendo questi due grafi ad altre fonti esterne potrebbe essere possibile identificare effettivamente un utente e tracciarne le attività.

Esempio reale: un furto

Il 13 Giugno 2011 sembra sia avvenuto un furto di circa 25000 BTC.
Analizzando il flusso delle transazioni si è potuto osservare come il furto abbia coinvolto più di 34100 indirizzi, alcuni mai visti prima ed altri appartenenti a entità note come il gruppo hacker LulzSec (non associabile al furto) e il servizio MyBitcoin.
Sfruttando le tecniche descritte è stato possibile unificare più indirizzi diversi ad una stessa entità, dimostrando quindi come sia possibile minacciare la privacy di un utente aggregando le informazioni disponibili online e offline.

Seguire le transazioni