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

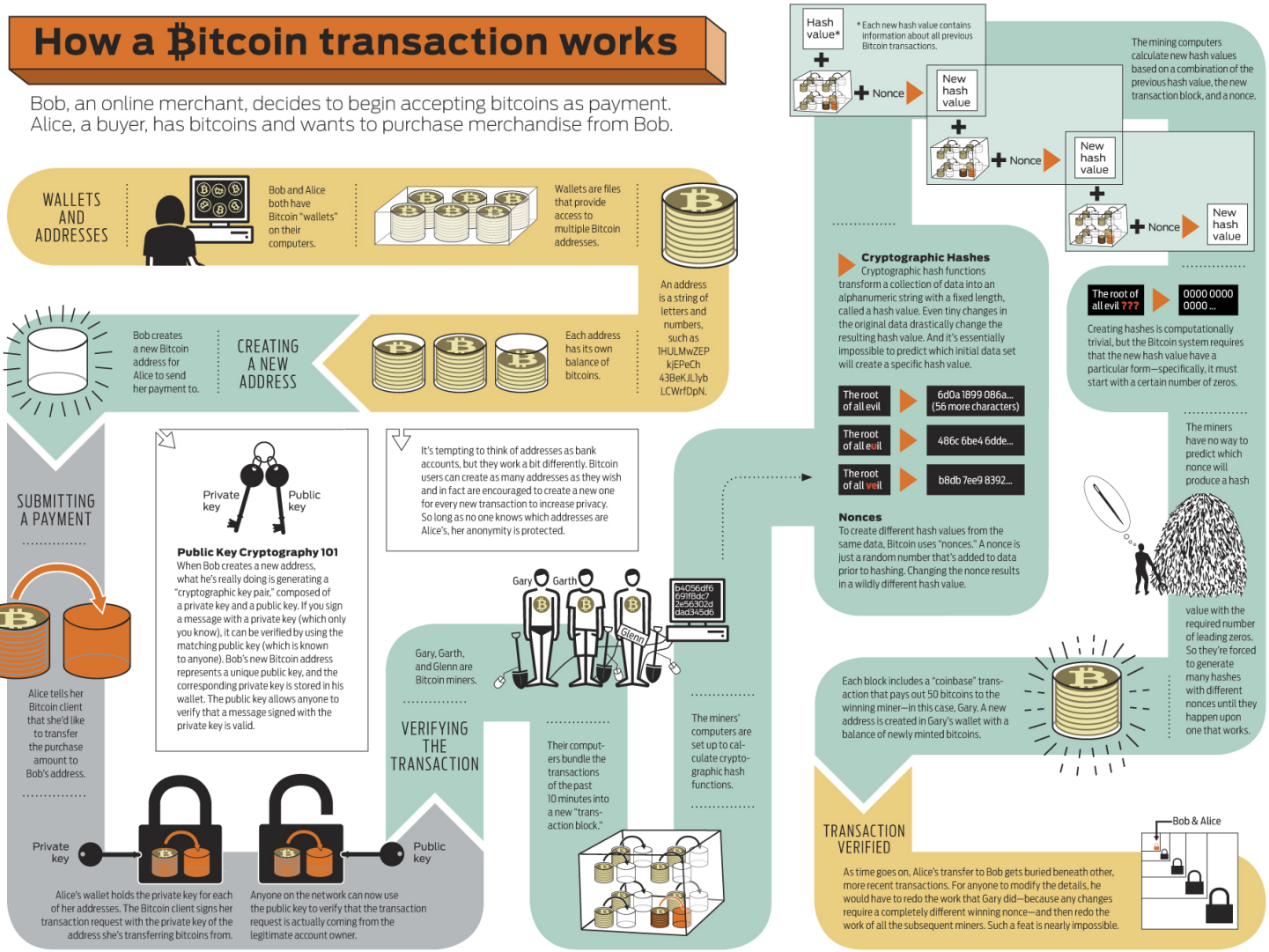
- L'input di una transazione può solo essere l'output di una precedente transazione.
- Non è possibile spendere denaro che non è stato inviato ad un indirizzo di cui non si possiede la chiave privata.
- Le transazioni sono bloccate nel tempo da un timestamp e da un hash che le identifica in modo permanente.
- 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.
  - La catena di blocchi usata per fissare tutte le transazioni prende il nome di Blockchain.

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!

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 ogni 210000 blocchi 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 ogni 210000 blocchi 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 ogni 210000 blocchi 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

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 che implementano situazioni diverse dal semplice pagamento.

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

Scripting

Il protocollo sfrutta un linguaggio di scripting che permette di verificare le transazioni ma anche di crearne alcune 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.

Deflazione

L'elevato valore tendenzialmente crescente di una singola BTC rende più attraente l'idea di accumularle invece che di spenderle. Questo è vero per almeno il 55% delle BTC prodotte. L'accumulazione di BTC provoca la seguente catena di eventi:

1. Meno transazioni.

Deflazione

L'elevato valore tendenzialmente crescente di una singola BTC rende più attraente l'idea di accumularle invece che di spenderle. Questo è vero per almeno il 55% delle BTC prodotte. L'accumulazione di BTC provoca la seguente catena di eventi:

1. Meno transazioni.
2. Meno blocchi nell'unità di tempo.

Deflazione

L'elevato valore tendenzialmente crescente di una singola BTC rende più attraente l'idea di accumularle invece che di spenderle. Questo è vero per almeno il 55% delle BTC prodotte. L'accumulazione di BTC provoca la seguente catena di eventi:

1. Meno transazioni.
2. Meno blocchi nell'unità di tempo.
3. Meno nuove monete.

Deflazione

L'elevato valore tendenzialmente crescente di una singola BTC rende più attraente l'idea di accumularle invece che di spenderle. Questo è vero per almeno il 55% delle BTC prodotte. L'accumulazione di BTC provoca la seguente catena di eventi:

1. Meno transazioni.
2. Meno blocchi nell'unità di tempo.
3. Meno nuove monete.
4. Meno motivazione a diventare miner.

Deflazione

L'elevato valore tendenzialmente crescente di una singola BTC rende più attraente l'idea di accumularle invece che di spenderle. Questo è vero per almeno il 55% delle BTC prodotte. L'accumulazione di BTC provoca la seguente catena di eventi:

1. Meno transazioni.
2. Meno blocchi nell'unità di tempo.
3. Meno nuove monete.
4. Meno motivazione a diventare miner.
5. Meno utenti che verificano la correttezza delle transazioni.

Deflazione

L'elevato valore tendenzialmente crescente di una singola BTC rende più attraente l'idea di accumularle invece che di spenderle. Questo è vero per almeno il 55% delle BTC prodotte. L'accumulazione di BTC provoca la seguente catena di eventi:

1. Meno transazioni.
2. Meno blocchi nell'unità di tempo.
3. Meno nuove monete.
4. Meno motivazione a diventare miner.
5. Meno utenti che verificano la correttezza delle transazioni.
6. Maggiore debolezza ai devastanti attacchi basati su potenza di calcolo e verifiche di transazioni.

Deflazione

L'elevato valore tendenzialmente crescente di una singola BTC rende più attraente l'idea di accumularle invece che di spenderle. Questo è vero per almeno il 55% delle BTC prodotte. L'accumulazione di BTC provoca la seguente catena di eventi:

1. Meno transazioni.
2. Meno blocchi nell'unità di tempo.
3. Meno nuove monete.
4. Meno motivazione a diventare miner.
5. Meno utenti che verificano la correttezza delle transazioni.
6. Maggiore debolezza ai devastanti attacchi basati su potenza di calcolo e verifiche di transazioni.

Bitcoin è fortemente dipendente da una comunità attiva e da un costante fluire della moneta: in mancanza di ciò, perde il suo valore avviando potenzialmente una spirale deflazionistica.

Questioni Legali

Data la sua natura volutamente ambigua, dal punto di vista legale ancora molto poco è stato definito per Bitcoin, e solo in ambiti limitati.

Questioni Legali

Data la sua natura volutamente ambigua, dal punto di vista legale ancora molto poco è stato definito per Bitcoin, e solo in ambiti limitati.

- Le Bitcoin sono una forma di valuta?

Questioni Legali

Data la sua natura volutamente ambigua, dal punto di vista legale ancora molto poco è stato definito per Bitcoin, e solo in ambiti limitati.

- Le Bitcoin sono una forma di valuta?
- Come verifico la proprietà di un oggetto acquistato con BTC in mancaza di ricevuta?

Questioni Legali

Data la sua natura volutamente ambigua, dal punto di vista legale ancora molto poco è stato definito per Bitcoin, e solo in ambiti limitati.

- Le Bitcoin sono una forma di valuta?
- Come verifico la proprietà di un oggetto acquistato con BTC in mancaza di ricevuta?
- Sotto quale giurisdizione ricadono le BTC?

Questioni Legali

Data la sua natura volutamente ambigua, dal punto di vista legale ancora molto poco è stato definito per Bitcoin, e solo in ambiti limitati.

- Le Bitcoin sono una forma di valuta?
- Come verifico la proprietà di un oggetto acquistato con BTC in mancaza di ricevuta?
- Sotto quale giurisdizione ricadono le BTC?
- Come risolvo il problema del riciclaggio di denaro?

Questioni Legali

Data la sua natura volutamente ambigua, dal punto di vista legale ancora molto poco è stato definito per Bitcoin, e solo in ambiti limitati.

- Le Bitcoin sono una forma di valuta?
- Come verifico la proprietà di un oggetto acquistato con BTC in mancaza di ricevuta?
- Sotto quale giurisdizione ricadono le BTC?
- Come risolvo il problema del riciclaggio di denaro?
- Sono un bene da tutelare?

Questioni Legali

Data la sua natura volutamente ambigua, dal punto di vista legale ancora molto poco è stato definito per Bitcoin, e solo in ambiti limitati.

- Le Bitcoin sono una forma di valuta?
- Come verifico la proprietà di un oggetto acquistato con BTC in mancaza di ricevuta?
- Sotto quale giurisdizione ricadono le BTC?
- Come risolvo il problema del riciclaggio di denaro?
- Sono un bene da tutelare?
  - Come identifico un eventuale ladro se è tutto anonimo?

Questioni Legali

Data la sua natura volutamente ambigua, dal punto di vista legale ancora molto poco è stato definito per Bitcoin, e solo in ambiti limitati.

- Le Bitcoin sono una forma di valuta?
- Come verifico la proprietà di un oggetto acquistato con BTC in mancaza di ricevuta?
- Sotto quale giurisdizione ricadono le BTC?
- Come risolvo il problema del riciclaggio di denaro?
- Sono un bene da tutelare?
  - Come identifico un eventuale ladro se è tutto anonimo?
  - Come calcolo le tasse, ammesso che debba calcolarle?

Questioni Legali

Data la sua natura volutamente ambigua, dal punto di vista legale ancora molto poco è stato definito per Bitcoin, e solo in ambiti limitati.

- Le Bitcoin sono una forma di valuta?
- Come verifico la proprietà di un oggetto acquistato con BTC in mancaza di ricevuta?
- Sotto quale giurisdizione ricadono le BTC?
- Come risolvo il problema del riciclaggio di denaro?
- Sono un bene da tutelare?
  - Come identifico un eventuale ladro se è tutto anonimo?
  - Come calcolo le tasse, ammesso che debba calcolarle?
  - Come gestisco le eredità in caso di portafogli cifrati e mancanza di chiave privata?

Litecoin ed altre

Creata nel 2011, è una variante di Bitcoin che sta avendo notevole diffusione:

- Un blocco ogni 2.5 minuti.
- 84 milioni di LTC.
- Ricompensa dimezzata ogni 840000 blocchi.

Esistono moltre altre monete elettroniche...

Litecoin ed altre

Creata nel 2011, è una variante di Bitcoin che sta avendo notevole diffusione:

- Un blocco ogni 2.5 minuti.
- 84 milioni di LTC.
- Ricompensa dimezzata ogni 840000 blocchi.

Esistono moltre altre monete elettroniche...

- ... alcune diffuse come Namecoin, PPCoin e Mastercoin ...

Litecoin ed altre

Creata nel 2011, è una variante di Bitcoin che sta avendo notevole diffusione:

- Un blocco ogni 2.5 minuti.
- 84 milioni di LTC.
- Ricompensa dimezzata ogni 840000 blocchi.

Esistono moltre altre monete elettroniche...

- ... alcune diffuse come Namecoin, PPCoin e Mastercoin ...
- ... altre meno note come Megacoin e Anoncoin ...

Litecoin ed altre

Creata nel 2011, è una variante di Bitcoin che sta avendo notevole diffusione:

- Un blocco ogni 2.5 minuti.
- 84 milioni di LTC.
- Ricompensa dimezzata ogni 840000 blocchi.

Esistono moltre altre monete elettroniche...

- ... alcune diffuse come Namecoin, PPCoin e Mastercoin ...
- ... altre meno note come Megacoin e Anoncoin ...
- ... e altre ancora umoristiche create apposta per farsi quattro risate, come Dogecoin e Coinye ...

Litecoin ed altre

Creata nel 2011, è una variante di Bitcoin che sta avendo notevole diffusione:

- Un blocco ogni 2.5 minuti.
- 84 milioni di LTC.
- Ricompensa dimezzata ogni 840000 blocchi.

Esistono moltre altre monete elettroniche...

- ... alcune diffuse come Namecoin, PPCoin e Mastercoin ...
- ... altre meno note come Megacoin e Anoncoin ...
- ... e altre ancora umoristiche create apposta per farsi quattro risate, come Dogecoin e Coinye ...

... Ma tutte basate sugli stessi principi di decentralizzazione e anonimato e tutte perfettamente "funzionanti".