Sicurezza dei sistemi e delle reti[1]

Mattia Monga

Dip. di Informatica
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2014/15

Lezione XXII: Reti p2p e privacy

Reti p2p

peer-to-peer

Un gruppo di nodi che opera sia come client che come server (ogni nodo è in grado di svolgere le stesse operazioni)

Napster-like un server centrale conserva un indice dei servizi

Gnutella-like anche l'indice è distribuito fra i peer (eccetto un elenco di bootstrapping)

Privacy delle operazioni

- L'indice (chi fornisce che cosa) è sostanzialmente pubblico
- La fruizione del servizio generalmente è HTTP (vedi privacy web)
- In alcuni casi (p.es. BitTorrent) i metadati contengono molte informazioni personali
- Potrebbero essere necessarie anche operazioni in cui non si è direttamente interessati (In Svizzera p.es., dove è permesso il download di materiale protetto da copyright, è vietato condividerlo)

Freenet

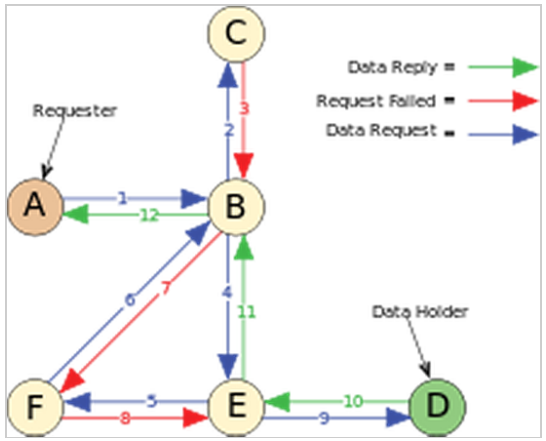
Un tentativo di realizzare un sistema di pubblicazione di contenuti **resistente alle censure**

- peer-to-peer e completamente decentralizzato
- i dati vengono criptati e replicati su molti nodi
- diventa estremamente difficile sapere chi ha che cosa
- i singoli nodi non hanno modo di sapere cosa mettono a disposizione

Architettura di Freenet

- Ogni contenuto è identificato solo da un hash SHA-256 (non c'è supporto diretto alle ricerche)
- Ogni nodo "conosce" solo un numero ristretto di altri nodi che può raggiungere direttamente
- I contenuti vengono passati ai vicini (e posti in una cache locale), senza sapere se è la destinazione finale
- key-based routing euristico

Freenet routing



Freenet

- Un nodo inserisce un file *nella rete*: a quel punto può anche disconnettersi, perché il file viene spezzato e conservato fra i peer attivi
- I contenuti piú richiesti vengono inseriti piú frequentemente nelle cache (mentre quelli non richiesti tendono a sparire)
- Opennet (chiunque può connettersi) e Darknet (rete fra trusted node con topologia manuale)

Freenet

Lettura obbligatoria:
Clarke, Ian, et al. "Protecting free expression online with Freenet." Internet Computing, IEEE 6.1 (2002): 40-49.

I2P

Invisible Internet Project (I2P) è una rete per servizi anonimi (con possibilità di gateway verso l'internet tradizionale).

- Inizio nel 2003, parziale spin-off di Freenet e Invisible IRC
- Si tratta di una "overlay network": la comunicazione avviene tramite *I2Ptunnel* (equivalenti ai circuiti TOR)
- I tunnel vengono cambiati ogni dieci minuti
- Le applicazioni per usare I2P devono essere riscritte, utilizzando un'apposita API (Simple Anonymous Messaging oppure Basic Open Bridge)

eepsite

I siti web di I2P vengono chiamati eepsite e sono identificate da chiavi crittografiche (anziché numeri IP): esiste anche una forma simbolica (dominio `.i2p`).

- un *eeproxy* è necessario per collegarsi agli *eepsite* con un normale browser
- la topologia della rete e la risoluzione dei nomi simbolici avviene tramite un netDB: una base di dati distribuita gestita con modalità DHT simili a quelle viste per Freenet

Obiettivi e limiti

I2P è complementare a TOR (che prevede una modalità simile tramite gli "hidden service"): l'obiettivo è creare una rete alternativa il piú possibile anonima.

- Sono noti attacchi "Sybil" che permettono di controllare il netDB controllando una porzione di nodi (2%-20%)
- È molto facile da usare, ma non ha la massa critica (e quindi il suo potenziale di anonimato) di TOR

Bitcoin

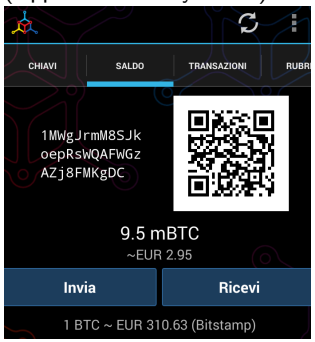
Si tratta di una moneta scritturale.
L'obiettivo del progettista (Satoshi Nakamoto, 2008):

> Bitcoin
> Due soggetti possono **direttamente** concordare una transazione, *senza la necessità di una terza parte fidata.*

- La transazione non può essere annullata/ripudiata
- Il sistema funziona correttamente nell'ipotesi che gli "onesti" controllino collettivamente piú potenza di calcolo dei potenziali disonesti.

Come si usa

(App Android: Mycelium)



`https://github.com/mycelium-com/wallet`

1. Serve un indirizzo (un identificatore di una coppia di chiavi crittografiche: può essere generato autonomamente)
2. Servono **bitcoin**, ottenibili tramite:
   - beni, servizi, altra moneta
   - "mining": produzione di nuovi bitcoin usando potenza computazionale
3. Si indica l'indirizzo di un destinatario
4. Eventualmente proponendo un premio per la chi collaborerà alla garanzia della transazione (transaction fee)
5. Si invia la transazione che verrà validata in una **decina di minuti**

Come fa a funzionare

Bitcoin stabilisce un protocollo per mantenere un "log" distribuito di tutte le transazioni, in modo che sia possibile sapere se lo stato di ogni "moneta", garantendo che non venga **spesa piú volte** simultaneamente.
Le scritture contabili sono mantenute coerenti **senza un'autorità centrale:**

- Crittografia asimmetrica (firme digitali)
- Catene di hash-crittografici
- Timestamp garantiti da computazioni onerose
- Pubblicità totale (sincronizzata tramite bittorrent)

Transazioni

Un transazione è un messaggio che dice:

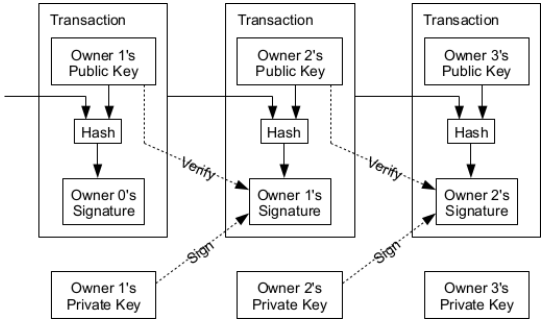
- Il soggetto A cede x bitcoin
- Il soggetto B riceve y bitcoin
- f bitcoin servono come premio per chi collabora alla validazione della transazione (*transaction fee*)

Naturalmente: $x = y + f$

Transazioni firmate

Ogni soggetto ha una coppia di chiavi asimmetriche: una (**privata**) serve per garantire l'autenticità (firma), l'altra (**pubblica**) per verificare le firme.

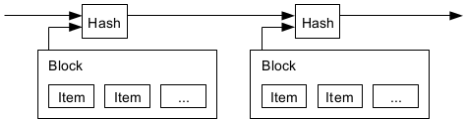
Owner 1 $\rightsquigarrow$ Owner 2



Hash chain

Ogni transazione (in realtà un blocco contiene generalmente molte transazioni) è collegata a quelle precedente perché include uno **hash** (256 bit che "riassumono" l'informazione in una maniera difficile da falsificare) di quelle precedenti: P.es.:

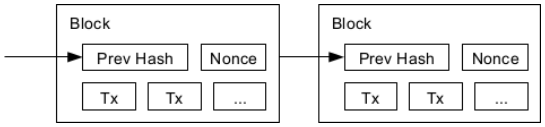
Hash SHA256 della Divina Commedia curata da G. Petrocchi $\rightarrow$
`5b57a696ac3bdb48cb09b1d0998f9d582660f5cbd9463e2ef5d5ea4e0f6d5671`
Al momento non si conosce un metodo per trovare un'altra stringa di caratteri con lo stesso hash piú efficiente del provare a caso.



Per calcolarlo devono esistere gli hash precedenti: se H_0 viene pubblicato il 1 gennaio 2014, la transazione che contiene lo hash di H_0 deve essere temporalmente successiva.

Accordo distribuito

Ma come si fa a concordare una singola storia? Un'unica block chain?
Il meccanismo con cui si risolve questo problema (in generale insolubile!) è l'introduzione di **proof of work**: non basta calcolare uno hash, lo si vuole anche "particolare":



Bisogna trovare un 'nonce' che dia luogo a uno hash che inizia con un certo numero (parametro di difficoltà) di zeri.
`000000000000000001237535293c120a0b9d4d4ac7bac9911c48357bf0f694d26`
Se SHA256 mantiene le sue promesse, non c'è modo migliore che quello di provare a caso... Siccome però ci provano in molti, il tempo in media col quale lo si trova è 10 minuti.

Bitcoin miners

Ma perché dovrebbero provarci in molti?

Perché c'è un **premio** per chi ci riesce: attualmente 25BTC, dimezzato circa ogni 4 anni.
Chi riesce a trovare un nonce che dà luogo a uno hash opportuno può intestarsi una transazione da 25BTC piú i transaction fee di tutte le transazioni nel blocco.
Nel caso (abbastanza improbabile) che ci siano piú blocchi validi, si prende il ramo con il maggior sforzo computazionale (la catena piú lunga).

Avendo sufficiente potenza computazionale è possibile accreditare transazioni false, ma l'ipotesi è che: (1) gli "onesti" siano computazionalmente piú potenti; (2) "conviene" usare la computazione per ottenere i premi di mining.

Il protocollo

1. Firmo una transazione e la annuncio *broadcast*
2. Ogni nodo disponibile al mining colleziona gli annunci in un blocco
3. Ogni miner cerca un nonce per la *proof of work*
4. Chi trova la *proof of work* la annuncia broadcast
5. L'annuncio del blocco validato viene confermato e la transazione può essere considerata **genuina**.

Riassumendo

- L'anonimato non è un obiettivo di progetto: anche se le transazioni avvengono fra **pseudonimi**
- Il numero di bitcoin è limitato ($21 \cdot 10^6$ frazionabili fino a 10^{-8})
- La difficoltà di mining è un parametro del sistema: il tasso di creazione di moneta può essere controllato (fine prevista 2140).
- Le transazioni sono irreversibili: si tutela il venditore, ma non il compratore (il contrario di quanto dovrebbe avvenire con le carte di credito...)

"È virtuale".

da Internazionale 1038

Riferimenti

- Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008
- Khan Academy: `https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-what-is-it`
- Esplorare la block-chain: `http://blockexplorer.com`
- Conviene il mining: `http://tpbitcalc.appspot.com/`