

UNIVERSITÀ DEGLI STUDI DI UDINE

Facoltà di Scienze Matematiche, Fisiche e Naturali

Corso di Laurea Triennale in Informatica

Tesi di Laurea

BITCOIN
MONETA ELETTRONICA
PEER-TO-PEER

./img/uniud_lite-eps converted to .pdf

Relatore:
Prof. IVAN SCAGNETTO

Laureando:
MATTEO PAOLUZZI

ANNO ACCADEMICO 2012-2013

Ai miei genitori
per non avermi tagliato i viveri

Sommario

Sommario della tesi in italiano

Abstract

Sommario della tesi in inglese

Indice

1	Introduzione	1
1.1	Distribuzione File	1
1.1.1	Scalabilità	1
1.2	Localizzazione dei contenuti	2
1.2.1	Directory centralizzata	2
	Bibliografia	3

Capitolo 1

Introduzione

P2P come alternativa a client-server puro Esempio di una ricerca MP3 [8] Chiarire come ogni peer è contemporaneamente sia un client che un server, in tal senso il paradigma è sempre client-server: esempio: se scarico via http, ogni peer è sia un client web che un web server temporaneo (temporaneo perché IP non è fisso).

1.1 Distribuzione File

Ciascun peer distribuisce la quantità di contenuti in suo possesso mentre scarica da altri peer quello che gli manca

1.1.1 Scalabilità

u_s frequenza di upload verso il server

u_i frequenza di upload dell' i -esimo peer

d_i frequenza di download dell' i -esimo peer

F dimensione in bit del file da distribuire

N numero di peer che vuole una copia del file

D_{cs} tempo di distribuzione del file per l'architettura client-server

Implicazione: condizioni ottimali di distribuzione (rete dedicata)

Client-Server

Osservazioni:

- Il server deve trasmettere il file a N peer, quindi NF bit. Data la frequenza di upload u_s , il tempo per distribuire il file deve essere almeno NF/u_s .

-
- sia $d_{min} = \min\{d_1, d_p, \dots, d_N\}$ la frequenza di download del peer con il valore più basso. Tale peer riceverà il file in almeno F/d_{min} secondi, che è quindi il tempo minimo di distribuzione.

Da cui

$$D_{cs} \geq \max \left\{ \frac{NF}{u_s}, \frac{F}{d_{min}} \right\}$$

Questo è il limite inferiore al tempo di distribuzione minimo per l'architettura client-server. Trattiamo il caso ottimo e consideriamolo come il tempo di distribuzione effettivo, ovvero:

$$D_{cs} = \max \left\{ \frac{NF}{u_s}, \frac{F}{d_{min}} \right\} \quad (1.1)$$

1.2 Localizzazione dei contenuti

1.2.1 Directory centralizzata

Si usa un servizio centrale per fornire un servizio di directory, che i peer contattano per sapere quali peer hanno quali file e per rendere disponibili agli altri peer i propri file. Il server usa una connessione TCP permanente con ogni peer o invia pacchetti per sapere quando questo va offline

Svantaggi

Unico punto di rottura

Collo di bottiglia delle prestazioni

Violazione del copyright

Bibliografia

- [1] *Bitcoin Wiki*. <https://en.bitcoin.it/wiki/>.
- [2] Androulaki, Elli, Ghassan Karame, Marc Roeschlin, Tobias Scherer e Srdjan Capkun: *Evaluating User Privacy in Bitcoin*. Cryptology ePrint Archive, Report 2012/596, 2012. <http://eprint.iacr.org/2012/596.pdf>.
- [3] Babaioff, Moshe, Shoham Dobzinski, Sigal Oren e Aviv Zohar: *On bitcoin and red balloons*. Nel *Proceedings of the 13th ACM Conference on Electronic Commerce*, EC '12, pagine 56–73, New York, NY, USA, 2012. ACM, ISBN 978-1-4503-1415-2. <http://doi.acm.org/10.1145/2229012.2229022>, Disponibile in download gratuito all'indirizzo <http://arxiv.org/pdf/1111.2626.pdf>.
- [4] Barber, Simon, Xavier Boyen, Elaine Shi e Ersin Uzun: *Bitter to Better - How to Make Bitcoin a Better Currency*. Nel Keromytis, AngelosD. (curatore): *Financial Cryptography and Data Security*, volume 7397 della serie *Lecture Notes in Computer Science*, pagine 399–414. Springer Berlin Heidelberg, 2012, ISBN 978-3-642-32945-6. http://dx.doi.org/10.1007/978-3-642-32946-3_29, Disponibile in download gratuito all'indirizzo <http://www.cs.stanford.edu/~xb/fc12/>.
- [5] Clark, Jeremy e Aleksander Essex: *CommitCoin: Carbon Dating Commitments with Bitcoin*. Nel Keromytis, AngelosD. (curatore): *Financial Cryptography and Data Security*, volume 7397 della serie *Lecture Notes in Computer Science*, pagine 390–398. Springer Berlin Heidelberg, 2012, ISBN 978-3-642-32945-6. http://dx.doi.org/10.1007/978-3-642-32946-3_28, Disponibile in download gratuito all'indirizzo <http://eprint.iacr.org/2011/677.pdf>.
- [6] Engle, Marling e Javed I. Khan: *Vulnerabilities of P2P Systems and a Critical Look at their Solution*. Rapporto Tecnico, Kent State University, Networking and Media Communications Research Laboratories, Department of Computer Science, 233 MSB, Kent, OH 44242, November 2006. <http://medianet.kent.edu/technicalreports.html>.

-
- [7] Kshemkalyani, Ajay D. e Mukesh Singhal: *Peer-to-peer computing and overlay graphs*, capitolo 18. Cambridge University Press, The Edinburgh Building, Cambridge CB2 8RU, UK, first edizione, 2008.
- [8] Kurose, James F. e Keith W. Ross: *Applicazioni peer-to-peer*, capitolo 2, pagine 131–144. Pearson Education, Addison-Wesley, quarta edizione, 2006.
- [9] Moore, Tyler e Nicolas Christin: *Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk*. Nel *Proceedings of Financial Cryptography 2013*, April 2013. <http://www.truststc.org/pubs/907.html>, Disponibile in download gratuito all'indirizzo <http://fc13.ifca.ai/proc/1-2.pdf>.
- [10] Nakamoto, Satoshi: *Bitcoin: A Peer-to-Peer Electronic Cash System*. satoshin@gmx.com. www.bitcoin.org.
- [11] Reid, Fergal e Martin Harrigan: *An Analysis of Anonymity in the Bitcoin System*. Nel Altshuler, Yaniv, Yuval Elovici, Armin B. Cremers, Nadav Aharoni e Alex Pentland (curatori): *Security and Privacy in Social Networks*, pagine 197–223. Springer New York, 2013, ISBN 978-1-4614-4138-0. http://dx.doi.org/10.1007/978-1-4614-4139-7_10, Disponibile in download gratuito all'indirizzo <http://arxiv.org/pdf/1107.4524.pdf>.
- [12] Ron, Dorit e Adi Shamir: *Quantitative Analysis of the Full Bitcoin Transaction Graph*. Cryptology ePrint Archive, Report 2012/584, 2012. <http://eprint.iacr.org/2012/584.pdf>.
- [13] Rosenfeld, Meni: *Analysis of Bitcoin Pooled Mining Reward Systems*. CoRR, abs/1112.4980, 2011. Disponibile in download gratuito all'indirizzo <http://arxiv.org/pdf/1112.4980v1.pdf>.
- [14] Schoeder, Detlef, Kai Fischbach e Christian Schmitt: *Core Concepts in Peer-to-Peer Networking*, capitolo 1. Idead Group Inc., 2005.