Distributed Marketplaces using P2P Networks and Public-Key Cryptography

Alessio Signorini
Dept. of Computer Science
University of Iowa, IA
alessio-signorini@uiowa.edu

Antonio Gulli
Ask.com R&D
Pisa, Italy
agulli@ask.com

Alberto Maria Segre
Dept. of Computer Science
University of Iowa, IA
alberto-segre@uiowa.edu

ABSTRACT

In the last years the Internet has deeply changed the business world and introduced many new opportunities. Every day billions of dollars are spent in on-line services and electronic transactions among users all over the world. Travel agencies, on-line shops and on-line banking are probably the most popular services nowadays, together with auction websites like Amazon or eBay. Unfortunately, maintaining such services with a centralized architecture is very difficult and expensive. In this paper we introduce a possible architecture for a decentralized marketplace like eBay, that uses an existing P2P networks and well-known cryptographic methods to support secure exchanges and user reputations tracking.

Categories and Subject Descriptors

H.3.4 [**Information Storage and Retrieval**]: Systems and Software—*Distributed systems*; K.4.4 [**Computers and Society**]: Electronic Commerce—*Distributed commercial transactions*

General Terms

Distributed Marketplaces

Keywords

Distributed Marketplaces, eBay, P2P Networks, Public-Key Cryptography

1. INTRODUCTION

The Internet revolution of the last 10 years has changed the ways we work, play, shop, communicate and interact with each other. The improvements in the reliability of the cell phones networks, the introduction of special Internet flat rates, and the multitude of wireless hot spots available today in every hotel, airport or local coffee shop allow people to stay connected from virtually everywhere in the world. Today, lots of companies heavily rely on computers networks, emails and online instant messages to run their businesses, speed up transactions, offer additional services, or expand their market contacting potential clients hundreds of miles away. Videogames, once played only by teenagers, captured the attention of users of all ages since they started to allow players to compete against each other online. Virtual communities like MySpace, Facebook, Wikipedia, Flickr or eBay are currently used by millions of users in their daily lives, to share knowledge and media, find information and products, or simply to communicate with each other.

Unfortunately, all of these useful services rely on some hardware to store their data and serve them to the users, and as should be obvious, services able to store millions of documents and provide access to many users simultaneously necessitate significant infrastructure. Those systems are usually composed by dozens of high-end servers connected together by a very fast network, that not only needs to be able to crunch data at high speed, but must also be completely reliable. Any failure of the system will directly translate in the loss of users and their trust, resulting in reduced company earnings. In the computer world ”fast” and ”reliable” are usually accompanied by ”expensive”: centralized systems are very expensive to buy and costly to maintain.

In this paper we present a simple but effective way to distribute the load of an auction service like eBay among computers of the users, using well-known cryptographic methods and existing P2P networks, to increase reliability and reduce the costs.

In Section 1 we give the basic the eBay system, Peer-to-Peer (P2P) networks and the cryptographic algorithms used in the paper. Details on the approach presented in this paper can be found in Section 2, while Section 3 tries to predict possible issues and propose some solutions. Section 4 introduces and compares related work.

1.1 eBay

Founded in 1995, eBay is without a doubt the most successful example of an online marketplace. It currently has more than 100 million users, including individual buyers and sellers, small businesses and even enterprises. As its own literature describes it ”From the buyer who shops on eBay for practical needs or for fun, to the seller who relies on eBay as a primary source of income, eBay is for its members a part of daily life”.

eBay has today 28 well-defined selling categories which range from Antiques to Cell Phones, from Dolls to Jewelry, from

INFOSCALE 2008, June 4-6, Vico Equense, Italy
Copyright © 2008 978-963-9799-28-8
DOI 10.4108/ICST.INFOSCALE2008.3572

Sports gadgets to Real Estate, and many more. Recently, to better handle the amount of traffic generated, eBay started a parallel marketplace for vehicles called Motor eBay[1] with a separate set of security features and buyer insurance.

Feedback Score The eBay system is based on a centralized database accessible through their website. Users are required to register before making any transaction, and the history of their behaviors are maintained on eBay's servers. The reputation of each user, called a Feedback Score[2], is given by comments and ratings other users leave after each concluded transaction. Positive ratings increase the Feedback Score, while negative ones decrease it. This score is presented to the users through colored stars next to usernames that represent users' trust and experience in the eBay Community. During recent years, eBay has introduced numerous features[3] to fight scams or illegal activities that populated its website: they applied data mining mechanisms to identify suspicious behaviors, introduced a browser toolbar to identify fake eBay websites, and added a type of insurance through its subsidiary PayPal[4].

Attacks Over the years eBay has been subject to numerous attacks, from simple email phishing, in which a malicious user sends emails to potential eBay users inviting them to login on a fake (but identical) eBay login page, to Denial Of Service (DoS) attacks, were the attackers use hundreds of computers to simultaneously request information from the eBay server paralyzing it with unexpected heavy traffic. While the purpose of this second attack is just to block the services offered, the goal of phishing emails and other types of direct attacks is to steal users information. Millions of personal profiles, including credit card numbers and other private information are saved on eBay servers, and a leak in the security of even one of these could expose an enormous amount of sensitive data.

1.2 Cryptography

Cryptography is the art of scrambling information in such a way that only who knows both the method and the secret can reconstruct the original information. While cryptographic methods became popular only in the last decades, it is a science that has been used [5] since the Roman Empire, where the first known cryptographic system has been attributed to emperor Julius Caesar.

Different cryptographic strategies have been developed [4] over the years. These methods can be mainly subdivided in two broad categories distinguished by the number of keys used: single key cryptography and double key cryptography. In *traditional (shared) key cryptography* a single method and key is known by both parties, which use it to encrypt and decrypt the information. In double key cryptography, often called *public (dual) key cryptography*, the cryptographic method (usually a one-way mathematical function) is known by both parties, but here each one has a pair of keys: a public key, which is distributed to the world, and a private key, kept secret. When Alice needs to send a message to Bob, she will encrypt the content using Bob's public key and then deliver the result. Upon receipt of an encrypted message, Bob will decode it using his private key and encrypt his reply using Alice's public key.

RSA The well-known and widely used public-key cryptography algorithm [16] was introduced in 1977 at MIT by Ron Rivest, Adi Shamir and Leonard Adleman. The algorithm is generally referred to as RSA, which are the initials of the authors' surnames. This method uses prime factorization as the trapdoor one-way function and the pair of keys is derived through a set of operations applied on the result of the multiplication of two large prime numbers. RSA keys are typically 1024-4096 bits long. In May 2005, Jens Franke et al. at the University of Bonn factored[5] an integer of 200 digits (663 bits) using the General Number Field Sieve (GNFS) algorithm [14] and a distributed parallel system. Most experts believe that 1024 bits keys will be breakable in the near term, while few consider breaking 4096 bits keys feasible in any foreseeable future.

Digital Signature A very nice benefit of modern double-key encryption schemes as the RSA algorithm is the possibility of unequivocally signing messages [2]. When Alice wants to make sure that the Bob will believe the messages are authentic, she just needs to encrypt them using her private key and send the encrypted message (the signature) along with the original one. Whoever wants to verify the authenticity of the messages can do so by decrypting the scrambled signature using Alice's public key to obtain the original message. Due to the complexity of encryption and decryption operations, and since messages can be quite long, the signature is usually applied on an encoding (hash) of the original message to reduce computational time, optimize bandwidth, and avoid distributing too many pairs of encrypted and original tex ts, which may give codebreakers some advantages.

Cryptographic signatures are widely used in electronic commerce [8] and authentication schemes, and with adequate key length they have yet to be proven breakable [17].

1.3 P2P Networks

When fast Internet connection (DSL, cable, fiber optics, ...) became widely available, people started using the Internet as a transfer medium with progressively more and more data and documents exchanged and distributed through the global network rather than using some other physical medium. With an exponential increase in the number of Internet users, popular file transfer services started to suffer: it was not possible, nor economical, to sustain such high traffic demand.

Peer-to-Peer (P2P) networks were created to provide an economical solution to these problems. Instead of distributing the data through a single server, they could be divided into small pieces and distributed on separate (and possibly geographically scattered) servers, in such a way that whoever was interested in them could retrieve each piece from the closest (and/or less loaded) server, thus reducing overall demand for bandwidth.

[1] http://www.motors.ebay.com/

[2] http://pages.ebay.com/services/forum/feedback.html

[3] http://pages.ebay.com/aboutebay/trustandsafety.html

[4] http://www.paypal.com

[5] http://www.crypto-world.com/announcements/rsa200.txt

Various strategies for P2P networks have been created and widely used. One of the first networks was Napster[6], which allowed users to share pictures, music, videos and software. Other important names on the P2P file-sharing scene are FastTrack, Gnutella, eDonkey and Bittorrent. Each protocol uses a different approach to peer connection, promotion, search distribution and message passing. Although there is no clear winner, the Gnutella network is the most popular P2P network on the Internet with more than 40% of market share according to a Digital Music News survey [11] of September 2007. Cheap Internet connections and the wide availability of P2P software clients, inspired communities of users to use these networks to exchange copyrighted material like movies and music tunes. However, P2P networks are also widely used for VoIP communications. The most popular example is Skype[7], which offers outstanding call quality for both audio and video over encrypted channels.

Dynamic Topology In a typical P2P network, the participants are called peers, and, depending on the network strategy, they may have different roles and importance. The topology of a P2P network is very dynamic since peers can join and leave at any moment. A new peer joins the network by opening a connection to an existing peer and communicates with the network through it. In some cases, peers are promoted or demoted depending upon the necessities of the network and the resources available. For example, a leaf node might become a hub (ultrapeer) which connects a large community of nodes, while an existing hub might be demoted to simple peer due to bandwidth restrictions.

Network Searches Searches are usually initiated by a peer and broadcasted/diffused on the network through other peers. Unfortunately, due to the large dimension and the irregular topology of the network, it might not always be possible for a search to reach all the peers connected. To reduce the amount of communications in the network, search messages are often broadcast only for a pre-determined number of hops after which they are dropped. In recent years, various techniques have been developed and implemented to improve the efficiency and effectiveness of searches in P2P networks. Examples of those methods are Query Routing Protocol [18] (QRP), which tries to optimize the search distribution by forwarding the messages only to the peers which most likely have the target information, and Dynamic Querying [7] (DQ), which terminates the search as soon as enough results have been acquired. Generally, unless the network is small and has a regular topology, no search is guaranteed to reach all the peers connected.

2. OUR APPROACH

The approach proposed in this paper is a simple but effective way to distribute the load of an auction service like eBay among the computers of the participants, using well-known cryptographic methods and existing P2P networks.

2.1 Basic Requirements

To allow the realization of the proposed Distributed Marketplace the following conditions have to be met: (1) a P2P network exists, (2) every user is able to connect to the network through some local client, and (3) participants are able to generate a pair of public and private keys that will be used to publish and sign their transactions.

Software Client To allow a wide use of the proposed method, an easy-to-use software client must be developed. Such a client must implement the necessary features to connect to the P2P network and perform the required operations. The software needs to create the necessary abstraction from the protocol implementation for the user, who should be able to seamlessly interact with the distributed marketplace as they currently do with eBay, without knowing the details of the network or the protocol. The minimum required capabilities for the client are: login and authenticate the user, publish auctions, search for auctions (either by title, description, username or public key of the auctioneer), and make offers. Additional features, such as the possibility of uploading pictures and automatic re-bidding, are also desirable in a more complete implementation.

Key Generation As previously stated, all the peers who desire to participate to the distributed marketplace must generate a pair of public and private keys using a known cryptographic algorithm as described in Section 1.2. While on eBay each participant is associated to a personalized username, the proposed distributed marketplace identifies each user using their public key. Usernames are supported by the system but only used for human reference. To avoid bottlenecks there is no central repository for usernames or public keys. Every action (auctions, bids, comments, ...) performed by a participant contains their username, their public key and their signature, thus keeping such information distributed on the network itself.

2.2 Joining the Marketplace

When a new participant (Alice) wants to join the distributed marketplace, she needs to connect to a peer (Bob) already in the P2P network. While connecting, Alice will submit to Bob her public key and prepare to answer a challenge. To verify the authenticity of Alice, Bob will encrypt some random text with the public key received and send it back to the peer. If Alice is really the owner of the given public key, she will just decrypt the message using her private key and provide the unencrypted text to Bob as proof. If Alice does not reply to the challenge, or the unencrypted text does not match, Bob will terminate the connection with the (fraudulent) peer.

Usernames If the distributed marketplace must provide support for unique usernames, it is necessary to perform some extra verification during the connection of new peers. When Alice connects to Bob she has two options: (1) generate a new never-before used username, or (2) use an existing one by providing some corroborating identification credentials. The username is sent to Bob along with the public key during the connection process. Once Bob has verified the ownership of the public key as described above, he will search the network looking for past transactions which include the given username. If no transaction is found, then the username is assumed to be new and Alice is allowed to join the network. On the other hand, if some past transaction is found, Bob will verify that the public key provided

[6] http://www.napster.com

[7] http://www.skype.com

by Alice and the one in the transaction match, refusing the connection otherwise.

Reputation While searching for Alice's transactions, either by username or public key, Bob will obtain a subset of the transactions concluded by Alice, together with the positive and negative opinions left about her by other parties. This information make it possible for Bob to assess Alice's reputation and perhaps refuse her request to join with the aim of keeping the marketplace free of bad auctioneers. As explained in Section 1.3, due to the topology of the network it is possible that Bob will not be able to find any past transactions for Alice, even when some exist on the network. Although such a situation is possible, since network users typically connect from the same locations to a restricted pool of local peers, the number of search hops allowed should be sufficient to find any evidence of a past user transaction. Every user has likely found and participated in auctions reachable by its local peers, and thus, the transaction performed should also always be reachable from those.

2.3 Publishing an Auction

When Alice is interested in selling an item she needs to publish an auction, demonstrating her will to sell the article to the user of the market who will offer the highest amount of money. In auction lingo, the user who hosts the auction is generally called the *auctioneer*, while the one who offers money is called *bidder*.

To publish the auction, Alice will prepare a document A' which includes at least: (1) the description of the item, (2) the starting price, (3) the current timestamp and (4) the ending time of the auction.

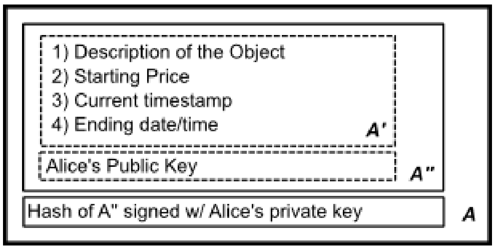

Figure 1: Alice's Auction Message (A)

As on eBay, additional details could be added to this document to help the bidders decide (images, videos, links, reviews of the object, payment and expedition conditions, etc.) as well as personal information about the auctioner (real name, username, etc.) or the physical location of the object (town, city, state, etc.).

Once ready, Alice will wrap A' and her public key together forming A'' and sign it using her private key. The resulting message A, graphically depicted in Figure 1, is what she will actually publish on the marketplace, sharing it on the P2P network through her client.

2.4 Looking for Auctions

Searches are performed by the participants of the marketplace through their software clients. As on eBay, different parameters can be used while looking for an existing auction, from simple keywords to be matched in the description of the object, to finer details like maximum price, expiration date, or object's location.

As explained in Section 2.1 such capabilities are independent from the underlying P2P network and must be offered and supported by the software clients. When a search is performed, a packet is distributed by the client of the user to the ones of the connected peers, which will keep forwarding it according to the network policies.

Due to the unstable topology of the network or its routing policies (refer to Section 1.3), search packets might not reach all the peers in the network, but with a sufficient number of peers connected and a large number of auctions offered this will rarely be a problem.

2.5 Placing an Offer

When a user finds an interesting object being auctioned, it will want to participate to the auction by making an offer. Offers in auction lingo are called *bids*, and they represent the price at which the bidder is willing to buy the auctioned item.

Assuming that Bob found Alice's auction A and is interested in making a bid, he will have to prepare a message B' containing at least: (1) the original auction message A, and (2) the amount of money offered. Bob will then wrap together the offer message B' and his public key, apply his digital signature and publish it on the market sharing the message B just created (Figure 2).

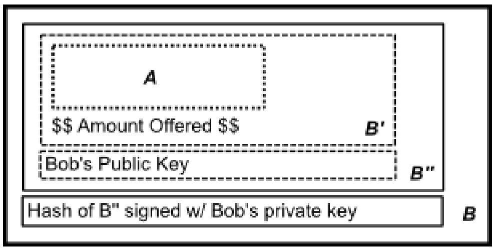

Figure 2: Bob's Offer Message (B)

Although shared on the network and visible to everybody, a bid is accepted and becomes official only when the auctioneer acknowledges its presence (either manually or automatically) as explained in Section 2.6. For this reason the bidder might want to push his offer directly to the auctioneer's client instead of waiting for it to be discovered through the auctioneer's periodic searches.

Auctions IDs Since the auction message A can be quite large (especially if contains pictures, videos, etc), Bob could use some identification mechanism to refer to the auction in his bids. To be usable, such an identification method must be known and shared among all the peers of the network and supported by their clients. Examples of valid methods are well-known hash functions such as MD5 [15] or SHA-1 [12], although collisions might rarely occur. If Bob uses an identifier in place of the original auction message, he might want to replicate the original auction message A and share it on the P2P network through his client, to ensure that his offer can be verified at any time (even when the auctioneer is not reachable).

2.6 Offer Receipts

Bob's bid becomes official and effective only when Alice discovers and acknowledges it. To do so, Alice needs to prepare an offer receipt C' which contains at least: (1) the bid B and (2) the current timestamp. Alice will then generate her signature on C' and wrap them up together sharing on the network the resulting message C.

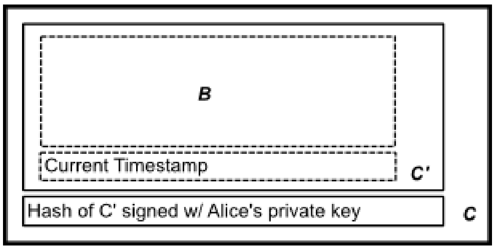

Figure 3: Alice's Offer Receipt for Bob (C)

This receipt will be seen by all the users that will look for the object of the auction, and can be used by Bob to leave a comment on Alice if something goes wrong with the auction (refer to Section 2.8). On the other hand, Alice might refuse to acknowledge Bob's offer and produce a receipt if Bob's reputation, assessed through a search as explained in Section 2.1, is too low.

Although not necessary, it might be useful for auctioners to keep track of the bidders' IP addresses. Doing so will allow the auctioner to: (1) send the receipt directly as confirmation, (2) report warnings and errors in case of problems, (3) communicate that their offer has been superceded by another bidder, and (4) announce the winner at the end of the auction. These functionalities are network agnostic and need to be implemented and supported in the software clients.

2.7 Announcing the Winner

At the end of each auction, the host (Alice) must refuse any further offer and announce the winner producing a closing receipt which she will then share on the network.

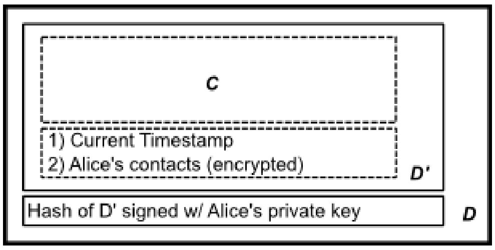
C
1) Current Timestamp
2) Alice's contacts (encrypted)
D'
Hash of D' signed w/ Alice's private key
D

Figure 4: Alice's Closing Message (D)

Assuming that Bob's offer B was the highest, Alice will prepare a closing receipt D' containing at least: (1) Bob's offer receipt C, (2) the current timestamp, and (3) her contact information encrypted with Bob's public key. Alice will then generate her signature for the message and share on the network the closing receipt D.

Bob will acquire the message (either directly from Alice or through a search on the network) and share a replica of it on the network through his client to ensure redundancy. This receipt will also allow Bob to leave a comment on Alice as explained in the following Section 2.8.

The closing receipt officially signals the end of the auction. Participants' software clients must recognize such messages and inform the users accordingly.

2.8 Concluding the Transaction

Once the auction is closed the winning bidder must contact the auctioner to arrange the last details for the sale. The bidder can decrypt the contact information of the auctioner from the closing message. Such information has been encrypted using the winner's public key and can thus be decrypted using its private key.

Bob will then decrypt Alice's contact information and privately agree with her on payment method and delivery. At the end of the exchange, whether successfull or not, they will both be able to leave a permanent comment on the other party.

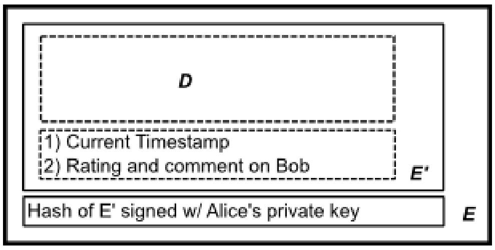
D
1) Current Timestamp
2) Rating and comment on Bob
E'
Hash of E' signed w/ Alice's private key
E

Figure 5: Alice's Comment on Bob (E)

If the transaction has been concluded successfully, Alice will create a comment message E' containing at least: (1) the closing receipt D, (2) the current timestamp, and (3) her rating and final comment of Bob. Alice will then attach to it her signature and share the resulting message E on the network as proof of positively concluded transaction. Similarly, Bob will create a comment message F' containing at least: (1) the closing receipt D, (2) the current timestamp, and (3) his rating and final comment of Alice. Bob will sign it and share the resulting message F on the network.

If the transaction has not been concluded successfully, either because one of the parties did not contact the other or because someone did not send its share of the trade, the other party can always use the last message received to release a comment. Alice can always use the closing receipt to leave a negative comment on Bob, and Bob can do the same for Alice. If Alice did not release a closing receipt, Bob can use her last offer receipt. Each message exchanged contains the original auction document, identifies both the users, and report the last transaction, permitting a good identification of the state of the transaction.

Comment Trading When a transaction concludes succesfully, both parties are encouraged to keep online their comments in exchange for the other party to do the same. On the other hand, when the transaction did not conclude succesfully, "revenge" will push each party to keep online any negative comments. The distribution of comments and ratings among the peers of the network avoids the necessity of a centralized database, but it also introduces some problems. Alice could, for example, change her comment about Bob at any time. While this problem surely exists, it is mainly a one-to-one problem and does not affect the all market: if user X changes its opinion about user Y and modifies all its comments on their past transactions, surely they should fear that Y might do the same to ruin their (X's) reputation. A comment released on a message different from the last one (i.e., the closing receipt) is always superexceded by comments released on successive messages. As a consequence, only a maximum of one message per party should be considered when computing the rating of each user.

3. LIMITATIONS

The distribution of auctions, bids, comments and ratings among the peers of the P2P network avoids the necessity of having a main database which could be the single point of failure in a centralized system. Unfortunately, the nature of a distributed solution introduces some other possible problems, caused by faulty networks, bad routing protocols, buggy clients or dishonest participants.

Faulty Networks While centralized systems like eBay spend millions of dollars each year to ensure that their redundant data-center will be online at all times, distributed systems solve this problem relying on redundancy of information and resources among the peers of the network. Whenever a peer is down, which might happen often since peers can connect and disconnect at any time, there likely is another peer with the same information ready to replace it. The method proposed in this paper mostly relies on the presence of just 2 copies of each message to be available in the network. While this is sufficient for most of the cases, there might be occasions in which the offline time of a critical peer could result in no information being found during a search and possibly create some adverse issues.

Bad Routing Protocols As briefly explained in Section 1.3, network searches are rarely complete. Due to the very unstable network topology is impossible to guarantee that a message sent by a peer will reach every other peer in the network in a finite amount of time. Trying to guarantee such a condition would result in intolerable overhead, making the quest very impractical and likely unfeasible. In addition, as mentioned in Section 2.2, with a sufficient number of local peers connected, no routing problem should ever arise, since most of the searches will likely return some results from close neighbors (perhaps a desiderable property given that the auctioned items have to be finally exchanged through snail-mail).

Buggy Clients Centralized systems rely on complex monolithic software, often developed in-house, which are tuned and optimized for the underlying hardware. Such closed solutions allow complete control of the software during its realization, deployment, any eventual updates. On the other hand, P2P networks are composed by a large number of different software clients and versions, which collaborate together thanks to the protocol imposed by the network itself. Unfortunately, protocol details are often unclear, and developers tend to introduce small differences in their software in order to improve the end user's satisfaction. Such small differences might generate an unfortunate and unpredicteable series of events that can sometimes result in the paralysis of parts of the network due to a faulty message being sent and broadcast by non compliant clients.

Dishonest Participants A dishonest peer could generate hundreds of key pairs on its own machine, create inexistent items and auctions, and release thousands of positive comments about a specific user heavily boosting its rating on the network. To avoid this problem, it is sufficient to temporarily link users and IP addresses, that is, only one user's comments are allowed from each IP that answers a search. Although possible, with the progressive retirement of P2P-open proxy servers and the imminent IPv6 deployment, the possibility of collisions among users who share the same IP address and have results for a given search is very low.

4. RELATED WORKS

In 1999 Dogac et. al. proposed in [3] a general architecture for distributed marketplaces. In the framework proposed agents use a centralized Intelligent Directory Service (IDS) to discover each other and open standards to expose their metadata (RDF), to describe (XML) the resources available, and to allow data access (DOM) to each other.

Kemper and Wiesner designed in [6] a web-based architecture for an electronic Business-to-Business distributed marketplace. Their approach is based on *HyperQueries* which are essentially query evaluation sub-plans sitting behind hyperlinks.

Both systems use a centralized database to "index" where the information are stored. Has in the eBay system this single point of failure might raise reliability issues. In addition, these systems were designed to support normal marketplaces, where the role of buyers and sellers is static and well defined, and have no specific support for auctions and bidding.

Among related work is necessary to mention the many different protocols for secure communications over insecure networks proposed in the last years. The *Needham-Schroeder protocol* [19] generates one-session keys between the two peers and uses them for encryption. It has two different variants: the first is based on symmetric encryption and is used as basis for the well-known Kerberos protocol [10], while the second is based on public-key cryptography and also provides mutual authentication. The fundamental principle of both variants is the *nonce* [8], a random token generated and exchange by peers signed with the public key. The original proposal has been proven to be vulnerable to classic man-in-the-middle attacks and a new version of the protocol, known as *Needham-Schroeder-Lowe* [9], has been proposed. The *Otway-Rees protocol* [13] and *Wide Mouth Frog protocol* [1] are other mechanisms used to estabilish secure communications but these have already been proven vulnerable to eavesdropping and replay attacks using one of many formalisms proposed to prove the robustness of security protocols [1].

[8] A one-time use (pseudo)-random number

5. CONCLUSIONS AND FUTURE WORK

The Internet has changed our means to communicate, work and shop. Every day billion of dollars are spent in online stores or marketplaces like eBay. Unfortunately, ensuring the reliability of such centralized systems is difficult and expensive. In this paper we proposed a protocol for a distributed marketplace that uses common and well-known technologies: Peer-to-Peer networks to connect the users and distribute the load, and Public-Key Cryptography to guarantee the authenticity of the transactions.

The method described does not have restrictive requirements and can be generalized to many other applications. In future works we plan to extend the protocol proposed adding support for different model of auctions (Dutch auction, Sealed-bid auction, ...) and increasing its strength.

6. ACKNOWLEDGMENTS

We would like to thank Michelle Capobianco for patiently error-proofing many versions of this paper. We would also like to thank Alessandro Arzilli and Naftaly Minsky for the useful discussions and numerous insights.

7. REFERENCES

[1] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. 426(1871), 1989.

[2] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.

[3] A. Doğaç, I. Durusoy, S. Arpınar, N. Tatbul, and P. Köksal. An electronic marketplace architecture. February 1999.

[4] O. Goldreich. *Foundations of Cryptography*, volume 1: Basic Tools. Cambridge University Press, 2001.

[5] D. Kahn. *The Codebreakers.* 1967.

[6] A. Kemper and C. Wiesner. Building scalable electronic market places using hyperquery-based distributed query processing. *World Wide Web*, 8(1):27–60, 2004.

[7] Limeware LLC. Dynamic querying. `http://wiki.limewire.org/index.php?title=Dynamic_Querying`.

[8] S. Mason. *Electronic Signatures in Law.* Tottel, 2nd edition, 2007.

[9] R. Needham and M. Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12):993–999, December 1978.

[10] C. Neuman and T. Tsó. Kerberos: An authentication service for computer networks. *IEEE Communications*, 32:33âĂŞ38, 1994.

[11] D. M. News. Digital media desktop report. `http://www.digitalmusicnews.com/report/desktopq407`, September 2007.

[12] N. I. of Standards and Technologies. *Secure Hash Standard, FIPS-180-1.* U.S. Department of Commerce, April 1995.

[13] D. Otway and O. Rees. *Operating Systems Review*, volume 21, chapter Efficient and timely mutual authentication, pages 8–10. 1987.

[14] C. Pomerance. A tale of two sieves. *Notices of the AMS*, 43(12):1473–1485, December 1996.

[15] R. Rivest. *The MD5 Message-Digest Algorithm.* Network Working Group, April 1992.

[16] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[17] S. Robinson. Still guarding secrets after years of attacks, rsa earns accolades for its founders. *SIAM News*, 36(5), 2003.

[18] C. Rohrs. Query routing for the gnutella network. `http://rfc-gnutella.sourceforge.net/src/qrp.html`, December 2001.

[19] M. Schroeder and R. Needham. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21:993–999, 1978.