An Exchange Protocol for Alternative Currencies

Yiyao Hao, Daniel M. Havey and David A. Turner
Department of Computer Science California State University,
San Bernardino San Bernardino, CA 92407
(hyy92507@yahoo.com, dhavey@yahoo.com, dturner@csusb.edu)

Abstract

Alternative currencies are currencies issued by individuals or entities other than national governments for the purpose of improving the economic well being of individuals by cultivating new trading relationships. We present a currency exchange protocol for use in alternative currency markets, such as those based on the Lightweight Currency Protocol, Local Exchange Transaction Systems, and Time Dollar Systems. In order to further enable the benefits derived from the use of alternative currencies, we propose the establishment of an exchange protocol that enables users to swap currencies. In this paper, we define the protocol we developed for this purpose, and describe the systems we prototyped to demonstrate the practicability of the currency exchange protocol.

Keywords: micro-currency, alternative currency, community currency, e-commerce.

1. Introduction

We refer to currencies based on the Lightweight Currency Protocol (LCP) as LCP currencies [1]. LCP is an account-based micro-payment system that operates over the Internet. Any person or organization is free to issue or publish an LCP currency. Issuers of LCP currencies imbue value into their currencies by backing them with a commodity, so that holders may redeem units of an issuer's currency for these commodities. Some of the commodities that have been considered as backing for LCP currencies are storage/bandwidth [2], spam reduced email [10, 11, 12], pdf document stores, video streaming, and content distribution.

The motivation for this research is to increase the value of using alternative currencies such as Local Exchange Time Systems (LETS), Time Dollars, and LCP currencies [3, 4, 5, 16, 17, 18]. To accomplish this purpose we have developed an Internet currency exchange protocol based on secure SOAP messaging. Our approach was to develop a prototype currency exchange server and prototype currency exchange client to test and refine our protocol. Throughout this paper we refer to the currency exchange as the X-Server. To test the server, we developed a currency exchange agent for use by managers of banks holding LCP currencies. The idea was to better understand how a bank would manage large reserves of multiple alternative currencies.

Currently there are more than 600 alternative currencies being used in Japan [3]. Although Japan has the largest number of alternative currencies in use other areas such as the United States, Europe, South America, and many other areas [16, 17, 18] have alternative currencies of their own. The use of these alternative currencies has been and continues to be strong because of their ability to cultivate new trading relationships. To further the reach of these community building currencies we propose the adoption of a standard currency exchange protocol that can be implemented by competing currency exchange service providers. The benefit of having an open and non-proprietary currency exchange protocol is that the market mechanism will help keep exchange fees to a minimum.

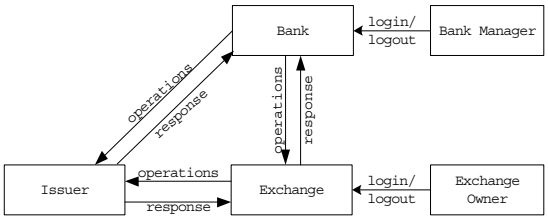

Figure 1: Communications Diagram for Currency Exchange Protocol

We used SOAP based web services in the development of our protocol because the availability of web service tools and frameworks should facilitate the adoption of the protocol among alternative currencies.

This paper is organized as follows. In section 2, we describe the exchange protocol and its implementation in the X-Server. In section 3, we present a typical example of the exchange protocol being used, and we explain our experiments with our prototype X-Server and prototype LCP bank system. Section 4 describes future work and extensions to accommodate other currencies.

2. Exchange Protocol Operations

Figure 1 illustrates the main components in this prototype. Bank managers log into the bank's system from an administrator interface. They can view the bank's currency reserves, and make decisions regarding which currencies to sell and which currencies to buy. In the bank's interface, they specify the exchange operations, which the bank system translates into SOAP messages and delivers to the exchange service. The exchange service processes the requests from banks and sends back responses to the banks to indicate whether the requests are successfully processed. The manager of the exchange service uses a browser to login to the administration interface of the exchange system. The exchange service manager can study customer transactions, manage the exchange's currency reserves, and set service fees. Whenever the operation is to transfer currencies between banks and the exchange service, the currency issuers will participate in the transaction.

The Internet Currency Exchange Protocol (ICEP) is a secure request/response protocol. All messages are delivered over HTTPS. The exchange server authenticates to the client using a certificate signed by a trusted authority. The client authenticates to the exchange certificate by including a user name and password within each request message except for the get commission operation.

For all operations invoked on it, the X server returns an XML response message containing the following attributes: a success code, an error message when the operation fails, a success message when the operation succeeds, and transaction fee details. The success code is a boolean value indicating the success or failure of an operation. The error message is a string indicating the reason if any for failure of an operation. The success message is an array of strings containing information related to the successful completion of the operation. The transaction fee details indicate the currency issuer and amount.

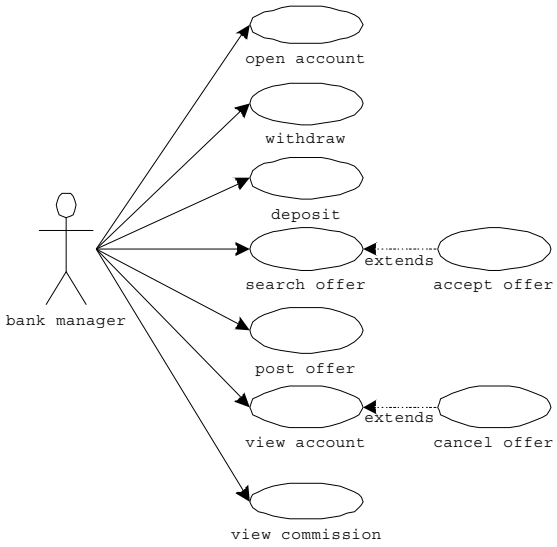

Figure 2: Bank Manager Operations

As can be seen from the use case diagram in Figure 2, the X server has nine operations. The two operations available to a user who wishes to make an exchange offer are: post offer, and cancel offer. The two operations available to a user who wishes to find and accept an offer are: search offer, and accept offer. Before users can invoke any of the above operations they need to establish an account and deposit funds. To do this there are two operations available: open account, and deposit. When a user wishes to access funds in her account there is one operation available: withdraw. Finally there are two operations available to view a user's balance and the X-Server's schedule of fees: get balance, and get commission. In the following subsections, we detail each operation in the currency exchange protocol.

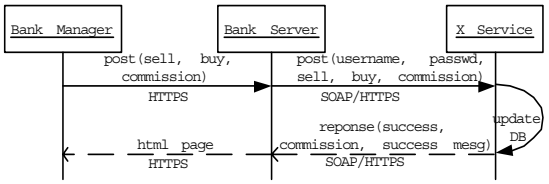

Figure 3: Post Offer Operation Sequence Diagram

The post offer operation

As illustrated in Figure 3, a bank manager offers to exchange some amount of a currency by sending a post offer request message to the X-Server. The post offer request message contains an attribute indicating the number of units in a currency that the seller is offering

to sell. The buy attribute specifies the number of units in a currency that the seller will accept to make the deal. The commission attribute specifies the number of units in a currency that the seller agrees to pay the exchange for posting her offer. The reason for this attribute is to ensure that the exchange client is aware of the current schedule of fees. If the fee schedule has changed then the X-Server will reject the operation with an appropriate error message, which allows the client's agent to either update its record of exchange fees and/or inform the user of the change.

When the X-Server processes and accepts the post offer operation, it subtracts the transaction fee from the users balance and makes the offer publicly available. The X-Server will return a response message indicating the success or failure of the post offer operation.

Search offers operation

In the search offers operation, the exchange client includes attributes within the request message similar to the post offer operation: sell, buy, and commission. The X-Server performs conditional select operations on its offer database to generate a list of offers that match the buyers search criteria. The X-server then returns this list of offers to the buyer in the response message.

Accept offer operation

The accept offer operation takes a list of ids for those offers the buyer wishes to accept. The X-Server performs the operation by adjusting its database to reflect the transfer of funds between the accounts of the buyer and sellers. There is no commission charged for accepting offers. The X-server then returns a response message to the buyer.

Cancel offer operation

The cancel offer operation specifies an offer to cancel by supplying the offer id. After authentication, the X-server cancels the offer, if it has not yet been accepted by some buyer. The X-server will then return a response message. Note that accepted offers are no longer pending, and thus the cancel offer operation will return an error response if invoked on an already accepted offer.

Operations that interact with currency issuers

The deposit, withdraw, and open account operations require a two-step interaction with a currency issuer. The X-Server prototype currently supports LCP currency issuers. LCP currency issuers also use SOAP over HTTPS in a request/response protocol. When an LCP currency user invokes a transfer funds request on a currency issuer the issuer returns a payment token if the operation succeeds. The sender of funds then gives the payment id to the recipient of the funds. The recipient of the funds then provides the payment id to the issuer in a verify operation in order to verify the payment. All three operations of deposit, withdraw, and open account require this two-step process with the currency issuer.

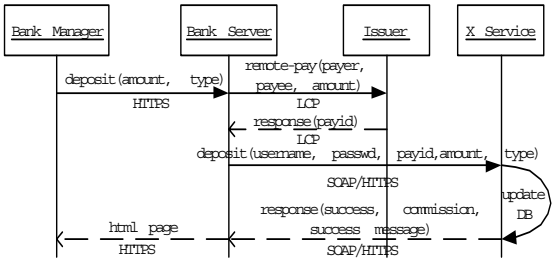

Figure 4: Deposit Operation Sequence Diagram

Deposit operation

As shown in Figure 4, the exchange client deposits currency units in its exchange account by transferring those units to the X-server's account with the currency issuer. The X-server then verifies the deposit by invoking a verify operation on the currency issuer. The X-Server then deducts a commission, if any, and adds the balance to the exchange client's account.

Withdraw operation

The exchange client withdraws funds for its use outside of the exchange by invoking the withdraw operation in which it specifies the number of units in a currency that it wishes to withdraw. When the X-Server receives a withdraw request, it checks that the client's balance in the given currency is sufficient. If the balance is sufficient, the X-Server then invokes a transfer funds operation on the currency issuer transferring funds from its account with the issuer to the client's account with the issuer. When this operation completes the X-Server receives a payment id from the issuer, which it returns to the client. The

client then verifies the operation with the currency issuer.

Open account operation

Figure 5 shows the sequence of interactions for an open account operation. To open an account the exchange client first transfers funds to the X-Server, which results in a payment token. The client then invokes an open account operation in which it specifies the payment token for the funds it just transferred to the X-Server. When the X-Server receives the open account request, it verifies the client's payment using the payment token. If the verification operation is successful, the X-Server establishes a balance for the client in the currency it has just received. The client's initial balance will equal the amount she transferred minus the commission charged by the X-Server for opening the account.

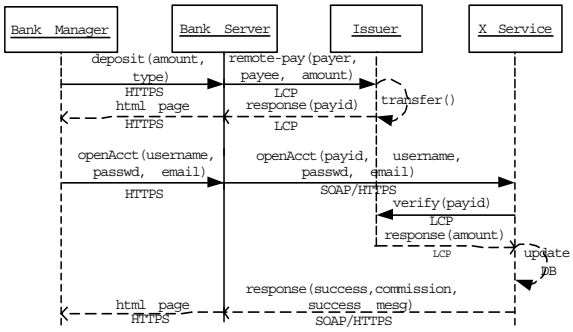

Figure 5: Open Account Operation

View account operation

In order to view information about its account or the schedule of fees, the exchange client uses two operations: get balance and get commission. These operations return the balance and the schedule of fees, respectively. The get commission operation is the only operation that does not require user authentication, and is the only operation that can be invoked over a non-secure channel. This is to allow prospective clients to view the schedule of fees before opening an account.

3. The exchange protocol market

In this section, we present a typical usage of the X-Server in an LCP currency exchange. Suppose Alice issues a currency that is backed by a storage/bandwidth service. That means holders of Alice's currency may redeem their currency for storage/bandwidth services provided by Alice. Suppose also that Bob issues a currency that is redeemable for viewing video content. Suppose that Claire uses payment based email as described in [11], and has received units of Bob's currency by collecting email delivery fees.

Alice desires to view one of Bob's videos, and therefore she needs Bob dollars. Claire desires to use Alice's storage service, and therefore she needs Alice dollars.

Alice opens an account at an X-Server by depositing 1000 units of her own currency, and posts an offer to exchange 100 Alice dollars for 200 Bob dollars. Claire opens an account at the same X-Server by depositing 1000 Bob dollars. Claire locates Alice's offer through a search operation, which she accepts by invoking an accept offer operation. The X-Server then reduces Alice's balance of Alice dollars by 101 units (assuming a 1 unit commission), and increases Alice's balance of Bob dollars by 200. Similarly, the X-Server reduces Claire's balance of Bob dollars by 202 units (assuming a 2 unit commission in Bob dollars), and increases Claire's balance of Alice dollars by 100 units. Alice and Claire are now able to withdraw the funds that they need to purchase their desired commodities.

In the above described scenario, the X-Server facilitated a trading relationship that would have been otherwise difficult or impossible. A large amount of such potential trading relationships exist across alternative currencies. Such exchange services are needed for alternative currencies to gain wider acceptance.

Another scenario that illustrates the use of our exchange protocol involves a community of Local Exchange Transaction System (LETS) users. In this scenario, Alice works at her local public library and gets paid in LETS dollars. Alice uses the LETS dollars she earned to pay Bob to mow her lawn. Bob in turn uses the X-Server to exchange the LETS dollars that he earned from Alice with Claire for Claire LCP dollars. Bob uses his Claire dollars to buy network resources and Claire uses her LETS dollars to pay her library fines.

4. Conclusion

The main goal of the X-Server project is to strengthen the viability of alternative currencies by providing a means for users of alternative currencies to reach wider markets by exchange their currencies. This is a need cited by Kytojoki in [9]. Currently, the

X-Server fulfills this role for LCP currencies. By extending the X-Server to operate with other currency systems, these exchanges of currencies could happen anywhere in the emerging world of alternative currencies.

5. References

[1] David A. Turner and Keith W. Ross. A Lightweight Currency Paradigm for the P2P Resource Market. *Seventh International Conference on Electronic Commerce Research*, Dallas, TX, Jun 2004.

[2] David Turner, Daniel Havey and John Ewart. Allocating Resources in Storage Cooperatives with Pseudo Currencies. In *proceedings of the International Conference on Computer Science and its Applications*, San Diego, CA, July 2003.

[3] Lietaer Bernard. Complementary Currencies in Japan Today: History, Originality and Relevance. *International Journal of Community Currency Research.* Vol.8, pp.1-23

[4] Seyfang, Gill. Tackling social exclusion with community currencies: learning from LETS to Time Banks. *International Journal of Community Currency Research.* 2002: Volume 6

[5] Plinge, Walter. *Commodity Currencies for Fair and Stable International Exchange Rate.* International Journal of Community Currency Research. 2001: Volume 5

[6] R. L. Rivest and A. Shamir. *Payword and micromint: Two simple Micropayment schemes.* In Security Protocols Workshop, pages 69-87, 1996.

[7] B. Yang and H. Garcia-Molina. *PPAy: Micropayments for Peer-to-Peer Systems.* In Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), oct 2003

[8] C. Schmidt & R. Müller, "undated". "A Framework for Micropayment Evaluation," Sonderforschungsbereich 373 1998-66, Humboldt Universitaet Berlin.

[9] Kytojoki, Jari and Karpijoki, Vesa. *Micropayments – Requirements and Solutions.* Tik-110.501 Seminar on Network Security (3 cr), 2000 Jan.

[10] David Turner and Ni Deng. Payment-Based Email. *5th International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD2004)*, Beijing, China, Jun/Jul 2004.

[11] David Turner and Daniel Havey. Controlling Spam through Lightweight Currency. In *proceedings of the Hawaii International Conference on Computer Sciences,* Honolulu, HI, Jan 2004.

[12] Cashette, inc. Payment based email service. http://www.cashette.com/.

[13] Abrazhevich, D. (2001) *A Survey of User Attitudes towards Electronic Payment Systems.* Proceedings of Joint AFIHM-BCS Conference on Human-Computer Interaction IHM-HCI'2001, Volume 2.

[14] Bakos, Y. and Brynjolfsson, E. *Aggregation and Disaggregation of Information Goods: Implications for Bundling, Site Licensing and Micropayment Systems*, in Proceedings of Internet Publishing and Beyond: The Economics of Digital Information and Intellectual Property. D. Hurley, B. Kahin, and H. Varian, eds. MIT Press, Cambridge, Massachusetts (August 2000).

[15] Bakos, Y. *Towards Friction-Free Markets: The Emerging Role of Electronic Marketplaces on the Internet*, Communications of the ACM, Volume 41, Number 8 (August 1998), pp. 35-42.

[16]Rolf F. H. Schroeder. Talente Tauschring Hannover (TTH): Experiences of a German LETS and the relevance of theoretical reflections. *International Journal of Community Currency Research,* 2002: Volume 6.

[17] Jeffrey Jacob, Merlin Brinkerhoff, Emily Jovic and Gerald Wheatley. HOUR Town - Paul Glover and the Genesis and Evolution of Ithaca HOURS. *International Journal of Community Currency Research,* 2002: Volume 8.

[18] Stephen DeMeulenaere. Reinventing the Market: Alternative Currencies and Community Development in Argentina. *International Journal of Community Currency Research,* 2000: Volume 4.