Electronic Currency for the Internet

NetCash is a framework for electronic currency being developed at the Information Sciences Institute of the University of Southern California. NetCash will enable new types of services on the Internet by providing a real-time electronic payment system that satisfies the diverse requirements of service providers and their users. Among the properties of the NetCash framework are: security, anonymity, scalability, acceptability, and interoperability.

** by Gennady Medvinsky and*
Dr. B. Clifford Neuman
University of Southern California

One of the primary goals of NetCash is to facilitate anonymous electronic payments over an unsecure network without requiring the use of tamper-proof hardware. NetCash is designed to provide secure transactions in an environment where attempts at illegal creation, copying, and reuse of electronic currency are likely. In order to protect the privacy of parties to a transaction, NetCash provides financial instruments that prevent traceability and preserve the anonymity of users. Furthermore, with NetCash, service providers and their users are able to select payment mechanisms based on the level of anonymity desired, ranging from non-anonymous and weakly anonymous instruments that are scalable, to unconditionally anonymous instruments that require more resources of the currency server.NetCash provides scalable electronic currency that is accepted across multiple administrative domains. Using the NetCash framework, parties that are customers of different banks can accept each other's currency. To provide interoperability across currency servers, NetCash integrates anonymous electronic currency into the non-anonymous electronic banking infrastructure that has been proposed for routine transactions. This article presents a brief overview of NetCash; a more detailed description can be found in [3].

Requirements

Among the desirable properties for an electronic currency system are: security, anonymity, scalability, acceptability, and interoperability.

❐ *Security:* Forging paper currency is difficult. However, electronic currency is just data and is easily copied. Copying or double spending of electronic currency should be prevented or detected. Ideally the illegal creation, copying, and reuse of electronic cash should be unconditionally or computationally impossible. Some systems rely instead on post-fact detection and punishment of double spending [1].

❐ *Anonymity:* The identity of an individual using electronic currency should be protected; it should not be possible to monitor an individual's spending patterns, nor determine one's source of income. An individual is traceable in traditional transaction systems such as checks and credit cards. Some protocols are unconditionally untraceable, where an individual's spending can not be determined even if all parties collude [1]. For some transactions, weaker forms of anonymity may be appropriate, e.g. traceability can be made difficult enough that the cost of obtaining such information outweighs the benefit.

❐ *Scalability:* A system is scalable if it can handle the addition of users and resources without suffering a noticeable loss of performance. The existence of a central server through which transactions must be processed limits the scale of the system. The mechanisms used to detect double spending also affects scalability. Most proposed e-cash protocols assume that the currency server will record all coins that have been previously spent and check this list when verifying a transaction [1,5,6]. This database will grow over time, increasing the cost to detect double spending. Even if the life of a coin is bounded, there is no upper bound on the amount of storage required since the storage requirement depends on the rate at which coins are used, rather than on the number of coins in circulation.

❐ *Acceptability:* Most e-cash proposals use a single bank [1,5,6]. In practice, multiple banks are needed for scalability, and because not all users will be customers of a single bank. In such an environment, it is important that currency minted by one bank be accepted by others. Without such acceptability, electronic currency could only be used between parties that share a common bank. When currency minted by one bank is accepted by others, reconciliation between banks should occur automatically. To our knowledge, NetCash is the first system that satisfies this requirement.

❐ *Interoperability:* Users of the Internet will select financial instruments that best suit their needs for a given transaction. It is likely that several forms of electronic currency will emerge, providing different tradeoffs for security, anonymity, and scalability. In such an environment it is important that funds represented by one mechanism be easily convertible into funds represented by others.

Framework

The NetCash infrastructure is based on independently managed, distributed currency servers that provide a point of exchange between anonymous electronic currency and non-anonymous instruments such as electronic checks. In the framework, checks based on the global accounting infrastructure [4] support the transfer of funds between currency servers, forming a financial federation where currency minted by different servers is accepted. An organization wishing to set up and manage a currency server obtains insurance for the new currency from an agency similar to the United States Federal Deposit Insurance Corporation; the currency is backed by account balances registered to the currency server in the non-anonymous accounting infrastructure. A certificate of insurance allows the coins minted by a currency server to be

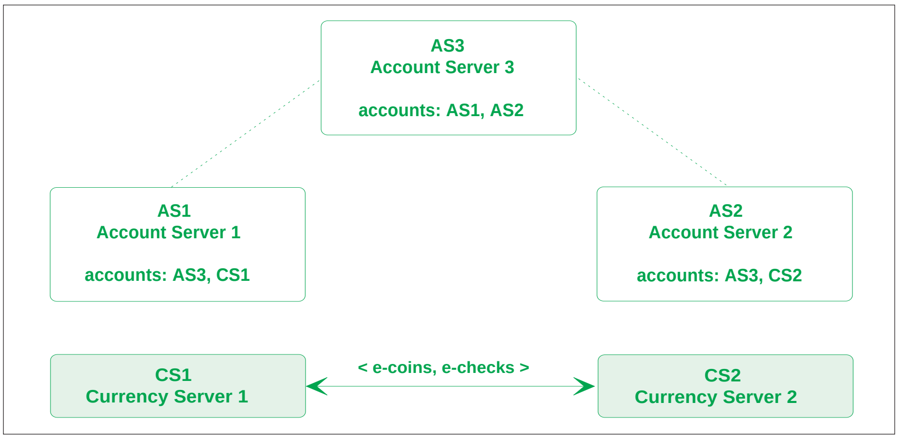
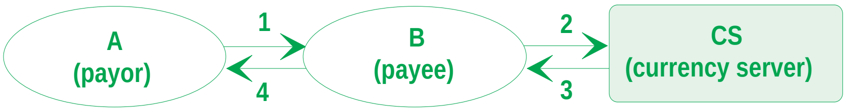


Figure 1: Financial federation sample

accepted across administrative domains.

Figure 1 shows a financial federation consisting of several accounting servers (AS1, AS2 and AS3) and several currency servers (CS1 and CS2). The accounting servers maintain accounts for the currency servers and other clients. Funds can be transferred between currency servers when one (the payor) issues a check authorizing another (the payee) to transfer funds from the payor's account to that of the payee. The accounting hierarchy allows the clearing of such checks between the accounting servers that maintain the accounts for the respective currency servers. Although the currency servers are identified in such transactions, the end-users are not.

Such transfers provide for anonymous currency transactions between users in different administrative domains. To verify a coin issued by another currency server, a user's local currency server contacts the remote currency server to convert the coin, accepting in return a check payable to the local currency server. This check is then cleared through the global accounting infrastructure, and a new coin issued by the local currency server is returned to the user.



Protocol steps

1. {coins, SK_{AN}, K_{AN}, S_id} K_B
2. {coins, SK_{BN}, transaction} K_{CS}
3. {instrument} SK_{BN}
4. {{amount, T_id, date} K_B^{-1}} SK_{AN}

SK_{AN}	A's freshly generated secret key
SK_{BN}	B's freshly generated secret key
K_{CS}	Currency server's public key
K_B	*B's* public key
K_B^{-1}	B's private key
K_{AN}	A's freshly generated public sesssion key
S_id	Service identifier
T_id	Unique identifier

Figure 2: Protocol for routine monetary transactions using NetCash

Electronic Currency Transactions

NetCash provides a framework for integrating currency servers using different electronic currency protocols, providing a range of anonymity guarantees. Electronic currency mechanisms providing unconditional or weak anonymity can be tied to the framework. Either the payor, the payee, or both parties may remain anonymous. The integration of multiple mechanisms allows a tradeoff between the anonymity guarantees and the resulting overhead of the electronic currency mechanism. Economic incentives can be used to encourage the selection of an appropriate mechanism.

Chaum and others have proposed protocols supporting unconditionally untraceable electronic currency [1]. While those protocols may be used within the framework we are developing, we have chosen to concentrate our efforts on protocols that provide weaker anonymity guarantees. The protocols we are developing are described briefly here; additional detail is available in [3].

Figure 2 shows a protocol for routine monetary transactions using NetCash. A payment is made by A (the payor) to B (the payee). A remains anonymous and B is protected from fraud. It is assumed that A can determine B's public key and B can determine the public key of the currency server. In the first step, A sends coins, the identifier of the desired service *S_id*, and two keys, a freshly generated secret key SK_{AN} and a public session key K_{AN}, all encrypted in B's public key. B records the newly chosen secret key SK_{AN} which will be used to establish a secure channel with A at a later time. A public session key can also be used to verify that subsequent requests originate from the principal that paid for the service.

After receiving coins from A, B verifies the validity of the coins with the currency server. In the second step, B sends to the currency server the coins, SK_{BN}, a newly chosen secret key, and an indication of what it wants back: new coins known to be valid, or a check made payable to a named principal. This message is encrypted in the currency server's public key. Upon receiving the coins, the currency server verifies the validity of the coins. If the coins haven't been spent already, the server returns the desired instrument sealed with SK_{BN}. In the final step, B returns a receipt signed with its private key and encrypted with SK_{AN}. The receipt includes amount paid, date and a unique identifier *T_id* that will be used along with the session key to obtain the service.

One shortcoming of this protocol as described is that it provides protection from fraud only by the payor. B can spend A's coins without providing a valid receipt. Extensions to the protocol supporting protection against fraud for both parties, anonymity provisions for the payee, and partially offline transactions are described by the authors in [3].

Project Status

Several security projects are under way at ISI that provide the necessary infrastructure for NetCash. One project is developing a proxy mechanism using the Kerberos authentication system [7]. This mechanism provides the authorization services needed for the non-anonymous accounting infrastructure that connects currency servers. Work is also under way to develop the accounting databases that are needed for the non-anonymous accounting infrastructure and the currency databases needed by electronic currency servers.

References ■

[1] *Chaum, D.; Fiat, A.; Naor, N.:* Untraceable Electronic Cash, in: Proceedings of Crypto '88, 1988.

[2] *Even, S.; Goldreich, O.; Yacobi, Y.:* Electronic Wallet, in: Proceedings of Crypto '83, 1983.

[3] *Medvinsky, G.; Neuman, B. C.:* Netcash: A Design for Practical Electronic Eurrency on the Internet, in: Proceedings of the First ACM Conference on Computer and Communications Security, November 1993.

[4] *Neuman, B. C.:* Proxy-based Authorization and Accounting for Distributed Systems, in: Proceedings of the 13th International Conference on Distributed Computing Systems, May 1993.

[5] *Okomato, T.; Ohta, K.:* Universal Electronic Cash, in: Proceedings of Crypto '91, 1991.

[6] *Pfitzmann, B.; Waidner, M.:* How to Break and Repair a 'Provably Secure' Untraceable Payment System, in: Proceedings of Crypto '91, 1991.

[7] *Steiner, J.G.; Neuman, B.C.; Schiller J.I.:* Kerberos - An Authentication Service for Open Network Systems, in: Proceedings of the Winter 1988 Usenix Conference, February 1988, pp 191-201.

** Gennady Medvinsky is a Ph.D. student in the Computer Science Department at the University of Southern California. Dr. B. Clifford Neuman is a scientist at the Information Sciences Institute and a faculty member in the Computer Science Department. He is one of the principal designers of the Kerberos authentication system. The work described in this article was supported in part by the Advanced Research Projects Agency under NASA Cooperative Agreement NCC-2-539. The views and conclusions presented should not be interpreted as representing the official policies of the funding agencies.*