In Berkshire Encyclopedia of Human Computer Interaction,
ed. W. Bainbridge, Berkshire Publishing, 2004, pp. 167-170

DIGITAL CASH

The use of digital cash has increased in parallel with the use of electronic commerce; as we purchase items online, we need to have ways to pay for them electronically. Many systems of electronic payment exist.

Types of Money

Most systems of handling money fall into one of two categories:

1. Token-based systems store funds as tokens that can be exchanged between parties. Traditional currency falls in this category, as do many types of stored-value payment systems, such as subway fare cards, bridge and highway toll systems in large metropolitan areas (e.g., FastPass, EasyPass), and electronic postage meters. These systems store value in the form of tokens, either a physical token, such as a dollar bill, or an electronic register value, such as is stored by a subway fare card. During an exchange, if the full value of a token is not used, then the remainder is returned (analogous to change in a currency transaction)—either as a set of smaller tokens or as a decremented register value. Generally, if tokens are lost (e.g., if one's wallet is stolen or one loses a subway card), the tokens cannot be recovered.
2. Account-based systems charge transactions to an account. Either the account number or a reference to the account is used to make payment. Examples include checking accounts, credit card accounts, and telephone calling cards. In some instances, the account is initially funded and then spent down (e.g., checking accounts); in other instances, debt is increased and periodically must be paid (e.g., credit cards). In most account-based systems, funds (or debt) are recorded by a trusted third party, such as a bank. The account can be turned off or renumbered if the account number is lost.

The more complex an electronic payment system is, the less likely consumers are to use it. (As an example, a rule of thumb is that merchants offering "one-click ordering" for online purchases enjoy twice the order rate of merchants requiring that payment data be repeatedly entered with each purchase.)

Electronic Payment Using Credit Cards

The most common form of electronic payment on the Internet today is credit card payment. Credit cards are account based. They are issued by financial institutions to consumers and in some cases to

organizations. A consumer presents the credit card number to a merchant to pay for a transaction. On the World Wide Web credit card account numbers are typically encrypted using the Secure Socket Layer (SSL) protocol built into most Web browsers. The merchant often attempts to verify the card holder by performing address verification (checking numbers appearing in an address) or by using a special verification code (typically printed on the reverse side of the credit card). In the United States credit card users typically enjoy strong rights and can reverse fraudulent transactions.

Although the SSL protocol (in typical configurations) provides strong encryption preventing third parties from observing the transaction, risks still exist for the credit card holder. Many merchants apply inadequate security to their database of purchases, and attackers have gained access to large numbers of credit cards stored online. Moreover, some merchants charge incorrect amounts (or charge multiple times) for credit card transactions. Although fraudulent transactions are generally reversible for U.S. residents, time and effort are required to check and amend such transactions. In some instances, criminals engage in identity theft to apply for additional credit by using the identity of the victim.

To reduce these risks, some experts have proposed a system that uses third parties (such as the bank that issued the card) to perform credit card transactions. A notable example of this type of system is Verified by Visa. However, the additional work required to configure the system has deterred some consumers, and as a result Verified by Visa and similar systems remain largely unused. The most elaborate of these systems was the Secure Electronic Transactions (SET) protocol proposed by MasterCard International and Visa International; however, the complexity of SET led to its being abandoned. In these systems credit card purchases are usually funded with a fee that is charged to the merchant. Although rates vary, typical fees are fifty cents plus 2 percent of the purchase amount.

Third-Party Payment Accounts

A merchant must be able to process credit card payments. This processing is often inconvenient for small merchants, such as people who sell items in online auctions. As a result, a market has opened for third-party payment processors. Today, the largest third-party payment processor is PayPal, owned by the eBay auction service. Third-party payment processor systems are account based.

Consumers can pay for third-party purchases in three ways: by paying from an account maintained with the third party, by paying from a credit card account, and by paying from a checking account. Merchants' rates for accepting funds from a credit card account are slightly higher than their rates for accepting funds from a conventional credit card account.

Third-party payment accounts are convenient because they are simple to use and provide consumers with protection against being overcharged. However, they tend not to provide the same degree of protection that a credit card-funded purchase provides. Because third-party payment accounts are widely used with auction systems, where fraud rates are unusually high, the degree of protection is a serious consideration.

Smartcards and Other Stored-Value Systems

Stored-value systems store value on a card that is used as needed. Smartcards are a token-based payment system. Many smartcards use an integrated circuit to pay for purchases. They are widely used in Europe for phone cards and in the GSM cellular telephone system. Mondex is a consumer-based system for point-of-sale purchases using smartcards. Use of smartcards is limited in Asia and largely unused in North America. (In North America only one major vendor, American Express, has issued smartcards to large numbers of users, and in those cards the smartcard feature is currently turned off.)

Experts have raised a number of questions about the security of smartcards. Successful attacks conducted by security testers have been demonstrated against most smartcard systems. Experts have raised even deeper questions about the privacy protection provided by these systems. For example, in Taiwan, where the government has been moving to switch from paper records to a smartcard system for processing National Health Insurance payments,

considerable public concern has been raised about potential privacy invasions associated with the use of health and insurance records on a smartcard system.

A number of devices function like a smartcard but have different packaging. For example, some urban areas have adopted the FastPass system, which allows drivers to pay bridge and highway tolls using radio link technology. As a car passes over a sensor at a toll booth, value stored in the FastPass device on the car is decremented to pay the toll. The state of California recently disclosed that it uses the same technology to monitor traffic flow even when no toll is charged. The state maintains that it does not gather personal information from FastPass-enabled cars, but experts say that it is theoretically possible.

Anonymous Digital Cash

A number of researchers have proposed anonymous digital cash payment systems. These would be token-based systems in which tokens would be issued by a financial institution. A consumer could "blind" such tokens so that they could not be traced to the consumer. Using a cryptographic protocol, a consumer could make payments to merchants without merchants being able to collect information about the consumer. However, if a consumer attempted to copy a cryptographic token and use it multiple times, the cryptographic protocol would probably allow the consumer's identity to be revealed, allowing the consumer to be prosecuted for fraud.

Anonymous digital cash payment systems have remained primarily of theoretical interest, although some trials have been made (notably of the Digicash system pioneered by David Chaum). Anonymous payment for large purchases is illegal in the United States, where large purchases must be recorded and reported to the government. Moreover, consumers generally want to record their purchases (especially large ones) to have maximum consumer protection. Some researchers have demonstrated that anonymous digital cash payment systems are not compatible with atomic purchases (that is, guaranteed exchange of goods for payment). The principal demand for anonymous payment appears to be for transactions designed to evade taxes, transactions of contraband, and transactions of socially undesirable material.

Micropayments

One of the most interesting types of electronic payment is micropayments. In many instances consumers wish to purchase relatively small-value items. For example, consider a website that vends recipes. Each recipe might be sold for only a few cents, but sold in volume, their value could be considerable. (Similarly, consider a website that offers online digital recordings of songs for ninety-nine cents each.) Currently, making small payments online using traditional payment methods is not feasible. For example, as mentioned, credit card companies typically charge merchants a processing fee of fifty cents plus 2 percent of the purchase amount for credit card transactions—clearly making credit card purchases for items that cost less than fifty cents impractical. Most merchants refuse to deal with small single-purchase amounts and require that consumers either buy a subscription or purchase the right to buy large numbers of items. For example, newspaper websites that offer archived articles typically require that consumers purchase either a subscription to access the articles or purchase a minimum number of archived articles—they refuse to sell archived articles individually.

To enable small single purchases, a number of researchers have proposed micropayment systems that are either token based or account based. An example of an account-based micropayment system is the NetBill system designed at Carnegie Mellon University. This system provides strong protection for both consumers and merchants and acts as an aggregator of purchase information. When purchases across a number of merchants exceed a certain threshold amount, that amount is charged in a single credit card purchase.

An example of a token-based micropayment system is the PepperCoin system proposed by Ron Rivest and Silvio Micali and currently being commercialized. Peppercoin uses a unique system of "lottery tickets" for purchases. For example, if a consumer wishes to make a ten-cent purchase, he might use a lottery ticket that is worth ten dollars with a probability of 1 percent. The expected value paid by the consumer would be the same as the items he purchased; but any single charge would be large enough to justify being charged using a traditional payment mechanism (such as a credit card).

Despite the promise of micropayment systems, they remain largely unused. Most merchants prefer to support small-value items by using Web-based advertising or subscriptions. Nonetheless, advocates of micropayment systems maintain that such systems enable new classes of electronic commerce.

Challenges for Digital Cash

Although digital cash is being increasingly used, a number of challenges remain. The principal challenge is associating payment with delivery of goods (this challenge is often known as the "atomic swap" or "fair exchange" problem.) Merchants also need to be protected from using stolen payment information, and consumers need to be protected from merchants who inadequately protect payment information (or, even worse, engage in fraud.) Finally, effective payment methods need to be developed and accepted to support both large and small purchases. A balance must be reached between consumers who want anonymous purchases and government authorities who want to tax or record purchases. These challenges make digital cash a rapidly developing research area.

J. D. Tygar

See also E-business

FURTHER READING

Chaum, D., Fiat, A., & Naor, M. (1990). Untraceable electronic cash. In G. Blakley & D. Chaum (Eds.), *Advances in cryptology* (pp. 319–327). Heidelberg, Germany: Springer-Verlag.

Electronic Privacy Information Center. (2003). *Privacy and human rights 2003*. Washington, DC: Author.

Evans, D., & Schmalensee, R. (2000). *Paying with plastic: The digital revolution in buying and borrowing*. Cambridge, MA: MIT Press.

Kocher, P., Jaffe, J., & Jun, B. (1999). Differential power analysis. In M. Weiner (Ed.), *Advances in cryptology* (pp. 388–397). Heidelberg, Germany: Springer-Verlag.

Mann, R., & Winn, J. (2002). *Electronic commerce*. Gaithersburg, MD: Aspen Publishers.

O'Mahony, D., Peirce, M., & Tewari, H. (2001). *Electronic payment systems for e-commerce* (2nd ed.). Norwood, MA: Artech House.

Tygar, J. D. (1998). Atomicity in electronic commerce. *Networker, 2*(2), 23–43.

Wayner, P. (1997). *Digital cash: Commerce on the Net* (2nd ed.). San Francisco: Morgan-Kaufmann.