In ACM NetWorker, 2:2, April/May 1998, pp. 32-43

Atomicity in Electronic Commerce

J. D. Tygar

There is a tremendous demand to electronically buy and sell goods over networks. This field is called electronic commerce, and it has inspired a large variety of work. Unfortunately, much of this activity ignores traditional transaction processing concerns — chiefly atomicity. This paper discusses the role of atomicity in electronic commerce, pointing out various atomic flaws. Special attention is given to the atomicity problems of digital money proposals. Two examples of highly atomic electronic commerce systems, NetBill and cryptographic postage indicia, are presented.

ELECTRONIC COMMERCE

If you regularly use the World Wide Web, you have probably noticed that much of the information on it is worth what you pay for it. To improve the quality of available electronic information, we must create mechanisms to conveniently compensate the creators and owners of network information. If we want to put the Library of Congress online, we will first have to find a way to compensate copyright owners.

Electronic commerce is an attempt to address such problems. The idea is to build mechanisms that make it simple to buy and sell goods online. These mechanisms have attracted significant interest. Besides enabling a new type of commerce, they appear to offer a variety of benefits, including increasing the range of information readily available to most people,

making automatic search and retrieval of that information easy, and reducing costs by simplifying or eliminating human involvement in processing and fulfilling orders.

Here is one indicator of the excitement over electronic commerce: The June 12, 1995, issue of *Business Week* includes the following projection of the role of electronic commerce. This projection is probably overly optimistic, but it is a sign that electronic commerce is being taken seriously in some quarters.

YEAR	TRADITIONAL COMMERCE (BILLION $)	ELECTRONIC COMMERCE (BILLION $)
1994	5,150	245
2000	8,500	1,650
2005	12,000	2,950

Here is another indicator: In 1994, J. C. Penney, a well-known American retailer with a reputation for not being especially high-tech, sold $17 million worth of goods directly to customers over computer networks (including both the Internet and private services such as CompuServe, America Online, Prodigy, etc.).

For many more indicators, visit the WWW site *http://www.yahoo.com*, and see the tens of thousands of electronic storefronts available.

There are many attempts to build electronic commerce systems. Prominent examples of organizations that have accomplished such efforts are CMU (NetBill), CyberCash (and CyberCoin), DigiCash, DEC (MilliCent), First Virtual, FSTC (E-check), GCTech, IBM (iKP), MasterCard and Visa (SET), Open Market, Netscape (SSL) and the U.S. Postal Service. (More firms join this list every day. Any bibliographic listing of references will rapidly become dated, but endnotes [11], [35] and [36] contain a nice summary of most of this work.)

Conferences on Principles of Distributed Computing (PODC) have contributed concepts that are used heavily in electronic commerce. The most important are:

- Atomic transactions
- Cryptographically secure protocols
- Secure computation
- Safe voting
- High reliability

This paper is concerned with the first concept, atomic transactions. I will discuss a variety of types of electronic commerce, and after a discussion on atomicity, I will consider the atomic properties of several electronic commerce protocols. This will be followed by a discussion of the development of two highly atomic protocols: the NetBill protocol and cryptographic postage indicia.

My tone throughout the paper is informal. I am afraid that you will not find formal definitions of types of electronic commerce atomicity below; indeed, I consider the formulation of those formal definitions an open problem. For those who crave more details presented in a more formal manner, endnote [8] and the appendix of [33] contain technical expositions of the NetBill protocol; endnote [11] is the best reference for a formal exposition of cryptographic postage indicia.

Note that throughout the text I use male pronouns to refer to merchants and female pronouns to refer to customers.

ELECTRONIC COMMERCE PROPERTIES

How can we characterize electronic commerce protocols? Although there are a variety of properties that we can use, this paper focuses on atomicity. Since properties often interact in a variety of non-trivial ways, however, it is important to review several of them.

Atomicity

Atomicity allows us to logically link multiple operations so that either all of them are executed or none of them. For example, in transaction processing one may execute a sequence of code as follows:

```
<begin-transaction>
state-changing operation 1;
```

```
state-changing operation 2;
. . .
state-changing operation n;
<end-transaction>
```

When this block of operations is executed, all of the state-changing operations inclusively from 1 to *n* will be executed, or the state of the system will be as if none of them had been executed.

Why would atomicity ever fail to occur? Well, if the transactions are being executed in a distributed environment on multiple processors, then one of the processors executing a state-changing operation or communication between two processors executing state-changing operations may fail. In either case, it may be impossible to complete the entire block of state-changing operations. When this happens, it is necessary to roll back the processors to a state consistent with the transaction having never been initiated in the first place.

Atomic transactions form the cornerstone of modern transaction processing theory. (Nancy Lynch and her fellow researchers have written an encyclopedic book about atomic transactions [16]; a tremendous resource for those implementing atomic transaction processing systems is the standard textbook [10]; and for a thorough review of powerful rollback methods in the context of computer security and electronic commerce, see [29], [30], and [31].) No non-atomic distributed transaction system would ever be tolerated by customers of data processing. As we shall see below, however, the story is quite different in the world of electronic commerce protocols. Most of the proposed protocols are not atomic. For example, if I interrupt a communication between a merchant and a customer, I can often throw an electronic commerce protocol into an ambiguous state. Money or electronic cash tokens may be copied (with different parties each believing that it has the true, valid copy) or destroyed.

The following are three levels of atomicity that protect electronic commerce protocols.

Money Atomicity

Money-atomic protocols effect the transfer of funds from one party to another without the possibility of creating or destroying money. For example, a cash transaction is usually money-atomic (unless the possibility exists of money being counterfeited or destroyed). Money atomicity is a basic level of atomicity that each electronic commerce protocol should satisfy.

Goods Atomicity

Goods-atomic protocols are money-atomic, and also effect an exact transfer of goods for money. That is, if I buy a good using a goods-atomic protocol, I will receive the good if and only if the money is transferred. For network protocols, goods atomicity is especially important for information goods. There must be no possibility that I can pay without getting the goods, or get the goods without paying. (Anyone who has had an interrupted file transfer while downloading information on the Internet is aware of the importance of goods atomicity.) For example, a cash-on-delivery parcel delivery is a good real-world approximation to an electronic commerce protocol. I get the parcel exactly when I have paid the delivery agent. Goods atomicity is an important property that each electronic commerce protocol intended for information transactions should satisfy.

Certified Delivery

Certified-delivery protocols are money-atomic

J.D. Tygar <tygar@cs.cmu.edu> is Associate Professor in the Computer Science Department at Carnegie Mellon University in Pittsburgh. This article is part of the book *Internet Besieged: Countering Cyberspace Scofflaws*, edited by Dorothy E. Denning and Peter J. Denning (Addison-Wesley, 1997), which was reviewed in the November/December 1997 issue of *netWorker*.

and goods-atomic protocols that also allow both a merchant and a customer to prove exactly which goods were delivered. If I buy a document entitled "How to Make a Million Dollars Fast on the Internet" and receive an electronic copy of some unrelated material, I will want to complain to an authority. To rapidly resolve the question, both the merchant and the customer will want to be able to prove the exact contents of what was delivered. For example, a certified-delivery protocol corresponds to a cash-on-delivery parcel delivery when the contents of the parcel are opened in front of a trusted third party who immediately and permanently records the exact contents of the parcel.

Certified-delivery protocols are helpful when merchants and/or customers are not trusted. Today, there is no effective way to distinguish a large, trustworthy WWW merchant from a fly-by-night impressive electronic storefront that actually connects to a shop that contains a fraudulent operation.

Anonymity

Some people want to keep their purchases private. They do not want to have third parties (or even merchants) know their identity. The customer may want to be anonymous because she is buying a good of questionable social value (for example, pornography); does not want to have her name added to a marketing or mailing list; or simply personally values privacy. It may be for illegal reasons, for example, tax evasion.

Although most paper money contains serial numbers, cash transactions can often have anonymous properties. Serial numbers are rarely traced and recorded, and if I buy something from a merchant who does not know me or from a vending machine, my purchase is often effectively anonymous.

David Chaum has been the most influential advocate of anonymous electronic commerce protocols. He has written a number of highly influential papers on topics such as "anonymous digital cash"; these in turn have inspired many electronic commerce researchers who have improved his protocols. A sophisticated representative example of the current version of his protocols can be found in [4].

Here is the way these protocols work:

1. A customer withdraws money from the bank, receiving a cryptographic token that can be used as money;
2. The customer applies a cryptographic transformation to the money that still allows a merchant to check its validity, but make it impossible to trace the customer's identity.
3. The customer spends the money with the merchant. (In doing so, the customer applies a further cryptographic transformation so that the merchant's identity is used in the data.)
4. The merchant checks to make sure that he has not received the token previously.
5. The merchant sends the goods to the customer.
6. At a later point, the merchant deposits his electronic tokens at the bank.
7. The bank checks the tokens for uniqueness; the identities of the customers remain anonymous except in the case when a customer had double-spent a token. If a token was double-spent, the identity of the customer is revealed and the network police are notified of attempted counterfeiting.

Now consider when a communication failure happens around step (3). The customer has no way of knowing if the merchant has received her token or not. The customer has two options:

- ✗ The customer can return her electronic token to the bank (or spend it on a different merchant). If she does this, and the merchant actually received her token, then when the merchant cashes in the token, the customer's identity will be revealed. Even worse, the customer will likely be accused of fraud.
- ✗ The customer can take no action, failing

to return her token. If she does this, and the merchant never received her token, then she is in danger of losing her money. She will have never received the good she attempted to purchase, and she will be unable to use her money.

In either case, money atomicity breaks down.

In many countries, most anonymous transactions are illegal. For example, in the United States the Money Laundering Act (12 USC §1829) requires that electronic commerce systems should both promptly report any transaction over $10,000 and store a copy of any transaction over $100. These requirements have not been tested in court for digital cash systems. It is clear, however, that as currently proposed, digital cash systems are illegal.

I also note that it is often possible to achieve a limited form of anonymity by having a proxy agent complete purchases for the customer. In this case, the transaction may be easily traced to the proxy agent who privately keeps the identity of the true customer.

Security

Can we trust anyone in cyberspace? Communications can be easily intercepted, messages inserted, and the absolute identity of other parties left uncertain. Clearly, security is important for any electronic commerce protocol.

By contemporary standards, it is unlikely that the current form of the credit card, which reveals a customer's identity and charge numbers to a merchant or to anyone who can obtain a copy of the receipt, would be accepted if it were introduced today.

Many electronic commerce systems depend on some ultimate, trusted authority. For example, NetBill depends on the trustworthiness of a central server. However, even in the case where a trusted server is used, the effects of the security failures of that server can be minimized. For example, in NetBill, detailed cryptographically unforgeable records are kept so that if the central server is ever corrupted, it would be possible to unwind all the corrupted actions and restore any lost money.

Transaction Size

The average credit card transaction has typically been estimated to be on the order of $50. Depending on the arrangements made with a bank, a merchant is paid approximately 30 cents plus 2% of the purchase price for each transaction. For many telephone or mail order businesses, the actual rate is closer to 50 cents plus 2.25%.

If one is engaged in a transaction that is only worth 10 cents or even 1 cent, the standard credit card rates would dominate the cost of the item. Thus, a number of parties have proposed support for microtransactions, or transactions less than $1. (By no means is 1 cent the minimum transaction value of interest; Mark Manasse's electronic commerce system is named MilliCent [17].)

Both NetBill and cryptographic postage indicia are predicated on the concept of supporting microtransactions. Some of the design decisions made for those systems can only be understood by the microtransaction requirement. However, a detailed discussion of microtransactions is beyond the scope of this paper. (For those who are curious: The key to most microtransaction protocols is to aggregate many small transactions using specially optimized protocols, and then charge the aggregated total as a large value transaction, a beautiful application of protocol nesting. For a discussion of microtransactions in NetBill, see [27]; for a completely different approach, see [17]).

NON-ATOMIC ELECTRONIC COMMERCE PROTOCOLS

DigiCash

DigiCash uses an anonymous digital cash protocol. As discussed earlier, digital cash protocols are not money-atomic; indeed, in the event of a communication failure, they can fail to be anonymous, too. Digital cash protocols use

several rather computationally intense cryptographic operations and are thus quite expensive. I estimate that the real cost of processing a single digital cash transaction is on the order of $1 per transaction; DigiCash reportedly has relatively high fees, suggesting that this expectation is correct. DigiCash in its current form is not useful for microtransactions.

First Virtual

First Virtual allows users to buy goods freely and then uses e-mail to confirm each and every transaction with the customer. Aside from the acceptability of flooding a user with e-mail for purchases in this way, this model clearly preserves money atomicity but fails goods atomicity (since the customer can buy an item without paying for it). (First Virtual takes a dim view of communications security and encryption in any form; in [3] Borenstein argues that communications security is "irrelevant" and dismisses electronic commerce designers who postpone deployment of their systems in order to guarantee strong security measures.)

First Virtual's system can easily be a target of fraud and atomicity failures. It is somewhat better than digital cash, but inferior to other electronic commerce systems. Ultimately, First Virtual translates each electronic commerce transaction into a credit card transaction, making it of limited value for microtransactions in its current form. (First Virtual suggests using aggregation, but aggregation cannot be done across different merchants in a single credit card transaction.)

SSL

Using cryptography, the Secure Socket Layer (SSL) approach sets up a secure communication channel to transfer a customer's credit card number to the merchant. This approach is equivalent to reading your credit card number over the phone to a merchant using a secure telephone connection.

This approach offers money atomicity to the extent that credit card transactions are money-atomic. However, its security properties are less clear; for example, since a (potentially unscrupulous) merchant has the customer's credit card number, he can use it to commit fraud. (Merchant fraud is one of the most serious problems facing the credit card industry [37]. Lyndon LaRouche is a well-known example of a person who was charged with committing merchant credit card fraud.) Goods atomicity is not addressed by SSL.

In its current form, SSL is clearly of limited value for microtransactions.

SET

Secure Electronic Transactions [18] represent a compromise between a variety of similar protocols: STT (Visa/Microsoft), SEPP (MasterCard), and the iKP family of protocols (IBM). SET, and the protocols from which it is adapted, is an example of a secure credit card-based protocol. In SET, the customer digitally signs a purchase request and a price and then encrypts payment information (in the form of a credit card number, for example) with a bank's public key. The merchant acknowledges the purchase, and forwards the request to the bank. The bank processes the request, and if the prices match, the bank charges the customer's account and instructs the merchant to complete the sale.

Like SSL, this approach offers money atomicity to the extent that credit card transactions are money-atomic. However, the security properties of SET are superior since they prevent merchant fraud. Goods atomicity is not addressed by SET.

In its current form, SET is of limited value for microtransactions.

NETBILL

My co-researchers and I developed NetBill to provide all three levels of atomic transactions. Here, I give a broad sketch of the NetBill format and some rough arguments as to why it satisfies all three atomicity conditions: money atomicity, goods atomicity, and certified deliv-

ery. However, to keep my explanation simple, I do not cover the details of the protocol; for those, see endnotes [8] and [33]. For example, I do not discuss how NetBill protects against message replay, communication security, or various timing attacks.

The NetBill protocol exists among three parties: customer, merchant, and NetBill server. Think of a NetBill account held by a customer as equivalent to a virtual electronic credit card account.

The following is an outline of the NetBill protocol:

1. The customer requests a price from the merchant for some goods. This step is necessary because the price of a good may depend on the identity of the customer; for example, a student ACM member may qualify for a discount on some items.
2. The merchant makes an offer to the customer.
3. The customer tells the merchant that she accepts the offer.
4. The merchant sends the requested information goods, encrypted with key *K*, to the customer.
5. The customer prepares an electronic purchase order (EPO) containing a digitally signed value (for: price, cryptographic-checksum of encrypted goods, time-out). The customer sends the signed EPO to the merchant.
6. The merchant countersigns the EPO, assigns the value of *K*, and sends both values to the NetBill server.
7. The NetBill server checks the signature and counter-signature on the EPO. It then checks the customer's account to ensure that sufficient funds exist to approve the transaction, and also checks that the time-out value in the EPO has not expired. Assuming that all is OK, the NetBill server transfers price funds from the customer's account to the merchant's account. It stores *K*, and the cryptographic-checksum of the encrypted goods. NetBill then prepares a signed receipt that includes the value *K*, and it sends this receipt to the merchant.
8. The merchant records the receipt and forwards it to the customer (who can then decrypt her encrypted goods).

This protocol thus transfers an encrypted copy of the information goods, and records the decryption key in escrow at the NetBill server. Now let us see how this protocol provides various types of atomicity protection:

Money atomicity: All funds transfers occur at the NetBill server, and since the NetBill server uses a local atomic database to store fund values, no money can be created or destroyed.

Goods atomicity: If the protocol fails as a result of communications failure or processor failure before the NetBill server atomically processes the transaction in step (7), then money does not change hands, and the customer does not receive the decryption key or gain access to the encrypted information goods. On the other hand, if step (7) succeeds, then both the merchant and NetBill server will record the value of *K*. Normally, these values would be forwarded back to the customer as a result of step (8), but if something goes wrong, the customer can obtain *K* from either the merchant or NetBill server at any time.

Certified delivery: Since we have goods atomicity, we know that the customer received something in exchange for money. Now, suppose that the customer claims that she has received goods different from what she ordered. Since the NetBill server has a cryptographic-checksum of the encrypted goods that has been countersigned by both the customer and the merchant, the customer can present her encrypted goods to a judge and verify that she has not tampered with them. Now, since a merchant-signed value of *K* is stored with both the customer and the merchant, the judge can decrypt the goods and determine whether the goods were delivered as agreed or not.

NetBill is an example of a highly atomic electronic commerce protocol. We have currently built an alpha version of NetBill at Carnegie Mellon (in conjunction with our development and operations partners, Mellon Bank and Visa International), and hope to prove that NetBill is not only highly atomic but has the performance, scalability, and efficiency to handle a large number of microtransactions.

CRYPTOGRAPHIC POSTAGE INDICIA

Is it possible to achieve money atomicity without using a central server? Yes, and one way to do this is by securing hardware. For example, FIPS 140-1 [20] specifies support for tamper-proof and tamper-resistant devices that can store information and perform processing tasks. These devices are secure in the sense that any attempt to penetrate them will result in erasure of all information stored inside them. We could use this to store an electronic wallet; when a charge is made, the electronic wallet withdraws funds. We call these tamper-proof devices *secure coprocessors*.

Now the design of such a system is not easy [38], and there are quite a few risks associated with customer approval of transactions [9]. However, with careful design it can be made to work. My research group has been working with the U.S. Postal Service to develop standards for PC-generated laser-printed indicia for postage meters. These are designed to meet the needs of the Postal Service Information-Based Indicia Program [34].

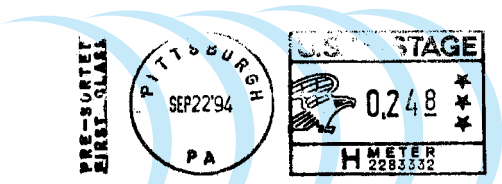

Figure 1. Traditional indicia are easy to copy.

As Figure 1 shows, it is commonplace to copy traditional indicia using a scanner and a computer. It is equally easy to forge dates and postage values on counterfeited indicia. (Note: If you ever decide to take up the life of a criminal and forge indicia, make sure to add smudges to the indicia — indicia that are reproduced too clearly can easily be recognized as forged.)

Using a secure coprocessor, it is easy to store an account balance for postal customers. This account balance is decremented whenever postage is printed. Now, the secure coprocessor prepares a cryptographically signed message that contains envelope data (sender address, receiver address, date sent, and sequence number). This information is then printed on the envelope using an efficient data representation such as PDF417 [14].

When mail is received at a postal sorting facility, the data block is checked to see if it matches the address used for sorting, and to verify the uniqueness of the sequence number. (Note that all mail to a given address will be processed by a single sorting station.) Indicia remain valid for six months. (The U.S. Postal Service claims to deliver more than 90% of all first-class mail within three days of its being sent, and more than 99% in seven days. Thus, six months would appear to be a generous parameter for mail delivery.) The database stored at a local sorting station can be regularly purged of entries with a date older than six months.

If an adversary attempts to break money atomicity by forging indicia, he must do one of two things: copy existing indicia, which then will only be valid for the encrypted delivery address and will be caught at the sorting station; or attempt to find the value used to digitally sign the cryptographic indicia, which will require opening the secure coprocessor, erasing all the vulnerable data within.

For a more technical exposition on secure coprocessors, see [11], [38], and [39].

OPEN PROBLEMS

The field of electronic commerce has many open problems. Here are some of my favorites:

- What is the relationship between atomicity and anonymity? Can they be mutually compatible? (In recent work my students and I have made significant progress toward this question; see [5].)
- What is the relationship between atomicity and security? Can they be separated?
- What other atomicity models exist in electronic commerce besides money atomicity, goods atomicity, and certified delivery? Is there a general schema?
- What is the minimum number of message exchanges necessary in an atomic purchase?
- What atomic electronic commerce mechanisms can be built for multiple banks or billing servers?
- Can atomicity be used for continuously delivered information (such as continual stock market updates) or very large objects (such as video programs)?
- Can atomicity be formally defined?
- How can we prove that a protocol is atomic?
- Is it possible to express atomic properties in terms of model checking? (See [11] for an initial attempt on this problem.)
- Can we extend electronic commerce models to auctions? Can we make them efficient and fair?
- Can we extend electronic commerce models to auction markets such as stock markets?
- Can we protect redistributed information or the reselling of information? (This is the so-called superdistribution

AN UPDATE ON ELECTRONIC COMMERCE

Since my article "Atomicity in Electronic Commerce" appeared last year, new developments in electronic commerce have been coming thick and fast. Here are some of the more salient changes as they relate to my original paper.

As the reprinted article mentions, even in 1994 total electronic commerce (including business-to-business, financial and consumer) exceeded $245 billion. We've all noticed the tremendous expansion of financial services available electronically, but especially dramatic has been the growth in consumer-level electronic commerce. Estimates vary on the dollar volume of consumer-based electronic commerce sales in 1997, from Forrester Research's $2.4 billion to American Express's estimate of $4 billion to $6 billion. IDC predicts that consumer sales will reach $20 billion by the end of 1998.

And indications point to widespread acceptance of electronic commerce by the public. Here are just a few examples: A study by Ernst & Young of a shopping cart of consumer goods indicated that in 90% of all cases, the best prices were found on the World Wide Web. Dell now sells $3 million worth of computers each day from its Web site. Egghead Software has decided to abandon its retail stores and switch to a Web-only presence. And 10% of all flower orders received by 1-800-FLOWERS arrive via the Web.

Nonetheless, the vast majority of consumer-oriented electronic commerce is transacted by fairly simple means — usually, credit card numbers exchanged via SSL (or, surprisingly often, in the clear). As I discussed in my article, this has negative implications for both atomic transactions and for microtransactions. The result is that the sale of information goods over the Web has been inhibited, and electronic commerce microtransactions are rare.

When microtransactions are permitted, they usually take place in the framework of subscriptions to a service. For example, *The Economist*, a financial newsmagazine, sells archived articles to subscribers. The old articles cost $1 each, but a user must purchase a minimum of $10 in credits since individual microtransactions are not supported at that Web site. Many researchers, including me, believe that highly atomic purchases and microtransactions represent vast markets to be mined.

Atomic Protocols in the Marketplace

What about the two highly atomic protocols — NetBill and cryptographic postage indicia — that I described at length in my article? Both of these systems have become commercialized. The NetBill project has been completed at Carnegie Mellon, and the technology has been licensed to CyberCash, which uses certified delivery in its CyberCoin product. (For

of Mori and Kawahara [19]).

- Can we devise effective digital watermarks that clearly indicate the purchaser of illegally pirated or redistributed information?
- How can we represent and enforce electronic contracts governing the use, distribution, and payment conditions for information goods and software?
- Can we make a fault-tolerant version of electronic commerce protocols that remain stable even when banks fail? (The results of T. Rabin and Ben-Or [24] seem to be appropriate here.)
- Can we build systems to allow anonymous charitable contributions? Can we extend them to allow documentation so that one can take a tax credit?
- What is the smallest microtransaction that can be supported in electronic commerce? The smallest atomic microtransaction?
- We can express money as tokens or as entries in a server (see [6]). Is there a way to express a formal equivalence between these two methods?

ACKNOWLEDGEMENTS AND FURTHER SOURCES OF INFORMATION

I would like to thank the following people:

- Bennet Yee, as all of the work described here regarding secure coprocessors and cryptographic postage indicia is joint work I've done with Bennet. We jointly observed that Chaum-like digital cash protocols fail to work properly if communications are interrupted, thus inspiring this work. Portions of our work

more details, see *http://www.cybercash.com and http://www.netbill.com.*) Cryptographic postage indicia are now formally approved for use in the U.S., as part of the U.S. Postal Service's Information Based Indicia Program. On March 31, the first official cryptographic indicia were applied to envelopes in a ceremony at the Smithsonian National Postal Museum. E-Stamp Corp. is the first vendor producing cryptographic postage indicia. For more information, go to *http://www.usps.gov* and *http://www.e-stamp.com.*

The SET standard discussed in my article has continued to develop slowly. SetCo (*http://www.setco.org)* has assumed responsibility for maintaining the SET standard. SET has not been widely deployed, however, and the standard has been criticized in *The New York Times* and elsewhere for its complexity and ambiguous security properties. For example, in SET a key design issue is to prevent a merchant from obtaining, and perhaps improperly using, a consumer's credit card number, but SET has a mode in which credit card numbers are explicitly sent back to a merchant. Today, SET's security model is not clear, and that will impede its acceptance. SetCo has an opportunity to address many of SET's shortcomings in the new SET-2 standard.

DigiCash vendors have dramatically lowered the cost of providing DigiCash service. Mark Twain International Markets in St. Louis, for instance, has reduced the cost of providing a single DigiCash transaction to 1.9% of purchase price and a $50 annual fee, making its system comparable to a credit-card transaction system. Mark Twain has not released detailed information about the costs of processing those transactions, so we can only guess at the complete cost of DigiCash transactions, but evidence indicates that they are substantially more expensive than other forms of electronic commerce. (See *http://www.digicash.com* and *http://www.marktwain.com* for more information.)

A number of new electronic commerce systems have been proposed. One of the most interesting is Digital Equipment Corp.'s MilliCent system for microtransactions (*http://www.millicent.digital.com*). While MilliCent provides only money atomicity, it is one of the most aggressive uses of microtransactions to date.

For more detailed information on developments in electronic commerce and related areas, take a look at the extensive set of links maintained by Hal Varian at UC Berkeley (*http://www.sims.berkeley.edu/resources/infoecon/*). Additional information, including technical details of the systems discussed in the article, is available at my Web site (*http://www.cs.cmu.edu/~tygar/*).

previously appeared in [38] and [39]).

- Nevin Heintze, who contributed to the later development of cryptographic postage indicia as represented in [11]); and Ali Bahreman, who started me thinking about certified delivery in [1].
- Ben Cox, Tom Wagner, and Marvin Sirbu, my collaborators in the NetBill protocol; see [27].
- Jean Camp, who made an initial division between money atomicity and goods atomicity; see [6].
- Thomas Alexandre, Brad Chen, Howard Gobioff, Mike Harkavy, Maurice Herlihy, David Johnson, Michael Rabin, Mahadev Satyanarayanan, Sean Smith, Alfred Spector, Jiawen Su, Mark Tuttle, Jeannette Wing, and Hao-Chi Wong, for their useful comments.

I gratefully acknowledge support from various sources for this work: Department of Defense (Advanced Research Projects Agency contracts F33615-90-C-1465, F19628-93-C-0193), IBM, the Information Networking Institute, Motorola, National Science Foundation (under Presidential Young Investigator Grant CCR-8858087 and Cooperative Agreement No. IRI-9411299), TRW, the U.S. Postal Service, and Visa International. Appendix A is drawn from a report that was additionally supported by ARPA contract F19628-95-C-0018. The views and conclusions contained in this document are those of the author and should not be interpreted as reflecting the official policies, either expressed or implied, of ARPA, the National Science Foundation, the U.S. Government or any part thereof, or any other research sponsor.

More information on NetBill can be found at *http://www.ini.cmu.edu/netbill/*. More information on cryptographic postage indicia and secure coprocessors can be found at *http://www.cs.cmu.edu/afs/cs/project/dyad/www/*.

REFERENCES

1. A. Bahreman and J. D. Tygar. "Certified Electronic Mail." *Proceedings of the Internet Society Symposium on Network and Distributed System Security,* pp. 3–19, February 1994.
2. M. Bellare, et al. "iKP Family of Secure Electronic Payment Protocols." *Proceedings of the First Usenix Workshop on Electronic Commerce,* pp. 89–106, July 1995.
3. N. Borenstein. "Perils and Pitfalls of Practical Cyber Commerce: the Lessons of First Virtual's First Year." Presented at Frontiers in *Electronic Commerce,* October 1994.
4. E. Brickell, P. Gemmell, and D. Kravitz. "Trustee-based Tracing Extensions to Anonymous Cash and the Making of Anonymous Change." *Proceedings of the Sixth ACM-SIAM Symposium on Discrete Algorithms*, pp. 457–466, 1995.
5. L. Camp, M. Harkavy, J. D. Tygar, and B. Yee. "Anonymous Atomic Transactions." *Proceedings of the Second Usenix Workshop on Electronic Commerce,* pp. 123-134, November 1996.
6. L. Camp, M. Sirbu, and J. D. Tygar. "Token and Notational Money in Electronic Commerce." *Proceedings of the First Usenix Workshop on Electronic Commerce,* pp. 1–12, July 1995.
7. B. Cox. *Maintaining Privacy in Electronic Transactions*. Information Networking Institute Technical Report TR 1994–8, Fall 1994.
8. B. Cox, J. D. Tygar, and M. Sirbu. "NetBill Security and Transaction Protocol." *Proceedings of the First Usenix Workshop on Electronic Commerce,* pp. 77–88, July 1995.
9. H. Gobioff, S. Smith, and J. D. Tygar. *Smart Cards in Hostile Environment*. CMU-CS Technical Report CMU-CS-95-188, September 1995.
10. J. Gray and A. Reuter. *Transactions Processing: Techniques and Concepts*. Morgan Kaufmann, 1994.
11. N. Heintze, J. D. Tygar, J. Wing, and H. Wong, "Model Checking Electronic Commerce Protocols." *Second Usenix Workshop on Electronic Commerce,* pp. 147-165, November 1996.
12. N. Heintze, J. D. Tygar, and B. Yee. "Cryptographic Postage Indicia." *Concurrency, Parallelism, Programming, Networking, and Security.* Springer-

Verlag Lecture Notes in Computer Science 1179, pp. 378-391, December 1996.

13. IEEE Spectrum, *Special Issue on Electronic Money.* February 1997.
14. S. Itkin and J. Martell. *A PDF417 Primer: A Guide to Understanding Second Generation Bar Codes and Portable Data Files*. Technical Report Monograph 8, Symbol Technologies. April 1988.
15. S. Kent. RFC 1422: *Privacy Enhancement for Electronic Mail: Part II: Certificate-Based Key Management*. Internet Activities Board Request For Comments 1422, February 1993.
16. N. Lynch, M. Merritt, W. Weihl, and A. Fekete. *Atomic Transactions.* Morgan Kaufmann, 1994.
17. M. Manasse. "The Millicent Protocols for Electronic Commerce." *Proceedings of the First Usenix Workshop on Electronic Commerce,* pp. 117–123, July 1995.
18. MasterCard Inc. and Visa Inc., SET Draft Specification.
19. R. Mori and M. Kawahara. "Superdistribution: the Concept and the Architecture." *Transactions of the Institute of Electronics, Information, and Communication Engineers (Japan),* E73(7), pp. 1133–1146.
20. National Institute of Standards and Technology. FIPS 140-1: *Security Requirements for Cryptographic Modules,* January 1994.
21. National Institute of Standards and Technology. *FIPS 180: Federal Information Processing Standard: Secure Hash Standard (SHS),* April 1993.
22. National Institute of Standards and Technology. FIPS 186: *Federal Information Processing Standard: Digital Signature Standard (DSS),* May 1994.
23. B. Neuman. "Proxy-Based Authorization and Accounting for Distributed Systems." *Proceedings of the 13th International Conference on Distributed Computing Systems,* pp. 283–291, May 1993.
24. T. Rabin and M. Ben-Or. "Verifiable Secret Sharing and Multiparty Protocols with Honest Majority." *Proceedings of the 21st ACM Symposium on Theory of Computing,* pp. 73–85, May 1989.
25. R. Rivest, A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." *Communications of the ACM,* 21(2), February 1978.
26. B. Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* Wiley, 1994.
27. M. Sirbu and J. D. Tygar. "NetBill: An Internet Commerce System Optimized for Network Delivered Services." *IEEE Personal Communications,* 2(4), pp. 34–39, August 1995.
28. A. Somogyi, T. Wagner, et al. *NetBill.* Information Networking Institute Technical Report TR 1994–11, Fall 1994.
29. S. Smith. *Secure Distributed Time for Secure Distributed Protocols*. Ph.D. Thesis, Carnegie Mellon University, September 1994.
30. S. Smith, D. Johnson, and J. D. Tygar. "Completely Asynchronous Optimistic Recovery with Minimal Rollbacks." *Proceedings of the 25th International IEEE Symposium on Fault-Tolerant Computing,* pp. 362–372, June 1995.
31. S. Smith and J. D. Tygar. "Security and Privacy for Partial Order Time." *Proceedings of the ISCA Intl. Conference on Parallel and Distributed Computing Systems,* pp. 70–79, October 1994.
32. J. Steiner, B. Neuman and J. Schiller. "Kerberos: An Authentication Service for Open Network Systems." *Usenix Winter Conference,* pp. 191–202, February 1988.
33. J. D. Tygar. "Atomicity in Electronic Commerce." *Proceedings of the 15th Annual ACM Symposium on Principles of Distributed Computing,* pp. 8 - 26.
34. U.S. Postal Service. *Information Based Indicia Program (IBIP) New Direction Metering Technology,* May 1995.
35. Usenix Association. *Proceedings of the First Usenix Workshop on Electronic Commerce,* July 1995.
36. Usenix Association. *Proceedings of the Second Usenix Workshop on Electronic Commerce,* November 1996.
37. Visa USA and Andersen Consulting. *1992 Credit Card Functional Cost Study,* September 1992.
38. B. Yee. *Using Secure Coprocessors.* Ph.D. Thesis, Carnegie Mellon University, May 1994.
39. B. Yee and J. D. Tygar. "Secure Coprocessors in Electronic Commerce Applications." *Proceedings of the First Usenix Workshop on Electronic Commerce,* pp. 155–170, July 1995. ~