CONSUMER PAYMENTS OVER OPEN COMPUTER NETWORKS

by
John Wenninger and Daniel Orlow

Federal Reserve Bank of New York
Research Paper No. 9603

March 1996

This paper is being circulated for purposes of discussion and comment only. The contents should be regarded as preliminary and not for citation or quotation without permission of the author. The views expressed are those of the author and do not necessarily reflect those of the Federal Reserve Bank of New York or the Federal Reserve System.

Single copies are available on request to:

Public Information Department
Federal Reserve Bank of New York
New York, NY 10045

Consumer Payments Over Open Computer Networks

John Wenninger and Daniel Orlow[1]

Introduction

The increasing prospects for large volumes of commerce taking place in "Cyberspace" has created considerable interest in the available technology for making secure payments over open computer networks, commonly referred to as the Internet.[2] These payment initiatives for computer networks rely heavily on encryption technology, and include both cash based (stored value) systems and account based systems (credit card and bank deposit).[3] In this article, we begin with a brief description of the Internet. Next, we look at the encryption technology used to create secure "cyberpayments." Finally, we show how conventional payment instruments could be created using this technology.[4]

Our main conclusions are: (1) currency, check and credit card transactions can all be recreated in an electronic format for use on open networks, with a certifying authority playing a role in this process, and (2) the electronic security for these

[1] The views contained in this paper do not necessarily reflect the position of the Federal Reserve Bank of New York or the Federal Reserve System.

[2] For a general introduction to the issues raised by electronic payments over open networks, see Paul Bauer, "Making Payments in Cyberspace," Economic Commentary, FRB Cleveland, October 1, 1995.

[3] For a detailed discussion of the many efforts now underway to develop payments technology for open networks, see Peter Wayner, Digital Cash, Commerce on the Net, AP Professional, 1996.

[4] For a statement of the Federal Reserve System on electronic commerce and related matters, see, the Testimony of Vice Chairman Alan S. Blinder, The Future of Money, before the House Banking and Financial Services Committee, October 11, 1995.

payment instruments will require a dynamic approach that constantly improves as the computing power and the break-in techniques available to criminals improve over time.

Background

The Internet was designed by the Advanced Research Project Agency of the U.S. Department of Defense to provide a communication medium capable of withstanding nuclear attack. While initially a system connecting governmental and academic institutions, the Internet has expanded beyond its initial design participants and now consists of 45,000 computer networks, 300 Internet service providers, and worldwide user estimates ranging from 30-60 million. It is difficult to assess the number of users as user numbers are estimated based on predictions of average mainframe network size and by average account size. Adding just one additional user by account or network changes the estimate dramatically. However, while these numbers are by no means firm, but they are growing rapidly.

The Internet works as follows. Mainframe computers act as nodes. Each individual computer uses a standard protocol, the Transmission Control and Internet Protocols (TCP/IP), which allows data to be uniformly transmitted between non-affiliated mainframe computers. The common protocol essentially serves as a common language of digital translation, thereby allowing for transmission between any and all points on the network without requiring additional software or hardware.

It is also important to note that the definition of the Internet is itself changing. Smaller computer systems which have their own internal protocols for intra-network transmission often access the Internet through gateways equipped with TCP/IP, thereby allowing inter-network transmission. Whether these networks should technically be considered part of the Internet is unclear. Thus, what the Internet consists of is exactly is open to question, because the range of connected systems and methods for data transmission continue to expand and develop. Nonetheless, a basic definition is that the Internet is comprised of computer and data transfer systems which rely on, use, or have access to TCP/IP equipped computer systems.

Due to its design, the Internet has two principal features which make it potentially attractive to consumers and merchants. First, access is open, easy, and inexpensive, involving the linking of a personal computer to one of the many mainframe computers that route messages through the system. Second, the network is resilient, in that it does not rely on any central computer to route messages. Messages can be processed and forwarded even if an individual mainframe that supports the network is not operational.

From a security perspective, however, these two features represent problems for making secure payments. Payment messages could be intercepted and altered or duplicated. Open access also implies that senders or receivers of payment messages might misrepresent their identity. We turn next to a discussion of the basic encryption technology that can be used to deal with these problems.

Encryption

For the most part, these electronic payment arrangements rely on message encryption (encoding and decoding) technology. This technology, private and public key encryption, is the first line of defense against the interception, duplication, and alteration of a payment message.[5] This approach is designed both to keep the contents of the message secret and to enable the receiver of the message to verify the identity of the sender independently.

To accomplish these dual goals of message secrecy and sender identification, both the sender and the receiver must each establish an unique set of private and public keys. A key is a parameter within astandardized algorithm which the user can select. The public and private key pair are large or mathematically difficult prime numbers. Since prime numbers cannot be factored, a private key solution must be completely accurate or it will not unlock the message. The most common key systems are based on large primes, elliptical curve systems, or discrete logarithms.

An individual's private key is kept absolutely secret, while his public key is made readily available to anyone who might want to send him a message. The message would be coded (but could not be decoded) with the public key. The

[5] Public key encryption ("PKE") is also called asymmetric key encryption, while private key encryption is sometimes referred to as either symmetric or DES encryption. DES stands for Digital Encryption Standard, the most commonly used basis for symmetric encryption systems. For a detailed discussion of encryption technology, see Bruce Schneier, Applied Cryptography, Wiley and Sons, 1995; see also, "Answers to Frequently Asked Questions About Today's Cryptography", RSA Laboratories (1993). For additional details as to the theory of public key cryptography, see Martin Hellman, "The Mathematics of Public Key Cryptography", Scientific American, August 1979.

receiver would then use his private key to decode the message; only the receiver's private key would be capable of decoding the message.

The private key also is used to create a digital signature which further reinforces the goals of secrecy and authenticity. The digital signature can be verified by anyone with access to the matching public key. Chart 1 illustrates the sequence of how this dual-key technology can be used to send a secure, sender-identifiable message. First the sender creates the message to be delivered to the receiver. The sender encodes the message using the receiver's public key (R+). A computer process then condenses the unencoded message to a unique sequence of uniform length. The sender then creates a digital signature by signing the condensed message using the sender's private key (S-). Both encrypted message and the digital signature are then sent to receiver.

When the message arrives at the receiver's location, the receiver first verifies the identity of the sender by taking the sender's public key (S+) and reading the digital signature. The public key (+) can only recognize the signature created by the corresponding private key (-). The receiver then uses the condensing algorithm to verify the relationship between the condensed message and the encrypted message. If the condensed message cannot be verified mathematically, then the message is discarded as either the product of alteration or faulty transmission. Once the sender's identity has been established, the receiver proceeds to use his own private key (R-) to decode the message (which had been encoded originally by the sender in the receiver's public key).

As Chart 2 shows, this dual-key technology creates a logical structure, in which each key can either encode or decode a given message, but cannot do both. The dual elements of sender's message of "R+/S-" are analogous to the features of a bank safety deposit lockbox. Like a lockbox, two keys, one held by the bank (the public key) and one held by the owner (the private key) are needed to open the box/message.

However, due to the computational structure of PKE, only the non-encoding key can be used to decode. In terms of the lockbox analogy, the lockbox ("R+/S-") can only be unlocked by using the reverse keys of "R-/S+". This logic allows a message to be delivered securely (without someone else reading it) and the identity of the sender to be independently verified.[6]

PKE only works as long as the (1) there is confidence that the public key holders are who they claim to be, (2) a private key cannot be determined from an intercepted message, and (3) private keys cannot be stolen. The first security threat,

[6] Digital signature here refers to a technical application, which increasingly has legal significance. In assessing a signature's validity, "[t]he question always is whether the symbol was executed or adopted [i.e. signed] by the party with present intention to authenticate the writing." U.C.C. Article l, §. 1-201(39), and Comment. See generally, Digital Signature Guidelines, Draft, American Bar Association, Information Security Committee, Electronic Commerce and Information Technology Division, Science and Technology Section, October 5, 1995. See also Comptroller General of the United States, Matter of National Institute of Standards and Technology, Use of Electronic Data Interchange Technology to Create Valid Obligations, December 13, 1991, File B-245714 (digital signatures will meet standards for handwritten signatures). Several states have enacted or considering digital signature legislation.

certainty of electronic commercial identity, is addressed by use of a recognized and trusted certification authority. The second concern, message integrity, is addressed by the computational and mathematical difficulty of PKE. The answer to the third involves key management, and securing the private key from outside attacks and internal misfeasance. Next, we explore each of these security problems in more detail.

Role of the Certification Authority There are no handshakes in cyberspace. Confidence in party identity is the most important issue for electronic commercial security after technical issues of message security. This final element to designing reliable message transmission is established by use of digital certificates which are appended to the digitally signed and encrypted message. These certificates are issued by certification authorities (CAs), the linchpin of reliability in electronic commerce.[7]

In its most basic form, a digital certificate is a participant's public key signed by the CA with the CA's private key. Certificates are digital documents that can contain as little as a public key and name, but typically contain the expiration date of the key, the issuing CA's name, the serial number of the certificate, and the digital signature of the CA. By including this information--and possibly more-- a message recipient can verify a digital signature and the digital certificate. Certification indicates that the participants are who they purport to be. The CA's signature itself

[7] See Michael S. Baum, Federal Certification Authority Liability and Policy, National Technical Information Service/U.S. Department of Commerce (1994).

can also be verified, by using the CA's public key to check the CA's "official digital signature."

A number of entities might conceivably provide CA services. Major credit card companies might function as a CA for their membership. In a sense, they already perform this function by giving the merchant the ability to check the validity of a credit card on-line before each transaction is completed. The U.S. Post Office is also considering a CA role for electronic mail messages, possibly during this calendar year. Generally, an organization seeking to serve in a CA role will have to enjoy both the resources to develop the operational system, and as the confidence of potential users. In the case of processing transactions, major credit card companies have experience. However, if electronic commerce is essentially an information delivery system, then the Post Office might offer certain advantages, such as thousands of physical locations where participants could register their identity.

Chart 3 illustrates the components of an encrypted message. First, the message text is created. This text is then condensed, and the digital signature is added by the sender signing the condensed message with his private key (S-). The digital certificate from the CA is added, along with the full message text encrypted with the receiver's public key (R+). The three message elements of (1) encrypted message, (2) digital signature, and (3) digital certificate are then sent as a single message to the receiver.

Upon receipt, the process is reversed. The receiver decodes the composite message using the sender's public key, verifies the digital certificate using the CA's public key, verifies the sender's digital signature using the sender's public key, and then decodes the message text using receiver's private key. The receiver establishes message integrity by making certain that the composite message and the full message text agree. If they disagree, the receiver can assume the message had been tampered with.

The potential importance of the CA in this process is significant. The CA addressess the commercial needs for legitimacy, authentication, and efficiency. First, the CA issues the certificates attesting that the public key and the user are uniquely co-identified. This belief in legitimacy is an essential element that creates a belief in the reliability of the system. Moreover, without certification, neither a merchant nor a consumer can transact business premised on PKE technology. The CA, in short, establishes commercial identity on the Internet.

Second, the CA publishes and distributes public keys. Centralizing these administrative functions simplifies key management and creates efficiencies for electronic commercial transactions. In a sense, the CA offers a type of information clearinghouse for electronic commerce participants.

Third, the CA is essential to creating a digital signature. As discussed above, digital signatures help provide certainty of the sender's intent to transact. The digital signature is partially based on use of the sender's digital information, at minimum the use of sender's private key. Decrypting the signature requires a public key, and public keys are organized and certified as reliable by the CA.

In sum, PKE together with a robust CA system helps address and reduce the Internet's principal design and transactional security weaknesses. PKE provides message integrity and CA's help establish message authenticity. Each complements the other. However, the system is still open to other sources of attack.

Public Key Attacks Public and private keys can be used to encrypt and decrypt messages because the keys are mathematically related. Creating the mathematical relationship between the keys involves the use of a computation which creates an inverse relationship between the keys. Only the creator of the key pair knows the mathematical relationship and the parameters used to create it.

The relationship between the encrypted message and the decrypting key is often compared to opening and closing a trap door. After the message passes through the trap door (encrypted by using the public key), an intercepting party could have both the encrypted message and the public key. However, the trap door is not sprung and the actual information is not released unless the precise key, the inverse private key, is used. Without this information regarding both the algorithm and the inverse relationship, it is both theoretically and practically difficult to compute the decoding key.

However, just because the decoding key is secret initially does not mean it will remain secret. For instance, people with access to the private key might by design or by accident breach private key security. Alternatively, one could use powerful computers and mathematical programming to solve for the key solution. This process, called factorization, is both expensive and time-consuming.[8]

In addition, the reward for the solution is uncertain unless inside information is available. Until actual decryption occurs, there is no way to know what the payoff might be. For instance, it makes little sense to produce a one-time solution to a hypothetical consumer transaction where the computation costs will likely be a very large amount, and the credit card number obtained might be a very small amount remaining against the credit limit. Moreover, the solution would only be one key pair. Therefore, securing a message with a computationally difficult mathematics problem may provide adequate security because the time and cost are not justified given the uncertainty of the outcome.

Whatever mathematical procedure is used to generate the key pair and message, encryption experts are quick to point out that they cannot prove that the relationship cannot be broken. For example, a new technique for solving a difficult mathematics problem such as factorization might be discovered.[9] Encryption

[8] For a short discussion of factorization, computational infeasibility, and the issue of computing power advances and the costs for breaking secure codes, see Andrew Odlyzko, "The Future of Integer Factorization", AT&T Laboratories, Murray Hill, New Jersey, July 11, 1995.

[9] See e.g., Paul C. Kocher, "Cryptanalysis of Diffie-Hellman, RSA, DSS, and Other Systems Using Timing Attacks", December 7, 1995 (security systems may retain vulnerability to timing attacks used to determine encryption mechanism). Overall security for an open communications network is, of course, much more complex than indicated by the three security issues listed above. For a brief introduction to the range of security issues, see Afterward by Matt Blaze in

(continued...)

problems that had been virtually impossible to solve would become simple computational questions. Alternatively, more powerful computers might be developed, allowing high-speed, iterative techniques for factorization and decryption. These types of breakthroughs could result in a systemic attack because all the private\public key combinations could be derived. Therefore, message security is likely to be a dynamic process, requiring constant vigilance and change as technology evolves.

An additional aspect of factorization is the inherent tension between law enforcement and national security concerns, and cryptography. Larger primes yield increases in computational difficulty. However, there are national security concerns over the size and use of cryptographic systems. Thus, while increasing the size of public key systems might answer certain commercial security concerns, national security places constraints on the type of cryptography available for use and export. Moreover, there are additional concerns about the use of cryptography by criminals seeking to hide illegal activities (and profits) from law enforcement officials. [10]

(...continued)
Bruce Schneier, Applied Cryptography. Also see R.J. Anderson, "Why Cryptosystems Fail", Communications of the ACM, v. 37, n. 11, November 1994 at 32-40.

[10] See e.g. Testimony of Raymond G. Kramer, Deputy Director, National Institute of Standards and Technology; before the House Committee on Banking and Financial Services, Subcommittee on Domestic and International Monetary Policy. October 11, 1995 ("Encryption can frustrate legally authorized criminal investigations by the federal, state, and local law enforcement agencies . . . lawful electronic surveillance has proven to be one of law enforcement's most effective investigative techniques available to investigate serious criminal activities.")

Key Management PKE systems and CAs address technical and organizational elements of electronic commerce. However, the most significant security concerns are those of key management and the security provided by people with access to a private key. Accordingly, robust key management practices depend on system controls and design to eliminate opportunities for error or crime by those with private key access. For instance, responsibility for private key access and use is predicated on security protocols in both physical and hierarchical authorization procedures to prevent outside access and insider mis- or malfeasance. A PKE system, in short, is only as strong as its private key security.

There are additional elements to key management. System design is an integral element of access security. Whether a participant would rely on hardware or software applications will depend on the anticipated scope and volume of electronic commercial activity. Generally, as the amount of value increases, the emphasis on hardware solutions also increases. Hardware solutions may be appropriate and even standard for private key security, including physical immobilization and control as a security feature.

System architecture is essential to guarding and strengthening the electronic commercial transaction platform.[11] System design begins with private key control,

[11] For additional discussion of key management and system protection issues, see Frederick C. Cohen, Protection and Security on the Information Superhighway pp. 44-54 (1994). See also D.W. Davies and W.L. Price, Security for Computer Networks (1984) (for an introduction to the data security in teleprocessing and electronic funds transfer).

but also includes physical and procedural elements to prevent unauthorized access to data and systems control. Chart 4 illustrates five aspects of system design.

(1) A filter/router system which intercepts certain types of messages and prevents their passage through to the receiver's computer where damage or theft could be done.

(2) Firewalls which allow access to the computer services offered, a World Wide Web page or electronic mail for instance, but limit that access to the designated applications.

(3) Barriers which act like a filtering router service, but block access from certain senders but not others.

(4) System partitions which are used in conjunction with the above, but limit internal and external access within the receiver's computer. Segmentation operates as a form of internal barrier or firewall to limit internal users' physical and application intra-system access.

(5) Unconnected devices that are used to make security calculations and store sensitive information "off-line."

These elements of security architecture limit outside access to particular computer activities. Another option is to store sensitive information and make sensitive calculations on unconnected devices, loading the information onto an active system only when actually needed. These and other elements of design architecture provide technical and procedural guards both for incoming and outgoing messages. Using security architecture, viruses, 'hacking', general server attacks, information theft, and fraudulent messaging can be addressed and controlled.[12]

[12] See Mitre/NIST, Public Key Infrastructure Study (1994) (copy on file with authors).

Payment Instruments

Next, we will illustrate how this dual-key technology can be used to construct common, retail payment instruments in a secure, electronic format. Our illustrations are examples of the underlying logic only; they are not intended to represent any individual developer's product, which could vary somewhat in the details.

Electronic checks. A paper check is basically a message to a consumer's bank to transfer funds from his account to someone else's account. This message is not sent directly to the bank, but rather to the intended receiver of the funds who must arrange to collect the funds. After the funds have been transferred, the cancelled check is returned to the sender and can be used as proof of payment. Can an electronic check replicate all the features of a paper check?

Chart 5 illustrates the steps that would be involved in sending an electronic check. Chart 5 is similar to Chart 1 except that a third party has been added, the bank. The sender would create the electronic check by encoding the sensitive information (his account number, the dollar amount, etc.) by using the intended receiver's public key. The sender would then endorse the check using his private key. The receiver would verify the signature on the check by using the sender's public key and would decode the sensitive payment information using his own private key. He would then endorse the check using his private key, and recode the original sensitive information, along with his account number, using the bank's public key. When the bank received the electronic check for deposit, the bank would verify both the receiver's and the sender's signatures using their public keys and would decode the sensitive information (dollar amount of the transfer and account numbers of the sender and receiver) using its own private key.

If everything was in order, the bank at this point would transfer the funds indicated on the check. The bank would certify the funds transfer by using its private key to sign the check. Finally, the bank would recode the information using the original sender's public key and return the cancelled check to the sender. The cancelled check would contain the payment information and the unique digital signatures of the receiver and the bank, creating the basic proof the original sender would want to retain for his records that the payment was made.

In virtually all respects, the electronic check can accomplish what the paper check does.[13] It functions as a message to the sender's bank to transfer funds, but like a paper check, the message is given initially to the receiver who, in turn, endorses the check and presents it to the bank to obtain the transfer of funds. The electronic check, however, could turn out to be superior to the paper check in one respect. The sender could encode his account number with the bank's public key (rather than the receiver's public key). In this way, the sender would not need to reveal his bank account number to the receiver, an additional level of security the paper check cannot offer.

[13] On September 21, 1995, the Financial Services Technology Consortium, a group of banks, technology companies, and governmental agencies, arranged for the sending of flowers to Vice President Gore, and paid for the transaction by electronic check.

Next, we turn to electronic credit card transactions and electronic cash transactions. These are illustrated in the fourth chart in somewhat less detail than the electronic check because the concept of dual-key technology should be familiar by this point.

Credit card. In a credit card transaction, the consumer presents preliminary proof (his credit card number) to the merchant that a bank is willing to extend credit to the consumer and pay the merchant. The merchant can verify this with the bank and create an instrument for the consumer to endorse. The merchant then uses this instrument to collect from the bank, and the consumer receives a statement from the bank on the next billing cycle with a record of the transaction. The consumer also receives a receipt from the merchant at the point of sale.

The top part of Chart 6, labeled "account based" illustrates how the dual-key technology can be used to securely charge a purchase to a credit card account. Suppose the consumer purchased some software from the merchant for $100. The merchant would create an invoice for that amount stating the details of the sale in plain language in much the same way a merchant would for a conventional credit card transaction. The merchant would also encrypt that information and his account number using the bank's public key, sign the invoice using his private key, and then forward the message to the consumer. The consumer would read the plain language part of the message and, if accurate, would encrypt that information and his account number, also using the bank's public key. The consumer would also verify the identity of the merchant by checking the merchant's signature using the merchant's public key. The consumer then signs the message using his private key, and returns the message to the merchant. A copy can be kept for the consumer's records as a receipt. The merchant could verify the consumer's signature using the consumer's public key and would assume the consumer had agreed to the terms of the sale (at this point, the merchant can only assume the consumer encoded the correct information because the information is encoded in the bank's public key which the merchant cannot read). The merchant would then forward the invoice to the bank.

The bank, in turn, would use the merchant's and the consumer's public keys to verify the signatures and the bank's own private key to obtain the terms of the sale as recorded in the bank's public key by both the merchant and the consumer. If both the merchant and the consumer have encrypted the same information, the bank would check the consumer's credit line and, if the consumer qualified for the additional credit, charge the $100 to the consumer's credit card account and retain other information regarding the software sale for inclusion on the consumer's monthly statement. Finally, the bank would arrange for the merchant to receive payment.

If the consumer did not qualify for the additional extension of credit, the bank would return the message to the merchant with a rejection notice encrypted with the merchant's public key and endorsed with the bank's private key. This authentication process occurs on-line now for most credit card transactions, but takes place before the consumer endorses the instrument. In an electronic credit card transaction over an open network, the card itself is not used to identify the consumer; hence all the information must be made available to the bank on the encoded message.

It would, of course, be much simpler for the consumer to just encode his credit card number with the merchant's public key and sign the message with his own private key and send the information directly to the merchant. While catalogue transactions are often made this way currently, this approach might not work well over a large, open computer network on which many merchants might not be well known to the consumer. The consumer could be revealing his credit card number to the merchant without knowing how safe the information would be kept. In addition, the consumer would be trusting the merchant to charge the correct amount to his credit card account. The more complex approach outlined here allows the consumer to keep his account number confidential, and the consumer's bank makes the actual charge to the consumer's account after verifying the amount from both the merchant's and consumer's perspective. These additional safety features may be worth the additional complexity.

As with the electronic check, the dual key technology can be used to securely make a credit card transaction and retain the relevant information about the terms of the sale for later use. In this case, the bank has paid the merchant, but given the consumer credit based on a document created by the merchant and endorsed by the consumer, similar to the way conventional credit card transactions are processed.

Electronic credit card transactions could turn out to be better than current credit card transactions because the consumer would not need to reveal his credit card number to the merchant.

Electronic Currency. This form of electronic payment is illustrated in the lower panel of Chart 6. The consumer initially obtains an electronic note from his bank by paying the bank from his checking account. The bank creates the electronic note by inputting the relevant information (dollar amount, serial number) and endorsing it with its digital signature, using the bank's private key. The bank records the serial number and the face value of the note before sending the note encrypted with the consumer's public key on to the consumer.

The consumer decodes the note using his private key and then verifies the dollar amount and the endorsement using the bank's public key. The consumer then encodes the note with the merchant's public key, but would not endorse the note with his private key if he desired to remain anonymous (one of the key attributes of cash payments). Upon receiving the note, the merchant would use his private key to decrypt the note and would use the bank's public key to verify the face value and the bank's endorsement.

Finally, the merchant would encode the note using the bank's public key and send the note to the bank for deposit. The bank would decode the note using its private key and check the face value and serial number to determine if this note had been deposited before and hence might be counterfeit. If the note was legitimate, the bank would deposit the value into the merchant's bank account.

Unlike the electronic check and electronic credit card payments outlined above, electronic currency like paper currency must be withdrawn from the bank before the payment can be made. Similarly, paper currency and electronic currency both allow for anonymous payments from the consumer to the merchant, while conventional and electronic credit card and check payments do not permit anonymity. In addition, methods have been developed to enable the consumer to obtain the electronic note from the bank without the bank recording the serial number and with alternative mechanisms for the bank to detect counterfeit notes. These cash systems, however, become quite complex and require sending and processing considerably larger amounts of information.[14]

One important difference, however, may develop between electronic currency and paper currency. While it is not safe to send paper currency through the mail, encryption technology may make it safe to send electronic currency over open networks, no longer limiting currency to a point-of-sale payment instrument.

Conclusions The attraction of the Internet lies in its open access and durability--anyone virtual and virtually anyone can use the Internet. However, these same design strengths also create security weaknesses. Encryption techniques used for keeping

[14] For greater detail, see David Chaum, "Achieving Electronic Privacy", Scientific American, August 1992, pp. 96-101.

messages secure on an open network can also be adapted to create electronic forms of the payment instruments commonly used by the consumer sector, including currency, checks, and credit cards. The role of the certifying authority is signficant, and will likely continue to be refiend and developed. However, without adequate security, and without a certifying authority, consumers and merchants will not have the confidence to use these payment mechanisms for electronic commerce.

The greater computing power now available at low cost can be used to provide high levels of security. But that same computing power (along with more sophisticated 'hacking programs') will be available and used --eventually-- to attempt to break through those same security systems: an economic incentive will be created for criminal activities if large amounts of monetary value are flowing over a network.

Nonetheless, if enough potential profit exists in virtual commerce, techniques could be developed for making secure payments over the Internet. But these techniques cannot be static, because the attacks will change as both the technology and the technology infrastructure develop. Constant vigilance and innovation in security will be needed, and refinements in both technological and the human element of key management will probably become the standard of practice for electronic commerce participants.

Chart 1

PUBLIC AND PRIVATE KEYS FOR MESSAGE ENCRYPTION

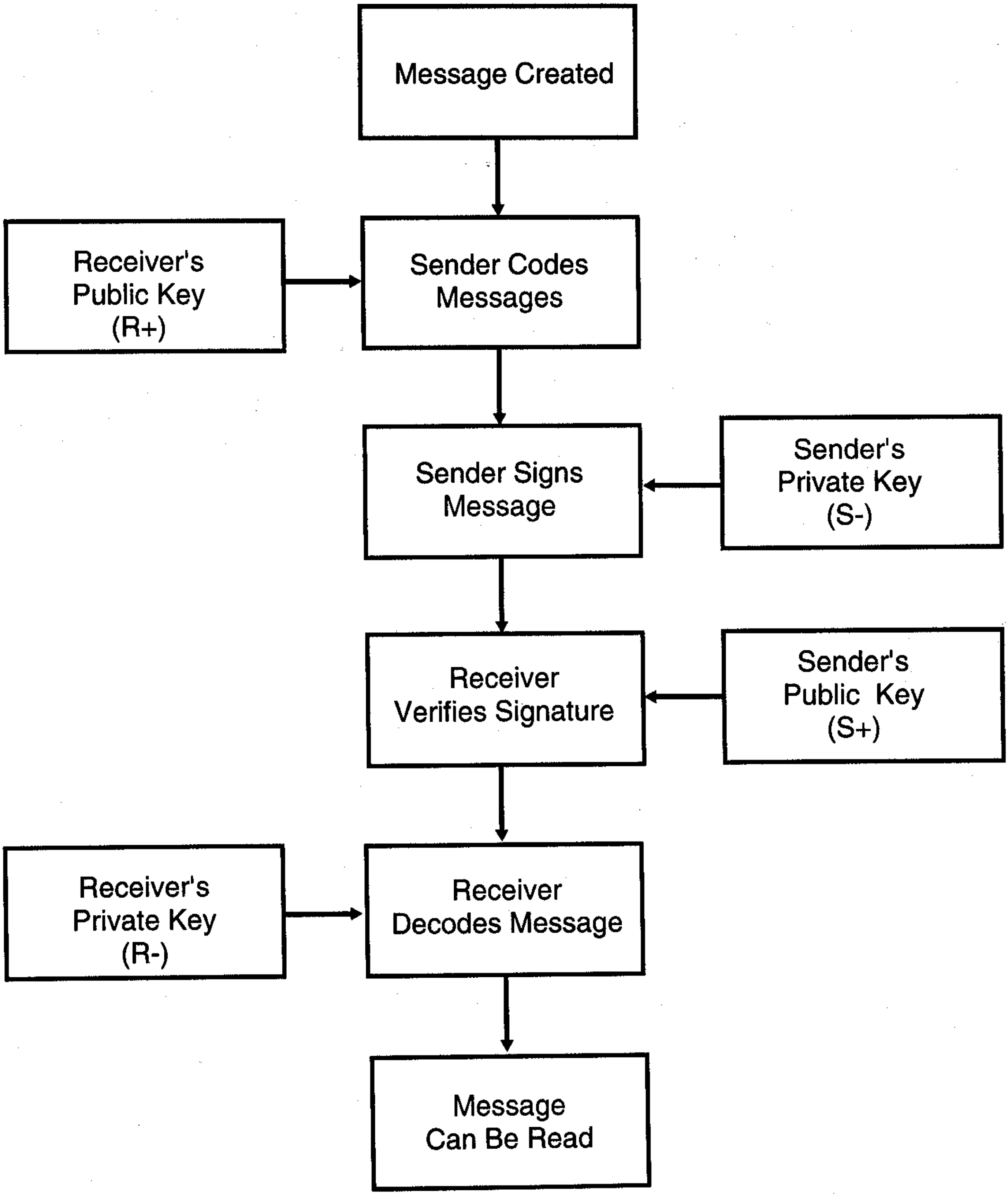


Chart 2

Integrity Structure

Message Text & Digital Signature		Message Text	Digital Signature
		Key Use	
Sender	Encode	R+	S-
Receiver	Decode	R-	S+

Key Code:
Public Key = +
Private Key = -

Chart 3

Message Creation

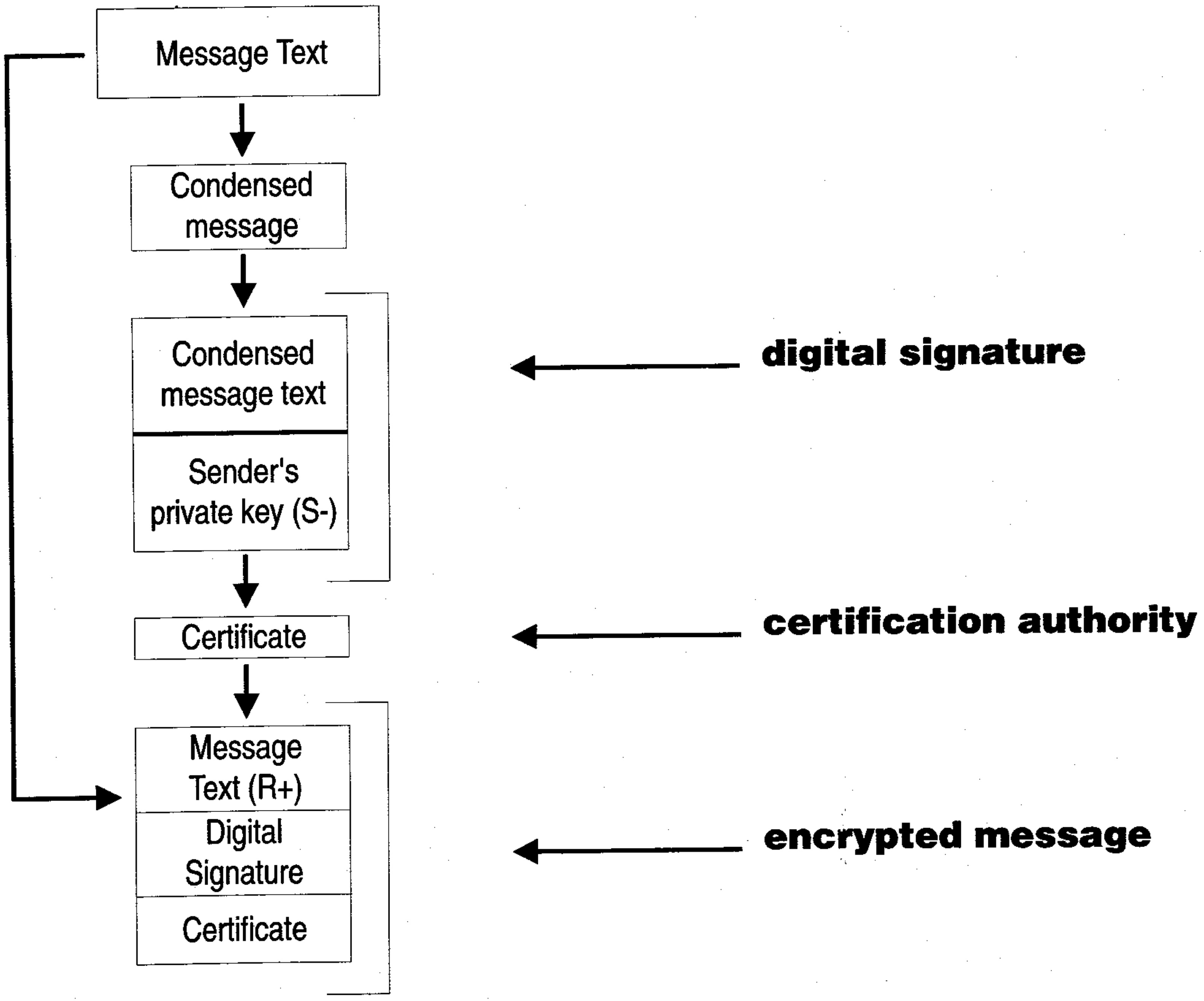


Chart 4

Security Design for Key Management

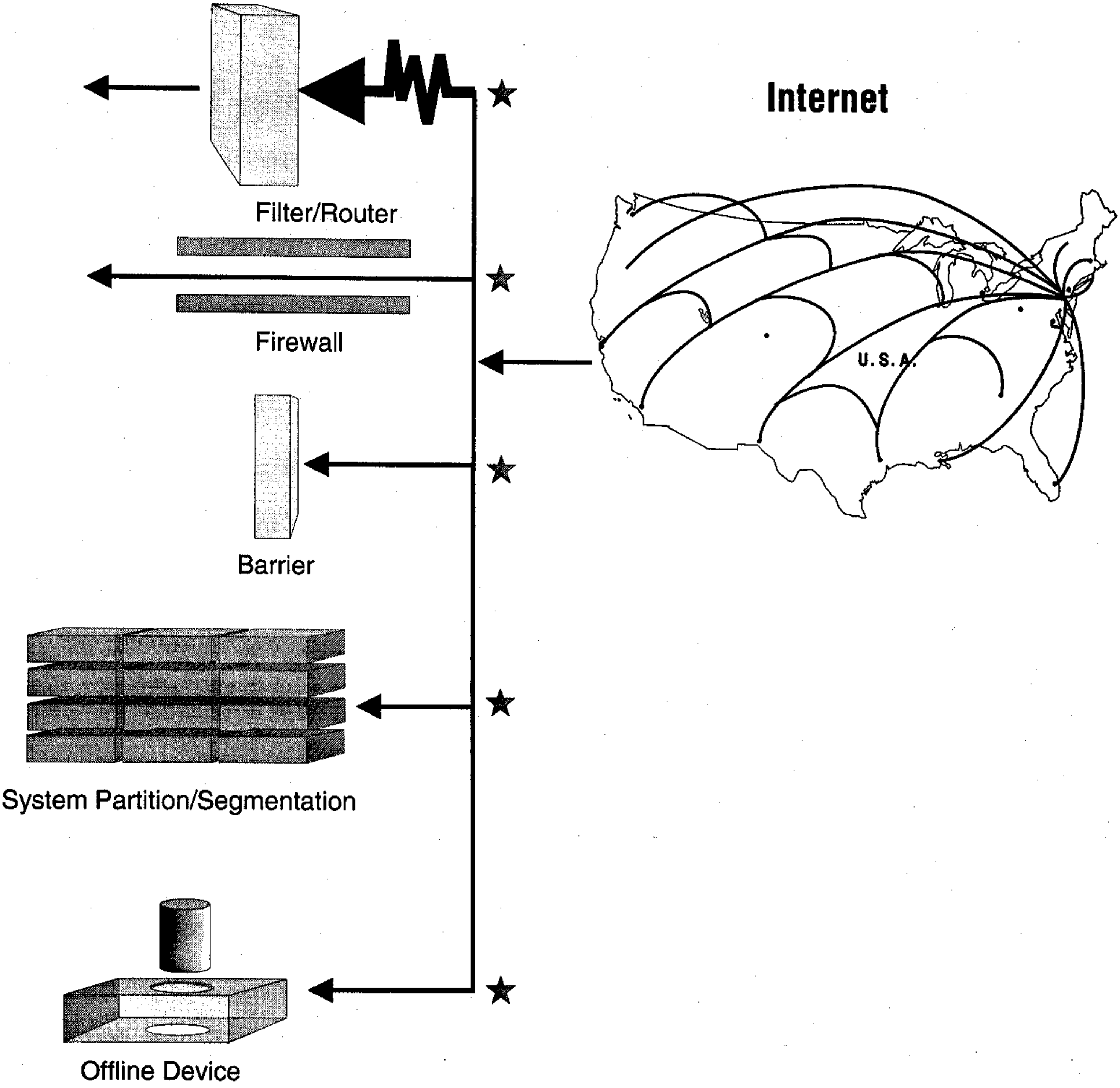


Chart 5

Electronic Checks

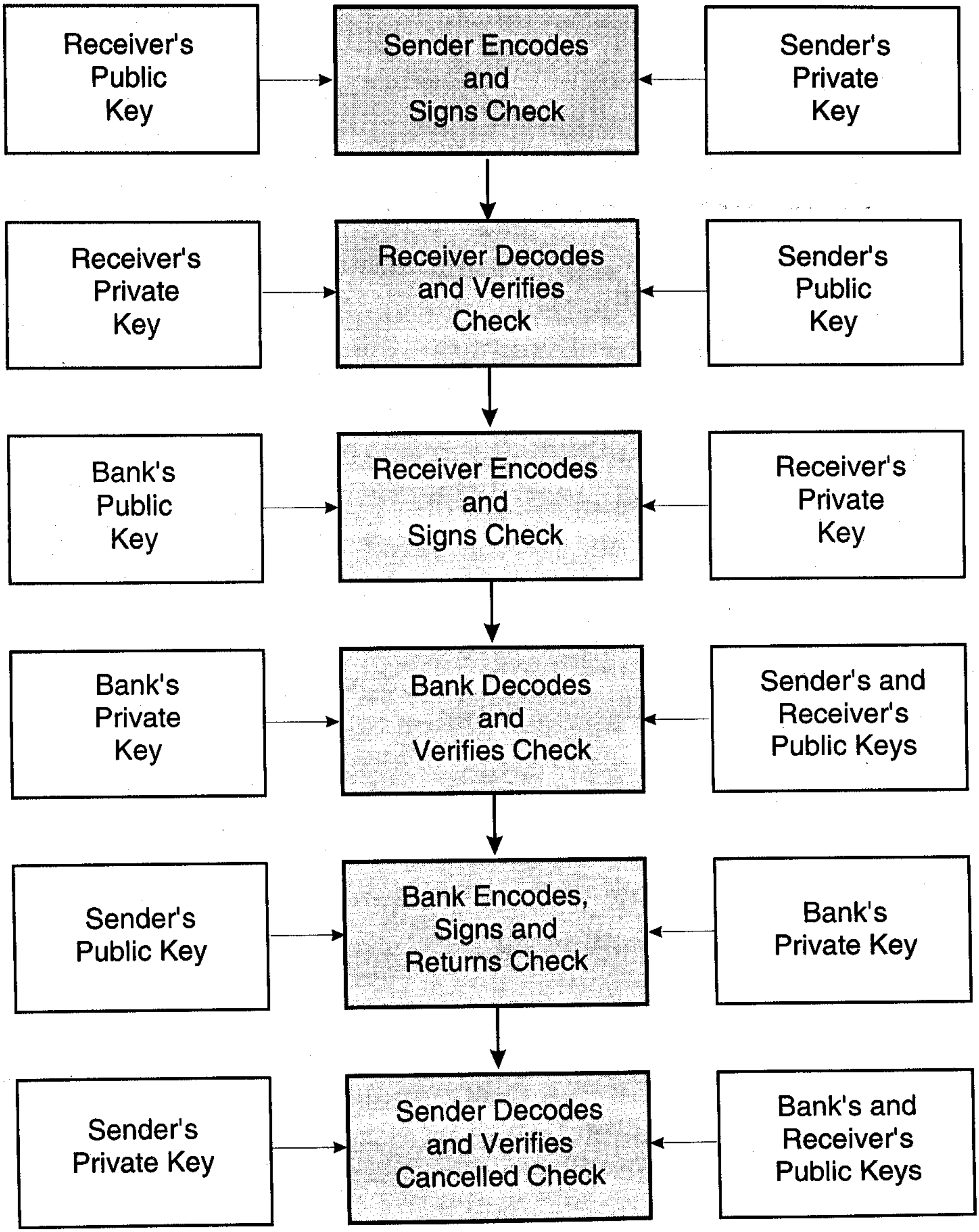
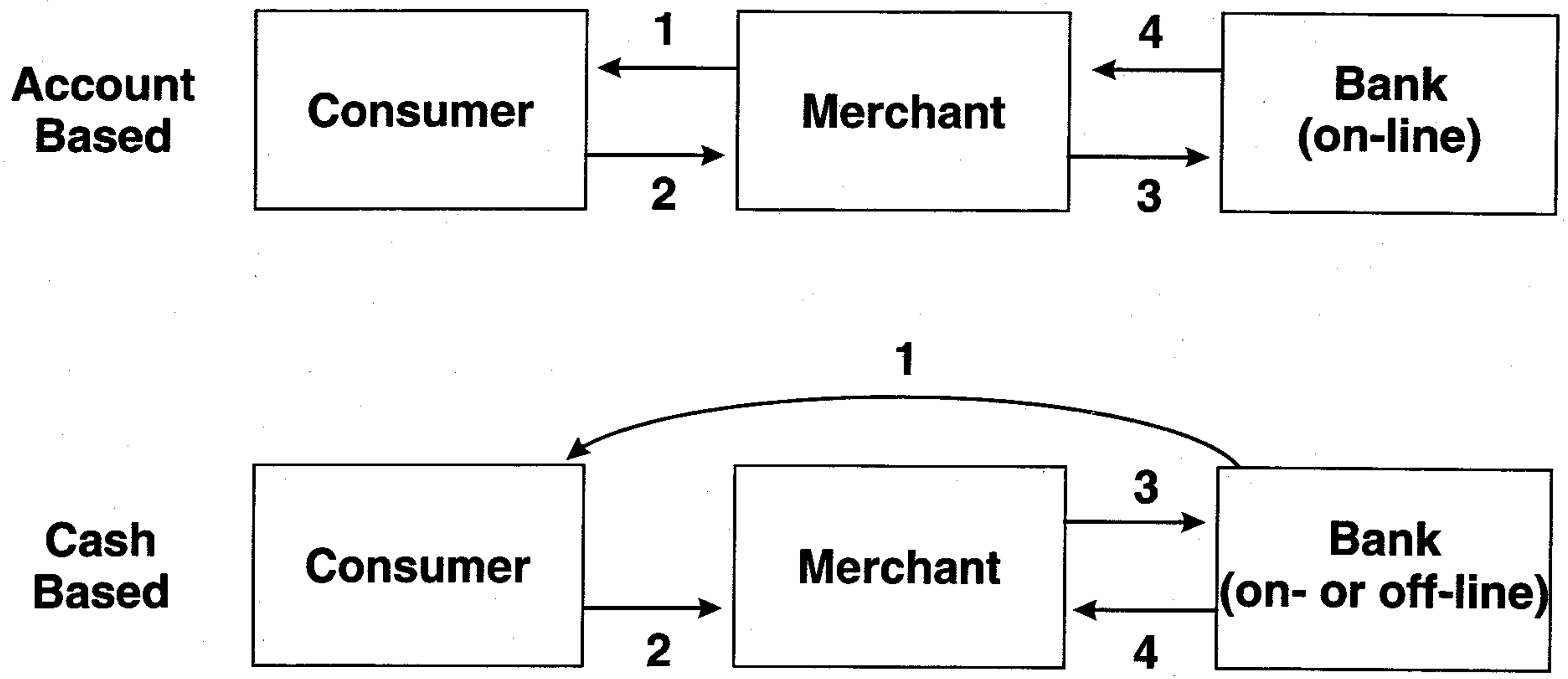

Receiver's Public Key
Sender Encodes and Signs Check
Sender's Private Key
Receiver's Private Key
Receiver Decodes and Verifies Check
Sender's Public Key
Bank's Public Key
Receiver Encodes and Signs Check
Receiver's Private Key
Bank's Private Key
Bank Decodes and Verifies Check
Sender's and Receiver's Public Keys
Sender's Public Key
Bank Encodes, Signs and Returns Check
Bank's Private Key
Sender's Private Key
Sender Decodes and Verifies Cancelled Check
Bank's and Receiver's Public Keys

Chart 6

Comparison of Account Based and Electronic Cash Based Value Flows Over Computer Networks


Account Based
Consumer
1
2
Merchant
4
3
Bank (on-line)
Cash Based
1
Consumer
2
Merchant
3
4
Bank (on- or off-line)