Making Payments on the Internet

James J. McAndrews*

The Internet has begun to make the idealized marketplace discussed in economic textbooks seem more plausible. It allows low-cost, speedy, convenient, and informative communication across the world. However, to become an active market in goods and services the Internet must overcome a fundamental hurdle: a way must be devised for buyers and sellers to securely and conveniently exchange payment over the Internet. Software companies and financial institutions are now developing methods that will allow people to pay on the Internet.

*James McAndrews is a senior economist and research advisor in the Banking and Financial Markets section of the Philadelphia Fed's Research Department.

A review of these efforts reveals the importance of security, authenticity, and privacy, which are often overlooked or taken for granted in other instances of making a payment.

Money is an ancient human artifice. For approximately 3000 years coins have been minted in India and Greece. Minting coins for use as media of exchange was a significant improvement over the alternative: exchange of metals by weight for purchases. Coins made a particular amount and quality of metal easily recognizable and hard to counterfeit. Milling the edges of coins made the practice of removing small amounts of metal from the coins very easy to detect. The creation of banks of deposit and their vaults made safeguarding coins easier.

Hence, coins became readily identifiable and transferable, attributes that raw metals did not possess. These attributes made trade easier.

Our society is grappling with ways to create, once again, a way to make payments in a new medium: the Internet. The designers of Internet means of payment have the same concerns that occupied mints centuries ago: how to make the proposed means of exchange easy to recognize and authenticate, but hard to counterfeit and steal. Today's designers work with powerful mathematical means of encryption, which can serve the same roles for Internet payments that minting coins served for earlier payment systems.

Several attributes of a successful medium of exchange—one of money's primary roles—have emerged over the centuries. Money should be identifiable, divisible, easy to transfer (both technologically and in the sense of there being widespread acceptance), and easy to protect against theft. The attempts to create successful media of exchange over the Internet reveal the importance of these attributes as well as the difficulties of successfully designing a system with those attributes.

THE INTERNET

The Internet, a network of computers that use a common method of communication, has experienced rapid growth in recent years. While estimates of Internet size and usage are imprecise, one estimate shows that the number of computers linked to the Internet increased from 213 in August 1981 to 3,864,000 in October 1994 and to 9,472,000 in January 1996. The amount of message traffic across one part of the Internet is estimated to have grown from 85 million packets in January 1988 (a *packet* is approximately 200 bytes; a byte holds one alphabetic character) to more than 60 billion packets in January 1995.[1] The Internet is used to send mail, to transfer files, and—using the World Wide Web—to transmit graphics and sound.[2]

The impressive growth of the Internet has been facilitated to some extent by the steadily declining cost of computers. Furthermore, in many cases, individual users of the Internet (or their employers or sponsoring organizations) pay a fixed fee, or a fee that does not vary with the number of sites from which they gather information, and there is no marginal fee for the use of the network facilities in sending or receiving information. This zero marginal cost of usage makes sending a message across the country essentially free for many users.

The Internet differs from telephone networks in that each message does not have a *circuit* dedicated to it. Instead, a message on the Internet is divided into packets, each with the address of the message attached to it, and the individual packets are sent through computers (known as routers) to their destinations. This *packet switching* method allows many packets to simultaneously share the physical telecommunication lines across which the packets travel. This greatly economizes on the use, and therefore the costs, of telephone lines, relative to telephone calls, which use a *circuit switching* method that dedicates a circuit to a particular call.[3]

This inexpensive and increasingly ubiquitous form of communication and information transmission has made it possible to imagine continuous, worldwide electronic commerce. On the Internet, one can comparison-shop, read

---

[1]The first of the two estimates was made by network analyst Mark Lottor, and the second refers to message traffic across the NSFNET backbone—that part of the transmission lines funded by the National Science Foundation. These estimates are reported by the Merit Network, Inc., a nonprofit corporation providing a number of Internet services.

[2]The World Wide Web is a communications protocol developed for graphical content and sound.

[3]A good discussion of the Internet is given by Jeffrey K. MacKie-Mason and Hal Varian in "Economic FAQs About the Internet," *Journal of Economic Perspectives,* Volume 8, Number 3, Summer 1994, pp. 75-96.

warranties, establish accounts, view images of products, and order goods and services from companies located anywhere in the world. Home shopping on the Internet could reduce the transaction costs of shopping significantly; many believe that it is the "killer app" of the Internet.[4] To flourish as a marketplace, however, the Internet needs a means of payment, but payment over the Internet faces some unique barriers. In particular, the challenge is to devise ways to protect against theft while conveying payment information that is recognized as authentic.

CAN I PAY WITH A CREDIT CARD OVER THE INTERNET?

When I make a phone call to my favorite mail-order catalog to order a pair of shoes, the only parties to the call are the order taker and me. If I were to send an e-mail over the Internet to the catalog company instead, the information may be routed through many computers not party to the transaction before it reaches the merchant, allowing others to intercept my message. If my credit card number is included, others can steal it. Furthermore, if a hacker has infiltrated either the merchant's computer network or the one of my Internet access provider, the hacker could intercept, read, and alter messages. Because of that, I can't be sure that my messages haven't been read or altered after I've sent them. The activity of intercepting and reading others' messages is known as snooping.

While telephone fraud is a big problem, the ease with which criminals can fake e-mail messages of others—someone with sufficient knowledge of computer systems can connect to the victim's mailserver on the Internet and send the fake message from it (an activity known as spoofing)—makes enhanced security a necessity. It is also much easier for criminals

to establish untraceable computer accounts to fraudulently collect credit card numbers (if they were unencrypted). It is much more difficult to do so with telephone mail-order operations.

The real possibility of theft of the information has precluded the widespread use of unencrypted credit card numbers over the Internet. Furthermore, the ease with which criminals can adopt fraudulent identities and untraceable addresses on the Internet deters people from attempting to purchase items over the Internet. Therefore, new means of making payment must be devised.

Designing a method of Internet payments, therefore, requires attention to two features of money that are necessary to securely convey payment information. Authentication of messages is important for both parties to a transaction. Finding a means to prevent eavesdropping is important, so that criminals cannot steal payment-related information, such as credit card numbers, as they are transmitted over the Internet. It may be that secret coding of information can solve both of these problems.

ENCRYPTION

As with all types of money, identification and recognition are necessary before a seller will accept a payment. Payment systems today use various means to identify a payer. In credit card transactions conducted in person, possession of the card and a signature matching the one on its back suffice. For point-of-sale transactions with a debit card, possession of the card and a password identify the account holder. When paying by check, a signature (and often a photo identification card) is necessary. For cash transactions, the currency is examined to authenticate it.

On the Internet this means that correctly identifying the customer and maintaining the integrity of the information are vital. A password—even one that has been encoded by some encryption device—is not enough to identify a person if it is used more than once (because of

---

[4]A killer app is an application of a particular technology that many potential users find irresistible.

the possibility of theft of the password). If an encoded message is used more than once, it could be duplicated and sent by some other person posing as the original sender.

None of the measures used to authenticate the means of payment today are foolproof. Counterfeit currency and check and credit card fraud are significant problems. But the ease with which snoopers can intercept unencrypted messages has led security experts to believe that encryption of financial information is necessary to approach the levels of security that people now enjoy with cash, checks, and routine credit card payments.

Privacy. Securing the integrity of a message sent on the Internet poses a difficult problem. Even when a message is encoded, if criminals were to decode the message, or steal the "key" by which the original message was encoded, the integrity of the message would be lost. With traditional encryption methods the sender and receiver have to share the key to successfully encrypt and decrypt a message. Therefore, the sender has to give the key to the receiver in some way. This makes the management of the secret key extremely difficult because it is much more likely to be stolen as it is shared with many parties (for example, all the merchants that accept a type of credit card) and as it is being communicated to all the parties to a message. Furthermore, with traditional methods of encryption, once someone has stolen the key, messages can be both decoded and encoded. Hence, a criminal, armed with the key, can pose as a legitimate party to the encryption system, and no one could detect the deception.

A new type of encryption was discovered in the 1970s by Whitfield Diffie and Martin Hellman, two American mathematicians. Their contribution to encryption theory was to recognize that systems of encryption can be created that use a pair of keys, one to encrypt the message and another to decrypt it. One type of these "asymmetric" cipher systems is a "public key/private key"cipher (commonly referred to

simply as a public key cipher) in which the encrypting key need not be kept secret to ensure a private message.[5] The decrypting key (the "private key") need never be shared with anyone else and, therefore, is much less susceptible to theft. (See *Keys to Establishing Trust in Cyberspace.*)

Under public key cryptography, if two people wish to exchange private messages, they each create a pair of public and private keys. Alice obtains Bob's public encryption key, uses it to encrypt a message to Bob, and sends it to him. Bob can then decrypt it using his private key. Only someone who has Bob's private key can decrypt messages encoded with his public key. To reply, Bob obtains Alice's public key, encrypts a message, and sends it to Alice. She deciphers the message using her private key. This system of encryption offers a great deal of security in managing the private keys because they never have to be shared with anyone. Clever applications of this type of cryptography can be used to verify identity (using a "digital signature"), authenticate messages, and provide a record of when a transaction occurred— all vital aspects of a trustworthy means of payment on the Internet.

Encryption of electronic financial information traveling across the Internet offers a safeguard against theft of information, and the digital signature offers a way to authenticate the message. Hence, these sophisticated mathematical devices play the roles that other devices that prevent the theft of money—such as vaults, wallets, and commonsense security precautions—and devices that authenticate money—such as watermarks, specially printed paper, passwords, telephone authorization, and signatures—play in other forms of money.

---

[5]A good discussion of public key cryptography is contained in Bruce Schneier's book *Applied Cryptography,* John Wiley and Sons, Inc., second edition, 1996.

APPROACHES TO INTERNET PAYMENTS

There are currently several approaches to offering payment services on the Internet: credit-card-based systems (which represent an extension of credit by the issuer of the credit card to the holder); payment orders (much like a check is an order to one's bank to make payment); or a new form of payment, digital cash.[6] Most use some form of the public key/private key encryption system, but others safeguard financial information in other ways.

Trusted Third Party. At least one firm offers a trusted-third-party method of payment: a customer authorizes the trusted third party to make payments on her behalf. In such a system the customer supplies (over the phone or through the mail) the trusted third party with her credit card number or a voided check and written authorization to effect payment on her behalf. The customer is supplied with a password. As the customer orders a product over the Internet, she supplies the seller with her password; the seller reports this to the trusted third party; and it, in turn, sends to the customer a report of the transaction and asks the customer to confirm it. Once confirmed, the trusted third party conveys the payment information through the automated clearing house system (the electronic interbank system that banks use to exchange small-value payments). This system avoids the problem of eavesdropping, which is a concern in transmitting payment information across the Internet.

The trusted-third-party method offers the benefit of securing credit card or checking account information against theft. It requires, however, sellers as well as buyers to accept payment by the trusted third party; therefore, widespread acceptability is a potentially difficult hurdle for the system. As in all the systems we discuss, the security of the system itself is vital. Such security requires electronic firewalls that cannot be breached by a hacker.

Digital Cash. At least one firm is offering customers the ability to make payments in "electronic," or digital, cash, and others plan to do so.[7] Digital cash consists of messages that use a sophisticated set of variants on the public key/private key encryption system. It is stored on a computer's hard disk and is electronically transferred to a payee. It may also be electronically replenished by transfer from one's account at a participating bank. A digital cash system employs software held by the participating financial institutions, their customers, and merchants. Using that software, the customer creates digital messages that are authenticated by the issuing institution in a way that third parties can recognize. The issuer's authenticated message is returned to the customer and acts as a substitute for cash. A merchant that receives the digital cash can send it on to its bank and have its account credited or it can spend the digital cash.

Digital cash systems typically propose to prevent counterfeiting by virtue of the issuer's digital signature on the digital cash, which verifies its authenticity. Issuers intend to prevent double spending of the cash by "reissuing" or replacing digital cash each time it is spent; participating financial institutions will not accept cash with serial numbers that indicate it has already been spent.

Digital cash has the potential for a feature many believe is increasingly important in an electronic information age: anonymity. In principle, the merchant need not know who is spending the digital cash it receives: the cash is

---

[6]An extensive list of such approaches is maintained by Michael Pierce on the Internet; the address is http://ganges.cs.tcd.ie/mepierce/Project/oninterest.html. There are links at this site to many firms offering some of the services described in this article; those sites typically provide descriptions of the services and plans of the firms.

[7]See "Banks Get the Green Light to Hit the Internet," *Bank Network News,* July 12, 1995.

Keys to Establishing Trust in Cyberspace

Cryptography is the science of hiding the contents of messages from eavesdroppers by means of "secret writing." It has been explored and developed spectacularly in the last quarter of a century—a happy coincidence given the security needs of the world's ever-expanding communication networks. Cryptography can assist in providing the necessary identifiability and protection against theft that a digital or electronic means of exchange requires. But, first, some definitions are needed.

Cipher. A cipher is a mathematical function used for encrypting (or coding) and decrypting (or decoding) a message. One example is the Caesar cipher, in which each letter in a message is replaced by the third letter following it in the alphabet: a is replaced by d, b by e, and so on, with x replaced by a, y by b, and z by c. Modern ciphers use a key, which can take on many values (and are usually very large numbers). The value of the key affects the cipher; for example, the Caesar cipher is a simple substitution of one letter of the alphabet for another, with a key value of 3. If we change the key value to 5, then a is replaced by f, b by g, and so on.

Key. There are two types of key-based ciphers: secret key ciphers, in which the same key is used for encryption and decryption, and public key ciphers, in which a pair of keys is created, one for encryption and one for decryption. In a secret key system, a group that wishes to exchange messages must share the key to communicate but keep it secret from third parties. Secret key, or symmetric, cryptography is most useful for long messages. In a public key system, one of the keys (typically the one used for encryption) can be made public, but the private key (typically the one used for decryption) need not be shared with anyone else. Furthermore, if the keys are chosen well, it is practically impossible to determine the private key even with knowledge of the public key.* Public key systems make *key management*, which refers to the way keys are created, stored, and maintained, much simpler and less susceptible to attack.

Public key systems have many useful features that can aid in authenticating a message, uniquely identifying a person, confirming receipt of a message, and enhancing the privacy of the message. They have the drawback of being costly in terms of computing time and effort, relative to secret key systems, for encrypting and decrypting large amounts of text.
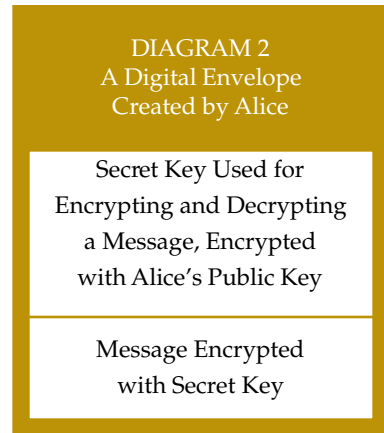
Authenticating a Message. A public key system can assist in authenticating a message by incorporating a "digital signature" in the message. A digital signature is a clever double use of a pair of public key ciphers. Alice, in sending a message to Bob, appends her signature to the message, and she encrypts her signature by means of her private key (usually used for decrypting a message). She then uses Bob's public key to encrypt this "signature" and sends it on to Bob. Bob uses his private key to decrypt the

message and, seeing a potential signature of Alice, uses her public key to decrypt it. Upon successful decryption, Bob realizes that only Alice could have sent the message because only she has the private key counterpart to her public key. Hence, the digital signature has authenticated the message Alice sent to Bob.

Identifying a Person. But how does Bob know that Alice is in possession of her private key? It's possible that an impostor, claiming to be Alice, sent out the public key in Alice's name simply to intercept messages intended for Alice. How then to verify that the person who claims a public key in Alice's name is Alice? A "digital certificate" can serve to verify the identity of the person holding a particular key because it contains that person's name and public key, a digital signature, the name of a trusted *certificate authority,* a serial number, and a set of dates for which the certificate is valid. The certificate authority thereby verifies that the public key in the certificate belongs to the person whose name is attached to it. The process of obtaining a certificate for one's public key requires a high degree of trust and may involve visiting the authority in person and showing proof of identity.

Confirming a Message. Alice can cheat in this system. First, she purchases an item using her credit card and a digital signature and certificate. After she receives the item, she publishes her private key. She then reports that her private key has been compromised, and she did not authorize the purchase. One way to lessen the possibility of this type of cheating is for the receiver, Bob, to have the message *time-stamped* by an authority upon receipt. The time-stamp would be similar to the digital signature of the time-stamping authority and cannot be altered. Alice would have had to declare her private key compromised before the purchase, making it possible for the certificate authority to repudiate its certificate for Alice before Bob receives the message. Diagram 1 shows a digital certificate with a time-stamped message.

Enhancing Privacy. Using public key cryptography for sending a long message would be costly in terms of computing time; therefore, secret key, or symmetric, cipher is preferred. The difficulty lies in how to communicate the secret key, which cannot be revealed publicly without compromising the encryption. Public key cryptography can solve the problem by encrypting the secret key using the public key. Then the secret key would be hidden from everyone except the holder of the associated private key. This encryption of the secret key is called a digital envelope (Diagram 2). Digital envelopes are useful when sending a long message. Most payment messages would not be long enough to require the use of secret key cryptography. The public key cipher could be used directly to encrypt the message.

DIAGRAM 1
Alice's Digital Certificate
Alice's Identifying Information: Name, Organization, Address
Alice's Public Key
Certificate Serial Number
Certificate Validity Dates
Issuing Authority's Digital Signature and I.D. Information
Message with Time-Stamp

DIAGRAM 2
A Digital Envelope Created by Alice
Secret Key Used for Encrypting and Decrypting a Message, Encrypted with Alice's Public Key
Message Encrypted with Secret Key

---

* Decrypting a message in a secret key system requires finding the inverse of the key; for example, in the Caesar cipher one substitutes a letter three places to the left of the encrypted letter to decrypt a message. Finding the inverse of a public key is practically impossible for large keys because it would require extraordinarily large amounts of computing.

authenticated by the bank, not the customer. The merchant might sell an item and be directed to send it to a computer account (if it is a piece of information that can be sent over computer networks) or to a post office box, not knowing who requested it. If the merchant is paid in digital cash and does not know the identity of the holder of the computer account, there is no way the merchant can find out the identity of the buyer.[8]

The concern for privacy is increased today because of the greater ease of compiling information electronically. Many firms sell information on their customers to other organizations for marketing purposes. The enhanced privacy that is possible in a digital cash system comes at a cost of more complex software to run the system.

Credit Card Methods. Visa International and MasterCard announced on February 1, 1996, that they have agreed to jointly develop a standard to solve the problems of snooping and spoofing. American Express later joined the effort as well. The standard is called secure electronic transactions (SET), and it is based on public key cryptography. The developers of the standard will attempt to ensure the integrity of credit card numbers that a cardholder sends to a merchant by encrypting the numbers. Prior to any transaction, however, the developers of SET propose to verify the identity of both merchant and cardholder by having either the bank that issues the card (in the case of the cardholder) or the merchant's bank that processes the transaction (in the case of the merchant) provide both parties with "digital certificates." These certificates may bear the digi-

tal signature of Visa or MasterCard or some certifying authority (see *Keys to Establishing Trust in Cyberspace*). Verifying that the digital certificate does indeed bear the digital signature of the expected certifying authority should help to assure the cardholder that the merchant has a legitimate relationship with a bank and is therefore not attempting to fraudulently collect credit card information for later criminal use. Furthermore, the proposed design for SET seeks to ensure that the merchant will not be able to decrypt the holder's card number; rather authorization from the merchant's bank will ensure payment, and the consumer's number will remain unreadable to the merchant.

Prior to their February announcement, Visa and MasterCard had embarked on creating separate standards for securing credit card transactions on the Internet. The subsequent decision to join forces to create and adopt a single standard will simplify the process of using the software that will operate the standard. With a single standard a merchant will be able to identify itself and secure its payment information using only one system. The decision to jointly develop the system avoided a potentially costly duplication of effort on the part of the card associations, banks, and merchants.

Internet Banking. At least one bank exists primarily for banking on the Internet: it has only a small physical office, but a "virtual branch" on the Internet. While this bank does not offer a direct method of payment on the Internet, it allows its customers to pay bills by writing checks or making an electronic payment through the automated clearing house. This method is a variant of trusted-third-party payments because information flows through private interbank networks.

Other banks and technology companies have created the Financial Services Technology Consortium. This group is sponsoring research into electronic commerce over open networks, such as the Internet. One of their ventures is the electronic check project, an attempt to create a pay-

---

[8]If the merchant were to find that the cash had previously been spent, it would seem to have no recourse, given the cloak of buyer anonymity. However, David Chaum, an expert in cryptography, ingeniously devised a system in which the buyer's identity is revealed only if the buyer attempts to spend the cash twice.

ment method that will be accepted much as a paper check is today. It, too, proposes to rely on encryption to secure account numbers and digital signatures to verify identities, but it will provide access to one's bank account, rather than create digital cash.

ACCEPTANCE OF THE NEW MEANS OF PAYMENT

There are many approaches to payment over the Internet. Will they all survive? It is too early to determine whether the different means of payment are useful and cost-effective, but as in non-Internet-based payments, it may be that different forms of payment may survive for different uses and for different users.

Many competing and complementary means of payment exist today. For example, while credit cards are useful for international and many retail and mail-order transactions, only some merchants are able to accept credit cards (that is, they are "signed-up" customers of banks' credit card services). Nor do all consumers have sufficiently high credit ratings to obtain a credit card. Credit card payments are relatively costly to make because they involve an extension of credit by the issuing bank. Furthermore, credit cards typically are not useful for paying a friend. Checks, while convenient for payments to individuals, are not as useful for international transactions. Checks are also fairly costly because of the care that must be taken in routing the paper check through the banking system and back to the one who wrote the check. Cash is convenient for low-value purchases and can be used anonymously in some circumstances, but it is costly to hold in inventory.

Many foresee demand for a way to make very low-value payments over the Internet. For example, a person may wish to purchase a photograph of a movie star for $0.50. For such small payments it is costly to write a check or to use a credit card (which usually requires a minimum payment of about $20 because of relatively high cost per use). Typically, one uses cash for such a small payment. Hence, digital cash, if it proves sufficiently convenient and low cost, would be much in demand for low-value payments. The cost of a digital cash system is not yet known. Until such a system is operating on a fairly large scale, it is not certain that it can be operated at a sufficiently low cost to make payments for, say, less than a dollar economical.

Credit card methods may prove useful for larger dollar amounts on the Internet. People may be discouraged from using digital cash for large-value payments because they enjoy less float when using digital cash—a debit method of payment—than when using a credit card. Furthermore, many credit-card holders already use their cards to make payments by phone and may therefore be more willing to make the leap to using them over the Internet.

Privacy and security concerns may induce some people to use the trusted-third-party method of payment as well as digital cash. Both of these methods avoid sending credit card information over the Internet, even in a highly secure encryption scheme. In addition, a consumer may wish to withhold his identity from a merchant to avoid having the information used either for marketing purposes or by law enforcement agencies if he is engaging in illegal activities.

PUBLIC POLICY CONSIDERATIONS

The ways that payments are made in the United States today are governed and supported by law and public policy. For example, the laws, policies, and contracts that govern the rights of the various parties involved in a check transaction are well established. These policies help to make checks a reliable and predictable method for making a payment for all the parties involved in the checking system.

For the proposed Internet payment systems, issues such as consumer protection, disclosure and assignment of participant liability, and privacy are being addressed by regulators and law-

makers. The resolution of these policy issues will affect the development and acceptance of the proposed systems.

In particular, questions about the degree to which disclosure requirements, account statements, and some form of electronic receipt would be useful and appropriate for Internet payment systems remain largely unanswered. Required disclosure of liability can help inform parties to a system about their responsibilities and thereby improve decision-making, although such disclosures impose an administrative cost on the system's operator, which, if the system is to succeed, will be collected in some way from the consumers of the service. Account statements and electronic receipts would assist users of payment systems in reconstructing their activities in case there were questions about unauthorized use of their accounts or unauthorized payments—again, at a cost of record-keeping for the system and its users. Resolution of these issues will clarify the obligations of the parties and, with a careful balancing of the costs and benefits involved, will advance the development of acceptable forms of payment systems on the Internet.

Recently, for example, the Federal Reserve suggested modifying some provisions of its Regulation E, which governs many (conventional) electronic methods of payment, as it applies to stored-value cards.[9] The Board's proposal suggested that cards that can store no more than $100 be exempted from the provisions of the regulation, and it makes further exceptions for various specific types of cards. For example, under the proposal, a merchant would not be required to issue paper receipts when certain types of stored-value cards are used for payment. Furthermore, in the proposal the Board also recognized that stored-value systems (such as various digital cash systems) are being developed for the Internet: "Systems are being proposed, for example, for making payments over computer networks, such as the Internet"; it also requested comments on the extent to which the Board should consider applying Regulation E to "various types of network payment products."

Another legal and contract issue is that, on the Internet today, the merchant (and the system operator and the consumer, for that matter) has no standardized or generally accepted and enforceable way to verify the signature or password of the other party to the transaction. As a result, the liabilities of the parties are unclear in the event of a repudiation of a transaction by a customer when the transaction was authorized using the customer's digital signature. In contrast, the assignment of liability in a credit card or (off-line) debit-card transaction is well established. The credit card associations were instrumental in standardizing the form of the contracts used today in the credit card industry. If Internet payment systems not based on credit cards are to succeed, such an association may be helpful in organizing contracts and standards that would form the basis for widespread merchant and bank acceptance of the systems.

A widespread acceptance of contractual standards that make the digital signature of the customer binding may be desirable to address the issue of how liability is to be assigned in the case of a repudiated payment.[10] This issue is complicated by the fact that the federal gov-

---

[9]See the proposed rule of the Federal Reserve System, 12 CFR Part 205, Regulation E; Docket No. R-0919, April 3, 1996.

[10]Such a repudiation may be done fraudulently; that is, a consumer may make a purchase using a payment system based on digital signatures and then later fraudulently claim not to have made the purchase. Hence, the effort to make it difficult to repudiate one's digital signature will reduce fraud of this sort. (Alternatively, the consumer may have mismanaged his or her private key, thereby allowing someone else to make a purchase using his or her digital signature, and repudiated the transaction for that reason.)

ernment has chosen a standard for digital signatures that is different from the standard that has emerged in private industry. Neither has the force of law behind it. Recently, two states, Utah and California, have passed laws giving digital signatures the same validity as handwritten signatures. Similar legislation is pending in other states. These laws should reduce the possibility for repudiation and thereby advance the development of systems using digital signatures.

A second issue regarding digital signatures is who should be allowed to be a certifying authority for the public key used to create such signatures (see *Keys to Establishing Trust in Cyberspace* for a description of the role of a certifying authority for public keys). The certifying authority, in granting a certificate to a party, puts its stamp of approval on the certificate holder's management of the private key and provides the certificate holder a proof of identity. Such certification may carry an implicit guarantee of performance and hence may require the certifying authority to bear a considerable amount of risk. The authority may therefore require considerable oversight power for those to whom it grants a certificate.

Digital cash also entails policy considerations. The creators of digital cash envision individuals transferring it among themselves with no intermediary, which raises the issue of what kind of backing digital cash must have. For instance, must digital cash be backed by currency 100 percent? This would involve an issuer's holding $1 in currency in its vaults for every $1 of digital cash created. Alternatively, should the issuer buy short-term securities, such as U.S. Treasury bills, as backing for the digital cash? Under this system, the creation of digital cash could represent an increase in the money supply. Beyond this issue lies the possibility for "designer digital cash," which could be backed by gold or issued in foreign currencies or which could earn interest. There are few technological limitations on the backing and characteristics of digital cash.

Should digital cash be covered by deposit insurance? This question needs to be settled in part to determine who is liable in the event of the failure of an issuer of digital cash. The Federal Deposit Insurance Corporation (FDIC) recently issued a notice and request for public comment addressing stored-value cards and other electronic payment systems and their eligibility for deposit insurance.[11]

The proposed Internet payment systems require areas of expertise new to most banks. Such expertise is typically found in software companies. Banks and bank holding companies are allowed to engage only in activities that are "closely related" to banking. It is clear from our discussion that encryption systems, among other things, are vital to the success of Internet payment systems. But is developing an encryption system an activity "closely related" to banking? By approving the acquisition of a home-banking software company by a group of U.S. and Canadian banks, and by approving the acquisition of an Internet banking software company by a subsidiary of a bank holding company, the Federal Reserve System and the Office of the Comptroller of the Currency have shown a willingness to allow banks to provide services in this area.[12]

Encryption systems raise issues that go beyond banking. There is a tension between the security of financial messages traveling the Internet (by means of strong encryption systems) and the security of the nation and the ability of its law enforcement authorities to prevent illegal financial transactions. The United States closely regulates the use of strong levels

---

[11]See the notice of the FDIC in the *Federal Register,* August 2, 1996, pp. 40494-97.

[12]See the orders of the Board of Governors of the Federal Reserve System in the *Federal Reserve Bulletin*, April 1996, pp. 363-65, and in the issue of July 1996, pp. 674-76.

of encryption because of its important role in national security. Some commentators fear that denial of licenses to export software that includes strong levels of encryption may put U.S. firms at a competitive disadvantage. At least one firm, though, has won approval to export software based on strong levels of encryption; its software was for financial use only, and it was felt that the encryption system could not be removed from the software.[13]

The need for confidentiality of payment information on the Internet is great because of the greater ease of compiling histories of consumers' purchases. Enhancements to consumer privacy laws may be needed to preclude the misuse of consumer information by nonfinancial firms that may offer payment services or affiliated software. The question of how much confidentiality is needed in Internet commerce has

spawned a debate about the merits of a *completely* anonymous payment system versus the merits of lower cost, more conventional systems of credit card and electronic checks that allow merchants, banks, and system operators to maintain data bases of user information.

CONCLUSION

Efforts to create a form of Internet money are attempts to put old wine in new bottles. Money must be easily identifiable, easy to protect from theft, widely acceptable, and easy to transfer. Providers of Internet payment systems are attempting to meet these requirements in various ways. Sophisticated methods of encrypting the financial information used in payments may prove to be the modern equivalent of vaults, signatures, and watermarks. Public policy will play a role in securing the legal foundations that can help pave the way to widely acceptable and secure ways to pay on the Internet.

---

[13]"Cybercash Gets Clearance to Sell Product Abroad," *Wall Street Journal*, May 8, 1995.

The Economic Benefits and Risks Of Derivative Securities

*Keith Sill**

Derivative security markets have shown extraordinary growth over the past 10 years. But certain events have raised concern about the risks associated with derivatives trading. The stock market crash of October 1987 has, in part, been blamed on portfolio insurance strategies that used futures markets. Large losses associated with the use of derivatives by firms such as Procter & Gamble ($137 million), Metallgesellschaft ($1 billion), and Barings PLC ($1.3 billion), and by Orange County, California ($1.7 billion) have led to fear among some market participants that derivatives trading is a very risky activity that could lead to a widespread disruption of the financial system.

What sometimes gets lost in the popular discussion about derivative-related losses are the benefits that derivative securities provide to firms, investors, and the economy as a whole. Derivative securities such as options, forwards and futures, and swaps can provide firms and investors with opportunities that might not otherwise be available. Derivatives aid in the allocation of risk across investors and firms, and they can lower the costs of diversifying portfolios. Derivative prices reveal information to investors that can make financial markets more stable.

But do derivative securities add significant risk to financial markets over and above the

*Keith Sill is a senior economist in the Research Department of the Philadelphia Fed.

risks already present? The risks associated with derivatives are related to how these securities are used in a specific market setting and economic environment. Since derivatives are contracts, their use can entail legal risks. Derivatives may carry credit risks in that one party to the contract may default. Problems may also arise concerning the liquidity of derivative securities or the ease with which they can be traded. These same risks are, to one degree or another, associated with almost all financial assets.

THE DEVELOPMENT
OF DERIVATIVES MARKETS

Derivatives markets are successful institutions because they make financial markets more efficient. This generally means that borrowing and lending can occur at lower cost than would otherwise be the case because derivatives reduce transaction costs. For example, more efficient mortgage markets mean that homeowners can borrow at lower cost. Similarly, firms can raise funds for investment at a lower cost when financial markets are efficient. This in turn can lead to faster economic growth.

The most common types of derivative securities are equity and interest rate options, currency derivatives, futures and forward contracts, and swaps.[1] In each case the derivative security is a contract between two parties. One party receives a claim on an underlying asset or on the cash value of the asset; the other party has an obligation to meet the corresponding liability (see *Derivatives Defined*).

Trading in derivative contracts has a long history. The first recorded accounts of derivative contracts can be traced back to the philosopher Thales of Miletus in ancient Greece, who, during winter, negotiated what were essentially call options on oil presses for the spring olive harvest. De la Vega reported in 1688 that options and futures, or "time bargains" as they were then known, were trading on the Amsterdam Bourse soon after it was opened. Evidence also suggests that futures contracts for rice were traded in Japan in the 17th and 18th centuries.[2]

The first formalized futures exchange in the United States was the Chicago Board of Trade, which opened in 1848 with 82 members. In March 1851, the first futures contract was recorded. The contract called for the delivery of 3000 bushels of corn in June at a price of one cent per bushel below the March price. Listed stock options began trading in April 1973 on the Chicago Board Options Exchange (CBOE). Other exchanges began offering stock call options in 1975 and put options in 1977. Today, options on more than 1000 stocks trade on five U.S. exchanges.

In the United States, stock index futures began trading in 1982 and stock index options in 1983. By the end of 1993, stock index futures markets were established in 14 countries covering 95 percent of world equity market capitalization.[3]

No one knows how big the derivatives markets really are, in part because trading is global in scope and regulatory responsibility is fragmented. Data taken from a Congressional Research Service report on derivative financial markets show that the notional value of derivatives rose from about $1.6 trillion in 1987 to about $8 trillion in 1991 (Table). Notional value reflects the sum of the value of all the assets. However, notional value tends to overstate the size of the derivatives market, since it does not take into account offsetting transactions. If a bank undertakes a $200 million swap of floating assets for fixed-rate ones, then later cancels

---

[1]For a discussion of currency derivatives, see the article by Gregory Hopper.

[2]See page 3 in the book by Darrell Duffie.

[3]See the article by Joanne M. Hill.

Derivatives Defined

Forward Contract: A contract to buy or sell a specified amount of a designated commodity, currency, security, or financial instrument at a known date in the future and at a price set at the time the contract is made. Forward contracts are negotiated between the contracting parties and are not traded on organized exchanges.

Futures Contract: A contract to buy or sell a specified amount of a designated commodity, currency, security, or financial instrument at a known date in the future and at a price set at the time the contract is made. Futures contracts are traded on organized exchanges and are thus standardized. These contracts are marked to market daily, with profits and losses settled in cash at the end of the trading day.

Option Contract: A contract that gives its owner the right, but not the obligation, to buy or sell a specified asset at a stipulated price, called the strike price. Contracts that give owners the right to buy are referred to as call options and contracts that give the owner the right to sell are called put options. Options include both standardized products that trade on organized exchanges and customized contracts between private parties.

Swap Contract: A private contract between two parties to exchange cash flows in the future according to some prearranged formula. The most common type of swap is the "plain vanilla" interest rate swap, in which the first party agrees to pay the second party cash flows equal to interest at a predetermined *fixed* rate on a notional principal. The second party agrees to pay the first party cash flows equal to interest at a *floating* rate on the same notional principal. Both payment streams are denominated in the same currency. Another common type of swap is the currency swap. This contract calls for the counterparties to exchange specific amounts of two different currencies at the outset, which are repaid over time according to a prearranged formula that reflects amortization and interest payments.

out its position by entering a $200 million contract of fixed-rate for floating-rate debt with the same counterparty, notional value is recorded at $400 million, despite the fact that the two transactions offset each other.

Growth in the use of derivative contracts has proceeded at a rapid pace since 1991. The Bank for International Settlements (BIS) conducted a survey of foreign exchange and derivative market participants worldwide. The survey found a notional value of $47 trillion for over-the-counter (OTC) derivative contracts outstanding at the end of March 1995.[4] Of that total $17.7 trillion represented foreign exchange derivatives and $28.8 trillion represented interest rate derivatives. The survey also calculated a notional value for exchange-traded derivative contracts of $8.2 trillion.[5] Daily average turnover in OTC derivative contracts was found to be $880 billion and that of exchange-traded contracts was $570 billion.

The size of the markets suggests that users of these contracts derive significant benefits from including derivatives in their investment

---

[4]OTC derivatives are contracts not traded on organized exchanges but rather negotiated privately between parties.

[5]The figures from the BIS are not directly comparable to those in the table because the surveys differ.

strategies. At the same time, the size of the derivatives market has led to fears that a disruption could have a wide-ranging impact on financial markets in general. We will focus first on some of the economic benefits of derivatives: they reallocate risk among financial market participants, help to make financial markets more complete, and provide valuable information to investors about economic fundamentals. Then we will discuss risks associated with the use of derivatives.

SOME ECONOMIC BENEFITS OF DERIVATIVE SECURITIES

At first glance, the economic benefits of derivatives might not be apparent, since derivatives are zero-sum monetary games: the amount paid by one side of the contract is the amount received by the other side.[6] When the contract expires or is exercised, the gains and losses completely offset each other. But even though derivatives represent zero-sum monetary games, they need not represent zero-sum economic games.

Individuals and firms that use derivative instruments can do so to hedge, to speculate, or

TABLE

Markets for Selected Derivative Instruments, Notional Principal Values at Year End
in Billions of U.S. Dollar Equivalent

	1987	1989	1991
Exchange-Traded Instruments[a]	725	1762	3518
Interest Rate Futures	488	1201	2159
Interest Rate Options[b]	122	387	1072
Currency Futures	14	16	18
Currency Options[b]	60	50	59
Stock Index Futures	18	42	77
Stock Index Options[b]	23	66	132
Over-the-Counter Instruments[c]	867	2402	4449
Interest Rate Swaps[d]	683	1503	3065
Currency and Cross-Currency[d,e] Interest Rate Swaps	184	449	807
Other Instruments[d,f]	---	450	577
TOTALS	**1592**	**4164**	**7967**

[a]Excludes options on individual shares and derivatives involving commodity contracts.

[b]Calls plus puts.

[c]Excludes data on forward rate agreements, OTC currency options, forward foreign exchange positions, equity swaps and warrants on equity. Data collected by International Swap Dealers Association (ISDA).

[d]Contracts between ISDA members reported only once.

[e]Adjusted for reporting of both currencies.

[f]Caps, collars, floors, and swaptions

Source: As reported by the Bank for International Settlements: Futures Industry Association; ISDA; and various futures and options exchanges worldwide.

to engage in arbitrage. When individuals or firms hedge risks with derivatives, they are attempting to use these contracts as a kind of insurance against a bad future outcome.

Hedging. An example of using derivative instruments to hedge is provided by an adver-

---

[6]We are ignoring transaction costs for now.

tisement by the Student Loan Marketing Association (Sallie Mae) in the *Wall Street Journal* for December 31, 1991. Sallie Mae is a publicly held company that provides private capital funding for guaranteed student loans. The ad showed how Sallie Mae used combinations of swap arrangements to hedge the risks of borrowing money overseas.

Suppose Sallie Mae sells bonds with fixed interest rates and denominated in pounds sterling in the U.K. financial market. Sallie Mae, which is a U.S.-based organization, would like to avoid exchange rate risk between the U.S. dollar and the pound sterling and so enters into a currency swap arrangement. Sallie Mae swaps the principal amount of the bond in pounds sterling for U.S. dollars at the current exchange rate. When Sallie Mae has to pay interest to its U.K. bondholders, the parties swap payments again, with Sallie Mae receiving pounds sterling to meet interest payments in exchange for U.S. dollars at the rate fixed in the swap contract. Finally, when the bonds come due, the counterparties swap the principal payment. The swap arrangement allows Sallie Mae to insure itself against exchange rate fluctuations, since the total cost of interest and principal is fixed in U.S. dollar terms.

Derivative contracts are widely used to hedge a variety of risks. In 1993, the Group of Thirty published *Derivatives: Practices and Principles,* which reported on the use of OTC derivatives by various categories of users. Of the private-sector nonfinancial corporations responding to the survey, 87 percent used interest rate swaps, 64 percent used currency swaps, 78 percent used forward foreign exchange contracts, 40 percent used interest rate options, and 31 percent used currency options.

How do firms use derivative contracts to hedge the risks they face? Of the respondents, 82 percent indicated they used OTC derivatives to hedge risks arising from new financing, 33 percent to hedge exposure from foreign currency translation, 69 percent to hedge foreign

exchange transaction exposures, and 78 percent to manage or modify the characteristics of their existing assets and liabilities.

Financial institutions are major players in the derivatives markets as well. According to the Group of Thirty report, 92 percent of financial institution respondents used interest rate swaps, 69 percent used forward foreign exchange contracts, 69 percent used interest rate options, 46 percent used currency swaps, and 23 percent used currency options. This group of respondents uses derivatives to hedge risk arising from new financing (84 percent), foreign currency translation exposures (46 percent), and transaction exposures (39 percent), and to offset option positions embedded in the institutions' assets and liabilities (39 percent).[7]

When used to hedge risks, derivative instruments transfer the risks from the hedgers, who are unwilling to bear the risks, to parties better able or more willing to bear them. In this regard, derivatives help allocate risks efficiently between different individuals and groups in the economy.

Speculating. Investors can also use derivatives to speculate and to engage in arbitrage activity. Speculators are traders who want to take a position in the market; they are betting that the price of the underlying asset or commodity will move in a particular direction over the life of the contract. For example, an investor who believes that the French franc will rise in value relative to the U.S. dollar can speculate by taking a long position in a forward contract on the franc. If the value of the franc on the expiration date is above the delivery rate set when the forward contract was written, the speculator earns a profit on the contract.

The use of a forward contract for speculation has an advantage over actually buying

---

[7]The option positions embedded in institutional assets and liabilities include such things as call or prepayment features in loans and bonds.

francs and holding them because neither party puts any money up-front when entering into the forward contract.[8] Thus, the forward contract gives the investor much more leverage than buying the underlying asset in the cash market.

While speculation may seem to be no more than gambling on future price movements, speculators play an important role in financial markets because they provide liquidity. This liquidity enables other investors, who may be using derivatives to hedge risks, to more easily buy and sell derivative contracts.

Arbitrage. Arbitrageurs represent another important group of derivatives users. Arbitrageurs look for opportunities to earn riskless profits by simultaneously taking positions in two or more markets. Arbitrage opportunities can occur when prices in financial markets get out of sync. When this happens, arbitrageurs step in and, by doing so, help to get market prices back into alignment. This activity helps to keep prices consistent across markets. Arbitrage trades can be quite complex, but we will give a simple example to show how such trades can work.[9]

Suppose that the interest rate on 13-week Treasury bills is 10 percent and the rate on 26-week Treasury bills is 10.5 percent. The rates on the two Treasury bills imply that the 13-week Treasury bill rate in three months will be about 11 percent.[10] Also, suppose that a T-bill futures

contract allows one to buy or sell a 13-week T-bill for delivery in three months at a rate of 10.75 percent. Since these two future interest rates differ, there is an opportunity to earn a risk-free profit. Arbitrageurs can exploit this mispricing if, in three months, they can borrow money at 10.75 percent and invest it at 11 percent. They do so by trading the futures contract and Treasury bills.[11]

Arbitrage activity also helps to keep asset markets liquid and thus reduces transaction costs. Arbitrageurs are taking positions in derivative instruments and in the assets that underlie them. Therefore, arbitrage helps to reduce liquidity premiums, or the difference between the purchase price and the sale price of the underlying assets.

Leverage. Derivative contracts also aid in risk allocation because of the cheap leverage opportunities they provide to the investor. We've already hinted at the leverage obtained by using forward contracts. In that case, leverage comes about because no cash has to be put up at the time the parties enter into the contract.

Options are also leveraged investments. Take the case of a call option on a stock like AT&T. On March 28, 1996, a July call option on 100 shares of AT&T stock with a strike price of $60 sold for $400. AT&T shares in March were selling for a little less than $62. To purchase 100 shares of AT&T would have cost an investor close to $6200. If, in July, AT&T shares sell for $65 per share, the holder of the option will exercise it and reap a profit of approximately

---

[8]Recall that a forward contract is an agreement between two parties to buy or sell an asset at a specific time in the future. The price at which the asset is to be delivered on that future date is called the delivery price. The delivery price is set in such a way that the price of the forward contract at the time it is made is zero to both parties.

[9]For more detail on arbitrage and derivatives, see the book by John C. Hull.

[10]This follows from the fact that the return on the 26-week T-bill can be expressed as a geometric average of the returns on two successive 13-week T-bills:
$(1.105) \approx \sqrt{(1.10)(1.11)}$.

---

[11]This requires three steps. First, sell the futures contract short, which means that the arbitrageur will be committed to delivering T-bills with an implied rate of 10.75 percent in 90 days. Second, borrow money at the 10 percent rate for 13-week T-bills. Third, invest the borrowed money in 26-week T-bills at 10.5 percent. Steps two and three guarantee that a rate of 11 percent is earned on T-bills after 90 days, while step one guarantees that a T-bill yielding 10.75 percent can be sold after 13 weeks.

$100 on his $400 investment in the call option.[12] If the shares had been bought outright, the investor would have gained $300 on a $6200 investment.[13] Of course, if AT&T shares sell for $62 in July, the investor loses the $400 investment in the call option. But if he owned the shares outright, his dollar loss would be negligible.

Is leverage a good thing for financial markets? Generally yes, because leveraged positions give investors access to risk-return tradeoffs they otherwise would not have. Broadening the menu of available choices helps individuals tailor risk to their own investment, hedging, or arbitraging situation. Derivative contracts allow investors to leverage relatively small amounts of funds over a wide class of assets and thus diversify their portfolios.

However, leverage can work to an investor's disadvantage as well. In the Orange County, California, bankruptcy episode, the investment fund took a highly leveraged bet that interest rates would not rise. When rates did rise, the fund lost value to a much greater extent than it would have, had it not been leveraged (see *Orange County and Derivative Securities*).

Complete Markets and Derivative Instruments. In addition to efficient allocation of risk, derivatives offer another important benefit: they can provide investors with opportunities that would otherwise be unavailable to them at any price. That is, derivatives can provide payoffs that simply cannot be obtained with other, existing assets.

In theory, derivative contracts can be written to provide any conceivable pattern of payoffs that depend on future conditions. Or, in economists' language, derivatives can make markets complete. Why are complete markets desirable? Because they provide maximum flexibility for investors, since any possible pattern of returns can be achieved using a portfolio of existing securities.[14] In addition, economic theory tells us that a complete market is economically efficient, which means that resources cannot be reallocated in such a way as to make everyone better off.

In reality, there are obstacles to achieving complete financial markets. For example, writing and enforcing contracts that cover certain contingencies present difficulties; costs make some transactions infeasible; and government regulations may interfere with the market's ability to provide some payouts. Given these obstacles, we want to create securities that will help us get closer to complete markets. This is where derivative instruments come in: derivatives can help move financial markets toward completeness.[15]

Furthermore, it may be much less costly to complete markets by using derivative securities than by creating new basic securities. Thus, derivative securities can lower transaction costs for investors.

TRANSACTION COSTS AND INFORMATION

The standard method for calculating the prices of options and other derivative securities assumes that securities markets are effec-

---

[12]If the call is exercised, the profit on the transaction can be expressed as the difference between the underlying asset price and the option strike price, less the cost of purchasing the call.

[13]Leverage can be gained in stock market transactions by purchasing stocks on margin. Current regulations allow up to 50 percent of a long position in a stock to be borrowed. However, the leverage obtained by using derivatives on stocks is substantially higher than the leverage obtained by purchasing stock on margin.

[14]For a detailed discussion of options and complete markets, see the articles by Stephen Ross and Nils Hakansson.

[15]It need not be the case that partially completing an incomplete market is always best. For example, the article by Franklin Allen and Douglas Gale shows that, under certain conditions in an incomplete market, financial innovation may not be efficient.

Orange County and Derivative Securities

Orange County, California, declared bankruptcy in December 1994 after an investment fund run by the county treasurer reported losses that eventually amounted to $1.7 billion. News reports of the incident highlighted the fact that the Orange County Investment Pool (OCIP) held derivative securities and often gave the impression that derivatives were to blame for the county's losses. The OCIP did hold derivative securities, which amounted to about 40 percent of invested funds. But OCIP lost about 20 percent of its investors' funds because of a risky bet on the direction of interest rates that turned out to be terribly wrong.

The county's investment strategy was essentially to borrow short and lend long. Usually, long-term interest rates are higher than short-term interest rates because the short-term return to holding long-term bonds is risky. A higher interest rate on long-term bonds helps compensate investors for bearing this risk. When short-term interest rates are lower than long-term rates, it can be profitable to borrow at the short-term rate and lend the borrowed money at the long-term rate. So funds from the OCIP were invested in long-term bonds. The OCIP got more bang for its buck by leveraging up its investment: the pool posted the long-term bonds as collateral and borrowed against them at the short-term interest rate. It then took the borrowed money and purchased more long-term bonds.

The strategy was profitable as long as interest rates stayed the same or declined. But in February 1994 interest rates began rising. When interest rates rise, the price of bonds falls. As a result, the long-term bonds in the OCIP declined in value at the same time that the cost of short-term borrowing was rising.

The OCIP also invested in interest rate derivative securities called inverse floaters. These derivatives gain value when interest rates fall and lose value when they rise. When interest rates rose in 1994, these securities took a big hit.

The losses in the OCIP can be approximately broken down as follows.* The initial value of the OCIP portfolio was $7.6 billion. Through leverage, however, the total value of invested funds was on the order of $20 billion. The OCIP had a $12 billion investment in fixed-rate bonds that had an average maturity of four years. When interest rates rose in 1994 these bonds lost about $360 million. About $8 billion of OCIP funds were invested in inverse floaters, which lost about $620 million. Short-term borrowing of about $12.4 billion led to additional losses, through the payment of interest, on the order of $620 million.

---

*These figures are taken from the book by Philippe Jorion.

---

tively complete. Nils Hakansson has pointed out that this is something of a paradox. If markets are complete, options are redundant assets. So why do they exist?

Transaction Costs. Robert Merton has developed one solution to this paradox. Individual investors may face high transaction costs for certain types of financial trades, but large firms will have lower transaction costs in securities markets because of the large volume of trades they undertake. For these large firms, markets will be effectively complete, since they can create different securities by engaging in carefully constructed trading over time (called dynamic trading) at low cost. The firms can then sell claims on these dynamic trades as derivative securities to individuals, passing on the lower transaction costs. The assumption of market completeness, and thus standard option-pricing theory, would be approximately correct because of the presence of these large firms with their low transaction costs.

In reality, derivative securities provide investors with low-cost ways to diversify portfolios. For example, stock index options allow their users to trade an entire portfolio of stocks as a single financial product. It is much more difficult, and expensive, for individual investors to trade a basket of stocks representing, say, the S&P500 on the stock exchange, than it is to trade

an S&P500 stock index futures contract. In addition, it is almost always the case that an option on a portfolio is less expensive than a portfolio of options on the underlying stocks.[16] Stock index options and futures allow investors to trade at a fraction of the cost of trading the underlying basket of stocks on the cash market or buying portfolios of options.[17]

Derivatives also provide beneficial opportunities for diversification because they offer easy and cheap access to classes of assets, such as commodities, that would otherwise be very expensive. For example, investors can buy futures contracts on oil, corn, gold, and a host of other commodities to help diversify their portfolios. In addition, investors can buy futures on commodity indexes. To purchase these underlying commodities in the cash market would require a large investment. By purchasing futures, investors can benefit from favorable price movements in these classes of assets in a relatively inexpensive way. Of course, investors would also risk large losses from adverse price movements.[18]

Derivatives and Market Information. We saw that, in complete markets, derivatives provide no new investment opportunities beyond what is available from existing assets. Indeed, modern finance methods compute the price of an option by finding a dynamic trading strategy using the underlying asset and T-bills that

replicates the payout of the option. A dynamic trading strategy means that the amount of money invested in the asset and in T-bills is adjusted over time to ensure that the portfolio payout is the same as the option payout.

But even if these option-pricing models are accurate, options are not necessarily redundant assets. Sanford Grossman contends that the prices of traded options convey information about the underlying stock that may serve to lower its volatility. Grossman argues that many large investors using dynamic trading strategies instead of traded options to achieve desired returns can cause an increase in the volatility of the underlying stock.

Consider the case of portfolio insurance. Portfolio insurance refers to the desire of portfolio managers to eliminate the risk that their portfolios' value will fall below a certain level. One method of implementing portfolio insurance is by using put options. If an investor buys a put option on a stock, the risk that the value of the portfolio composed of the put and the stock will fall below the strike price of the put is eliminated.[19] However, when investors' portfolios contain many stocks, it may not be possible to buy puts on all of them. In this case, the portfolio manager can implement portfolio insurance by using a dynamic trading strategy that replicates the payout of a put option on the portfolio.

Portfolio managers who use dynamic trading strategies are counting on their ability to sell shares of the stocks in the portfolio before the market price of the shares falls below their

---

[16]An option on a portfolio will be cheaper than the portfolio of options provided the underlying assets are not perfectly correlated. When assets are not perfectly correlated, diversification has benefits, since it lowers the volatility of the portfolio. Option prices fall as volatility falls.

[17]In some cases the investor may be able to purchase shares in a mutual fund that closely approximate his desired portfolio. This would also be a low-cost way to diversify, but it does not give the leverage opportunities that come with using derivatives.

[18]See the article by Anatoli Kuprianov for case studies of the Metallgesellschaft and Barings derivatives losses.

---

[19]On exercise, the payoff function for a put option can be expressed as the difference between the strike price and the underlying stock price. If we denote the strike price by K and the stock price by S, in the event that S is less than K at exercise, the put option payoff is K - S. If we hold both the stock and a put on the stock, when the stock price falls below K and the option is exercised, the total value of the portfolio is S + (K - S) = K. K represents a floor below which the value of the portfolio will not fall.

floor. But if many portfolio managers are using dynamic trading to implement portfolio insurance, many traders are attempting to sell shares once the market begins falling. But as everyone tries to sell, the market is forced lower and lower, and thus the dynamic trading strategy may not work since traders find they are unable to sell stock at a price above the targeted floor: prices may fall too far, too fast.

Suppose, though, that put options were available to those portfolio managers who wanted insurance. If everyone were trying to buy puts to implement insurance, the price of puts would go up. In essence, insurance would become more expensive. As insurance becomes more expensive, there will be less demand for it, and so, fewer portfolio managers would use insurance. Since the demand for insurance is a driving factor in the determination of stock volatility, the higher price of the puts is telling market participants that stock market volatility is expected to be higher in the future and that the net demand for insurance is high.[20] The price of the put options serves to coordinate the strategies of the users of portfolio insurance by revealing expectations about stock price volatility.

If everyone is using a dynamic trading strategy and cannot observe a price for insurance, there is no way to easily tell how large the net demand for portfolio insurance is. Stock market volatility could then be higher when dynamic trading strategies are used to implement insurance compared to the case where put options are used. According to the Brady Commission report, portfolio insurance and index arbitrage accounted for about 20 percent of to-

tal sales on the New York Stock Exchange on October 19, 1987, the day the stock market crashed.

When financial markets are complete and there are no frictions like transaction costs and imperfect information, derivative instruments are redundant assets. In such a setting, the presence or absence of derivatives has no implications for the riskiness of financial markets or the volatility of underlying assets. In reality, financial markets are not complete and there are frictions, so the presence or absence of derivatives matters for the economy.

The theoretical and empirical evidence on how the introduction of derivatives affects the economy is limited. However, the existing evidence suggests that derivatives do not appear to add to financial market risk as a whole.[21] However, they do involve some risks to individuals and firms.[22]

RISKS ASSOCIATED WITH THE USE OF DERIVATIVE INSTRUMENTS

Many firms and individuals use derivative instruments as part of an overall strategy to manage the various risks they face. Sophisticated risk-management techniques evaluate the overall riskiness of investment portfolios that include options and other derivatives. However, assessing the risks of these portfolios generally requires practitioners to use models of option pricing that are only approximations. Sometimes these models do not perform as well as practitioners would like, and, after the fact,

---

[20]An investor using an insurance strategy will sell equity after a fall in price and purchase equity after a rise in price. A net demand for portfolio insurance manifests itself in an increase in equity price volatility regardless of whether the insurance is implemented by the use of put options or by dynamic trading strategies. See the articles by Sanford Grossman for details.

[21]Jerome Detemple and Philippe Jorion review some of the theoretical and empirical work on the effects of option introduction on the stock market. The empirical work in the article suggests that after the introduction of an option, the price of the underlying stock rises and the volatility of the underlying stock falls.

[22]The paper by Rajna Gibson and Heinz Zimmermann has a more detailed discussion of the risks associated with the use of derivatives.

the firm can find itself exposed to more or less risk than it desired. In addition, financial innovation has led to new and more exotic securities that are increasingly difficult to price. Thus, the *inaccuracies in various pricing models* may lead investors and traders astray.

Another risk is that one party may default on the contract, which is called *credit risk.* Credit risk is not much of a problem for derivatives traded on organized exchanges, since these exchanges are designed in such a way that their contracts are almost always honored.[23] Credit risk is much more of a problem in the OTC market, where two parties negotiate a derivative contract specific to their needs. For example, a bank may enter into offsetting swap arrangements with two firms. If neither firm defaults, the bank is fully hedged. But if one firm defaults, the bank will still have to honor its arrangement with the other firm, and so it faces a credit risk. Banks can try to mitigate some of this risk by requiring collateral from the firms participating in the swap arrangement or by obtaining third-party guarantees.

Another risk in the use of derivative instruments is *liquidity risk,* which refers to the ease with which the contract can be traded. Liquidity risk is not specific to derivative contracts; it can play a significant role in any financial market during periods of high volatility or signifi-

cant changes in economic fundamentals. However, even during the market crash of October 1987, both standardized and OTC derivative markets remained viable, and no market collapse or major liquidity crisis occurred. The structure of the standardized and OTC markets appears to have been adequate to manage liquidity risk in the past. Further, there is little evidence that liquidity risk has increased with the size of derivatives markets.

When securities become illiquid, however, it is more difficult to determine their market value. As a consequence, when firms try to sell illiquid securities they may find that the market value of their portfolios and securities differs substantially from the values that are "on the books." The models that firms use to manage their risks and make financial decisions may then give incorrect answers because incorrect values for the securities were used in the analysis.

CONCLUSION

Derivatives markets have shown tremendous growth over the last 10 years. While much has been made of recent derivatives-related losses, the economic benefits provided by derivative securities are more important. Derivatives help the economy achieve an efficient allocation of risk. They assist in completing markets, thereby providing firms and individuals with new investment opportunities. Derivatives provide information to financial market participants and may help reduce overall market volatility.

---

[23]Organized exchanges use arrangements such as daily marking to market and clearinghouses to guarantee performance of the contract.

REFERENCES

Allen, Franklin, and Douglas Gale. "Arbitrage, Short Sales, and Financial Innovation," *Econometrica,* 59 (1991), pp. 1041-68.

Bank for International Settlements. *Central Bank Survey of Foreign Exchange and Derivatives Market Activity 1995.* Basle: Bank for International Settlements, May 1996.

REFERENCES (continued)

Cox, John C., and Mark Rubenstein. *Options Markets.* Englewood Cliffs: Prentice-Hall, 1985.

Detemple, Jerome, and Philippe Jorion. "Option Listing and Stock Returns," *Journal of Banking and Finance,* 14 (1990), pp. 781-801.

Duffie, Darrell. *Futures Markets.* Englewood Cliffs: Prentice-Hall, 1989.

Gibson, Rajna, and Heinz Zimmermann."The Benefits and Risks of Derivative Instruments: An Economic Perspective," Geneva Papers (1994).

Grossman, Sanford. "Insurance Seen and Unseen: The Impact on Markets," *Journal of Portfolio Management,* Summer (1988a), pp. 5-8.

Grossman, Sanford, "An Analysis of the Implications for Stock and Futures Price Volatility of Program Trading and Dynamic Hedging Strategies," *Journal of Business,* 61 (1988b),pp. 275-98.

Group of Thirty. *Derivatives: Practices and Principles.* Washington, D.C: Group of Thirty, 1993.

Hakansson, Nils. "The Fantastic World of Finance: Progress and the Free Lunch," *Journal of Financial and Quantitative Analysis,* 14 (1978), pp. 717-76.

Hill, Joanne M. "The History of Equity Derivatives," in Jack C. Francis, William W. Toy, and J. Gregg Whittaker, eds., *The Handbook of Equity Derivatives.* Chicago: Irwin, 1995, pp. 33-48.

Hopper, Gregory P. "A Primer on Currency Derivatives," Federal Reserve Bank of Philadelphia *Business Review* (May/June 1995).

Hull, John C. *Options, Futures, and Other Derivative Securities.* Englewood Cliffs: Prentice-Hall, 1993.

Jorion, Philippe. *Big Bets Gone Bad: Derivatives and Bankruptcy in Orange County.* San Diego: Academic Press, 1995.

Kuprianov, Anatoli. "Derivatives Debacles: Case Studies of Large Losses in Derivatives Markets," Federal Reserve Bank of Richmond *Economic Quarterly* (Fall 1995).

Merton, Robert C. *Continuous-Time Finance.* Oxford: Basil-Blackwell, 1990.

Ross, Stephen A. "Options and Efficiency," *Quarterly Journal of Economics,* 90 (1976), pp. 75-89.

U.S. House of Representatives, "Derivative Financial Markets," Congressional Research Service Report, Subcommittee on Telecommunications and Finance, 1993.

Vega, J.P. de la. *Confusion de Confusiones,* translated by H. Kellenbenz, No. 13, The Kress Library Series of Publications, The Kress Library of Business and Economics, Harvard University, Cambridge, MA.