FEDERAL RESERVE BANK OF PHILADELPHIA

Ten Independence Mall
Philadelphia, Pennsylvania 19106-1574
(215) 574-6428, www.phil.frb.org

Working Papers

Research Department

WORKING PAPER NO. 97-9

BANKING AND PAYMENT SYSTEM STABILITY IN AN ELECTRONIC MONEY WORLD

James J. McAndrews
Federal Reserve Bank of Philadelphia
Presented at the
Conference on the Foundations of Policy Toward Electronic Money
December 3, 1996
Federal Reserve Bank of Minneapolis

Revised July 1997

WORKING PAPER NO. 97-9
BANKING AND PAYMENT SYSTEM STABILITY IN AN ELECTRONIC MONEY WORLD

James J. McAndrews
Federal Reserve Bank of Philadelphia

Presented at the
Conference on the Foundations of Policy Toward Electronic Money
December 3, 1996
Federal Reserve Bank of Minneapolis
Revised July 1997

*I wish to thank Leonard Nakamura for helpful comments and conversations that helped shape this paper, although he bears no responsibility for its shortcomings.

Banking and Payment System Stability in an Electronic Money World

I. Introduction

Today we observe the rapid development of information-processing systems that are likely to displace, over time, many of the systems by which payment-related information is communicated. Indeed, stored-value systems, as well as credit-based and deposit account-based systems, that communicate instructions or transfer value over open communication and computer networks represent new techniques (based on encryption schemes) to initiate payments. These new techniques hold a great deal of promise in that they potentially offer added convenience to the consumer. This promise is qualified by the question of whether these new means of payment add to the perennial risks of instability in the payment system and the banking system.

The new forms of payment being developed can be broadly grouped into three categories: those that allow payments to be made using credit cards over communication systems such as the Internet; those, like the electronic check, that involve transmitting instructions to banks to transfer funds from one deposit account to another; and those, like some forms of stored-value cards and digital cash, that represent the electronic equivalent of bank notes. For the time being we will dub all these systems that transmit payment or payment instructions over open networks "emoney."

Many of these new systems will clear and settle the system's payments in a special-purpose private bank--a clearinghouse. Issues of settlement risk in clearinghouses are reasonably well understood as a practical matter. Several principles are practically implemented in the

operating rules of many clearinghouses, including CHIPS.[1] These rules attempt to ensure adequate liquidity of the settlement facility, especially in times when members of the system experience financial distress. This "settlement risk" is indeed a concern for the new payment systems, and we will review this concern in greater depth.

However, it is not conventional settlement risk that poses a novel threat to the smooth operation of the payment and banking systems from the introduction and widespread acceptance of emoney. Rather, the threat arises principally from the uncertainty regarding fraud and operational risks to the systems because the uncertainty can lead to runs that risk large-scale disruption to the banking and payment systems.

These risks may be exacerbated by the type of industrial organization emerging in the emoney industry. The American banking industry is unique for its decentralization. The current trend of consolidation in banking is changing this feature of American banking only slowly. Payments have been cleared and settled through clearinghouses (and the Fed) and correspondent networks that were, for the most part, invisible to the retail customer. The new means of payment, in contrast, are provided to a large extent in "branded networks," in which the clearinghouse and its identity have a strong retail presence and are the foremost link with the product in the consumer's mind. This type of organization in payments is illustrated today by the credit card associations, Visa and MasterCard. The nature of competition in which such networks engage, in conjunction with the liquidity, fraud, and operational risks to which they are subject, can also pose risks to the stability of the payments system.

---

[1]Among these principles are "Know your counterparty"; "Manage counterparty risk through bilateral net debit limitations"; "Manage system risk with limits on total, multilateral net debit limits."

The next section will briefly review some of the likely forms of emoney in more detail. In the third section I will provide an overview of systemic payment risk issues and their applicability to emoney systems. In section four, I will review the variant experiences of payment and banking system stability in the Free Banking era and in the National Bank period. In section five I will consider the effects of emoney branded network competition on the stability of the payment system. I will conclude the paper in section six with a discussion of lessons learned concerning banking and payment system regulation and control.

II. Forms of Emoney and Emoney Firms

In some ways, the emoney world is here now. Indeed it has been for some time in the guise of Fedwire and the automated clearing house (ACH), automated teller machines (ATMs), and point-of-sale (POS) debit card networks and credit card networks. These electronic systems are highly automated and efficient forms of payment that provide services on "closed" networks of computers. Access to all these systems is highly restricted. Merchants that accept credit cards are carefully screened by their banks prior to being given the ability to accept credit card payments. ATM networks conduct transactions over dedicated phone lines. In addition to access restrictions, several important security aspects, including encryption, ensure the privacy and accuracy of Fedwire, ACH, credit card, and ATM network messages.

Providing security over "open" networks, in which there are no access restrictions, is a fundamentally different, and more difficult, problem than is the case with closed networks. An open network is one in which the information flows over the network can be observed, or intercepted, by a third party. For example, messages sent over the Internet presumably can be intercepted. The first and most vexing problem confronting security over open networks is how

to identify the individual sending a message from a computer linked to the network. Another problem is how to verify that the message the individual sent has not been altered in transmission. Yet another problem is how to safeguard the message from being "overheard" (and understood) or redirected to some other destination.

Answers to these problems exist. The means to accomplish these security tasks typically involve the use of sophisticated modern cryptography, including public key cryptography. The ways in which cryptography can safeguard electronic messages is sophisticated and elegant. The nature of the security problem of open networks can be likened to trying to create a "virtually closed" network.[2]

A virtually closed network is one whose encryption-based security procedures are so complete and well executed as to provide the same level of security (or even an enhanced level of security) as exists for restricted-access or closed networks. This is the desire of designers of the money systems.

Fedwire and the ACH do not fully meet the designation of emoney because they are primarily wholesale systems. The emoney development we see today is primarily in retail payment systems. The retail payment system in the U.S. today primarily consists of cash, checks, credit cards, and debit cards. What forms of payment will emoney take?

To date, it has taken the form of electronic bank notes, such as the embedded-chip card known as Mondex, or "ecash," for transfer over open computer networks; an electronic check, such as a system proposed by the Financial Service Technology Consortium, for transfer over

---

[2]See Bruce Schneier's *Applied Cryptography* (1993) for a thorough introduction to this subject.

open computer networks; and enhancements to credit card communications. Clearly, the digital cash systems designed for transfer over the Internet are designed for use on open networks, as are the systems to transmit credit card information. Many embedded-chip card systems too are designed to operate in an open environment, and when I discuss such cards, I refer to those systems. All of these systems rely on public key cryptographic security procedures to create a "virtually closed" network to protect the content of the messages sent in the system.

An important aspect of emoney is that all three of these systems are likely to be provided by what I'll call retail "branded networks." Branded networks consist of a group of providers that use a retail brand identification for marketing purposes and use the central organization for establishing network operating rules, business strategy, and network operations (in the case of emoney, a clearinghouse). The central organization may or may not be owned by members. In the credit card marketplace, Visa and MasterCard are owned by their members, while American Express and Discover Card are owned by single organizations that provide a stand-alone network to compete against the larger Visa-MasterCard networks. Some ATM networks are owned by all members, while some are owned by a small group; still others are owned by third-party firms.

The tendency in the larger credit card and ATM networks, however, as documented in McAndrews and Rob (1996), is for the network to be owned by a group of "downstream" users. That is, for ATM networks, the largest ones tend to be owned by a group of banks that issue ATM cards prominently marked with their own network's brand. The underlying reason for this type of organization is threefold. First, the need for widespread acceptance in payments means that there is a "network externality" in demand: the value to any user is increased as other potential users adopt the system. Second, in what is a common theme for vertical integration in

other industries, the tendency for downstream users to own the upstream network organization better aligns the interests of the upstream and downstream sectors.[3] Finally, it is an equilibrium phenomenon that larger scale can be achieved through the organization of the industry in this manner.

The Mondex system provides a classic example of this type of organization. Mondex was started by National Westminster Bank in the UK, and its U.S. rights have been purchased by a coalition of 16 banks (including the AT&T credit card bank). MasterCard purchased a large interest in the worldwide rights to Mondex. These emoney firms, then, will likely be joint ventures of banks and technology firms, which together will establish a brand identity, a clearinghouse for the clearing and settlement of payments, and a central organization that determines network rules, business strategy, and enforcement policy. This type of organization of the firm has been seen in the credit card and ATM industries.

III. Systemic Payment Risk

The growth of large-value transfers in the industrialized countries in the last decade has increased the concern within central banks about the risks posed by these systems. This concern has led to significant policy actions and studies at various central banks and at the Bank for International Settlements. A taxonomy of risks associated with payment systems is now fairly standard. The risks are typically categorized as credit or solvency risk, liquidity risk, market risk, Herstatt risk, fraud risk, operational risk, and systemic risk. This extensive categorization is not mutually exclusive.

---

[3]In other words, it tends to reduce, if not fully eliminate, the "double margin" of price markups among the upstream and downstream sectors; see McAndrews (1996) for an illustration of this effect.

Credit risk and *market risk* refer to the possibility that a settlement will not be realized at full value. The cause of this default could be the *insolvency* of the counterparty to the payment; the insolvency could be caused by the loss in market value, between the time of purchase and the time of settlement, of the object for which the payment is intended. The settlement could be delayed because of *illiquidity* of one party at the time of settlement. *Herstatt (or time-gap) risk* refers to the possible consequences of a time delay in delivery and payment (typically of two currencies in a foreign exchange transaction). The possibility that one party could go bankrupt after the counterparty has made payment exposes one party to default risk in the intervening period. *Fraud risk* reflects the possibility that counterparties, customers, employees, or third parties may misrepresent themselves in ways that increase the liabilities of the payor, or in some other way that subverts the workings of the payment system to their own benefit. *Operational risk* exists in any payment system and concerns the possibility that breakdowns in the planning or execution of the payments, such as a breakdown in the operation of the central computer, expose the participants to unexpected liquidity shortfalls. Finally, *systemic risk* entails a serious liquidity shortfall, on the part of one or several participants, that cascades to threaten the stability of all or a large number of the system's participants.

If we confine our consideration to retail payment systems, there is little reason to believe that emoney will greatly add to the credit, market, and Herstatt risks in payment systems in the short run. Most of these risks pose little danger in the context of retail payment systems.

In the long run, both the clearance (the exchange of information about payments entered into the system) and the settlement (final discharge of payment obligations) of emoney payments will likely take place through the branded network. Settlement may occur in the short run across

established bank settlement systems. These bank settlement systems then will experience larger volumes of business, but not problems of a different nature. Also, in the long run, settlements will most likely move away from the Fed settlement system (associated with check clearance) and toward the private settlement systems associated with the emoney branded networks.

Liquidity risk is always with us, and possibly this risk will be increased in certain emoney systems for a number of reasons. Electronic bank note systems foresee placing all the system's assets and liabilities in a special-purpose bank. The liquidity arrangements for these institutions will have to be well designed because the private settlement systems of the branded emoney networks will be designed as net, rather than gross, settlement systems. Netting systems, by economizing on liquidity, are typically less costly to the participants. Recent research by Emmons (1995), Kahn and Roberds (1996), and Lacker (1996) suggests that private netting systems tend to shift settlement risk to the deposit insurer. They also expend too many resources and tend to be subject to greater risk of failure than do gross systems. Because of the substitution of private net settlement systems for the central bank gross settlement system, the long-run development of emoney could add to the liquidity and systemic settlement risk in society.

As I will discuss in the section on emoney competition, emoney systems are likely to proliferate in the near term, followed by a gradual winnowing out of the systems. Research and policy work at the Bank for International Settlements has suggested that netting systems must be well designed to accomplish a possible reduction in settlement risk.[4] With systems proliferating in the short run, close attention should be paid to a system's risk controls.

Another area that gives rise to concern about liquidity risk is the role of nonbanks. While

[4]For example, in the Lamfalussy report (Bank for International Settlements, 1990).

nonbanks typically disclaim the role of issuer, the legal liability in the case of failure because of the performance of a nonbank and the ability of the system to perform should a nonbank become illiquid are important factors that may pose liquidity risks to the system.

For fraud and operational risk, emoney systems present new risks to banks and payment systems. Fraud is of great concern to operators of all payment systems. Most systems attempt to counter the possibility for fraudulent entry of payment orders by erecting elaborate firewalls that prevent unauthorized access to the system. The Federal Reserve, for example, knows the physical device from which a message is received, and the users of Federal Reserve payment services have passwords that they must reveal prior to gaining entry into a specific application, such as the ACH. Dedicated lines increase the level of assurance that the passwords have not been intercepted.

The open networks across which emoney will be transmitted require a whole new apparatus to prevent fraudulent access to the system. Because of the ability to intercept messages in open networks, passwords are insufficient to prevent criminals from entering the system—hence, the need for heavily encrypted messages. Because individuals and the transactions they make will not be identified with a specific physical device (except for the case where certain types of smart cards come to dominate money), the need to identify individuals (in the context of open networks), or individual notes, requires new methods of identification—hence, the digital signature and digital certificate.

The insufficiency of passwords in a world in which appearances deceive is demonstrated by the case of the fraudulent ATM. In May 1993 two criminals placed an ATM in a Connecticut mall. The ATM had popular network logos on it and was being run with software designed to

simulate a working ATM, but it was, in fact, not connected to any ATM network switch. Instead, the ATM would allow people to place their card in the machine and enter their password (their personal identification number, or PIN). The machine would then report that it was out of service. The criminals then used the card numbers and PINs they had collected to counterfeit new cards and steal over $100,000. They were later arrested.[5]

This crime is an archetype of the fraud that is possible over the Internet. Something more than logos or pretty pictures must be shown to establish the true identity of the merchant with which the customer wishes to trade. The same goes for the merchant regarding the customer's identity. The public key infrastructure is intended to fill this gap in electronic communications.

The need for the new security apparatus or infrastructure to protect the integrity of payment instructions in an emoney world places significant burdens on the designers and sponsors of these systems. Creating a new "public key infrastructure," as it has been called, is an enormous undertaking, requiring a high degree of coordination among a wide variety of participants.[6]

A few of the issues that confront the participants in this effort include the degree of standardization across different systems (the federal government, for example, has chosen as its standard for the digital signature one that is different from the one typically employed by business); the willingness to accept a particular authority as providing a valid digital certificate; the amount of credit risk a certificate authority may assume as a result of issuing a digital

---

[5]See "The Case of the Phony ATM Nears an End," *Bank Network News*, July 12, 1993.

[6]See the remarks of Stephen Cohn, vice president, Network Security, BBN Corporation, "Principles of Public Key Infrastructure," presented at the FBMA CyberPayments '96 Conference, June 1996, Dallas, Texas.

certificate, either by contract, law, or court decision; the compatibility of the hardware employed by the different systems; and the different users of the systems. Daunting though this list may be, the longer there is only partial resolution of these issues, the greater the possibility for criminals to slip through the interstices of the security system. Fraud can creep into a heavily encrypted system through the system's hardware, without ever compromising the encryption.

The recent case of massive fraud in Japanese Pachinko parlors is instructive in this regard.[7] The National Police Agency of Japan, in concert with Sumitomo, Mitsubishi Corporation, and Nippon Telephone and Telegraph, designed a heavily encrypted, counterfeit-proof magnetic stripe prepaid card to be used in Pachinko parlors, in an effort to rid the parlors of cash and the associated tax evasion. Although the card readers were heavily guarded, organized gangs managed to steal the machines and reverse-engineer the process for writing to the cards. Rather than counterfeiting the counterfeit-proof cards, the gangs recycled used cards and wrote over them. They never had to crack the encryption on the cards. The losses sustained by the system's sponsors were reported to exceed $600 million.

There are at least two lessons to take away from this episode. Where there is a prize of this size available for the taking, we can expect extensive efforts to break the security system. Furthermore, encryption is only one component of the security system of readers, authentication devices, and devices that can write value to chips or magnetic stripe cards; it is a significant challenge to make all facets of the system as secure in practice as the best encryption systems are in theory.

---

[7]See Andrew Pollack, "Counterfeiters of a New Stripe Give Japan One More Worry: Fake Cards Thwart Efforts to End Pinball Crime," *New York Times*, Thursday, June 20, 1996, Col.2, Pg.1, Section D.

Operational disruptions also pose a similar risk to the stability of the system. There are numerous examples of severe problems caused by failures of operations: the Bank of New York's computer problem, which resulted in a $22 billion overdraft in 1985; the "worm" virus that disrupted the operation of the Internet in 1987; the shutdown—caused by a roof collapse after a heavy snow—of an Electronic Data Systems facility for processing ATM transactions in 1993, which affected over 5000 ATMs across the nation.[8] Since emoney is a networked product, the processing of many emoney transactions will take place in centralized switch facilities.[9] Any interruption in the operation of the software supporting the system—because of a virus, for example—or of the centralized switching facility—because of a sustained attack on the facility by an adversary—can conceivably interrupt the whole payment system.[10] The process of creating and installing software and its updates, the development of new generations of hardware, and the establishment of security procedures all leave room for glitches to occur. Here again, operational risk is not solved merely by having a backup facility but involves a host of considerations that encompass the design of the whole system.

Based on the discussion of the typical settlement risk issues posed by emoney, one might

---

[8]See "Bank Computer Fails, Disrupts US Securities," *American Banker*, November 25, 1985, and "Aftermath of an Avalanche: Closer EFT Scrutiny," *Bank Network News*, September 13, 1995 for descriptions of these events.

[9]A "networked product" means forms of emoney that will use physical networks of the Internet and other systems of compatible hardware devices (such as embedded-chip cards and their readers) and software.

[10]The type of attack that one might expect over open networks was seen recently when an Internet access provider was shut down by an adversary that directed thousands of messages per second to the provider. The rate of incoming messages exceeded the computer facility's ability to recognize messages and, in that way, overwhelmed the facility.

imagine that emoney would not raise new or additional systemic concerns for the banking and payment systems. However, the fraud and operational risks in emoney systems are, in many conceivable cases, risks of a systemic nature. Indeed, systemic risks in the context of emoney systems pose new challenges to payment providers. David Chaum, president of the DigiCash Corporation and an expert cryptographer, has pointed out a shortcoming of the Mondex system (a competitor to DigiCash's smart-card system): Mondex allows person-to-person transfer, which opens the possibility of the total collapse of the Mondex system if an organized criminal group were to compromise the security of one card.[11] By compromising one card (or one card reader in the case of the Japanese Pachinko card scheme), a criminal organization could transfer funds to other cards ad infinitum, eroding the value of even 100 percent backing.

[11]"Making E-Money Anonymous," David Chaum, presented at "The Future of Money in the Information Age," Cato Institute's 14th Annual Monetary Conference, May 23, 1996.

IV. Issue of Private Notes in the U.S.

Private issue of bank notes—private banks' liabilities that function as currency—was a widespread practice in the Free Banking era of 1837 to 1863. There were significant differences in banking and payment system stability between the Free Banking era and the National Bank era of 1863 to 1914. According to research by Rolnick and Weber (1985), the Free Banking era, while characterized by many individual bank failures, did not suffer widespread banking and payment system panics. The National Bank period, on the other hand, suffered seven widespread panics that involved suspension of convertibility of deposits into currency. Why the difference in performance of the two eras?

The free banks, so-called because of the relatively easy entry into banking in various states, were state chartered and could issue notes, typically backed by state-issued bonds. The notes did not always trade at par. In fact, specialized publications, called Bank Note Reporters, monitored the prices of the numerous notes in circulation and reported on types of counterfeits as well. If the market perception was that the bonds backing a particular bank's notes were likely to default, the bank's notes would trade at a greater discount from par. Rolnick and Weber find that the contagion effect—failure in one bank triggering a panic in other banks—did not operate. Their explanation asserts that the backing for the state bank notes was transparent. Since banks did not have large interbank liabilities as a result of clearing notes, note holders could adequately distinguish the risks of holding the notes of various banks, discounting the prices of those whose backing was weak, thus leaving the other notes and banks unaffected.

In the National Bank era, bank notes declined as a percentage of the money supply, as Congress placed a 10 percent tax on the issue of state bank notes, and deposits rose in

substitution. National banks issued bank notes backed by federal government bonds, which didn't suffer the default risk associated with some of the state-issued bonds in the earlier era. Deposit money was backed by whatever the bank had on hand as assets— a mixture of loans and securities. Hence, the backing for deposit money was less transparent than the backing for either the national bank notes or the state bank notes of the Free Banking era. Furthermore, the system of payment by check necessitated a clearing and settlement mechanism that was far more elaborate than that for bank notes. Although banks often imposed "exchange fees" to settle a check drawn on one of its accounts, checks of individual banks were not discounted as bank notes were in the Free Banking era. Within systems of correspondent banks, and within the developing check clearinghouses—many of which survive today—checks were settled essentially at par, with only a tiny, standardized exchange fee being collected.

There are three salient differences, then, between the bank note money of the Free Banking era and the deposit money of the National Bank era. First, the backing for state bank notes was more transparent—its value was more easily determined—than for deposit money. Second, the bank notes traded at bank-specific discounts, related to the value of the backing of the notes, while deposit money traded essentially at par (in any case at par less an exchange charge unrelated to the value of the backing of the deposit). Third, the system for clearing the deposits was more elaborate, necessitating the creation of clearinghouses and extensive correspondent networks. Consequently, in the National Bank era, more significant interbank liabilities were involved in the clearing process than in the Free Banking era.

Each of these differences is implicated in the panics of the National Bank era. Little transparency in the value of a bank's assets meant little hope for explicit pricing of deposits, in

contrast to the case bank notes. Hence, uninformed depositors could learn nothing from the exchangeability of their deposit money until it was too late. If backing for deposits consisted of general bank assets, then near business-cycle peaks, when the value of the average bank's assets is expected to decline, a depositor would be more concerned about the value of his own bank's assets. Gorton (1988) has shown that all of the panics occurred near business-cycle peaks (and that most, but not all, business-cycle peaks involved panics). Furthermore, more elaborate interbank clearing systems maintained par exchangeability within the clearinghouse. So when any one member was threatened by a run, the other members were more likely to be forced into a suspension of convertibility themselves because of interbank liabilities that underlay the settlement process. The depositors of clearinghouse members did not know how much of their own deposits were backed by "due froms" of the threatened clearinghouse member.

If these features of the deposit system in the National Bank era tended to preclude the dissemination of bank-specific information by means of explicit pricing of the bank's deposit liabilities, they also contributed to a much more efficient payment system than existed in the Free Banking era. The more generalized acceptance of a monetary instrument at par--National Bank notes away from home, and checks in the local area—lessened the costs of transactions throughout the economy. The necessity of consulting Bank Note Reporters in the Free Banking era and the uncertainty associated with accepting state bank notes were a costly and, I would argue, a socially wasteful process for making payments.

V. Emoney Competition

Emoney competition is itself a possible source of instability in the banking and payment systems. Emoney falls into three broad categories: enhancements to credit card systems,

electronic checks, and electronic bank notes, and as I pointed out previously, competition will primarily take place among firms organized as joint ventures that conduct business as a "branded network." Today, the credit card marketplace and the ATM card marketplace are already ones in which competition is, to a large extent, a competition among such brands. Hence, we can take these markets as paradigms for the type of competition likely to develop in other forms of emoney.

This type of organization for issuance of notes is quite different from the way notes were issued in the Free Banking era, in that they will be issued by a coalition of a joint venture's members and participants, rather than by an individual bank. It is different, too, from the more wholesale organization of the clearinghouses of the National Bank era in that the branded networks will be integrated into both the wholesale (or clearinghouse) and retail (or brand marketing) ends of the market. Several aspects of network competition are worth reviewing for their possible impact on the stability of the payment system.

One observed regularity of competition in such markets is illustrated by the ATM industry. McAndrews (1991) documents that there was a rapid proliferation of ATM networks in the 1980s, cresting at almost 200 different branded ATM networks serving the nation. Subsequently, because of the desire for ubiquitous access by consumers, and because of economies of scale in operations, this number has dwindled to fewer than 50 today. In fact, in 1995 only 20 major brands accounted for 95 percent of ATM activity. A similar dynamic pattern, although with fewer firms, characterized the credit card industry. We can expect the same to occur in electronic bank notes and electronic checks. The early competition is a race for "critical mass": the number of consumers and merchants necessary to provide a useful, convenient, and

widely accepted payment product, even if others compete for the same business. Not all of the entrants will succeed in reaching a critical mass of acceptance.

In network industries, a brand that can quickly establish a large base of users holds a significant advantage. We see in Visa and MasterCard two dominant competitors in the credit card marketplace. Given their "duality" agreement, which allows a bank to belong to both of the systems, there has been no entry into the bank credit card marketplace. Indeed, American Express is currently challenging a Visa rule that forbids a bank both to belong to Visa and to issue American Express credit cards. Being an early leader and requiring exclusive membership can provide significant business advantages, both in achieving the necessary scale to succeed and in deterring potential competitors from entering the industry. This incentive is a key ingredient in causing the rapid proliferation of firms early in the product's life cycle.

The nature of the competition in branded network products itself can be a stability concern in that the competition among the networks can lead to instability in market shares.[12] For example, suppose we have two branded network clearinghouses competing in the same market and they each need (and have) 50 percent of the market, thus obtaining the critical mass of users necessary to make them cost-efficient and sufficiently convenient versus other methods of payment. Because of a merger of member banks, one bank migrates from network A to network B. Suddenly network A is inefficient relative to other payment methods and relative to network B. There is a "run" on the payment instrument offered by A. Now, if branded network B

[12]See "Antitrust in Network Industries," an address by Carl Shapiro, Deputy Assistant Attorney General, Antitrust Division, U.S. Department of Justice, before the American Law Institute and American Bar Association, January 25, 1996, for an overview of competitive practices of firms in network industries.

can quickly handle the increased volume from the former members of A, this may not cause a big problem. But if it can't, systemic problems can arise. In the extreme case, an operational problem caused by the increase in system load may cause significant problems in B and, therefore, for all users of that type of emoney.

Of course, it is an admittedly extreme example to suppose there is a knife-edge critical mass below which the firms cannot fall. But it is a feature of network competition that a critical mass of users is necessary to enter a market or, if a firm is already in the market, to continue to provide services economically. Hence, it is a feature of network competition that networks that steadily lose market share can fail quickly once it is believed that the network's market share will fall below the level necessary to maintain a critical mass.

In the ATM market, the Quest network in Kentucky provides an example. Several owner-member firms of the Quest network joined other networks. Although the Quest network was planning to offer new products and services, it suddenly announced its closure in 1995, because it had lost the ability to maintain a critical mass of users.[13] This does not cause a huge problem in the ATM marketplace because the banks can establish links quickly with alternative providers that can easily handle the increased scale of business. But the problem can be significant if networks have practiced exclusivity (that is, not allowed users to connect to alternative suppliers) or pursued incompatibility (that is, used devices that will not accept the messages of other suppliers).

Exclusivity and incompatibility are strategic choices of firms to achieve acceptance. Exclusivity is a strategy to enforce agents that issue a certain brand of emoney to issue no other

[13]See "EPS' Antitrust Concerns Aren't Over Yet," *Bank Network News,* March 27, 1995.

brand of emoney at the same time. Incompatibility would be achieved with a different security system or other features of the software system that would make communication across different networks practically impossible. Both strategies have long histories in network industries, and both can be justified in economic models, at least for networks that do not dominate their markets. We can expect some emoney competition to be characterized by these practices. However, in the context of system stability, they have the unfortunate effect of limiting the ability of the issuers of one system (which may have failed) to quickly migrate to another system because of the time necessary to install and test the incompatible system.

There are advantages to the prospect of branded network competition, as I have outlined it, in the emoney world. Perhaps monetary exchange in the Free Banking era was impeded by the regrettable necessity of consulting Bank Note Reporters for many transactions. The lack of uniformity of backing for bank notes--even though their backing may have been transparent—was a costly bother when one considers the advantages of a widely accepted means of exchange. Branded networks would work to overcome this problem, at least for electronic bank notes. By placing the backing for the electronic notes in the branded network bank, the networks may prevent the type of confusion over the value of the backing that the National Bank era clearinghouses suffered when one of their members failed or suffered a run. Assets that back electronic checks will likely stay on the books of individual banks. But electronic checks, which are likely to be covered by deposit insurance, do not suffer the problems associated with checks in the National Bank era.

There are some disadvantages associated with the prospect of network competition as well. For example, in the event of a failure or interruption in the operation of the network bank,

the issuer banks will most likely face demands by customers to honor the system's liabilities. Some network business strategies that emphasize incompatibility and exclusivity leave the system unable to cope with the failure of one of the competing networks.

A final issue concerning the likely organization of emoney firms as joint ventures of firms is, who issues the money? First, let's focus on the electronic bank note. Who is the issuer of the electronic bank note? Is it Mondex (or some alternative branded network), or a member bank of Mondex? This may be a trivial question in the sense that for credit cards the same type of organization has been operative for many years. But Visa and MasterCard have faced the issue of merchant banks that go bankrupt owing merchants tens of millions of dollars. The central organizations have not hesitated to pay the merchants to protect the brand.[14] This blurs the distinction between the issuer and the network and raises the question of where the liability for an electronic note lies.

Suppose a bank goes bankrupt after having issued electronic notes (not covered by deposit insurance). News of the bank's failure is known quickly. Is there an increased risk of failure of the branded network organization? The clearinghouses found themselves in this situation in the National Bank era. For the electronic note, Mondex and the proposed SmartCash organization plan to forestall any problems of this sort by putting funds from the sale of electronic notes into a special "bank" in which all electronic note liabilities and assets to back those liabilities are held. Presumably then the failure of a bank would not affect the

[14]This is based on personal communication with officials of Visa and MasterCard. To my knowledge the organizations do not have formal rules for loss sharing in this instance--the issuing banks had already made payment to the merchant banks, which then failed before making payment to the merchant.

creditworthiness of a note it issued. But how would the failure of the branded network bank affect the issuing bank? Would its customers—holders of electronic notes it issued—be satisfied with the answer that it had no liability to them? Indeed, a bank cannot assume that it is absolved of liability in all instances because it deposited all assets and liabilities that back electronic notes in the branded network bank.

For electronic checks the failure of an individual bank once again could jeopardize the solvency of the branded network clearinghouse if individuals felt that the interbank liabilities were of sufficient size to imperil the value of the assets of the clearinghouse. It is not clear how the electronic check providers plan to organize the clearinghouses, but it is likely that individuals' deposit accounts will stay on the books of the individuals' banks and that the clearinghouse for electronic checks will look much like conventional clearinghouses. This subjects them, though, to the same lack of transparency that plagued the clearinghouses of the National Bank era. The difference is that the electronic check will most likely be protected by deposit insurance; therefore, the clearinghouse's balance sheet is less likely to be a concern for systemic stability.

Based on the experience of the National Bank era, it is a sensible idea for the issuers of electronic notes to place all the associated assets and liabilities in the centralized (clearinghouse) branded network bank. This increases transparency of the backing of the issue and reduces the concern when a member issuing bank fails.[15] The experience of the Free Banking era suggests that there are advantages to issuing notes through a branded network. Such a network, if of

[15]However, as we just pointed out, it does not absolve issuing banks of residual liability in the event of failure of the branded network bank.

sufficient size, can increase the acceptability of the bank's notes and reduce the discount (to zero) on the notes by enforcing standard backing for them. One question to ask of these specialized banks is, how much liquidity should they hold against electronic notes? The answer is that, because of fraud risk, 100 percent backing may be insufficient. The risk of what we might call digital counterfeiting is that if it is done well, it can wipe out the reserves of any system. The danger of this for the designers of emoney payments is that the threat of counterfeiting may trigger a run on the bank that can also break the bank. While in the Free Banking era counterfeiting (and the threat of counterfeiting) would affect the prices and acceptability of a bank's notes, the problem of counterfeiting in the emoney world can threaten the systemic stability of banks. The situation is similar for operational risks in large networks, which can cause significant problems for all the users of the network, with implications for the system's stability.

VI. Conclusion: Lessons for Regulation and Control of the Payment and Banking Systems

The fraud and operational risks associated with the emoney world will require solutions to new problems. It is not clear how to protect new systems from fraud. Cryptographers place greater trust in a cryptographic system that has been known and used for a long time without being cracked.[16] Among algorithms of equal mathematical complexity, there is no generally accepted way to judge the efficacy of cryptographic security other than experience. Hence, we can see the difficulties of judging and foreseeing the weak spots in a cryptographic-based security system on open computer networks.

How do system operators react to fraud? In the Japanese case, the first response was to

[16]See Chapters 1 and 7 of Bruce Schneier's *Applied Cryptography* (1993).

lower the amount of value the cards could carry. This action greatly lowers the net benefit of the counterfeit operation, since, in that case, there was a fixed cost to reusing a used card and writing over it. As the value per counterfeit is lowered, the net benefits to counterfeiting fall. Other responses included placing stronger controls on the merchants (the Pachinko parlor operators) who were tolerating obvious fraud (sometimes because of physical threats made by the criminals) in their stores.

The first response corresponds with the cryptographic wisdom that the cost of computing necessary to break a code should exceed the possible gains from breaking it. Therefore, one lesson from these experiences is that the value of retail emoney systems should be of limited amounts. One would think that self-regulation and the risk-aversion of banks would be sufficient to enforce this commonsensical recommendation, but the Japanese case gives one pause in this regard. Moreover, the criticisms from cryptographers concerning the design characteristics of the Mondex system, combined with the discovery of a possible way to compromise the security of a Mondex card, suggest that the risk of counterfeiting will continue to be of concern for these systems.[17]

The operational problems that we've seen in networked payment products, such as the failure at the EDS processing facility, are preventable to the extent that backup facilities are available to fill the gap. I've argued that because of the possibility of rapid migration of customers from one system to another, the planning for backup systems is difficult and may be impossible in a run. Of course, because of the networked nature of emoney, backup facilities

---

[17]See "A Security Scare Ruffles Smart Card Feathers," *Bank Network News*, October 11, 1996.

alone do not address the need for recovery in a crisis; the backup facility may suffer from the same virus that caused the problem in the primary facility.

The uncertainty concerning fraud and operational problems gives rise to the risk of a run on an emoney system. If the public believes that a system's security has been compromised, they may well attempt to shift funds away from the threatened system. This makes important both the liquidity facilities of an emoney system, and the ability of the system to credibly detect and contain fraud and operational problems.

The importance of sufficient liquidity in a payment system clearinghouse is a well-known issue in central banking. In the case of emoney, one novel aspect concerns the role of nonbanks in the provision of payments and the degree to which they will hold adequate reserves for their issuance of actual money (in the form of an emoney system, such as stored-value cards). Another likely result of the development of emoney is the proliferation of private net settlement arrangements within the branded emoney networks. Research by McAndrews and Wasilyew (1995) suggests that even retail net settlement systems, if composed of large number of firms, can lead to significant systemic risk.

Research by McAndrews and Roberds (1995) shows that clearinghouses that can't compel firms to join, or that have limited enforcement powers, are at risk of insufficient provision of reserves as member banks attempt to free ride on the liquidity of their fellow members. This suggests that the Federal Reserve System is the appropriate authority to establish emoney reserve requirements if needed, to monitor and examine the clearinghouses or special-purpose banks of the emoney systems, and to be an enforcement authority over them. As Gilbert and Summers (1996) point out, some new legislation may be required for the Fed to have this

authority. Ultimately, the Fed will be the institution to which these systems turn in a time of crisis, for the lender of last resort is the only agent in the economy that can access liquidity at will. The Fed should have the authority to supervise them, to enforce liquidity provisions that are prudent, and to maintain other standards of operation and risk controls by which modern clearinghouses operate.

The competitive practices of the nascent branded network payment systems will display typical features of network industries. There will be a proliferation of systems, followed by a reduction in the number of independent systems. If some systems should fail quickly, other policies of the competitors can lead to systemic risks. There will be various policies in the different systems, and these policies will be concerned with access to the systems by competitive and complementary system operators and participants; competing standards for products that seek to serve the same market; compatibility among providers' hardware and software; exclusivity agreements among providers and their customers; and the ability to leverage the market power in one product into a dominant position in other products. Such competitive practices, while of antitrust concern for large networks (such as Visa and MasterCard), are potentially at issue regarding payment system stability. The possibility exists for a network to lose critical mass and fail rapidly. This can lead to instability of the payment system if other providers use incompatible technology or are unable to quickly add customers. At the same time some competition among systems is likely to reveal design successes and failures that would not be discovered with a single approach to creating emoney systems.

The emoney world will be unlike the Free Banking era in that it will be coalitions of banks tied together in a branded retail network that will provide emoney—one form of which

will be an electronic bank note. For the electronic bank note, the branded network will likely set up a special-purpose bank to hold the assets and liabilities associated with the issued notes. This arrangement will provide transparency of backing, but it will likely not eliminate all the risks of system failure from the banks. Consequently, banks will retain some risk. Because the electronic check may well have the advantage of deposit insurance, an advantage missing in the National Bank era, it is, in and of itself, not a cause for instability in the banking or payment system. As in the electronic bank note, though, the electronic check will be as much identified with a branded retail network as with the bank that holds the deposit. Banks have experience with this fact in the credit card marketplace.

The organization of emoney firms as branded joint ventures of banks and technology firms gives rise to the uncertainty of who bears the risk of loss under various circumstances. For example, suppose someone steals my digital signature (one means of identification in emoney systems) because of a technology snafu. Does the technology firm that issued the keys to my digital signature bear the loss that occurs when someone then accesses my bank deposit account? Suppose a merchant loads counterfeit change onto my electronic bank note card (while I complied with all the rules of the network). Does the bank honor it? How is the consumer to know the answer to such questions?

I'd like to suggest a "Truth in Minting" act for emoney that spells out the liability and procedures to resolve problems in case of counterfeiting (when a consumer has no way of knowing that counterfeit money is being loaded on to his card), operational failure, theft of security devices (such as the digital identification system of customers), and financial failure of the firm. Such disclosures are important in winning the acceptance of emoney; assuring the

public that the joint venture has thought through the consequences of counterfeiting, theft of identification devices, and so on; and stemming any runs that might be initiated because of uncertainty about these policies (in a time when rumors circulate about possible counterfeits, for example).

I'd also like to suggest further research on the implications of the movement from public to private settlement systems. I've already noted a number of articles in that area, but more needs to be done to assist policymakers in the transition to this new system of payment settlement in our economy. Further research on the industrial organization of financial branded network industries, on the issues of fraud and operational risks in emoney systems, and on the roles disclosure and liability limits can play in the development of risky technologies would all be useful.

The emoney world is one of great promise, partly because of the convenience that it may bring to consumers. But it comes with its own set of risks, which are more likely to be risks of fraud (including counterfeit) and operational risks. The role of nonbanks in the provision of emoney is likely to raise a new concern of adequate liquidity for such firms. Furthermore, the nature of competition among branded retail networks raises the possibility that, just as a firm can quickly gain dominance in such an industry, so too can a firm quickly fail.

All of these issues raise concerns about the stability of the banking and payment systems in the emoney world. There is no way to avoid this world or its risks. However, system operators should learn the lessons of previous failures in similar systems and limit the possible profits obtainable from fraud. Redundancy in operating facilities and extensive testing will certainly need to be standard in emoney systems. The Fed should have the ability to examine and supervise

the clearinghouses associated with the provision of emoney. Emoney providers should have well-understood procedures to resolve problems and to detect and stem losses from counterfeiting or other fraud. Consumers should be informed of these system guidelines to reduce the uncertainty that otherwise exists. Such uncertainty increases the probability of a run on a system rumored to be under attack from counterfeiters.

References

The American Banker, Thompson Information Services, Inc. New York, NY, various issues.

Bank for International Settlements, *Report of the Committee on Interbank Netting Schemes of the Central Banks of the Group of Ten Countries*. Basle, 1990.

Bank Network News, a publication of Faulkner and Gray, Chicago, IL, various issues.

Emmons, William R. "Interbank Netting Agreements and the Distribution of Bank Default Risk," Federal Reserve Bank of St. Louis, Working Paper 95-016A, 1995.

Gilbert, R. Alton, and Bruce J. Summers, "Clearing and Settlement of U.S. Dollar Payments: Back to the Future?" Federal Reserve Bank of St. Louis, May 1996.

Gorton, Gary, "Banking Panics and Business Cycles," *Oxford Economic Papers* 40, 751-781, 1988.

Lacker, Jeffrey M. "Clearing, Settlement, and Monetary Policy," Federal Bank of Richmond, October 1996.

Kahn, Charles M., and William Roberds, "Payment System Settlement and Bank Incentives," Federal Reserve Bank of Atlanta, September 1996.

McAndrews, James, "The Evolution of Shared ATM Networks," *Business Review*, Federal Reserve Bank of Philadelphia, May/June 1991.

McAndrews, James, "Pricing in Vertically Integrated Network Switches," Federal Reserve Bank of Philadelphia, Working Paper No. 96-19, November 1996.

McAndrews, James and Rafael Rob, "Shared Ownership and Pricing in a Network Switch," *International Journal of Industrial Organization*, December 1996.

McAndrews, James and William Roberds, "Banks, Payments, and Coordination," *Journal of Financial Intermediation*, Volume 4, Number 4, 305-327, October 1995.

McAndrews, James, and George Wasilyew, "Simulations of Failure in a Payment System," Federal Reserve Bank of Philadelphia, Working Paper No. 95-19, June 1995.

Rolnick, Arthur J., and Warren E. Weber, "Banking Instability and Regulation in the U.S. Free Banking Era," Federal Reserve Bank of Minneapolis *Quarterly Review*, Summer 1985, 2-9.

Schneier, Bruce, *Applied Cryptography*, John Wiley & Sons, Inc. New York, NY, 1993.