INTERNATIONAL JOURNAL OF BUSINESS, 13(4), 2008 ISSN: 1083–4346

Internet Payment and Banks

Jean-Michel Sahut
Professor of Finance, Amiens School of Management
& CEREGE – University of Poitiers, France
jmsahut@gmail.com

ABSTRACT

In the context of the development of e-commerce on the Internet, a lot of electronic payment systems have been set up in order to secure online payments. To understand the success of Internet payment systems it is necessary to analyse the strategies of e-commerce actors: consumers, "cyber merchants", managers of networks (telecommunications and payment), suppliers of electronic payment services and banks. Our results provide objective explanations of the success factors of Internet payment systems, and the domination of SSL card payment in the market (Turban and Alii, 2006). Moreover, unsuccessful experiences show that it is necessary to consider network effects (Shapiro and Varian, 1998; Shy, 2001) and which business models to implement in order to avoid killing a new Internet payment system before it is launched. This article investigates also the stakes for the banking environment of the Internet payment systems and the problem of money creation.

JEL Classification: E42, E51, G21, G29

Keywords: Electronic payment; Electronic money; Bank; Network effects; Security

I. INTRODUCTION

The electronic commerce procures several benefits to his participants including merchants and consumers, like time savings and convenience. In order to provide these benefits in business to consumer (B2C) transactions, e-commerce needs effective payment systems (Hassler, 2001). Nowadays, online B2C payments are increasing in power in all areas of e-commerce. The enthusiasm caused by the Internet is moderated by the reservations of consumers and companies, due to the chronic insecurity reputation of the Internet. Since the mid- '90s, a plethora of innovative e-payment solutions have emerged. By way of quotation, in November 2001, ePSO (Electronic Payment Systems Observatory) counted nearly 180 systems in Europe (ePSO, 2002). However, in spite of this diversity of payment solutions, we note that the most of them approached the problems of payments from the exclusive angle of security. It created a virulent debate on the liberalization of the use of "strong" cryptography tools which facilitated regulation changes in this field in many countries.

These changes have allowed the emergence of secure Internet payment systems. However, despite its lack of security, payment cards with the Secure Socket Layer (SSL) protocol, which is a communication protocol, but not a payment protocol, always dominate the Internet payment market. In fact, the success of payment solutions can be understood only through the strategies of e-commerce actors: consumers, "cyber merchants", managers of networks (telecommunications and payment), suppliers of electronic payment services and banks.

The object of this article is thus to analyze the Internet payment solutions and their stakes for the banking environment. From this point of view, we will study the needs of users (clients and merchants), and evaluate how the payment systems apply to them. Firstly, after describing the different systems, we will present the set of analysed criteria and justify their importance in the context of users' preferences. Next, we will evaluate, with a panel of experts, electronic payment systems under the criteria previously described in order to understand the success of payment solutions like SSL card payments, despite their defects (Caunter, 2001; Wales, 2003). We will then discuss the stakes of this market. Lastly, we will consider the impact of the diffusion of these payment solutions on the banking environment.

II. INTERNET PAYMENT SYSTEMS

A lot of initiatives tried, on the one hand, to apprehend these various systems, and on the other hand, to compare them. In order to be able to analyze these systems, it is of primary importance to present their features and especially to establish a typology.

Before exposing typologies and features of electronic payment systems, a brief definition of an electronic payment system is essential because, in the literature, the term "electronic payment system" (e-payment system) is used often with senses very different.

In our article, electronic payment systems permit to "*transfer funds without restriction, nor definition as for the support or to the technology used for this purpose*" (Yuan, 2003). They consist "of the instructions to transfer value bundled together with

the communications system" (Kuttner and McAndrews, 2001). These systems introduced thus far generally fall into a special category.

In the literature, we find several proposals for electronic payment systems` typology. The first classification of electronic payment systems, proposed by Medvinsky & Neuman (1993), was based on two criteria, namely the form of the money and the transfer's way of the funds. The authors distinguished between electronic money based systems and credit-debit card based systems.

However, with the evolution of Internet, the development of cryptography and the emergence of several kinds of payment solutions, other classifications have come. First, we note the study of Havinga and alii (1996) which distinguishes between systems based on traditional means of payment, especially bank cards, virtual money and credit-debit systems based on virtual accounts. Then, in 1997, Wayner introduces a new more practical typology by keeping the category of "virtual money based systems" (presented previously by Medvinsky and Neuman (1993) and Havinga and alii (1996)) and distinguishing the category of "account based systems". Asokan and alii (1997) proposed also another typology based on the flows exchanged between the payer and the paid. After that, a second wave of classification will follow, we noted the researches of Kuttner & McAndrews (2001), Abrazhevich (2001) and Stroborn and alii (2004). The analysis of all these works carried out us to conclude that electronic payment system thus far generally fall into one of two major families: those based on accounts and those based on electronic money. OECD (2000) proposed this classification too. Nevertheless, the contribution of the present article is to detail these two families of systems. Indeed, we were able to identify several categories constituting each family based on their operational principle. Thus, our approach reveals two levels in classification of electronic payment systems. So, we keep the first level of classification that distinct between of "account-based systems" and "electronic money based systems". In the second level, for the first family, we brought together payment systems in five main categories: smart card based systems, electronic checks, email payments, other electronic systems for micro payment, and mobile payments. For the second family, we distinguish between electronic wallet, virtual wallet and virtual money. The following scheme summarizes our typology of electronic payment system.

In Table 1, we present the classification of payments systems, accompanied by a brief description of each of them. Next, we expand on their characteristics.

Table 1
Payment systems characteristics

Systems	Types	Examples	Features	Transaction Value
Account Based Systems				
Card Based Systems	Traditional card based systems	Cybermut Telecommerce Payline SIPS	Based on the SSL protocol Security problems with buyer and vendor authentication	Macro-payments (due to relatively high costs of a single transaction)
	Dynamic virtual card	GIE Carte Bancaire		
	SET – CyberCOMM	GIE Carte Bancaire	Alternative solutions focused on security improvement	
Electronic Checks		NetChex CheckFree	Dematerialization of traditional checks Have not gained large acceptance More popular in the USA and France	Macro-payments (cheaper than card systems but still relatively expensive)
E-mail Payments		Paypal, Billpoint, Yahoo PayDirect, Citibank's C2it	E-mails used for notification P2P market	Micro-payments Macro-payments P 2 P payments
Other Electronic Solutions for micro payments	Telecom kiosk	Tel2Get, EasyClick	Service included in phone bill	Micro-payments
	ISP kiosk	w-HA	Monthly payments per use, act, volume or subscription	
	Personal account	Firstgate, Clik&Buy	Service included in Internet bill	
	Pre-paid card	EasyCode, Carte à Plus	Scratch and phone cards	
Mobile Payments	Mobile wallet Mobile data verification Built-in data-storing chip Built-in smart card reader	Platform initiatives: J2ME (SunMicrosystems) Mobile Payment Services Association (Orange, Telephonica Mobiles, T-Mobile, Vodafone)	Development phase Attempts to create an interoperable platform	Planned common use for micro-payments Application to macro-payments rather doubtful
Electronic Money Systems	Electronic or virtual wallet	Proton, Moneo, Geldkarte, Visa Cash	Based on smart cards or software Prepayment systems Bank does not participate in transactions	Micro-payments
	Virtual money	Cyberbucks (Digicash), Beenzs		

A. Account-based Systems

Credit and debit card payment with the SSL (Secure Socket Layer) protocol is the most common way of paying on the Internet. An SSL-based transaction assures the encryption and integrity of a transferred message. Merchants can use it in two ways: with or without an intermediary. The version without intermediary (SSLWI) assures message encryption and integrity but exposes both parties to other risks. As a customer communicates their card number and expiry date directly to a merchant, the card number can be illegally used. Moreover, the existence of the merchant is not ensured. The vendor in turn does not have a guarantee that the buyer exists and that they will not repudiate the purchase afterwards. The version with an intermediary (SSLI) assumes the participation of a third trusted party, which guarantees the existence of the vendor as well as denying them access to the buyer's card data. It increases security on the customer's side, assuring them of the merchant's authentication and data confidentiality. Nonetheless, the latter is still not able to identify the buyer. This asymmetry can be eliminated by integrating an electronic signature system into the technology. The electronic signature allows the authentication of the buyer. However, such a solution requires the buyer to have a card reader (CyberCOMM[1]) or an electronic certificate (SET: Secure Electronic Transaction), which, because it involves additional costs, would have more difficulty in achieving a sufficient market acceptance. Due to the failure of SET, Visa decided to develop the payment protocol 3D Secure[2], which was inspired by SET but makes it much less constraining for merchants (installation of a plug in software only). Thus this system moves complexity towards the e-commerce platform of Visa and banks, and merchants do not have the responsibility of engaging in the validation procedure of the transaction. Moreover, Visa guarantees non-repudiation transactions to the merchants, and thus removes the unpaid transactions (about 5% of all transactions in France[3]). At the same time, dynamic virtual bank cards (DVC) have emerged. They allow banks to generate a single-use card, cryptogram number and expiry date every time the card user buys online. This solution does not require any additional applications for merchants and significantly minimizes the risk of the transaction. In France, the GIE Carte Bancaire launched e-Carte Bleue in April 2002[4].

An electronic check is the transposition of a traditional check into a dematerialised environment. It uses a digital signature based on key public infrastructure (PKI) that can be automatically verified for authenticity. The customer sends his payment order to a merchant, who presents it to an e-check issuing institution, in order to authenticate it and make the payment. Then, the data related to the e-check is transmitted to a clearing system. The procedure of fund transfer is the same as in the case of a paper check. Similar to the card based system, electronic checks are used for macro-payments but their unit transaction costs are lower. Nevertheless, due to their limited popularity in traditional payments (in fact, used only in the United States and France), they do not constitute a serious threat to card based systems.

E-mail based payments are also used for micro-payments. They are designed for small businesses as well as for P2P (person-to-person) transactions. Online auctions constitute the largest source of e-mail payment revenues. However, they are also used to pay for online gambling and adult entertainment, as well as low-value international

payments. As a matter of fact, e-mail payments are not processed via e-mail. E-mails are used for notification, but funds are transferred in the same way banks settle inter-bank transactions. A customer loads an amount of money from his bank account into a service provider account, then specifies the sum of money to be sent and enters the email address of a recipient. Both customer and recipient are notified that the money has been sent. The recipient receives the money and withdraws it from their bank account.

Apart from electronic/virtual wallets and e-mail payments, micro-payments can be handled by incorporating the consumption of a service into phone or Internet billing. Payments included in the phone bill are paid via a telecom kiosk, while Internet bill-based solutions can be operated in Internet service provider (ISP) kiosks and personal account systems. These solutions are very easy to use but they are more expensive than the other micro-payment solutions and have some serious limitations, as they frequently require two telephone lines - lines using ADSL or additional applications. Another solution is based on pre-paid phone and scratch cards but it has just started to be commercially deployed.

Mobile payments are the payments carried out by PTDs (Personal Trusted Devices), such as wireless phones or PDA (Personal Digital Assistant), as well as by other emerging ones such as set-top boxes for interactive television systems or game consoles. Mobile payments can be used for: wireless Internet shopping, face-to-face shopping, vending machines, event and public transport ticketing, P2P (Person-to-Person) payments, pay-as-you-use payments, etc. Although mobile commerce and mobile payment seem very attractive and convenient to users, after a few years of research and different projects, their popularity is still far from ubiquitous.

B. Electronic money based Systems

At the outset, electronic money included three types of payment systems: electronic wallets, virtual wallets and virtual money. Electronic and virtual wallets first require money to be deposited with the manager of the payment system, by various traditional means of payment. Electronic wallets are based on smart card technology, which is used to store data about the customer's funds. Cash is loaded into the e-wallet by a transfer from the cardholder's account. In this way, banks are not involved in the transaction at the moment of purchase. E-wallets mainly target the micro-payment market. At present, they can be used at points of sale, vending machines, parking meters, ticket machines, public payphones, and set-top boxes for interactive TV, etc. The integration of this system into Internet payments requires a smart card reader on the customer’s side. The simplest and most realistic way to achieve this is to build readers into mobile phones. Such a solution can accelerate the development of pay-per-use services, such as online games, music, ticketing or mass transit systems. Systems based on the virtual wallet are quite similar to those based on electronic wallets. The only difference is that cash is stocked on the software instead of on a smart card. After having created an account at the system issuer, the buyer only has to enter their ID and password at the moment of transaction. The virtual wallet is used for macro and micro-payments via the Internet. Virtual money, like Cyberbuck (Digicash) or Beenz, were pure electronic currencies. The consumer buys coins from the provider of this sort of

money and stores them on his hard drive. Each coin is protected by an encrypted number and an encoded signature, in order to avoid unauthorized duplication or counterfeiting. The shape of this sort of money is not very different from the money included in virtual wallets. But the principles are different because it is not necessary to deposit money before receiving electronic money and there is no official exchange rate for it, as with an official currency like the US dollar.

III. METHODOLOGY AND CRITERIA

This study contains two parts: the selection of criteria and the evaluation process of payment solutions. In the first part, we have selected the criteria and their importance from a review of the literature and individual interviews with the 32 French experts who participated in the evaluation process in March 2005.

For the second part of our study, we used a modified Delphi process[5]. A Delphi panel offers a systematic way to reach a consensus thanks to the judgement of experts or professionals in a given field, (who consult each other at periodic intervals during a given period). The same participants are generally consulted on a number of different series of questions, by means of short questionnaires or by discussions in groups. In phase one, we collected the opinions of 32 French experts. In phase two, a small panel of 7 experts interpreted the results from the participants of the first phase and drew conclusions by consensus.

Our review of the literature enabled us to identify several researches which tried to develop and introduce criteria permitting to assess the electronic payment systems on Internet. For this purpose, Schmidt and Muller (1999) affirm to have identified more that 30 assessment criteria in the literature. In what concerns us, we distinguish two literature development phases. The first phase relates to "constructivists" work in the matter. The main researches are those of Neuman and Medvinsky (1995), Furche and Wrightson (1996), Havinga and alii (1996), Asokan and alii (1997), MacKie-Mason and White (1997) and Wayner (1997). These papers developed and insisted, especially, on the technical aspects as determinant criteria of success of an electronic payment system. But, the use's experience feedback of those systems demonstrates that costumers use mainly the solutions which one notes problems regularly, namely the bank cards (Caunter, 2001; Wales, 2003). For that, at the beginning of the years 2000, the second phase of research works which granted, in addition to the technical dimension, an importance to the various users' needs of electronic payment systems, immersed (Bellare and alii, 2000; Wright, 2002; Tsiakis and Stephanides, 2005).

We recall that MacKie-Mason and White (1997) and Schmidt & Muller (1999) highlight the significant number of the criteria identified to assess an electronic payment system. They also underline that these criteria are not the same from an author to another. We point out that this number certainly increased with the advent of the literature's second phase. Nevertheless, a thorough reading of the literature allows us to define the main criteria of evaluation and the elements of measurement.

The following table synthesizes the four types of criteria as well as the review of the literature which justifies them.

Table 2
Criteria in electronic payment literature

Criteria	Elements of measurement	Source in literature
Security	• Identification • Confidentiality • Authentification • Integrity • Customer solvability • Non-repudiation • Durability • Liquidity/convertibility • Anonymity	• Bellare and Alii (2000) • Abrazhevich D. (2001) • Sahut (2001) • Wright (2002) • Peffers and Ma (2003) • Tsiakis and Stephanides (2005)
Cost	• Customer • Seller	• Schmidt and Müller (1999) • Hadidi and Siripaiboon (1999) • Wright (2002) • Chou, Lee, and Chung (2004)
Convenience	• Installation/subscription • Process complexity/speed	• Wright (2002) • Lee and Tsang (2003) • Chou, Lee, and Chung (2004)
Universality	• Payment type • Interoperability	• Hadidi and Siripaiboon (1999) • Abrazhevich (2001) • Kannen and Alii (2003)

A. Security

According to the literature and professional studies, the greatest deterrent for customers paying via the Internet is the possibility of fraud. Forrester (2004) proved that for every $1,000 of Internet business transactions, $1 is still fraudulent[6]. Then, we have decided to attribute the highest importance to the set of security factors. Having analysed the components of security systems, we have distinguished nine levels of security: identification, confidentiality, authentication, data integrity, customer solvability, non-repudiation, durability, liquidity/convertibility and anonymity/traceability. This distinction is based on already existing research works (e.g., Sahut, 2001) and enriched with three additional factors mentioned by Peffers and Ma (2003). All of the evaluation criteria have been attributed the same relative weight in the composition of the global security score. The only exceptions are the non-repudiation and anonymity/traceability criteria, which are considered a particularly important component of security systems. It is difficult to balance the protection of sellers and the control of personal data use. A great concern of online customers is the possibility of keeping payment activities private and of preventing third parties from observing and tracking spending habits (Camponovo and Pigneur, 2003).

The nine security criteria are provided below:

1. **Identification:** in order to initiate a transaction both parties have to be identified: a buyer, who is obliged to pay, and a merchant, who is obliged to provide a product or service. When buyers pay online they cannot use clues from direct observation of the vendor's appearance and behaviour to identify them,, as would be possible if they were face-to-face. The same risk applies to the merchants; buyers can acquire goods without paying.
2. **Confidentiality:** only indispensable transaction details are revealed to the parties, other data remain unknown. For instance, the vendor should not know a customer's card number when an intermediary provides him with a payment certification. The intermediary, in turn, is not supposed to be informed of purchase details. Another problem is to ensure that an unintended third party will not intercept data, as their possible abusive use is the major Internet risk concern.
3. **Authentication:** electronic transactions have to be authenticated. Honest intentions of trading parties are ensured by the terms of transaction (product features and quantity, price, delivery date etc.). The electronic translation of this contract is the key factor of the future development of electronic commerce. Customers require a guarantee that a merchant will not charge them for an imaginary purchase.
4. **Data integrity:** during the session, payment data cannot be intentionally or unintentionally tampered with.
5. **Non-repudiation:** merchants want to be sure that the payment obligation will not be repudiated afterwards.
6. **Customer solvency:** customer solvency can be verified by a merchant or, to a certain extent, guaranteed by a bank.
7. **Durability:** users want to be sure that their data or transaction details can be verified and are not going to be misused after a certain period of time. The transaction system has to be resistant to any hardware or software defaults.
8. **Liquidity/convertibility:** transferred money can be withdrawn or converted to another currency immediately, without any additional procedures.
9. **Anonymity (Privacy):** anonymity (or privacy) refers to a customer's ability to do a transaction on the Internet, without her/his identity being known. When a credit card is used, the user needs to be identified in order to have a secure payment. But customers want to be anonymous to the merchants and prefer not to leave any traces of completed transactions.

B. Cost

The cost of an e-payment system is often an under estimated criterion when considering users' choices, as is the development of e-payment systems through network effects. A crucial condition to the payment system's success is that the cost of payment systems, to both the customer and the merchant, should be inexpensive, especially at the beginning in order to reach a large base of users, which leads to positive network effects (Leibbrandt, 2004). The solutions that designers also have to pay attention to are the fixed transaction fees and charges. This risk factor is particularly important in the case of micro-payments, as a unit transaction cost determines a minimal payment that yields profits. Nevertheless, the global weight of this factor is lower than the

importance of the security criteria. In most of the existing business models the transaction costs are covered by sellers who, subsequently, get their money back by charging customers for other services.

Customer cost: depending on business models, costs can include installation, subscription and recurrent usage. The recurrent costs can take the form of commissions on transactions, or monthly subscription fees.
Seller cost: sellers are able to cover the installation or subscription costs. However, they can also be charged recurrent transaction fees.

C. Convenience

Other than a small number of technological enthusiasts, most parties to electronic transactions are reluctant to learn about complex processes or applications. Convenience is considered one of the deciding factors of the system's success (Lee and Alii, 2003). Payment systems are expected to be transparent and integrated with a universal net environment (e.g., SSL card payment). Thus, payment systems should require the least amount of effort and equipment. Consequently, complex proprietary solutions, requiring installation of additional software or equipment, (e.g., CyberCOMM) were rejected soon after their introduction. This criterion in our analysis has the same global importance as the universality criterion.

Installation/subscription: payers are unwilling to follow lengthy or over-sophisticated installation and subscription procedures.
Process complexity/speed: all users (buyers and sellers) expect the payment system to be fast and trouble-free. They do not want to waste their time on complex payment procedures.

D. Universality

According to Kannen and alii (2003), payment systems should have as few constraints as possible, as far as software, localization, minimal or maximal amount of payment, or currency of payment are concerned, to allow adoption by any customer or merchant. This feature is also attributed a lower weight than security factors[7]. The lack of interoperability among systems is a great barrier to their future development. This problem has also led to many failures of electronic payment solutions.

Payment type: this criterion depends on the possibility of making micro-payments, macro-payments and payments in foreign currencies.
Interoperability: this criterion measures the payment system compatibility with other electronic payment systems and infrastructures.

Table 3 summarizes the set of criteria and their relative importance to the success of electronic payment systems, defined from the expert interviews. The maximum score corresponds to the relatively highest importance of the feature.

Table 3
Set of evaluation criteria

Feature	Weight
Security	
▪ Identification	2
▪ Confidentiality	2
▪ Authentification	2
▪ Integrity	2
▪ Customer solvability	2
▪ Non-repudiation	3
▪ Durability	2
▪ Liquidity/convertibility	2
▪ Anonymity	3
Total Security Score	**20**
Cost	
▪ Customer	5
▪ Seller	5
Total Cost Score	**10**
Convenience	
▪ Installation/subscription	5
▪ Process complexity/speed	5
Total Convenience Score	**10**
Universality	
▪ Payment type	5
▪ Interoperability	5
Total Universality Score	**10**
Maximal Score	**50**

IV. RESULTS AND INTERPRETATION

A first analysis makes it possible to distinguish three groups from the systems, according to their mark.

mark ≤ 30: characterizes systems that have disappeared, like SET or CyberComm. These very secure solutions neglect the other factors, so their global mark is bad. In particular, SET-based systems were too slow.

30 < mark < 35: systems whose development is still dubious, like e-check or e-carte bleue. They are less secure than the first group's systems, but their cost and convenience partially fills this gap.
mark > 35: it is a group where the payment systems are already successes, even if the mark, as regards security, of the systems tested is rather average.

The mark obtained by the email payment system Paypal shows that it could, in the middle term, compete with the SSL card payment. Moreover, the structure of risks

is different for email payments compared to SSL payments: the management of the email payment system appears as a risk factor, because it can go bankrupt (which harms the durability and the liquidity/convertibility of the payment system) but the global security increases (security mark going from 8 to 15).

Table 4
Evaluation of payment system

Legend:
SSLI = credit and debit card payment with the SSL protocol 3.0 with an intermediary (bank or payment service provider) who insure the payment processing and can guarantee payments.
SSLWI = credit and debit card payment with the SSL protocol 3.0 without an intermediary.
For a description of SSL protocol 3.0: http://wp.netscape.com/eng/ssl3/3-SPEC.HTM#2
DVD = Dynamic Virtual Card

	SET	**SSLI**	**SSL WI**	**Cyber Comm**	**E-carte Bleue** (DVC)	**Odysseo** (virtual wallet)	**eCheck .Net**	**Paypal**
Security (max 20)								
▪ Identification	1.5	1	1	2	1.5	1.5	1	1.5
▪ Confidentiality	2	2	2	2	2	2	2	2
▪ Authentification	1.5	1	1	2	1.5	1	1	2
▪ Integrity	2	2	2	2	2	2	2	2
▪ Customer solvability	2	1	0	2	0	2	0	2
▪ Non-repudiation	3	0	0	3	1	3	3	1.5
▪ Durability	2	2	2	2	2	1	2	1
▪ Liquidity/convertibility	2	2	2	2	2	0	2	1
▪ Anonymity (Privacy)	2	2	0	2	2	3	2	2
Total Security Score	**18**	**13**	**10**	**19**	**14**	**15.5**	**15**	**15**
Cost (max 10)								
▪ Customer	3	5	5	1	1	3	4	5
▪ Seller	0	2	5	0	4	2	2	4
Total Cost Score	**3**	**7**	**10**	**1**	**5**	**5**	**6**	**9**
Convenience (max 10)								
▪ Installation/subscription	2.5	5	5	0.5	3	2	2.5	3.5
▪ Process complexity	0.5	3	5	0.5	4	2	2.5	4.5
Total Convenience Score	**3**	**8**	**10**	**1**	**7**	**4**	**6**	**8**
Universality (max 10)								
▪ Payment type	3	3	3	3	3	4.5	3	4
▪ Interoperability	2	5	5	2	5	1	3	3
Total Universality Score	**5**	**8**	**8**	**5**	**8**	**5.5**	**6**	**7**
TOTAL (max 50)	**29**	**36**	**38**	**26**	**34**	**30**	**32**	**39**

The domination of SSL card payment on the market is also explained by network effects where the cost of the system plays a dominating role at its beginning.

In general, consumers do not take into account the network effects they may cause that can, in some cases, lead to a blockage. Consumers do not make their choice of consumption based on intrinsic technological quality, but according to the number of people who have already chosen the system. This makes technology gravitational and increases its chances of becoming essential in the future. The launching of a payment system must be done on the basis of an economic logic and, more importantly, on a logic of "network good". The network effects are thus starting to increase the levels of adoption. In the same manner, the means of Internet payment falls under these problems of "network good", which makes it possible to understand why the market is dominated by SSL card payment despite its precarious security. Its facility and ease of use, together with its integration with the two principal browsers, "Internet Explorer" and "Netscape Navigator", have created an established base of users, with which other systems such as SET, cannot compete, in spite of their superiority in terms of security. Leibbrandt (2004) suggests subsidizing the development, using the most effective technology in order to generate a significant established user base, could lead to increased product or service prices afterwards.

To avoid the death of highly secure solutions, and thus more expensive solutions, it is necessary to question which business model to implement. Indeed, the traditional business models used by the banks (direct invoicing of buyers and merchants) led to resounding failures.

V. IMPACT ON THE BANKING SYSTEM

As money is the lifeblood of economies, electronic payments have strongly influenced the banking sector. Banks are no longer the only managers of money flows. Moreover, they seem to be losing control over their creation. The problem of uncontrolled money creation outside the usual banking institutions is considered quite serious and constitutes a topic of many economic debates. Nowadays, money can be created independently of the banking systems by e-payment providers. This happens when the e-payment providers grant consumer credits. The dilution of the role of central banks in monetary policy can lead to a huge dysfunction in the whole banking system. Endless discussions have led to the conclusion that e-payment providers should not be permitted to award credit unless they have the status of credit institutions. However, the dynamic development of the Internet economy weakens the decision-making power of banks and the banking system. Therefore, they have to search for alternative solutions. Currently, central banks can compensate the loss of control over money creation by issuing electronic money or augmenting the level of obligatory reserves. In the long term new tools will have to be provided, otherwise economies may experience very serious problems.

The loss of control is not the only consequence of the development of e-payment systems. Another issue results from the fact that banks exposed to tough competition from new entrants can no longer be sure of the stability of their profits. The growing number of payment service providers decreases the predictability of customer choices and increases the variability of revenue. Moreover, since a significant part of information on customers' investments, solvency, credit strategies etc. is no longer

registered in the databases of central banks, the ability of central banks to identify the objectives and priorities of monetary policy is significantly undermined.

All of these factors can lead to serious deregulation of banking systems. Economies may face serious problems resulting from their unpreparedness for the new marketplace. Therefore, we cannot neglect the urgent necessity of adjusting financial and legal systems to the rules of the Internet economy.

VI. CONCLUSION

Since the emergence of electronic payments, their features and strategies of development have been constantly changing. At the outset, e-payment providers focused exclusively on security issues proposing proprietary systems that were quite expensive and user-unfriendly. Having realized that the market rejects such solutions, they started concentrating on costs and convenience, proposing less secure systems. Surprisingly, they did much better. The best example is the SSL card payment, which has always been heavily criticized for its insecurity. Its leading position in macro-payments is due to several factors: simplicity, interoperability and popularity of the original payment mode (offline transactions by card) in traditional payment systems.

This article shows that for an Internet payment system to be successful it is important that it is designed to meet the user's need. To be the best in one aspect, like security, is not enough to get a large market share. SSL card payments achieved a critical market share because of its ability in terms of cost and convenience, despite its insufficiencies with respect to security. They now dominate the e-payment market. It is a non-optimal equilibrium because it is the most widely-used payment system, but its low security slows down e-commerce development. This situation seems difficult to change because network effects play a crucial role. Only email payment systems appear as a serious competitor. Another solution is governmental intervention because consumers do not take into account the network effects that they cause, which lead to a blocking on SSL - a very non-efficient technology.

The first step to take to get out of this vicious circle is to make all interested parties realise that a change in the present situation can bring important benefits. The introduction of a new, more advantageous system could increase the level of payment service security, decrease losses caused by frauds as well as allowing the better positioning of participants within the value chain. However, the real introduction of such a system requires a joint effort of all parties and this condition is the fundamental factor impeding the changes. Although governmental interventionism is inconsistent with the rules of free market economy, it seems that imposing legal restrictions could constitute an efficient way to induce some changes. The introductions of normalisation standards or of administrative constraints are examples of possible state actions.

ENDNOTES

1. http://www.journaldunet.com/9911/991116cybercomm.shtml (accessed 12/05/07)
2. http://partnernetwork.visa.com/pf/3dsec/main.jsp (accessed 12/05/07)
3. http://www.fia-net.com/ (accessed 27/02/07)
4. http://www.e-cartebleue.com/client/home.asp (accessed 27/02/07)

5. Linstone H. (1975), *The Delphi Method*, Addison Wesley, Linstone H. & M. Turoff : http://www.is.njit.edu/pubs/delphibook/ (accessed 10/04/07)
6. http://www.forrester.com/find?N=50058 (accessed 27/12/06)
7. http://searchcio.techtarget.com/originalContent/0,289142,sid19_gci798143,00.html (accessed 27/12/06)

REFERENCES

Abrazhevich, D., 2001, "Classification and Characteristics of Electronic Payment systems", *Lecture Notes in Computer Science*, VOL. 2115, pp. 81-90.

Asokan, N., Janson, P., Steiner, M., and Waidner, M., 1997, "The State of the Art in Electronic Payment Systems", IEEE Computer 30, no. 9, p. 28–35.

Baddeley, M., 2004, "Using E-Cash in the New Economy: An Economic Analysis of Micropayments Systems", *Journal of Electronic Commerce Research*, VOL. 5, NO.4, novembre 2004, pp. 239-53.

Bella, G., Massacci, F., and Paulson, L.C., 2005, "An Overview of the Verification of SET", *International Journal of Information Security*, *Springer-Verlag*, Volume 4, No. 1.

Bellare, M., Garay, J.A., Hauser, R., Herzberg, A., Krawczyk, H., Steiner, M., Van Herrenweghen, E., and Waidner, M. "Design, Implementation and Deployment of the iKP Secure Electronic Payment System". *IEEE Journal on Selected Areas in Communication*, special issue on Network Security, April.

Bounie, D. and Vaninetti, L., 2001, "E-payments: Which Systems in Europe for the Coming Years?" *Issue Report* N.13, June.

Camponovo, G. and Pigneur, Y., 2003, "Analyzing the M-Business Landscape", *Annales des Télécommunications*, janvier.

Caunter, N., 2001, "The Real Cost of Fraud to E-Tailers", *Computer Fraud & Security*, No. 1, p. 17.

Chou, Y., Lee, C., and Chung, J., 2004, "Understanding M-commerce Payment Systems through the Analytic Hierarchy Process", *Journal of Business Research*, Vol.57, 1423-1430.

ePSO, 2002, "E-Payments in Europe - The Eurosystem's Perspective", *Issues Paper, Banque Centrale Européenne, septembre*, 2002, p. 48.

Furche, A. and Wrightson, G., 1996, "Computer Money: A Systematic Overview of Electronic Payment Systems", *Morgan Kaufmann Pub*, October 1996, p. 108.

Hadidi, R., Siripaiboon, J., 1999, "A Comparative Evaluation of Electronic Payment Systems," In Proceedings of the Association for Information Systems (AIS) Americas Conference, Milwaukee, Wisconsin, August.

Hassler, V., 2001, "Security Fundamentals for E-Commerce" *Artech House, Massachusetts.*

Havinga, P.J., Smit, G.J., and Helme A., 1996, "Survey of Electronic Payment Methods and Systems", Proceedings *Euromedia '*96, pp. 180–192.

Kannen, M., Leischner, M. and Stein, T., 2003, "A Framework for Providing Electronic Payment Services", *10th annual workshop of HP-OVUA*, July 6-9, Geneva.

Kuttner, Kenneth N. and McAndrews, James, 2001, "Personal On-Line Payments". *Economic Policy Review*, Vol. 7, No. 3, December.

Lee, T.O., Yip, Y.L., Tsang, C.M., and Ng, K.W., 2003, "An Agent-Based Micropayment System for E-Commerce", *Lecture Notes in Computer Science, Springer-Verlag Heidelberg*, June, p 247.

Leibbrandt, J.G., 2004, "Payment Systems and Network Effects", *Thesis*: University of Maastricht, June.

Mackie-Mason, J. and White, K., 1997, "Evaluating and selecting digital payment mechanisms, interconnection and the Internet", Telecommunications Policy Research Conference, Mahwah, NJ, pp. 113–34.

Medvinsky, G. and Neuman, B.C., 1993, "Electronic Currency for the Internet", NASA, ISI/RS-93-414.

Neuman, C. and Medvinsky, G., 1995, "Requirements for Network Payment: The NetCheque Perspective", *Proceedings of IEEE Compcon '95*, mars 1995, p. 5.

Peffers, K., and Ma, W., 2003, "An Agenda for Research about the Value of Payment System for Transactions in Electronic Commerce", *Journal of Information technology Theory and Application*, 4:4, p. 1-16.

Potter, R.E. and Balthazard, P.A., 2002, "Understanding Human Interaction and Performance in the Virtual Team", *The Journal of Information Technology Theory and Application*, 4:1, p. 1-23.

Sahut, J-M., 2001, "Les paiements électroniques sur Internet", *Gestion 2000, Mars-Avril.*

Shapiro, C and Varian, H.R., 1998, "Information Rules: A Strategic Guide to the Network Economy", *Harvard Business School Press.*

Schmidt, C. and Müller, R., 1999, "A Framework for Micropayment Evaluation", *Netnomics*, Volume 1, No. 2, pp. 187-200.

Shy, O., 2001, "The Economics of Network Industries", *Cambridge University Press.*

Stroborn, K., Heitmann, A., Leibold, K. and Frank, G., 2004, "Internet Payments in Germany: A Classificatory Framework and Empirical Evidence", *Journal of Business Research*, Elsevier Science Publishing Company, Inc., pp. 1431-1437.

Turban, E., King, D., Lee, J.K., and Viehland, D., 2006, *Electronic Commerce: A Managerial Perspective*, Prentice-Hall, New York.

Tsiakis, T. and Stephanides, G., 2005, The Concept of Security and Trust in Electronic Payments. *Computers & Security* 24(1): 10-15.

Wales, E., 2003, "E-Commerce Counts Cost of Online Card Fraud", *Computer Fraud & Security*, No. 1, 9-11.

Wayner, P., 1997, *Digital Cash: Commerce on the Net*, (2nd ed.), AP Professional, London.

Wright, D., 2002, "Comparative Evaluation of Electronic Payment Systems", *INFOR*, Volume 40, No. 1, 71-85.

Yuan, L.C., 2003, « Nouveaux Instruments de Paiement: Une Analyse du point de vue de la Banque Centrale », Working papers, n°10, Banque Centrale du Luxembourg, novembre 2003, p. 60.