

## The Evolution of Internet Banking

Mohammed Sohail Mustafa\*

### *Abstract*

*The transformation of business caused by E-business & E-commerce applications of the Internet & related technologies demonstrates that information systems & information technology are essential ingredients for business survival & success. This paper focuses on the problems & hurdles that ravaged so many would-be startups are well known & the Internet banking model has been re-engineered as a result. It is too early to tell whether these second generation Web banking ventures will succeed or not; however, they have improved their odds by addressing the fundamental problems that plague their stand-alone counterparts. Since only few banks (especially foreign banks & some local private banks) recently launched their services through on-line banking, so the concepts of electronic banking is still not so much popular to the users. In preparing this article, I also found that local banks are misinterpreting the mechanisms of on-line banking with off-line banking services, such as: by introducing off-line automated teller machine. So I did not only emphasize on the functions of on-line banking, but also discussed about different procedures, mechanisms, prerequisites & requirements of a bank to go for on-line banking.*

---

\* Lecturer, School of Business, North South University.

**Key Words:** <sup>1</sup>WWW, <sup>2</sup>HTTP, <sup>3</sup>URL, <sup>4</sup>Financial Institutions, <sup>5</sup>E-cash.

## 1. Introduction

Consumer behavior is changing partly because of more spare time. The way of use of financial services is characterized by individuality, mobility, independence of place and time, and flexibility. Financial transactions caused by purchases will more and more be carried out by non-and near-banks. These facts represent big challenges for providers of financial services. More and more the Internet is considered to be a "strategic weapon".

Financial services companies are using the Internet as a new distribution channel. The goals are:

- Complex products may be offered in an equivalent quality with lower costs to more potential customers;
- There may be contacts from each place of earth at any time of day or night.

This means that financial institutions may enlarge their market area without building new offices or field services. Because of its image as an innovative corporation, better interacting possibilities, the usage of rationalization potentials as, the improvement of its competitive situation by development of core competencies together with the construction of market entry barriers, it may be possible to increase profits and market shares.

One way of exploiting rationalization of potentials is the implementation of the entire transaction (from purchase to payment) under a common user interface. Information collected in operative database of financial institutions allows them to act as information brokers. Offering special information closed user groups may result in more intense customer commitments, as well as customer bonding. Know-how that is built up by Internet presence may be used to facilitate Internet pres-

ence of smaller companies. The use of digital coin-based money to completely settle transactions in the Internet is a new service provided by financial institutions.

## **2. Internet as a Distribution Channel**

Distribution channels are physical capacities to build up customer contacts in a systematic way in order to inform, counsel and sell products and services. Like American Online or CompuServe, the Internet is a so-called electronic distribution channel. Combined with self-service terminals and telecommunication equipment, electronic distribution channels are technical channels within the class of media distribution channels. Another example for a media distribution channel is direct mail.

Today, media distribution channels are an important way of distributing information and managing standard transactions. Counseling is mostly done in branch offices or by field workers. Together, personal and media distribution channels are called internal distribution channels. On the other side there are external distribution channels like salesman or franchising partners.

The world-wide web (WWW, 3W, W3) is the most well-known and most important Internet service. A standard user interface to be able to address a large number of users was one of the development goals of the WWW. The WWW is a world-wide network consisting of a large number of various computers. The user interface integrates other Internet services like ftp, telnet, email, etc. The WWW is based on hypertext and hypermedia principles. Therefore, it is possible to present information in a well-structured manner. Documents are connected via links. Besides text documents, it is possible to include pictures, sound and videos.

The client/server-architecture forms the basic implementation platform of the WWW. Data are stored on a WWW-server. The server

software responds to inquiries from WWW-clients and sends files to the clients. The client interprets the files and presents the information on its screen. In modern browsers features allowing execution of application modules on client computers are implemented. Corresponding programming languages are Java, JavaScript or ActiveX.

Communication between client and server is done through the hypertext transfer protocol (HTTP). HTTP is a very simple protocol. It allows short(er) response times and reduced use of the server. On the other hand, a connection has to be build up for each inquiry. Each document is addressed by a unique key. The uniform resource locator (URL) is formed by the address of the server, the (directory) path and the file name. Sometimes it is useful to append further data, e.g. to control programs that may be executed.

### **3. Areas of Use of the Internet in Financial Institutions**

Generally we may distinguish four classes of Internet use in financial institutions :

- Information presentation;
- Information presentation together with two way (asynchronous) communication (e.g. email to request further information);
- Interaction with user (e.g. execution of programs with individual customer data);
- Transaction banking (e.g. electronic payments).

#### **3.1 Information Presentation**

Information may be providing in connection with one or two way communication. One-way communication means that the institution uses the Internet only as a presentation medium for its products and services. The simplest way to use two-way communication is to allow users to send electronic mails to the server in order to ask for further information or make suggestions with respect to the Internet site.

Interaction with customers requires quick information exchange. Information provided by the user controls the information offered by the server. If the customer is identified and authenticated, connecting to operative systems of the financial institution may be possible. Then, often very little information has to be provided by the customer since data stored in the databases of the financial institution may be used.

Presentation of product information may be used to initiate new contacts. Implemented product models permit the constructions of optimal insurance or financing contracts by using simpler components [Sei 97]. Using mathematical models the customer may analyze his portfolios. To do so, he may use simulation techniques, what-if-analysis and other similar techniques.

### **3.2 Internet Transactions**

There are a large number of different financial institutions are doing Internet transactions to facilitate customer payments, securities transactions, applications for loans or insurance acquisitions.

Due to the structure and the intention of the Internet to be an open network, high security risks are involved with financial transactions. Today, various techniques and standards are offered in order to control or even avoid these risks. Basic requirements are as follows:

- Customer and financial institution have to authenticate each other.
- Private data have to be encoded. Cryptographic algorithms used need to have certain characteristics.
- A digital signature is necessary to get binding legal contracts. These digital signatures have to secure the integrity of signed documents.

Based on these requirements, HTTP is extended to S-HTTP. Because the security level of this protocol still is not high enough various addi-

tional techniques and standards have been developed. Examples are the home-banking communication interface (HBCI), secure electronic transactions (SET) or secure socket layer (SSL).

Different types of methods are used or currently tested. These methods may be classified into hardware-and/or software-based solutions. Hardware-based solutions use chip that is physically located between computer and keyboard. Such a chip is unique. Note, that the system is hardly usable with laptop computers and/or with different financial institutions.

More often software-based methods are used. Personal identification numbers (PIN) identify the user. For each transaction, a transaction number (TAN) is necessary. Data are encoded using algorithms like IDEA with a 128 bit-key or RSA with a 1.024 bit-key. A higher level of security may be reached by means of a so-called electronic fingerprint. This fingerprint is taken before and after the transmission. Then, both versions are compared. In case of any differences the transactions are aborted.

## **4. Digital Coin-based money**

### **4.1 Basic Requirements**

Digital money may only be used for electronic commerce in an efficient and effective way if an infrastructure on a high technical level exists. A large transmission rate is a prerequisite for simultaneous transmission of product information to potential customers. Access has to be simple and economical. Therefore, private households need PCs with suitable software. If these technical conditions are met, security problems have to be addressed [Oma 97].

## 4.2 Actors Involved

New payment systems like digital coin-based money are only successful if they are accepted by a large number of persons. To get this acceptance all actors involved should have sufficient benefits that exceed their costs.

- The primary interest of customers is to carry out purchase in a comfortable manner. Associated payments should be possible from home in a simple and efficient way.
- The dealer usually has to bear the costs of payment transactions. On the other hand, he may benefit through an improved image (being innovative) and possibly higher sales. Also, he may be able to reduce branch offices and sales personnel.
- System providers are intermediaries. Dealer's sales are forwarded to the financial institution. The system provider is responsible for transactions clearance. Moreover, he provides supporting services (problem management, user training). Again, revenues consist of fees and service charges.
- *Financial institutions* may promote certain systems. As was already mentioned, confidence in electronic payment systems is a key success factor. Note, however, that a large number of financial institutions, typically smaller ones in regional markets, may have difficulties to participate due to high costs and know-how required.
- *Trust center* control digital signature keys. They are responsible for the integrity of transmitted data and the authenticity of contractors. Trust centers help to secure confidence in a certain payment system. Their revenues consist of royalties and other service fees.

## 4.3 System Requirement

The following requirements are implementation independent. They are useful in comparing different payment systems.

- Open systems need security features to manage electronic payments. Security may be realized by cryptographic methods in connection with transaction numbers (TAN).
- A large number of customers have to be able to simultaneously carry out payment transactions. The systems have to work with a large number of customers and should be easily expandable. Hence, scalability is an important criterion.
- Small and smallest payments (micro- and pico-payments) should be possible. The corresponding accounting systems have to be efficient and effective.
- The system has to be transparent. Customers have to be aware that payment actually takes place. System usage has to be simple.
- Private households should be able to accept digital money (micro-merchants).
- Electronic data transfers, as well as electronic payments may be traceable. Then it is possible to analyze e.g. payment information and to construct detailed customer profiles. In most cases customers wish to stay anonymous.
- Digital coin consists of a number of bits. Hence, there is some possibility that copies of the coins are made and eventually put into circulation. This phenomenon is known as the *double spending problem*. Hence, the payment system needs mechanisms to recognize and/or prevent repeated payments with the same digital coin.
- Digital coin-based payment systems have a nominal value problem. In order that a certain amount may be paid in the form of new coins. Alternatively, all coins have the same smallest possible face value (e.g. one cent or even a fraction in the US). The last alternative requires that a large number of digital coins have to circulate and to be checked for authenticity.
- Digital money should be convertible into "real" money, whenever this is desired.

- Confidence in electronic currency means that stable exchange rates between electronic and "real" currencies necessary. If the exchange rates are unstable there is a chance of arbitrage profits. This, in turn, would reduce confidence since losses due to value fluctuations are possible.
- Digital money is stored locally on hard disks or other media. In case of disk crashes or other problems mechanisms to recover the original state are necessary.

#### **4.4 Basic Principles of Electronic Coin-based Payments Systems**

Due to the increasing importance of electronic commerce via the Internet the importance of digital money increases. Representing virtual money in an electronic world means that properties and functionalities like anonymity, authenticity, as well as pico-payments are considered. Like virtual money, digital coins have an inherent value.

Depending on the way digital money is implemented there exist different cryptographic methods and organizational precautions to avoid the usage of forged money. Basically, there are two different types of digital coin-based money :

- Using specific cryptographic method, the anonymity of digital money may be achieved. Then neither the financial institution nor the dealer may build up a connection between the customer and coins used by them [Cha 92, p. 96].
- Coins with customer identifying characteristics allow the financial institution to identify the customer and to follow up on payments where the coin has been used in.

Also, the payment process may be classified into online and offline transactions. Figure 1 summarizes the different approaches.

- If an online payment takes place, the coins will be checked immediately for authenticity. This implies that a digital coin is used

only once. The financial institution needs to check the authenticity by using a list of all coins that have been issued or a list of all coins that have been sent in for credit.

- In case of offline payments, the coins may be used more than once. To avoid double spending, it is necessary to store information about the user or the user on the coin in order to be able to perform checks later. Anonymity may be guaranteed by so-called secret sharing. Then, the financial institution only gets information in case of double spending.

	Offline Payments	Online Payments
Anonymous digital coins	Secret sharing by storing some information on the coin.	Blinding and immediate check by the financial institution.
Coins with identifying characteristics	Storage of information about the transaction on the coin.	Immediate check by the financial institution.

Figure 1: Security approaches to avoid copying digital coins [Sch 97, p. 59].

## 4.5 Examples of Digital Coin-based Money

### 4.5.1 E-Cash

E-Cash is anonymous digital money whose validity is checked online by the corresponding financial institution. E-Cash is developed by DigiCash and is offered by Mark Twain Bank, St. Louis since 1995. Deutsche Bank AG, Frankfurt (main) offers E-Cash as a pilot project to its customers since October 1997.

The customer withdraws digital money from his eCash-account using so-called blinding method and stores it on its hard disk. The blinding method works as follows. The client encodes a serial number and sends it to the financial institution. The financial institution certifies the coin and transfers it back to the customer. The customer then

decodes the serial number. Hence, the serial number is not known to the financial institution, which guarantees anonymity. In order to avoid double spending, the financial institution has to record the serial numbers of all incoming coins. At each purchase via the Internet the customer gives digital coins to the dealer. The dealer immediately transfers the coins to his bank in order to check for validity. The dealer's bank registers the numbers of the coins issued without tracing them back to the customer. *Finally*, the dealer is credited and delivers products and services ordered [Pan 96].

Digital coins may be used only once. E-Cash may be considered to be a currency of its own. Financial institutions have to use special accounts. They also guarantee conversion into "real" money. As a consequence, central banks like the Bundesbank or the Federal Reserve Bank have difficulties in controlling money supply (financial institutions may create additional money and thereby increase the amount of money supplied; this is well-known in the case of so-called check booker deposit money [Eva 92, and bnbsp; p. 410])

E-Cash security is achieved by using an asymmetric cryptographic algorithm. Account access may be protected additionally by using personal passwords. The storage of a coin's serial number does prevent double spending. There may be a problem with scalability, however. The costs of checking for authenticity of coins are relatively high because checks have to be done online. This means that the suitability for micro- and pico-payments has to be evaluated carefully. Each person who has an eCash-account may accept eCash coins. The blinding method, as was already indicated, guarantees anonymity.

#### **4.5.2 NetCash**

The NetCash method is developed at the University of Southern California. One important goal of this project is the use of already existing accounting systems and procedures in financial institutions. This

reduces initial investment costs. In contrast to eCash, this method is based on a decentralized approach. Consequently, problems associated with a large number of coins and participants may be solved more easily. Therefore, reduced anonymity is accepted and the corporation of all participating financial institutions is required.

The system is based on independent distributed currency servers. Currency servers are locations to exchange anonymous into non-anonymous money. Each currency server possesses an account on an accounting server. Clearing is done by the currency servers. It is necessary that the integrity of the servers is certified and that currency servers accept coins from other currency servers. NetCash-coins have a face value and a serial number. Also, the address of the issuing server and an expiry date is stored.

The payment process using NetCash is as follows:

- i. The customer gets NetCash-coins from a currency server;
- ii. These coins are encoded with a public key and send to the dealer;
- iii. Anonymity of the customer may be guaranteed by using a new session key for each message;
- iv. The dealer transfers the coins received immediately to his currency server. From the currency server he neither receives new coins nor the corresponding value will be credited to his account;
- v. The currency server does final clearing.

### **4.5.3 Millicent**

The Millicent method is developed by Digital Equipment Corporation (DEC) to manage and smallest payments (e.g. payment for getting information from the Internet about news and stock quotations or payment for small programs like Java-applets)

The customer buys broker scrip with a defined value using his credit or by debating a suitable bank or broker account. Such scrip is like a

telephone card. At the time of purchase the customer exchanges parts of the scrip into a dealer's scrip. This scrip is then send to the dealer. The dealer collects all scrip and exchanges them into "real" money.

To guarantee the security of this method one-way-hash-functions that may be evaluated quickly (e.g.MD-5) are used. Furthermore, the costs of illegally decoding scrip (this means finding the inverse of the hash-function used) are much higher than the scrip's value. A large number of transactions are possible at low costs compared to other two methods discussed. In principal, each person may be registered at a broker and may then accept digital payments. There is no anonymity but there is the possibility to buy scrip from different brokers. Thus, no comprehensive user profile may be built.

## 5. Conclusion

Currently most financial institutions use the Internet as a presentation medium. Often there is a possibility to request additional information or to perform individual calculations. Business transactions are rather rare at least in most European countries. On the other hand, a lot of effort is devoted to construct solutions to manage financial routine transactions like money transfers, opening and closing of accounts, implementation and deletion of standing orders and much more. Payment systems are developed to facilitate electronic commerce. In order to realize significant rationalization potentials, no isolated but integrated solutions that support existing business processes are required [Sei 97]. Collaboration between competing financial institutions may be necessary to cut down development costs [Sti 97b].

In general, financial institutions have to decide on their Internet presence. Is it worth to invest significant sums? It can be shown that there are not necessarily first mover advantages [Sti 97a]. On the other hand, fast reactions to actions of competitors are difficult since significant know-how is required to quickly build up an Internet presence.

This implies that waiting too long may be extremely harmful and expensive. Consequently, a good strategy should be built up know-how by means of small or medium pilot projects. Actions of competitors, as well as the development of the Internet should be monitored closely.

## References

1. [Cha 92] Chaum, D. (1992): Achieving Electronic Privacy. In: Scientific American, August, pp. 97-101.
2. [Eva 92] Evans, J. (1992): International Finance. A Markets Approach. Orlando.
3. [Oma 97] O'Mahony, D., Peirce, M., Tewari, H. (1997): Electronic Payment Systems. Boston, London.
4. [Pan 96] Panurach, P. (1996): Money in Electronic Commerce: Digital Cash, Electronic Funds Transfer, and E-cash. In: Communications of the ACM, Vol. 39, No. 6, pp. 45-50.
5. [Sch 97] Schuster, R., Farber, J., Eberl, M. (1997): Digital Cash. Berlin.
6. [Sei 97] Seitz, J., Stickel, E. (1997): Cooperative Software Development Supporting Financial Product Representation and Distribution in the World-wide Web. In: Wojtkowski, G. & Wojtkowski, W. & Wrycza, S. (Eds.): Proceedings of the Sixth International Conference on Information Systems Development (ISD '97), Boise: Plenum Press.
7. [Sti 97a] Stickel, E. (1997): Problems Associated with Cost/benefit Analysis for strategic Information Systems. In: Wojtkowski, G. & Wojtkowski, W. & Wrycza, S. (Eds): Proceedings of the Sixth International Conference on Information Systems Development (ISD '97), Boise: Plenum Press.
8. [Sti 97b] Stickel, E. (1997): Collaboration among Competitors- A first Economic Analysis.

9. Berryman K., Harrington L., Layton-Rodin D., Rerolle V. (1998): Current Research: Electronic Commerce: Three emerging strategies. *The Mckinsey Quarterly*, 1998 Number 1, pp. 152-159.
10. Geyer J. (1997): Adoption of e-Finance. Research Note SPA-101, Gartner Group, 28/5/1997.

#### URL

- <http://www.electronicbanker.com>
- <http://www.open-vision.com>
- <http://www.firstdirect.co.uk>
- <http://www.advance-bank.de>
- [http://www.soversignbank.com"](http://www.soversignbank.com)
- <http://www.soversignbank.com>
- <http://www.amcity.com>