A Common Currency System for Spontaneous Transactions on Public Networks
-
Is it feasible?

Wolfgang Röckelein, Ronald Maier

Department of Business Informatics
University of Regensburg
Universitätsstraße 31
D-93053 Regensburg
Germany

E-Mail: [wolfgang.roeckelein, ronald.maier] @wiwi.uni-regensburg.de
WWW: http://www-informatik.wiwi.uni-regensburg.de/wi3/
Tel. +49-941-943-2998 or -2273
Fax: +49-941-943-4986

To appear in the Proceedings of the
Ninth International Conference on EDI-IOS
Electronic Commerce for Trade Efficiency and Effectiveness
Bled, Slovenia, June 10-12, 1996

Abstract

The aim of this paper is to examine indications for a common currency system on the Internet for spontaneous transactions. First the framework for such a currency system and the theoretical background on common currencies are discussed. Examples of common currencies already in use are evaluated according to a set of criteria developed by the authors. Furthermore the theoretical ideas and the insights gained by the evaluation of these currency systems are synthesized to answer the question in the title. The paper ends with an outlook into the future.

1. Introduction

The Internet is a large international network, which has already proven its great flexibility in the past. The number of users is estimated as well over 20 million people worldwide today (see [RESNICK94], p. xxi). Although the Internet has its roots in a university background the vast growth in the last years is due to the commercial area. In most countries there are several competing service providers (see [SCHELLER94], pp. 14-17 for a list of providers in Germany) which are connected with one another.

Open electronic networks, especially the Internet, have shown an enormous growth during the last years. Much of this growth is attributed to commercial activities. Among marketing activities and pre-arranged transactions (like EDI on the Internet) there is already a place for spontaneous purchases (see [RÖCKELEIN95] for a list of systems for purchases on the Internet). A vital part of a purchase is the payment subtransaction. The global nature of public networks like the Internet leads to special problems concerning the currency used for such a transaction. Both parties might be located in different countries and might have no idea of the value of the currency of the other country. Some participants might be reluctant to use the currency of another country, even the almost ubiquitous US dollar is avoided by some people, perhaps for economic, political or cultural reasons. Systems for spontaneous electronic payments should therefore consider the global nature of the Internet. A solution to this might be a common currency for the Internet.

In chapter two we lay the theoretical background of our work by defining the basic terms used in this paper and by summarizing the theory of optimum currency areas and the free banking theory. These theories are used as the theoretical basis for our analysis of the feasibility of common currency systems in the Internet. In chapter three a set of criteria used for the evaluation of the common currency systems already available in the Internet is described. In chapter four the results of the application of this framework to the existing common currency systems are presented. In chapter five we synthesize the theoretical ideas of chapter two and the insights gained by the evaluation of the currency systems in use and try to give an answer to the question in the title of our paper. Chapter six summarizes our findings and gives an outlook to the future.

2. Theoretical Background and Definitions of Terms

The following terms are central to our arguments: purchases, Internet economy, common currency and spontaneous transaction.

(1) Purchases in the German civil law

For the analysis of purchases a model that subdivides such a transaction seems to be appropriate. The authors have chosen the model used in the German civil law.
According to German civil law (as laid down in the BGB - Bürgerliches Gesetzbuch) a successful purchase consists of the following steps:

(a) The merchant places an “invitation to offer." This can be via advertising, via a store front window with products and price tags and similar means.

(b) The buyer makes an offer to purchase something. For example he asks the clerk “I want to buy that vase from your ad in the newspaper today.”
(c) The merchant agrees to that. With these two declarations of will the two parties enter a legal contract.
(d) The handing over of the object purchased constitutes a separate contract.
(e) Similarly the payment is also a separate contract.

While this view of the purchase with the base contract and the two separate “abstract” fulfillment contracts is not known in many other countries (see e.g. [LARENZ81], pp. 10-21) it helps in the discussion of conducting purchases in electronic networks because of the clear separation of the different steps. This paper focuses exclusively on subpart (e).

(2) Internet economy

The term „economy“ refers to the complex structure of economic relations which result from the process of collaboration between public and private actors (e.g. state, companies, private households) [VAHLEN93]. It can be characterised in many ways (e.g. the economic system, the social system, the degree of exchange with other economies). Apart from standing for „real“ systems (e.g. the German economy) the term „economy“ also denotes a hypothetic construct which is used as the basis of economic modelling.

The term „Internet economy“ as used in this paper refers to those economic relations which take place in the Internet. The definition is not a strict one, however, as the great majority of economic relations only partially takes place on the Internet. We want to focus on those economic activities, for which the use of the Internet helps to reduce the distance between producer and customer **substantially**. In this sense the following three types of activities can be distinguished:
strong reduction: e.g. subscription of an electronic periodical in which all three contracts (base contract, handing over and payment) are handled over the Internet;
medium reduction: e.g. the purchase of genuine specialities of certain areas (e.g. Scottish whiskey, cuckoo clocks of the German Black Forest) in which the Internet brings together producer and customer, supports the payment procedure and eventually mediates the actual shipping of the product;
low reduction: e.g. the purchase of groceries at a local store after seeing an electronic advertisement (in the sense of an invitation to offer) in which the Internet is of no great use in reducing the distance between producer and customer.

(3) Common currency

The term „currency“ is used in (at least) two ways [PEARCE81]:
- strictly, that component of a country’s money stock that literally circulates from hand to hand, i.e. coin and banknotes;
- in a broader sense, a country’s money, e.g. sterling, the US dollar, in which case it refers to the total money stock of that country.

In this paper the first definition is not applicable for obvious reasons. Considering the second definition one can argue that the strict reference to a country is not necessary so that one could define the term „currency“ comprising a „money“ which is used in more than one country (as is the case with the ECU, see below). The term „common currency“ refers to this

type of currency which is used in an area not restricted to national boundaries even if it substitutes the national currencies of the countries involved (as would be the case if the European Community (EC) countries would form a monetary union) or if it is issued addition to the national currencies (as is the case with the US dollar, which is used in many countries along with the national currencies). In the case of the Internet, a common currency could be used throughout the wired world.

When discussing the issue of a common currency on the Internet the following question arises: Do common currency systems provide real „currencies“ in a conventional sense or simply new financial instruments (like cheques)?

First the answer of this question depends on the design of the system. Whereas the current systems tend to resemble a new financial instrument, one can also imagine the creation of „real“ cash. Currently, electronic cash systems require centralized clearing to eliminate double spending and to mint new coins which is not necessary in the case of real cash. Electronic cash systems are more like an order to transfer funds from one account or place of holding to another which is very similar to the definition of cheque. However, there are also some differences between traditional financial instruments and electronic cash: e.g. electronic cash is basically anonymous, untraceable and it is a bearer instrument. So it seems to us that the current definitions are poor in capturing the notion of electronic cash.

(4) Spontaneous transaction

According to the intensity of the reflection involved one can classify purchases as follows (see [BÄNSCH93], p. 10; the types of purchases are sorted so that the intensity decreases):

- extensive purchases,
- limited purchases,
- habitualized purchases,
- spontaneous purchases (also called „impulse“ purchases).

The term „spontaneous transaction“ describes a transaction in which the „customer“ reacts without gathering, ordering and evaluating information (in the sense of developing criteria and comparing alternatives) before the decision. The reaction comes directly to the stimuli of certain offerings (see [BÄNSCH93], p. 231). Spontaneous transactions usually involve small amounts.

In the following we discuss two theories which can be applied to the evaluation of common currencies: the theory of optimum currency areas by Mundell with its extensions by McKinnon and DeGrauwe and the free-banking theory by Hayek.

The theory of optimum currency areas

A theory of optimum currency areas was first developed by Robert Mundell in 1961 (see [MUNDELL61]). This theory can be applied to evaluate the economic consequences of introducing a common currency. According to his work the feasibility of a common currency (that is of fixed exchange rates opposed to floating ones) for two regions depends on the extent of the factor mobility between those two regions. Factor mobility means that capital and labor can freely float back and forth between the regions. After some disturbance the adaption through the transfer, especially of labor, substitutes the adaption through a change of

the exchange rate that would take place otherwise. This theory was expanded by McKinnon shortly after (see [MCKINNON63]). He states that it is not only the factor mobility that plays an important role in determining the advantage of a common currency but also the extent of the trade volume between those two regions (called „openness“ of regions).

DeGrauwe [DEGRAUWE94] combines these approaches and uses the theory of optimum currency areas to compare costs and benefits of a monetary union. The cost side of a common currency stems from the fact that when a country relinquishes its national currency, it also relinquishes an instrument of economic policy. Difficulties arise if the countries using a common currency are hit by asymmetric shocks (both demand and supply shocks), if the countries have different preferences about inflation and unemployment, if the differences in labour market institutions are substantial, if the growth rates of GDP are different and/or if different fiscal systems exist („Seigniorage“ problem). The benefits of a common currency result from eliminating transaction costs (direct: elimination of costs for exchanging money; indirect: reducing the scope for price discrimination) and from welfare gains through less uncertainty about future exchange rates (which results e.g. in a better working price mechanism) (for a detailed description of costs and benefits of a common currency see [DEGRAUWE94], pp. 5ff and 60ff).

The comparison of costs and benefits leads to the conclusion that the usefulness of a common currency depends heavily on the two variables „real divergence of the economies of the countries involved“ and „labour market flexibility“. The more the regions (or countries) that are planning to introduce a common currency differ from one another, the more labour market flexibility is needed to equalize asymmetric shocks.

The free-banking theory

A common currency of the Internet would be supranational hence it will likely also be non-governmental. Thus another currency theory should be considered here, the free banking theory. A well-known advocate of free banking was the Nobel laureate F.A. Hayek who devoted a whole book (“Denationalization of money” [HAYEK90]) to this theory. Free banking means that private owned banks can issue their own (paper) money. These different sorts of money compete for the acceptance by the market participants. This happens through the extent of trust people place into these different currencies[1]. This is a radicalization of the free commerce idea (versus communist state-controlled economy): Not only the economy is relatively free from state influence but also the monetary system. Note that this does not prevent governments from setting framework rules for the private currencies as they currently do for the economy.

Case Study: The Private ECU[2]

Some of the ideas of these theories have become reality with the use of the private ECU. The ECU (which stands for “European Currency Unit”) was created by the countries of the EC in 1978. It is defined as a basket index of several national currencies of EC countries. Although

1 One often voiced critique uses Gresham’s Law (see for example [DEGRAUWE94], p. 174f) which claims that bad money drives out good money. Note that this applies only if both currencies are legal tender and therefore has no relevance here (see [BOFINGER84], p. 934). Instead the opposite will happen: good money drives out the bad (see [HAYEK90], p. 41ff and p. 43). However, this process can be delayed by the limited speed of the spread of information.

2 Another kind of money not under direct governmental/central bank control is the Eurodollar market, see [GLASNER89], p. 161ff.

it was introduced at first only to support accounting among the EC institutions, it was soon much wider used in the private market (see for example [MEHNERT88] or [LOWRY93]). [HERLT94] places the ECU as third in the euro-bond market for 1991, for the international bond market the ECU is on the fifth place with a share of 8% for the same year (according to [BUNDESBANK92], p. 200). For private use financial instruments such as travelers' checks, credit cards, current and saving accounts denominated in ECU where created. Also, the ECU is used for the settlement of import and export. It must be stressed that all this took place without enforcement from the governments of the EC countries. As opposed to the plans of the EC countries signed in the Maastricht treaty, some authors even recommend to use a sort of private ECU (or in some cases a new currency, called „hard ECU") to ensure a smooth transition to a monetary union in Europe. The argument runs that thus the European citizens, not the governments, would decide when they are willing to abolish their national currencies (see e.g. [DEGRAUWE94], who presents also arguments against this view).

3. Framework for payment transactions on the Internet

We developed a set of criteria which can be used to evaluate systems for conducting spontaneous payment transactions on the Internet. The criteria are classified into the following three groups: mandatory or kill requirements, important requirements and optional requirements. Without paying attention to the mandatory requirements the system is most probably simply not credible enough to survive. The important requirements refer to those properties that make the system usable which is a necessary prerequisite for acceptance of the system. For money that is not accepted is worthless, the „important" criteria are in a sense „mandatory", too. However, we want to make a distinction between the more technical arguments and those criteria that refer to the actual use of the systems. The optional requirements are somewhat „nice-to-have". Maybe different systems for conducting payment transactions on the Internet provide different features referring to these criteria. The development of the following requirements was based on the theoretical analysis of common currencies (see chapter 2) and on literature dealing with electronic cash systems in detail (see e.g. [MATONIS95] whose additional properties result basically from the differences among current or proposed schemes).

In addition to these requirements the start-up-procedure of a currency system is another major issue. At first a basic stock of money has to be brought into circulation. This, however, can lead to inflation from excessive money supply which has to be avoided in order to induce credibility into the system.

3.1 Mandatory Requirements

Security

- transmission security: The payment transmission across the public network should be immune to alteration or eavesdropping.
- prevention and detection of fraud: Fraud (for example orders for which other people are billed, theft, sellers place a higher charge than the agreed amount, etc.) is prevented or can at least be detected and the identity of the defrauders can be revealed.

Backing
The value of the electronic cash has to be backed by some commodity perceived as highly valuable (e.g. gold), institution (e.g. a government or a bank which is credible around the world) or it has to be indexed (e.g. to other currencies or to a basket of currencies, see [GLASNER89], p. 227-241).

3.2 Important Requirements

Provision for anonymity
There are different types of anonymity:

- counterparty anonymity: Both contract parties do not know the identity of each other. This can also be unidirectional (for example the buyer knows the merchant but not the other way round as it is with day-to-day cash purchases on the street).
- issuer anonymity: The company employing the payment system is not able to collect data on the individual purchases like the amount or the goods involved.
- pseudonymity: This is a weaker form of anonymity. If a party is known only via a pseudonym, the link between the real person and the pseudonym can only be found by a third party that might be the company running the payment system. In this way the merchant can link different purchases by the same customer with each other but not with the real person.)

The reason for this criterion is that most people like to enjoy some privacy, especially concerning spontaneous transactions. Merchants and payment system providers should be unable to build extensive customer profiles.

Setup and transaction costs
The cost for the setup of such a system (such as opening an account) and the transaction cost should be low. High setup costs would be an obstacle to a wide acceptance of the system. Considering the rather small amounts of money which are likely to be exchanged in spontaneous transactions neither the producers/retailers nor the customers will accept a payment system which requires high transaction costs.

Easy use
A payment system should be easy to install and use. No deep knowledge of technical and network issues should be necessary. The user should never be left unclear on the parameters of the financial transaction he is conducting at the moment. Important parameters are e.g. the identity of the recipient and the amount involved. Financial systems and especially currencies work only if they are used by a sufficient number of people. Thus, the entry barriers should be low, so that every Internet user can easily use the system.

Two-way transactions
Users are not divided into two classes (merchants and consumers), so everybody can act as the originator or recipient of a cash transfer. This is an important prerequisite because otherwise the electronic cash is only a poor substitute for „real“ cash.

Portability of coins

One should be able to move electronic cash from one computer to another, and this should also be possible via non-network means (e.g. disks). This criterion goes along with the criterion „easy use“, as portability makes the handling of electronic cash easier. It would be especially useful during the start-up phase of an electronic cash system as for example a certain amount of electronic money on disk could be handed out for free with the purchase of goods.

Off-line capability
Users can conduct transactions even in the absence of a network connection, and especially without a connection to some central computer operating the system. This is an important prerequisite as spontaneous transactions are not carried out if they cannot be completed within a certain amount of time.

3.3 Optional Requirements

Duration of the coins
Cash coins should not expire, that is they should never loose their value. For security reasons in some systems it is required that cash coins have to be used for transactions within a certain period of time from issuing. After that time they cannot be used freely and have to be returned to the issuing bank.

Divisible coins
Cash coins should be divisible by the customers themselves, that is they can be divided into smaller coins without having to call in a bank to change. Thus, an advantage of electronic currency over real currency would be given as no changing would be necessary throughout the system (which lowers transaction costs all the more, see [OkOh92] and [Wayner96], p. 68-74 who describe such a system).

Use of non-political unit of value
The currency is not denominated in an existing national currency (see also chapter 2). This would certainly increase the willingness to accept the currency in some parts of the world where the people, the national governments or the central banks respectively are not eager to accept another nation’s currency.

4. Technology for Common Currency Systems

In this chapter we evaluate the common currency systems currently provided on the Internet using the set of criteria we developed in chapter three. Beforehand we illustrate the credit card transaction as a surrogate for a common currency. We investigate its shortcomings which makes this system unsuitable for **spontaneous** transactions on the Internet.

4.1 Credit Card Transaction as a Surrogate for a Common Currency

The present day settling method for international financial transactions of the laypeople is the use of credit cards (CC for short). A buyer communicates some data from the credit card (a set of credit card number, expiration date and the name of the holder is regularly used) to the

seller, who first performs some checks[3] on the data. The merchant then initiates a transaction through the world wide CC system to credit him with the amount and to debit the customer. The communication necessary to initiate such a transaction can easily be accomplished on the Internet. This could be done via electronic mail or via forms on the WorldWideWeb, see figure 1.

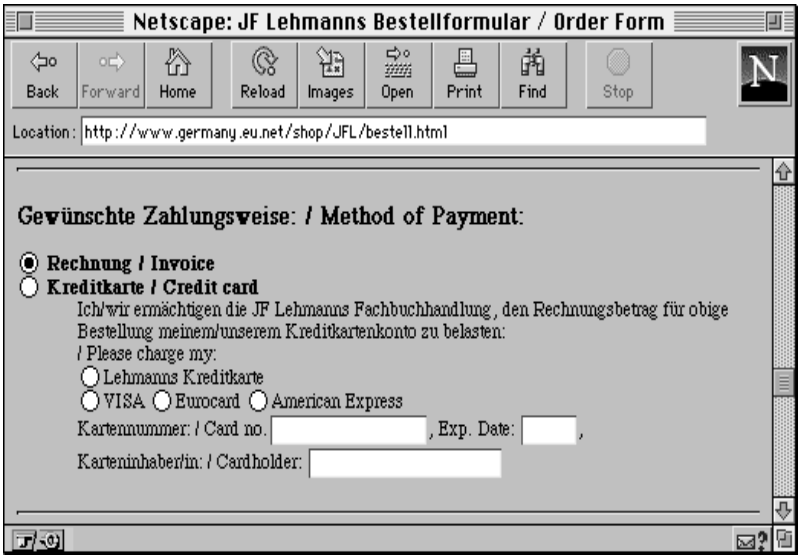

Figure 1: Form on the WorldWideWeb to input CC details

Unfortunately such a scheme has severe security problems. Since Internet transmissions are normally clear text and travel through lots of intermediate routers automated snooping of credit card details poses a real threat, for everyone who has got access to the above mentioned dataset could place orders using this data. CC account holders are able to revoke any fraudulant debits but this requires close monitoring of their monthly receipts. Also each reversed transaction is costly since it requires manual processing and thus raises the cost of the credit card system. There are several solutions in development, one of which is to encrypt transmissions involving sensitive data. A WorldWideWeb form similar to that in the figure above, but employing encryption is shown in figure 2 (Note the unbroken key in the lower left corner indicating this fact).

3 A credit card number for example has a check digit.

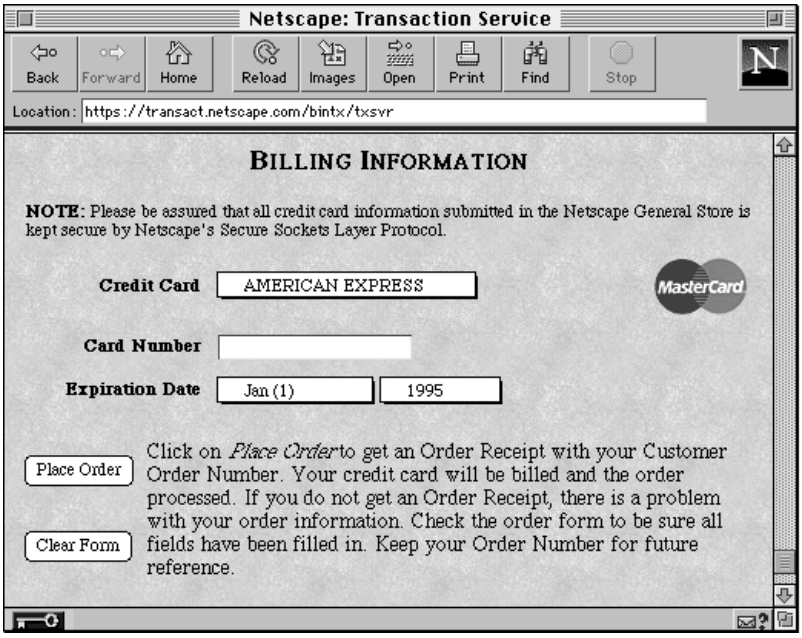

Figure 2: Secure form for CC purchases, CC data will be transferred in encrypted form

Another development for the secure transmission of CC data across the Internet is SET („Secure Electronic Transaction“, see [SET96a] and [SET96b]). This is a joint effort by CC organizations (Mastercard and VISA) and software companies (IBM, Microsoft and Netscape among others). Another system called “First Virtual” (already in existence for more than a year; see [WAYNER96], S. 85-100) relies on pre-transfer via fax or snail mail of the CC data. With this system only a unique identifier (and not the CC data itself) is transmitted via the internet and each transaction has to be separately confirmed via electronic mail.

There are, however, several basic problems with credit cards:

- One has to have a credit card to participate.
- CC transactions normally use the currency of the country where the merchant is located. Therefore, for a participant unfamiliar with this currency the “easy use” criterion is not fully satisfied.
- Since all CC transactions are cleared through the CC organizations that are aware of the identities of the participants and since the merchant learns the identity of the buyer, the anonymity criterion is not satisfied.
- CC transactions carry a base transaction cost that is high enough to make them unsuitable for transactions involving small amounts.
- The protocol structure e.g. of SET is complex (see [SET96b], p. 133); this can lead to long delays resulting in cancellations of spontaneous transactions.

While being a widely available alternative today for transactions involving higher amounts, all these points show that the use of credit cards as a surrogate for a common currency system is not adequate.

4.2 Electronic Cash Systems

Common Technological Background

All electronic cash systems stem from cryptographic algorithms developed in the eighties (see [CHAUM92] or [WAYNER96], p. 49-65 for a good introduction to the technique; [WAYNER96], p. 15-45 also explains the basic algorithms). The basic approach is: Each electronic coin is a globally unique string of digits (serial number) that is electronically signed (for electronic signatures see [RÖCKELEIN95], p. 259 or [WAYNER96], p. 28ff) by the issuing bank while debiting the account of the user. This coin can then be transferred to

another user who presents it to the bank to credit his account. The bank keeps a list of all the serial numbers and the depositors of the coins it receives so it can prevent double-deposits of coins (This results in an online check and no privacy). To achieve privacy Chaum adds a technique called "blind signatures" (see [CHAUM82]). The bank "blindly" signs the coin, so it cannot link a coin to the person who withdrew it later. To get rid of the online checks reuired to prevent double deposits, another algorithm is used (see [ChFiNa88]). Its principle procedure is as follows: With each payment the software of the payer has to answer a question to the software of the merchant. When the merchant deposits the coin at the bank after that, he includes the received answer. A single answer reveals nothing to the bank, but two answers (from a double-deposit) are enough to identify the person who withdrew the coin. So when two coins with an identical serial numbers show up at the bank, all three possible fraudsters can be identified (the two merchants and the customer).

Magic Money

Magic Money from Pr0duct Cypher (see for example [WAYNER96], p. 169-176) is a freely available implementation of an electronic cash system using all of the above explained techniques (so the following requirements are intrinsically fulfilled: security, anonymity, two-way transactions, portability of coins, off-line capability). It can be used to create a private currency system. There have been several trials to build a currency with Magic Money. Matt Thomlinson conducted a free (no setup and transaction cost) experimental trial, in [THOMLINSON96] he reported some of his findings: One major problem was backing, as this was an experiment only. Several enthusiasts pledged some coke cans or beer at the local pub to back the currency. Another drawback was the user interface. It is text and command-line based only, and requires four manually initiated messages per transaction. A problem was also how to get started, i.e. how to increase the money stock circulating without inducing inflation (see chapter 3). The currency was denominated in „GhostMarks". Actual use was restricted to a fairly exclusive circle (about 30 people and 200 GhostMarks).

Thus the application of the criteria listed above to Magic Money based on this trial gives:

Security	reasonable, esp. if combined with transport security for example secure electronic mail
Backing	weak
Provision for Anonymity	yes
Setup and Transaction Costs	zero
Easy Use	low
Two-way Transactions	yes
Portability of Coins	yes
Off-line Capability	yes
Infinite Duration	basically yes, but only experimental trial
Divisible Coins	no
Use of non-Political Unit of Value	yes

Ecash from DigiCash

David Chaum, who basically invented electronic cash and holds several key patents to it, has founded a company called DigiCash. This company produces electronic cash software called "ecash". The software is based on the above mentioned techniques but currently uses online

checking for fraud detection. So the following requirements are intrinsically fulfilled: security, anonymity, two-way transactions. The client software has a GUI for user interaction (see the figures 5 and 6) and is very easy to operate. Unfortunately the bank software is not available, so it is not possible to create your own currency at the moment. The software interacts with the WorldWideWeb, the prevalent service on the Internet nowadays. It can also be used standalone with manual initiation of an ecash transfer. It can also put electronic coins in a file so that they can be transferred via other means, for example electronic mail or disks (thus fulfilling the requirement „portability of coins"). The operation principle when initiated via the WorldWideWeb is depicted in figure 3.

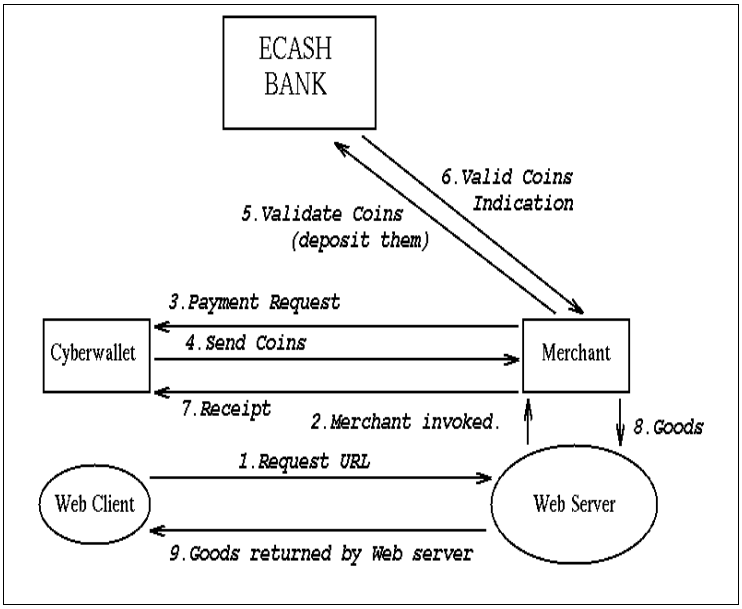

Figure 3: Operating principle of Ecash, taken from [PEIRCE95]

On a WorldWideWeb page there can be a special link to initiate an ecash transaction through a click by the user in the Web client software (step 1). The Web server opens a connection to a special server program that is part of the ecash software (step 2). This program then sends a request through the network to the computer of the client, which is handled by the ecash client program (step 3). When the user confirms the transaction, the coins are sent to the server (step 4). The server validates the coins with the bank software (step 5 and 6) and sends the client software a notification of acceptance of the coins (step 7). It then instructs the Web Server (step 8) to deliver the goods (e.g. the result of a database query, software, etc.) to the user (step 9). The client software can also be configured to automatically accept specified payment requests to ease the operations. Ecash can be either an account operated by the bank software or it can reside inside files on the computer of the user. Therefore, in case of problems with the computer[4] on which the user runs the client software, not all of his money would be lost[5] (money in the account would never be affected by such a failure). Deposit and withdraw operations moving money back and forth between the two locations can be initiated from the client software. DigiCash is constantly improving its software, latest additions are reported to be multi-currency capabilities.

Cyberbucks field trial[6]

DigiCash has set up a free field trial for ecash (see for example [WAYNER96], p. 159-167). Their currency is called "cyberbucks". They issued 100 cyberbucks to the first 10.000 people who applied for an account. This field trial attracted a lot of people both as users (more than

4 for example a hard disk crash

5 Backups can of course prevent this and in addition the newest software version contains provisions to recover such lost ecash.

6 There were several software versions used in the trial. This section is based on version 2.1.5a.

60.000 showed interest in an account) and merchants (DigiCash reports more than 100 shops on their WorldWideWeb pages).
Even physical goods (for example postcards or T-shirts) can be bought with cyberbucks. Dollar to cyberbuck exchange rates are quoted, see figure 4 for an example. Mark Grant reports an exchange rate of 4 British pounds for 100 cyberbucks on actually completed exchanges in August/September 1995. Otherwise no backing was used. However the huge interest in the system (as it is a „cool thing“ to have) gives some intrinsic value to cyberbucks.

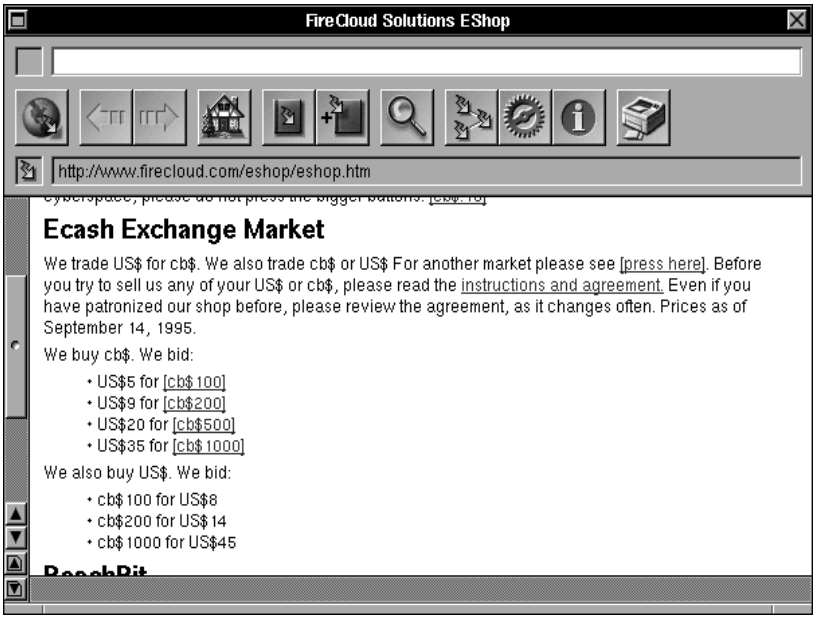

Figure 4: Dollar to cyberbucks exchange market

One of the authors of this paper participates in this field trial. In figure 5 the status of a fresh cyberbuck account is depicted. Most of the money is in the account and 10 cash cyberbucks are available. They are broken into small amounts, so that at least eight payments can be made with them before a change of coins would be necessary.
When a transaction is initiated, the user is prompted to confirm an incoming payment request (see figure 6).

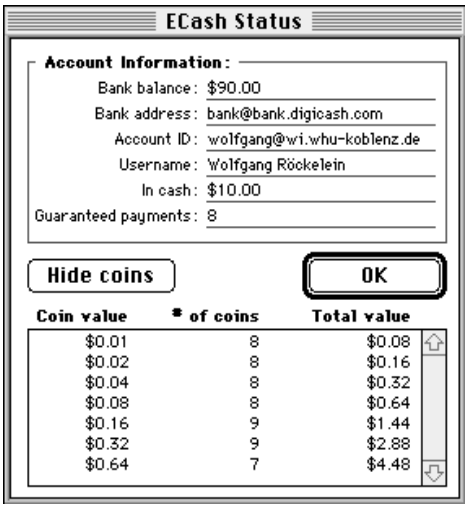

Figure 5: Ecash status window

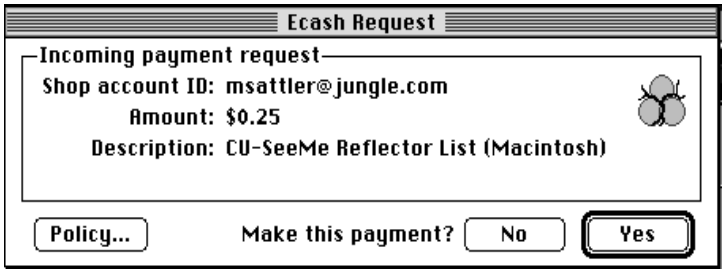

Figure 6: Ecash payment request

With the DigiCash software coins can be put in a file for offline transmission. Figure 7 contains 1/100 cyberbuck[7].

7 Warning: Trying to deposit this in a cyberbuck account will result in a double spending error (Of course, not for the first one to try this, only for all successors).

```
-----BEGIN ECASH PAYMENT-----
oLmQgwABJaGgiqCukIEOkIECkIEBkIEBkIEBkYQxD93ZkIQxIlLZkIEOkoFAlJSJ
VuPHV5hMST6D01XiKKZAZXSf0ZSUV9DXfyOz6yp4dv2rP7oo9g2M9T+QgRCSrFRo
aXMgaXMgb25seSBhIHRlc3QgZm9yIHRoZSBCbGVkIGNvbmZlcmVuY2UhkoCUgJCB
BJGEAAAAAJCBAKGguKCrkIIBgJPAJ+sRKm3kUmoR7M39mwZ2+gZdvavteX7rmpoy
ypU1+kh9YnQVBOvQfuF82CVG0i55cL7Wyiy6yC8Awkso3eYfppPAYSlEww7kqliy
3f7v2d3nQAyf9NKBE6QlcVpzM7UhvSuHcJ2Cif0S9rAYwg/AEF3SE0gTVs3mGNBA
qqcanI/zYZCBAaGhod==
-----END ECASH PAYMENT-----
```

Figure 7: 1/100 cyberbuck from the Ecash trial

The application of the criteria listed above to the cyberbuck system gives:

Security	high
Backing	no (although intrinsic value)
Provision for Anonymity	yes
Setup and Transaction Costs	zero
Easy Use	high
Two-way Transactions	yes
Portability of Coins	yes
Off-line Capability	limited (online clearing: at the time of the reception of coins an online connection to the bank is necessary)
Infinite Duration	no (but long grace period to change old coins into new ones)
Divisible Coins	no
Use of non-Political Unit of Value	yes

Ecash from Mark Twain bank

Recently DigiCash has begun to partner with banks to set up other currencies. One effort started in October 1995 together with the Mark Twain Bank, St. Louis (Missouri, USA).[8] Their currency is linked to the US dollar; that means one "dollar" from the Mark Twain/DigiCash system is always worth one US dollar. Mark Twain charges an initial setup cost, a monthly amount and a fee for exchanges of US dollar to and from "ecash from Mark Twain" (as of January 1995 prices started at $11/$1/$3 respectively). Transactions within the Mark Twain ecash system are free.

The fulfillment of the criteria is similar to the cyberbuck system with three exceptions: the currency is backed by indexation to the dollar, it is not free and it uses a political unit of value (US dollar).

5. Synthesis

The Internet has several properties that conform to some of the above mentioned prerequisites of both theories. In the following some arguments are outlined which we think have to be

8 Another such effort was started in Finland on March 13, 1996.

considered to answer the question of feasibility of common currency systems for spontaneous transactions on public networks from an economic point of view.

The application of the theory of optimum currency areas is quite difficult as the electronic cash systems do not substitute national currencies (at least not in the beginning). So, the cost side stated by the theory cannot be evaluated very well. Nevertheless, some of the basic insights can help us to decide what the conditions are on which electronic cash systems can be designed viably. Important factors will be:

- **credibility of the system**: The case study of the ECU shows a way to achieve price level stability by linking the currency to an index. [GLASNER89], p. 227- 241, discusses several further index options. As a common currency system for the Internet would merely be a complement to existing national currencies, a similar approach as in the case of the ECU (i.e., an index to a basket of currencies) seems to be feasible.
- **the „openness" of the Internet economy**: For Internet transactions there are no geographic limitations and fast transfer especially of "information goods" is possible. Therefore a high factor mobility is "virtually" given to those goods for which the reduction of the distance between producer and customer is substantial (e.g. on the Internet it does not matter where the database queried is actually located on the globe). Information spreads more quickly on the Internet than anywhere else (see e.g. [BaBa95]), so information consistency problems (which for example would delay the driving out of bad money and thus yield trouble for a free banking system) do not apply here. Additionally, since the Internet is a global phenomenon it brings together participants of all appearances, races, ages, countries etc. Thus, economic transactions on the Internet are more likely to cross national boundaries than in existing economic systems.
- **the size of the „Internet economy":** The Internet economy is still in its infant stage so there is not yet a firm monetary system established. However, considering the enormous growth rate of this system one can expect a substantial part of (especially cross-border) transactions to be supported by the Internet soon. Thus, the Internet economy should be large enough to make an own currency desirable.
- **the size of transaction costs to be saved:** As already pointed out, the transaction costs within an electronic cash system are much lower than in real currency systems. Additionally, the transaction costs to exhchange national currencies have to be compared with the transaction costs to exchange national currencies and the electronic cash as a lot of transactions will take place outside the Internet. In our view the savings from eliminating transaction costs are substantial and even higher than the savings of a monetary union which are expected by the EC countries (relatively, of course, not in absolute terms).

In our view the initial question - A common currency system for spontaneous transactions on public networks - is it feasible? - can be answered along the following lines:

- technically feasible? - Yes, the technology for electronic cash transactions on the Internet is already available (see chapter 4), however, DigiCash's reluctance to license its system[9] is currently an obstacle to a significant spread;
- economically feasible? - Yes, but it depends heavily on the design of the system (see chapter 3 and our arguments above);

9 This is necessary since DigiCash holds several patents in this area.

- politically feasible? - We cannot say yet! There are already regulatory statutes[10] by national governments or central banks respectively.

All these points together make the issue of a common currency system on the Internet promising.

6. Conclusion and Future Developments

The theoretic foundations for a common currency system on the Internet were shown and an existing example (DigiCash) modeled according to the theory and satisfying most of the mentioned prerequisites was depicted. The huge success of this system gives a promising future to similar systems. Since the ecash system from DigiCash has proven that it works and thus built up reputation, systems using it could take advantage of this trust in technical security to achieve trust in the currency. A common currency system could be built upon several similar currencies leading to a free banking system on the Internet.

Hayek states in his free banking theory that there will be competition among the various currencies launched in the Internet. The best currency (in terms of credibility) will then succeed. Gresham predicts the plain opposite: „bad money“ will drive out „good money“ (in terms of inflation). We note that issues of credibility and usability will play the key role in the question of feasibility of electronic cash systems.

However, on the Internet the stage is set for the biggest field trial of Hayeks free-banking theory we have ever seen.

7. Bibliography

[BaBa95] Baar, James; Baar, Theodore: The Pentium Bug War ends PR as we know it, in: KT News, April 1995, online available under http://www.omegacom.com/news1.html; the authors' names come from the prepublication online available under http://www.popco.com/hyper/internet-marketing/archives/9412/0587.html

[BÄNSCH93] Bänsch, Axel: Käuferverhalten, 5th edition, Munich, Vienna 1993

[BOFINGER84] Bofinger, Peter: Die ECU als Währung, in: Zeitschrift für das Kreditwesen, 15.10.1984, p. 934&936

[BUNDESBANK92] author unknown: Internationale Organisationen und Gremien im Bereich von Währung und Wirtschaft, Sonderdruck Nr. 3 der Deutschen Bundesbank, 4. edition, June 1992

[CHAUM82] Chaum, David: Blind Signatures for Untracable Payments, in: Advances in Cryptology: Proceedings of the Crypto'82, p. 199-202

[CHAUM92] Chaum, David: Achieving Electronic Privacy, in: Scientific American, August 1992, p. 76-81

[ChFiNa88] Chaum, David, Fiat, Amos, Maor, Moni: Untraceable Electronic Cash, in: Advances in Cryptology: Proceedings of the Crypto'88, p. 319-327

[DEGRAUWE94] Grauwe, Paul de: The Economies of Monetary Integration, 2nd edition, Oxford (GB) 1994

10 Governments and central banks have put up numerous obstacles to free banking. To examine all these legal ramifications is beyond the scope of this paper.

[GLASNER89] Glasner, David: Free Banking and Monetary Reform, Cambridge et al. 1989

[HAYEK90] Hayek, F.A. von: Denationalisation of money, 3rd edition, London (GB) 1990

[HERLT94] Hertl, Rudolf: Die Zwitterrolle des ECU, in: Finanz und Wirtschaft, Zürich (Switzerland) 05.02.1994, also in: Deutsche Bundesbank - Auszüge aus Presseartikeln, Frankfurt (Germany) 9.02.94, p. 8f

[LARENZ81] Larenz, Karl: Lehrbuch des Schuldrechts, 12th ed., C.H.Beck, Nördlingen (Germany) 1981

[LOWRY93] Lowry, Amanda: Private Ecu gets promotion, in: International Corporate Law, May 1993, p. 21-22

[MATONIS95] Matonis, Jon: Digital Cash and Monetary Freedom, in: Chon, Kilnam (Ed.): Proceedings of the INET'95, San Francisco (USA) 1995, online available under http://www.interfinance.com/digicash.html and under http://info.isoc.org/HMP/PAPER/136/ps/paper.ps

[MCKINNON1963] McKinnon, R.: Optimum Currency Areas, in: American Economic Review, 1963, p. 717-725

[MEHNERT88] Mehnert, Ralph J.: The ECU's Growing Role in Private Transactions, in: Europe, September 1988, p. 20&22

[MUNDELL61] Mundell, R.: Theory of Optimum Currency Areas, in: American Economic Review, 1961, p. 657-665

[OkOh92] Okamoto, T., Ohta, K.: Universal electronic cash, in: Advances in Cryptology - CRYPTO '91, New York et al., 1992

[PEARCE81] Pearce, David W.: The Dictionary of Modern Economics, Cambridge, Massachusetts, 1981

[PEIRCE95] Peirce, Michael; O'Mahony, Donal: Scalable, Secure Cash Payment for WWW Resources with the PayMe Protocol Set, in: Proceedings of 4th International World Wide Web Conference, Boston (USA)1995, online available under http://www.w3.org/pub/Conferences/WWW4/Papers/228/

[RESNICK94] Resnick, R., Taylor, D.: The Internet Business Guide, Indianapolis (USA) 1994

[RÖCKELEIN95] Röckelein, Wolfgang: Systems for Purchases on the Internet - Requirements and Evaluation, in: Clarke, Roger; Griÿcar, Joÿze; Novak, Joÿzica (Editors): Electronic Commerce for Trade Efficiancy: Proceedings of the Eighth International Conference on EDI and Inter-Organizational Systems, Bled (Slovenia) 1995, p. 250-267, online available in a slightly revised and complete version under http://www.whu-koblenz.de/wi/Purchases/

[SCHELLER94] Scheller, M., Boden, K.-P., Geenen, A., Kampermann, J.: Internet: Werkzeuge und Dienste, Berlin (Germany)1994

[SET96a] author unknown: Secure Electronic Transaction(SET) Specification Book 1: Business Description, DRAFT for public comment, February 23, 1996, online available under http://www.visa.com/sf/set/SETBUS.PDF

[SET96b] author unknown: Secure Electronic Transaction(SET) Specification Book 2: Technical Specifications, DRAFT for public comment, February 23, 1996, online available under http://www.visa.com/sf/set/SETTECH.PDF

[THOMLINSON96] Thomlinson, Matt: Re: Magic Money and Phantom Exchange, private email correspondence with the author, Message-Id: red-18-msg960202182407MTP[01.52.00]000000c2-13653

[VAHLEN93] Dichtl, Erwin, Issing, Otmar (ed.): Vahlens großes Wirtschaftslexikon, 2nd ed., Munich 1993

[WAHLIG87] Wahlig, Bertold: Rechtliche Aspekte zur Verwendung des "privaten" ECU, lecture held on 08.12.1987, in: Hahn, Hugo (Editor): Geldverfassung und Ordnungspolitik, Baden-Baden (Germany) 1989, p. 65-78

[WAYNER96] Wayner, Peter: Digital Cash, Chestnut Hill (USA), 1996