Cashing Up With Mobile Money – The FairCASH Way

Heinz Kreft
Institute for Informatics,
University of Kiel,
Hermann-Rodewald-Str. 3, 24118 Kiel, Germany
E-mail: hk@informatik.uni-kiel.de
http://www.informatik.uni-kiel.de/inf/Schimmler/forschung-faircash-e.shtml
Phone: +49 431 880 5305
Fax: +49 431 880 4612

Abstract: *Today we still do not have a widely available digital cash system for the masses. This is not because there are no inventions in this area or the money community is out of ideas on how to construct such a system. It is mainly because there are conflicts of interests between banks, government and community. In this paper we first present a short history of money and look at these conflicts. Then we focus on the so-called success-factors, which are essential for a highly accepted e-Payment system. Based on these success-factors, we will present a new system called FairCASH. By adopting our FairCASH system, users will be able to make payments of any value, including micro payments. FairCASH is a multi-purpose, multi-currency, pre-paid inter-operable scheme for domestic usage and cross border payments. It features non-account-related completely anonymous payment transactions by encrypting the transferred e-Tokens. There is no need of registration for users of the FairCASH e-Money system. It is suitable for person-to-person, chip-to-chip or P2P money transfers. It is independent of the communication platform or the digital transmission standard. Highlights are the inherent zero transaction costs for B2C, B2B and C2C operations. Last but not least, we would like to point out that the system posses the multi-hopping capability allowing e-Token circulation that is very advantages for users of such system.*

Keywords: Digital cash, e-Money, m-Money, Open-Loop, Multi-Hop, e-Cash, CASTOR, P2P, Pre-Paid, Micro-Payment, G2G, G2B, G2C, B2C, B2B, C2C, m-Commerce, m-Payment, m-Banking, e-Government.

1. Introduction

Until today, the definition of the term "money" in particular concerning its form is still a hotly discussed economic subject. Apart from the general concepts, new definitions and ideas are constantly being introduced through research conducted in the legal and economic field. Furthermore, due to the continuous distinctions of exchange relations and increasing requirements on monetary transaction, new forms of money were developed. These usually first appear as a surrogate and will be subjected to a period of evaluation. Then, they either find general recognition as money or disappear forever.

The very first money was created when exchange-partners began to bear some relation with each other using neutral elements. Fig. 1 shows a possible classification of the money evolution process. Therewith the medium 'means of payment' was established, although the modification wasn't permanent due to the money form (shells, bones etc.). A more advanced money definition took form with the discovery of metals. At approximately 680 BC in Asia, metal bars and subsequently coins were established as a currency standard for the first time. At the beginning, these coins have an intrinsic value (gold standard). Since then, the currencies in all countries evolved step-by-step into modern systems of attainments – oriented and coupled to the current changes of the society and technology. An essential concept for the currency is the replacement of the nominal value by the notional value, for example the guaranteed assurance redeeming of paper money and coins.

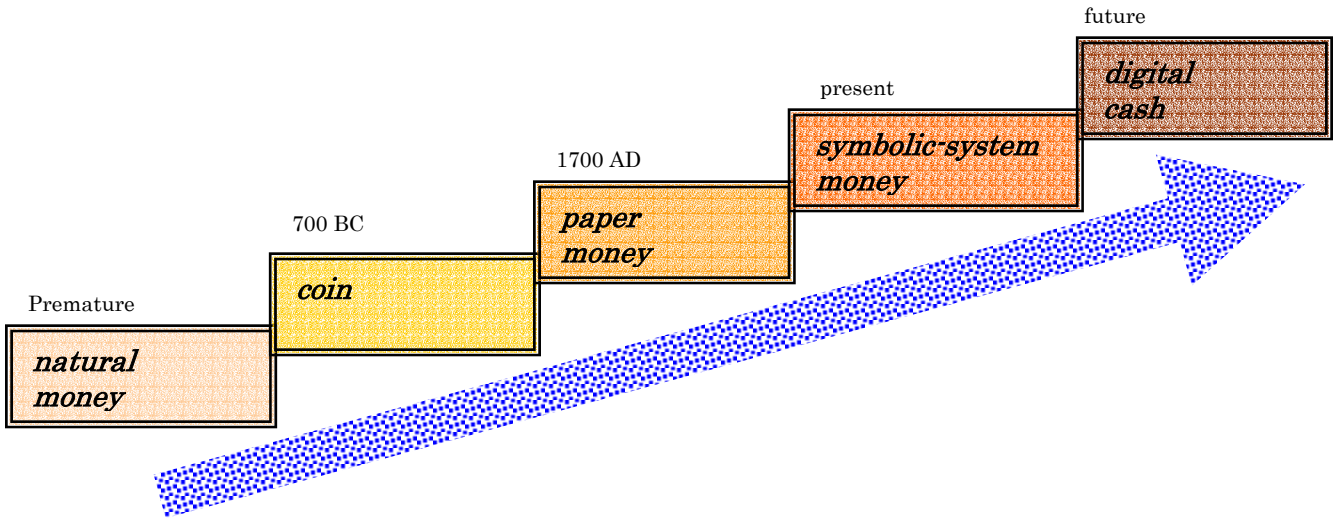

Fig. 1: Graphic diagram shows the evolution of Money.

The next major „step" in the evolution of payment system is just ahead of us - the complete digitalisation of the money. The payment system will be suitable for users of m-Commerce and e-Government. It can be used for payment of virtual (non material) services and goods. At this point the dematerialization process would be terminated, because the money has reached zero nominal value.

Here it can be seen that the history of money consists of a permanent new redefinition of the value-carrier. Due to its definition, the electronic cash represents a new final form of money in the continuous process of dematerialisation. It is defined completely in the domain of IT-space as a data object in which single values "banknotes or coins" are represented as e-Tokens. For us the concept of money shall be based on e-Tokens of cash related payment systems (digital cash) for carrying out a modern high-performance exchange relation (as part of interactions) between economy subjects. Fig. 2 illustrates outward forms of money:

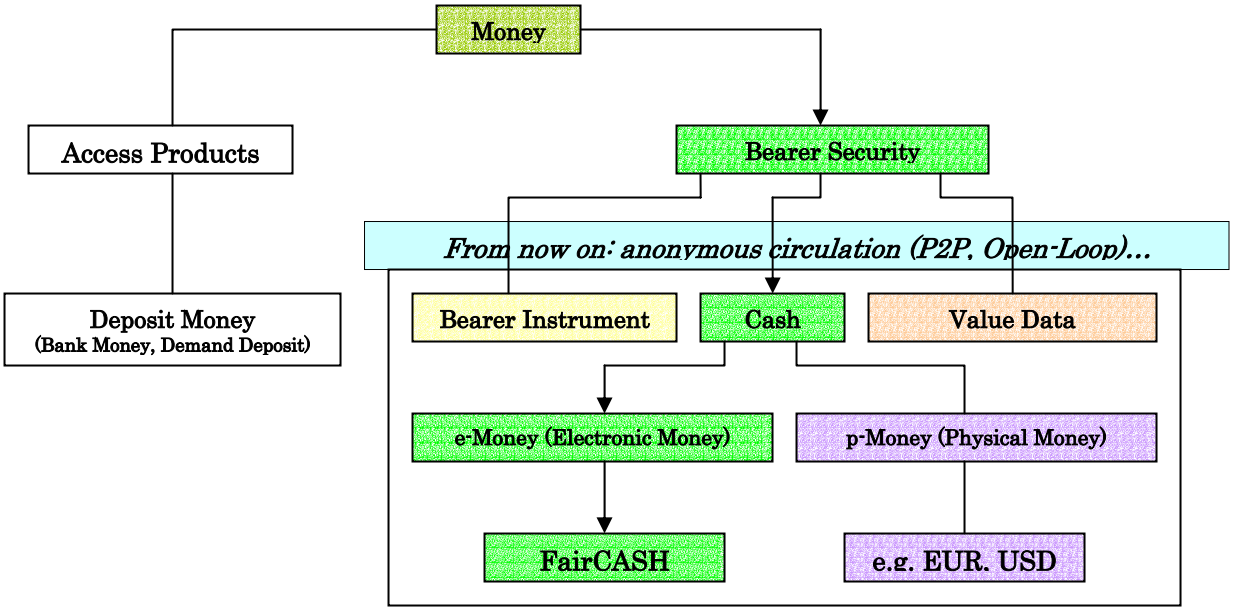

Fig. 2: Graphic representation of the various meanings of Money.

Most of the developments in the field of innovative e-Money systems are technologically based on the European Union project CAFE (Conditional Access for Europe), which was terminated in 1997. Additionally, we should also mention OPERA (open Payments European Research Association), SEMPER (Secure electronics Marketplace for Europe) and the Chablis Payment server. All of these projects, except OPERA, were merely integrators of existing e-Money payment schemes and none of them resulted in new or further developments in the area of e-Money.

CAFE is based on the developments of David Chaum (Digicash Ecash) and Dr. Stefan A. Brands (Brands Cash). Various projects were carried out by different interest groups, such as SOSCARDS that makes use of smartcards or MILLION that uses PDA´s to integrate the payment function with the Internet. Both do not interoperate with other pilot projects even though they rely on the same e-Payment procedure. Furthermore, the mixing of different objectives (political, directive or commercial) has resulted in no break-through for these systems until today. The following table (Fig. 3) summarises these facts by only highlighting the reason for their failure:

e-Money Scheme	Invented by	Introduced (died†)	Killed by / Remarks
e-cash (DigiCash)	David Chaum	1994 (2001 †)	tricky, no cash, closed-loop
CyberCoin (CyberCash)	Carnegie Mellon Uni	1994 (2000 †)	tricky, no cash, closed-loop
Brands Cash	Dr. Stefan A. Brands	1993	never activated
Universal Electronic Cash (UEC)	T. Okamoto and K. Ohta	1991	too fungible
Conditional Access for Europe (CAFÉ)	ESPRIT Project 7023	1992 (1997 †)	limited transferability
Mondex	Jones u. Higgins (NatWest UK)	1990 (2001 †)	money generator in Smartcard Chip
OPERA (Open Payments Europ. Research Association)	CAFÉ	1995 (1996 †)	limited anonymity
MILLION (CAFÉ with PDA´s)	ESPRIT Project 20772	1995 (1997 †)	no e-Money relation
SOS cards (implementation of café on smart cards)	ESPRIT III Project 9259	1994 (1996 †)	no e-Money relation
EMS (Electronic Monetary System)	Sholom S. Rosen (Citibank)	1991	not disclosed completely

Fig. 3: Some former e-Money schemes or projects in the field of e-Payment.

Most of the systems deployed in the market have not been able to fulfill the needs of their users. Therefore, they have completely disappeared from the market. An indication for rejecting any electronic cash was mainly by definition, when the system is less efficient in its fundamental properties than the traditional cash. For this purpose, the existence of complete anonymity is included, in contrast to methods such as "owner tracking", "coin tracing" or adding the ability of anonymity revocation to an e-Money scheme. With the attempt to replace established payment systems by the so-called payment system innovations, all electronic cash oriented payment systems encounter some or all of the following "problems":

- Existing oligopolies in the telecommunications industry,
- Scheme provider cartel in the credit card industry,
- National level shaped interests within the scope of e-Government,
- Conflict of interest between the Government and financial institutions,
- Potentially cannibalising traditional finance business.
- Financial institutions don't like loosing control of the payment activities,
- Financial institutions don't want to loose control over the already installed POS[1]-system,
- No established or de-facto e-Payment standard,
- Too complicated,
- Poor promotion and too little support from the banks,
- Unable to reach critical mass,
- Households are not comfortable with new forms of money substitute,
- No perfect anonymity.

This paper presents a comprehensive non-technical survey about some of the mechanism found in the living space of electronic cash by presenting reasons on why we currently don't have a functioning e-Money system

[1] Point-of-Sell.

in use. It's the opinion of the author that this non-existence will last until our future e-Money system carries all of the positive attributes of e-Money (e.g. unlinkability and untraceability). We step into this issue a little deeper in section 2. Then we will focus on the success factors in section 3 which will be the principal guide in creating our electronic cash money system. This system is called FairCASH and it will be described in section 4 and 5. In section 6 we present some positive effects of having FairCASH in use. Finally, we summarise our findings in the last section.

2. Economics and regulations

In Germany, the Central Credit Committee (ZKA) represents the overall interest of the banks and equals to an association power. This is used, among others, to standardise the de facto mandatory industry-specific standards for players in the various value creation stages. Thus the banks determine the distribution of the economic creation of value from the electronic monetary transaction.

They establish and transform the certification and admission functions. Moreover, they strengthen the claim to power over the enterprise initial special value creation stage, for example the technology manufacturers.

Small enterprises can enter this highly regulated market, when the innovation is a radical technology jump, such as the introduction of a new digital payment system. However, it must be clear that to develop and deploy such a system, it requires many cooperating institutions such that the system will have a broad market with an effective network. From the customer's and producer's point of view, the opening up of a new market is only possible through the standardisation process.

In the context of reputation mechanisms, the innovation induced cooperation form of a participant network model seems attractive since they represent a larger economic entity. Therefore, they can act as a closed common source of innovation. In this context, the consumer view banks as particularly trustworthy and the bank can use this reputation to its advantage. Thus the explanation appears coherent and comprehensible.

Many payment transaction systems are patented and form a market entry barrier for institutions. Thereby they are in conformity with the requirements of bank permission, as well as to obtaining the Central Credit Committee permission and certification requirements.

The EU comprehensive regulation for e-Money institutes actually strengthens the barrier effect. The possibility of using negotiations, cooperation's or lobbying in overcoming the institutional market barrier is attractive for an outsider of the market. The following table of EC-directives (Fig. 4) shows perfectly, how close the embracement between financial institutions and the government already is:

EC-Directive	Disposed on	Implemented	Meaning of the Directive
93/22/EEC	10.05.1993	31.12.1995	Investment services in the securities field
1999/93/EC	13.12.1999	19.07.2001	Community framework for electronic signatures (EESSI)
2000/12/EC	20.03.2000	15.06.2000	Taking-up & pursuit of the BIZ of credit institutions
2000/31/EC	08.06.2000	23.10.2002	Electronic commerce (ECRL)
2000/28/EC	18.09.2000	27.10.2000	Taking-up & pursuit of the BIZ of credit institutions
2000/46/EC	18.09.2000	27.04.2002	Electronic money institutions (ELMI)

Fig. 4: List of the most important EC-Directives in the field of electronic money.

Profitable cooperation for participants with lesser negotiation power with strong partners in the competence area of other value creation stage can produce an attractive win-win situation for both. If - for example - an innovative payment system like FairCASH will be used for shopping purposes, then both partners will have a larger share in the value creation process. In such cases, the distribution of the value creation potential of an innovation concentrates primarily on the cooperating partners and less on other enterprises positioned in the different stages of the value creation. Due to the continuous tussle in the payment system market, it is not only an essential strategy to concentrate on the development and execution of innovation activities for a

technically optimal solution, but also by influencing the relevant institutions through standard bodies and other means of cooperation and regulation activities.

3. Success factors for e-Money

Based on the experience of previous and current payment systems, we now know the factors that affect a digital payment system. These factors determine whether a payment system can be successful or not. They formed what we call a taxonomy-profile that can be used to construct a more adaptable and better e-payment system. We list these essential success points in the following table (Fig. 5):

Atomic Success factor	e-Money	(p-Money – for a compare)
High distribution degree (global standard, Critical mass)	not yet	worldwide
quick and simple in the application	ok	ok
zero transaction times	ok	ok
great confidence ("good" feeling, ease of use)	achievable	ok
Micro payment capable	ok	ok
high system security (fraud protection)	ok	ok
perfect anonymity	ok	ok
no transaction charges	ok	ok
immediate fulfilment of the paying amount	ok	ok
usable in third world countries (everywhere)	ok	ok
secure end-to-end (P2P) infrastructure	ok	ok
Perfect for mobile, ubiquitous use	ok	ok
No Fungibility (coin splitting is insecure)	ok	ok
Cost-effective, e-Money is cheaper then p-Money	true	true
Transferability, Untraceability	ok	ok
Off-line Ability	ok	ok
Portability, Interoperability, Generality	ok	ok
Long Validity	achievable	ok
Robustness & Reliability	achievable	ok
Profit of Seigniorage[2] for Issuer/Clearer	ok	ok
Cross-Boarder & international Payments	ok	no
Seigniorage profits minimized the total system costs	ok	ok

Fig. 5: These Success factors are forming the core taxonomy-profile of our e-Money system.

Therefore, in order to create the conditions for a successful product placement, FairCASH sets the following prerequisites:

- Standardisation of e-Money e-Tokens, algorithms and procedures,
- Establishment of a worldwide, opened and accepted e-Money standard,
- Interchange ability and compatibility of all deployed crypto- and safeguarding methods,
- Creation of an extensive license free usable technology for future e-Payments systems,
- Specification of functional elements and properties of secure silicon containers (CASTOR),
- Development of a FairCASH-PAY-Chip as a reference for a highly secure functional hardware,
- Integration by interface (slot) standardisation for ubiquitous devices (e.g. mobile phones etc.),
- Long-term system security, in order to protect against future attack methods (e.g. quantum computers).

4. The FairCASH system

FairCASH is an electronic cash payment transactions system which is based on a combination of hard- and software elements. It is secured by the latest and most secure encryption technology (which is out of the scope

[2] Seigniorage is the net revenue derived from the issuing of currency. It arises from the difference between the face of a coin or bank note and the cost of producing and distributing it. Seigniorage is an important source of revenue for the issuing institution.

of this paper). It offers the user many advantages such as a bilateral "Multi-Hop-Capable (MHC)"-system, which provides complete anonymity. In contrast to many other e-payment systems, FairCASH does not rely on the Digicash patents of David Chaum (no Blinding, no Secret Splitting).

FairCASH is a monetary, prepaid, digital and intrinsic e-Money payment-instrument functioning as a substitute for physical cash: an electronic exchangeable value-unit, known as e-Token, is stored in a physically and cryptographically secured e-Token container (FairCASH-PAY-Chip is also called CASTOR[3]).

It can be deployed on any communication platform in the virtual and physical world. This value transfer payment system contains direct inter-object payments between contracting parties such as institutions, corporations, or persons – without the participation of a third-party, who are not the issuer of the value-devices. Thus, these conditions create a perfect P2P capable e-Token system, with circulating capability (or transferability).

E-Money e-Tokens are issued as encrypted IT data objects in exchange for p-Money. The aggregate value mustn't be lower than the issued monetary value and has to be accepted as means of payment by third parties. Transactions are conducted without the use of accounts, but by the exchange of e-Money bearer securities as a bond. This means outstanding debits have to be exchanged with the e-Money issuer.

The coins and bills of FairCASH consist of digital encrypted data objects. Their well defined bit structure is stored in protected digital money storage, the FairCASH-PAY-Chip (CASTOR).

Besides storing the e-Tokens, the highly secured FairCASH-PAY-Chip[4] also contains some intelligent subunits. These subunits are responsible for the cryptographic related computation (crypto-coprocessor) and for the highly secured P2P-protocol (talk controller), ensuring that two FairCASH-PAY-Chips can be linked logically with each[5] other over an insecure channel (Fig. 6) to carry out the payment transaction.

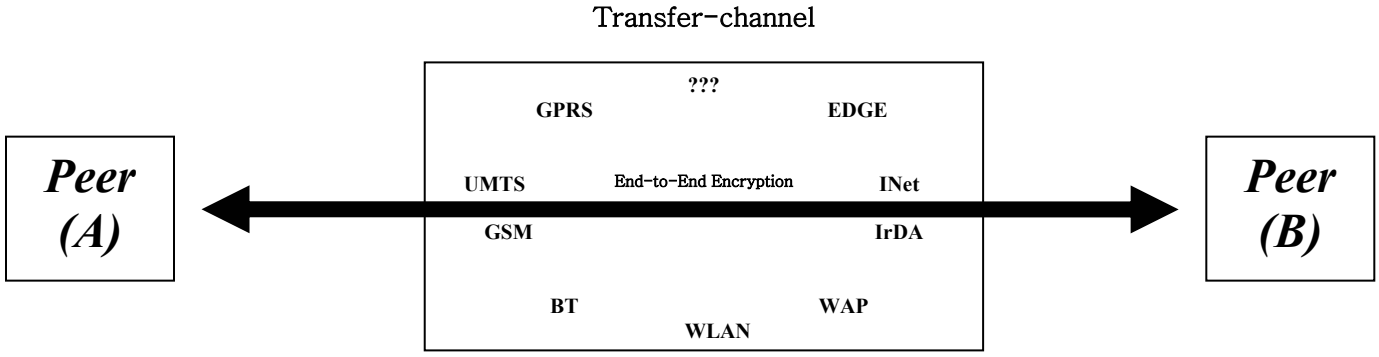

Fig. 6: FairCASH communication can used virtually any insecure channel to exchange e-Token´s.

Users neither need accounts nor credit guarantees (credit standing examination), due to the circulation ability (transferability). This is due to the fact that an intermediary is not needed (disintermediation) making it freely convertible.

FairCASH can be used just like p-Money, however it is especially for:

- eGOVERNMENT projects
  [Payment of charges, G2C, G2B, G2G]

[3] Tamper-resistent hardware.
[4] The systems security of FairCASH exists independently of the resistance of the chip against Reverse-Engineering.
[5] The transfer procedure is not only a simple copying process, but based on a „shift-by-shift" transmission process.

- eBUSINESS projects
  [mobile Money, P2P capable invoice models, B2C, B2B, C2C]
- eCOMMERCE projects
  [micro payment without fees]

The development of a practicable, acceptable, ease of use, robust and innovative cash substitute is the main priority in the R&D of FairCASH. Furthermore, the following rules form the basic concept of the system:

- Abolition of the anonymity of users or coins is not possible,
- Tracing of users or coins is not possible,
- Users' exchanges are always anonymous, never pseudonymously,
- For the users, there are no requirements for an account or registration,
- The user is not required to trust anyone (except for the promised clearing),
- No blind signature/secret sharing methods are used.

FairCASH is not:

- A system whereby the anonymity can be lifted later through third parties (e.g. trustee, ombudsman) - no threat of deanonymity,
- An account-based system – FairCASH users does not have to maintain any account,
- A user or coin tracing system. Even with the cooperation of all parties involved, tracing is still impossible,
- E-Wallets are not account managers or bank branch offices, but are safe containers (CASTOR) for e-Money. This analogy follows the physical world's purse for coins and paper money.

5. FairCASH e-Token chain circulation

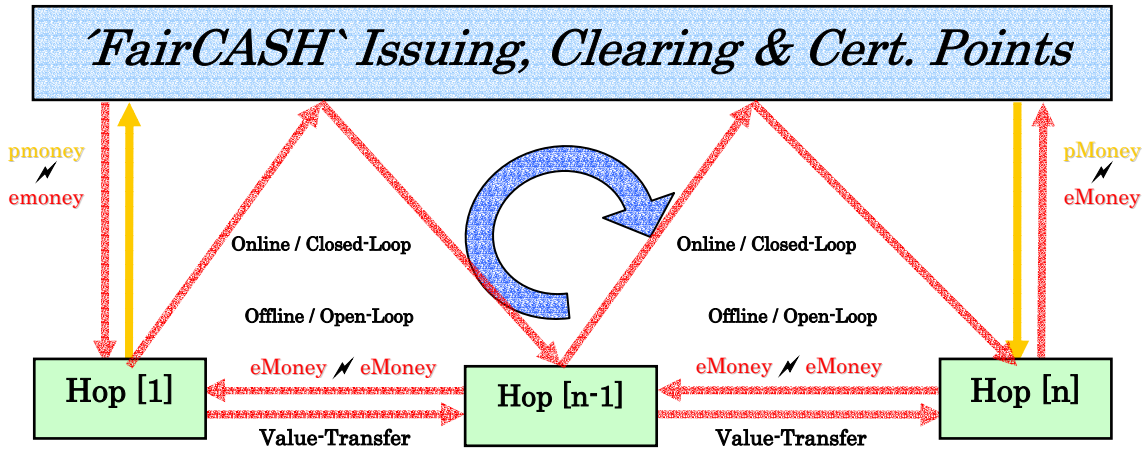

Fig. 7 : FairCASH e-Token chain circulation (Open-Loop and Closed-Loop).

This picture (Fig. 7) illustrates the two possible circulation possibilities: A "hop" can be done on- or offline. Nevertheless, the loop chain will be terminated, if the e-Token is cleared by the issuer.

(Phase i)- After a cash deposit, an account debit, or a credit card transaction to the account of the FairCASH issuer, the FairCASH user will receive a set of e-Tokens, which represent the same monetary value, transferred to his SVS/CASTOR device. The encrypted serial number (which is not usable to trace the user) of the transferred FairCASH e-Tokens will be stored in a multispending database (run by the issuer).

(Phase ii)- With any participating partner or any person/device, owning a compatible SVS/CASTOR, these e-Tokens can be exchanged. Parents for instance can transfer an appropriate amount to the FairCASH enabled cell (mobile) phones of their children to pay for their voice- and data services. Besides paying for virtual goods and services, FairCASH can also be used for paying online purchases of almost everything offered via the Internet without the risk associated with providing credit card details.
(Phase iii)- Received e-Tokens can be passed on to other users until the Maximum-Hop-Count (MHC) is exhausted or when it has reached its expiration date. After this event, e-Tokens can only be transferred back to the initiator for clearing, in which the user will receive an equivalent amount credited into the account of his choice. The clearing house will then delete all the serial numbers for the deposited e-Tokens from the multi-spending database. If the serial number cannot be found in the database, then it must have been cleared in a previous transaction and the e-Token might represent illegal copies.

(Phase iv)- All SVS/CASTOR will maintain a local log[6] of e-Tokens received together with the ID of the transmitting SVS/CASTOR. This provides the user with a means to prove his innocence with regards to counterfeiting 'money'. The analysis of that log requires the owner's cooperation as centralized log databases are not supported. Because of the inherent data structure of the e-Tokens and protocols utilized in the transfer, actual copying of FairCASH e-Tokens by breaking the payment scheme will be more expensive as compared to doing the same with physical cash (Euro-, Dollar-bills …).

6. Some ideas on what can be done with such a system like FairCASH

Anonymous immaterial electronic e-Tokens, based on systems of values, develop their usefulness not only within cash like transaction systems (digital cash, micro payment and mobile paying), but also in the following applications:

- Ticketing (cinema, theatre, tickets, world championship 2008),
- Stamps,
- IPR management (DRM-methods and others),
- Toll-collect systems,
- Bonus methods (Miles & More, discount cards),
- Invoice of supply goods, disposal goods[7], CoD[8],
- Application support in the field of e-Business, e-Government, m-Commerce, e-Economy,
- Accounting systems for radio data transmission,
- Billing solutions for national mobile network providers,
- E-Payment for the DSRC[9] project in the context of the EU initiative[10].

An outstanding quality of the FairCASH System is the cross compatibility designed for transportation level 4, such as for the Internet, WLAN, BT[11], IrDA and GSM This makes the payments transaction cost-free and allow offline transaction between two POS communication partners. With this, the mobile phone can become a mobile purse for ad-hoc payments in the micro and macro payment range. It is not only suitable for the payment of services in the mobile phone industry or in the DRM area, but also for the ordering of a Pizza, paying a taxi or shopping in the supermarket. In essence, it possesses the entire prerequisite for a mobile p-Money substitute. The modern e-society will have cash like payment transactions system at its disposal. This has the following advantages:

[6] under user control regarding „enabling, disabling, copying and clearing of the logging trace".
[7] Electric current, gas, water.
[8] Contend-on-Demand.
[9] Dedicated Short-Range Communication (DSRC).
[10] Industry Initiation to introduce Automatic Tolling in Vehicles in Europe (INITIATIVE).
[11] Bluetooth.

i. The provision costs are so low, that it can be provided to every user free of costs (like material cash). Thanks to the insubstantial of e-Tokens, such a system is less prone to robbery[12]. Current p-Money systems allow the user to use it free of charge everywhere in this world. Nevertheless, sometimes the expenditures must still be borne by the user through some mixed calculation models (taxes). Based on the assumption that in Germany alone all cash payments of less than 25 Euro will be replaced by FairCASH, it will result in a replacement share of 10.5%. In such assumption, the FairCASH issuer can achieve a seigniorage profit of 1 billion Euros per annum. Therefore, FairCASH can finance itself completely from the interest gained (pre-paid) and offer its services to the user free of charge. For the users of FairCASH, this actually means the following: no transaction charges, no time delay and also no expenses or basis costs due to the payment system's model.

ii. The resistance to counterfeiting (including the building of duplicates) is much stronger for FairCASH in comparison with conventional cash and all of this is achieved with almost zero production costs

iii. Complete anonymity has been enjoyed by the consumer for a very long time and this property should remain. FairCASH offers both perfect anonymity and privacy (non-observable and not interlinked).

iv. Efficiency, profits and real convergence without media excrescence[13] mean clear advantages for the users with regard to simplicity and the ability of handling payments.

v. Due to its favourable cost architecture, such payment transaction system will be suitable for all modes of payment including micro payments.

vi. Costs for a credit investigation are not required; there are also no charge-backs (pre-paid payment).

vii. The total introduction costs of the Euro in the course of cash conversion in the European Union were estimated by the former EZB president Wim Duisenberg to be between 19 and 52 billion Euro. These costs were also imposed to the consumers.

Furthermore various positive macro and micro-economic changes in our society will arise as a result of the process of innovation for the economy subjects as the existence of an e-Payment system permits the establishment of e-Commerce! Therefore the beginning of electronic cash is to view as the demise of paper and deposit money. This is unavoidable as it is a natural result from the technological advancement.

7. Conclusions

In this paper we have presented the process of turning ancient money into a modern currency, called digital cash. We have discussed and presented some of the obstacles faced in the mass introduction of digital cash that are found in the financial industry. In addition to that, the strategy of the EU government is not to legalise e-Money with perfect anonymity.

Nevertheless, we have presented such a valuable e-Money payment instrument named FairCASH in this paper. We highlighted that the existence of such an e-Payment system would have a great impact to our society. We believe, that the development of FairCASH will be standardising in the same way as the standardisation of mobile phones in the market. This is similar to the development of today's computers. Broad establishment of electronic government services like G2G, G2B and G2C are unthinkable without such a service. With the increase deployment of standardised hardware, the Telecommunication enterprises and IT industry will align themselves in a horizontal market and must differentiate themselves through software and services. Thus, the non-speech oriented data services including VoIP may become the key of future growth.

[12] Discussion of this complex of themes is out of scope of this paper.
[13] Convergence at this point of view means the use of identical 'means of payment' - physically and virtually.

FairCASH is an elementary basic service, which will allow a simple and economical billing of future services. In addition to that, it also represents an end-usage customer oriented service.

I would like to especially thank my following colleagues for their assistance in reviewing this manuscript:

Prof. Dr. rer. nat. Manfred Schimmler, Professor, Institute of Computer Science, University Kiel, Germany.
Prof. Dr. Wael Adi, Com. Eng. Dep., Etisalat College of Engineering, Sharjah, United Arab Emirates.
MEng. Ching Yen Choon, Research Scientist, Multimedia University, Cyberjaya, Malaysia.
Dipl.-Ing. (TU) Gerd Pfeiffer, Research Scientist, Institute of Computer Science, University Kiel, Germany.

References

Booz, Allen, Hamilton, (2002), „E-Government und der moderne Staat“, ISBN 3-934191-50-9, FAZ Institut.

Boyed, Colin and Foo, Ernest, (1998), „Off-line Fair Payment Protocols Using Convertible Signatures”, ASIACRYPT'98.

Brands, Stefan A., (2001), „Rethinking Public Key Infrastuctures and Digital Certificates“, ISBN 0-262-02491-8, MIT-Press.

Brands, Stefan, (1993), "Untraceable Off-line Cash in Wallets with Observers (Extended Abstract)" in Advances in Cryptology-CRYPTO'93, pp.302-318.

Brands, Stefan, (1995), "Electronic Cash on the Internet," Proceedings of the Internet Society 1995 Symposium on Network and Distributed System Security, San Diego, California, February 16-17.

Brickell, E, Gemmell, P. and Kravitz, D., (1995), "Trustee-based tracing extensions to anonymous cash and the making of anonymous change," Proceedings of the 6th Annual ACM-SIAM Symposium on Discrete Algorithms, pp. 157-166.

Camenisch, J., Maurer, U. and Stadler, M., (1996), "Digital payment systems with passive anonymity-revoking trustee," Computer Security - ESORICS 96, LNCS 1146, pp. 33-43.

Camenisch, J., Piveteau, J.-M. and Stadlerr, M., (1996) "An Efficient Fair Payment System," Proceedings of 3rd ACM Conference on Computer Communications Security, ACM press, March 1996, pp. 88-94.

Chaum, David, Pedersen, Torben P., (1992), "Transferred Cash Grows in Size," in Advances in Cryptology-EUROCRYPT'92, pp.390-407.

Chen, Kai, Zhang Yuqing and Xiao, Guozhen. (1999) "A Practical Efficient Anonymous Divisible E-Cash System," International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC '99).

Chen, L. and Mitchell, C.J., (1997), "An anonymous and undeniable payment scheme," Information and Communications Security LNCS 1334, pp. 478-482.

Davies, Glyn, (2002), „A History of Money“, ISBN 0-7083-1773-1, Creative Print and Design.

Eng, T. and Okamoto, T., (1995), "Single-term divisible electric coins," in Advances in Cryptology-EUROCRYPT'95, LNCS 950, pp. 306-319.

Eng, Tony, Okamoto, Tatsuaki, (1994), "Single-Term Divisible Electronic Coins," in Advances in Cryptology-EUROCRYPT'94, pp. 306-319.

Escher, Dr. Markus, (2003), „Bankaufsichtsrechtliche Rahmenbedingungen des elektronischen Geldes, erschienen im Beck Verlag zum Thema e-Geld.

Frankel, M. and Yung, M., (1992), "Towards probably secure efficient electronic cash," Columbia Univ. Dept. of C.S. TR CUCS-018-92.

Frankel, Yair, Tsiounis, Yiannis and Yung, Moti, (1992), "Fair Off-Line Cash made easy," ASIACRYPT'98.

Franklin, M. and Yung, M., (1993), "Secure and efficient off-line digital money," Proceedings of ICALP'93, LNCS700, pp. 265-276.

Fujisaki, E. & Okamoto, (1996), "Practical escrow cash systems," Security Protocols, LNCS 1189, pp. 33-48.

Hartmann, Monika E., (2000), “Elektronisches Geld und Geldpolitik”, ISBN 3-8244-7228-7, Gabler Verlag.

Jakobsson, M. and Yung, M., (1996), "Revokable and versatile electronic money," 3rd ACM Conference on Computer and Communications Security, pp. 76-87.

Jakobsson, M., (1997), "Privacy vs. Authenticity", Ph.D. thesis.

Juels, Ari, (1999), "Trustee tokens: Simple and practical anonymous digital coin tracing," Financial Cryptography.

Kahmann, Martin, (2001), “Report Mobile Business”, ISBN 3-933814-67-7, Symposion Verlag, 2001.
Ketterer & Stroborn, (2002), „Handbuch ePayment“, ISBN 3-87156-463-X, Deutscher Wirtschaftsdienst.
Lacoste, Gérald, Pfitzmann, Birgit, Steiner, Michael, (2000), Michael Waidner, “SEMPER – Secure Electronic Marketplace for Europe”, ISBN 3-540-67825-5, Springer Verlag.
Moribatake, H., Abe, M., Fujisaki, E. and Nakayama, Y., (1997), "Electronic cash scheme," Proceedings of 1997 Symposium on Cryptography and Information Security, SCI97-3C.
Okamoto, T. and Ohta, K., (1991), "Universal electronic cash," In Advances in Cryptology-CRYPTO'91, LNCS 576, pp. 324-337.
Okamoto, Tatsuaki, (1995), "An Efficient Divisible Electronic Cash Scheme," in Advances in Cryptology-CRYPTO'95, pp. 438-451.