Wallet Based E-Cash System for Secured Multi-hop Cash Exchange

Heinz Kreft
Christian Albrecht University of Kiel
Kiel, Germany
hk@informatik.uni-kiel.de

Wael Adi
Technical University of Braunschweig
Braunschweig, Germany
w.adi@ieee.org

Abstract—The majorities of contemporary proposed digital cash techniques have many disadvantages in being directly or indirectly account based or not anonymous and offer no offline peer-to-peer transferability. This is for the majority of users - in general - not acceptable. Such an approach fails to replace the role of cash in e-commerce systems.

The basic result of this research is a new prepaid multi-hop (transferable) cash payment system solution based on hardware technology implementing an electronic wallet (e-wallet) to accommodate digital coins. Transparent cash transfer (exchange) protocol software can serve at any network device as Internet host, mobile device or any future general purpose communication link. The result is a peer to peer (P2P) electronic cash transfer equivalent to a physical cash transfer in public use. This e-cash system could be a possible alternative to the physical coins & bills. It is a multi-purpose inter-operable digital cash payment scheme for domestic usage. This e-cash system could be a possible alternative to the physical coins & bills. It is a multi-purpose inter-operable digital cash payment scheme for domestic usage. The system is suitable for low and high value money exchange, regardless of the communication environment as:

- Cellular networks like GPRS, EDGE, UMTS for Cell/Mobile phones for remote payments,
- Local PAN and WLAN like Bluetooth, IEEE802.11a/b/g/h/n for face-to-face payments,
- Generic Ethernet based Internet IP devices and more.

The particular advantage of the system is that it is a non-account-related anonymous payment system. There is on-demand registration for the user; participation is possible by just getting an e-wallet to start with. The e-coins are offline transferable in an open-loop chain. The usage is simple; it works like usual cash with the ability to "fly" over IT highways. It has the attractive cash re-spend feature ('Multi Hop Capability') or transferability without any grow in size for the e-coin. Nearly any modern device can be enabled utilizing virtually any communication platform (network) either off-line or on-line, allowing borderless and long distance transfers usable for POS (Point Of Sale) transactions (B2C (Business to Customer), B2B (Business to Business), C2C (Customer to Customer), G2B (Government to Business) and G2C (Government to Citizen)). The system is suitable for Person-to-Person (Chip-to-Chip) transfers as a (local & personal) secure money storage solution for e-coins, completely under individual owner’s spending control but with autonomous integrity enforcement.

The e-cash system can be seen as an application of digital cash with an e-wallet, e-coins and an Internet based back office architecture, where the bank provides an e-mint service while a X.509-like Certification Authority architecture provides wallet authentication. Fresh e-coins can only be created –or minted – and cleared by the e-mint authority. They are strongly encrypted e-tokens, which may be transferred between partners participating on a value exchange transaction.
and can be passed on in consecutive transactions. These e-coins are digitally stored in a user owned e-wallet, based on the so called castor chip, acting as a local storage and personal payment server.

Due to its P2P transactions, e-coins flow directly from one e-wallet to another e-wallet. The transfer protocol is a type of an optimistic fair exchange one with extreme high probability acting without any trusted third-party (TTP), so only the holders of the two e-wallets are involved. Only in rare error conditions, an e-mint-TTP needs to be off-time contacted by presenting a proof for lost e-coins recreation actions.

The proposed Digital Cash can be a new electronic mobile payment technology that works just like the conventional physical cash exchange system – just better prepared for the electronic commerce. It involves the exchange of digital coins (e-coins) with fixed denominations and unique serial numbers among participating users. The e-coins are stored in a hardware device called e-wallet. The functional center of this e-wallet is the Castor unit as shown in Fig. 2. The whole e-wallet can be integrated into devices such as mobile phones, vending machines, slot metering (electricity, gas, heat, and water), cash registers and legacy Auto Teller Machines (ATM). In fact each e-wallet functions such as an ATM itself. This end-point connected infrastructure based on existing networks like Internet or Mobile Communication Networks (ATM). In fact each e-wallet functions such as an ATM itself. This end-point connected infrastructure based on existing networks like Internet or Mobile Communication Networks will enable everybody to use the e-coins in the daily payment. This payment can be either physical proximity or remote. A unique feature will be that the e-coins can be reused in their original form for further transactions until they have reached their expiration date or cleared by the e-mint.

II. STATE OF THE ART

The first notion of e-cash was conceived by David Chaum [1]. Subsequently, many different types of e-cash system had been proposed [2-32]. They came with various properties such as divisibility, online or offline, anonymity, tracing with or without trustee using different cryptographic techniques (i.e. blind signature, group signature, zero-knowledge protocol etc). A list of schemes that were actually implemented is given in table 1.

All the projects listed in table 1 were not successful to cover the practical demands as a replacement for physical cash. In [33], the reasons on why they failed are discussed. The major challenging reasons rest on the fact that the proposed e-cash systems do not behave like existing physical cash, in that they cannot be transferred among the users directly in an offline mode. The reason for lacking of this basic property is due to the fact that digital information can be easily copied. Thus, to allow an e-coin to be transferred from one to another user requires not only using cryptographic techniques against copy protection, but also physical hardening techniques to make e-wallets temper-protected. In [5] Chaum showed that the size of the e-coins will increase with every cash transfer, storing the hop-chain into the e-coin. This is considered as an unacceptable effect in that technology. The comprehensive reference list shows major publications dealing with such difficulties.

Many other non-technical reasons like political and bank concerns have led to the limited expansion of all the proposals so far introduced and prototyped. We are only concerned with the technical issues.

<table>
<thead>
<tr>
<th>e-Money Scheme</th>
<th>Invented by</th>
<th>Introduced</th>
<th>Killed by / Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>e-Cash (DigitCash)</td>
<td>Dr. David Chaum</td>
<td>1994</td>
<td>tricky, no cash, closed-loop</td>
</tr>
<tr>
<td>CyberCoin (CyberCash)</td>
<td>Carnegie Mellon Uni</td>
<td>1994</td>
<td>tricky, no cash, closed-loop</td>
</tr>
<tr>
<td>Brands Cash</td>
<td>Dr. Stefan A. Brands</td>
<td>1993</td>
<td>never activated</td>
</tr>
<tr>
<td>Universal Electronic Cash (UEC)</td>
<td>T. Okamoto &amp; K. Ohta</td>
<td>1991</td>
<td>too fungible, limited Anonymity</td>
</tr>
<tr>
<td>Conditional Access for Europe (CAFÉ)</td>
<td>ESPRIT Project 7023</td>
<td>1992</td>
<td>limited Transferability</td>
</tr>
<tr>
<td>Mondex</td>
<td>Jones u. Higgins (NatWest UK)</td>
<td>1990</td>
<td>money Generator on Chip</td>
</tr>
<tr>
<td>OPERA (Open Payments Europ. Research Ass.)</td>
<td>CAFE</td>
<td>1995</td>
<td>limited Anonymity</td>
</tr>
<tr>
<td>MILLION (CAFÉ with PDA’s)</td>
<td>ESPRIT Project 20772</td>
<td>1995</td>
<td>no e-Money relation</td>
</tr>
<tr>
<td>SOS cards (implementation of CAFE on smart cards)</td>
<td>ESPRIT III Project 9259</td>
<td>1994</td>
<td>no e-Money relation</td>
</tr>
<tr>
<td>EMS (Electronic Monetary System)</td>
<td>Sholom S. Rosen (Citibank)</td>
<td>1991</td>
<td>not disclosed completely</td>
</tr>
</tbody>
</table>

Table 1 Classification of the implemented and published e-cash systems

III. SYSTEM CONCEPT

The particular advantage of the proposed system is that it is a non-account-related anonymous payment system. There is no registration for the user; participation is possible by just getting a certified trustable electronic wallet to start with. The e-coins are offline transferable in an open-loop chain. The usage is simple; it works like usual cash with the ability to “fly” over the IT highways. It has the attractive cash re-spend feature (‘Multi Hop Capability’ or transferability). Nearly any
modern device can be enabled utilizing virtually any communication platform (network) allowing borderless and long distance cash transfers. The system offers a suitable secure money storage solution for e-coins, completely under individual owner’s control. The whole system principle is depicted in Fig. 1. The e-cash system can be seen as an application of digital cash with an e-wallet (a), e-coins and an Internet based back office architecture, where the bank provides an e-mint service (b) while the CA (Certification Authority) provides the e-wallet authentication (a). Fresh e-coins can only be created –or minted– and cleared by the e-mint authority. They are strongly encrypted e-tokens, which may be transferred off-line between partners (c) participating on a value exchange transaction and can be passed on in consecutive transactions.

These e-coins are digitally stored in a user owned and operated e-wallet, based on a novel device the so called CAsk for Storage and Transport Of access Restricted value data (Castor) Chip as a core part of the e-wallet, acting as local cash storage. Fig 2 illustrates the basic concept of a Castor unit within the e-wallet. Due to its P2P transactions, e-coins flow directly from one e-wallet to another e-wallet. No online trusted third-party (TTP) or intermediary clears are required. Only the holders of the two e-wallets are involved.

Possible Business case: The minting bank cashes a huge amount of money which is virtually kept in circulation between users. The bank can make use of this money as the reclaim rate is usually very low. The gain of the users is a simple e-cash exchange through the modern networks. Many new applications in e-commerce would be realizable. Another business case for the mobile operator is a new traffic for digital payment service. That is users would link their e-wallets to the mobile device, which means additional pay load on the mobile network.

**IV. UNCLONABLE E-WALLET**

The key functionality of the system is based on the hard wired e-wallet which should act as an unclonable certified entity in the system. Once a wallet is activated and certified it is deemed through hardware one-way-functions to generate once and forever its own secret identity through a hardware random generator. The generated identity is only provable but it is unknown similar to the physical unclonable functions PUF concept [34]. It proposed identity differs from the PUF in that it is error-free and self-generated and is principally clonable however an electronic evolution process is incorporated to the root identity during the lifetime of the device. This gives that identity a growing strength with the progress of time depending on its interaction history similar to identifying a living person depending on the person’s interaction profile with the environment. The profile starts by the birth certificate and is updated after each interaction as it happens in real life. A precise technology is under development. Fig. 3 shows a conceptual block diagram of that identity technology. In reference to Fig.3 the identity setup proceeds roughly as follows:

1. A random process (as a binary symmetric source BSS) generates at the birth (or personalization) time a random unknown binary string. The result is called a mutated secret device identity MSDI. This unknown permanent secret string of at least say 128 bits would serve as a DNA like provable identity root. The identity could also be combined with a real PUF identity.
2. A trusted authority TA certifies the identity by inserting unreadable secret device identity SDI. This unknown permanent secret string of at least say 128 bits would serve as a DNA like provable identity root. The identity could also be combined with a real PUF identity.
3. Joining the authority certificate SDI with the device own secret MSDI results with a mutual authentication procedure which is not easy to abuse even if the trusted authority is willing to cheat.
A possible simple joint authenticated common key KCt at some time can be generated with the help of the TA as the original certifier for all devices. The principle of a possible simplified mutual authentication scenario is shown in Fig. 3 using two time stamps t1 and t2 on both sides and exchanging fresh challenges in connection with the “practically unclonable” identities MSDI1 and MSDI2. The transactions history can contribute to the identity using the evolution register ER. ER includes important information about the transactions history profile of the device as a living entity. The trusted authority should not be capable to break the system as the common KCt’s should be only possible to generate exclusively within the certified hardware environment.

Having reached this security quality, a secured exclusive link tunnel can be established between any two members of the certified e-wallet group.

We call the secured electronic transfer “teleportation” which should be equivalent to the physical transport of coins a “teleportation or Singleton” within the research group. The “singleton” operation has a wide spectrum of applications in modern communication systems. Once a secured e-transport is achieved, a variety of very interesting applications in licensing and usage of electronic services can be assured.

Fig. 3 Basic possible secret key identification concept

The general exchange mode of e-coins is then accomplished as indicated in the Fig 1. The first initial load of e-coins is a transfer between the wallet and the bank as the e-mint in Fig 1 (b). The peer to peer exchange is then accomplished as in Fig. 1 (c). Moving any coins from one wallet to the other should be accomplished using a trustable soft and hardware environment called as e-castor. It is a secured hard and software environment deployed to control the traffic of coins between the two parties according to a simplified transaction interface to allow the user to set up and execute a cash exchange to fulfill a transaction and assure that the moved coin from one to the other e-castor is really removed from the spending castor to the receiving castor without a possibility of multi-spending. A hardwired secured algorithm tied to the unique e-wallet and its secured mutually authenticated virtual private link should allow such off-line exchange operation. Fig. 4 shows the initial hardware components of the e-wallet incorporating the e-castor.
V. SUMMARY AND CONCLUSION

An electronic cash system with off-line capability is presented. The system should exhibit nearly the same physical cash properties regarding anonymity and multi-spending (re-spending) without the need for a bank account. The system needs a trusted authority which should act as catalyses to enhance the trust and possible abuse traceability. The system is expected to be self-stabilizing and self healing in the sense that if a part of the system is abused, then the system would retain stable and have a limited loss without being completely compromised. Further future research is concentrating on minimizing the trusted authority and still keep the same security level and operational stability.

REFERENCES