A Comparison Of Electronic Cash Schemes and Implementations

ECE 646 Presentation
13 December 2001

Wook Jung
Andrew Kirby
Rajesh Kolluri
Kenneth Shannon
Yeo-won Yoon

Cold, Hard, Cash

• Advantages
  – Highly portable
  – No apparent cost
  – No audit trail
  – $3.4 Trillion exchanged
    300 Billion transactions
    avg of $11
  – By far, the preferred payment scheme for small anonymous transactions

• Disadvantages
  – $1 bills have a finite lifetime (18 months) at 4c per bill
  – Large quantities must be secured during transfer
  – Can be counterfeited
  – Cost is not negligible
Digital Cash: Six Ideal Properties

- Independence - no vault or geographic location required
- Security - no counterfeiting or double spending
- Privacy (untraceability) - a user’s purchases and identity cannot be linked
- Offline Payment - execution of transfer protocol needs no real-time link to bank
- Transferability - digital cash can flow to another user
- Divisibility - amounts must be easily subdivided to some smallest denomination

Finding: No existing electronic cash scheme meets all six ideals!
Data requirements/performance prohibit all 6
**Cheating…**

- Digital money nothing but a string of bits!
  - Bits can be copied more easily than cash
  - Anonymity, untraceability, guarantee trouble

- Multiple ways to cheat
  - Fraud, Counterfeiting
  - Double spending
  - HW tampering

- Complex cryptographic protocols necessary
  - Blind signatures [Schnoor, Brand, et. al.]
  - 11 step protocol to prevent cheating by all parties!

#### Representative Electronic Cash Schemes

<table>
<thead>
<tr>
<th>Online transaction</th>
<th>Offline transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traceable</td>
<td>Mondex</td>
</tr>
<tr>
<td></td>
<td>Mondex</td>
</tr>
<tr>
<td></td>
<td>Millicent, MicroMint, Payword</td>
</tr>
<tr>
<td></td>
<td>E-cash, Netcash, SET</td>
</tr>
<tr>
<td>Untraceable</td>
<td>CAFE</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Individual Systems

CAFE

CAFÉ (1)

- Status: developmental 92-95, trial 95-today, no real user base
- Online vs. Offline: offline unless $ > limit
- Protocol: withdraw -> pay -> deposit
- Security: totally open using RSA Public Key, known hashes, blind signatures [Chaum, Schnoor]
- Cheating: not possible for user or merchant
- Anonymity: for *user* not double spending
CAFÉ (2)

- Restrictions: none on divisibility in the pay slip mode
- Fault Tolerance: yes, even if wallet lost
- Operating Systems: special HW wallet not designed for general network use
- Cost: probably under $200 to user
- Performance: slow, cryptographically complex, but not a real-time system

CAFÉ: Digital-Cash Ideals

- Independent? Not entirely – not designed for use over Internet or networks at user end
- Secure? YES, complex cryptographic tools
- Private? YES, to responsible users (not merchants)
- Offline? YES, if below threshold
- Transferable? NO, payment only to merchant
- Divisibility? 2 operational modes: pay slip completely divisible, coins discreet.
- SCORE = 4.5
Blind Signature: Basic Concept

Original Message

Blinding Process

Envelope containing Message and Carbon Paper

Sent to Signer

Signed Message

Message has now been signed

Envelope Removed

Signed Message

Untraceable Cash - Blinding

- Blinded RSA signatures
  - One way hash function $f$
  - RSA key pair $(PU_k, PR_k)$ chosen by bank for each denomination

- Denomination
  - Amount (serial number), $f(\text{amount $})$ \text{PR}_k$

- Withdraw and Spend

\[
\text{Person}: \quad f(\text{\$}) \cdot \frac{R}{R} = f(\text{\$}) \quad \text{PR}_k
\]

\[
\text{BANK}: \quad \left( f(\text{\$}) \cdot \frac{R}{R} \right)^{PU_k} \quad \left( f(\text{\$}) \cdot \frac{R}{R} \right)^{PR_k}
\]

\[
\text{Merchant}: \quad \frac{f(\text{\$})}{PR_k} \cdot \frac{R}{R} = f(\text{\$}) \quad PR_k
\]
Mondex

Mondex (1)

- Status: Production. Wholly owned subsidiary of MasterCard International. Licensed in more than 80 territories worldwide.

- Online vs. Offline: Both Online (Internet, Mondex enabled phones) and Offline (Electronic Purse) capability.

- Cheating: Relatively impossible, the cost of the technology capable of making counterfeit chip is too expensive to be viable.

- Anonymity: Not completely Anonymous, merchants can find out the identity of the users.
Mondex (2)

- Security: Security mechanism used in Mondex is not public but it uses the combination of the following:
  - DES signature generation: CBC single/triple DES
  - Encryption/decryption: ECB single DES
  - RSA: Up to 1024 bit using both normal and CRT modes
  - SHA-1
  - Asymmetric HASH functions

- Protocol: Value Transfer Protocol

Mondex (3)

- Restrictions: None. Upper limits being varies for different countries.

- Fault Tolerance: Yes, even if wallet is lost

- Operating Systems: MULTOS, runs on a H8/3112 Hitachi chip. On PC, the program runs on Windows 3.x or Windows 9x operating system, and are equipped with SmartMouse card readers.

- Cost: Varies on what the consumer buys

- Performance: 1024 bit RSA executed in 480ms
Mondex Hardware

Mondex: Digital-Cash Ideals

- Independent? Yes – designed for use over Internet or networks at user end
- Secure? YES, complex cryptographic tools
- Private? Partly Anonymous
- Offline? YES, using smart cards
- Transferable? Yes, using smart cards
- Divisibility? Yes, to the lowest
- SCORE = 5.5
Untraceable Cash - Blinding

- Blinded RSA signatures
  - One way hash function $f$
  - RSA key pair $(PU_k, PR_k)$ chosen by bank for each denomination

- Denomination
  - Amount (serial number), $f(\text{amount }$) $PR_k$

- Withdraw and Spend

\[ \text{Person} \] $\rightarrow \left[ f(\text{amount } \cdot R) \right]^{PU_k} \rightarrow \text{BANK} \]

\[ \left[ f(\text{amount } \cdot R) \right]^{PR_k} \rightarrow \text{Merchant} \]

\[ \rightarrow f(\text{amount})^{PR_k} \cdot R/R = f(\text{amount})^{PR_k} \]

NetCash

- The buyer sends the electronic coins in payment, identifier, secret key, public session key, all encrypted with merchant's public key, to the merchant.
  \{Coins, SK[Buyer], K[Public, Buyer], S_id} K[Public, Merchant]

- The merchant checks coins validity to send them to the currency server to be exchanged for new coins or for a cheque.
  \{Coins, SK[Merchant], transaction_type} K[Public, CS]

- The currency server checks that the coins are valid by checking its database. Then the server returns new coins or cheque, encrypted with merchant's session key.
  \{New_coins} SK[Merchant]

- The merchant knows that he has been properly paid by the buyer. He now returns a receipt, encrypted with his private key and buyer's secret key.
  \{\{Amount, transaction_id, date\} K[Private, Merchant]} SK[Buyer]
### Comparison of Ecash/NetCash

<table>
<thead>
<tr>
<th></th>
<th><strong>E cash</strong></th>
<th><strong>NetCash</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overview</strong></td>
<td>Anonymous, untraceable, online token payment system by Digicash</td>
<td>Real-time payment across multiple administrative domain on an unsecured network by USC</td>
</tr>
<tr>
<td><strong>Online vs offline</strong></td>
<td>Online only</td>
<td>Online but partially support offline when the parties are offline during the final exchange</td>
</tr>
<tr>
<td><strong>OS</strong></td>
<td>Support any kind of platform</td>
<td>Unknown</td>
</tr>
<tr>
<td><strong>Restrictions</strong></td>
<td>Size of the database of spent coins</td>
<td>Fraud by payee is possible</td>
</tr>
<tr>
<td><strong>User-base</strong></td>
<td>No real user base - free trial</td>
<td>No response from the Software Agents Inc.</td>
</tr>
<tr>
<td><strong>Anonymity</strong></td>
<td>Yes, Completely guaranteed by blind signature</td>
<td>Weaker than unconditional anonymity of Ecash but more scalable</td>
</tr>
<tr>
<td><strong>Cheating</strong></td>
<td>No.</td>
<td>Possible</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>Triple DES, digital signature, RSA, SHA</td>
<td>Symmetric/asymmetric cipher, digital signature, certificate, hash</td>
</tr>
<tr>
<td><strong>Implementation</strong></td>
<td></td>
<td>?</td>
</tr>
<tr>
<td><strong>Fault-tolerance</strong></td>
<td>Good. Even if the network fails and coin be lost, it can be recovered</td>
<td></td>
</tr>
<tr>
<td><strong>Cost</strong></td>
<td>Low.</td>
<td>High</td>
</tr>
</tbody>
</table>

### Meeting Six criteria

<table>
<thead>
<tr>
<th></th>
<th><strong>E cash</strong></th>
<th><strong>NetCash</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Independence</strong></td>
<td>Potentially low</td>
<td>Good. Scalable electronic currency that is accepted across multiple administrative domains</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Fully anonymous by blind signature. Payee anonymity is guaranteed in Ecash only</td>
<td>practical level of anonymous less absolute than Ecash</td>
</tr>
<tr>
<td><strong>Privacy</strong></td>
<td>Yes. Guaranteed anonymity</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Offline</strong></td>
<td>No</td>
<td>Basically online base but partially</td>
</tr>
<tr>
<td><strong>Transferability</strong></td>
<td>No. None of them allow a note to pass from user to user without the bank’s intervention.</td>
<td></td>
</tr>
<tr>
<td><strong>Divisibility</strong></td>
<td>Yes</td>
<td>Unknown</td>
</tr>
<tr>
<td><strong>Score</strong></td>
<td>4</td>
<td>3.5</td>
</tr>
</tbody>
</table>
## SET

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Drawbacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Provides confidentiality thru strong 1024-bit public key encryption vs. 128-bit SSL</td>
<td>- Customers reluctant to shop via Internet</td>
</tr>
<tr>
<td>- Provides authentication of every party to online transaction</td>
<td>- Increased complexity degrades performance – delays!!</td>
</tr>
<tr>
<td>- Provides integrity via hashing and digital signing</td>
<td>- Expensive to implement - $$$</td>
</tr>
<tr>
<td>- Guaranteed payment to merchant can expand Internet business</td>
<td>- Global compliance issues</td>
</tr>
<tr>
<td>- Certificates backed by CA and financial institution</td>
<td>- Interoperability among software vendors</td>
</tr>
<tr>
<td></td>
<td>- Not portable</td>
</tr>
<tr>
<td></td>
<td>- Use of smartcards increases customer security</td>
</tr>
</tbody>
</table>
### SSL vs. SET

<table>
<thead>
<tr>
<th>Authentication of All Parties</th>
<th>SSL</th>
<th>SET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usually only the shop is authenticated. However, option for certificate based authentication of client/customer has been added later on.</td>
<td></td>
<td>All parties including consumers need digital certificates.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Message Integrity</th>
<th>SSL</th>
<th>SET</th>
</tr>
</thead>
<tbody>
<tr>
<td>128-bit encryption</td>
<td>1024-bit encryption</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Overall Security</th>
<th>SSL</th>
<th>SET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less secure. However, recent attempts for adding authentication of client/customer by passwords, certificates or smart cards have added to the security level.</td>
<td>Inherently stronger security design.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ease of Implementation</th>
<th>SSL</th>
<th>SET</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Cost</th>
<th>SSL</th>
<th>SET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less expensive</td>
<td>Greater cost due to certificate process</td>
<td></td>
</tr>
</tbody>
</table>

### SET Participants

**Internet**

- **Electronic Certification**
  - **Certificate Authority**
  - **Cardholder (digital wallet)**
  - **Merchant (Storefront)**
  - **Acquirer-Gateway (Payment auth.)**

**Electronic Commerce**
SET: Step by Step

SET: Digital-Cash Ideals

- Independent? YES – designed for use over the Internet, across multiple platforms
- Secure? YES – provided by combination of strong encryption with added integrity via hashing and digital signing
- Private? YES – separate 1024-bit public keys: merchant sees only order information; payment gateway sees only payment instruction
- On-line? YES - payment authorization provided during transaction session
- Transferable? NO - payment request made only from unique computer containing digital wallet.
- Divisibility? YES - divisible to smallest denomination
- SCORE = 5.0
Micropayment

In General

What is Micropayment?

• A business transaction type, which specialized in the sub-dollar range
• On-line services providing newspaper, magazines, or digital information (documents, music, even movies) could be inexpensive if it sold separately
• For example, a monthly $20 150-hour Internet Dial-up Service costs 13 cents per hour, a $4 100-page magazine costs 4 cents per page. If you are only interested in a 5-page article, 20 cents will do it
• Pay-per-view, pay-per-login, or pay-per-download…
Micropayment Scheme

- Demands of the protocol make it practical for small payments amounts
- Computation (processing) time and storage requirements must be suitable for low-value (fractions of a cent) and fast transaction
- To reduce processing and storage requirements, minimize the use of public key algorithm and online verification
- Apparently, the security of micropayment scheme is not as good as that of macropayment scheme

Common Features

- Use token (coin) as a payment for purchasing
- Use fast one-way, collision-resistant hash function (such as MD5 or SHA1) for generating token or signature
- Decentralized validation (off-line processing)
- Provide decent level of security/privacy
- Involve three parties:
  - the user(U): makes the purchase
  - the vendor(V): sells the goods
  - the broker(B): keeps the accounts for U and V
- Token can be generated by all the parties
Basic Flow of Micropayment

1. request coin
2. return coin
3. purchase
4. goods
5. redemption

User → Broker → Vendor

Six Ideal Properties

- Independence: YES, physical location anywhere
- Security: YES, forgery is possible, but detectable
- Privacy (Untraceability): NO, cannot protect user’s information and payment records are traceable
- Off-line Payment: YES, no need to connect for validation with central authority (the broker)
- Transferability: No, user-specific token is used
- Divisibility: YES, token can represent any denomination
- SCORE = 3.8
Summary

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Independent</th>
<th>Secure</th>
<th>Private</th>
<th>Offline</th>
<th>Transferable</th>
<th>Divisibility</th>
<th>SCORE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAFÉ</td>
<td>Partial</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>4.5</td>
</tr>
<tr>
<td>Mondex</td>
<td>YES</td>
<td>YES</td>
<td>Partial</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>5.5</td>
</tr>
<tr>
<td>Ecash</td>
<td>Partial</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>3.5</td>
</tr>
<tr>
<td>NetCash</td>
<td>YES</td>
<td>Partial</td>
<td>YES</td>
<td>Partial</td>
<td>NO</td>
<td>YES</td>
<td>4</td>
</tr>
<tr>
<td>Micropayment</td>
<td>YES</td>
<td>Partial</td>
<td>Partial</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>3.8</td>
</tr>
</tbody>
</table>

Qualitative vs. Quantitative Scoring…
General Conclusions

- All security requirements can be implemented with existing cryptographic tools!
  - Authentication, Confidentiality, Integrity
  - Privacy / anonymity / untraceability
- Most systems don’t implement all tools
  - Complexity, performance penalties
  - Not necessary, desirable for every application
- No scheme (Mondex?) with widespread base
- Anonymity may not be essential or a driver

Electronic Cash: Outlook

- Digital cash won’t likely replace cold, hard cash
  - Not the vision, not a paperless society…
  - Issues of trust for some
- Cheaper HW, SW – no cost barriers to users
  - Card readers interfaced to PCs
  - Smart-cards, electronic wallets, purses
- Increasing speed, bandwidth - more crypto w/o penalties
  - “Moore’s” law valid for another decade
  - Complex protocols implemented more easily
Electronic Cash: Outlook

• Schemes should achieve all six ideals
  – Anonymity not a driver, nor a threat
  – $ Losses comparable to credit cards (for all parties)
  – Counterfeiting, fraud, double spending all manageable

• Major questions remain…
  – Will US banks / financial institutions wean themselves off profitable credit cards?
  – Will pay ahead systems ever compete in US with buy now pay later borrowing?
## Back Up Slides

### Categories of Characteristics

<table>
<thead>
<tr>
<th>User-related category</th>
<th>System category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymity</td>
<td>Authorization type</td>
</tr>
<tr>
<td>Applicability</td>
<td>Divisibility</td>
</tr>
<tr>
<td>Ease of use (Usability)</td>
<td>Scalability</td>
</tr>
<tr>
<td>Tracebility</td>
<td>Reliability</td>
</tr>
<tr>
<td>Trust</td>
<td>Efficiency</td>
</tr>
<tr>
<td></td>
<td>Convertibility</td>
</tr>
<tr>
<td></td>
<td>Interoperability</td>
</tr>
<tr>
<td></td>
<td>Security of transactions and database</td>
</tr>
</tbody>
</table>