Real Electronic Cash versus Academic Electronic Cash versus Paper Cash

Yvo Desmedt
BT Chair of Information Security
University College London
UK

January 28, 2008

1. Issue: What is e-cash?

Example: Should phone cards be viewed as electronic cash?

So, we will use a broad definition of electronic cash. Any payment method involving electronics may be viewed as electronic cash.

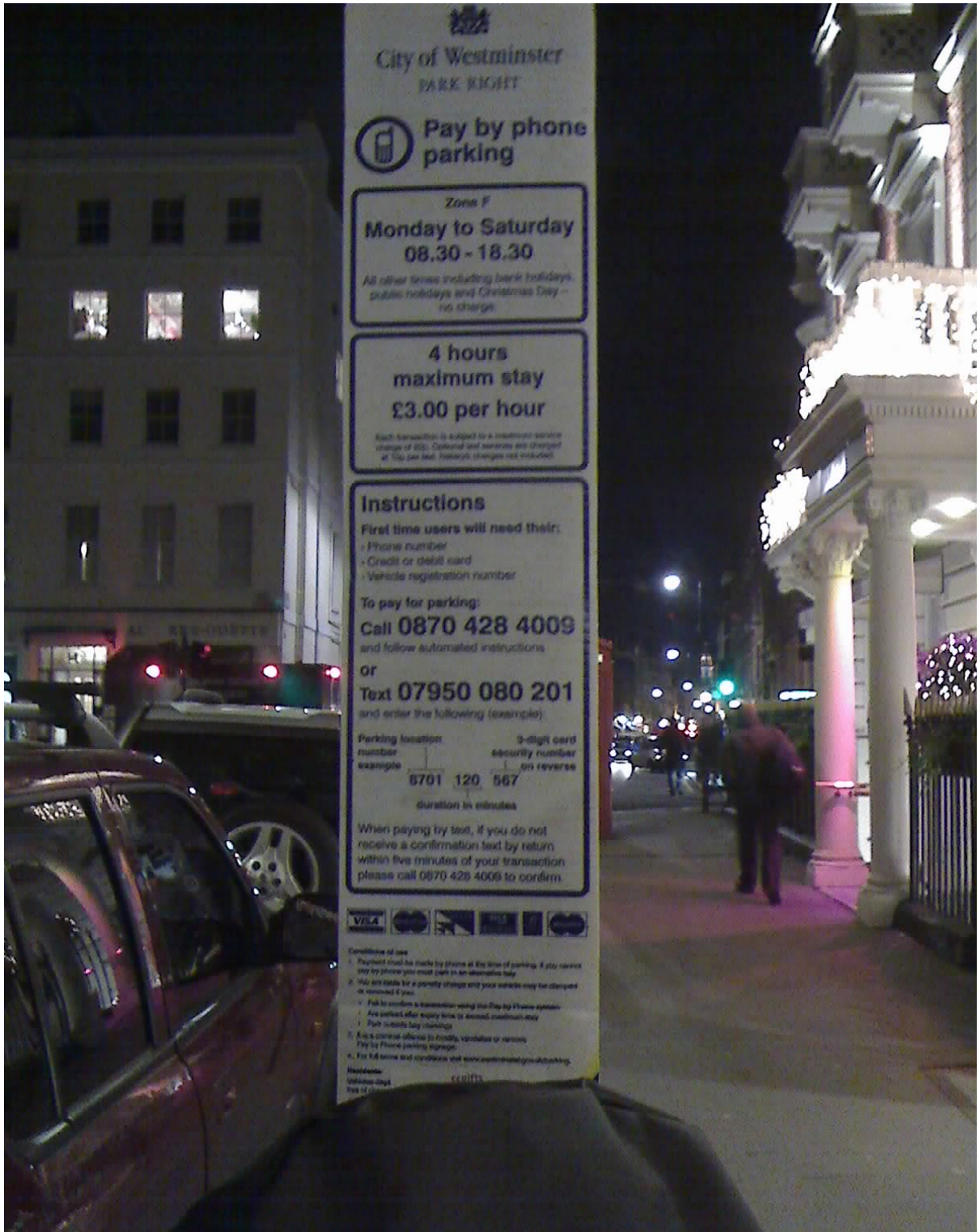
Evidently, different people may agree/disagree on this definition. Indeed, credit card payments could be viewed as a replacement for checks. However, today they are used for smaller and smaller transactions.

Many issues we address in the panel are sufficiently general that making a distinction is irrelevant.

UCL

2. ISSUE: PAPER CASH GETTING UNTENDERABLE TODAY AND OBSOLETE IN 20(?) YEARS

Parking “meters” in Westminster (a city in London)


City of Westminster
PARK RIGHT
Pay by phone parking
Zone F
Monday to Saturday
08.30 - 18.30
All other times including bank holidays, public holidays and Christmas Day – no charge
4 hours maximum stay
£3.00 per hour
Instructions
First time users will need their:
- Phone number
- Credit or debit card
- Vehicle registration number
To pay for parking:
Call 0870 428 4009
and follow automated instructions
or
Text 07950 080 201
and enter the following (example)
Parking location number example
3-digit card security number on reverse
8701 120 567
duration in minutes
When paying by text, if you do not receive a confirmation text by return within five minutes of your transaction please call 0870 428 4009 to confirm.


Each transaction is subject to a maximum service charge of 20p. Optional text services are charged at 10p per text. Network charges not included.
Instructions
First time users will need their:
› Phone number
› Credit or debit card
› Vehicle registration number
To pay for parking:
Call 0870 428 4009
and follow automated instructions
or
Text 07950 080 201
and enter the following (example):
Parking location number example
3-digit card security number on reverse
8701 120 567
duration in minutes
When paying by text, if you do not receive a confirmation text by return within five minutes of your transaction please call 0870 428 4009 to confirm.
VISA
Conditions of use

Sydney Harbor bridge

Today: can still pay cash at booths. However, the Sydney Harbor Tunnel booths only accept wireless e-cash. Moreover, the goal is to switch the bridge too (85% of the users used cash in 2004).

Is paper cash (and coins) going the way of audio/video tapes, Long Play, typewriters, etc.? Is e-cash the digital replacement of paper cash, as MP3 is for CDs, DVDs for video tapes, laptops and keyboards/PCs for typewriters, etc.?

If so, we better understand the impact before we regret this!

3. ISSUE: RELIABILITY OF REAL E-CASH

Example:

On October 15, 2006 at 7:07:48 AM local time an 6.7 earthquake hit near Hawaii. It knocked out ATM systems. Although the Hawaii earthquake affected a small number of people, it just illustrates what a more major natural disaster could do to electronic cash.

Large meteor impact with earth will cause a huge EMP! So, when you want to avoid a lawless society, e-cash no longer working will worsen the situation.

Any evidence? Look at the history of the Bank of America (formerly called Bank of Italy) and the earthquake in San Francisco!

4. ISSUE: REAL E-CASH SYSTEMS ARE INCOMPATIBLE

It seems we are in for a repeat of history. Indeed: e.g., in the US (from the US Secret Service WWW):

> During . . . (1793 - 1861), approximately 1,600 private banks were permitted to print and circulate their own paper currency under state charters. Eventually, 7,000 varieties of these ”state bank notes” were put in circulation, each carrying a different design!

How incompatible is e-cash? Plenty of examples: phone cards from different countries. Here an extreme example:
the Roam Express Visitor’s e-PASS that can be used to pay the Lane Cove Tunnel in Sydney cannot be used on the Sydney Harbor Tunnel.

5. Issue: Social, health, etc.

Several issues:

Barriers:

Economic: Not everybody has a credit card (Sydney tunnels, Westminster parking)

User unfriendly: e.g. the Westminster (London) parking system (accordingly to Stephen Johnston)

Health: Research showed a relationship between cell phone by males and a decline in fertility.

Legality:

Question: is the Westminster parking solution legal?

A document from the UK Treasury explicitly states under D3.8 that:

Cash is legal tender and therefore must be accepted by all retailers at its face value.

However, not accepting cash in Australia seems legal!

Longlivity: E-Cash often expires. E.g., SingTel electronic cash expires after roughly 1 year!

Privacy: E.g. Westminster parking enforcement: know who is parked where. To enforce the new system, extra cameras are installed that will view 80% of the license plates in the parking areas.

Xenophobia: Does it promote xenophobia? Some claims/questions:

- Oyster (London Public Transportation) card: not easily available to foreigners. Many charges are 50% compared to paper tickets.
- No exchange boots for real electronic cash systems.

- E-Cash often expires!
- Belgium: buying gas (petro) with international credit is almost impossible. One needs a local card.
- France:
  - no public phone booths accept Euros!!
  - using an automatic booth to buy a train ticket at Charles de Gaulle Airport in Paris: only chip and pin credit cards are accepted!

6. ISSUE: ACADEMIC CASH VS REAL E-CASH

Academic cash focuses on the following security goals/threaths:

Counterfeiting: using for example blind signatures.

Deniability: Can "deny" having . . .

Double spending: first one who rushes to bank is the legitimate one.

Privacy: Issues as anonymity and deniability have been studied extensively. However, only a fraction of e-cash systems deployed take privacy concerns into account.

Wallet vs. non-wallet: most research proposes non-wallet solutions. Impact: requirement of bank increases: Hawaii earthquake!!!

Although cryptography is used to protect chip card technology, few

payment systems studied by researchers are widely deployed. This poses/raises several questions/issues:

- Most users view many of above issues as irrelavant. So, is the research relevant?
- Most research does not address compatibility, exchangeability, reliability, etc. Many of these aspects, such as reliability, can be considered as being much more important than anonymity!
- What role can cryptography play, in particular to come to a standard?
- Is it time for an international electronic cash standard which allows electronic cash which is exchangeable, reliable, universal, etc?

7. POTENTIAL SOLUTIONS

To address:

Universability: DoCoMo phones in Japan. One can port RFID based e-cash systems onto the phone. Saw them at work.

Disadvantage: cell (mobiles) phones are very good tracking devices!

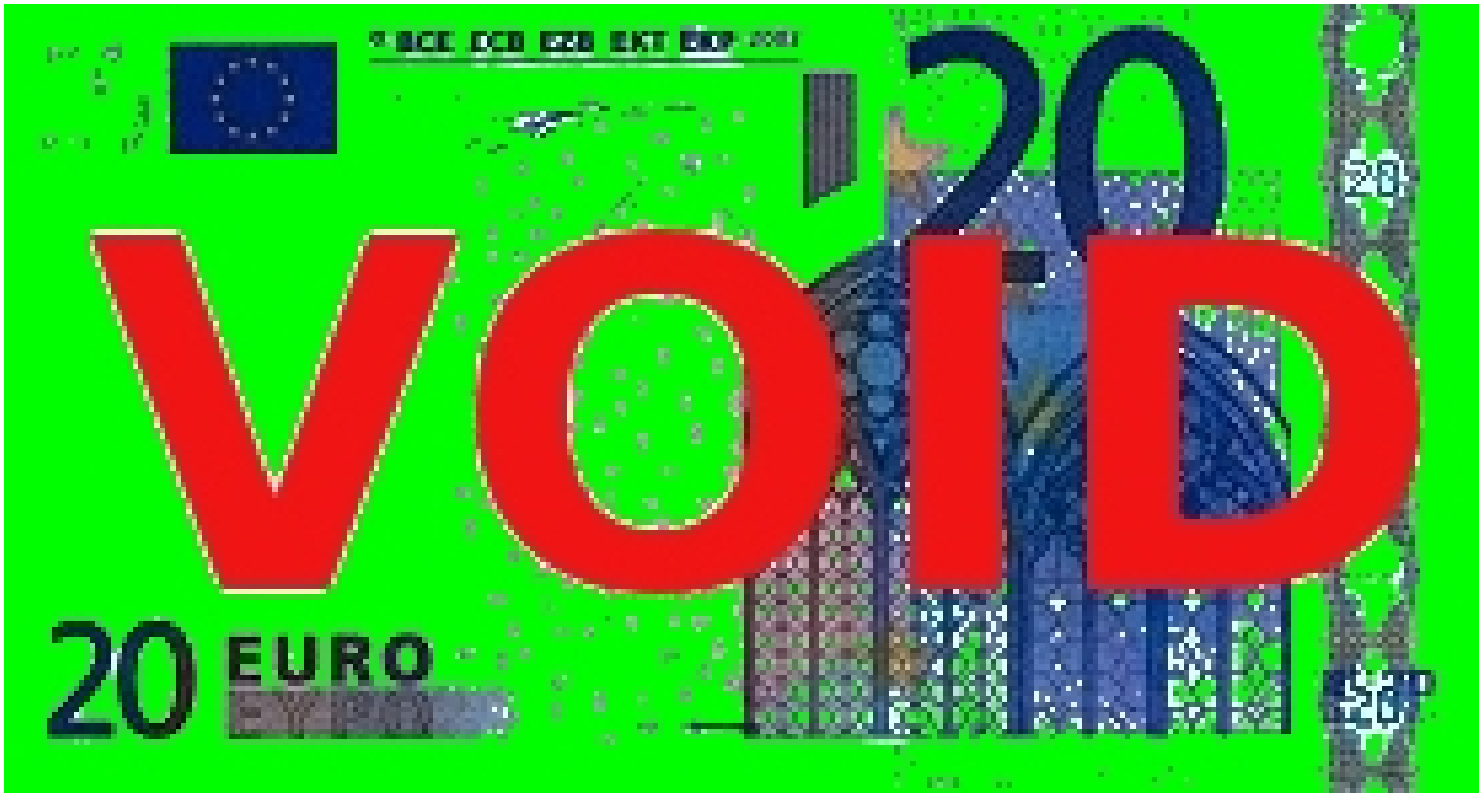
Reliability: some research in crypto has addressed the issue of combining privacy and reliability. However, heavily focussed on transmission and no research on private and reliable e-cash.

Alternative solution: “erasable paper cash” when equipped with RFID.

Typical 20 Euro note (with RFID chip)

Typical 20 Euro note (with RFID chip): spending the money

Spent the money!!!



8. CONCLUSIONS

- We see a few examples of paper cash getting untenderable. If paper cash goes the same as typewriters, etc., paper cash might be obsolete in 20 years. Is this a good idea?
- Research on e-cash does not take into account: reliability, compatibility, user friendliness, etc.
- What should we do?

  Should we as scientists warn the Treasuries of different countries that e-cash is displacing “paper” cash and what the consequences might be?

9. PANEL MEMBERS

Jon Callas	PGP Corporation, USA
Yvo Desmedt (moderator)	University College London, UK
Daniel Nagy	ELTECRYPT, Eotvos University, Hungary
Akira Otsuka	National Institute of Advanced Industrial Science and Technology, Japan
Jean-Jacques Quisquater	Universite Catholique de Louvain Belgium
Moti Yung	Google Research, USA