ROUGH DRAFT
On-line versus Off-line Electronic Cash Systems

Chris Laas

June 42, 2000

Id

1 Introduction

2 Several On-line Systems

2.1

Dan Simon's chits

2.2

Chaum's cash checks

2.3

Brands stored value (worth even mentioning?)

2.4

Non-anonymous systems? PayWord, MicroMint (both micropayment systems, not necessarily representative)?

3 Several Off-line Systems

3.1

Brands '95, a popular one.

3.2

Pick-a-provably-secure-system, all broken?

3.3

"Universal Electronic Cash"

4 Um, Arguments

Complexity: on-line systems are relatively simple. E.g. Dan Simon's chits. Off-line systems are complex to implement. E.g. Universal Electronic Cash. Also note that other operational aspects of the system are bound to be equally complex to the actualy cryptographic aspects.

Level of anonymity: definitions of anonymity vary subtly. For example, Dan Simon's system is anonymous in a different sense than most systems.

Double-spending: on-line systems prevent double-spending, short of a break in the cryptographic security. Off-line systems only provide detection of double-spending. OTOH, off-line systems provide immediate prevention of double-spending when in on-line mode. However, an off-line fallback mode invites DOS attacks, which are not easily avoidable. However, widespread DOS attacks can be countered by communication through out-of-band mechanisms (i.e. phone, radio, TV, etc).

Liability for fraud. Who is liable if Mallory spends a $50 bill 1000 times simultaneously and then skips the country? The situation is theoretically impossible in a totally on-line system (which shuts down if the network is unavailable); however, it is possible in an off-line fallback scenario in which Mallory disrupts the network at the central bank. Who loses money in this case? Does the bank charge a percentage on each transaction to cover fraud? (But is this compatible with the concept of "cash"?) OTOH, do the merchants simply suck it up? (This is what happens with forged cash today; however, note that there exists the Secret Service; also, consider perceptions of electronic money, in which banks seem to be expected to suck up damages.) Consider that perhaps there must exist some form of "insurance" in the system if merchants are not to suck up these damages.

Perceptions of liability.

Detection of fraud. In which systems is fraud detectable? By which channels? Is framing detectable? Where can the concept of "hidden predicates" be used?

5 Conclusions

Tentative? conclusion: off-line systems, which normally operate in an on-line mode, provide the greatest level of flexibility to the system's users. Merchants may choose the tradeoff between security and continuing business in the case of network unavailability. In the face of a network outage, Max's Diamond Shop may disable electronic cash payments altogether (perhaps falling back to personal checks or another mechanism); the Coop might decide to require additional identification of some sort along with payments (for example, "anonymous" digital photos); LaVerde's Sub Shop might decide to enable off-line electronic cash after phoning in to the Bank to confirm that the outage is local; and the Coke machine on the corner might decide to simply fall back to off-line mode. (After all, it probably costs Mallory more than 75 cents per Coke machine to perpetrate his crime. And even if he succeeds, how is he going to sell a thousand stolen cans of Coke on the black market? We can't consider Mallory to be a prankster kid who is stealing Cokes, either, because the double-spending will be detected and punishment meted out after the fact.)

Tradeoffs to weigh:

- Cost of potential fraud due to network outages versus cost of lost business due to network outages.
- Likelihood of fraud via various channels (double-spending, cryptosystem break, embezzlement).
- Perception of liability in the system.