Electronic Cash summary

zondag 8 januari 2023 11:49

Conventional cash properties

- Different values
- Transferable
- Anonymous
- Untraceable
- Unforgeable
- Hard to duplicate

Simple schemes

Needed protocols

- Deposit
- Payment
- Withdrawal

Initial solution to double spending problem: give digitally signed bill to bank, only accepted if not deposited before.

Cut and Choose

1. Create k checks with random serial numbers and amount.
2. Send envelopes *(with carbon paper, so that signature ends up on check)* to bank and tell them amount.
3. Bank opens $k-1$ envelopes at random and verifies amount.
4. Bank signs remaining envelope, withdraws amount and sends back envelope.
5. User takes out check and verifies signature.

Blind signatures

Blind signatures allow to hide the message that is being signed. That is, the signer is provided with the blinded message $b(M)$, then provides a signature σ' on $b(M)$, from which a signature σ on M can be extracted.

Security properties

- One-More Unforgeability: from l oracle calls, no more than l valid signed messages should be obtainable.
- Unlinkability: the signer should be unable to link any particular signature with a specific execution of the signing protocol. *Possible using RSA signatures.*

Multiple roots-solution

Use different public exponents (e_i) to encode different denominations of electronic coins. As long as the e_i's are relatively prime, index calculus-like attacks do not work.

Offline version of protocol

Include $y_j = H(x_j)$ and $y_j' = H(x_j')$ in the bill, where the XOR of x_j and x_j' gives the user's identity. Then, use the approach with unblinding $k-1$ bills again (on top of this).
If the user attempts to spend a bill twice, (a part of) the user's identity is leaked.

Bitcoin

Transactions contain arbitrarily many inputs and a maximum of two outputs. A block includes a periodical ('*timestamped*') snapshot of all transactions. The proof of work mechanism *de facto* functions as a distributed timestamp server. Search for a hash less than target value is adjusted so that the search always takes about 10 minutes.

- Bitcoin rewards work in the form of creating new Bitcoins and obtaining transaction fees.
- Rough idea to prevent malicious behavior (e.g. forking): undermining the system does not earn as much as sticking by the rules. *(This does not always work, though.)*