Properties of cash

- Cash has a **value**. It can be traded for goods or services;
- It is **anonymous** (unlinkable anonymity). Previous owners of the cash are not known and in general it is not possible to keep track of by whom and where the cash is spent.
- It is **secure**. Cash currency is specifically designed to deter counterfeiting.

Requirements for e-cash

- Okamoto and Ohta (1992):
  - Privacy;
  - Security;
  - Transferability;
  - Divisibility;
  - Hardware Independence;
  - Scalability;
  - Acceptability.
Privacy and Security

- Privacy ("Untraceability" or "Anonymity"):
  - The privacy of the user should be protected. The relationship between the user and his purchases must be untraceable.

- Security:
  - The aim of security in cash payment protocols as in is to prevent any party from cheating the system

  (compulsory requirements)

Transferability

- Transferability:
  - the transfer of "coins" (units of electronic cash) from individual to individual may be allowed in a system;
  - Unlimited transferability is not without problems. It may conflict with the security requirement.

  (optional requirement)

Divisibility

- A cash scheme which satisfies the divisibility requirement allows an electronic coin to be divided into smaller parts;
- E-cash as compared with the conventional cash may provide greater degree of divisibility (micropayments in the fraction of pence)

  (optional requirement)

Acceptability

- The acceptability property allows an anonymous payment scheme with multiple banks to accept coins minted by other banks;

  (optional requirement)
Blind Digital Signatures

- First introduced by D. Chaum, 1985;
- One of the most important mechanisms used in e-cash;
- The main aim of the blind signature is to allow a participant to sign a particular message without gaining knowledge of the message.

RSA-based blind digital signatures, I

- Let \((e,n)\) be the bank’s public key and \((d,n)\) the bank’s private key.
- The customer chooses a random value \(k\), between 1 and \(n\). \(k\) is the blinding factor. The customer blinds the message \(m\) by calculating: \(t = mk^e \mod n\). The customer sends \(t\) to the bank.
- The bank signs \(t\) by applying \(d\): \(td = (mk^e)^d \mod n\). The bank returns the signed message \(td\) to the customer;

RSA-based blind digital signatures, II

- The customer unblinds by calculating \(s = td/k \mod n\);
- Thus \(s = m^d \mod n\). The blinding factor has been removed;
- Anyone can check that \(m\) has been signed by the bank, by applying the bank’s public key \(e\);
- At the same time the bank has not learned anything about \(m\).

Basic e-cash system with blind signatures
Withdrawal

1. The payer generates a coin \( \text{coin} \) with an operation \( \text{gencoin} \). For example the payer generates a random value \( c \), which is 160 bits shorter than \( n \), and sets \( \text{coin} = (c, \text{hash}(c)) \).

2. He transforms it with an operation \( \text{blind} \) by multiplying coin by blinding factor (modulo \( n \)). We call the result \( \text{blindcoin} \).

- 3. He sends the blinded coin to the bank together with a withdrawal order stating what amount he wants, e.g., 1 Euro, and from which account.
- 4. The bank subtracts the amount from the account and signs \( \text{blindcoin} \) with a special key depending on this amount.
- 5. The bank sends the resulting signature, \( \text{sigblind} \), back to the payer, who tests it.

Payment with deposit

- 6. The payer uses an operation \( \text{unblind} \) on the signature and get the result \( \text{sig} \). He needs stored parameters (blinding factor) from \( \text{blind} \) for this.
- 7. He sends \( (\text{coin}, \text{sig}) \) to the recipient.
- 8. The recipient simply forwards this to the bank to make an online verification against double spending.
- 9. The bank verifies the signature and checks in a database that this coin was not deposited
  - before. If all is ok, it enters the coin there and adds the amount to the recipient’s account.
- 10. The bank tells the recipient the result of the tests.
- 11. If it was ok, the recipient typically signs a receipt or gives the payer goods.

Withdrawal and payment

Property of the basic system

- Payer anonymity with unlinkability;
- Transferability;
- but
- No recipient anonymity;
- No divisibility;
- No security in disputes;
- Bank involvement in all transactions! – Cryptocurrencies (Bitcoin, etc) can do better (will look later in the course)