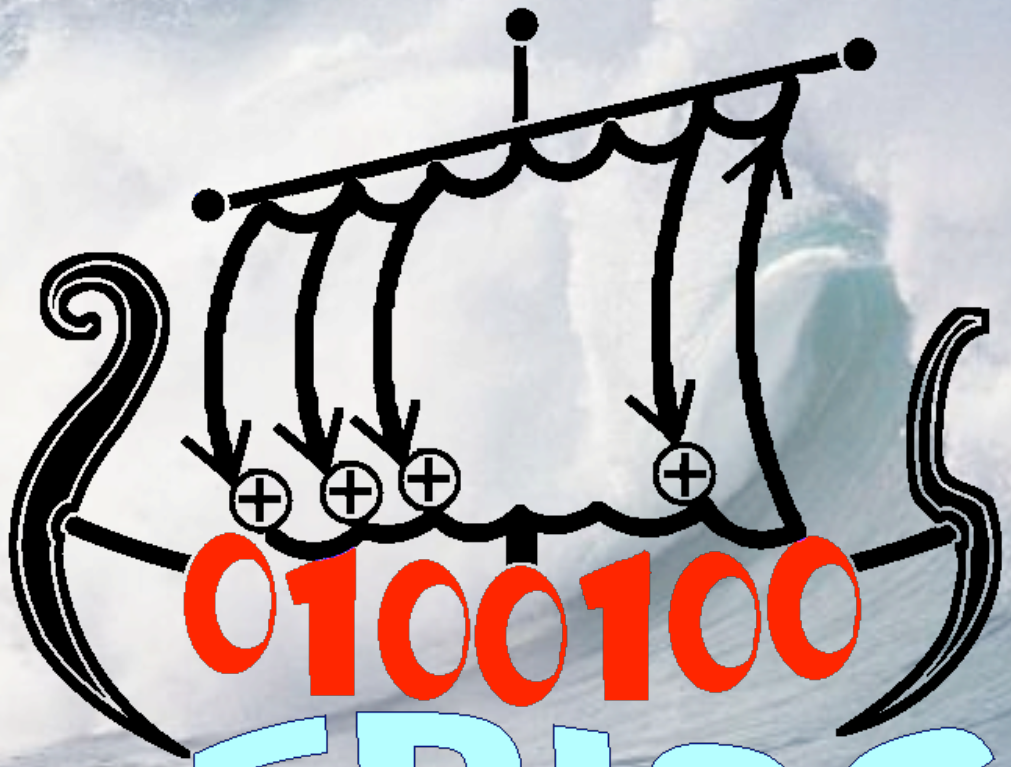
Forum for Research and Innovation in Information Security and Communications



FRISC.NO

Frokostmøte
MOBIL BETALING

Rica Nidelven, 4.april 2014

Meny

Mobil Betaling

Internett og mobil kommunikasjonsteknologi bringer nye digitale betalingsinstrumenter. Hvilke muligheter og utfordringer foreligger? Hva vil virke? Kan norske IKT-bedrifter bidra med teknologi og løsninger? Tre innledere belyser dette aktuelle temaet fra ulike ståsteder:

- Stig Frode Mjølsnes, professor, NTNU:

Betalingstransaksjoner som infosikkerhet-system, gamle instrumenter blir som nye, digital valuta, ecash, bitcoins, mobil betaling, SIM eller smartkort, …

- Ola Martin Lykkja, R&D engineer, Q-FREE

Krav fra myndigheter, publikum, anonymitet, nye teknologier, GPS-basert veiprising, betalingsløsninger, forhåndbetaling, kreditt-kort…

- Thor Ragnar Klevstuen, Business Developer, Financial Services, EVRY

Hvilke trender er viktigst i fremtidens betalingslandskap? Hvem er de globale aktører i denne konkurransen? Hva gjør vi her i Norden for å skape denne fremtiden!

Spørsmål og diskusjon.

Tid: **Fredag 4. april 2014 kl 8.30 – 10.00**. Frokost serveres fra kl 8.00.

Mobil Betaling

Stig F. Mjølsnes, NTNU

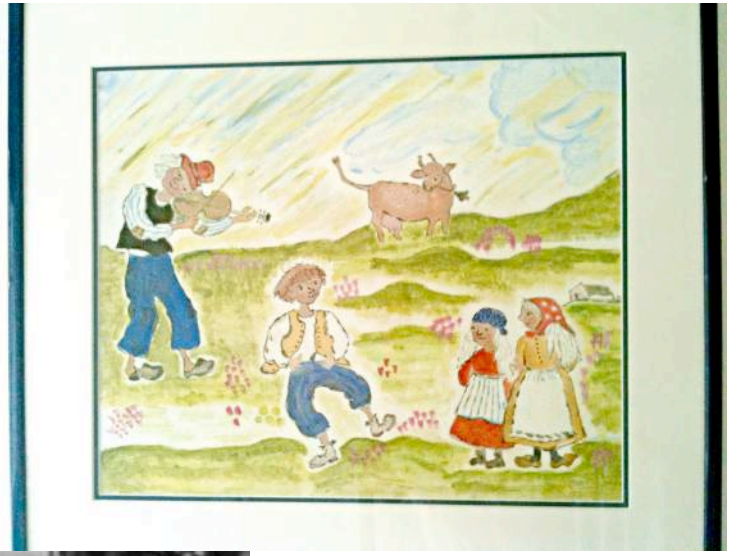
FRISC frokostmøte
Rica Nidelven, 4.april 2014

Gammelt blir som nytt

Deposit checks from your smartphone or

Why drive to the bank when using your smartphone or iPa QuickDeposit℠? Just snap a your endorsed check with yo send it using the Chase Mobi **free** for eligible Chase check customers.

Byttemiddel

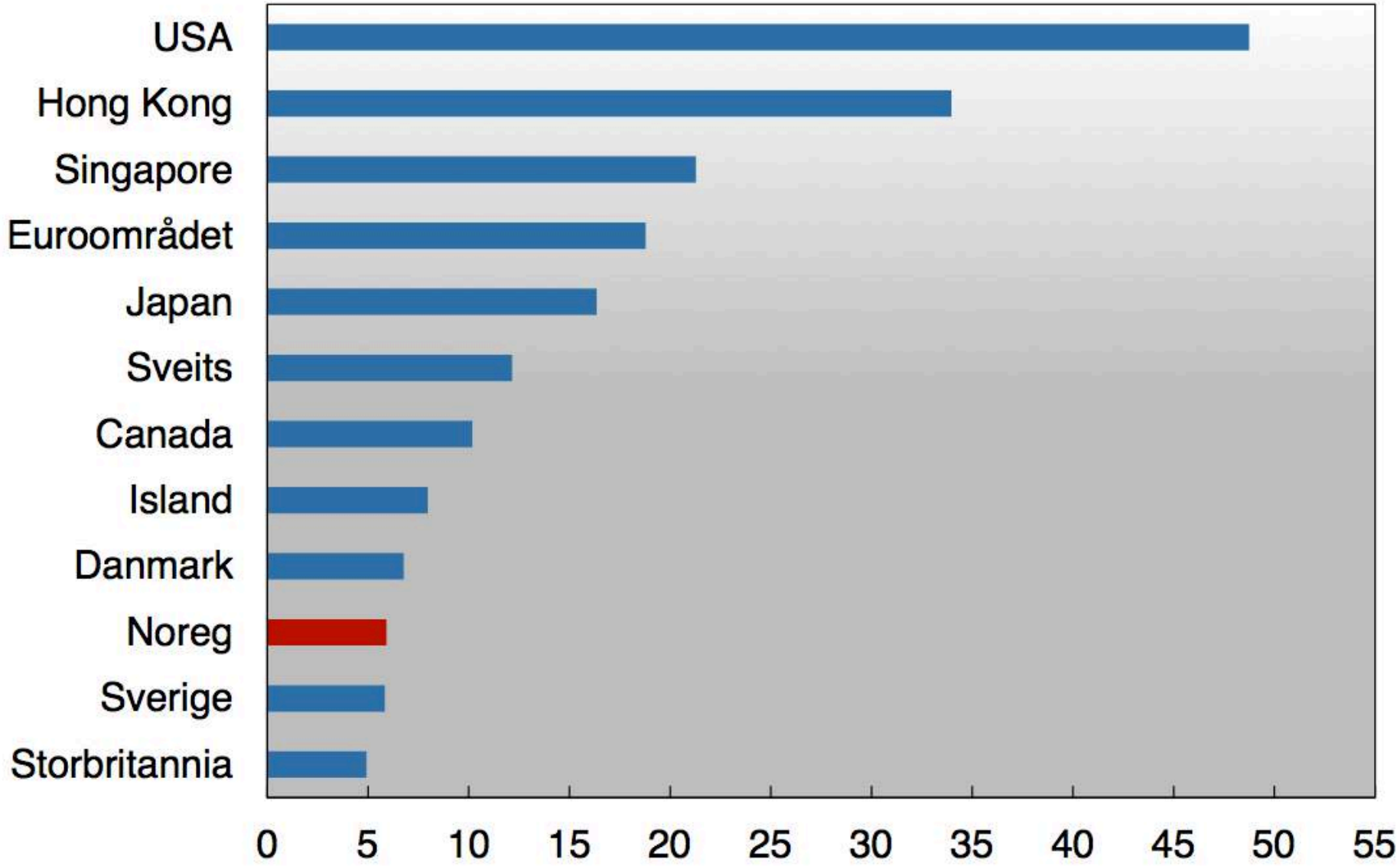


Walking a Tightrope
With the mark almost worthless, bartering made a comeback. Germans are seen here swapping bread, sausages and jam for tickets to the circus.

Portable Byttemidler

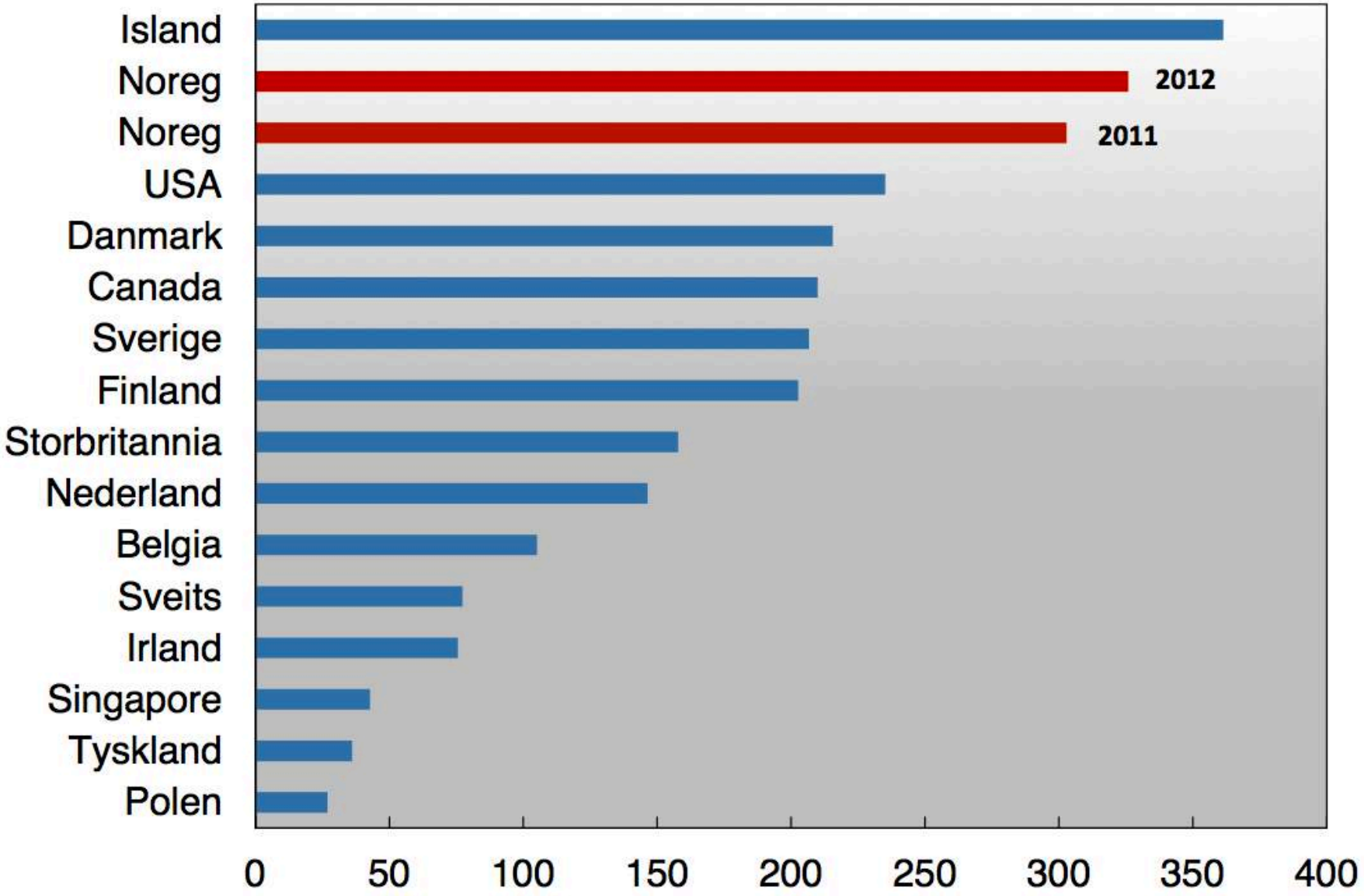
- Edle metaller
- Mynter (fellesnevner, valuta)
- Papir (seddel, veksel, sjekk,..)
- Fysiske penger
  - Pålydende >> egenverdi
  - Ingen innløsningsrett ”fiat”
    - Ingen øvre grense for pengemengde
  - Tvunget betalingsmiddel
  - Ikke renter
- Immaterielle penger
  - Digitale bitstrenger ”data”
  - Datamaskiner lagrer og behandler
  - Betaling: Datakommunikasjon, meldinger

Figur 1.2 Kontantar som del av betalingsmiddel (M1) i utvalde land.
Prosent. 2011



Kjelder: Noregs Bank, ESB, BIS/CPSS og Seðlabanki Íslands

Figur 1.4 Korttransaksjonar per innbyggjar, betalingar og kontantuttak. 2011



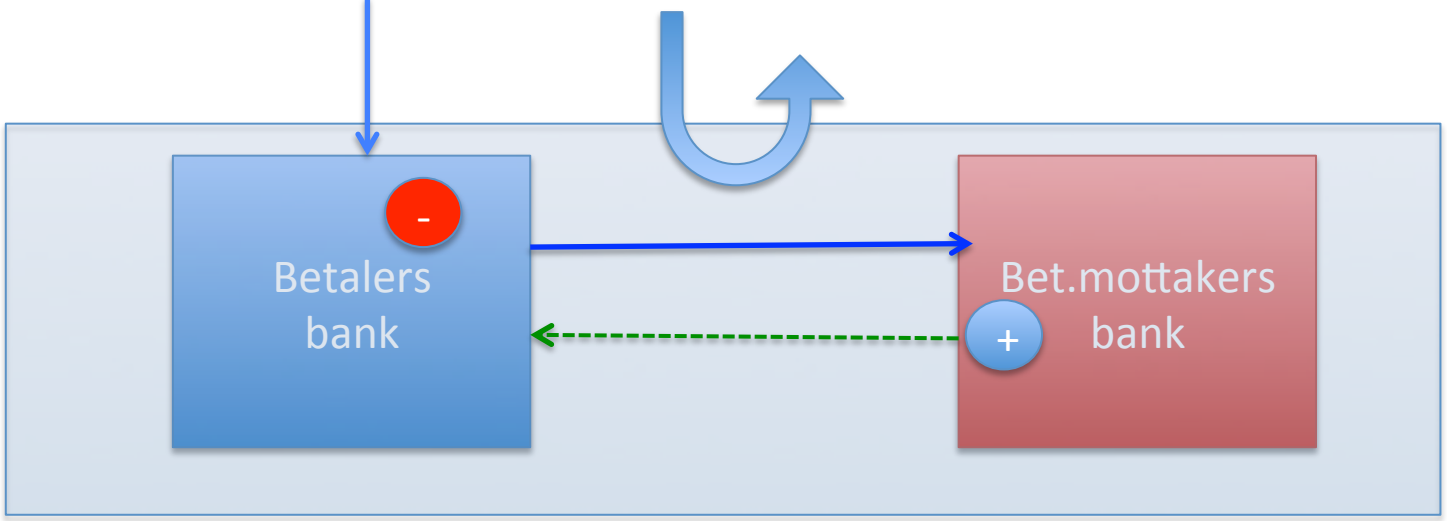
Kjelder: Noregs Bank, ESB, BIS/CPSS og Seðlabanki Íslands

Måter å betale

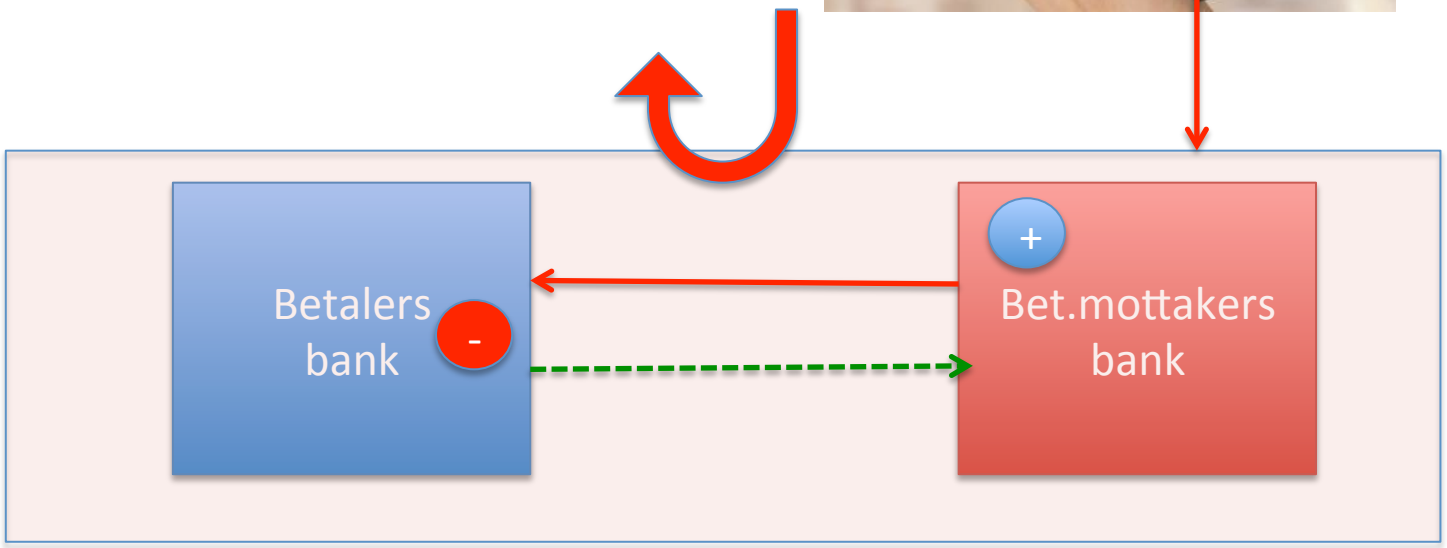
1. **Direkte** fra betaler til mottaker
   - Her og nå, lokalt, kontant, desentralisert
2. **Formidlet** betaling
   - *Push* melding, fra betaler til "Systemet"
     - Til betalers bank, andre formidlere,
     - Bankgiro, IBAN, BIC/SWIFT/wire transfer, kontantuttak,..
   - *Pull* melding, fra betaler via betalingsmottaker til "Systemet"
     - debetkort, sjekk, fullmakt, kredittkkort, forhåndsbetalt, ..

Push

Betalings mottaker

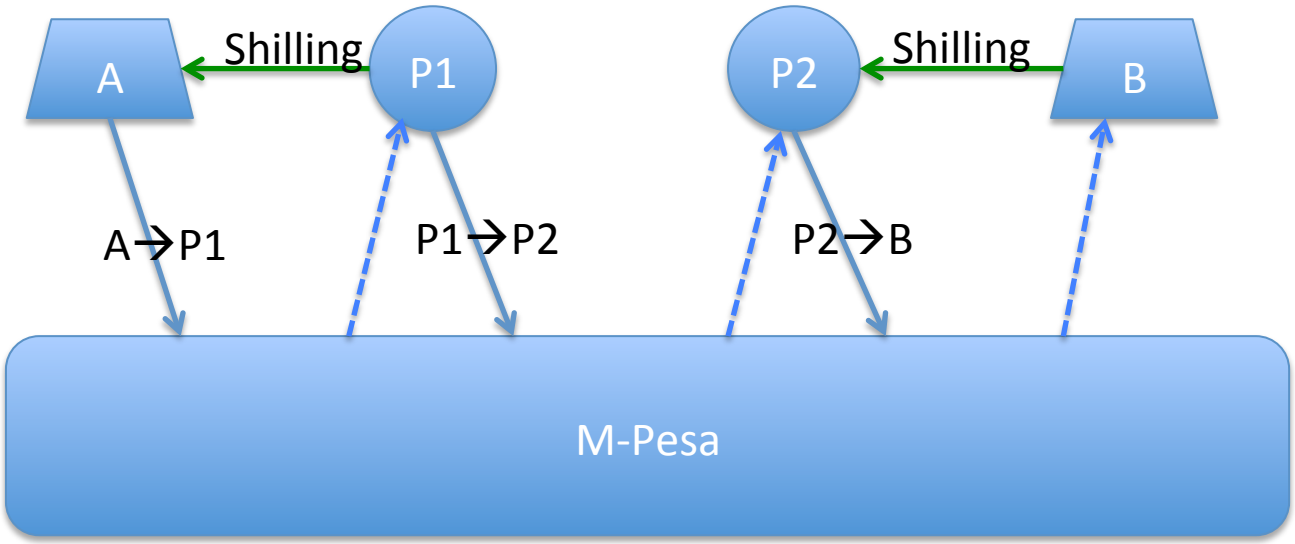


Pull



M-Pesa
(”Mobil Penger” er enkelt)

- Enkelt: GSM SMS tekst, SIM Toolkit menyer
- Navn&Autentisering: Mobilnummer&SIMkort
- Kenya, Tanzania, Afghanistan, Syd-Afrika, India, Egypt, …



E-pengeforetakslov (2002) etter EU-direktiv

- Hensikten et kostnadseffektivt alternativ til tradisjonelle betalingsmåter som bruk av kontokort og kontanter.
- For småbetalinger med kontanter. Max 150 Euro på mediet, utsteder inntil 6 millioner Euro.
- En pengeverdi representert ved
    - En fordring på utsteder
    - Lagret på et elektronisk medium
    - Utstedt etter mottak av midler
    - Innløsingsrett til mynter/sedler
    - Anerkjent betalingsmiddel av andre foretak enn utstederen
- Kontanter i elektronisk form
  - Pengeverdien lagres direkte på den elektroniske innretningen, og ikke også på en konto.
  - E-penger skal ikke være rentebærende

Dagens utfordring

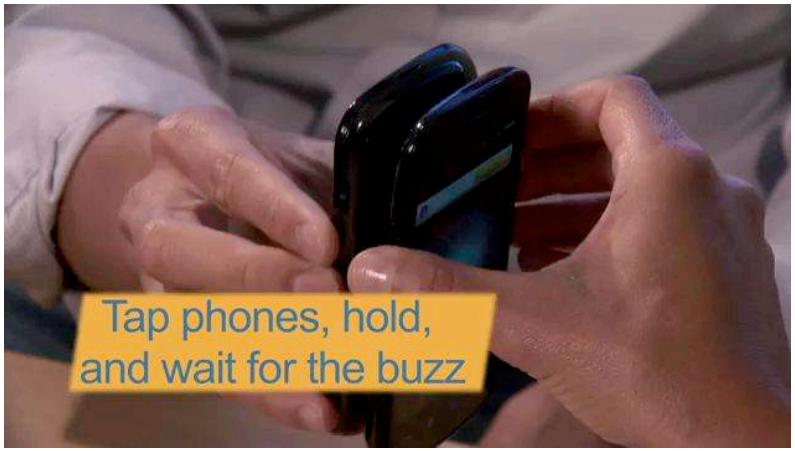
Direkte elektronisk betaling?

Tellerverdi i fiklesikker elektronikk, småpengekort klippekort osv. krever spesielt betalingsapparat

Er det mulig uten mellommann/formidler, altså P2P?

- Ingen interessant forretningsmodell?
- Er det samfunnsmessig ønskelig?

Likevel, er det mulig? Hvordan?



Privatlivets fred og IKT

Hvem tar vare på bekymringen for privatlivets fred (privacy) ?

- Bedrifter har ingen egeninteresse, tvert imot
- Offentlige etater har ingen egeninteresse, tvert imot
- Folk flest bryr seg ikke (ennå)

Enorme kommersielle interesser for persondata

- Prisdifferensiering for beste market yield

Etterforskningsformål

Nasjonal sikkerhet

Bitstrenger som valuta?

- En ide: Digital Signatur
  - Utsteders signatur på spesielle bitstrenger
  - Alle kan sjekke ektheten av pengene
- Ihendehaver-penger?
  - hvordan flytte en bitstreng fra betaler til betalingsmottaker?
  - Lokalt, kontant,
- Kopiering?
  - Hvordan unngå at betaler ikke bruker samme bitstrenger i flere betalinger?

Kontanter med digitalsignatur

1981 E-cash ide

Emulerer kontant betaling

- Uttak fra bank-konto
- Personvern
  - betaler-anonymitet
  - Betalingene kan ikke kobles
- Sentral identifisering ved kopiering/gjenbruk

1989 Digicash (online payments)

1992 CAFE (offline payments)

- Både for butikken og for nett

Mjølsnes (2001)

Localized Credentials for Server Assisted Mobile Wallet

Int. Conf. On Computer Networks and Mobile Computing, 2001

We propose a fully distributed multiparty secure architecture so that the user can leave most of the content of his electronic wallet in the security of his home while travelling with his mobile terminals. Emerging GSM and UMTS mobile terminals supporting both short range Bluetooth and cellular GPRS are excellent platforms.

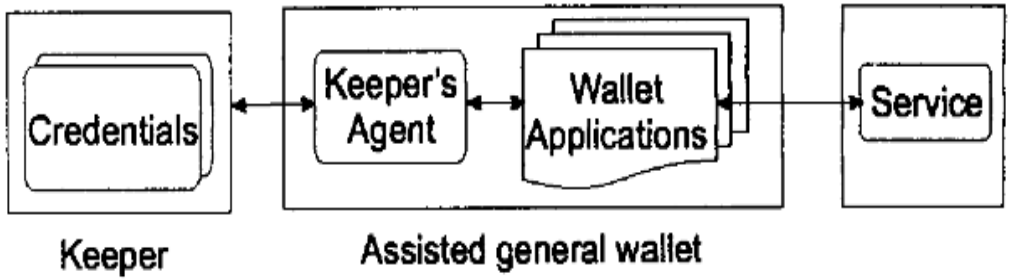
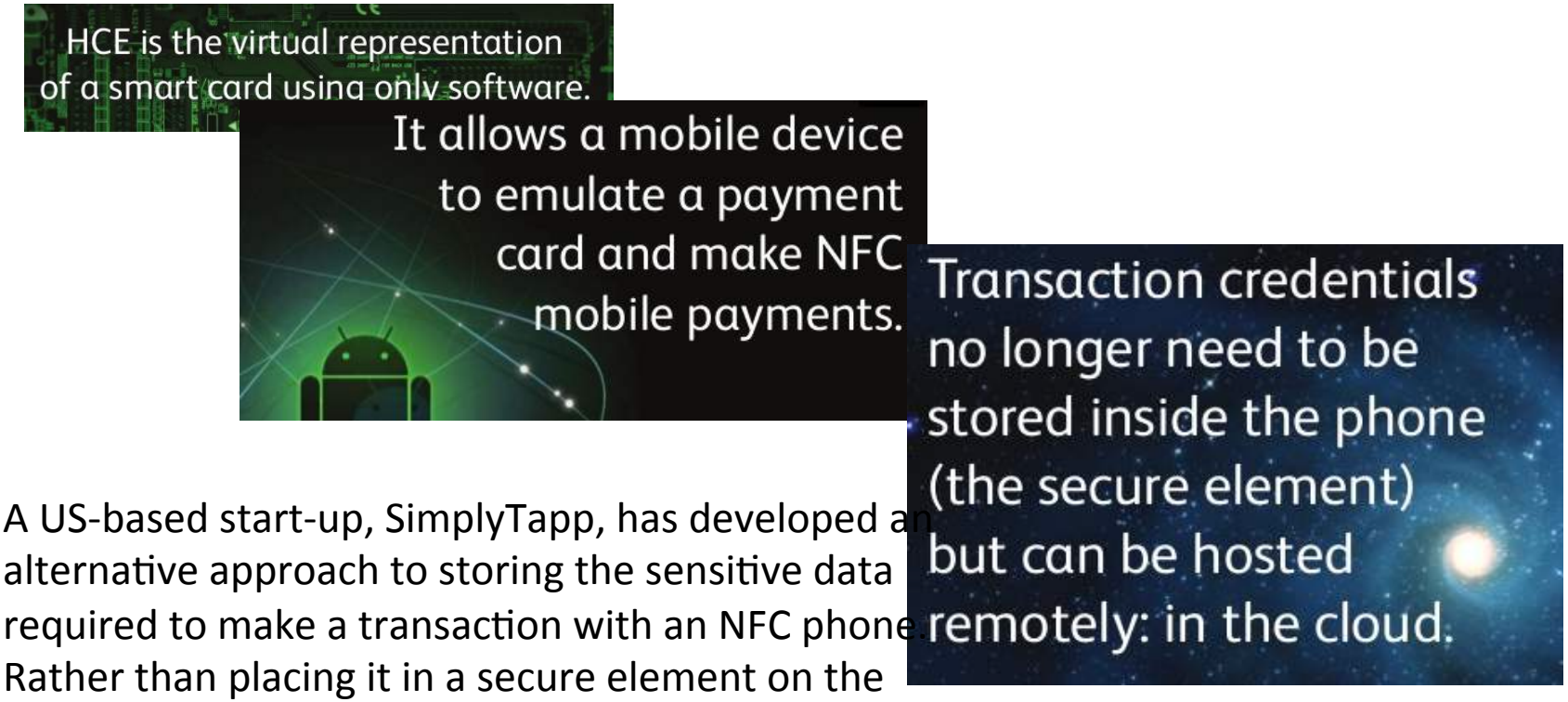


Figure 5. The assisted wallet in general with multiple applications that may be assisted through the keeper's agent by the keeper's credential computations, based on the credential hardware mounted in the keeper.

Host Card Emulation (HCE)

Yeager and Fifelski,2011

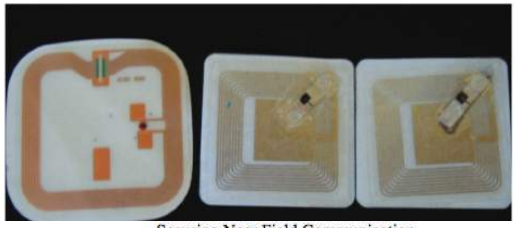


A US-based start-up, SimplyTapp, has developed an alternative approach to storing the sensitive data required to make a transaction with an NFC phone. Rather than placing it in a secure element on the phone, SimplyTapp stores the data in the cloud on a "remote secure element" and passes encrypted transaction data through the phone to a point-of-sale terminal when the user makes a purchase.

NFCworld By Sarah Clark • September 19th, 2012

Eavesdropping Near Field Communication (2009)

Henning Siitonen Kortvedt and Stig F. Mjølsnes



Securing Near Field Communication

Figu

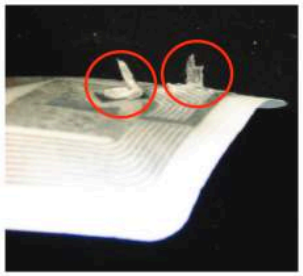


Figure 21: Modified label with marking of connection points

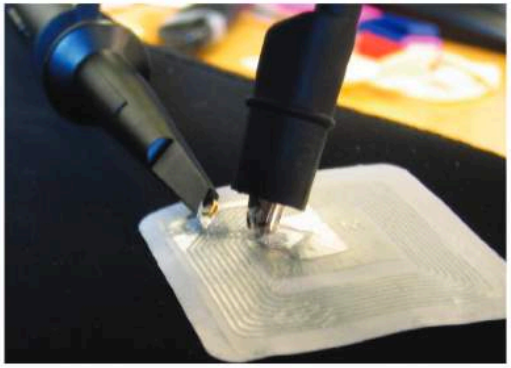


Figure 22: Modified label with measurement probe connected.

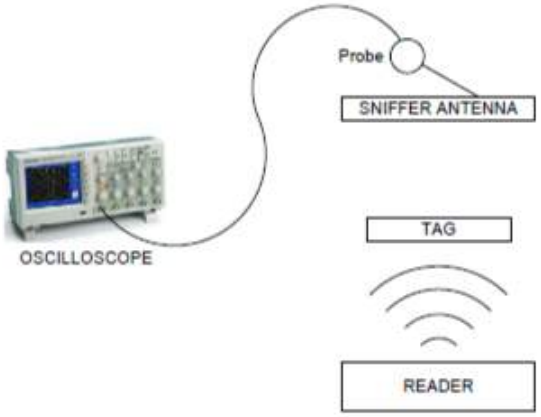


Figure 17: Test set-up illustration.

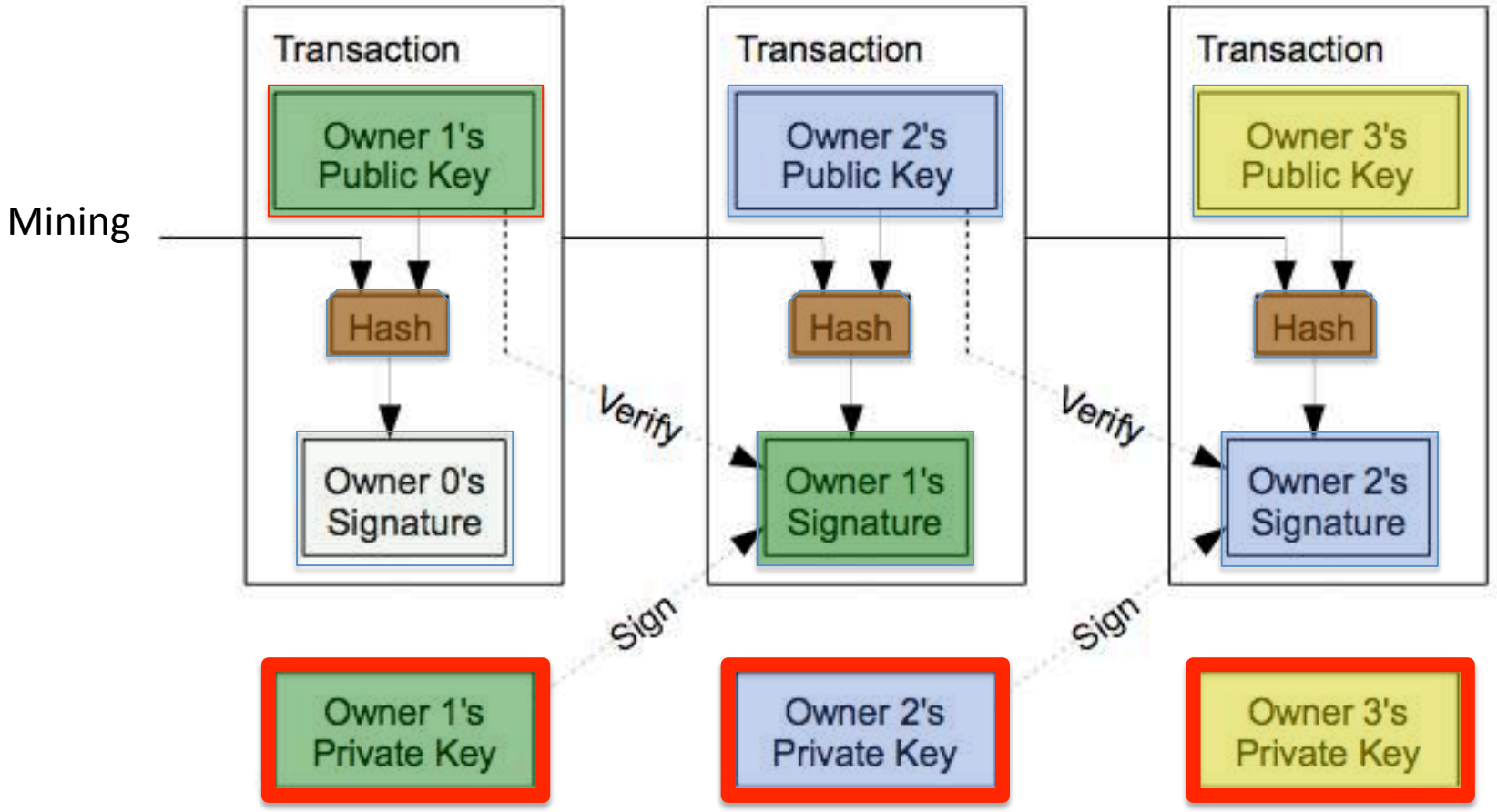
Figure 31: Load modulation from NOKIA 6212 classic.

000000000000[illegible]7252333f7aeb619c89d220985a70ac0e015248e0

BitCoin (2009)

- En desentralisert løsning på kopieringsproblemet
- Pengeoverføringen føres inn i en betalingslogg.
- ”Alle” vedlikeholder denne ”på nettet”, en slags crowdsourcing av betalingsformidleren
- Essensielt en flerparts kryptografisk protokoll
  - Digital signatur: privat signaturnøkkel og tilhørende verifiseringsnøkkel.
  - En betaling: En signering over til ny eier (ny signatur- og verifiseringsnøkkelpar), og kringkaster dette for innføring i betalingsloggen.
- Siste ledd i kjeden inneholder verifiseringsnøkkelen til nåværende eier, dvs. den som er i stand til å lage neste ledd slik at signaturen stemmer, dvs. den som har signaturnøkkelen.

Bitcoin: a chain of digital signatures



Noen Vurderinger

- En avart av digitale kontanter
  - En uheldig sammenblanding av
    - Store of value (”utvinning av spesielle bitsekvenser”) investeringsspekulasjon
    - Medium of exchange (”hovedbok føres av alle”)
- Greshams lov for konkurrerende penger
  - ”Bad money drives out good”
  - Altså de dårlige pengene blir brukt, de mer verdifulle blir beholdt.
    - Historisk dokumentert tilbake til 405 f.Kr
- Fullstendig uten sentralisering?
  - Ja, ingen clearingsentral eller sentral kontroll av dobbeltbruk.
  - Nei, oppsett, software og protokoller/regler må sentralstyres.
- Inspirerende ide for desentralisert funksjonalitet, mange varianter forslås, også til andre anvendelser…
- Persondata? Ikke strengt anonymt betalingsmiddel.
- Ugjenkallelig transaksjon.
- Ytelse: Tidkrevende betalingstransaksjon i praksis pga. ”Føring av hovedboken”

Utviklingen?

- Hvem får beste plassen?
  - På nettenden (Bank,..)
    i nettet (Telekom,…) eller
    andre…
- Teknologiske utslag
  - Fiklesikring: SIM eller MTM?
  - Kommunikasjon: NFC eller BLE?
  - Tjeneste: App eller SIM Toolkit?
  - …

En kort oppsummering

1. Bitstrenger kan være penger
2. Elektronisk lommebok, en ide fra 1992
3. Mobilpenger, suksess i Afrika
4. Bitcoins dårlig egnet som betaling
5. Åpent problem: Kontant P2P betaling?