Nicolas Frespech, Copyleft: http://artlibre.org/licence/lal/de

Internet der Dinge

Sichere anonyme

Aufwertung und Belastung

elektronischer Geldbörsen

aç

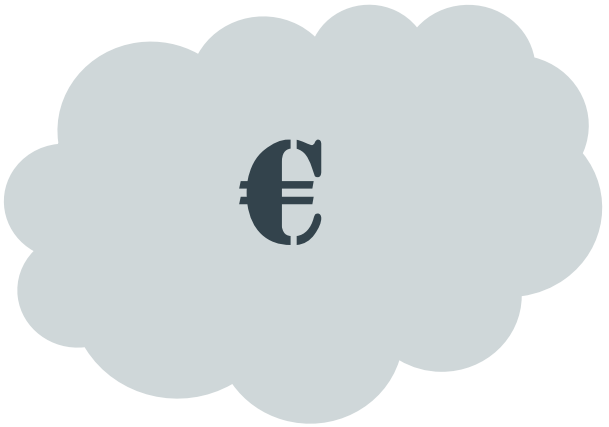
Agenda

1. Bezahlsysteme
2. Technische Herausforderungen
3. Gesellschaftliche Herausforderungen
4. Konzeptstudie
5. Prozessor-Speicherchip
6. Teilguthaben
7. Umsatzkorrektur
8. Transaktionspseudonym
9. Ausblick / Fazit

Bezahlsysteme

Netzgeld

- Debitkarten
- Kreditkarten
- Paypal, Bitcoin, ...



Kartengeld

- Telefonkarten, Paysafecard
- Die Geldkarte, girogo, …
- NFC-Karten
- Secure Element, HCE, ...

Technische Herausforderungen

- Ausfälle, Katastrophen
- Angriffe durch Kriminelle
- lange Betriebsdauer eingebetteter Systeme
- Beweis der Fehlerfreiheit nicht möglich
- Prozessstörungen

  → Zahlung muss korrigierbar sein
  → ungewollte Geldschöpfung verhindern

Gesellschaftliche Herausforderungen

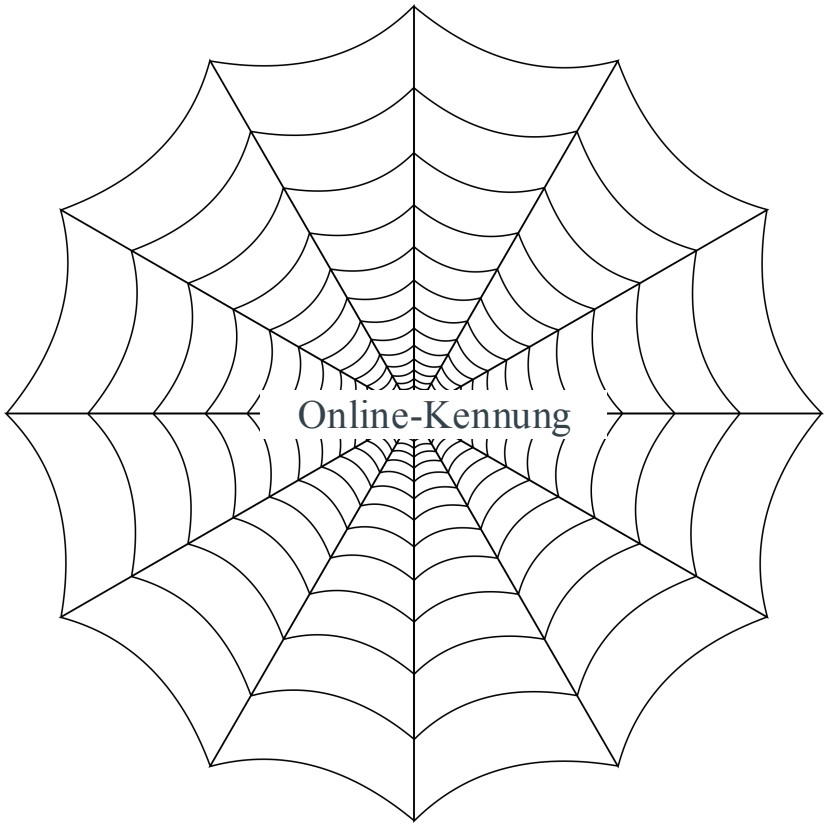
- Vorratsdatenspeicherung

– Datennutzungskontrolle

– Marktverzerrungen

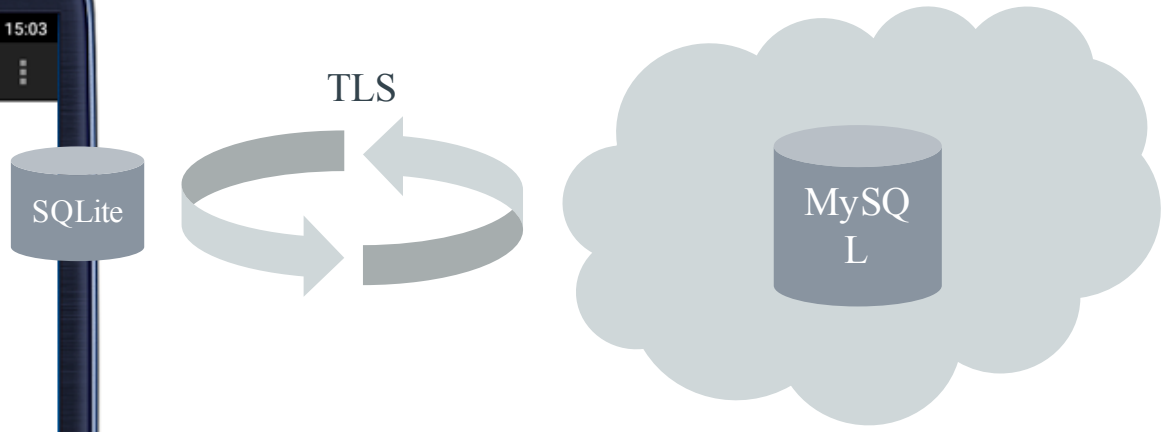
– Massenüberwachung

– Entzug von Zahlungsmitteln



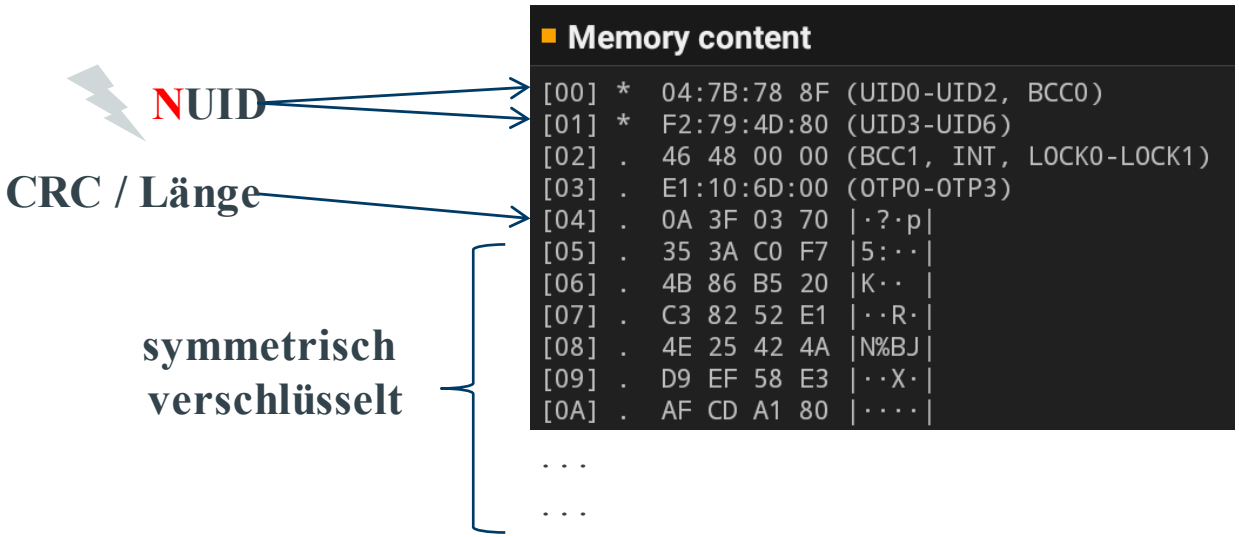
→ Gefährdung von Grundrechten

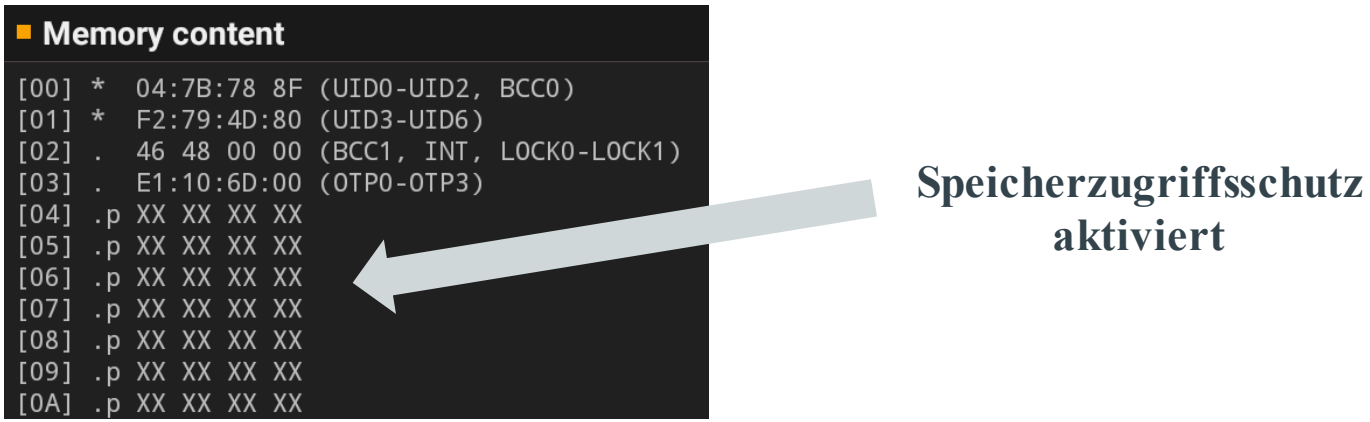
Konzeptstudie



- hybrides System mit replizierter Schattendatenbank
- Prozessor-Speicherchip nach ISO/IEC 14443-A

Prozessor-Speicherchip





Teilguthaben

p_k - 232bit Zufallszahl

Darstellung:
Base64 (hash (f(p_k)))

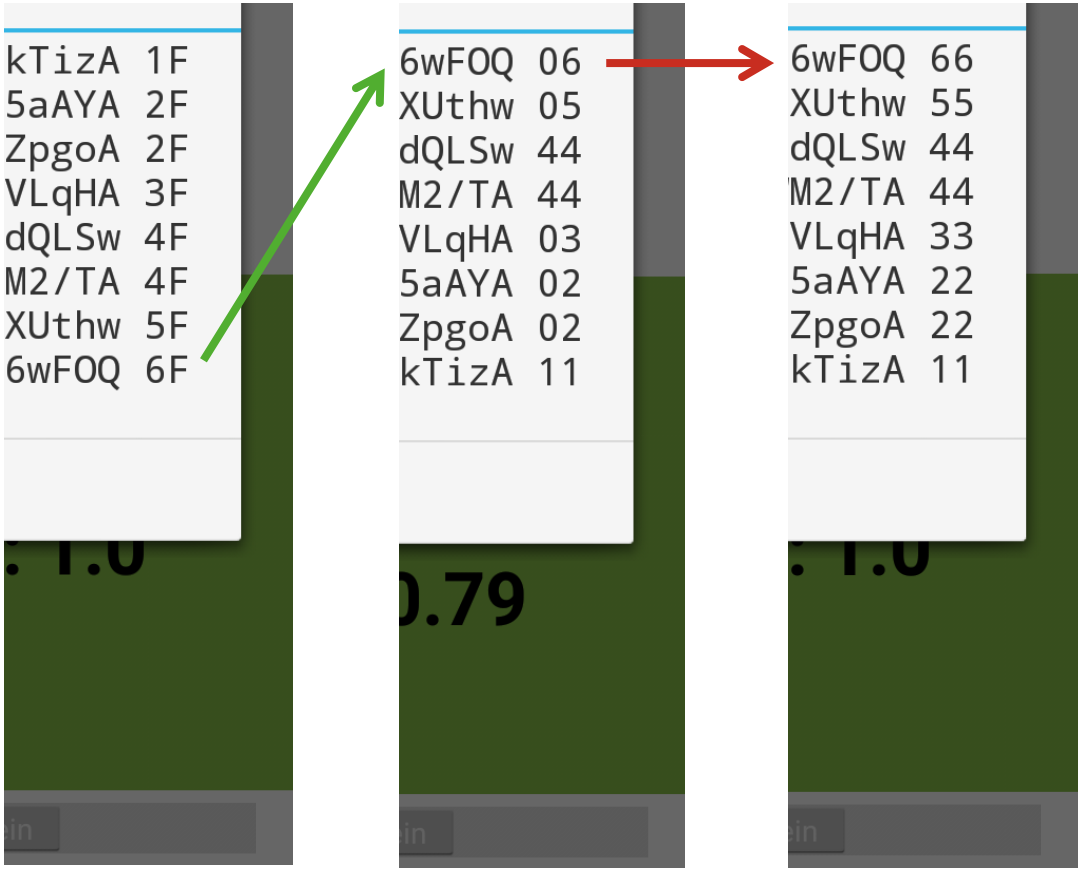
„Seriennummer“

0,01
0,02
0,02
0,05
0,10
0,10
0,20
0,50

→ 1 EUR Guthaben

Jeder auf eine Aufwertung folgender Bezahlvorgang ist passend ausführbar.

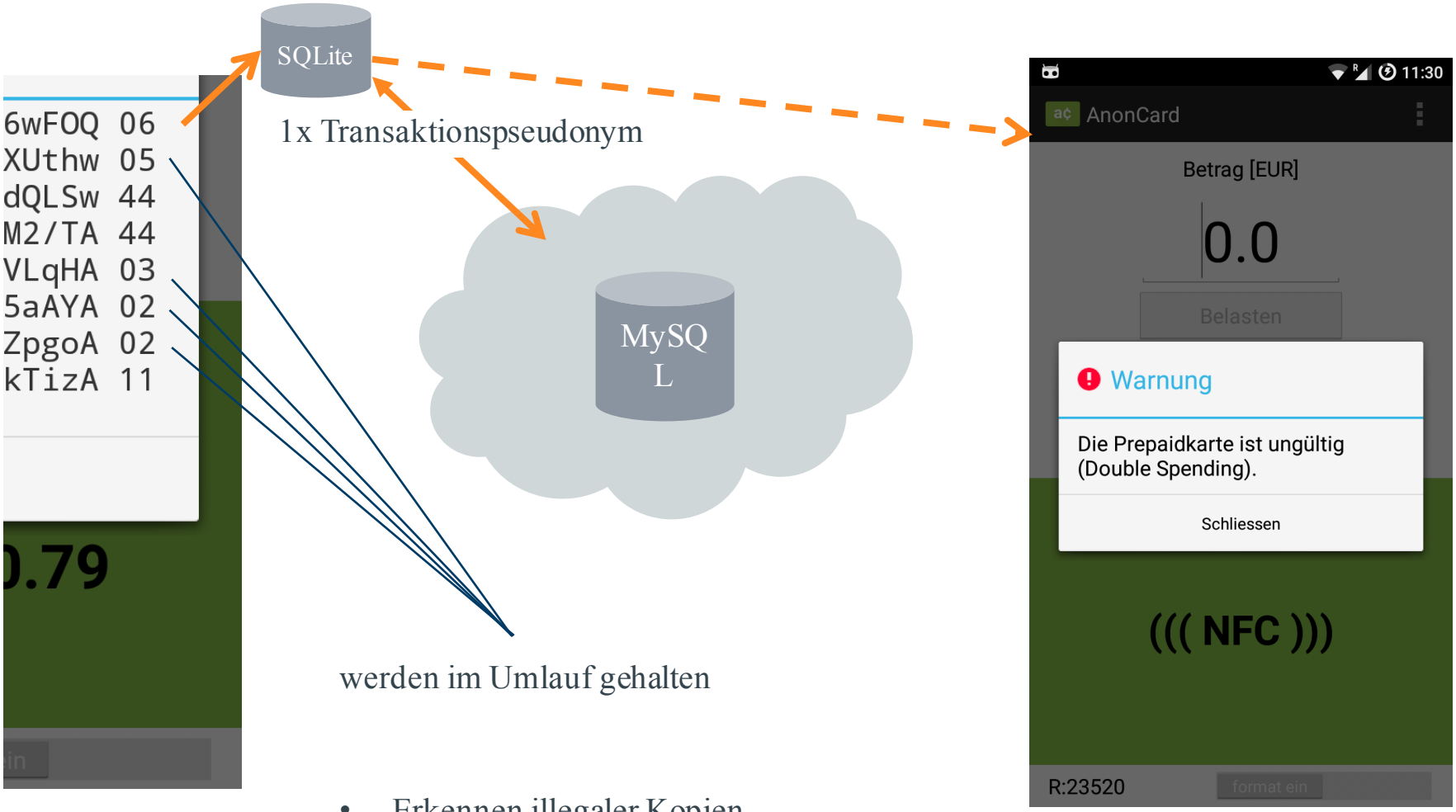
Korrektur



alt = „none“ (0xF) >> 4 neu = alt

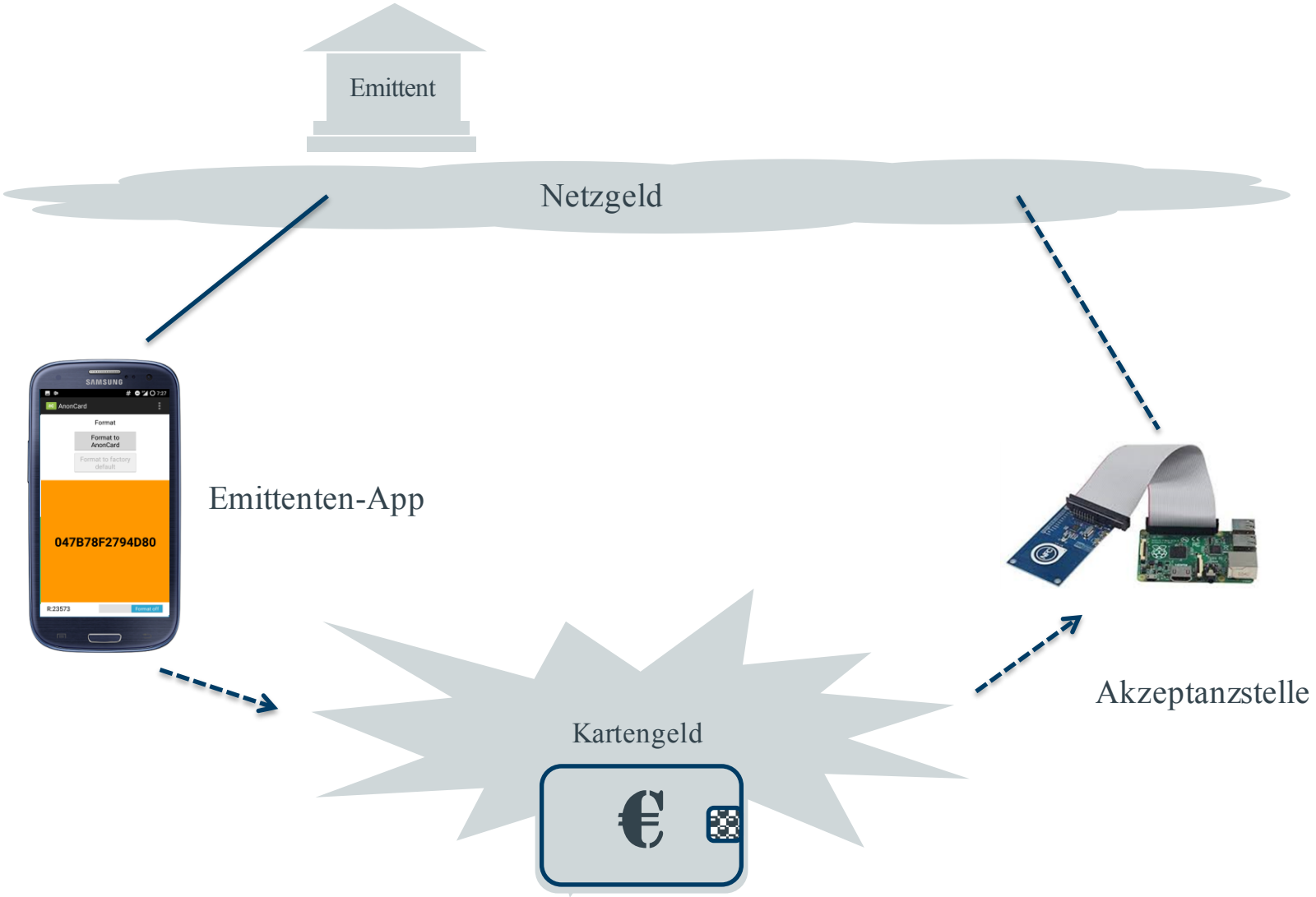
- Bezahlen
- Korrektur
  - neu <= alt
  - neu ϵ {0,nominal}
  - alt ϵ {0,nominal,none}

Transaktionspseudonym



- Erkennen illegaler Kopien
- Nachweis einer Transaktion („Kassenbon“)
- Minimierung des Speicherbedarfs der Schattendatenbank

Ausblick


Emittent
Netzgeld
Emittenten-App
047B78F2794D80
Kartengeld
Akzeptanzstelle

Fazit

- Übertragbarkeit, Abstreitbarkeit
- starke Pseudonyme, Unverkettbarkeit
- lokal autonom im Katastrophenfall
- Double Spending-Schutz
- Korrekturmöglichkeit bei Prozessstörungen
- 1 Mrd. Transaktionen pro Jahr realistisch

Der Schutz persönlicher Freiheiten

im Internet der Dinge ist möglich.

https://play.google.com/store/apps/details?id=eu.anoncard

https://github.com/AnonCard-eu/AnonCard

https://www.anoncard.eu

Vielen Dank für Ihre Aufmerksamkeit.