Technologie und Wissenschaft

fairCASH

Heinz Kreft

25. Januar 2011 bei TELI + PresseClub in München (initial).

Inhalt

1. Einführung
2. Journalistische Relevanz
3. Was ist (fair)Cash
4. Warum gibt es (noch) kein digitales Bargeld
5. Grundlagen von fairCASH
6. Mögliche Konsequenzen einer fairCASH Existenz
7. Zusammenfassung

Einführung

Evolution der Zahlungsinstrumente

Natur Geld
[frühe Vorzeit]

Edelmetall Geld
[650 B.C.]

Papier Geld
[1700 A.D.]

Symbol Geld
[heute]

Digitales Bargeld
[Zukunft]

Permanenter evolutionärer Prozess

fairCASH Alleinstellungsmerkmal: Cash im Internet

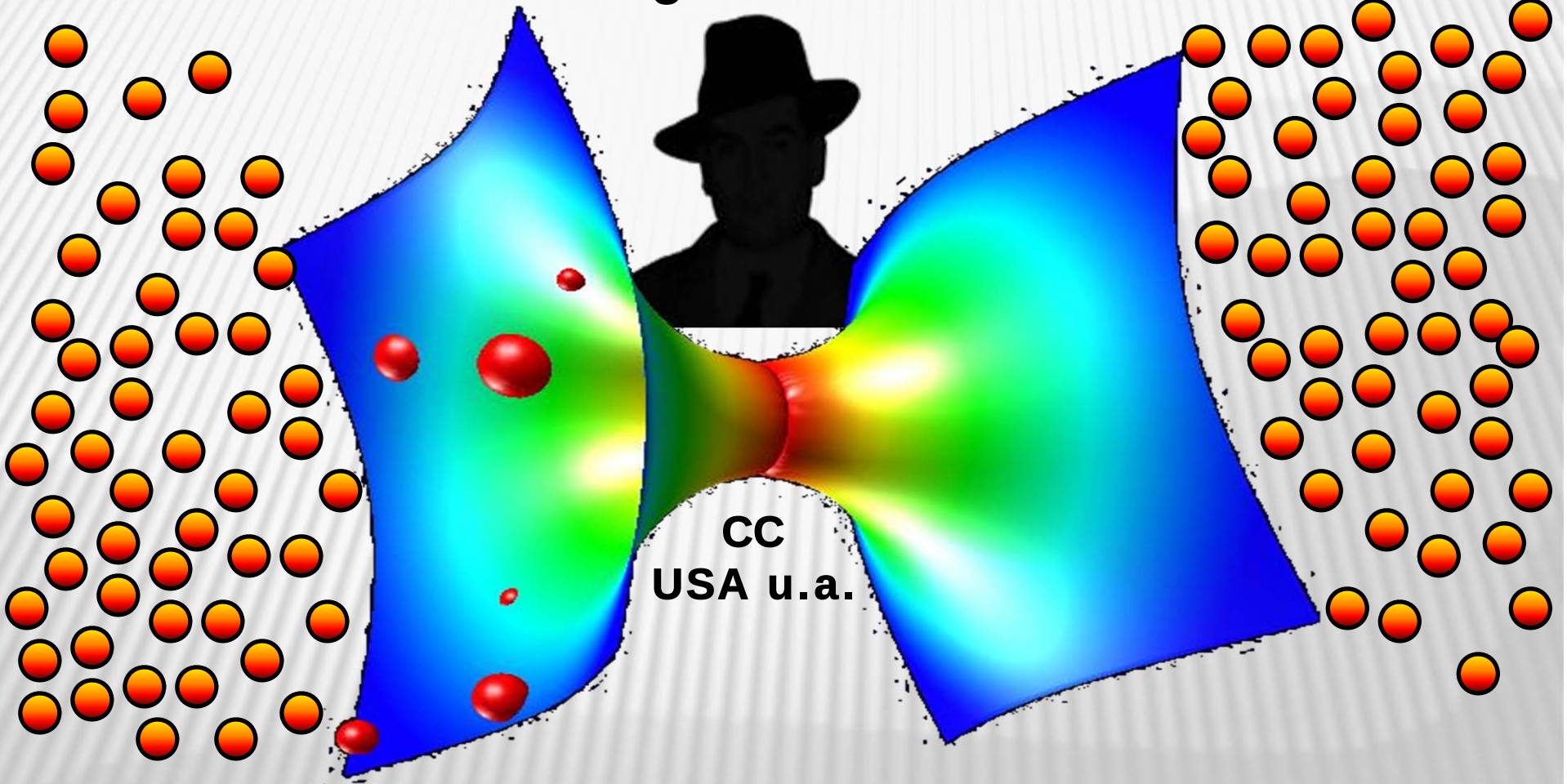
Kontoverfahren als Universalprinzip

- Fiatgeld, Notengeld, Giralgeld (EC-Karte).
- Kreditkarten (VISA-Karte).
- Elektronisches Geld (PayPal).
- Bezahldienste (Paysafecard).

Münzen als Universalprinzip

- Bargeld, Eigentumsübertragung (€uro).
- Zertifikatshandel (CO_2 Verschmutzungsrechte, namenslose Aktienübertragung)
- Multimedia Verteilung & digitale Leihe (übertragbare eBooks).
- Lizenzdistribution (übertragbare Software, z.B. “Apps”).

Kontobasierte Zahlungen: TARGET2* & S.W.I.F.T**



*Trans-European-Automated-Real-time-Gross-Settlement-Express-Transfer.

**Society for Worldwide Interbank Financial Telecommunication.

Haupteigenschaften beider Prinzipien

Konto

- Zentralistische Architektur, kompliziert.
- Nur Online-fähig.
- Immer mit „dritter Partei“ (Intermediate).
- Niemals anonym (im besten Fall pseudonym, z.B. Nummernkonten).
- Internet Tauglichkeit „künstlich konstruiert“, vielfache Medienbrüche.
- Hohe Betriebskosten des Business Models.

eMünzen (fairCASH Technologie)

- Verteilte Architektur, einfach.
- Offline-fähig.
- Immer direkt (Peer-zu-Peer, Person-zu-Person).
- Anonym oder identifiziert (Wahlfreiheit für den privaten Anwender).
- Natives Internet-Verfahren, ohne Medienbrüche.
- Moderate Betriebskosten des Business Modells (keine Transaktionskosten).

Zahlung der Rechnung: Carrier Billing

Nokia: 40% Umsatzabschöpfung.

RIM: 30% Umsatzabschöpfung.

Apple: 30% Umsatzabschöpfung.

Mesopayment: 20% Gebühren*.

Geldsendung: bis zu 20% Gebühren.**

*Quelle: Ernst & Young Unternehmensberatung.

**Quelle: http://remittanceprices.worldbank.org/.

Es wird immer schlimmer mit „Hot Spot“ Zahlungen

Skimming und Phishing

- Betrug durch Kartendiebstahl, Daten-/Bankkontoabgriff oder PIN klauen.
- ALDI informiert Juni 2010 Kunden über manipulierte Bankkartenterminals.
- Gehackte iTunes-Konten für 3,50 € zu verkaufen (Spiegel Online, 06. Januar 2011).

Abkassieren

- Hohe Überziehungszinsen, hohe Transfergebühren, hohe Servicekosten.

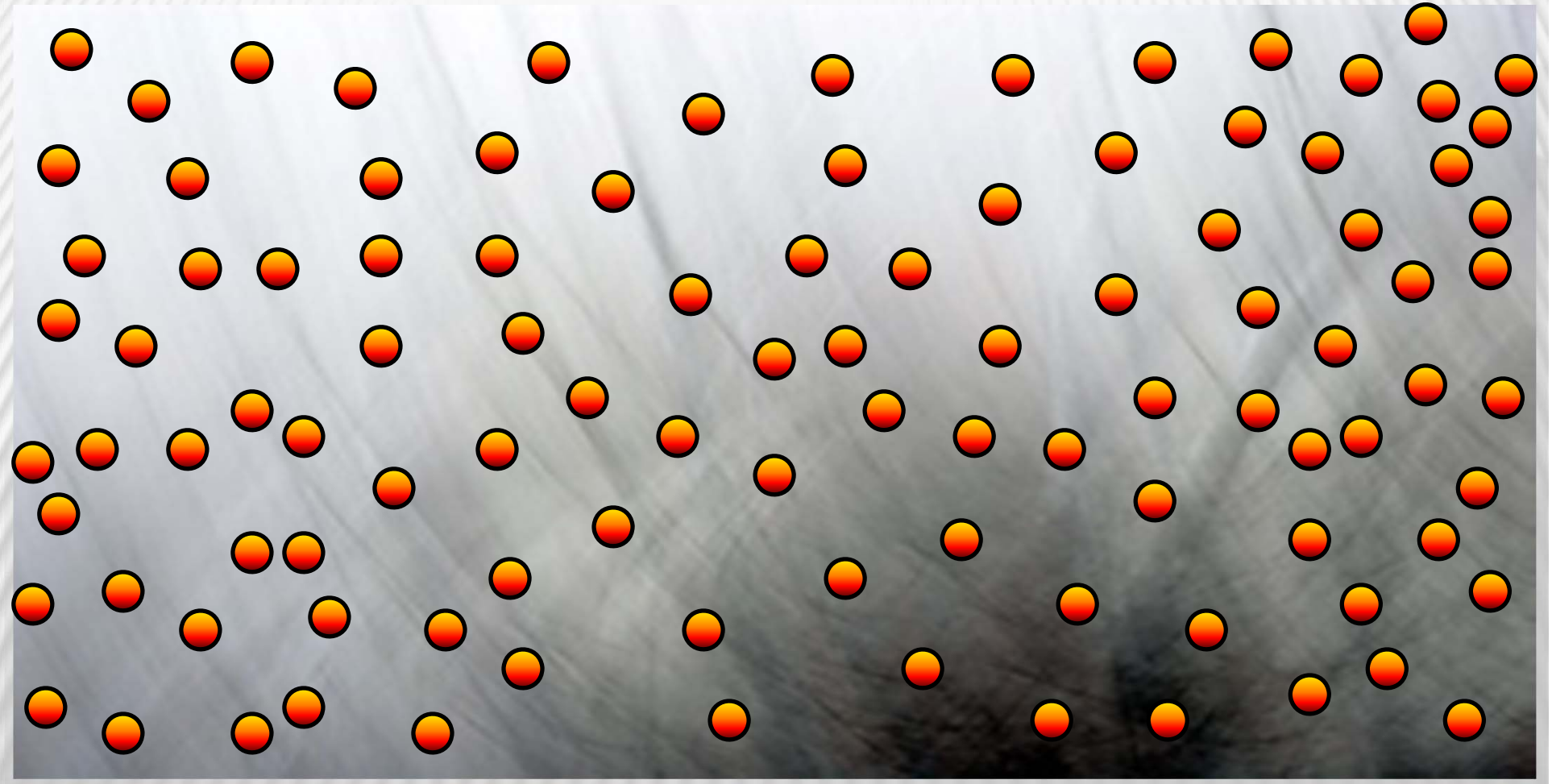
Daten abzapfen

- Easycash greift Kundennutzungsprofile zu Scoring-Zwecken ab und verkauft sie.
- Kreditkartenunternehmen prüfen Einkäufe, um die Kreditwürdigkeit zu ermitteln.
- Kontrolle und Filterung: Glücksspiele, Unterstützung von Freiheitskämpfern u.a..

oder

- Bann nach Belieben: PayPal, Visa, Mastercard & PostFinance (WikiLeaks u.a.).

Digitale bargeld-basierte Zahlungen: P2P*



*offline anonym Peer-zu-Peer / Person-zu-Person.

Ein paar Fakten* über unsere €uro Währung

- **1,6 realisierte Transaktionen pro Tag von jedem Deutschen.**
- **318 transferierte €uro pro Woche von jedem Deutschen.**
- **118 €uro (5 Scheine & 16 Münzen) in jeder deutschen Börse.**
- **85% aller 460 Milliarden p.a. PoS EU Zahlungen sind bar (2009).**
- **Falsch: 5 Scheine & 9 Münzen alle zehntausend Portmonees.**
- **Gefälscht (2010): 751.000 Blüten versus 13,6 Milliarden echter im Umlauf befindlichen Geldscheine.**

*Quelle: H. Kreft, Dissertation, „fairCASH based on Loss resistant Teleportation", Kiel, 2010.

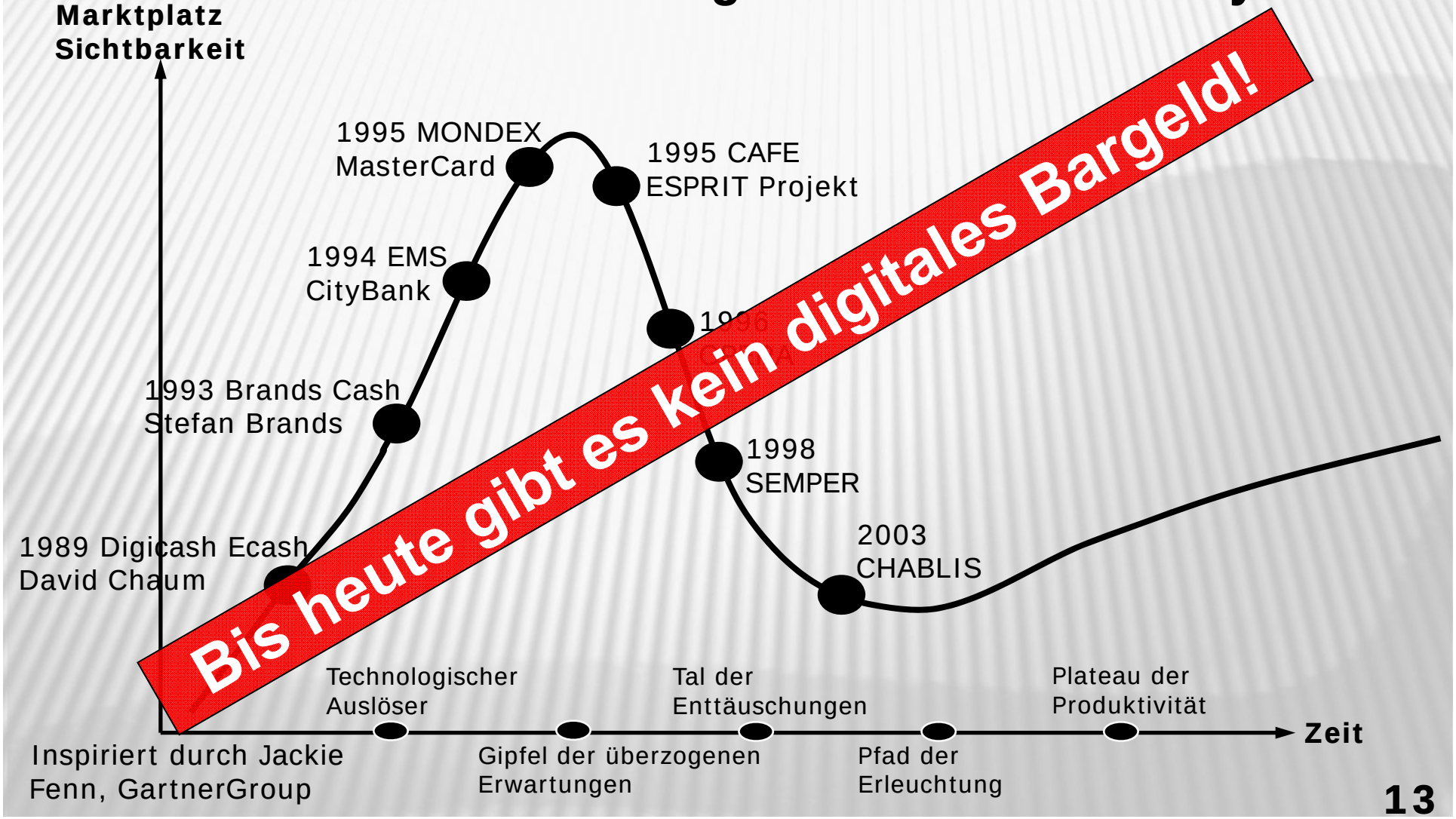
Zeit für Veränderungen

- *Physikalisches Geld hat Nachteile*:
  - Der Umlauf kostet etwa 0.4-0.6% des EU's BIP*, so in etwa €45-70 Milliarden** p.a.
  - Es fehlt ein automatisch erzeugter Beweis für eine vollzogenen Zahlung (Quittung).
  - Physikalisches Bargeld funktioniert nicht im Internet.

*__B__rutto__i__nland__p__rodukt.

**Quelle: Peter Jones, „Europe Set to Lose its War on Cash", PSE Consulting, London, 2008.

Gescheiterte Versuche dig. Cash ähnlicher Systeme



Journalistische Relevanz

Eine Stimme aus der Blogosphäre

„Das Bezahl-”Konzept” des „Abendblattes” ist kein neues Geschäftsmodell. Es ist der verzweifelte Versuch, das alte, für die Verlage komfortable Geschäftsmodell des Abonnements und des Kaufs ganzer Zeitungen, in ein neues Medium zu retten, das die Kunden von den Fesseln solcher Geschäftsmodelle befreit.“*

*Quelle: www.stefan-niggemeier.de/blog/aussichtslos-selbstmoerderisch-unverschaemt/, 2009

Wenig Akzeptanz für bestehende Zahlungssysteme

- Zu teuer.
- Nicht anonym.
- Nicht nutzbar ohne vorherige Registrierung.

Mäßige Akzeptanz für existierende Bezahlsysteme

schlecht

Grafik geschnappt von einem großen Geldtransferunternehmen.

Bezahlinhalte: BDZV-Studie vom 29. April 2010

- Zukünftig: Verleger werden ein Drittel ihrer online Umsätze mit Bezahlinhalten generieren.
- 15% aller Kunden erzeugen 75% aller „Page Impression“ der Webseiten der Verlagshäuser.
- Bezahlinhalte hatten einen schlechten Start aufgrund der verwendeten Bezahlsysteme.

Barrieren für Bezahlinhalte

- **Zwangsregistrierungen bei einer Vielzahl unterschiedlicher Zahlungssysteme (PayPal,Apple,...).**
- **Nutzer wollen keine Subskription, sie bevorzugen Auswahl und Bezahlung *einzelner* Artikel.**
- **Es gibt kein Mesopayment.**

Massenmedien zu Medienmassen

Eines der wesentlichen Merkmale des Medienwandels ist, dass sich Massenmedien nun in Medienmassen verwandeln. Die Angebote werden vielfältiger und zugleich kleinteiliger*.

*Quelle: frei nach dem Verleger Hubert Burda (“lousy pennies“).

Was ist (fair)Cash

eGeld: kein perfekter Ersatz für Bargeld

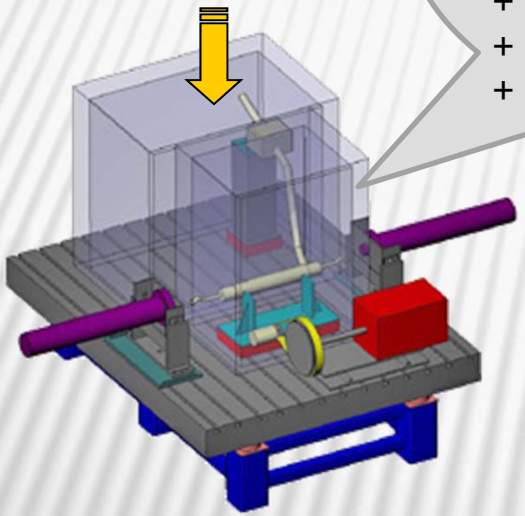
Zahlungs-system

+ Null Transaktionskosten?
+ direkt transferierbar?
+ offline nutzbar?
+ anonym?
+ zahlen und bezahlt werden?
+ Portmonee basiert?
+ finale Zahlungen?

Cash

Entscheidung

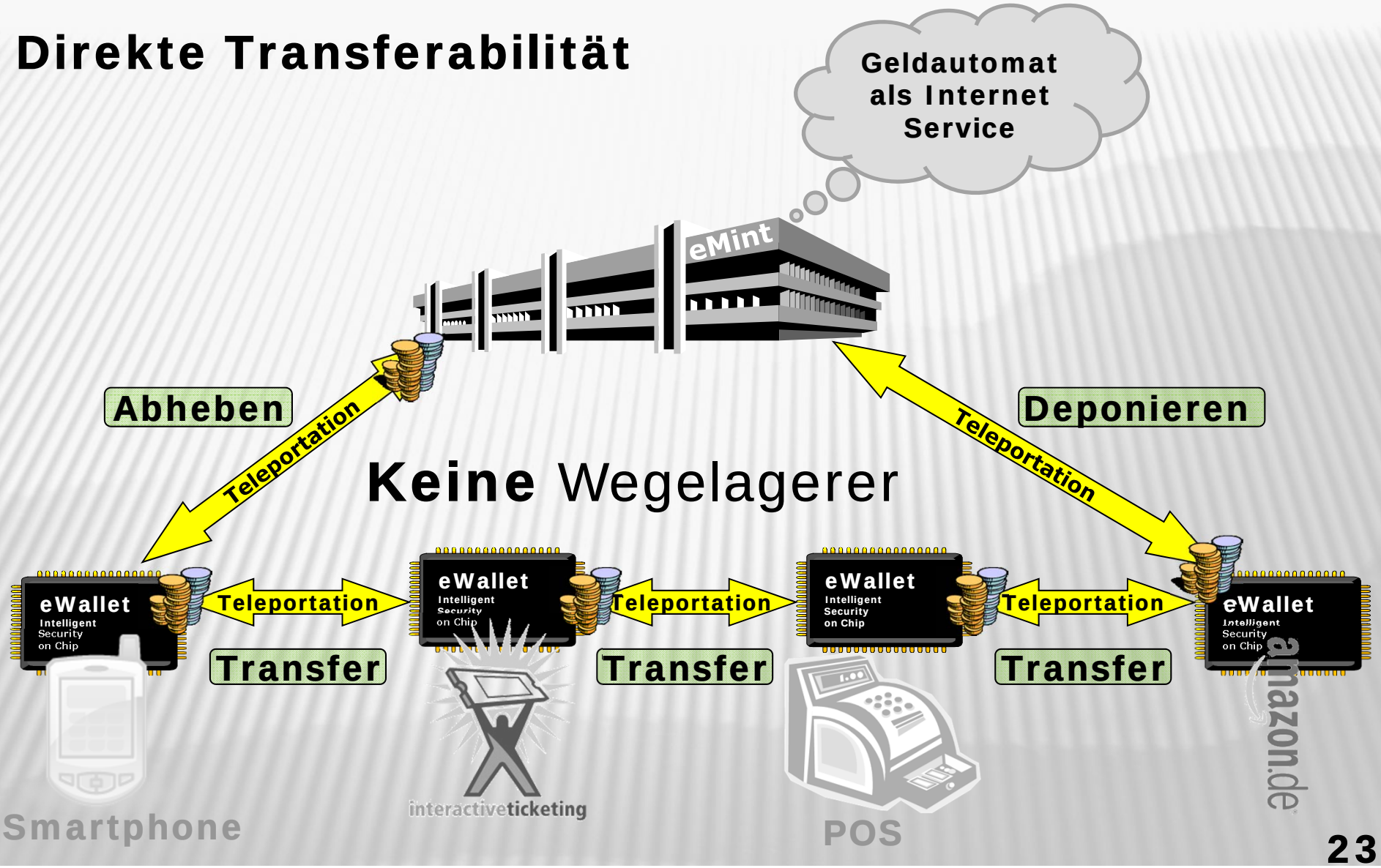
kein Cash



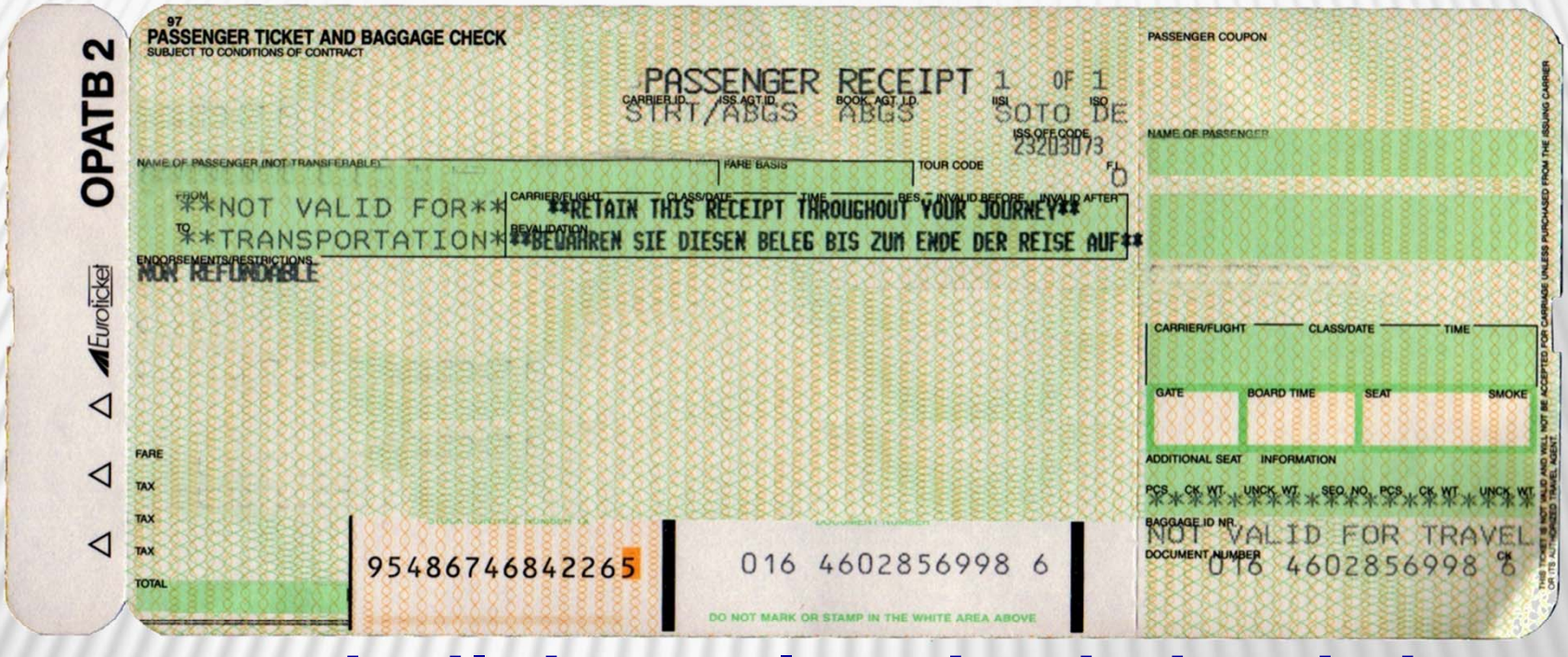
Test Ausrüstung*

*Unsere Testmaschine honoriert keine regulierungs/politischen Eigenschaften wie etwa die finale Vereinbarungsdirektive für Kreditzusagen oder kontobasierte Übertragungen.

Direkte Transferabilität



Ticketing inkludiert



Als Bestandteil der Unleugbarkeit wird u.a. eine Quittung als Beweis erzeugt und übertragen. Diese kann als Ticket verwendet werden.

Warum gibt es (noch) kein digitales Bargeld

Warum es (noch) kein digitales Bargeld gibt

- eMünzen sind – wie andere Dateien auch – unvermeidbar perfekt reproduzierbar (durch Kopieren).
- Unkontrollierbare Reproduktion (Kopierbarkeit), wie auch immer, bedeutet Multispending.
- **Multispending macht dig. Bargeld unmöglich.**

wirklich?

Erfordernisse und Ziele zur Ermöglichung

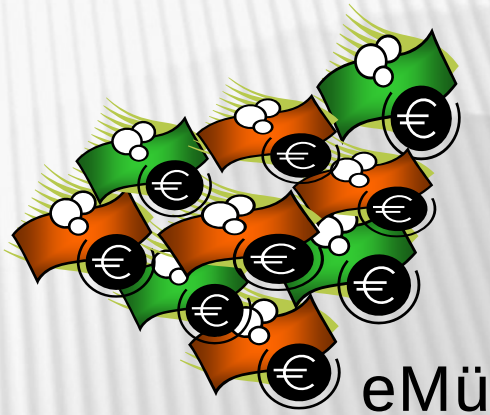
- Weg um transiente eMünzen zu bewegen (Transferierbarkeit).
- Lösung zur Verhinderung von Multispending.
- Garantie, um nur mit legalen Geld arbeiten zu können.
- Mehr als nur manipulationsgeschützte Hardware, um Hacker sicher zu stoppen.

Grundlagen von fairCASH

Elemente von fairCASH unter persönlicher Kontrolle

Physikalisches Bargeld

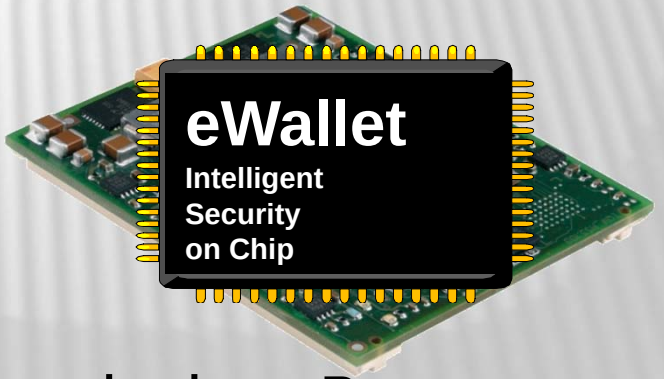
Transformation



eMünzen

Leder Portmonee

Transformation



Elektronisches Portmonee

Protagonisten von fairCASH basiertem Bargeld

eMünzen

eHandy

eBörse

Kontrolle des Kopierprozesses: Nano-Tresore

- Anwendung Hochsicherheitshardware*.
- Anwendung Kryptografie.

Dies wird durch den CASTOR** (**CA**sk for **S**torage and **T**ransport **O**f access **R**estricted secrets) Ansatz in Kombination mit einer PKI*** realisiert.

Regulierung **schwarze Listen**

*Keine absolut abschreckende Barriere, da Sicherheit immer ökonomischen Prinzipien unterliegt.
**Bestandteil der Dissertationsthesis über fairCASH.
***Public-Key-Infrastruktur, ähnlich vergleichbar wie etwa die ePA & eID Architektur.

Das Problem:

- Die Qualität des physikalischen Nachrichtenkanales ist immer unzuverlässig.
- Es wird eine Lösung zur Behandlung möglicher Kanalzusammenbrüche benötigt.

Die Lösung: P2P-Teleportation

- im Erfolgsfall: Beleg, sonst Rückabwicklung.
- P(Erfolgsfall) > 97 % (untere Schranke durch QoS u. Protokoll).

In der Praxis besser als 99,999 % erwartet

Mögliche Konsequenzen der fairCASH Verfügbarkeit

Mögliche Konsequenzen der fairCASH-Verfügbarkeit

- **Etablierung eines Internet Bargeld Standards (wie WEB, SSL/TLS, P2P, FTP).**
- **Verdrängung unbarer Zahlungssysteme (VISA, PayPal, Click & Buy).**
- **Neubewertung von Werbewährungen (Google, sozialen Netzwerken, Online-Spielen).**
- **Begünstigung kleiner Marktplätze (im Gegensatz zu Amazon, eBay, iTunes, App-Store, etc.).**
- **(Re)-Etablierung des Bankgeheimnisses.**

Nicht länger benötigt: separate Zahlungsverfahren

- für multimediale Inhalte.
- für digitale Waren und Dienstleistungen.
- für Gemeinschaftsspiele u. ‘in-Game‘ Zahlungen.
- für soziale Netzwerke.
- für Handy Bezahlverfahren.
- für kreditkarten-substituierte Barzahlungen.

Zusammenfassung: fairCash

Resultat | **Fazit** | **Ausblick**

Einschluss von eMünzen (nano-Tresore) und verlust-resistenter Teleportation ermöglicht digitales Bargeld.

Technologie ist fertig und verfügbar!

Nächster Schritt: Der Prototyp.

Und zum Schluss

Vielen Dank
Für Ihre Aufmerksamkeit

Sie finden eine PDF-Kopie dieser Präsentation auf der Website der TELI Süd unter http://teli.tomsnetworking.de.

fairCASH bewirbt sich im Rahmen des Success-for-Future-Awards in der Kategorie „BT Green Economy Award“: www.sucessforfuture.de

Autor: Dr.-Ing. Heinz Kreft
eMail: heinz.kreft@faircash.org