

Technologie, Wirtschaft und Politik

# **Geld aus dem Rechner: Digitale Bezahlssysteme**



**Dr.-Ing. Heinz Kreft, fairCASH Place**

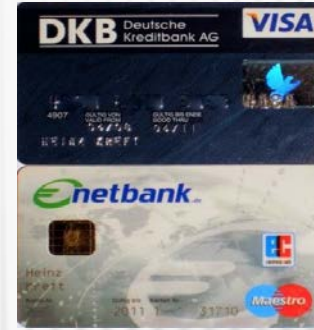
**Präsentation anlässlich der Medientage NORD am 17.11.2011 in Kiel**

1. Einführung
2. Grundformen von Geld
3. Konkretisierung „virtuelle Währung“
4. Spotlight: BitCoin
5. Digitale Bargeld-Technologie: fairCASH
6. fairCASH aus regulatorischer Sicht
7. Das technische fairCASH Fundament
8. Zusammenfassung

# Evolution der Zahlungsinstrumente



**Digitales-Bargeld  
[Zukunft]**



**Symbol-Geld  
[heute]**



**Papier-Geld  
[1700 n.Chr.]**



**Edelmetall-Geld  
[650 v.Chr.]**







**Naturalien-Geld  
[frühe Vorzeit]**

**permanenter, evolutionärer Prozess**

# **Grundformen von Geld**

# Cash vs. Konto

## Münzen als Universalprinzip

-  Bargeld, Eigentumsübertragung (€uro).
-  Zertifikathandel (CO<sub>2</sub>-Verschmutzungsrechte, namenslose Aktien).
-  Multimedia-Verteilung & digitale Leihe (z.B. übertragbare eBooks).
-  Lizenz-Distribution (übertragbare Software, z.B. „Apps“).

## Kontoverfahren als Universalprinzip

-  Fiat-Geld\*, Noten-Geld, Giral-Geld (z.B. EC-Karte).
-  Kreditkarten (z.B. VISA-Karte).
-  Elektronisches Geld (z.B. PayPal).
-  Bezahldienste (z.B. Paysafecard).

\* [econ.] Geld als Verrechnungszählgröße, z.B. in Form eines Kontostands

# Haupt-Eigenschaften von Konto- und Cash-Prinzip



## Konto (Unbar-Technologie)



**Zentralistische Architektur, komplex, Bank-orientiert.**



**Wenn digital, dann ausschließlich online-fähig.**



**Immer mit „dritter Partei“ (Intermediäre).**



**Niemals anonym (bestenfalls pseudonym, z.B. Nummern-Konten).**



**Internet-Tauglichkeit „künstlich nach-konstruiert“, vielfache Medienbrüche.**



**Hohe Betriebskosten der Business-Modelle (lange Wertschöpfungskette).**



## eCoins (Bar-Technologie)



**Verteilte Architektur, Deployment und Handhabung einfach, Internet-orientiert.**



**Offline- (und online-) fähig.**



**Immer direkt (Peer-zu-Peer, Person-zu-Person).**



**Anonym oder identifiziert (wahlfrei für den privaten Anwender).**



**Natives Internet-Verfahren, keine Medienbrüche.**






**Moderate Betriebskosten des Business-Modells (keine Transaktionskosten).**

# Risiken von Kontosystemen



## Skimming und Phishing

-  Betrug durch Kartendiebstahl, Daten-/Bankkonto-Abgriff oder PIN-Diebstahl.
-  ALDI informierte Juni 2010 Kunden über manipulierte Bankkarten-Terminals.
-  Gehackte iTunes-Konten für 3,50 € zu verkaufen (Spiegel Online, 6. Januar 2011).






## "Fette" Kosten

-  Hohe Überziehungs-Zinsen, hohe Transfer-Gebühren, hohe Service-Kosten.



## Transaktions-Daten-Verwertung

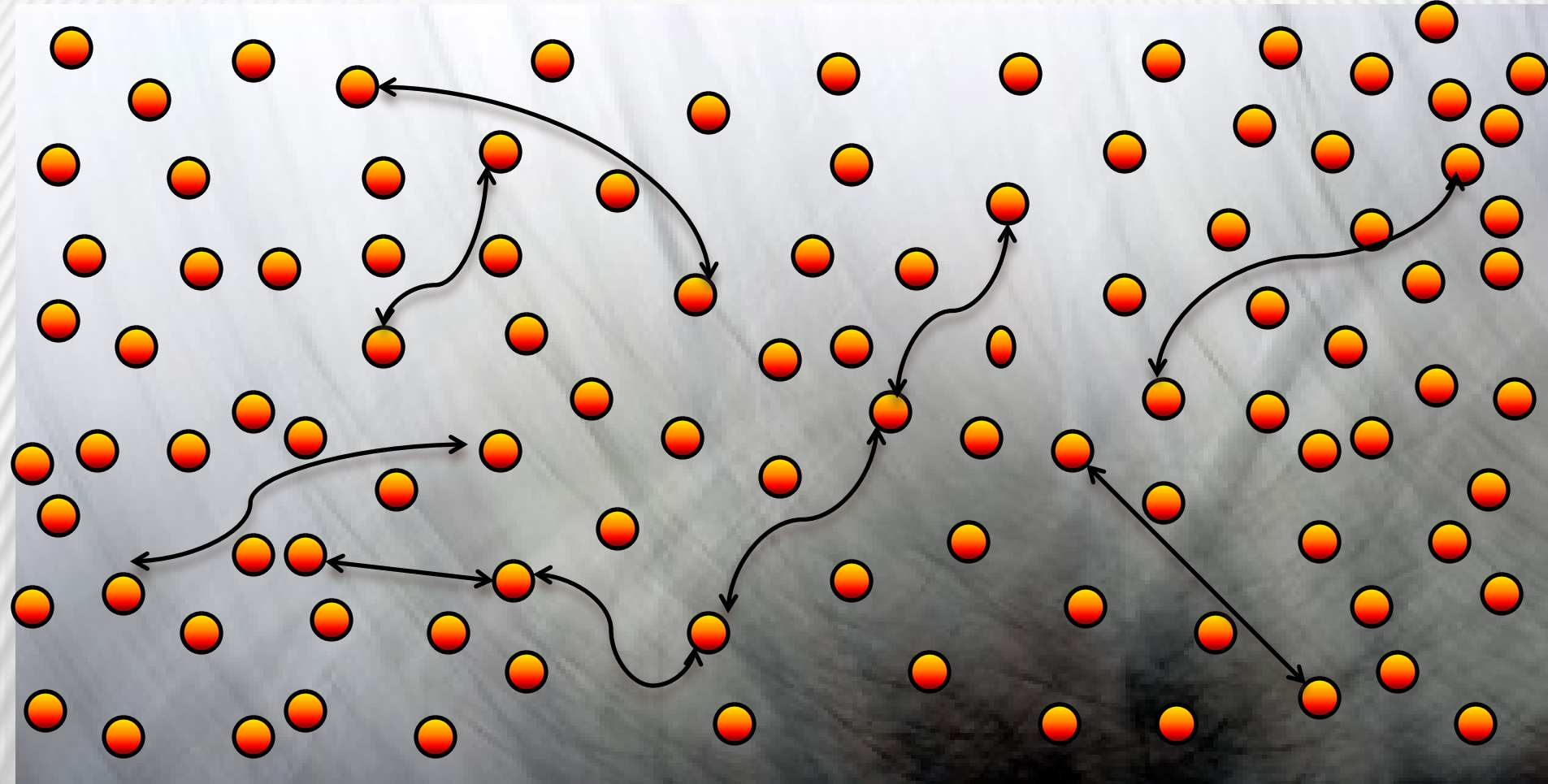
-  Easycash greift Kundennutzungs-Profile zu Scoring-Zwecken ab und verkauft sie.
-  Kreditkarten-Unternehmen prüfen Einkäufe, um die Kreditwürdigkeit zu ermitteln.
-  Kontrolle und Filterung: Glücksspiele, Unterstützung von Freiheitskämpfern u.a.



## oder Betreiber-Willkür

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

# Bargeld-Zahlungen: P2P\*, daher leicht skalierbar



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

# Einige Fakten\* über Euro-Bargeld

- **Ø 1,6 realisierte Transaktionen pro Tag von jedem Deutschen.**
- **Ø 318 transferierte Euro pro Woche von jedem Deutschen.**
- **Ø 118 Euro (5 Scheine, 16 Münzen) in jeder dt. Geldbörse.**
- **85% aller 460 Milliarden PoS-EU-Zahlungen 2009 erfolgten bar.**
- **Bargeld ist sehr sicher!  
13,6 Milliarden echten Geldscheinen im Umlauf stehen ganze  
751.000 Blüten gegenüber\*\*.**




\* Quelle: Heinz Kreft, Dissertation: „fairCASH based on Loss resistant Teleportation“, Kiel, 2010.


\*\* Das entspricht einer Quote von lediglich 0,06‰





# **Was ist eine Währung?**

# Eine Wahrung

 **ist das Geldwesen eines politischen Ordnungskonstrukts**

-  in einer geografischen Gebietshoheit (Wahrungsraum),
-  in einer abgegrenzten Community (Volkswirtschaft),
-  in einem staatlichen Machtsystem (Zentralbankensystem).

 **unterliegt wesentlichen Fragestellungen wie etwa**

-  Vertrauen in die politische und wirtschaftliche Stabilitat (Konjunktur\*),
-  Grad der Konvertibilitat\*\* / Konvertierbarkeit (Einschrankungen, ...),
-  Ausdehnung des Einflussbereiches (regionales Tauschmittel oder Leitwahrung),
-  Grundlagenbezug zur Geldordnung eines Landes oder Wirtschaftsraumes.

\*lat. coniunctura „Verbindung“

\*\*lat. convertere „umwandeln“

# Gestaltungsformen von Währungen

Wir folgen hier der u.a. im Gabler Wirtschaftslexikon\* referenzierten internationalen Definition:



## Gebundene Währungen:

Beispiel: Metallische Währungssysteme auf Basis von Gold oder Silber.



## Freie (manipulierte) Währungen:

Diese versuchen die wirtschaftliche Bedeutung der Recheneinheit durch Knapphaltung oder Flutung des Zahlungsmittel-Umlaufs zu bestimmen. Beispiel: Währungen wie das Euro-System mit zentral gelenkter Kredit-Schöpfung, die den Zahlungsmittel-Bedarf und Umlauf an die „wirtschaftlichen Notwendigkeiten“ anpasst.



## Internationales Währungssystem:

Fiktion! Hat es nie gegeben. Vor dem ersten Weltkrieg gab es den internationalen Gold-Standard, danach folgte kurzzeitig das System der Gold-Devisenwährung, und nach dem zweiten Weltkrieg legte das Bretton-Woods-Abkommen (im Wesentlichen ein Primat fester Wechselkurse) den US-Dollar als Leitwährung fest. Seit 1973 nur noch freie Wechselkurse für Fiat-Geld.

\*<http://wirtschaftslexikon.gabler.de/Archiv/6603/waehrungssystem-v8.html>

# **Was bedeutet virtuell?**

# Virtuell\* bezeichnet ein

- + Synonym mit „in der Wirkung oder dem Anschein nach“ vorhanden / wirken. Umgangssprachlich teilweise in Verbindung mit „fiktiv“ verwendet.
- + Beispiel aus der Optik: Die Spiegelung ist virtuelles Abbild des realen Objekts.
- + Gegenteil von „vollständig physisch real“.
- + Es gibt keine vollständige Übereinstimmung zwischen einer virtuellen und einer realen Entität; die virtuelle Entität deckt zumeist nur einen Bruchteil aller Eigenschaften der realen Entität ab.

**Was ist folglich eine  
virtuelle Wahrung?**

# Die Sprachkonstruktion „virtuelle Währung“ ist

**eine Chimäre, also ein Trugbild, eine Einbildung, Täuschung – mit anderen Worten: Blödsinn!**

Begründung: Das Konstrukt einer Währung hat nichts mit der Ausgestaltung der Access-Instrumente zu tun, also der Art und Weise, etwa wie Werte bei Transaktionen übertragen werden.

Dies geschieht in Konto- oder Bargeld-basierten technischen Ausgestaltungen. So ist es beispielsweise der Euro-Währung egal, ob sie in Form einer giraler Rechengröße als Kontobewegung oder als Papierschein den Besitzer wechselt.

Da letztlich die Aussage einer Währung – im Wesentlichen das Einlöse-Versprechen – auf wirtschaftspolitischen, immateriellen Faktoren basiert, ist das semantische Konstrukt „virtuelle Währung“ bestenfalls eine sprachliche Entgleisung.

# Vorschlag Neusortierung „virtuelle Währung“

- Seit Urzeiten existieren regionale Tauschmittel.
- Heutzutage sind das sogenannte Komplementär-Währungen, genannt:
  - „Local Exchange Trading Systems“ (LETS) oder
  - „Global Exchange Trading Systems“ (GETS).
- Sie genügen der Definition „Ersatz-Währung“.

**„Virtuelle Währungen“ weisen einige Eigenschaften dieser Barter-Ringe\* auf, weshalb sie eher diesem Währungs-Typus zugeordnet werden können.**

\*englisch barter „(Natural-) Tausch, (Waren-) Austausch“









# Faktische Erkenntnisse

- **Web.Cent, Linden-Dollar, Facebook-Credit, BitCoin et al. sind technische LETS-/GETS-Ausprägungen von Kunstwährungen.**
- **Viele von ihnen oktroyieren ein absolutistisches Plattform-Modell, dessen Betreiber die Spielregeln exklusiv regelt – etwa den Zwang zur ausschließlichen Nutzung oder die beliebige Verfügungsgewalt über die „Transferregeln“ zu Geldwährungen (die Bestimmungshoheit bei den Wechselkursen\*).**

\*über diesen Mechanismus erfolgt die Umsatzabschöpfung, i.d.R. 30% oder mehr.

# BitCoin

# Ein paar technische Fakten über Bitcoin

-  Sui generi\* einer pseudonymen, digitale P2P-Online-Kunstwährung der Bitcoin-(Glaubens-) Gemeinschaft.
-  Open-Source-Software-Projekt, 2008 initiiert von Satoshi Nakamoto.
-  Die Geldschöpfung ist ein Belohnungsprozess für die Teilnahme am Quorum-Consensus-Verfahren (Vertrauen auf Schwarm-Intelligenz).
-  Werte werden mit Hilfe eines speziellen Service über das Netzwerk zwischen zwei als Software-App realisierten eWallets transferiert. Eine Transaktion wird frühestens nach 60 Minuten final (am PoS untragbar!).
-  Konto-basiertes (!) Zahlungs-System mit Überweisungen, selbst wenn die Wortwahl „**Bitcoin**“ ein Münz-Verfahren suggeriert.
-  Bitcoin-Konto-Bewegungen sind öffentlich (lokal replizierte Log-Datei) und bilden ein von jedermann einsehbares Bewegungsprofil (keine Anonymität).
-  Die Bitcoin-Menge ist abgeschlossen (21 Mio.); Bitcoins sind teilbar.
-  Kein System-immanenter Zahlungs-Beleg (Vertragssicherheit und Beweisbarkeit nicht integriert).

\*lat. „eigener Art“

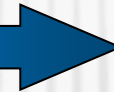
# **Digitales Bargeld**

# fairCASH-Elemente unter individueller Kontrolle

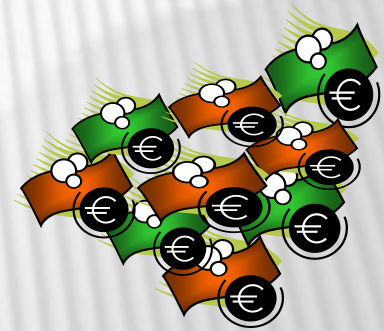
physikalisches Bargeld



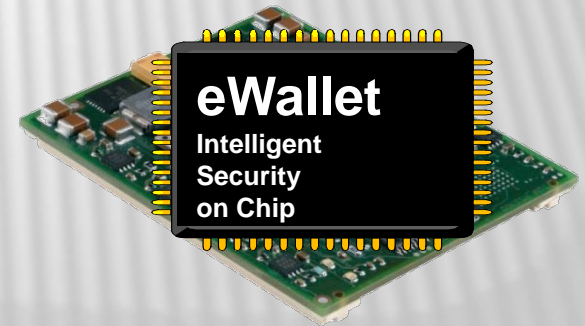
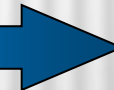
Transformation



eCoins



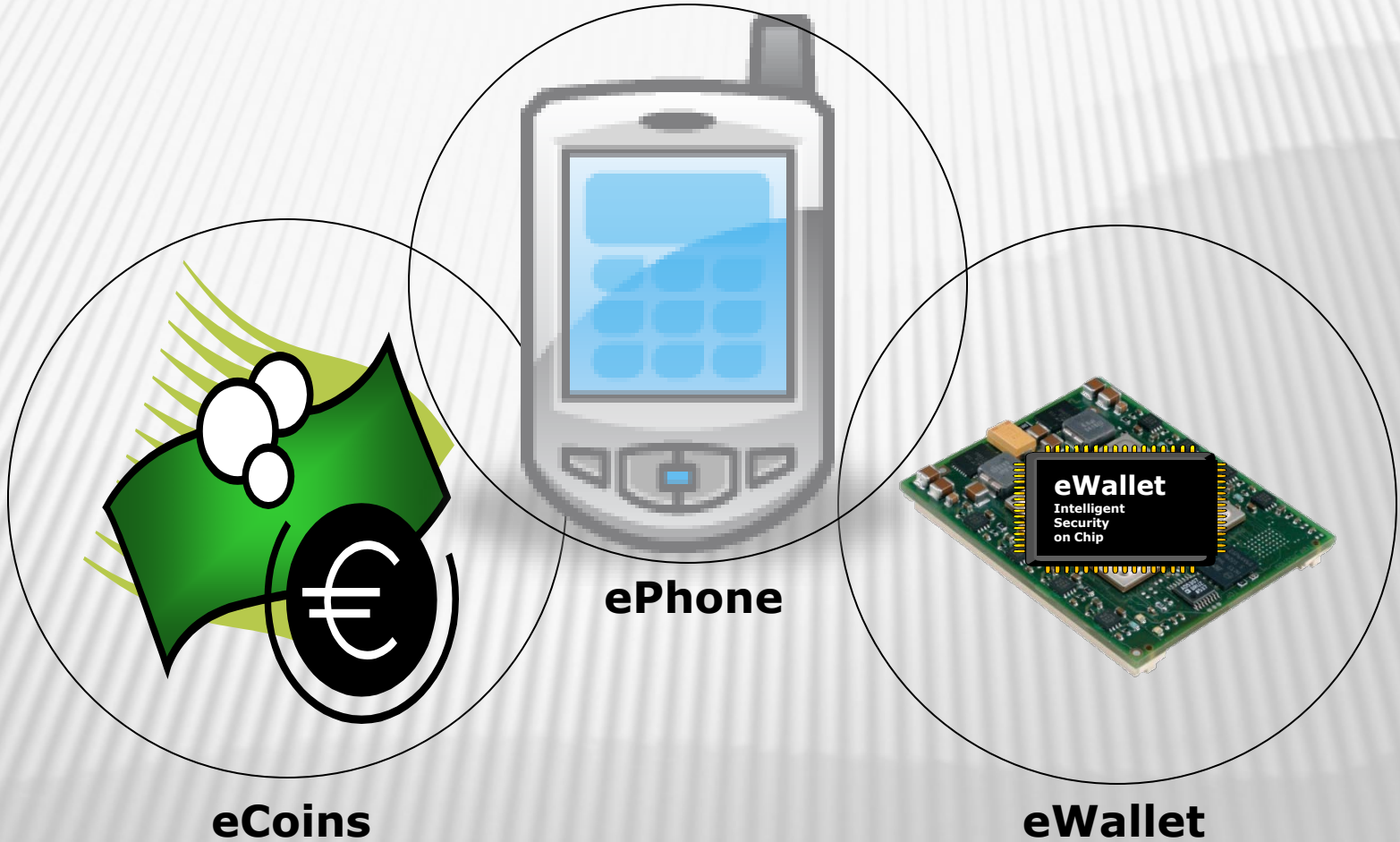
Transformation



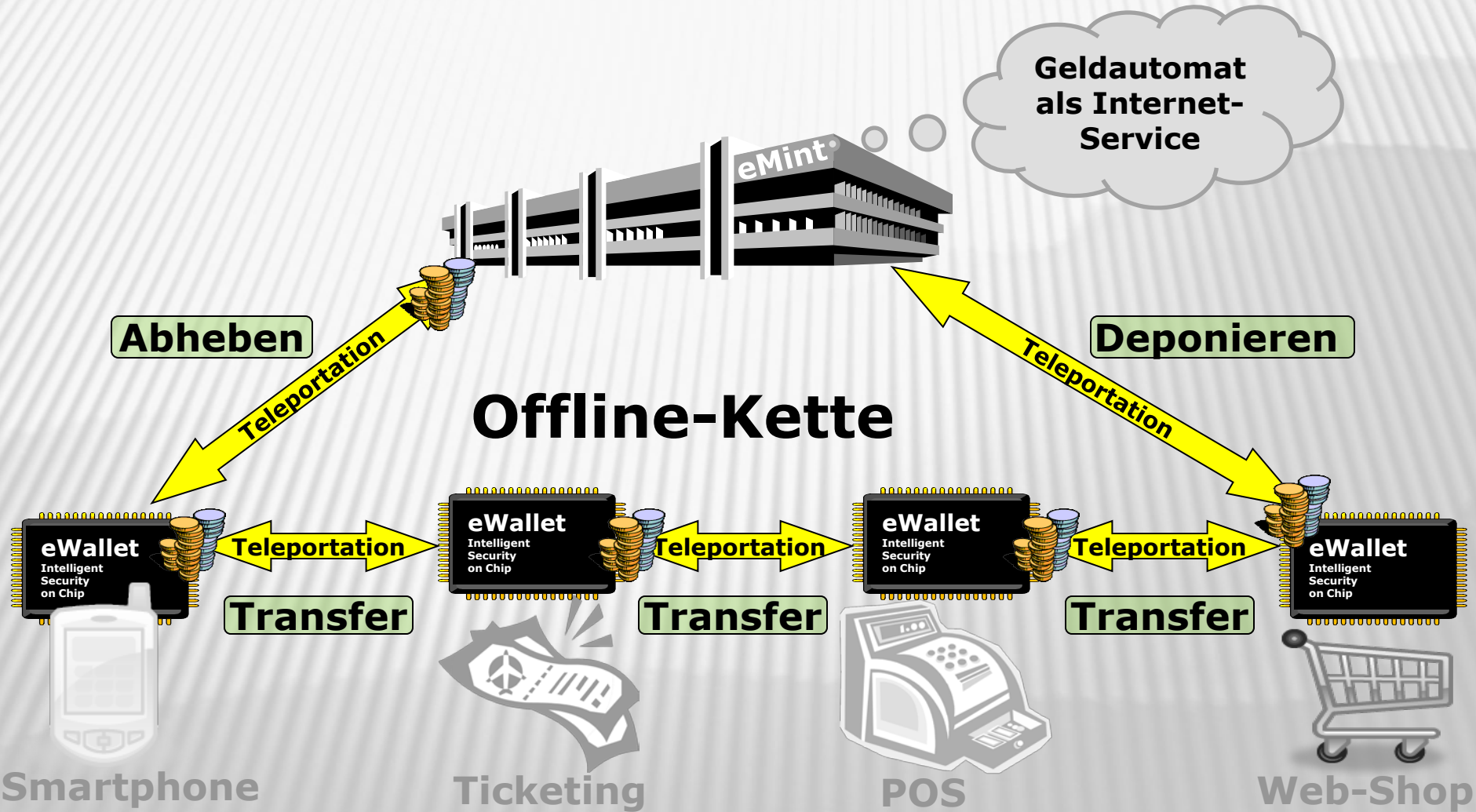
Leder-Portemonnaie

eWallet

# Protagonisten fairCASH-basierten Bargelds



# Direkte Transferabilität

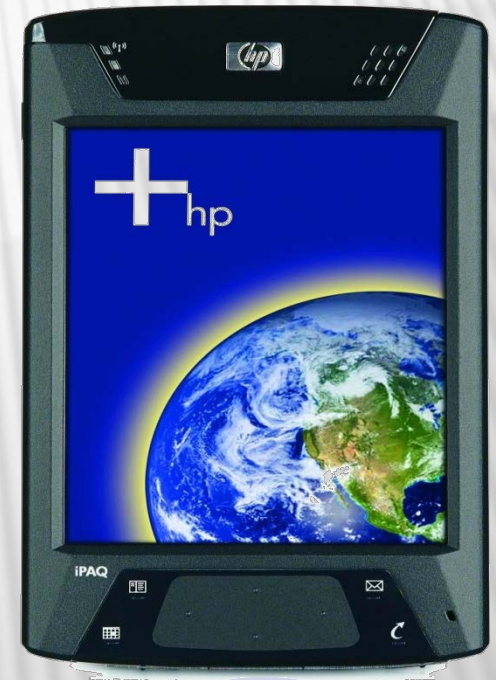


# Ablauf einer fairCASH-Transaktion

Zahler



Bezahler



- 1 – Pairing\*
- 2 – VPN-/VPC-Aufbau\*\*
- 3 – Verhandlung/Rechnung
- 4 – Werte-Transfer
- 5 – Bestätigung/Quittung



\*beinhaltet ein Digital-Zertifikat auf Basis von ITU-T X.509v3

\*\* **V**irtual **P**ivate **C**hannel



# **Warum digitales Bargeld (unverzichtbar ist)**

# **Intention für digitales Bargeld**

- Das Bezahlen zum zeitgemäßen Ereignis machen,**
- Bargeld 2.0 einen klaren Sinn und Zweck geben,**
- Einfach „zahlen“: leicht, intuitiv und effizient.**

# Schlüssel-Argumente pro fairCASH



**Zahlungs-Systeme sind im Internet-Zeitalter die Schlüssel zu Inhalten, Diensten und Waren. Dabei kann fairCASH die Rolle eines Passepartouts spielen.**



**Eröffnung neuer „Spielräume“ wie die Aufhebung des Zwangs zu physischer Nähe bei Barzahlungen, die Nutzung von ISPs als „Bit-Pipes“ und die drastische Verkürzung der Wertschöpfungskette.**



**Risiko-Minimierung der „Vor-Ort“-Bargeld-Haltung (Internet-Transfer zwischen PoS / Konto).**



**Kostenfreie Nutzung für Endkunden.**

# fairCASH-Alleinstellungs-Merkmale (USPs)

- 1 Digital, wodurch Bargeld endlich im Internet nutzbar wird.**
- 2 Bezahlen ohne Anmeldung an fairCASH-Akzeptanz-Stellen.**
- 3 Bedingungslos anonymes Bezahlen.**
- 4 Selbst bei gestörter/schwacher Infrastruktur funktionsfähig.**
- 5 Rechtssicherheit: automatische Quittung als Nachweis.**
- 6 Verlustschutz: Kompensation via eindeutige Seriennummer.**

# **Regulatorische Sicht auf fairCASH**

# „Zwei-Welten“-Modell von fairCASH

- Bankensystem
- S.W.I.F.T / TARGET2
- Online
- Konto-Transaktionen
- In der EU stark reguliert

Zweite E-Geld-Richtlinie 2009/110/EG

ID-Monitoring und -Logging §3 Abs.2 Satz 3 neu GwG

eCoins erzeugen  
eCoins herausgeben

1

eCoins vernichten  
eCoins zurücknehmen

4

§1a Abs.2 ZAG

eCoins empfangen  
eCoins weitergeben

2

§1 Abs.10 Nr. 1 ZAG

... ... ...

eCoins einlösen  
eCoins empfangen

3

„Zahlungsvorgänge, die ohne zwischengeschaltete Stellen ausschließlich als unmittelbare Bargeldzahlung vom Zahler an den Zahlungsempfänger erfolgen“ **sind keine Zahlungsdienste!**

- Informationssystem
- P2P-Teleportation
- Offline
- Bar-Transaktionen
- Regulatorisch fragmentiert

Finanz-  
Welt

Giral-  
Umlauf

Bar-  
Umlauf

Internet-  
Welt

System  
Schnitt-  
stelle

Deanonymisierung

Deanonymisierung

**Warum es bislang kein  
digitales Bargeld gibt**

# Warum es (noch) kein digitales Bargeld gibt

- eMünzen sind – wie andere Dateien – unvermeidlich (durch Kopieren) perfekt reproduzierbar.
- Unkontrollierbare Reproduktion (Kopierbarkeit), wie auch immer realisiert, bedeutet jedoch Multispending.
- Multispending macht digitales Bargeld unmöglich.

**Wirklich?**

# **Grundlagen von fairCASH:**

- **technisch,**
- **wissenschaftlich und**
- **kryptographisch**

# Unterbindung des Kopier-Prozesses durch Teleportation der eCoins in Nano-Tresore

- Einsatz von Hochsicherheits-Hardware\*.
- Einsatz von Kryptografie.

Realisierung durch so genannten CASTOR\*\*  
(**CA**sk for **S**torage and **T**ransport **O**f access **R**estricted secrets)  
in Kombination mit einer PKI\*\*\*.

**Hochflexibler  
„Moderator“**

**schwarze Listen**



\* Keine absolut abschreckende Barriere, da Sicherheit immer ökonomischen Prinzipien unterliegt.

\*\* Bestandteil der Dissertation über fairCASH.

\*\*\* **P**ublic-**K**ey-**I**nfrastruktur, ähnlich vergleichbar wie etwa die ePA & eID Architektur.

# Haupt-Problem digitalen Bargelds: das sichere Bewegen von eCoins\*:



**Die Qualität des physikalischen Nachrichtenkanales ist immer unzuverlässig.**



**Es bedarf einer Lösung zur Behandlung möglicher Zusammenbrüche des Übertragungs-Kanals während eines eCoin-Transfers.**

# Technologische Lösung der Herausforderung

## P2P-Teleportation statt Kopie

**in der Praxis  
besser als  
99,999%  
erwartet**

 Im Erfolgsfall automatisch generierter Beleg,  
andernfalls automatische Rückabwicklung.

 Wahrscheinlichkeit  $P(\text{Erfolgsfall}) > 95\%$   
(untere Schranke durch QoS und Protokoll).

# Haupteigenschaften der Teleportation

- **Zwei Parteien: Peer-zu-Peer-Übertragung (P2P).**
  - **VPN-/VPC-Tunneling basierend auf Zertifikaten.**
  - **Verbindlichkeit basierend auf digitalen Signaturen.**
  - **Verlustnachweis & Verifikation durch Protokoll-Beweis.**
- 
- **Verlust-Kompensation durch Gutscheine.**

# Zusammenfassung

## Fakten

**Es gibt mehr als nur kontobasierte Verfahren.  
Virtuelle Währungen gibt es gar nicht!**

## Fazit

**Am PoS eröffnet digitales Bargeld neue Perspektiven.  
Mobile Money ist ein weiterer Hot-Spot-Bereich.**

## Ausblick

**Die Zukunft bleibt spannend.**



**Sie finden eine PDF-Kopie dieser Präsentation auf  
der fairCASH Website unter <http://fairCASH.org>.**

**Danke.**

Autor: Dr.-Ing. Heinz Kreft  
E-Mail: [heinz.kreft@faircash.org](mailto:heinz.kreft@faircash.org)  
Tel.: +49 176 41392865