fairCASH-Vision

letzte Modifikation: 18-04-2011

Kurzbeschreibung

Das vorliegende Dokument beschreibt die Vision eines Startups im Bereich der Informations- und Kommunikations-Technologie. Das grundlegende „IP" ist die Übertragung werthaltiger Dateien (sogenannter eToken, hier eCoins), welche in Chip-Tresoren an jeweils mobilen Endpunkten sicher gelagert werden. Diese Technologie ist Bestandteil einer umfassenden Patentstrategie und wurde mit Datum vom 11.03.2011 in Form eines PCT Antrages prioritätsgesichert. Entwickelt wurde die zugrunde liegende Technik während eines Zeitraumes von über zehn Jahren und kulminierte unter anderem in der Dissertationsthesis mit dem Titel „fairCASH based on Loss resistant Teleportation", die in der Informatik der Technischen Fakultät der Universität zu Kiel (CAU) Mai 2010 eingereicht wurde. Mit den dort dokumentierten Basisverfahren ist es nun möglich, den Aufbau und Betrieb hochsicherer Informations- und Kommunikations-Systeme zur Realisierung **digitalen Bargeldes** im Internet zu implementieren. Beide Basisdokumente, sowohl die Dissertation als auch die Patentschrift sind über verschiedene Quellen der Öffentlichkeit zugänglich, so beispielsweise unentgeltlich auf der Web-Präsens www.faircash.org im Downloadbereich.

Die nachfolgende Grafik zeigt phänomenologisch und exemplarisch das im kommerziellen Fokus des Startups stehende Produkt „digitales Bargeld":

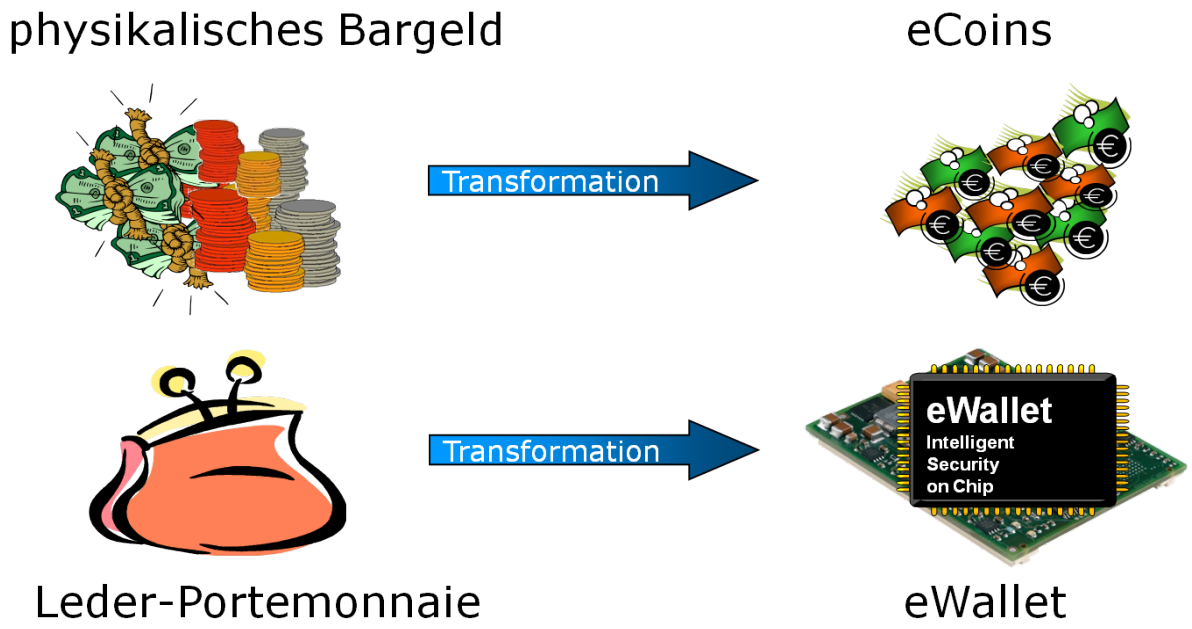

Abbildung 1: Äquivalenz von physischem und digitalem Bargeld.

Dieses Vision Dokument ist eine knappe Zusammenfassung der zugrundeliegenden Mechanismen von fairCASH und der Vision einer Lösung, die zu einer globalen Verfügbarkeit von digitalem Bargeld führen soll. Dadurch kann den physischen Bargeldsystemen dieser Welt zukünftig eine „digitale Schwester" an die Seite gestellt werden, die einerseits bereits alle von Papiergeld und Metallmünzen bekannten Eigenschaften besitzt, andererseits im Internet medienbruchfrei einsetzbar ist.

Inhaltsverzeichnis

Executive Summary

Zahlungsmechanismen gibt es seit frühester Vorzeit. Waren es zunächst Bar-Zahlungsmittel wie Fischzähne, Muscheln, Silber- und Goldmünzen, begann im 11. Jahrhundert in Europa der erste bargeldlose Zahlungsverkehr mit Gut- und Lastschriften sowie Überweisungen – das Girokonto (von ital. Giro und lat. Computus) war erfunden. Das aus islamischen Ländern bekannte konto-basierte Hawala-Finanzsystem wurde erstmals 1327 dokumentiert. Mit der flächendeckenden Einführung des modernen Girokontos (um 1960 in Deutschland) endete die Zeit der Lohntüten. Fortan wurden Löhne und Gehälter statt sie bar auszuzahlen via Girokonto überwiesen – das Zeitalter von Bankgebühren und Zinsen war eingeläutet, das Konto-Prinzip gesellschaftlich verankert. eGeld-Verfahren wie Click&Buy, PayPal, WebCent, Giropay oder „NFC-Handy-Zahlungen" basieren ebenfalls auf dem Konto-Prinzip. Der derzeitige Status quo in Deutschland wurde im November 2009 mit der EU-Direktivenumsetzung des einheitlichen Euro-Zahlungs-Verkehrsraumes SEPA in nationales Recht erreicht.

Und was hat sich bei der Barzahlung getan? 85% der jährlich 460 Mrd. Bezahlvorgänge in der EU werden „cash" abgewickelt. Die Betriebskosten des Bargeldumlauf liegen EU-weit alljährlich 45 bis 70 Mrd. €, wobei der Wert von 80% der Bargeldtransfers im Taschengeld-Rahmen (<20 €) liegt. Das erklärt einen Teil der Bisanz des Bargeldes und den Versuchen, es auch im Internet verfügbar zu machen. Aus dem Jahr 1989 ist ein vielbeachteter Versuch (von David Chaum) zu berichten, mittels eCash ein bargeldähnliches Digital-Verfahren einzuführen. Aufgrund von Defiziten wie der nur teilweisen Umsetzung des Bar-Prinzips sind dieses System und seine Nachfolger erfolglos geblieben. Seitdem stagniert die Entwicklung digitaler Münz-Technologien.

Eine zentrale wirtschaftliche Forderung an digitales Bargeld ist seine Umlauffähigkeit, die so genannte **Transferabilität**, die „offline" in direkter Weise (P2P) geschieht. Dies steht in scheinbarem Widerspruch zum Problem der Entstehung und Verwendung von Münz-Kopien, dem „Multi-spending". Zur Auflösung dieses Konfliktes verwenden nahezu alle bisherigen Verfahren das Prinzip der konditionierten Anonymität von Einweg-Token-Systemen, das die Identität des Besitzers zum festen Bestandteil einer jeden digitalen Münze macht. Grund: Sollte ein solches eCoin mehrfach verwendet werden, lässt sich die Identität ihres Besitzers rechtlich eindeutig ermitteln. Die Probleme einer derartigen Lösung sind jedoch die damit verbundenen Konsequenzen für Anonymität und Transferabilität: Diese beiden wesentlichen Bargeld-Eigenschaften gehen verloren. Diese bislang physischem Bargeld vorbehaltenen Eigenschaften ließen sich bis heute technisch für elektronische Token **nicht** realisieren.

fairCASH definiert eine Anti-These zu kontobasierten Hot-Spot-Verfahren. fairCASH

- kann als digitales Cash-2.0-Zahlungssystem Bargeld-Eigenschaften vollständig in das Internet transponieren,
- nutzt vorhandene ITK-Infrastrukturen wie Bluetooth-, WLAN-, DSL-, GSM-, UMTS- und LTE-Übertragungs-Mechanismen,
- und ergänzt darüber hinaus sogar Eigenschaften, die physikalischem Bargeld fehlen.

Als digitales Bargeldsystem des Internetzeitalters kombiniert fairCASH neueste Erkenntnisse aus der Kryptografie und aus dem Bereich des eCommerce. Unter einem solchen System werden finanzielle Rotationssysteme mit anonym zirkulierenden, serialisierten, authentisierten und zertifizierten Bitmusterentitäten zur Wertaufbewahrungs- und Zahlungsfunktionalität verstanden. Zentraler Bestandteil des vorgestellten Technologie-Frameworks bildet ein "Teleportation" genanntes Offline-Transferprotokoll, das durch flächendeckend fein verteilt auszubringende „nano-Tresore" gestützt wird.

Die Abbildung aller Bargeldeigenschaften, einschließlich der unentgeltlich unbegrenzten Weitergabe und der Anonymität in einem mobilen digitalen Medium wie dem Internet, definiert ein Versprechen des eCommerce der New Economy wesentlicher ökonomischer Taxonomie-Faktoren.

Der Transportmechanismus

fairCASH verwendet zur Übertragung der eCoins ein neuartiges Transportverfahren für nichtstoffliche digitale Münzen über das Internet in einer Weise, dass der Transport eine Teleportation und keinen Kopiervorgang darstellt. Der Begriff "Teleportation" (teles: fern, portare: überbringen) beschreibt ein sehr bekanntes (und triviales) Prinzip, das dem Transport aller substanziellen Dinge innewohnt: Das Bewegen eines Gegenstandes weg von Ort „A" hin zu Ort „B". Bei Materie ist ein Transport immer mit dem Verschwinden am Ursprungsort und dem Wiederauftauchen am Zielort verbunden. Es handelt sich also gewissermaßen um eine „langsame" Teleportation.

Im Internet hingegen sind **bisher** alle Transporte immer Kopiervorgänge, erfolgen dafür annähernd mit Lichtgeschwindigkeit. Weil die betroffenen Datenobjekte jedoch vervielfacht werden, handelt es sich NICHT um Teleportation. fairCASH kombiniert erstmals beide Transportprinzipien: Teleportation UND Lichtgeschwindigkeit, um damit einen Transportmechanismus für digitale Münzen bereit zu stellen. Dieses Verfahren ermöglicht die unmittelbare direkte Weitergabe, so wie dies seit langem beim Bargeld üblich ist.

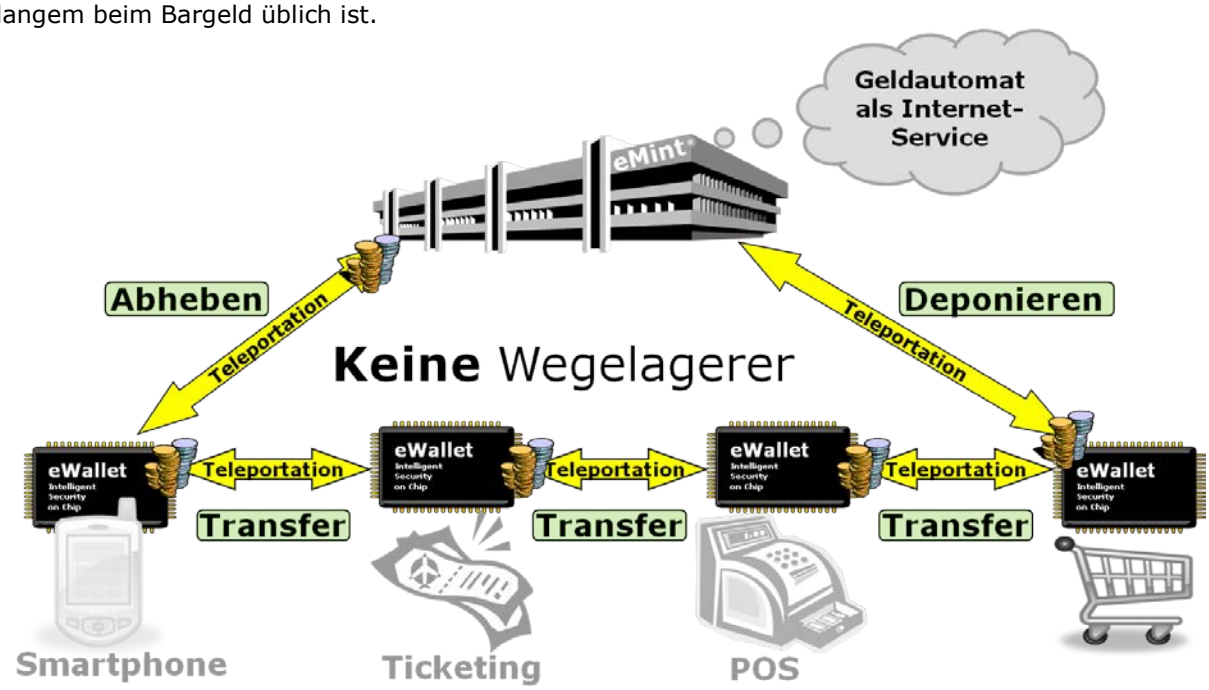

Abbildung 2: Direkte Übertragbarkeit von fairCASH-eCoins.

Eine zentrale Rolle spielt die Sicherheit. Hierzu wurde ein Transfer-Protokoll entwickelt, das elektronische Münzen kopierfrei auf Peer-to-Peer-Basis teleportiert und damit die gewünschten Bargeld-Eigenschaften verwirklicht: Jeder durch dieses Protokoll veranlasste eCoin-Transfer zeichnet sich dadurch aus, dass er die Münzen **bewegt**, aber **nicht kopiert**: Sie verschwinden beim Absender um beim Empfänger wieder zu erscheinen. Vorhandene unikative Eigenschaften bleiben erhalten. Elektronische Portemonnaies, sogenannte eWallets, bilden als Chip-Tresore die Endpunkte der Bargeld-Übertragung und sichern sie physikalisch und kryptografisch gegen Analyse, Manipulation und Duplikation.

Nano-Tresore im Chip

Dass die Teleportation das Entstehen von Münzkopien verhindert ist zwar notwendig, reicht aber für ein digitales Bezahl-System noch nicht aus. Denn nicht nur „reisende Münzen" –"transiente eCoins"– müssen sicher geleitet, sondern auch "ruhende eCoins" geschützt werden.

Der Bereitstellung eines sichereren stationären Zustands, also einer Ruheposition, die an dieser Stelle "persistent" genannt werden soll, kommt eine gleichgewichtige Bedeutung zu. Denn was nützt eine narrensichere Übertragung, wenn an einem der Endpunkte (vor oder nach einer Übertragung) die eCoins dann doch kopiert werden? Um das zu verhindern gibt es bereits viele Verfahren, darunter sogar einige recht brauchbare. Die Weiterentwicklung der besten dieser Verfahren führt zu einem Nano-Tresor auf IC-Basis, der im fairCASH-Kontext "CASTOR[1]" genannt wird. Ein CASTOR ist ohne weitere Härtungsmaßnahmen zwar nicht unbedingt feuerfest, und auch einen Meteoriteneinschlag wird er kaum überstehen. Aber er kann die in ihm untergebrachten persistenten eCoins ausreichend sicher[2] vor unbefugten Zugriffen schützen. Darüber hinaus ist er in der Lage, autonome Entscheidungen in unsicheren Umgebungen zu treffen. Dies ist von essenzieller Bedeutung, damit beispielsweise das Teleportations-Protokoll von außen unbeeinflussbar ablaufen kann.

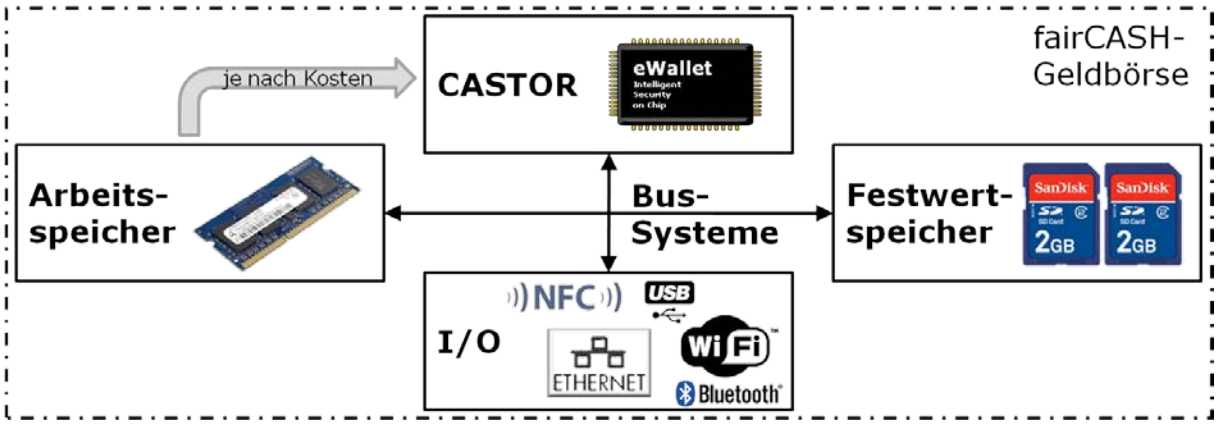

Abbildung 3: Bestandteile einer fairCASH Geldbörse.

Ein solches fairCASH-Portemonnaie ist in der Lage, digitale Münzen per Teleportation mit einem seiner Pendants autonom und sicher auszutauschen. Die wesentlichen Bestandteile hierzu finden sich in der Abbildung 3: Der eWallet-Chip beinhaltet die erforderliche Logik der Portemonnaie-Funktionalität einschließlich der Teleportations-Logik. Sein Arbeitsspeicher kann separat auf einem PCB oder integriert im CASTOR-Chip realisiert werden; ausschlaggebend sind letztlich die Produktionskosten; beide Möglichkeiten sind aufgrund der eingesetzten Krypto-Verfahren gleichsicher! Zum Schutz vor Datenverlust kommen zum Abspeichern der verschlüsselten digitalen Münzen gespiegelte Flash-Speicher (daher doppelt) zum Einsatz. Zur Kommunikation zwischen zwei eWallets lassen sich grundsätzlich alle digitalen Schnittstellen verwenden. Sinnvoll erscheinen aufgrund der marktgängigen I/O-Systeme vornehmlich NFC, USB, Ethernet, WiFi sowie Bluetooth.

Eine fairCASH-Geldbörse lässt sich völlig autonom von einer Kommunikations-Infrastruktur betreiben, etwa durch die drahtlose Device-Koppelung über Bluetooth-Profile oder WLAN an ein vorhandenes Smartphone aber auch durch direkte Integration in Systeme, die mit einer Bezahlfunktion ausgerüstet werden sollen: Fernseher, Elektro-Autos, Router, Computer und viele andere, nicht zuletzt Smartphones oder Spielkonsolen der nächsten Generation.

[1] **CA**sk for **S**torage and **T**ransport **O**f access **R**estricted secrets.
[2] Darunter wird eine betriebswirtschaftliche Definition von Sicherheit verstanden (siehe auch Dissertation).

eCoin Infrastruktur und Sicherheit

Die Teleportation stellt das technische Vehikel bereit, das den eCoin-Transport auf den Straßen des Internets realisiert. Für die Erzeugung und das „in den Verkehr bringen" der digitalen Münzen und für deren Erhalt ist bei fairCASH eine Institution namens eMint (elektronische Münzanstalt) zuständig. Dabei handelt es sich um eine Art Bundesdruckerei für eCoins. Außerdem ist es erforderlich, Spielregeln und Vertrauen zu erzeugen. Hierfür ist ein so genanntes Trustcenter, die so genannte Certification Authority (CA), zuständig. Das Trustcenter wie auch die eMint und alle anderen Services werden in Form eines ganz üblichen, ISO-genormten Standards für eine Public-Key-Infrastruktur (ITU-T X.509v3) integriert, wie sie bereits seit vielen Jahren im Internet verwendet und gleichfalls vom neuen deutschen Personalausweis (nPA) genutzt wird.

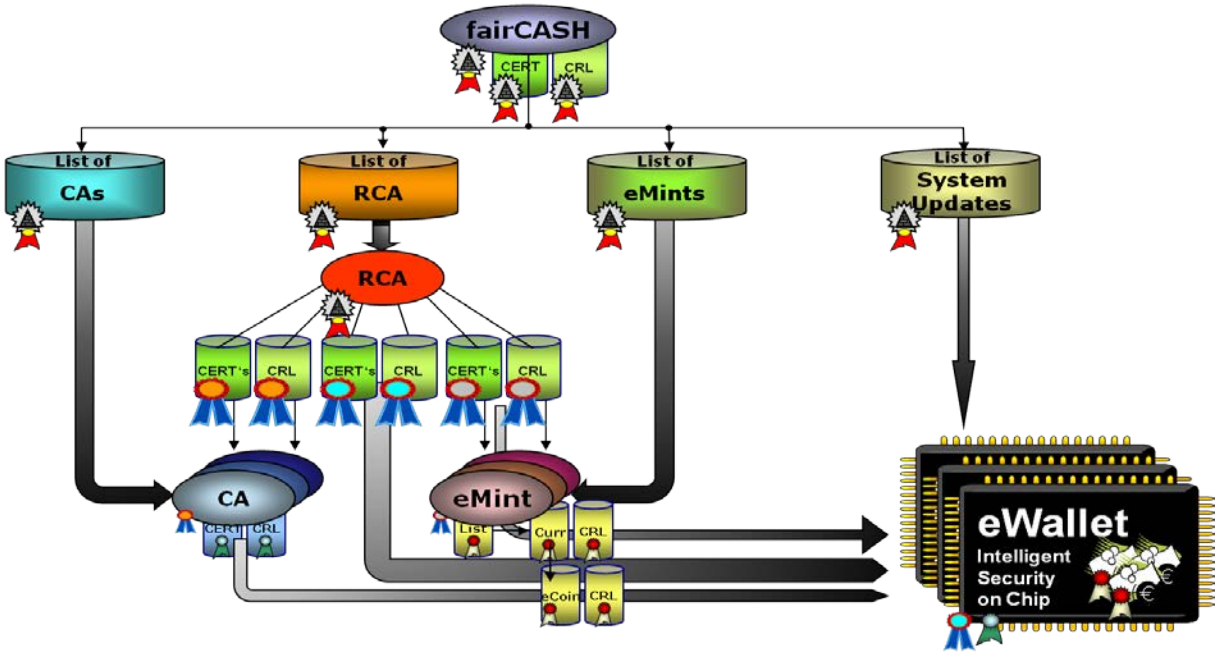

Abbildung 4: Hierarchische Public-Key-Infrastruktur.

eCoins erhält der fairCASH-Anwender im einfachsten Fall direkt aus einer Art Geldautomat. Dabei handelt es sich, wie schon beim physikalischen Bargeld, letztlich um einen Transfervorgang Giralgeld → Bargeld. Analog zum herkömmlichen Bargeld wird vom Kundenkonto (via EC- oder Kreditkarte) ein Ausgabevorgang initiiert, jedoch mit kleineren Unterschieden:

1. Der Geldautomat steht bei fairCASH im Internet, so dass sich der Anwender zum „Abheben" des Bargelds nicht zu einem physischen Automaten hin bewegen muss,
2. der fairCASH Bankautomat nimmt auch digitales Bargeld wieder zurück und überträgt dieses auf das (ein) Konto des Anwenders,
3. das Ganze funktioniert Internet-weit und verursacht keine Transaktionskosten,
4. alternativ kann ein fairCASH-Anwender eCoins sogar ohne ein vorhandenes Giro-Konto beziehen, etwa wenn sein Arbeitgeber ihn in eCoins auf sein eWallet bezahlt (Prinzip der digitalen Lohntüte).

Die Abbildung 4 zeigt das Zusammenspiel der im fairCASH-System in einzelne Instanzen gekapselten Funktionalitäten:

- Die **fairCASH**-Company betreibt den Business-Case durch die Zurverfügungstellung der erforderlichen Technologie. Defacto stellt sie einen Teil der RCA.
- Die **RCA** ist die operierende oberste Instanz in der fairCASH Infrastruktur.
- Die Münzerzeugung wird über die **eMints** realisiert. Dies sind die digitalen Münzanstalten, in denen die eCoins „gedruckt" werden.
- Die Wahrnehmung der Regulierungs-Interessen (in Deutschland zuständig: die BaFin) und die Ausgabe der Betriebszertifikate für die digitalen eWallets werden bei fairCASH über die Trust-Center (**CAs**) realisiert.
- Die **eWallets** stellen die Portemonnaie-Komponente für das digitale Geld bereit.

Digitales Bargeld

Geld ist eine altbekannte Sache und lässt sich bis in die Frühzeit der Menschheitsgeschichte zurückverfolgen. Bargeld –wie es aus dem realen Leben bekannt– gibt es bis heute im Internet nicht. Das will fairCASH ändern, dessen zugrundeliegende Technologie erstmals die Internet-Umsetzung dieses seit Menschengedenken erfolgreich erprobten Konzepts ermöglicht. Die fairCASH-Macher "bauen" **digitales Bargeld**.

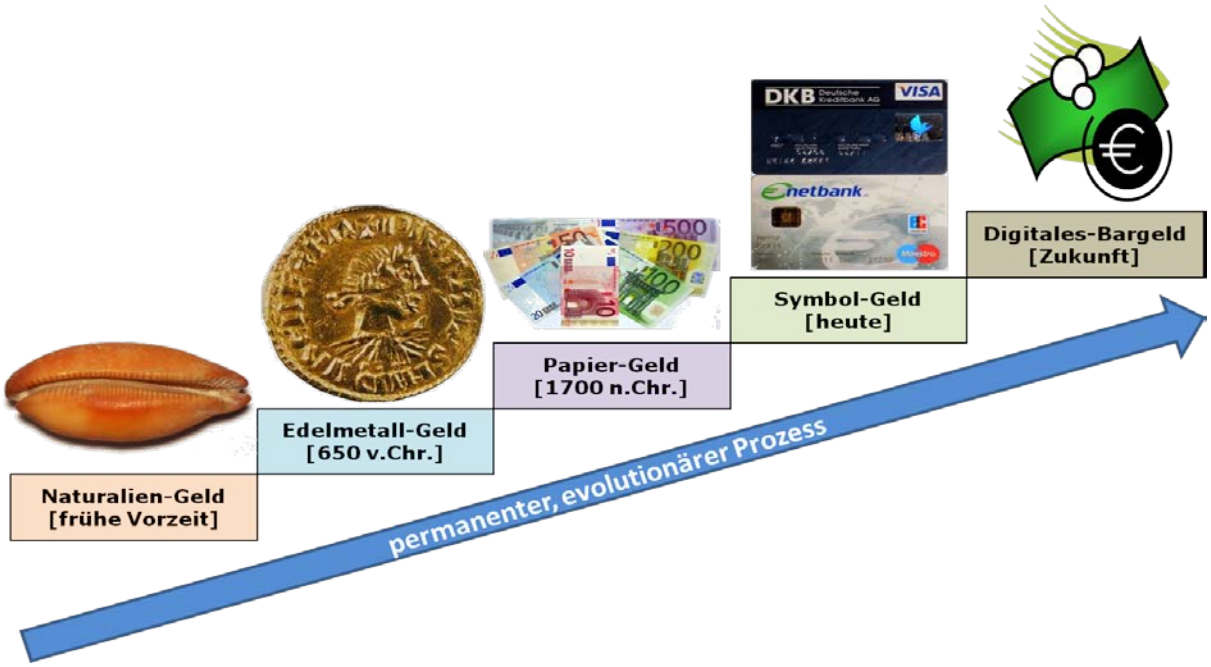

Abbildung 5: Evolution der Zahlungsinstrumente.

Verfolgt man den in Abbildung 5 gezeigten Evolutions-Pfad, stellt digitales Bargeld den Endpunkt des aktuellen Entwicklungsprozesses dar. Die erforderlichen Protagonisten sind in der Abbildung 6 zu sehen:

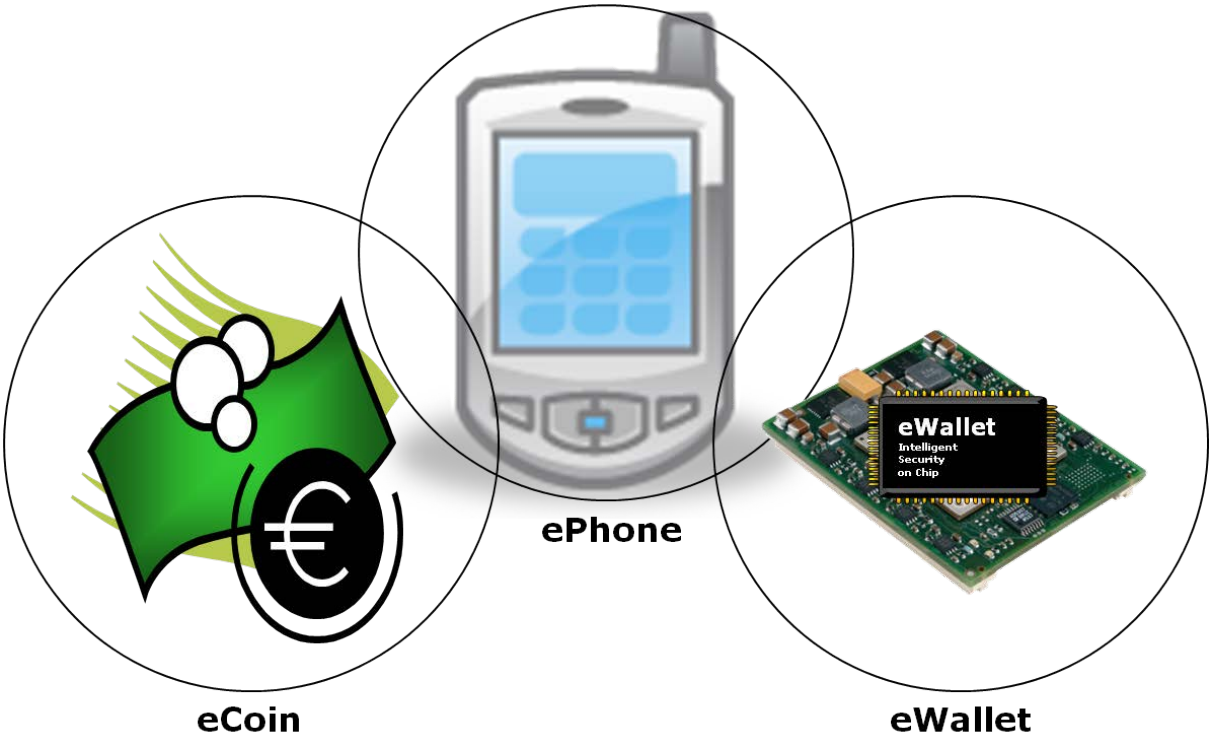

Abbildung 6: Protagonisten des fairCASH basierten digitalen Bargeldes.

Dualismus: Barprinzip versus Kontoprinzip

Aus Sicht der Ökonomen lassen sich heute drei Formen des Geldes unterscheiden:

- Zentralbankgeld[3] (Bargeld),
- Giralgeld[4] (Buchgeld) und
- elektronisches Geld (eGeld).

Dabei wird die Notenbank-Geldmenge aus dem Bargeld und den Giro-Guthaben aller inländischen Banken gebildet. Zur Vereinfachung ist es jedoch für fairCASH-Zwecke ausreichend, argumentativ bei den Geldarten nur noch folgende technische Unterscheidung zu treffen:

- Konto-Prinzip und
- Münz-Prinzip.

In diesen beiden Begriffskategorien lassen sich technisch sämtliche existente Geld-Konzepte unterbringen:

Konto-Prinzip:
Bei den Verfahren in der Konto-Kategorie entscheidet das so genannte Zugriffsprinzip (Access-Mechanismus) über die Funktionalität beim Anwender. Das kann klassisch eine EC- bzw. Kreditkarte sein oder ein Instrument nach dem Standard „Common Electronic Purse Specification" (CEPS) wie die Geldkarte vom ZKA[5] oder hierzulande weniger bekannte Systeme wie Edy, Suica, M-PESA oder Obopay sein. Systeme auf einer SMS-, NFC-Basis oder der QR-Code Methode sind ebenfalls bekannt. Hinzu kommen eGeldverfahren wie PayPal, Giropay oder Click&Buy.

Münz-Prinzip:
Münzgeld findet sich bis heute nur in der physikalischen Welt, meistens „auf der letzten Meile". Trotzdem ist es weltweit das meistgenutzte Zahlungssystem. Wesentlich an dieser Stelle ist die Erkenntnis, dass Geld im Internet heute immer kontobasierend ist. (Gutscheinsysteme zählen nicht zum Münzprinzip). Münzsysteme gibt es hingegen nur außerhalb des Internets. Zwar hat es immer wieder Versuche gegeben das zu ändern, doch all diese Lösungs-Ansätze waren samt und sonders nicht mit Erfolg gesegnet: Entweder wurde als Münz-Konzept gesprungen und als Konto-System gelandet, oder es blieb zu wenig von der Münz-Attraktivität übrig, um gemäß Robert B. Woodruff[6] einen Kundenwert erbringen zu können.

[3] Vielfach auch als Geldmenge M0 bezeichnet.
[4] Summe der Sichteinlagen (M1), der Spareinlagen (M2) und der Terminaleinlagen (M3).
[5] Im Zentralen Kreditausschuss (ZKA) sind seit 1932 die fünf Spitzenverbände der deutschen Kreditwirtschaft (Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V., der Bundesverband deutscher Banken e.V., der Bundesverband Öffentlicher Banken Deutschlands e.V., der Deutscher Sparkassen- und Giroverband e.V. sowie der Verband deutscher Pfandbriefbanken e.V.) zusammengeschlossen. Er versteht sich als Interessen-Vertretung.
[6] Emeritus Professor an der Universität von Tennessee, College of Business Administration, Knoxville. In der BWL bekannter Wissenschaftler für „Customer Value und Satisfaction Determination" Prozesse in Verbindung mit Marketing Management.

fairCASH und Markt

Der technologische Motor bei fairCASH umfasst zwei wesentliche Elemente: Die Teleportation und den CASTOR, wobei der CASTOR das Herzstück eines elektronischen Portemonnaies darstellt. Mit diesen beiden Elementen lässt sich das Prinzip Bargeld so umsetzen, das SÄMTLICHE Attribute des bekannten Bargeldverfahrens in das Internet überführt werden können. Dies sind insbesondere

- die **Anonymität** als Voraussetzung für die Offline-Transferabilität,
- die **Peer-to-Peer-Fähigkeit** (P2P) in Kombination mit einem **Offline-Transfer** (so können zwei fairCASH-taugliche Handys im tiefsten Urwald ohne Mobilfunknetz oder Internet-Zugang einen Zahlungstransfer durchführen, solange sie sich nur im Kommunikationsradius ihrer lokalen Funksysteme wie Bluetooth oder WLAN befinden) und
- die **Transferabilität**, also die in ihrer Häufigkeit unbegrenzte Offline-Weitergabe-Möglichkeit für digitale Münzen.

Die fairCASH-Technologie realisiert **digitales Bargeld** erstmals kompromisslos. Diese Erkenntnis impliziert die Frage, wer derlei in der heutigen Zeit benötigt, in der es doch außer physischem Bargeld bereits „electronic Cash", Giropay, Visa und Co. gibt und, sollte das noch nicht ausreichen, der Zugriff auf Internet-Zahlungs-Dienste wie PayPal, Click&Buy, etc. möglich ist.

Realistisch gesehen, ist der Betrieb heutiger Zahlungsverkehrssysteme durchaus aufwändig zu nennen. Die mit Abstand teuersten Implementierungen sind wahrscheinlich physikalische Bargeld-Verfahren. Das mag auf den ersten Blick verwundern, weil Anwender keine „Rechnung" für die Benutzung von Bargeld erhalten, das ihnen also kostenfrei erscheinen muss. Doch dies ist eine unzutreffende Fiktion: Die Betriebskosten des Euro-Systems verschlingen jährlich 45-70 Milliarden Euro, eine Summe, die letztlich von den Nutzern getragen werden muss.

Unsere Gesellschaft akzeptiert nicht sonderlich nachhaltige, zudem einen wachsenden Kostenanteil allein für die Abwicklung der Bezahlung zu bezahlen, sei es für Grund-, Kontoführungs-, Überweisungs- oder Transaktions-Gebühren. Den wenigsten Kreditkarten-Benutzer ist wahrscheinlich bewusst, dass die meisten Anwendungen (ebenso das Gros der Zahlungen im Internet) tatsächlich KEINEN Kredit erfordern! Sie zahlen also für eine nicht benötigte Kreditleistung oder besser: Die Transferleistung ist der bezahlte Wert. Fairerweise muss man hier erwähnen, dass bei Kreditkarten die vorgehaltene Infrastruktur global ist und dem Kunden Versicherungsleistungen geboten werden (Sicherung gegen Verlust oder Missbrauch).

Real weisen fast alle kontobasierten Verfahren **Schwundgeld** auf, da vom Initiator oder Empfänger (oder von beiden) des Geldtransfers Transaktionskosten erhoben werden. Bei vielen Verfahren tritt der Anwender darüber hinaus zwangsweise einige seiner Verfügungsrechte an die kontoführende Stelle ab, etwa beim Umgang mit der so genannten **Wertstellungspraxis**. Es gibt also fundamentale Unterschiede prinzipieller Art zwischen Konto und Münze. Die Frage ist nur: Sind all diese Einschränkungen respektive Randbedingungen überhaupt (in jedem Fall) erforderlich? Ließe sich nicht einen Großteil dieser Leistungen einfach durch einen Wechsel der Basistechnologie systemimmanent effektiver gestalten?

Darüber hinaus ist es nicht sonderlich fair, Nichtnutzer ebenfalls zur Finanzierung eines Geschäftsmodelles heranzuziehen. Die Bankenbranche hat aber genau dies geschafft: Ein deutsches Gesetz verbietet einen Aufschlag für Zahlungen mittels Kreditkarte zu erheben, selbst wenn sich nicht alle immer daran halten (darunter diverse Billig-Flug-Linien). Damit sind also die Kosten für eine Kreditkartenzahlung bei den teilnehmenden Akzeptanzunternehmen in die Dienstleistungen und Waren bereits eingepreist[7].

[7] Wenn man einmal den „Trick" draufhat, alle zwangsweise zahlen zu lassen, ist man entweder eine Regulierungsbehörde oder ein systemkritisches Unternehmen.

Modalitäten von Zahlungssystemen

Ein genauerer Blick auf das Business-Modell eines typischen Zahlungssystems ist lohnenswert. Prinzipiell müssen Zahlungssysteme für deren Betreiber einen Gewinn abwerfen. Doch darum geht es nicht primär sondern vielmehr um die Frage, wie ein Unternehmen den Gewinn realisiert und wie teuer es für seine Kunden letztlich wird — zumal eine Vollkostenrechnung nur selten einfach zu bewerkstelligen sein dürfte. Flatrate- und Pay-per-Use-Modelle stellen bei derlei Betrachtungen die beiden „Antipoden" der möglichen Basisabrechnungs-Modelle dar. Das Euro-System ließe sich etwa als ein per Regulierung festgelegtes Flatrate-System interpretieren, wobei über die Intensität der individuellen Nutzung hinaus noch der jeweils Bargeld systemimmanente Zinsverlust hinzukommt. Die meisten Alternativ-Modelle (fairCASH ebenso) basieren allerdings auf einer Mischung dieser beiden Basisabrechnungs-Modelle. Kostenfrei für die Anwender sind indes nur wenige, häufig aus Gründen des Wettbewerbs quersubventionierte Systeme, obwohl sie dennoch sehr wohl Kosten verursachen. Dazu zählen beispielsweise das bekannte Girokonto (mit der systemischen und teuren Bargeld-Schnittstelle "Geldautomat") sowie Konto-zu-Konto-Überweisungen im EU-Binnenbereich (SEPA). In Systemen jenseits des Bereichs von Girobasiskonten erheben die allermeisten Anbieter Transaktions-Gebühren, die sich zumeist aus einem Fixbetrag und einer prozentualen Abgabe auf den Transferbetrag zusammensetzen. So fallen in den Basistarifen etwa für den Initiator eines PayPal-Transfers in Deutschland mindestens 35 Cent pro Transaktion an, bei MoneyBookers beträgt die fixe Mindestgebühr 29 Cent (Stand: 2011).

Eine Alternative wäre eine Flatrate bei privater Nutzung für einen konkreten Zeitraum, verbunden mit einer Art „All-you-can-eat"-Prinzip. Machbar wäre dies jedoch nur dann, wenn die Mehrzahl der Transaktionen eines solchen Systems real keine Betriebskosten verursacht. Dies ist bei einem fairCASH-basierten Digital-Cash-System der Fall: Zahlungstransfers laufen „in-band" und auf der Infrastruktur des Anwenders ab. Ganz kostenfrei ist der Betrieb natürlich auch bei fairCASH nicht: Der Betrieb der eMint und des Trustcenters sowie die grundsätzlichen Aufwendungen eines Zahlungssystems verursachen Kosten. Der entscheidende Faktor ist aber deren Größenordnung, und die fällt bei fairCASH substantiell geringer aus als bei einem physikalischen Bargeldverfahren (wie auch im eGeld-Vergleich).

Allen dirigistischen Verfahren (so auch das kontobasierende System) beinhalten prinzipbedingt einen Machttransfer der Anwender an den „Man in the Middle". Dies könnte den einen oder anderen an die Stimmrechtsübertragung der Einzelaktionäre an den Fondverwalter eines Aktiendepots erinnern. Egal, ob dabei über die Verwertung persönlicher SWIFT-Daten scheingefochten oder fundamental reguliert wird, um Eigeninteressen durchzusetzen: **Zentralistische Systeme laden immer zum Missbrauch ein und werden oft missbraucht.** Sie stehen darüber hinaus auf der Top-Ten-Liste von Hackern und locken sie an wie Nektar die Bienen (Honey-Pots). So werden etwa Kontodaten gleich millionenfach von Kriminellen geraubt (die Geschädigten erfahren davon meist erst dann, wenn es bereits zu spät ist oder gar nie). Der als rechtskonform definierte Raubzug von SWIFT-Transaktionsdaten soll hier als weiteres Beispiel genannt sein.

Ein besser an die demokratische Grundordnung angepasstes Zahlungsverkehrssystem erfüllt hingegen die Forderung nach einer **flächendeckenden, autarken und demokratisch verteilten Architektur.** Das Modell einer feinmaschigen, verteilten Infrastruktur kommt in den Sinn, Straßen etwa, die nur dann einen volkswirtschaftlichen Nutzen darstellen, wenn sie in der Fläche als Netzgut mit möglichst einfachem Zugang für viele Menschen erreichbar sind. Wer das nicht glaubt, sollte bei Gelegenheit nach Madagaskar fahren (oder sich der Bedeutung eines ubiquitären Maut-Systems bewusst werden) ….

Wie sehr flächenorientierte Netzgüter-Systeme wie das Internet durch die Rückführung von Machtbefugnissen den Prozess einer Re-Demokratisierung unterstützen, bemerken mittlerweile immer mehr Menschen auf dieser Welt. Stellte man dem Internet ein bargeldbasiertes digitales Zahlungssystem zur Seite, können sich systemrelevante Zentralsysteme langfristig hin zu vitalen, gesunden und verteilten Strukturen entwickeln. So, wie das Internet Backbones, Hochleistungs-Server und Service-Wolken zu einer funktionalen Mischung zusammenfügt, würde auch die Rückführung der unter ihrer systemimmanenten Wichtigkeit zusammengebrochenen Finanzinstitutionen zu einer fundamentalen ökonomischen und soziologischen Stabilisierung führen können (Stichwort: Systemrelevanz). Mit einer eMint unter Kontrolle des Souveräns würde eine flächendeckende, autarke und demokratisch verteilte Architektur gleichzeitig dessen Erpressbarkeit, Slogan: "Too Big to Fail", beenden. Sie kann darüber hinaus in beträchtlichem Umfang innere Reibung bestehender Zahlungssysteme eliminieren: So könnten Peer-to-Peer-Direkt-Transfers volkswirtschaftlich nutzlose Giralgeld-Transfer-Kosten minimieren.

Ein bisschen Historie

Die Geschichte der bisherigen Versuche, Bargeldverfahren ins Internet zu bringen, lässt sich wie folgt zusammenfassen:

Generation I: [1990]
Im Internet bedarf es besonderer elektronischer Bezahlmethoden und Systeme, damit die Geschäfte in Gang kommen können. Es wurden sowohl reine Software-Modelle (eCash von David Chaum und Brands Cash von David Brands als auch Portemonnaie-basierte Verfahren (Mondex von MasterCard) ausprobiert, als auch die Idee eines international gültigen Bargeldes geträumt. Vertraglich geregelte Anbieter-Kunden-Beziehung (z.B. Abonnenten-Modelle) und Inkasso-Systeme standen im Vordergrund.

Generation II: [2000]
Die Systeme der Generation I sind gescheitert. Die Gründe hierzu sind vielfältiger Natur, im Wesentlichen lag das daran, dass ihnen essentielle Bargeldeigenschaften fehlten. In der Folge wurden im Internet unbare Zahlungsverfahren wie Kreditkartenzahlung, Scheckeinreichung, Lastschriftverfahren und Überweisungen üblich. Aus der Perspektive der Kreditwirtschaft ist dieser Schritt nachvollziehbar: Der unbare Zahlungsverkehr ist schon seit Jahren vollständig DV-gestützt und man bemüht sich, den Point-of-Sale über das electronic-Cash-Verfahren (Giralgeld) und die Bankverbindung mit Hilfe des Homebankings an die unbare, elektronische Zahlungsabwicklung anzukoppeln.

Generation III: [2010]
fairCASH repliziert sämtliche vom physischen Bargeld her bekannte Eigenschaften.

Dieser Prozess der Entwicklung und Etablierung von Zahlungssystemen für das Internet währt immer noch fort, sowohl seitens der technischen als auch von der sozialen Gestaltung. Diese sozio-technische Genese eines vernetzten großtechnischen Systems, welches einen wesentlichen Teil der Infrastruktur der Informationsgesellschaft ausmacht, umfasst vom Potential her als spektakulärste Innovation das „digitale Bargeld". Dieses wird sicherheitstechnisch heftig hinterfragt, aber auch von den geldpolitischen Konsequenzen her besonders skeptisch beäugt. Aus Effizienzgründen haben die konventionellen Zahlungssysteme zwar noch immer eine gewisse Berechtigung. Da sie aber das Potential der immer erfolgreicher agierenden elektronischen Märkte nicht oder nur wenig nutzen, werden besser adaptierte Mechanismen immer stärker erforderlich – vor allem im Zusammenhang mit digitalen Leistungen und Gütern, welche direkt über elektronische Netzwerke ausgeliefert werden (Stichwort „Cloud"). Hier sind neue Mechanismen notwendig, die eine unmittelbare Bezahlung zulassen.

Operatives Geschäftsmodel bei fairCASH

Die systemische Leistung, das in den Umlauf bringen von Bargeld, dessen Verknüpfung mit dem Giralgeld-Kreislauf und umgekehrt das „Wieder-aus-Cashen" bezeichnet man landläufig als Barzahlungsverkehrs-System. Das operative Betreiben eines fairCASH-Zahlungssystems ist im Gegensatz zu den vielfältigen Zahlungsabwicklungsverfahren sogenannter Intermediates ein echtes **Systemgeschäft mit Basisfunktionalität**. Im Vordergrund steht das eigenständige Agieren, Betreiben und Anbieten eines Bankgeschäftes, nicht das Management von Zahlungen im Spannungsfeld von Zahlungssystem-Anwendern und -Anbietern (Stichwort: Forderungsmanagement[8]).

Wodurch sich bei fairCASH operativ Geld verdienen lässt, ist nachfolgend punktuell aufgelistet:

1. **Umsatzorientierte Nutzungsgebühr für kommerzielle Anwender**
   Ein geschäftlich agierender Anwender kann aus naheliegenden und offenkundigen Gründen nicht anonym agieren. Für sein eWallet benötigt er daher ein identifiziertes Nutzungszertifikat. Für dieses kommerziell genutzte eWallet wird eine dem Cashflow adaptierte, prozentuale Nutzungsgebühr fällig.

2. **Verkauf von eWallets**
   eWallets werden benötigt, um das fairCASH-System überhaupt nutzen zu können. Ob dies nun separate Geräte sind, die sich über Draht- oder Funkschnittstellen mit einer Bediensoftware (a.k. Terminal) verbinden, oder ob es sich um integrierte Anwendungen (beispielsweise ein Mobiltelefon-Portemonnaie) handelt, ist für die Nutzung ohne Relevanz. Da eWallets aufgrund von Sicherheitsüberlegungen nicht unbegrenzt lange nutzbar sein werden, ihre operative Lebensdauer[9] daher konstruktiv begrenzt ist, kann in der Wertschöpfungskette durch den kontinuierlichen Verkauf von eWallets ebenfalls ein entsprechender kalkulatorischer Gewinn entstehen.

3. **Zinsgewinne**
   Bargeld auf €uro-Basis kann über den EURIBOR[10]-Zinssatz ohne Risiko verliehen werden. Die eMint nimmt diesen Zinsgewinn ein.

[8] welches es bei fairCASH gar nicht gibt.
[9] LifeCycle Management.
[10] http://de.euribor-rates.eu/.

Populäre eGeld-Systeme

Nachfolgend sind die größten eGeld-Zahlungssysteme in Deutschland genannt (Reihung nicht größenrelevant):

- Paypal,
- Click&Buy,
- T-Pay,
- Paysafecard,
- Sofortüberweisung.de,
- Infin-Micropayment,
- WebCent und
- Giropay.

Bekannte eGeldsysteme:

- WebMoney - http://www.wmtransfer.com/eng/about/
  Online payment system. Vermutlich im Besitz der Russenmafia.
- eGold - http://www.e-gold.com/
  ist in den regulierten Staaten gebannt (Geldwäsche).
- uKASH - http://www.ukash.com/de/de/home.aspx
  online Gutschein System.
- Paysafecard – http://www.paysafecard.com/de/
  Online PIN System.
- PayBox – 2003 in DL eingestellt
  Lastschrift per Handy PIN (nur noch in Österreich aktiv).
- Iclear – http://www.iclear.de/
  treuhänderisches Zahlungssystem für den Online-Handel.
- StreetCash – eingestellt
  ähnlich PayBox, arbeitet mit SMS.
- Crandy – Webseite www.crandy.com ist abgeschaltet
  Mobile Payment System für Handy.
- PayPal – www.paypal.de
  Das weltweit größte Online-Bezahlsystem.
- Click & Buy – http://www.clickandbuy.com/DE_de/bezahlen/index.html
  Online-Zahlsystem der Deutsche Telekom.
- Web.Cent – https://www1.webcent.web.de/
  Das System kann nur von Web.de-Usern genutzt werden.
- Paysafecard – http://www.paysafecard.com/de/
  Online Prepaid-PIN.
- MicroMoney – http://www.t-pay.de/t-pay-info/shoppen-mit-micromoney.html
  Anonymes Prepaid System der Telekom.
- Infin-Payment – http://www.infin.de/service/payment-online-kasse.htm
  Abrechnungsverfahren über die Telefonrechnung (SMS, 0900-Nummer)
- GiroPay – http://www.giropay.de/
  Online-Bezahlverfahren der deutschen Banken und Sparkassenverbände.
- Wirecard - http://www.wirecard.de/startseite.html
  Virtuelle Kreditkarte. Diese wird per Bareinzahlung, Überweisung oder Lastschrift aufgeladen. Mit der virtuellen Karte können User dann bei allen Onlineshops zahlen, die eine Mastercard akzeptieren.
- Moneybookers – http://www.moneybookers.com/app/
  Ähnlich wie Paypal.
- Sofortüberweisung – https://www.payment-network.com/sue_de
  Käufer füllt auf Shopseite ein Überweisungsformular aus. Problem: PIN und TAN.
- Mpass – http://www.mpass.de/
  Handynummer und Mpass-PIN eingeben. Anschließend Bestätigungs-SMS (19 cent). Anschließend erfolgt eine Lastschrift oder Kontoüberweisung.

Glossar

IP	- **I**ntellectual **P**roperty.
CAU	- **C**hristian-**A**lbrechts-**U**niversität zu Kiel.
P2P	- Peer-to-Peer
CASTOR	- **CA**sk for **S**torage and **T**ransport **O**f access **R**estricted secrets
HSM	- **H**ardware **S**ecurity **M**odule
SE	- **S**ecure **E**lement
PKI	- **P**ublic-**K**ey-**I**nfrastructure
eMint	- **e**lektronische Münzanstalt
eCoin	- **e**lektronische Münze
CA	- **C**ertification **A**uthority, Trustcenter
ISO	- **I**nternational **O**rganization for **S**tandardization
ITU-T	- **I**nternational **T**elecommunication **U**nion, Sektor **T**elekommunikation
X.509	- Standard für eine Public-Key-Infrastruktur
eGeld	- **e**lektronisches Geld (kein Bargeld!)
EC	- **E**lectronic **C**ash (kein Bargeld!)
CEPS	- **C**ommon **E**lectronic **P**urse **S**pecification
ZKA	- **Z**entraler **K**redit-**A**usschuss
SMS	- **S**hort **M**essage **S**ervice
M0	- Geldmenge der Summe des Bargeldes
M1	- Geldmenge der Summe der Sichteinlagen
M2	- Geldmenge der Summe der Spareinlagen
M3	- Geldmenge der Summe der Terminaleinlagen
EU	- **E**uropäische **U**nion
S€PA	- **S**ingle **E**uro **P**ayments **A**rea
SWIFT	- **S**ociety for **W**orldwide **I**nterbank **F**inancial **T**elecommunication
BT	- **B**lue**t**ooth
WLAN	- **W**ireless **LAN**
Euribor	- **Eur**o **I**nter**b**ank **O**ffered **R**ate

Referenz

http://www.faircash.org/