fairCASH-Vision

letzte Modifikation: 05-01-2011

Kurzbeschreibung

Das vorliegende Dokument beschreibt die Vision eines Startups im Bereich der Informations- und Kommunikations-Technologie. Das geplante Produkt ist Know-how (Intellectual Property), das den Aufbau und Betrieb hochsicherer Informations- und Kommunikations-Systeme zur Realisierung **digitalen Bargeldes** ermöglicht.

Dieses Dokument basiert auf einer Technologie, die von Dr.-Ing. Heinz Kreft als Dissertationsthesis in der Informatik der Technischen Fakultät der Universität zu Kiel (CAU) 2010 eingereicht wurde.

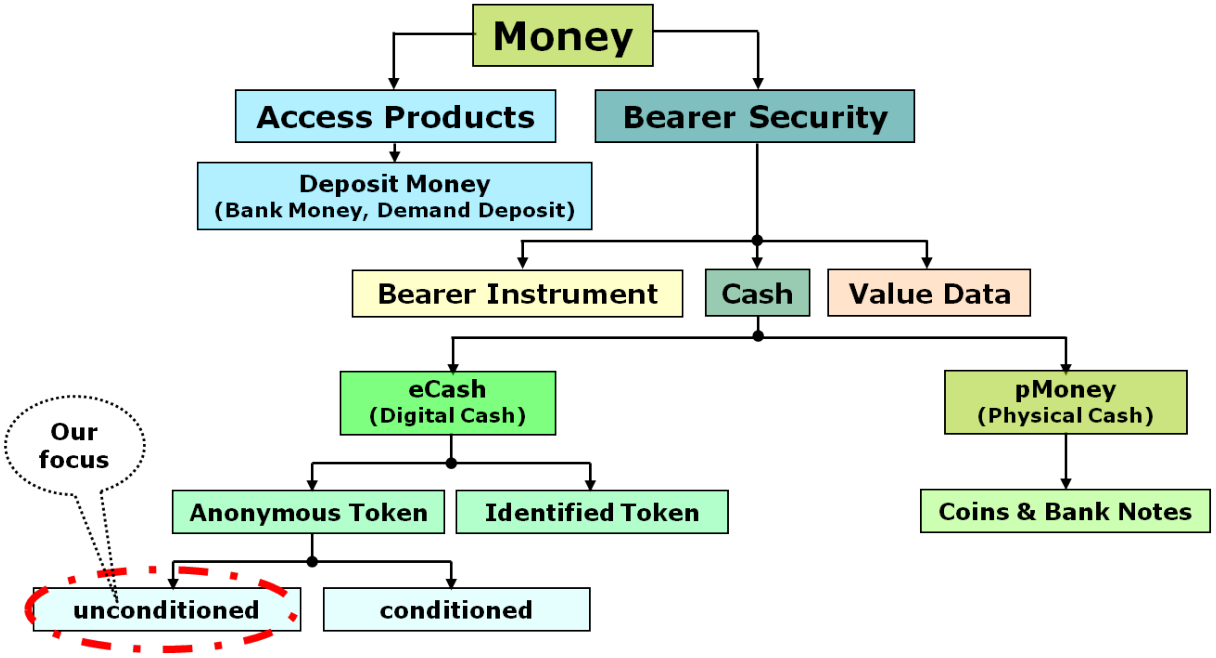

Abbildung 1: Verschiedene Arten von Geld.

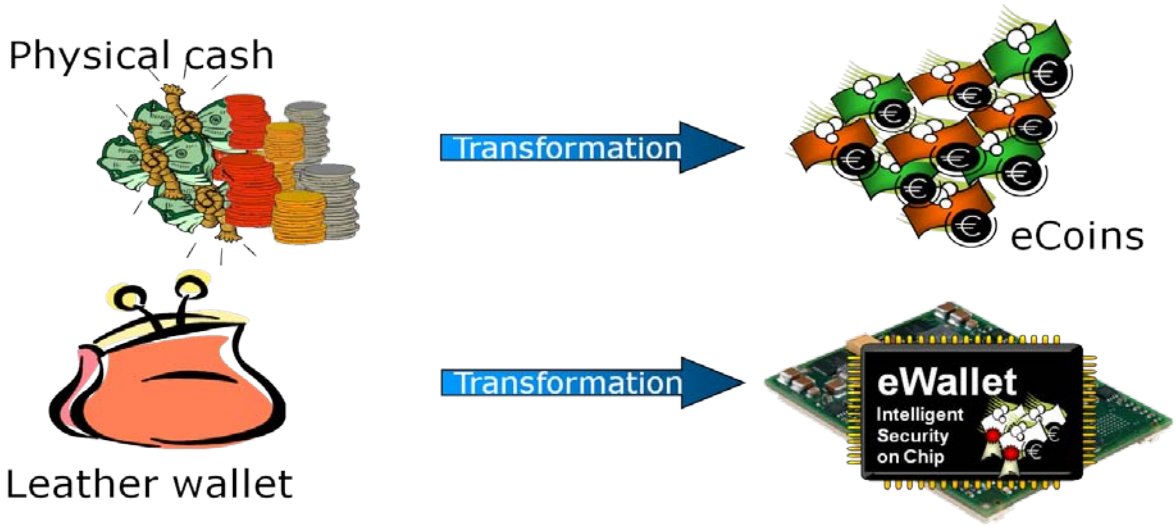

Abbildung 2: Äquivalenz von physischem und digitalem Bargeld.

1 [fairCASH digitales Bargeld: Internet-tauglich, anonym, peer-to-peer/offline und unbegrenzt transferabel]

Inhaltsverzeichnis

Executive Summary fairCASH Thesis

Digitale Bargeldsysteme kombinieren 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. Eine zentrale wirtschaftliche Forderung ist dabei die Umlauffähigkeit, auch als **Transferabilität** bezeichnet, die „offline" in direkter Weise geschieht. Dies steht in scheinbarem Widerspruch zum Problem der Entstehung und Verwendung von Münz-Kopien, dem „Multi-Spending". Zur Auflösung dieses Konfliktes verwenden fast alle bisherigen Verfahren das Prinzip der konditionierten Anonymität von Einweg-Token-Systemen, das die Identität des Besitzers zum festen Bestandteil einer jeden solchen digitalen Münze macht. Grund: Sollte eine solches eCoin mehrfach verwendet werden, lässt sich die Identität des Besitzers rechtlich eindeutig ermitteln. Die Probleme so einer Lösung sind jedoch die damit verbundenen Konsequenzen bezüglich Anonymität und Transferabilität, weil wesentliche Bargeld-Eigenschaften verloren gehen. Solche, bislang physischem Bargeld vorbehaltene, Eigenschaften ließen sich bis heute technisch für elektronische Token **nicht** realisieren.

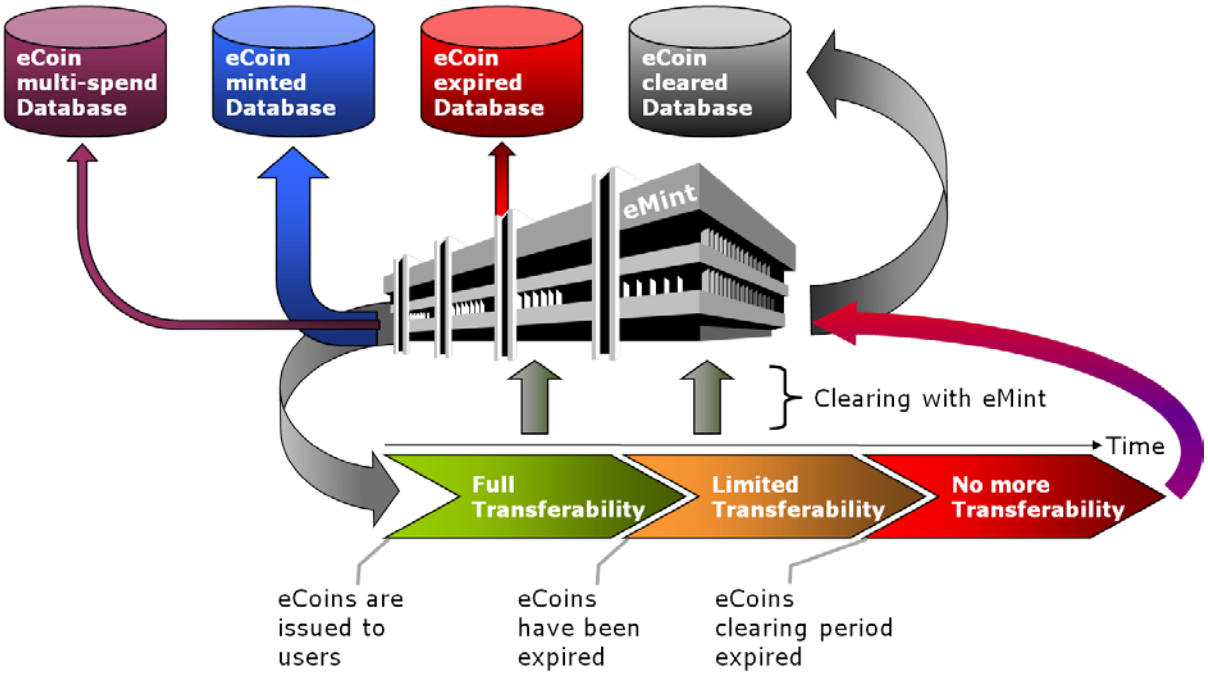

Abbildung 3: Übertragbarkeits-Phasen-Modell für eCoins.

Digitales Bargeld ist machbar

Die Dissertation "fairCASH based on Loss resistant Teleportation" zeigt, dass digitale Bargeld machbar ist. Die Aufgabe bestand in der Entwicklung eines Systemkonzepts für die Mehrweg-Token-System-Alternative, welche die meisten Eigenschaften physischen Bargelds in einem digitalen Medium wie dem Internet abbilden kann, insbesondere die essentiellen Eigenschaften der unbegrenzten Weitergabe und der Anonymität, ohne dass dafür Abstriche bei der Systemsicherheit in Kauf zu nehmen sind. Bargeld-artige Systeme ohne solchen Mehrwert erscheinen aus Anwendersicht wenig attraktiv.

Diese Dissertation wagt die These, dass sich die Versprechen des eCommerce der New Economy ohne die Einlösung ökonomischer Taxonomie-Faktoren eines mobilen, anwenderfreundlichen Bargeld-Systems nicht optimal erfüllen lassen. Im Blickfeld der Dissertation stehen die Voraussetzungen einer konkreten Machbarkeit digitalen Bargeldes mit den Eigenschaften seines physikalischen Pendants unter Verwendung heute verfügbarer Basistechnologien.

Eine zentrale Rolle spielt die Sicherheit. Hierzu wurde ein kopierfreies Transfer-Protokoll entwickelt, das die anonyme Übertragung elektronischer Münzen, so genannter eCoins, auf Peer-to-Peer-Basis in Form einer Teleportation ermöglicht und damit die gewünschten Bargeld-Eigenschaften verwirklicht: Jeder durch dieses Protokoll veranlasste eCoin-Transfers zeichnet sich dadurch aus, dass Münzen **bewegt**, aber **nicht kopiert** werden: Sie verschwinden beim Absender um dann beim Empfänger wieder zu erscheinen. Vorhandene unikative Eigenschaften bleiben erhalten. Elektronische Portemonnaies, so genannte eWallets, bilden als Chip-Tresore die Endpunkte der Bargeld-Übertragung und sichern sie physikalisch und kryptografisch gegen Analyse und Manipulation.

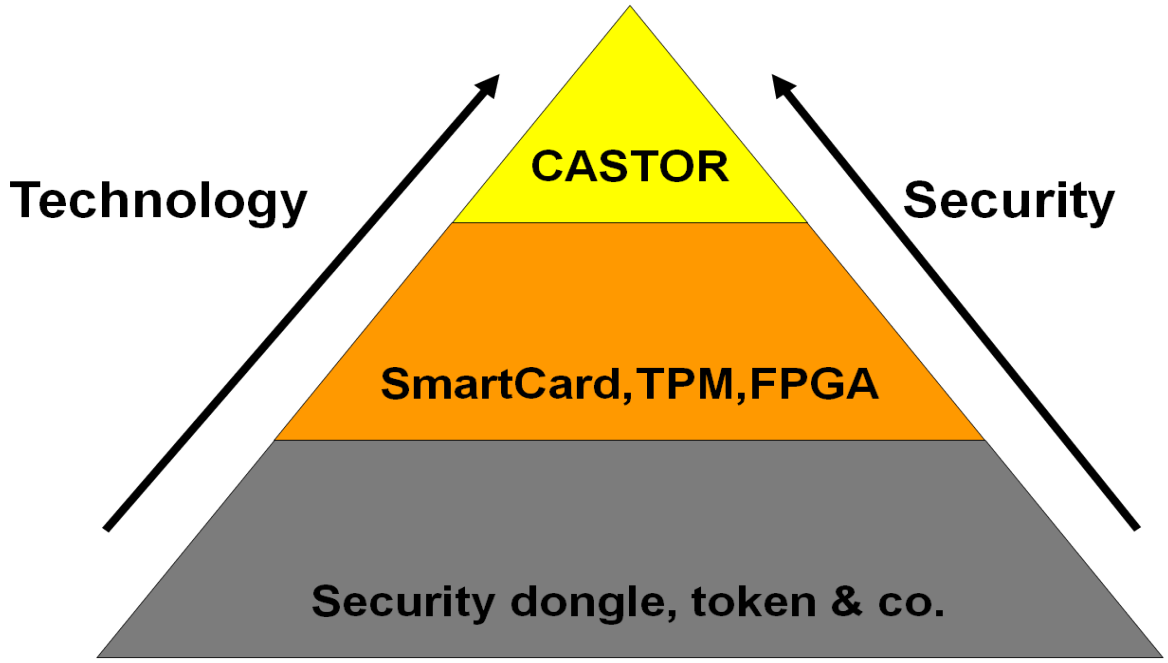

Abbildung 4: Sicherheitsgrade von Halbleiter-Systemen.

Der in dieser Arbeit vorgestellte Ansatz eines „CAsk for Storage and Transport Of access Restricted secrets" (CASTOR) realisiert das bekannte Prinzip eines **„Hardware Security Modules"** (HSM) oder **„Secure Elements"** (SE) auf neuartige Weise und reduziert so in Verbindung mit infrastrukturellen PKI-Architekturen ein komplexes Angriffsszenario auf wenige, beherrschbare Elemente. Dennoch verbleibt eine grundsätzliche Hürde, die als Status- bzw. Bestätigungsproblem in Erscheinung tritt. Dabei handelt es um ein algorithmisch nicht lösbares, fundamentales „common knowledge"-Paradigma bei verteilten Systemen, welches auch als **„coordinated attack problem"** bekannt ist und dann auftritt, wenn der Übertragungskanal *innerhalb eines kritischen Zeitfensters* zusammenbricht. Das ist in realen Übertragungssystemen grundsätzlich unvermeidlich. Dieses Problem wird als **„fair exchange Defizit"** verstanden und ist nicht nur technisch substanziell sondern auch wirtschaftlich signifikant. Transaktionen in (unterschiedlich regulierten) virtuellen (Rechts-) Räumen müssen mit allen verfügbaren technischen Mitteln und Methoden die Entstehung von Fairness-Defiziten vermeiden, besonders wenn sie „cross-boarder" realisiert werden sollen.

Das fairCASH-Lösungskonzept sieht für diesen Fall die offline durchzuführende gezielte Vernichtung betroffener Münzobjekte vor. Im Gegenzug konstruiert sie einen kryptografischen Verlustbeweis, der dann zu einem späteren Zeitpunkt jederzeit online gegen neue Münzen eingetauscht werden kann. Systemimmanente Sicherheitsmaßnahmen sorgen für eine missbrauchsfreie Nutzung.

Diese Aufteilung zum einen in die offline durchgeführte Münzweitergabe und zum anderen in die online durchzuführender Erstattung fehlerhafter Abbrüche kompensiert den Effekt, der als das Problem der "Byzantinischen Generäle" bekannt ist. Dabei handelt es sich um ein Problem der Übereinkunft, das historisch darin bestand, dass räumlich getrennte Heerführer einstimmig beschließen mussten, ob sie eine feindliche Armee angreifen oder nicht und dazu auf hin- und hergeschickte Boten angewiesen waren. Dieses Problem ist fundamental und besteht auch in der heutigen Telekommunikation. Der eigentliche Transfer wird als „delayed-true two-party fair exchange of eCoins for a receipt" bezeichnet.

Der Transportmechanismus

fairCASH umfasst als Sammelbegriff all das, worauf sich die zugrunde liegende Technologie anwenden lässt. Dabei geht es – einfach ausgedrückt – um ein Verfahren zum Transport nicht-stofflicher Wertdaten (Geheimnisse) über das Internet, und zwar erstens so, dass sie weiterhin Geheimnisse bleiben, und zweitens so, dass der Transport eine Teleportation und keinen Kopiervorgang darstellt. Hinter dem Begriff "Teleportation" (teles: fern, portare: überbringen) verbirgt sich ein sehr bekanntes (und einfaches) 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 sind hingegen **bisher** alle Transporte immer Kopiervorgänge, dafür erfolgen sie annähernd mit Lichtgeschwindigkeit. Weil die betroffenen Datenobjekte jedoch vervielfacht werden, handelt es sich NICHT um Teleportation. fairCASH kombiniert erstmals beide Transportprinzipien: Teleportation UND Lichtgeschwindigkeit und stellt damit einen Transportmechanismus für digitale Geheimnisse (eCoins) bereit.

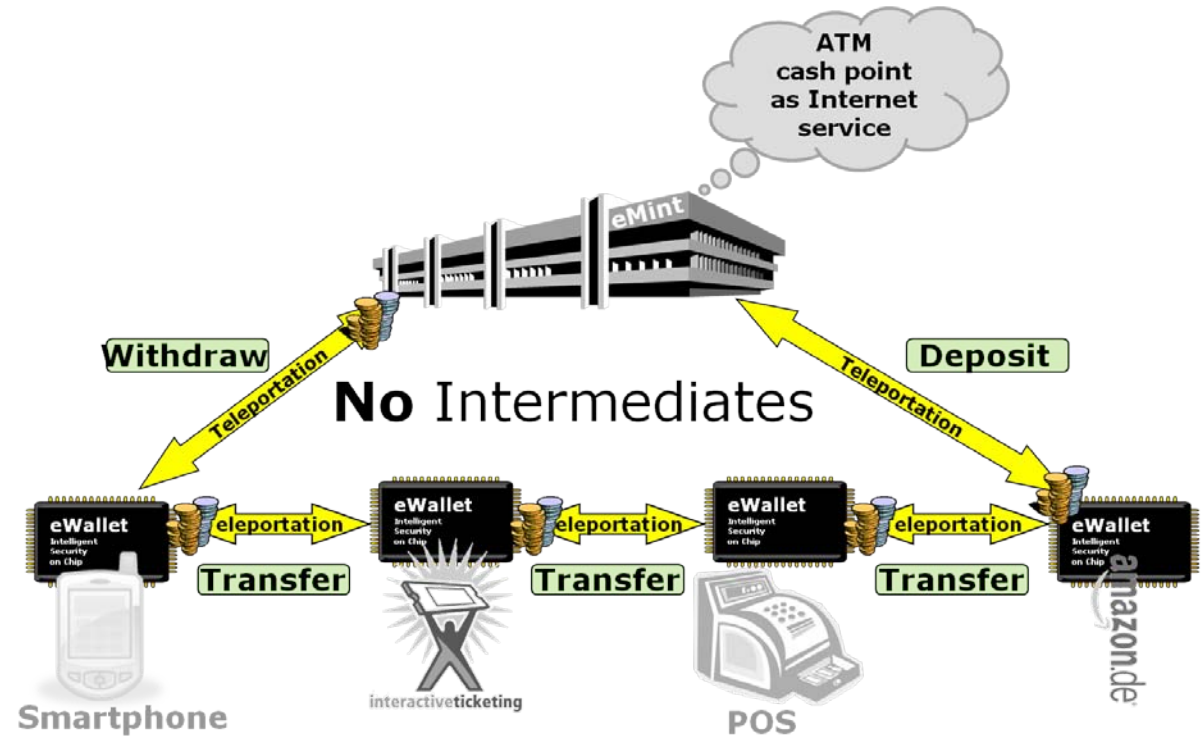

Abbildung 5: Direkte Übertragbarkeit von fairCASH-eCoins.

Nano-Tresore im Chip

Dass die Teleportation das Entstehen von Kopien verhindert ist notwendig, reicht aber für ein elektronisches Bezahl-System noch nicht aus. Denn es müssen nicht nur „reisende Geheimnisse" – auch "transiente Geheimnisse" genannt – sicher geleitet, sondern auch "persistente Geheimnisse" geschützt werden:
Der Bereitstellung eines sichereren stationären Zustands, also einer Ruheposition, die an dieser Stelle "persistentes Geheimnis" genannt werden soll kommt eine gleichgewichtige Bedeutung zu. Denn was nützt eine narrensichere Übertragung, wenn an einem der Endpunkte (vor oder nach einer Übertragung) das Geheimnis dennoch gelüftet werden kann? 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" 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 Geheimnisse ausreichend sicher 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 unbeeinflusst ablaufen kann.

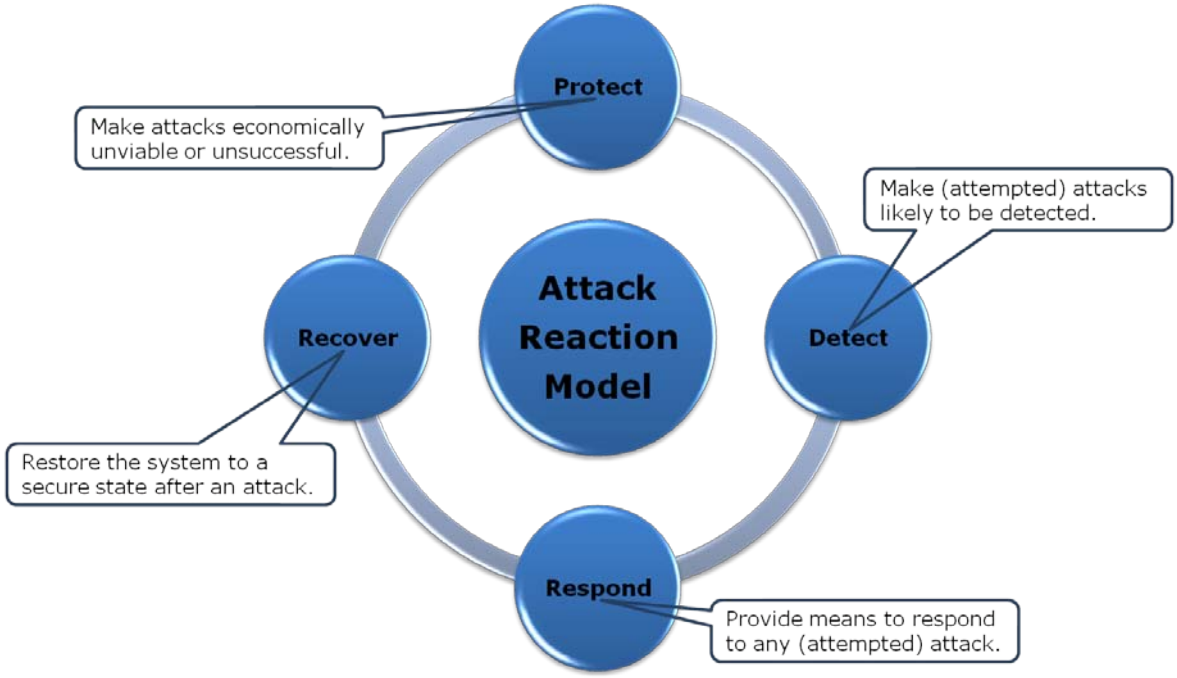

Abbildung 6: Zielsetzungen für Sicherheits-Prozesse im Risiko-Management.

Geheimnisverschiebungen

Nun gibt es also ein technisches Vehikel, mit dem ein Geheimnistransport auf den Straßen des Internets realisiert werden kann. Für die Erzeugung und das „in den Verkehr bringen" der digitalen Geheimnisse und für deren Erhalt ist bei fairCASH eine Institution namens eMint (elektronische Münzanstalt) zuständig. Dabei handelt es sich um so etwas wie eine Bundesdruckerei für Geheimnisse. Außerdem ist es erforderlich, Spielregeln und Vertrauen zu erzeugen. Dafür ist ein so genanntes Trustcenter, auch Certification Authority (CA) genannt, 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 auch vom neuen deutschen Personalausweis (nPA) genutzt wird.

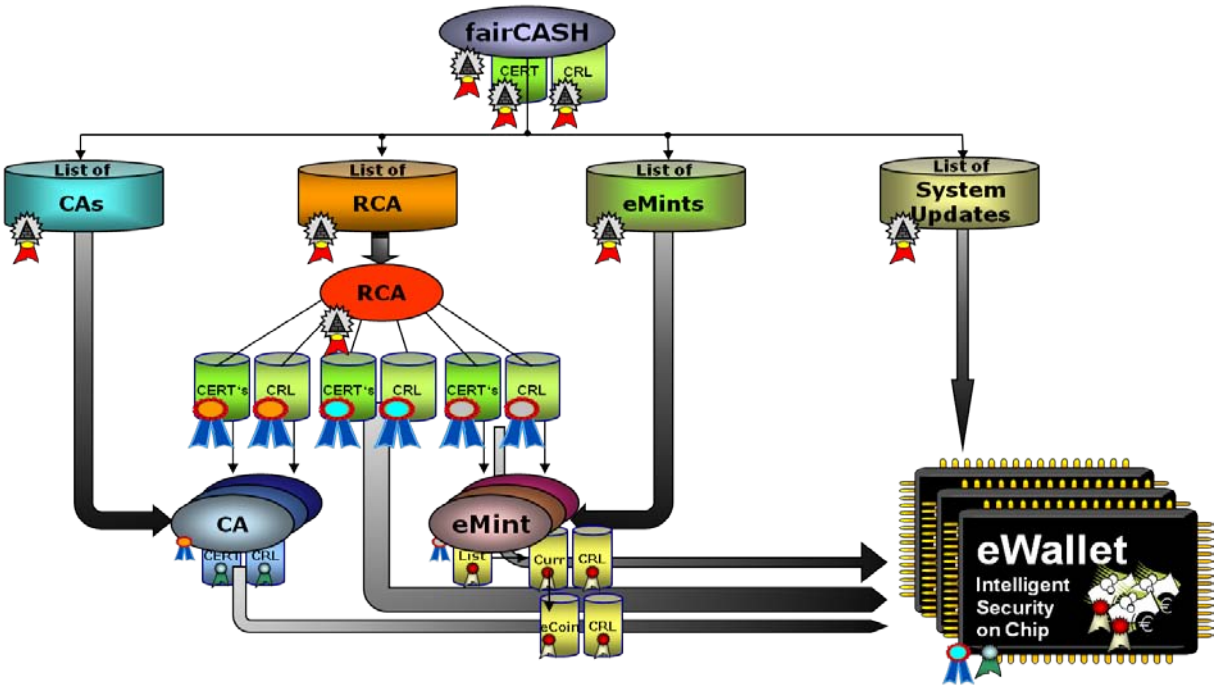

Abbildung 7: Hierarchische Public-Key-Infrastruktur.

Digitales Bargeld

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

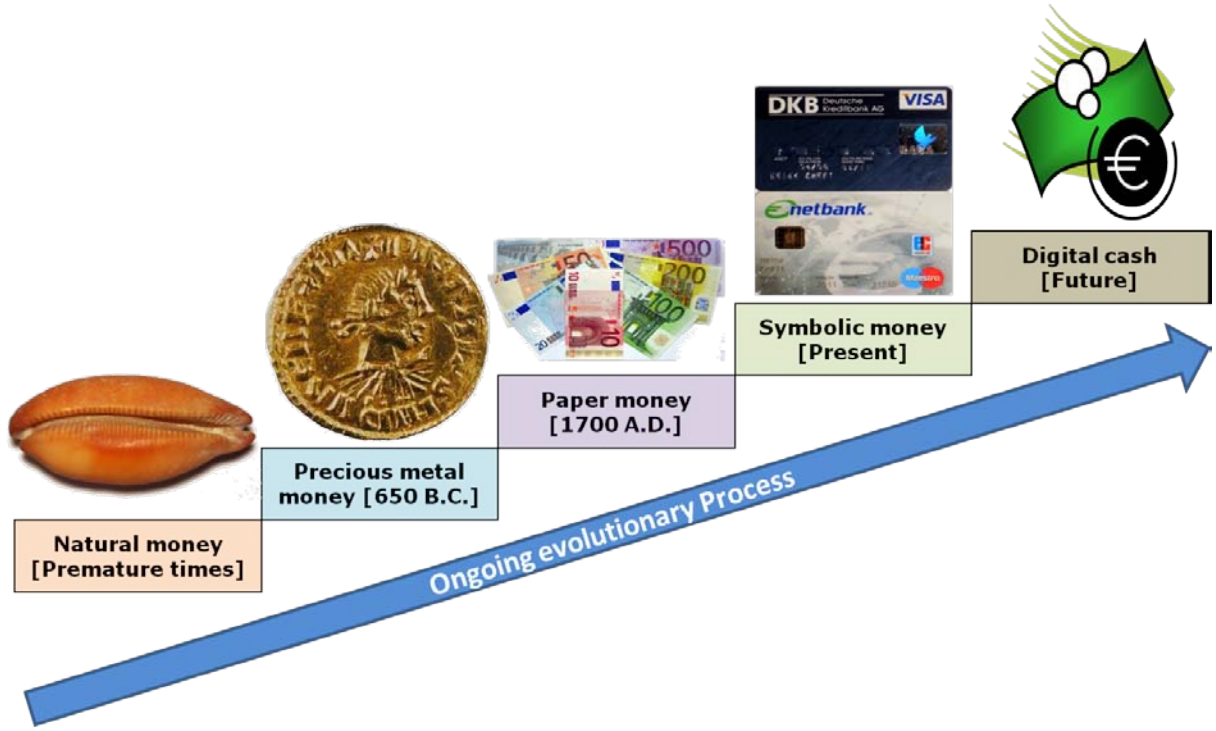

Abbildung 8: Evolution der Zahlungsinstrumente.

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

- Zentralbankgeld[1] (Bargeld),
- Giralgeld[2] (Buchgeld) und
- elektronisches Geld (eGeld).

Dabei wird die Notenbankgeldmenge aus dem Bargeld und den Giroguthaben 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.

Mehr nicht. In diesen beiden Begriffskategorien lassen sich technisch sämtliche existenten Geldkonzepte unterbringen.

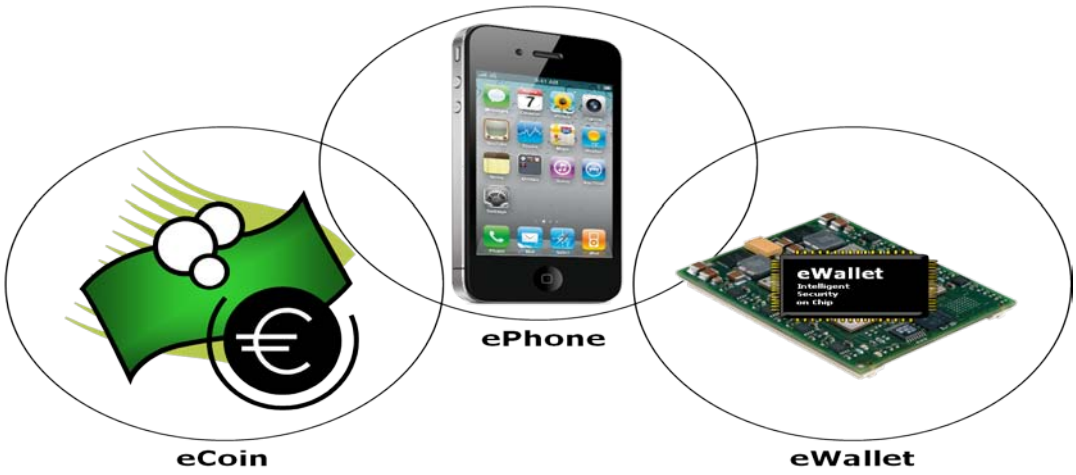

Abbildung 9: Protagonisten des fairCASH basierten digitalen Bargeldes.

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 etwa die Geldkarte vom ZKA[3] oder hierzulande weniger bekannte Systeme wie Edy, Suica, M-PESA oder Obopay. Systeme auf der SMS-Basis 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 meistverwendete 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 verschiedenste Versuche gegeben, daran etwas 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[4] einen Kundenwert erbringen zu können.

---

[1] Vielfach auch als Geldmenge M0 bezeichnet.
[2] Summe der Sichteinlagen (M1), der Spareinlagen (M2) und der Terminaleinlagen (M3).
[3] 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 Interessenvertretung.
[4] 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 realisiert Digitales Bargeld – für wen?

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

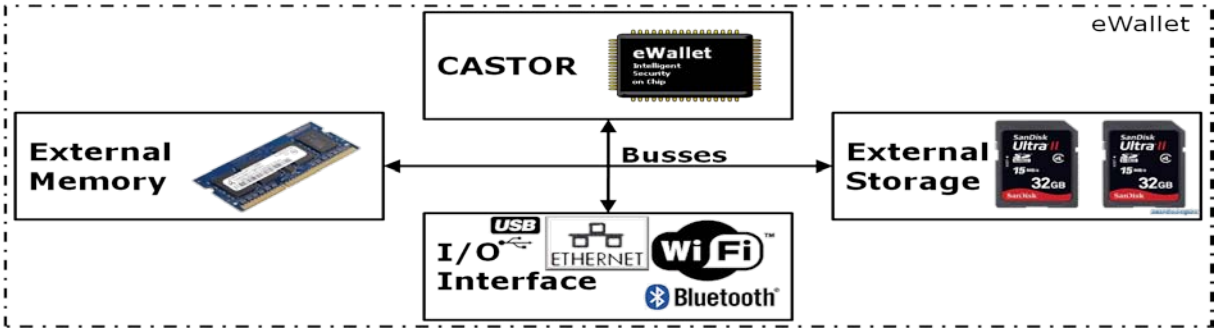

Abbildung 10: Komponenten einer elektronischen Geldbörse (eWallet).

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 „elektronic 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 Bargeldverfahren. Das mag auf den ersten Blick verwundern weil Anwender keine „Rechnung" für die Benutzung von Bargeld erhalten, das also kostenfrei zu sein scheint. 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, was auch der Fall ist, wie die Dissertation belegt. Ein nicht sonderlich nachhaltiger Effekt unserer Gesellschaft ist, dass sie akzeptiert, einen wachsenden Kostenanteil allein für die Abwicklung der Bezahlung zu bezahlen, sei es für Grund-, Kontoführungs-, Überweisungs- oder Transaktions-Gebühren. Die wenigsten Kreditkarten-Benutzer wissen wahrscheinlich, dass die meisten Anwendungen (etwa das Gros der Zahlungen im Internet) real 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 gerade 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** aus, da vom Initiator des Geldtransfers Transaktionskosten verlangt 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: Ist das denn überhaupt (in jedem Fall) erforderlich? Könnte man nicht einen Großteil dieser Leistungen einfach durch einen systemimmanenten Wechsel der Basistechnologie effektiver gestalten? Darüber hinaus ist es nicht sonderlich fair, auch Nichtnutzer zur Finanzierung eines Geschäftsmodelles heranzuziehen. Die Bankenbranche hat aber genau dies geschafft: Es gibt ein Gesetz in Deutschland, das es verbietet, einen Aufschlag für Zahlungen mittels Kreditkarte zu erheben, selbst wenn sich nicht alle immer daran halten (etwa diverse Billig-Flug-Linien). Damit sind also die Kosten für eine Kreditkartenzahlung bei den teilnehmenden Akzeptanzunternehmen in die Dienstleistungen und Waren bereits eingepreist[5].

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

Modalitäten von Zahlungssystemen

Ein näherer Blick auf das Business-Modell eines typischen Zahlungssystems ist lohnenswert. Prinzipiell sind Zahlungssysteme Unternehmungen, und die müssen für deren Betreiber einen Gewinn abwerfen. Doch darum geht es nicht primär. Es geht vielmehr um die Frage, wie ein Unternehmen das das macht und wie teuer das für dessen Kunden letztlich wird, zumal eine Vollkostenrechnung nur selten einfach zu bewerkstelligen sein dürfte. Flatrate- und Pay-per-Use-Modelle stellen bei solchen Betrachtungen die beiden „Antipoden" der möglichen Basisabrechnungs-Modelle dar. So könnte man das Euro-System als ein per Regulierung festgelegtes Flatrate-System interpretieren, wobei über die Intensität der individuellen Nutzung noch der jeweils bei Bargeld systemimmanente Zinsverlust hinzukommt. Die meisten anderen Modelle (fairCASH ebenfalls) 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 teueren Bargeld-Schnittstelle "Geldautomat") sowie Konto-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. Eine Alternative wäre eine Flatrate bei privater Nutzung für einen konkreten Zeitraum, mit dem dann das „All-you-can-eat"-Prinzip verbunden wäre. Machbar wäre dies jedoch nur dann, wenn die Mehrzahl der Transaktionen eines solchen Systems real keine Betriebskosten verursachen würden. 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 ist bei fairCASH substantiell geringer als bei einem physikalischen Bargeldverfahren (und im eGeld-Vergleich sowieso).

Allen dirigistischen (kontobasierenden) Verfahren ist prinzipbedingt der Machttransfer der Anwender an den „Man in the Middle" systemimmanent. Dies könnte den einen oder anderen an die Stimmrechtsübertragung der Einzelaktionäre an den Fondverwalter eines Aktiendepots erinnern. Egal ob da über die Verwertung von persönlichen SWIFT-Daten scheingefochten oder fundamental reguliert wird, um Eigeninteressen durchzusetzen: **Zentralistische Systeme werden meist missbraucht.** Sie stehen darüber hinaus auf der Top-Ten-Liste von Hackern und ziehen diese ähnlich an wie Nektar die Bienen (Honey-Pots). So werden etwa Kontodaten gleich in Millionenanzahl von Kriminellen geraubt (und die Geschädigten erfahren es meistens erst dann, wenn es bereits zu spät ist). 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 einem 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….

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, so können sich langfristig systemrelevante Zentralsysteme hin zu vitalen, gesunden und verteilten Strukturen entwickeln. So, wie das Internet Backbones, Hochleistungsserver und Service-Wolken zu einer funktionalen Mischung zusammenfügt, würde auch die Rückführung der unter ihrer systemimmanenten Wichtigkeit fast zusammengebrochenen Finanzinstitutionen zu einer fundamentalen ökonomischen und soziologischen Stabilisierung führen können (Stichwort Systemrelevanz).
Mit einer eMint vollständig im Besitz 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 Entwicklungshistorie

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

Generation I: [1990]
Im Internet bedarf es besonderer elektronischer Bezahlmethoden und Systeme, damit die Geschäfte in Gang kommen können. Es wurden sowohl reine Softwaremodelle (eCash von David Chaum und Brands Cash von David Brands als auch Portemonnaie-basierte Verfahren (Mondex von MasterCard) ausprobiert. Es wurde 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 Generation I Systeme sind gescheitert. Die Gründe hierzu sind vielfältiger Natur, wie die Dissertation belegt. Zusammenfassend lässt sich allerdings sagen, dass sie essentielle Bargeldeigenschaften nicht besaßen. Nun werden im Internet unbare Zahlungsverfahren wie Kreditkartenzahlung, Scheckeinreichung, Lastschriftverfahren und Überweisungen möglich. Aus der Perspektive der Kreditwirtschaft ist dies nachvollziehbar: der unbare Zahlungsverkehr ist schon seit Jahren vollständig EDV-gestützt und man bemüht sich, den Point-of-Sale über das electronic cash-Verfahren 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 ausmachen wird, umfasst vom Potential her als spektakulärste Innovation „digitales 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 immer stärker besser adaptierte Mechanismen erforderlich – vor allem im Zusammenhang mit digitalen Leistungen und Gütern, welche direkt über elektronische Netzwerke ausgeliefert werden. Hier sind neue Mechanismen notwendig, die eine unmittelbare Bezahlung zulassen.

Operatives Geschäftsmodel bei fairCASH

Die systemische Leistung, das in den Verkehrsumlauf bringen von Bargeld, dessen Verknüpfung mit dem Giralgeld-Kreislauf und umgekehrt das „Wieder-aus-cachen" 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**. Nicht das Management von Zahlungen im Spannungsfeld von Zahlungssystem-Anwendern und -Anbietern steht im Vordergrund, sondern das eigenständige Agieren, Betreiben und Anbieten eines Bankgeschäftes.

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

1. **Flatrate-Nutzungsgebühr für private Anwender**
   Benutzer von fairCASH benötigen für den Betrieb Ihres eWallets ein Nutzungszertifikat. Dieses ist für private Nutzer i.d.R. anonym und kann anonym online erworben werden. Vor dem Ablauf des Gültigkeitszeitraumes kann der Nutzer eine Verlängerung seiner Nutzung veranlassen bzw. nach Beendigung ein neues Zertifikat erwerben. Ohne gültiges Nutzer-zertifikat ist ein eWallet nur noch imstande, das in ihm gespeicherte Geld an die eMint zur Auszahlung zu transferieren, nicht aber weiterhin mit dem Geld offline zu bezahlen.

2. **Umsatzorientierte Nutzungsgebühr für kommerzielle Anwender**
   Ein geschäftlich agierender Anwender kann aus naheliegenden Gründen nicht anonym agieren. Er benötigt daher ein identifiziertes Nutzungszertifikat für sein eWallet. Hier wird eine dem Cashflow adaptierte prozentuale Nutzungsgebühr fällig.

3. **Verkauf von eWallets**
   eWallets werden benötigt, um nutzend am fairCASH System teilzuhaben. Ob dies nun separate Geräte sind, die sich über Draht- oder Funkschnittstellen mit einer Bediensoftware (a.k. Terminal) verbinden, oder um integrierte Anwendungen (beispielsweise in ein Mobiltelefon integriertes Portemonnaie), ist für die Nutzung nicht von Relevanz. Da aufgrund von Sicherheitsüberlegungen eWallets nicht unbegrenzt lange nutzbar sein werden, ihre operative Lebensdauer[6] daher konstruktiv begrenzt ist, kann auch durch den kontinuierlichen Verkauf von eWallets ein entsprechender kalkulatorischer Gewinn in der Wertschöpfungskette entstehen.

4. **Zinsgewinne**
   Bargeld auf €urobasis kann über den EURIBOR[7]-Zinssatz ohne Risiko verliehen werden. Die eMint nimmt diesen Zinsgewinn ein.

5. **Abschreibungen (Write-offs)**
   Kommt es bei Bargeld zur Vernichtung, ohne das im Nachhinein ein Besitz bewiesen werden kann, so ist dieses Geld unwiderruflich verloren und führt somit zur Deflation der ausgegebenen Geldmenge. Die eMint kann nach dem Ablaufen der Gültigkeit der entsprechenden Münzgeneration diese Wertmenge für sich verbuchen.

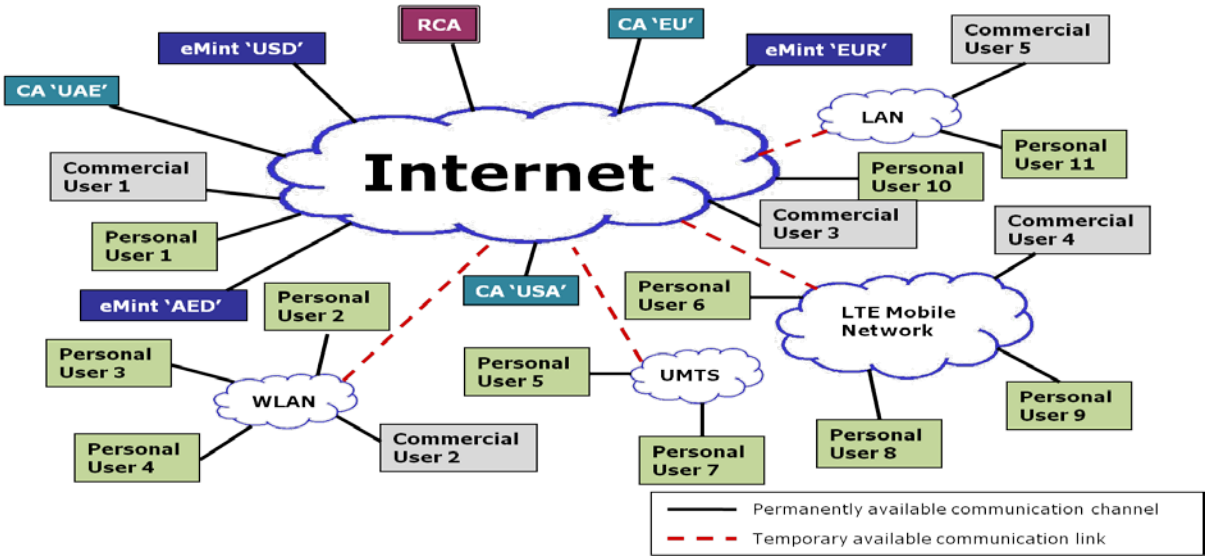

Abbildung 11: Ausbreitungspfade für eCoins im Netzwerk.

Geldschöpfungsgewinne (sogenannte Seignorage-Profite) können auf Dauer nur von einer Zentralen Bank erwirtschaftet werden, da aufgrund der Endlichkeitsfiktion alle anderen Betreiber spätestens am Ende Ihrer Geschäftstätigkeit sämtliche eCoins wieder in den Giralgeldkreislauf rückinjizieren müssen.

[6] Das optimale LifeCycle Management liegt etwa zwischen 3 und 5 Jahren nach der CASTOR Chip Herstellung.
[7] http://de.euribor-rates.eu/.

Lizenzgeschäft für den Technologie-Provider

Die Technologie-Vermarktung des IP von fairCASH manifestiert sich über das Modell eines Patent-Lizenzvertrages mit den Lizenznehmern. Dabei kommen unterschiedliche Formen einer Lizenzierung in Betracht, so etwa auch der Verkauf von eWallet-Chips.

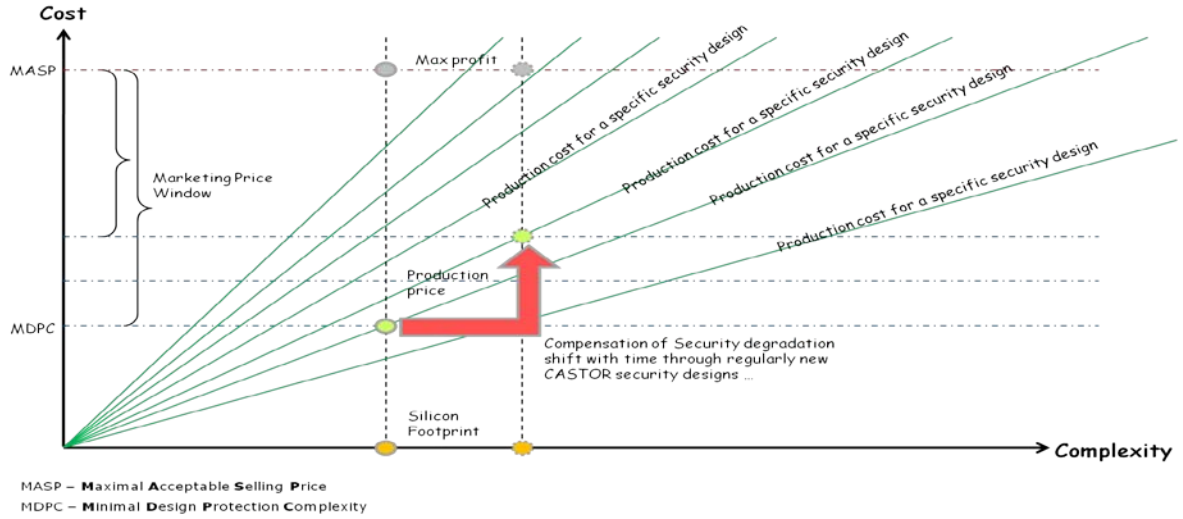

Abbildung 12: Preismodell-Fenster für CASTOR-Chips im Kosten-Komplexitäts-Zusammenhang.

Virales Marketing

Als sogenanntes Netzgut unterliegt fairCASH der kritischen Masse, auch als Henne-Ei Problem bekannt. Neben einer Vielzahl von bekannten Maßnahmen, bei denen es um die möglichst schnelle Durchdringung der operativen kritischen Masse geht, sind sogenannte virale Marketing-Mechanismen seit einigen Jahren beliebt geworden. Aus technischer Sicht bietet fairCASH alle Möglichkeiten, um ein virales Modell anzustoßen.

So könnte beispielsweise der Gutschein-Mechanismus dazu verwendet werden, einem bisher fairCASH-losen Nutzer ein Startguthaben zukommen zu lassen, welches er sich nur mit einem eigenen eWallet abholen kann. Durch Marketing-Maßnahmen ließen sich mitgliederstarke Vereinigungen von technikaffinen Mitgliedern mit eWallets ausstatten.

Werbe-Einblendungen auf Internet-Seiten ließen sich schon mit kleinen eCoin-Beträgen als „Giveaways" zur Steigerung der Akzeptanz und zur viralen Verbreitung des fairCASH-Systems nutzen, weil nur ein eWallet diese Beträge summiert kann.

Die effiziente Unterdrückung von SPAM wird mit fairCASH möglich. Fügt man jeder versendeten eMail einen Betrag von einem Cent bei, so ist dies bei normaler Nutzung weder ein finanzielles Problem, noch laufen effektiv große reale Kosten auf. Diese Überlegung basiert auf der Annahme, dass sich das Versenden und Empfangen von nützlicher eMail sich in etwa die Waage hält. Somit ist die resultierende Rotation (Wirbeldichte) praktisch Null. Massenwerbesendungen würden aufgrund ihres einseitigen Charakters für den Versender entweder richtig teuer (kein Cash-Reflow) oder eben nicht mit Geld bestückt. Dies ließe sich als Filterkriterium verwenden.

Wie starten

Das fairCASH-System könnte direkt dem Markt zwar als konkurrierendes Zahlungssystem angeboten werden. Aus vielen Gründen ist dieser Weg als relativ unpraktisch zu bewerten: Das hängt einmal mit dem Zeitfaktor zusammen, den es braucht, um auf diesem Weg „über den Rauschteppich" hinaus zu wachsen. Darüber hinaus dürfte es einem Startup mental schwer fallen, sein technologisches Geschäft mit den operativen Erfordernissen eines Bank-Business verknüpfen zu müssen. Da ist es vielleicht sinnvoller, einen Partner zu suchen, der bereits operative Erfahrung im Geldgeschäft besitzt und darüber hinaus mit Problemen konfrontiert ist, Stichwort: Micro-Payment[8], zu deren Lösung fairCASH etwas beitragen könnte.

Eines dieser Probleme lässt sich bei den Printmedien identifizieren. Die Art und Weise, wie Online-Medien heute arbeiten, spiegelt stark die Art und Weise der Papier-Phase wieder. Dies ist durchaus typisch, denn Menschen versuchen immer erst einmal auf dem Stand weiterzuarbeiten, den sie gewohnt sind. Online-Medien werden in Zukunft jedoch nicht länger so aussehen, wie ihre Print-Vorläufer (Stichwort: Entbündelung, aka iTunes bei Musik). Vermutlich werden, ja müssen, journalistische Dienstleistungen in Zukunft auf einer per-Artikel Basis vermarket werden, um deren Qualität auch im Internet-Zeitalter zu sichern. Hier werden Suchmaschinen einen wesentlichen Faktor darstellen. Es muss aber gelingen, die Bezahlwährung "Werbung" aus dem Spiel zu nehmen. Dies könnte den Produktionsprozess journalistischer Inhalte wieder einen klar erkennbaren Wert zuweisen, indem ein für alle einfach nutzbares Zahlsystem integriert wird, das ohne Registrierung, ohne PIN und TAN, anonym, ohne transaktionsbedingten Schwund und mit einem Doppelklick auf den Artikel führt. Das jedoch ist mit den heutigen Systemen technisch nicht darstellbar. fairCASH als technologische Innovation könnte hier Abhilfe schaffen.

So eine Unternehmung würde darüber hinaus gesellschaftlichen Zusatznutzen schaffen, da ein solches System sozio-ökonomische und sozio-kulturelle Strukturbrüche weitgehend vermeidet. fairCASH könnte auf gute Weise die Profit- u. Gewinnmaximierung besser ausgestalten, und so die „Regeln des Spiels" neu definieren. Bestehende „old Economy" basierte Finanztransaktionssysteme im Internet könnten durch eine überlegene technologische Innovation ersetzt werden.

Ein institutioneller Investor könnte fairCASH in dem Technologieprozess unterstützen, die Entwicklung in den politisch, ökonomisch und sozio-kulturell geprägten Kontext einzufügen und damit zu einem globalen Prozess zu machen. Interessen einer Kapitalverwertung manifestieren sich dann vor allem in den Mechanismen einer strukturellen Finanzökonomisierung im Fokus methodisch wirksamer technischer, sozialer und politischer Kriterien. Weitere potentielle fairCASH-Anwendungen könnten sich aufgrund der anderen Kosten-Struktur von fairCASH in den nachfolgend genannten Bereichen etablieren:

- Journalistischer Paid-Content,
- Pay-per-View- und Pay-TV Systeme,
- Elektronische Lohntüte,
- Online-Spiele,
- Taschengeld,
- Glücksspiele,
- Familiengeld (Sozialgeld),
- Intelligente Stromzähler,
- Elektromobilität,
- Abrechnung von Cloud-Services,
- Help-Desk-Anwendungen,
- Internet-Versteigerungs-Plattformen,
- Internet-Partner-Börsen,
- Interaktive TV-Angebote (Mitmach-Fernsehen),
- SPAM-Filter[9],
- Spendensysteme, etwa für Wikileaks,
- u.v.a.

Eine Ausgestaltung der „Early Adopters" liegt vermutlich bei den privaten Anwendern von Android, Black-Berry und iPhone sowie bei ausgesuchten Infrastruktur-Providern im Internet und Öffentlichen (Nah) Verkehr vor.

[8] Formal handelt es sich um Meso-/Makro-Payment, da Beträge kleiner 1 €urocent nicht sinnvoll erscheinen.
[9] Sinnvolle eMail wird mit einem Cent „bestückt", SPAM kommt ohne Wert.

Populäre eGeld-Systeme

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

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

Ein paar untersuchte auch in Deutschland verfügbare 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
SEPA	- **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/

Presentation materials are published on the above website.