

28

PROPOSTA DE METODOLOGIA PARA ESTIMULAR A ADOÇÃO DE  
PRODUTOS INOVADORES PELO MERCADO PRINCIPAL, O PÚBLICO  
COM PERFIL MAIS CONSERVADOR:

CASO DE SISTEMAS DE MEIO DE PAGAMENTO ELETRÔNICO

**Banca examinadora**

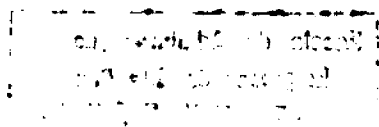
Orientador: Prof. Dr. Marcos Henrique Nogueira Cobra

Prof. Dr. \_\_\_\_\_

Prof. Dr. \_\_\_\_\_

Prof. Dr. \_\_\_\_\_

Prof. Dr. \_\_\_\_\_



**FUNDAÇÃO GETULIO VARGAS**  
**ESCOLA DE ADMINISTRAÇÃO DE EMPRESAS DE SÃO PAULO**

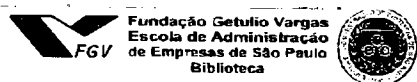
**LEOPOLDO CSILLAG**

**PROPOSTA DE METODOLOGIA PARA ESTIMULAR A ADOÇÃO DE  
PRODUTOS INOVADORES PELO MERCADO PRINCIPAL, O PÚBLICO  
COM PERFIL MAIS CONSERVADOR:**

**CASO DE SISTEMAS DE MEIO DE PAGAMENTO ELETRÔNICO**

Tese apresentada ao Curso de  
Pós-Graduação da FGV/EASEP  
Área de Concentração: Mercadologia  
como requisito para obtenção de título de  
doutor em administração.

Orientador: Prof. Dr. Marcos Henrique Nogueira Cobra



500/2000



1200000600

**SÃO PAULO**

**2000**

Escola de Administração de Empresas da São Paulo	
Data	658.8 C958p
Tombo	Tese V.I e. 12

CSILLAG, Leopoldo. Proposta de metodologia para estimular a adoção de produtos inovadores pelo mercado principal, o público com perfil mais conservador:

o caso de sistemas de meio de pagamento eletrônico.

São Paulo: EAESP/FGV, 2000. (Tese de Doutorado apresentada ao Curso de Pós-Graduação da EAESP/FGV, Área de Concentração: Mercadologia).

Resumo: Apresentação de uma metodologia sistêmica para abordar o mercado principal com vistas à adoção deste de sistemas de meio de pagamento eletrônico; um produto com inovações de tecnológicas e de conceito.

Palavras-Chaves: Adoção de Tecnologia, Mercado Principal, Meio de Pagamento Eletrônico, Comércio Eletrônico.

## ÍNDICE

<b>1. Introdução .....</b>	<b>1</b>
<b>2. Internet .....</b>	<b>4</b>
<b>3. Comercio Eletrônico .....</b>	<b>9</b>
<b>4. Meio de Pagamento Eletrônico .....</b>	<b>34</b>
<b>5. Difusão de inovações .....</b>	<b>234</b>
<b>6. Objetivo .....</b>	<b>257</b>
<b>7. Justificativa .....</b>	<b>258</b>
<b>8. Delimitação do Tema .....</b>	<b>259</b>
<b>9. Hipóteses .....</b>	<b>260</b>
<b>10. Metodologia .....</b>	<b>261</b>
<b>11. Resultados da Pesquisa de Campo .....</b>	<b>270</b>
<b>12 Avaliação sob o Enfoque Sistêmico das Causas de Resistência à Adoção de Meios de Pagamento Eletrônico pelo Mercado Principal .....</b>	<b>290</b>
<b>13. Elaboração das Ações Necessárias .....</b>	<b>315</b>
<b>14. Metodologia Proposta .....</b>	<b>331</b>
<b>15. Conclusão .....</b>	<b>336</b>
<b>16. Bibliografia .....</b>	<b>338</b>
<b>17 Anexos .....</b>	<b>365</b>



Agradeço

a meu pai João Mario Csillag

pelo incentivo e exemplo.

## **I. Introdução**

Há momentos em que o mundo experimenta uma revolução tecnológica que muda a maneira como as pessoas vivem e interagem. Na antiguidade, houve o surgimento da agricultura, da irrigação e da engenharia civil. Estes desenvolvimentos levaram à criação das cidades e da cultura urbana. Na época medieval houve a invenção da imprensa, possibilitando a realização de livros, revistas, jornais. No início dos tempos modernos, com a Revolução Industrial, surgiram novas áreas da ciência, novas invenções. A tecnologia progrediu então dramaticamente após a metade do século XIX com o surgimento do telégrafo, telefone, rádio, automóveis, aviões, televisores, satélites e do computador. Estas invenções foram surgindo cada vez mais rapidamente, num avanço exponencial do desenvolvimento tecnológico.

Atualmente vive-se um momento de revolução tecnológica que tem propiciado mudanças velozes na sociedade, principalmente em virtude da tecnologia digital, dos computadores, da Internet e do comércio eletrônico. É a Era Digital.

Hardware e Software tem tido preços acessíveis e meios de distribuição abrangentes tornando-se presentes em todos os segmentos da vida, o que potencialmente precede uma revolução (DERTOUZOS, 1997). O encontro da informática com os sistemas de comunicações, analisado por YOFFIE e CUSUMANO (1998) vem atingindo o mercado com preços baixos, buscando meios de distribuição mais agressivos e possibilitando a comunicação entre os computadores de maneira mais intensa.

Com esse cenário várias previsões foram lançadas, em parte baseadas no que já vinha acontecendo.

Os computadores interconectados globalmente, formarão uma rede que está sendo chamada de estrada da informação. Um precursor direto é a Internet atual. [...] Não está longe o dia em que você poderá realizar

negócios, estudar, explorar o mundo e suas culturas, assistir a um grande espetáculo, fazer amigos, freqüentar mercados da vizinhança e mostrar fotos a parentes distantes sem sair de sua escrivaninha ou de sua poltrona. Ao deixar o escritório ou a sala de aula você não estará abandonando sua conexão com a rede. Ela será mais que um objeto que se carrega ou um aparelho que se compra. Será seu passaporte para uma nova forma de vida, conectada. (GATES, 1995).

Nesta Era Digital, um componente significativo que deverá ocasionar grandes transformações na sociedade é o comércio eletrônico. As suas implicações na sociedade, seus efeitos e resultados possuem um potencial transformador (COMMERCENET, 1998).

Essa nova perspectiva de comunicações e interação baseada na possibilidade de informatização das informações e das comunicações, propicia a existência de agentes novos na economia que DAVIS e DAVIDSON (1993) chamaram de comerciantes *infomediários* que são empresas que usam as várias formas e funções da informação para aproximar compradores e vendedores, eletronicamente. Esses comerciantes também podem aproximar produtores de consumidores, os que estão no começo ou no fim da cadeia de produção, fornecedores e usuários, e remetentes e destinatários. Ao permitir que essas partes obtenham mutuamente informações melhores, e mais rápidas, eles criam um valor. Com o acesso cômodo e direto durante 24 horas por dia, eles permitem resultados em tempo real para atender as necessidades do consumidor. Os infomediários são superiores aos intermediários tradicionais, que oferecem serviços mais caros, mais demorados e limitados. Eles proporcionam uma variedade maior de opções do que os serviços tradicionais, porque concentram informações inexistentes em qualquer outra fonte. Em lugar de providências numerosas e demoradas, cuidam do pedido, processamento e transação, tudo ao mesmo tempo. Facilitam os negócios personalizados e podem prever resultados de qualquer seleção ou decisão. Os intermediários informatizados, criarão e oferecerão esses serviços a todos os interessados, daqui a uma geração.

Aqueles que não se informatizarem nesse prazo, com toda probabilidade fecharão suas portas.

Enquanto essas previsões são divulgadas, os números do comércio eletrônico tem provocado euforia, encorajando empresas a se arriscarem para conquistar essa fronteira ainda não explorada. Estudos divulgados pela COMMERCE NET / NIELSEN (1999) mostram que o mercado mundial já ultrapassava US\$ 5 bilhões em 1997, US\$ 62 bilhões em 1998 e 181 bilhões em 1999 .

O crescimento espetacular projetado é de US\$ 300 bilhões em 2001, conforme WTO (1998) referente ao comércio doméstico interno dos países. O comércio internacional, através de comércio eletrônico, deve ficar em US\$ 60 bilhões, gerado basicamente pelos negócios com os EUA. Outra previsão do mesmo estudo é que o comércio eletrônico deva abranger 2% de todas as transações comerciais até 2003. Segundo pesquisas da INTELLIQUEST (1997-1999), em junho de 1999 havia 91 milhões de usuários (empresas e pessoas físicas) na Internet nos EUA, um crescimento de 46 % sobre junho de 1998. Contudo, segundo a pesquisa citada do COMMERCE NET / NIELSEN (1999) somente 10 % dos usuários *web* compram regularmente pela Internet.

Como surgiu e o que é esse agente que está provocando essas alterações?

## II. Internet

A Internet é uma rede de milhares de computadores de diversos portes e capacidade de processamento distribuídos por todo o mundo.

Na verdade, é uma rede de redes, baseada em tecnologias de software que direcionam os computadores a enviarem, receberem e localizarem pacotes de informações que viajam por uma estrada mundial eletrônica. (YOFFIE e CUSUMANO, 1998).

CRONIN (1994) comenta que ela surgiu da necessidade de comunicação do departamento P&D, pesquisa e desenvolvimento, do complexo militar norte-americano que atuava como condutor de pesquisas para o governo, universidades e grandes empresas. Evoluiu de uma rede militar fechada com computadores de pesquisa para um grande fórum público de comunicação.

Começou como a ARPANET durante a guerra fria em 1969. Foi desenvolvida pelo Departamento de Defesa Norte-Americano (DOD) em conjunto com parceiros comerciais e universitários para explorar as possibilidades de comunicação em rede, que poderia “sobreviver” a um ataque nuclear. O projeto só teve continuidade porque o DOD e seus contratados comerciais e universidades perceberam que era uma maneira bastante conveniente de se comunicar (PARKER, 1997).

Na primeira década de existência a Internet, era utilizada basicamente para tráfego de correio eletrônico (e-mail), grupos de discussões, acesso à base de dados distante e atender as necessidades de trocas de arquivos entre agências governamentais, empresas contratadas e universidades. (DOUBA, 1995)

Durante o início da década de 1980, todas as redes de pesquisas interconectadas foram convertidas para o protocolo TCP/IP (o que permitia à todas as redes da Internet enviar e receber dados), e a ARPANET passou a ser a espinha dorsal (a conexão física entre as

principais redes) da nova Internet, que compreendia todas as redes TCP/IP conectadas à ARPANET. Essa conversão ao TCP/IP foi completada no final de 1983, e assim nasceu a Internet.

A adoção do TCP/IP foi uma das principais virtudes técnicas dessa rede pois permitiu à computadores não-similares comunicarem-se; e de um método de rotear as informações através de múltiplos caminhos alternativos, utilizando pacotes de dados com seus próprios endereços de destino e origem anotados. (DERTOUZOS, 1997 e STEVENS, 1994).

Essa evolução da rede com a existência de computadores com características técnicas diferentes, permitiu o desenvolvimento de aplicativos que facilitassem a comunicação (PARKER, 1997).

Além dessa característica técnica, motivada por necessidades militares, que possibilitou um crescimento rápido, por não impor grandes restrições nas características dos computadores que poderiam ligar-se à rede, existiram os motivadores desse crescimento.

MAGID, MATTHEUS e JONES (1995) observam que o desenvolvimento e utilização de programas aplicativos de comunicação como correio eletrônico (e-mail) e em 1990 com o desenvolvimento da parte gráfica (World Wide Web) com o HTML, (um protocolo de hipertexto que pode apresentar informações gráficas), por Tim Berners-Lee e com o surgimento dos browsers como Mosaic e seus sucessores, permitiram um verdadeiro crescimento no potencial de comunicação entre os usuários da Internet .

KROL (1994) comenta que a utilização desses sistemas tem permitido a analogia da “criação de um mundo virtual” onde os participantes podem fazer contatos com outras pessoas com interesses semelhantes.

Um levantamento que indica o crescimento do interesse público na Internet é o crescimento da cobertura da mídia sobre o assunto. Segundo ELLSWORTH (1994) em 1992 os jornais nos EUA tinham em média 3

artigos sobre Internet por mês, em 1993 já haviam aproximadamente 70 artigos por mês, em 1994 esse número já ultrapassava 300 por mês. Hoje (2000) é praticamente impossível encontrar qualquer grande jornal nos EUA ou no Brasil, ou qualquer revista de grande circulação, sem ter algum artigo ou reportagem sobre a Internet, produtos ou aplicações.

Os números de crescimento da Internet são incríveis. CRONIN (1995) conta que em 1995 já havia mais de 15.000 redes conectando mais de 38 milhões de pessoas, com uma taxa de crescimento de 15.000 pessoas por mês. Hoje além das várias estatísticas de utilização da Internet começam a surgir tentativas de censos. O primeiro grande desafio é medir o tamanho de um público em crescimento constante e bastante disperso. WINFIELD e STEWART (1999) diz que hoje não se tem conhecimento exato do número de usuários, mas levantamentos publicados em GLOBAL REACH (2000) indicam um número superior à 262 milhões.

A Internet tem um escopo global e é fortemente descentralizada, isto é, não há um organismo que a governe. As redes físicas que compõem a Internet formam uma hierarquia, na qual o nível mais alto é a rede estrutural de alta velocidade mantida pela MCI. A maioria do tráfego na Internet está afunilada e esta rede estrutural através de pontos de acesso da rede (NAPs), que são mantidos pela Sprint, MFS e outros e estão localizados em áreas metropolitanas estratégicas nos Estados Unidos. (KOSIUR, 1997).

A forma mais utilizável da Internet é a World Wide Web, ou mais conhecida como Web, que é um aplicativo da Internet. Aparentemente da noite para o dia, a Web transformou um cenário textual e sem graça da Internet em um mundo cibernético colorido permeado de oportunidades comerciais, artísticas e sociais (COMMERCE NET, 1997).

KALAKOTA e WHINSTON (1997, 1998) comentam que a Web é uma arquitetura global de compartilhamento de informações que integra vários servidores de informações de maneira rápida, fácil e barata. A Web é a sustentação de software sobre a qual novos aplicativos de comércio

eletrônico baseiam-se; é uma interface com o usuário utilizável com um mouse. Em termos de conteúdo, pode ser pensada como uma gigantesca biblioteca na Internet.

Pode-se dizer que a Web é uma coleção de documentos distribuídos denominados páginas, localizados em computadores (ou servidores) por todo o mundo. Os servidores estocam arquivos em linguagem de hipertexto (HTML) e respondem a pedidos. Através da utilização de um browser, usuários de computadores pessoais podem localizar e visualizar documentos baseados nos servidores.

Os conceitos de Internet e Web estão revolucionando a maneira como tem sido realizada tradicionalmente a prática do comércio e das trocas na economia industrial.

ANGEL e HESLOP (1994) comentam que nos primórdios da Internet, até meados 1995, havia uma proibição, já revogada, de utilizar a infraestrutura da rede para comércio. Essa era uma política bastante simpática aos usuários acadêmicos na época. Até 1996, havia ainda o mito de que qualquer atividade comercial seria estritamente proibida, ainda da época em que a *National Science Foundation* (NSF) norte-americana assumia partes significativas da rede.

Segundo CRONIN (1994), o tráfego comercial seria perfeitamente legal, desde que não partisse do *backbone* da NSF.

A medida em que a Internet atrai mais usuários, novas abordagens comerciais foram surgindo, principalmente na área de segurança e criptografia o que tem gerado um dos grandes debates da história da informática, com restrições de exportações de sistemas por parte do ITAR – órgão que regula exportação de armas dos EUA. (COOPER et al., 1995).

O rápido desenvolvimento da Internet, provocando mudanças de paradigmas, tem gerado experiências interessantes de registro como, por exemplo, a chamada capsula do tempo digital, feita no MIT. Uma capsula



com descrição de novas tendências e desafios em 1999. Essa capsula será aberta em 2004, para avaliação do desenvolvimento. (MEDIALAB, 1999)

Vários dos paradigmas que foram mudados ou que poderão sofrer alterações são na área de comércio.

### III. Comércio Eletrônico

#### 1. Introdução

O grande crescimento da Internet e em particular da Web (WWW), propiciou a existência de uma massa crítica de consumidores e empresas que participam de um mercado global. A rápida adoção da Internet com finalidades comerciais tem permitido às empresas descobrir técnicas inovadoras de praticar marketing com seu mercado, num ambiente mediado por software e computador, a maneira adequada de atender seus clientes e clientes potenciais. Esses desenvolvimentos da Internet estão crescendo além da utilização como meio de comunicação, para a percepção da Internet como um novo mercado. Com isso vários conceitos de como atender esse mercado com comércio eletrônico tem surgido.

Um conceito amplamente utilizado para a definição do que é o comércio eletrônico é a compra e venda de produtos e serviços através da Internet. Entretanto, há vários outros aspectos relevantes, uma vez que as oportunidades para as empresas são maiores do que a mera adoção da visão tradicional de comércio simplesmente realizado através de redes eletrônicas.

Desde o seu início, o comércio eletrônico incluía transações de compras e transferências de fundos através de redes de computadores. O intercâmbio de dados eletrônicos *Electronic Data Interchange* (EDI), realizado em redes privadas começou na década de 60. Essas ferramentas e conceitos que vinham sendo aplicados foram em boa parte migrados para o desenvolvimento de sistemas de comércio eletrônico na Internet. Os bancos têm utilizado redes exclusivas para a transferência de fundos eletrônicos *Electronic Fund Transfer* (EFT) também desde então. CLARKE (1993) comenta que as conexões entre fabricantes e distribuidores ou

corretoras e bolsas, através de canais de comunicação informatizado já eram utilizados em redes proprietárias e com sistemas fechados . Com a difusão da Internet os conceitos de EDI passaram a ser mais difundidos e aplicados na rede publica.

Alguns autores passaram a definir publicações eletrônicas como *subset* de comércio eletrônico, onde bens são preparados digitalmente para consumo pelos sentidos humanos (CLARKE, 1999). No sentido ampliado, compreende texto, dados estruturados, imagens, animações, sons, em qualquer combinação. As novas tecnologias que tem surgindo nessa área como XML tem grande potencial para os sistemas de comércio eletrônico.

Apesar desse início com transações entre grandes empresas, bancos e outras instituições financeiras, a utilização da Internet como uma maneira de trazer o comércio eletrônico ao consumidor individual trouxe toda uma nova visão a este comércio. (KOSIUR, 1997)

ZWASS (1996) define o comércio eletrônico como o compartilhamento de informações, manutenção de relacionamentos e condução de transações de negócios através de uma rede de telecomunicações.

Segundo KALAKOTA e WHINSTON (1997), dependendo de a quem a pergunta é feita, há diferentes definições para comércio eletrônico:

De um ponto de vista de comunicação, o comércio eletrônico é a entrega de informações, produtos/serviços ou pagamentos via linhas telefônicas, redes de computadores ou quaisquer outros meios.

De um ponto de vista empresarial, o comércio eletrônico é a aplicação da tecnologia para a automação das transações empresariais.

De um ponto de vista de serviços, o comércio eletrônico é um instrumento que atende os desejos de empresas, consumidores e gerências para

reduzir custos enquanto melhora a qualidade dos bens aumentando a velocidade da entrega de serviços.

De um ponto de vista *online*, o comércio eletrônico proporciona a capacidade de comprar e vender produtos e informações na Internet e outros serviços *online*.

No comércio tradicional, para suprir as necessidades do mercado, as empresas projetam e produzem novos produtos, veiculam-nos, distribuem-nos e oferecem serviços ao consumidor, gerando receitas para si ao longo do processo. Os consumidores têm que identificar primeiramente uma necessidade, quer seja de um produto físico, um serviço ou uma informação. Depois eles precisam buscar informações a respeito daquele produto ou serviço, encontrar locais que vendem tal produto e comparar as opções que encontraram (preços, serviço, reputação, etc.) antes que efetivamente comprem o produto. Realizar a venda ainda pode implicar numa negociação do preço, quantidade, termos de entrega e talvez até questões legais. O ciclo da venda não termina com a entrega do produto ou serviço; o atendimento ao cliente acrescenta novas etapas neste processo ao gerar benefícios a ambos os lados - os consumidores recebem o que eles precisam para manter seus produtos funcionando bem e os fornecedores aprendem mais sobre as necessidades do mercado. Ao longo deste processo, os bancos e outras instituições financeiras lidam com a transferência de fundos entre os compradores e vendedores, quer sejam consumidores individuais ou grandes empresas multinacionais. (CHOI, STAHL, WHINSTON, 1997)

O comércio eletrônico é um sistema que inclui não somente aquelas transações que se concentram na compra e venda de bens e serviços para gerar receitas diretamente, mas também aquelas transações que apoiam a geração de receitas, tais como a geração de demanda para tais bens e serviços, a oferta de serviços ao cliente ou a facilitação da comunicação entre parceiros empresariais.

Comércio eletrônico é um nome novo, mas seu uso já data de meio século, segundo SEIDERMAN (1996), a tecnologia conhecida como EDI emergiu da organização voltada para suprir Berlim quando a cidade estava bloqueada pelos soviéticos em 1948. Na prática, o EDI – *Electronic Data Interchange* que é a troca eletrônica de informação, promove a troca computador-a-computador de documentos através de transações eletrônicas padronizadas. Apesar de não limitarmos o comércio eletrônico ao EDI, seu uso levou à mais significativa transformação organizacional e de marketing, segundo JELASSI e FIGON (1994). Alguns casos notórios são o Wal-Mart, Levi Strauss, General Motors e outras companhias que construíram novos relacionamentos com seus fornecedores e consumidores através de links eletrônicos.

A integração eletrônica levou à mudanças drásticas na definição de uma empresa, pois surgiram as empresas virtuais cuja capacidade de entrega de seus produtos no mercado é amplamente definida pela habilidade em organizar e manter relacionamentos de negócios por rede, mais do que por sua habilidade em manufaturar um produto ou entregar um serviço. Novas redes de negócios foram criadas apoiadas nessa forma de integração e indústrias inteiras estão sendo radicalmente modificadas. Para entender uma empresa específica ou o negócio específico, segundo KAMBIL E SHORT (1994), é necessário estudar a rede de negócios na qual ela se encontra.

A arquitetura básica do comércio eletrônico baseado na Web inclui: um browser do cliente, um servidor da Web e serviços de terceiros. O browser do cliente interage com o servidor da Web, que então intermedia a interação com serviços de terceiros. As funções do servidor da Web podem ser categorizadas em: retenção de informação, gerenciamento de dados e de transações e segurança. Os serviços de terceiros podem ser outros

servidores da Web que fornecem conteúdo, instrumentos de processamento de informações e sistemas de pagamento eletrônico.

O comércio eletrônico incrementa as vantagens e estruturas do comércio tradicional ao acrescentar as flexibilidades oferecidas pelas redes eletrônicas. Ao operar com informações digitais em redes eletrônicas, o comércio eletrônico traz consigo algumas novas oportunidades para a condução de atividades comerciais, como a facilitação de trocas de informações dentro de uma empresa que está buscando criar um novo produto.

A chegada do uso comercial da Internet vem definindo o novo comércio eletrônico. O *e-commerce* está emergindo da convergência de várias tecnologias e práticas administrativas. Conforme ZWASS (1996), tecnologia engloba: rede de computadores e telecomunicações; computação cliente/servidor, multimídia (e hipermídia em particular); sistemas de recuperação de informação, troca eletrônica de informação (EDI); manuseio de mensagens e fluxo de sistemas de gerenciamento; sistemas eletrônicos de reuniões; criptografia de chave pública / privada. Em um sentido mais amplo, as grandes tecnologias de informática e telecomunicação, e particularmente o gerenciamento de bancos de dados, fortaleceram o comércio eletrônico. Essas tecnologias estão incorporadas à Internet. Esse conglomerado é uma tecnologia em transformação que mudou velhas concepções e ajudou a moldar novos espaços, organizações e mercados.

Conduzir atividades comerciais através de redes eletrônicas também elimina certas restrições físicas. Por exemplo, sistemas de computadores na Internet podem ser estabelecidos de forma a oferecer um atendimento aos clientes por 24 horas ao dia, por 7 dias da semana. Os pedidos para os produtos também podem ser aceitos a qualquer hora e a qualquer lugar.

O comércio eletrônico permite novos tipos de negócios, bem como novas formas de se fazer negócios. É notório como a Amazon.com, uma livraria com sede em Seattle, Washington, efetua suas vendas. A empresa não tem lojas físicas, vende todos os seus livros através da Internet e coordena as entregas diretamente com empresas de transportes e as editoras para que não precisem manter um estoque.

No ambiente atual, onde as fronteiras operacionais entre empresas tornam-se fluidas, seria infrutífero separar os processos interorganizacional e intraorganizacional. Comércio Eletrônico inclui relações de compra e venda, transações entre companhias e processos corporativos de comércio dentro de empresas individuais.

A definição de comércio eletrônico varia de autor para autor e também de acordo com os pontos considerados. Nesta tese é proposta a seguinte definição:

## **2. Definição de comércio eletrônico**

Comércio eletrônico, corresponde a transações interativas que são estabelecidas de maneira digital e assíncrona entre uma empresa e seus clientes, com transação monetária. Os termos para essa definição aqui criada são explicados abaixo.

Transações interativas são todas as que permitem que a cada ação uma reação correspondente, em tempo de resposta adequado, seja devolvido ao cliente.

Digital contrapõe-se a analógico, e facilita a reprodução dos comandos ou respostas. As informações digitais tem como características a fácil armazenagem, reprodução mais precisa, e maior facilidade de manipulação em relação aos processos analógicos.

Assíncrona refere-se a capacidade de armazenar requisições ou respostas, para serem utilizadas conforme demanda. Dessa maneira não pressupõe necessariamente de um operador humano no instante da solicitação ou ocorrência.

Na definição de JURAN (1992), clientes são todos aqueles que são afetados pelas atividades da empresa.

Transação financeira é a troca de valores monetários entre duas ou mais parte (MAYER, 1997).

A definição aqui proposta pelo autor desta tese, foi desenvolvida a partir de diferentes textos e experiência pessoal.

### **3. Como as empresas estão utilizando o Comércio Eletrônico**

Os serviços eletrônicos, como por exemplo o e-mail, tem sido usados por várias organizações profissionais para diversas finalidades. As empresas podem obter novas vendas e novos canais de marketing através da Web. A WWW permite às organizações apresentar materiais como catálogos de produtos e lista de preços *on-line* (YOFFIE, 2000).

Várias empresas tem vendido diretamente ao seu mercado. Empresas tem oferecido suporte técnico *on-line*, permitindo que os clientes encontrem facilmente respostas para os problemas e realizem *download* de softwares 24 horas por dia, 7 dias por semana.

As tecnologias de comércio eletrônico podem ser usadas em qualquer ambiente onde os documentos podem ser trocados entre organizações, inclusive ordens de compras.

O comércio eletrônico tem benefícios potenciais tanto para o fornecedor quanto ao comprador, na redução de papéis e tempos de processos administrativos.



### **3.1. Requisitos para o Comércio Eletrônico**

Comércio Eletrônico pode ser entendido como uma metodologia de negócio moderna que atende as necessidades de organizações, comerciantes e consumidores simultaneamente.

As atividades de processamento das informações realizadas para o comércio eletrônico é geralmente na forma de transações de negócios, para os quais diversas categorias são observadas:

- transações entre a empresa e o consumidor através de redes públicas com a finalidade de home shopping ou home banking
- transações entre parceiros comerciais usando EDI,
- transações para coleta de informações como pesquisa de mercado,
- transações para distribuição de informações com clientes potenciais.

Para satisfazer esses requisitos, o mercado eletrônico será estruturado como uma rede amplamente distribuída de produtos e serviços.

## **4. Vantagens do Comércio Eletrônico**

Existem vantagens na adoção do comércio eletrônico para o consumidor e para a empresa comerciante.

### ***4.1. Vantagens para o consumidor***

#### ***4.1.1. Acesso à mais informações***

Um dos benefícios associados com o marketing na Web, é o acesso à maiores volumes de informações dinâmicas para atender as consultas do consumidor no seu processo de decisão. Levantamento com usuários Web identificou que a busca de informações para o processo de compra era das atividades mais comuns na Internet (GUPTA, 1999). A natureza interativa da Web e o ambiente de hipertexto permite buscas não-lineares iniciadas e controladas pelo consumidor. Dessa forma as comunicações de marketing na Web são mais direcionadas ao consumidor que as disponibilizadas pela mídia tradicional.

#### ***4.1.2. Pesquisa e comparações mais fáceis***

A habilidade da Web para levantar, analisar e controlar grandes quantidades de dados especializados pode permitir a comparação de preços e produtos e acelerar a busca de bens. A Web facilita testes de produtos (DERTOUZOS, 1997) e permite uma gratificação instantânea; consumidores podem testar produtos *on-line*, o que pode estimular a compra. Existe também o potencial de maior disponibilidade de produtos difíceis de encontrar e maior seleção de itens devido à abrangência e eficiência do canal.

#### **4.1.3. Custos e preços mais baixos**

O aumento da competição à medida que novos fornecedores são capazes de competir num mercado aberto provoca uma maior concorrência o que tende a reduzir preços, maior qualidade e variedade de bens através de um mercado expandido e a habilidade de produzir bens sob medida.

### **4.2. Vantagens do comerciante**

#### **4.2.1. Melhor distribuição**

Empresas se beneficiam na utilização da Web como canal de distribuição. Em alguns setores o custo de distribuição pode cair a zero, como no caso de produtos digitais. Nesses casos a existência do intermediário pode desaparecer. Compradores e vendedores podem se comunicar diretamente eliminando os custos de marketing e restrições impostas por tais limitações no mundo terrestre. Esse efeito sobre o canal de distribuição pode tornar a distribuição mais eficiente, reduzindo os custos através da integração e automação. O tempo necessário para realizar as transações pode ser reduzido.

As vendas pela Internet exigem mais funções de venda por parte do consumidor, através do preenchimento de formulários. Isso ainda permite uma outra vantagem, na forma de coleta de informações sobre o consumidor. A capacidade de reter informações dos clientes e avaliar suas preferências e necessidades são de extrema valia.

#### **4.2.2. Comunicação de Marketing**

A distribuição de informações através da Web, sobre a empresa e seus produtos para o mercado é um dos benefícios. A característica interativa da Web pode permitir uma melhor postura em relação ao relacionamento com os clientes. A comunicação da empresa pode esclarecer as necessidades latentes do consumidor, ampliar o conhecimento da marca, ampliar o conhecimento do produto, aperfeiçoar a imagem da marca, melhorar a imagem da empresa e ampliar a preferência da marca (COBRA, 1990).

A disponibilidade das informações 24 horas por dia, permite que as informações sejam consumidas dentro da conveniência de ambas as partes, fato que torna-se importante quando as partes estão em regiões com fusos horários diferentes. As informações podem ser preparadas sob medida para algum consumidor em particular, ou todos em geral, dentro do conceito de customização de massas de PINE (1999). Essa característica permite que algum consumidor em particular, solicite quanta informação achar necessária – o que facilita que a empresa esteja lhe atendendo mais satisfatoriamente no futuro.

#### **4.2.3. Benefícios operacionais**

Benefícios operacionais da Web para vendedores industriais são redução de erros, de tempos e de custos no processo de informação.

O acesso a novos mercados (especialmente locais à remotos geograficamente) é facilitado.

## **5. Comércio Eletrônico: Estruturas e Características**

Comércio eletrônico não deve ser interpretado como um desenvolvimento puramente tecnológico. Esse modo de fazer negócios pode ser entendido como extensão das tecnologias da informação e dos avanços gerenciais e organizacionais que o impulsionam e por ele são impulsionados. Alguns desses avanços são a organização de trabalho em grupo com equipes internacionais trabalhando ininterruptamente, *tele-trabalho*, mover produtos e operações para cadeias de valor virtuais e organizações multinacionais. Na destruição criativa de Schumpeter (BOTTOMORE, 1992), o uso de tecnologias transformacionais desafia modos pré-existentes de administração, colaboração e competição. Em um âmbito maior, a tecnologia de conectividade global, acessível e não-proprietária muda muitos aspectos de nossas vidas, e deve ser encarada como tal.

### **5.1. O Sistema de Comércio Eletrônico**

Segundo BRADLEY e NOLAN (1998), para analisar e desenvolver sistemas muito complexos – como o comércio eletrônico – deve ser visualizado como uma estrutura hierárquica composta de vários níveis, sendo que os níveis mais altos entregam funções bem definidas aos níveis mais baixos. Tal hierarquia é mostrada na tabela abaixo, adaptado de KALAKOTA e WHINSTON (1996).

Tabela 1 : Sistema hierárquico do comércio eletrônico

Nível	Função	Exemplo
<b>Produtos e Estruturas</b>		
7	Hierarquias e mercados eletrônicos	Leilões eletrônicos, concessões, corretagem e mercados de busca direta. Gerenciamento da cadeia interorganizacional de suprimentos.
6	Produtos e Sistemas	Serviços remotos ao consumidor (shopping, bancos, mercado de ações) Demanda de informação (sites pagos, ofertas educacionais) Links fornecedor-consumidor Marketing on-line Sistemas de benefícios eletrônicos Sistemas de colaboração em Intranets
<b>Serviços</b>		
5	Serviços de capacitação	Catálogos/listas eletrônicas, smart agents Meios de pagamento eletrônicos, serviços de autenticação digital Bibliotecas digitais, serviços de proteção ao direito autoral Auditoria de tráfego Sistemas de smart-cards
4	Troca segura de mensagens	EDI, e-mail, EFT
<b>Infraestrutura</b>		
3	Gerenciamento de objetos hipermídia/multi mídia	World Wide Web com Java
2	Meios de comunicação públicos e privados	Internet e value-added networks (VANs)
1	Infraestrutura de telecomunicação em áreas amplas	Redes sem fio

O sistema apresentado por KALAKOTA e WHINSTON (1996), mostra que o comércio eletrônico é formado por três meta-níveis:

- **Infraestrutura:** hardware, software, bancos de dados e telecomunicações que permitem a funcionalidade da World Wide Web e/ou suportam o EDI e outras formas de mensagens na Internet ou em VANs.
- **Serviços:** mensagens e outras variedades de serviços que permitem achar e entregar a informação, assim como transações, negociações e acordos administrativos.
- **Produtos e Estruturas:** provisão direta de serviços comerciais a consumidores e parceiros, colaboração e compartilhamento de informações intraorganizacionais e organização de mercados eletrônicos e redes de fornecimento.

Os níveis individuais que constituem esses três meta-níveis serão discutidos agora, seguidos por um exame das questões geradas por suas funções.

## ***5.2. Infraestrutura tecnológica***

Os primeiros três níveis do sistema hierárquico do comércio eletrônico formam sua estrutura tecnológica. A base é a rede de telecomunicações de grande alcance e as redes metropolitanas, de alcance local. Empregando meios de transmissão via cabo (fibra ótica e cabo coaxial) e sem fio (ondas de rádio e satélites) controlados por computadores, essas redes englobam o mundo. Por isso, o comércio eletrônico é fundamentalmente global. Porém, existem grandes diferenças no desenvolvimento da infraestrutura regional e nacional, bem como na política de telecomunicações,

como monopólios governamentais que limitam o desenvolvimento e elevam seus custos em vários países. Na Europa e na América Latina um movimento de privatização vem produzindo efeitos de redução nos preços e serviços. Em Cingapura, programas governamentais nacionais de desenvolvimento, fomentam o comércio eletrônico (BARRO, 1998).

As vantagens das telecomunicações chegam ao uso administrativo de duas maneiras essenciais. A velha ordem era a das value-added networks (VANs) proprietárias estabelecida por comerciantes para a entrega de serviços e licenciadas pelo governo para fornecer serviços de comunicação ao público. A Internet é a nova ordem e se tornou o principal veículo de comércio eletrônico. As características que se sobressaem são: acesso público fácil e relativamente barato; ausência de controle centralizador e conseqüente crescimento orgânico combinados com segurança, confiabilidade e banda de transmissão limitadas, confiança em um simples protocolo de transferência de pacotes (TCP/IP), facilidade de ligação de redes adicionais aos roteadores com padronização gerenciada pela Sociedade da Internet e suas subsidiárias (tais como Internet Architecture Board).

A Internet assumiu a liderança do comércio eletrônico graças à invenção da World Wide Web como meio principal de compartilhamento de informações. A Web transformou a Internet em um banco de dados de hiperlinks globais. Ao utilizar a arquitetura cliente/servidor, a Web gerou o modelo descentralizado da Internet. É fácil juntar-se a ela e organizar um espaço de informação para um determinado grupo. Conforme SPAR e BUSSGANG (1996), as comunidades da Internet podem moldar o espaço que se adapta a



seus propósitos. A Web pode servir como meio de apresentação, distribuição e venda de software e informação, por exemplo.

A Web pode ser vista como a incorporação das visões de memex (coleção de documentos com hiperlinks) de BUSH (1945), a noosfera (a camada da pensante da biosfera) de TEILHARD DE CHARDIN (1976) ou as interações holísticas entre as esferas de existência e consciência de VERNADSKY (1998).

### **5.3. Serviços: Comunicação Interpessoal e Comércio**

O meta-nível dos serviços é a garantia de mensagens seguras e a viabilidade do comércio eletrônico. Juntos, esses serviços garantem a infraestrutura administrativa do *e-commerce*.

Mensagens seguras no processamento de transações comerciais precisam apresentar os seguintes atributos: privacidade (conseguida através de criptografia, mas a logística de chaves seguras continua sendo um problema mesmo nos sistemas com chave pública/privada); integridade da mensagem (conseguida através de divisões totais ou elementos similares que acompanham a mensagem); autenticação de ambas as partes (geralmente através de uma assinatura digital e posse de uma chave privada) e aceitação dos dois lados (alcançada através de uma combinação dos meios mencionados antes). Algumas transações necessitam de atributos adicionais; a geração de moeda eletrônica pode exigir anonimato da parte que a recebe (conseguido com um fator de obscurecimento durante a criptografia) (FORD e BAUM, 1997).

Dentre os principais serviços de mensagens estão o EDI, o EFT (transferência eletrônica de fundos) e o e-mail; mensagens de voz e telefax estão também disponíveis. A motivação básica para a

implantação do EDI é a economia. As corporações gastam em torno de US\$150 para processar um pedido no papel e apenas US\$ 25 se o pedido for eletrônico (VERITY, 1996). Além da economia, as companhias procuram benefícios estratégicos, tais como ciclos de negócios comprimidos e intensificação de relacionamento com os parceiros.

O EDI tradicional baseia-se amplamente no modelo *hub-and-spoke* (FORD e BAUM, 1997), tendo um parceiro dominante (o *hub*) que gradualmente vai se cercando de seus fornecedores, consumidores e colaboradores. Essa forma de EDI tem ainda uma grande base VAN, com padrões proprietários e custos de serviços relativamente altos. Enquanto os padrões industriais emergiram em alguns segmentos, o padrão internacional EDIFACT contou apenas com uma pequena adesão. Nessa altura, muitas companhias mudavam suas comunicações EDI para a Internet, buscando custos menores e aparente conectividade mundial (BAER, 1996). Essa mudança trará grandes conseqüências para a indústria e a economia, principalmente se combinada com o EDI-aberto. O EDI-aberto deverá oferecer padrões internacionais para cenários administrativos comuns. O objetivo é interagir espontaneamente com um novo parceiro comercial, sem um acordo a priori com relação a um protocolo de interação. Espera-se que o comércio eletrônico global business-to-business traga grandes benefícios ao passar das simples transações EDI para o cenário mais elaborado e customizável do EDI-aberto (open-EDI) (LEE e BONS, 1996). Outra forma de mensagem é um tipo seguro de EDI usado em sistemas de transferência eletrônica de fundos (EFTS) que permite transferências de fundos entre bancos na forma de informação (FORD e BAUM, 1997).

O correio eletrônico (*e-mail*) tornou-se um meio de comunicação muito difundido, geralmente com profundos efeitos organizacionais. E-mail é o uso mais popular na Internet. Ele poderá continuar assim se incorporar a transmissão de documentos multimídia e ao se combinar a outros serviços tais como instrumentos de negociação e smart software agents. (RAPAPORT 1996).

A mais turbulenta atividade tecnológica e empreendedora ocorre no nível de serviços de capacitação (GOGAN, APPLEGATE, 1997). Esses serviços facilitam as buscas por informações e parceiros de negócios, negociação e manutenção de relacionamentos comerciais e realização de transações por acordos financeiros. Esse nível inclui as bibliotecas digitais (FOX, 1995), catálogos e diretórios eletrônicos, agentes inteligentes que auxiliam na procura de uma determinada mercadoria ou serviço, autenticação eletrônica que ajuda a estabelecer a confiança no parceiro, serviços de proteção de direitos autorais (possivelmente marcas d'água digitais), auditoria de tráfego para estabelecer o valor de um site para propósitos de propaganda (ainda a maior fonte de renda de *sites* que possuem renda) e uma variedade de outros serviços que estão sendo inventados a todo instante.

O desenvolvimento da moeda eletrônica será analisado adiante. Hoje a forma de pagamento é uma das barreiras mais sérias para o desenvolvimento do Comércio Eletrônico, Conforme ZWASS (1996) e FORD e BAUM (1997)

#### **5.4. Produtos e Estruturas do Comércio Eletrônico**

Produtos e estruturas do comércio eletrônico cobrem três categorias: comércio orientado ao consumidor, *business-to-business* e

negócios intraorganizacionais. Espera-se grande desenvolvimento dos três, porém com diferentes resultados econômicos.

As aplicações mais procuradas no comércio eletrônico são as orientada ao consumidor. Elas incluem negociações remotas como compras (*home shopping*), banco (*home banking*) e mercado de ações, juntamente com (e, em muitos casos, patrocinadas por) propagandas *on-line* (CRONIN, 1997). O fato de lojas de certo sucesso serem tão conhecidas é um testemunho dessa carência. Essas lojas incluem Amazon.com, uma livraria com um estoque enorme (virtual). Para ter chance de sucesso nesse mercado, a empresa deve identificar a real necessidade do consumidor e o relacionamento entre eles deve ser construído pela interatividade (HOFFMAN, NOVAK e CHATTERJEE, 1996).

Outro importante segmento orientado ao consumidor é o de informação e entretenimento. Esse segmento constrói um novo meio de comunicação na Web cuja natureza ainda está sendo explorada. Esse "Infotainment" abrange educação – através de informações especializadas – e entretenimento. Muitos produtos educativos respondem a requerimentos especializados. Alguns programas e cursos educacionais têm créditos apropriados e graus; estão inclusive surgindo universidades virtuais (CUSHMAN, 1996). O segmento também inclui as "*webzines*" como HotWired e Slate, jornais e livros eletrônicos e acesso a relatórios analíticos e opiniões de especialistas. Do lado do entretenimento há várias categorias de webzines e livros eletrônicos, vídeos, realidade-virtual e games. A categoria de orientação ao consumidor pretende se expandir de várias maneiras, mas só algumas podem ser previstas (GRAY, 1998). Por exemplo, sistemas eletrônicos para distribuição de transferências pela Internet, que podem ser usados em pagamentos

diretos; uma variedade de interações eletrônicas com geradores de "infotainment" (HOFFMAN, NOVAK e CHATTERJEE, 1996).

A categoria de comércio eletrônico melhor estabelecida é o *business-to-business* mantido com EDI. Segundo estimativa de VERITY (1996) as empresas americanas estimam comprar U\$500 bilhões por ano em mercadorias, eletronicamente. Essa categoria tende a se expandir significativamente com o novo comércio eletrônico, levando, em muitos casos, ao gerenciamento interorganizacional em cadeia. *Business-to-business* é facilitado por consórcios tais como CommerceNet e por empresas que organizam mercados industriais na *Web*, como a Industry.net. *Business to business* e mercado orientado ao consumidor são as áreas mais importantes do comércio eletrônico (GVU, 1999).

A área que mais cresce nesse nível de comércio eletrônico é o compartilhamento de informações e colaboração em intranet. As intranets suportam a abertura de bancos de dados e *data-warehouses* organizacionais, além de equipes espalhadas pelo mundo (KEELER, 1995). Uma intranet típica usada pelo Morgan Stanley mostra o Web site gerado automaticamente com dados resumidos e atualizados das posições de investimentos da companhia. Essa foi a solução para os problemas administrativos da empresa (SPROUT 1995). Usos mais ativos das intranets estão sendo desenvolvidos, incluindo colaboração *on-line* em projetos comuns através de documentos eletrônicos e da videoconferência. A Ford usa sua intranet para unir seus centros de design nos Estados Unidos, Europa e Ásia, permitindo que os engenheiros desenvolvam protótipos eletrônicos *on-line* de carros e peças. Ao incluir uma ampla variedade de informações, as intranets podem se tornar uma nova forma de memória organizacional (STEIN e ZWASS 1995).

O ápice do comércio eletrônico são os mercados eletrônicos e as hierarquias eletrônicas que facilitam os relacionamentos comerciais. Os mercados eletrônicos são criados para facilitar as transações em redes de telecomunicações entre múltiplos compradores e fornecedores. As hierarquias eletrônicas são relacionamentos comprador-fornecedor duradouros entre empresas mantidos por redes de telecomunicações e amplamente coordenados por gerenciamento e não por forças do mercado.

A coordenação baseada em mercado pode ser classificada em quatro categorias (como proposta por GARBADE, 1982): mercado de busca-direta (onde um futuro parceiro procura o outro), mercados de ações (onde um corretor assume a função de busca), mercado de fornecedores (onde os fornecedores possuem inventários com os quais eles compram e vendem) e os mercados de leilões. Industry.Net é um exemplo de mercado de busca-direta de produtos industriais; Onsale Inc. oferece um mercado de leilão eletrônico (ROBERTS, 1996). LEE e CLARK (1996) oferecem vários outros exemplos de corretagem eletrônica e leilão.

A formação de hierarquias eletrônicas interorganizacionais está sendo feita com cadeias de fornecimento integradas, promovendo a produção imediata que atende ao pedido do consumidor. Essa cadeia entre os parceiros é feita em grande parte por sistemas de informações e redes de telecomunicações. Esse modo de operação impõe fortes restrições à coordenação intra e interorganizacional onde as intranet e a Internet podem desempenhar um papel importante. A confiança na tecnologia é vital para a integração.

As hierarquias das empresas e os mercados abertos podem ser interpretados como os dois lados de um continuum administrativo, tendo no centro as hierarquias eletrônicas. A difusão do novo

comércio eletrônico irá modificar as vantagens comparativas entre coordenação baseada em mercado e baseada em hierarquia e também entre os vários modos de se estruturar o mercado (ROBERT, 1995) .

### ***5.5. Problemas para o desenvolvimento do Comércio Eletrônico***

As restrições ao desenvolvimento do comércio eletrônico são grandes e reflete a profundidade das mudanças causadas por sua rápida expansão (STORROSTEN, 1999). Os fatores chaves dentro do sistema hierárquico da estrutura baseada no modelo de KALAKOTA e WHINSTON (1996), indo da infraestrutura para a condução dos negócios, são:

### ***5.6. Limitações e Assimetrias da Infraestrutura***

Uma infraestrutura apropriada é necessária para o desenvolvimento do comércio eletrônico. A infraestrutura da Internet já apresentou problemas. As questões dependem da existência de bandas de transmissão e dos problemas criados pela natureza descentralizadora da Internet. Muitos consideram a banda larga uma limitação. O atual backbone da Internet 2.0 opera com 45–155 megabits por segundo e não é suficiente para a visualização de vídeos, por exemplo. A baixa performance experimentada pelos usuários, no entanto, deriva geralmente das limitações dos equipamentos e das conexões de seus provedores e não pela banda larga limitada do backbone. Assimetrias significativas existem entre as bandas disponíveis nas grandes organizações e as de pequenas empresas e casas (onde estão os consumidores). Resolver esse problema fora dos centros urbanos é extremamente caro. Além disso, os 50 países menos desenvolvidos possuem apenas 23

máquinas hosts (NEGROPONTE, 1998) em um total de 9.5 milhões em todo o mundo (janeiro, 1999) (LOTTOR, 1999).

As soluções de mercado, algumas vezes estimuladas por intervenção governamental, são a meta de vários países. Várias corporações americanas adquirem a banda larga necessária de redes paralelas e acessam sites comerciais duplicadamente (COY, JUDGE, 1998). A tendência é a expansão. O futuro desenvolvimento do backbone da Internet 3.0 que poderá transportar dados, vídeo e voz simultaneamente é uma questão aberta. A despeito dos riscos financeiros e dos problemas tecnológicos, certamente surgirá uma política pública de acesso, em todos os países.

Várias limitações são aparentes na infraestrutura da Web e chegam a se transformar em problemas. Muitas das soluções de integração são feitas por sistemas localizados entre o software do cliente e o do servidor. É preciso se identificar em todo o *site* durante uma única sessão para negociar. Não há como saber quem está acessando o *site* e assim fazer uma oferta ao visitante em sua próxima visita. Essa limitação reforça os limites da tecnologia e ressalta suas conseqüências não desejadas, como invasão de privacidade (instalar um *cookie* no sistema do usuário é um jeito de ultrapassar esse limite de maneira invasiva) (LIU, PEEK, JONE, BUUS, NYE, 1994).

### **5.7. Integrando o pagamento eletrônico ao processo de compra**

O consumidor deve poder pagar por uma compra na Web com rapidez e segurança. Apesar de toda a experiência de compra, percepção de produtos e serviços ao consumidor na Web atual levar a uma significativa insatisfação entre consumidores potenciais



(JARVENPAA, TODD, 1997) e exigir a atenção dos profissionais de marketing e pesquisadores, uma solução sistêmica é possível.

NEGROPONTE (1998) destaca a necessidade de romper com a barreira imposta pelos meios de pagamento, hoje variações dos tradicionais, para o real desenvolvimento do comércio eletrônico.

### **5.8. Montando um Mercado para o Consumidor**

As compras não são o grande motivo de uso da *Web*, e acredita-se que a facilidade de acesso e de pagamento determinará o sucesso desse comércio (GUPTA, 1999). Uma interface pobre para o consumidor pode ser um grande desincentivo. Mas novos métodos de comércio devem tirar vantagem do novo meio (BERTHON, PITT, WATSON, 1998). Corporações multinacionais podem se sentir efetivamente desafiadas por pequenos concorrentes na *Web* e resolvem rever seus modelos de negócios (QUELCH, KLEIN, 1998). A variedade de possíveis *sites* comerciais é analisada por HOFFMAN, NOVAK e CHARTEJEE (1996); técnicas de venda na *Web* são discutidas por GOGAN e APPLGATE (1997). O processo de logística, principalmente de entrega das mercadorias foi analisada por TSE (1997).

### **5.9. Situação atual do comércio eletrônico**

O Comércio Eletrônico traz inúmeras oportunidades e desafios para a economia e sociedade. Expansão do comércio e inovações tecnológicas são dois propulsores de crescimento econômico, conforme destacado por MOKYR (1990). Essas forças estão presentes no comércio eletrônico. Os efeitos macroeconomicos do comércio eletrônico nas economias nacionais, regionais e internacionais ainda não estão claras. Instituições tradicionais como

bancos comerciais, universidades, intermediários comerciais bem estabelecidos, mídia, editoras, entre outros estão sendo desafiadas pelo novo conceito, e tendo que redefinir seus negócios para esse ambiente que está surgindo (CLEMONS, REDDI, ROW, 1996).

Para esse sistema emergente, onde novas formas de transação são necessárias, os meios de pagamento eletrônicos, que tem sido chamados de reengenharia da moeda, são considerados como ponto necessário para o real desenvolvimento e consolidação do comércio eletrônico (CLEMONS, CROSON, WEBER, 1997).

## **IV. Meio de Pagamento Eletrônico**

As transferências monetárias no ambiente de comércio eletrônico tem recebido bastante atenção, e várias propostas tem sido apresentadas, e várias disponibilizadas operacionalmente.

O problema de transferência monetária fica ainda mais crítico quando se trata de comércio bastante distribuído, com parceiros anônimos ou de valores transacionados baixos.

Será apresentado o resultado de uma pesquisa extensiva de todos os Meios de Pagamento Eletrônicos propostos, operacionais ou não, pesquisados até janeiro de 1999.

Meio de pagamento eletrônico é uma série de transações, ao fim da qual um pagamento é efetuado através de pacotes de informações emitido por uma terceira parte (LAW, SABETT, SOLINAS, 1996).

Os meios de pagamento foram catalogados, em função de características e requisitos do MPE (meio de pagamento eletrônico). Uma síntese é apresentada relacionando aspectos técnicos e econômicos.

Abaixo estão apresentados inicialmente os critérios adotados para classificação. Esses critérios foram adaptados a partir dos critérios destacados por cada MPE.

### **1. Características**

Para descrever e classificar os sistemas de pagamento digital, serão analisados diferentes características para determinar como as necessidades do usuário podem ser atingidas. Em todos os sistemas existentes, o propósito básico é transferir valores monetários de uma parte para outra (OWEN, 1997).

Os sistemas diferem em muitos aspectos tais como o grau de segurança, garantia de privacidade ou modo de unir o movimento do valor monetário real a uma transação digital.

### **1.1. *Econômicas***

**Nome:** a marca pela qual o sistema de pagamento é conhecido.

**Origem:** Os autores do sistema de pagamento, sua empresa ou instituto e as instituições e organizações de apoio. Esses dados dão uma indicação da possibilidade de sucesso de um dado sistema.

**Status:** O status de desenvolvimento de um sistema de pagamento é interessante no que diz respeito à escolha de um determinado sistema para uso prático. Esses sistemas podem ser apenas propostas teóricas ou um primeiro protótipo, podem estar em fase de teste, o software pode estar com o código aberto, podem já estar em uso ou ser um embrião de futuros sistemas.

**Datas:** As datas que levam ao atual status indicam a aceitação e o suporte a um determinado sistema.

**Valor do pagamento:** O valor do pagamento deve ser avaliado de acordo com a estrutura de preço que ele cobre. O valor mínimo e máximo dos pagamentos deve ser comparado ao valor típico da transação. Macro-pagamentos estariam acima de 10 US\$. Micro-pagamentos podem envolver frações de centavos.

**Risco:** O risco no uso de sistemas de pagamentos deve ser considerado. O risco pode ser de quem paga, de quem recebe ou do banco. O risco de perdas financeiras para cada uma das partes envolvidas na transação deve ser baixo e aceitável e estar diretamente ligado à segurança do sistema. As perdas para o consumidor podem ser limitadas ao se estabelecer um valor

máximo para cada transação e com uma aprovação especial para grandes transações.

**Taxas:** Taxas propostas pelo fornecedor do sistema de pagamento digital devem ser consideradas para determinar se o sistema pode ser usado economicamente. As taxas podem ser impostas (para o comerciante e/ou consumidor) para o acerto inicial, por transação e por saque ou depósito de fundos.

**Base de Uso:** A base de usuários do sistema de pagamento do comerciante e do consumidor determina a continuidade e propagação de seu uso. As estatísticas de uso seriam de especial interesse nesse contexto.

**Pré-requisitos:** As plataformas disponíveis determinam a infraestrutura, hardware e software necessários para a operação. Devem se ajustar à infraestrutura já em uso.

**Política de Informação:** A política de informação da companhia pode ser uma indicação da qualidade e segurança do sistema de pagamento (SCHOETER, WILLMER, 1997).

## 1.2. Tecnológicas

### 1.2.1. Participantes

A figura abaixo mostra o cenário básico do sistema de pagamento digital.

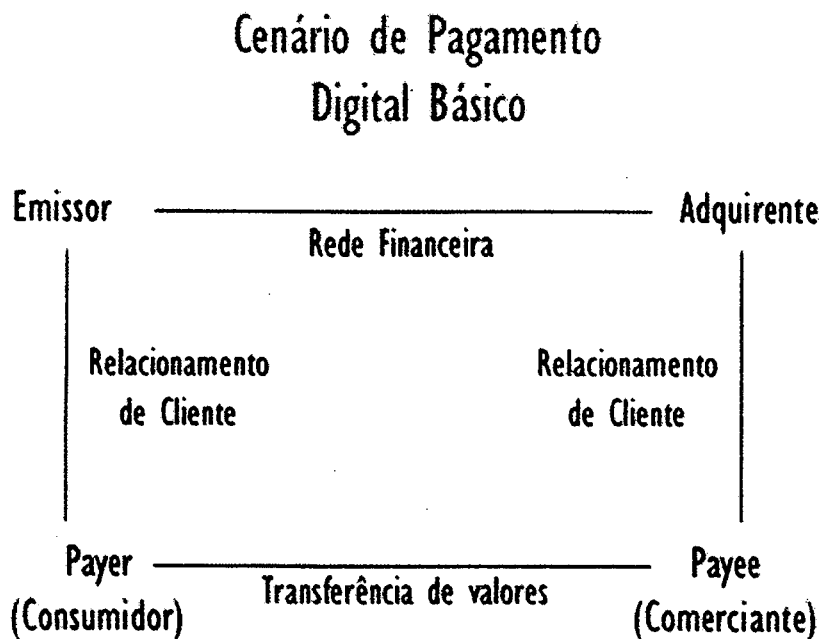


Figura 1 – Cenário de pagamento digital básico

Participantes e partes envolvidas são *brokers* ou agentes intermediários, emissores, adquirentes, *payer's* ou consumidores, *payee's* ou comerciantes, observadores, árbitros... (ABAD-PEIRO, ASOKAN, STEINER, WAIDNER, 1996) O objetivo de um pagamento é a transferência de valores monetários do payer para o payee.

- **Payer:** É o que faz o pagamento. Normalmente é o consumidor ou comprador em um cenário de comércio eletrônico. Será usado também o termo consumidor.

- **Payee:** É o que recebe o pagamento. Normalmente é o comerciante ou vendedor em um cenário de comércio eletrônico. Será também usado mais o termo comerciante, embora payee seja mais abrangente.
- **Emissor:** O emissor é a terceira parte que interage com o payer, ou seja, normalmente o banco ou prestadora de serviço do payer.
- **Adquirente:** O adquirente é a outra parte do payee, i.e normalmente o banco ou prestadora de serviço do payee.
- **Broker:** É uma combinação de emissor e adquirente se o protocolo necessitar de uma terceira parte comum ao payer e ao payee. O agente intermediário.
- **Observador:** Uma terceira parte que não se envolve e que é usada na análise da privacidade de um sistema de pagamento. O observador tenta obter informações da transação.
- **Certificação:** Muitos esquemas de pagamento baseiam-se na existência de um registro e de uma autoridade de certificação para o gerenciamento da autenticação e das chaves simétricas como Kerberos (BRYANT, STEINER, KOHL, 1989) ou certificação de chaves públicas (SCHNEIER, 1996).
- **Árbitro:** O árbitro pode envolver-se em disputas do sistema. Em muitos sistemas, a presença do árbitro não é explícita. As disputas dependem da política de decisão dos usuários e dos bancos.
- **Terceira Parte:** Algumas vezes são usados notários para reforçar notificações de pagamentos, clareza e testemunho de transações.

### 1.2.2. Modelos de Moedas

Modelos de moedas determinam o meio de troca de valores em uma transação de pagamento (CAMP, SIRBU, TYGAR, 1995).

- **Token:** *Tokens* têm seu próprio valor (como moedas) ou seu valor é baseado na credibilidade do *status* e solvência das entidades que o emitem. O sistema de *Tokens* não sustenta dívida. O uso de sistemas de moeda digital com *tokens* de valor pré-definido gera o problema de troco se o consumidor não tiver *tokens* com preço exato.
- **Notacional:** O valor é armazenado e trocado após autorização como em uma conta bancária. O banco mantém um registro da quantia na conta. Sistemas notacionais suportam débito quando permitem balanços negativos. Não há necessidade de troco. Trocas baseadas em moeda notacional debitam da conta dos *payers* e creditam na conta dos *payees*.



### **1.2.3. Modelos de Pagamento**

Modelos de pagamento classificam os sistemas de pagamento digital de acordo com a necessidade do fluxo de informação entre os participantes de uma transação eletrônica (ABAD-PEIRO, ASOKAN, STEINER, WAIDNER, 1996). A diferença básica é a presença ou a ausência de uma comunicação direta entre payer e payee. No caso da comunicação indireta, o pagamento diz respeito apenas ao iniciador do pagamento - que pode ser o *payer* ou o *payee* - e ao emissor e adquirente. Os sistemas de pagamento indireto são considerados parte do *home banking* no contexto de pagamento digital na *Internet*. A maioria dos sistemas implementa pagamentos diretos. Outra diferença é quando o valor é de fato tirado do *payer*, ou seja, sistemas de pré ou pós-pagamentos. Isso corresponde diretamente aos modelos de moedas *token* ou notacional. Sistemas de pré-pagamento são chamados de *cash-like* ou baseados em *tokens* e os de pós-pagamento são conhecidos como *account-based* ou notacionais. A transação com cartão de crédito segura pela *Internet* faz uso da infraestrutura já existente dos cartões.

a. *Direct Cash Like*:

### Modelo de Pagamento Direct Cash Like

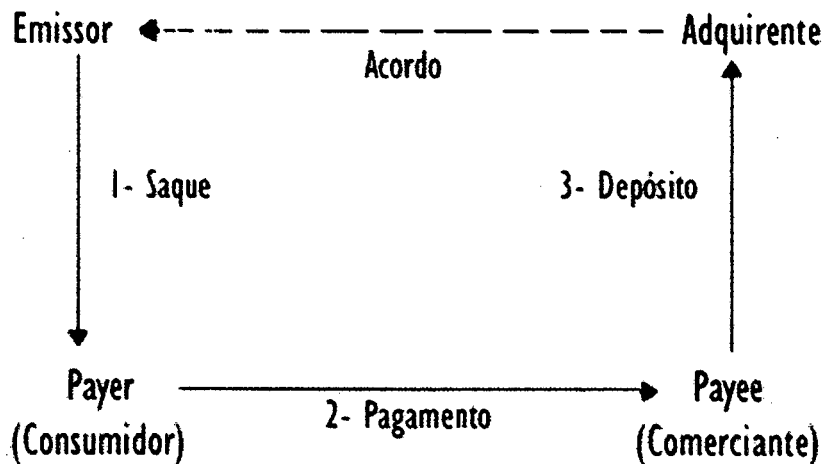


Figura 2 – Modelo de Pagamento *Direct Cash like*

No sistema *Direct Cash Like* o *payer* saca dinheiro do emissor, entrega os *tokens* ao *payee* que, por sua vez deposita a quantia em seu adquirente. A figura acima mostra esse cenário.

O sistema de pagamento *Direct Cash Like* usa o modelo de moeda *token*. Tal sistema normalmente envolve elementos do tipo *smart cards*, como o Mondex, ou validação *on-line* feita pelo emissor, como Ecash.

*b. Direct Account Based:*

O sistema *Direct Account Based* lembra o sistema convencional de cheques. Ele permite ao payer emitir uma autorização de pagamento (cheque) ao *payee*, que entrega essa mesma autorização a seu adquirente que por sua vez resgata-a com o emissor. É o emissor que informa ao payer a conclusão do processo. A figura abaixo mostra esse cenário. O sistema *Direct Account Based* usa o modelo de moeda notacional.

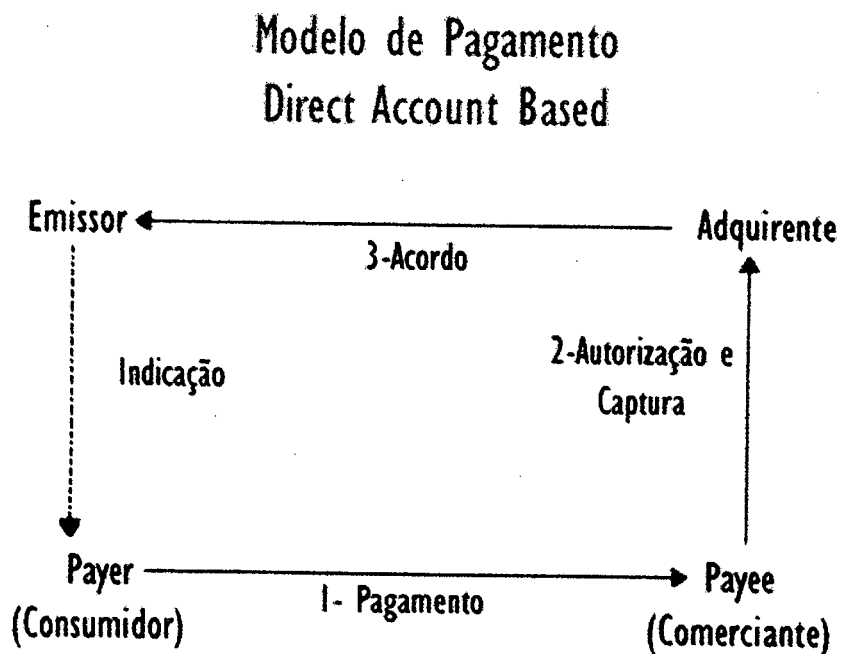


Figura 3 – Modelo de pagamento *Direct Account Based*

*c. Indirect Push Account Based:*

Com esse modelo de pagamento, o payer instrui o emissor para transferir fundos para a conta do *payee* no adquirente. Esse modelo lembra a tradicional transferência bancária. O *payee* é apenas notificado do pagamento efetuado. A figura abaixo mostra esse cenário.

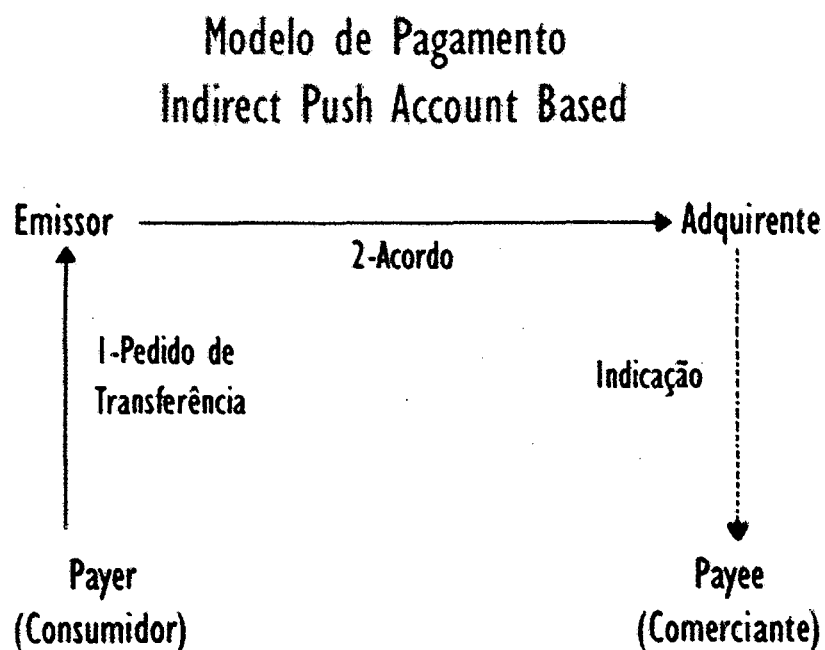


Figura 4 – Modelo de pagamento *indirect account based*

**d. Indirect Pull Account Based:**

Nesse modelo, o *payee* instrui o adquirente a cobrar os *payers* através do emissor. É o equivalente ao aviso de débito. O *payer* é apenas notificado do pagamento efetuado. A figura abaixo mostra esse cenário.

**Modelo de Pagamento  
Indirect Pull Account Based**

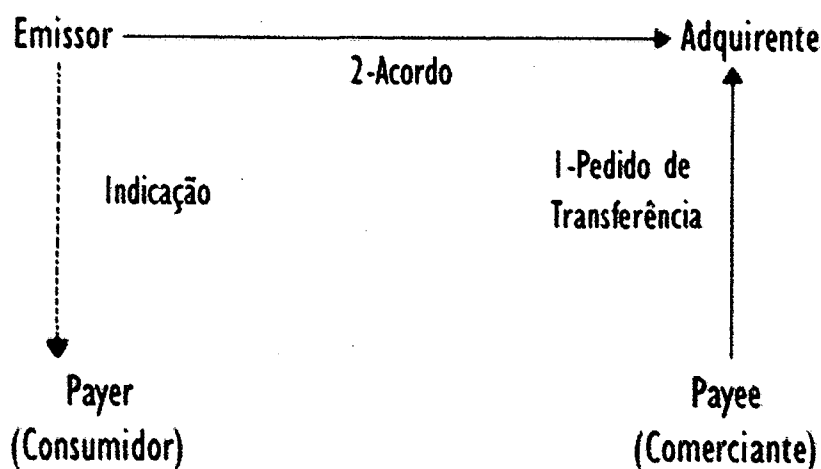


Figura 5 – Modelo de pagamento *indirect pull account based*

**e. Apresentação Segura de Cartão de Crédito:**

Sistemas de pagamento baseados em apresentação segura de cartão de crédito pela *Internet* fazem uso direto da estrutura já existente, como o SET. O ponto mais importante desse modo de pagamento é a transmissão segura dos dados do cartão. O *payer* transmite os dados do cartão ao *payee* que o submete ao adquirente para validação on-line. O adquirente completa o pagamento

através da rede financeira. Não há necessidade de contas especiais para o *payer* nem para o *payee* além das solicitadas pelo cartão. A desvantagem dos cartões de crédito é que eles não fazem micro-pagamentos.

#### **1.2.4. Validação**

A validação de pagamentos garante a conexão da transferência do valor real a um pagamento eletrônico. O método de validação depende de cada protocolo em particular. O tempo da validação está diretamente relacionado à eficiência do sistema de pagamento digital (OWEN, 1997).

##### **a. On-line:**

O sistema de validação *on-line* necessita da comunicação do *payer* e/ou do *payee* com uma terceira parte (emissor e/ou adquirente) que valida o pagamento, assim o *payee* tem o recebimento do valor monetário garantido por uma terceira parte na hora do pagamento. Portanto, sistemas *on-line* são geralmente considerados mais seguros.

##### **b. Offline:**

Sistema de validação *offline* envolve apenas comunicações entre *payer* e *payee* na hora do pagamento. Em sua maioria, esses sistemas de validação são feitos por *smartcards* e suas carteiras eletrônicas.

##### **c. Semi-on-line:**

Esse sistema de validação necessita de uma certa interação com uma terceira parte, mas não a cada

pagamento. Alguns sistemas *semi-on-line* pedem que o pagamento inicial seja *on-line* e as transações subseqüentes envolveriam somente *payer* e *payee*. Outros sistemas *semi-on-line* reforçam uma interação da terceira parte quando determinados limites de gastos são atingidos. A validação local do *payee* é permitida pela localização de *tokens*, ou seqüências correlatas de pagamento.

#### **1.2.5. Mecanismos de segurança**

Mecanismos de segurança de um sistema de pagamento individual dependem das características dadas e da hipótese de confiabilidade. No entanto, os requisitos básicos de segurança em todos os sistemas são integridade, autorização, sigilo, disponibilidade e confiabilidade. O protocolo de qualquer sistema de pagamento deve ser aberto ao público assim como a segurança de um sistema de pagamento não deveria depender do sigilo de seu protocolo. Integridade de um sistema de pagamento significa que apenas pagamentos autorizados podem ocorrer. Autenticar uma mensagem significa provar a identidade de sua origem. A autorização do pagamento pode ser obtida de diversas maneiras (LYNCH, LUNDQUIST, 1996).

##### **a. Out-band:**

Autorização *out-band* significa que a parte verificadora - normalmente o banco - manda uma notificação ao *payee* e solicita a aprovação ou negação do pagamento usando

um canal seguro como o correio, o telefone ou o e-mail (como o First Virtual).

**b. Senha:**

Na criptografia de chave compartilhada a parte verificadora solicita uma senha conhecida apenas pelas partes autorizadora e verificadora para ser incluída em todas as mensagens de pagamento (algo como o *Personal Identification Number* - PIN – ou outra senha secreta) (SCHNEIER, 1996 e BRYANT, STEINER E KOHL, 1989). A mensagem é autenticada através de um valor de conferência criptografado, o Código de Autenticação de Mensagem (MAC).

**c. Assinatura:**

A parte verificadora pede uma assinatura digital da parte autorizadora. Isso envolve assimilação de mensagem e criptografia de chave pública (RIVEST, 1992 e SCHNEIER, 1996). Na criptografia de chave pública, cada parte tem um par de chaves. A chave da assinatura é mantida em segredo. A chave de verificação é pública e possui um certificado que liga a identidade do dono a ela. Os certificados são assinados por uma autoridade notória chegando-se assim a uma corrente de confiança. As assinaturas geram aceitação, pois somente a parte autorizadora conhece a chave secreta.

**d. Dual Signature (Assinatura Dupla):**

Existem casos onde é necessário juntar a autorização de pagamento à oferta que recebe essa autorização, como o



SET. Uma *dual signature* permite combinar duas mensagens separadas de tal modo que elas não possam ser usadas separadamente. Uma mensagem pode ser enviada separadamente e verificada pela *dual signature* como pertencente ao contexto da outra mensagem. *Dual signature* concatena a assimilação da oferta com a assimilação da autorização do pagamento e assina a nova assimilação resultante para obter provas do pagamento sem revelar a oferta (MASTERCARD–SET, 1996).

*e. Blind Signature:*

A técnica de *blind signature* pode ser usada na obtenção de não-rastreamento. Ela permite que o banco emissor autorize o pagamento digital feito pelo *payer* sem ler o número de série único do *token* que foi gerado pelo *payer*. O *payer* omite o número de série e o submete ao emissor para autorização. O emissor assina o *token* que possui o número oculto e devolve-o ao *payer* após deduzir o valor do *token* da conta do *payer*. Depois, o *payer* revela o número de série e o *token* mantém sua assinatura válida.

*f. Offline Tokens:*

Para sistemas *off-line*, sem opção de conferência antes ou durante a transação, foi desenvolvida uma modificação nessa técnica. Uma vez escondida, duas vezes revelada, como no CAFE. Isso inclui o compartilhamento do segredo que permite revelar a identidade do *payer*. Cada *token* contém uma parte da identidade do *payer* e se ele gastar a mais, será possível achar a identidade do *payer* através das várias cópias. Duas transações de pagamento

completas, nas quais o *payer* participa usando as mesmas moedas, tornaria necessária sua identificação. Se ele fizer apenas uma transação com cada moeda, ele ainda manteria seu anonimato.

*g. Challenge Response:*

As técnicas de *Challenge Response* permitem a autenticação sem que nenhuma informação seja revelada (prova de conhecimento zero) (SCHNEIER, 1996), portanto protegendo contra ataques. Uma parte envia uma mensagem aleatória e a parte desafiada dá a resposta computada pela chave compartilhada. Essa técnica é muito usada em autenticação de *smart cards* entre si.

*h. Divisão em cadeia:*

Pagamentos subseqüentes ao mesmo payee podem ser feitos por pagamentos em corrente, como no PayWord, que podem ser verificados com base nos recebimentos anteriores. Esse método só é interessante para micro-pagamentos.

### **1.2.6. Custos**

O custo de uma transação refere-se aos custos técnicos e não às taxas baseadas na política imposta pelo fornecedor.

Reembolsar compradores, risco de crédito, manutenção de registros, propaganda e custo de promoção, alta margem de lucro, custos operacionais de servidores, comunicação e custo de estoque e processamento são outros fatores de custo de sistemas de pagamento digital.

*a. Setup do sistema:*

Os custos da instalação do sistema cobrem a fase de decidir-se por um determinado sistema de pagamento até ele estar pronto para a primeira operação. Isso pode, por exemplo, compreender custos para obtenção de um *smart card* e equipamentos de leitura, custo para ajustar uma oferta digital juntamente com o sistema de pagamento, custo para se obter credenciais que permitam que o *payer* efetue o pagamento ou o custo que permite que o *payee* receba o pagamento, isto é, custo de instalação e registro. Para se adotar um protocolo de pagamento, o custo médio por transação deve ser baixo.

*b. Transação:*

Os custos da transação cobrem os custos para pagamentos individuais. Os custos de uma transação de pagamento podem ser estimados considerando-se sua latência (explicado abaixo). O custo da transação para o primeiro pagamento a um *payee* pode diferir dos custos para pagamentos subseqüentes para o mesmo *payee*, como no MilliCent . Os custos regulares da transação podem diferir dos custos de transações excepcionais, isto é, se os limites forem ultrapassados, como no Mini-Pay. Normalmente, sistemas que permitem micro-pagamentos oferecem uma estimativa de custo detalhada para diferentes situações (LEHRE, 1997).

*c. Latência:*

Esse estado descreve o tempo necessário para completar a transação. O número da operação da chave pública e/ou o volume de mensagens solicitadas para completar a transação podem ser usados na estimativa e na comparação da latência, que deve ser a menor possível.

**1.2.7. Genealogia**

A genealogia de um sistema de pagamento ajuda a compreender mais facilmente esse sistema. Relações com outros sistemas de pagamento – como herança, influência ou similaridade – podem ser usadas para caracterizar um sistema mais fácil e eficientemente.

## 2. Requisitos

Definimos aqui os requisitos dos sistemas de pagamento eletrônico para a *Internet*. A importância dessas características individuais é determinada pela necessidade do usuário. Por exemplo, um usuário que dê maior importância ao anonimato nas transações, um outro que faça transações de baixo valor e não se importe muito com o anonimato. Ao optar por um determinado sistema (MACKIE-MASON, WHITE, 1997), essas características devem ser levadas em conta.

### 2.1. Transação

Uma transação monetária deve estar em conformidade com as condições ACID (CAMP, SIRBU, TYGAR, 1995).

#### 2.1.1. Atomicidade

A transação é completa ou então não ocorre.

- **Transferência de fundos:** Uma simples transferência de fundos é atômica. Isso quer dizer que ou há o débito em conta da quantia correspondente ou não há débito nenhum.
- **Transferência completa:** A transferência de fundos e a transferência de dinheiro são ligadas e atômicas. Isto é, uma entrega de documento está ligada ao seu pagamento e ambos ocorrem ou não. Essa é a idéia básica do protocolo de troca. (CAMENISCH, PIVETAU, STADLER, 1995; STADLER, PIVETAU, CAMENISCH, 1996; e ZWISSLER, 1996).

### **2.1.2. Consistência**

Todas as partes envolvidas devem estar de acordo com os fatos relevantes da transação, isto é, concordam com a quantia a ser transferida, com o motivo da transferência e com o fato da ocorrência da transação.

### **2.1.3. Isolamento**

As transações devem ser independentes umas das outras. O resultado de transações concomitantes deve ser o equivalente a uma sequência de transações.

### **2.1.4. Durabilidade:**

A recuperação do último estado consistente deve ser possível. Mesmo depois da queda de um sistema, o estado deve ser recuperável, por exemplo, a quantia de dinheiro disponível deve ser a mesma.

## **2.2. Segurança**

Sistemas de pagamento digital devem possuir questões de segurança como proteção contra fraudes e garantia de privacidade (GARFINKEL, 1995), gerando assim um instrumento confiável. Os consumidores geralmente preferem anonimato quando utilizam dinheiro digital.

### **2.2.1. Proteção contra fraudes**

Os sistemas de pagamento digital devem ser invioláveis e protegidos contra ataques. O uso ilegal de dinheiro digital deve ser evitado ou pelo menos devem existir meios de detecção e punição para o seu mau uso. A falta de proteção resultaria na perda da confiabilidade. O sistema deve oferecer proteção contra ataques como modificação ou recusa de mensagens de pagamento. A origem e o destino dos dados devem ser autenticados. Criptografia, assinaturas e mensagens podem ter essa finalidade. Alguns sistemas também usam medidas de segurança *out band* (ASOKAN, JANSON, STEINER E WAIDNER 1997) como reconfirmação por *e-mail* ou fax (First Virtual).

- **Sem duplo gasto:** Questão importante a ser tratada. O dinheiro digital é representado por *bytes* que podem facilmente ser copiados e gastos mais de uma vez. Isso preocupa não só o consumidor, mas também o comerciante. Bancos de dados de gastos duplos são usados para registrar o gasto do dinheiro digital.
- **Sem falsificação:** O dinheiro só pode representar valores se for impossível falsificá-lo. Pelo menos, o uso

desse dinheiro ilegal deve ser facilmente detectável (CAMP, SIRBU, TYGAR, 1995).

- **Sem gastos acima do limite:** Deve haver uma prevenção contra gastos acima dos limites (HETTINGA, 1997).
- **Não refutável:** As partes envolvidas devem poder verificar a realização do pagamento e qual foram os dados e o total da transação. Deve haver um registro da transação. Isso envolve perda de privacidade (FAJEN, 1996).
- **Hardware inviolável:** Alguns sistemas dependem de hardware inviolável como smart cards na prevenção de duplo gasto e falsificação (DIGICASH, 1995) e podem ser usados offline. No entanto, a quebra desse hardware possibilitaria ataques (ANONYMOUS, 1997). A confiabilidade do hardware deve ser certificada.
- **Uso não autorizado:** O mecanismo de pagamento não pode ser passível de roubo nem ter seu uso efetuado sem autorização.

### **2.2.2. Controle de privacidade**

Os consumidores preferem que seus hábitos de consumo sejam confidenciais. Alguns até mesmo preferem que nem o comerciante nem o banco possam rastrear e observar seus gastos. Quando uma parte possui uma informação que a outra parte desconhece, essa informação é dita privada (CAMP, SIRBU, TYGAR, 1995). Os participantes da transação podem querer ter o controle do nível de



privacidade em diferentes elementos da transação como quantia, data, hora, local, produto e identidade. A informação pode ser facilmente observada, pode ter uma gama limitada de valores, pode ser observada apenas sob determinadas circunstâncias ou ser completamente oculta. Restrições legais podem ser aplicadas. O monitoramento do padrão de gastos do usuário e a determinação de seu perfil devem ser impossíveis. Esse fato deveria pelo menos ser dificultado para desestimular a tentativa de rastreamento do indivíduo. Os sistemas de pagamento tradicionais como cartões de crédito e cheques permitem que as ações do usuário sejam conhecidas, o que não ocorre com o dinheiro vivo.

- **Privacidade:** A observação de transações em sistemas de pagamento eletrônico é uma preocupação para os usuários que preferem conduzir confidencialmente seus negócios. Portanto, a privacidade é essencial para a aceitação de um sistema de pagamento. A criptografia pode ocultar os dados em trânsito entre consumidor e comerciante.
- **Anonimato:** A identidade do usuário de moeda digital deve ser protegida. Quando sua identidade está oculta, a transação é dita anônima (CAMP, SIRBU, TYGAR, 1995). O anonimato pode existir na relação consumidor/comerciante ou em todas as relações, incluindo bancos. Pseudônimos podem ser usados no lugar da identidade real.
- **Impossibilidade de rastreamento:** Quando não há a possibilidade de juntar diferentes pagamentos feitos pelo

mesmo usuário, a transação é não rastreável, além de anônima (ASOKAN, JANSON, STEINER, WAIDNER, 1997). Uma terceira parte pode fornecer meios que garantam essas características. *Blind signatures* (CHAUM, 1982) dispensam essa terceira parte e podem garantir anonimato e não rastreamento para o comerciante e também para os bancos emissores e adquirentes.

## **2.3. Interoperabilidade**

No cenário do comércio eletrônico, diferentes partes e objetivos estão envolvidos, como diferentes consumidores e comerciantes, seus bancos e provedores de serviços, quantias, moedas e sistemas de pagamento.

### **2.3.1. Divisibilidade**

A moeda eletrônica deve permitir transações pequenas e grandes. Portanto, a divisibilidade deveria garantir que uma única transação de alto valor pudesse ser dividida em várias transações de menor valor (CAMP, SIRBU, TYGAR, 1995). Isso apenas se aplica a sistemas com *tokens*.

### **2.3.2. Bidirecionamento**

Comerciante e consumidor podem receber pagamentos. Tal sistema permite reembolsos eficientes. Por exemplo, um cheque é bidirecional e o cartão de crédito não.

### **2.3.3. Gasto encadeado**

Quem recebe a moeda digital pode transferi-la a outra pessoa, como o dinheiro normal, sem a intervenção de uma terceira parte (como um banco). O *payee* não precisaria de etapas intermediárias para gastar o pagamento recebido. Por exemplo, o pagamento feito com cartão de crédito precisa ser depositado em um banco, não permitindo assim um gasto encadeado. Os pagamentos digitais que permitem essa transferência podem ser não-rastreáveis, mas têm uma segurança menor do que os sistemas supervisionados.

#### **2.3.4. Aceitação**

O dinheiro eletrônico emitido por um banco deve ser aceito por outros bancos. Consumidores e comerciantes precisam usar o mesmo banco para poderem operar. Isso sustenta a escalabilidade de um sistema de pagamento digital.

#### **2.3.5. Suporte a várias moedas**

O valor de um sistema de pagamento digital aumenta de acordo com o número de usuários que o aceitam. O suporte a uma única moeda impede uma aceitação mundial. Portanto, é necessária uma conversão entre várias moedas (CAMP, SIRBU, TYGAT, 1995).

#### **2.3.6. Intercâmbio**

É a facilidade de troca entre um sistema de pagamento digital por outro. As diferentes necessidades dos usuários facilitariam a coexistência de vários sistemas de pagamento o que permitiria a escolha do sistema que melhor se encaixasse a uma determinada transação. Além disso, haveria a possibilidade de transformar a moeda de um sistema em moeda de outro.

#### **2.3.7. Possibilidade de transferência**

O instrumento de pagamento não deve estar vinculado a um indivíduo em particular. Ele deveria ser usado por outras pessoas que não o dono. Isso envolve uma perda de segurança. Por exemplo, o dinheiro vivo e um cartão de telefone são transferíveis, o cartão de crédito não.

### **2.3.8. Portabilidade**

Segurança e usabilidade do sistema de pagamento não devem depender da localização física, por exemplo, um determinado computador.

### **2.3.9. Flexibilidade**

Diferentes níveis de segurança são necessários, dependendo das necessidades das partes envolvidas, como quantia a ser transferida, duração do pagamento ou prova de transação. Uma infraestrutura ideal de pagamento aceitaria vários métodos de pagamento integrados em um sistema comum (ABAD-PEIRO, ASKAN, STEINER, WAIDNER, 1996), como o InterPay, JEPI ou JECF. Para isso, o sistema deve possuir uma interface de programação padronizada.

## **2.4. Escalabilidade**

Uma grande base de consumidores e comerciantes de um dado sistema é pré-requisito crucial para sua aceitação. Ao se adicionar novos recursos e novos usuários, o sistema deve continuar a funcionar sem perda de performance. Os sistemas de pagamento digital devem suportar muitos usuários fazendo compras concomitantes de vários comerciantes. Alguns sistemas, como, por exemplo, o Ecash, registram em um servidor central todas as moedas gastas para prevenir seu gasto duplo, checando o identificador único dessa moeda antes da de cada transação. Essa base de dados crescerá diminuindo assim sua escalabilidade, pois as buscas às bases de dados aumentam. O protocolo deveria limitar o número total dos consumidores por comerciante ou o número de transações que podem ser feitas com um dado vendedor.

- **Operações off-line:** Consumidores e comerciantes deveriam poder negociar sem uma terceira parte que estivesse o tempo todo on-line. Isso reduz a demora e aumenta a disponibilidade do sistema de pagamento além de fornecer as bases para a escalabilidade. Um sistema de pagamento que necessita de operações on-line está sujeito a demoras decorrentes do congestionamento das redes, diminuindo assim a sua credibilidade.

## **2.5. Micro Economia**

Serviços de informação serão oferecidos fragmentados, como um verbete de enciclopédia ou de lista telefônica, mecanismos de busca ou artigos de jornal. O pagamento dessas mercadorias pede por um sistema que viabilize transações de baixos valores (menos de um dólar ou um centavo). Esses serviços seriam solicitados por inúmeras pessoas o que pediria técnicas de micro-pagamento rápidas e baratas.

### **2.5.1. Baixos custos**

O custo de execução dessas transações deve ser baixo o suficiente para viabilizar preços mínimos. Mesmo a transferência de micro quantias deve ser economicamente viável. O protocolo de pagamento deve adaptar-se às transações de valores iguais ou inferiores a um centavo.

### **2.5.2. Eficiência**

A compra de serviços de informação muitas vezes pede por pagamentos freqüentes de valor reduzido. Os sistemas de pagamento digital devem efetuar esses micro-pagamentos sem perda de performance. Essa eficiência traz uma perda na segurança. Deve permitir apenas o uso de criptografia leve ou mesmo nenhuma.

## **2.6. Economia Geral**

Para se tornar economicamente aceito, o sistema de pagamento digital precisa oferecer serviços confiáveis e economicamente viáveis para uma comunidade suficientemente grande. Deve ser de fácil integração e uso para ser aceito por consumidores e comerciante.

### **2.6.1. Operacional:**

O sistema deve ser operacional para ser empregado nesse momento. Propostas teóricas são de pouca valia para resolver problemas atuais.

### **2.6.2. Grande base de usuários:**

Para um comerciante, o grande atrativo de um sistema de pagamento é o seu número de usuários e vice-versa. O número de consumidores usando um determinado sistema determina o esforço do comerciante em adotá-lo. Os consumidores por sua vez, tendem a adotar os sistemas que ofereçam acesso a muitas lojas.

### **2.6.3. Baixo risco:**

O risco de perda financeira associado ao uso de sistemas de pagamento deve ser baixo e controlável.

### **2.6.4. Confiabilidade:**

O sistema de pagamento eletrônico deve ser totalmente disponível e confiável em suas operações. Mesmo falhas temporárias podem ser fatais para os interesses econômicos dos usuários, acabando por inutilizá-lo.



#### **2.6.5. Conservação:**

A moeda digital deve ser fácil de guardar e recuperar e não ser inutilizada com o tempo (CAMP, SIRBU, TYGAR, 1995). O usuário também tem que ter a possibilidade de acessar esse dinheiro remotamente.

#### **2.6.6. Facilidade de Integração:**

Aplicações e ofertas já existentes precisam ser modificadas para permitir o uso do sistema de pagamento digital. Uma interface de programação padronizada do sistema facilitaria essa tarefa (ABAD-PEIRO, ASOKA, STEINER, WAIDNER, 1996). As solicitações de pagamentos seriam integradas em protocolos de respostas padronizadas nas quais as aplicações poderiam operar, como no InterPay.

## **2.7. Facilidade de uso**

Um sistema de pagamento digital deve ser transparente e de fácil compreensão. Os usuários devem achar o processo de pagamento acessível, efetivo e rápido. As operações devem ser simples, principalmente o início de uma transação deve ser claramente definido para que o usuário não se perca. Nenhuma habilidade especial deve ser necessária. Os parâmetros que influenciam a aceitação são: portabilidade, necessidade de conta, independência de hardware, ergonomia, ausência de criptografia, instalação de software e baixas taxas.

### **2.7.1. Sem obstrução:**

Este é um importante fator para a facilidade de uso dos sistemas de pagamento. Os usuários não devem ser interrompidos para fornecer informações de pagamento o tempo todo. A maioria dos pagamentos deve ocorrer automaticamente. Isso é particularmente importante para pequenos pagamentos. O consumidor não precisa iniciar novas ações para efetuar um pagamento. Devem ser necessários poucos passos para completar a transação. O usuário deve poder setar um perfil de gasto para controlar sua conta. Os pagamentos que ultrapassem um certo limite devem pedir uma reconfirmação.

### **2.7.2. Baixa latência:**

A transação de pagamento deve ser rápida e não deve atrasar o ato da compra.

### **2.7.3. *Baixos custos de transação:***

As transações não devem ser caras. O valor de uma transação deve ser relativo ao valor da transferência. As taxas cobradas dos intermediários devem ser baixas, uma porcentagem da quantia negociada.

### **2.7.4. *Baixos custos fixos:***

Instalar e usar um sistema de pagamento deve ser barato.

### **2.7.5. *Independência de hardware:***

Não deve haver necessidade de hardware especializado.

### 3. Perfis

#### 3.1. *Perfil de características*

##### Definição das Características

- **Endereço Web:** URL
- **Nome:** Nome do sistema.
- **Origem:** Autores e patrocinadores do sistema.
- **Status:** Status do sistema de pagamento e datas.
- **Tamanho do pagamento:** Tamanho ideal, mínimo e máximo do pagamento.
- **Modelo de moeda:** Modelo da moeda usada pelo sistema, isto é, token ou notacional.
- **Modelo de Pagamento:** Modelo de pagamento usado pelo sistema, por exemplo, cash-like, account-based, apresentação segura do cartão de crédito.
- **Validação:** Tipo da validação do pagamento, isto é, on-line, offline ou semi-on-line.
- **Controle de Privacidade:** Nível de privacidade, anonimato e possibilidade de rastreamento que o sistema oferece.
- **Mecanismo de segurança:** Tecnologias de segurança usadas, por exemplo, senhas, assinaturas, criptografia.
- **Pré-requisitos:** Hardware, software e outras necessidades do sistema.

- **Risco:** Quem tem risco de perda financeira.
- **Taxas:** política de taxas do sistema de pagamento digital.
- **Latência/Custos:** Duração e custo de uma transação de pagamento individual.
- **Base de usuários:** Número de consumidores e comerciantes que utilizam o sistema.
- **Limites:** Limites do sistema de pagamento, por exemplo, operacional apenas nos Estados Unidos.
- **Notas:** Outras características especiais do sistema.
- **Genealogia:** Características herdadas de outros sistemas. Sistemas similares

### 3.2. Perfil de requisitos

Comparação dos requisitos dos sistemas de pagamento tradicionais

Tabela 2 : Requisitos dos sistemas de pagamento tradicionais

<b>Requisitos/Sistema</b>	<b>Dinheiro</b>	<b>Cheque</b>	<b>Cartão de Crédito</b>
Sistema de token	Sim	Não	Não
<b>Transação</b>			
Atomicidade	Sim	Não	Não
Consistência	Sim	Sim	Sim
Isolamento	Sim	Não	Não
Durabilidade	Sim	Sim	Sim
<b>Segurança</b>			
Sem gasto dobrado	Sim	–	–
Sem falsificação	Alguma	Não	Não
Sem limite de gastos	Sim	Não	Não
Não-refutável	Não	Sim	Sim
Sem uso não-autorizado	Não	Algum	Algum
Anonimato	Sim	Não	Não
Sem traços	Sim	Não	Não
<b>Interoperabilidade</b>			
Divisibilidade	Sim	–	–
Bidirecionamento	Sim	Sim	Não
Gasto encadeado	Sim	Não	Não
Aceitação	Sim	Sim	Sim
Suporte a várias moedas	Sim	Sim	Sim
Possibilidade de troca	Sim	Parcial	Não
Possibilidade de transferência	Sim	Não	Não
<b>Escalabilidade</b>			
Escalabilidade	Sim	Sim	Sim
Operações Offline	Sim	Sim	Não
<b>Questões Econômicas</b>			
Operacional	Sim	Sim	Sim
Grande base de usuário	Sim	Sim	Sim
Risco do comprador	Sim	Não	Limitado
Risco do vendedor	Não	Sim	Não
Confiabilidade	Sim	Sim	Sim
Conservação	Sim	Sim	Sim
<b>Facilidade de uso</b>			
Sem obstrução	Sim	Sim	Sim

Baixa latência	Sim	Sim	Sim
Micro-pagamentos	Sim	Não	Não
Macro-pagamentos	Não	Sim	Sim
Baixos custos fixos	Sim	Sim	Sim
Independência de hardware (consumidor)	Sim	Sim	Sim
Independência de hardware (vendedor)	Sim	Sim	Não

A tabela acima mostra os requisitos dos sistemas tradicionais (CAMP, SIRBU, TYGAR, 1995). No caso do dinheiro, as propriedades ACID são alcançadas. Os cheques não são atômicos devido à demora no desconto. O cartão de crédito pode parecer ter uma transferência atômica para o vendedor, mas o emissor pode sofrer perdas devido ao atraso no desconto. Uma transação com cheque ou cartão não é isolada por causa da demora do desconto. Essa demora pode causar alteração na conta e o resultado da transação pode ser alterado. Divisibilidade é uma preocupação apenas dos sistemas de tokens. Sistemas de cheque e cartão de crédito não necessitam de troco.

### 3.3. Perfil de visibilidade

As questões controle de privacidade e revelação de informações associadas a uma transação podem ser caracterizadas por tabelas de visibilidade (CAMP, SIRBU, TYGAR, 1995). As tabelas mostram a visibilidade da informação para cada uma das partes envolvidas na transação direta ou indiretamente. Cada pagamento tem seu próprio perfil de visibilidade intrínseco. Essas características fazem um protocolo adaptar-se melhor a uma situação do que a outras.

Tabela 3 : Visibilidade do dinheiro vivo

<b>Quem/O que</b>	<b>Comerciante</b>	<b>Comprador</b>	<b>Data</b>	<b>Quantia</b>	<b>Item</b>
Comerciante	–	Parcial	Sim	Sim	Sim
Comprador	Sim	–	Sim	Sim	Sim
Banco	Não	Não	Não	Não	Não
Observador	Sim	Parcial	Sim	Sim	Sim

A tabela acima mostra que a transação com dinheiro é completamente privada e anônima em relação ao banco, mas não em relação ao consumidor, comerciante e observador.

Tabela 4 : Visibilidade da transação com cheque

<b>Quem/O que</b>	<b>Comerciante</b>	<b>Comprador</b>	<b>Data</b>	<b>Quantia</b>	<b>Item</b>
Comerciante	–	Sim	Sim	Sim	Sim
Comprador	Sim	–	Sim	Sim	Sim
Banco	Sim	Sim	Sim	Sim	Não
Observador	Sim	Sim	Sim	Sim	Sim

As transações com cheque e cartão de crédito são menos anônimas do que a transação com dinheiro vivo. A tabela acima mostra o perfil de visibilidade de um cheque pessoal cruzado (CAMP, SIRBU, TYGAR, 1995).



Tabela 5 : Visibilidade em uma transação com cartão de crédito

<b>Quem/O que</b>	<b>Comerciante</b>	<b>Comprador</b>	<b>Data</b>	<b>Quantia</b>	<b>Item</b>
Comerciante	–	Sim	Sim	Sim	Sim
Comprador	Sim	–	Sim	Sim	Sim
Banco	Sim	Sim	Sim	Sim	Não
Observador Físico/ Digital	Sim/Parcial	Parcial	Sim	Sim/ Não	Sim/Não

A tabela acima mostra o perfil de visibilidade de uma transação EFTPOS com cartão de crédito (CAMP, SIRBU, TYGAR, 1995). Neste caso, dois tipos de observadores são possíveis. O observador físico, que está presente na loja e o observador digital que monitora o tráfego na rede, mas não pode ler a informação criptografada.

Nos sistemas de pagamento digital e transações eletrônicas, apenas os observadores digitais são relevantes. Algumas transações digitais podem ser mais confidenciais, anônimas e de difícil rastreamento do que as tradicionais, pois escondem do comerciante a identidade do consumidor e vice-versa.

#### **4. Classificação e Visão Geral dos Sistemas**

Será apresentada uma visão geral dos sistemas de pagamento digital e suas propostas, que serão analisados em detalhe mais adiante. Esta sessão tem como objetivo dar uma visão rápida dos diferentes sistemas de pagamento digital. Para ajudar na tarefa de selecionar um desses sistemas, eles podem ser classificados de acordo com subconjuntos de suas características, dependendo dos interesses do leitor ou analista.

Esses grupos precisam estar em uma divisão apropriada, ou seja, é melhor que eles não sejam nem muito grandes, nem muito pequenos, para possibilitar a obtenção de informações úteis. Deste modo, algumas ramificações têm que ser abortadas em um certo nível para evitar grupos vazios ou com poucos componentes.

#### 4.1. Classificação tecnológica

Classificação tecnológica dos sistemas de meio de pagamento eletrônico

Tabela 6 : Classificação tecnológica dos mpe

Modelo	Token	Notacional		
<b>Validação</b>	Direct Cash	Direct Account	Cartão de Crédito	Push Account
<b>On-line</b>	Ecash	BankNet	ACC	AIMP
	MagicMoney	CyberCoin	C.-POINT	ATS
	NetCash	FSTC	Carteira Bradesco	CheckFree
	PayMe	NetBill	CyberCash	eVend
		NetCheque	First Virtual	NetFare
		DSR	iKP	
			Secure Courier	
			SET	
			VeriFone	
			Yahoo Purse	
<b>Semi-on-line</b>	MilliCent	Agora		
		Mini-Pay		
		Polling		
<b>Offline</b>	<i>Hardware</i>	CyberCents		
	Brands	InterCoin		
	CAFE			
	Geldkarte			
	Mondex			
	<i>Cadeias</i>			
	MPTP			
	Mykro-iKP			
	NetCard			
	PayWord			
	PhoneTicks			
	SubScrip			
	<i>Outros</i>			
	Lottery			
	MicroMint			
	TUB			

Essa tabela mostra uma possível classificação dos sistemas de pagamento digital por tecnologia. Os modelos de moeda são *token* e notacional. Os modelos de pagamento são: *direct cash-like*, *direct account based*, *indirect push account based* e apresentação

segura de cartão de crédito. A validação pode ser feita *on-line*, *offline* ou *semi-on-line*. A segurança básica é fornecida com *smart cards*, divisões em cadeia ou outros meios.

Sistemas notacionais baseados em indirect push account são, por definição, validados *on-line*, porque o banco é uma terceira parte envolvida em cada pagamento. Esquemas notacionais de apresentação segura de cartão de crédito são validados *on-line* também, porque freqüentemente grandes pagamentos estão envolvidos nessas transações. Sistemas de pagamentos validados *offline* ou *semi-on-line* mexem com pequenos ou micro-pagamentos, e um certo risco no pagamento é aceito para melhorar a eficiência.

## 4.2. Classificação Econômica

Tabela 7 : Classificação econômica dos sistemas de meio de pagamento eletrônico

Status/Tamanho	Macro-pagamentos	Pequenos Pagamentos	Micro-pagamentos
<b>Operacional</b>	ATS	Cybercoin	
	BankNet	eVend	
	Carteira Bradesco	InterCoin	
	CheckFree		
	CommercePOINT		
	CyberCash		
	First Virtual		
	Secure Courier		
	VeriFone		
	Yahoo Purse		
<b>Teste</b>	NetCheque	CAFE	MilliCent
		Ecash	
		MagicMoney	
		Mondex	
		NetBill	
		NetCash	
<b>Em desenvolvi- mento</b>	FSTC	Geldkarte	Mini-Pay
	SET	CyberCents	NetFare
<b>Proposta</b>	ACC	Brands	Agora
	AIMP	PayMe	DSR
	iKP		Lottery Tickets
			MicroMint
			MPTP
			Mykro-iKP
			NetCard
			PayWord
			PhoneTicks
			Polling
			SubScrip
			TUB

Essa tabela mostra uma possível classificação econômica dos sistemas de pagamento digital. O tamanho do pagamento pode variar entre macro, pequenos e micro pagamentos. O status de um sistema de pagamento pode ser operacional, uma proposta (talvez

incluindo um protótipo), em desenvolvimento, testes públicos ou fechados (Davies, 1997).

A maiorias dos sistemas que estão em funcionamento envolvem soluções não padrão a respeito de apresentação segura de cartão de crédito ou esquemas que mantêm simples contas com o comerciante ou com o banco. Sistemas em teste algumas vezes podem não passar para o estágio operacional em função de dúvidas sobre a segurança e riscos advindos do comprometimento do sistema. Existem várias propostas de esquemas de micro-pagamentos, mas nenhuma conseguiu uma grande aceitação até o momento.

## 5. Propostas Individuais

Serão apresentadas as propostas de meio de pagamento eletrônico, operacionais ou não. As propostas significativas, assim como algumas de menor relevância, estão descritas com os conceitos básicos, medidas de segurança e etapas de transação e classificadas conforme os critérios apresentados anteriormente.

### 5.1. ACC

EndereçoWeb:

<http://portal.research.bell-labs.com/lateinfo/projects/ecom.html>

Nome: ACC

Status: proposta, 1994.

Genealogia: extensão a proposta AIMP

ACC, protocolo de cartão de crédito anônimo. Proposta de D. Kristol, S. Low, N. Maxemchuck e S. Paul da AT&T Bell Labs de 1994. (KRISTOL, LOW, MAXEMCHUCK, 1994a e LOW, MAXEMCHUCK, PAUL, 1994)

A idéia central é separar todas as informações necessárias para uma transação em componentes diferentes e utilizar técnicas de criptografia para ocultar os componentes que não são necessários a uma determinada parte.

Com o ACC, o comprador está fisicamente na loja e faz uma compra física. Sua identidade está escondida. O Protocolo é estendido para uso na *Internet* no trabalho dos autores sobre AIMP, protocolo mercantil anônimo da *Internet*.

## **5.2. AGORA**

Endereço Web: <http://www.bell-labs.com/user/eran/agora.html>

Nome: Agora

Origem: E. Gabber e Silberschatz da AT&T Bells Lab.

Status: proposta e pequeno protótipo, Novembro 1996.

Pagamentos: micro-pagamentos, talvez grandes.

Agora pretende ser um protocolo de distribuição mínima para comércio eletrônico proposto por E. Gabber e A. Silberschatz do Bell Labs (GABBER, SILBERSCHATZ, 1996). Foi apresentado no workshop de comércio eletrônico USENIX em 1996. Existe um protótipo com applets Java para o Netscape e scripts cgi conectados a um banco de dados do servidor NCSA.

Agora suportaria um alto volume de transações a um baixo custo. É um protocolo notacional baseado em contas de crédito, ou seja, identificadores de contas são usados no pagamento. Compradores e comerciantes precisam ter contas válidas em seus respectivos bancos. Agora trabalha com vários bancos que se conectam através de uma rede financeira e com um modelo de custos pay per view.

Agora é autenticado por assinaturas digitais. Todas as partes envolvidas necessitam de suas próprias chaves pública e privada. O emissor e o adquirente proporcionam, respectivamente ao consumidor e ao comerciante, identificadores válidos para um certo período para se identificarem através da certificação da chave pública de seus clientes que vem juntamente com um nome único, data de validade e número da conta do identificador. Os consumidores e comerciantes devem saber a chave pública de



todos os bancos envolvidos. Os falsificadores seriam detectados na checagem do nome único com o nome esperado.

O protocolo é chamado de mínimo, pois seu custo é reduzido. São necessárias quatro mensagens para completar uma transação com o Agora, incluindo a transferência de bens sem nenhum acesso on-line a uma autoridade central. Quando usado como um protocolo de comércio na Web, essas mensagens podem ser adicionadas a mensagens http já existentes, sem a necessidade de outras novas.

O fluxo de mensagem básico para uma transação de compra é o seguinte:

- O cliente solicita uma oferta do comerciante, por exemplo, pedindo uma página de menu pelo método GET.
- O comerciante retorna junto com sua identificação assinada pelo adquirente uma oferta obrigatória assinada, que contém uma identificação original da oferta, por exemplo, retornando uma página do menu como formulário de ordem gerado.
- O cliente verifica a validade da identificação do comerciante e a exatidão da assinatura na oferta. Então retorna junto com sua identificação assinada pelo emissor uma ordem assinada baseada nos dados da oferta, por exemplo, através de uma solicitação pelo método GET.
- O comerciante verifica a validade da identificação do cliente e a exatidão da assinatura na ordem assim como os dados da ordem que correspondem aos dados da oferta. Então o comerciante fornece os bens ao cliente, por exemplo, liberando a página *pay per view*.

Os comerciantes submetem periodicamente ao adquirente ordens acumuladas para o estabelecimento. Uma dupla cobrança pode ser detectada pelo banco graças à identificação original da ordem. A oferta e a ordem fornecem juntas a prova da transação.

Agora é distribuído e escalável. Os comerciantes podem autenticar clientes sem acessar uma terceira parte. Os clientes com contas válidas podem compra de todas as lojas sem nenhuma preparação especial. Os bancos transmitem listas de clientes com identidades bloqueadas aos comerciantes que podem armazenar e segurar estas listas. O problema de gastos elevados é dirigido introduzindo-se um algoritmo probabilístico que ofereça um controle de fraudes. Um comerciante pede ao adquirente autorização on-line com uma determinada probabilidade ou cada vez que o total de ordens de um cliente exceder um limite predefinido.

Tabela 8 : Perfil de visibilidade do Agora:

<i>Quem/O que</i>	<b>Comer- ciante</b>	<b>Comprador</b>	<b>Dat a</b>	<b>Quan- tia</b>	<b>Ite m</b>
Comprador	Sim	–	Sim	Sim	Sim
Comerciante	–	Parcial- mente	Sim	Sim	Sim
Emissor	Sim	Sim	Sim	Sim	Não
Adquirente	Sim	Parcial- mente	Sim	Sim	Não
Árbitro	Sim	Parcial- mente	Sim	Sim	Sim
Observador	Sim	Parcial- mente	Sim	Sim	Sim

A tabela acima mostra o perfil de visibilidade em uma transação Agora. O protocolo pode dar um certo anonimato ao consumidor, pois usa apelido de contas e não nomes de contas reais. O protocolo não remete a nenhuma questão de privacidade. O uso do http revela muitas informações do cliente para o servidor e a criptografia não faz parte do protocolo do Agora.

O protocolo introduz a arbitragem on-line – uma terceira parte que resolveria disputas. Quando faz uma queixa, o consumidor submete a oferta e o pedido ao árbitro que, por sua vez, envia a solicitação da mercadoria à loja. Se eles correspondem ao pedido, o árbitro os retransmite ao consumidor, ou este cancela o pedido junto ao adquirente.

Tabela 9 : Perfil de Requisitos do Agora

<b>Requisitos/Sistema</b>	<b>Agora</b>
Sistema de token	Não
<b>Transação</b>	
Atomicidade	Sim
Consistência	Sim
Isolamento	Não
Durabilidade	Sim (loja precisa de uma boa base de dados)
<b>Segurança</b>	
Sem gasto dobrado	–
Sem falsificação	Sim
Sem limite de gastos	Limitado, abordagem probabilística.
Não-refutável	Sim
Sem uso não-autorizado	Sim
Anonimato	Sim
Sem traços	Sim, limitado e apenas do lado da loja.
<b>Interoperabilidade</b>	
Divisibilidade	–
Bidirecionamento	Não
Gasto encadeado	Não
Aceitação	Sim
Suporte a várias moedas	Sim, via banco.
<b>Escalabilidade</b>	
Escalabilidade	Sim
Operações Offline	Sim, apenas provável verificação on-line
<b>Questões Econômicas</b>	
Operacional	Não
Grande base de usuário	–
Risco do comprador	Nenhum ou limitado, depende da política do banco.
Risco do vendedor	Sim, depende da política do banco.
Confiabilidade	–
Conservação	Sim
<b>Facilidade de uso</b>	
Sem obstrução	Sim
Baixa latência	Sim
Micro-pagamentos	Sim
Macro-pagamentos	Talvez, limitado.
Baixos custos fixos	–
Independência do HW	Sim

### 5.3. AIMP

EndereçoWeb:

<http://portal.research.bell-labs.com/lateinfo/projects/ecom.html>

Nome: AIMP

Origem: D. Kristol, S. Low, e N. Maxemchuck da AT&T Bell Labs.

Status: proposta e talvez pequeno protótipo, março 1994.

Tamanho do pagamento: Macro-pagamentos, talvez vários micro-pagamentos.

O Protocolo Mercantil Anônimo da *Internet* (AIMP) visa a transferência anônima de fundos pela rede. É uma proposta de D. Kristol, S. Low, e N. Maxemchuck da AT&T Bell Labs, Murray Hill (KRISTOL, LOW, MAXEMBRUCK, 1994b), Nova Jersey de março de 1994. O protocolo aplica os princípios da separação da informação e é uma extensão de um trabalho anterior dos autores, o ACC (cartões de crédito anônimos).

A questão principal do AIMP é facilitar a transferência de fundos anônimos e mercadorias pela *Internet*, protegendo os interesses das partes envolvidas. Procura, proteger os interesses dos comerciantes transferindo fundos e garantindo anonimato ao consumidor através da separação das informações e prova da transação.

AIMP é um protocolo notacional baseado em conta de débito, isto é, identificadores de contas são usados para pagamento. O depósito para o comerciante é feito com o modelo indirect push account based, ou seja, o consumidor transfere fundos para a conta do comerciante como pagamento. Consumidores e comerciantes precisam de contas bancárias válidas. AIMP atende a vários

bancos. Os fundos são transferidos apenas entre entidades de confiança. O protocolo introduz uma terceira parte, um agente. Esse agente permite aos consumidores e vendedores comunicarem-se anonimamente e transferir fundos entre bancos, pois ele intermediaria a troca de informações e a transferência de fundos entre bancos. Para essa transferência de fundos, todos os bancos teriam uma conta com esse agente e todas as transferências seriam assinadas e efetuadas por ele.

Os passos básicos para uma operação de aquisição são as seguintes (nota: todas comunicações são feitas através do agente, todas as mensagens são criptografadas com a chave pública do recipiente):

- O consumidor tem a chave pública do comerciante e - enviando a sua própria chave pública - faz o pedido e obtém anonimamente a conta do comerciante criptografada através do agente.
- O consumidor tem a chave pública do banco do comerciante e transfere fundos anonimamente para essa conta através do emissor e do agente do seguinte modo:
  - O emissor autentica o consumidor por uma senha, debita de sua conta e autoriza o agente a transferir a quantia debitada.
  - O agente transfere fundos da conta do emissor para a do adquirente e o autoriza a transferir a quantia creditada.
  - O adquirente credita na conta do comerciante, gera um recibo e o envia anonimamente através do agente ao consumidor e ao comerciante permitindo a conferência da transação.

- Anonimamente, o consumidor faz o pedido ao comerciante e este deduz o preço da conta da sessão. O pedido é entregue criptografado com a chave pública especificada pelo consumidor. O depósito de fundos adicionais durante uma sessão adiciona mais contas de sessão à mesma.
- Quando o consumidor recebe o que solicitou, envia uma mensagem de saída para o comerciante contendo sua conta anônima. Qualquer quantia que restar nessa conta de sessão é novamente creditada em sua conta. O consumidor recebe um recibo de depósito assinado pelo emissor. Para várias compras pequenas efetuadas ao mesmo comerciante, o consumidor pode escolher manter uma conta de sessão por um longo tempo.

AIMP é confidencial, autenticado e aceito por ambos os lados devido ao uso da criptografia e assinaturas digitais. Todas as partes envolvidas têm seu par de chaves pública e privada. Timestamps e contadores evitam o *replay*.

Tabela 10 : Perfil de Visibilidade do AIMP

<b>Quem/O que</b>	<b>Comerciante</b>	<b>Comprador</b>	<b>Data</b>	<b>Quantia</b>	<b>Item</b>
Comprador	Sim	-	Sim	Sim	Sim
Comerciante	-	Não	Sim	Sim	Sim
Emissor	Não	Sim	Não	Soma	Não
Adquirente	Sim	Não	Não	Soma	Não
Agente	Parcialmente	Parcialmente	Sim	Soma	Não
Observador	Não	Não	Sim	Não	Não

Essa tabela mostra o perfil de visibilidade do AIMP. Depois de uma transação, o comerciante sabe que recebeu pela mercadoria, mas não sabe de quem. O emissor e o adquirente sabem do valor do depósito e do saque, mas desconhecem o destino/fonte e o propósito do pagamento. O agente conhece o emissor e o adquirente, mas não as contas individuais. Nenhuma parte pode associar o consumidor à mercadoria.

Tabela 11 : Requisitos do AIMP

<b>Requisitos/Sistema</b>	<b>AIMP</b>
Sistema de token	Não
<b>Transação</b>	
Atomicidade	Não
Consistência	Não
Isolamento	Sim, pré-pago.
Durabilidade	Sim
<b>Segurança</b>	
Sem gasto dobrado	-
Sem falsificação	Sim
Sem limite de gastos	Sim, pré-pago.
Não-refutável	Sim
Sem uso não-autorizado	Sim
Anonimato	Sim
Sem traços	Sim, necessita de convivência.
<b>Interoperabilidade</b>	
Divisibilidade	-
Bidirecionamento	Sim
Gasto encadeado	Não
Aceitação	Sim
Suporte a várias moedas	Sim, via banco.
<b>Escalabilidade</b>	
Escalabilidade	Sim, vários agentes possíveis.
Operações Offline	Não
<b>Questões Econômicas</b>	
Operacional	Não
Grande base de usuário	-
Risco do comprador	Limitado a depósitos.
Risco do vendedor	Não
Confiabilidade	-
Conservação	Sim
<b>Facilidade de uso</b>	
Sem obstrução	Questionável
Baixa latência	Não
Micro-pagamentos	Parciais
Macro-pagamentos	Sim
Baixos custos fixos	-
Independência do hardware	Sim



#### **5.4. ATS**

Endereço Web: <http://www.merchantrust.com/>

Nome: ATS

Status e Marco: Operacional

Modelo de Pagamento: Indirect push account based, modelo de transferência de fundos. Conta e cartão de crédito seguros.

Mecanismo de Segurança: SSL e out-band, ou seja, e-mails de confirmação.

Serviços de Transação Automática (ATS) facilita pagamentos seguros com cartões de crédito. Os detalhes do pagamento ocorrem entre o consumidor e o gateway da ATS e o comerciante recebe a indicação de falha ou sucesso. A ATS envia e-mails de confirmação como uma segurança adicional para o consumidor e o comerciante.

### **5.5. BANKNET**

Endereço Web: <http://mkn.co.uk/bank>

Nome: BankNet

Origem: BankNet e MarketNet, Grã-Bretanha.

Modelo de pagamento: Direct account based, cheques digitais.

Status: Operacional desde maio de 1995.

Controle de Privacidade: Sem anonimato, completa autenticação do usuário.

Pré-requisitos: Sem hardware, para os cheques digitais WorkHorse para Windows.

Mecanismo de segurança: SSL, cheques eletrônicos criptografados com chave pública e assinatura. Mudando para o SET.

Taxas: Várias taxas para serviços especiais.

Base de usuários: Em torno de 2000 usuários por dia.

Limites: Não acessível entre 1:30 e 7:00 horas; cheque eletrônico somente entre contas do BankNet; disponível somente na Grã-Bretanha.

Nota: Conta checada on-line; sem taxas para transações; limites autodefinidos.

BankNet, uma companhia da MarketNet, opera no Reino Unido e oferece um sistema de cheque eletrônico. Similar ao home banking. Permite que os usuários chequem suas contas e emitam cheques eletrônicos. Outras vantagens estão em desenvolvimento.

BankNet é o provedor de pagamento do MarketNet, um shopping baseado em SSL. Necessário o uso do software WorkHorse para o SSL de 128 bits. Os certificados da MarketNet são assinados pela Eurosign. O sistema do Echeque digital da BankNet está disponível a todos seus correntistas. MarketNet integrará o SET ao serviço bancário do BankNet.

## **5.6. BRADESCO-CARTEIRA ELETRÔNICA**

Endereço Web: <http://www.bradesco.com.br/>

Nome: Carteira Eletrônica Bradesco.

Origem: Banco Bradesco.

Status: Operacional

Tamanho de Pagamento: Macro-pagamentos.

Modelo de Moeda: Notacional.

Modelo de Pagamento: Apresentação Segura de Cartão de Crédito

Validação: on-line.

Controle de Privacidade: Criptografado, não anônimo, rastreável.

Mecanismos de Segurança: Criptografia de chave pública, PIN.

Pré-requisitos: Software para o consumidor e para o comerciante e conta corrente no banco.

Riscos: Consumidor.

Taxas: Para o comerciante, R\$1050,00 na implantação.

Latência/Custos: Baixo.

Base de Usuários: 280 comerciantes

Genealogia: SET *like*

## Transação Carteira Eletrônica Bradesco

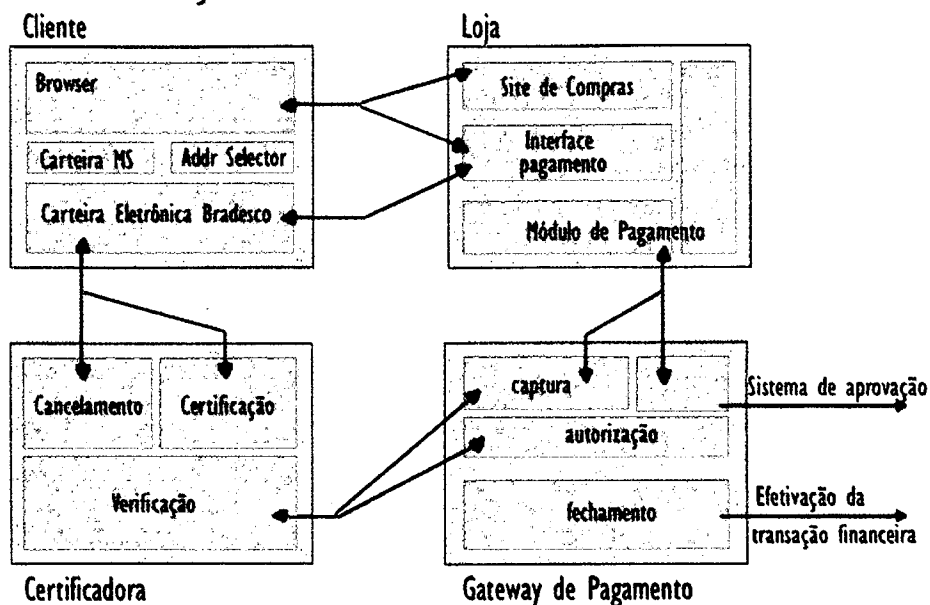


Figura 6 – Transação carteira eletrônica Bradesco

Criada pelo Banco Bradesco. Necessita de software instalado tanto no consumidor quanto no comerciante. Cada consumidor tem um PIN (Número de Identificação Pessoal), que é associado a um número de cartão do banco (débito, crédito, etc). Quando a compra é realizada com algum comerciante conveniado, e escolhida a carteira eletrônica Bradesco como meio de pagamento, o software (carteira) do lado do cliente passa o número de identificação para o servidor do Bradesco. Associado a esse identificador, o número da transação é enviado. Esse registro é enviado para o sistema instalado no site do comerciante. Maiores especificações técnicas ainda não foram divulgadas.

### **5.7. BRANDS CASH**

Endereço Web: <http://www.cwi.nl/~brands/cash.html>

Nome: Brands Cash

Modelo de Pagamento: Token

Status: Proposta de 1994.

Controle de Privacidade: Confidencial, anônimo e sem traços.

Mecanismo de segurança: Criptografia com chave pública, assinaturas, offline tokens, hardware inviolável.

Pré-requisitos: Smartcard e leitor, software especial.

Genealogia: Base para o CAFE

Mecanismo de pagamento pela *Internet* envolvendo Smart Cards.  
Base para o projeto CAFE. O autor é agora pesquisador da Digicash. (BRANDS, 1993, 1994, 1995a, 1995b, 1995c)

## **5.8. CAFE**

Endereço Web: <http://www.cwi.nl/cwi/projects/cafe.html>

Nome: CAFE

Origem: Digicash, CWI, Siemens, universidades de Leuven, Aarhus, Hildesheim, Karlsruhe, e outras, projeto da CE.

Status: Em teste. Projeto terminado em 1997, fase piloto desde 1997, projeto subsequente OPERA .

Tamanho do pagamento: Muito eficiente, com tamanho mínimo e máximo.

Modelo de moeda: Token

Modelo de Pagamento: Como dinheiro vivo.

Validação: Offline

Controle de Privacidade: Criptografia, anonimato, sem traço.

Mecanismo de segurança: Senha, criptografia com chave pública e assinatura, blind signature, token offline, hardware inviolável, base de dados de gasto de tokens.

Pré-requisitos: Carteira, smart cards com terminal do comerciante.

Risco: Transação POS (Point of Sale), dependendo da política do banco, algum risco de perda ou dano na carteira do consumidor.

Taxas: Segurança em todas as partes, várias moedas e suporte do banco.

Latência/Custos: Baixa; autorização local; detecção de gasto duplo após o ocorrido.

Limites: Em teste, momentaneamente para uso fora da *Internet*.

Genealogia: Baseado no Ecash da Digicash e Brands Cash.

O projeto CAFE (Acesso Condicional para a Europa) da União Européia é um esquema direct cash-like offline que garante o anonimato do consumidor. Esse projeto foi terminado em meados de 1997, mas teve continuidade com o projeto OPERA. Os parceiros do OPERA, isto é, bancos que suportam CAFE, continuam com os testes para melhorar o sistema.

Treze parceiros de vários países europeus estão envolvidos no projeto. Digicash e Siemens entre eles. Basicamente, o sistema foi desenhado para uso em lojas e não na *Internet*. De certo modo, é a versão offline portátil do Ecash da Digicash. Baseia-se no sistema proposto pela Brand's cash. O protocolo é aberto ao público. Uma importante característica do CAFE é a segurança de todas as partes. Não há a necessidade de confiança entre partes com interesses conflitantes (CWI, DIGICASH, SIEMENS, 1996b).

CAFE é um sistema aberto seguro. Ele suporta múltiplas edições de valores eletrônicos e múltiplas moedas, incluindo câmbio durante o pagamento. Ele dá ao consumidor um log do histórico de seus pagamentos. O sistema usa assinatura e criptografia de chave pública e permite compras offline. O modo de transação de compra básico é anônimo, não deixa rastros para o consumidor e é feito offline. Não há necessidade de conexão com terceiros. Saques e depósitos são identificados e rastreados on-line. Se o pagamento excede uma determinada quantia, uma confirmação é solicitada, o que pede uma interação on-line.

CAFE prevê o ressarcimento de cartões perdidos, roubados ou danificados. Mesmo sendo pré-pago, há uma tolerância à perda e



permite que os consumidores recuperem seu dinheiro em caso de extravio da carteira. Para isso, uma versão criptografada de todos os tokens emitidos para o consumidor é mantida em local seguro. O consumidor precisa abrir mão de seu anonimato para reaver seus dados. Para garantir certa tolerância às carteiras roubadas, o consumidor deve autenticá-la através de uma senha (PIN - Personal Identification Number) antes da compra.

O device recebe moedas sacando-as da conta do emissor via Banco 24 Horas usando o método da blind signature. CAFE é pré-pago e os tokens do device não existem como moeda em nenhum outro lugar. Quando o consumidor gasta dinheiro, o device transmite um ou mais tokens para o comerciante e marca-os como gastos no device. A conexão é feita por canais infravermelhos. O comerciante, por sua vez, já tem o valor desses tokens que precisam ser depositados no adquirente e aceito pelo emissor. Portanto, o fluxo primário de valores no CAFE é o do saque, pagamento e depósito, ou seja, o modelo tem a abordagem direct cash like.

O hardware básico é uma carteira eletrônica, que será usada para o pagamento das compras feitas pelo consumidor, e acesso a serviços de informação e identificação. As carteiras eletrônicas e os smart cards (o hardware) devem ser padronizados e disponibilizados em lojas como qualquer outro bem de consumo eletrônico. A carteira contém um “guardião”, um smart card com um processador criptografado. A carteira protege os interesses do consumidor, o “guardião” protege os interesses do emissor e ambos contém parte de cada token sacado. Nenhuma transação é possível sem a cooperação do “guardião”, que mantém um registro de todos os tokens gastos para evitar um gasto dobrado. O chip “guardião”

autoriza cada pagamento assinando-o. Os tokens do CAFE não ficam em circulação como os tokens do dinheiro real. O gasto duplo é explicitamente bloqueado, a carteira emite uma assinatura para quem recebe e apenas esse pode depositar o token.

Quando o “guardião” é danificado, CAFE usa moedas digitais offline que garantem o padrão *“once concealed, twice revealed”*. O dinheiro é criptografado e a identidade do consumidor é codificada no número do token. Isso é feito de um jeito tal que a identidade do consumidor só pode ser revelada através de um gasto duplo. Isso funciona basicamente assim: quando o consumidor usa um token para efetuar um pagamento, o comerciante lhe solicita uma parte de sua identidade codificada. Uma parte sozinha não revela nada útil. Se, no entanto o consumidor tentar gastar novamente o mesmo token, outra parte da sua identidade será revelada, o que aumentará consideravelmente a possibilidade de ser rastreado. Por causa disso, o emissor tem que manter um banco de dados de todos os tokens reembolsados.

Perfil de visibilidade do CAFE:

Tabela 12 : Perfil de visibilidade do CAFE

<i>Quem/O que</i>	<b>Comerciante</b>	<b>Comprador</b>	<b>Data</b>	<b>Quantia</b>	<b>Item</b>
Comprador	Sim	Parcialmente	Sim	Sim	Sim
Comerciante	Sim	Sim	Sim	Sim	Sim
Broker	Sim	Não	Sim	Sim	Não
Observador	Sim	Parcialmente	Sim	Sim	Sim

O perfil de visibilidade do CAFE assume um observador físico, pois a transação é offline e o tráfego de informação é feito por um canal infravermelho. Além disso, como a carteira só pode ser usada com uma senha, presume-se que o comprador seja o seu legítimo usuário. E como a carteira mantém um registro básico das

transações, o consumidor pode ter um controle de seus gastos.  
(CWI, DIGICASH, SIEMENS, 1996a)

Tabela 13 : Requisitos do CAFÉ

<b>Requisitos/Sistema</b>	<b>CAFÉ</b>
Sistema de token	Não
<b>Transação</b>	
Atomicidade	Sim para o consumidor, não para o comerciante.
Consistência	Sim
Isolamento	Sim, pré-pago.
Durabilidade	Sim
<b>Segurança</b>	
Sem gasto dobrado	Sim, rastreamento viável após o ocorrido.
Sem falsificação	Sim
Sem limite de gastos	-
Não-refutável	Sim
Sem uso não-autorizado	Sim
Anonimato	Sim, identidade revelada após duplo gasto.
Sem traços	Sim
<b>Interoperabilidade</b>	
Divisibilidade	Sim
Bidirecionamento	Não
Gasto encadeado	Não
Aceitação	Sim
Suporte a várias moedas	Sim, no cartão.
<b>Escalabilidade</b>	
Escalabilidade	Sim
Operações Offline	Sim
<b>Questões Econômicas</b>	
Operacional	Parcialmente, em teste.
Grande base de usuário	n.d.
Risco do comprador	Limitado a conteúdo do cartão.
Risco do vendedor	Não
Confiabilidade	n.d.
Conservação	Sim
<b>Facilidade de uso</b>	
Sem obstrução	Questionável
Baixa latência	Sim
Micro-pagamentos	Sim
Macro-pagamentos	Não
Baixos custos fixos	n.d.
Independência do hardware	Não, sistema de smart card.

Nas transações, CAFE é atômico para o usuário, mas não para o vendedor. Os tokens que o comerciante aceita como pagamento devem ser depositados em um adquirente e aceitos pelo emissor antes que seu valor monetário seja percebido pelo comerciante. O valor sai do consumidor, mas não chega imediatamente ao vendedor. ( BOLDY, BOSSELAERS, CRAMER, MICHELSEN, MJOLSNES, MULLER, PEDERSEN, PFITZMAN, ROOJI, SCHOENMAERS, SCHUNTER, VALLEÉ, WAIDNER, 1994; SCHUNTER, WEBER, 1995).

## **5.9. CHECKFREE**

Endereço Web: <http://www.checkfree.com/>

Nome: CheckFree

Modelo de pagamento: Indirect push account based.

Status: 1988.

Controle de privacidade: Nenhum.

Mecanismo de segurança: Códigos de segurança no sistema de processamento do cheque.

Pré-requisitos: Software para Windows, OS/2 e Macintosh.

Taxas: Primeiros 30 dias livres e depois US\$ 5,95 para os primeiros 20 pagamentos e US\$ 2,95 a cada dez pagamentos. Pelo menos US\$ 5,95 por mês.

Base de usuário: não disponível

Limites: Apenas para cheques nos Estados Unidos.

Notas: Carteira do CyberCash.

CheckFree Corp. mantém uma vasta linha de soluções para comércio eletrônico, incluindo gerenciador on-line de portfolio compartilhado (em conjunção com o sistema PAWWS) (<http://www.pawws.com>) e sistemas on-line de pagamento de contas.

Ela oferece um serviço chamado de pagamento de cheque eletrônico como substituto dos cheques tradicionais. Esse sistema de pagamento resultou num serviço similar para ordem bancária. Seu software é compatível com a carteira eletrônica da CyberCash. O processo de pagamento CheckFree é descrito a seguir:

1. Consumidor recebe uma conta e manda os detalhes de pagamento para a CheckFree.

2. CheckFree paga a conta

3. Contas pagas são listadas em uma cobrança mensal do consumidor.

Ainda não está claro como a CheckFree pega o dinheiro para fazer o pagamento das contas, nem exatamente quando será exigido o pagamento do consumidor. Presumivelmente a conta da CheckFree estará ligada por débito direto às contas dos consumidores. Usando como fonte a pouca informação disponível, esse sistema parece ser mais uma maneira conveniente de pagamento de contas do que um sistema de transações on-line.

### **5.10. ClickShare**

Endereço Web: <http://www.clickshare.com/>

Nome: ClickShare

Modelo de pagamento: registros e faturas.

Controle de privacidade: Nenhum.

Mecanismo de segurança: Senhas.

Pré-requisitos: Conta em um comerciante ClickShare.

Taxas: Nenhuma para o consumidor, pequena porcentagem sobre transação para o comerciante.

Base de usuário: não disponível

ClickShare é um sistema comercial da Newshare baseado em senha. O consumidor ClickShare tem um par de identificador/senha para acessar todos os comerciantes ClickShare.

O sistema permite registro, validação e perfis dos consumidores.

Ele permite micro-transações econômicas e seguras pela *Internet* sem necessitar de software especial para consumidor. ClickShare agrega várias compras e faz as cobranças periodicamente (mensalmente) por um cartão de crédito, crédito convencional ou conta de dinheiro digital.

Os consumidores necessitam de uma conta com um dos comerciantes ClickShare. Isso permite que eles tenham acessos a todos os outros comerciantes ClickShare. A ClickShare valida os consumidores, junta seus pedidos e providencia um boleto para o comerciante que armazena cada conta.

O modelo de negócios utilizado implica numa pequena taxa por transação cobrado pela ClickShare.

### **5.11. CommercePOINT Payments**

Endereço Web: <http://www.ibm.com/software/>

Nome: Commerce POINT.

Origem: IBM

Modelo de pagamento: Apresentação segura de cartão de crédito.

Status: Desenvolvimento, 1997.

Controle de privacidade: Confidencial.

Mecanismo de segurança: Em concordância com SET.

O sistema da IBM CommercePOINT Payments procura desenvolver um sistema de pagamento baseado em cartão de crédito compatível com o SET.

CommercePOINT irá disponibilizar os seguintes programas: Carteira eletrônica para o consumidor, eTill para os comerciantes e gateway para os processadores de pagamentos.



### **5.12. Cybank**

Endereço Web: <http://www.cybank.net/>

Nome: Cybank

Status: Operacional, 1996.

Tamanho dos Pagamentos: Pequenos pagamentos

Modelo de pagamento: Account based, cartão de crédito.

Controle de privacidade: Confidencial, pseudônimos, logs de transação, múltiplas contas.

Mecanismos de segurança: Criptografia de chave pública, criptografia tripla de senha.

Pré-requisitos: Software de smart card virtual, disponível para Windows, cartão de crédito.

Taxas: 5% sobre saques da conta do Cybank

Base de usuários: Por volta de 2.000 usuários.

Limites: não disponível

Notas: Transação reversível se o consumidor não estiver satisfeito.

Cybank disponibiliza um serviço pagamento baseado em contas para consumidores com cartão de crédito. Ele funciona com um smart card virtual baseado em software. Uma lista de todas as transações será acessível via Web. O sistema alega suportar transações tão baixas quanto 1 centavo.

A conta do Cybank é portátil, de forma que pode ser colocada em um disquete e usada em outro computador. Cada conta tem um identificador único. São permitidas várias contas para o mesmo consumidor.

Como características de segurança o seu Web site tem criptografia tripla DES e criptografia de chave pública para a transmissão da chave DES. Cybank mantém um chamado Secure Relay Proxy (SRP) para proteger as transações entre o consumidor e o comerciante e para prevenir bookmark da URL de envio.

### **5.13. CYBERCASH**

Endereço Web: <http://www.cybercash.com/>

Nome: CyberCash

Origem: CyberCash Inc., colaboração de grandes bancos e empresas como Netscape, Oracle, VeriFone, etc. Projeto alemão com o Dresdner Bank AG e Sachsen LB.

Status: Operacional desde abril de 1995.

Tamanho dos Pagamentos: Macro-pagamentos

Modelo de moeda: Notacional

Validação: on-line

Controle de privacidade: Consumidores usam pseudônimos, CyberCash pode ler as informações do cartão de crédito. O comerciante não pode. Os bancos podem rastrear qualquer transação (CyberCash, 1997a).

Mecanismos de segurança: Criptografia RSA e DES, assinaturas e senhas.

Pré-requisitos: Software da Carteira CyberCash. É necessário o uso de um cartão de crédito para cidadãos não-americanos. Os americanos podem usar sua conta bancária.

Risco: Companhias de Cartão de Crédito

Taxas: Vendedores pagam taxa por transação

Latência/Custos: 15-20 segundos por transação

Base de usuários: Mais de 500.000 carteiras distribuídas

Limites: Apenas cidadãos americanos podem vincular sua conta bancária à carteira

Notas: Poucas informações técnicas disponíveis

Genealogia: Futuramente, em acordo com SET.

CyberCash foi fundado em 1994 e proporciona uso seguro de cartão de crédito desde abril de 1995. Fornece soluções para o comércio que vão de sistemas de pagamento com cartões de crédito até sistemas seguros de micro-pagamentos. Existe pouca informação técnica detalhada. Basicamente, o sistema forma um gateway para unir comerciantes a sistemas de pagamento como cartões de crédito ou contas bancárias. Um segundo sistema é o CyberCoin feito para transações on-line de pequenos pagamentos (de 25 centavos até 10 dólares).

O sistema de pagamento CYBERCASH baseia-se em pagamentos seguros com cartões de crédito fazendo uso do sistema já existente e também sistemas de contas bancárias simplesmente integrando o software do comerciante como se fosse um terminal real de POS, tendo os servidores CyberCash agindo como um gateway entre o comércio da *Internet* e os bancos em uma rede financeira segura.

Esse sistema usa criptografia de 1024-bit RSA e 56-bit DES. Ele obteve uma licença mundial para o uso do algoritmo de criptografia de 1024-bit. Cyber Cash tenta proteger a privacidade de seus consumidores dando-lhes pseudônimos, ou seja, os identificadores de suas carteiras, omitindo, assim, as informações de seus cartões de crédito dos comerciantes. O software CyberCash adotará o padrão SET.

A carteira CyberCash é usada pelos consumidores em seus computadores. Algumas carteiras possuem rótulos privados como

o CheckFree. Mais de 500.000 dessas carteiras foram distribuídas. O servidor dos comerciantes é suportado por um servidor Vendor. Existem cerca de 77 comerciantes que usam o software da carteira. Os softwares servidores da carteira e do Vendor são gratuitos e rodam em plataformas Unix e Windows.

O software permite que o consumidor crie o Identificador da Carteira, que é necessário para o processo de identificação no ato da autenticação. Para preparar uma Carteira para uso pessoal, o consumidor precisa registrá-la. Deve fornecer uma senha, um Identificador da carteira e um Identificador de verificação. Esses dados são criptografados e enviados ao CyberCash. O identificador da Carteira é vinculado a um cartão de crédito ou conta bancária. O backup pode ser feito em um disquete para garantir a portabilidade.

A carteira fica no PC do consumidor e será inicializada automaticamente quando o consumidor clicar em um determinado botão na página de pedido do comerciante. Para abrir a Carteira, é necessária uma autenticação de senha e só então a Carteira conecta ao CyberCash. Quando os consumidores efetuam uma compra, o comerciante usa a informação de pagamento para informar o CyberCash, que por sua vez descriptografará os detalhes do pagamento, e os envia ao adquirente. Depois que o emissor e o adquirente aprovarem o pagamento, os servidores do CyberCash criptografam o resultado e devolvem-no ao comerciante que envia um recibo eletrônico e a mercadoria.

## Pagamento CyberCash

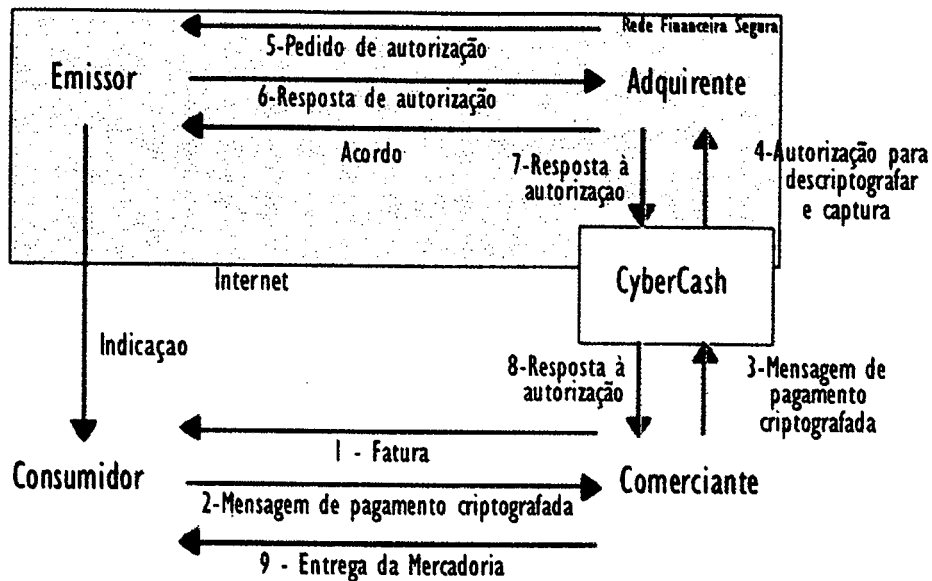


Figura 7 – Pagamento CyberCash

A imagem acima mostra um esquema de pagamento com o CyberCash. Um pagamento típico com esse sistema desenvolve-se da seguinte maneira:

- O consumidor faz o pedido ao comerciante e recebe uma fatura detalhando a compra e os custos.
- O consumidor usa a Carteira CyberCash para efetuar o pagamento entrando com os detalhes do cartão de crédito. Isso gera uma mensagem de pagamento criptografada que é enviada ao comerciante junto com a fatura original.
- O comerciante remove os detalhes do pedido na mensagem, assina o aviso de pagamento e envia-o para o servidor CyberCash. O comerciante não vê o número do cartão de crédito, pois a mensagem está criptografada e só pode ser reconhecida pelo CyberCash.

- O servidor CyberCash retira o processo da *Internet*, descriptografa a mensagem de pagamento, reformata-a e envia-a ao adquirente.
- O adquirente retransmite-a ao emissor que devolve sua aprovação ou reprovação.
- Essa resposta é devolvida ao servidor CyberCash.
- CyberCash manda a mensagem de aprovação ou reprovação para o vendedor.

Os passos 1, 2, 3 e 7 ocorrem na *Internet* e envolvem uma combinação de operações de chave pública e simétrica. Os passos 4 e 6 ocorrem em linhas dedicadas. O passo 5, na rede financeira segura. A transação se encerra em 15–20 segundos. Os bancos gostam desse sistema, pois ele utiliza redes seguras de transação. Além disso, não é necessário que o comerciante estabeleça novos relacionamentos bancários.

Tabela 14 : Perfil de Visibilidade CyberCash

<b>Quem/O que</b>	<b>Comerciante</b>	<b>Comprador</b>	<b>Data</b>	<b>Quantia</b>	<b>Item</b>
Comerciante	–	Não	Sim	Sim	Sim
Comprador	Parcial	–	Sim	Sim	Sim
CyberCash	Sim	Não	Sim	Não	Não
Banco	Sim	Sim	Sim	Sim	Não
Observador	Não	Não	Sim	Não	Não

A tabela acima mostra o perfil de visibilidade do CyberCash. Ele funciona como um intermediário nos processos de pagamento.

Tabela 15 : *Requisitos do CyberCash*

<b>Requisitos/Sistema</b>	<b>CyberCash</b>
Sistema de token	Não
<b>Transação</b>	
Atomicidade	Não
Consistência	Sim
Isolamento	Não
Durabilidade	Sim
<b>Segurança</b>	
Sem gasto dobrado	–
Sem falsificação	Não
Sem limite de gastos	Sim, autorização on-line.
Não-refutável	Não, mas com autenticação do comerciante.
Sem uso não-autorizado	Sim
Anonimato	Parcial, entre os comerciantes.
Sem traços	Não
<b>Interoperabilidade</b>	
Divisibilidade	–
Bidirecionamento	Não
Gasto encadeado	Não
Aceitação	Sim
Suporte a várias moedas	Sim, no cartão.
<b>Escalabilidade</b>	
Escalabilidade	Sim
Operações Offline	Não
<b>Questões Econômicas</b>	
Operacional	Sim
Grande base de usuário	Sim
Risco do comprador	Não, risco para a companhia do cartão.
Risco do vendedor	Não, risco para a companhia do cartão.
Confiabilidade	Sim
Conservação	Sim
<b>Facilidade de uso</b>	
Sem obstrução	Sim
Baixa latência	Não, 15–20 segundos por transação.
Micro-pagamentos	Não
Macro-pagamentos	Sim
Baixos custos fixos	Não
Independência do hardware	Sim



A tabela acima mostra o perfil do CyberCash. As transações não são anônimas. São verificadas e autenticadas on-line. Através do comerciante, o consumidor usa um pseudônimo gerado pela Carteira. O sistema não é econômico para pequenos pagamentos, pois utiliza cartão de crédito como instrumento financeiro. (CYBERCASH, 1998; CYBERCASH, 1996; CYBERCASH, 1997b; CYBERCASH, 1997e; CYBERCASH 1997c; EASTLAKE, BOESCH, CROCKER, YESIL, 1995).

#### **5.14. CyberCents**

Endereço Web: <http://www.outreach.com/>

Nome: CyberCents

Origem: Outreach Communications.

Status: Desenvolvimento, 1997.

Modelo de pagamento: Direct account based com apresentação segura de cartão de crédito no início.

Controle de privacidade: Nenhum. O comerciante mantém uma conta do consumidor.

Mecanismo de segurança: Senhas, STOMP Commerce Engine com SSL da mesma companhia garante segurança para o início da operação (cartão de crédito).

Pré-requisitos: Consumidor precisa de cartão de crédito, comerciante precisa de software de contas.

Risco: Banco

Taxas: Provavelmente cobrarão pelo software e porcentagem sobre vendas.

Base de usuários: 200 consumidores.

Limites: Consumidor pode ter que lidar com várias contas de consumidores. Não seria para compras eventuais, mas sim para longos relacionamentos consumidor/comerciante.

Notas: Simples mas com poucas informações técnicas disponíveis.

OutReach é uma empresa privada de software e serviços sediada em Austin, Texas, fundada em junho de 1995. CyberCents 2.0 é um

servidor Web para micro-pagamentos especialmente desenhado para permitir transações de venda seguras e automáticas tão pequenas quanto 1 centavo. Ele é pré-pago pelo consumidor numa conta do comerciante. O consumidor não necessita de qualquer carteira eletrônica (RICHARDS, 1996).

Não existe informação disponível sobre o atual status do sistema. Desta forma ele é colocado como em desenvolvimento.

Consumidores compram blocos de créditos CyberCents dos seus respectivos comerciantes em uma transação de apresentação segura de cartão de crédito automatizada e então gasta eles com diferentes itens no decorrer do tempo. As transações com cartão de crédito são processadas usando o Processador de Transações Seguras e Gerenciador de Pedidos OutReach (STOMP) que é baseado em SSL. OutReach disponibiliza seu serviço em seu próprio servidor para os comerciantes usando o processador de cartões dele e relações bancárias. A Outreach pretende incorporar o SET em seus produtos.

### **5.15. CYBERCOIN**

Endereço Web: <http://www.cybercash.com>

Nome: CyberCoin

Origem: CyberCash

Status: Operacional desde outubro de 1996.

Tamanho do Pagamento: Pequenos pagamentos, entre 25 centavos e 10 dólares.

Modelo de Moeda: Notacional

Validação: on-line

Controle de privacidade: Consumidor usa pseudônimo, CyberCash pode ler as informações da conta e o comerciante não. Os bancos podem rastrear todas as transações.

Mecanismo de segurança: Criptografia RSA e DES, assinaturas e senhas.

Pré-requisitos: Software da Carteira CyberCash. Cartão de Crédito para cidadãos não-americanos e os americanos podem usar a conta bancária.

Risco: Banco

Taxas: Vendedores pagam taxa por transação

Latência/Custos: Presumivelmente alto, pois vários bancos estão envolvidos.

Base de usuários: Mais de 500.000 carteiras distribuídas

Limites: Apenas cidadãos americanos podem vincular sua conta bancária à carteira

Notas: Poucas informações técnicas disponíveis

Genealogia: Um produto CyberCash.

O sistema notacional CyberCoin foi desenvolvido para ser um extensão da Carteira CyberCash e para micro-pagamentos (entre 25 centavos e 10 dólares). Saques múltiplos de 20 dólares até 80 dólares por mês.

Os consumidores podem usar suas contas bancárias para transações com o CyberCoin. O dinheiro é transferido da conta bancária do consumidor para a conta do CyberCoin através de redes financeiras seguras. CyberCoin só trabalha com dólares americanos e com comerciantes que possuam conta em bancos americanos. Consumidores com cartões de crédito também podem usar o serviço, mas não têm a possibilidade de reembolso.

Durante a instalação da carteira, os consumidores podem registrar suas contas bancárias e ligá-las à Carteira. Então poderão “carregar” a Carteira, isto é, transferir dinheiro de suas contas para sua conta CyberCoin no banco usado pelo CyberCash. Nenhum valor monetário é guardado no PC do usuário, por isso não há perda de dinheiro em caso de pane no computador e também suas contas podem ser acessadas de outros PCs. Não existe possibilidade de gasto duplo por não ser este um sistema de tokens, mas sim notacional. Além disso, não há o problema do troco.

Durante o pagamento, o banco do CyberCoin é informado que o consumidor quer efetuar um gasto em um comerciante do sistema e transfere a quantia em questão para a conta do vendedor. Nenhum valor sai da rede financeira.

Tabela 16 : Perfil de Visibilidade CyberCoin

<b>Quem/O que</b>	<b>Comer- ciante</b>	<b>Compra- dor</b>	<b>Dat a</b>	<b>Quan- tia</b>	<b>It em</b>
Comer- ciante	-	Não	Sim	Sim	Sim
Comprador	Parcial	-	Sim	Sim	Sim
CyberCash	Sim	Não	Sim	Não	Não
Banco	Sim	Sim	Sim	Sim	Não
Observador	Não	Não	Sim	Não	Não

A tabela acima mostra o perfil de visibilidade do CyberCoin. CyberCash difere dos bancos (emissor e adquirente) pois o sistema CyberCoin apenas gera uma interface de notificação segura aceita em vários bancos.

Tabela 17 : Requisitos do CyberCoin

<b>Requisitos/Sistema</b>	<b>CyberCoin</b>
Sistema de token	Não
<b>Transação</b>	
Atomicidade	Não
Consistência	Sim
Isolamento	Não
Durabilidade	Sim
<b>Segurança</b>	
Sem gasto dobrado	-
Sem falsificação	Não
Sem limite de gastos	Sim, autorização on-line.
Não-refutável	Não
Sem uso não-autorizado	Sim
Anonimato	Parcial, banco e CyberCash podem ver todas transações
Sem traços	Não
<b>Interoperabilidade</b>	
Divisibilidade	-
Bidirecionamento	Não
Gasto encadeado	Não
Aceitação	Sim
Suporte a várias moedas	Potencialmente, através dos bancos, ainda não implementado.
<b>Escalabilidade</b>	
Escalabilidade	Sim
Operações Offline	Não
<b>Questões Econômicas</b>	
Operacional	Sim
Grande base de usuário	potencialmente
Risco do comprador	Não
Risco do vendedor	Não

Confiabilidade	Sim
Conservação	Sim
<b>Facilidade de uso</b>	
Sem obstrução	Sim
Baixa latência	Não, muitas interações on-line são necessárias.
Micro-pagamentos	Não realmente, mínimo de 25 centavos.
Macro-pagamentos	Não
Baixos custos fixos	Não
Independência do hardware	Sim

A tabela acima mostra os requisitos do CyberCoin. O sistema não é anônimo e as transações podem ser rastreadas como no CyberCash. As informações financeiras das transações usam criptografia de 768-bit RSA. O protocolo do CyberCoin também contém uma certa segurança. A Carteira irá liberar CyberCoins para o comerciante apenas depois do consumidor receber a mercadoria. Portanto, nesse sistema os consumidores estão protegidos da perda de dinheiro causada por erros ou fraudes nas transferências eletrônicas. CyberCoin não possibilita transações pessoa-a-pessoa. (CYBERCASH, 1997d, 1996b).

### **5.16. Digital Silk Road**

Endereço Web <http://www.agorics.com/dsr.html>

Nome: Digital Silk Road

Origem: Norman Hardy e Eric Dean Tribble da Agorics.

Status: Proposta, 1997.

Tamanho do pagamento: Nano-pagamentos

Modelo de moeda: Token

Modelo de pagamento: Protocolo de links que inclui um campo de dinheiro em alguns pacotes.

Controle de Privacidade: Nenhum.

Mecanismo de segurança: Nenhum.

Notas: Bom para nano-pagamentos.

Agorics é uma empresa de desenvolvimento de software especializada em todas as faces do comércio eletrônico.

A idéia básica é um protocolo no nível dos links entre os sites incluindo um campo financeiro em alguns pacotes. Este campo não é cifrado e nunca é negativo. Ele tem 32 bits e seu valor é o mais baixo do pacote. É denominado em unidades de milésimo de centavo ou menos. Como esses pacotes passam através de uma interface entre dois sites, X e Y, um acumulador que fica conceitualmente entre X e Y armazena o fluxo financeiro. O acumulador é, provavelmente, implementado nos dois sites. Os respectivos operadores de X e Y lêem periodicamente o acumulador e transferem dinheiro real de acordo com o valor do acumulador, que é depois resetado. Esta transferência de fundos é acompanhada de uma EFT convencional. (HARDY, TRIBBLE, 1997)



### **5.17. ECASH**

Endereço Web: <http://www.digicash.com/>

Nome: Ecash

Origem: Digicash, D. Chaum, CWI, cooperação de grandes bancos, projetos alemães com o Deutsche Bank AG

Status: Operacional desde outubro de 1995

Tamanho do pagamento: Pequenos pagamentos

Modelo de moeda: token

Modelo de pagamento: Direct cash like

Validação: on-line

Controle de Privacidade: Confidencial, anônimo, não-rastreável

Pré-requisitos: Conta em um dos bancos emissores, Carteira (Unix, Macintosh, Windows)

Risco: Risco limitado para o consumidor; nenhum risco para o comerciante devido à validação on-line e contas pré-pagas.

Taxas: Taxa de instalação de 11 dólares, taxa mensal de 1 dólar

Latência/Custos: Nem sempre muito curto

Base de Usuários: Mais de 3.000 no Banco Mark Twain.

Limites: Necessidade de conta bancária em uma dos bancos emissores.

Notas: Interface gráfica; offline possível, mas não recomendado; extensa documentação; sistema bidirecional.

Genealogia: Versão on-line do CAFE; gasto duplo pode ser detectado na maneira reversa do NetCash

Ecash é o sistema de pagamento da Digicash anônimo, não-rastreável e com tokens on-line. O consumidor utiliza um software gráfico, a Carteira. O comerciante também possui uma carteira que pode ser acessada por linha de comando. Na verdade, Ecash permite pagamentos bidirecionais. Não há diferença entre consumidor e comerciante no tocante a pagamentos. Os dois lados podem fazer e receber pagamentos.

Após a instalação do software, é feita uma conexão com o banco do consumidor e este pode converter uma determinada quantia de sua conta corrente em tokens digitais que ficarão em seu PC. Com esses tokens, as compras podem ser efetuadas (CHAUM, BRANDS, 1997).

O lançamento comercial do Ecash envolvendo o uso de dinheiro real foi precedido por grandes fases de teste com dinheiro de teste. Este teste envolveu 30.000 consumidores, 60 lojistas e quatro bancos. No momento, há um segundo teste sendo feito com uma nova versão do software que é incompatível com a primeira. No banco americano Mark Twain, no finlandês EUNET Merita Bank e no australiano Advance Bank já há o uso do Ecash com moedas locais. O Mark Twain cobra uma taxa de instalação de 11 dólares, uma taxa mensal de 1 dólar e mais taxas por transação.

O software da Ecash é adaptado para várias plataformas, como Unix, Macintosh e Windows. Interface gráfica e linha de comando são usadas.

Ecash usa criptografia RSA de chave pública em suas transações. Usa blind signatures na autorização dos tokens e garante

anonimato e não-rastreamento aos consumidores. O gasto em dobro é detectado através de referencia on-line com o banco de dados que possui a relação dos tokens já utilizados.

O dinheiro é guardado localmente, mas é necessário que o consumidor tenha uma conta em um banco digital de onde eles irão sacar o dinheiro. O sistema é baseado em moeda e, portanto necessita da liquidação das moedas pelo banco emissor.

Ecash garante um total anonimato de todas as partes, mas a recente implementação prevê apenas o anonimato do consumidor com relação ao comerciante. Ao se completar uma transação, o comerciante é identificado pelo banco e os consumidores permanecem anônimos a menos que escolham revelar sua identidade.

### Transação de pagamento com o Ecash

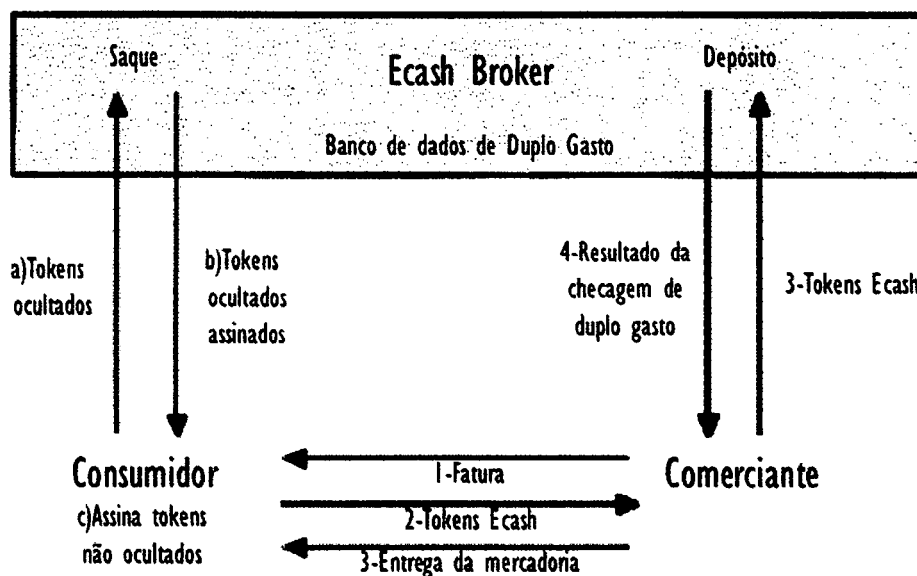


Figura 8 – Transação de pagamento com o Ecash

A figura acima mostra um pagamento efetuado com o Ecash. A transação funciona da seguinte maneira:

- O consumidor conecta-se ao emissor de Ecash e compra uma determinada quantia em moedas eletrônicas. Essas moedas são geradas em um esquema de blind signature, garantindo assim

seu anonimato. O consumidor gera a identificação dos tokens, oculta-os, determina sua denominação, transmite-os ao emissor que fará sua blind signature, devolvendo-os em seguida ao consumidor que os manterá em sua Carteira, no PC.

- O usuário pode então gastar esse tokens transmitindo-os via rede ao comerciante.
- Assim que receber os tokens, o comerciante deve apresentá-los ao emissor para a verificação. O banco consulta o banco de dados dos tokens já gastos para confirmar sua validade.

A geração de identificação pelo consumidor poderia levar a uma duplicação de tokens por diferentes consumidores mesmo sem existir um duplo gasto. Mas a utilização de longos ids torna esse fato altamente improvável. D. Chaum afirma que a utilização de 100 dígitos nos números seriais dos tokens reduziria essa probabilidade a proporções ínfimas.

Tabela 18 : Perfil de Visibilidade Ecash

<i>Quem/O que</i>	<b>Comerciante</b>	<b>Comprador</b>	<b>Data</b>	<b>Quantia</b>	<b>Item</b>
Comerciante	-	Parcial	Sim	Sim	Sim
Comprador	Sim	-	Sim	Sim	Sim
Banco	Sim	Não	Sim	Sim	Não
Observador	Parcial	Parcial	Sim	Não	Não

Tabela 19 : *Requisitos do Ecash*

<b>Requisitos/Sistema</b>	<b>Ecash</b>
Sistema de token	Sim
<b>Transação</b>	
Atomicidade	Não
Consistência	Não
Isolamento	Não
Durabilidade	Não
<b>Segurança</b>	
Sem gasto dobrado	Sim, validação on-line.
Sem falsificação	Sim
Sem limite de gastos	-

Não-refutável	Sim
Sem uso não-autorizado	Sim
Anonimato	Sim, para o consumidor.
Sem traços	Sim, para o consumidor.
<b>Interoperabilidade</b>	
Divisibilidade	Sim
Bidirecionamento	Sim
Gasto encadeado	Não
Aceitação	Talvez potencial, pois vários emissores não estão interoperando.
Suporte a várias moedas	Não
<b>Escalabilidade</b>	
Escalabilidade	Não, banco de dados central de gastos efetuados.
Operações Offline	Não
<b>Questões Econômicas</b>	
Operacional	Sim
Grande base de usuário	Sim, em teste, potencialmente em operação.
Risco do comprador	Limitado à quantia pré-paga.
Risco do vendedor	Sim, se não houver validação on-line.
Confiabilidade	Sim
Conservação	Sim, mas os tokens têm uma vida limitada e precisam ser regularmente renovados.
<b>Facilidade de uso</b>	
Sem obstrução	Sim
Baixa latência	Não, mas normalmente aceitável.
Micro-pagamentos	Não realmente, baixos e não micro.
Macro-pagamentos	Não
Baixos custos fixos	não disponível
Independência do hardware	Sim

A falta de atomicidade na transação básica pode ser causada por uma transferência corrompida entre o consumidor e o comerciante. Existe então a possibilidade de ambas as partes acreditarem que não possuem o token. Isso também viola o isolamento e a durabilidade. Um token de conciliação ajudaria nessa situação e restituiria a atomicidade, consistência e isolamento do protocolo. (DIGICASH, 1997; BARNES, 1997; CHAUM, 1988; CHAUM, 1992; CHAUM 1989; CHAUM 1994; CHAUM 1995; DIGICASH 1996a, 1996c, 1996b; GOLDBERG 1996).

### **5.18. eVend**

Endereço Web: <http://www.evend.com>

Nome: eVend

Origem: eVend Inc., Sausage Software.

Status: Operacional, 1997.

Modelo de pagamento: Indirect push debit account.

Controle de Privacidade: Nenhum.

Mecanismos de segurança: Senha, dados criptografados, apresentação segura do cartão de crédito, SSL.

Pré-requisitos: Um servidor para o comerciante com páginas Web com Cashlets. Os consumidores precisam de cartão de crédito.

Taxas: US\$ 50 para o software InfoSeller, taxa mínima de 20 centavos por transação. Acima de US\$ 2, 30 centavos mais 2,95% de taxa sobre o total.

Base de Usuários: Diz ter 380 lojistas.

Limites: Limite de depósito de US\$ 50 na conta do consumidor.

Notas: Sistema de Hub.

Sausage Software, uma subsidiária da eVend propôs esse sistema central de pagamento. eVend é um sistema de comércio eletrônico baseado em Java para transações pay-per-view para pagamento de informações. Ele é baseado em apresentação segura de cartão de crédito. Comerciantes necessitam do programa InfoSeller e também precisam colocar os chamados Cashlets em suas páginas, applets Java que fazem as transações de pagamento para os

consumidores. Os consumidores não precisam instalar nenhum software. Os sistemas para os comerciantes estão disponíveis para o Windows. eVend disponibiliza um sistema de processamento de transações para realizar as operações com cartão de crédito.

eVend é um sistema baseado em uma conta de débito indirect push. Consumidores podem usar os cashlets disponibilizados pelos comerciantes para abrirem contas eVend e depositar dinheiro nelas via apresentação segura de cartão de crédito. As contas são protegidas por senha. Uma vez obtida a conta e efetuado o depósito, os consumidores podem usá-la para comprar produtos dos comerciantes eVend disponíveis.

Uma transação de compra se inicia com um consumidor clicando no cashlet mostrado na página do comerciante. O consumidor precisa se autenticar para o eVend e o preço do produto é deduzido da conta do consumidor e adicionado à conta do comerciante.

### **5.19. FIRST VIRTUAL**

Endereço Web: [www.fv.com](http://www.fv.com)

Nome: First Virtual

Origem: First Virtual Inc.

Status: Operacional desde outubro de 1994.

Tamanho do pagamento: Macro-pagamentos

Modelo de moeda: Notacional

Modelo de pagamento: Intermediário no pagamento com cartão de crédito

Validação: on-line

Controle de Privacidade: Pseudônimos.

Mecanismos de segurança: Consumidor recebe reconfirmação por e-mail para cada compra. PIN virtual no lugar do número do cartão de crédito.

Pré-requisitos: Cartão de Crédito

Risco: Risco para o comerciante; para o consumidor, risco agravado com a companhia de cartão de crédito.

Taxas: 2 dólares de taxa anual

Latência/Custos: Alto

Base de Usuários: Mais de 2.650 vendedores e 180.000 compradores registrados.

Limites: –



Notas: Sistema muito simples.

Genealogia: Irá se ajustar ao SET.

First Virtual foi fundado em 1994. Desde então, mais de 2.650 lojas e 180.000 compradores em 166 países registrados. InfoHaus é o shopping da *Internet* feito pelo First Virtual, com 180 lojas. FV oferece um sistema pagamento pela *Internet* que utiliza a troca de mensagens por e-mail entre lojista, comprador e a própria FV. Não há a necessidade de hardware ou software especiais. O e-mail é suficiente e não necessita de criptografia.

O consumidor precisa ter um cartão d crédito. Ao se registrar no FV, ele recebe um PIN que funciona como pseudônimo para seus dados e dados de seu cartão de crédito. Os detalhes do cartão são transmitidos por telefone, fax ou carta. A taxa anual por consumidor é de 2 dólares que também é cobrada no cartão. Cada conta no FV possui um endereço de e-mail e uma conta real com uma moeda associada pré-definida. Para os consumidores, a conta do cartão precisa ser informada e, para os consumidores, uma conta bancária.

Após o registro, usando o PIN virtual, as compras podem ser feitas em lojas que aceitam o FV. O comerciante informaria o FV da intenção da compra. O consumidor receberia um e-mail da FV de confirmação da transação. O consumidor poderá responder com um sim, um não ou fraude. A resposta "Sim" confirma a transação e o débito é feito no cartão de crédito pala FV e não pelo comerciante. "Não" cancela a compra. "Fraude" é usado quando o consumidor é cobrado por uma transação nunca feita. Quando isso ocorre, o PIN do consumidor é invalidado e outro terá de ser gerado. O risco para o consumidor é a companhia do cartão de crédito (em caso de fraude).

O sistema oferece anonimato ao comprador devido a seu pseudônimo, isto é, o comerciante vê apenas o PIN e não os dados do cartão de crédito. O sistema FV baseou-se no Green Commerce Model. Esse modelo diz que o risco (muito baixo) de pagamento é do comerciante.

Uma típica transação FV ocorre da seguinte forma:

- O consumidor inicia a compra entrando com os dados de seu PIN no formulário de pedido do lojista.
- O lojista envia à First Virtual por e-mail esses dados recebidos, além do seu próprio PIN e de uma descrição da compra.
- A First Virtual automaticamente envia um e-mail ao consumidor pedindo a reconfirmação.
- O consumidor responde “Sim” à First Virtual.
- First Virtual processa a transação do cartão de crédito através da rede financeira segura.
- Após o término dessa transação, o comerciante recebe um número de autorização.

Tabela 20 : Perfil de visibilidade do First Virtual

<b>Quem/O que</b>	<b>Comerciante</b>	<b>Comprador</b>	<b>Data</b>	<b>Quantia</b>	<b>Item</b>
Comerciante	-	Parcial	Sim	Sim	Sim
Comprador	Parcial	-	Sim	Sim	Sim
First Virtual	Sim	Sim	Sim	Sim	Sim
Banco	Sim	Sim	Sim	Sim	Não
Observador	Parcial	Parcial	Sim	Sim	Sim

A tabela acima mostra o perfil de visibilidade do First Virtual. O consumidor é relativamente anônimo com relação ao comerciante, mas a transação é rastreável pela conta bancária vinculada ao PIN.

A visibilidade do consumidor e do comerciante entre si e com relação a um observador é parcial, pois os e-mails podem ser vistos e o PIN do consumidor pode ser visto pelo comerciante. Um observador pode ver e-mail e PIN de ambas as partes, mas não consegue usar essa informação para rastrear as respectivas contas bancárias.

Tabela 21 : Requisitos do First Virtual

<b>Requisitos/Sistema</b>	<b>First Virtual</b>
Sistema de token	Não
<b>Transação</b>	
Atomicidade	Não
Consistência	Sim
Isolamento	Não
Durabilidade	Sim
<b>Segurança</b>	
Sem gasto dobrado	-
Sem falsificação	Sim, fraude pode ser detectada por e-mail.
Sem limite de gastos	Sim, validação on-line.
Não-refutável	Não
Sem uso não-autorizado	Sim, fraude pode ser detectada por e-mail.
Anonimato	Sim, para o consumidor.
Sem traços	Não
<b>Interoperabilidade</b>	
Divisibilidade	-
Bidirecionamento	Não
Gasto encadeado	Não
Aceitação	Sim
Suporte a várias moedas	Sim
<b>Escalabilidade</b>	
Escalabilidade	Sim
Operações Offline	Não
<b>Questões Econômicas</b>	
Operacional	Sim
Grande base de usuário	Sim
Risco do comprador	Limitado ao risco do cartão de crédito.
Risco do vendedor	Sim
Confiabilidade	Sim
Conservação	Sim
<b>Facilidade de uso</b>	
Sem obstrução	Não
Baixa latência	Não
Micro-pagamentos	Não
Macro-pagamentos	Sim
Baixos custos fixos	Sim
Independência do hardware	Sim

A tabela acima mostra os Requisitos do First Virtual. Essencialmente, transações-padrão de cartões de crédito, pois estão vinculadas ao cartão do consumidor. (ROSE, BORENSTEIN, 1996; STEIN, STEFFERUD, BORENSTEIN, ROSE, 1996).

### **5.20. FSTC ELECTRONIC CHECK**

Endereço Web: <http://www.fstc.org>

Nome: FSTC Electronic Check

Origem: Financial Services Technology Consortium (FSTC).

Tamanho do pagamento: Macro-pagamentos

Modelo de moeda: Notacional

Modelo de pagamento: Direct account based; cheque eletrônico; diferentes variantes de protocolo.

Status: Em teste, 1997.

Validação: on-line

Controle de Privacidade: Nenhuma ressaltada.

Mecanismos de segurança: hardware inviolável, assinaturas, certificados, autoridades certificadoras.

Pré-requisitos: Hardware de talão de cheque eletrônico; smart card; software apropriado.

Risco: Risco para o comerciante.

Taxas: não conhecido

Latência/Custos: Alto

Base de Usuários: não conhecido

Limites: –

O Financial Services Technology Consortium (FSTC) é um grande consórcio de bancos, financiadoras, laboratórios nacionais,

universidades e agências governamentais patrocinando e colaborando na pesquisa e desenvolvimento de projetos técnicos. Seu projeto de cheque digital é parte do Sistema de Pagamento Bancário na *Internet* (BIPS), que está pesquisando uma arquitetura de acesso a bancos pela *Internet*. O FSTC Electronic Check é modelado para se parecer com o cheque tradicional aplicado a um contexto digital, tentando reproduzir o fluxo tradicional do cheque. O processo começa digitalmente, o consumidor usa uma assinatura digital e o comerciante também, para endosso. Certificados digitais autenticam o pagador, o emissor e a conta bancária.

O FSTC Electronic Check proporciona um modelo genérico para todos os instrumentos de pagamento eletrônico, assinado e autenticado digitalmente. Ele não apenas representa o cheque pessoal básico como também se assemelha a outros sistemas de pagamento, tais como cartões de débito, travelers checks e cheques certificados. Sua proposta inicial é fazer pagamentos eletrônicos em redes públicas. Porém, a familiaridade do consumidor com o cheque tradicional e as instituições financeiras como agentes certificadores pode promover uma rápida aceitação desse sistema. O projeto pretende possibilitar seu uso em qualquer situação, por exemplo, bancos que usam cheques para receber depósitos de seus clientes conseguindo assim facilidade de home-banking. Em um estágio mais adiantado, o sistema visa a implementação de transações POS, o que depende da existência de um mercado para isso.

O FSTC Electronic Check pode ser entregue diretamente ou por e-mail. Os pagamentos são coletados por bancos via e-mail e pago através da rede financeira, integrando-os de maneira segura com a *Internet*. Smartcards com assinaturas invioláveis ou outro tipo de

hardware são necessários para computar assinaturas sem comprometer a chave privada do assinante. O consumidor assina o cheque e inclui seu certificado de autenticação assinado pelo banco emissor que é assinado por alguém tipo Federal Reserve. Para isso, o consumidor possuirá um talão de cheques eletrônico portátil. Esse talão pode ser visto como um equivalente à Carteira do CAFE.

Esse talão conteria a chave privada do consumidor e manteria um log de todos os cheques emitidos. O risco seria perda ou roubo dos talões.

Aplicações básicas:

**5.20.1. Preenche:**

Gera um cheque, anexa-o a uma conta e o assina.

**5.20.2. Co-assina:**

Anexa mais uma assinatura ao cheque.

**5.20.3. Verifica:**

Valida as assinaturas em um cheque e a associação a uma conta.

**5.20.4. Endossa:**

Valida assinaturas no cheque, anexa o endosso e assina o cheque a ser depositado ou descontado.

#### **5.20.5. Leitura de registro:**

Lê o log do cheque no talão.

#### **5.20.6. Registro da entrada:**

Adiciona uma entrada ao log do cheque.

O FSTC Electronic Check pretende se adaptar aos seguintes cenários:

#### **5.20.7. Depósito e pagamento:**

O consumidor recebe uma conta ou fatura do consumidor, emite um cheque eletrônico e o envia. O comerciante apresenta o cheque ao adquirente que, por sua vez, acertará a transação com o emissor.

#### **5.20.8. Dinheiro vivo e transferência:**

O consumidor recebe uma conta ou fatura do consumidor, emite um cheque eletrônico e o envia. O consumidor apresenta o cheque diretamente ao emissor que depositará a quantia na conta do comerciante no adquirente.

#### **5.20.9. Lockbox:**

O consumidor recebe uma conta ou fatura do consumidor, emite um cheque eletrônico e o envia para o adquirente, diretamente ou por um lockbox. O adquirente notifica o comerciante e completa o pagamento junto ao emissor.



#### 5.20.10. Transferência de fundos:

O consumidor recebe uma conta ou fatura do consumidor, emite um cheque eletrônico e o envia para o emissor. O emissor transfere fundos para a conta do comerciante no adquirente.

Tabela 22 : Perfil de visibilidade do FSTC Electronic Check

<i>Quem/O que</i>	<i>Comerciante</i>	<i>Comprador</i>	<i>Data</i>	<i>Quantia</i>	<i>Item</i>
Comerciante	–	Sim	Sim	Sim	Sim
Comprador	Sim	–	Sim	Sim	Sim
Banco	Sim	Sim	Sim	Sim	Não
Observador	n.d.	n.d.	Sim	n.d.	Não

O perfil de visibilidade do FSTC Electronic Check lembra muito o do cheque tradicional. No entanto, o protocolo do FSTC não reforça a criptografia do cheque, apenas pede uma assinatura digital para a autenticação. Não fica muito claro quanto das informações no cheque são criptografadas. Sem a criptografia, as transações com o FSTC seriam visíveis a um observador digital. A documentação diz que os cheques eletrônicos podem ser criptografados para serem enviados pela *Internet*.

#### Requisitos do FSTC Electronic Check

Tabela 23 : Requisitos do FSTC Electronic Check

<b>Requisitos/Sistema</b>	<b>FSTC Electronic Check</b>
Sistema de token	Não
<b>Transação</b>	
Atomicidade	Sim
Consistência	Sim
Isolamento	Não
Durabilidade	Sim
<b>Segurança</b>	
Sem gasto dobrado	–
Sem falsificação	Sim, assinatura digital e hardware inviolável.
Sem limite de gastos	Não
Não-refutável	Sim

Sem uso não-autorizado	Sim, se o talão de cheque eletrônico não for roubado ou perdido.
Anonimato	Não
Sem traços	Não
<b>Interoperabilidade</b>	
Divisibilidade	-
Bidirecionamento	Sim, potencialmente.
Gasto encadeado	Não
Aceitação	Sim, potencialmente.
Suporte a várias moedas	Sim, pelos bancos.
<b>Escalabilidade</b>	
Escalabilidade	Sim
Operações Offline	Não
<b>Questões Econômicas</b>	
Operacional	Não, apenas teste.
Grande base de usuário	-
Risco do comprador	Não
Risco do vendedor	Sim
Confiabilidade	Sim
Conservação	Sim
<b>Facilidade de uso</b>	
Sem obstrução	Não
Baixa latência	Não
Micro-pagamentos	Não - improvável.
Macro-pagamentos	Sim
Baixos custos fixos	depende da política do banco.
Independência do hardware	Não, talão eletrônico é um hardware.

A tabela acima mostra as propriedades de uma transação de um cheque eletrônico. (FSTC, 1997a, 1997b, 1997c).

### **5.21. GELDKARTE**

Endereço Web: <http://www.gdm.de>

Nome: Geldkarte im *Internet*

Origem: Giesecke & Devrient

Status: Primeiro teste programado para início de 1998.

Tamanho do pagamento: Pequenos pagamentos

Modelo de moeda: token (envolvendo contadores).

Modelo de pagamento: Direct cash like, contas ocultas.

Validação: Offline

Controle de Privacidade: Nenhum. Se necessário, recomenda-se o uso de SSL. Se um Geldkarte for vinculado a uma conta bancária, será vinculado ao consumidor. O sistema é rastreável e não-anônimo. Uma versão não vinculada ao consumidor está sendo planejada.

Mecanismos de segurança: Hardware inviolável, assinaturas, certificados, contas ocultas.

Pré-requisitos: Leitor do Geldkarte do comerciante (Hardware terminal e respectivo software).

Risco: Consumidor e comerciante têm risco de perda.

Taxas: 0,3% por transação

Latência/Custos: Baixa

Base de Usuários: não disponível

Limites: Quantia carregada no Geldkarte.

Notas: Interoperabilidade.

Genealogia: não disponível

A proposta de uso do Geldkarte na *Internet* é de Giesecke & Devrient. Envolve o uso de um hardware inviolável e smart cards. Já pode ser usado em cartões Eurocheque (ec) que tenham o chip do Geldkarte para transações POS em algumas lojas. Envolve dinheiro de verdade com a moeda do banco emissor. O ZKA (Zentraler Kredit Ausschuss) precisa ainda certificar a proposta do Geldkarte na *Internet* antes do início do teste envolvendo dinheiro. O protocolo do Geldkarte é basicamente o mesmo do ec com um chip, suplementado com um tratamento de “timeouts”. O protocolo é aberto ao público. Todo hardware e software usado pelo Geldkarte precisa ser certificado pelo ZKA para estar em concordância com o protocolo antes de ser usado operacionalmente. O consumidor precisa utilizar o Windows (95 ou NT) e o comerciante, Windows NT.

Geldkarte possui um contador de onde é deduzido cada pagamento. O Geldkarte não pode ser bloqueado em caso de perda e não é protegido por senha. O consumidor precisa de um Geldkarte identificado por seu número. O comerciante precisa de um terminal. Cada Geldkarte tem sua própria conta oculta em um centro de desconto. Cada consórcio bancário tem seu próprio centro de desconto. O comerciante coleta os pagamentos offline durante o dia e os submete aos vários centros de desconto no fim do dia. Ele detém o potencial risco caso o consumidor use um cartão comprometido. Reembolso de pagamentos são deduzidos da conta oculta do Geldkarte. Por isso, um Geldkarte comprometido pode ser detectado rapidamente. Os bancos têm uma comissão de 0.3% sobre cada pagamento efetuado e não será menor que 2 DPF. Isso

significa que o Geldkarte é bom para pequenos pagamentos, mas não para micro-pagamentos.

Em uma transação POS, o consumidor insere seu Geldkarte em um terminal do comerciante. Na transação pela *Internet*, o Geldkarte será inserido no leitor de seu PC e, com o auxílio de um software local, o cartão estabelecerá uma conexão com o terminal remoto do lojista. O cartão do consumidor e o terminal (“cartão” do comerciante) autenticam-se mutuamente, trocando certificados. Um canal de comunicação seguro, com SSL, é recomendado. A infraestrutura do Geldkarte também envolve uma certificação. O Geldkarte assina cada pagamento.

### Transação Geldkarte via Internet

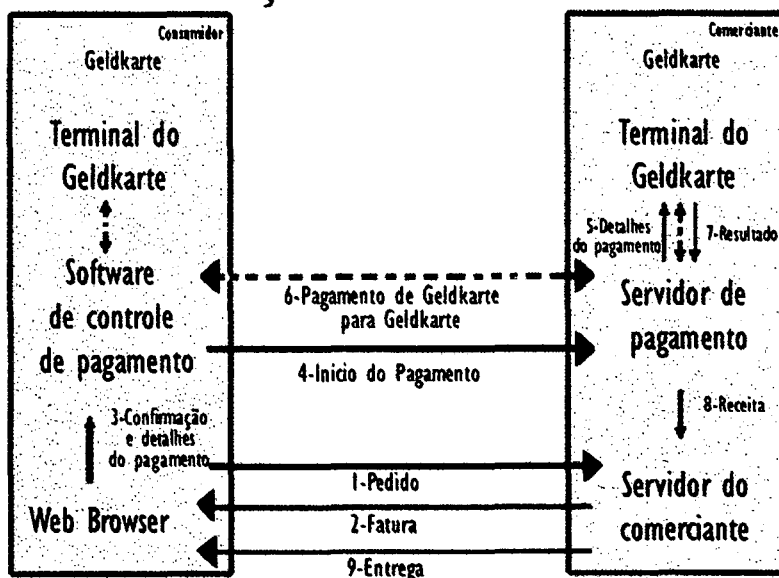


Figura 9 – Transação Geldkarte via Internet

A figura acima mostra um pagamento efetuado com Geldkarte. Uma transação de pagamento típica é a seguinte:

- O consumidor obtém o Geldkarte que contém um identificador e um certificado do banco. Há uma conta oculta para o Geldkarte no centro de desconto. O consumidor carrega o Geldkarte pela

*Internet* ou em um terminal bancário. O banco tem um ganho pré e pós-transação.

- O consumidor seleciona uma loja e faz um pedido.
- O comerciante envia uma fatura ao consumidor.
- O consumidor confirma a fatura e autoriza seu software de controle a fazer o pagamento.
- O software de controle de pagamento do Geldkarte inicia a transação de pagamento. O servidor de pagamentos do comerciante, em colaboração com o do consumidor, conecta o Geldkarte com o terminal do vendedor que fará a autenticação e conduzirá o pagamento. O Geldkarte assina todo pagamento.
- O terminal do comerciante entrega o recibo ao servidor que o entregará ao comerciante. Esse recibo irá, junto com a mercadoria, para o comprador.
- Ao fim de cada dia, o terminal do vendedor submete os pagamentos desse período aos centros de pagamento apropriado para reembolso.

O problema da autenticação ainda é um problema. Vários produtores podem oferecer leitores de Geldkarte para os consumidores. O terminal do lojista e o software do consumidor são fornecidos pela Giesecke & Devrint. Os primeiros testes não oficiais na *Internet* mostraram que o sistema funciona. O sistema não é bidirecional, apenas estornos limitados são possíveis.

Tabela 24 : Perfil de visibilidade do Geldkarte

<i>Quem/O que</i>	<b>Comerciante</b>	<b>Comprador</b>	<b>Data</b>	<b>Quantia</b>	<b>Item</b>
Comerciante	–	Parcial	Sim	Sim	Sim
Comprador	Sim	–	Sim	Sim	Sim
Banco	Sim	Sim	Sim	Sim	Não
Observador	Sim	Parcial	Sim	Sim	Sim

A tabela acima mostra o perfil de visibilidade do Geldkarte. O consumidor só é visível para o comerciante através do id de seu Geldkarte. O banco pode achar uma conta pessoal também através do id do Geldkarte.

Tabela 25 : Requisitos do Geldkarte

<b>Requisitos/Sistema</b>	<b>Geldkarte</b>
Sistema de token	Sim
<b>Transação</b>	
Atomicidade	Sim
Consistência	Sim
Isolamento	Sim, se o hardware não estiver quebrado.
Durabilidade	Sim
<b>Segurança</b>	
Sem gasto dobrado	–
Sem falsificação	Sim
Sem limite de gastos	Sim, se o hardware não estiver quebrado.
Não–refutável	Sim
Sem uso não–autorizado	Não, quem estiver com o Geldkarte pode usar o dinheiro nele contido.
Anonimato	Não, mas o vendedor vê apenas o id do Geldkarte.
Sem traços	Não
<b>Interoperabilidade</b>	
Divisibilidade	–
Bidirecionamento	Não
Gasto encadeado	Não
Aceitação	Sim
Suporte a várias moedas	Sim
<b>Escalabilidade</b>	
Escalabilidade	Sim
Operações Offline	Sim
<b>Questões Econômicas</b>	
Operacional	Não
Grande base de usuário	Sim, potencialmente.
Risco do comprador	Sim, pode não receber a mercadoria.
Risco do vendedor	Sim, consumidor pode usar hardware danificado.
Confiabilidade	Sim
Conservação	Sim
<b>Facilidade de uso</b>	
Sem obstrução	Sim, potencialmente.
Baixa latência	Sim

Micro-pagamentos	Limitado
Macro-pagamentos	Não
Baixos custos fixos	Sim, potencialmente.
Independência do hardware	Não

Tabela acima mostra o perfil do Geldkarte. Esse sistema possibilita pequenos pagamentos e pode ser usado tanto na *Internet* quanto em pequenas transações POS do dia-a-dia. O risco de cartões danificados é limitado pelo uso de contas ocultas. O sistema tem grande potencial de aceitação por bancos. (DIETZE, 1997)



### **5.22. GlobeID**

Endereço Web: <http://globeid.gctech.fr> ; <http://www.kleline.com> ;  
<http://www.gctec.com>

Status: Protótipo, 1997.

Modelo de pagamento: Home banking.

Pré-requisitos: Módulo de interface de carteira.

O protótipo de pagamento GlobeID da GCTech é operado pelo French Bank of Mars e permite que consumidores testem compras seguras e certificadas de comerciantes através da *Internet* sem envolver dinheiro real. O software de pagamento do GlobeID está rodando no site da KLELine. Kleline é um intermediária de confiança operando os serviços de pagamento GlobeID em nove países da Europa (Bélgica, França, Alemanha, Itália, Luxemburgo, Portugal, Espanha, Suíça e Reino Unido) (KLELINE, 1997).

Consumidores necessitam de uma carteira chamada WIM (Módulo de Interface de Carteira). Esta carteira contém os sistemas de pagamento como dinheiro, cartões de crédito, etc. Tanto os consumidores quanto os comerciantes necessitam ser registrados com um banco que ofereça tanto o GlobeID quanto os serviços bancários tradicionais.

O Centro de Serviços para a Carteira GlobeID permite ao consumidor realizar transações de Home Banking e pagamento com sua carteira GlobeID. Essas operações são as mesmas oferecidas por um banco para seus consumidores: criar uma conta, fechar uma conta, encher a carteira, mudar o número de identificação, etc.

### 5.23. iKP

EndereçoWeb:

<http://www.zurich.ibm.com/Technology/Security/extern/ecommerce/iKP.html>

Nome: iKP (1KP, 2KP, 3KP\\0

Status: Proposta, 1996.

Modelo de pagamento: Apresentação segura de cartão de crédito.

Controle de privacidade: Depende dos parâmetros; sem anonimato com o banco.

Mecanismo de segurança: Criptografia RSA e assinaturas.

Pré-requisitos: Software iKP, cartão de crédito.

A IBM propôs protocolos e arquitetura para pagamentos seguros através de redes. *Internet Keyed Payment Protocols* (iKP) implementa transações seguras criptografadas baseadas em cartão de crédito. iKP é uma família de protocolos de pagamento seguro de cartão de crédito.

Ele está obsoleto agora, e foi englobado pelo SET, mas muitos detalhes do iKP influenciaram o SET e a IBM é uma das maiores contribuidoras na especificação do SET. Europay também usou iKP como base de seu protocolo baseado em smart card, mas está se movendo para o SET no momento.

iKP pretendia ser um protocolo aberto evitando problemas que poderiam surgir com soluções proprietárias. Ele utiliza também pesadas técnicas de criptografia sem violar as regras de exportação americanas. Um protótipo inicial foi desenhado para cartões de crédito, mas pode ser estendido para qualquer sistema de

pagamento. A *Internet* permite aos consumidores colocarem ordens enquanto existirem as redes financeiras que executam o verdadeiro pagamento. (BELLARE, GARAY, WAIDNER, et al., 1995).

#### **5.24. INTERCOIN**

Endereço Web: <http://intercoin.com>

Nome: InterCoin

Status: Teste, 1997.

Modelo de moeda: Notacional.

Modelo de pagamento: Direct account based.

Controle de privacidade: InterCoin mantém os dados do consumidor confidenciais, lojistas só vêem o pseudônimo da conta.

Mecanismo de segurança: Senha e SSL.

Taxas: US\$ 10 de registro

Notas: Pegue primeiro, pague depois.

InterCoin quer disponibilizar um serviço amigável para o consumidor. Consumidores necessitam ter uma conta InterCoin.

InterCoin criou uma espécie de compra shareware através da *Internet*. Consumidores podem utilizar os produtos primeiro e pagar depois quando estiverem satisfeitos com eles. Os produtos serão cobrados no final de cada mês.

### **5.25. LotteryTickets**

EndereçoWeb:

<http://www.theory.lcs.mit.edu/~rivest/Rivest-MD5.txt>

Nome: LotteryTickets

Origem: R. Rivest, MIT Computer Lab.

Status: Proposta, 1997.

Modelo de moeda: Notacional.

Modelo de pagamento: Direct account based, cheques probabilísticos.

Controle de privacidade: Basicamente nenhum, mas possível uso de pseudônimos, apenas algumas transações são reportadas ao banco.

Mecanismo de segurança: Nem todo pagamento é associado a valores monetários, somente os dos tokens vencedores, lei de grandes números.

Genealogia: Similar ao TUB.

LotteryTickets é uma proposta da RIVEST (1997) para um sistema probabilístico de pagamento. Nem todos os pagamentos estão associados com valor monetário, mas apenas aqueles envolvendo tokens vencedores. A justiça é alcançada pela lei de grandes números e pequenos valores.

Os comerciantes podem calcular se um token é vencedor e se necessitam reembolso apenas deles. Consumidores não sabem quais tokens são vencedores. LotteryTickets é um protocolo muito eficiente para micro-pagamentos de frequência altíssima. Ele

funciona offline, é validado localmente e tem poucas necessidades de armazenamento. LotteryTickets não é um esquema anônimo, mas pseudônimos podem ser utilizados e somente poucas transações são levadas aos bancos.

Um LotteryTicket com um preço de US\$10,00 e uma chance de vitória de 1/1000 tem um valor esperado de 1 centavo. Se um consumidor quer pagar um centavo para um comerciante, ele precisa utilizar um desses LotteryTickets. Um LotteryTicket contém um número e um indicador de número vencedor. Este indicador pode ser uma parte de um número vencedor que foi definido pelo comerciante antes da geração do LotteryTicket cuja divisão foi dada pelo emissor para incluí-la em cada LotteryTicket daquela série. Desta forma, o comerciante pode identificar os tíquetes vencedores facilmente, mas o emissor não sabe os números vencedores.

A chance de um tíquete ser vencedor precisa ser conhecida para determinar o valor esperado do tíquete. O comerciante precisa lidar com o risco de o emissor não querer pagar, mas os maus emissores vão ser expulsos com o tempo. Consumidores podem ser certificados pelo emissor para criarem seus próprios LotteryTickets.

### **5.26. MagicMoney**

Endereço Web: <http://www.unicorn.com/pgp/mm-readme.html>

Nome: MagicMoney

Origem: Product Cypher.

Status: Implementação de domínio público, 1997.

Modelo de pagamento: Direct cash like.

Controle de Privacidade: Anônimo, não rastreável, confidencial.

Mecanismo de segurança: PGP, blind signatures.

Pré-requisitos: Servidor, cliente, e-mail, PGP.

Base de Usuários: não disponível

Notas: Para e-mail.

Genealogia: Influenciou o MPTP.

MagicMoney é um sistema de dinheiro digital desenhado para ser utilizado via e-mail. O sistema é on-line e não rastreável. Cada transação envolve uma troca com o broker central para prevenir duplo gasto. É impossível para qualquer parte envolvida ou observador rastrear transações, ou trocar uma retirada com um depósito, ou trocar dois tokens de um consumidor de qualquer maneira. MagicMoney é uma espécie de implementação pública do DigiCash Ecash para e-mail.

O sistema consiste de dois módulos, servidor e cliente. MagicMoney utiliza PGP para todas as suas comunicações entre servidor e cliente, e todas as mensagens são criptografadas. As mensagens do servidor para o cliente são também assinadas. A não

possibilidade de rastreamento é conquistada por meio de blind signatures.

MagicMoney utiliza tokens de valor fixo, escolhido pelo operador do servidor. Os tokens são assinados com um par diferente de chaves para cada valor. O servidor aceita tokens velhos, assina "blind" tokens novos, e lista tokens reembolsados na lista de duplo gasto.

O servidor não armazena nenhum token, mas todos os tokens são armazenados pelo módulo cliente. Tokens recebidos são imediatamente reembolsados no servidor e trocados por novos tokens que estão armazenados no módulo cliente do vendedor. Isso simula reação do usuário da mesma forma que o NetCash.



### **5.27. MICROMINT**

Endereço Web: <http://theory.lcs.mit.edu/~rivest/RivestShamir-mpay.ps>

Modelo de pagamento: Direct cash like

Status: Proposta, 1996.

Mecanismo de segurança: Chave pública, hash collisions.

Notas: Custo inicial e de instalação muito alto.

MicroMint é uma proposta de Rivest e Shamir. São moedas que podem ser produzidas eficientemente apenas em larga escala e são difíceis de produzir em pequenas quantidades. A validade da moeda é facilmente verificada. MicroMint é otimizada para pagamentos não relacionados de pequenos valores. Ele não utiliza nenhuma operação de chave pública. Apesar disso o esquema é altamente complexo e pode precisar de muito esforço operacional e inicial. Porém não parece que ele nunca irá ganhar importância prática.

Um broker irá emitir novas moedas no início de um período a revogar aquelas do período anterior. Moedas consistem de múltiplas divisões de colisão, isto é, valores diferentes irão alcançar o mesmo valor de divisão. O broker cunha moedas calculando essas divisões de colisão. Para este processo, muitos cálculos são necessários, mas cada vez mais colisões são detectadas com a computação contínua. O broker vende essas moedas MicroMint em lotes para os consumidores. Moedas não utilizadas podem ser devolvidas para o broker no final de um período, por exemplo, um mês.

Consumidores utilizam moedas MicroMint como pagamento para comerciantes. Estes podem facilmente checar a validade de uma moeda aplicando a função de divisão para cada moeda e verificando que todas

têm o mesmo valor. Comerciantes retornam suas moedas no final de cada dia e as moedas são checadas pelo broker para evitar duplo gasto. Caso exista alguma moeda utilizada duas vezes, todos os comerciantes perdem, com exceção um, escolhido aleatoriamente. O broker paga a taxa de ressarcimento deste comerciante (LAW, SOLINAS, 1996).

A MicroMint desencoraja a geração em pequena escala em função das pequenas somas envolvidas e falta de crédito e remoção dos maus usuários. Apesar disso a MicroMint não oferece qualquer proteção contra atitudes maliciosas. Para reduzir esse risco, o broker pode personalizar moedas para consumidores e o usuário para os comerciantes.

Falsificações de larga escala na tentativa de produzir moedas como se fosse um broker são eliminadas com a imposição de dificuldades. O broker utiliza um período para produzir moedas para o próximo, utilizando muito poder de cálculo e requer hardware especializado. No início de um novo período o broker publica a função de hash e vende as moedas. Um falsificador somente então poderia começar a falsificar moedas, o que requer muito tempo e poder de cálculo. Várias outras técnicas são propostas para evitar possíveis falsificações.

## **5.28. MILLICENT**

Endereço Web: <http://www.millicent.digital.com>

Nome: MilliCent

Origem: M. Maneasse, S. Glassman da Digital Equipment.

Status: Em teste, desde dezembro de 1997.

Tamanho do pagamento: Micro-pagamentos

Modelo de moeda: Token

Modelo de pagamento: Direct cash like, dinheiro local, conta do consumidor no broker.

Validação: Semi-on-line – transações envolvem somente o comprador e o vendedor, mas algumas preparações envolvem o broker também.

Controle de Privacidade: Escalável, de confidencial a não-confidencial, não anônimo, rastreável.

Mecanismos de segurança: Senhas, assinaturas, segurança leve em geral.

Pré-requisitos: Carteira Millicent e servidor que funciona como proxy entre o browser do consumidor e o servidor web do vendedor.

Riscos: Para o consumidor.

Taxas: não disponíveis

Latência/Custos: Baixa

Base de Usuários: não disponível

Notas: Interoperabilidade.

Genealogia: Influenciou o MPTP.

Millicent é um sistema de micro-pagamento digital baseado em voucher proprietário da Digital Equipment. Tem como meta o segmento de micro-pagamentos do comércio eletrônico e suporta transações de frações de centavos. Por representar moedas muito pequenas, Millicent possui medidas de segurança mais relaxadas. Um teste público desse sistema começou em dezembro de 1997 com dinheiro sem validade.

O sistema usa vouchers específicos, chamados de scrip, uma forma de token que só é válida com determinados comerciantes por um período de tempo limitado. Os Brokers são intermediários entre os vendedores e os compradores. O fato de o scrip valer apenas para um vendedor faz com que não seja necessário o contato com a central emissora para validar o token. Isso reduz o tráfego na rede e o custo de validação. Para evitar que os consumidores mantenham contas separadas com vários comerciantes, os brokers agem como intermediários. Os longos relacionamentos são entre brokers e consumidores e brokers e comerciantes.

### Transação de pagamento com Millicent

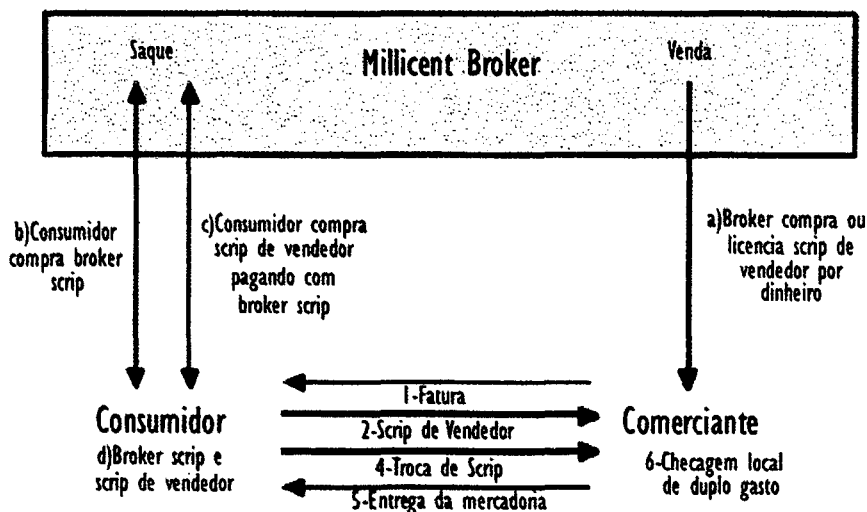


Figura 10 – Transação de pagamento Millicent

A figura acima mostra uma transação com o Millicent. A seqüência básica de interações é a seguinte:

- O consumidor obtém uma quantidade de broker scrip.
- Ele solicita scrips de vendedor, que são pagos com broker scrip.
- O broker obtém o scrip de vendedor solicitado.
- O broker vende os scrips de vendedor para o consumidor.
- O consumidor compra o serviço com scrip de vendedor.
- O vendedor dá o troco em scrip de vendedor.

Os itens de 1 à 4 não são feitos em todas as transações, pois o consumidor pode comprar scrips que durem um certo período. Do mesmo jeito, o broker pode estocar scrip de vendedor para atender a vários pedidos ou pode ter uma licença para emitir esses scrips. Esse sistema acaba com o gargalo de um simples emissor ser contatado durante cada transação, principalmente quando os passos 1, 2, 3, e 4 estão completos. Testes na Digital indicam que o Millicent é eficiente para transações bem baixas, do tipo 1/10 de centavo.

Um outro lado do econômico protocolo Millicent é o uso de uma criptografia leve, pois o custo de quebrá-lo seria maior que o valor do próprio scrip. Millicent oferece três versões de protocolo: privado e seguro, seguro sem criptografia e scrip às claras. Seguro sem criptografia significa que o consumidor e o vendedor compartilham o segredo (assinatura) do primeiro que vai anexado ao pedido de compra. O comerciante confere essa assinatura com a cópia que ele tem em seu poder. Se as assinaturas conferem, o pedido é válido.

Tabela 26 : Perfil de visibilidade do Millicent

<b>Quem/O que</b>	<b>Comerciante</b>	<b>Comprador</b>	<b>Data</b>	<b>Quantia</b>	<b>Item</b>
Comerciante	–	Parcial	Sim	Sim	Sim
Comprador	Parcial	–	Sim	Sim	Sim
Broker	Sim	Sim	Não	Não	Não
Observador	Parcial	Parcial	Sim	–	Não

A tabela mostra o perfil de visibilidade do Millicent. Cada versão do protocolo do Millicent oferece um nível diferente de visibilidade. O menos privado é o scrip às claras. Nesse caso, o scrip é transmitido sem nenhuma criptografia ou proteção. Isso permitiria que observadores copiassem o scrip e eles mesmos o gastariam. Mesmo roubando quantias tão pequenas, o incômodo seria muito grande. Mas a melhora do sistema é relativamente barata, quer seja com alta criptografia ou com assinaturas seguras.

Millicent inclui um campo no scrip que contém informações do consumidor, como por exemplo, sua idade ou qualquer outra informação necessária para um desconto. A menos que esse campo seja criptografado, essas informações podem ser vistas por um observador. Se a versão do protocolo usada for privada e segura, um observador não teria nenhuma informação.

Tabela 27 : Requisitos do Millicent

<b>Requisitos/Sistema</b>	<b>Millicent</b>
Sistema de token	Sim
<b>Transação</b>	
Atomicidade	–
Consistência	–
Isolamento	Sim
Durabilidade	–
<b>Segurança</b>	
Sem gasto dobrado	Sim
Sem falsificação	Sim
Sem limite de gastos	–
Não-refutável	Sim
Sem uso não-autorizado	Sim
Anonimato	Não, mas sem autenticação.
Sem traços	Não
<b>Interoperabilidade</b>	

Divisibilidade	Não, mas oferece troco.
Bidirecionamento	Não
Gasto encadeado	Não
Aceitação	–
Suporte a várias moedas	Sim, possível através do broker.
<b>Escalabilidade</b>	
Escalabilidade	Sim
Operações Offline	Sim, parcialmente.
<b>Questões Econômicas</b>	
Operacional	Não, apenas teste.
Grande base de usuário	Potencialmente
Risco do comprador	Não
Risco do vendedor	Sim
Confiabilidade	Sim
Conservação	Questionável
<b>Facilidade de uso</b>	
Sem obstrução	Sim
Baixa latência	Sim
Micro-pagamentos	Sim
Macro-pagamentos	Não
Baixos custos fixos	Sim, potencialmente.
Independência do hardware	Sim

Atomicidade, consistência e durabilidade não são diretamente suportadas pelo Millicent. Mas, a quantia em risco em qualquer transação é suficientemente pequena para não representar um grande risco.

As transações do Millicent não são anônimas e muitas são offline. O consumidor não é anônimo e os detalhes da conta são mantidos pelo broker. O sistema é offline, pois nenhuma conexão a um servidor é necessária. (DEC RESEARCH CENTER, 1996 e 1997; MANASSE, 1995; GLASSMAN, MANASSE, ABADI, GAUTHIER, SOBALVARRO, 1995).

### **5.29. MONDEX**

Endereço Web: <http://www.mondex.com>

Nome: Mondex

Origem: Mondex, MasterCard, baseado no Reino Unido

Status: Tentativa fechada desde julho de 1995.

Tamanho do pagamento: Micro-pagamentos.

Modelo de moeda: Token.

Modelo de pagamento: Parecido com dinheiro direto, smart card.

Validação: Offline

Controle de privacidade: Nenhum.

Mecanismo de segurança: Smart cards, assinaturas, senhas, quase nenhuma informação concreta disponível.

Pré-requisitos: Cartões Mondex e vários outros hardwares

Riscos: Consumidor

Taxas: Sem taxas para o projeto piloto

Latência/ Custos: Baixa

Base de usuários: 48000 consumidores

Limites: Sistema proprietário, fechado. Máximo de 500 GBP por transação

Notas: Poucas informações técnicas disponíveis.

Genealogia: Parecido com o CAFE.



A Mondex (MONDEX, 1996) disponibiliza dinheiro eletrônico em um smart card, como no CAFE, mas o seu projeto está em um estágio bem mais avançado de desenvolvimento. Vários testes de campo têm sido feitos no Reino Unido e outros países utilizando Mondex como um sistema de pagamento do dia a dia nas transações POS (Locais de Venda). Em 1997, a MasterCard adquiriu 51% da Mondex. O Mondex é um sistema não-anônimo, offline e baseado em token. Existem poucas informações técnicas disponíveis sobre o seu protocolo. O sistema usa hardware de propósito especial, como smart cards para aumentar a segurança criptográfica.

Existem planos de se utilizar o Mondex na *Internet*, onde um leitor de cartões compatível com o Mondex é conectado ao computador do consumidor. Quando uma transação necessita ser processada o computador e o cartão se comunicam via esse leitor. Desta forma o sistema Mondex pode ser usado tanto para transações POS quanto para *Internet*.

Para usar o sistema Mondex os consumidores necessitam de um smart card da Mondex que armazena dinheiro digital e pode manipular até cinco tipos diferentes de moedas. Com o Mondex, os consumidores podem pagar comerciantes equipados com um terminal de venda do sistema, que é usado para transferir dinheiro do cartão Mondex do consumidor para o cartão Mondex do comerciante.

O sistema Mondex utiliza o seguinte hardware:

- Smart card da Mondex.
- Terminal de venda da Mondex, usado para transferir fundos do cartão do consumidor para o terminal do comerciante.

- Carteira Mondex, uma unidade de bolso para armazenar quantias maiores de dinheiro digital do que o cartão poderia suportar. A carteira permite que as pessoas realizem transferências entre cartões.
- Leitor de balanço Mondex, um pequeno dispositivo que checa o balanço atual do cartão Mondex. Este item foi criado devido ao pedido de usuários do piloto.
- Mondex hotline utilizada para acessar a conta bancária para transferir dinheiro para o cartão, para checar o balanço e para transferir dinheiro para os outros portadores de cartão.
- Mondex ATM (Máquinas de carregamento automático) usadas para recarregar cartões ou para transferir dinheiro para a conta, etc.

Basicamente consumidores não precisam de nenhum outro hardware além do próprio cartão, mas projetos piloto têm mostrado que consumidores desejam ao menos ler o balanço do seu cartão a qualquer hora.

Basicamente, nenhuma autenticação é necessária, mas é possível bloquear o cartão Mondex com uma senha. O limite por transação é de 500 libras. O cartão Mondex grava todas as transações. Ele armazena um identificador único de 16 dígitos do consumidor registrado no banco onde as informações pessoais do consumidor estão guardadas. Dessa forma cartões Mondex que foram perdidos podem ser devolvidos para os seus donos. O cartão Mondex gera uma assinatura digital que é reconhecida pelas outras partes da transação, de modo que dois cartões podem se autenticar. Valor monetário pode ser transferido somente de um proprietário do cartão Mondex para um terminal compatível ou armazenado em um

dispositivo Mondex. Assume-se que uma fraude seria antieconômica porque envolveria duplicação de hardware. Além disso, a Mondex planeja trocar o complexo chip de segurança em uma base bastante freqüente, porém irregular, para minimizar os riscos de ataques desse tipo. A Mondex quer utilizar esse exemplo para identificar fraudes e usos irregulares de seus cartões facilmente.

O Mondex não é anônimo, o banco pode investigar todas as transações e construir perfis de consumidores. Porém, devido à ausência de especificações técnicas para o público não é possível gerar um perfil de visibilidade do sistema. (ANONYMOUS, 1997 ; JONES, 1996)

### **5.30. MPTP**

Endereço Web: <http://www.w3.org/pub/WWW/TR/WD-mptp>

Nome: MPTP

Origem: W3 Consortium.

Status: Estudo, 1995.

Tamanho do pagamento: Micro-pagamentos

Modelo de moeda: Token.

Modelo de pagamento: Provavelmente, cash like.

Notas: Sem progresso.

Genealogia: Implementa idéias do PayWord, MilliCent e iKP.

O Protocolo de Transferência de Micro Pagamentos (MPTP) é uma proposta do Grupo de Pagamentos Eletrônicos do Consórcio W3C. Ele foi lançado em 1995 e não teve progressos significativos desde então. MPTP é um protocolo para transferência de pagamentos através de um corretor comum, que promete ser econômico para pequenos pagamentos e aplicações interativas. O protocolo implementa uma variação da proposta PayWord do Rivest e Shamir e foi inspirado pela proposta MilliCent de Manasse e do iKP da IBM.

Para eficiência, é desejável poder combinar instruções de transferências de pagamentos acompanhados do envio de produtos. Por esta razão, MPTP pode ser agregado em vários protocolos da *Internet* incluindo SMTP e HTTP. Apesar desse protocolo ser otimizado para uso como um esquema de pagamento, ele é utilizável para a transferência de grandes quantias. O protocolo pode ser utilizado também para controle de acesso ou mecanismo de alocação de recursos. Com algumas modificações, ele pode ter garantia de anonimato (HALLAM-BAKER et al, 1995).

### **5.31. Mykro-iKP**

EndereçoWeb:

[http://www.zurich.ibm.ch/Technology/Security/publications/1996/H  
SW96.ps.gz](http://www.zurich.ibm.ch/Technology/Security/publications/1996/H<br/>SW96.ps.gz)

Nome: Mykro-iKP

Origem: Waidner, M. et al. da IBM.

Status: Proposta, 1997.

Tamanho do pagamento: Micro-pagamentos

Modelo de moeda: Token.

Modelo de pagamento: Provavelmente, cash like.

Notas: Pode ser transferido para o SET.

Genealogia: Similar ao PayWord, baseado no iKP.

Esta proposta da IBM envolve divisões em cadeia similares ao PayWord. Ele implementa um sistema de micro-pagamento no topo do iKP. Uma descrição detalhada de um sistema de cadeias é dada no NetCard. Aqui, são apontados apenas alguns aspectos específicos do Mykro-iKP.

O sistema é baseado em uma divisão em cadeia. Ele faz micro-pagamentos revelando pré-imagens de uma assinatura Winternitz. Os pagamentos são assegurados e pré-autorizados em uma transação inicial iKP, que assegura ao comerciante o crédito do consumidor. Cada micro-pagamento individual é assinado pelo consumidor. Um tipo de esquema de assinatura dual é utilizado para atrelar um micro-pagamento a um micro-envio.

O sistema necessita de um hábito repetitivo de gastos do consumidor. Para hábitos não repetitivos de gastos a Mykro-iKP propõe os chamados micro payment brokers, um mecanismo que não parece ser econômico (HAUSER, STEINER, WAIDNER, 1996).

### **5.32. NETCHEQUE**

Endereço Web: <http://gost.isi.edu/info/netcheque>

Nome: NetCheque

Origem: G. Medvinsky e B.C. Neuman da University of Southern California

Status: Protótipo disponível, dezembro 1994.

Tamanho do Pagamento: Micro-pagamentos.

Modelo de Moeda: Notacional

Modelo de pagamento: Direct account based, tipo cheque.

Validação: on-line.

Controle de Privacidade: Não anônimo, rastreável, não confidencial.

Mecanismos de segurança: Autenticação Kerberos

Pré-requisitos: Software NetCheque

Risco: Comerciante

Taxas: não disponível

Latência/Custos: Muito alta devido à autorização on-line.

Base de Usuários: -

Limites: Restrições de exportação do Kerberos.

Nota: O site da Web não contém material recente.

O NetCheque de G. Medvinsky e B.C. Neuman é um serviço para cheques digitais, enquanto que o projeto NetCash, dos mesmos autores, descreve um sistema de moeda eletrônica.

NetCheque permite que os consumidores usem contas em bancos de sua escolha, permitindo a escalabilidade. Com uma conta NetCheque, o cliente pode emitir e reembolsar cheques digitais. O NetCheque também pode ser usado para descontar o NetCash entre diferentes servidores.

Originalmente, o sistema de conta do NetCheque foi desenvolvido para manter quotas para recursos de sistemas distribuídos, como impressos, que envolve transações de pequenas quantias. Por isso o NetCheque se encaixa bem em micro-pagamentos. É usada criptografia de chave compartilhada, ou seja, a autenticação Kerberos. Normalmente, sistemas baseados em cheques usam assinaturas de chave pública e criptografia, como por exemplo, o FSTC. Mas o grupo do NetCheque afirma que as chaves simétricas são mais rápidas e portanto melhores para micro-pagamentos. Devido às restrições de exportação do Kerberos, o NetCheque só está disponível dentro dos Estados Unidos. Seu software já está disponível para SunOS e HP-UX.

As transações do NetCheque são rastreáveis e on-line e ocorrem dessa maneira:

- Moeda e quantia do cheque, data de validade, conta e destinatário são escritos no cheque.
- Para emitir um cheque, o sistema NetCheque obtém um ticket Kerberos para autenticar o pagador e usa essa informação como assinatura do cheque.
- O cheque “assinado” é codificado (base64) e enviado ao destinatário pelo e-mail ou on-line.



- Para depositar o cheque, o destinatário decodifica-o e obtém um ticket Kerberos que garante que o cheque só pode ser creditado em sua conta.
- O destinatário abre uma conexão criptografada com o servidor de contas do emissor para descontar o cheque.

Esses cheques podem ser descontados on-line ou processados em lote. Outras funções do NetCheque permitem a visualização dos balanços e transações.

Tabela 28 : Perfil de visibilidade do NetCheque

<b>Quem/O que</b>	<b>Comerciante</b>	<b>Comprador</b>	<b>Data</b>	<b>Quantia</b>	<b>Item</b>
Comerciante	-	Sim	Sim	Sim	Sim
Comprador	Sim	-	Sim	Sim	Sim
Banco	Sim	Sim	Sim	Sim	Não
Observador	Sim	Sim	Sim	Sim	Não

A tabela acima mostra o perfil de visibilidade do NetCheque. É um sistema de total identificação. Como o cheque não é criptografado, um observador pode lê-lo. O observador só não pode ver o item negociado se o pedido não estiver conectado ao pagamento.

Tabela 29 : Requisitos do NetCheque

<b>Requisitos/Sistema</b>	<b>NetCheque</b>
Sistema de token	Não
<b>Transação</b>	
Atomicidade	Sim
Consistência	Sim
Isolamento	Não
Durabilidade	Sim
<b>Segurança</b>	
Sem gasto dobrado	-
Sem falsificação	Sim
Sem limite de gastos	Não
Não-refutável	Não
Sem uso não-autorizado	Sim
Anonimato	Não
Sem traços	Não
<b>Interoperabilidade</b>	
Divisibilidade	-

Bidirecionamento	Sim
Gasto encadeado	Não
Aceitação	Sim
Suporte a várias moedas	Sim
<b>Escalabilidade</b>	
Escalabilidade	Sim
Operações Offline	Não
<b>Questões Econômicas</b>	
Operacional	Não, apenas uma comunidade fechada de usuários
Grande base de usuário	-
Risco do comprador	Não
Risco do vendedor	Sim
Confiabilidade	-
Conservação	Sim
<b>Facilidade de uso</b>	
Sem obstrução	Não
Baixa latência	Não
Micro-pagamentos	Sim, limitado.
Macro-pagamentos	Sim, muito limitado.
Baixos custos fixos	-
Independência do hardware	Sim

O perfil de Requisitos é muito similar ao cheque tradicional exceto pelo fato de ser mais econômico para micro-pagamentos.

NEUMAN, MEDVINSKY (1995)

### **5.33. NETBILL**

Endereço Web: <http://www.netbill.com>

Nome: NetBill

Origem: CMU

Status: Teste local, 1997.

Tamanho do Pagamento: pequenos pagamentos.

Modelo da Moeda: Notacional.

Modelo de pagamento: Direct account based, incluindo modelo de transação segura.

Validação: on-line

Controle de privacidade: Não anônimo, rastreável, servidor NetBill pode guardar dados confidenciais.

Mecanismo de segurança: Chave de criptografia pública/simétrica e Kerberos.

Pré-requisitos: Software Money Tool.

Taxas: Comerciantes pagam.

Latência/Custos: Relativamente alta, portanto ruim para micro-pagamentos.

Base de Usuários: 100.

Notas: Segurança financeira e proteção à fraude.

NetBill é o projeto de servidor de pagamento para *Internet* da Carnegie-Mellon University, usado como método de pagamento na compra de informação e serviços. O sistema cobra por transações

e o consumidor precisa ter uma conta NetBill pré-paga da qual todos os pagamentos são deduzidos. NetBill usa chaves de criptografia simétrica e pública. Usa o Kerberos para autenticação.

O servidor de contas, chamado servidor NetBill, mantém contas dos consumidores e dos comerciantes. O sistema age como agregador ao combinar pequenas e grandes transações. Portanto, comprador e vendedor devem confiar no servidor NetBill.

O protocolo básico é o seguinte:

- Comerciante envia a mercadoria criptografada para o computador do consumidor.
- O software no computador do consumidor verifica o recebimento e envia uma verificação para o software do comerciante.
- O comerciante envia ao servidor NetBill a mensagem de verificação do consumidor, informações da conta do consumidor e chave de descriptografia.
- O servidor verifica se o dinheiro na conta do consumidor é suficiente para o pagamento. Se houver saldo, ele transfere fundos, chave de descriptografia e relatório para o software do comerciante.
- O comerciante, então, envia a chave de descriptografia que é usada pelo software do consumidor para descriptografar a mercadoria. Se houver qualquer problema por parte do servidor do comerciante, o software do consumidor pode conseguir sua chave do servidor NetBill.

O servidor NetBill mantém contas para todos os lojistas e compradores. As contas estão vinculadas a contas em bancos

tradicionais. O sistema está em fase de teste no Campus da Carnegie-Mellon. Há uma demonstração on-line do NetBill. O software está disponível para Solaris, Windows NT e Windows 95.

Tabela 30 : Perfil de visibilidade do NetBill

<b>Quem/O que</b>	<b>Comerciante</b>	<b>Comprador</b>	<b>Data</b>	<b>Quantia</b>	<b>Item</b>
Comerciante	–	Sim	Sim	Sim	Sim
Comprador	Sim	–	Sim	Sim	Sim
Banco	Sim	Sim	Sim	Sim	Parcial
Observador	Parcial	Parcial	Sim	Não	Não

NetBill não é um sistema anônimo. O grupo do NetBill sugere um sistema alternativo onde as transações são mediadas por uma terceira parte, por exemplo, o banco com o servidor NetBill.

Tabela 31 : Perfil de visibilidade do NetBill com Mediador

<b>Quem/O que</b>	<b>Comerciante</b>	<b>Comprador</b>	<b>Data</b>	<b>Quantia</b>	<b>Item</b>
Comerciante	–	Não	Sim	Sim	Sim
Comprador	Não	–	Sim	Sim	Sim
Banco	Sim	Sim	Sim	Sim	Parcial
Observador	Não	Não	Sim	Não	Não

Usando uma terceira parte e criptografia, comerciante, comprador, quantia e itens ficam ocultos para o observador. O servidor NetBill ainda terá total conhecimento das identidades das partes e dos detalhes da transação.

Tabela 32 : Requisitos do NetBill

<b>Requisitos/Sistema</b>	<b>NetBill</b>
Sistema de token	Não
<b>Transação</b>	
Atomicidade	Sim
Consistência	Sim
Isolamento	Sim
Durabilidade	Sim
<b>Segurança</b>	
Sem gasto dobrado	–
Sem falsificação	Sim

Sem limite de gastos	Sim, pré-pago.
Não-refutável	Sim
Sem uso não-autorizado	Sim
Anonimato	Não, basicamente não.
Sem traços	Não
<b>Interoperabilidade</b>	
Divisibilidade	-
Bidirecionamento	Não
Gasto encadeado	Não
Aceitação	n.d.
Suporte a várias moedas	Potencialmente, via servidor NetBill.
<b>Escalabilidade</b>	
Escalabilidade	Não
Operações Offline	Não
<b>Questões Econômicas</b>	
Operacional	Não
Grande base de usuário	-
Risco do comprador	n.d.
Risco do vendedor	n.d.
Confiabilidade	n.d.
Conservação	Sim
<b>Facilidade de uso</b>	
Sem obstrução	Questionável
Baixa latência	Não
Micro-pagamentos	Talvez baixo, mas não micro.
Macro-pagamentos	Sim
Baixos custos fixos	-
Independência do hardware	Sim

Economia e escalabilidade são questionáveis por causa do grande tráfego na rede durante uma transação e a interação com o servidor NetBill. ( SIRBU, TYGAR ,1995; CAMP, SIRBU, TYGAR 1995b).

### **5.34. NETCARD**

Endereço Web: <http://www.cl.cam.ac.uk/users/cm213/Project>

Nome NetCard

Origem: Universidade de Cambridge

Status: Protótipo de demonstração, 1996.

Tamanho do pagamento: Micro-pagamentos

Modelo de Moeda: Tipo de token

Modelo de pagamento: Direct cash like.

Validação: Offline

Controle de privacidade: Não anônimo, mas consumidor pode usar pseudônimos, rastreável, pouco confidencial.

Mecanismo de segurança: Divisões em cadeia, criptografia de chave pública, certificados, assinaturas, smart cards invioláveis.

Pré-requisitos: Software e smart card

Risco: Comerciante

Taxas: cobradas dos comerciantes.

Latência/Custos: Baixa

Base de Usuário: –

Genealogia: Similar ao PayWord, Mykro-iKP ou PhoneTicks.  
Proposta baseada no SET.

NetCard foi desenvolvido para micro-pagamentos pela Cambridge University. A participação de especialistas em smart cards e de

bancos ingleses garante a integração financeira e tecnológica. O projeto visa desenvolver um protocolo de rede e gateways para suportar redes de comunicação com grande volume de dados incluindo funções de controle que formarão a base de protocolos de alta velocidade (NETCARD, 1996).

NetCard é um mecanismo de pagamento que envia pagamentos consecutivos ao comerciante usando divisões assinadas em cadeia e smart cards para controle de assinatura e gastos dobrados.

O projeto prevê soluções para o desenvolvimento de uma série de protocolos e mecanismos de smart card para gerenciar as funções de autenticação, autorização, contabilidade e rejeição. A tecnologia NetCard foi avaliada em um sistema de teste multimídia conectando as universidades de Cambridge e Manchester.

Os usuários do NetCard recebem sua chave pública e seu contexto de pagamento, por exemplo, limite de crédito ou pseudônimo, certificado pelo emissor.

Descrição de uma transação básica com o NetCard:

- O emissor dá ao consumidor as moedas assinadas, isto é, grupo de tokens numerados em uma série, criptografados.
- Se o consumidor resolve efetuar uma compra, ele divide os tokens de uma moeda assinada incluindo um identificador de transação único, por exemplo, pseudônimos do consumidor e do comerciante e uma seqüência de números, começando pelo último token e o primeiro identificador. Depois assina a divisão final (do primeiro token), junto com o certificado do consumidor. Assinatura, divisão e armazenagem de tokens são supervisionados pelo smart card inviolável.



- Para iniciar o pagamento consecutivo repetido, o consumidor envia ao comerciante o certificado assinado e a divisão do primeiro token (isto é, a última divisão computada). O comerciante verifica a assinatura com o certificado do emissor.
- Para gastar o primeiro token, o consumidor envia ao comerciante o primeiro token junto com a divisão do segundo (ou seja, a penúltima divisão computada). Se a divisão do primeiro token enviada na mensagem anterior combinar com a divisão computada pelo comerciante do primeiro token e a divisão do segundo, o token é aceito como válido. Tokens consecutivos são tratados de maneira similar.
- Para resgatar os tokens, o comerciante apresenta a assinatura do consumidor ao adquirente, os tokens gastos e os valores correspondentes das divisões. O banco verifica os tokens e checa o gasto em dobro.

#### Transação do NetCard com SET:

- O consumidor cria uma série de moedas, formando um grupo, assina-o e divide-o como descrito acima. A soma das moedas no grupo de pagamento representa o limite máximo das compras pretendidas.
- O consumidor envia o certificado assinado, a primeira divisão e o limite máximo de compra para o comerciante junto com os detalhes de seu cartão de crédito em uma transação SET. O comerciante consegue uma pré-autorização para a quantia no ambiente SET para prevenir gastos dobrados.
- O consumidor efetua repetidas transações de pagamento consecutivas revelando um token por vez, como descrição acima.

- Depois que o consumidor assinala o fim da transação, o comerciante envia uma mensagem de captura SET para receber a quantia de tokens. Ele inclui os tokens, assinaturas e divisões recebidas como prova da transação.

Essa versão do protocolo representa mais uma transação direct account based notacional de curta duração com uma apresentação segura de cartão de crédito do que um protocolo de pagamento baseado em tokens. (ANDERSON, MANIFAVAS, SUTHERLAND, 1996)

Tabela 33 : Perfil de visibilidade do NetCard com Mediador

<b>Quem/O que</b>	<b>Comerciante</b>	<b>Comprador</b>	<b>Data</b>	<b>Quantia</b>	<b>Item</b>
Comerciante	-	Parcialmente/ Sim	Sim	Sim	Sim
Comprador	Sim	-	Sim	Sim	Sim
Banco	Sim	Sim	Sim	Sim	Não
Observador	Sim	Parcialmente/ Sim	Sim	Sim	Sim

A identificação do consumidor depende do uso de pseudônimos.

Tabela 34 : Requisitos do NetCard

<b>Requisitos/Sistema</b>	<b>NetCard</b>
Sistema de token	Sim (primeira versão), não (segunda versão)
<b>Transação</b>	
Atomicidade	n.d.
Consistência	n.d.
Isolamento	n.d.
Durabilidade	n.d.
<b>Segurança</b>	
Sem gasto dobrado	Sim, smart card. Base de dados de gastos dobrados no banco
Sem falsificação	Sim
Sem limite de gastos	Sim, com a pré-autorização do SET.
Não-refutável	Sim
Sem uso não-autorizado	Sim, smart cards e assinaturas.
Anonimato	Não, mas consumidor pode usar pseudônimo.
Sem traços	Não
<b>Interoperabilidade</b>	
Divisibilidade	Não
Bidirecionamento	Não

Gasto encadeado	Não
Aceitação	Potencialmente
Suporte a várias moedas	Potencialmente.
<b>Escalabilidade</b>	
Escalabilidade	Sim
Operações Offline	Sim
<b>Questões Econômicas</b>	
Operacional	Não
Grande base de usuário	-
Risco do comprador	Não
Risco do vendedor	Sim
Confiabilidade	-
Conservação	Sim
<b>Facilidade de uso</b>	
Sem obstrução	-
Baixa latência	Sim
Micro-pagamentos	Sim
Macro-pagamentos	Não
Baixos custos fixos	-
Independência do hardware	Não, smart card.

### **5.35. NETCASH**

Endereço Web: <http://nii-server.isi.edu/info/netcash>

Nome NetCash

Origem: G. Medvinsky e B.C. Neuman da University of Southern California

Status: Teste fechado, 1966.

Tamanho do pagamento: Micro-pagamentos

Modelo de Moeda: Token

Modelo de pagamento: Direct cash like.

Validação: on-line

Controle de privacidade: Anônimo, não rastreável, mas não com relação ao servidor de Moeda NetCash, questões de privacidade não mencionadas.

Mecanismo de segurança: Certificados, assinaturas, base de dados de gastos duplos.

Pré-requisitos: Software do NetCash

Risco: Consumidor

Taxas: não disponível

Latência/Custos: Razoavelmente alta.

Base de Usuário: -

Limites: não disponível

Notas: Web site não contém material recente

Genealogia: Integrado com o NetCheque.

NetCash descreve um sistema de moeda eletrônica para pagamentos real-time digitais, seguros e anônimos. Esse sistema procura integrar moeda eletrônica anônima a infraestrutura bancária. Se houver uma maior necessidade de segurança, o sistema pode ser estendido. NetCash não necessita de hardware inviolável ou redes seguras e se adapta bem à *Internet* (NETCASH, 1996).

A estrutura básica consiste de servidores de moeda independentes que funcionam como um link entre moedas eletrônicas anônimas e serviços não anônimos, como os cheques digitais da NetCheque. O servidor de moeda atende ao consumidor, como a detecção de gasto em dobro, troca de moeda e compra de moeda com cheque (NETCHEQUE, 1996).

NetCash usa autenticação de múltiplas camadas, similar à adotada pelo FSTC. Para a instalação de um servidor de moeda, a nova moeda precisa ser segurada por uma seguradora, como o Federal Reserve. O servidor é integrado à rede estabelecendo-se uma conexão segura entre ele e a seguradora para obter sua chave pública e o certificado único de identidade do servidor. Esse certificado permite que o novo servidor crie e gerencie a moeda digital que será aceita por outros servidores de moeda e bancos. A moeda produzida por ele precisa estar vinculada a balanços das tradicionais contas bancárias.

A moeda NetCash contém o nome do servidor que a emitiu, um número de série único, uma referência ao certificado da seguradora e é assinada pelo servidor de moeda. Quem a receber poderá verificar sua validade.

NetCash tem um sistema que detecta gasto dobrado.. O servidor de moeda do Netcash registra o número de série único de cada moeda emitida. Se o consumidor tentar gastar uma moeda que já foi usada ou que tenha um número não registrado, o servidor de moedas não aceitará a transação.

O grupo do NetCash alega que esse sistema é melhor do que o Ecash, pois no Ecash, a lista de moedas gastas deve ser mantida por um tempo indefinido para prevenir o gasto duplo ou então as moedas têm data de validade. O Ecash não possui uma lista das moedas emitidas devido ao esquema de blind signature que garante o anonimato.

Tabela 35 : Perfil de visibilidade do NetCash

<b>Quem/O que</b>	<b>Comerciante</b>	<b>Comprador</b>	<b>Data</b>	<b>Quantia</b>	<b>Item</b>
Comerciante	–	Não	Sim	Sim	Sim
Comprador	Não	–	Sim	Sim	Sim
Banco	Sim	Sim	Sim	Sim	Não
Observador	Não	Não	Sim	Sim	Sim

As transações do NetCash são validadas on-line e alegam manter o anonimato do consumidor. No entanto, esse anonimato não é valido para o servidor de moedas que pode rastrear quem comprou e quem resgatou as moedas. É necessário que consumidores e comerciantes confiem no servidor NetCash pois as transações não possuem log.

NetCash oferece um grau escalável de anonimato, dependendo das necessidades de transação. Isso dificulta a definição do perfil de visibilidade. NetCash pode rastrear as moedas emitidas e a única coisa que garante que isso não será feito é a palavra de honra. A tabela acima mostra o perfil de visibilidade possível e não o prometido.

Tabela 36 : Requisitos do NetCash

<b>Requisitos/Sistema</b>	<b>NetCash</b>
Sistema de token	Sim
<b>Transação</b>	
Atomicidade	n.d.
Consistência	n.d.
Isolamento	n.d.
Durabilidade	n.d.
<b>Segurança</b>	
Sem gasto dobrado	Sim
Sem falsificação	Sim
Limite de gastos	-
Não-refutável	muito provavelmente
Sem uso não-autorizado	muito provavelmente
Anonimato	Sim, mas não com o servidor de moeda.
Sem traços	Sim, mas não com o servidor de moeda.
<b>Interoperabilidade</b>	
Divisibilidade	Sim
Bidirecionamento	Sim
Gasto encadeado	Não, apenas simulado.
Aceitação	Potencialmente
Suporte a várias moedas	Potencialmente, se suportado por bancos
<b>Escalabilidade</b>	
Escalabilidade	Sim
Operações Offline	Não
<b>Questões Econômicas</b>	
Operacional	Não
Grande base de usuário	-
Risco do comprador	Sim, limitado ao número de moedas.
Risco do vendedor	Não
Confiabilidade	-
Conservação	Sim
<b>Facilidade de uso</b>	
Sem obstrução	-
Baixa latência	Não
Micro-pagamentos	Sim
Macro-pagamentos	Não
Baixos custos fixos	-
Independência do hardware	Sim

Escalabilidade depende de múltiplos servidores de moedas e a interoperabilidade depende da cooperação entre esses servidores.

( MEDVINSKY, NEUMAN, 1993)

### **5.36. NetFare**

Endereço Web: <http://www.netfare.com>

Nome: NetFare

Status: Em construção, 1997.

Tamanho do pagamento: Micro-pagamentos.

Modelo de moeda: Notacional.

Modelo de pagamento: Indirect push account based.

Validação: on-line

Controle de privacidade: Nenhum.

Mecanismo de segurança: Senha (PIN).

Pré-requisitos: Cartão NetFare e PIN; software.

Limites: Apenas dólares.

Risco: Consumidor.

Taxas: –

Latência/Custos: Muito alta devido à autorização on-line.

Base de usuários: –

Notas: Sistema muito simples.

NetFare é um cartão pré-pago, similar a um cartão telefônico, para uso na *Internet* principalmente. Seu Web site contém apenas uma pequena descrição do sistema. Atualmente eles estão conduzindo uma pesquisa para descobrir quem poderia estar interessado no sistema (NETFARE, 1996).



Consumidores necessitam comprar os cartões NetFare, que são identificados por um número e autenticados com um PIN. Eles correspondem a contas pré-pagas no servidor central NetFare. Consumidores podem checar seus balanços on-line com o número de seu cartão e seu PIN.

Em uma requisição de pagamento de um comerciante, o servidor NetFare precisa do número do cartão e o PIN do consumidor e verifica o balanço da conta do usuário. Se o pagamento desejado é possível, NetFare transfere a quantia para a conta do comerciante e dá a ele um sinal para enviar os produtos. Os comerciantes são reembolsados uma vez por mês.

### **5.37. OpenMarket**

Endereço Web: <http://www.openmarket.com>

Origem: Open Market Inc.

Modelo de pagamento: Software de negócios eletrônicos.

Status: Operacional, 1994 (como companhia).

Genealogia: Incluirá facilidades de pagamento SET.

Open Market Inc. foi fundada em fevereiro de 1994 e faz soluções de comércio eletrônico. Seu produto para comércio para *Internet* é o Transact, que gerencia comércio pela *Internet* dentro de uma corporação ou operações de provedores de serviços comerciais. O sistema oferece funcionalidade como gerência, serviço on-line para o consumidor, segurança, autenticação, gravações, compras variadas, modelos de pagamento e processamento seguro de transações incluindo taxas de vendas e de embarque.

Open Market participou na primeira demonstração conjunta do SET e está compatibilizando seu sistema Transact com o SET. Open Market coopera com MasterCard e Visa.

### **5.38. PayMe**

EndereçoWeb:

<http://www.w3.org/Conferences/WWW4/Papers/228>

Nome: PayMe

Origem: M. Peirce e D. O'Mahony do Computer Science Department. Trinity College, Dublin, Irlanda.

Status: Proposta, 1995.

Tamanho do pagamento: Micro-pagamentos.

Modelo de moeda: Token.

Modelo de pagamento: Direct cash like.

Validação: on-line

Controle de privacidade: Pouco anônimo, pouco rastreável, confidencial, como NetCash.

Mecanismo de segurança: Senhas, assinaturas, criptografia.

Pré-requisitos: Software da carteira PayMe.

Risco: Consumidor.

Genealogia: Tenta combinar características do Ecash e NetCash

O sistema PayMe tenta combinar as melhores características do Ecash e do NetCash. Ele é um projeto dos mestrandos M. Peirce e D. O'Mahony do Departamento de Ciência da Computação da Faculdade de Trinity em Dublin, Irlanda. Um protótipo foi implementado. A força do Ecash é o total anonimato garantido e a

impossibilidade de rastreamento, e o seu principal problema é o tamanho da base de moedas utilizadas, para evitar duplo gasto. As vantagens apontadas do NetCash são a sua escalabilidade e segurança e sua desvantagem é não permitir total anonimato e ser rastreável.

O sistema PayMe alega ser um serviço anônimo e escalável de dinheiro eletrônico, que usa o seu próprio protocolo seguro de comunicações, o Protocolo PayMe de Transferência (PMTP), para comunicação entre as partes envolvidas. PayMe utiliza tanto chaves simétricas quanto criptografia de chave pública. Todas as partes envolvidas têm seu próprio par de chaves públicas. O protocolo é confidencial e todas as mensagens são criptografadas. Ele oferece aproximadamente o mesmo anonimato e impossibilidade de investigação do NetCash.

Um banco PayMe cunha tokens, mantém um base de dados com todos os tokens que não foram resgatados para evitar duplo gasto, troca tokens por demanda e gerencia contas de seus clientes. Clientes PayMe são consumidores e comerciantes, mas o sistema é bidirecional. Pagamentos precisam ser exatos. Não é dado troco.

Uma transação PayMe ocorre da seguinte forma:

- Para comprar produtos, uma URL de compra apontando para um script cgi é selecionada. Isso causa a abertura da carteira do comerciante através do servidor Web.
- A carteira do comerciante recebe os detalhes dos produtos e o endereço IP do cliente.
- A carteira do comerciante calcula o valor total e contacta a carteira do consumidor, pedindo o pagamento.

- O comprador é notificado do pedido e poderá recusar ou aceitar o pedido de pagamento. Ao aceitar a carteira do consumidor seleciona as moedas necessárias para fazer o pagamento exato e as envia para a carteira do comerciante.
- A carteira do comerciante valida as moedas de duas formas: ou as troca anonimamente por novas moedas ou depositando elas em uma conta de banco. Uma troca precisa ser feita com o emissor. Um depósito pode ser feito com o adquirente. O emissor faz a verificação de gasto duplo e remove as moedas reembolsadas de sua base de dados. Em uma troca o comerciante recebe novas moedas, de outra forma a quantia é creditada a conta do adquirente.
- A carteira de comerciantes recebe uma indicação do banco se as moedas eram válidas. Podem ser novas moedas ou uma mensagem de sucesso de depósito.
- A carteira do comerciante envia um sinal de recebimento para o consumidor e envia os produtos. O servidor do consumidor então os manda para o cliente.

A proposta não mostra de que forma ela é superior ao Netcash no que diz respeito a anonimato e impossibilidade de rastreamento. Ela parece se comportar da mesma maneira que o outro sistema.

### **5.39. PayNow**

Endereço Web: <http://www.cybercash.com>

Nome: PayNow

Origem: CyberCash Inc.

Status: Teste, 1997.

Modelo de pagamento: Direct account based, parecido com cheque.

Mecanismo de segurança: Integrado à carteira CyberCash

Esquema de cheque eletrônico da CyberCash, integrado dentro da sua carteira. Funciona como apresentação segura de cartão de crédito, e será bidirecional. As informações disponíveis são quase nulas.

#### **5.40. PayWord**

EndereçoWeb:

<http://theory.lcs.mit.edu/~rivest/RivestShamir-mpay.ps>

Nome: PayWord

Origem: Rivest e Shamir

Status: Proposta, 1995.

Modelo de pagamento: Direct cash like

Controle de privacidade: Nenhum.

Mecanismo de segurança: divisões em cadeia, assinaturas.

A proposta de Rivest e Shamir envolve pagamentos encadeados. Uma descrição detalhada de um sistema encadeado é dada no NetCard. Aqui apenas alguns aspectos especiais do PayWord são apontados.

PayWord é baseado em crédito. O consumidor tem uma relação de espera com um broker. O consumidor é certificado mensalmente pelo broker para enviar cadeias PayWord. Para um comprometimento inicial com um comerciante, o consumidor gera e assina um compromisso para uma nova cadeia específica consumidor/comerciante de paywords. Todos paywords

de uma cadeia devem ter o mesmo valor. Paywords são computados por hash repetidas e um salto inicial. O último a ter seu valor gerado é chamado de root da cadeia payword que não tem valor próprio e é assinado pelo consumidor como compromisso e dado ao comerciante na transação inicial.

Então o consumidor subsequente trocava os paywords na ordem inversa da geração ao comerciante. O comerciante pode verificar o pagamento verificando a hash do payword atual e checando se ele é igual ao valor anterior. No fim de cada dia o comerciante tem todos os compromissos e paywords para o reembolso do broker.

O PayWord não garante anonimato. Consumidores que excedem os valores podem ser retirados após esse fato. Comerciantes e broker compartilham o risco de perdas (RIVEST, SHAMIR, 1995)



#### **5.41. PC-PAY**

EndereçoWeb: <http://www.innovonics.com/pcpay/pcpayhome.html>

Nome: PC-Pay

Modelo de pagamento: Direct cash like com smart card.

Controle de privacidade: Anônimo

Mecanismo de segurança: Criptografia em hardware.

Pré-requisitos: Smart card e leitor, software de interface.

Taxas: US\$ 595 para os pré-requisitos.

O sistema PC-Pay desenvolvido pela Innovonics Inc. Utiliza hardware inviolável, um smart card que criptografa a informação de pagamento antes que ela chegue ao PC. O leitor de cartões é desenhado para agir com um terminal ATM com algumas características adicionais. Não existem informações detalhadas disponíveis de como o sistema funciona.

#### **5.42. PhoneTicks**

Status: Teste, 1995.

Modelo de pagamento: Direct cash like.

Mecanismo de segurança: Divisões em cadeia.

Genealogia: Similar à do PayWord, Mykro-iKP ou NetCard, proposta implementada no CAFE.

Esta proposta de Torbe Pedersen envolve divisões em cadeia. Ela é similar ao PayWord. PhoneTicks supostamente está implementado no CAFE e pode ser colocado como uma tentativa.

Uma detalhada descrição de sistemas encadeados é dada no NetCard. Os detalhes técnicos do PhoneTicks não são de grande profundidade e não parece conter qualquer novidade ou idéia especial em relação às outras propostas de pagamentos encadeadas (PEDERSEN, 1995).

### **5.43. Polling**

Endereço Web: <http://www.research.att.com/~amo/doc/polling.ps>

Nome: Polling

Origem: A. Odlyzko, AT&T.

Status: Proposta, 1997.

Modelo de moeda: Notacional.

Modelo de pagamento: Direct account based.

Tamanho do pagamento: Micro-pagamento.

Mecanismo de segurança: Validação on-line probabilística.

Esquemas de pagamentos existentes podem ser aprimorados na sua eficiência e se adequar para micro-pagamentos ao utilizar eleição probabilística. Esta proposta foi feita por S. Jarecki e A. M. Odlyzko, da AT&T (JARECKI, ODLYZKO, 1997).

Ela permite controle de estouro de gastos a um custo modesto de aumento nas comunicações com relação a um esquema offline. A proposta elabora detalhadamente os parâmetros de votação e analisa seus impactos e riscos, espera e custos de comunicação. Como os autores são matemáticos, não é surpreendente o fato do artigo ser altamente técnico.

Um de seus exemplos propõe a aplicação de votação no PayWord. Sua proposta também inclui a descrição de um registro de um comerciante e esquema de notificação, onde comerciantes registram cada transação inicial com um consumidor em um broker, e no caso de estouro de limite de gastos o broker notifica o comerciante registrado, em vez de uma notificação geral lançada pelo comerciante.

#### **5.44. Redi-Check**

Endereço Web: <http://redi-check.com>

Status: Operacional, abril 1995.

Modelo de pagamento: Direct account based, cheques eletrônicos.

Controle de privacidade: Redi-Check mantém os dados dos consumidores confidenciais.

Mecanismos de segurança: SSL, PGP e SET.

Base de Usuários: 45.000 consumidores e 200 lojistas.

Redi-Check oferece um serviço de preenchimento de cheques. Consumidores precisam apenas de um endereço eletrônico e uma conta bancária com cheque. Sua segurança é baseada em SSL e PGP. Envolve versões digitais dos tradicionais cheques de papel.

#### **5.45. Sandia Lab's Electronic Cash**

Endereço Web: [http://www.cs.sandia.gov/HPCCIT/el\\_cash.html](http://www.cs.sandia.gov/HPCCIT/el_cash.html)

Status: não disponível

Modelo de pagamento: nd

Controle de privacidade: nd

Mecanismos de segurança: TTP, terceira parte.

Sandia Lab's Electronic Cash utiliza uma terceira parte para rastrear transações e ao mesmo tempo tentar manter o anonimato do consumidor. As palavras chaves são rastreamento baseado em confiança. Eles alegam ter um sistema eletrônico comprovadamente anônimo. Somente com a cooperação de diversas terceiras partes é que seria possível o rastreamento.

#### **5.46. SECURE COURIER**

Endereço Web: <http://www.netscape.com/newsref/std/credit.html>

Origem: Netscape, T. Elgamal.

Status: Operacional, julho 1995.

Modelo de pagamento: Apresentação segura de cartão de crédito.

Controle de privacidade: Confidencial

Mecanismo de segurança: SSL; será substituído por SET.

Secure Courier é um esquema de apresentação segura de cartão de crédito baseado em SSL da Netscape. Foi englobado pelo SET.

### **5.47. SET**

Endereço Web: <http://www.visa.com/cgi-bin/vee/sf/set/inro.html>  
<http://www.mastercard.com/set>

Nome: SET (Transações Eletrônicas Seguras).

Origem: Visa, MasterCard, CyberCash, Netscape, IBM, Microsoft, DigiCash e várias outras empresas.

Status: Proposta, 1996, Teste de submissão, 1998.

Tamanho do Pagamento: Macro-pagamentos.

Modelo de Moeda: Notacional.

Modelo de Pagamento: Apresentação segura de cartão de crédito.

Validação: on-line

Controle de Privacidade: Confidencial, não anônimo, investigável.

Mecanismos de Segurança: RSA, DES, criptografia, assinaturas, senhas, certificados, cadeia de confiança, dupla assinatura.

Pré-requisito: Carteira eletrônica, cartão de crédito, talvez um smart card no futuro.

Riscos: Consumidor

Taxas: Provavelmente nenhuma, além das taxas normais do cartão de crédito.

Latência/Custos: Bastante alta por causa da autorização on-line, da criptografia cuidadosa e de esquemas de assinatura.

Base de Usuários: Vários sistemas de comércio eletrônico estão ficando compatíveis com o SET.

Limites: não disponível

Notas: Reembolso das transações de cartões de crédito é suportado

Genealogia: Apesar de alguns protocolos obsoletos mencionados acima, SET é fortemente influenciado pelo CyberCash e pelo iKP.

IBM, MasterCard e Visa anunciaram uma aliança para apresentação segura de cartão de crédito pela *Internet*, o Sistema de Transações Eletrônicas Seguras (SET). Após alguns esforços individuais para conseguir seu próprio padrão, as maiores companhias de cartão de crédito, comércio eletrônico, software e hardware se juntaram para desenvolver um modelo industrial unificado, o SET.

Os seguintes padrões proprietários influenciaram e foram englobados pelo SET:

SEPP: Protocolo de pagamento eletrônico seguro obsoleto da MasterCard, IBM, Netscape, GTE e CyberCash

STT: Tecnologia de transações seguras obsoleta da Visa e Microsoft.

SCC: Esquema de cartões de crédito seguros obsoleto da MasterCard e Visa.

iKP: Protocolo de key payment obsoleto da IBM.

CyberCash: Sistema de pagamento de apresentação segura de cartão de crédito atualmente operacional feito pela CyberCash Inc., está ficando compatível com o SET.

O protocolo SET é suportado pela Visa e pela MasterCard, e procura prover um padrão uniforme para transações seguras na





- O comerciante envia a confirmação do pedido para o consumidor.
- O comerciante manda o produto para o consumidor.
- O comerciante faz a requisição do acordo com o emissor, através do adquirente.

Os participantes de uma transação SET são:

***5.47.1. Consumidor/Portador do cartão de crédito:***

O consumidor, ou portador do cartão de crédito (como ele é chamado no SET), usa o cartão que lhe foi enviado pelo emissor para comprar produtos com os comerciantes.

***5.47.2. Emissor:***

O emissor é um banco que mantém uma conta para o consumidor e lhe enviou um cartão de crédito. O emissor garante o pagamento das transações autorizadas.

***5.47.3. Comerciante:***

O comerciante oferece benefícios e recebe pagamentos de cartão de crédito SET. Ele tem um relacionamento financeiro com o adquirente.

***5.47.4. Adquirente:***

O adquirente é um banco que mantém uma conta para o comerciante e processa autorizações e pagamentos de cartão de crédito.

#### **5.47.5. Gateway de pagamento:**

O gateway de pagamento é um dispositivo operado pelo adquirente ou por um terceiro que processa as mensagens de pagamento do comerciante, incluindo instruções para os consumidores. No CyberCash, esse gateway de pagamento é representado pelo servidor da CyberCash.

#### **5.47.6. Autoridade de Certificação:**

É necessário que todos os consumidores e comerciantes sejam registrados com uma Autoridade de Certificação SET antes de eles iniciarem transações. Todos os gateways de pagamento, emissores e adquirentes também devem estar registrados com a Autoridade de Certificação.

As transações SET são não-anônimas e verificadas on-line. Todas as partes envolvidas são conhecidas e autenticadas, todas as transações devem ser on-line para assegurar autenticações e autorizações.

Por utilizar uma combinação de operações de chave pública RSA e chave simétrica DES combinadas com uma cadeia de confiança de certificados digitais, SET identifica e autentica todas as partes envolvidas e assegura o sigilo. Todas as mensagens trocadas no SET são assinadas. Todos os certificados SET podem ser verificados seguindo a cadeia de confiança até a sua raiz. Todas as mensagens contendo dados críticos são criptografadas, ou com uma chave pública ou com uma chave simétrica, e assinadas. Chaves simétricas são utilizadas apenas uma vez, geralmente.

O SET usa dupla assinatura que permite ligar criptograficamente duas mensagens de modo que uma terceira parte possa verificar se uma requisição de pagamento diz respeito a uma certa oferta, sem ver quais são os detalhes dela. Isto é feito criando o sumário tanto da mensagem de pagamento quanto da oferta, concatenando os dois sumários e assinando esse novo sumário criado. Então uma parte que tenha o sumário da oferta e da mensagem de pagamento pode recalcular e verificar a mensagem de dupla assinatura.

As principais transações SET que são utilizadas no registro e compra estão simplificados a seguir:

#### ***5.47.7. Registro do portador do cartão de crédito:***

Os consumidores necessitam do registro no CA antes de poder enviar mensagens SET para comerciantes e também precisam ter um par de chaves para assinatura. A CA verifica os dados do consumidor com o emissor, e gera um certificado de validade limitada para ele com os detalhes do cartão de crédito. Esse certificado é enviado ao consumidor então.

#### ***5.47.8. Registro do comerciante:***

Os comerciantes precisam ser registrados com a CA antes de poderem receber instruções de pagamento SET dos consumidores e eles têm que ter uma chave de troca e um par e chaves de assinatura. A CA verifica os dados do comerciante com o adquirente e gera um certificado de validade limitada para ele, além de lhe certificar a chave de assinatura. Depois, esses certificados são enviados para o comerciante.

#### **5.47.9. Pedido de compra:**

Esta requisição é chamada após o consumidor ter completado a escolha, ter aprovado o formulário de compra completo e selecionado um cartão de crédito para o pagamento. Ao contrário das transações tradicionais com cartão de crédito, que são iniciadas pelo comerciante, no SET o consumidor que a inicia. Ele cria a informação do pedido e as instruções de pagamento, gera a dupla assinatura para essas duas mensagens e as transmite para o comerciante. Os detalhes do cartão de crédito podem ser lidos apenas pelo gateway de pagamento. O comerciante retorna um recibo e processa o pedido.

#### **5.47.10. Autorização de pagamento:**

Durante o processamento de uma ordem, comerciantes precisam receber a autorização de pagamento do gateway. O comerciante envia os detalhes da transação junto com as instruções de pagamento do consumidor para o gateway. Este verifica a dupla assinatura do portador do cartão na instrução de pagamento e assegura a consistência entre os detalhes da transação do comerciante e a instrução de pagamento do consumidor. Então ele obtém uma autorização de pagamento via rede financeira e retorna um token de recebimento para o comerciante. O comerciante então pode continuar processando a ordem.

#### **5.47.11. Recebimento do pagamento:**

Após completar o processamento de uma ordem, ou até mesmo várias ordens, comerciantes vão requisitar o pagamento. Eles enviam os detalhes dos pedidos de captura junto com o token de recebimento para o gateway. Este assegura a consistência entre os detalhes de captura e o token e envia o pedido de recebimento para o emissor pelas redes financeiras, mandando para o comerciante a resposta.

Além disso, transações SET incluem:

#### **5.47.12. Consulta de Certificado:**

Se a CA está incapacitada de completar uma requisição de certificação on-line, consumidores registrados ou comerciantes podem checar novamente mais tarde com essa mensagem para determinar o status daquele pedido de certificação.

#### **5.47.13. Consulta da compra:**

Se um comerciante não conseguir completar uma transação de compra on-line, o consumidor pode verificar novamente mais tarde com essa mensagem para determinar o status do seu processo de pagamento.

#### **5.47.14. Anulação de Autorização:**

Esta transação permite comerciantes corrigirem pedidos prévios de autorização. Ela pode ser aplicada para todo o processo ou apenas parte da ordem para a qual a autorização de pagamento foi requisitada.

#### **5.47.15. Anulação de recebimento:**

Esta transação permite aos comerciantes corrigirem erros nos pedidos de recebimento.

#### **5.47.16. Crédito:**

Esta transação permite aos comerciantes dar crédito para uma conta de cartão de crédito do consumidor, por exemplo, se o produto for devolvido.

#### **5.47.17. Anulação de crédito:**

Esta transação permite que comerciantes revoguem créditos enviados.

#### **5.47.18. Pedido de certificação do gateway de pagamento:**

Esta transação permite aos comerciantes obter todos os certificados atuais e chaves públicas do gateway de pagamento.

#### **5.47.19. Administração de lotes:**

Esta transação permite aos comerciantes comunicarem para o gateway de pagamento seus lotes de processamento.

Tabela 37 : Tabela de visibilidade SET

<b>Quem/O que</b>	<b>Comerciante</b>	<b>Comprador</b>	<b>Data</b>	<b>Quantia</b>	<b>Item</b>
Comerciante	-	Parcial	Sim	Sim	Sim
Comprador	Parcial	-	Sim	Sim	Sim
Banco	Sim	Sim	Sim	Sim	Não
Observador	Não	Não	Sim	Não	Não

A tabela acima mostra a visibilidade entre as entidades no SET. O comerciante enxerga apenas parcialmente o consumidor, já que os dados da conta e do cartão de crédito são criptografados e visíveis apenas para o gateway de pagamento e o banco. O "banco" pode ser distribuído em diferentes entidades, mas como essas entidades podem cooperar para reconstruir transações caso seja necessário, elas são tratadas como uma parte unificada no esquema. No SET, os participantes não são anônimos, mas graças ao esquema de dupla assinatura os detalhes dos produtos dessa transação são confidenciais mesmo para o banco.



Tabela 38 : Tabela de Requisitos SET

<b>Requisitos/Sistema</b>	SET
Sistema de token	Não
<b>Transação</b>	
Atomicidade	Não
Consistência	Sim
Isolamento	Não
Durabilidade	Sim
<b>Segurança</b>	
Sem gasto dobrado	-
Sem falsificação	Sim
Limite de gastos	Não
Não-refutável	Sim
Sem uso não-autorizado	Sim
Anonimato	Não
Sem traços	Não
<b>Interoperabilidade</b>	
Divisibilidade	-
Bidirecionamento	Não
Gasto encadeado	Não
Aceitação	Sim
Suporte a várias moedas	Sim
<b>Escalabilidade</b>	
Escalabilidade	Sim, muito provavelmente.
Operações Offline	Não
<b>Questões Econômicas</b>	
Operacional	Não ainda, mas muitas soluções SET compatíveis estão em desenvolvimento.
Grande base de usuário	Sim, potencialmente.
Risco do comprador	Sim, limitado pelo limite de gastos do cartão de crédito.
Risco do vendedor	Não
Confiabilidade	Sim
Conservação	Sim
<b>Facilidade de uso</b>	
Sem obstrução	Não
Baixa latência	Não
Micro-pagamentos	Não
Macro-pagamentos	Sim
Baixos custos fixos	provavelmente iguais aos de um cartão de crédito.
Independência do hardware	Sim, mas pode integrar smart cards.

O SET não define qualquer sistema de pagamento eletrônico tradicional subordinado a ele, e pode trabalhar com cartões de débito e de crédito. Porém, o SET tem certas propriedades de qualquer sistema de pagamento tradicional.

O SET é muito cuidadoso a respeito de autenticação e autorização. Isto o torna inadequado para micro-pagamentos, ainda mais se o

sistema de pagamento eletrônico subordinado for cartão de crédito. O SET requer quatro mensagens entre o consumidor e o comerciante. Essas quatro mensagens envolvem quatro assinaturas digitais, quatro operações de criptografar e descriptografar com chaves RSA, uma com chave simétrica DES, duas validações de certificado e uma autorização de pagamento pelo gateway para o comerciante, o que consiste em duas mensagens com duas assinaturas digitais, três operações de criptografar e descriptografar com chaves simétricas DES, cinco com chaves públicas RSA e duas verificações de certificados. A questão da escalabilidade aparece com a necessidade de servidores centrais e verificação on-line.

A instituição de sistemas de pagamentos financeiros da IBM PBS/Europay

(<http://www.europe.ibm.com/nc/customer/pbseuro.htm>) está se compatibilizando com o SET. PBS, Europay, IBM e MasterCard se juntaram para criar esse sistema. Um primeiro piloto foi instalado na Dinamarca. (SET 1997a, 1997b e 1997c)

#### ***5.48. Transferências de Dados do Cartão de Crédito via SSL***

Endereço Web: [www.netscape.com](http://www.netscape.com)

Nome: Transferências de dados do cartão de crédito via SSL.

Origem: Netscape e Consórcio W3C

Status: Operacional

Tamanho de Pagamento: Macro-pagamentos

Modelo de Moeda: Notacional

Modelo de pagamento: Apresentação Segura de Cartão de Crédito

Validação: on-line.

Controle de Privacidade: Criptografado, não anônimo, rastreável.

Mecanismos de Segurança: Criptografia de chave pública e chave simétrica. Órgão certificador.

Pré-requisitos: Servidor Web baseado em SSL, browser compatível.

Riscos: Consumidor.

Taxas: Taxas cobradas pelos órgãos certificadores e das administradoras de cartões de crédito.

Latência/Custos: Alta. Todas as certificações são on-line, todas as mensagens são criptografadas.

Base de Usuários: Não disponível.

Genealogia: Baseado em RSA e DES.

Método para apresentação segura de cartão de crédito. É baseado em criptografia com os algoritmos RSA e DES. Necessita de um

browser e de um servidor Web que aceitem SSL. Envolve uma autoridade de certificação. A comunicação entre o servidor e o browser ocorre da seguinte forma:

O browser pede o certificado do servidor, e verifica se ele é válido utilizando para isso a chave pública do emissor do certificado. Se ele for válido, a chave pública do servidor é retirada do certificado e utilizada para enviar mensagens para o servidor (MUDRY, 1995).

Por esse meio seguro de comunicação, são enviadas as informações pessoais e do cartão de crédito. (SIYAN, HARE, 1998)

#### **5.49. SUBSCRIP**

EndereçoWeb:

<http://www.cs.newcastle.edu.au/Research/afurche/subscrip.ps>

Status: Proposta, 1996.

Modelo de pagamento: Notacional.

A. Furche e G.Wrightson da Universidade de Newcastle propõem um sistema de micro-pagamentos repetidos baseados em contas temporárias dos consumidores com os comerciantes. Essas contas são pré-pagas com um sistema de pagamento convencional. Esse sistema convencional de pagamento precisa aceitar reembolso também. (FURCHE e WRIGHTSON, 1996)

### **5.50. TUB**

Endereço Web: <ftp://ftp.cl.cam.ac.uk/users/djw3/tub.ps>

Nome: TUB

Modelo de Pagamento: Micro-pagamentos

Origem: D. Wheeler

Status: proposta, abril 1996.

Genealogia: Similar ao Lottery Tickets

Transações que utilizam apostas (TUB) são uma proposta simples de Daniel Wheeler. Ela é eficiente em micro-pagamentos por utilizar apostas entre o comerciante e o consumidor. Se o consumidor vence, o serviço é de graça. Se o comerciante vence, o consumidor paga o valor estabelecido que pode ser muito maior que o valor do serviço.

Funciona por meio de números grandes e, no lugar de vários pequenos pagamentos somente alguns de valor mais substancial são efetuados. O consumidor pode pagar essas apostas perdidas com um sistema de pequenos ou macro pagamentos existente. (WHEELER, 1996)

Os passos propostos são:

- O comerciante e o consumidor fazem um acordo a respeito da soma da aposta, uma função de aposta  $f$  e um serviço que tem certo valor.
- O comerciante manda  $r = \text{hash}(R)$  para o consumidor.
- O consumidor manda um número randômico  $X$  para o comerciante.

- O comerciante envia  $R$
- O consumidor verifica que  $r = \text{hash}(R)$
- O comerciante e o consumidor calculam  $f(R, X)$  e determinam quem ganhou a aposta.

O protocolo não é especificado em detalhes.

### **5.51. VERIFONE**

Endereço Web: <http://www.verifone.com/products/commerce>

Status: Operacional, junho 1996.

Modelo de pagamento: Apresentação segura de cartão de crédito, diz suportar moeda eletrônica e micro-pagamentos.

Controle de privacidade: Confidencial, não-anônimo, rastreável.

Mecanismo de segurança: Criptografia de chave pública RSA, busca de uma solução de hardware.

Pré-requisitos: Software para consumidores e comerciantes, cartão de crédito.

Notas: Será compatível com SET.

VeriFone mantém um programa de apresentação segura de cartão de crédito e planeja integrar um smart card nesse esquema. Está ficando compatível com o SET também.



### **5.52. VIACHECK**

Endereço Web: <http://theyellowpages.com/Viacheck>

Nome: ViaCheck

Status: Operacional, setembro 1995.

Modelo de Pagamento: Apresentação segura de cartão de crédito.

Mecanismo de segurança: o software de criptografia vem do servidor do comerciante, todos os dados do consumidor serão criptografados.

Pré-requisitos: Cartão de Crédito.

ViaCheck mantém software para comerciantes que permitem apresentação segura de cartão de crédito via um Web browser e um servidor.

### **5.53. YAHOO PURSE**

Endereço Web: <http://www.yahoo.com>

Nome: Carteira Eletrônica Yahoo

Origem: Yahoo

Status: Operacional.

Tamanho de Pagamento: Macro-pagamentos.

Modelo de Moeda: Notacional.

Modelo de Pagamento: Apresentação Segura de Cartão de Crédito.

Validação: on-line.

Controle de Privacidade: Criptografado, não anônimo, rastreável.

Mecanismos de Segurança: Criptografia de chave pública, PIN.

Pré-requisitos: Nenhum.

Taxas: Taxas da administradora de cartão de crédito.

Latência/Custos: Baixo.

Base de Usuários: Não disponível.

Genealogia: Não disponível.

Não é necessária a instalação de nenhum software no lado do consumidor. Ele deve preencher um formulário, informando, além dos dados pessoais, o número de seu cartão de crédito. Essa será a única vez que o número do cartão será passado, a partir daí ele estará armazenado no servidor do Yahoo. Cada usuário tem um número de identificação. Quando for pagar uma compra em loja conveniada, deverá entrar apenas com o seu número de identificação e sua senha. Todas as lojas conveniadas estão no próprio site do Yahoo.

## 6. Sumário

Serão comparados os protocolos de pagamento apresentados anteriormente em função dos seus requisitos principais.

### 6.1. Perfis

Tabela 39 : Comparação dos protocolos baseados em token

Sistema	A N O N I M O	O N - L I N E	A T O M I C I D A D E	C O N S I S T Ê N C I A	I S O L A M E N T O	D U R A B I L I D A D E	E C O N O M I C A M E N T E	D I V I S I B I L I D A D E	E S C A L A B I L I D A D E	I N T E R O P E R A B I L I D A D E	C O N S E R V A Ç Ã O
Cash	S	N	S	S	S	S	S	S	S	S	N
CAFE	S	N	-	S	S	S	S	S	S	-	S
Ecash	S	S	N	N	N	N	S	S	-	-	S
Geld- karte	N	N	S	S	S	S	S	-	S	S	S
MilliCent	N	N	-	-	S	-	S	S	S	S	-
Mondex	N	N	S	S	S	S	S	S	S	-	S
Net- Cash	N	S	-	-	-	-	S	S	S	S	S

Essa tabela mostra uma comparação dos protocolos de pagamento baseados em token. Devido à transmissão de informações através de uma rede insegura, é difícil garantir atomicidade real em sistemas baseados em token. É relativamente possível assegurar que nunca o consumidor e o vendedor pensarão ter acesso legítimo a um mesmo token ao mesmo tempo, mas não é possível evitar que nem o vendedor nem o consumidor não se considerem donos de um

token, ou seja, sempre existe uma certa probabilidade de se perder valor monetário.

Tabela 40 : Comparação dos protocolos notacionais

Sistema	A N O N I M O	O N - L I N E	A T O M I C I D A D E	C O N S I S T Ê N C I A	I S O L A M E N T O	D U R A B I L I D A D E	E C O N O M I C A M E N T E	D I V I S I B I L I D A D E	E S C A L A B I L I D A D E	I N T E R O P E R A B I L I D A D E	C O N S E R V A Ç Ã O
Cheque	S	N	S	S	S	S	S	S	S	S	N
Credit	S	N	-	S	S	S	S	S	S	-	S
Cyber-Cash	S	S	N	N	N	N	S	S	-	-	S
FSTC	N	N	S	S	S	S	S	-	S	S	S
FV	N	N	-	-	S	-	S	S	S	S	-
Mini-Pay	N	N	S	S	S	S	S	S	S	-	S
NetBill	N	S	-	-	-	-	S	S	S	S	S
NetChe-que											
SET											

Essa tabela mostra uma comparação dos protocolos notacionais de pagamento. Sistemas notacionais são geralmente ligados a sistemas tradicionais de pagamento e tendem a herdar as suas propriedades.

## **6.2. Discussões**

No momento, existem várias diferenças entre os sistemas MPE's que concorrem entre si. Como existem diferenças e conflitos nos requisitos entre as diferentes formas de transações comerciais, provavelmente nenhum sistema irá dominar o mercado. Com micro-pagamentos, eficiência e velocidade são fatores dominantes e questões de segurança podem ser tratadas com uma prioridade menor, porque o ganho com uma fraude será muito pequeno. Com macro-pagamentos, a segurança é o fator mais importante e sistemas poderosos de criptografia são necessários para proteger tanto os detalhes da transação quanto as partes envolvidas.

### **6.2.1. Macro-pagamentos**

O campo de macro-pagamentos (a partir de US\$10,00) parece estar na dianteira. As questões aqui são claramente definidas e podem em grande parte ser derivadas dos sistemas tradicionais de pagamento existentes como cartões de crédito e cheques. As partes envolvidas estão interessadas principalmente em ser autenticadas para se proteger de fraude ou erros. A troca de informações deve ser segura e confidencial para evitar que terceiros tenham acesso a detalhes da transação. O pagamento de dinheiro deve ser assegurado por verificação on-line.

O protocolo SET da MasterCard e Visa é o que está mais próximo de ser dominante. Microsoft, Netscape, CyberCash, IBM e muitas outras empresas grandes estão suportando o protocolo e vêm desenvolvendo novos sistemas ou reformulando aqueles já existentes para que fiquem compatíveis com o SET. Sistemas utilizados

atualmente para apresentação segura de cartão de crédito com SSL e SHTTP irão recuar diante desses sistemas de pagamento compatíveis com o SET.

### **6.2.2. *Pagamentos pequenos.***

Um ponto de vista é que pequenos pagamentos (pelo menos US\$0,10) são melhores se forem tratados como dinheiro. Propriedades do dinheiro como anonimato do consumidor e a impossibilidade de rastreamento têm que ser garantidas e a falsificação deve ser evitada. Soluções com várias moedas também são necessárias para permitir uma aceitação mundial.

Sistemas baseados em cartões com chip, como Geldkarte são os mais dominantes nessa área por sua aprimorada segurança, escalabilidade e por ser offline. Outros exemplos de sistemas que suportam pequenos (mas não micro) pagamentos são o CAFE, Digicash Ecash, Mondex ou NetCash.

O outro ponto de vista para pequenos pagamentos é que eles têm que ser vistos como notacionais assim como os macro-pagamentos. Aqui, falsificação é bem difícil, mas anonimato não é facilmente assegurável. Um exemplo de sistema notacional para pequenos pagamentos é o CyberCoin.

Qual o sistema (ou sistemas) para pequenos pagamentos que será dominante depende não somente das necessidades dos usuários, como por exemplo, quão importante é o anonimato para ele, mas também do

contexto legal, isto é, qual atitude os governos tomarão diante dessas questões. Se a legislação considerar anonimato e não-rastreamento indesejáveis, esses sistemas de pagamento não conseguirão ganhar uma posição maior no mercado.

### **6.2.3. *Micro-pagamentos***

Com micro-pagamentos (até frações de centavos) a situação não está clara até o momento. Não podemos determinar no momento que sistema (ou sistemas) irá ter larga aceitação.

A maioria dos sistemas de micro-pagamentos suporta eficientemente apenas pagamentos repetidos com o mesmo comerciante. Sistemas baseados em token, que funcionam bem com compras repetidas, são sistemas localizados como o MilliCent, que está em teste público no momento, ou sistemas de divisões em cadeia como PayWord. Um sistema baseado em contas para repetidos pagamentos é o SubScrip. Esses sistemas dependem normalmente de algum sistema de macro-pagamentos ou outra operação cara para a transação inicial.

Um exemplo de um sistema notacional de micro-pagamentos, que pode suportar pagamentos ocasionais não relacionados de uma maneira prática é o Mini-Pay, que atualmente está entrando em uma fase de testes. Ainda não está claro se os riscos para os comerciantes e consumidores serão aceitáveis nesse sistema (HERZBERG, YOCHAI, 1997).

Vários esquemas altamente complexos são teoricamente impraticáveis, como por exemplo, LotteryTickets, uma proposta especializada para micro-pagamentos de alta frequência não repetidos. Por essa razão ele provavelmente não terá grande aceitação do público. Outro exemplo é o MicroMint, uma proposta especializada para micro-pagamentos ocasionais não repetidos, que necessita investimento enorme de esforços por parte dos potenciais emissores.



## 7. Orgãos Certificadores

### 7.1. VeriSign

Endereço Web: <http://www.verisign.com>

Nome: VeriSign.

Origem: VeriSign Inc.

Objetivo: Autoridade de certificação.

Status: Operacional

Pré-requisitos: Smart card.

VeriSign é um provedor de serviços de certificação digital. Ele utiliza smart cards que podem ser verificados on-line. Esta autenticação portátil habilita usuários a acessarem seus negócios e informações pessoais de uma maneira autenticada em qualquer lugar.

VeriSign coopera com a produtora de smart cards Schlumberger, com a produtora de leitores de smart card Litronic e com a Microsoft. Esses cartões podem ser usados com MS *Internet Explorer* e todos os comerciantes que aceitam os identificadores digitais da VeriSign.

## **7.2. GTE CyberTrust**

Endereço Web: <http://www.cybertrust.gte.com>

Nome: GTE Cybertrust.

Origem: GTE CyberTrust Solutions Inc.

Objetivo: Autoridade de certificação.

Status: Operacional

Pré-requisitos: Autoridade de certificação.

GTE CyberTrust Solutions Inc. alega ser a maior companhia de telefonia pública do mundo, suas vendas anuais passam de US\$21.000.000,00 (1998).

GTE fornece produtos e serviços de autorização de certificação para uso das instituições financeiras, empresas e agências do governo e para a segurança de um vasto número de aplicações baseadas em rede. GTE age como uma CA para o SET e para o SSL.

## 8. Projeto de Interfaces de Pagamento

### 8.1. BIPS

Endereço Web: <http://www.fstc.org/projects/bibs>

Nome: BIPS.

Origem: FSTC.

Objetivo: Infraestrutura de banco eletrônico.

Status: Projeto de pesquisa desde 1996.

Pré-requisitos: Hardware e software especiais.

O sistema bancário de pagamento pela *Internet* (BIPS) procura ajudar comerciantes e consumidores a processarem pagamentos eletrônicos na *Internet* através do desenvolvimento de vários componentes que são necessários para transações eletrônicas seguras.

- Uma arquitetura
- Uma especificação aberta
- Uma metodologia segura para instruções de pagamento espontâneo para ser iniciada através das redes públicas abertas.
- Uma interface padrão para os sistemas de pagamentos bancários.

BIPS é patrocinado por um consórcio de bancos líderes em tecnologia, e um centro para encorajar companhias a iniciarem uma variedade de transações de pagamento via *Internet* através de aprimorados sistemas de segurança.

Os participantes do projeto BIPS atualmente são: Citibank, Concept Five Technologies, Fujitsu, Glenview State Bank, GlobeSet, Mellon Bank, NCR, Tandem Computers, CommerceNet, The Retail Payments Office of the Federal Reserve System e SWIFT, entre outros.

O projeto BIPS procura demonstrar a possibilidade de uma infraestrutura segura largamente disponível, confiável e compreensível para criação, desenvolvimento e integração dos componentes necessários para proteger e ligar sistemas de pagamento existentes com os clientes corporativos dos bancos através de redes públicas abertas. Ele tem como objetivo produzir uma especificação de um servidor seguro que os bancos utilizarão para disponibilizar serviços de transações de pagamentos na *Internet*. As características são:

- Permitir que consumidores e vendedores cheguem a um acordo com relação aos termos e mecanismos de pagamento.
- Estar habilitado a acessar múltiplos sistemas bancários de pagamento, permitindo a consumidores e bancos escolherem o meio de melhor relação custo-benefício para realizar um pagamento.
- Disponibilizar um meio de selecionar com inteligência o mecanismo apropriado de pagamento para o consumidor baseado nas suas necessidades e custos
- Disponibilizar autenticação on-line de consumidores e vendedores e autorizações para as transações.

## **8.2. InterPay/UPAI**

EndereçoWeb:

<http://robotics.stanford.edu/users/ketchpel/dags4.html>

Nome: Interpay/UPAI.

Origem: H. Garcia-Moulina, S. Ketchpel, et al., projeto de bibliotecas digitais de Stanford.

Objetivo: Protocolo para integração de sistemas de pagamento.

Status: Projeto de pesquisa desde 1995, diz ter implementado um protótipo.

Pré-requisitos: Software especial.

InterPay e UPAI unificam o acesso a sistemas de pagamento. Arquitetura de camadas. Projeto das Bibliotecas digitais da Stanford (COUSINS, KETCHPEL, PAEPKE, GARCIA-MOULINA, et al, 1995b; KETCHPEL, GARCIA-MOLINA, PAEPCKE, HASSAN, COUSINS, 1996; COUSINS et al, 1995a; KETCHPEL, 1996).

### **8.3. IPAY**

Endereço Web: <http://www.imc.org/ietf-pay/ietf-pay-charter>

Nome: IPAY.

Origem: IMC

Objetivo: Protocolo de negociação de pagamento automático entre computadores e estruturas de comerciantes.

Status: Projeto de pesquisa desde abril de 1997.

Pré-requisitos: Software especial.

Rascunho do Grupo de Trabalho sobre Pagamento da IETF. O grupo teve três linhas mestras:

- Negociação do esquema de pagamento e protocolo
- Transporte das mensagens de pagamento
- Métodos para os comerciantes oferecerem os produtos e preços.

Proposto em Abril/1997, mas sem resultados divulgado.

#### **8.4. JECF**

Endereço Web: <http://java.sun.com/products/commerce>

Nome: JECF.

Origem: Sun, Javasoft.

Objetivo: protocolo para integração de sistemas de pagamentos.

Status: Projeto de desenvolvimento desde 1996.

Pré-requisitos: Software especial.

Acesso unificador da Sun JavaSoft para sistemas de pagamentos

## **8.5. JEPI**

Endereço Web: <http://www.w3.org/pub/WWW/Payments/JEPI.html>

Nome: JEPI.

Origem: W3 Consortium, CommerceNet, CyberCash, Microsoft, NetBill, OSF, OpenMarket et al.

Objetivo: Protocolo para negociação de pagamentos automatizados entre computadores, determinando o mecanismo de pagamento mais apropriado para a transação em andamento.

Status: Projeto de pesquisa desde dezembro de 1995.

Pré-requisitos: Smart card e software, provavelmente.

A Iniciativa Conjunta de Pagamentos Eletrônicos (JEPI) foi feita para permitir a negociação automatizada do meio de pagamento entre computadores.

Ela é um projeto do Consórcio W3C. Procura resolver as seguintes questões:

- Um protocolo de negociação de propósito geral baseado no PEP (Protocolo de Extensão de Protocolos). Ele permite que um cliente Web e um servidor questionem-se sobre quais módulos de extensão cada um aceita, negociem parâmetros para essas extensões e perguntem para o outro se é possível utilizar essa extensão. Este trabalho está sendo armazenado dentro das especificações do HTTP 1.2 durante os processos da IETF.
- Um módulo de extensão específica, UPP (Preâmbulo Universal de Pagamento), utilizado para negociar sobre o instrumento de pagamento (cheque, cartão de crédito, cartão de débito, dinheiro eletrônico, etc), marca (Visa, MasterCard, American Express, etc) e protocolo de pagamento (SET, CyberCash, GlobeID, etc).



São participantes:

- Fornecedores de browsers: Microsoft
- Fornecedores de Servidores: IBM e Mercado aberto.
- Sistemas de pagamento: CyberCash e GCTech.
- Comerciantes: Xerox e British Telecom
- Design de entrada adicional: Digital Equipment Corporation e
- VeriFone.

O JEPI será projetado para agir como um sistema geral no qual mecanismos de pagamentos podem ser embutidos e irá conter propriedades mínimas de pagamento dele próprio. Além disso, as propriedades do protocolo JEPI podem ser restritas para o uso de certos mecanismos de pagamento, por exemplo, para respeitar anonimato. Vários rascunhos estão sendo publicados na *Internet* detalhando esses protocolos. (EASTLAKE, 1997; EASTLAKE, KHARE, MILLER, 1997; KHARE, 1997).

### **8.6. SEMPER/iKP**

Endereço Web: <http://www.semper.org>

Nome: Semper/iKP.

Origem: Waidner, M. et al. da IBM de Zurique.

Objetivo: Protocolo para negociação de pagamentos automatizados e integração de sistemas de pagamento. Sistema de pagamento genérico.

Status: Projeto de pesquisa desde 1996.

Pré-requisitos: Software especial.

O projeto da IBM Suíça de um serviço de acesso unificado e seleção de sistema de pagamento.

## **V. Teorias de Adoção de Inovações**

### **1. Introdução**

Uma reportagem de capa da Business Week (Abril 29, 1991) descreve como consumidores ficam frustrados com produtos inovadores que consideram difícil de operar. O artigo destaca que mesmo Keven Olsen, fundador da DEC confessou que não tinha a mínima ideia como esquentar um copo de café no forminho de microondas da empresa. Como entender essas barreiras ? Porque algumas pessoas não se aproximam de objetos inovadores ? Quais as melhores estratégias e ações para comercializar massivamente produtos e serviços inovadores ?

Diferentes pessoas quando na direção das empresas, imprimem diferentes rumos à essas empresas, de acordo com seu perfil mais conservador ou mais inovador. Um modelo de excelência que permite uma avaliação das empresas de acordo com seu perfil inovador será tratado abaixo.

### **2. Teorias de perfil de empresas**

Vários autores tem destacado evidências de princípios que estariam relacionados com perfil mais conservador ou inovador das empresas e como se relacionam com as diversas situações. ARGYRIS (1992 e 1993) e SENGE (1990) destacam o princípio de aprendizado contínuo. ACKOFF (1981, 1986, 1994) gerou as bases de processos de pensamento. A importância da criação de valor e suas mensurações foram articuladas por COLLINS e PORRAS (1994) na empresa de consultoria Stern Stewart & Company, que popularizou o conceito de *economic value added* (EVA). JURAN (1992) e DEMING (1993) criaram um movimento ao redor da ideia de qualidade do processo.

Métodos para encarar incertezas de maneira racional foram desenvolvidas por Pierre-Simon Laplace e Daniel Bernoulli, e tem sido descritos em textos de análise de decisão e psicologia cognitiva (HOWARD & MATHESON, 1983 ; RUSSO & SCHOEMAKER, 1989).

MATHESON & MATHESON (1998) relacionaram a partir de pesquisas nove critérios que avaliados em conjunto permitem identificar se a empresa tem um perfil mais conservador ou mais inovador. Uma empresa de perfil inovador tem as seguintes características de forma mais marcante:

*Cultura para criação de valor* – a organização tem um objetivo. Todos na organização entendem esse objetivo e usam esse entendimento como balizador para testar se suas estratégias e ações estão criando valor para a organização e seus clientes. Criação de valor é um argumento decisivo para mudanças, rompendo barreiras criadas por tradições, limites funcionais, ambições pessoais e até limitações orçamentárias.

*Criação de alternativas* – uma decisão razoável só pode ser tomada como escolha entre uma série de alternativas razoáveis. O processo requer a criação de alternativas e não tomarão ação estratégica antes que várias alternativas sejam criadas e avaliadas.

*Aprendizado contínuo* – a organização deve saber criar mais valor frente a mudanças. Os membros da organização respondem à informações potencialmente ameaçadoras de maneira não defensiva. A empresa identifica oportunidades e mudanças de paradigmas e encontra maneiras novas e melhores de criar valor.

*Enfrentando incertezas* – não existem fatos sobre o futuro, só incertezas. Membros de uma organização inovadora entendem como trabalhar com incertezas. Eles avaliam o desconhecido e gerenciam os riscos associados. Não negam a incerteza, mas

reconhecem quando realizam decisões. Incertezas são entendidas, comunicadas e gerenciadas.

*Perspectiva estratégica, de fora para dentro* – a empresa inicia o processo estratégico com uma visão ampla, para onde o mundo está indo, como seus clientes e setor estão mudando, e depois trabalha internamente sobre quais são as implicações para si.

*Pensamento sistêmico* – o desenvolvimento de nova tecnologia, produto ou processo cria um desafio no mundo dos clientes e concorrência, estimulando uma reação competitiva, produtos de nova geração etc. A empresa inovadora utiliza processos sistêmicos de pensamento para avaliar as implicações de longo prazo de suas decisões.

*Sistemas abertos de decisão* – a organização inovadora cria um sistema aberto e irrestrito de informações entre todos os seus membros. O hábito de reter informações como fonte de poder é abolido.

*Empowerment* – a empresa inovadora utiliza participação no processo de decisão. O entendimento das estratégias para criação de valor coordena a organização.

*Processo de tomada de decisão disciplinada* – a empresa inovadora cria processos para reconhecer a necessidade de decisões estratégicas. Para o processo de decisão aplica um processo disciplinado e sistemático que define os passos para alcançar conclusões.

Esse processo bastante completo para identificar o perfil das empresas, foi o adotado, para caracterizar o comportamento das organizações.

### **3. Teorias de adoção de inovações**

Teorias de adoção de inovação buscam um entendimento do processo pelo qual produtos com características novas são incorporados pelo mercado.

ROGERS (1995) descreve e analisa como as inovações são adotadas pelas pessoas. A teoria de ROGERS (1995), editada pela primeira vez em 1962, depois em 1971 com Shoemaker, em 1993, e 1995, de difusão de inovações evoluiu nos últimos quase 40 anos, com uma série de idéias, que tem uma considerável influência em autores de marketing (MAHAJALAN & MULLER, 1979; e KOTLER, 1994) e em estudos relativos à adoção de tecnologia de informação (IT) (FICHMAN, 1992; e LEVINE, 1994).

Uma outra teoria, que apresenta uma maneira diferente de olhar as inovações tecnológicas é o conceito de translação (MCMASTER, VIDGEN e WASTELL, 1998). Essa teoria avalia o mecanismo envolvido na transição tecnológica, a transferência de tecnologia na sua terminologia (LAW, 1986, CALLON, 1986, LATOUR, 1987, 1993).

Serão aqui apresentados as duas teoria para explicar o processo de adoção de inovações.

### **3.1. Teorias Gerais de Difusão**

O estudo de difusão de inovações é recente. Ryan e Gross citados por ROGERS (1995) elaboraram um estudo em 1943 no campo da sociologia rural que foi a genesis da pesquisa moderna de difusão de inovações. A sociologia rural é um aspecto da sociologia focada nos problemas sociais da vida rural. Esse estudo influenciou a metodologia, a base teórica e as interpretações de estudos posteriores de difusão de inovação. Analisaram a difusão da semente de milho híbrido entre os fazendeiros de Iowa, EUA. A semente de milho híbrido começou a ser disponibilizada na região em 1928. A nova semente aumentou as colheitas, era mais tolerante às secas, e se adequava melhor à colheita mecanizada. Por volta de 1941, aproximadamente treze anos após a introdução na região, a inovação já era adotada por quase cem por cento dos fazendeiros de Iowa. Estudaram a rápida difusão do milho híbrido para levantar o que poderiam aplicar à difusão de outras inovações rurais. Usaram entrevistas com adotantes de inovações, para examinar fatores relacionados à adoção. A metodologia de pesquisa baseada em entrevistas tem sido o método predominante de estudo desde então.

Uma série de outros pesquisadores na área de sociologia rural, como FLIEGEL e KIVLIN, (1962) e em outros campos (WEINSTEIN, 1986) desenvolveram pesquisas e apresentaram teorias relacionadas ao trabalho pioneiro de RYAN e GROSS (1943).

O pesquisador que fez o trabalho mais significativo para sintetizar as descobertas e teorias associadas ao processo de difusão foi Rogers. O trabalho publicado originalmente em 1960 e agora na quarta edição (ROGERS, 1995) se aproxima de uma teoria unificada de difusão de inovações, abordando quatro teorias a saber, decisão do

processo de inovação, características de inovação individual, taxa de adoção e atributos percebidos.

### **3.1.1. *Decisão do processo de inovação***

A teoria do processo de decisão de inovação (ROGERS, 1995) afirma que difusão é um processo que ocorre ao longo do tempo e possui cinco estágios diferentes. Os estágios no processo são conhecimento, persuasão, decisão, implementação e confirmação. De acordo com a teoria, os potenciais adotantes de uma inovação devem conhecer a inovação, serem persuadidos sobre os méritos da inovação, decidir adotar, implementar a inovação e confirmar (reafirmar ou rejeitar) a decisão para adotar a inovação.

Essa teoria tem sido tão citada que autores como SACHS (1993) afirmam que

...após rever as pesquisas na área, temos a impressão de que a única coisa importante que precisamos saber sobre como provocar a adoção de inovações ou de como ser um melhor agente de transformação, é de que existem cinco estágios para o processo de adoção de inovações. SACHS (1993)

conclui que muitos outros critérios importantes no processo de difusão de inovações tem sido relegados incompreensivelmente à um segundo plano.



### **3.1.2. Características de inovação individual**

A teoria de ROGERS (1995), que segmenta os indivíduos de acordo com as características individuais de predisposição à adotar inovações. Indivíduos com perfil inovador irão adotar inovações antes de indivíduos com perfil mais conservador. Rogers segmentou os indivíduos em cinco categorias: pioneiros, primeiros adotantes, primeira maioria, segunda maioria e retardatários. Esses conceitos como definidos por Rogers (1995) são:

*Pioneiros* – são os primeiros 2,5% de indivíduos no sistema que adotam uma inovação. A propensão à aventuras é quase uma obsessão com os pioneiros. Esse interesse em novas idéias leva-os a relacionamentos sociais mais cosmopolitas. Padrões de comunicação e amizades entre alguns pioneiros são comuns, mesmo que as distâncias geograficas sejam grandes. Ser um inovador tem alguns pré-requisitos, acesso à recursos financeiros ajuda a absorver a possibilidade de perdas de alguma inovação não proveitosa; a capacidade de entender e aplicar conhecimentos técnicos complexos é necessária; e, deve ser capaz de lidar com o alto grau de incerteza de uma inovação quando for adotar.

*Primeiros adotantes* – São os 13,5% seguintes de indivíduos no sistema a adotar um inovação. Os primeiros adotantes são uma parcela mais integrada ao sistema local que os pioneiros. Enquanto os pioneiros são cosmopolitas, primeiros adotantes tendem a ser mais regionais, mas mantem o perfil inovador.

*Primeira maioria* – Os 34 % seguintes de indivíduos em um sistema a adotar uma inovação. A primeira maioria adota novas idéias antes que a média do sistema. Essa primeira maioria se referencia constantemente. Representam uma parcela bastante numerosa da população. Geralmente demoram algum tempo antes de adotar a nova idéia.

*Segunda maioria* – Os 34 % seguintes de indivíduos num sistema a adotar uma inovação. A segunda maioria adota novas ideias após a primeira maioria. Como a primeira maioria, representam um terço do total de membros do sistema.

*Retardatários* – Representam os últimos 16% de membros de um sistema a adotar uma inovação. O referencial que possuem é o passado. Decisões são tomadas em função do que foi feito no passado.

Em uma ponta estão os pioneiros com perfil inovador, que aceitam tomar riscos e que adotam inovações mais cedo no processo de difusão, e na outra extremidade estão os retardatários que resistem à adoção de inovações, com perfil mais conservador.

Curva tendendo à normal, proposta por Rogers, conforme características de inovação individual

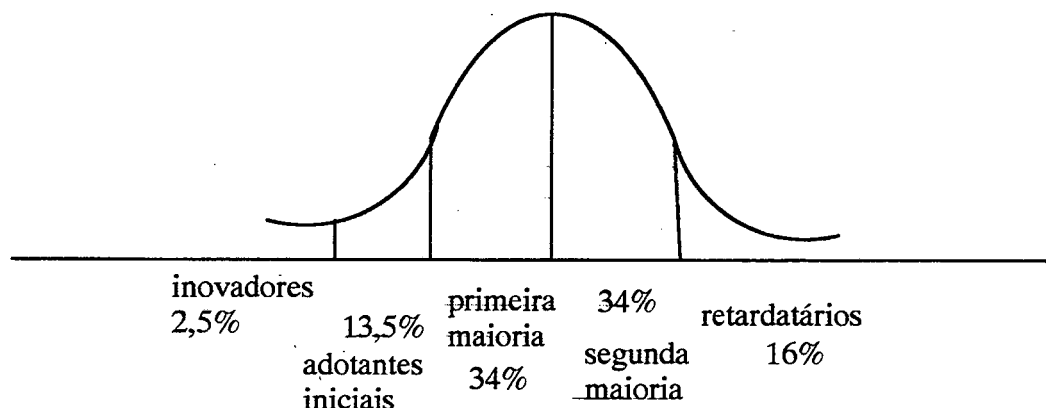


Figura 12 – curva tendendo à normal, conforme inovação individual

Para efeito deste trabalho, serão tratadas as duas primeiras categorias definidas por ROGERS (1995) (pioneiros e adotantes iniciais ou primeiros adotantes), como inovadores, sendo as terminologias usadas indistintamente a não ser quando destacado em contrário. O restante do mercado de perfil mais conservador, principalmente as duas categorias seguintes, a primeira maioria e a segunda maioria, poderá também ser tratada como mercado principal.

As aplicações dessa teoria também tem sido muito intensas. HOIBERG (1997), MARDSEN (1998), HAHN e SHOCH (1998), LEWIS (1997), KAUTZ e MCMASTER (1994), ARDIS e FURCHTGOTT (1994), para citar alguns estudos que caracterizaram o mercado em função dos comportamentos em relação à inovação.

Um autor, que tem feito bastante sucesso e recebido bastante divulgação a partir de aplicações das teorias de ROGERS,

principalmente em relação às características de inovações individuais, traduzidas sem grande critério para o ambiente de empresas é MOORE (1991, 1995)

### 3.1.3. Taxa de Adoção

A terceira teoria de difusão discutida por ROGERS (1995) é a teoria de taxa de adoção. Explica que as inovações são difundidas ao longo do tempo em um padrão que lembra uma curva-s. A taxa de adoção de inovação passa por um período de crescimento lento e gradual antes de um crescimento rápido e dramático. Após um período de rápido crescimento, a taxa de crescimento das inovações irá gradualmente estabilizar e eventualmente declinar.

Diversos autores tem explorado essa teoria, entre eles podem ser citados, BROWN (1992), ROGERS e SCOTT, (1997), DEKIMPE, PARKER, SARVARY (1996), estudando o comportamento de crescimento das taxas de inovações.

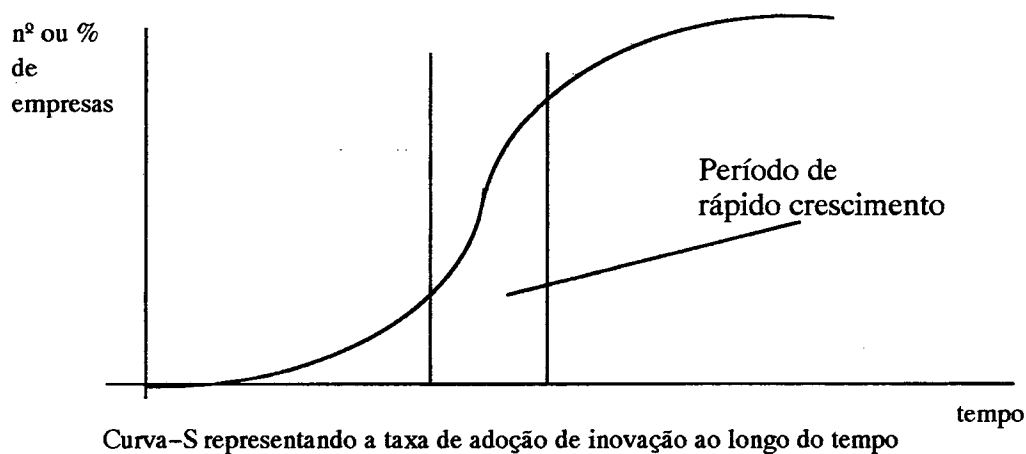


Figura 13 – Curva-S, representando taxa de inovação

### **3.1.4. Atributos percebidos**

A teoria dos atributos percebidos (ROGERS, 1995), afirma que os adotantes potenciais julgam uma inovação baseados nas percepções em relação à cinco atributos da inovação. Esses atributos são: possibilidade de testar, possibilidade de observar, vantagem relativa, complexidade e compatibilidade.

Possibilidade de testar – é o grau em que uma inovação pode ser experimentada em base restrita. Novas idéias que podem ser testadas de maneira limitada serão geralmente adotadas mais rapidamente do que inovações que não possuem esta propriedade. Uma inovação que pode ser testada, segundo ROGERS (1995), representaria menos incerteza para o indivíduo que está considerando a adoção.

Possibilidade de observar – é o grau de resultado de uma inovação que pode ser visível à outros. Quanto mais fácil for para outros indivíduos verem os resultados de uma inovação, mais facilmente as adotarão. Essa visibilidade estimula a discussão de uma ideia nova entre pares, a medida que amigos e vizinhos de um adotante requisitam informações sobre a inovação/avaliação. (ROGERS e SCOTT, 1997).

Vantagem relativa – é o grau em que uma inovação é percebida como melhor que a que pretende substituir. O grau de “vantagem relativa” pode ser medido em termos econômicos, mas prestígio social, conveniência e satisfação também são fatores importantes. O fato do indivíduo

perceber a vantagem relativa de uma inovação torna seu processo de adoção mais rápido. ROGERS e SCOTT (1997).

Complexidade – é o grau em que uma inovação é percebida como difícil de ser entendida e utilizada. Algumas inovações são rapidamente entendidas pela maioria dos membros de um sistema social; outras são mais complicadas e serão adotadas mais lentamente. Novas idéias que são facilmente compreendidas seriam mais rapidamente adotadas que inovações que exigem o desenvolvimento de novas habilidades e entendimentos por parte do usuário (ROGERS 1995);

Compatibilidade – é o grau pelo qual uma inovação é percebida como sendo consistente com os valores existentes, experiências passadas e necessidades de adotantes em potencial. Uma idéia que é incompatível com os valores e normas vigentes num sistema social não será adotado tão rapidamente como uma inovação que é compatível. A adoção de uma inovação incompatível geralmente requer a adoção anterior de um novo sistema de valor. (ROGERS e SCOTT, 1997)

Resumindo, a teoria afirma que uma inovação terá um aumento na taxa de difusão se adotantes potenciais perceberem: que a inovação pode ser testada de maneira limitada antes da adoção; permitir resultados observáveis; tiver uma vantagem relativa em relação à outras inovações (ou ao *status quo*); não for muito complexa; e , for compatível com com práticas e valores existentes.

A teoria de atributos percebidos tem sido usada como base teórica para vários estudos de adoção de produtos de base tecnológica. Percepções de compatibilidade, complexidade, vantagem relativa tem sido associadas como pontos significativos no processo de adoção, por WYNER (1974) e HOLLOWAY (1977) , que associaram percepções de vantagem relativa e compatibilidade são significativas no processo de adoção para o mercado que estudaram. EADS (1984) encontrou que compatibilidade era muito importante no segmento que estudou, e SURRY (1993) associou vantagem relativa, complexidade e compatibilidade como considerações muito importante para o mercado que estudou.

### **3.2. Definições associadas à teoria de difusões de inovações**

#### **3.2.1. Difusão**

Difusão, segundo KEGERREIS (1970), é o processo pelo qual comunicações com significado são trocadas entre membros da sociedade. Essa definição está em conformidade com os conceitos usados na física, na antropologia e na sociologia.

#### **3.2.2. Inovação**

Existem diferentes definições para inovações. Teorias de marketing tem sido definidas ao redor dessa definição. CONVERSE (1965), apresenta uma visão bastante restritiva, limitando o termo a desenvolvimentos de produtos de base tecnológica. ALDERSON (1965), foi mais flexível enfatizando as possíveis variações na magnitude relativa das bases tecnológicas dos produtos inovadores. WASSON (1960), e ROGERS (1995) definiram inovação como: qualquer coisa percebida como nova por um usuário potencial. A ênfase de percepção nessa definição permite que qualquer coisa possa ser inovação para algum indivíduo e não para outro. KNIGHT (1984) também evitou o problema de diferenciação entre pequenos e grandes melhoramentos, definindo uma inovação como a adoção de uma mudança que é nova para uma organização e para o ambiente relevante. BECKER e WHISLER (1967) dizem que inovação implica em liderança por parte do adotante, que é mais significativa que uma mera mudança. LAZER e BELL (1966) definem inovação como qualquer produto que tenha atingido menos de x por cento da penetração do mercado independente do tempo.



O antropólogo BARNETT (1983), definiu inovação como qualquer pensamento, comportamento ou coisa que é nova porque é qualitativamente diferente das formas existentes. Essa definição fica um pouco vaga, difícil de quantificar pois, o que seria qualitativamente diferente como critério? Operacionalmente, FRANK, MASSY, MORRISON (1970) , desenvolveram definições de inovação como qualquer produto que tenha aparecido no mercado recentemente. Essa definição aparece em diversos estudos citados por KELLY (1983).

Como definição de inovação, adotaremos a formulada por KEGERREIS, ENGEL e BLACKWELL (1976) de que uma inovação é qualquer coisa percebida como nova pelo potencial usuário, e sua adoção tenderá a alterar significativamente os seus padrões atuais de comportamento.

#### **4. Actor–Network Theory**

Uma abordagem para avaliar o desenvolvimento social e tecnológico simultaneamente, foi desenvolvida como Teoria Ator–Rede, Actor–Network Theory, ANT. Essa abordagem é um desdobramento da Construção Social de Tecnologia um movimento recente na sociologia, associado principalmente a dois autores, Latour e Callon. A teoria descreve a sociedade em humanos e não-humanos como atores equivalentes amarrados em redes e mantidos em ordem para atingir um objetivo em particular.

##### **4.1. Conceitos centrais**

LATOUR (1993) afirma que a *Actor–Network Theory* pretende resolver o que ele chama de grande equivoco do modernismo e pós-modernismo, o fatiamento de uma realidade híbrida em domínios analíticos. Nesse sentido de sistema, pretende integrar os domínios de natureza, sociedade e linguística., o que serviria para destacar como humanos e não-humanos podem ser atores que estão integrados em redes, as vezes seladas em caixa preta. Essas redes podem ser interpretadas através da inscrição nos intermediários que circulam por essas redes. O resultado dessas redes podem variar, podem ser fatos científicos (LATOUR, WOLGAR, 1986 ; LATOUR, 1986), tecnológico (BIJKER, 1994; LAW, CALLON, 1992; LATOUR, 1991), e pode ser relativo à sociedade (WOOLGAR, LATOUR, 1990). O significado e produtos dessas redes, nunca são de uma única natureza, são sempre híbridas, abrangendo os três domínios. O sistema como “unidades que se autoreferenciam” (STALDER, 1999), seguem os modelos autopoieticos descritos por MATURANA e VARELA (1987 e 1980) e MINGERS (1995).

Ator são as entidades que fazem coisas (LATOUR, 1993),  
extendendo a definição para qualquer um ou qualquer coisa que é  
representado atuando. (LATOUR, 1996)

Caixa Preta, contém o que já não precisa ser considerado, todas as  
coisas que podem ser tratados com indiferença.

Rede, depois de ator, é o segundo conceito em importancia. É  
definido como um grupo de relações não especificadas entre  
entidades que tem natureza indeterminada. Uma rede amarra dois  
sistemas de aliança. Pessoas – todos que estão envolvidos na  
invenção, construção, distribuição e utilização de um produto (a  
descrição desse sistema leva a um sociograma, como apresentado  
por WASSERMAN, FAUST, 1994; WELLMAN, 1983). Coisas – todos  
os pedaços que já estavam em cena ou tiveram que ser trazidos para  
conectar as pessoas (a descrição desse sistema leva a um  
tecnograma).

Interrelações entre tecnograma e sociograma são evidentes, por  
exemplo, quando um produto não é aceito pelos usuários ao qual foi  
planejado. Uma maneira de reagir à esse desencontro pode ser  
alterar o produto, trazer uma rede tecnológica diferente em cena para  
obter a aceitação pelos usuários, ou mudar o sociograma. Para  
compreender a dinâmica em um nível da rede é necessário examinar  
a dinâmica da outra parte.

Ator e rede são constitutivos. Um ator não pode atuar sem uma rede  
e uma rede é constituída por atores. (CALLON, LATOUR, 1981)  
Atores e rede constantemente redefinem-se, um é dependente do  
outro (CALLON, 1987).

Intermediarios, fornecem a ligação faltante entre os conceitos centrais que precisam ser definidos. Conectam atores e redes e definem as próprias redes. São a linguagem da rede.

## **4.2. Utilização da Teoria**

Vários conceitos foram desenvolvidos para entender as restrições e forças que entram em consideração através de uma inovação tecnológica, um novo procedimento ou descoberta científica. A atividade do analista é chamada de descrição “que é a análise do que vários atores em uma cena estão fazendo para cada um” (AKRICH, LATOUR, 1992).

### **4.2.1. Dinâmica da rede**

Para estudar a dinâmica da rede são identificadas três fases:

#### ***a. Emergência***

Redes são postas em funcionamento por atores. Como não existem atores sem rede, novas redes devem emergir de outras redes já em funcionamento. As vezes ocorre através de mudanças mínimas, às vezes através de desenvolvimento revolucionário que pode diminuir o elemento de continuidade que é parte de toda dinâmica.

#### ***b. Desenvolvimento***

Uma rede pode desenvolver-se em duas direções diferentes, para convergência ou divergência de seus atores. Acrescentando novos atores à uma rede, a princípio aumenta sua divergência. O processo de tradução pelo qual a vontade de um ator é transferida para outro ator é inicialmente mais difícil pois os atores existentes podem estar alinhados com outros objetivos.

### *c. Estabilização*

As redes não conseguem estabilizar-se e depois desaparecer de cena, aqueles que conseguiram atingir alguma convergência proliferam e transformam-se em ponto de partida para novas redes. Um ator-rede busca a estabilização, porque sem ela nenhuma das entidades que a constituem podem existir sem a estabilização.

### **4.3. Análises da adoção de inovações realizadas à luz da Teoria Ator-Rede**

Alguns estudos foram realizados para avaliar o processo de adoção de inovações, utilizando a teoria Ator-Rede. GUESNERIE (1996) , inovou na abordagem de mercado como rede, os agentes possuem seus próprios interesses e realizam cálculos econômicos que podem ser vistos como operação para otimização ou maximização. Os agentes geralmente tem divergências de interesse, o que os permite realizar transações que solucionam o conflito através do preço. Consequentemente o mercado opõe compradores e vendedores, e o preço resolve o conflito. (GUESNERIE, 1996).

Montando os tecnogramas e sociogramas, conforme prevê a teoria, levantando as diversas interações entre os agentes, MCMASTER, VIDGEN, WASTELL, (1998) concluem que

emergência de uma nova tecnologia é resultado da emergência simultânea de novas redes de relacionamentos sociais, materiais e processos, que produz, sustenta e integra novos artefatos. Para criar uma tecnologia estável devem existir um compartilhamento de linguagem e material, e de elementos humanos e manufaturados. (MCMASTER, VIDGEN, WASTELL, 1998)

Nessa linha, STALDER (1999), estudou o processo de difusão do sistema Mondex, em suas diversas experiências pelo mundo. Analisou como

as interações complexas de elementos heterogeneos foram criadas, dentro da ótica *actor-network*. Esse estudo exploratório analisou os padrões da rede Mondex enquanto emergiam na interseção da dinâmica técnica, institucional e social. Esses padrões foram analisados em relação à segurança do sistema e da privacidade de seus usuários. Apesar da rede Mondex ainda não estar estabilizada, conseguiu um 'momento institucional', com a mobilização de grandes instituições financeiras que estão levando em frente o processo de montagem da rede. Contudo o esforço das instituições financeiras em montar essa rede é contestada por uma série de atores independentes, como tecnologias alternativas, *hackers* tentando violar os chips, e usuários reticentes para usar a tecnologia que foi oferecida a eles. Esses atores heterogêneos estão todos envolvidos na criação do mundo técnico-social da Mondex"

#### **4.4. Implicações da Teoria de Ator-Rede**

A teoria de Ator-Rede (ANT), foi desenvolvida através da combinação de uma série de idéias radicalmente diferente do modelo de ROGERS (1995). É relacionada com a geração de fatos (*black-boxes*).

Os fatos (máquinas, inovações), não esperam para ser descobertos ou inventados, ao invés disso, são criados através do tempo e espaço de cadeias de associações fracas para fortes de alianças entre humanos e não humanos. Isso ocorre em virtude de convergência relativa de seus respectivos interesses. Essa criação e fortalecimento de laços entre atores heterogeneos (LAW, 1986), num primeiro momento "uma montagem de aliados desordenados e não confiáveis", lentamente evolui para algo que "relembra uma

caixa preta” (LATOUR 1987). Cada novo aliado fortalece a cadeia, fazendo a caixa mais preta, o fato mais consistente, a medida que a rede aumenta através do tempo e espaço. Cada ator traduz e contribui com seus próprios recursos para o formato final da caixa preta emergente.

LATOUR (1986) destaca uma série de estratégias para envolver outros na criação da caixa preta: “apelar para o interesse explícito do outro, fazer com que os outros sigam nossos interesses, sugerir um atalho (especialmente quando a estrada estiver bloqueada), alterar os interesses e objetivos por táticas como inventar novas metas, inventando novos grupos, ou, se tornando indispensável para os outros. Para criar uma caixa preta outros tem que ser envolvidos para que o fato embrionário seja aprovado através do tempo e espaço; uma vez envolvidas, as necessidades dos outros tem que ser mantidos em consonância para que o fato traduzido permaneça reconhecidamente o mesmo, fortalecendo a caixa preta a medida que a rede se propaga. A teoria destaca que o controle de qualquer ator individual sobre esse processo é necessariamente limitado; a tradução inevitavelmente abrange metamorfose e perda de soberania, apesar do esforço de manter controle”.

#### ***4.4.1. Considerações do Estudo da Mondex***

A construção do ator-network da Mondex, é direcionada por um forte momento institucional (HUGHES 1994); um grande número de instituições financeiras multinacionais desenvolveram vários interesses que são dependentes da continuação do projeto Mondex. A rede criada, com a integração e compartilhamento de controle centralizado em poucas instituições, uma abordagem de cima para baixo para desenvolver serviços, guardar segredos e uma distribuição



desigual de confiança. Contudo nem mesmo esse forte momento institucional foi forte o suficiente para determinar o resultado do processo de criação da rede. Ainda há uma gama de outros atores que precisam ser incluídos ou excluídos.

Depois de 10 anos de desenvolvimento, a primeira fase do projeto Mondex chegou ao fim. Três testes públicos extensivos foram desenvolvidos, e foi impossível desenvolver um sociograma para suportar o tecnograma de uma única forma de MPE. Todas as tentativas para traduzir consumidores e comerciantes em membros do mundo Mondex falharam. (STALDER, 1999)

## **5. Avaliação das Teorias**

A teoria de difusão, caracterizam os mercados de indivíduos, conforme o perfil mais inovador ou mais conservador, e com isso buscam explicar o comportamento da difusão das inovações ao longo do tempo (ALLEN, 1997). As classificações criadas pelas teoria de difusão são classificatórias (BESSELMAN, 1994) mas conforme destacado por BIHARI e VARNER (1994) oferece nomenclaturas para bem identificar cada segmento e perfil.

Avaliando estudos de difusão de inovações elaborados à ótica da teoria ANT, como STALDER (1999) e MCMASTER, VIDGEN e WASTELL (1998), percebemos a busca de correlações entre o comportamento dos diversos atores, para explicar o quão forte ou fraco a rede é. Todas as sugestões de aplicação, como as de LATOUR e STALDER conforme citado, partem das correlações de comportamentos, conforme MCMASTER, VIDGEN e WASTELL (1998) de outras redes. O objetivo dessas correlações é de explicar acontecimentos e buscar padrões para repetições de ações, sem levar em consideração causa-efeito, apesar da abordagem sistêmica.

## **VI. Objetivo**

Será objetivo do presente trabalho propor uma metodologia para provocar a adoção de um meio de pagamento eletrônico, pelo o mercado principal.

O tema é de grande atualidade, pois o comércio eletrônico que vem crescendo explosivamente ainda está utilizando os meios tradicionais de pagamento, com todas as desvantagens inerentes. No momento em que o grande público adotar meios de pagamento eletrônico, haverá uma facilidade maior para todas as partes envolvidas.

## **VII. Justificativa do Tema**

A popularização de sistemas de meios de pagamento eletrônico (MPE) é vantajosa para sistemas de Comércio Eletrônico. Permitirá transações mais rápidas e seguras, o que tenderá a atrair mais consumidores e mais comerciantes. A rapidez e segurança na transação permitirá que os custos associados às transações baixem. Essa queda de custo do sistema atrairá mais atores, ampliando o mercado.

O sistema MPE não será popularizado ou grandemente adotado até que seja difundido pelo mercado principal, a grande maioria do mercado. Esse processo de disseminação trará vantagens para o público dos comerciantes, dos consumidores e dos agentes financeiros envolvidos na transação.

A avaliação do processo de disseminação, com a proposta de uma metodologia sistêmica para trabalhar o mercado principal ajudará a compreender melhor o processo de adoção de produtos inovadores por essa parcela significativa do mercado. Pretende-se com esta tese contribuir para melhor compreensão dos critérios de adoção por parte do mercado principal que compreende 68% da população a ser abordada.

## **VIII.Delimitação do Tema**

Os Meios de Pagamento Eletrônico podem ser utilizados em diversas situações de compras, como por exemplo, estacionamento, pagamento de onibus, supermercado etc. (Mondex, 1996).

Para efeito desta pesquisa serão apenas tratados os meios utilizáveis em comércio eletrônico através da Internet.

A pesquisa coletou dados até setembro de 1999 com lojistas de qualquer parte do mundo que tenham estabelecido alguma forma de comércio eletrônico através da Internet, em língua inglesa; no Brasil, em português; ou que tenham sido referenciadas por algum produtor de meio de pagamento eletrônico.

## **IX. Hipóteses**

- 1– O comportamento de empresas é similar ao de pessoas quanto a decisão e adoção de nova tecnologia de Meio de Pagamento Eletrônico.
- 2– Há vários perfis de empresas usuárias que adotam Meios de Pagamento Eletrônico.
- 3– Há uma separação entre os diferentes perfis de adotantes, originada na diferença de percepção de valor.
- 4– Cada um dos segmentos, agregados pelos perfis, possui um primeiro adotante
- 5– Quando um ator percebe-se ameaçado por alguém que já adotou meios de pagamento eletrônico no seu mercado, passa a adotar a tecnologia.
- 6– Há um dinamismo constante no mercado onde as empresas referenciam-se continuamente.

## **X. Metodologia**

Os Meios de Pagamento Eletrônicos começam a ser utilizados por mostrarem aparente vantagem sobre os sistemas tradicionais principalmente em sistemas de comércio eletrônico via Internet. Os primeiros adotantes conforme definido por ROGERS (1995), satisfazem-se com a promessa dos fornecedores e a própria intuição, e trabalham com muita intensidade para conseguir obter os resultados esperados. O segmento seguinte de usuários, a grande maioria, segundo ROGERS (1995) possui um perfil diferente, pois enquanto não são convencidos por meio de resultados palpáveis, com nítida relação de vantagem na relação custo/benefício e riscos minimizados, tanto técnicos quanto financeiros, não adotam o novo sistema.

Os atores mais importantes em questão são os produtores de sistemas de meios de pagamento eletrônicos e os usuários do sistema.

### **1. Pesquisa de Campo**

Foram realizadas pesquisas de campo de caráter exploratório, com os dois públicos diferentes, visando buscar melhor entendimento do problema.

Nestas pesquisas o objetivo principal foi levantar as preocupações e dificuldades dos produtores e usuários responsáveis por sistemas de comércio eletrônico via Internet, considerando os critérios de qualidade conforme descrito por JURAN (1992), e classificar as preocupações do mercado em função do perfil inovador ou conservador, conforme usado entre outros autores, por MATHESON e MATHESON (1998) e por KEYS (1995).

#### ***1.1. Pesquisa com Produtores de Meios de Pagamento Eletrônico***

Esta pesquisa foi realizada em dezembro de 1997, por correio eletrônico (anexos 1 e 2) com os oito produtores de meios de pagamento eletrônico identificados através de pesquisa em literatura, que tinham produtos sendo comercializados em 1997.

O objetivo foi identificar o processo de melhoramento contínuo dos seus sistemas e as dificuldades encontradas no processo de colocação no mercado dos meios de pagamento eletrônicos.

Foi enviado um único questionário e a partir das respostas, foram trocados novos e-mails, conforme necessidade.

Os aspectos que foram contemplados neste questionário com produtores, foram:

- a base de clientes comerciantes, para que pudessem ser contatados na segunda pesquisa,
- sobre a consideração de estar o produto completamente pronto ou ainda em processo de desenvolvimento,
- a respeito de quanto tempo é necessário para um ciclo de melhoramento,
- sobre as informações que são utilizadas para o melhoramento do produto,
- sobre as objeções mais frequentes por parte do cliente para a adoção do sistema
- a maneira de como os clientes ou usuários resolvem os seus problemas técnicos.

Observação: os produtores de meios de pagamento eletrônicos tem o hábito de divulgar como base de clientes o número de usuários finais (consumidores dos lojistas / comerciantes), dando à impressão de base instalada grande. Sabendo desse fato a pergunta feita na pesquisa insiste na base instalada em quantidade de comerciantes.

## **1.2. Pesquisa junto aos lojistas que operam com sistemas de comércio eletrônico via Internet**

A segunda pesquisa foi realizada com comerciantes que utilizam sistemas de comércio eletrônico via Internet. O objetivo desta pesquisa foi classificar essas organizações comerciantes de acordo com seus perfis, mais inovador ou mais conservador. Foi também objetivo identificar barreiras para a adoção, na visão de cada um desses públicos, dos meios de pagamento eletrônicos.

### **1.2.1. Identificação do universo pesquisado**

Através de pesquisa com os produtores de meios de pagamento eletrônico foram levantados os nomes e endereços de lojistas que adotam o MPE específico (Anexo 6). Esses nomes foram completados e atualizados por pesquisa nos *sites* dessas organizações, em janeiro de 1999. Dessa forma foi pesquisado o universo de organizações que adotam o MPE específico de cada fabricante.

Para identificar lojistas que não adotam os MPE entre os fabricantes, foi realizada uma pesquisa sistemática conforme descrito por KOSTER (1996) e LAWRENCE e GILES (1997) junto aos *sites* de procura internacionais e no Brasil como altavista, cade, hotbot, infoseek, uol e yahoo. Foram utilizados os recursos particulares de cada um dos sistemas de busca para estender a procura até o final da cadeia, sendo posteriormente analisados os endereços para testar se eram nomes e endereços únicos.

Partindo da hipótese que todo lojista que trabalha com comércio eletrônico pela Internet, faz o possível para estar cadastrado junto aos instrumentos de busca o quanto antes, pode ser concluído que foram identificados a quase totalidade das lojas com comércio eletrônico via Internet, de língua inglesa assim como em língua portuguesa no Brasil (.com.br), além dos



comerciantes que utilizavam os meios de pagamento eletrônicos entrevistados na primeira pesquisa, até 1998, em qualquer parte do mundo.

### **1.2.2. Instrumental de pesquisa**

Uma vez identificados os endereços, foi especialmente construído um programa de computador que lê as primeiras páginas de cada loja, para identificar contatos de e-mail.

Essa pesquisa resultou em 73 % de sucesso. Para os 27% restantes, foram incrementadas as buscas para os 3 primeiros níveis de páginas, o índice de sucesso passou para 83 % dos nomes. A lista resultante das empresas pesquisadas, com 8835 nomes e url's (endereços web) encontra-se no Anexo 5.

Para essa lista foram enviados em março/99 emails (Anexos 3 e 4), com *link* contendo um identificador único, para o endereço no servidor aonde estava o questionário montado em html (anexo 7), o questionário está transcrito nos Anexos 3 e 4, para leitura.

O identificador único, para cada uma das 8835 empresas, continha 20 algarismos, para dificultar que algum respondente entrasse como outra empresa. O programa para gerar números únicos de 20 algarismos está no anexo 7.

Como não foi registrado nenhum caso de identificador falso (número que não foi distribuído), podemos assumir que não houve caso de alteração.

Os formulários foram transmitidos por cgi (comunicação cliente-servidor, baseado em http, protocolo de comunicação web, DECEMBER e GINSBURG, 1995) (anexo 7), ao servidor, e os resultados foram armazenados em arquivo, para tratamento de dados. Caso a mesma empresa tentasse responder ao

questionário uma segunda vez, o questionário seria apresentado novamente, o registro seria mantido, mas no programa de tratamento dos dados (anexo 7), o último lote de resposta, desde que válidas, é o que seria considerado.

Não foi registrado nenhum caso de lote de respostas duplicadas.

### **1.3. Montagem do questionário**

Um primeiro bloco de questões, tratou:

- do setor de atividade,
- das datas de adoção do sistema de comércio eletrônico,
- de valores médios transacionados com meio de pagamento eletrônico,
- do país em que tem sede,
- da data em que adotou o sistema de meio de pagamento eletrônico,
- de perguntas para identificar se existe alguma referência com seu setor e seus fornecedores,
- de perguntas para identificar o quanto pesquisaram sobre as práticas de comércio eletrônico e meios de pagamento no seu setor,
- de perguntas para identificar fontes de informação utilizadas para obter conhecimentos sobre meios de pagamento eletrônicos,
- de preocupações que tinham antes de adotar MPE,
- de como resolvem problemas técnicos associados ao sistema MPE.

A partir da metodologia desenvolvida por MATHESON e MATHESON (1998) para classificar as empresas de acordo com o perfil mais conservador ou mais inovador, em função das posições quanto:

- ao processo de criação de valor,
- ao processo para criar alternativas,
- ao aprendizado contínuo,
- às incertezas,
- à perspectiva estratégica,
- ao pensamento sistêmico,
- ao fluxo aberto de informações,
- ao empowerment,
- ao processo de tomada de decisão,

foi usado um segundo bloco de questões. Foi montada uma sequência de 9 blocos de perguntas, com 5 questões em cada um. Foram preparadas respostas para cada um dos extremos de perguntas, e montada uma escala de 7 valores (-3, -2, -1, 0, 1, 2, 3) para que escolhessem qual a situação que mais se aproxima da realidade da organização pesquisada.

#### ***1.4. Tratamento das respostas***

A partir dos dados obtidos, as empresas foram classificadas de acordo com seu perfil. As respostas do primeiro bloco de perguntas foram analisadas o que permitiu entender melhor o público estudado, que corresponde à primeira maioria conforme ROGERS (1995). Para essa primeira maioria, foram identificadas as preocupações e atitudes que inibiam a adoção de meios de pagamento eletrônico.

## 2. Análise Sistêmica dos Dados Obtidos

Uma metodologia com abordagem sistêmica desenvolvida por GOLDRATT (1986) na década de 1980 declara que todo o sistema é composto de partes que interagem, possui um objetivo e que este objetivo é limitado por uma restrição. Baseado nestas três premissas, o autor construiu uma teoria conhecida como Teoria das Restrições, que analisa os sistemas baseando no fato de que todo sistema possui uma restrição, que o impede de caminhar em direção ao seu objetivo (DETTMER, 1997).

Para a sistematização das preocupações será empregada a técnica de identificação do problema-raiz, conforme descrito por GOLDRATT (1986; 1990a; 1990b) e por WILSON, DEIL e ANDERSON (1993).

Essa metodologia parte do pressuposto de que existe um ou poucos problema-raiz responsáveis pelas várias preocupações, e sugere uma técnica para identificação destes problemas raiz (CSILLAG, 1995).

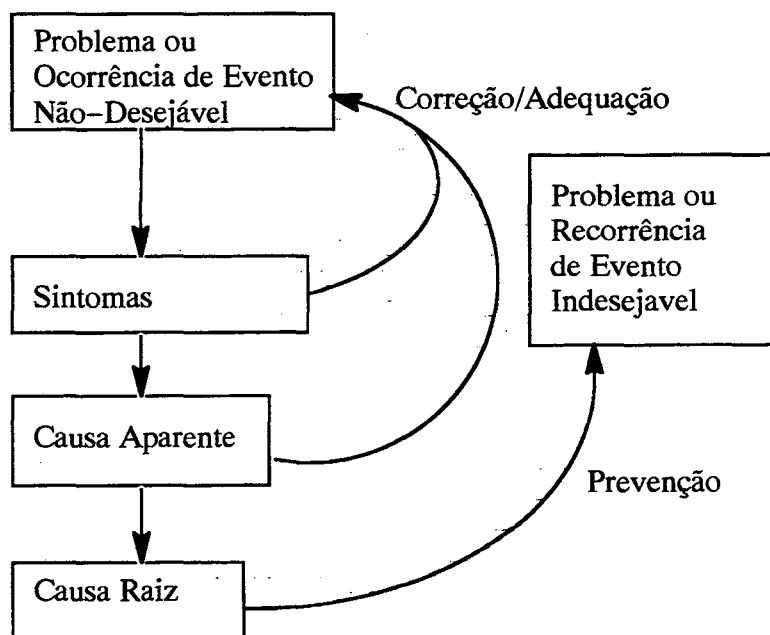


Figura 14 – relacionamento entre causa-raiz e problemas

Para utilizar essa técnica parte-se do princípio de que estamos estudando um sistema. Pela definição de von BERTALANFFY (1976) sistema é um conjunto de componentes (ou elementos) que estão interligados e interagem.

O estudo de um sistema, pode mostrar ter vários efeitos indesejáveis, mas somente um problema ou causa-raiz.

Conforme esta metodologia, deve ser primeiramente estabelecido o cenário analisado, identificados os efeitos indesejáveis, para depois poder identificar o problema-raiz.

Utilizando esta forma de pensar, foram analisadas e trabalhadas as preocupações recolhidas durante as pesquisas e utilizado um diagrama de relação de causa e efeito. Foi identificada a causa-raiz destas preocupações. O raciocínio que embasa esta ação reside no fato de que sendo esta causa-raiz a restrição que impede o sistema de caminhar em direção ao objetivo, basta atuar nela, que estarão também eliminadas as preocupações, pois estando frente a um sistema, todas as suas partes interagem. De posse da causa raiz encontrada, e utilizando um diagrama de conflito que mostra condições necessárias, procurou-se identificar pressupostos implícitos que embasam estas condições necessárias, explicando assim a maneira de pensar do público em questão (GOLDRATT, 1990a). Procurou-se em seguida uma idéia mobilizadora, que se, aplicada poderia conduzir numa relação de causa e efeito num conjunto com uma série de outras ações, à resultados que eliminassem as preocupações inicialmente recolhidas (SCHEINKOPF, 1999). Esta série de ações quando devidamente sincronizadas e sistematizadas se constituem na metodologia aqui proposta com vistas a atingir o grande público vencendo todas aquelas preocupações inicialmente recolhidas como genéricas. As preocupações coletadas se constituem na abordagem genérica. Para cada segmento da primeira maioria devem ser recolhidas preocupações específicas que seguem abordagem identica ao caso genérico, e são implementadas em conjunto.

Uma vez trabalhado um segmento da grande massa de usuários potenciais, virão outros até que com os diferentes *loops*, propositadamente provocados trarão uma realimentação positiva acelerando o processo de adoção da nova tecnologia.

## **XI. Resultados das Pesquisas de Campo**

### **1. Resultado da Pesquisa com os produtores de meios de pagamento eletrônico.**

A partir do questionário enviado para os 8 produtores de meios de pagamento eletrônicos, em operação na época da pesquisa, foi concluído que o total de 689 lojistas que adotavam seus meios de pagamento (Anexo 6) é um número muito pequeno para que o sistema meio de pagamento eletrônico possa ser considerado como popular ou difundido.

A postura que todos os fabricantes apresentaram em relação ao produto, de considerar o sistema como em contínuo desenvolvimento indica tanto uma postura de qualidade, de melhoramento contínuo (JURAN 1992), como de reconhecimento das dificuldades de abranger todas as situações possíveis em ambiente de teste.

Os tempos de ciclos de melhoria do sistema de aproximadamente 2 anos (anexo 2), demonstram a complexidade do sistema e uma eventual dificuldade de recolher informações como base de melhoria.

As fontes de informações levantadas, para o melhoramento do produto foram:

- ◆ retorno (*feedback*) do cliente,
- ◆ levantamento de tendências do mercado,
- ◆ levantamento junto ao governo e órgãos oficiais,
- ◆ levantamento junto à integradores,
- ◆ levantamento junto ao mercado financeiro.

As dificuldades enfrentadas pelos produtores de meios de pagamento eletrônicos para obter as informações abaixo são causadas pela pequena base de clientes.

- ◆ pouco volume de retorno (*feedback*) de clientes,
- ◆ poucos integradores,

## **2. Dificuldades enfrentadas pelos produtores de meio de pagamento eletrônico para colocação de seus produtos no mercado**

O levantamento junto a esses produtores sobre as objeções encontradas no mercado, para colocação dos meios de pagamento eletrônico foram :

- ◆ mercado afirma que “poucas pessoas do mercado compreendem o sistema MPE na sua totalidade”
- ◆ reclamam que há varios sistemas e nenhum reconhecido como padrão
- ◆ de insegurança quanto à aspectos técnicos (coisas não previstas – *Murphy*)
- ◆ interpretam notícias da mídia como desestimulantes à adoção de MPE
- ◆ a relação custo / benefício é desfavorável
- ◆ mecanismos de crédito não estão associados ao MPE atualmente
- ◆ não sentem segurança no sistema (medo de *hackers*)
- ◆ não acreditam no comércio eletrônico, pois conforme divulgado, empresas que atuam não tem lucro
- ◆ não estão “preparados nem adequados para fazer experiências com nosso mercado”
- ◆ barreira de idioma



Para resolver os problemas, os clientes recorriam a solicitações de ajuda ao fabricante, buscando um integrador de sistemas ou mesmo sozinhos, utilizando pessoal interno.

A partir das respostas obtidas com os fabricantes, foi preparado o questionário para os comerciantes que operam com comércio eletrônico via Internet.

### **3. Resposta do questionário aos enviado aos comerciantes que adotam comércio eletrônico via Internet**

O questionário foi enviado para 8835 empresas (anexo 5) obtendo 153 respostas (1,7%) com os dois e-mails enviados. Com o primeiro e-mail foram recebidas 65 respostas, e com o segundo e-mail foram recebidas mais 88 respostas.

Cada vez que, pelo menos oito perguntas não eram respondidas consecutivamente, o questionário era cancelado. Duzentas e cinquenta e uma empresas que acessaram o questionário e deixaram pelo menos oito perguntas consecutivas sem resposta. Para reduzir este problema numa próxima pesquisa, reduzir o número de perguntas do formulário, principalmente na caracterização do perfil das empresas, com o risco de não ser tão preciso na conclusão. (Formulário nos Anexos 3 e 4).

#### ***3.1. Distribuição por setor entre os pesquisados***

Os setores pesquisados podem ser agrupados conforme a tabela abaixo:

Tabela 41 : Distribuição por setores entre pesquisados

categoria	inclui:
Livros e Mídia	Livros e Publicações Música Vídeos e cdrom
Moda	vestuário acessórios jóias e relógios
Hobby e diversões	hobbies esportes brinquedos turismo
Serviços empresariais	serviços industriais serviços de escritório
Alimentação	bebidas alcoolicas cestas de presentes supermercados cigarros produtos gourmet
Casa e Jardim	automoveis lojas de departamento produtos para jardim produtos domésticos animais de estimação
Produtos Eletro-eletrônicos	hardware (informática) software periféricos e produtos eletrônicos
Presentes	Galerias de Arte Artesanatos
Família	produtos para crianças saúde e nutrição beleza religião

A frequência por setor é mostrada na figura a seguir

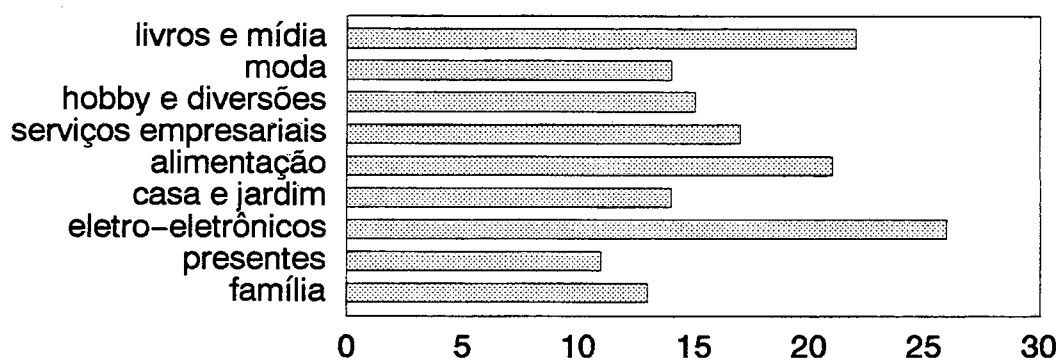


Figura 15 – Frequência por setores

### 3.2. Distribuição por país entre os pesquisados

A distribuição por país entre as empresas pesquisadas pode ser vista no gráfico abaixo

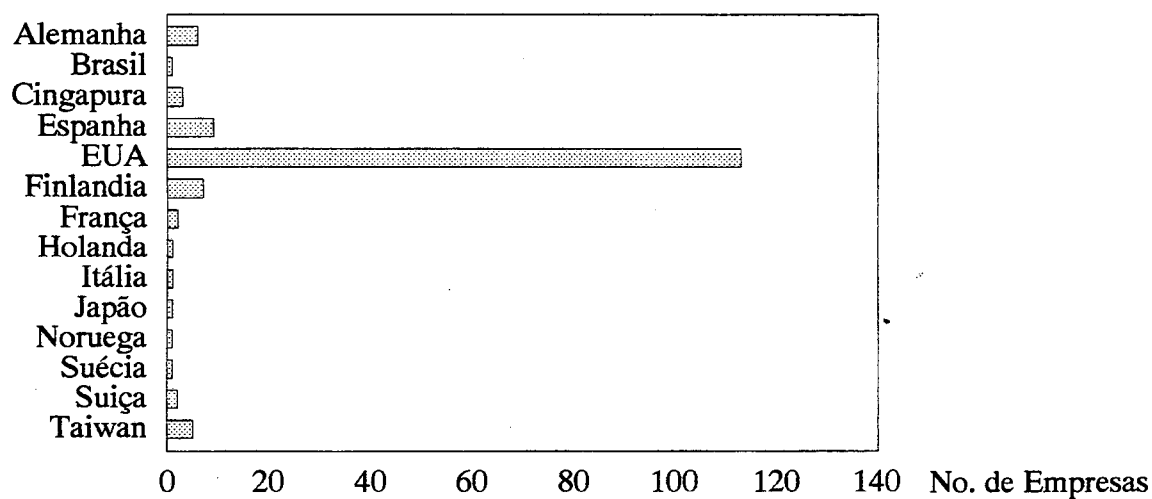


Figura 16 – Distribuição por países

### 3.3. Valor médio transacionado

O valor médio transacionado através de sistema de comércio eletrônico pelas empresas respondentes teve uma grande concentração entre US\$ 1 e US\$ 50, com concentração maior entre US\$ 10 e US\$ 50.

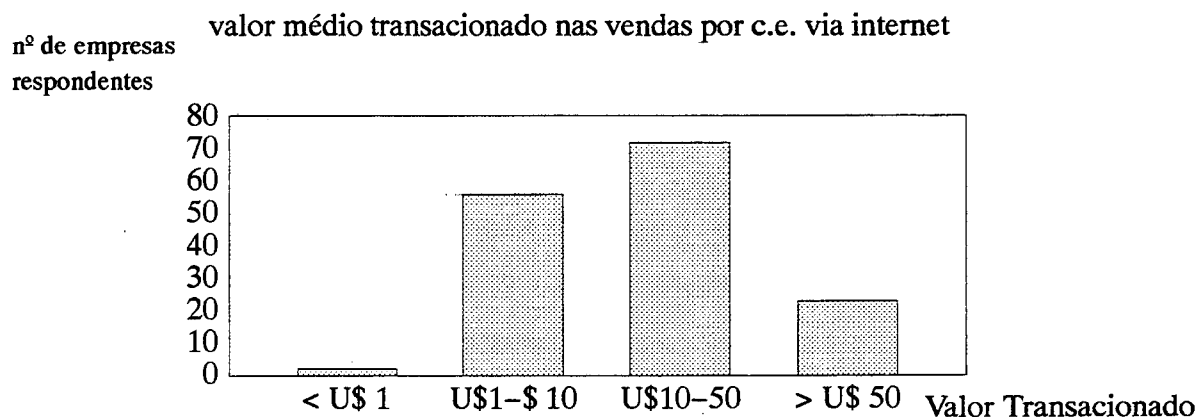


Figura 17 – Valor médio transacionado por comércio eletrônico via Internet

### 3.4. Data em que adotaram sistemas de comércio eletrônico e meios de pagamento eletrônico

O quadro abaixo mostra a distribuição das datas em que os respondentes da pesquisa iniciaram as operações de comércio eletrônico.

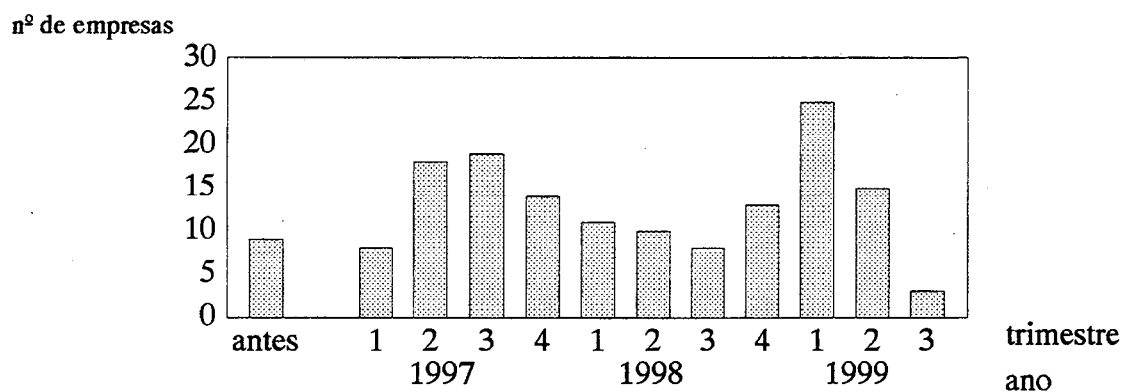


Figura 18 – Data em que adotaram sistemas de ce e mpe

A maior parte das empresas definiu o MPE quando da implementação do sistema de comércio eletrônico (86%), mas uma parcela ainda aderiu à novos sistemas após a implantação (14 %).

Tabela 42 : Data em que definiram mpe

Data em que definiram o MPE	nº de empresas respondentes
junto com Comércio Eletrônico	132 empresas
após a adoção do Comércio Eletrônico	21 empresas

### 3.5. Caracterização do perfil das empresas

Utilizando a metodologia para caracterizar o perfil organizacional das empresas respondentes em função, do perfil mais inovador ou mais conservador, foi obtida a seguinte distribuição (valores associados a cada pergunta, variando entre -3, -2, -1, 0, 1, 2, 3 ; ver questionário anexos 3 e 4 foram totalizados).

Uma vez caracterizados os perfís das empresas como mais inovadoras ou menos inovadoras, surge a distribuição de frequências como segue:

Distribuição pesquisa comportamento organizacional

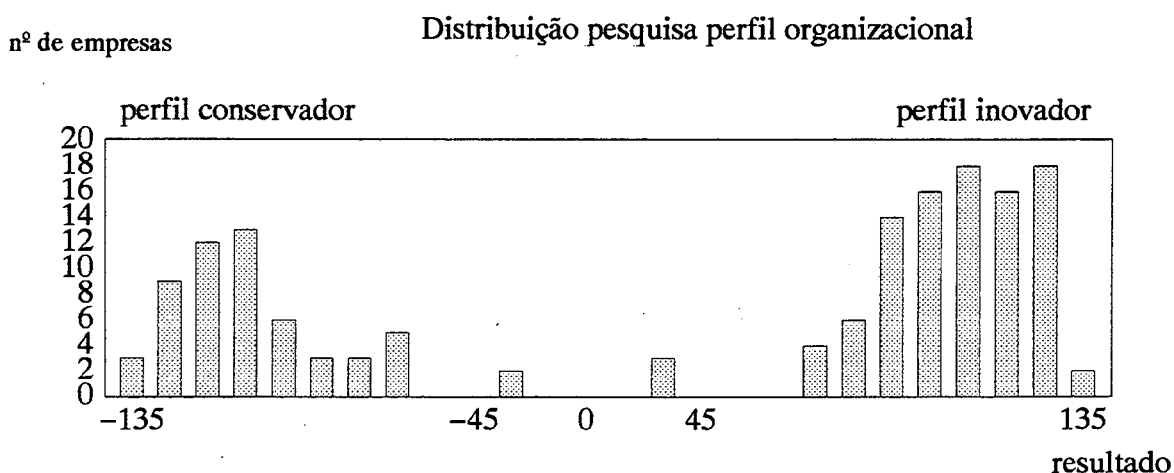


Figura 19 – Distribuição por perfil organizacional

O gráfico mostra 94 empresas com perfil inovador e 54 empresas com perfil conservador, além de 5 empresas com perfil não muito bem definido. Para essa classificação foram considerados o total de pontos abaixo de -45 como perfil conservador e acima de 45 como perfil inovador.

Na tabela abaixo, observa-se o detalhe dos intervalos de distribuição.

Tabela 43 : Intervalos de distribuição

<b>intervalo de resultados</b>	<b>nº de empresas classificadas no intervalo</b>
-135 --(- 125	3
-125 --(- 115	9
- 115 --(- 105	12
- 105 --(- 95	13
- 95 --(- 85	6
- 85 --(- 75	3
-75 --(- 65	3
- 65 --(- 55	5
-55 --(- 45	
-45 --(- 35	
- 35 --(- 25	2
-25 --(- 15	
-15 --(- 0	
0 --(- 15	
15 --(- 25	
25 --(- 35	
35 --(- 45	3
45 --(- 55	
55 --(- 65	4
65 --(- 75	6
75 --(- 85	14
85 --(- 95	16
95 --(- 105	18
105 --(- 115	16
115 --(- 125	18
125 --(- 135	2

### 3.6. Existe referência com o seu próprio setor

Usando essa classificação para entender as respostas, pode-se perceber que empresas que foram classificadas com perfil inovador tendem a utilizar o produto mesmo quando não sabem de ninguém que o tenha adotado antes.

Já empresas com perfil conservador tendem a utilizar com mais frequência a inovação quando percebem-se ameaçados por algum concorrente.

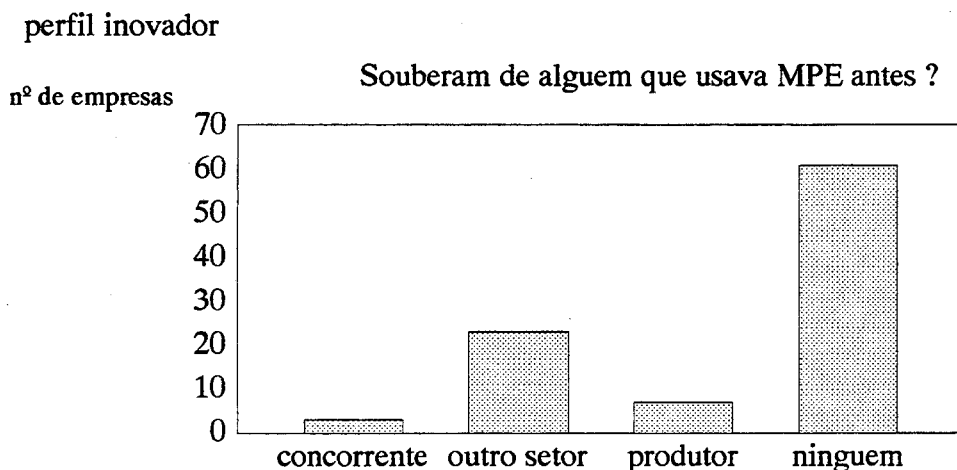


Figura 20 – Perfil Inovador – souberam de alguém que usava mpe antes

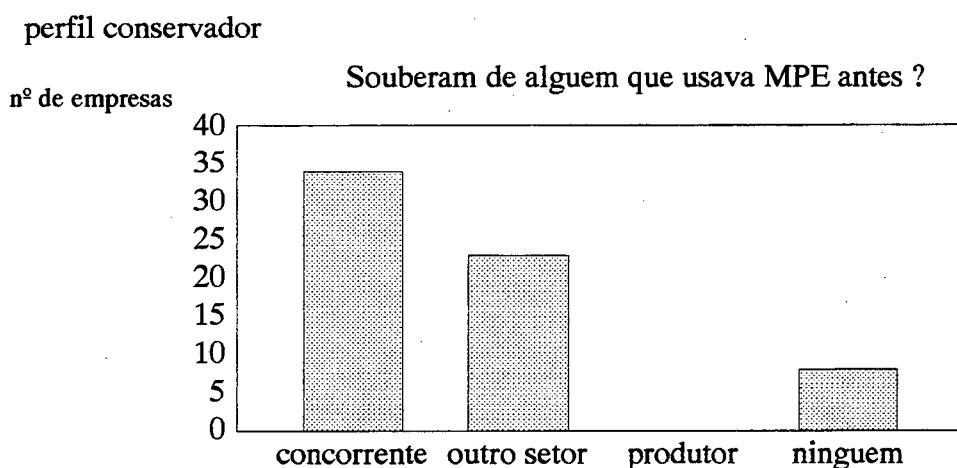


Figura 21 – Perfil conservador – souberam de alguém que usava mpe antes?



### **3.7. Motivos para adoção de sistemas de meios de pagamento eletrônico**

Foram listados abaixo os motivos que levaram as empresas pesquisadas a adotar o sistema de pagamento eletrônico, considerando ambos os perfis. Isto porque tanto o perfil inovador quanto o conservador eram sensíveis a argumentos de que o sistema se mostrou eficiente em outros setores, na redução de custos em relação aos meios de pagamentos adotados assim como trazendo maior integração com os clientes.

Tabela 44 : Motivos para adoção de mpe's

O que levou sua empresa a adotar o(s) sistema(s) de meio de pagamento eletrônico ?		
perfil conservador		perfil inovador
	acreditam no potencial do sistema	13
23	o meu setor já utiliza	
6	o sistema se mostrou eficiente em outros setores	16
	confiança no produtor / integrador	21
	buscando vantagem competitiva	6
2	redução de custo em relação aos meios de pagamento que usamos	6
	redução de custo de transação de pedido	3
	criação de imagem corporativa	19
12	necessidade competitiva, outros já adotaram	
	diferenciação	15
	maior poder alternativo em relação aos sistemas de cobrança	1
	criar barreira competitiva	2
4	maior integração com os clientes	6
7	integrador que instalou sistema de CE instalou tudo	

Das empresas que responderam a maioria, independente do perfil, também aceita receber os dados de cartão de crédito por telefone, que é uma forma de pagamento convencional.

adotam outras formas de pagamento para comércio eletrônico ?

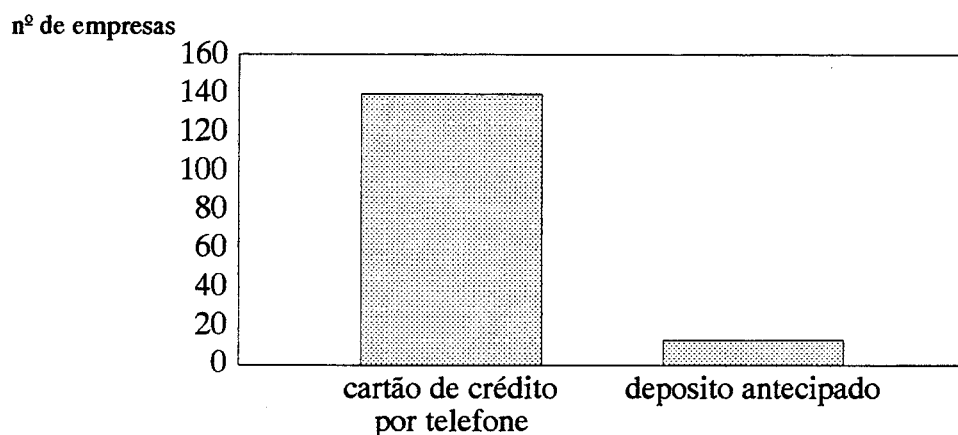


Figura 22 – Outras formas de pagamento para c.e.

Das empresas pesquisadas, todas responderam estar satisfeitas com os sistemas de MPE,

Tabela 45 : Satisfação com os sistemas adotados

Voces estão satisfeitos com o(s) sistema(s) adotado(s) ?	
sim	100%
não	—

e a maior parte, afirmam não saber se essa satisfação é generalizada entre os usuários de MPE.

Tabela 46 : Sabe se outras empresa que utilizam mpe estão satisfeitas ?

Sabe se outras empresas que utilizam MPE estão satisfeitas ?		
perfil conservador		perfil inovador
10 respostas (18,5 %)	sim	24 respostas (25,5 %)
44 respostas (81,5 %)	não	70 respostas (74,5%)

Em nenhum dos setores pesquisados, se consideram os únicos adotantes atualmente, o que indica que reconhecem que o seu mercado está utilizando algum sistema de MPE.

Tabela 47 : Outras empresas do setor já adotaram ?

Outras empresas do seu setor já adotaram ?	
sim	100%
não	-

Empresas classificadas com perfil inovador tem a percepção de que foram os primeiros a adotar o sistema MPE.

Tabela 48 : Quantos por cento do seu segmento adotava mpe quando sua empresa adotou ?

Quantos por cento do seu segmento de mercado (concorrentes) adotava o sistema de MPE quando sua empresa adotou?				
perfil conservador			perfil inovador	
20 %	11 empresas	< 10 %	89 %	84 empresas
80 %	43 empresas	10 % – 35 %	11 %	10 empresas
-	-	35 % – 65 %	-	-
-	-	> 65 %	-	-

### 3.8. Fontes de informações sobre meio de pagamento eletrônico

Independente do perfil, os vendedores de sistemas (produtor ou integrador), tem tido um papel fundamental na difusão dos conceitos do produto. A literatura especializada tem tido maior resultado entre as empresas de perfil inovador.

Tabela 49 : Fontes de informação

Como ficou sabendo do sistema MPE ?				
perfil conservador		através de :	perfil inovador	
3 empresas	5%	consultor	10%	9 empresas
3 empresas	5%	outra empresa	5%	5 empresas
3 empresas	5%	concorrente	2%	1 empresas
3 empresas	5%	associações	15%	13 empresas
5 empresas	8%	escola	8%	7 empresas
1 empresa	2%	publicações	20%	18 empresa
15 empresas	30%	vendedor do produto	30%	27 empresas
21 empresas	40%	vendedor de parceiro do produtor	10%	14 empresas

Para adequações no produto, empresas de perfil inovador tem demandado muito mais participação do produtor do sistema, enquanto empresas de perfil conservador tem se valido muito mais de integradores de sistemas, provavelmente com quem já tinham algum relacionamento anterior. Um dado interessante como visto na tabela é que um número significativo de empresas com perfil conservador, acreditam não ter sido necessário nenhum ajuste ou adequação ao sistema.

Tabela 50 : Coordenação das adaptações do produto

Quem coordenou as adaptações para ajustar o produto existente às suas necessidades ?				
perfil conservador			perfil inovador	
–	–	o produtor	80 empresas	85 %
57,5 %	31 empresas	integrador de sistemas	2 empresas	2%
–	–	nós mesmos	12 empresas	13%
42,5 %	23 empresas	não foi necessário	–	–

### **3.9. Objeções por parte dos comerciantes que adotam comércio eletrônico via Internet para adoção de meio de pagamento eletrônico**

Quanto as barreiras que essas empresas tinham (ou ainda tem) para usar algum sistema de meio de pagamento eletrônico, levantado a partir das pesquisas com os produtores, somente a barreira da língua que havia sido levantado por um produtor não recebeu nenhuma confirmação; e duas barreiras adicionais foram acrescentadas, a situação de não sentir confiança no vendedor (ele não quer resolver o meu problema), e reclamações de limite de valor máximo permitido para as transações, junto a empresas com perfil conservador.

As objeções levantadas junto aos fabricantes de meios de pagamento eletrônico e confirmadas junto ao mercado deles é a seguinte:

- poucas pessoas de nosso mercado compreendem o sistema MPE na sua totalidade
- há varios sistemas e nenhum reconhecido como padrão
- insegurança quanto à aspectos técnicos (coisas não previstas – *Murphy*)
- interpretam notícias da mídia como desestimulantes à adoção de MPE
- a relação custo / benefício é desfavorável
- não senti confiança que o vendedor de MPE quer resolver o problema da minha empresa
- o limite do valor do MPE é insuficiente para a transação

- mecanismos de crédito não estão associados ao MPE atualmente
- não sinto segurança no sistema (*hacker*)
- não acredito no comércio eletrônico, empresas que atuam não tem lucro
- não estamos preparados nem adequados para fazer experiências com nosso mercado

Essas objeções foram todas levantadas por empresas com perfil conservador.

Empresas com perfil inovador enviaram 56 respostas como não tendo problemas, e três objeções não levantadas com os produtores de meios de pagamento eletrônico foram apontadas como as principais:

- faltam detalhes sobre o mecanismo de funcionamento das transações necessárias ao funcionamento do meio de pagamento eletrônico,
- faltam informações sobre o mecanismo de criptografia adotado,
- faltam detalhes de quem é a empresa, e quem são as pessoas, por traz do meio de pagamento eletrônico.

### 3.10. Como resolveram problemas técnicos

Quando houve problemas, foram resolvidos basicamente pelo fornecedor / parceiro para ambos os perfis.

Tabela 51 : Como resolveram os problemas

Quem resolveu ?		
perfil conservador		perfil inovador
92,5%	fornecedor / parceiro	94,5%
–	internamente à empresa	5,5%
7,5%	ainda não foi resolvido	–

### 3.11. Se fornecedores podem ter pressionado a adoção

Avaliando a cadeia de fornecedores, dos comerciantes que operam com comércio eletrônico via Internet um número pequeno utiliza comércio eletrônico. Isso indica que esses segmentos estão na frente, no processo de adoção de MPE, em relação aos fornecedores.

Tabela 52 : Quantos de seus fornecedores usam c.e. ?

Quantos de seus fornecedores usam comércio eletrônico ?				
perfil conservador			perfil inovador	
–	–	+ 60%	–	–
5 empresas	9%	40% – 60%	–	–
5 empresas	9%	20% – 40%	20%	19 empresas
44 empresas	82%	– 20%	80%	75 empresas

### 3.12. Sobre acesso à informações técnicas

Sobre dados técnicos mais específicos, empresas com perfil inovador parecem ter muito mais acesso às informações,

Tabela 53 : Acesso à informações técnicas

Você conhece estudos técnicos, ou resultados estatísticos de utilização de MPE ?				
perfil conservador			perfil inovador	
21 empresas	39%	sim	90%	85 empresas
33 empresas	61%	não	10%	9 empresas

para os dois perfis, dos que tiveram acesso às informações, a literatura técnica é uma fonte importante. Para fonte de informações, aparentemente o integrador de sistemas tem desempenhado um papel importante junto às empresas de perfil conservador.

Tabela 54 : Fonte de acesso às informações

Como teve acesso aos dados ?				
perfil conservador			perfil inovador	
12 empresas	58 %	literatura técnica	60%	51 empresas
3 empresas	14 %	vendedor	20%	17 empresas
3 empresas	14 %	integrador	–	–
3 empresas	14 %	congressos/ simpósios	20%	17 empresas

À luz desse fatos, por não ter grande disposição para buscar na literatura técnica informações sobre MPE, o público com perfil conservador também terá a mesma restrição com outros assuntos da literatura técnica associada, como segurança de sistemas e meios de pagamentos de um modo geral.



### 3.13. Sobre as datas de adoção de comércio eletrônico

As datas de adoção de meio de pagamento eletrônico são fortemente ligadas com as datas de adoção do comércio eletrônico.

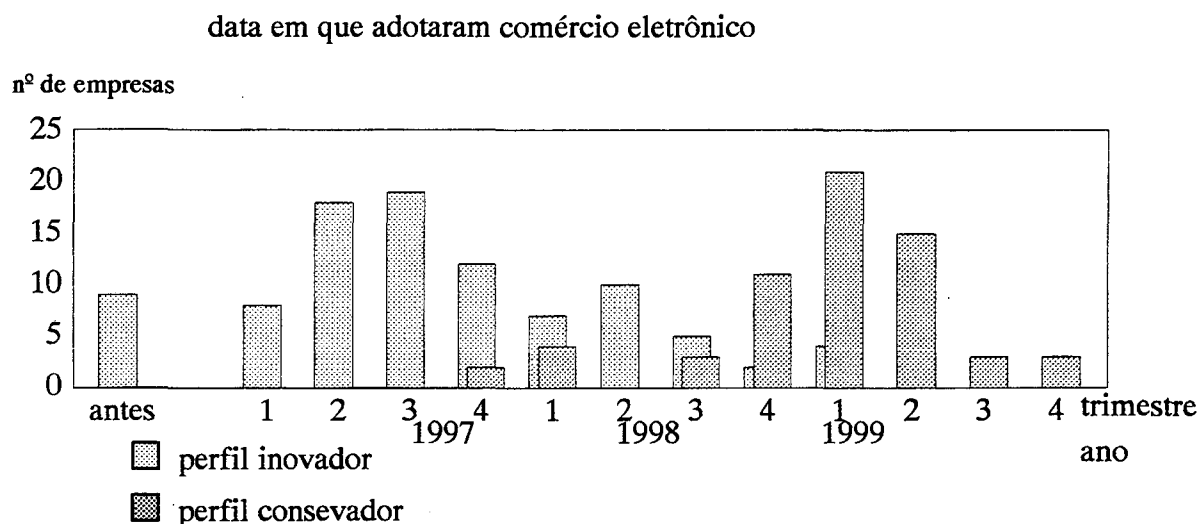


Figura 23 – Distribuição da data de adoção de sistemas de comércio eletrônico, por perfil organizacional

Pode ser percebida uma tendência de existência de duas curvas, uma para o perfil conservador e outra para o perfil inovador. Essa distribuição tem uma série de implicações.

Pode ser afirmado que o comportamento das empresas é similar ao de pessoas quanto à decisão de adoção de nova tecnologia de meio de pagamento eletrônico. Existem pelo menos dois perfis identificados, os mais inovadores e os mais conservadores. A separação originada na diferença de percepção de valor define duas abordagens diferentes para cada mercado.

Como o mercado com determinado perfil não se esgota antes do mercado seguinte começar a adotar o MPE, existe um período de tempo onde estratégias voltadas para qualquer um dos dois públicos

surtirá efeito. Contudo o tamanho potencial do mercado com perfil conservador, a primeira maioria do mercado, é maior, de acordo com os modelos de difusão de inovações.

Cada um desses segmentos, agregados por perfis de mercado possui um primeiro adotante, ou grupo de adotantes. Uma explicação para esse comportamento ao longo do tempo, é que as informações não se difundem simultaneamente por todos os locais e pessoas.

O modelo aqui sugerido como comportamento de adoção entre os segmentos de perfis de mercado, lembra uma *banana-split* derretida, onde as curvas podem se sobrepor em alguns instantes no tempo. Os comportamentos são agregados, conforme constatado na pesquisa; quando um ator percebe-se ameaçado por alguém que já adotou no seu mercado, passa a adotar esta tecnologia. Esse conhecimento do que pode afetar seu mercado, mostra que as empresas referenciam-se continuamente.

Isso reforça a afirmação de que o comportamento das empresas é similar ao de pessoas quanto à decisão de adoção de nova tecnologia, no caso de meios de pagamento eletrônico.

## **XII. Avaliação sob o enfoque sistêmico das causas de resistência à adoção de Meios de Pagamento Eletrônico pelo mercado principal**

### **1. Introdução**

Várias são as causas que explicam a resistência à adoção de MPE por parte do mercado principal. Pesquisa junto aos produtores de sistemas de meios de pagamento eletrônico e usuários que administram sistemas de comércio eletrônico indicaram as seguintes objeções da primeira maioria, o mercado principal:

- ◆ poucas pessoas de nosso mercado compreendem o sistema MPE na sua totalidade,
- ◆ existem vários sistemas e nenhum reconhecido como padrão,
- ◆ insegurança quanto à aspectos técnicos (*Murphy*),
- ◆ interpretam notícias da mídia como desestimulantes à adoção de MPE,
- ◆ a relação custo/benefício é desfavorável,
- ◆ não senti confiança que o vendedor de MPE quer resolver o problema da minha empresa,
- ◆ o limite do valor do MPE é insuficiente para a transação,
- ◆ mecanismos de crédito não estão associados ao MPE atualmente,
- ◆ não sinto segurança no sistema (*hackers*),
- ◆ não acredito no comércio eletrônico, empresas que atuam não tem lucro,
- ◆ não estamos preparados nem adequados para fazer experiências com nosso mercado.

Essas causas foram todas identificadas em pelo menos duas fontes diferentes, na pesquisa.

Conforme definição utilizada na pesquisa, baseada nas características primeiramente apresentadas por ROGERS (1995) para indivíduos, o mercado principal é composto por empresas com perfil mais conservador, que pode ser identificado através:

- ◆ da cultura para criação de valor, aonde a criação de valor é um argumento propulsor para mudanças,
- ◆ do processo de criação de alternativas, com várias alternativas sendo criadas e avaliadas,
- ◆ do aprendizado contínuo, melhoramentos são constantemente identificados e ações são tomadas para aproveitá-los,
- ◆ da abordagem de encarando incertezas onde, o processo de incertezas é entendido, comunicado e gerenciado,
- ◆ da perspectiva estratégica de “fora para dentro”, com informações significativas do ambiente externo é disponibilizado,
- ◆ do pensamento sistêmico em que, os membros da empresa compreendem relações complexas de causa-efeito,
- ◆ do processo disciplinado de tomada de decisão em que os, processos sistemáticos de tomada de decisão são usados rotineiramente,
- ◆ do *empowerment*, onde um entendimento comum das estratégias para criação de valor direciona a empresa,
- ◆ do fluxo de informações livre, em que os membros da empresa têm acesso rápido e irrestrito às informações.

Segundo o modelo da “banana–split derretida”, que foi identificado através dos resultados da pesquisa, o mercado com as características acima, inicia o processo de compra após o mercado dos inovadores, pioneiros e adotantes iniciais, mas não obrigatoriamente quando esses se esgotam, conforme identificado na pesquisa. Assim pode ocorrer de num mesmo instante, ao longo do tempo, haver vendas tanto para público com perfil mais inovador quanto para público com um perfil mais conservador. O motivo disso é que a informação não é disponível simultaneamente para todos.

Para avaliar sob o enfoque sistêmico as causas de resistência identificadas na pesquisa, foi utilizada a metodologia da teoria das restrições (TOC) que interrelaciona as causas com efeitos entre os problemas identificados.

## **2. Problema avaliado**

As empresas possuem comportamentos de compra diferentes, especialmente em relação à adoção de produtos inovadores; em função desse perfil de compra podemos segmentar o mercado em inovadores e mercado principal. O problema avaliado é como fazer com que o mercado principal, mais numeroso e conservador adote o meio de pagamento eletrônico específico, pois existem vários sistemas concorrentes.

### ***2.1. Primeira etapa – porque o mercado principal não adota MPE.***

A descrição que segue provem da árvore de realidade atual (TOC) que segue uma lógica rigorosa.

Avaliando o resultado da árvore lógica da metodologia sistêmica adotada, existem algumas sequências que levam o público principal à não adotar sistemas de meio de pagamento eletrônico.

### ***2.1.1. Necessidade de Crédito para determinadas transações comerciais***

Existem casos em que há necessidade de crédito para realização da venda para algum mercado. Mecanismos de crédito não estão associados aos sistemas de MPE atualmente desenvolvidos, conforme pesquisa realizada para identificar os sistemas de meio de pagamento eletrônico hoje em operação. Dessa forma para várias operações aonde o crédito poderia ser necessário, os sistemas de MPE passariam a ser inadequados, quando há necessidade de crédito, o mercado principal não adota os MPE. Este raciocínio está representado na Figura 24-2/8.

### ***2.1.2. Limites de valores inadequados para algumas transações***

Existem casos em que é necessário um valor grande de transação, valores maiores que limites existentes em alguns meios de pagamentos, conforme identificado na pesquisa dos meios de pagamento eletrônico em operação ou na forma de proposta. Os MPE hoje operam com limites de valor máximo transacionado. Para esses casos, os MPE atualmente existentes são inadequados, e portanto não são adotados pelo mercado principal. Isto está mostrado na Figura 24-2/8.

### ***2.1.3. Por falta de avaliação e acreditarem que não estão preparados para MPE***

O mercado principal, conforme identificado pela pesquisa não quer descontinuidade. As questões sobre como abordar

incertezas, receberam para esse público com perfil conservador, uma média de -13 pontos (vide questionário anexo 3 e 4). Essa característica é reforçada pela pesquisa de ROGERS (1995), de MATHESON e MATHESON (1998), pelas constatações de MOORE (1991) e pelas pesquisas de BOLTON (1996) e de CHEN e CROWSTON (1997). Como, por definição descontinuidades implicam em risco, e o público do mercado principal não quer descontinuidades em seu processo, pode ser afirmado que o público do mercado principal não quer assumir riscos. A Figura 24-6/8 mostra na entidade 1 que “se o mercado principal não quer descontinuidade” e “descontinuidade implica em risco”, então ocorre necessariamente a entidade 17 “o mercado não quer assumir riscos”.

Como esse público não quer assumir riscos, então também não querem adotar novidades que implicam em mudanças de paradigma (Figura 24-2/8). A pesquisa indicou que empresas conservadoras não adotam novidades que não são plenamente dominadas. Estas constatações combinadas com as considerações anteriores permitem concluir que o público do mercado principal é conservador. (Figura 24-2/8)

A pesquisa de ROGERS (1995), MATHESON e MATHESON (1998), MOSTON e EMMANOUILIDE (1997) e FICHMAN (1995) indicaram que conservadores não adotam novidades que não são plenamente dominadas. A pesquisa realizada identificou que o público conservador do mercado principal não se considera preparado, nem se sente em condições para fazer experiências de novos sistemas no mercado.

A presente pesquisa identificou que o público a ser atingido atingir, a primeira maioria, obedeceu aos perfis identificados em outras pesquisas como VENKATRAMAN (1994), THORENSEN (1996), GATIGNON (1989) e BRAA e SORGAARD (1997) que apresenta esse mercado com características conservadoras. Essas características, identificadas vão de encontro com as pesquisas de MATHESON & MATHESON (1998) e ROGERS (1995).

Sendo conservadores, isto é, não querendo mudanças no *status quo*, o mercado principal racionaliza argumentos para não mudar. Com essa postura de evitar mudanças o mercado principal se considera não preparado para os novos MPE. Dessa forma consideram o produto como inadequado para a situação específica deles e não adotam o sistema.

A postura no mercado principal de racionalizar argumentos para não mudar faz com que esse público aceite os argumentos tão comuns, de que comércio eletrônico não dá lucro. Esses argumentos tem sido bastante difundidos na imprensa internacional, como o de casos pioneiros de comércio eletrônico pela Internet. Atualmente esta em evidência o caso da Amazon.com (Business Week, 1998; Fortune, 1999, Time 1999), empresa acompanhada por muitos analistas financeiros e também pela grande maioria do segmento (ZWASS 1996). Como MPE é característico de Comercio Eletrônico, essas empresas nem avaliam MPE. Dessa forma consideram MPE como inadequado para a situação específica deles e não adotam MPE (Figura 24-2/8)



#### **2.1.4. Mercado com perfil conservador não quer descontinuidade**

A pesquisa indicou que o mercado principal, não quer assumir riscos. Com essa postura o público alvo não estará disposto a adotar novidades que impliquem em mudanças de paradigma. Essa constatação reforça, juntamente com a indicação de que conservadores não adotam novidades que não são plenamente dominadas, de que o público alvo é conservador.

Entendendo que o público não quer assumir riscos, pelo fato de que situações de risco podem implicar em descontinuidade, e de que descontinuidade sempre implica em risco. Esse público com perfil conservador do mercado principal, a primeira maioria a ser atingida, não quer descontinuidade. Não querem descontinuidade em relação ao mercado e questões externas à empresa, nem querem descontinuidade em relação aos processos internos, conforme indicou a pesquisa.

Essa postura de não querer descontinuidades, de preferir manter o status quo atual está relacionado com todos os motivos de não adoção de MPE's pelo público principal, conforme exposto nos relacionamentos indicados na montagem da árvore de realidade atual, elaborada a partir das objeções levantadas na pesquisa (Figura 24–6/8).

Prosseguindo na análise das posturas conservadoras do mercado principal, o público alvo quer manter os paradigmas que conhece.

### ***2.1.5. O mercado conservador não quer mudanças de paradigma***

O paradigma ainda vigente nessas empresas, conforme a pesquisa, é de utilizar resultados locais para medir desempenho. Existem hoje vários modelos e teorias conforme descrito entre outros por BROWN e EISENHARDT (1998), que partem de novo paradigma, que implica em abordagem sistêmica, utilizando resultados globais para medir resultados. Contudo uma mudança de paradigma implica em descontinuidade, então essas idéias e ferramentas não são adotadas pois abandonar a idéia de resultado local, adotando resultado global implica em mudança de paradigma. Então as empresas com esse perfil continuam decidindo em função do desempenho de resultados locais (Figura 24–3/8).

Como apenas empresas que decidem com abordagens sistêmicas, avaliam resultados globais, contemplando a interação entre as várias partes do sistema, apenas elas é que conseguem desprezar resultados locais em função de resultados globais. Como esse público alvo não pensa sistemicamente então essas empresas não avaliam o impacto positivo global de um novo MPE. Como o custo do sistema é conhecido (no mínimo parte dele é passado em proposta pelo produtor do meio de pagamento eletrônico ou integrador de sistemas), então uma avaliação do custo / benefício é desfavorável, pois os benefícios não estarão claros e presentes. Pela pesquisa foi constatado que o público do mercado principal, notadamente a primeira maioria só investe quando a relação custo benefício for

compensadora, então esse público em questão, não adota meios de pagamento eletrônico (Figura 24–6/8; 3/8; 1/8).

Uma outra situação que reforça o evento acima ocorre quando o vendedor apresenta o sistema à organização. Foi identificado na pesquisa, que existem situações em que o interlocutor do lado da empresa tem a sensação de que o vendedor não conhece os problemas da organização dele. O vendedor parece só querer vender, a qualquer custo. Como o público da primeira maioria não quer descontinuidade, então ele não aceita propostas que podem causar turbulências na organização, ou seja, que não conheça meus problemas. Dessa forma o vendedor não inspira confiança ao interlocutor da organização, e ele não dará a devida atenção ao vendedor. O vendedor explica a vantagem do MPE, mas o interlocutor não compreende ou acredita nas vantagens apresentadas, como levantado na pesquisa.

Não acreditando ou conhecendo as vantagens totais do MPE, essas empresas não poderão avaliar o impacto positivo global de um novo meio de pagamento. Não avaliando positivamente os benefícios do sistema e tendo os custos conhecidos, não terão uma boa relação custo/benefício. Com isso o mercado principal não adota MPE (Figura 24–3/8; 1/8).

#### ***2.1.6. Implicações da existência de vários sistemas***

Conforme a pesquisa realizada, existem vários sistemas implementados ou como propostas de meios de pagamento eletrônico e nenhum reconhecido como padrão, e ainda não existe nenhum critério para definir padrões para MPE. Por outro lado existem também vários sistemas MPE surgindo,

reduzindo assim a possibilidade de um MPE adotado pela empresa em questão seja definido como padrão.

Para a existência de padrão, deve haver uma terceira parte reconhecida, pelo mercado com perfil conservador, para avaliar o sistema. A percepção é que essa parte reconhecida como maior possa reduzir o trauma de descontinuidade, o que é muito importante para esse público com perfil conservador.

Se há risco de um sistema diferente do adotado pela empresa virar padrão, então há risco de perder dinheiro, pois o sistema terá que ser trocado ou readequado. Se há risco de perda de dinheiro então o mercado principal não adotará o sistema de MPE.

Vários governos tem começado a tomar posição quanto à meios de pagamento eletrônico. As principais são a posição do Comitê de Economia e Política Monetária e Industrial do Parlamento Europeu (1998) , do G-10 (1997), e do governo norte americano (U.S. Department of the Treasury, 1998). Interessante notar como Alan Greenspan (1997) também tem opinado sobre o assunto. As posições oficiais tem sido de deixar acontecer, pelo menos no primeiro instante. Como meios de pagamento afetam a base monetária de um país, e a base monetária é controlada pelos bancos centrais dos países, que tende a ter uma política monetária alinhada com as definições oficiais, hoje as posições oficiais são de cuidadosa vigilância (Figura 24-8/8).

Como há qualquer instante governos podem impor restrições à operação de meios de pagamento eletrônico, um sistema

diferente do adotado pela empresa alvo poderá virar padrão, o que leva ao risco de perda de parte do investimento realizado pela empresa. Essa hipótese faz com que o mercado principal não adote meios de pagamento eletrônico.

#### ***2.1.7. Insegurança do sistema***

A pesquisa indicou que os sistemas de meios de pagamento eletrônico tem pouco retorno dos clientes para saber seus problemas. Isso indica que não há um histórico mostrando segurança dos meios de pagamento eletrônicos.

Ocorrem ataques com sucesso em sistemas “seguros”. Vários casos já foram relatados por diversos meios, como HAFNER e MARKOFF (1995), MARTIN (1996), Folha de S.Paulo (1999) e CREED (2000).

Como indicado na pesquisa, e na árvore lógica de realidade atual o público com perfil conservador não entende ataques nem planeja defesa.

Portanto o mercado principal, não sente segurança no sistema. A falta de segurança é traduzida como risco de perder dinheiro, e com isso os meios de pagamento eletrônico não são adotados (Figura 24–7/8).

#### ***2.1.8. Processo de Desenvolvimento do Produto***

Segundo SCHULMEYER e MCMANUS (1999); FLORAC e CARLETON (1999) e ENGLISH e ELLIOT (1999) sistemas robustos passam por varios ciclos de melhorias. Definimos sistema robusto como aquele que não apresenta surpresas

técnicas. Segundo HORCH (1996) e TEXEL e WILLIAMS (1997) um ciclo de melhoria requer correção de problemas detectados ao longo do tempo. Como um sistema robusto não apresenta surpresas, sem que um sistema robusto e tem vários ciclos de melhorias.

A pesquisa indicou que um ciclo de melhoria aplicada pelos produtores de sistemas de meios de pagamento eletrônico levam aproximadamente 2 anos. Como sistemas de meio de pagamento eletrônico existem há não mais de cinco anos, não tem havido tempo útil para haver volume suficiente de retorno dos clientes para saber seus problemas, então sistemas MPE não são robustos.

Como o mercado principal não quer descontinuidade, então só adotam inovações, como no caso meios de pagamento eletrônico quando o sistema for robusto. Como os MPE's ainda não passaram por vários ciclos de melhoria então o mercado com perfil conservador não adota MPE's (Figura 24-7/8).

Por ainda não serem robustos, os sistemas MPE podem apresentar surpresas técnicas desagradáveis, conforme JACOBSON, CHRISTERSON, JONSSON e OVERGAARD (1992) e ZAHRAN (1998). Como o mercado principal não quer descontinuidade que traz riscos, podemos concluir que, conforme constatado na pesquisa, o público com perfil inovador é avesso à risco. Levando em conta os pontos acima, e o fato constatado em pesquisa de que o integrador de sistemas é o agente apropriado para resolver problemas pode ser, concluído que o mercado principal poderia adotar MPE não robusto apenas com auxílio de integrador. Na

pesquisa com os produtores de MPE foi identificado que não existem integradores de sistema em quantidade suficiente para atender o público com perfil conservador para MPE. Considerando as observações acima, pode ser dito que o mercado principal não adota sistemas de meio de pagamento eletrônico (Figura 24-5/8).

### **2.1.9. Efeito das manchetes da grande mídia**

A literatura da grande mídia não detalha o suficiente nem aborda assuntos com a devida amplitude, conforme análises, entre outros, de PARENTI (1996); HALLORAN, LINNGEE e HAMELINK (1994); e CORNER (1999) .

O público do mercado principal é avesso a novidades que causem grandes mudanças, como identificado na pesquisa, pois não sabem lidar com descontínuidades. Como o assunto da grande mídia não tem grande amplitude e nem profundidade, o público com perfil conservador não cria barreiras contra a grande mídia. A grande mídia tem uma grande distribuição, então o público do mercado principal é atingido pela grande mídia.

A literatura especializada trata do assunto MPE de maneira hermética para o público do mercado principal. Como esse público é avesso à novidades que causem grande mudanças, então, o esse público não pesquisa literatura especializada em MPE, conforme foi constatado pela pesquisa. Dessa forma o mercado principal é atingido somente pela grande mídia. Como a grande mídia divulga apenas fatos pontuais, sem uma abordagem sistêmica, então, o mercado principal interpreta as notícias da mídia como desestimulantes para a adoção de MPE.

Essa interpretação dos fatos divulgados pela grande mídia, faz com que MPE's ainda não tenham despertado interesse do público do mercado principal. Isso faz com que poucas pessoas desse mercado compreendam sistemas MPE na sua totalidade. Como poucos, ou nenhum resultado confiável



sobre desempenho e aplicações de MPE são divulgados, como constatou a pesquisa, podem ser entendido o porque do mercado principal ficar inseguro quanto à adoção de sistemas MPE, em relação aos aspectos técnicos do resultado. Como esse público é avesso à risco, então o mercado principal não adotará sistemas de MPE.

### **3. A Causa–Raiz dos Efeitos–Indesejáveis**

As várias conclusões convergem para a entidade 29 (Figura 24–1/8) que declara “o mercado principal não adota MPE”. Analisando as entidades de entrada da árvore de realidade atual composta pela Figura 24–(1/8 até 8/8) pode ser concluído que a entidade 1 que declara “o mercado principal não quer descontinuidade” é a causa de todas as demais, inclusive as entidades de números 16, 18, 19, 22, 12, 25, 2, 26, 13 e 28 da Figura 24–1/8, que são os efeitos indesejáveis. Assim pode ser concluído que 1 é a causa–raiz procurada.

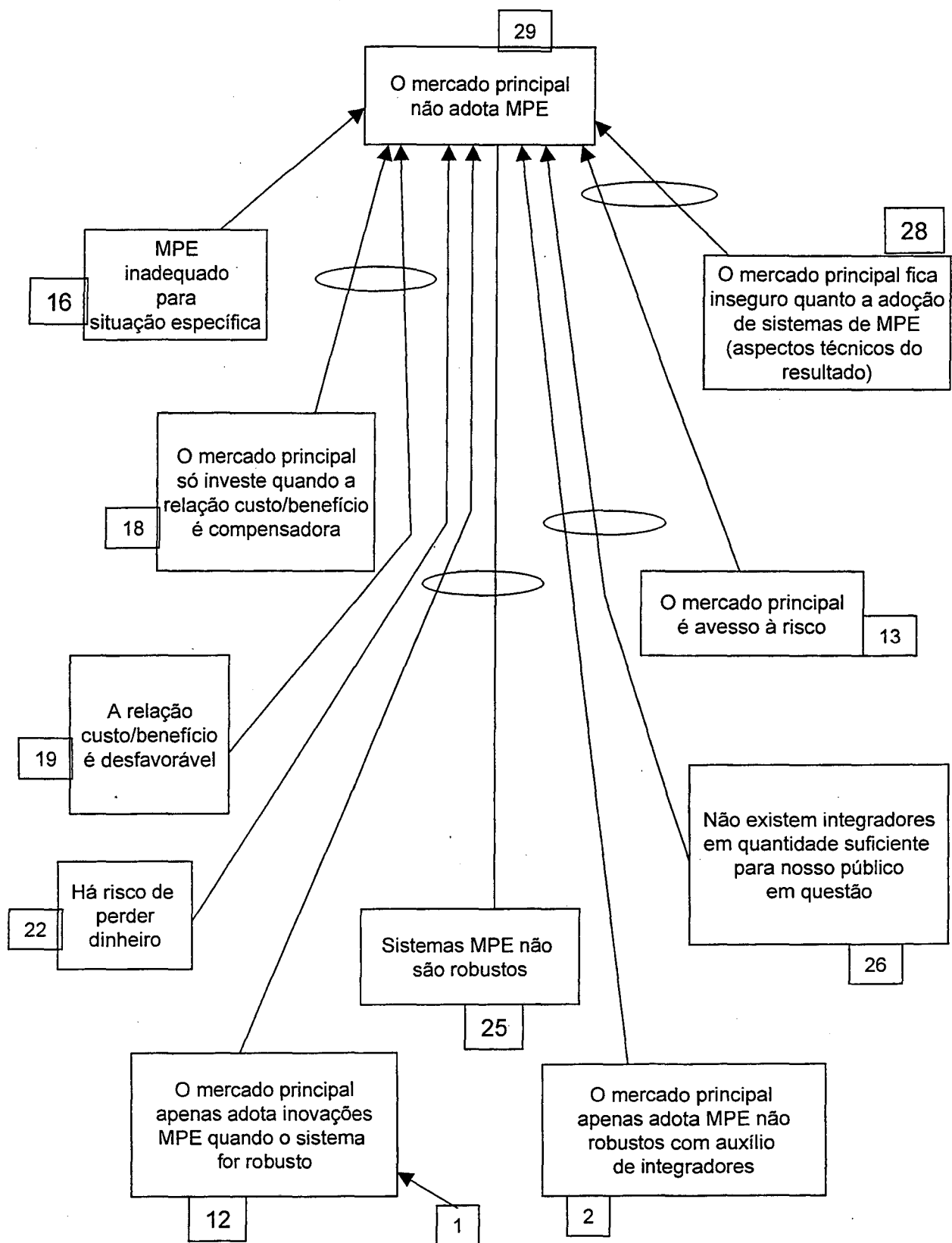


Figura 24 : Árvore da Realidade Atual 1/8

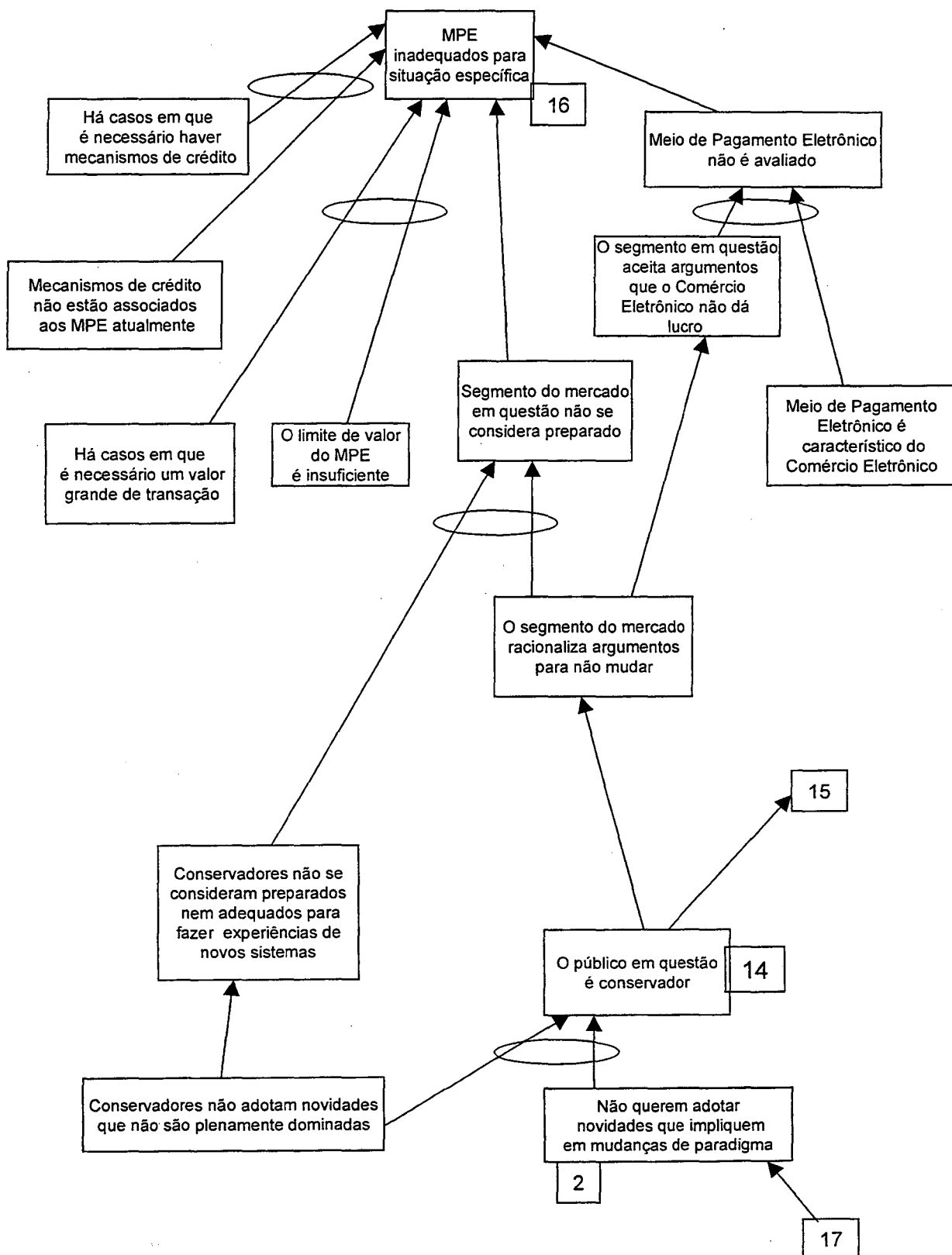


Figura 24 : Árvore da Realidade Atual 2/8

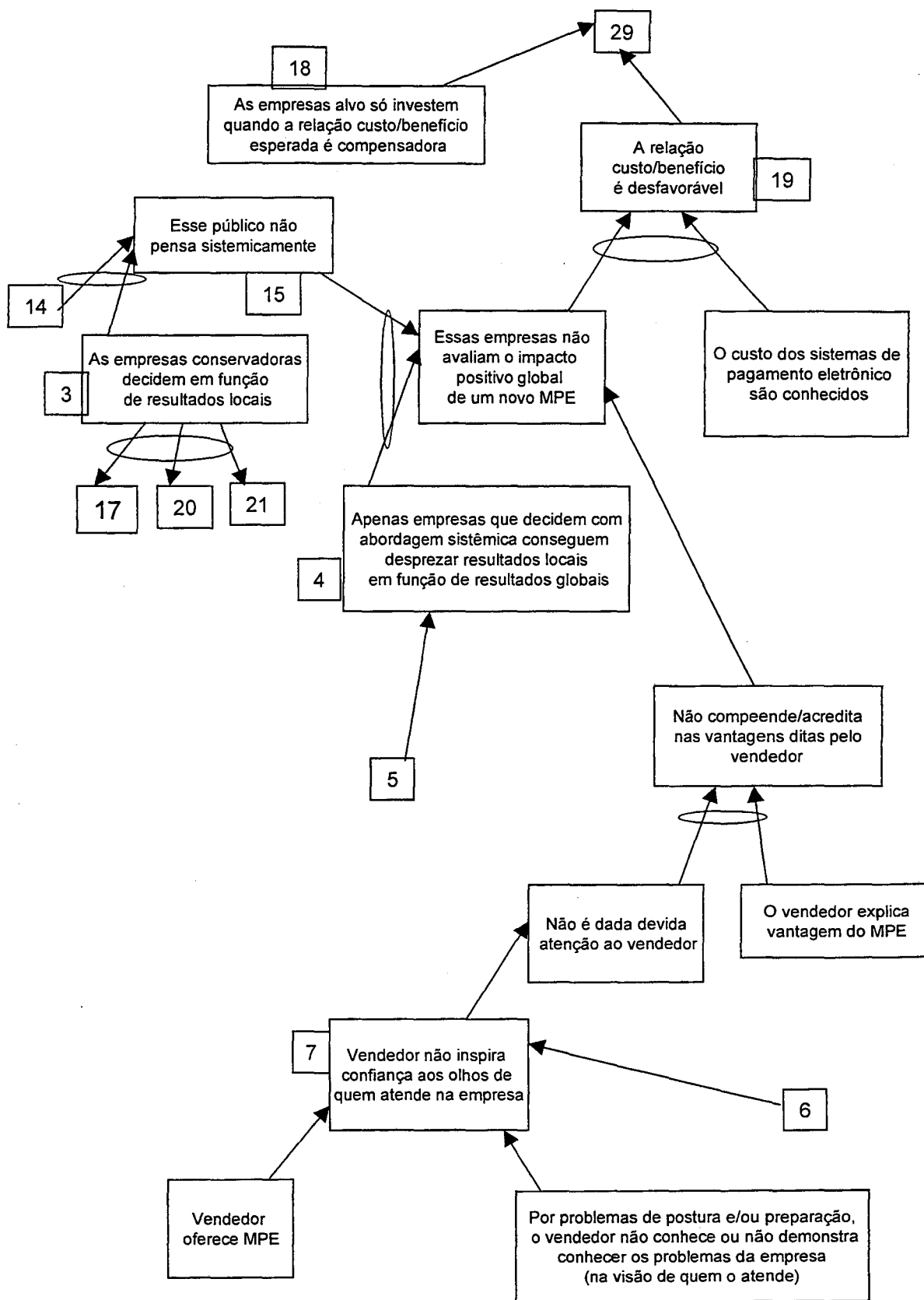


Figura 24 : Árvore da Realidade Atual 3/8

309

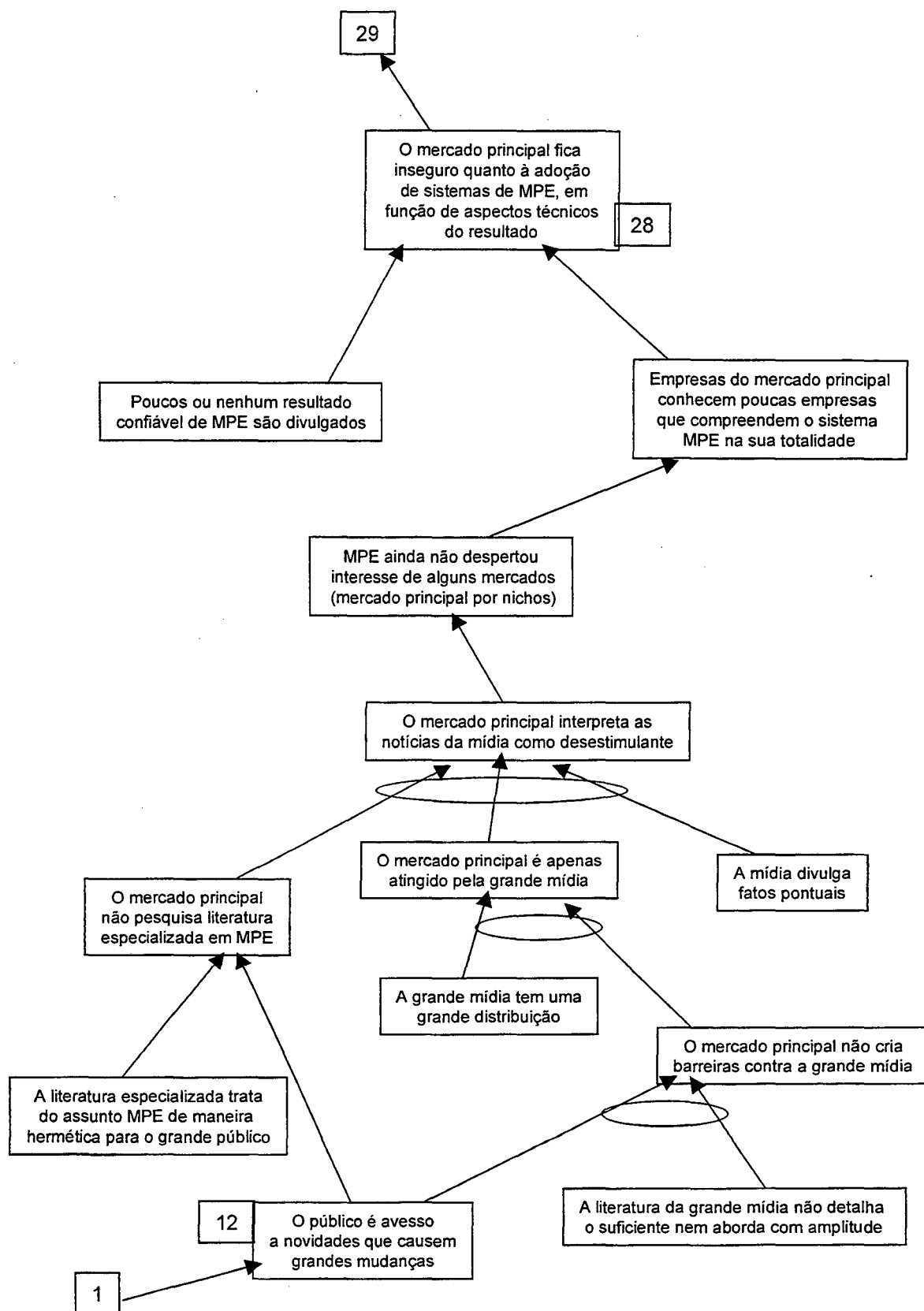


Figura 24 : Árvore da Realidade Atual 5/8

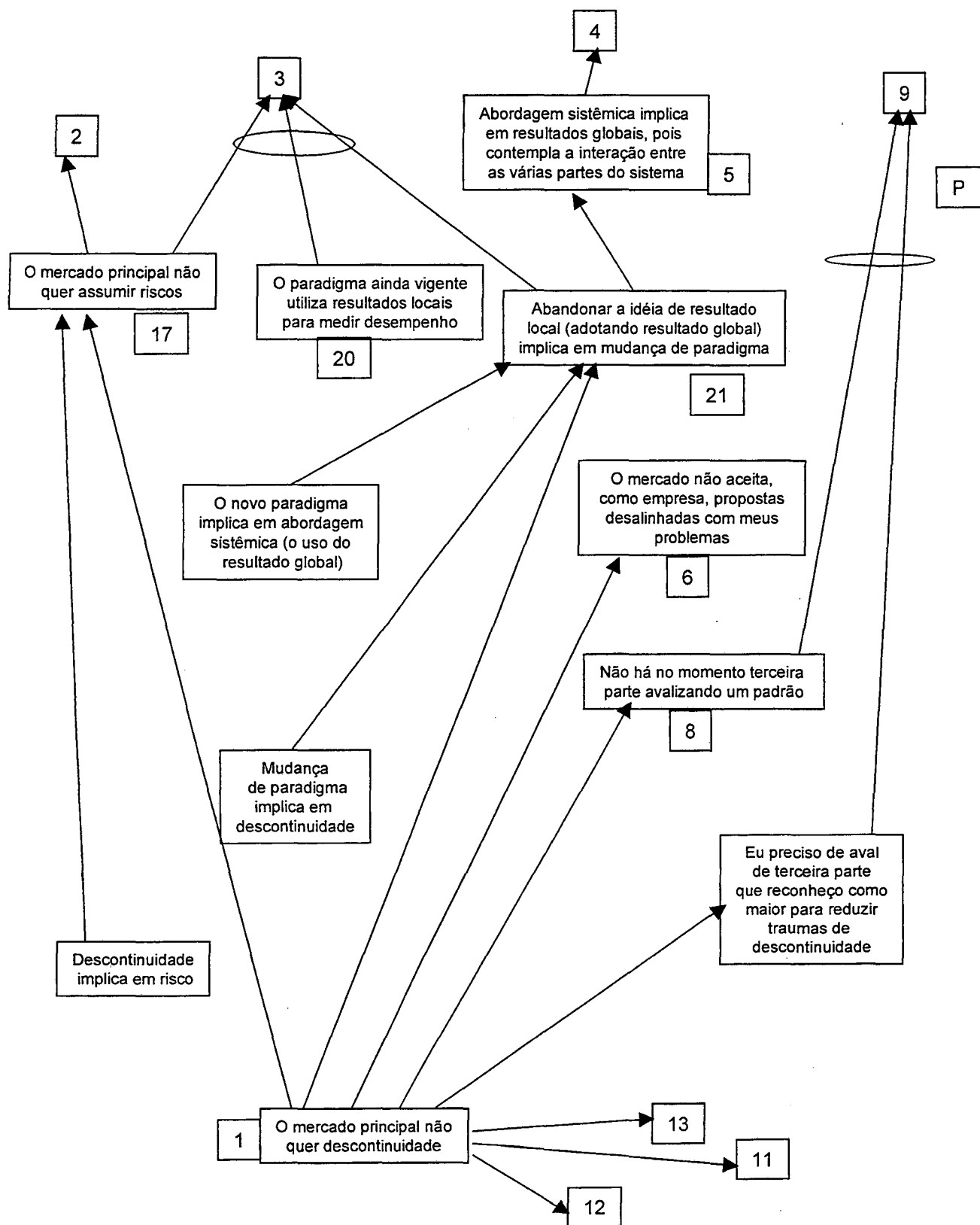


Figura 24 : Árvore da Realidade Atual 6/8





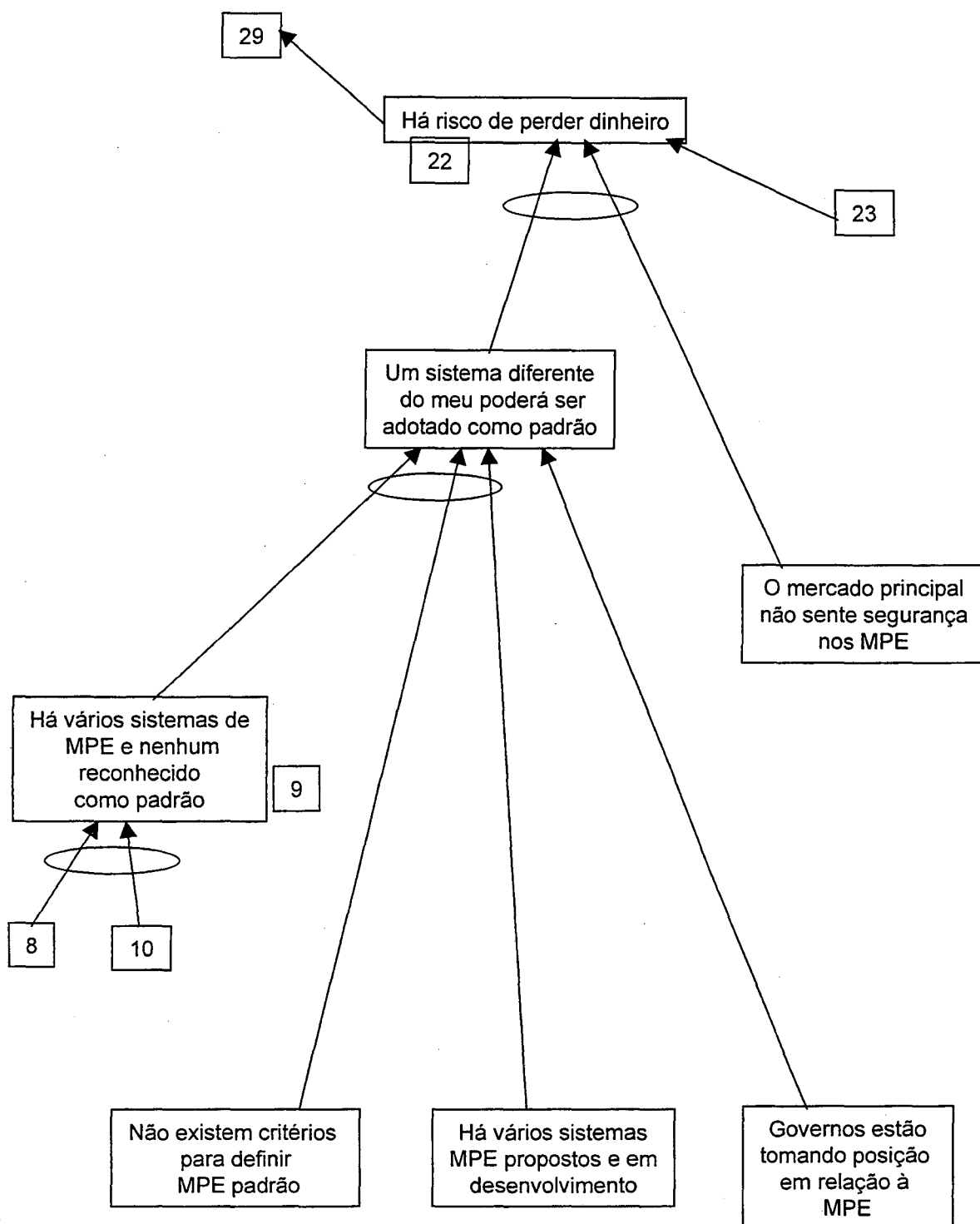


Figura 24 : Árvore da Realidade Atual 8/8

#### **4. Quebrando barreiras**

Os diversos pontos levantados na pesquisa foram avaliados pela metodologia sistêmica, através de montagem da árvore de realidade atual, permitindo entender o encadeamento de processos que levam à não adoção pelo mercado principal dos MPE's.

Acompanhando a montagem da árvore, pode ser visto que o grande público é avesso à descontinuidade, à qualquer alteração no *status quo* que os afete. A partir desse levantamento metodológico, será proposto um o processo de como atingir o nosso objetivo, isto é, como desenvolver atividades mercadológicas para que o público que estudado, a primeira maioria, adote o MPE em questão.

### **XIII. Elaboração das Ações Necessárias**

Existe uma situação de equilíbrio indesejável a ser rompida, pois se nada ocorrer, o público alvo não adota o MPE pela causa já apontada.

#### **1. Entendendo o conflito**

O que se quer provocar é que o público do mercado principal aceite uma descontinuidade em questão, o oposto da causa raiz identificada anteriormente. isto é, “empresas em questão aceitam descontinuidade”.

Para empresas aceitarem descontinuidade podem ser colocadas como condições necessárias, que elas devem aproveitar as vantagens da descontinuidade e ao mesmo tempo não enfrentar desafios. Para aproveitar as vantagens do MPE, as empresas alvo devem adotá-la. Por outro lado para não enfrentar desafios, as empresas não devem adotar MPE. O conflito fica caracterizado. Resumindo, para que as empresas-alvo aceitem descontinuidade elas devem adotar MPE para aproveitar suas vantagens, mas por outro lado, não devem adotar MPE para aproveitar evitar enfrentar desafios. Como sair do conflito ? GOLDRATT (1990a) , advoga que se identificar pressupostos que embasam qualquer das afirmações acima, basta encontrar uma injeção (ação que muda a realidade) que questiona o pressuposto, que o conflito se desfaz. Assim, se o público-alvo for abordado de maneira que não aparente desafio, ou mesmo que o estimule, fica desfeita a afirmativa que para não enfrentar desafios o público não deve adotar MPE.

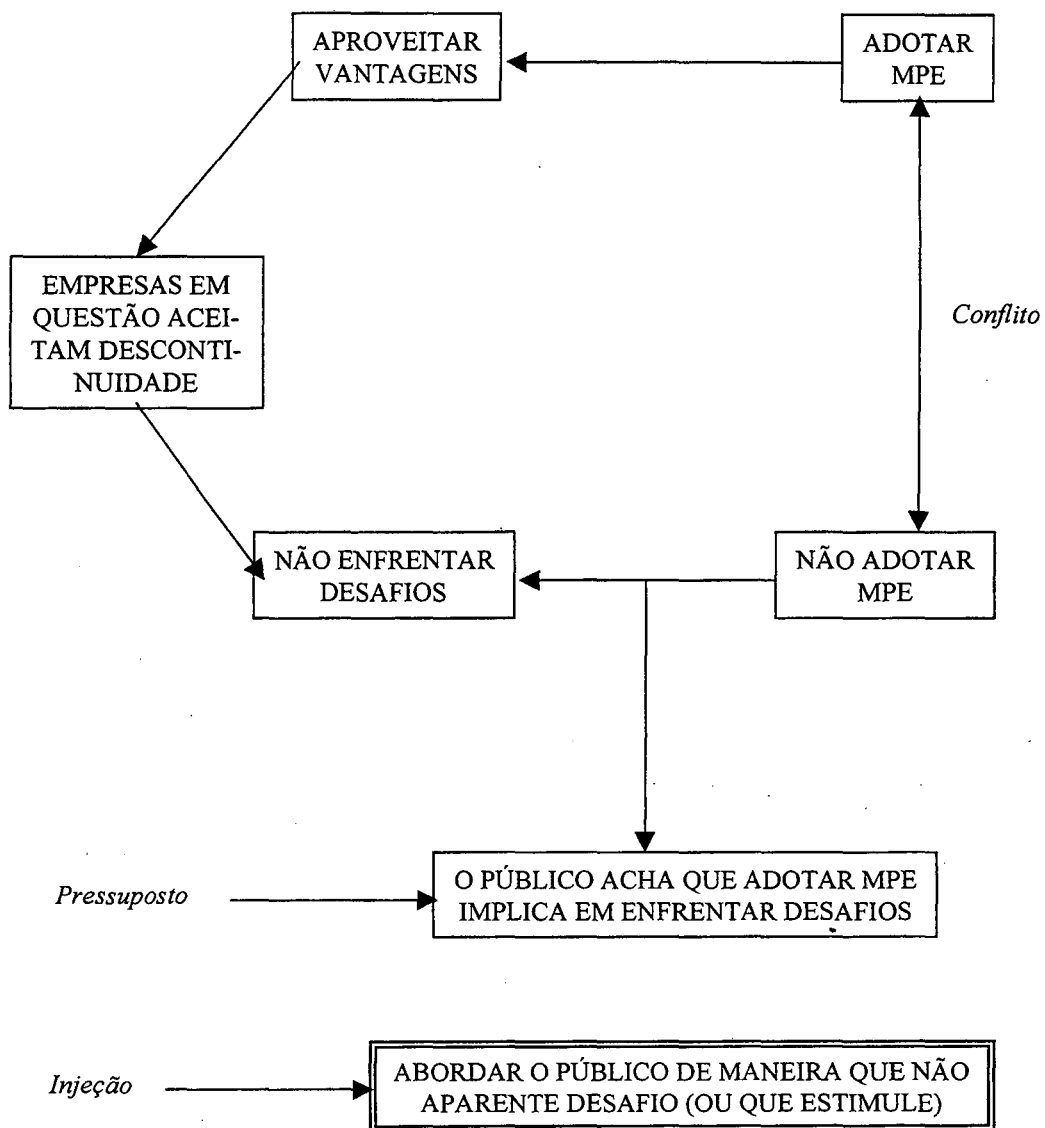


Figura 25 : Diagrama de Conflitos

## **2. Resolvendo o conflito**

Abordar o público do mercado principal de maneira que não aparente desafio, ou que estimule uma situação de desafio é a ação mobilizadora a ser empreendida.

A partir dessa injeção no sistema, e da análise sistêmica desenvolvida, com base na pesquisa de campo e bibliográfica, foi estruturado um encadeamento de passos para levar o público com perfil conservador do mercado principal a adotar o MPE em questão.

## **3. Análise das etapas para Provocar a adoção de MPE pelo mercado principal**

Foram identificadas várias objeções junto ao mercado com perfil mais conservador, a primeira maioria. O conjunto de etapas a seguir neutralizarão essas barreiras, e permitirão levar esse público a adotar o MPE em questão.

O encadeamento lógico com relação de causa e efeito das várias ações que seguem está mostrada na árvore de realidade futura (Figura 26–1/6; 2/6; 3/6; 4/6; 5/6; 6/6).

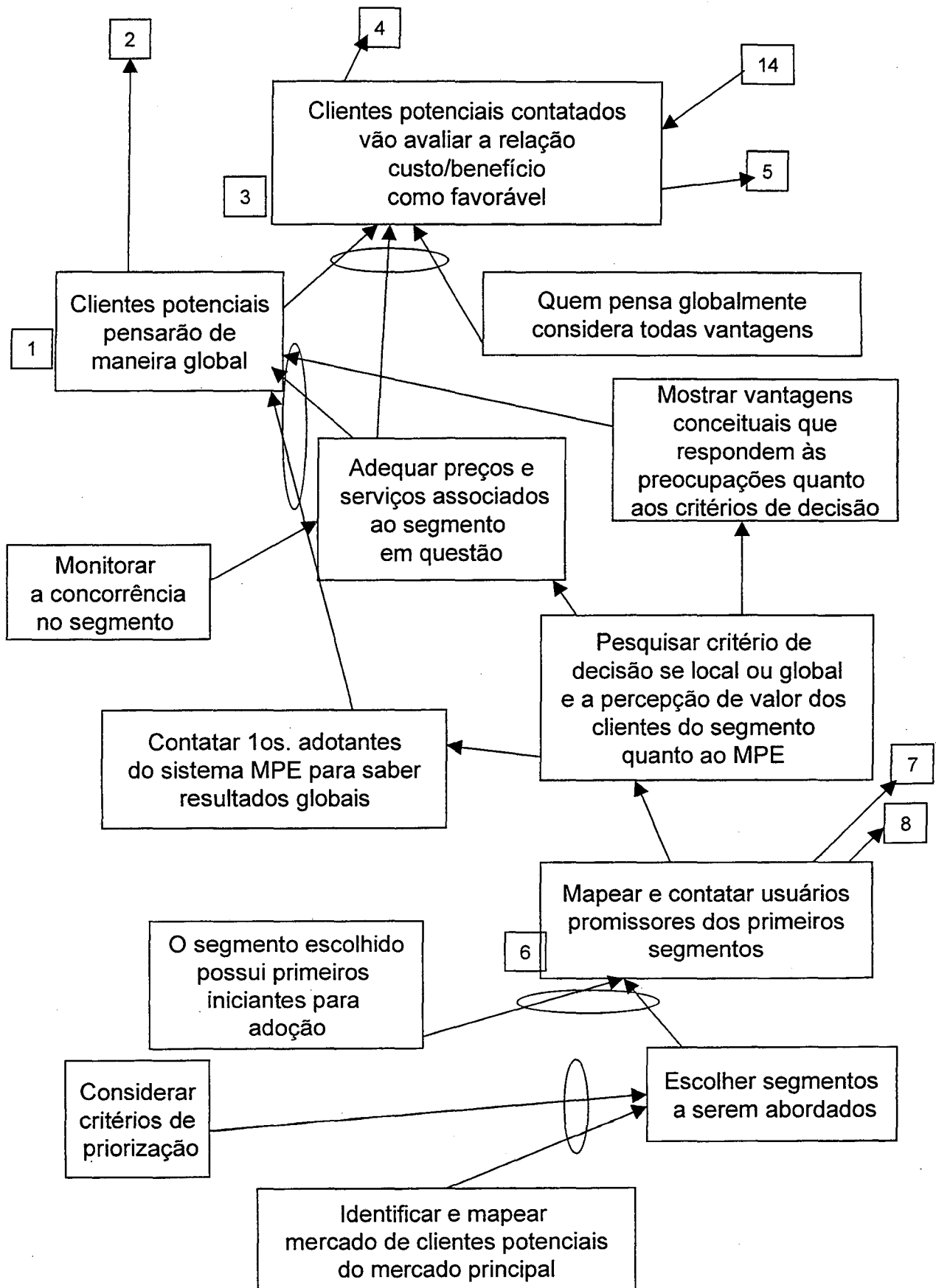


Figura 26 :Árvore da Realidade Futura 1/6









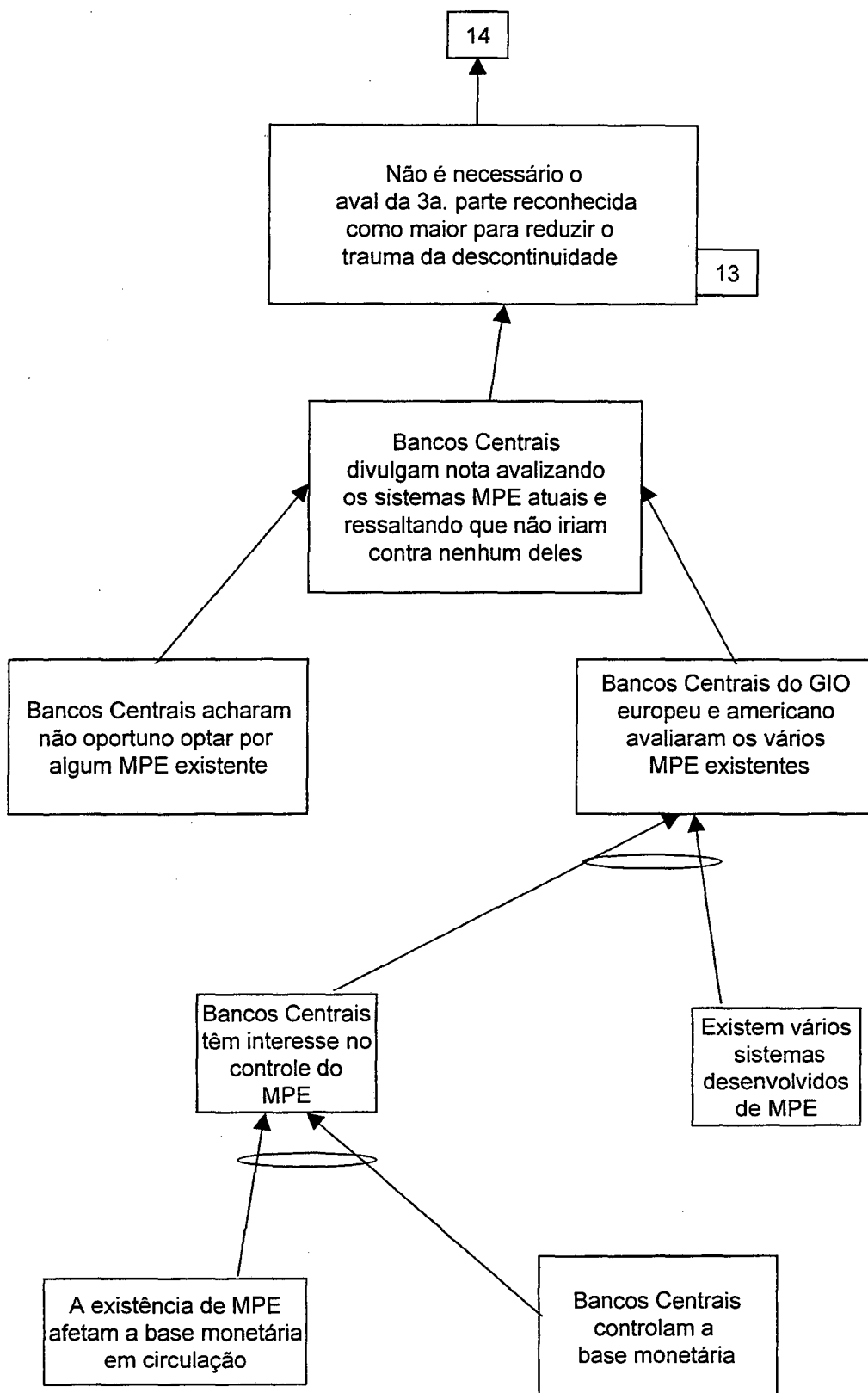


Figura 26 :Árvore da Realidade Futura 5/6

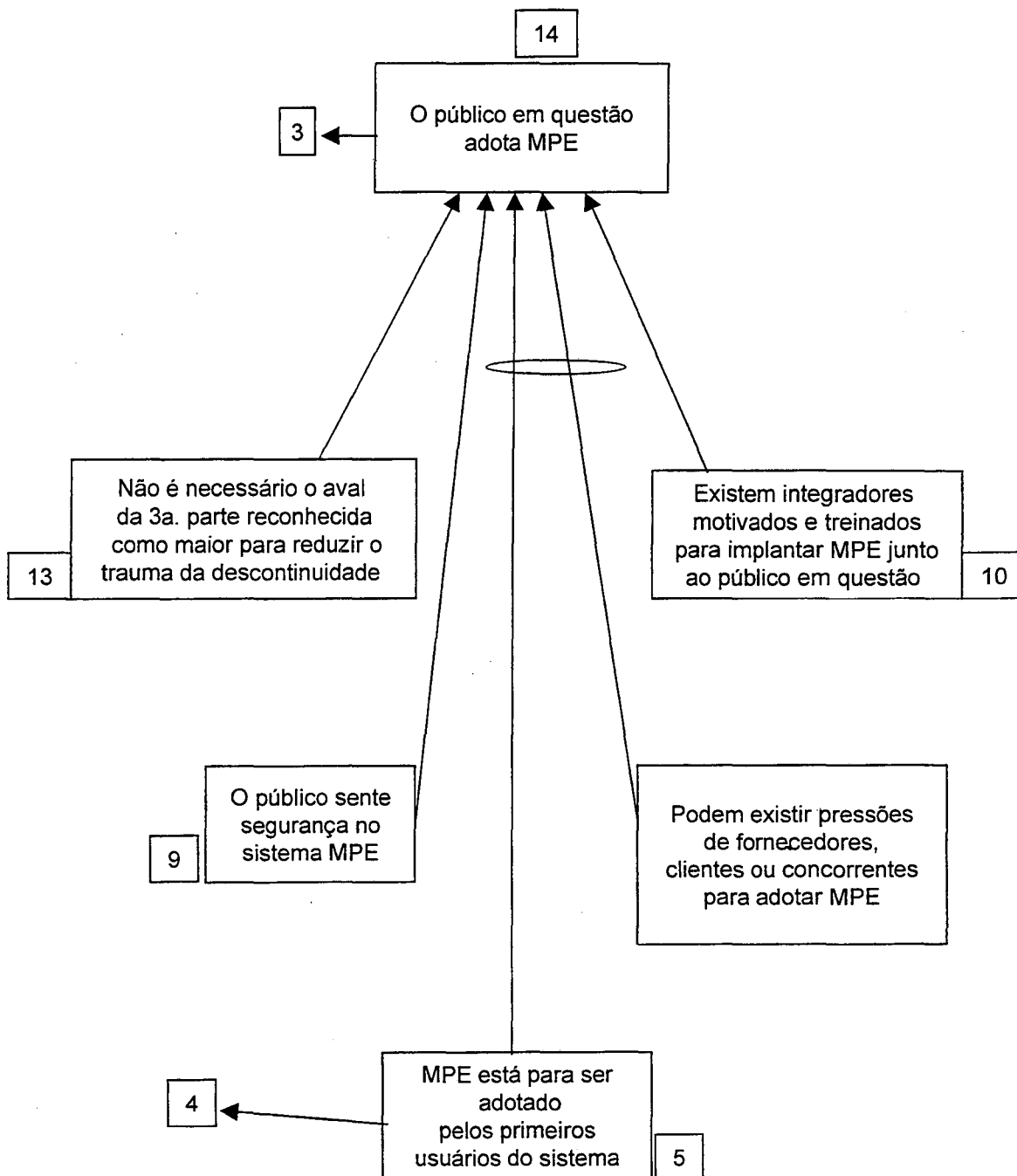


Figura 26 :Árvore da Realidade Futura 6/6

### ***3.1. Em relação as atividades das autoridades monetárias internacionais***

Bancos Centrais controlam a base monetária de países. A existência de meios de pagamento eletrônico afetam a base monetária em circulação. Dessa forma os Bancos Centrais tem interesse no controle dos meios de pagamento eletrônicos (Figura 26-5/6).

Existem vários sistemas desenvolvidos e outros propostos, de meios de pagamento eletrônico. Os Bancos Centrais europeus e norte-americano, avaliaram os vários MPE existentes. Bancos Centrais acharam não oportuno no momento optar por algum MPE existente, ou avalizar qualquer proposta (COMITÉ DE ECONOMIA E POLÍTICA MONETÁRIA E INDUSTRIAL DO PARLAMENTO EUROPEU, 1998; G-10, 1997, GREENSPAN, 1997).

A nota divulgada pelos Banco Centrais, avalizou os sistemas MPE atuais e ressaltou que não iriam contra nenhum deles. Como Bancos Centrais já são reconhecidos como terceira parte, maior, não é necessário o aval de outra 3a. parte reconhecida como maior para reduzir o trauma da descontinuidade. Isso leva o público do mercado principal que se preocupava com a possível intervenção de autoridades monetárias internacionais a adotar MPE.

### ***3.2. Provocando a avaliação favorável da relação custo / benefício por parte dos clientes***

Identificar e mapear o mercado de clientes potenciais e definir critérios de priorização para os diferentes segmentos dos clientes potenciais, isso permitirá segmentar o mercado e definir melhor o alvo (Figura 26-1/6).

As técnicas de segmentação de mercado constituem hoje a base da formulação das estratégias de marketing e de vendas. Servem,

também para a alocação de recursos para cada segmento importante de mercado (COBRA, 1994)

Aplicando os critérios de priorização no mercado identificado, podem ser escolhidos os segmentos a serem abordados e para ele devem ser mapeados os usuários promissores dos primeiros segmentos.

Para estes usuários, pesquisar o critério de decisão se local ou global e a percepção de valor dos clientes do segmento quanto ao MPE.

Pesquisando junto aos primeiros adotantes de MPE, inclusive de sistemas concorrentes, devem ser levantados os resultados globais obtidos, assim como monitorar a concorrência de outros MPE's no segmento.

Esse monitoramento e a pesquisa dos critérios de decisão dos clientes potenciais do segmento, permitirão adequar os preços e serviços associados ao segmento em questão.

A pesquisa dos critérios de decisão, permitem elaborar vantagens conceituais que respondam às preocupações sob a ótica dos critérios de decisão do público alvo.

Três conclusões contribuirão para que os clientes potenciais pensem de maneira global em relação ao MPE. A primeira delas decorre do levantamento dos resultados globais levantados junto aos primeiros adotantes dos sistemas MPE; A segunda é associada com as vantagens conceituais elaboradas, que respondam às preocupações quanto aos critérios de decisão; a terceira conclusão tem a ver com os preços e serviços associados adequados ao segmento em questão.

Pensando globalmente, irão avaliar todas as vantagens, com os preços e serviços associados adequados ao público em questão; os

clientes potenciais contatados irão avaliar a relação custo / benefício como favorável.

### ***3.3. Garantir a existência de integradores treinados e motivados para implantar MPE junto ao público em questão***

Mapear usuários iniciantes e pesquisar como melhorar o sistema MPE para o segmento escolhido, assim como problemas encontrados (Figura 26–3/6).

O público em em questão é numeroso e para lidar com público numeroso é necessário uma estrutura que deverá ser criada. Essa estrutura irá solicitar informações dos usuários iniciais de MPE, inclusive levantar problemas.

Uma vez trabalhados os problemas levantados, devem ser introduzidas as soluções desses problemas nos sistemas existentes. Na medida em que problemas são levantados e soluções trabalhadas, ocorrem ciclos de melhorias.

Após vários desse ciclo os sistemas MPE ficam mais robustos e adequados para o público em questão.

Como as necessidades dos consumidores não são estáticas, ao contrário são dinâmicas, e a ação do meio ambiente pode tornar o produto ou serviço de uma empresa obsoleto, o jeito é adaptar-se para fazer frente às condições que se alteram (COBRA, 1989).

Melhoramentos obtidos são enviados aos usuários gratuitamente, assim como para integradores . São feitas divulgações ao mercado que será abordado.

Como os melhoramentos são enviados sem custo, os usuários de MPE retornam com entusiasmo informações sobre o desempenho de MPE, o que reforça o *loop*, e permite uma base maior para trabalhar melhoramentos.

O público em questão é muito numeroso e, conforme identificado, necessita de integradores para implantar MPE. Como já estão sendo mapeados usuários promissores dos primeiros segmentos; identificar o que os clientes potenciais, do público em questão, esperam de um integrador.

A partir da pesquisa, identificar empresas com o perfil desejado para serem integradores. Fazer um programa de parcerias com integradores é o próximo passo, para em seguida treina-los objetivando o público em questão.

Com as providências acima existirão integradores motivados e treinados para implantar MPE junto ao público em questão. Os melhoramentos obtidos que são enviados gratuitamente aos integradores, ajudam a mantê-los motivados.

Com o auxílio desse integradores, a parcela da primeira maioria que se preocupava com essa questão passa a adotar MPE.

### ***3.4. Provocando o desejo de adoção de MPE por parte do mercado principal***

A partir do mapeamento dos usuários promissores dos primeiros segmentos, devem ser pesquisados temores e preocupações específicas dos usuários potenciais do segmento escolhido.

Temores e preocupações específicas são aquelas que não estão abrangidas nas entidades da árvore lógica desenvolvida a partir dos



problemas identificados nessa pesquisa, pois aquelas foram consequências das preocupações identificadas nas pesquisas feitas enquanto que as específicas devem ainda ser levantadas para cada segmento (Figura 26–1/6).

Para esses problemas específicos, deve haver avaliação sistêmica, construindo uma árvore de realidade atual tal qual feito na Figura 24.

A partir da árvore de realidade atual, identificar uma ação mobilizadora através de diagrama de conflitos (Figura 25). Construir a árvore de realidade futura. Conforme feito na Figura 26.

Transmitir as conclusões aos usuários potenciais. Como conclusões bem fundamentadas transmitem confiança, o público em questão encara sem temor e com confiança, a ideia de adoção de MPE, uma vez que preocupações dissiparam.

O público apesar de conservador ficará imunizado contra afirmações pontuais como “comércio eletrônico não é lucrativo”, se abrindo para mudança de paradigma e informações sem grande amplitude da mídia (Figura 26–4/6).

Como a mídia bombardeia continuamente o público em questão com notícias jornalísticas sem grande amplitude. Então o público alvo interpreta criticamente as notícias da grande mídia e fica interessado em obter mais detalhes.

Quando oferecida literatura especializada acessível e adaptada ao segmento escolhido para o público em questão, o público aceita discutir avaliação de MPE.

Neste momento o sistema MPE é proposto para o público em questão, já tendo recebido diversos melhoramentos. O MPE é avaliado pelos clientes potenciais contatados. A relação custo /

benefício sendo favorável, irá criar uma propensão a adoção de MPE pela grande maioria.

Com essa propensão, e a existência de algum fator de pressão como de fornecedores, clientes ou concorrentes, o mercado principal passa a adotar MPE.

### ***3.5. Fazer com que o público em questão não tenha medo de ataques de segurança do sistema***

Como os clientes potenciais contatados irão avaliar a relação custo / benefício como favorável, e como o MPE está para ser implementado pelos primeiros adotantes do segmento, o fato de existirem ataques possíveis contra o sistema, criará a propensão por parte do público para entender os ataques e processos de defesa.

Neste momento são enviadas informações referentes à questões de segurança ao usuários potenciais.

O público em questão entende os ataques possíveis contra o sistema e seus efeitos. Como este público entende a relação de causa-efeito entre as partes de um sistema MPE, então, o público planeja defesa contra ataques. Sabendo avaliar as consequências financeiras para as defesas planejadas, então o público sente confiança no sistema MPE.

Com isso MPE é adotado pelo mercado principal.

#### **4. Encadeamento das Ações Necessárias**

O conjunto de entidades da árvore de realidade futura, mostrado nas Figuras 26–(1/6, 2/6, 3/6, 4/6 e 5/6) levarão à finalização mostrada na Figura 26–6/6, em que o público em questão adote o MPE.

Um fator muito importante é a realimentação positiva que está sendo feita da entidade 5 para 4, 11 para 12, 11 para 10, 14 para 3 a entidade “usuários de MPE retornam com entusiasmo informação sobre o desempenho de MPE” para “Pesquisar como melhorar o sistema MPE para o público em questão” e finalmente da entidade 1 para 3.

A natureza da relação de causa e efeito garante a adoção do MPE caso as várias ações indicadas na árvore de realidade futura sejam tomadas nas condições descritas, conforme apresentado na metodologia proposta.

## XIV. Metodologia Proposta

Com base nas pesquisas realizadas e análises desenvolvidas, está sendo proposta uma metodologia para abordar o mercado principal de MPEs, composta por 12 passos encadeados. Essa proposta foi desenvolvida para meio de pagamento eletrônico, visando atingir especificamente o público com perfil mais conservador, isto é a primeira maioria do mercado ou o mercado principal, para um produto específico.

Essa é uma metodologia ainda não testada, e os produtos continuam sendo pouco utilizados. No entanto ela irá contribuir como um passo para o desenvolvimento de uma metodologia de causa-efeito para produtos com inovação tecnológica.

Existem no momento duas teorias que tratam da adoção de tecnologia. A primeira compreende os modelos desenvolvidos por Rogers para descrever o processo de adoção de tecnologia podem ser entendidos, como fundamentais para definir boas nomenclaturas e caracterização dos diversos perfis. A segunda teoria de ator-rede (ANT) define o funcionamento de uma rede de atores a partir dos relacionamentos entre as partes, identificadas a partir de um tecnograma e um sociograma. Essa teoria ainda não permite entender os motivos do funcionamento, ou não funcionamento ideal do sistema. Dessa forma não há como saber aonde atuar para obter os resultados esperados.

A metodologia de trabalho proposta, *cadeia de dominós crescentes*, evoluindo a partir das teorias anteriores e das relações de causa-efeito identificadas em pesquisa, e testadas logicamente através da teoria das restrições, apresenta uma sequencia de etapas para atingir o mercado principal, um público bastante grande, com perfil mais conservador, e que justifica economicamente a existência de MPE. Esta metodologia visa atingir inicialmente os primeiros iniciantes do grande público pertencentes a um segmento escolhido. Na

medida em que o segmento vai sendo conquistado, a realimentação das informações se incumbirá de reforçar e acelerar o processo de adoção iniciado. Virá em seguida o segmento seguinte e assim por diante. Cada vez que determinado segmento inicia, é como se fosse uma sequência de dominós caindo, empurrados pelos anteriores. Cada segmento novo inicia com dominós maiores com o sistema de MPE mais conhecido e mais robusto.

## **1. Objetivo da Metodologia Proposta**

Definir etapas sincronizadas de trabalho para provocar a adoção de um MPE específico por parte do mercado principal.

## **2. Sequência de Etapas**

### ***2.1. Mapear Mercado***

Mapear o mercado como um todo. Esse mapeamento deve levar em consideração os usuários atuais e potenciais.

### ***2.2. Identificar e Classificar os Segmentos de Mercado***

O mercado mapeado será segmentado por área de atuação.

Esses segmentos serão classificados por atratividade. A atratividade é uma função da relação custo / benefício em abordá-los. Deve ser levada em consideração a facilidade de acesso à esse mercado, os custos, e o resultado potencial em abordá-lo.

Os nichos classificados serão identificados, com nomes e endereços.

### **2.3. 3– Abordar Clientes**

a) abordar os pioneiros que já utilizam meios de pagamento eletrônico (que não devem ser muitos, inclusive alguns utilizando o sistema de concorrentes), para pesquisar o grau de satisfação, especialmente as experiências negativas que tiveram, os problemas e dificuldades que vem tendo, e na medida do possível os resultados que vem obtendo com os sistemas MPE.

b) abordar os segmentos escolhidos para recolher preocupações, receios, desconfortos e bloqueios que inibem o grande público de aprofundar o entendimento de MPE, assim como seus desejos e necessidades em relação ao MPE

b1) classificar as preocupações coletadas de acordo com aquelas já identificadas no modelo analítico sistêmico, a árvore de realidade atual. No caso de haver algum dos receios não classificados, considerá-los em separado; estes serão os de preocupação específica do segmento.

### **2.4. Adequar o Produto**

A partir da pesquisa com 3a e 3b, o produto deve ser adequado ao segmento escolhido levando em consideração as características, necessidades e desejos deste público, além das soluções das preocupações.

### **2.5. Identificar Valor para Cliente**

Monitorar a concorrência e identificar a percepção de valor que o segmento em questão tem do sistema MPE e adequar o preço para o público alvo.

## ***2.6. Elaborar Material***

A partir do levantamento realizado em 3b e 3b1, elaborar material em linguagem atrativa e compreensível pelo primeira grande maioria do mercado. Esse material deve demonstrar e destacar a robustez do sistema MPE, as vantagens em relação aos custos envolvidos e considerar as preocupações específicas, assim como resultados obtidos dos pioneiros e primeiros usuários eventuais.

## ***2.7. Estabelecer Canal de Comunicação***

Estabelecer canal de comunicação para divulgação do material entre os membros do segmento escolhido, visando atingir os primeiros usuários da primeira maioria deste segmento.

## ***2.8. Monitorar Segurança***

Monitorar constantemente ataques à sistemas de MPE e articular estratégias de defesa mostrando a vigilância e o cuidado de preservar a segurança do sistema MPE em questão. Estas informações serão introduzidas no canal de comunicação em 2.7.

## ***2.9. Monitorar Autoridades***

Monitorar continuamente as atividades das autoridades monetárias internacionais com relação a sistemas MPE e introduzir as informações trabalhadas para o público alvo no canal de comunicação em 2.7.

## ***2.10. Formar Integradores***

Formar integradores em quantidade adequada em função do número de usuários potenciais identificados e criar relação de parceria com

eles, tendo em vista aumentar a exposição do sistema MPE em questão ao público da primeira maioria.

### ***2.11. Realimentar Positivamente***

Formar diferentes loops de realimentação positiva de informações colhidas:

- dos usuários,
- dos integradores,
- do contínuo desenvolvimento do produto cada vez mais robusto,
- das vantagens técnicas,
- de benefícios em relação a custos,
- de defesas desenvolvidas aos ataques que ameaçam a segurança do sistema,
- das vantagens do sistema proposto em relação a concorrência,

aos usuários atuais, aos integradores parceiros e ao público potencial da primeira maioria.

### ***2.12. Identificar Próximos Segmentos para Abordar***

Conforme disponibilidade de recursos, identificar os próximos segmentos a serem abordados do grande público, seguindo os passos acima descritos.



## **XV. Conclusão**

O presente trabalho estudou o problema de adoção de novas tecnologias, especificamente de meios de pagamento eletrônico, utilizados em sistemas de comércio eletrônico, através da Internet.

Uma pesquisa bibliográfica contextualizou o ambiente da Internet e do Comércio Eletrônico, apresentando as implicações do sistema no atual estágio. Foi investigado que o meio de pagamento eletrônico é uma das restrições para o bom desenvolvimento do comércio eletrônico.

Foi realizado uma pesquisa bastante abrangente das propostas de sistemas de meio de pagamento eletrônico, operacionais ou na forma de proposta. Os sistemas foram analisados em função das suas características, requisitos e perfis, técnicos e economicos. Essa análise que abrangeu também as atividades dos órgãos certificadores e projetos de interfaces de meios de pagamentos, permite ter uma visão do ambiente competitivo aonde esses produtos concorrem.

Foram analisadas as duas diferentes teorias para adoção de inovações, a teoria de difusão de inovações e a teoria de translação. A teoria de difusão de inovações foi desenvolvida para indivíduos. Para adequar sua aplicação ao ambiente das organizações, foi utilizada a teoria de perfil organizacional.

Com base nesses modelos foram desenvolvidas pesquisas de campo para compreender melhor o comportamento de adoção dessa nova tecnologia, o meio de pagamento eletrônico pelo mercado principal.

A pesquisa levou a formulação do modelo da “banana-split derretida” para explicar o processo de adoção de tecnologias entre o público com perfil mais inovador e o público com perfil mais conservador, o mercado principal. Esse modelo explica que empresas com perfis inovadores tendem a iniciar o processo de adoção de uma nova tecnologia após empresas com perfil mais inovador. Contudo existe um período de tempo onde existem os dois perfis adotando simultaneamente o MPE. A interpretação do problema sob a ótica desse modelo permeou a continuidade da análise.

A partir de uma abordagem sistêmica, foi avaliado o processo de restrição à adoção do meio de pagamento eletrônico pelo mercado principal e proposta uma metodologia de abordagem, “cadeia de dominos crescentes”, para promover a adoção do meio de pagamento eletrônico no mercado principal.

A metodologia de abordagem apresentada, é sustentada por uma teoria baseada em relações de causa e efeitos, e prevê a existência de situações dinâmicas de mercado, aonde não existe situação definitiva, mas soluções poderosas. A “cadeia de dominós crescentes” cria um efeito positivo derrubando objeções e provocando novas adoções de meio de pagamento eletrônico pelo mercado principal.

## XVI. Bibliografia

- [ 1 ] Abad-Peiro, J.L., Asokan, N., Steiner, M., Waidner, M., *Designing a generic payment service*, Technical Report 212ZR055, IBM Zurich Research Laboratory, <http://www.semper.org/info/212ZR055.ps.gz>, November 1996.
- [ 2 ] Ackoff, R.L., *Creating the Corporate Future*, John Wiley & Sons, 1981.
- [ 3 ] Ackoff, R.L., *Management in Small Doses*, John Wiley & Sons, 1986.
- [ 4 ] Ackoff, R.L., *The Democratic Corporation*, Oxford University Press, 1994.
- [ 5 ] Akrich, M., Latour, B., *A convenient Vocabulary for the Semiotics of Human and Nonhuman Actors in Bijker, W., Law, J. eds , Shaping Technology / Building Society Studies in Sociotechnological Change*. MIT Press, 1992.
- [ 6 ] Alderson, W., *Dynamic Marketing Behavior: A Functionalist Theory of Marketing*, Homewood, Illinois, 1965.
- [ 7 ] Allen, J.P., *The selective adoption of information systems: Assessing practically, trustworthiness and fairness*, in McMaster, T., Mumford, E., Swanson, E.B., Warboys, B. and Wastell, D. eds., *Facilitating technology transfer through partnership: Learning from practice and research*, Chapman and Hall, 1997.
- [ 8 ] Anderson, R., Manifavas, C., Sutherland, C., *Netcard – a practical electronic cash scheme*, in Cambridge Workshop on Security Protocols, 1996.
- [ 9 ] Angel, D. e Heslop, B., *The Internet Business Companion*, Addison-Wesley Publishing Company, MA, 1994.
- [ 10 ] Anonymous, *Mondex's pilot system broken*, <http://jya.com/mondex-hack.htm>, september, 1997.

- [ 11 ] Ardis, M.A., Furchtgott, D.G., *Research and development: differences are barriers to transfer*, in Levine, L. (eds) Diffusion, transfer and implementation of information technology, Elsevier Science BV, Amsterdam, 1994.
- [ 12 ] Argyris, C., *On Organizational Learning*, Blackwell Publishers, 1992.
- [ 13 ] Argyris, C., *Knowledge for Action*, Jossey-Bass, 1993.
- [ 14 ] Asokan, N., Janson, P., Steiner, Waidner, M., *Electronic Payment Systems, Technical Report 211ZR019*, IBM Zurich Research Laboratory, <http://www.semper.org/info/211ZR019.ps.gz>, 1997.
- [ 15 ] Baer, T., *Don't try this @home*, Computerworld Electronic Commerce Journal, April 29, 1996.
- [ 16 ] Barnes, D., *Identity agnostic online cash*, <http://www.c2.net/~cman/agnostic.html>, 1997.
- [ 17 ] Barnett, H.G., *Innovation: The Basis of Cultural Change*, McGraw-Hill, 1983.
- [ 18 ] Barro, K.C., *Trustbusters just don't get high tech, the industry is fluid*, Business Week August 1998.
- [ 19 ] Becker, S.W., e Whisler, T.L., 1967, *The Innovative Organization: A Selective View of Current Theory and Research*, Journal of Business, vol XL outubro 1967, in Blackwell, R.D., Innovativeness and Diffusiveness, A Marketing View, Ohio State University Press, 1984, 1967.
- [ 20 ] Bellare, T.J., Garay, J.A., Waidner, M., et al., *ikp – a family of secure electronic payment protocols*, in 1st USENIX workshop on Electronic Commerce, <http://www.zurich.ibm.ch/Technology/Security/publications/1995/ikp.ps>, July, 1995.

- [ 21 ] Bertalanffy, L., *Teoria dos Sistemas*, RJ, Ed. FGV, 1976
- [ 22 ] Berthon, P., Pitt, L.F., Watson, R.T., *The World Wide Web as an advertising medium*, Journal of Advertising Research, 1998.
- [ 23 ] Besselman, J., *Position statement on software process innovations and informal organizational networks*, in Levine, L. eds., Diffusion, transfer and implementation of information technology, Elsevier Science BV, 1994.
- [ 24 ] Bihari, T.E., Varner, M.O., *Practical issues in information technology transfer*, in Levine, L., eds., Diffusion, transfer and implementation of information technology, Elsevier Science BV, 1994.
- [ 25 ] Bijker, W. , 1994, *Of Bicycles, Bakelites and Bulbs, Toward a Theory of Sociotechnical Change*, MIT Press, 1994.
- [ 26 ] Boly, J.P., Bosselaers, A., Cramer, R., Michelsen, S., Mjolsnes, S., Muller, F., Pedersen, T., Pfitzner, B., Rooji, P., Schoenmaers, B., Schunter, M., Vallée, L., Waidner, M., *The esprit project cafe – high security digital payment systems*, Third European Symposium on Research in Computer Security, Brighton,  
[http://www.informatik.uni-hildesheim.de/FB4/Projekte/sirene/publ/BBCM1\\_94CafeEsorics.ps.gz](http://www.informatik.uni-hildesheim.de/FB4/Projekte/sirene/publ/BBCM1_94CafeEsorics.ps.gz), 1994.
- [ 27 ] Bottomore, T.B., *Between Marginalism and Marxism: The Economic Sociology of J.A. Schumpeter*, St. Martin's Press, Inc, 1992.
- [ 28 ] Bolton, T, *To modern Rock innovators, Fans and the Vast Majority*, Fifteenth Annual Macromarketing Seminar, Proceedings, 1996.
- [ 29 ] Braa, K., Sorgaard, P., *Stages and diversity in the implementation of World Wide Web and document technology*, in McMaster, T., Mumford, E., Swanson, E.B., Warboys, B. and Wastell, D. (Eds) Facilitating technology transfer through partnership: Learning from practice and research, Chapman and Hall, 1997.

- [ 30 ] Bradley, S.P., Nolan, R.L., *Sense & Respond*, Harvard Business Review, 1998.
- [ 31 ] Brands, S., *Untraceable off-line cash in wallet with observers*, in LNCS 773, *Advances in Cryptology – CRYPTO'93*, Springer Verlag, <http://www.cwi.nl/ftp/brands/crypto93.ps.Z>, 1993.
- [ 32 ] Brands, S., *Off-line cash transfer by smart cards*, in First smart card research and advanced application conference, Lille, France, <http://www.cwi.nl/ftp/brands/CS-R9455.ps.Z>, 1994.
- [ 33 ] Brands, S., *Off-line electronic cash based on secret-key certificates*, in LATIN'95, <http://www.cwi.nl/ftp/brands/latin95.ps.Z>, April 1995.
- [ 34 ] Brands, S., *Publication on electronic cash*, <http://www.cwi.nl/~brands/cash.html>, 1995b.
- [ 35 ] Brands, S., *Restrictive blinding of secret-key certificates*, in LNCS 921, *Advances in Cryptology – EUROCRYPT '95*, <http://www.cwi.nl/ftp/brands/CS-R9509.ps.Z>, 1995c.
- [ 36 ] Brown, R., *Managing the "S" Curves of Innovation*, in *Journal of Consumer Marketing*, 9(1): 61–72, 1992.
- [ 37 ] Brown, S.L., Eisenhardt, K.M., *Competing on the Edge, Strategy as Structured Chaos*, Harvard Business Review Press, 1998.
- [ 38 ] Bryant, B., Steiner, J., Kohl, J., *Kerberos Installation Notes*, DRAFT Initial Release, <ftp://aeneas.mit.edu/pub/kerberos/doc.split/installtio.ps>, 1989.
- [ 39 ] Bush, V., *As we may think*, *The Atlantic Monthly*, July, 1945.
- [ 40 ] Business Week, *The Education of Marc Andreessen*, April 13, 1998.
- [ 41 ] Business Week, *I Can't work this thing*, April 29, 1991.

- [ 42 ] Callon, M., *Society in the Making: The Study of Technology as a Tool for Sociological Analysis* in Bijker, W., Hughes, T.P., pinch, T.J. eds, *The Social Construction of Technological Systems , New Directions in the Sociology and History of Technology*, MIT Press, 1987.
  
- [ 43 ] Callon, M., *Some elements of a sociology of translation: domestication of the scallops and the fishermen of St. Brieuc Bay*, in Law, J. (ed.), *Power, Action and Belief: A New Sociology of Knowledge?*, Sociological Review Monograph, no 32, Routledge, 1986.
  
- [ 44 ] Callon, M., Latour, B. 1981, *Unscrewing the Big Leviathan: How Actors Macro-Structure Reality and How Sociologist Help Tem to do so* in Knorr-Cetina, K., Cicouvel, A.V. eds. *Advances in Social Theory and Methodology: Towards an Integration of Micro and Macro-Sociology*. Boston, MA; London. Routledge, 1986., 1981.
  
- [ 45 ] Camenisch, J., Piveteau, J.M., Stadler, M., *For anonyme payment system*, GSI 95, Springer Verlag, 1995.
  
- [ 46 ] Camp, L.J., Sirbu, M., Tygar, J.D., *Token and notational money in electronic commerce*, in Usenix Workshop on Electronic Commerce, <http://almond.srv.cs.cmu.edu/afs/cs/user/jeanc/www/usenix.html>, July 1995.
  
- [ 47 ] Camp, L.J., Sirbu, M., Tygar, J.D., *Token and notational money in electronic commerce*, in Usenix, 1995b.
  
- [ 48 ] Chaum, D. ,*Blind signatures for untraceable payments*, in Chaum, D., Rivest, R.L., Sherman, A.T., ed. *Advances in Cryptology, Crypto'82*, 1982.
  
- [ 49 ] Chaum, D., *Online cash checks*, in J.J. Quisquater and J. Vandewalle, ed. *Advances in Cryptology, EUROCRYPT'89*, <http://www.digicash.com/publish/online.html>, 1989.
  
- [ 50 ] Chaum, D., *Achieving electronic privacy*, Scientific American, <http://www.digicash.com/publish/sciam.html>, August, 1992.

- [ 51 ] Chaum, D., *Prepaid smart card techniques: A brief introduction and comparison*, <http://www.digicash.com/publish/cardcom.html>, 1994.
- [ 52 ] Chaum, D., *Security without identification: Card computers to make big brother obsolete*, <http://www.digicash.com/publish>, 1995.
- [ 53 ] Chaum, D., Brands, S., *Minting electronic cash*, IEEE Spectrum, February, 1997.
- [ 54 ] Chaum, D., Fiat, A., Naor, M., *Untraceable electronic cash*, in S.Soldwasser, ed. *Advances in Cryptology, Crypto '88*, 1988.
- [ 55 ] Chen, H. e Crowston, K., *Comparative Diffusion: Reciprocal Interdependence between Clients and Servers*, Syracuse University School Press, 1997.
- [ 56 ] Choi, S.Y., Stahl, D.O., Whinston, A.B., *The Economics of Electronic Commerce*, Macmillan Technical Publishing, 1997.
- [ 57 ] Clarke, R., *EDI is But One of Electronic Commerce*, paper presented at thr 6th International EDI Conference, Bled, Slovenia, June 1993.
- [ 58 ] Clarke, R. *Key Issues in Electronic Commerce and Electronic Publishing*, paper presented at Information Online and On Disc99, Sydney, 21 January 1999.
- [ 59 ] Clemons, E.K., Croson, D.C., Weber, B.W., *Reengineering money*, International Journal of Electronic Commerce, 1997.
- [ 60 ] Clemons, E.K., Reddi, S.P., Row, M.C., *The impact of information technology on the organization of electronic activity: the move to the middle hypothesis*, Journal of Management Information Systems, 10, 2., 1996.
- [ 61 ] Cobra, M. H. N., *Administração de Vendas*, 3a. ed. , Atlas, 1994.



- [ 62 ] Cobra, M. H. N., *Administração de Marketing*, Atlas, 1990.
- [ 63 ] Cobra, M. H. N., *Plano Estratégico de Marketing*, Atlas, 1989.
- [ 64 ] Collins, J.C., Porras, J.I., *Built to Last*, Harper–Collins., 1994.
- [ 65 ] Comitê de Economia e Política Monetária e Industrial do Parlamento Europeu, *Study on Electronic Payment Systems*, Sevil, 1998.
- [ 66 ] CommerceNet, *Barriers & Inhibitors to the Widespread Adoption of Internet Commerce 1997*.CommerceNet Research Report #97–05, April 1997.
- [ 67 ] CommerceNet, *Overview of the 1998 Barriers and Inhibitors Research project* CommerceNet Research Bulletin #98–08, 1998.
- [ 68 ] CommerceNet/Nielsen, *Media Demographic and Electronic Commerce Study*, Chilton Research Services, survey, 1999.
- [ 69 ] Converse, P.D., *Marketing Innovations: Inventions, Techniques, institutions*, in Webster Jr., F.E. (ed.) *New Directions in Marketing*, American Marketing Association, 1965
- [ 70 ] Cooper, F.J., Goggans, C., Halvey, J.K., Hughes, L., Morgan, L., Siyan, K., Stallings, W., Stephenson, P., *Implementing Internet Security*, New Riders, 1995
- [ 71 ] Corner, J., *Studying Media: Problems of Theory and Method*, Edinburgh University Press, 1999.
- [ 72 ] Cousins, S., et. al. , *InterPay: Managing multiple payment mechanisms in digital libraries*, in DL'95 proceedings, <http://csdl.tamu.edu/DL95/papers/cousins/cousins.html>, 1995.

- [ 73 ] Cousins, S.B., Ketchpel, S.P., Paepke, A., Garcia-Moulina, H., et. al., *Interpay: Managing multiple payment mechanisms in digital libraries*, in The Second Annual Conference on the Theory and Practice of Digital Libraries, Digital Libraries 95, <http://www.csd.tamu.edu/DL95/papers/cousins/cousins.html>, June 1995b.
- [ 74 ] Coy, P., Judge, P.C., *Limo service for cruiing the Net*, Business Week, June 22, 1998.
- [ 75 ] Creed, A., *RSA Security Web Site Defaced*, Newsbytes.com, <http://www.newsbytes.com>, 2000.
- [ 76 ] Cronin, M.J., *Doing Business on the Internet*, Van Nostrand Reinhold, 1994
- [ 77 ] Cronin, M.J., *Doing More Business on the Internet*, Van Nostrand Reinhold, 1995
- [ 78 ] Cronin, M.J., *Banking and Finance on the Internet*, Wiley, John & Sons, 1997.
- [ 79 ] Csillag, L., *Estrutura e Dinâmica do Setor de Capital de Risco, na Criação de Empresas de Base Tecnológica no Brasil*, Dissertação de Mestrado, FEA-USP, 1995
- [ 80 ] Cushman, J.H., *Virtual university will offer authentic degrees by e-mail*, New York Times, June, 25, 1996.
- [ 81 ] CWI, DigiCash, Siemens, et. al., *The cafe project*, <http://www.cwi.nl/cwi/projects/cafe.html> ,1996a
- [ 82 ] CWI, DigiCash, Siemens, et. al., *The opera project*, <http://www.cwi.nl/cwi/projects/opera.html> ,1996b.
- [ 83 ] CyberCash, *Corporate Profile*, May, 1996a.

- [ 84 ] CyberCash, *Cybercash launches cybercoin service*, press release, <http://www.cybercash.com/cybercash/news/releases/1996/96sept30.html>, September 1996b.
- [ 85 ] CyberCash, *Acquiring internet transaction* (financial services white paper), <http://www.cybercash.com/cybercash/wp/bankwp.html>, 1997a.
- [ 86 ] CyberCash, *Cybercash and german banks dresdner bank and sachsen lb form a working group to offer secure internet transactions in germany*, press release, <http://www.cybercash.com/cybercash/news/releases/1997/97mar07dresdner.html>, March 1997b.
- [ 87 ] Cybercash, *Ensuring secure payment for internet commerce*, <http://www.cybercash.com/cybercash/wp/merchwp.html>, 1997c.
- [ 88 ] Cybercash, *Introducing cybercoin*, <http://www.cybercash.com/cybercash/shoppers/coingenpage.html>, 1997d.
- [ 89 ] CyberCash, *The six steps in a secure internet credit card payment*, <http://www.cybercash.com/cybercash/info/sixsteps.html>, 1997e.
- [ 90 ] Cybercash, Web Page, <http://www.cybercash.de>, 1998.
- [ 91 ] Davies, R., *Money – past, present & future*, Exeter University, <http://www.ex.ac.uk/~RDavies/arian/money.html>, 1997.
- [ 92 ] Davis, S. e Davidson, B., *Visão 2000*, Editora Campus, 1993
- [ 93 ] December, J. e Ginsburg, M., *HTML e CGI Unleashed*, SamsNet, 1995
- [ 94 ] Dekimpe, M.G., Parker, P.M., Sarvary, M., *Global Diffusion of Technological innovations: A Coupled-Hazard Approach*, Rand D., 1996.
- [ 95 ] Deming, W.E., *The New Economics*, MIT, 1993.

- [ 96 ] Dertouzos, M., *What Will Be*, Harper Collins, 1997.
- [ 97 ] Dettmer, H.W, *Goldratt's Theory of Constraints*, ASQC Press, 1997.
- [ 98 ] Dietze, C., *Electronic System Payment – Internet Based*, Giesecke & Devrient, 1997.
- [ 99 ] Digicash, *Digital signatures and smart cards*, <http://www.digicash.com/publish/digsig/digbig.html> , 1995
- [ 100 ] Digicash, *Ecash issuers*, <http://www.digicash.com/ecash-issuers.html>, 1996a.
- [ 101 ] Digicash, *Ecash payment mechanism*, <http://www.digicash.com/ecash/shop/paymentmethod.html>, 1996b.
- [ 102 ] Digicash, *Ecash trial*, <http://www.digicash.com/ecash/trial.html>, 1996c.
- [ 103 ] Digicash, *An introduction to ecash*, [http://www.digicash.com/publish/ecash\\_intro.html](http://www.digicash.com/publish/ecash_intro.html), 1997.
- [ 104 ] Digital Equipment Research Center, *Millicent*, <http://www.research.digital.com/SRC/millicent/>, 1996
- [ 105 ] Digital Equipment Research Center, *Millicent frequently asked questions*, [http://www.research.digital.com/SRC/millicent/pages\\_faq.html](http://www.research.digital.com/SRC/millicent/pages_faq.html), 1997.
- [ 106 ] Douba, S., *Networking Unix*, Sams Publishing, 1995.
- [ 107 ] Eads, G.M., *Manipulation of innovation attributes and impact on attitude formation*. Dissertation Abstracts International, University Microfilms No 84-26, 311, 1984.
- [ 108 ] Eastlake, D.E., *Universal payment preamble*, <http://www.w3.org/pub/WWW/Payments/specs/upp.txt>, 1997.

- [ 109 ] Eastlake, D., Boesch, B., Crocker, S., Yesil, M., *CybeCash credit card protocol* version 0.8, <ftp://ds.internic.net/internet-drafts/draft-eastlake-cybercash-v08-00.txt>, 1995.
- [ 110 ] Eastlake, D.E., Khare, R., Miller, J., *Selecting payment mechanisms over http*, <http://www.w3.org/pub/WWW/Payments/JEPI/UPPFlow.html>, 1997.
- [ 111 ] Ellsworth, J.H., e Ellsworth, M.V., *The Internet Business Book*, John, Wiley & Sons, 1994
- [ 112 ] English, L.P., Elliot, R.M., *Improving Data Warehouse and Business Information Quality: Methods for Reducing Costs and Increasing Profits*, Wiley, John & Sons, 1999.
- [ 113 ] Fajen, R., *Electronic payment schemes on the internet and their influence on electronic commerce*, <http://rcs.urz.tu-dresden.de/~marvin>, 1996.
- [ 114 ] Fichman, R.G., *Information technology diffusion: A review of empirical research*, Proceedings of the 13th International Conference on Information Systems, Dallas, 1992.
- [ 115 ] Fichman, R.G., *The Illusory Diffusion of Innovation: An Examination of Assimilation Gaps*, MIT Sloan School of Management, MIT Press, 1995.
- [ 116 ] Fliegel, F.C., Kivlin, J.F., *Differences among improved farm practices as related to adoption*. University Park, PA: Penssylvania Agricultural Experiment Station Research Bulletin 691., 1962.
- [ 117 ] Florac, W.A., Carleton, A.D., *Measuring the Software Process: Statistical Process Control for Software Process Improvement*, Addison Wesley Longman, Inc., 1999.
- [ 118 ] Folha de S.Paulo, *Internet sofre maior ataque pirata*, pags. 1, 1-15, 1-16. 10 de fevereiro de 2000.

- [ 119 ] Ford, W., Baum, M., *Secure Electronic Commerce*, Prentice Hall PTR, 1997.
- [ 120 ] Fortune, *Goldman Goes Shopping*, vol 139, no. 9, 1999.
- [ 121 ] Fox, E., *Digital Libraries, Special Section*, Communications of the ACM, 38, 4 , April 1995.
- [ 122 ] Frank, R.E., Massy, W.F., Morrison, D.G., *The Determinants of Innovative Behavior with Respect to a Branded Frequently Purchased Food Product*, in in Kollat, D.T., *Research in Consumer Behavior*, Holt, Rinehart and Winston, 1970
- [ 123 ] FSTC, *Electronic payments infrastructure: design considerations*, <http://www.fstc.org/projects/eccheck> , 1997a.
- [ 124 ] FSTC, FSTC Electronic check project, <http://www.fstc.org/projects/eccheck/index.html> , 1997b.
- [ 125 ] FSTC, Home page, <http://www.fstc.org> , 1997c.
- [ 126 ] Furche, A. e Wrightson, G., *Subscrip*, <http://www.cs.newcastle.edu.au/Research/afarche/subscrip.ps>. 1996.
- [ 127 ] G-10, *Electronic Money, consumer protection, law enforcement, supervisory and cross border issues, report of the working party on electronic money*, International Monetary Fund, 1997.
- [ 128 ] Gabber, E., Silberschatz, A., *Agora: A minimal distributed protocol for electronic commerce*, in 2nd USENIX workshop of electronic commerce, <http://www.bell-labs.com/user/eran/agora-ec96.ps>, November 1996.
- [ 129 ] Garbade, K., *Securities Markets*, McGraw-Hill, 1982.
- [ 130 ] Garfinkel, S., *PGP*, O'Reilly e Associates, 1995

- [ 131 ] Gates III, W.H., *The Road Ahead*, Viking Penguin, 1995
- [ 132 ] Gatingnon, H. and Robertson, T.S., *Technology diffusion: an empirical test of competitive effects*, in Journal of Marketing, vol 53, January, 1989.
- [ 133 ] Glassman, S., Manasse, M., Abadi, M., Gauthier, Sobalvarro, *The millicent protocol for inexpensive electornic commerce*, in 4th International World Wide Conference, <http://www.research.digital.com/SRC/millicent/papers/millicent-w3c4/millicent.html>, December 1995.
- [ 134 ] Global Reach, *Global Internet Statistics*, 20 fevereiro de 2000. [glreach.com/globstats](http://glreach.com/globstats), 2000.
- [ 135 ] Gogan, J.L., Applegate, L.M., *The Web's impact on selling techniques: historical perspective and early observations*, international Journal of Electronic Commerce, 1997.
- [ 136 ] Goldberg, I., *Some thoughts on a api for ecash*, <http://HTTP.CS.Berkeley.EDU/~iang/ecashapi>, 1996.
- [ 137 ] Goldratt, E.M., Cox, J., *The Goal*, North River Press, Inc, New York, 1986.
- [ 138 ] Goldratt, E.M., *The Haystack Syndrome, Sifting Information Out of the Data Ocean*, North River Press, Croton-on-Hudson, NY, 1990b
- [ 139 ] Goldratt, E.M., *Theory of Constraints*, North River Press, Inc., Croton-on-Hudson, New York, 1990a
- [ 140 ] Gray, M., *Internet Growth Report*, MIT Press, 1998.
- [ 141 ] Greenspan, A., *Regulating Electronic Money*, Cato Policy Report, vol XIX, no 2, 1997.
- [ 142 ] Guesnerie, R., *L'Economie de marché*, Paris, 1996.

- [ 143 ] Gupta, S.H., *A research project on the commercial uses of the World Wide Web*. MIT Press, 1999.
- [ 144 ] GVU, *10th WWW Users Study, 1999*, Georgia Tech Research Corporation, 1999.
- [ 145 ] Hafner, K., Markoff, J., *Cyberpunk*, Simon & Schuster, 1995.
- [ 146 ] Hahn, K.L., Schoch, N.A., *Applying diffusion theory to electronic publishing: A conceptual framework for examining issues and outcomes*, in *The Information Society*, 11, 1998.
- [ 147 ] Hallam-Baker, P. et al., *W3c micro payment transfer protocol – mptp*, <http://www.w3.org/pub/WWW/TR/WD-mptp>, 1995.
- [ 148 ] Halloran, J.D., LinnGe, O., HamelinkC.J., *Mass Communication Research: On Problems and Policies*, Ablex Publishing Corporation, 1994.
- [ 149 ] Hardy, N. Tribble, E.D., *The digital silk road*, <http://www.agorics.com/dsr.html>, 1997
- [ 150 ] Hauser, R., Steiner, M., Waidner, M., *Micro-payments based on ikp*, IBM Research Lab, <http://www.zurich.ibm.ch/Technology/Security/publications/1996/HSW96.ps.gz>, February, 1996.
- [ 151 ] Hettinga, R., *The e\$ home page*, <http://www.shipwright.com>, 1997.
- [ 152 ] Herzberg, A., Yochai, H., *Mini-pay: Charging per click on the web*, in 6th International World wide Conference, Network Computing and Security Group, IBM Research – Haifa Research Lab, Tel-Aviv Anne, <http://www6.nttlabs.com/HyperNews/get/PAPER99.html>, April 1997.
- [ 153 ] Horch, J.W., *Practical Guide to Software Quality Management*, Artech House, 1996.



- [ 154 ] Hoffman, D.L., Novak, T.P., Chatterjee, P., *Commercial scenarios for the web: opportunities and challenges*, Journal of Computer-Mediated Communication, 1, 3, 1996.
- [ 155 ] Hoiberg, E. , *Ex-ante Diffusion Research*, Iowa State university Press, 1997.
- [ 156 ] Holloway, R.E., *Perceptions of an innovation: Syracuse university Project Advance*. Dissertation Abstracts International, University Microfilms No. 78-11, 656. 1977.
- [ 157 ] Howard, R.A., Matheson, J.E., *Readings on the principles and applications of decision analysis, vols I, II* , Strategic Decisions Group, 1983.
- [ 158 ] Hughes, T., *Technological Momentum, in Does Technology Drive History? The Dilemma of Technological Determinism*, eds M.R.Smith and L.Marx, MIT Press, 1994.
- [ 159 ] Intelliquest, *Internet user study – 1997 – 1999*, Intelliquest, 1999.
- [ 160 ] Jarecki, S., Odlyzko, A.M., *An efficient micropayment system based on probabilistic polling*, in Financial Cryptography 1997, Lecture Notes in Computer Science No. 1318, AT&T, <http://www.research.att.com/amo/doc/polling.ps>, 1997.
- [ 161 ] Jacobson, I., Christerson, M., Johnsson, P., Overgaard, G., *Object-Oriented Software Engineering*, Addison-Wesley, 1992.
- [ 162 ] Jarvempaa, S.L., Todd, P.T., *Consumer reactions to electornic shopping on the World Wide Web*, International Journal of Electronc Commerce, 1997.
- [ 163 ] Jelassi, T., Figon, O., *Competing through EDI at Brun Passot, ambitions in the European Market*, MIS Quarterly, 18, 4 , December, 1994.
- [ 164 ] Jones T., *Mondex on 'the future of money'*, <http://www.mondex.com/hserrep.htm>, 1996.

- [ 165 ] Juran, J.M., *Juran on Quality by Design*, Free Press, 1992.
- [ 166 ] Kalakota, R., Whinston, A.B., *Electronic Commerce – A Manger’s Guide*, Addison–Wesley, 1998.
- [ 167 ] Kalakota, R., Whinston, A.B., *Readings in Electronic Commerce*, Addison–Wesley, 1997.
- [ 168 ] Kalakota, R. Whinston, A.B., *Frontiers of Electronic Commerce*, Addison–Wesley, 1996.
- [ 169 ] Kambil, A., Short, J.E., *Electronic Integration and Business Network Redesign: a roles–linkage perspective*, Journal of Management Information Systems, 10, 4., 1994.
- [ 170 ] Kautz, K., McMaster, T., *The failure to introduce systems development methods: a factor–based analysis*, in Levine, L. (eds), Diffusion, transfer and implementation of information technology, Elsevier Science BV. 1994.
- [ 171 ] Keeler, L., *CyberMarketing*, American Management Association, 1995
- [ 172 ] Kegerreis, R., *Innovativeness and the Characteristics of Adopters*, Holt, Rinehart and Winston, 1970.
- [ 173 ] Kegerreis, R.J., Engel, J.F., Blackwell, R.D., *A Marketing View of Earliest Adopters*, in Kotler, P (org.) Consumer Behavior, Holt, Rinehart and Winston, 1976.
- [ 174 ] Kelly, R.F., *The Diffusion Model as a Predictor of Ultimate Patronage Levels in New Retail Outlets*, in Raymond Hass (ed.), Science Technology & Marketing , Holt, Rinehart & Winston, 1983
- [ 175 ] Ketchpel, S., *Transaction protection for information buyers and sellers*, in DAGS’95 – Electronic Publishing and the Informatio Superhighway, <http://robotics.stanford.edu/users/ketchpel/dags4.html>, 1995.

- [ 176 ] Ketchpel, S.P., *Interpay: A project in the stanford digital library*, <http://robotics.edu/~ketchpel/diglib/interpay>, 1996.
- [ 177 ] Ketchpel, S., Garcia-Molina, H., Paepcke, P., Hassan, S., Cousins, S., *Upai: A universal payment application interface*, Stanford University, <http://www-diglib.stanford.edu/diglib/WP/PUBLIC/DOC97.ps>, 1996.
- [ 178 ] Keys, J., *Technology Trendlines*, VNR, 1995.
- [ 179 ] Khare, R., *Http/1.2 extension protocol*, <http://www.w3.org/pub/WWW/TR/WD-httpd-pep.html>, 1997.
- [ 180 ] Kleline, *Home Page*, <http://www.kleline.com>. 1997.
- [ 181 ] Knight, K.E., *A Descriptive Model of the Intra-Firm Innovation Process*, Journal of Business, vol XL outubro 1967, in Blackwell, R.D., Innovativeness and Diffusiveness, A Marketing View, Ohio State University Press, 1984
- [ 182 ] Kosiur, D., *Understanding Electronic Commerce*, Microsoft Press, 1997.
- [ 183 ] Koster, M. *Web Robots*, Free Press, 1996.
- [ 184 ] Kotler, P., *Marketing Management: Analysis, Planning, Implementation & Control*, 6 th Ed., Prentice-Hall International, 1994.
- [ 185 ] Kristol, D., Low, S., Maxemchuck, N., *Anonymous credit cards*, in Globecom'94, <ftp://ftp.research.att.com/dist/anoncc/anoncc.ps.Z>, 1994a.
- [ 186 ] Kristol, D., Low.S., Maxemchuck, N., *Anonymous internet mercantile protocol*, AT&T Bell Labs, <ftp://research.att.com/dist/anoncc/accinet.ps.Z>, 1994b.
- [ 187 ] Krol, E., *The Whole Internet* , O'Reilly & Associates, 1994.
- [ 188 ] Latour, B., *Aramis, or, The Love of Technology*, Cambridge, MA, Harvard University Press, 1996.

- [ 189 ] Latour, B., *We Have Never Been Modern*, Harvester Wheatsheaf, 1993.
- [ 190 ] Latour, B., *The Sociology of a Few Mundane Artifacts*, in Bijker, W., Law, J. eds *Shaping Technology Building Society Studies in Sociotechnological Change*, MIT Press, 1992.
- [ 191 ] Latour, B., *Technology is Society Made Durable*, in Law, J. ed. *A Sociology of Monsters: Essays on Power, Technology and Domination*, Routledge, 1991.
- [ 192 ] Latour, B., *Science in Action: How to Follow Scientists and Engineers Through Society*, Open University Press: Milton Keynes, 1987.
- [ 193 ] Latour, B., *The Pasteurization of France*, Cambridge MA, Harvard University Press, 1986.
- [ 194 ] Latour, B., Woolgar, S., *Laboratory Life: The [Social] Construction of Scientific Facts*, Princeton University Press, 1986.
- [ 195 ] Law, J., *Laboratories and Texts*, in Callon, M., Law, J., Rip, A. eds. *Mapping the Dynamics of Science and Technology*, London:MacMillan, 1986.
- [ 196 ] Law, J. Callon, M., *The Life and Death of an Aircraft: A Network Analysis of Technological Change* in Bijker W., Law, J. eds. *Shaping Technology / Building Society Studies in Sociotechnological Change*, MIT Press, 1992.
- [ 197 ] Law, L. Sabett, S., Solinas, *How to make a mint: The cryptography of anonymous electronic cash*, National Security Agency, <http://jya.com/nsamint.htm>, 1996.
- [ 198 ] Lawrence, S., Giles, L., *Accessibility and Distribution of Information on the Web* NEC Research Institute, 1997.
- [ 199 ] Lazer, W., Bell, W.E., 1966 *The Communication Process and Innovation*, Journal of Advertising Research, vol 6, no 3, setembro, in Blackwell, R.D., *Innovativeness and Diffusiveness, A Marketing View*, Ohio State University Press, 1984

- [ 200 ] Lee, R., Bons, R.W.H., *Soft-coded procedures for open-EDI*, International Journal of Electronic Commerce, 1, 1, 1996.
- [ 201 ] Lee, H.G., Clark, T., *Impacts of electronic marketplace on transaction cost and market structure*, International Journal of Electronic Commerce, 1,1, 1996.
- [ 202 ] Lehre, S., *Electronic Cash, Tokens and Payments in the National Information Infrastructure*, Rostock, 1997.
- [ 203 ] Levine, L. (ed.), *Diffusion, Transfer and Implementation of Technology*, Elsevier / North-Holland, 1994.
- [ 204 ] Lewis, G.A., *Leadership Products as Innovations in the Context of Rogers' Diffusion Theory*, dissertation, VT ETD Collection, 11997-1767, 1997.
- [ 205 ] Liu, C., Peek, J., Jone, R. Buus, B. e Nye, A., *Managing Internet Information Services*, O'Reilly & Associates, Inc., 1994
- [ 206 ] Lottor, M., *Surveu of the Internet Hosts* , Network Wizards, January, 1999
- [ 207 ] Low, S., Maxemchuck, N., Paul, S., *Collusion in a multiparty communication protocol for anonymous credit cards*, in IEEE/ACM Transactions on Networking, <ftp://ftp.research.att.com/dist/anoncc/collude.ps.Z>, 1994.
- [ 208 ] Lynch, D.C., Lunquist, L. *Digital Money: The New Era of Internet Commerce*, John Wiley & Sons, 1996.
- [ 209 ] MacKie-Mason, J. White, K., *Evaluating and selecting digital payment mechanisms*, School of Information, University of Michigan, <http://www-personal.umich.edu/~jmm/papers/digidoll.pdf>, November 1997.
- [ 210 ] Mahajan, V. & Muller, E., *Innovation diffusion and new-product growth models in marketing*, Journal of Marketing, vol 43, 1979.

- [ 211 ] Magid, J., Matthews, R.D., Jones, P., *The Web Server Book*, Ventana Press, 1995
- [ 212 ] Manasse, M., *The millicent protocols for electronic commerce*, in *1st USENIX workshop on Electronic Commerce*, USENIX, <http://www.research.digital.com/SRC/millicent/papers/mcentny.htm>, July 1995.
- [ 213 ] Mardsen, P., *Journal of Memetics – Evolutionary Models of Information Transmission*, Centre in the Social Sciences, University of Sussex, 1998.
- [ 214 ] Martin, J., *Cybercorp*, AmaCom, 1996.
- [ 215 ] MasterCard–SET, *Home page*, <http://www.mastercard.com/set>, 1996.
- [ 216 ] Matheson, D., Matheson, J., *The Smart Organization*, Harvard Business Review, 1998.
- [ 217 ] Maturana, H., Varela, F., *The three of knowledge: Biological Roots of Human Understanding*. Boston: Shambala Publications, 1987.
- [ 218 ] Maturana, H., Varela, F., *Autopoiesis and Cognition: The Realization of the Living* Boston:Reidel, 1980.
- [ 219 ] Mayer, M., *The Bankers, the next generation*, Truman Talley Books, 1997.
- [ 220 ] McMaster, T., Vidgen, R.T., Wastell, D.G., *Towards an understanding of technology in transition – two conflicting theories*, University of Salford, UK, Time Research Institute, 1998.
- [ 221 ] MediaLab, *Time Capsule*, <http://www.sloan.edu>, 1999.
- [ 222 ] Medvinsky, G., Neuman, B.C., *Netcash: A design for practical electronic currency on the internet*, in *Proceedings of 1st the ACM Conference on Computer and Communication Security*, <ftp://prospero.isi.edu/pub/papers/security/netcash-cccs93.ps> , 1993.

- [ 223 ] Mingers, J., *Self-Producing Systems: Implications and Applications of Autopoiesis*, Plenum Press, 1995.
- [ 224 ] Mokyr, J., *The Lever of Riches: Technological Creativity and Economic Progress*, Oxford University Press, 1990.
- [ 225 ] Mondex, *Home Page*, <http://www.mondex.com>. 1996.
- [ 226 ] Moore, G.A., *Crossing the Chasm*, HarperCollins, 1991
- [ 227 ] Moore, G.A., *Inside the Tornado*, HarperCollins, 1995
- [ 228 ] Moston, S. e Emmanouilide, C., *Diffusion of Interactive Mass Media Applications: Scenarios for the Future*, London Business School Working Papers #97-801, 1997.
- [ 229 ] Mudry, R.J., *Serving the Web*, Coriolis Group Books, 1995
- [ 230 ] Negroponte, N., *The next billion users*, Wired, June 1998.
- [ 231 ] NetCard, *Home Page*, <http://www.cl.cam.ac.uk/users/cm213/Project>, 1996.
- [ 232 ] NetCash, *Home page*, <http://nii-server.isi.edu/info/netcash>, 1996.
- [ 233 ] NetCheque, *Home page*, <http://gost.isi.edu/info/netcheque>, 1996.
- [ 234 ] NetFare, *Home page*, <http://www.netfare.com>, 1996.
- [ 235 ] Neuman, B.C., Medvinsky, G.M. *Requirements for network payment: The netcheque perspective*, in COMPCON'95, <ftp://propsero.isi.edu/pub/papers/security/netcheque-requirements-compcon95.ps>, MArch 1995.
- [ 236 ] Owen, C.A., *Internet micro payment protocols*, Artech House, 1997.

- [ 237 ] Parenti, M., *Dirty Truths: Reflections on Politics, Media, Ideology, Conspiracy, Ethnic Life and Class Power*, City Lights Books, 1996.
- [ 238 ] Parker, T., *TCP/IP*, Sams Publishing, 1997.
- [ 239 ] Pedersen, T. *Electronic payments of small amounts*, Aarhus University, Denmark, August 1995.
- [ 240 ] Pine, J.B., *Mass Customization: The New Frontier in Business Competition*, Harvard Business School Publishing, 1999.
- [ 241 ] Quelch, J.A., Klein, L.R., *The Internet and international marketing*, Sloan Management Review, 1998.
- [ 242 ] Rapaport, R., *Interview with John Gage*, Fast Company, April–May, 1996.
- [ 243 ] Richards, D., *Requirements analysis for library accounting systems*, <http://www.ub.uni-bielefeld.de/aktuell/kongress/vortraeg/richard.htm>, 1996.
- [ 244 ] Rivest, R.L., *The md5 message digest algorithm*, Internet RFC 1321, <http://theory.lcs.mit.edu/~rivest/Rivest-MD5.txt>, April 1992.
- [ 245 ] Rivest.R., *Electronic lottery tickets as micropayments*, in proceedings of Financial Cyptography '97, <http://theory.lcs.mit.edu/~rivest/lottery.ps>, February 1997.
- [ 246 ] Rivest, R.L., Shamir, A., *Payword and micromint–two simple micropayment schemes*, <http://theory.lcs.mit.edu/~rivest/RivestShamir–,pay.ps>, May 1995.
- [ 247 ] Robert, M., *Product Innovation Strategy*, McGraw Hill, 1995
- [ 248 ] Roberts, B., *Online auction house finds growth with secondhand merchandising*, Web Week, June 17, 1996.



- [ 249 ] Rogers, E.M., *Diffusion of innovations*, 4a ed., Free Press, 1995.
- [ 250 ] Rogers, E.M., Scott, K.L., *The Diffusion of Innovations Model and Outreach from the National Network of Libraries of Medicine to Native American Communities*, University of New Mexico Press, 1997.
- [ 251 ] Rose, M.T., Borenstein, N.S., *The simple mime exchange protocol*, <http://www.fv.com/pubdocs/smxd-spec.txt>, 1996.
- [ 252 ] Russo, J.E., Schoemaker, P.J.H., *Decisions Traps*, Doubleday, 1989.
- [ 253 ] Ryan, B., Gross, N.C., *The diffusion of hybrid seed corn in two Iowa communities*. Rural Sociology (8) 15–24, 1943.
- [ 254 ] Sachs, S.G., *The Diffusion of Innovations: The Overlooked Literature*. AECT, 1993.
- [ 255 ] Scheinkopf, L.J., *Thinking for a Change*, St. Lucie Press /APICS, 1999.
- [ 256 ] Schneier, B., *Applied Cryptography*, 2nd ed. Wiley, 1996.
- [ 257 ] Schoeter, A., Willmer, R., *Digital money online*, Intertrader Ltd., <http://www.intertrader.com/library/DigitalMoneyOnline/dmo/dmo.htm>, 1997.
- [ 258 ] Schulmeyer, G.G., McManus, J.I., *The handbook of software quality assurance* , Prentice Hall, 1999.
- [ 259 ] Schunter, M., Weber, A., *News from cafe – the high security digital payment system*, [http://www.informatik.uni-hildesheim.de/FB4/Projekte/sirene/publ/ScWe\\_95CafeNews.ps.gz](http://www.informatik.uni-hildesheim.de/FB4/Projekte/sirene/publ/ScWe_95CafeNews.ps.gz), June, 1995.
- [ 260 ] Seideman, T., *What Sam Walton learned from the Berlin airlift*, Audacity: The Magazine of Business Experience, 1996.

- [ 261 ] Senge, P., *The Fifth Discipline*, Doubleday, 1990.
- [ 262 ] SET, *Business Description*,  
<http://www.visa.com/cgi-bin/vee/sf/set/setbus.html>, 1997a.
- [ 263 ] SET, *Set Programmer's Guide*,  
<http://www.visa.com/cgi-bin/vee/sf/set/setprog.html>, 1997b.
- [ 264 ] SET, *Set Protocol Description*,  
<http://www.visa.com/cgi-bin/vee/sf/set/setprog.html>, 1997c.
- [ 265 ] Sirbu, M., Tygar, J.D., *Netbill: An Internet commerce system optimized for network delivered services*, in COMPCON'95,  
[http://www.ini.cmu.edu/netbill/pubs/CompCon\\_TOC.html](http://www.ini.cmu.edu/netbill/pubs/CompCon_TOC.html), MArch 1995.
- [ 266 ] Siyan, S, Hare, A., *Secure SSL Systems*, in Netscape,  
[http://www.netscape.com/ssl\\_system/wp/ssl.html](http://www.netscape.com/ssl_system/wp/ssl.html), 1998.
- [ 267 ] Spar, D., Bussgang, J.J., *Ruling the Net*, Harvard Business Review, may-june, 1996.
- [ 268 ] Sprout, A., *The Internet inside your company*, Fortune, November 27, 1995.
- [ 269 ] Stadler, M., Pivetau, J.M., Camenisch, J., *An efficient fair payment system*, in CCS'96, India,  
[ftp://ftp.inf.ethz.ch/pub/publications/papers/ti/isc/acm\\_ccs.ps](ftp://ftp.inf.ethz.ch/pub/publications/papers/ti/isc/acm_ccs.ps), 1996.
- [ 270 ] Stalder, F., *Emerging Patterns: Reading an Actor-Network of Electronic Cash*, The Information Society, julho, 1999.
- [ 271 ] Stein, E.W., Zwass, V., *Actualizing organizational memory with information systems*, Information Systems Research, 6,2 June 1995.
- [ 272 ] Stein, L.H., Stefferud, E.A., Borenstein, Rose, M.T., *The green commerce model*, <http://www.fv.com/pubdocs/gree-model.txt>, 1996.

- [ 273 ] Stevens, W.R., *TCP/IP Illustrated, vol 1, the protocols*, Addison-Wesley, 1994.
- [ 274 ] Storosten, M.N., *Barriers to Electronic Commerce*, paper presented at Esprit Emmsec 99, Bordeaux, France, September 1999.
- [ 275 ] Surry, D., *Perceptions of weather forecasters in regard to innovative computer based training*, University Microfilms No 104-216, 1993.
- [ 276 ] Teilhard de Chardin, P. , *The Phenomenon of Man*, HarperTrade, 1976.
- [ 277 ] Texel, P.P., Williams, C.B., *Use Cases combined with booch, omt, uml*, Prentice Hall PTR, 1997.
- [ 278 ] Thoresen, K., *Learning at work*, in Kautz, K. and Pries-Heje, J., eds., *Diffusion and adoption of information technology*, Chapman and Hall, 1996.
- [ 279 ] Time, *Harnessing the power of ideas*, May 24, 1999.
- [ 280 ] Tse, A., *The impact of the Internet on Marketing*, The Chinese University of Hong Kong, 1997.
- [ 281 ] U.S. Department of the Treasury, *Implications of the Development of Electronic Money*, June, 4, 1998.
- [ 282 ] Venkatraman, N., Loh, L., Koh, J., *The adoption of corporate governance mechanisms: A test of competing diffusion models*, in *Management Science*, vol 40 (4). 1994.
- [ 283 ] Verity, J.W., *Invoice?What's an Invoice?* Business Week, June 10, 1996.
- [ 284 ] Vernadsky, V.I., *The Biosphere: Complete Annotated Ed.* , Springer-Verlag, 1998.
- [ 285 ] Wasserman, S., Faust, K., *Social Network analysis: Methods and Applications*. Cambridge MA: University of Cambridge Press, 1994.

- [ 286 ] Wasson, C.R., *"What is "new" about a new product?"*, Journal of Marketing, julho, 1960, in Kollat, D.T., *Research in Consumer Behavior*, Holt, Rinehart and Winston, 1970.
- [ 287 ] Weinstein, S.H., *Military or civilian use of instructional innovations: Is there a difference?* San Francisco: National Society for Performance and Instruction, 1986.
- [ 288 ] Wellman, B., *Network Analysis: Some Basic Principles*, in Collins, R. ed. Sociological Theory, Jossey-Bass Inc. , 1983.
- [ 289 ] Wheeler, D., *Transactions using bets*, <ftp://ftp.cl.cam.ac.uk/users/djw3/tub.ps>, April 1996.
- [ 290 ] Wilson, P.F., Deil, L.D., Anderson, G.F., *Root Cause Analysis*, ASQC Quality Press, 1993
- [ 291 ] Winfield, G. , Stewart, L.C., *Designing Systems for Internet Commerce*, Addison-Wesley, 1999.
- [ 292 ] Woolgar, J.S., Latour, B., *Laboratory Life, the construction of scientific facts*, Princeton University Press, 1990.
- [ 293 ] WTO, *Electronic Commerce and the Role of the WTO*. WTO Secretariat, March 1998.
- [ 294 ] Wyner, N.B., *A study of diffusion of innovation: Measuring perceived attributes of an innovation that determine rate of adoption*. Dissertation Abstracts international, University Microfilms No 74-26, 628, 1974.
- [ 295 ] Yoffie, D.B., Cusumano, M.A., *Competing on Internet Time*, Free Press, 1998.
- [ 296 ] Yoffie, D.B., *Strategic Management in Information Technology*, Harvard Business School, 2000.

- [ 297 ] Zahran, S., *Software Process Improvement: Successful Models and Strategies*, Addison Wesley Longman, Inc., 1988.
- [ 298 ] Zwass, V., *Electronic Commerce: Structures and Issues*, International Journal of Electronic Commerce, vol 1, no. 1., 1996.
- [ 299 ] Zwissler, S. *Sistematic Method for Electronic Transactions*, PhD thesis, Universitat Karlsruhe, April 1996.