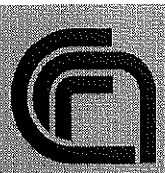


Consiglio Nazionale delle Ricerche

Commercio Elettronico e Sistemi di Pagamento in Internet

Fabrizio Fabbrini, Massimo Marra

B4-33
dic-1999

Commercio Elettronico e Sistemi di Pagamento in Internet

Fabrizio Fabbrini[1], Massimo Marra[2]

[1] - *Istituto di Elaborazione dell'Informazione, CNR, Pisa*
[2] - *Area Servizi Informatici, Università di Lecce*

Electronic Commerce (E-commerce) is the globality of business transactions carried on by means of electronic tools. It includes sharing business information, maintaining business relationships, conducting business transactions, and transferring funds by means of telecommunications networks. The Internet and the Internet's World Wide Web, with their phenomenal growth over past few years, have become the primary driver of contemporary EC. The paper focuses on Electronic Fund Transfers and Internet Payment Systems, providing a description and comparison of a number of existing and proposed electronic transaction systems, including both cash and transfer systems, but concentrating on those designed to operate across public networks. A perspective analysis of their impact is provided.

1 Sistemi di pagamento

1.1 Trasferimenti elettronici di fondi

I sistemi per il trasferimento elettronico di fondi (Electronic Fund Transfer Systems, EFTS) sono sistemi di pagamento elettronici, che realizzano, cioè, il pagamento tramite il mezzo elettronico, indipendentemente dal fatto che il pagamento stesso sia reale o virtuale, cioè che si tratti di moneta elettronica o di banconote.
Si definiscono trasferimenti elettronici di fondi *on-line*, tutti quegli EFT che comportano l'effettuazione in tempo reale del regolamento contabile relativo all'ordine di pagamento. Sono invece detti EFT *off-line* tutti quei trasferimenti elettronici di fondi per i quali il regolamento contabile relativo all'ordine di pagamento viene effettuato successivamente allo stesso, in modo tradizionale.
I sistemi di pagamento in Internet (Internet Payment Systems, o IPS), sono invece mezzi elettronici atti ad effettuare un pagamento avente anch'esso forma elettronica, tramite la rete Internet. Quest'ultima tipologia di pagamento elettronico presenta quindi un campo di esistenza ben limitato rispetto agli altri sistemi di trasferimento elettronico di fondi, pur essendovi ricompresa.

1.1.1 Aspetti tecnologici

Sussistono molteplici tecnologie di realizzazione degli EFTS tra le quali toccheremo le più importanti:

- ATM (Automatic Teller Machines). Sono sportelli bancari automatizzati come quelli dediti al servizio Bancomat. Consistono in un sistema di computers con terminali posizionati in punti vendita POS (Point Of Sale). Al momento del pagamento l'acquirente inserisce la propria carta di riconoscimento e digita un codice personale. Questa operazione implica che attraverso una rete telematica, l'importo negoziato venga addebitato all'acquirente e accreditato all'operatore commerciale nei conti correnti presso le rispettive banche.
- ACH (Automated Clearing House). Stanza di compensazione automatica. Sono sistemi che provvedono alla compensazione elettronica delle operazioni compiute dalle banche, tramite un meccanismo centralizzato su cui gli istituti finanziari si accordano per scambiare ordini di pagamento. Le banche sistemano gli scambi in un tempo prestabilito, seguendo le regole e le procedure della Clearing House. Attraverso questa tecnologia viene resa possibile la cosiddetta "chèque truncation" cioè, il troncamento della circolazione di un titolo di credito presso la prima banca che ne viene a contatto. Al momento della presentazione per l'incasso il titolo di credito viene trattenuto dalla banca la quale registra su un nastro magnetico le sue caratteristiche peculiari; trasformato così in un messaggio elettronico il titolo viene inviato alla banca del debitore tramite una ACH.
- Internet. La rete Internet è lo strumento più recente in materia di trasferimenti elettronici di fondi, se pensiamo che, ad esempio, il servizio Bancomat in Italia è in funzione dall'ottobre del 1983: il cambiamento che essa potrebbe introdurre nel mondo dei trasferimenti elettronici di fondi è tuttavia decisivo. Attraverso la rete è infatti, per esempio, possibile attuare il trasferimento di moneta elettronica virtualizzando così non soltanto

l'ordine di pagamento, ma addirittura il tramite stesso del pagamento; altro esempio delle potenzialità di Internet è la sua applicazione al pagamento tramite carta di credito, effettuabile comunicando il numero attaverso la rete.

1.2 Carte di pagamento

Un trasferimento elettronico di fondi può essere avviato mediante svariati mezzi, fra i quali rientrano le carte di pagamento. Questo termine presenta però molte possibilità di utilizzo: ci sono carte che servono per effettuare pagamenti in tempo reale,addebitando il conto del titolare, altre attraverso cui il saldo delle operazioni effettuate nell'arco di un certo periodo di tempo avviene in un momento differito rispetto a quello della transazione commerciale. La quasi totalità delle carte di pagamento è direttamente coinvolta nell'attività bancaria quotidiana e sempre più la banca del futuro si troverà ad operare con sistemi di pagamento basati su carte. La notevole evoluzione tecnologica che ha investito e sta investendo la categoria in questione, inoltre, porta ad un intreccio di rapporti con la problematica del trasferimento elettronico di fondi, in quanto, anche se non tutte, la maggioranza delle tipologie di carte danno luogo ad un EFT. Non tutti i trasferimenti elettronici di fondi, d'altra parte, sono attuati tramite carte di pagamento: pensiamo al trasferimento elettronico di fondi che consegue all'invio di un codice personale identificativo dell'utente (non necessariamente un PIN, ma anche una chiave di crittazione) che viene trasmesso per via telematica. Per cercare di trovare un approccio sistematico alla materia, cercheremo, innanzitutto, di mettere ordine in una varietà di carte che popolano, e sempre più popoleranno, la nostra vita quotidiana, tentando di capire, in primo luogo, cosa sia una carta di pagamento e quale ne sia l'origine.
Da un punto di vista tecnologico possiamo operare una classificazione delle carte credito in carte telematiche e carte ordinarie (non telematiche). Le carte ordinarie sono plastificate con i dati necessari all'identificazione scritti in rilievo, a volte contengono dei codici a barre che devono essere letti in appositi lettori per autorizzare la transazione. Le carte telematiche sono quelle che danno luogo ad una trasmissione diretta, tramite un canale telematico, dei dati dell'utente e della transazione in corso; esse si dividono in magnetiche e elettroniche. Le carte magnetiche sono così dette perché presentano una striscia di materiale magnetico posta sul retro. Le carte elettroniche contengono uno o più microcircuiti che consentono la memorizzazione e elaborazione dei dati. Le laser card o carte a memoria ottica sono un particolare tipo di carte elettroniche che basano la registrazione dei dati su delle memorie ottiche. Le carte elettroniche vanno a loro volta distinte in carte a memoria e carte intelligenti. Le carte a memoria contengono solo circuiti di memoria per immagazzinare i dati e i circuiti necessari per comunicare con la macchina lettrice ed è quest'ultima a contenere il software di controllo. Le carte intelligenti (*smart card*) contengono, invece, dei veri e propri microelaboratori e con essi, anche il software di controllo. Le carte elettroniche sono più costose delle carte magnetiche ma sono più resistenti in quanto la banda magnetica è sottoposta ad usura meccanica; sono più affidabili e sicure in quanto non possono essere lette se non si conosce la chiave di accesso alla memoria interna della carta o PIN (Personal Identification Number) e anche la loro duplicazione si rivela molto più complicata e costosa di quella delle carte magnetiche. Le carte laser offrono una capacità di memoria notevole: fino ad oltre 100 MB. La carta laser è inoltre molto più economica ed affidabile delle carte elettroniche, la sua sperimentazione è ancora agli inizi ma sembra lo strumento più adatto per la realizzazione di progetti come le carte personali (archiviazione di dati sanitari, civili,...) e i progetti di portafoglio elettronico.

1.3 Internet Payment Systems

Gli Internet Payment Systems (IPS), come suggerisce il nome, sono sistemi di pagamento implementati sulla rete Internet: realizzano quindi una integrazione della transazione commerciale convenzionale (tramite assegno, carta di credito o contante) nel nuovo sistema di comunicazione. Tre tipi principali di pagamento elettronico possono essere implementate su Internet:

- Ordini di pagamento basati su carte di credito.
- Ordini di pagamento basati su assegni elettronici (Electronic chèque, o E-chèque). Si tratta di un ordine elettronico di pagamento, cioè di un documento digitale che contiene le istruzioni necessarie a trasferire denaro da un conto bancario.
- Ordini di pagamento basati su denaro elettronico (Electronic cash, o E-cash). Questo termine è genericamente impiegato per indicare qualsiasi schema di pagamento elettronico che ricordi all'utente l'utilizzo di denaro contante: infatti, come il nome implica, il denaro elettronico è un tentativo di progettare e implementare un sistema di pagamento elettronico modellandolo sul sistema convenzionale di denaro contante. In realtà, parlando di electronic cash, si dovrebbe intendere uno schema in cui il denaro è fisicamente conservato all'interno di un computer o di una smart card.

1.3.1 Denaro elettronico

Spesso il concetto di "denaro elettronico", identificato con il termine inglese *e-cash*, è utilizzato in modo piuttosto vago: prima di proseguire cercheremo di dare contorni più definiti al concetto stesso e, come conseguenza, ai sistemi di trasferimento elettronico di fondi che ne derivano. Il denaro elettronico è un valore monetario espresso in unità correnti, immagazzinate in formato elettronico su un supporto tecnologico in possesso del consumatore. Si tratta in altre parole di un fondo elettronico che può essere acquistato dal consumatore e, una volta immagazzinato nell'adeguato supporto, viene ridotto a scalare ogni volta che il consumatore utilizza il supporto stesso per effettuare un acquisto. Si tratta di una forma di pagamento differente dai tradizionali mezzi di pagamento elettronici come le carte di credito o di debito, le quali richiedono tipicamente un'autorizzazione on-line e coinvolgono il conto corrente bancario del consumatore dopo la transazione. Ci sono due tipi fondamentali di mezzi elettronici atti a supportare il denaro elettronico: le carte prepagate e i prodotti software che includono sistemi di prepagamento. Con le carte prepagate il valore elettronico viene immagazzinato in un chip inserito in una carta e il valore viene tipicamente trasferito inserendo la carta in un apposito lettore. Nel caso dei prodotti software il valore elettronico viene invece immagazzinato sull'hard disk di un computer e viene trasferito attraverso reti telematiche di comunicazione come Internet, quando si effettua la transazione. Secondo questa definizione l'e-cash è diverso da quelli che vengono detti prodotti di accesso (access products) i quali permettono ai consumatori di utilizzare mezzi elettronici di comunicazione per utilizzare sistemi di pagamento altrimenti convenzionali. Infatti l'uso di un computer per trasmettere un ordine di pagamento, per esempio, è cosa ben diversa dal denaro elettronico propriamente detto. Trasmettere il numero della propria carta di credito per via telematica al fine di effettuare un trasferimento elettronico di fondi, è un fenomeno inerente più ad una fattispecie di ordine elettronico (ovvero elettronicamente trasmesso). Quando si parla di denaro elettronico invece, ci riferiamo a un fenomeno nel quale il denaro si trova fisicamente (se poi così si può dire) nel computer o nella smartcard. Ci sono varie tipologie di e-cash che sono in corso di sviluppo e differiscono di molto nelle loro caratteristiche: innanzitutto le tipologie di denaro elettronico differiscono tecnologicamente, ovvero nel sistema con cui il denaro è implementato nel mezzo elettronico. Nel caso delle carte intelligenti il microcircuito integrato nella carta è un componente specializzato mentre le tipologie software-based utilizzano personal computer nei quali viene installato un programma apposito. I prodotti differiscono tra di loro poi nel coinvolgimento o meno di una terza parte garante della transazione: alcune forme di e-cash consentono un trasferimento diretto tra i due utenti del servizio; molto più spesso le uniche transazioni permesse sono quelle consumatore-commerciante con l'obbligo di trasferire periodicamente le somme ricevute alla propria banca che così provvede a versarle nel conto corrente del mercante. Un'altra caratteristica distintiva tra le varie forme di denaro elettronico è il luogo dove le informazioni sulla transazione vengano registrate. Più frequentemente vengono immagazzinate in un database centralizzato che è così possibile monitorare. La minoranza delle tipologie di pagamento su e-cash tengono solo alcune limitate informazioni o non le tengono affatto. Ovviamente in quei modelli per cui sono consentite transazioni tra due utenti consumatori queste informazioni possono venir memorizzate solo sul supporto dell'utente (carte a microchip) e i dati possono venire trasmessi all'ente distributore del servizio solo in particolari occasioni come quando, ad esempio, la carta viene ricaricata. Può essere interessante conoscere quali sono i sistemi basati su denaro elettronico attualmente in circolazione. Il più noto è sicuramente "E-cash" di Digicash. Gli utenti di tale sistema utilizzano denaro corrente per comprare un ammontare equivalente di Digital Cash dalla Mark Twain's Bank. È un sistema software-based e questo significa che l'utente deve installare sul suo personal un prodotto software che funzionerà come un salvadanaio virtuale. A quel punto non si deve far altro che spendere il proprio denaro navigando sul web in qualcuno dei molti siti convenzionati con la Digicash.

Cybercash offre un servizio molto simile a Digicash, diverso è invece il modello di First Virtual la quale ha costruito un sistema di carte di credito che poggia su una rete privata per prevenire i problemi di sicurezza dovuti all'utilizzo di Internet. Questo sistema ha incominciato ad operare alla fine del 1994. Commercianti e consumatori devono avere dei conti correnti presso First Virtual, quando il compratore desidera fare un acquisto dà al venditore il proprio numero di conto, quindi questo spedisce la merce e manda una e-mail con la lista degli acquisti a First Virtual. La banca risponde a sua volta con un'e-mail per confermare

la transazione; ora, se interviene la conferma del consumatore a procedere First Virtual trasferisce il denaro da un conto all'altro, altrimenti blocca il regolamento.

2 Una analisi dei Sistemi di pagamento in Internet

2.1 Criteri di caratterizzazione

I sistemi per il trasferimento elettronico di fondi attualmente esistenti non sono altro che l'esecuzione, tramite calcolatore, di quanto avviene tra cliente e venditore in una transazione tradizionale. In considerazione di ciò è lecito pensare che qualsiasi sistema proposto debba avere le stesse proprietà di uno dei tradizionali sistemi di pagamento. Conseguentemente, una prima distinzione può, quindi, essere fatta tra [16]:

- **Sistemi Token**, in cui il denaro utilizzato per pagare è un insieme di segnali ognuno dei quali rappresentante un determinato valore e la cui somma equivale all'importo dell'operazione, e
- **Sistemi Notational**, in cui il denaro utilizzato per pagare è un messaggio generato dall'acquirente contestualmente all'effettuazione dell'ordine e indicante l'importo della transazione.

2.1.1 Proprietà della transazione commerciale elettronica

2.1.1.1 Proprietà principali

In campo informatico con il termine transazione s'intende un insieme d'operazioni fatte su un insieme di dati. Affinché questo insieme di operazioni venga eseguito in modo corretto, devono essere soddisfatte determinate proprietà.

Si definiscono ora le proprietà principali proprie di una transazione commerciale elettronica e si rimanda al paragrafo successivo per quelle accessorie.

Il gruppo di **proprietà principali**[1] è definito come segue:

- **Atomicità**: la transazione deve occorrere nella sua interezza o in nessuna sua parte
- **Consistenza**: tutte le parti devono convenire sui fatti dello scambio
- **Isolabilità**: la transazione deve essere indipendente da ogni altra
- **Correttezza**: la transazione deve far passare il sistema da uno stato corretto in uno stato anch'esso corretto. Qualora ciò non fosse possibile, deve essere sempre possibile ripristinare l'ultimo stato corretto.

Il gruppo NetBill[2] suddivide la proprietà dell'atomicità in :

- *Atomicità del trasferimento di denaro*: trasferimento atomico di denaro
- *Atomicità del trasferimento di merci*: trasferimento atomico di merci e denaro.

Nel seguito per atomicità ci si riferirà esclusivamente all'atomicità del trasferimento di denaro.

2.1.1.2 Proprietà accessorie

Il gruppo di **proprietà accessorie**[3] è così definito:

- **Economicità**: eseguire la transazione non deve essere costoso né in termini di tempo né in termini di denaro. In particolare si cercherà di distinguere tra :
  - *economicità computazionale*: tempo e risorse di calcolo richieste per eseguire la transazione
  - *costo di gestione*: suddivisa in
    - *costo iniziale*: per l'acquisto del dispositivo o della carta di credito
    - *costo fisso*: canone mensile o annuale per poter usufruire del sistema
    - *costo per operazione*: commissione da pagare al proprietario/gestore del sistema per ogni operazione effettuata
- **Divisibilità**: deve essere possibile scambiare denaro per lo stesso importo (ad es. 10 pezzi da 1 con un pezzo da 10)
- **Scalabilità**: il sistema deve supportare efficientemente più utenti contemporaneamente
- **Compatibilità** : il proprio denaro deve essere compatibile con quello degli altri sistemi

---

[1] In letteratura tali proprietà sono note con il nome ACID dalle iniziali in inglese del nome della proprietà: Atomicity, Consistency, Isolation, Durability.

[2] Gruppo di ricerca statunitense ideatore di un sistema per il commercio elettronico.

[3] In letteratura queste proprietà sono note con il termine di EDSIC dalle iniziali in inglese di Economy, Divisibility, Scaleability, Interoperability, Conservation.

- **Conservabilità** : è composta da
  - *consistenza temporale* : il denaro conserva il suo valore nel tempo
  - *durabilità temporale* : il denaro è facile da immagazzinare e ritrovare.

2.1.2 Transazioni off-line e on-line

Si definisce:

- Transazione **on-line**: se necessita di autorizzazione e/o validazione da fare contestualmente all'ordine
- Transazione **off-line**: se non necessita di autorizzazione e/o validazione da fare contestualmente all'ordine.

Nel seguito si indicherà con +L la transazione on-line e con -L quella off-line.

2.1.3 Denaro anonimo e identificato

Una persona che vede un assegno è in grado di sapere chi è stata la prima persona ad averlo emesso e le altre che eventualmente ne sono entrate in possesso. Guardando una banconota, invece, non è possibile ricostruire alcun passaggio monetario. Da questa considerazione scaturisce la seguente classificazione:

- Denaro **identificato**: il venditore identifica il cliente per mezzo del denaro usato per il pagamento (ad es. assegno).
- Denaro **anonimo**: non è possibile per il venditore identificare il cliente per mezzo del denaro che questi ha usato per pagare.

Nel seguito si indicherà con +I il denaro identificato e con -I quello anonimo.

2.1.4 Proprietà combinate

Combinando le ultime due classificazioni si hanno i seguenti tipi di transazioni:

- **Identificate e on-line (+I+L)**: è la classica transazione fatta con carta di credito, in cui le parti si identificano e il passaggio di denaro deve essere autorizzato dalla banca nel momento stesso dell'acquisto
- **Identificate e off-line (+I-L)**: è la classica transazione fatta con assegno, in cui le parti si identificano e il venditore accetta l'effetto senza controllarne la validità
- **Anonimo e on-line (-I+L)**: è la transazione in cui il denaro usato dal cliente per pagare il venditore è accettato da questi solo dopo averne controllata la validità. In questa transazione il venditore resta anonimo.
- **Anonimo e off-line (-I-L)**: è la transazione fatta con denaro come avviene nella realtà. Il denaro, cioè, non è autenticato e le parti restano anonime.

2.1.5 Visibilità della transazione commerciale

Numerose sono le modalità con cui si può espletare una transazione commerciale, e anche se ai nostri fini interessano solo quelle che coinvolgono parti fisicamente lontane, una loro classificazione deve necessariamente prendere spunto da quella dei tradizionali sistemi di pagamento.
In particolare si cercherà, tramite l'ausilio di apposite tabelle, di caratterizzare la *proprietà della visibilità* distinguendo tra parti e dati. Come parte si considererà il venditore, il cliente, la banca (del cliente, del venditore e/o di entrambi), l'osservatore fisico e l'osservatore remoto. Per dati, invece, si intendono data, importo e dettagli. Nelle tabelle che seguono, in particolare, si dirà che la parte indicata dalla riga di riferimento ha nessuna visibilità oppure una visibilità piena o parziale della parte o del dato indicato dalla colonna a seconda che non lo conosca affatto oppure lo conosca appieno oppure lo conosca solo parzialmente.

2.1.5.1 Visibilità del denaro

	Venditore	**cliente**	**data**	**importo**	**dettagli**
Venditore	piena	parziale	piena	piena	piena
Cliente	piena	piena	piena	piena	piena
Banca	nessuna	nessuna	nessuna	nessuna	nessuna
Oss. Fisico	piena	parziale	piena	piena	piena
Oss. Remoto	nessuna	nessuna	nessuna	nessuna	nessuna

Consideriamo un cliente che entra in un forno a comprare un chilogrammo di pane. I dati propri della transazione sono conosciuti dal cliente, dal venditore, e da tutte le persone (osservatori) che sono in quel momento presenti nel negozio. Mentre però il cliente sa chi è il fornaio, o almeno saprebbe ritrovarlo, il fornaio, così come gli osservatori, non sa necessariamente chi è il cliente.

2.1.5.2 Visibilità dell'assegno

	venditore	cliente	data	importo	dettagli
Venditore	piena	piena	piena	piena	piena
Cliente	piena	piena	piena	piena	piena
Banca	piena	piena	piena	piena	nessuna
Oss. Fisico	piena	piena	piena	piena	piena
Oss. Remoto	nessuna	nessuna	nessuna	nessuna	nessuna

Con il pagamento tramite assegno, tutti i dati della transazione sono ben visibili alle parti in quanto:

1. il cliente per poter compilare correttamente l'assegno, deve identificare il venditore
2. il venditore deve identificare il cliente per non rischiare di avere un assegno falso
3. un osservatore fisico presente nel negozio assiste all'identificazione delle parti ed inoltre conosce tutti i dati della transazione
4. l'unica parte che non ha alcuna visione solo dei dettagli è la banca che garantisce il cliente nei confronti del venditore.

2.1.5.3 Visibilità della carta di credito

	Venditore	cliente	data	importo	dettagli
Venditore	piena	piena	piena	piena	piena
Cliente	piena	piena	piena	piena	piena
Banca	piena	piena	piena	piena	nessuna
Oss. Fisico	piena	parziale	piena	piena	piena
Oss. Remoto	parziale	parziale	piena	nessuna	nessuna

Comportando l'uso della carta di credito comunicazioni su rete aperta, si è dovuto distinguere tra osservatore fisico e remoto. *Nascondere i dati all'osservatore remoto è necessario per garantire non tanto la riservatezza delle informazioni, quanto per evitare il rischio di frodi o furti di denaro. Nel seguito, tutte le misure che saranno prese in considerazione al fine di rendere o considerare un sistema sicuro, sono mirate a rendere inoffensivo solo e soltanto l'osservatore remoto.*

2.1.6 Caratterizzazione dei sistemi di pagamento tradizionali

Prima di analizzare i diversi sistemi per il commercio elettronico è opportuno analizzare le proprietà delle tradizionali transazioni commerciali. La seguente tabella racchiude in modo sintetico le proprietà del pagare tramite contante, assegno e carta di credito.

	Tipo	Atom	Cons	Isol	Corr	Eco	Div	Sca	Comp	Cons
Contante	Token	Si	Si	Si	Si	Si	Si	Si	Si	No
Assegno	Notat	Si	Si	No	Si	No	-	Si	No	Si
Carta	Notat	Si	Si	No	Si	No	-	Si	No	-

Proprietà del contante: come già detto è di tipo token; ha proprietà dell'atomicità e di tutte le altre tranne che della conservabilità in quanto una banconota può variare il suo valore nel tempo. Si pensi, infatti, al mutamento di valore reale di una banconota da £ 1.000 nel 1960 e nel 1997.
Proprietà dell'assegno: è un sistema notational. La transazione non dovrebbe avere la proprietà dell'atomicità in quanto il tempo che intercorre tra l'emissione e l'incasso è variabile ed in tale periodo lo stato della transazione è indefinito; ma è coerente con la scelta fatta di attribuire la proprietà in considerazione del trasferimento di denaro. Non gode della proprietà dell'isolabilità perché può essere condizionata da altre transazioni. Infatti, se nel periodo

che intercorre tra l'emissione e il suo incasso l'acquirente ha spiccato altri assegni che riscossi hanno portato in rosso il suo estratto conto, la transazione non può, ovviamente, concludersi positivamente. Non gode inoltre della proprietà della conservabilità un quanto un assegno di £1.000 del 1960 non ha lo stesso valore di un assegno dello stesso importo ai giorni nostri.
Proprietà della carta di credito: è un sistema notational e non dovrebbe godere, come per l'assegno della proprietà dell'atomicità a causa della distanza delle comunicazioni che intercorrono tra cliente, venditore e issuer (istituto finanziario garante del cliente). Da notare che le proprietà della carta di credito sono identiche a quelle dell'assegno con l'eccezione della conservabilità che qui non è, ovviamente definita dato il mezzo di pagamento.

2.2 Classificazione e analisi

I sistemi di trasferimento elettronico di fondi proposti sono oltre che numerosi anche profondamenti differenti tra loro. In questo lavoro ci si è limitati alla descrizione di quei sistemi utilizzabili su reti aperte e Internet in particolare, sui quali si è riusciti a trovare informazioni sufficienti per classificarli sulla base dei criteri esposti nel precedente capitolo. Il materiale disponibile, infatti, è solamente quello reperibile presso il sito Internet dell'azienda gestore del sistema e perciò finalizzato all'aumento degli utenti. Di conseguenza le informazioni che si trovano sono quasi esclusivamente di tipo commerciale e non di tipo tecnico. Ad alcuni sistemi si sono pertanto attribuite delle proprietà solo per deduzione.
I possibili criteri per classificare questi sistemi sono numerosi ed eterogei [16]. Quello adottato in questo lavoro è conseguenza della rappresentazione del denaro; si è pertanto distinto tra quei sistemi che spediscono in rete messaggi di ordini di pagamento e quei sistemi che invece spediscono denaro digitale.
Nel seguito si utilizzeranno i termini *issuer* e *acquirer*, per indicare rispettivamente, l'istituto bancario garante del cliente e quello garante del venditore.

2.3 Sistemi basati su ordini di pagamento

In questi sistemi il cliente paga generando un messaggio rappresentante un ordine di pagamento. Questo messaggio, criptato o meno a seconda del particolare sistema, è spedito dal cliente, eventualmente utilizzando il venditore come tramite, ad un istituto finanziario il quale esegue il trasferimento di fondi vero e proprio.
I sistemi di questa categoria possono essere ulteriormente divisi in base all'uso della carta della credito o di assegni elettronici.

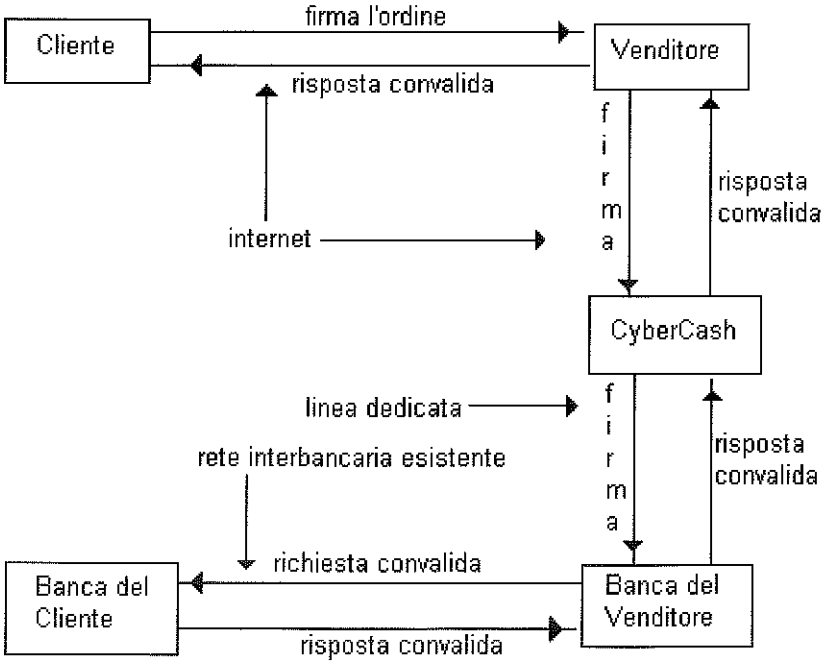
2.3.1 Sistemi basati su carte di credito

Questi sistemi necessitano, da parte del cliente, della titolarità di una carta di credito. Il numero di questa permette agli istituti bancari di identificare il conto corrente da cui prelevare il denaro.

2.3.1.1 CyberCash

La CyberCash Inc. è un istituto finanziario americano che si occupa esclusivamente d'intermediazione finanziaria nel settore del commercio elettronico. Il sistema CyberCash [1] è un prodotto solo software utilizzante algoritmi di codifica asimmetrici, ed attualmente in Europa è possibile utilizzarlo in Germania e in Gran Bretagna. Il grosso vantaggio ed anche la chiave del suo successo è la completa compatibilità con la rete interbancaria esistente.
Una rappresentazione grafica del come si svolge la transazione tramite CyberCash è la seguente:

2.3.1.1.1 *Come avviene la transazione*



Il cliente che decide di effettuare un ordine, genera un messaggio composto da due parti: il primo contiene gli articoli oggetto dell'ordine e il secondo le modalità di pagamento (numero carta di credito, importo dell'operazione). Dopo aver firmato il tutto con la propria chiave privata, spedisce quanto ottenuto al venditore con un normale messaggio di posta elettronica. Il venditore tiene per sé la prima parte del messaggio, firma la seconda parte e la spedisce alla CyberCash sempre come posta elettronica. La CyberCash usa un hardware dedicato per decriptare il messaggio e dopo averlo firmato spedisce il messaggio alla banca del venditore utilizzando non più Internet ma una apposita linea dedicata. La banca del venditore ricevuto il messaggio, lo spedisce alla banca del cliente utilizzando la rete interbancaria esistente. L'issuer, controllata la disponibilità economica dell'acquirente, provvede al trasferimento elettronico dei fondi sul conto del venditore e manda alla banca di questi un messaggio di convalida dell'operazione che si ripercuote all'indietro fino ad arrivare al cliente.
Il costo dell'uso del sistema CyberCash ricade esclusivamente sul venditore il quale inevitabilmente si rivarrà sulla propria clientela. In particolare, il venditore deve pagare a CyberCash un costo iniziale di $ 995 ed un fisso mensile di $ 25. Inoltre il venditore deve pagare per ogni operazione una commissione di $ 0.1 aumentata del 4% dell'importo della transazione. In ogni caso per il cliente vi è da pagare il costo della normale operazione bancaria condotta con carta di credito. Anche il costo computazionale si può dire che non sia basso in quanto il tempo necessario per eseguire la transazione è di circa 15-20 secondi.
Poiché le parti procedono ad una identificazione reciproca e poiché la transazione per poter essere portata a termine ha bisogno di una validazione immediata del denaro usato per pagare, le modalità della transazione sono (+I+L).
Le proprietà della transazione sono le seguenti:

	Token	Atom	Consi	Isol	Corr	Econ	Divis	Scal	Comp	Conse
CyberCash	no	si	no	no	si	no	-	no	si	si

Si nota per prima cosa, anche in considerazione di quanto detto precedentemente, che il sistema non è economico. Inoltre non gode della scalabilità in quanto tutte le operazioni devono avere il server della CyberCash come

intermediario con un inevitabile appesantimento del sistema. Gode della proprietà dell'atomicità in quanto la transazione è svolta da CyberCash direttamente collegato alla rete interbancaria esistente.
Per quanto riguarda la visibilità della transazione, bisogna necessariamente distinguere tra CyberCash che svolge il ruolo di intermediario e le Banche (sia del cliente che del venditore).

	Venditore	Cliente	Data	Importo	dettagli
Venditore	piena	piena	piena	piena	piena
Cliente	piena	piena	piena	piena	piena
CyberCash	piena	nessuna	piena	nessuna	nessuna
Banca	piena	piena	piena	piena	nessuna
Osservatore	nessuna	nessuna	piena	nessuna	nessuna

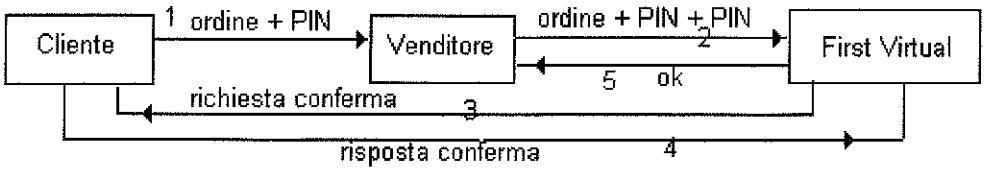
Si nota non solo la piena visibilità tra le parti coinvolte, ma anche che CyberCash non identifica il cliente, in quanto l'unico suo compito è quello di identificare il venditore che ha richiesto l'accredito e di trasmettere tale richiesta alla sua banca. Infine va osservato il buon livello di riservatezza offerto confermato dalla visibilità della transazione da parte dell'osservatore remoto.

2.3.1.2 First Virtual

Il sistema per il commercio elettronico su Internet offerto da First Virtual [2] è estremamente semplice e compatibile con l'infrastruttura interbancaria esistente. Va innanzi tutto precisato che First Virtual è stata la prima e tuttora l'unica banca completamente virtuale: una banca, cioè, che non ha alcun sportello fisico. Le informazioni relative all'operazione sono scambiate come normali e-e-mail tra cliente e venditore utilizzando First Virtual come intermediario. Il sistema non richiede l'uso di un particolare protocollo o software, ma soltanto che l'acquirente sia cliente della First Virtual cambiando la modalità di esecuzione della transazione a seconda che anche il venditore lo sia o no. Il venditore non identifica il cliente e non si ha alcuna trasmissione di dati bancari sulla rete. Se il venditore non è registrato, la transazione è svolta dalla banca per conto del cliente e la banca accredita i soldi sul conto corrente del venditore presso l'istituto finanziario di questi. Se invece, anche il venditore è registrato allora si utilizza un sistema chiamato VirtualPIN. Il nome deriva dal fatto che ogni utente riceve un proprio PIN al momento della registrazione e questo numero lo identifica univocamente in ogni transazione che effettua. Maggiore sicurezza al sistema è data dall'assoluta mancanza di relazione tra il PIN e qualsiasi codice bancario delle parti coinvolte.
Nel momento in cui un utente decide di aprire un conto presso la First Virtual, la banca gli assegna un indirizzo di posta elettronica, mentre l'utente sceglie le modalità di passaggio di denaro dal conto corrente reale a quello presso la First Virtual e viceversa specificando anche la moneta nazionale con cui vuole svolgere le transazioni. La FV, poi caratterizza ogni conto con uno stato indicante se è attivo, sospeso, annullato o riservato solo ai venditori. Gli utenti che vogliono utilizzare tale sistema per i loro acquisti, devono necessariamente disporre di una carta di credito. Per i venditori è richiesto un conto addizionale sul quale saranno effettuati i versamenti di cui sono beneficiari.

2.3.1.2.1 Come avviene la transazione

Il cliente, per registrarsi presso FV, deve compilare un apposito modulo disponibile on-line. Dopo pochi minuti viene chiamato al telefono e invitato a dare il numero della carta di credito e tutti gli altri dati necessari per espletare una normale transazione utilizzando questo metodo di pagamento. Dopo aver aperto il conto, il cliente può effettuare le sue operazioni. Consultato il sito del venditore e deciso quali articoli ordinare, indica nel modulo di acquisto non il numero della carta di credito, ma il PIN rilasciato da First Virtual. Il venditore manda una e-e-mail a First Virtual contenente il PIN del cliente e la descrizione dell'acquisto. First Virtual manda una e-e-mail al cliente chiedendogli conferma dell'operazione. Solo dietro risposta affermativa First Virtual inizia l'operazione di accredito dell'importo sul conto del venditore utilizzando la struttura interbancaria esistente. La First Virtual comunica poi al cliente l'avvenuto versamento.



Stando a quanto dichiarato da First Virtual, il costo per l'utilizzo del sistema è relativamente basso, ed anzi si sono realizzati diversi pacchetti da offrire ai venditori. Il problema dal punto di vista economico, quindi, non è nella commissione da pagare a FV, ma nei costi connessi all'uso della carta di credito che lo rendono poco economico. Il costo computazionale, invece, è molto basso, in quanto la transazione si espleta nella spedizione di e-e-mail non criptate.
Le modalità della transazione sono (-I+L) perché non è richiesta alcuna identificazione del cliente da parte del venditore, mentre si ha la validazione on-line effettuata da First Virtual.
Le proprietà della transazione sono:

	Token	Atom	Consi	Isol	Corr	Econ	Divis	Scal	Comp	Conse
First Virtual	no	si	si	no	no	no	-	no	si	si

Come già detto il sistema, dato l'utilizzo della carta di credito, non è da ritenersi economico. Nonostante il grande scambio di messaggi, il sistema è da considerarsi atomico in quanto il trasferimento di denaro è svolto da First Virtual. Se però avvenisse un fallimento di comunicazione, dopo l'addebito, il sistema transiterebbe in uno stato inconsistente e non corretto. Il sistema è ancora da ritenersi non scalabile in quanto tutte le transazioni vengono svolte da First Virtual, e anche se il tempo computazionale richiesto per ognuna di esse sembra abbastanza contenuto, è inevitabile un deterioramento delle prestazioni.
Per quanto riguarda la visibilità dell'operazione si ha:

	Venditore	Cliente	Data	Importo	dettagli
Venditore	piena	parziale	piena	piena	piena
Cliente	parziale	piena	piena	piena	piena
F. Virtual	piena	piena	piena	piena	piena
Banca	piena	piena	piena	piena	nessuna
Osservatore	parziale	parziale	piena	piena	piena

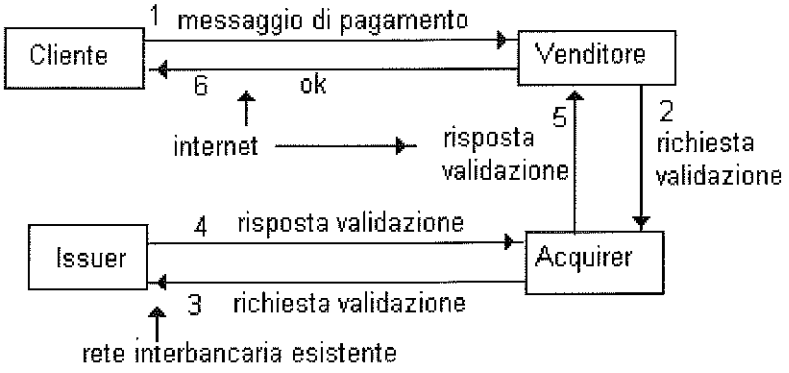
Da intendere come visibilità parziale da parte dell'osservatore, il fatto che questi può vedere sia numero di PIN che indirizzo di posta elettronica, ma non può in alcun modo risalire al numero di carta di credito e al relativo conto corrente. L'osservatore remoto può leggere i messaggi che sono spediti, ma non riesce a identificare pienamente le parti coinvolte nella transazione.

2.3.1.3 iKP

iKP [3] è un insieme di protocolli per pagamenti sicuri realizzato da IBM. Al fine di facilitarne la diffusione, lo sviluppatore ha rinunciato a tutti i diritti ed inoltre ha utilizzato algoritmi crittografici che non violano le restrizioni imposte da molti paesi. Il sistema è stato pensato per l'utilizzo delle carte di credito, ma l'impostazione è abbastanza flessibile da essere compatibile, come si vedrà in seguito, con altri sistemi di pagamento. iKP è un sistema software perché al momento dello sviluppo non era disponibile hardware sicuro per le transazioni tramite smart-card. Questo protocollo, dopo un buon successo iniziale, è stato abbandonato da alcuni istituti finanziari ed attualmente lo utilizza solo la Europay International.

2.3.1.3.1 Come avviene la transazione

Il cliente che volesse effettuare un ordine al venditore, deve per prima cosa registrarsi. In questa fase, al cliente viene rilasciato un PIN da indicare in ogni transazione e, qualora non l'avesse, un'apposita coppia di chiavi crittografiche asimmetriche. Ricevute queste chiavi e l'apposito software, il cliente compila un modulo in cui indica gli estremi della sua carta di credito e, crittografato il tutto, lo spedisce al venditore. Quando il cliente decide di acquistare qualcosa, spedisce al venditore un messaggio contenente gli estremi della merce indicata e il proprio PIN. Ricevuto l'invito a pagare, genera un messaggio di pagamento contenente l'importo ed i suoi dati identificativi, firma il tutto con la propria chiave privata e poi con la chiave pubblica del venditore. Il venditore riceve questo messaggio, lo decripta e dopo averlo criptato prima con la sua chiave privata e poi con quella pubblica della sua



banca, lo spedisce a quest'ultima. L'acquirer contatta l'issuer attraverso la rete interbancaria esistente e dopo aver accertato la disponibiltà economica del cliente, procede all'accredito. Effettuato l'accredito, un messaggio di avvenuta operazione viene spedito all'indietro fino al cliente.
Il costo dei sistemi basati sul protocollo iKP, essendo basato su carta di credito, non è economico. Inoltre, essendo ogni messaggio criptato con due chiavi, è anche computazionalmente costoso.
Le modalità della transazione sono (+I+L) perché il cliente e il venditore si identificano reciprocamente ed inoltre il venditore procede alla validazione immediata dell'operazione.
Per quanto riguarda le proprietà, si potrebbero caratterizzare come illustrato nella seguente tabella:

	Token	Atom	Consi	Isol	Corr	Econ	Divis	Scal	Comp	Conse
iKP	no	si	si	no	si	no	-	si	si	si

Il sistema gode delle proprietà principali della transizione tranne quella della isolabilità in quanto l'operazione viene effettuata solo se il cliente ha la disponibilità economica. Il sistema non è economico perché ad ogni operazione bisogna pagare la normale commissione per l'operazione bancaria; è scalabile perché la validazione è fatta dai vari istituti bancari.
Relativamente alla visibilità della transazione così condotta, non si fa alcuna differenza tra banca del cliente e quella del venditore, in quanto hanno entrambe una visione piena di tutto.

	Vendit	Cliente	Data	Importo	Dettagli
Venditore	piena	piena	piena	piena	piena
Cliente	piena	piena	piena	piena	piena
Banca	piena	piena	piena	piena	nessuna
Osservatore	nessuna	nessuna	piena	nessuna	nessuna

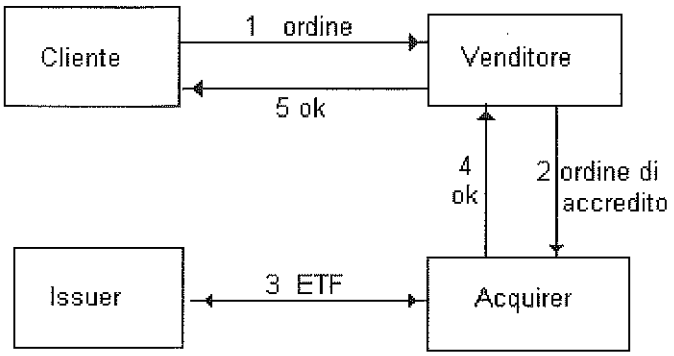
L'osservatore, invece, non ha alcuna visione dell'operazione.

2.3.1.4 SET

La necessità di avere un sistema sicuro per il trasferimento elettronico di fondi da utilizzare nell'ambito del commercio elettronico, ha spinto Mastercard e Visa alla realizzazione del protocollo SET [4] (Secure Electronic Transaction). In effetti il livello di sicurezza offerto è tale da incoraggiare il suo utilizzo sia come numero di transazioni sia come valore della transazione. Tutto si basa su certificati, ossia file digitali rilasciati da terzi con il fine di identificare le altre parti e al contempo accertarne l'autorizzazione all'acquisto e/o vendita on-line. Gli algoritmi crittografici utilizzati sono quelli a chiave asimmetrica e nessun messaggio o ordine viene spedito sulla rete senza che sia stato criptato con almeno una chiave.
Per poter effettuare transazioni tramite il protocollo SET, è necessario avere un conto presso un qualsiasi istituto finanziario convenzionato. Aperto il conto, la banca gli rilascia un certificato, naturalmente criptato, che lo "autorizza" all'acquisto on-line. Anche il venditore, per poter esercitare il suo ruolo, deve farsi rilasciare dalla propria banca (acquirer), un certificato dal quale risulta che è "autorizzato" a vendere. Una volta in possesso della coppia di chiavi e del certificato, il cliente può effettuare i suoi acquisti.

2.3.1.4.1 Come avviene la transazione

Il cliente, deciso che cosa acquistare, spedisce l'ordine al venditore tramite e-e-mail oppure compilando l'apposito form presso il sito di questi. A questo punto il procedimento è svolto per intero dal software a corredo del sistema (distribuito gratuitamente) che rende trasparente il tutto agli utenti. Il cliente riceve una copia del certificato del venditore e ne verifica la validità. Se la verifica termina con successo, al venditore viene spedito l'ordine di pagamento. L'ordine spedito è composto da più parti ognuna delle quali criptata con differenti chiavi in modo tale che siano leggibili solo ai legittimi destinatari. La parte dell'ordine contenente i beni o servizi acquistati è criptata con la chiave pubblica del commerciante, mentre le istruzioni di pagamento con il relativo importo della transazione sono criptate con la chiave pubblica dell'issuer. Viene inoltre aggiunto un piccolo messaggio, parte integrante dell'ordine, che autorizza il pagamento solo per l'ordine cui è allegato. Da notare che tale messaggio, è prima



criptato con la chiave privata del cliente e poi con le chiavi pubbliche dei destinatari. Il venditore che riceve l'ordine di pagamento, può, attraverso la propria chiave privata leggere la parte del messaggio di sua competenza e procedere all'autenticazione del cliente. Se l'autenticazione avviene con successo, il venditore manda al cliente un messaggio di avvenuto ricevimento dell'ordine e poi spedisce alla propria banca l'ordine di pagamento ricevuto. La banca autentica sia il messaggio che il venditore e se il tutto termina con successo, provvede all'informare l'issuer per l'addebito. Fatto l'accredito, invia un messaggio di avvenuto trasferimento di fondi al venditore, il quale, ricevutolo, ne inoltra una copia al cliente.
Il costo dell'uso di questo protocollo è alto in senso computazionale, visto che ogni messaggio è criptato con due chiavi, ed è alto anche in senso economico in quanto, allo stato attuale, i sistemi basati su questo protocollo permettono di pagare solo tramite carte di credito.
Le modalità della transazione sono (+I+L) perché le parti si identificano e la validazione è immediata.

Le proprietà della transazione sono le seguenti:

	Token	Atom	Consi	Isol	Corr	Econ	Divis	Scal	Comp	Conse
SET	no	si	si	no	si	no	-	si	si	si

E' possibile attribuire la proprietà dell'atomicità in quanto il trasferimento di denaro viene effettuato tra banche. Il sistema è ancora da ritenersi scalabile perché il processo di autenticazione viene fatto dal cliente, dal venditore, e dalla banca di questi, senza perciò creare un collo di bottiglia su un'unica parte.
La visibilità della transazione condotta con il protocollo SET è la seguente:

	vend	Cliente	Data	importo	Dettagli
Venditore	piena	parziale	piena	piena	piena
Cliente	parziale	piena	piena	piena	piena
Banca	piena	piena	piena	piena	nessuna
Osservatore	nessuna	nessuna	piena	nessuna	nessuna

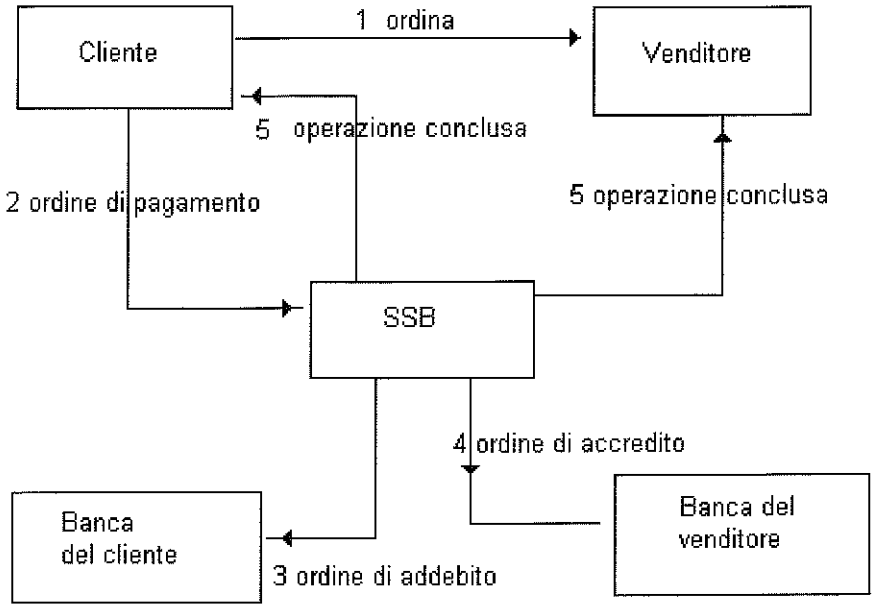
La visibilità parziale tra cliente e venditore e viceversa, è dovuta al fatto che ognuno dei due riceve il certificato dell'altro e controlla la validità di questo senza guardare a chi è intestato. Ma poiché nel certificato sono riportati i dati del suo titolare, se una parte volesse, potrebbe identificare pienamente l'altra trasformando la visibilità da parziale a totale. L'osservatore remoto, non ha alcuna visione né delle parti coinvolte, né dei dati della transazione.

2.3.1.5 TELEpay

TELEpay [5] è l'unico sistema italiano per il trasferimento elettronico di fondi on-line. Ideato dalla SSB (Società per i Servizi Bancari, di proprietà di 225 banche italiane), sembra destinato ad affermarsi in poco tempo. Queste rosee prospettive, non sono dovute tanto al seppur notevole livello di sicurezza, quanto al fatto che gli azionisti della società proponente sono, di fatto, la stragrande maggioranza degli istituti bancari italiani. Al momento la transazione con TELEpay necessita dell'uso della carta di credito con addebito in conto corrente, ma ben presto sarà possibile utilizzarlo anche senza ed è inoltre allo studio la realizzazione della compatibilità col sistema MINIpay (cfr. 5.2.1.2).
Il sistema può essere definito molto sicuro, infatti, la riservatezza e l'integrità dei dati relativi al pagamento sono garantite dal protocollo SSL (livello di trasporto) e da un protocollo proprietario SSB, basato sull'algoritmo RSA con chiavi a 1024 bit (livello di applicazione).

2.3.1.5.1 Come avviene la transazione

Per poter utilizzare il sistema TELEpay, è necessario recarsi alla propria banca (allo stato attuale sono pochi gli istituti aderenti all'iniziativa) e chiedere il rilascio di un apposito codice; nello stesso momento, bisogna indicare anche la password che si intenderà usare (è poi possibile cambiarla in qualsiasi momento). Collegatisi al sito della SSB e raggiunta la pagina per la registrazione al servizio TELEpay, utilizzando il codice appena avuto, si deve prima scaricare il certificato e poi l'apposito plug-in compatibile con le versioni recenti dei maggiori browser. A questo punto la SSB spedisce una e-mail alla quale è necessario rispondere con una conferma. Eseguiti questi passi, la registrazione è ultimata, ma l'abilitazione all'utilizzo del sistema di norma avviene entro il primo giorno lavorativo successivo. Dal punto di vista della sicurezza, va osservato che la fase di registrazione avviene utilizzando il protocollo SHTTP che è una estensione del protocollo HTTP (include apposite funzioni per la tutela della riservatezza dei dati).
Il cliente che vuole effettuare un acquisto si collega al sito del venditore e dopo avergli passato l'ordine, procede al pagamento. Il cliente, quindi, attiva il plug-in ottenuto in fase di registrazione e compila l'ordine con numero di carta di credito, password e codice. Il messaggio, criptato con l'algoritmo RSA, è spedito alla SSB, e dopo le opportune verifiche, se positive, viene dato il via alla normale operazione bancaria. Al termine di questa procedura, al cliente è inviato un messaggio notificante l'avvenuto addebito in conto, oppure, qualora la sua banca non offrisse ancora questo servizio, il messaggio di differimento dell'operazione economica vera e propria. In questo secondo caso, al momento dell'effettivo addebito, il cliente riceverà un ulteriore messaggio.



La registrazione al sistema, così come il software fornito, è gratuita e non ci sono né costi fissi, né costi variabili. Il costo dell'utilizzo di TELEpay, perciò, è dato dal costo di una normale operazione condotta con carta di credito. Il costo computazionale anche se non eccessivo è alto perché l'ordine di pagamento viene criptato sia con l'algoritmo RSA che con il protocollo SSL.
Le modalità della transazione sono (+I+L) perché la validazione (da parte di SSB) è on-line e il venditore procede all'identificazione del cliente.
Le proprietà della transazione sono le seguenti:

	Token	Atom	Consi	Isol	Corr	Econ	Divis	Scal	Comp	Conse
TELEpay	no	si	si	no	si	no	-	no	si	si

Il sistema è ovviamente di tipo notational e il fatto che soddisfa molte proprietà importanti indica una qualità abbastanza buona del sistema. Un punto debole è la scalabilità in quanto tutte le transazioni hanno come intermediario SSB e questo porta inevitabilmente ad una perdita di prestazioni. Riguardo alla proprietà della atomicità, il sistema sicuramente è atomico perché il trasferimento di fondi viene fatto da SSB.
La visibilità della transazione è la seguente:

	Venditore	Cliente	Data	Importo	Dettagli
Venditore	piena	nessuna	piena	piena	piena
Cliente	piena	piena	piena	piena	piena
SSB	piena	piena	piena	piena	nessuna
Osservatore	nessuna	nessuna	piena	nessuna	nessuna

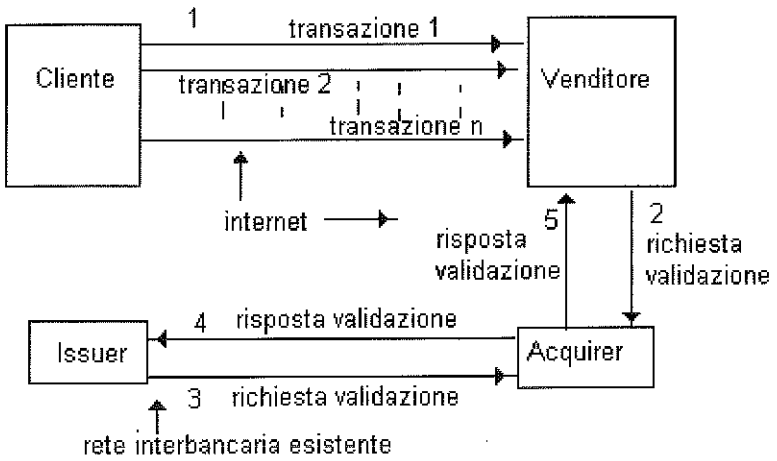
L'osservatore remoto, essendo tutti i messaggi criptati, non ha alcuna informazione.

2.3.1.6 μiKP

Questo sistema è una particolare implementazione del sistema iKP già presentato. Ci si limita quindi a trattare le differenze apportate per rendere tale protocollo adatto per i micropagamenti [6].

2.3.1.6.1 *Come avviene la transazione*

Il cliente per poter acquistare qualcosa presso il venditore, deve prima compilare un modulo di registrazione nel quale indica oltre i dati personali anche i dati identificativi del suo conto corrente presso un qualsiasi istituto finanziario. Il venditore registra tali dati e rilascia al cliente un PIN che dovrà essere utilizzato in ogni transazione. Se poi il cliente non ha una propria chiave crittografica, è il venditore che gliene assegna una dietro richiesta ad uno degli istituti autorizzati. La fase di inizializzazione si conclude con l'accordo tra cliente e venditore dell'importo massimo di credito concessogli.



Quando il cliente decide di acquistare, trasmette l'ordine e ricevuto l'invito a pagare, spedisce un messaggio contenente il suo PIN e l'importo della transazione crittografati con la sua chiave privata. Il venditore espleta l'ordine ma non procede alla validazione e/o incasso del denaro: si limita semplicemente ad aumentare il valore dei crediti vantati nei confronti di quel cliente. Quando poi il cliente acquista un bene il cui valore sommato a quelli precedenti sfonda il massimo credito concessogli, il venditore ricorre all'incasso immediato spedendo un messaggio alla propria banca in cui chiede l'accredito della somma totale. Un messaggio analogo viene inviato al cliente il quale può controllare l'esattezza dei crediti vantati dal venditore ed eventualmente opporsi alla validazione. Se le parti sono d'accordo, l'acquirer procede alla richiesta di versamento all'issuer e poi spedisce al venditore il messaggio di avvenuta operazione. A questo punto il venditore non vanta più alcun credito nei confronti del cliente e quindi si ritorna alla situazione iniziale.
Nonostante l'uso della carta di credito, il costo del sistema è abbastanza contenuto tanto da renderlo adatto ai micropagamenti. Si parla sia di risparmio economico: non si ha il costo della normale operazione bancaria per ogni transazione, ma solo una ogni tanto; sia di risparmio computazionale: i messaggi spediti su rete aperta, hanno la sola firma del mittente con la conseguenza che il messaggio può essere letto da tutti anche se non può essere alterato.
La transazione si svolge con modalità (+I-L) almeno nella maggior parte delle transazioni e diventando (+I+L) per le singole transazioni per cui il venditore richiede la validazione immediata.
Le proprietà della transazione sono le seguenti:

	Token	Atom	Consi	Isol	Corr	Econ	Divis	Scal	Comp	Conse
μiKP	no	si	no	no	no	si	-	si	si	si

Al sistema è attribuita la proprietà dell'atomicità perché il trasferimento è espletato dalla banca. La consistenza e correttezza non sono garantite in quanto il venditore e/o cliente potrebbe perdere alcune operazioni effettuate trovandosi così dei dati differenti di quelli dell'altra parte. La proprietà dell'economicità, inoltre, qui attribuita, va valutata in base al valore massimo del credito concesso portando a giudizi ben diversi nel caso in cui esso sia di 100$ o di 10.000$.

Per quanto riguarda la visibilità della transazione, bisogna tener conto che essendo gli ordini criptati con la sola chiave privata del cliente, questi sono leggibili, ma non alterabili, da tutti. L'osservatore remoto, in particolare, dall'osservazione di questi ordini, può identificare le parti coinvolte leggendo anche l'importo della transazione.

	Vendit	Cliente	Data	Importo	Dettagli
Venditore	piena	piena	piena	piena	piena
Cliente	piena	piena	piena	piena	piena
Banca	piena	piena	piena	piena	nessuna
Osservatore	piena	piena	piena	piena	nessuna

2.3.2 Sistemi basati su assegni

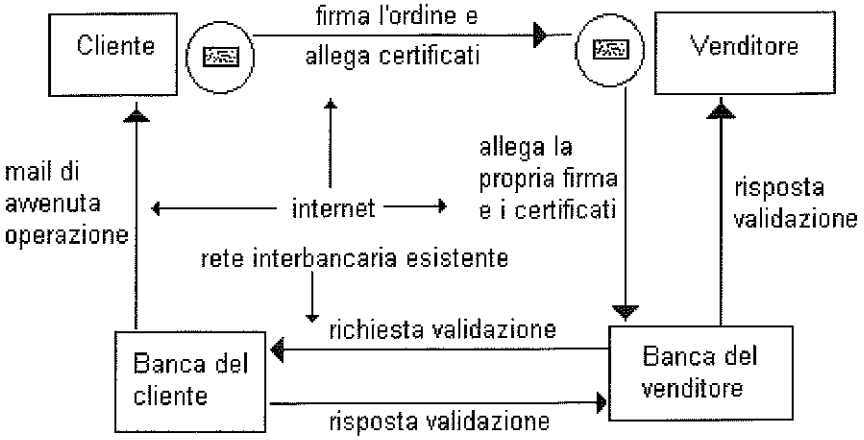
I sistemi appartenenti a questa categoria usano come ordine di pagamento un messaggio molto simile al normale assegno bancario. In genere il cliente identifica il venditore e genera un assegno compilandolo con i propri dati e con quelli del commerciante. Spedisce quindi il tutto al proprio istituto finanziario che procede all'accredito/addebito.

2.3.2.1 Electronic Cheque

Progettato da FSTC [7] (Financial Services Technology Consortium), un consorzio di circa 90 membri per la maggior parte istituti bancari americani, il sistema è stato concesso in uso proprio a questi. Nonostante si sia ancora in una fase di sperimentazione, i risultati ottenuti sono giudicati estremamente positivi. Il sistema utilizza la già esistente rete interbancaria per le operazioni di passaggio di denaro tra cliente e venditore e la rete aperta (Internet) per far viaggiare messaggi (e-e-mail) rappresentanti assegni.
Il cliente che decide di utilizzare questo sistema per saldare le sue transazioni commerciali, deve innanzitutto avere un conto corrente presso una delle banche aderenti alla sperimentazione, e dietro esplicita richiesta, gli viene recapitato un piccolo dispositivo elettronico paragonabile al tradizionale blocchetto di assegni. Questo dispositivo è una *smart-card* che collegata al computer per mezzo di un'apposita interfaccia, espleta la funzione di emissione e validazione di assegni. L'algoritmo crittografico usato è quello della chiave asimmetrica e ogni assegno emesso è criptato con la chiave privata dell'utente. Tale chiave è rilasciata da un istituto di certificazione su richiesta della banca la quale provvede ad inserirla nel dispositivo in modo permanente. Nel dispositivo, sono inoltre inseriti due certificati di cui il primo autentica l'issuer e il secondo autentica un altro istituto bancario garante di quello del cliente (negli USA la Banca Centrale). La smart card, come un normale blocchetto di assegni, tiene traccia di tutti gli assegni emessi e dei relativi dati ed inoltre, per poterla utilizzare è richiesto un PIN tramite il quale si presume che l'utilizzatore sia anche il legittimo proprietario.

2.3.2.1.1 Come avviene la transazione:

Il cliente si collega tramite Internet al sito del venditore. Una volta deciso cosa acquistare e comunicatolo al venditore, questo lo invita a spedirgli un assegno per l'importo corrispondente. Il cliente, quindi, crea una e-e-mail nella quale viene inserito l'ordine e l'assegno, aggiunge i due certificati autenticanti le banche, firma il tutto con la propria firma privata e spedisce il messaggio cosi ottenuto al venditore. Questi prende il messaggio ricevuto e ci aggiunge un documento contenente i suoi dati, il certificato autenticante il suo istituto di credito ed un altro certificato autenticante il garante della sua banca.



Firmato il tutto con la propria chiave privata, il messaggio cosi ottenuto è spedito alla banca del venditore. A questo punto la transazione abbandona Internet e si sposta sulla rete interbancaria esistente. La banca del venditore decripta il messaggio utilizzando le chiavi pubbliche del venditore e del cliente. Verifica poi l'autenticità dei certificati allegati e se tutto è corretto, spedisce le informazioni relative al pagamento alla banca del cliente. Questa, oltre a prelevare l'importo corrispondente dal conto del cliente e a spedirgli una e-e-mail indicante gli estremi dell'operazione, spedisce il messaggio di operazione eseguita alla banca del venditore, la quale incrementa il relativo conto e spedisce al venditore una e-e-mail notificandogli il buon esito della transazione.
Sebbene questo sia il metodo più usato nella transazioni con il sistema Electronic Cheque, sono ammessi anche altri metodi di pagamento del tutto analoghi a quelli effettuati con i tradizionali assegni cartacei. E' possibile, cioè, che il cliente spedisca l'assegno elettronico direttamente alla sua banca o alla banca del venditore. Sarà poi la banca a comunicare al commerciante l'esecuzione dell'operazione di accredito.
La FSTC si dichiara estranea all'utilizzo del sistema a fini commerciali e precisa che il suo ruolo si è limitato esclusivamente alla realizzazione del progetto.
Il sistema è ritenuto molto economico, perché l'hardware è al momento fornito gratuitamente dalle banche, e non vengono fatte pagare fissi mensili. Le uniche spese a carico degli utenti del sistema sono le normali spese di operazione di conto corrente ed una commissione fissa di 0.05 $ per operazione.
Data l'identificazione reciproca tra cliente e venditore e la validazione on-line, le modalità della transazione sono (+I+L).
Le proprietà della transazione svolta con il sistema Electronic Cheque, sono le seguenti:

	Token	Atom	Consi	Isol	Corr	Econ	Divis	Scal	Comp	Conse
Electronic Cheque	no	si	si	no	si	si	-	si	si	si

Come si vede il sistema che è di tipo Notational, gode di tutte le proprietà eccetto quella della isolabilità. Questo perché si conviene che un assegno può essere pagato solo se è coperto. Se non lo fosse, la transazione per la quale l'assegno è stato utilizzato, non sarebbe indipendente dalle altre.
Relativamente alla visibilità dell'operazione svolta con questo sistema, in generale tutti hanno una visione piena di tutto, con l'eccezione della banca, che come al solito non sa dei dettagli dell'operazione, e dell'osservatore (in questo caso esclusivamente remoto) che è in grado di rilevare solo la data.

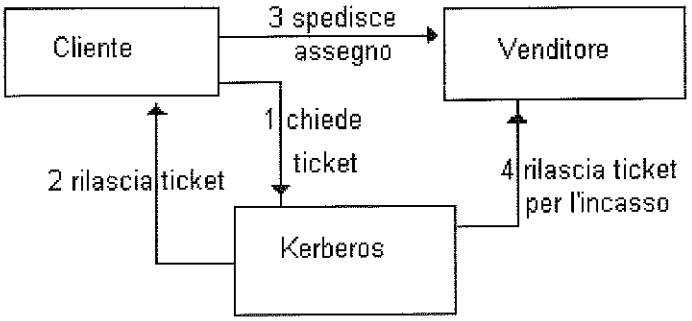
	Vendit	Cliente	Data	Importo	Dettagli
Venditore	piena	piena	piena	piena	piena
Cliente	piena	piena	piena	piena	piena
Banca	piena	piena	piena	piena	nessuna
Osservatore	nessuna	nessuna	piena	nessuna	nessuna

2.3.2.2 NetCheque

Questo sistema è stato realizzato al Dipartimento di Informatica della University of Southern California, e come si deduce dal nome è rivolto alla gestione degli assegni elettronici. NetCheque [8] è implementato utilizzando le caratteristiche di Kerberos[4] e permette l'emissione e l'incasso di assegni solo tra titolari di appositi conti. Si utilizzano algoritmi crittografici a chiavi simmetriche che si applicano esclusivamente per autenticare il richiedente un determinato servizio, e in nessun modo all'assegno che perciò è spedito in chiaro sulla rete sotto forma di e-e-mail.
In realtà, data l'infrastruttura utilizzata, il problema della sicurezza inteso come rischio di frodi non esiste, ma invece è evidente l'assoluta mancanza di riservatezza di quanto trasmesso.
D'altro canto bisogna considerare che questo sistema è stato pensato per transazioni di modesto valore, per cui l'obiettivo dell'economicità, inteso anche come economicità computazionale, è stato raggiunto proprio a scapito della riservatezza.

2.3.2.2.1 Come avviene la transazione.

Il cliente che decide di acquistare qualcosa, paga emettendo un assegno. Il messaggio rappresentante l'assegno, contiene oltre a data, numero di conto del traente e beneficiario, anche l'importo. Poiché nel sistema Kerberos, un utente può fare qualcosa solo dietro espressa autorizzazione, il cliente, prima di spedire l'assegno, deve chiedere il permesso (rilascio di un apposito ticket). Il venditore che riceve l'assegno sotto forma di e-e-mail, per poterlo incassare, deve anche lui chiedere il permesso. Solo dopo aver ottenuto l'apposito ticket può accreditarne l'importo sul proprio conto.



Il software concesso gratuitamente nasconde tutta questa complessa procedura rendendo molto semplice per l'utente l'emissione e/o l'incasso di assegni. Il costo per l'utilizzo del sistema è molto contenuto, tanto da renderlo adatto ai micropagamenti.
Le modalità della transazione sono (+I+L) in quanto cliente e venditore si identificano reciprocamente ed inoltre si ha la validazione immediata perché il venditore per poterlo incassare, deve avere la necessaria autorizzazione da Kerberos.
Le proprietà della transazione sono le seguenti:

	Token	Atom	Consi	Isol	Corr	Econ	Divis	Scal	Comp	Conse
NetCheque	no	si	si	no	si	si	-	si	si	si

Il sistema, che è di tipo notational, gode della proprietà dell'atomicità in quanto l'operazione di trasferimento di fondi viene fatta da Kerberos. La transazione, così come le altre condotte con assegno, non è isolabile perché il suo buon fine deriva dalla copertura economica dello stesso. Il sistema inoltre, poiché la validazione può essere richiesta da un qualunque server Kerberos è da ritenersi scalabile.
La visibilità della transazione è la seguente:

---

[4] Un sistema di autenticazione sviluppato presso il MIT e distribuito gratuitamente.

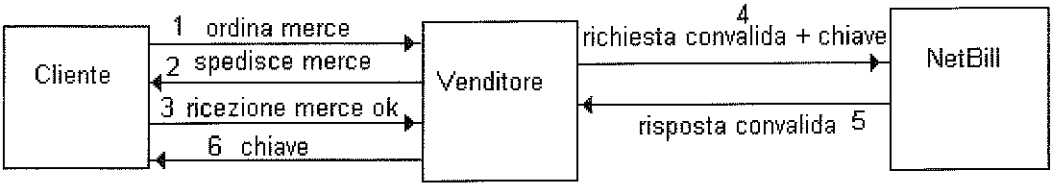
	vend	Cliente	Data	importo	dettagli
Venditore	piena	piena	piena	piena	piena
Cliente	piena	piena	piena	piena	piena
Kerberos	piena	piena	piena	piena	nessuna
Osservatore	piena	piena	piena	piena	nessuna

Come già detto, essendo l'assegno spedito in chiaro, i dati in esso contenuti sono visibili a tutti, anche all'osservatore remoto.

2.3.2.3 NetBill

E' un sistema [9] per il commercio elettronico finalizzato all'acquisto di merce digitale (foto, articoli, ecc..) e al contestuale pagamento del suo valore. Per la sicurezza e riservatezza delle informazioni si utilizzano sia chiavi simmetriche che asimmetriche e per poter effettuare acquisti è necessario avere un apposito conto NetBill. Tale conto è collegato a quello presso un normale istituto finanziario sul quale avvengono effettivamente le transazioni per mezzo della carta di credito. Ad ogni modo questo sistema è incluso nel gruppo di quelli basati su assegni perché il messaggio che il cliente spedisce al venditore ha molte somiglianze con questo tipo di pagamento.

2.3.2.3.1 Come avviene la transazione:



Il cliente si collega al sito del venditore e decide quale bene acquistare. Supponiamo che abbia scelto una fotografia. Inoltrato l'ordine, il venditore cripta la foto e la spedisce al cliente. Il software del cliente controlla l'integrità di quanto ricevuto e spedisce un messaggio di corretta ricezione al venditore. Il venditore prende questo messaggio, ci allega i dati del conto del cliente e la chiave con cui è stata criptata la foto e spedisce il tutto a NetBill. Questi, controllata la disponibilità economica del cliente, spedisce un messaggio di avvenuto accredito al venditore, il quale solo dopo che gli è stato notificato il versamento, spedisce al cliente la chiave di decodifica dell'immagine. Se la comunicazione fallisce, la chiave può essere richiesta dal cliente presso NetBill.
Il gruppo NetBill ha venduto i diritti per l'utilizzo del progetto a CyberCash, la quale al momento, non lo ha ancora trasformato in prodotto commerciale. Questo però non impedisce una stima del costo che usare il sistema comporta. A tal fine, è ragionevole supporre che il sistema non sia economico in quanto al costo dell'operazione con carta di credito, va aggiunta la commissione di competenza di NetBill per l'espletamento del ruolo di intermediario nella transazione. Inoltre il costo computazionale non è banale, in quanto anche se si utilizzano algoritmi a chiave simmetrica, il tempo necessario per espletare la transazione è abbastanza alto.
Le modalità della transazione sono (+I+L) in quanto le parti si identificano e il venditore controlla immediatamente la solvibilità del cliente.
Le proprietà della transazione condotta con il sistema NetBill sono le seguenti:

	Token	Atom	Consi	Isol	Corr	Econ	Divis	Scal	Comp	Conse
NetBill	no	si	si	no	si	no	-	no	no	si

Il sistema, di tipo notational, gode di tutte le proprietà principali, ma non è economico. Non è scalabile in quanto tutte le transazioni hanno come intermediario NetBill e non è compatibile con gli altri sistemi. Si attribuisce la proprietà dell'atomicità perché il trasferimento viene effettuato da NetBill; ad ogni modo anche se avvenisse un fallimento nella comunicazione, sono previste apposite procedure di ripristino.

La visibilità della transazione con il sistema NetBill è la seguente:

	Venditore	Cliente	Data	Importo	dettagli
Venditore	piena	piena	piena	piena	piena
Cliente	piena	piena	piena	piena	piena
NetBill	piena	piena	piena	piena	nessuna
Osservatore	nessuna	nessuna	piena	nessuna	nessuna

Poiché i messaggi viaggiano criptati, l'osservatore remoto non può conoscere i dati della transazione; le altre parti, invece, hanno una visione piena di tutto.

2.4 Sistemi che usano denaro digitale

In questo gruppo sono stati inclusi tutti quei sistemi che rappresentano, in un qualche modo, denaro elettronico. In questi sistemi il cliente, al momento della transazione commerciale, è già in possesso del denaro digitale e paga spedendolo direttamente al venditore.
Si è ritenuto opportuno creare un sottogruppo contenente solo i sistemi di portafoglio elettronico perchè, al momento, non prevedono un trasferimento di denaro on line al momento del pagamento.

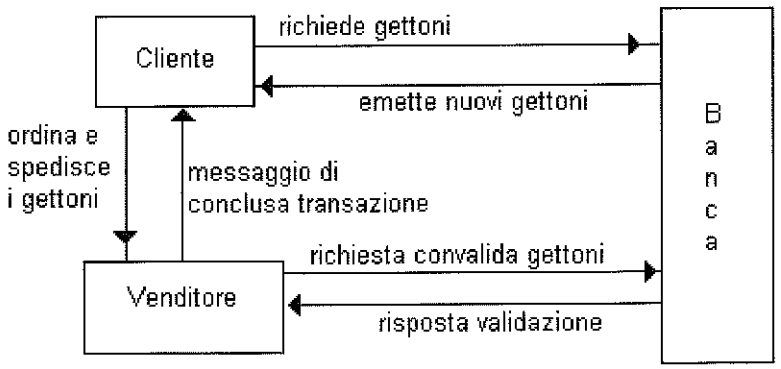
2.4.1 Con trasferimento di denaro on-line

2.4.1.1 DigiCash

Questo sistema [12], conosciuto anche con il nome di ecash™, è uno dei pochi che utilizza effettivamente denaro elettronico. E' un sistema solo software e il denaro è immagazzinato sul computer del cliente. La transazione non richiede che l'acquirente si identifichi al venditore, ma la banca è in grado di risalire al cliente per cui è stato emesso quel denaro. Il sistema è stato sperimentato con 30.000 consumatori, 60 venditori e attualmente sono 4 le banche che emettono questo denaro. I gettoni usati rappresentano dollari statunitensi e non possono essere scambiati con altre monete nazionali. Ad ogni modo, in Europa, il sistema è stato già accolto dalla Deutsche Bank e chiunque volesse usarlo, anche in Italia, non deve far altro che contattare la più vicina agenzia.

2.4.1.1.1 Come avviene la transazione:

Il cliente si collega alla banca e ordina di trasformare una parte dei soldi depositati sul proprio conto corrente in moneta elettronica. La banca genera dei gettoni per l'importo corrispondente, ne segna il numero di serie nell'archivio dei coin emessi e li spedisce al cliente che li immagazzina sul proprio PC. Quando questi decide di acquistare qualcosa, si collega al sito del venditore ed effettua l'ordine. Ricevuto l'invito a pagare, gli spedisce i gettoni per l'ammontare della transazione. Il venditore manda quanto ricevuto alla banca del cliente e ne richiede la validazione. La banca verifica l'autenticità controllando nell'archivio dei gettoni emessi e in quello dei gettoni già spesi, e poi invia al venditore un messaggio di validazione o di rifiuto della transazione a seconda dell'esito positivo o negativo dei controlli effettuati. Questi, ricevuto il messaggio ne manda una copia all'acquirente.
La transazione così realizzata potrebbe avere una serie di problemi. Per evitare rischi di frodi, il numero di serie dato ai gettoni, lungo circa 100 bit, non è progressivo ma generato casualmente. Potrebbe accadere, quindi, che a due clienti distinti sia emesso un gettone con lo stesso numero di serie creando problemi a colui che lo spende per



ultimo.
I gettoni sono utilizzabili per una sola transazione commerciale e al momento in cui il venditore li presenta per la validazione può scegliere se farsene rilasciare altri per un importo equivalente oppure se depositare il tutto sul proprio conto corrente.
Non è specificato quali siano gli algoritmi crittografici usati; è comunque realistico supporre che la banca emittente i gettoni, provveda a criptarli con una apposita chiave e che li spedisca al cliente. Poiché cliente e venditore non alterano in alcun modo il coin, quando questo ritorna alla Banca per la validazione, questa si limita a controllare che quel gettone sia stato criptato con la chiave di cui è in possesso, per cui è possibile per chiunque, leggerne il valore.
Il costo del sistema sia in termini economici che in termini computazionali è piuttosto basso. Infatti, il tempo necessario per eseguire la transazione è di pochi secondi (DigiCash stima in 3), ed il costo economico è solo la normale operazione bancaria da pagare quando si richiede il rilascio di nuovi gettoni.
La transazione con il sistema DigiCash ha modalità (-I+L) perché le parti non si identificano (-I) ed i gettoni usati sono validati on-line (+L).
Le proprietà del sistema DigiCash sono le seguenti:

	Token	Atom	Consi	Isol	Corr	Econ	Divis	Scal	Comp	Conse
DigiCash	si	no	no	no	no	si	si	si	si	si

Apparentemente la serie di no farebbe pensare ad un sistema di cui diffidare. In particolare, vengono a mancare tutte le proprietà principali della transazione. La proprietà dell'atomicità manca perché se un fallimento di comunicazione avviene nella fase di trasferimento dei gettoni dal cliente al venditore, la transazione non occorre nella sua interezza e il sistema arriva in uno stato inconsistente e incorretto. La proprietà della isolabilità manca a causa della possibilità dell'esistenza di due gettoni aventi lo stesso numero di serie. In questo caso, il possessore legittimo di un coin valido, non può incassarlo perché un altro legittimo possessore di coin altrettanto valido ha già provveduto all'incasso.
La visibilità della transazione può essere così rappresentata:

	Vend	Cliente	Data	Importo	Dettagli
Venditore	piena	nessuna	piena	piena	piena
Cliente	piena	piena	piena	piena	piena
Banca	piena	nessuna	piena	piena	nessuna
Osservatore	nessuna	nessuna	piena	piena	nessuna

Mentre il cliente sa chi è il venditore, questi non identifica in alcun modo il cliente, così come non lo identifica la Banca, la quale potrebbe solo registrare per quale utente è stato emesso quel determinato gettone. L'osservatore remoto ha una visibilità piena dell'importo della transazione perché può leggere il valore dei gettoni, ma non può identificare le parti.

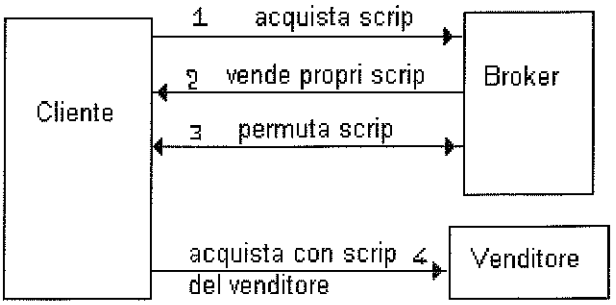
2.4.1.2 Millicent

Millicent [13] è un sistema realizzato da Digital e molto utilizzato in USA e Canada. E' di tipo token e i gettoni utilizzati per effettuare i pagamenti sono detti scrip. Questi scrip hanno, in genere, un valore di qualche frazione di $ e sono validi solo presso il venditore che li ha emessi e per un periodo limitato. La particolarità del sistema, infatti, è che il venditore accetta solo gettoni da lui stesso emessi. Per evitare che il cliente abbia tanti scrip quanti sono i venditori da cui acquista, la Digital, o più in generale un broker, svolge un ruolo di intermediario nella transazione. Millicent offre tre differenti tipi di scrip, ognuno dei quali con un differente livello di sicurezza. Si parte dallo *scrip base* che non ha alcuna misura di protezione, per arrivare allo *scrip sicuro* che utilizza apposite codifiche per renderlo inattaccabile e indecifrabile. Il sistema intermedio, chiamato *scrip inalterabile,* utilizza algoritmi crittografici che permettono a chiunque di leggerne il valore, ma non di alterarlo. Di fatto, dopo oltre un anno dall'utilizzo del sistema, più del 95% dei clienti usano lo scrip sicuro.

2.4.1.2.1 Come avviene la transazione

Il cliente che intende fare acquisti presso venditori che utilizzano questo sistema, contatta il suo broker e acquista, per un ammontare a piacere, non scrip di un particolare venditore, ma scrip del broker. Quando poi il cliente decide di comprare qualcosa, comunica il suo intento al broker spedendo gli scrip. Il broker prende dal proprio portafogli

gli scrip del venditore indicato dal cliente e glieli spedisce. Il cliente può a questo punto concludere la transazione spedendoli al venditore che provvede da solo alla validazione.



Il sistema, anche perché rivolto ai micropagamenti, è economico. Il software è gratuito e non bisogna pagare alcuna commissione al momento dell'acquisto e/o della permuta dei gettoni. L'unico vincolo è imposto da un limite inferiore di 10$ per la ricarica del portafoglio.
Le modalità della transazione sono (-I+L) perché il venditore non identifica il cliente e gli scrip utilizzati per pagare sono validati dal venditore al momento in cui li riceve. E' da notare, però, che il broker procede all'identificazione del cliente nel momento in cui questi chiede di permutare gli scrip, ma ai fini della nostra definizione di on-line tale identificazione non ha alcuna importanza.
Per quanto riguarda le proprietà del sistema Millicent abbiamo:

	Token	Atom	Consi	Isol	Corr	Econ	Divis	Scal	Comp	Conse
Millicent	si	no	no	si	no	si	si	si	no	no

Il sistema non è atomico perché un fallimento durante il trasferimento degli scrip causa la non esecuzione totale della transazione, ed inoltre porta in uno stato inconsistente e incorretto. Il sistema non è compatibile con gli altri sistemi ed addirittura non si ha la compatibilità di gettoni emessi da venditori differenti. Non gode inoltre della proprietà della conservabilità data la limitata validità temporale.
Supponendo di utilizzare il terzo sistema proposto, cioè quello più sicuro, la visibilità della transazione è la seguente.

	Venditore	Cliente	Data	Importo	dettagli
Venditore	piena	nessuna	piena	piena	piena
Cliente	piena	piena	piena	piena	piena
Broker	piena	piena	nessuna	nessuna	nessuna
Osservatore	piena	nessuna	piena	parziale	nessuna

L'osservatore remoto, osservando i gettoni, ha una visione piena del venditore ma non altrettanto del cliente. Non è chiaro se riesce a dedurre l'importo della transazione. In linea di massima si potrebbe dire che se il venditore emette coin di un solo valore, allora è possibile determinare quanto il cliente ha pagato contando il numero di gettoni spediti, se invece i gettoni hanno valore differente, tale operazione non è possibile.

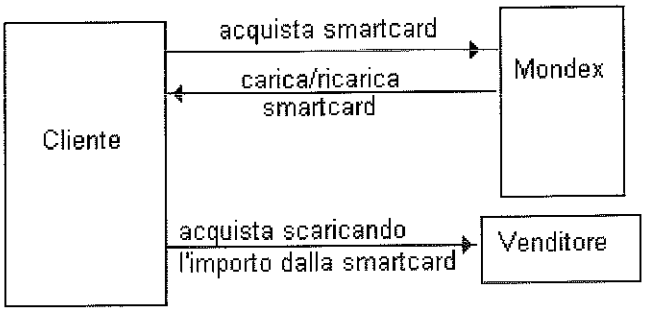
2.4.1.3 Mondex

Il sistema sviluppato da un'importante compagnia inglese, si rivolge a coloro che richiedono un elevato grado di sicurezza nell'effettuare pagamenti non solo su Internet. Per poter effettuare una transazione con Mondex [14] è necessario acquistare l'apposita smart-card e un apposito lettore dotato di interfaccia da collegare al calcolatore. La smart-card, infatti, può essere utilizzata non solo per i pagamenti su rete, ma anche come una normale carta di credito. La limitazione del sistema è il fatto che il denaro può essere trasferito esclusivamente tra smart-card, ma nei

paesi anglosassoni la quasi totalità dei venditore virtuali offre questo metodo di pagamento. La smart-card ha la funzione di svolgere tutte le operazioni crittografiche relativamente al denaro da usare, ed inoltre è l'unico luogo in cui i soldi sono immagazzinati. L'utilizzo delle più avanzate tecnologie, rende la carta estremamente sicura in quanto eventuali frodi dovrebbero essere necessariamente legate alla duplicazione della stessa il che renderebbe tali tentativi estremamente costosi. Il chip residente su di essa è dotato di appositi sensori che attivano un processo di autodistruzione in caso di rilevamento di radiazioni inusuali o attacchi software o elettrici. Il titolare può, in questo caso, rivolgersi alla propria banca e richiedere il rilascio di un'altra carta. Inoltre, le continue migliorie e modifica dei circuiti interni e delle chiavi, fatte gratuitamente dall'azienda ai propri clienti, riduce il propagarsi temporale di frodi. Bisogna aggiungere che sulla smart-card vi sono più chiavi crittografiche, in modo che il legittimo titolare possa scegliere di volta in volta, anche casualmente, quale usare. La carta tiene traccia delle ultime 10 transazioni effettuate ed in ogni momento non vi possono essere disponibili più di 500 sterline inglesi. Durante la transazione sono spediti: il numero identificativo della carta; il numero identificativo della transazione (generato casualmente); l'importo della transazione e la moneta nazionale da usare. La ricarica della disponibilità economica della smart-card, può avvenire collegandosi alla apposita pagina della Mondex oppure a quella del proprio istituto finanziario.

2.4.1.3.1 Come avviene la transazione:

Il cliente che decide di acquistare qualcosa, si collega al sito del venditore e una volta ordinato e ricevuto l'invito a pagare, gli spedisce un messaggio contenente l'importo e altri dati criptati prima con la propria chiave privata e poi con quella pubblica del ricevente. Il venditore che riceve questo messaggio, lo decripta e lo memorizza nel proprio dispositivo. Non è chiaro dalla documentazione disponibile se il denaro ricevuto può poi essere utilizzato dal ricevente per ulteriori operazioni o se deve essere necessariamente spedito alla banca per l'accredito.



Il costo della transazione condotta con Mondex è abbastanza contenuto, infatti, al costo iniziale di circa 30£ per l'acquisto del dispositivo, si sommano solo le commissioni bancarie per la ricarica del portafogli.
Le modalità della transazione sono (+I-L) perché il venditore identifica l'acquirente per mezzo delle chiavi asimmetriche usate. La validazione non è contestuale all'operazione, ma si ha solo quando il titolare della carta si presenta alla banca, anche in modo virtuale, e accredita il tutto sul proprio conto.
Dall'osservazione della seguente tabella, si può formulare un giudizio estremamente positivo sul sistema Mondex.

	Token	Atom	Consi	Isol	Corr	Econ	Divis	Scal	Comp	Conse
Mondex	si	si	si	si	si	si	si	si	si	si

Il sistema è da considerarsi atomico perché al momento del pagamento il cliente invia al venditore un unico gettone, creato in quel momento, per l'importo della transazione. In questa situazione un eventuale fallimento di comunicazione è rilevato dal cliente che provvede a rispedirlo senza per questo che venga considerata una doppia spesa.
Indicando con Mondex anche la banca del cliente e del venditore, la visibilità della transazione è la seguente.

	Vendit	Cliente	Data	Importo	Dettagli
Venditore	piena	piena	piena	piena	piena
Cliente	piena	piena	piena	piena	piena
Mondex	piena	piena	piena	piena	nessuna
Osservatore	nessuna	nessuna	piena	nessuna	nessuna

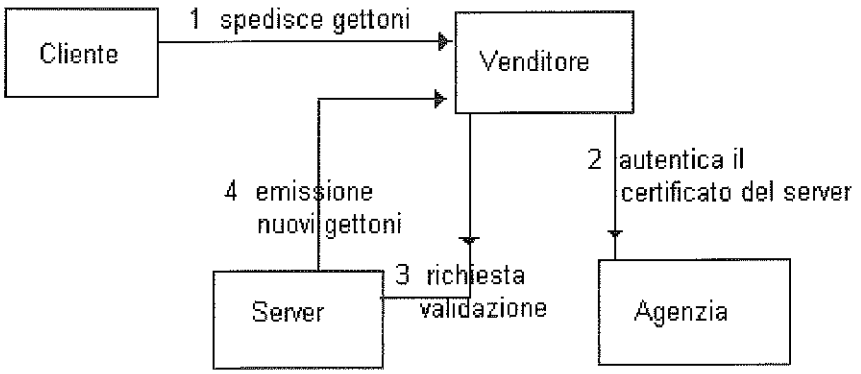
L'osservatore remoto non ha alcuna visibilità delle parti coinvolte né dell'importo della transazione. Per quanto riguarda le altre parti, invece, hanno una visione piena di tutto.

2.4.1.4 NetCash

Il sistema NetCash [15] è stato progettato e sviluppato all'ISI (Information Sciences Institute) della University of Southern California. E' una soluzione puramente teorica (quindi non un prodotto commerciale) al problema del trasferimento elettronico di fondi on-line che adotta valide soluzioni per l'autenticazione e per evitare il rischio di frodi. Il denaro è rappresentato da gettoni emessi da uno dei tanti server autorizzati. Ogni gettone, criptato con la chiave privata dell'emittente, contiene il nome del server che lo ha emesso, un proprio numero di serie (progressivo) e il suo valore. Il server, per poter essere autorizzato all'emissione di gettoni, deve registrare la propria coppia di chiavi asimmetriche e depositare quella pubblica presso un'apposita agenzia, la quale provvede al rilascio di un certificato e di un apposito numero identificativo (ID).
Su richiesta del cliente, il server genera i coin per l'ammontare stabilito e dopo averne memorizzato il numero di serie in un apposito archivio, li spedisce al richiedente. A questo punto il cliente può utilizzare tale denaro per effettuare le proprie transazioni commerciali.

2.4.1.4.1 Come avviene la transazione:

Spedito l'ordine al venditore, il cliente spedisce anche i gettoni per l'importo stabilito.
Il venditore che riceve i gettoni, tramite il collegamento alla chiave pubblica del server emittente, verifica l'autorizzazione di questi ad emettere denaro. Se il controllo ha successo, il venditore spedisce i gettoni ricevuti al server per la validazione. Questi, ricevuti i gettoni, controlla la presenza del loro numero di serie nell'archivio dei



gettoni emessi, riconoscendo e segnalando immediatamente eventuali tentativi di frode.
I gettoni validi presentati al server, sono immediatamente annullati ed al venditore ne sono spediti altri (cioè nuovi gettoni) per lo stesso importo.
Se il sistema fosse utilizzato a fini commerciali, dovrebbe avere un costo relativamente contenuto tale da renderlo adatto anche ai micropagamenti. Anche il costo computazionale è abbastanza contenuto essendo i messaggi criptati solo con una chiave.
Le modalità della transazione sono perciò (-I+L) in quanto il cliente e il venditore non si identificano, e la validazione avviene immediatamente.
Le proprietà della transazione condotta con NetCash possono essere così definite:

	Token	Atom	Consi	Isol	Corr	Econ	Divis	Scal	Comp	Conse
NetCash	si	no	no	no	no	si	si	si	si	si

Il sistema non è da ritenersi atomico in quanto il trasferimento di denaro potrebbe non avvenire in caso di un fallimento di comunicazione nel trasferimento dei gettoni, portando il sistema in uno stato incorretto e inconsistente. Il sistema è da giudicarsi, per quanto detto, economico ed inoltre è da ritenersi scalabile vista la molteplicità dei server autorizzati all'emissione e alla validazione dei gettoni.
La visibilità della transazione è la seguente:

	Venditore	Cliente	Data	Importo	Dettagli
Venditore	piena	nessuna	piena	piena	piena
Cliente	piena	piena	piena	piena	piena
Server	piena	parziale	piena	piena	nessuna
Osservatore	nessuna	nessuna	piena	nessuna	nessuna

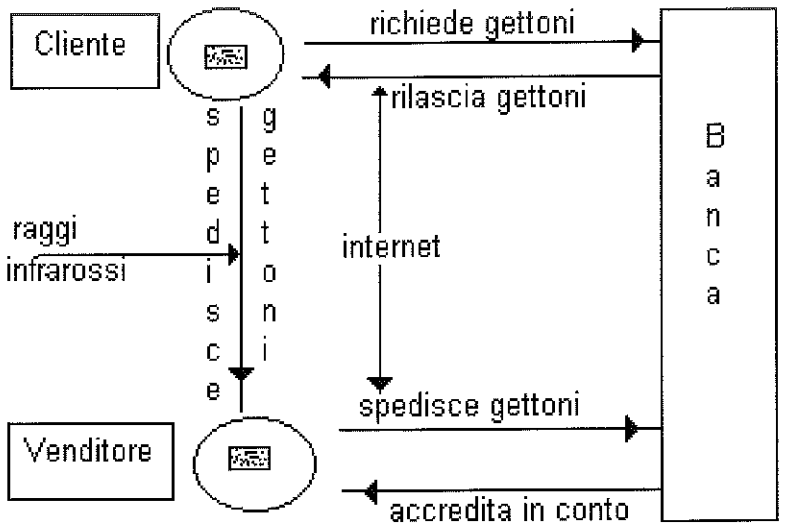
Se si suppone che il server emetta gettoni validi per più commercianti, l'osservatore remoto non ha alcuna visibilità delle parti coinvolte nella transazione. Se invece il server è di proprietà di uno specifico venditore (come per il sistema Millicent), allora l'identificazione del venditore è piena. Mentre poi il cliente ha una visibilità piena del venditore, questi non ne ha alcuna del cliente.

2.4.2 Portafogli elettronici

I due sistemi facenti parte di questo gruppo, entrambi in fase di sperimentazione sono l'analogo digitale di un comune portafoglio. Il primo dei due è stato inserito in questo lavoro perchè è possibile la ricarica on-line; il secondo perchè è italiano ed è prossima la compatibilità con TELEpay.

2.4.2.1 CAFE

Il sistema CAFE [10] (Conditional Access For Europe) è un progetto sviluppato da Digicash ed è ancora in fase di sperimentazione. CAFE consiste di un dispositivo hardware, il portafoglio elettronico tascabile, e di una smart card. La riservatezza dei messaggi è realizzata tramite algoritmi a chiave asimmetrica, le transazioni sono eseguite off-line e il flusso di denaro avviene in forma anonima.
Per entrare in possesso di un portafoglio elettronico CAFE, bisogna prima aprire un conto corrente presso una delle banche aderenti all'iniziativa. Questi rilascia sia il dispositivo che la smart-card e provvede poi a riempire il portafogli con gettoni digitali per un ammontare deciso dal cliente. E' da notare che i gettoni rilasciati dall'istituto sono firmati con la chiave privata di questi, in modo che chiunque possa verificarne autenticità e valore ed inoltre, nel momento in cui sono rilasciati, sono completamente anonimi. A garanzia del cliente, l'istituto rimborsa la somma non spesa in caso di smarrimento o furto del dispositivo.
Una rappresentazione grafica del sistema potrebbe essere la seguente:



2.4.2.1.1 *Ruolo del dispositivo e della smart-card*

Il dispositivo, cioè il portafoglio elettronico, serve a garantire l'utente mentre la smart card, che contiene un processore crittografico dedicato, serve a garantire l'istituto finanziario. Nessuna operazione è possibile senza la cooperazione di entrambi. Affinché il cliente possa pagare è necessario che dopo averlo acceso vi introduca il proprio PIN. In questo modo si ha la presunzione che l'utilizzatore sia anche il legittimo proprietario. La smart-card mantiene una lista di tutti i gettoni elettronici già spesi per evitare che siano riusati e, inoltre, autentica ogni pagamento apponendo sui coin usati per pagare la propria firma crittografica. Per la precisione, la smart card decripta tramite la chiave pubblica dell'issuer il gettone, lo codifica con la propria chiave privata, ci aggiunge il numero identificativo del dispositivo e poi codifica il tutto con la chiave pubblica dell'issuer. In questo modo chiunque volesse riutilizzare i gettoni non potrebbe farlo perchè alla firma della banca si è sovrapposta la firma della smart card. I gettoni necessari per effettuare il pagamento, dopo essere stati marcati come spesi, sono trasmessi, tramite raggi infrarossi, dal dispositivo del cliente a quello del venditore. Con questo sistema, la trasferibilità dei gettoni è limitata ad una sola transazione, per cui il venditore che riceve questi coin, non può utilizzarli per i suoi acquisti, ma deve necessariamente trasmetterli al proprio istituto bancario per l'accredito in conto.
In realtà il sistema CAFE è stato pensato più per lo shopping e per le piccole spese quotidiane che non per acquisti on-line. Ad ogni modo, il fatto che sia possibile per il titolare del portafoglio elettronico, ricaricarlo usando la rete, giustifica la sua presenza in questa panoramica.
Essendo il sistema in fase di sperimentazione, anche per facilitarne il suo diffondersi, ha costi molto contenuti ed in effetti, essendo finalizzato ai micropagamenti, non potrebbe essere altrimenti. In particolare, il costo di acquisto del dispositivo è puramente simbolico e qualche Banca lo concede addirittura gratuitamente. Non sono previsti costi fissi mensili o costi per ogni operazione di acquisto. E' invece a carico del titolare del portafoglio il normale costo di una operazione bancaria per la ricarica.
Poichè la transazione è effettuata senza che ci sia l'identificazione delle parti e senza ottenere la contestuale autorizzazione dall'issuer, le modalità della transazione sono quindi (-I-L). Però, ciò non priva il venditore della possibilità di validare on-line il denaro ricevuto, soprattutto in caso di importo cospicuo.
Le proprietà del sistema CAFE sono le seguenti:

	Token	Atom	Consi	Isol	Corr	Econ	Divis	Scal	Comp	Conse
CAFE	si	no	si	si	si	si	si	si	si	si

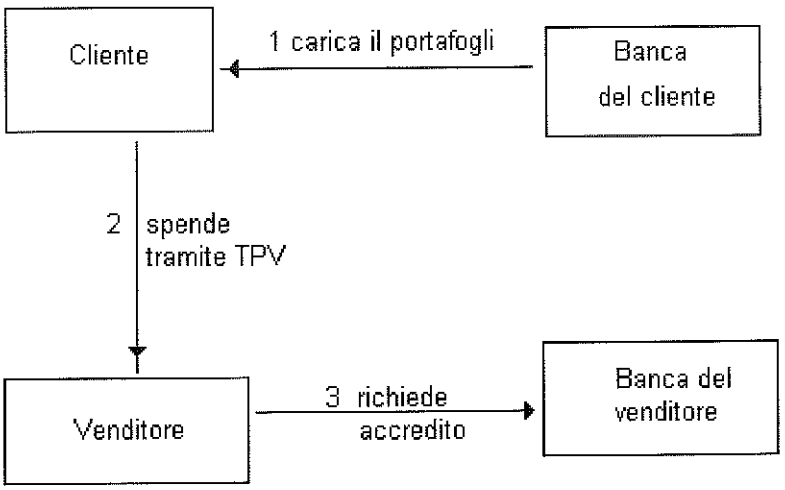
Come si può vedere, il sistema gode di quasi tutte le proprietà per cui può essere espresso un giudizio favorevole. Una piccola considerazione va però fatta sulla proprietà dell'atomicità che in questo sistema viene a mancare sia perché un fallimento potrebbe occorrere durante il trasferimento dei gettoni dal portafoglio del cliente a quello del venditore, sia perché non essendo la validazione immediata, al venditore potrebbero essere dati gettoni falsi.
Relativamente alla visibilità della transazione il tutto può essere riassunto nella seguente tabella:

	vend	Cliente	Data	importo	dettagli
Venditore	piena	nessuna	piena	piena	piena
Cliente	piena	piena	piena	piena	piena
Banca	piena	piena	piena	piena	nessuna
Osservatore	piena	nessuna	piena	piena	piena

Poiché la transazione si svolge off-line, l'osservatore non può che essere un osservatore fisico presente nell'esercizio commerciale al momento del trasferimento del denaro dal portafoglio del cliente a quello del venditore, per cui questi sa chi è il commerciante, ma non può in alcun modo sapere chi sia l'acquirente.
C'è da aggiungere che il venditore non identifica il cliente, ma si limita solo a registrare il numero del dispositivo di questi.

2.4.2.2 MINIpay

Il sistema MINIpay [11] è l'unico portafoglio elettronico italiano. Come TELEpay, è stato ideato e realizzato da SSB e anche se la sua diffusione è attualmente limitata ad alcune zone di Lombardia e Piemonte, ben presto il suo uso diverrà comune in tutta Italia e non solo. Il portafoglio è posto in vendita, ad un prezzo di poche decina di miglia di lire, in tutte le banche aderenti all'iniziativa e l'acquisto non è riservato ai soli correntisti. Il suo caricamento avviene utilizzando uno degli appositi terminali messi a disposizione presso le filiali delle banche convenzionate e l'importo minimo e massimo di ogni ricarica, è fissato rispettivamente in £ 10.000 e in £ 300.000. Acquistato qualcosa, il cliente paga inserendo il portafoglio nell'apposito lettore TPV (Terminale Punto Vendita) di cui sono forniti gli esercizi convenzionati. Una volta che sul display del TPV appare l'importo, è sufficiente dare conferma senza che venga richiesto alcun codice. Una volta compiuta questa operazione, il denaro passa nelle disponibilità del venditore, il quale potrà versarle sul proprio conto corrente collegando tramite telefono il proprio TPV alla banca oppure utilizzando una apposita carta esercenti da inserire in uno dei terminali che provvedono anche alla ricarica. Al momento il possessore può verificare il saldo solo attraverso le apparecchiature utilizzate per il caricamento oppure al momento di un acquisto. In futuro, saranno disponibili appositi lettori.
Il microprocessore della carta e i meccanismi di sicurezza realizzati da SSB, assicurano che la moneta elettronica non possa essere in nessun caso copiata o falsificata ed inoltre ogni passaggio di denaro è memorizzato in ognuno dei portafogli interessati all'operazione. Tuttavia, il fatto che al momento dell'acquisto non venga richiesto alcun codice, rappresenta un grave handicap per la sicurezza. Infatti, in caso di smarrimento del dispositivo, il denaro in esso contenuto può essere tranquillamente speso senza alcuna misura protettiva nei confronti del legittimo proprietario.
Oltre all'area per la memorizzazione del residuo, sul portafoglio, vi sono altre due aree grazie alle quali è possibile richiedere alla propria banca servizi aggiuntivi. La prima area è riservata ai cosiddetti servizi di "fidelizzazione/loyalty" e consente all'esercente di gestire formule di abbonamento, offerte speciali o altre tipologie promozionali di pagamento mirate a promuovere la fedeltà d'acquisto del cliente. La seconda area di memoria è utilizzabile o dalle singole banche per offrire servizi a valore aggiunto alla propria clientela oppure dalla pubblica amministrazione per servizi al cittadino.
Il portafoglio elettronico MINIpay, è compatibile con lo standard europeo, per cui darà la possibilità ai suoi possessori di avere una soluzione per le piccole spese non limitata dalle frontiere nazionali. Inoltre, la sua prossima compatibilità con il sistema TELEpay, permetterà il suo utilizzo negli acquisti on-line.
Le modalità della transazione sono (-I-L) in quanto il venditore non procede all'identificazione del cliente ed inoltre il denaro usato per pagare viene immagazzinato sul TPV del venditore e lì rimane fino a quando questi non procede all'accredito in conto.



Le proprietà della transazione sono le seguenti:

	Token	Atom	Consi	Isol	Corr	Econ	Divis	Scal	Comp	Conse
MINIpay	si	si	si	si	si	si	si	?	si	no

La transazione è da ritenersi atomica perché il trasferimento di denaro avviene dal portafoglio del cliente a quello del venditore presumibilmente senza fallimenti. L'unica proprietà su cui non è possibile esprimersi è la scalabilità in quanto il sistema non è fatto per acquisti on-line.
La visibilità della transazione condotta con MINIpay, è la seguente:

	Venditore	Cliente	Data	Importo	Dettagli
Venditore	piena	nessuna	piena	piena	piena
Cliente	piena	nessuna	piena	piena	piena
Banca	piena	piena	piena	piena	nessuna
Osservatore	?	?	?	?	?

I punti interrogativi sono dovuti al fatto che l'osservatore remoto non può avere alcuna visibilità della transazione in quanto questa si svolge fuori dalla rete. Il cliente ha una visibilità piena del venditore in quanto, anche se non lo identifica, saprebbe ritrovarlo. Il venditore invece, non ha alcuna visibilità del cliente.

2.5 Confronto riassuntivo

In questo paragrafo si confrontano i sistemi presentati in base a differenti criteri. Per farlo si utilizzano delle apposite tabelle che, grazie all'impatto grafico, permettono una piú rapida analisi.

2.5.1 Modalità di pagamento

La prima delle due tabelle proposte in questa sezione, raccoglie solo i sistemi di tipo Token. Non è difficile rendersi conto che i sistemi della tabella sono gli stessi del paragrafo 5.2.

	Atom	Consi	Isol	Corr	Econ	Divis	Scal	Comp	Conse
CAFÈ	no	si	si	si	si	si	si	si	si
DigiCash	no	no	no	no	si	si	si	si	si
Millicent	no	no	si	no	si	si	si	no	no
MINIpay	si	si	si	si	si	si	?	si	no
Mondex	si	si	si	si	si	si	si	si	si
NetCash	no	no	no	no	si	si	si	si	si

Si nota subito come ci siano tre proprietà godute da tutti i sistemi. Tra queste hanno sicuramente una certa importanza quella dell'economicità e della scalabilità. La proprietà della divisibilità è invece semplice conseguenza del tipo token.
I sistemi hanno quasi tutti la proprietà della compatibilità perché il denaro che si utilizza è generato da istituti bancari. Solo il sistema Millicent non ha questa compatibilità perché i gettoni sono emessi dal venditore.
MINIpay e Mondex hanno la proprietà dell'atomicità perché il trasferimento di denaro si riduce allo scambio di un solo gettone. Con queste modalità il cliente riesce a rilevare un eventuale fallimento nel trasferimento e quindi può ripeterlo senza per questo pagare due volte. Gli altri, invece, in generale trasferiscono più gettoni per cui non è possibile attribuire loro tale proprietà.
Il punto interrogativo che corrisponde alla scalabilità di MINIpay, è dovuto al fatto che non essendo il sistema attualmente utilizzabile on-line, il si o no dipende dalla particolare implementazione fatta.

La seconda tabella si riferisce ai sistemi Notational:

	Atom	Consi	Isol	Corr	Econ	Divis	Scal	Comp	Conse
CyberCash	si	si	no	si	no	-	no	si	si
Electronic Cheque	si	si	no	si	si	-	si	si	si
First Virtual	si	si	no	no	no	-	no	si	si
IKP	si	si	no	si	no	-	si	si	si
μiKP	si	no	no	no	si	-	si	si	si
NetBill	si	si	no	si	no	-	no	no	si
NetCheque	si	si	no	si	si	-	si	si	si
SET	si	si	no	si	no	-	si	si	si
TELEpay	si	si	no	si	no	-	no	si	si

Si osserva immediatamente come la colonna dell'atomicità abbia tutti "si". Questo perché il trasferimento di denaro, essendo effettuato tra istituti finanziari è da considerarsi atomico. Nonostante però tutti godano di questa proprietà, non tutti hanno quella della consistenza e dell'isolabilità. Il sistema μiKP non gode della consistenza in quanto cliente e venditore potrebbero non convenire sugli ordini effettuati e/o sul loro importo. Nessun sistema ha la proprietà dell'isolabilità perché l'istituto finanziario o l'intermediario in genere, effettua l'accredito/addebito solo se il cliente è coperto. Nella realtà le transazioni condotte con carte di credito sono eseguite senza che si controlli tale copertura al momento del pagamento. In ogni caso, qui si è supposto diversamente perché se l'intermediario è la banca del cliente, questa può procedere alla verifica della copertura prima del pagamento. Si nota, infine, che non tutti i sistemi sono economici; in particolare sono economici quelli basati su assegni, mentre non lo sono quelli basati su carte di credito.

2.5.2 Economicità della transazione

Un metodo per la classificazione dei sistemi è quello economico. Nel primo gruppo della tabella sono stati inclusi quei sistemi il cui costo di utilizzo è talmente basso da renderli adatti ai micropagamenti (frazioni di $ o poche migliaia di lire). Nel secondo gruppo sono contenuti quei sistemi ritenuti economici per transazioni di importo non elevato, ma in ogni caso costosi per importi modesti. All'ultimo gruppo appartengono invece i sistemi basati tutti su carta di credito che garantiscono una certa sicurezza e per questo costosi sia in termini economici che in termini computazionali.

	Token	Atom	Consi	Isol	Corr	Econ	Divis	Scal	Comp	Conse
Sistemi per micropagamenti										
CAFÈ	si	no	si	si	si	si	si	si	si	si
μiKP	no	si	no	no	no	si	-	si	si	si
Millicent	si	no	no	si	no	si	si	si	no	no
MINIpay	si	si	si	si	si	si	si	?	si	no
NetCash	si	no	no	no	no	si	si	si	si	si
Sistemi economici										
Electronic Cheque	no	si	si	no	si	si	-	si	si	si
DigiCash	si	no	no	no	no	si	si	si	si	si
Mondex	si	si	si	si	si	si	si	si	si	si
NetCheque	no	si	si	no	si	si	-	si	si	si
Sistemi non economici										
First Virtual	no	si	si	no	no	no	-	no	si	si
IKP	no	si	si	no	si	no	-	si	si	si
NetBill	no	si	si	no	si	no	-	no	no	si
CyberCash	no	si	si	no	si	no	-	no	si	si
SET	no	si	si	no	si	no	-	si	si	si
TELEpay	no	si	si	no	si	no	-	no	si	si

- I sistemi per micropagamenti sono tutti di tipo token, con l'eccezione di μiKP.
- I sistemi economici sono sia di tipo token che notational e hanno in comune la proprietà della scalabilità, compatibilità e conservabilità.
- I sistemi non economici sono quelli basati su carte di credito con l'unica eccezione di NetBill basato, invece, su assegni. Hanno tutti le proprietà di atomicità, consistenza e nessuno dell'isolabilità.

2.5.3 Modalità della transazione:

In base al tipo di pagamenti (anonimo/identificato) e di validazione (on-line/off-line) che caratterizzano la transazione, si possono derivare le seguenti classificazioni:

	I	L
TOKEN		
DigiCash	no	si
Millicent	no	si
Mondex	si	no
NetCash	no	si
portafogli		
CAFE	no	no
MINIpay	no	no
NOTATIONAL		
assegni		
Electronic cheque	si	si
NetBill	si	si
NetCheque	si	si
Carte di credito		
CyberCash	si	si
First Virtual	no	si
iKP	si	si
SET	si	si
TELEpay	si	si
μiKP	si	no

Nella colonna corrispondente ad I si indica se la transazione si svolge con denaro anonimo o identificato, cioè se il venditore identifica o meno il cliente al momento del pagamento.
Nella colonna corrispondente a L si indica se la transazione si svolge con validazione on-line oppure off-line.

La cosa che si può notare è che solo il sistema CAFE e il sistema MINIpay, entrambi portafogli elettronici, non usano denaro identificato e non hanno una validazione immediata dei soldi usati per pagare. In effetti questo rientra nelle finalità dei due sistemi, che essendo appunto dei portafogli, devono assomigliare (in senso di proprietà) il più possibile al denaro reale.

2.5.4 Distribuzione geografica

Per ogni sistema è indicato nella prima colonna, il paese in cui il progetto è stato sviluppato, nella seconda gli stati nei quali il sistema è utilizzato.

	Stato di	
	progettazione	utilizzo
Millicent	USA	USA
SET	USA	USA, Europa
NetCash	USA	-
Electronic Cheque	USA	USA
NetBill	USA	USA
NetCheque	USA	USA
CyberCash	USA	USA, Canada
First Virtual	USA	USA
iKP	Svizzera	?
μiKP	Svizzera	?
DigiCash	Olanda	Paesi Bassi
CAFE	Olanda	Paesi Bassi
Mondex	GB	GB, USA, Canada
MINIpay	Italia	Italia
TELEpay	Italia	Italia

Come si può osservare gli USA fanno la parte da leoni, sia nella realizzazione, che nell'utilizzo di tali sistemi. Per quanto riguarda l'Europa si sta affermando nei paesi inglesi il sistema Mondex mentre nei Paesi Bassi il DigiCash. Lontani da uno standard, le banche italiane hanno spinto per un proprio sistema che potrebbe ben presto varcare i confini nazionali.

2.5.5 Visibilità della transazione per l'osservatore remoto

	Venditore	Cliente	Data	Importo	Dettagli
CyberCash	nessuna	nessuna	piena	nessuna	nessuna
iKP	nessuna	nessuna	piena	nessuna	nessuna
SET	nessuna	nessuna	piena	nessuna	nessuna
TELEpay	nessuna	nessuna	piena	nessuna	nessuna
Electronic Cheque	nessuna	nessuna	piena	nessuna	nessuna
NetBill	nessuna	nessuna	piena	nessuna	nessuna
Mondex	nessuna	nessuna	piena	nessuna	nessuna
NetCash	nessuna	nessuna	piena	nessuna	nessuna
First Virtual	parziale	parziale	piena	piena	piena
μiKP	piena	piena	piena	piena	nessuna
NetCheque	piena	piena	piena	piena	piena
Millicent	piena	nessuna	piena	parziale	nessuna
DigiCash	nessuna	nessuna	piena	piena	nessuna

La tabella è stata divisa in due parti per evidenziare i sistemi in cui l'osservatore remoto ha una certa visibilità della transazione commerciale da quelli in cui non ne ha affatto. Si può dire che i sistemi della prima parte della tabella fanno un uso massiccio di algoritmi a chiave asimmetrica, mentre quelli della seconda parte, o non ne fanno uso o si limitano al suo utilizzo per l'autenticazione o dell'ordine di pagamento o del gettone. Mancano CAFE e MINIpay perché non espletano la transazione commerciale su Internet.

3 Trend

Alla fine del 1996 la società di ricerca e consulenza londinese Ovum Ltd. ha pubblicato uno studio sul futuro dell'e-cash intitolato: "Electronic Cash, Opportunities for Banks and IT Suppliers". Gli autori sono i consulenti D. Brown e W. Cappelli, I quali hanno analizzato il mercato della moneta digitale e hanno ipotizzato degli scenari di sviluppo per tale mezzo di pagamento. Vengono forniti dati quantitativi sulla crescita del mercato per la moneta digitale correlate dagli sviluppi degli altri sistemi di pagamento. Infine si analizzano alcuni aspetti della sicurezza delle trasmissioni elettroniche

3.1 Modelli di sviluppo per l'e-cash

Il business della moneta digitale sta attraversando una fase di confronto tra i possibili modelli di sviluppo. Innanzitutto si affrontano un modello centralizzato e un modello autonomo. Il modello centralizzato prevede la circolazione di una sola moneta digitale, il modello autonomo prospetta, invece, la coesistenza di più tipi di denaro elettronico emessi da più fornitori. All'interno di ciascuno dei due sistemi è inoltre necessario distinguere l'approccio token-based, il quale prevede che la moneta digitale rappresenti una somma depositata presso un conto bancario da uno float-based, secondo il quale, invece, il denaro elettronico è a tutti gli effetti "reale". Secondo quanto emerge dalla ricerca Ovum il modello che più ha possibilità di riuscire è quello centralizzato di tipo float-based, il quale offre le più ampie garanzie essendo appoggiato da grandi nomi come Visa, Europay, Mastercard. Al contrario il modello autonomo token-based dovrebbe espandersi con minori possibilità di successo, fatto salvo il caso degli acquisti internazionali che comportino lo spostamento di bassi importi di denaro sulla rete Internet. Le banche, in quanto istituti finanziari, hanno senz'altro la possibilità di entrare da subito nell'affare della moneta digitale e alcune di loro come Mark Twain's Bank e la First Network Security Bank hanno già compiuto grossi investimenti su questo fronte. Resta da vedere, prima di affrontare grossi investimenti, quali sono le possibilità per la banca di ottenere un ritorno economico. La prima fonte di guadagno per l'istituto mediatore del trasferimento di moneta elettronica è sicuramente la commissione sostenuta dal consumatore per acquisire una somma di denaro elettronico in cambio dei vantaggi che offre tale sistema di pagamento. Tali vantaggi possono identificarsi, per l'utente del servizio, innanzitutto in tempi fisici di pagamento minori e quindi in minori disagi: si pensi ad esempio alla semplice conseguenza dell'abbattimento delle code alle casse: si ricordi che parte del successo delle carte di debito come il Bancomat è dovuto proprio a questo tipo di vantaggio: nel senso della velocizzazione si potrebbe paragonare l'introduzione dell'e-cash anche all'introduzione delle tessere di pagamento nelle autostrade.
Per quanto riguarda poi le modalità di applicazione delle varie commissioni sul servizio, la ricerca Ovum sottolinea come attualmente sia lasciato un largo margine d'azione alle banche da parte delle società erogatrici e fornitrici di istemi tecnologici di e-cash. Gli approcci possono quindi essere diversificati: commissioni per il possesso di una carta di denaro elettronico o per l'apertura del conto corrente destinato all'uso di denaro digitale, commissioni in sede di ricarico della carta di pagamento, etc.
Altro vantaggio economico per la banca che si trova ad emettere float-based e-cash è di poter operare finanziariamente sulle somme prepagate dagli utenti: nel caso, ad esempio, che vengano pre-acquistati dieci lotti di moneta elettronica del valore di centomila lire, la banca avrà a disposizione per tutto il lasso di tempo che intercorre tra emissione del denaro elettronico e spesa effettiva del consumatore un milione di lire in più da gestire. Va inoltre osservato che l'intervallo temporale tra emissione di e-cash e suo utilizzo è destinato a crescere in favore delle banche mano a mano che il sistema di pagamento basato sulla moneta digitale andrà diffondendosi e si estenderà dal rapporto consumatori-dettaglianti al rapporto commerciante-fornitori e via via alla rete dei rapporti di fornitura tra imprese. Gli istituti finanziari potranno cioè operare nel tempo in modo da ampliare mano a mano la forbice tra acquisizione della moneta digitale e sostenimento della spesa. Il vantaggio dell'utilizzazione di denaro elettronico nei pagamenti non riguarda, tuttavia, esclusivamente gli istituti finanziari e la relativa utenza: gli istituti finanziari eserciteranno con molta probabilità nei confronti dei consumatori il ruolo sia di emissari di moneta elettronica sia di fornitori dei servizi per utilizzarla nel punto vendita: quest'ultimo potrebbe a sua volta ricercare, nell'accettare pagamenti in moneta elettronica, alcune opportunità di costo e operazionali. Per i punti di vendita al dettaglio, ad esempio, si profila l'abbattimento dei tempi di transazione, che si prefigurano come i più brevi possibili, e degli stessi costi relativi alla transazione, essendo minori gli step da effettuarsi da parte della moneta elettronica per acquistare validità rispetto ad altre forme di pagamento; non si dimentichi, inoltre, il vantaggio non indifferente apportato dalla possibilità di commerciare tenendo la minor quantità di contante possibile in cassa: ecco perché risulta prevedibile uno sviluppo della domanda di mediazione finanziaria relativa al servizio di pagamento elettronico in esame anche da parte dei piccoli commercianti. Sostenendo questi ultimi già oggi delle spese di commissione relative sia all'utilizzo di sistemi di pagamento elettronico come la carta di credito e la carta di debito che di sistemi di pagamento non elettronico come ad esempio l'assegno, è molto probabile che le società emettitrici

di carte di pagamento e gli istituti finanziari applicheranno commissioni sull'utilizzo di denaro elettronico anche alla parte dell'utenza "commerciale".

3.2 *Analisi di alcuni dati del rapporto e conclusioni*

Proponiamo qui di seguito una tabella contenente i dati provenienti da "Electronic Cash, Opportunities for Banks and IT Suppliers" e pubblicati su Aziendabanca (60) che quantificano in miliardi di dollari la ipotetica diffusione dei sistemi di pagamento elettronici a partire dal 1996 e per il ventennio successivo: ci proponiamo di commentarli analiticamente al fine di comprendere sulla loro base la reale portata del fenomeno e-cash.

	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006
checks	1000	940	884	831	781	734	690	648	610	573	539
cash	4500	4530	4550	4580	4610	4630	4660	4680	4680	4640	4610
e-cash	0.15	0.23	0.38	1	2	3	6	14	37	104	156
debit card	375	431	496	570	656	721	779	818	859	902	947
credit card	1130	1240	1360	1500	1650	1810	1090	8210	8340	8480	8630

Tabella 1 - Previsione della diffusione dei vari sistemi di pagamento (Dati in miliardi di dollari)

Rielaborando i dati relativi alla sola graduale diffusione relativa al contante elettronico, è possibile rendersi conto dell'evoluzione esponenziale che questa forma di pagamento subirà nel prossimo ventennio. La moneta digitale, attualmente sviluppata soprattutto in Europa e non come si potrebbe credere, negli Stati Uniti, potrebbe infatti conoscere alti tassi evolutivi soprattutto nei paesi che si affacciano sul Pacifico e nei paesi in via di sviluppo: per questi ultimi il contante elettronico potrebbe costituire un ausilio non indifferente alle attività commerciali; per questo già oggi esistono ben 38 progetti per la realizzazione di sistemi e-cash in 24 paesi, di cui molti extra occidentali (61).

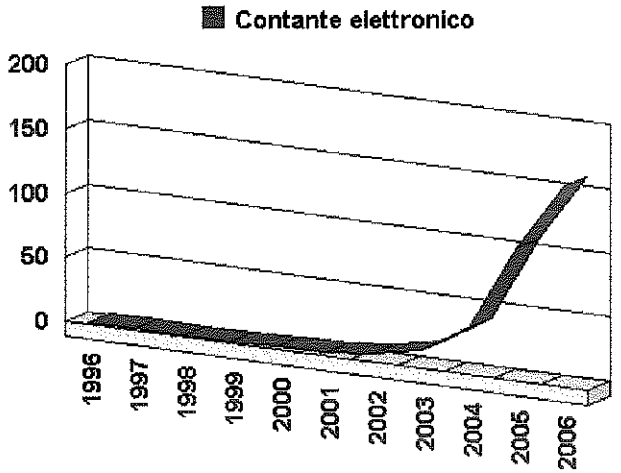


Fig. 1 - Crescita dell'impiego di contante elettronico nelle transazioni su scala mondiale 1996-2006.

In relazione ad altri sistemi di pagamento elettronico, tuttavia, la moneta elettronica conoscerà ancora nel 2006 una diffusione percentuale a dir poco irrisoria: il forte sviluppo di questo sistema pagamento non sarà cioè accompagnato da una corsa generale dell'economia nel suo insieme alla moneta elettronica.
La ragione potrebbe essere tuttavia riscontrata nel fatto che l'analisi prende in considerazione un periodo di tempo troppo breve per evidenziare quali saranno i reali effetti della nuova moneta, che oggi nuove i suoi primi passi, sulla totalità dell'economia (62). Questa considerazione assume più valore se si ritiene che la carta di credito nata negli anni venti in USA, secondo il rapporto in analisi, è attualmente a circa un terzo del proprio sviluppo percentuale rispetto agli altri sistemi di pagamento nel 2006. Non è d'altronde possibile sostenere che l'economia non cercherà di ridurre il più possibile le transazioni in denaro contante elettronico virtualizzandole: si prevede infatti che di qui a vent'anni la carta di credito avrà pressoché sostituito la funzionedell'attuale moneta contante. È vero anche che la

carta credito si presta ad una molteplicità di utilizzi rispetto alla moneta elettronica, potendo, come abbiamo visto sopra, essere mezzo di pagamento non soltanto per scambi effettuati in Internet, ma anche e prima di tutto al di fuori di essa.

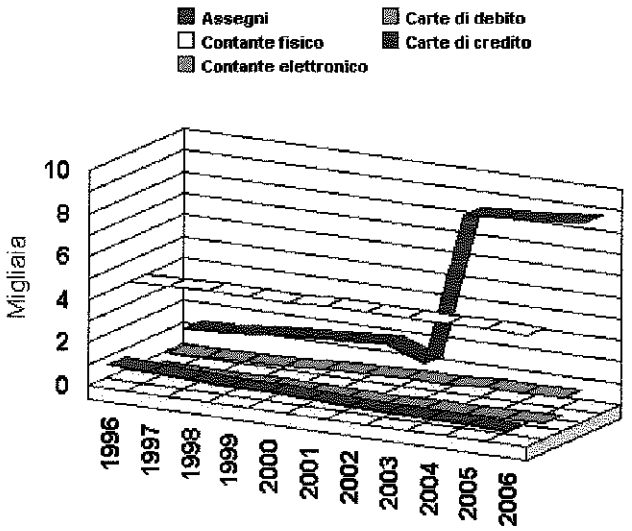


Fig. 2. - Andamento dell'impiego dei diversi sistemi di pagamento nelle transazioni su scala mondiale 1996-2006.

In conclusione, nonostante che il vero boom dei prossimi anni sembri essere quello della carta credito come è possibile notare in figura, il forte sviluppo di e-cash sembra denotare la sua evoluzione come sistema di pagamento per un determinato e specifico segmento di operazioni, probabilmente si tratterà di quelle svolte tramite l'Internet, dato che l'utilizzo di moneta elettronica al di fuori della rete tramite i cosiddetti borsellini elettronici dovrà subire la concorrenza delle più affermate e multifunzionali tessere Bancomat, oltre che delle carte di credito stesse.

4 Riferimenti

[1] http://www.cybercash.com
[2] http://www.fv.com
[3] http://www.zurich.ibm.ch/Technology/Security/extern/ecommerce/IKP_overview.html
[4] http://www.visa.com/SET/
[5] http://telepay.ssb.net/home/
[6] http://www.zurich.ibm.ch/Technology/Security/extern/ecommerce/
[7] http://www.fstc.org/
[8] http://nii-server.isi.edu/info/netcheque.html
[9] http://www.netbill.com
[10] http://www.digicash.com/products/projects/cafe.html
[11] http://www.minipay.com
[12] http://www.digicash.com/
[13] http://www.research.digital.com/SRC/millicent/
[14] http://www.mondex.com
[15] http://nii-server.isi.edu/info/netcash.html
[16] http://www.intertrader.com
[17] Lynch D., Lundquist L. H., Digital Money : The New Era of Internet Commerce, John Wiley & Sons, 1995.
[18] Loshin P. et al, Electronic Commerce: On-line Ordering and Digital Money, Charles River Media, 1997.