通信情報保護學會誌
第9卷 第1號, 1999. 3

전자화폐 시스템 개발 동향

A Development Trend of Electromic Cash System

오 형 근*, 이 임 영*

요 약

정보화 사회가 도래함으로써 기존의 상거래 시스템과 통화 시스템에도 큰 변혁이 시작되고 있다. 사이버 공간이 생겨나고 그 속에서 각종 상거래가 발생하며 그에 따라 대금 지불 수단이 필요하게 되었고 실물 화폐를 대신할 각종 전자화폐 시스템들이 등장하고 있다. 또한 이러한 전자화폐들과 함께 각종 전자 지불 시스템들의 출현으로 전자상거래는 다가오는 21세기에 우리 주위에서 흔히 볼 수 있는 상거래 관행으로 자리를 잡을 것이다. 그러나 동시에 디지털이 갖는 속성으로 말미암아 여러 가지 문제점들을 노출시키고 있는데 이러한 문제점을 극복하기 위해 선진 각국들은 많은 투자와 연구를 진행하고 있다. 이에 본 고에서는 각종 전자화폐 시스템의 연구, 개발 동향을 알아보고 현재 구현되어 있는 전자화폐 시스템을 비교, 분석한다.

I. 서 론

최근의 정보화 사회는 인터넷이라는 거대한 통신 네트워크에 의해 움직이고 있으며 폭넓은 컴퓨터의 보급에 힘입어 그 이용자 수는 급격히 증가하고 있는 실정이다. 이미 150여 개국 이상의 나라에서 수 천만 명이 인터넷에 접속하고 있는 것으로 조사가 되고 있으며 앞으로도 그 이용자수는 더욱 폭발적으로 증가할 것으로 예상되고 있다. 또한 기존의 단순 통신으로서의 기능에서 이제는 각종 서비스를 제공하거나 비즈니스가 가능한 새로운 기회의 무대로 그 모습을 바꾸어 가고 있다. 특히, 무한한 잠재력을 가진 시장으로서 인터넷을 이용하려는 시도가 증가하고 있는데 전자상거래(Electronic Commerce)가 그것이다. 전자상거래는 시간적, 공간적인 제약점을 극복하여 언제든지, 어디에 있는 상품이더라도 소비자가 선택하여 구입할 수가 있고 또한 상점에서도 전 세계에 퍼져 있는 인터넷 이용자를 대상으로 상품을 판매 할 수 있게 해 준다. 이러한 전자상거래의 등장은 기존의 비효율적인 상거래 패턴을 획기적으로 변모시킬 것이다.

전자상거래에 있어서 가장 중요한 것은 전자지불 시스템(Electronic Payment System)이며 안전한 전자 지불 시스템을 손에 넣는 것이 앞으로의 전자상거래 시대에 있어서 승자가 되게 될 것이다. 전자지불 시스템은 크게 지불

* 순천향대학교 컴퓨터학부

브로커(Payment Broker) 시스템과 전자화폐(Electronic Cash) 시스템의 두 가지로 나누어 볼 수가 있다. 지불브로커 시스템은 독립적인 신용구조를 가지고 있지 않으며 신용 카드나 은행의 계좌와 같이 지불과 관련된 데이터를 이용해 네트워크 상에서 지불을 하도록 연결시켜주는 구조로 되어 있다. 이러한 시스템은 기존의 신용 카드를 이용한 거래의 관행이 자리잡혀 있기 때문에 응용이 쉽고 소비자나 판매자 그리고 은행 등 전자상거래 참여자들이 쉽게 받아들일 수가 있기 때문에 현실적인 전자지불 시스템으로 받아들여지고 있다. 대표적인 것으로 1997년 5월에 Visa 카드사와 Master 카드사가 함께 개발한 신용카드 기반의 지불 시스템인 SET(Secure Electronic Transaction) 프로토콜이 있다. 반면에 전자화폐 시스템은 현재 사용되고 있는 화폐를 비트 스트림(Bit Stream)의 디지털 형태로 구현한 것으로 여기에는 화폐 발행처의 전자서명이 들어가 있으며 독립적인 신용 구조를 가지고 있어서 그 디지털 데이터 자체로서 유효성 여부를 검사할 수가 있다. 전자화폐는 '디지털 캐쉬', '사이버 캐쉬', '전자현금', 'Virtual Currency' 등으로 불리기도 하며 현대 암호 기술의 가장 중요한 응용 분야 중 하나이다.

II. 전자화폐(Electronic Cash)

사회의 모습이 기존의 산업 사회에서 정보화 사회로 변모하면서 아직 우리에게 낯설게만 느껴지는 전자상거래(Electronic Commerce)라는 상거래 형태가 다가오는 21세기에는 주위에서 흔히 볼 수 있는 서비스로서 자리를 잡게 될 것이다. 전자상거래는 안방에 앉아서 다른 지방에 있는 특산물을 구입할 수 있게 해 줄 수가 있으며 이러한 전자상거래는 안전한 디지털화폐, 즉 전자화폐 없이는 실현될 수가 없다. 사이버캐시(CyberCash)라고도 불리는 전자화폐는 동전과 지폐 등 기존 지불 수단을 완전히 대체할 것으로 예상되는 제 3의 지불 수단이다. 현재 기존의 화폐는 복사 기술의 발달로 인한 불법적인 복사에 의한 이중사용(Double-spending)의 문제, 화폐 제작시의 과다한 제작 비용 문제, 그리고 유지 비용 등 여러 가지 문제점들을 안고 있으며 네트워크 공간상의 사이버 스페이스 상에서 사용하기가 어렵다는 문제점들을 가지고 있다. 따라서 이러한 문제점들을 해결하기 위해 전자화폐가 등장하였으며 전자상거래의 관심이 고조됨에 따라 전자화폐 개발에 세계 각국은 눈을 돌리고 있다.

독립적인 신용 구조를 가지고 있는 전자화폐는 물품 구입시 은행이나 카드 발행사와 같은 제 3의 기관으로부터의 거래 승인이 필요없다. 또한 사용자간의 가치 이전도 가능한 현금과 유사한 개념으로써 전자지불 시스템이 지향하는 궁극적인 목표 시스템이다.

1. 전자화폐 요구 조건

전자화폐는 물리적인 매체에 의존하지 않고 디지털 데이터 그 자체로서 금액 가치를 가지며 인터넷과 같은 오픈된 네트워크를 통해 자유롭게 전송하고 유통시킬 수가 있다. 때문에 디지털 데이터라는 전자화폐의 속성은 기존의 화폐가 안고 있지 않았던 문제점들을 노출시키고 있다. 즉, 현실 세계에서의 화폐보다 훨씬 수월하게 대량으로 복사가 가능하며 네트워크 상으로 전송시 화폐의 위·변조가 가능하게 된다. 이에 안전한 전자화폐의 개발이 중요하며 이를 위해서는 다음과 같은 요구사항을 만족시켜야 한다.

- Independence(완전 정보화, 독립성)
  : 물리적인 존재에 의존하지 않고 디지털 정보만으로 실현할 수 있어야 한다.
- Security(보안성, 이중사용방지)

: 불법적인 복사로 인한 이중사용이 방지되어야 한다. 즉, 한 번 사용한 전자화폐는 다시 사용할 수가 없어야 한다.

- Off-line payment(오프라인 상에서의 지불)
  : 거래시 고객과 상점 이외의 제 3자가 개입하지 않고 상점에서의 지불을 처리할 수 있는 것으로 지불 프로토콜을 수행하는 동안에 은행이나 인증된 센터 등을 필요치 않고 프로토콜을 수행할 수 있는 특징을 가지고 있다.
- Transferability(가치 이전성, 양도성)
  : 사용자가 전자적으로 다른 사용자에게 현금 가치의 이동을 할수 있어야 하며 이때 전자 현금을 보낸 사람의 신원이 화폐에서 완전히 분리되어야 한다.
- Dividability(분할성)
  : 전자화폐의 금액은 보다 작은 액수로 나눌 수가 있어야 하며 반대로 작은 금액들을 다시 모을 수 있어야 한다. 즉, 일정한 금액을 가지고 있는 사용자는 그 금액만큼 자유롭게 사용할 수 있어야 한다.
- Untraceability(추적불가능성, 익명성)
  : 전자화폐의 사용으로 사용자의 개인정보가 노출이 되어서는 안되며 사용자가 구매한 내용과 연관 관계를 추적하는 것이 불가능해야 한다.

위와 같은 조건 이외에도 사용자의 프라이버시만을 강조한 나머지 이를 이용한 범죄 집단이나 불법 사용자들의 돈 세탁, 범죄 수단에의 이용 등과 같은 사회·경제적인 부작용들이 드러나게 됨에 따라 최근에는 무조건적인 추적불가능성을 제공하는 것이 아니라 부정사용시 사용자의 신분이 밝혀지게 하는 조건부 추적 가능성에 대한 요구에 대한 연구도 이루어지고 있다.

2. 연구 동향

전자화폐에 대한 연구개발은 1982년 David Chaum의 on-line형 전자화폐 시스템[1]이 처음 등장한 이래 전자화폐가 요구하는 여러 가지 조건들을 만족시키는 많은 방식들이 제안되어 오고 있다. 이 절에서는 전자화폐의 불추적성, 분할성, 이중사용방지, 효율성, 양도성 측면으로 분류하여 제안된 방식들의 연구 동향에 대해 간단히 알아보도록 한다.

● 불추적성(Untraceability)

1982년에 David Chaum은 사용자의 사생활을 보호하는 차원에서 은닉서명(blind signature)이 새로운 서명 방법을 제시하였다[1]. 이 방법은 사용자가 서명자에게는 문서를 비밀로 한 채 서명을 받는 서명 방법으로 이후 프라이버시를 보증 받는 기술로서 RSA 방식을 기반으로 하는 은닉서명 방법[1],[3], 영지식 증명을 근거로 한 은닉서명 방법[2], 이산대수 방식에 근거한 은닉서명 방법[8] 등이 나왔다. 1988년에는 개인의 프라이버시를 보장하면서 화폐의 이중사용을 방지하는 오프라인형 전자화폐시스템이 나왔다[6]. 여기서는 사용자의 프라이버시가 완전히 보호된다는 장점이 있으나 cut-and-choose방법을 사용하여 효율이 좋지 못하고 안전성에 대한 증명이 없다는 단점을 가지고 있다. 이밖에도 사용자의 프라이버시를 보호하기 위한 시스템들이 설계되어 오다가 이에 대한 여러 가지 문제점들이 노출됨으로써 익명성을 제한하는 시스템들이 나오게 되었다.

참가자들의 익명성은 전자상거래에 있어서 중요한 요구사항이 되고 있는데 이러한 익명성은 돈의 약탈이나 또는 돈 세탁과 같은 예에서 법 집행과 상충되기 때문에 참여자들의 익명성을 선택적으로 폐지할 수 있는 시스템들이 1995년 이후에는 설계되어 왔다.

Camenisch, Manrer 그리고 Stadler는 이러한 요구사항을 만족시키는 효율적인 전자 지불 시스템을 제안하고 있다[4]. 여기에서 익명성 취소에 대해 묘사하고 있는 기본적인 프로토콜은 off-line 지불 시스템이나 또는 on-line 지불 시스템에 적용될 수가 있다. 그리고 Frankel, Tsiounis 그리고 Yung은 off-ine 전자화폐에 있어서 사용자가 두 번 사용하게 된다면 그는 추적당할 수 있다는 것을 보여주고 있는데 아직 효율적이지는 않지만 제 3의 기관이 어떠한 능력을 가지고 있다는 것을 사람들에게 간접적으로 증명할 수 있는 "Indirect Discourse Proofs"에 대한 표기법을 제안하고 있다[5].

● 분할성(Dividability)

이 성질은 실제 화폐에서 제공되어지지 않고 전자화폐에서만 제공되는 기능으로서 사용자의 편리성을 위해 제공되는 것이 좋다. 1988년에 D.Chaum은 분할 이용 가능한 전자화폐의 하나로서 익명성을 갖는 수표와 유사한 구조를 가지는 시스템을 제안하였다[6]. 이 구조는 한번에 한해서 액면 금액 이하의 임의의 금액에 대한 지불이 가능하지만 잔금을 은행에서 환불 받아야 한다는 제약점이 있다. 또한 1991년에 Okamoto와 Ohta에 의해 추적이 불가능하며 분할 이용 가능한 전자화폐 시스템에 대해 제안하였다[3]. 이 시스템에서는 분할성을 위해 계층적인 structure table을 사용하고 있다. 이 table은 t단계의 트리 구조로 되어 있으며 각 노드는 두 개의 자손 노드들을 가지게 된다. 유일한 루트 노드는 트리 구조의 맨 위에 존재한다. 또한 여기서는 트리 구조와 관련하여 지폐를 사용하기 위해 두 가지의 제약점을 가지고 있다.

1. 어떤 한 노드의 해당 금액은 자식 노드들의 합계와 일치하며 어떤 노드도 한 번 이상 사용할 수 없다.
2. 어떤 한 노드가 사용이 되면, 모든 자식 노드와 부모 노드는 사용할 수가 없다.

그러나 이 방식은 전자화폐 구성시 많은 항(term)을 사용함으로서 비효율적이었는데 이를 개선하여 T.Eng와 T.Okamoto는 보다 효율적인 "분할성"을 가지는 오프라인 전자화폐 시스템에 대해 언급하고 있다[7]. 여기서는 cut-and-choose 방법을 사용하지 않았으며, 또한 전송되는 데이터 크기는 Okamoto와 Ohta 방식[3]보다 작았다. 그러나 이 방식에서의 전자화폐 크기는 이진 트리에 있어서 route들의 선택에 달려 있어서 만약 거의 최적으로 선택이 되지 않는다면 전송되는 데이터 크기는 거의 거의 Okamoto와 Ohta 방식만큼 커지게 된다는 단점을 가지고 있다. 이러한 계산량의 비효율성을 개선하여 1995년 Okamoto는 실질적으로 사용 가능한 작은 계산량을 가지는 전자화폐 방식[14]을 제안하고 있다.

● 이중사용(Double-spending) 방지

전자화폐는 디지털 데이터로서의 속성을 그대로 가지고 있기 때문에 디지털 데이터의 중요한 특징인 복사가능성에 대한 방지책을 세워야 한다.

1992년 D.Chaum과 T.P.Pederson은 observer형 전자화폐 시스템에 대해 제안하였다[8]. 그 방식은 schnorr-signature을 사용하여 새로운 은닉서명에 대해 언급하고 있으며 은행이나 카드 발행회사(서비스 제공자)의 지시대로 움직이는 Tamper-Resistant 장치(Observer)와 사용자가 제어할 수 있는 컴퓨터를 조합하여 서비스 제공자와 observer사이의 모든 통신에 사용자의 컴퓨터가 개재함으로써 사용자의 프라이버시를 지키고 또한 observer를 둠으로서 컴퓨터가 부정한 동작을 하지 못하도록 한다. 마찬가지로 observer형 전자화폐 시스템으로

Brands가 제시한 방법에서는 D.Chaum의 observer 개념을 응용해서 전자화폐의 이중 사용을 사전에 방지하는 방식을 제안하고 있다[9]. 이는 은행에서 인출된 모든 전자화폐를 사용자의 컴퓨터와 observer 양쪽으로 관리시켜 전자화폐를 사용할 때 전자화폐 내 observer의 서명이 필요한 구조를 가짐으로 이중 사용을 방지하고 있다. observer는 한 번 서명하면 두 번 다시 같은 전자화폐에 서명하지 않으며 observer가 파괴되더라도 은행에서 다시 이중 사용 여부를 검사, 예치시에 부정사용자의 ID를 노출시키고 있다.

● 효율성

Chaum-Fiat-Noar의 오프라인형 전자화폐는 사용자의 프라이버시가 완전히 보호된다는 장점이 있었으나 효율이 좋지 못하다는 단점을 가지고 있었다[6]. 그 후 영지식 증명을 사용하여 안전성이 증명되고 보다 효율적인 오프라인형 전자화폐가 제시되었으며[2] 1993년에 Franklin과 Yung은 영지식비대화 증명과 비밀분산법을 사용해 효율 좋은 전자화폐 방식이 구성될 수 있음을 나타내었다. 또한 1993년에 Brands는 높은 효율성을 가지는 시스템을 제안하고 있다[10]. 이전에 제안된 프라이버시를 보호하는 오프라인 전자화폐 시스템은 실행면에 있어서 비효율적이거나 또는 화폐의 안전성에 대해 증명할 수가 거의 불가능하다는 문제점을 안고 있었다. 게다가 이전의 방법들은 확장하기가 어려웠으나 여기서 제안하고 있는 시스템은 효율적이며 동시에 modular 설계에 의해 굉장히 큰 범위까지 그 시스템의 정확성을 증명할 수 있게 해 준다고 하고 있다. 또한 이 시스템은 계산상 조작 방지 다중 사용 가능한 동전, 익명성을 가지는 계정, 전자수표 그리고 observer를 가지는 Wallet 등으로 확장이 가능하다고 하고 있다.

1994년에 Yacobi는 전자화폐에 대한 새로운 패러다임을 제안하고 있는데 여기서는 전자화폐 시스템으로부터의 요구사항을 줄이고 scheme을 보다 간략하게 해주고 있다[11]. 이러한 것은 이전에 제시된 가장 효율적인 전자화폐 방법보다도 계산 복잡성 면에서 상당히 효율적이다.

● 양도성

1989년에 Okamoto와 Ohta는 일회성 영지식 인증 시스템(disposable zero-knowledge authentication system)이라는 새로운 타입의 인증 시스템의 제안하고 있다[2]. 이 인증 시스템에 기반하여 불추적성(Untraceability)과 재사용 불가능성(Unreusability)을 만족하는 새로운 "추적 불가능한 전자화폐 시스템"을 제안하고 있다. 또 한 앞에서의 두 가지 요소뿐만 아니라 양도성(Transferability)을 만족하는 '전송가능하며 추적 불가능한 전자화폐'인 - '추적 불가능한 전자쿠폰 티켓'을 제안하고 있다. 이 시스템에서는 전자화폐의 각 한 조각의 가치는 많은 조각으로 분할되어 사용할 수가 있으며, 또한 다른 사람에게 양도되어 사용할 수가 있다. 그리고 양도할 수 있는 전자화폐에 대해 지금까지 알려진 방법들은 각 지불이 증가한 후 화폐를 표현하는데 필요한 비트들의 수가 증가한다는 단점은 가지고 있었는데 Chaum-Pederson은 1992년에 화폐가 이전되었을 때 그 크기가 증가하는 이러한 특징이 없이 양도성을 제공하는 전자화폐 시스템을 구성하는 것은 불가능하다는 것을 보여주고 있다[12].

3. 각국의 개발 현황

디지털화의 큰 물결에 의해 국제적인 통화 시스템의 대변혁이 시작되고 있다. 21세기라는 새로운 세기를 맞이하고 있는 오늘날 현물 통화가 필요 없는, 현금 없는 시대를 향해서 전자화폐를 둘러싼 여러 가지 개발 경쟁, 즉 디

지털화된 전자화폐를 휴대하는 전자지갑의 개발, 개인의 전자화폐를 관리하는 가계부 소프트웨어의 개발, 가상 현실 공간을 만들어서 그곳에서 전자화폐가 사용되는 시스템 개발 등 디지털화 된 통화정보의 활용 방법을 둘러 싼 개발 경쟁이 일어나고 있는 것이다. 다음에서는 이 중 전자화폐가 사용되는 전자지불 시스템 개발에 초점을 맞추어 보기로 한다.

● 미 국

정 보 고 속 도 로 (National Information Infrastructure : NII) 구상과 더불어 네트워크 기술이 발달하였고 통신비용이 저렴한 미국에서는 온라인 상의 전자화폐를 중심으로 각종 지불 시스템이 개발되었다. 그러나 최근에는 IC 카드를 이용하는 형태의 지불 시스템들이 속속 개발되고 있으며 이러한 추세는 앞으로 더욱 증가할 것으로 보인다.

뉴욕 은행과 비자(Visa), 마스터 카드(Master Card)사, 베리폰(Verifone) 등은 1997년 10월부터 전자 화폐 시범 서비스인 이른바 '뉴욕시티 파일럿'을 시행하고 있다. 이 시범 서비스는 은행 고객 5만명을 대상으로 베리폰사[15]에서 개발한 '개인 휴대용 현금 인출기(Personal Automatic Teller Machines : PATM)'을 이용하여 은행에 가지 않고서도 전화선이나 근거리 통신망(LAN)에 접속을 하여 은행에 돈을 넣거나 인출해서 쓰고 있다. 이 PATM 단말기는 지폐나 동전 대신에 고도로 암호화된 디지털 신호의 조합인 전자현금을 사용하며 스마트 카드를 이용하여 대금지불이나 계좌이체, 세금 납부와 같은 업무를 해낸다.

DEC(Digital Equipment Corp.)사에서는 기존의 낮은 거래 비용으로 인하여 상거래 서비스가 이루어지지 못하는데 착안하여 인터넷상에서 소액 상거래를 이루기 위해 1997년 Millicent 계획[16]을 발표하였다. 이 시스템에서는 작은 금액의 정보를 사고 팔 수 있도록 고객들과 사업자들에게 새로운 방법을 제공하고 있으며 1센트보다도 작은 금액 거래도 가능하게 해 주고 있다. 이 시스템에서 거래되는 5달러 이하의 작은 거래들은 만화, clip art, 음악, 비디오 등을 판매할 수 있도록 해주며 전체 출판물이 아니라 일부분만에 대해서도 지불을 할 수 있기 때문에 사용자 측면에서도 유익하다.

CyberCash[18]사에서는 인터넷에서의 안전하고 편리한 지불을 위하여 2개의 서비스를 제공하고 있다. 하나는 신용카드나 직불 카드 등 각종 카드에 의한 지불 서비스이고 다른 하나는 현금 대신 사용할 수 있는 사이버 캐쉬 화폐 지불 서비스이다. 이 두 가지 모두 사이버 캐쉬 웰렛(CyberCash Wallet)이라는 전자지갑을 사용하여 대금 지불을 수행한다. 사이버 캐쉬 화폐는 신용 카드로 취급하기 어려운 소액 거래를 하기 위해 개발된 것으로 지불은 이용자의 본인 ID가 아닌 암호 키 상의 구좌 ID를 이용해서 행하여지기 때문에 강한 익명성(Strong Anonymity)을 제공한다. 실제의 자금은 가맹 은행에 있으며 은행만이 자금을 이동할 수 있기 때문에 높은 보안성을 제공한다. 현재 약 400,000여개의 Wallet이 보급이 되어 사용되고 있다.

IBM은 인터넷상에서 금융거래를 안전하게 관리하는 제품군을 발표하고 있으며 더욱이 유로페이 인터내쇼날과 제휴하고, 전자화폐를 넣고 다니는 IC 카드를 사용해서 네트워크용 전자상거래의 통합적인 시스템을 개발하려하고 있다.

● 영 국

유럽이나 프랑스에서는 거의 대부분의 카드가 스마트 카드이다. 부정 방지를 위해 도입되었던 스마트 카드이지만 전자화폐의 물결이 거세게 일어나면서 스마트 카드의 이용 범위는 넓어지고 있다. 이제 스마트 카드는 전자지

갑으로 진화하고 있으며 IC칩 내의 구좌로부터 현금을 전자적으로 불러내어 공중전화나 자동판매기에 사용한다. 소액 현금은 비밀번호를 입력하여 사용하지 않고 그대로 사용할 수도 있다. 이러한 스마트 카드를 더욱 진화시켜 "세계에 통용되는 전자현금"을 개념으로 한 것이 몬덱스[18]이다. 이 몬덱스는 1994년 영국의 내셔날 웨스트민스타 은행과 브리티쉬 텔레콤(BT)이라는 전화회사가 전략적 제휴를 통해 금융과 통신 기능을 융합시켜 개발한 새로운 전자화폐 시스템이다. 이 몬덱스 카드는 오프 라인(off-line)과 온라인(on-line)의 양쪽을 사용해 전자통화가 이루어지도록 설계되었다.

● 네덜란드

네덜란드에서는 디지캐쉬(DigiCash)[19]가 익명성의 전자화폐를 통해 세계의 통화 표준으로 하기 위해 노력하고 있다. D.Chaum이 설립한 디지캐쉬사에서는 은행들과 손잡고 소비자에게 64비트 암호파일 형태의 전자화폐를 'ecash'라는 이름으로 발행해 주고 있다. 이 ecash는 마치 여행자 수표처럼 사용할 수가 있는데 고객과 돈을 받는 쪽의 비밀을 완벽하게 지켜주는 것이 큰 장점이다. ecash는 인터넷상에서는 여행자 수표와 같은 대용 화폐를 사용한다. 이용자는 참가 은행으로부터 대용화폐를 사서 참가 가맹점에 지불하면 된다.

● 독 일

은행 등 금융 기관들이 잇따라 전자화폐용 IC 카드의 보급을 시작함으로써 전자화폐의 도입이 본격화 되고 있다. 독일 금융계가 도입하고 있는 전자화폐는 cash 카드 등에 정보를 입력할 수 있는 IC 칩을 넣은 것으로 고객은 은행에서 자기 계좌의 돈을 원하는 만큼 찾아 현금처럼 사용할 수 있게 하는 방식으로 금융업계에서는 지불용 단말기를 상점 등에 1백만대 이상 갖춘다는 계획을 가지고 있다.

● 프랑스

프랑스의 전자지불 시스템으로서 1991년부터 '텔레팩트'라고 불리는 서비스를 제공하고 있다. 이 서비스는 은행카드, 전자송금, 전자지불 수표의 세 가지 종류의 지불 서비스를 제공하고 있으며 티켓 구입이나 게임 이용 등의 지불에 관해서도 차츰 광범위해지고 있다. 또한 '미니텔'이라는 정보 단말기와 안전성을 위해 본인임을 인증 받기 위한 스마트 카드를 이용하여 이 서비스에 쉽게 접근할 수 있다. 아직 전자지불 시스템으로서의 자리를 잡은 것은 아니지만 1800만명이라는 이용자 수를 가진 온라인 서비스와 스마트 카드의 결합이라는 새로운 이용방법을 제시하고 있어 서비스 범위가 확장된다면 그 활용 가치는 굉장히 높을 것으로 생각된다.

4. 국내 동향

국내 동향으로는 아직은 선진국 수준에 미치지는 못하지만 통신회사와 일반 시중 은행들을 중심으로 전자화폐 개발 움직임이 활발히 일어나고 있다. 1996년부터는 은행, 업계, 전문가들로 실무작업반을 구성하여 은행 공동의 전자화폐 표준을 개발(1997년 표준안 확정)하고 전자화폐에 사용될 IC 카드의 개발을 의뢰하는 등 시스템 구축에 본격 착수하고 있다.

한국은행은 1998년부터 일부 시범 은행을 통해 발행되는 IC카드형 전자현금을 오는 2000년까지 단계적으로 확대, 모든 은행에서 전자현금을 발행 할 수 있도록 할 계획으로 있다. 이 IC카드형 전자화폐는 고객이 은행에 대가를 미리 지불한 뒤 그 금액만큼 내장된 IC카드형 전자화폐를 발급 받아 상품 구입 등 일반 소비에서 활용할 수 있도록 하고 있는데 기존의 신용카드, 직불카드 기능을 모두 수용할 수 있도록 시범사업을 추진 중에 있다. 또

한 일부 금융 기관과 IC 카드 전문 업체들이 전자현금 기능에 신용, 직불(현금) 카드 기능을 수용하는 방향으로 금융 IC 카드를 개발하기로 하였다. 이러한 IC 카드를 이용한 전자화폐 시행에 있어서 성공적인 예로 부산의 하나로 교통 카드를 들 수가 있다. 이 카드는 현재 버스, 지하철, 마을버스, 톨게이트 등에서 사용되고 있으며 다수의 이용자가 이용함으로써 전자화폐와는 구별되지만 IC카드 응용의 성공적 사례로 손꼽고 있다.

국내에서도 이미 30만장의 금융권 IC 카드가 보급이 되어 있고 비자, 마스터 카드를 비롯한 신용카드사의 전자지갑 카드와 한국 은행을 중심으로 한 국내 금융 기관 IC 카드가 곧 보급될 전망이다. 이러한 IC 카드의 등장은 급속하게 확산되고 있는 인터넷, PC통신 등 전산망 시스템, 그리고 기간 통신 사업자가 제공하는 가상은행 서비스 및 전자상거래 서비스 등과 직접 연결되어 새로운 형태의 정보서비스 시대로의 진입과 경제활동에 있어서의 획기적인 전환점을 맞이할 것으로 보인다.

III. 전자화폐 시스템

전자화폐는 크게 IC 카드형과 네트워크형의 두 가지로 구분해 볼 수가 있으며 지불 방식에 따라 다시 온라인(On-line)형과 오프라인(Off-line)형, 신용카드형, 선불카드형으로 나누어 볼 수가 있다. 그리고 IC 카드형은 다시 가치 이전성을 기준으로 폐쇄형(closed)과 개방형(open)으로 나누어 볼 수가 있다.

IC 카드형은 내부 정보에 대한 부정한 읽기 및 쓰기가 불가능하도록 Tamper Resistant 장치를 이용하는 것으로서 IC 카드 소유자일지라도 데이터의 부정사용이 어렵도록 하고 있다. 가장 대표적인 것으로서 Mondex가 있다. IC 카드형은 스마트 카드 기술이 앞서 있는 유럽에서 주류를 이루고 있으며 정보통신에 대한 네트워크 기술이 잘 구축되어 있는 미국을 중심으로는 네트워크형의 전자화폐 시스템 개발이 중심이 되고 있다. 네트워크형 전자화폐는 완전한 소프트웨어로 전자화폐를 실현하려는 것으로 IC 카드와 같은 하드웨어적인 안전성에 의존하지 않는다. 특별한 하드웨어 장치가 필요하지 않으므로 인터넷상에서의 전자상거래 지불수단에 활용할 수가 있다. 이러한 전자화폐 시스템으로는 ecash가 그 대표적인 예이다.

1. 네트워크형 전자화폐

최근에 스마트 카드와 같이 추가적인 하드웨어가 요구되지 않는 다음과 같은 대표적인 두 가지의 전자화폐 시스템들이 WWW상에서 지불을 할 수 있도록 개발되었다. 첫 번째가 완전한 익명성을 가지는 전자화폐 시스템인 ecash가 그것이다. 두 번째로는 완전한 익명성을 제공하는 것은 아니지만 좀 더 규모가 크며 신원확인이 가능한 전자화폐인 NetCash가 있다.

1.1 이캐쉬(ecash)

이캐쉬는 DigiCash사에서 개발된 전자화폐 시스템으로서 은닉서명 기술을 사용하여 온라인 상에서 완전한 익명성을 제공하고 있다.

이 시스템에서는 RSA 공개키 암호 방식을 사용하고 있으며 각 사용자는 자신들만의 공개키 쌍을 가지고 있게 된다. 그리고 이 시스템을 사용하기 위해서는 은행으로부터 전자화폐를 인출하고 예금할 때 사용하는 사용자의 전자지갑인 'cyberwallet'과 merchant 소프트웨어가 필요하다.

● 예금 인출 단계

예금을 인출하기 전에, cyberwallet은 인출

하기 원하는 전자화폐에 대한 100자리 정도의 random serial number를 생성하고 은닉서명 기법을 이용하여 은닉시킨다. 이것은 전자화폐에 랜덤인자를 곱하여 이루어지며, 사용자의 서명과 은행의 공개키로 암호화하여 은행에게 보내어진다. 은행은 사용자의 계정에서 인출을 원하는 금액만큼 공제한 뒤 전자화폐에 은행의 서명을 첨가한다. 그리고 사용자의 공개키로 암호화하여 사용자에게 다시 보내주면 사용자는 자신의 공개키로 복호화하고 자신이 곱했던 랜덤인자로 동전을 나누어 은닉된 동전을 해제시킨다. 은행은 사용자가 사용한 은닉인자를 알지 못한 채 서명을 했기 때문에 사용자에게 완전한 익명성을 제공한다.

● 지불 단계

상품을 구입하기 위해서는 [그림1]과 같은 단계를 거치게 된다.

1. 사용자의 web client는 Merchant의 URL을 요구하는 메시지를 보낸다.
2. 이 메시지는 Merchant의 CGI(Common Gateway Interface)를 호출한다.
3. TCP/IP 연결을 사용하여 구매자와 연결된 Merchant 소프트웨어는 지불 요구를 한다.
4. 지불 요구를 받은 cyberwallet은 지불 여부를 사용자에게 물어보고 동의한다면 전자화폐를 보낸다. 이때 이 동전(coin)은 Merchant의 공개키(K_M^U)로 암호화되어 전송된다.

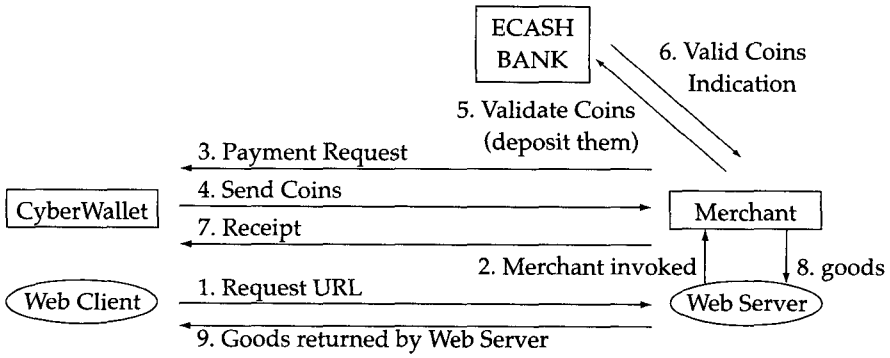
$$E_{K_M^U}(coin)$$

만약, 동의하지 않는다면 사용자들은 '거절' 메시지를 보낸다.

5. 전자화폐를 받은 Merchant는 전자화폐 발행 은행에 접속하여 전자화폐의 유효성과 이중사용여부를 확인하기 위해 자신의 서명을 붙이고 은행의 공개키(K_B^U)로 암호화하여 은행에 전송한다.

$$E_{K_B^U}(E_{K_M^R}(coin))$$

6. 은행은 데이터베이스를 확인하여 전에 사용되어 은행에 되돌아 왔는지를 serial number로 확인한다. 유효하다면 Merchant의 계좌에 동전만큼의 금액을 입금해 준 뒤 그 serial number를 은행의 데이터베이스에 저장한다.
7. 예금이 입금되었으면 Merchant는 구매자의 cyberwallet에 서명이 된 영수증을 보낸다.
8. 구입 목록을 Merchant ecash 소프트웨어로부터 Web server로 보낸다.
9. 구매자에게 구입 목록에 대한 정보를 전달한다.



[그림 1] ecash를 사용한 상품 구매 단계

1.2 NetCash

NetCash는 Southern California 대학의 Information Sciences Institute에서 개발한 전자화폐 프레임워크로서 이것은 PayMe 시스템의 기초가 되었다 이 시스템은 NetCheque와 같은 전자수표 등의 금융도구와 교환이 가능한 분산 Currency Server(CS)를 기반으로 하고 있으며 전자화폐로 바꾸어 사용할 수가 있다.

NetCash 시스템은 구매자와 상점 그리고 전자동전을 발행하는 CS들로 구성이 되어있다. CS는 공개키/개인키 쌍을 생성하며 이 공개키는 중앙 기관(FIC : Federal insurance corporation)의 서명이 되어 확인된다. 이 인증서(certificate)는 CS의 certificate ID(Cert_id)와 이름(CS_name), CS의 공개키(K^U_{CS}), 발행일(issue_date)과 유효기간(exp_date)등을 포함하고 있으며, 그리고 중앙 기관의 서명($E_{K^R_{Auth}}[M]$)이 되어 있다.

$$E_{K^R_{Auth}}(\text{Cert\_id, CS\_name, } K^U_{CS}\text{, issue\_date, exp\_date})$$

NetCash에서 쓰이는 동전(coin)은 CS의 이름(CS_name), CS의 주소(CS_addr), 화폐유효기간(exp_date_num), 화폐금액(coin_val)을 포함하며, CS의 개인키로 서명($E_{K^R_{CS}}[M]$)이 되어 있다.

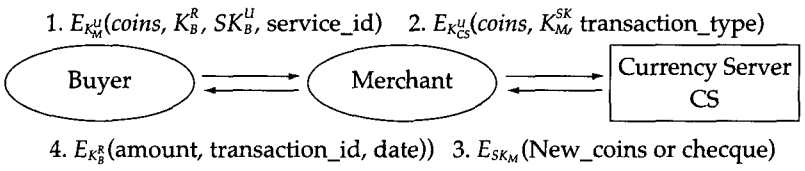
$$E_{K^R_{CS}}(\text{CS\_name, CS\_addr, exp\_date\_num, coin\_val})$$

CS는 모든 사용된 동전의 사용 경로를 유지하기 때문에 구입 단계에서 데이터베이스에 저장된 동전의 serial number를 확인함으로써 이중사용이 방지된다. 동전의 serial number가 확인이 되면 데이터베이스로부터 삭제하여 다시 새로운 동전으로 교환하여 줄 수가 있다 (coin exchange). 또한 전자수표도 CS에 의해 다시 전자동전으로 교환이 될 수 있다.

동전 소유자의 익명성을 제공하기 위해 소유자는 CS에 자신이 가진 동전을 제공하고 새로운 동전을 발행해 줄 것을 요구한다. CS는 누가 동전을 발행하였는지 알 수가 없으며 단지 그 동전들이 어디에서 왔는지 네트워크 주소만을 알 수가 있다. 동전을 교환하고 CS를 임의로 선택하기 때문에 동전의 사용 경로를 추적하기가 어렵다. 만약 자신이 발행하지 않은 동전을 받게 되면 CS는 발행서버와 연결하여 동전의 유효성을 체크한다.

[그림 2]는 상인으로부터 상품을 선택하여 지불을 하는 과정을 보여주고 있다. 이 교환에 있어서 상인은 구매자의 네트워크 주소만을 알기 때문에 구매자의 익명성을 유지할 수 있다.

1. 구매자는 동전(coin),구입한 서비스 id(service_id), 구매자의 새롭게 생성된 비밀키($K_B{}^R$), 그리고 public session key($SK_B{}^U$)를 상인의 공개키($K_M{}^U$)로 암호화하여 상인에게 전송한다.
2. 상인은 받은 동전(coins)이 유효한지 확인하기 위해 그것들을 Currency Server(CS)에게 보낸다. 이때 상인은 새로운 대칭 세션키(SK_M)와 CS사이의 거래형식(transaction_type)을 함께 보낸다.
3. CS는 자신의 데이터베이스를 확인하여 동전의 유효성을 확인한다. 유효한 동전의 CS의 데이터베이스에 시리얼 번호가 나타나게 된다. CS는 새로운 동전을 상점의 세션키로 암호화하여 상점에게 되돌려 준다.
4. 상인은 구매자에게 영수증을 되돌려준다.

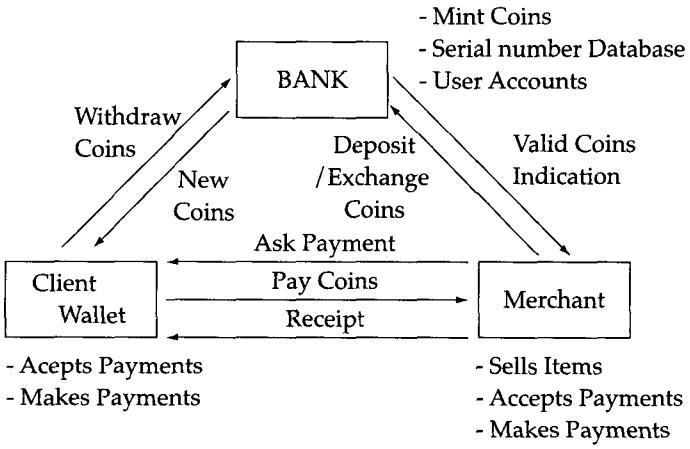


[그림 2] NetCash를 사용한 물품구입 단계

1.3 PayMe

PayMe[17]는 온라인 상에서의 전자화폐 시스템으로서 앞에서 언급한 ecash와 NetCash 시스템들의 장점만을 취합하여 만들어졌다. 이 시스템의 주된 목적은 NetCash의 특징에 Ecash의 익명성의 장점을 제공하기 위한 것으로 NetCash와 Ecash, Magic Money와 Netbill과 같은 관련이 있는 다른 시스템들에 많은 아이디어를 두고 있다. 참여하는 객체는 은행들과 사용자들이다. 사용자는 구매자와 Merchant가 될 수 있으며 같은 기능을 가지고 있다. 그들은 지불과정을 수행하고 지불을 받아들이거나 또는 은행과 거래를 한다. 각 은행은 시리얼 번호를 가지고서 자기 자신의 전자화폐를 발행한다. 전자화폐의 이중사용은 은행이 전자화폐에 대한 데이터베이스를 유지함으로써 방지된다. 이 PayMe 시스템에서 어떠한 사용자도 지불을 하고 전자화폐를 받아들일 수가 있다.

[그림 3]은 PayMe 시스템의 기본적인 기능들에 대해 보여주고 있다.



[그림 3] PayMe 시스템의 기본 기능

이 시스템에서는 대칭키와 공개키 암호 알고리즘을 사용하고 있으며 각 참여 개체는 그들 자신만의 공개키/비밀키 쌍을 가지고 있다. 이 PayMe 시스템에서는 두 개체 사이에서의 안전한 통신 프로토콜을 사용하기 위해 PMTP(PayMe Transfer Protocol)[17]이라는 자체 통신 프로토콜을 사용하고 있다. 이것은 보안성과 Web의 HTTP 프로토콜의 밖에서의 통신 방법을 제공하고 있다.

PMTP는 여섯 개의 request-response 메시지로 구성이 되어 있으며 각 메시지는 메시지 수신자에게 어떠한 행동을 취할 것을 요구하는 'request', request 메시지에 의해 취한 행동을 포함하는 'response' 그리고 response 메시지

에 대해 거절하는 메시지인 'refusal' 이라는 세 개의 다른 메시지들로 구성이 되어 있다.

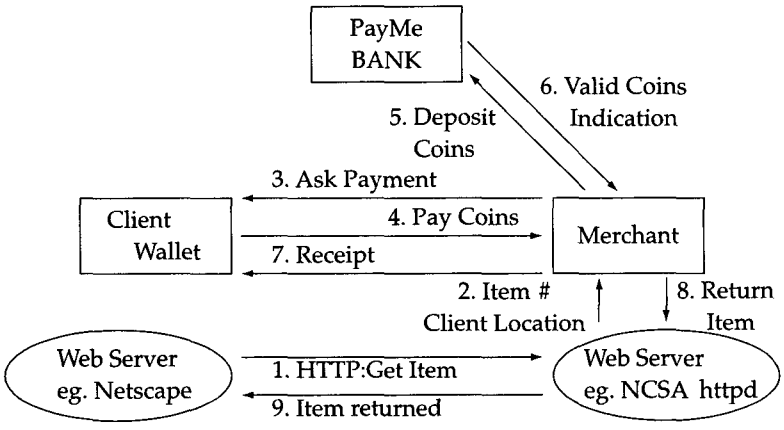
이 시스템 내에서 전자화폐는 표시된 금액만큼 나누어 사용할 수가 있다. 전자화폐는 공개키 암호 알고리즘을 이용하여 전자서명이 되어 있다. 각 전자화폐는 발행이 되었을 때 은행의 데이터베이스와 일치하는 시리얼 번호를 가지고 있다. 전자화폐는 화폐 발행 금액, 시리얼 번호, 은행의 id, 은행의 호스트 이름과 포트 번호 그리고 유효기간 항목이 있다. 이러한 다섯 개의 필드가 모두 기록이 되고 은행의 비밀키로 서명이 될 때 정당한 전자화폐가 발행이 되게 된다. 전자화폐의 자료구조 형태는 다음과 같다.

$E_{K_B^S}$(발행금액 ‖ serial_num ‖ Bank_id ‖ Bank_host_name ‖ Port_num ‖ exp_date)

● PayMe with the Web

Payme 프로토콜은 어떠한 웹 클라이언트와 서버사이에서도 사용할 수 있도록 만들어졌다. 사용자는 PayMe Wallet과 다른 웹 클라이언트를 가지고 물품 구입을 시작한다. 이 브라우저들은 HTML 문서로 만들어진 상점을 찾을 때까지 웹을 검색한다. PMTP 메시지들의 조합은 [그림 4]에서처럼 구매 거래를 하는데 사용이 된다.

1) 물품을 구입하기 위해 물품이 게재된 URL을 선택한다. URL이 선택이 되었을 때 웹 서버는 자동적으로 상점의 Wallet 소프트웨어를 가동시킨다. 이것은 CGI를 사용하여 작동한다.
2) Wallet은 물품과 클라이언트의 네트워크 주소를 선택한다.
3) Merchant의 Wallet은 가격을 보고 구매자의 Wallet에 접속하여 지불을 요청한다.
4) 구매자는 지불 요청에 대해 지불을 할 것인지 거절을 할 것인지 결정한다. 만약 구매 자가 지불을 할 경우에는 정확한 금액을 Merchant에게 보낸다.
5) Merchant는 새로운 동전으로 그 동전을 교환하거나 또는 은행에 입금함으로써 동전의 유효성을 확인한다.
6) Merchant는 exchange_coins_response와 deposit_coins_response와 같은 동전의 유효성 여부에 대한 응답을 받는다.
7) 지불이 성립되면 Merchant는 buyer에게 영수증을 보낸다.
8) 구입 목록은 Merchant로부터 웹 서버로 보내어진다.



[그림 4] PayMe를 사용한 물품 구매 단계

9) 그리고 나서 웹 서버는 웹 클라이언트에게 구입 목록을 전송한다.

1.4 밀리센트(Millicent)

밀리센트 전자화폐 시스템[16]은 현재 신용카드나 기타 지불 시스템으로 지불 처리를 하기 어려운 소액 거래를 이루기 위해 미국의 DEC(Digital Equipment Corp)사에서 개발한 대표적인 소액 지불 시스템이다. 이 시스템은 크게 사용자가 사용하는 전자 화폐인 스크립(Scrip)과 스크립을 판매하는 브로커(Broker)를 중심으로 하고, 여기에 물품을 판매하는 상점(Vendor)이 참여하는 가입자 기반의 전자화폐 시스템이다. 그리고 사용자는 클라이언트 소프트웨어인 Millicent Wallet을 사용하여 물건을 구입하고 대금을 지불한다.

다음에서는 이 시스템을 구성하고 있는 각 개체에 대해 살펴보도록 한다.

● 스크립(Scrip)

밀리센트에서는 물건을 구입하기 위해 현금을 사용하는 대신에 스크립이라고 하는 각 vendor마다 다른, 독특한 전자 현금을 사용한다. 스크립은 미리 대금을 지불한 선불 형태이며 해당 판매자(Vendor)에게만 사용이 가능하다. 밀리센트 시스템에 있어서 스크립은 브로커나 또는 판매자가 발행을 할 수가 있다.

Scrip Body	Vendor	Value	ID#	Cust_ID#	Expires	Props
Certificate	*H(Scrop Body ll master_customer_secret)*					

[그림 5] 스크립의 구조

1) Vendor : 스크립을 발행한 상거래 서버 ID
2) Value : 스크립의 화폐 가치
3) ID# : 스크립의 이중 사용을 막기 위한 일련의 유일한 번호. 이 번호는 나중에 Vendor나 Broker측에서 master_scrip_secret을 만드는데 사용된다.
4) Cust_ID# : 스크립을 사용하는 사용자의 ID.
   일부분이 master_customer_secret를 만드는데 이용된다.
5) Expires : 스크립의 유효기간.
6) Pros : 기타 데이타
7) Certificate : 스크립에 대한 변조 여부를 확인하기 위한 인증서로서 Scrip Body 부분과 master_customer_secret를 해싱한 결과이다.

● 스크립의 종류

1) customer_secret
   : 사용자(customer)에게 보내어지는 스크립
   : 사용자는 이 비밀키로 스크립의 소유권을 증명하는데 사용한다.
2) master_customer_secret
   : 상거래 서버(Vendor)가 사용하는 비밀키
   : 사용자(customer)가 보내온 스크립의 고객정보(Cust_ID#)로부터 customer_secret를 만드는데 사용한다.
3) master_script_secret
   : 이중 사용과 위조를 막기 위해 상거래 서버(Vendor)가 사용

: 스크립의 유효성을 확인하기 위해 Certificate를 만드는데 포함된다.

● 브로커(Broker)

사용자들과 vendor들의 계정을 관리하고 모든 실제 돈의 거래를 다루며 사용자들에게 스크립을 판매하고 vendor들에게 지불을 한다. 고객들은 브로커에 가입해서 계정을 가지려면 신용 카드나 더 안전한 전자 화폐 방식을 이용해서 등록을 하고 나중에 브로커로부터 스크립을 살 때 이들 지불 방식으로 지불하면 된다. 스크립은 해당 상인에게만 유효하기 때문에 다른 스크립을 사기 위해서 브로커를 통해 해당 상인과 거래를 하고 있는 다른 브로커로부터 해당 상인의 스크립을 구입하여 사용하게 된다.

● Millicent Protocol Transaction

다음에서는 Millicent를 이용하여 상점과의 거래를 하기 위해 수행해야할 등록, 스크립 구입, 상품 구입 및 결제 방법에 대해 설명하고 있다.

1) 등록

신용 카드와 같은 다른 지불 수단을 이용하거나 Millicent 프로토콜을 확장하여 보다 안전한 채널상에서 브로커의 스크립을 구입하고 사용자의 비밀키인 customer_secret을 브로커로부터 받는다.

2) Vendor Scrip 구입

사용자가 customer_secret과 브로커 scrip을 이용하여 브로커에게 거래하고자 하는 Vendor의 scrip을 구입 요청한다. Vendor로부터 이미 스크립 발행에 대한 정보 (master_scrip_secret, ID#, master_customer_secret)를 가지고 있는 브로커는 그 발행 범위내에서 Vendor 스크립을 발행한다. 이 때 사용자가 제시한 브로커 스크립과 브로커가 발행한 Vendor 스크립의 차는 다시 새로운 거스름 브로커 스크립을 발행함으로써 해결한다.

3) 상품 구입 및 결제

Vendor 스크립을 가지고서 Vendor측 서버에 접근하여 상품을 구입하는 단계이다. 먼저 customer는 Vendor에게 Request문(Request ll Scrip ll H(scrip ll master_scrip_secret) ll Customer_secret ll H(Request ll Scrip ll H(scrip ll master_scrip_secret))을 보낸다. 보다 강력한 보안을 제공하기 위해 Customer_secret을 관용 암호화 방식의 DES, RC4 또는 IDEA와 같은 알고리즘의 비밀키로 이용하여 데이터의 암호화 전송에 이용될 수도 있다. Request문을 받은 Vendor는 먼저 scrip 안에 포함되어 있는 Expires 필드를 이용하여 유효 기간과 Request문을 검사한다. 이는 Request문에 같이 붙어서 온 Request Signature와 (Request ll Scrip ll H(Scrip ll master_scrip_secret))을 해싱한 값을 비교하여 같으면 유효한 것으로 유효성 검사가 끝나면 Vendor는 사용자가 선택한 상품의 배송과 함께 거스름 스크립을 만들어 사용자에게 보낸다.

2. IC 카드형 전자화폐 시스템

2.1 몬덱스(Mondex)

몬덱스는 1994년 금융과 통신 기능을 융합시킨 새로운 IC 카드 중심의 전자화폐 시스템으로서 가장 대표적인 전자화폐 시스템이다. 이 몬덱스 카드는 현재 운용되고 있는 유일한 off-line 시스템으로 현금과 가장 유사하며 현금 지불의 장점과 카드 지불의 편리함을 결합한 새로운 지불 방식이다.

이 시스템의 특징은 거래시 어떤 기관이나 카드 발행사로부터 거래 승인이 필요 없고 개인간의 자금 이체가 자유롭게 이루어질 수 있으며 개인의 프라이버시가 완벽하게 이루어질 수 있다는 점에서 많은 주목을 받고 있다. 또한 몬덱스 카드는 5개국 통화로 가치를 저장할 수 있으므로 해외에서의 사용 및 송금과 외환 거래도 가능하다.

● 몬덱스 구성 장비

몬덱스에서는 실물 화폐를 대신하여 전자화폐가 사용되기 위해 필요한 7가지 항목을 제시하고 있다.

1) 세계 어디서도 이용 가능할 것.
2) 정산이나 결재 수속이 없고 회계 처리를 동반하지 않을 것.
3) 거래 장소에서 통화 지불이 즉시 이루어질 수 있을 것.
4) 개인간에 즉시 지불이 이루어질 것.
5) 각국의 통화 교환이 이루어질 수 있을 것.
6) 이용자에게 널리 사용될 수 있는 표준적인 카드 형식의 채용
7) 몇 번이라도 전자화폐를 카드에 재 입금할 수 있을 것.

이상과 같은 항목을 목표로 몬덱스에서는 상품 개발이 이루어져 다음과 같은 장비들이 구성되었다.

1) 몬덱스 웰렛(Mondex Wallet)

포켓 사이즈의 소형 IC 카드 단말기로 카드의 내용 표시나 개인간의 전자화폐 이체가 이루어지며 나중에 사용할 수 있도록 몬덱스 전자화폐를 저장하기도 한다. 이 Wallet은 은행이 고객에게 대여한다.

2) 몬덱스 밸런스 판독기(Mondex Balance Reader)

밸런스 판독기는 카드에 저장되어 있는 잔액을 나타내 준다.

3) 몬덱스 전화기(Mondex Telephone)

전화기와 판독 장치를 통합한 것으로 전화 회선을 통하여 카드에 입금은 물론 통신 판매 대금 결제와 개인간의 금전 거래도 가능하다. 사용되는 전화로는 가정용 전화와 공중 전화가 있다.

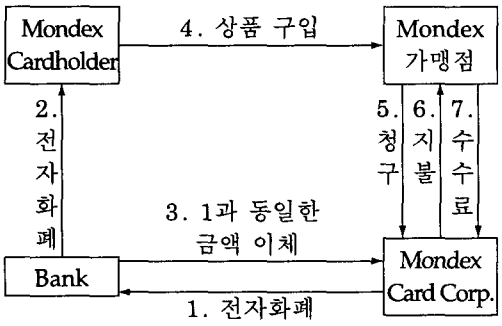
4) 몬덱스 카드(Mondex Card)

몬덱스 카드는 평범한 플라스틱 카드 안에 작은 마이크로 컴퓨터 칩이 포함되어 있는 통합 회로 카드(Intergrated Circuit Card : ICC), 즉 스마트 카드이다. 이 카드는 IC 카드에 대한 국제 기준인 ISO 7816 통합 회로 카드(ICC)의 형태를 띠고 있다. 은행이 발행하여 고객에게 대여하며 은행 계좌와 연동이 되어 추가 입금이 가능하다. 또한 비밀 번호에 의한 보안 기능이 있으며 IC 칩의 안전 관리는 은행이 담당하고 있다. 몬덱스 칩은 극도의 추위나 더위, 그리고 습기, X-ray 또는 전기적 간섭에 잘 견디도록 설계되었다. 또한 몬덱스사에서는 Multi-Application Operating System(MAOS)으로 불리는 COS(Chip Operating System) 개발에 나서 1999년 초에 MAOS에 기반한 실증실험에 나설 계획으로 있다. 이 COS는 IC카드에서 전자화폐 및 신용카드 등의 기능을 부여하는 응용 소프트웨어를 구동시킴으로써 사용자는 여러개의 카드를 갖고 다니는 불편을 해소할 수가 있게 된다. 현재 이 MAOS 기술은 차세대 전자화폐 기술로 인식돼 경쟁적으로 도입되고 있고 전자화폐 시대의 개막을 알기는 기술로 인식이 되고 있다.

● 흐 름

[그림 6]은 몬덱스 구성 장비를 이용하여 사용자(Cardholder)가 몬덱스 가맹점으로부터

상품을 구입하고 대금을 지불하는 과정을 나타내고 있다.



[그림 6] 몬덱스 거래흐름

1) 몬덱스사는 몬덱스 회원은행과 전자화폐를 실제 화폐로 교환하여 공급한다.
2) 몬덱스 카드를 소지한 고객은 은행의 ATM기나 또는 몬덱스 전화기를 통해 전자화폐 를 받는다.
3) 회원은행은 고객에게 전달한 금액만큼의 전자화폐를 몬덱스사의 계좌에 이체한다.
4) 몬덱스 카드에 전자화폐를 저장한 cardholder는 가맹점에서 물품을 구입하고 상점의 몬덱스 단말기를 통해 대금을 지불한다.
5) 전자화폐를 받은 몬덱스 가맹점은 통신요금을 절약하기 위해 일정 분량을 모아 몬덱스 서비스사에 통신 회선을 통해 전자적으로 청구한다.
6) 청구를 받은 몬덱스 서비스사는 제휴은행 가맹점 계좌에 물품 대금을 입금시킨다.
7) 그리고 동시에 일정의 가맹점 수수료를 가맹점의 예금 계좌에서 징수한다.

2.2 비자 캐쉬(Visa Cash)

비자에서 개발한 마이크로 칩이 내장된 선불 카드 개념의 비자 캐쉬[21]는 인터넷과 같은 개방 네트워크에서 소액 지불을 위한 지불 수단이다. 비자 캐쉬는 여러 가지의 형태가 있지만, 가장 대표적인 것이 'Disposable Visa Cash'와 'Reloadable Visa Cash'가 있다. 'Disposable Visa Cash(일회식 Visa Cash)'는 현재 사용되고 있는 지하철 패스나 버스 카드와 같은 개념의 선불카드로서 한번 구입한 카드는 사용 후 재사용할 수가 없다. 반면에 'Reloadable Visa Cash(재충전식 Visa Cash)'는 플라스틱 카드에 마이크로 칩이 내장되어 있어 화폐 가치를 저장하게 된다. 그리고 저장된 화폐 가치를 모두 사용한 후, 다시 금액을 저장하여 사용할 수 있다. 비자 캐쉬는 실생활에서는 물론 가상 쇼핑몰에서도 사용할 수가 있다. 사용자가 인터넷 쇼핑몰에서 사고 싶은 물품을 선택하고 지불 수단으로 비자 캐쉬를 선택한 후 비자 캐쉬 카드를 카드 리더기에 삽입하고 지불 수단으로 컴퓨터 화면상에 나타난 비자 캐쉬에 남아 있는 현금 가치와 구입품의 가격을 확인, 버튼을 클릭하면 된다. 이때 거래 금액이 비자 캐쉬 액면금액에서 차감 되면 거래는 완성된다.

비자 캐쉬는 'Visa Cash' 로고가 붙어 있는 가맹점이면 어디에서나 사용할 수 있으며 현재 비자 캐쉬가 통용되는 국가는 미국, 일본, 대만, 영국 외 11개국에서 사용할 수가 있다.

2.3 PC Pay

사용자의 PC에 설치되어 사용되고 있는 소프트웨어 형태의 암호 툴들은 인터넷상에서의 거래를 위해 오늘날 제안되고 있는 공통적인 접근 방식이다. 그러나 이러한 접근 방식은 여러 가지 취약점을 가지고 있는데 그 중 한가지는 현재의 금융 기관 구조를 간과하고 개발된 제품 위주의 접근 방식을 취한다는 것이다. 이것은 사실상 자유로운 접근 기회를 감소키고 수행 시간을 증가시키는 요인이 되고 있다. 또한 PC상에서의 암호화는 홈 뱅킹과 같은 거래를 이루도록 하는데에 있어서 다양한 형태의 공격을 당할 수가 있다. 이에 Innovonics사

에 의해 개발된 PC Pay 시스템[23]은 스마트 카드와 카드 리더기로 구성이 된 하드웨어에 기반하여 안전한 전자지불 시스템을 구성하고 있다.

PC Pay 시스템은 스마트 카드와 카드 리더기로 구성된 PC Pay device와 interface software로 구성이 되어 있다. 스마트 카드는 계좌에 접근하거나 전자화폐를 전송 받아 저장하며 신분 확인을 하는데에 이용할 수 있는 확실한 방법이다. 그러나 스마트 카드에 있는 정보는 PC상에 있는 소프트웨어에 의해 불법적인 접근이 가능하기 때문에 이를 방지하기 위해 스마트 카드 리더기는 PIN-pad를 가지고 있다. 또한 PC Pay device는 PIN 정보나 계좌 정보와 같이 중요한 정보가 PC상에 도달하기 전에 카드 리더기에서 안전하게 암호화하여 PC에 전송한다. PC Pay device는 ATM과 같이 안전하게 설계가 되었으며 신용카드나 또는 직불카드와 같은 마그네틱 테입을 읽을 수도 있으며 스마트 카드를 사용할 수도 있도록 설계가 되었다. 또한 자신의 PIN을 입력하고 이 PIN 정보와 계좌 번호의 조합은 DES 암호 알고리즘을 사용하여 암호화되며 암호화된 정보는 PC에 보내어진다. 그리고 현재 사용하고 있는 ATM과 유사한 통신 프로토콜을 사용하여 서버에 전송이 된다. 스마트 카드는 자신의 계좌에 접근하거나 전자화폐를 은행으로부터 전송 받아 저장할 때에 사용이 된다.

IV. 각종 전자 지불 시스템 비교 분석

[표 1] 각종 전자화폐 시스템의 비교

제 품	지불 메카니즘 형태	보안 메카니즘	S/W 요구사항	H/W 요구사항	익명성	양도성	이중사용 방지
Mondex	스마트카드를 이용한 전자화폐	마이크로칩	X	O	O (strong)	O	O
CyberCoin	소액지불을 위한 전자화폐	RSA, DES	O	X	O (strong)	X	O
PC Pay	스마트카드를 이용한 전자화폐	Hardware - based	O	O	O (strong)	X	O
ecash	전자화폐	RSA	O	X	O (strong)	X	O
PayMe	전자화폐	Symmetric & Asymmetric key encryption	O	X	O (Resonably)	X	O
NetCash	전자수표	Kerberos authentication	O	X	O (low)	X	O
Visa Cash	선불카드 개념의 전자화폐	마이크로칩	O	O	O	X	O
Millicent	소액지불을 위한 전자화폐	소액거래	O	X	O. (Reasonably)	X	O
EIPaN	전자화폐	microchip	X	O	O (strong)	X	O
NetFare	선불카드 개념의 전자화폐	card number & PIN	X	O	O (strong)	X	O

다음 [표 1]에서는 현재 개발되어 있는 각종 전자화폐 시스템을 지불 메카니즘, 보안 메카니즘, H/W 및 S/W 요구 사항, 익명성, 양도성, 이중 사용 방지 등의 특징별로 나누어 비교하고 있다

[표 1]에서는 대표적인 전자화폐 시스템들에 대해 비교하였으나 이밖에 선진 각국에서는 스마트 카드를 중심으로 하는 각종 전자화폐 시스템을 개발하고 있으며 벨기에의 Proton, 포르투갈의 MEP, 덴마크의 Danmont, 핀란드의 AVANT, 독일의 Chipknip 등이 있다. 대부분의 전자화폐 시스템들은 불추적성과 이중사용 방지는 만족시켜주고 있으나 양도성을 만족시켜 주고 있지는 못하며 완벽한 익명성을 요구하는 사용측의 입장과 전자화폐의 부정사용이나 돈 세탁 등을 방지하기 위한 통화 관리 차원에서의 추적 가능성을 요구하는 은행 당국 입장과의 차이를 얼마만큼 줄이느냐에 관한 관심도 증가하고 있다.

V. 결 론

현재의 전자 지불 시스템은 크게 지불 브로커형과 전자화폐형이 있으며 이 두 가지 방식의 각종 전자 지불 시스템들이 쏟아져 나오고 있다. 지불 브로커형으로써 요즘 크게 각광 받고 있는 SET 시스템은 신용카드를 기반으로 하는 것으로 현재의 상거래 관행에서 크게 벗어나지 않는다는 장점으로 인해 지불 시스템에 있어서 거의 표준으로 잡혀가는 것으로 보인다. 그러나 지불 브로커형은 현재의 시장 여건에 큰 충격을 주지 않기 위한 것일 뿐 궁극적으로 추구하는 시스템은 IC카드를 기반으로 하는 전자화폐 시스템이 될 것이다. 이같은 IC카드형 시스템과 인터넷으로 대표되는 네트워크 시스템과의 결합은 최근 세계적인 경향으로 추진되고 있으며 또한 고액 결제를 위해서는 온라인 방식을 취하고 소액 결제를 위해서는 오프라인 방식을 취하는 양쪽 모두를 혼용하여 쓰는 방식으로 진행되고 있다. 이러한 기술의 좋은 예가 현재 몬덱스에서 개발하고 있는 MAOS를 들 수 있을 것이다. 이 IC카드 안에는 EMV방식, 신용/직불 카드의 기능 그리고 전자화폐 저장 기능 등의 여러 가지 형태의 지불 수단이 가능한 것이 특징이다.

21세기를 눈앞에 둔 오늘날 기존의 상거래 시스템의 변혁은 시작이 되었으며 상거래 시스템에서 가장 중요한 지불 시스템을 확보하려는 선진국들의 경쟁도 이미 시작되었다. 아직 우리에게 피부에 와 닿지는 않지만 곧 우리 주위의 경제 활동은 사이버 공간에서 이루어지게 될 것이며 이를 위한 상거래 시스템을 누가 손에 쥐는가가 앞으로의 국가 경쟁력을 좌우할 중요한 변수로 등장하게 될 것이다. 이러한 전자지불 시스템 특히 IC카드를 기반으로 하는 전자화폐 시스템은 법, 제도적으로나 기술적으로 많은 연구와 투자가 이루어져야 하며 이러한 경쟁에서 뒤쳐진다면 국가나 기업 그리고 개인 모두에게 많은 피해를 안겨줄 것이다.

지금 이 순간에도 세계의 곳곳에서 새로운 금융 결재 시스템이 만들어지고 있다. 이에 본고에서는 현재 주목받고 있는 각종 전자화폐 시스템을 분석함으로서 기술 혁신이 초단위로 이루어지고 있는 현재 전자화폐 시스템의 최신 개발 동향을 파악하고 그에 대한 적절한 대비책을 세워나가 전자상거래 시대의 도래에 대비하고자 한다.

참고 문헌

[1] D.Chaum. "Blind Signature for Untraceable Payments". In Advances in Crytology - CRYPTO '82 Proceedings. Plenum Press. pp199-203, 1983.

[2] T.Okamoto and K.Ohta, "Disposable zero-knowledge authentication and their application to untraceable electronic cash", In Advances in Cryptology - CRYPTO '89. LNCS 435, Springer - Verlay, pp481-496, 1990

[3] T.Okamoto and K.Ohta, "Universal electronic Cash", CRYPTO '91, LNCS 576, Springer - Verlay, Berlin, pp324-337, 1992

[4] J.Camenisch, U.Manrer and M.Stadler, "Digital Payment Systems with Passing Anonymity-Revoking Trustees", In Esorics'96, Italy, 1996.

[5] Y.Frankel, Y.Tsiounis and M.Yung, "Indirect Discourse Proofs : Achieving efficient fair off-line coins", In Advances in Cryptology, Proc.of Asiacrypt'96, LNCS 1163, pp286-300, 1996

[6] D.Chaum, A.Fiat and M.Noar, "Untraceable Electronic Cash", CRYPTO '88, LNCS 403, Springer - Verlag, pp319-327, 1989

[7] T.Eng and T.Okamoto, "Single - term Divisible Electronic Coins", Advances in Cryptology, Proceedings of Eurocrypt '94, Springer-Verlag, pp311-323, 1994

[8] D.Chaum and T.P.Pederson, "Wallet databases with observes", Proproceeding of CRYPTO '92, Springer - Verlay, pp89-105, 1992

[9] S.Brands, "Untraceable off-line cash in wallets with observers", CRYPTO '93, Springer - Verlay, pp302-318, 1993

[10] S.Brands, "Electronics Cash System loased on the Representation Problem in Groups of Price Order", Techinical Report CS-R9323, CWI, Amsterdam, 1993

[11] Y.Yacobi, "Efficient electronic money", Advances in Cryptology, Proceedings of ASIA CRYPTO '94, Springer - Verlay, pp153-163, 1994

[12] D.Chaum and T.P.Pedersen, "Transferred Cash Grows in Size", presented at Eurocrypto '92, pp390-407, 1992

[13] M.O.Rabin, "Digital Signatures", Foundations of Secure Communication, NewYork:Academic Press, pp.155-168, 1978

[14] T. Okamoto, "An Efficient Divisible Electronic Cash Scheme", Advances in Cryptology, Proc. of Crypto '95, LNCS 963, pp.438-451, 1995

[15] 베리폰사, http://www.verifone.com

[16] Millicent Protocol, http://www.millicent.digital.com

[17] CyberCash사, http://www.cybercash.com

[18] 몬덱스사, http://www.mondex.com

[19] DigiCash사, http://www.digicash.com

[20] M.Peirce, "PayMe : Secure Payment for World Wide Web Services", B.A. (Mod) Project Report, Computer Science Department, Trinity College Dublin, Dublin2, Ireland, May 1995

[21] Visa 카드사, http://www.visa.com/cgi-bin/bee/pd/cash/fag.html

[22] Visa 카드 코리아, http://www.visakorea.com/product5.htm

[23] Innovonics사, http://www.innovonics.com/pcpay/pcpay/home.html

□ 著者紹介

오 형 근

1998년 2월 순천향대학교 전산학과 졸업(전산학사)
1998년 3월 ~ 현재 순천향대학교 대학원 전산학과 석사과정 재학중

※ 주관심분야 : 전자화폐, 전자상거래, 암호이론

이 임 영

1981년 홍익대학교 전자공학과 졸업(학사)
1986년 일본 오오사카대학 통신공학부(석사)
1989년 일본 오오사카대학 통신공학과(박사)
1992년 ~ 1994년 한국전자통신연구원 선임 연구원
1994년 ~ 현재 순천향대학교 컴퓨터학부 교수

※ 주관심분야 : 암호이론, 정보이론, 컴퓨터 보안