한국 금융구조형 전자화폐 모델에 대한 연구

최 승 우, 김 용 득
아주대학교 전자공학과
전화 : 031-219-2372

Study of Electronic Money for Korean Finantial Situation

Seung Woo Choi, Yong-Deuk Kim
Dept. of Electronic Engineering, Ajou University
E-mail : dul2csw@comnet.ajou.ac.kr

Abstract

In this treatise information communication indust based change phenomenon of payment system of money explain and study and compare way ago value that use electronic community of the world and presented correct electron money model in real condition of our country.

Draw payment way that consider particular situation and korean situation and that wi introduce electron money model of the world and analyze merits and demerits and is money here upon. Electron money introduction of smart card way that support all off-line and on-line that i currency and the nearest topology here directio must is insisting and relate in use of this or presenting value of money flowchart and draw the validity and hangup by introducing electronic mone model who is presenting in Kyong-gi Province and Su-won current and go forward group.

Proposed suitable electron money system in Korea situation by proposing money form and model of payment system that can satisfy all this all situation and physical special quality of mon by conclusion and clarify flow of the value.

I. 서론

현대의 과도기적 디지털화로 미루어 볼 때 가까운 미래에 정보통신의 기반 위에서 모든 행위가 일어나리라는 짐작을 쉽게 할 수 있다. 전자상거래가 활성화됨에 따라 자연히 기존의 현금이나 수표와 같은 결제방식은 전자상거래가 요구하는 실시간 결제에는 부적합하다는 것을 알 수 있다. 온라인 상으로는 물품을 구경만 하고 은행에 가던지 아니면 인터넷 뱅킹으로만 대금을 지불해야만 한다면 이는 반쪽 짜리 전자상거래임에 틀림없다. 아직 우리 주변에서 이러한 수준에 머물러 있는 쇼핑몰을 볼 수 있으며 이는 그 불편함으로 인해 개선되지 않는 한 곧 퇴화될 것이다.

아직까지 가장 널리 사용되고 있는 전자상거래 지불수단은 신용카드 방식이다. 신용카드는 후불이기 때문에 고객 입장에서는 당장 돈이 지출되는 입금보다 선호된다. 신용카드를 사용하기 위해서는 필연적으로 자신의 카드번호와 경우에 따라서는 비밀번호를 입력해야 하기 때문에 보안에 신경을 쓰는 고객의 경우에는 이 과정을 망설이게 된다. 이런 보안적인 취약점을 보완하기 위해 제시된 방법이 SSL(Security Socket Layer)이나, SET(Secure Electronic Transactions)와 같은 결제 보안이다. 그러나 오랜 기간 보안측면이 강화되어 온 신용카드 방식기반의 지불 시스템이라 할지라도 다음과 같은 단점이 있다

첫째, 확인과 정정이 필요한 시간 및 초과발생 등의 문제를 해결하기 위하여 결제 처리 시간이 필요하다.

둘째, 인터넷을 통한 전형적인 방법으로 결제하기 위해서는 소비자가 결제에 관련된 상세 정보와는 별도로 개인정보를 온라인으로 송부해야 한다. 그러나 전화 또는 우편으로 상세한 결제정보를 제공하는 것은 보안 문제를 야기 시킨다. 셋째, 적용 범위가 제한적이다. 넷째, 잠재적인 구매자는 신용카드와 수표계정에 적절한 신용등급을 보유하지 않아 사용에 부적합하다. 다섯째, 소액단위의 거래시 지원할 수 없다.

현재까지 소개된 전자화폐시스템은 크게 온라인 방식과 오프라인 방식, 혹은 IC 카드형과 네트워크형으로 나뉘어 지며, 가까운 미래에 지불수단이 하나로 통일된다는 가정하에서 볼 때 IC 카드형 전자화폐가 미래의 화폐유통시스템으로서 유력하다. 결과적으로 신용카드는 IC 카드형 전자화폐의 기능에 흡수되리라는 전망을 할 수 있다. 그리하여 본 고에서는 IC 카드형 전자화폐시스템의 종류별 분석 및 IC 카드형 전자화폐가 갖추어야 하는 보안 알고리즘과 유통구조, 사용되는 프로토콜을 조사해 보고 우리 나라에서 사용될 수 있는 IC 카드형 전자화폐시스템의 기준을 마련하여 방향을 모색해 보기로 한다.

II. 유형별 전자지불 시스템

전자상거래는 크게 상점시스템, 전자지갑, 인증기관 그리고 지불 시스템(payment system)으로 이루어진다. 전자화폐 시스템은 지불시스템으로서 그 주요 기능은 다음과 같은 서비스를 제공하는 것이다.

첫째, 지불인으로부터 수취인에게 가치를 전송할 수 있어야하며 둘째, 지불이 취소된 경우, 수취인으로부터 지불인에게 가치를 반환하여야 하고 셋째, 일반 화폐를 전자화폐로 변환 또는 그 반대로 전자적 가치(전자화폐)를 법정화폐로 변환하는 것을 가능케 하여야 한다. 이러한 전자지불시스템은 지불인(payer)과 수취인(payee)간의 통신, 이체시기, 온라인과 오프라인 능력 등의 기준에 따라 여러 가지로 구분될 수 있다.

아래의 흐름도에서는 지불 시스템 참가자들간의 정보흐름, 지불인과 수취인간의 통신, 선지불/후지불의 차원에서 4가지 유형의 지불 시스템 모형을 나타내고 있다. c와 d는 전자자금이체의 경우에 해당하며, 인터넷 지불 시스템의 대부분은 a 또는 b에 해당한다. 현금시스템의 경우, 지불인은 발행은행에서 전자화폐를 인출하여 수취인에게 지불한다. 수취인은 전자화폐를 거래은행인 매입사에 예금을 한다. 그 후 매입사는 발행사에 정산을 요청한다. 신용카드 결제와 같은 계정시스템의 경우, 지불인은 수취인에게 지불 정보를 통지한다. 수취인은 매입사로부터 지불 승인을 받고, 지불을 청구한다. 수취인으로부터 지불청구가 있은 후, 매입사와 발행사간에 정산이 이루어진다. 발행사는 지불인에게 지불내역을 통지한다.

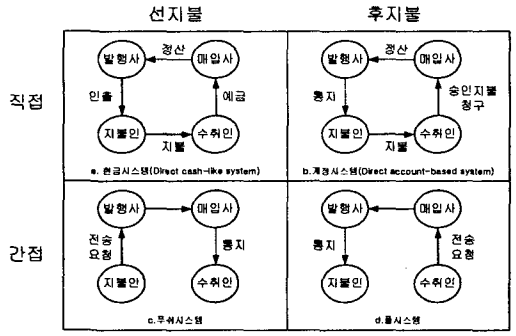

그림1 지불 모형

전자 화폐의 종류는 카드 소지자간에도 화폐가치의 이전 가능성에 따라 open-loop형과 closed-loop형으로 구분된다. closed-loop형의 경우 가치 흐름이 '카드 발행 기관 → 카드 소지자 → 가맹점 → 카드발행기관'으로만 흐르게 되어 있으며, open-loop형은 카드 발행기관에 통보할 필요 없이 카드 소지자간에도 자금 이전이 가능하다. 물론 기존의 현금과 유사한 형태의 가치흐름을 지닌 전자화폐의 종류는 open-loop형이라 할 수 있으며 open-loop형은 현재 영국의 Mondex카드가 유일하다. 다음의 표는 실제 사용되고 있는 전자화폐의 유형별 종류를 나타내고 있다.[2][10]

유형		명칭	특징
전자화폐형	네트워크형	E-Cash	네트워크 상에서 코인을 생성하여 이를 결제에 사용
		NetBill	네트워크 상에의 소비자와 판매자의 계좌를 설정하여 POS처럼 이체
	카드형	Mondex	카드 상에 현금가치를 이전하는 잔고보유 가능한 선불형 지갑카드로 제3자에게 가치 이전 가능
		Proton	선불형이며 제3자에게 가치 이전할 수 없음
전자수표형	FCTC	FCTC	카드에 내장된 저자수표장과 전자서명방식을 이용한 네트워크상의 수표
신용카드형	네트워크형	CyberCash	PC에 내장된 전용 소프트웨어가 미리 카드번호를 기억. 암호화된 카드 정보를 상인버캐쉬의 중계로 네트워크 상에서 결제에 이용
	카드형	FirstVirtual	일종의 회원등록과 같이 카드 정보를 사전에 등록. 전용회선번호로 네트워크 상에서 결제
전자자금 이체형		SENB	서비스를 제공, 지불대상과 금액만 입력하면 자금이체가 일어남

표1. 전자화폐의 유형별 종류

III. IC 카드의 특징

IC 카드는 기존 CREDIT 카드나 자기카드와 같은

크기, 같은 두께의 플라스틱 카드에 마이크로프로세서와 RAM, EEPROM, COS(Chip Operating System), 보안알고리즘 등을 갖춘 마이크로컴퓨터를 COB(Chip On Board) 형태로 내장한 카드를 말한다. 새로운 정보미디어의 총아로 불리는 IC카드는 다음과 같은 특징을 가지고 있다.

첫째, 높은 안정성을 들 수 있다. 마이크로프로세서를 내장하고 통신이 가능하며, 다양한 응용이 가능하다. 또한 연산처리를 할 수 있어 기밀 유지가 가능 할 뿐 아니라 위변조 등에 대한 안정성도 우수하다. 둘째, 대용량 메모리를 갖추고 있다. 자기카드의 100배에 해당하는 2K 또는 8K BYTE의 메모리 용량을 가지고 있고 데이터의 RANDOM한 읽기, 쓰기 및 수정이 가능하다. 셋째, 안정성이 높고 메모리 용량이 크기 때문에 여러 장의 카드를 소지해야 하는 불편을 덜 수 있다. 넷째, 정보의 분산 처리가 가능하다. Directory구조로 DATA FILE의 분산 보관이 가능하여 HOST 컴퓨터의 부담을 경감시킨다. 다섯째, 다양한 기능을 갖출 수 있다. IC카드에는 반도체 소자가 내장되어 있기 때문에 지적기능(정보의 저장/처리 기능, 프로그래밍 기능)을 부여할 수 있다. 따라서 그 이용분야가 다양하다. 여섯째, 높은 보안성 및 안정성을 들 수 있다. 일반적인 자기카드는 정보를 기억하는 매체인 자성체가 플라스틱 카드 표면에 부착되어 있어 기억된 정보나 데이터를 쉽게 해독 또는 임의 변경이 가능하기 때문에 정보의 안전성이 확실히 보호될 수 없었으나 IC카드는 이를 해소할 수 있다.

여덟째, 고도의 미디어 기능을 내포하고 있다. 다양한 접속성과 확장성에 의한 시스템 통합이 편리하며 Off-line 거래에 적합하다. 이러한 장점으로 인해 앞으로의 전자화폐는 스마트카드를 적극 활용한 형태가 될 것이다.[3][5]

IV. 스마트 카드의 통신 프로토콜

Reader state diagram 측에서는 다음과 같은 순서로 동작이 이루어진다. 리더기는 처음 Idle상태로 존재하며 카드가 삽입되면 카드에 파워를 공급해주고 ATR(answer to reset)을 기다린다. ATR을 받은 후 응용 단계 알맞은 protocol을 정립하고 명령어 휴지 상태에서 스마트 카드에 APDU(application protocol data unit)를 보낸 후 응답을 기다린다. 명령어에 대한 응답이 도착하면 다음 명령어를 보낼 준비를 하거나 리더기의 동작을 마친다.

Card state diagram 측에서는 리더기가 파워를 공급함으로써 카드 리셋이 실행되며 ATR을 보낸다. 그 후 리더기로부터 APDU가 전달되면, 디스패치해서 APDU를 처리한 후 리더기에 응답을 보내게 된다. 스마트 카드 형태의 전자화폐도 스마트 카드의 규격을 준수하는 한 기본적으로 이러한 메커니즘으로 동작하게 된다.[10]

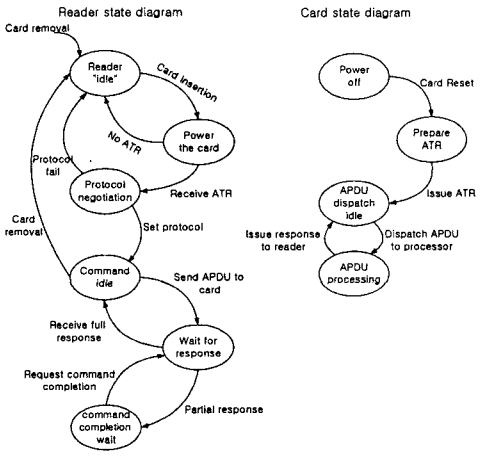

그림 2. 스마트 카드 통신 프로토콜

V. IC 카드형 전자화폐

IC 카드형 전자화폐는 플라스틱 카드에 은행 예금의 일부를 전자적인 방법으로 이전, 저장하였다가 단말기 등을 이용하여 현금처럼 사용하는 방식의 전자화폐로서 카드의 형태에 따라 접촉식, 비접촉식으로 분류될 수 있고, 카드의 종류에 따라 자기카드와 IC 카드로 분류된다. 접촉식카드는 IC 카드를 단말기에 삽입, 조작하면 저장된 전자화폐가 단말기로 이전되는 방식을 취하며, 원격지에서의 상품, 서비스 대금 지급 및 타인에 대한 자금이체가 가능하다. 반면, 비접촉식 카드는 IC 카드를 단말기와 접촉시키지 않고도 일정거리 이내에서 카드와 단말통신이 이루어지게 된다. IC 카드형 전자화폐 시스템은 IC 카드, read-writer 혹은 응용단말기, 발행 은행 호스트 컴퓨터, 매입 은행 호스트 컴퓨터, 통신망 중계 센터, 통신 시스템 및 통신회선 등의 구성요소로 이루어진다.

VI. 최적 전자화폐 모델 제안

전자 화폐 시스템은 보안서비스, 단순성 및 편리성, 프라이버시와 익명성, 시스템의 신뢰성 및 사용자수용성, 상호운영성 및 확장성, 소비자 보호, 국제적 접근능력, 이중사용 방지능력, 가분성, 내구성, 오프라인 능력, 개

인간 양도성, 휴대성, 저렴한 운영비용, 소액거래 지원도를 지원해야 한다. 이러한 것을 충족시키면서 다음과 같은 최종 구성을 갖추게 된다.

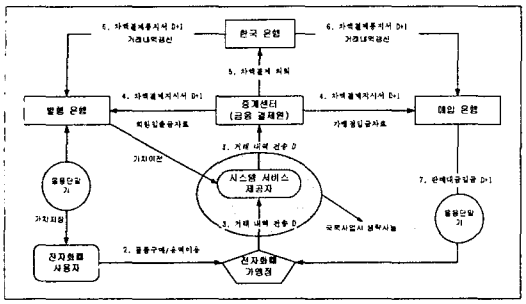

그림3. 한국적 전자화폐 모델제안

위 구조상에서의 가치흐름은 다음과 같은 기본적인 프로토콜을 만족하여야 한다. [2][7]

■인출 프로토콜 (withdrawal protocol) : 사용자와 은행 사이에서 수행되는 프로토콜로서 은행이 사용자에게 전자화폐를 발급해 주는 절차를 명세한 것으로서 전자화폐 시스템 설계 시 가장 중요한 부분이 된다.

■지불 프로토콜 (payment protocol) : 사용자와 상점 사이에서 수행되는 프로토콜로서 사용자가 구매대금으로 자신의 전자화폐를 상점에 지불하는 과정을 명세한 프로토콜이다.

■예치 프로토콜 (deposit protocol) : 상점과 은행 사이에서 수행되는 프로토콜로서 상점이 사용자로부터 받은 전자화폐를 은행이 결제해 주는 프로토콜이다.

한국에 맞는 전자화폐의 모델을 제안하기에 앞서 어떤 요소가 최소한 필요한지 점검할 필요가 있다. 우선 화폐를 발행하는 것이므로 한국은행이 관여해야 하고 대금을 결제하기 위해서 금융결제원을 중계센터로 두어야 하며 그 양측으로 발행은행과 전자가치가 입금되는 매입은행이 자리하게 된다. 매입은행과 전자화폐를 발행하는 발행은행은 중계결제기관으로부터 결제지시를 받고 중계센터는 한국은행은 매입은행 및 발행은행으로 결제통지를 하게 된다. 사용자간 가치이진 및 충전을 가능케 하기 위해서는 다른 방식의 구조가 필요하다. 또한 국가가 주도하여 전자화폐사업을 추진할 경우 시스템 서비스 사용자가 하는 기능, 즉 전자화폐의 인증부분을 처리하는 역할을 금융결제원 혹은 그 산하기관이 책임지도록 하여 결제 단계를 축소시킴과 동시에 금융결제원으로 부하가 집중되는 것을 막을 수 있을 것이다.

VII. 결론

본 고에서는 정보통신수단의 발전에 힘입어 미래의 가치교환수단이 실물화폐중심에서 전자화폐중심으로 이전한다는 가정에서 한국형 금융구조에 적합한 전자화폐 모델을 제시하였다. 외국의 여러 나라에서도 전자화폐사업을 추진하고 있으나 이를 변경 또는 실사없이 그대로 우리나라에 적용한다는 것은 무리일 것이다. 이에 전자화폐에 필요되는 미디어 및 금융구조에 맞는 가치흐름, 그리고 가치의 교환에 사용되는 각종 프로토콜을 정의하고 구현되어야 하는 각각의 기능을 명시하였다. 이러한 전자화폐 시스템의 조기구축으로 인하여 내적으로는 부정한 자금을 억제할 수 있고 자금의 흐름이 원활하게 되어 경제에 미치는 파급효과가 클것으로 예상된다. 여기에 국제성까지 가미하게 된다면 불필요한 환전 및 신용카드 수수료 필요없이 자유로운 해외활동을 보장받을 수 있을 것이다

참고문헌(또는 Reference)

[1] 탁승호 "전자화폐시대가 열린다." 대한상공회의소 2000년

[2] 탁승호 "전자화폐와 결제시스템" 더뱅커社 1996년

[3] "각국의 전자화폐 개발현황" 한국은행 금융결제부 1998년

[4] 이은령 외 "전자상거래 시스템 구축과 운영" 이한출판사 2001년

[5] 한국전자통신연구원 "암호학의 기초" 1999년

[6] 박창섭 "암호이론과 보안" 대영사 1999년

[7] 제일금융연구원 "새로운 돈의 혁명 전자화폐" 한국경제신문사 1997년

[8] 일본앤더슨컨설팅금융빅뱅전략본 "IT혁명과 금융기관의 생존전략" 미래와 사람들 2001년

[9] William stalling(윤덕우 역) "컴퓨터통신 보안 " 그린출판사 2001년

[10] 이만영 외 "전자상거래와 보안기술" 생능출판사 1999년

[11] Good Barbara Ann "The Changing Face of Money" Garland Pub 2000년