「經營情報硏究」 第19號
大韓經營情報學會
2006年 12月

전자상거래 기반에서 전자화폐의 효율성 향상을 위한 전자결제 연구 방안

안병태* · 이종하** · 정범석***

<목 차>

Ⅰ. 서 론

최근 정보통신 산업의 급속한 발달로 인하여 통신수단이 고도화되고 사회의 많은 부분에서 혁명적인 변화가 발생하고 있다. 특히, 인터넷 접속이 폭발적으로 증가함으로써 인터넷과 관련된 산업이 호황을 누리고 있으며 국내에서도 인터넷 쇼핑몰 등을 통한 전자상거래의 규모는 점차 증가하는 추세에 있다. 원격지에 있는 당사자 간의 비대면 거래인 전자상거래[1]에서는 필연적으로 그에 대한 지급방식도 그에 맞도록 변화될 것이 요구되며 물건의 수령 시에 대금을 지급하는 전통적인 지급방식 이외에도 네트워크 상에서 전자결제[2]를 통하여 거래의 대가를 지급하는 방식 등이 채택되고 있다.

전자결제를 통하여 거래의 대가를 지급하는 방식은 주로 은행지로를 통하는 방법이 많이 사용되어 왔으나 이는 은행의 개입이 없이 당사자 간에 네트워크 상에서 상거래 및 그에 대한 대금결제를 완결하기에는 부족함이 있음에 따라

*유한대학 경영정보학과 교수
**유한대학 경영정보학과 교수
***유한대학 경영정보학과 교수

보안성의 문제에도 불구하구 신용카드 정보를 전자적으로 전송함으로써 신용카드에 의한 결제를 하는 방식이 최근 많이 사용되고 있다. 그러나 현재 인터넷 쇼핑몰을 통한 상거래에서 신용카드로 결제를 하는 경우 신용카드를 소지하지 않은 자는 그러한 방식으로 결제를 할 수 없으며 아직까지는 대부분 소액의 구매에 그치고 있으므로 소액구매의 경우에 신용카드에 의한 결제는 인터넷 쇼핑몰이나 신용카드 회사의 업무 처리 비용의 면에서 부적절하다는 단점이 있다. 뿐만 아니라, 인터넷을 비롯한 네트워크가 해킹에 대비하여 100% 안전하다고 할 수 없으며 최근 보안사고가 증가하고 있다는 점에서 신용카드 정보의 유출의 가능성이 높고 사고의 발생 시에 대규모의 피해 발생이 예견되는 등의 문제점이 있다.

이러한 단점들을 극복하기 위한 전자결제 방식의 하나로서 전자화폐[3]가 사용되고 있다. 본 연구의 구성은 다음과 같다. 2장에서는 전자화폐의 관련연구를 살펴보고 3장에서는 우리나라 전자화폐의 현황에 대하여 살펴본다. 4장에서는 전자화폐 시스템의 기반기술을 알아보며 5장에서는 전자화폐의 도입과 문제점을 알아본다. 6장에서는 전자 화폐의 효율성 향상을 위한 전자결제 시스템의 개선 방안을 제안하며 끝으로 7장에서는 결론 및 향후과제를 알아본다.

Ⅱ. 전자화폐의 관련 연구

1. 전자화폐의 정의

통상적으로 전자화폐라 함은 전자매체를 통한 지급결제의 과정에서 화폐의 기능을 가지는 모든 수단을 말한다. 여기서 전자매체를 통한다고 하는 것은 두 가지 의미를 지니는데, 하나는 눈에 보이는 카드를 만들고 이를 사용하여 자금을 전자적으로 주고받는다는 의미이며 다른 하나는 전자적인 결제시스템으로 전자화폐를 설정하는 인터넷이나 퍼스널 컴퓨터 통신 등의 가상공간(cyber space)에서 사용할 수 있게 한다는 의미이다.

전자화폐는 은행 기타 전자화폐 발행자가 카드 또는 컴퓨터 시스템을 통하여 일정 화폐가치를 전자기호(proton)로 저장하고 그 지급을 보장하는 것으로 정보통신 회선을 통하여 자금결제가 이루어지는 화폐이다. 다른 한편으로는 전자화폐를 IC칩(Integrated circuit chip)이 내장된 플라스틱 카드(전자지갑)에 은행예

금의 일정액이 전자적 기호로 저장되어 있어 이를 일반적 물품 서비스 구매에 사용할 경우 동등의 저장금액(전자적 기호)이 판매자의 단말기 또는 전자지갑으로 이전되는 새로운 형태의 지급결제 수단을 의미한다. 전자화폐는 본질적으로 디지털 정보로 이루어진 화폐로써 기존의 화폐와 동일한 기능을 가져야 한다.

전자화폐는 기존의 화폐가 갖는 3대 기능인 가치척도 기능, 교환 지불 기능 및 가치저장 기능 이외에도 기존 화폐와 동일한 기능을 갖기 위해서는 다양한 조건들이 전제되어야 한다. 특히, 기술적으로 익명성(anonymity), 양도성(transferability), 오프라인 사용가능성(off-line capability), 분할성(divisibility), 이중사용(double spending) 방지, 휴대가능성(portability), 개발성이 보장되어야 한다. 하지만 현재까지 상용화된 전자적 지급수단 중에는 아직까지 기술적 또는 제도적인 제약으로 인하여 이러한 특성들을 모두 가지며 상용화된 전자화폐는 없다.

전자화폐는 현재도 다양한 형태로 발행되고 있으며 새로운 형태들이 계속하여 개발 중에 있다. 하지만 일률적으로 이를 모두 포괄하는 보편적인 넓은 의미의 전자화폐는 컴퓨터 시스템을 통하여 일정 화폐가치가 전자기적 기호로 저장되고 그러한 화폐가치의 이전으로 자금결제가 이루어지는 지급 수단이다. 좁은 의미의 전자화폐는 컴퓨터 시스템을 통하여 일정 화폐 가치가 전자기적 기호로 저장되고 그러한 화폐 가치가 온라인 또는 오프라인으로 전자화폐 발행자의 관여여부와 관계없이 익명성을 유지하면서 즉시 타인에게 이전될 수 있는 지급수단이다.

2. 전자화폐의 분류

전자적 수단을 이용한 지급 수단의 분류[4]는 여러 가지의 기준에 의하여 나누어 볼 수 있으나 일반적으로 가장 넓은 의미의 전자화폐는 (i) 카드 등 물리적인 저장매체를 이용하는 전자화폐와 인터넷 등 네트워크를 이용한 전자화폐, (ii) 은행계좌를 통하는 전자화폐와 은행계좌를 통하지 않는 전자화폐, (iii) 온라인형 전자화폐와 오프라인형 전자화폐, (iv) 개방형 전자화폐와 폐쇄형 전자화폐, (v) 범용 전자화폐와 단일목적용 전자화폐로 구분된다.

2.1 카드형 전자화폐와 네트워크형 전자화폐

전자화폐는 물리적인 가치 저장 수단이 요구 되는지의 여부에 따라 카드형

전자화폐와 네트워크형 전자화폐로 분류할 수 있다. 카드형 전자화폐는 카드나 전자기적인 방식으로 정보를 기록할 수 있는 매체에 화폐가치를 전자기적인 방법으로 이전 저장하였다가 단말기 등을 이용하여 저장된 화폐가치를 이전하여 지급에 사용하는 전자화폐이다. 네트워크형 전자화폐는 공중 정보통신망 특히 인터넷상에서 가상은행 또는 거래은행과 접속되는 컴퓨터에 가치를 저장하였다가 필요시 네트워크상에서 자금 결제를 하는 방식의 전자화폐를 말한다.

2.2 계좌형 전자화폐와 비계좌형 전자화폐

전자화폐는 거래기록의 관리 및 추적 여부에 따라서 계좌형 전자화폐와 비계좌형 전자화폐로 나누어 볼 수 있다. 계좌형 전자화폐는 전자화폐의 거래기록이 은행 등의 주전산기에 의하여 유지 관리되거나 기록의 추적이 가능한 전자화폐이고, 비계좌형 전자화폐는 가치 기록이 카드 자체 또는 기록매체 자체에만 기록되고 단말기에는 기록이 나타나지만 은행 등의 주선산기에는 거래량만이 전송되는 전자화폐를 말한다.

2.3 온라인형 전자화폐와 오프라인형 전자화폐

전자화폐는 사용 시에 전자화폐를 관리 운용하는 주전산기와 온라인으로 연결되어야 하는지 여부에 따라 온라인형 전자화폐와 오프라인형 전자화폐로 나눈다. 주전산기와 온라인으로 연결되어 있어야 한다는 것은 가치의 이전 시에 은행 등 제 3자의 개입이 필요하다는 것이다. 온라인형[5] 전자화폐는 전자화폐를 관리 운용하는 주전산기와 온라인 네트워크로 연결되어 주전산기에 의하여 사용자의 신분 및 비밀번호의 확인, 가치이전, 거래내역 입력 등이 행하여지는 전자화폐이다. 오프라인형 전자화폐는 주전산기와 연결되지 않고도 자체적으로 신문 및 비밀번호 확인, 가치이전, 거래내역 입력 등이 행하여지는 전자화폐로써 오프라인형 전자화폐는 주전산기와 연결되지 않고도 자체적으로 신문 및 비밀번호 확인, 가치이전, 거래내역 입력 등이 가능한 전자화폐이다[6]. 온라인형 전자화폐는 전자자금이체와 유사하게 은행 등 제 3자의 개입을 통하여 거래 당사자 간의 가치가 이전되며 오프라인형 전자화폐는 거래 당사가 간의 가치이전에 그러한 제 3자의 개입이 반드시 필요한 것은 아니므로 전산망의 장애 혹은 전산망의 가동시간 외에도 사용할 수 있다는 점에서 실적적인 차이가 있다.

2.4 개방형 전자화폐와 폐쇄형 전자화폐

전자화폐의 소지자간 가치의 이전성(transferability)을 기준으로 전자화폐는 개방형 전자화폐와 폐쇄형 전자화폐로 구분할 수 있다. 개방형 전자화폐는 전자화폐 소지자간에 화폐가치를 자유롭게 이전할 수 있는 전자화폐를 말한다. 반면, 폐쇄형 전자화폐는 화폐가치가 발행자에서 소비자로, 소비자에서 가맹점으로, 가맹점에서 전자화폐 발행자로의 일방적인 이전만이 가능함으로써 소지자간의 가치이전은 허용되지 않는 전자화폐를 말한다.

2.5 범용 전자화폐와 단일 목적용 전자화폐

전자화폐의 용도가 한정적인지의 여부에 의하여 범용 전자화폐와 단일 목적용 전자화폐로 구분된다. 범용 전자화폐는 전자화폐의 사용 용도가 특정 목적에 한정되지 않는 전자화폐를 말하며 단일목적용 전자화폐는 특정의 목적만을 위하여 사용될 수 있는 전자화폐를 말한다. 전통화폐의 대용 지급수단이라는 측면에서 단일목적용 전자화폐는 그 기능이 충분하지 않음으로 인해 현재는 대개 범용 전자화폐의 형태로 개발, 시험 운용되고 있다.

Ⅲ. 우리나라의 전자화폐 현황

1. 일반적 현황

우리나라에서는 은행을 중심으로 주로 IC카드방식[7]으로 전자화폐가 개발되고 있으나 아직 표준화는 이루어지고 있지 않다. 광주은행, 서울은행 및 주택은행 등에서 기장의 선점을 위하여 독자적으로 추진하고 있는 것으로 알려지고 있으나 표준화의 지체로 인하여 범용성에 있어서는 한계가 있고 널리 보급되고 있지 못한 실정이다.

2. 한국형 전자화폐(Korea- Cash, K- Cash)

한국은행은 금융정보화 추진은행 소위원회를 통하여 한국형 전자화폐인 K-Cash의 시범사업 실시지역과 시기를 확정하여 사용하고 있다. K- Cash는 고객의 예금에서 일정액을 인출하여 전자화폐 발행 계정에 입금한 후 동액을 IC카

드에 전자기호로 저장(이용자로부터 선지급을 받고 가치를 저장하는 형태)하는 형태로써 접촉식과 비접촉식의 겸용으로 발행된다.

3. 기타 국내의 전자화폐

최근에는 국내에서도 IC카드방식 이외에 네트워크형 전자화폐가 활발히 개발되고 있으며 주로 국내의 인터넷의 급속한 보급으로 인하여 전자상거래를 위한 인터넷상의 쇼핑몰들이 생겨나고 인터넷을 통한 대금지급의 필요성이 급증한 것에 기인한다고 할 수 있다. 그러한 대금지급의 필요성의 급증에 비하여 전통적인 전자결제 수단은 그러한 수요를 충족시키기에는 다음과 같은 문제점이 있다. 즉, 기존의 은행계좌를 통한 지로 등 전자자금 이체 방식을 이용하여 대금지급을 하는 경우에는 은행을 통하여 하는 불편함이 있으며 신용카드를 이용하여 대금지급을 하는 경우에는 신용카드 번호를 인터넷상으로 전송하여야 한다.

하지만 아직까지 비교적 소액의 물품의 구매가 활발한 인터넷상의 전자상거래에서는 사용자가 인터넷상의 보안사고의 위험성을 감수하여야 하는 문제점이 있다. 그러한 네트워크형 전자화폐는 주로 선불카드와 같이 일정한 금전적 가치를 미리 현금 또는 신용카드를 통하여 전자화폐의 발행자에게 지급하고 그로부터 일정한 가상 선불카드의 등록번호와 그에 대한 비밀번호를 발급 받은 후 이를 이용하여 대가를 전자상거래의 대가를 지급하는 방식이 많이 사용되고 있다.

이러한 방식은 신용카드를 사용하는 경우에도 신용도가 비교적 높은 전자화폐 발행자에게만 신용카드번호를 제공하여 전자화폐를 발행 받으며 이를 이용하여 네트워크상에서 사용을 하는 경우 신용카드번호의 유출이라는 보안상의 문제가 비교적 적을 것으로 예상된다. 뿐만 아니라 보안사고의 경우에도 대부분 발행금액에 대하여 최고한도의 재한을 두고 있으며 신용카드를 가지고 있지 아니한 경우에도 이용할 수 있고 소액의 결제도 가능할 것이라는 점에서 기존의 전자결제 수단에 대한 하나의 대안으로 이용될 수 있다[8].

Ⅳ. 전자화폐 시스템의 기반기술

본 4장에서는 현재 사용되고 있는 전자화폐의 기반 기술들을 알아본다. 전자화폐 시스템을 구성하는 프로토콜로는 은닉서명 프로토콜 기술, cut-and-

choose 기술, challenge-and-response 기술이 있다.

1. 은닉서명 프로토콜

전자화폐는 은행이 가치를 보증해 주는 일종의 가치 있는 디지털 정보이다. 이러한 전자화폐의 가치를 증명해 주기 위해서 은행이 이용할 수 있는 방법은 디지털 서명을 사용하는 것이다. 그러나 일반적인 디지털 서명을 사용하게 되면 사용자 프라이버시가 보장되지 않는다는 문제점이 발생하게 된다. 즉, 은행은 사용자가 서명 받기 원하는 메시지와 그에 대한 서명문을 알게 되기 때문에 전자화폐 발급 후 은행은 그것들을 서로 연결시킬 수 있게 되는 것이다.

그러므로, 전자화폐를 발급하기 위해서는 일반적인 디지털 서명이 아닌 새로운 종류의 특수한 디지털 서명이 필요하게 되며 이것은 전자화폐 시스템을 구성하는 프로토콜 중 인출 프로토콜을 설계하는데 기반이 된다. 은닉서명 프로토콜은 서명자(signer)가 제공자(provider)의 메시지를 볼 수 없는 상태에서 그것에 대한 서명을 해주며 제공자에게는 자신이 원하는 메시지에 서명을 받을 수 있게 해주는 역할을 수행한다. 구체적인 은닉서명 프로토콜의 내용은 아래와 같으며 여기서 사용되는 함수 및 프로토콜 절차는 아래와 같다.

1.1 함수(function)

- s'는 서명자만이 알고 있는 서명함수이며, 그것에 대한 역함수인 s는 s(s'(x))=x와 같이 검증함수로 사용되는 공개되어 있는 정보이다. 그러나 s는 s'에 대한 어떠한 정보도 제공하지 않는다.
- 가환함수 c와 그것의 역인 c'는 제공자에만 알려져 있는 함수이며 c'(s'(c(x)))=s'(x)와 같은 역할을 수행하며 여기서 c(x)와 s'는 x에 대한 어떠한 정보도 제공하지 않는다.
- r은 유효한 서명들을 찾는 것이 불가능하게 하도록 출분한 리던던시(redundancy)를 확인해 주는 리던던시 확인 함수(predicate)이다.

1.2 프로토콜(protocol)

- 단계 1) 제공자는 랜덤하게 r(x)인 x를 선택한 후 c(x)를 생성하고 나서 이것을 서명자에게 전송한다.
- 단계 2) 서명자는 s'를 이용하여 c(X)에 서명을 행한 후 그 결과 s'(c(x)를

제공자에게 전송한다.

- 단계 3) 제공자는 c'함수를 이용하여 c'(s'(c(x)))=s'(x)와 같이 s' (c(x))에서 s'(x)만을 추출한다.

-단계 4) 제3자는 서명자의 검증함수 s를 이용하여 r(s(s'(x)))을 확인함으로서 s'(x)가 서명자에 의해 서명된 것임을 확인할 수 있다.

상기에서 살펴본 은닉서명 프로토콜은 다음 세 가지의 안전성 성질들을 갖는다.

① 디지털 서명 : 누구나가 추출된 서명 s'(x)는 서명자의 비밀키 s'를 사용한 것이라는 사실을 확인할 수 있다.

② 은닉 서명 : 서명자는 s'(xi)와 같은 추출된 서명들의 집합과 s'(c(xi))와 같이 추출되기 전의 서명들의 집합 사이에서 서로 대응되는 쌍들을 찾을 수 없다.

③ 서명들의 보호 : 제공자는 서명자에 의해 서명된 각각의 것들에 대해 기껏해야 하나의 서명만을 추출할 수 있다. 즉, 제공자가 s'(c(x1)),... ,s'(c(xi))와 같이 추출된 서명들의 집합과 이에 대한 c, c', x를 가지고 있다 하더라도 r(y)를 만족하며 y=xi가 아닌 새로운 수 y에 대한 서명 s'(y)를 구하는 것은 불가능하다.

상기에서 발표된 은닉서명 프로토콜의 개념은 전자화폐 시스템의 인출 프로토콜에서 사용자의 프라이버시를 보장해주는 프리미티브(primitive)로 작용하는 중요한 역할을 담당하게 되었다.

2. cut-and-choose 기술과 challenge-and-response 기술

은닉서명 프로토콜이 제안한 이후 사용자의 프라이버시를 만족하는 최초의 오프라인 전자화폐 시스템이 1988년 CRYPTO에 발표되었다. 불추적성을 만족하는 오프라인 전자화폐 시스템을 설계하는 경우 가장 어려운 것은 이중사용을 검출할 수 있는 정보를 전자화폐에 넣는 방법이다[9]. 만약 이러한 은행 측에서 넣도록 한다면 은행이 부정행위를 하는 경우 그 정보를 이용하여 사용자의 프라이버시를 침해할 수 있으며 반대로 그 정보를 사용자 측에서 넣도록 한다면 은행 측에서는 은닉서명의 특성상 사용자의 메시지를 볼 수 없기 때문에 사용

자의 부정행위를 막을 수 없게 된다.

이러한 문제를 cut-and-choose 기술로 해결하였다. cut-and-choose 기술은 전송된 정보의 정확성을 확인하기 위해 같은 방법을 사용한 여러 정보들 중 일부의 내용 구성을 확인한 후, 그것의 확률로서 나머지 정보에 대한 정확성을 규정하고 그 정보들을 처리 대상으로 사용하는 것이다. 즉, 상기의 인출 프로토콜에서는 사용자가 랜덤 정보와 자신의 식별자를 넣은 전자화폐를 K개 생성한 후 그것들을 은행에 전송하게 되며 은행 측에서는 그것들 중 K/2개를 선택하여 사용자의 도움을 받아 선택된 정보들의 정확성을 검증한다. 그런 후에 선택되지 않은 K/2개의 정보들은 하나의 전자화폐로써 사용된다. 이 때, 생성된 전자화폐의 정확성은 $1-(1/2^{(K/2)})$이 된다.

그러나 상기와 같은 cut-and-choose 기술을 사용하는 전자화폐 시스템은 많은 오버헤드를 가지게 된다. 즉, 그러한 전자화폐 시스템은 인출 프로토콜이나 지불 프로토콜을 수행하는 경우 많은 통신량을 요하게 되며 더욱이 각각의 전자화폐가 차지하는 메모리 용량은 상당히 크다는 문제점을 가지게 된다. 결국, 이러한 문제점들은 전자화폐 시스템을 실제로 구현하는 경우 아주 큰 장애요소로 적용하게 되었다.

따라서 본 논문에서는 challenge-and-response[11] 기술을 사용한 전자화폐 시스템을 제안한다. challenge-and-response 기술은 cut-and-choose 기술의 문제점을 완전히 해결한 기반 기술로써 두 시스템 모두 비밀 공유 직선(secret sharing line)의 개념을 이용하였다. 그러나 Challenge-and-response 기술은 일반적으로 개인 식별에서 많이 사용되는 형태로써 사용자측은 먼저 승인을 보내고 이후 은행 측은 신청을 전송하며 마지막으로 사용자측이 기존에 보냈던 승인과 신청에 일관성을 갖는 response를 보내는 방식이다. challenge-and-response 기술을 cut-and-choose[10] 기술과 배교해 보면 많은 차이가 있음을 쉽게 알 수 있다. 우선, 검증할 메시지를 M이라고 가정하였을 경우 전송되는 통싱량을 비교해보면, challenge-and-response 기술은 [승인의 크기+신청의 크기+응답의 크기] 만큼의 통신량이 필요한 반면, cut-and-choose 기술은 $(1-1/(2^{K/2}))$의 정확성을 갖기 위해서 기본적으로 [(K*M)+((K/2)*M)+((K/2)*M)] 만큼의 통신량을 필요로 한다. 또한, cut-and-choose 방법에서의 안전성 파라메터는 K이기 때문에 보다 높은 안전성을 보장하기 위해서는 K에 비례하여 통신량이 증가하게 되는 반면, challenge-and-response 기술에서는 일반적으로 신청이 안전성 파라메터 역할을 수행하기 때문에 전체적인 통신량의 증가 없이 단

지 신청의 길이만 증가시킴으로써 안정성을 높일 수 있다. 따라서 본 논문에서는 전자화폐 시스템 설계 시 challenge-and-response 기술을 사용하는 것을 제안하며 이는 향후 전자화폐 시스템의 효율성을 개선시키는 기폭제가 될 것이다.

V. 전자화폐의 도입과 문제점

본 논문의 5장에서는 전자화폐의 도입과 보급이 성공적으로 활성화되기 위하여 선결적으로 해결되어야 할 문제점을 제시함으로써 향후 전자결제의 신뢰성과 안전성을 확고히 한다.

1. 위조 변조 가능성

전자화폐는 카드 혹은 컴퓨터시스템을 통하여 전자기적 기호로 저장된 일정한 화폐가치를 그 본질적인 요소로 한다. 그러한 화폐가치를 저장하고 이전함에 있어서 권한 없는 자가 저장되어 있는 화폐가치를 변조하거나 은행 기타 전자화폐 발행자 이외의 자가 전자화폐 발행사의 명의를 도용하여 전자화폐를 위조하는 경우에는 전자화폐로 지급 받은 거래상대방이 막대한 경제적인 손실을 입을 우려가 있다. 따라서 기술적으로 이러한 위조 또는 변조에 대한 방지장치가 우선적으로 개발되어야 할 것이며 제도적으로는 그러한 위조 또는 변조로 인한 경우에도 전자화폐의 궁극적인 지급 신뢰성을 상실하지 않으면서 전자화폐 발행자에게 예측 가능한 한도에서 손실을 최소화 할 수 있도록 보험 등의 제도적인 보완대책도 강구되어야 한다.

2. 개인 정보보호의 문제

넓은 의미의 전자화폐의 경우에는 현금거래와는 달리 지급의 내역이 기록되어 남아있는 경우가 있을 수 있다. 그러한 지급의 기록은 카드형 전자화폐의 경우에는 카드에, 기타 네트워크형 전자화폐의 경우에는 컴퓨터 시스템에 남아 있게 됨으로 그러한 개인적인 기록이 타인에게 유출되는 경우에는 개인의 사생활의 비밀이 침해될 우려가 있다. 그러한 개인정보의 보호가 기술적 법제도적으로 충분하지 않을 경우 전자화폐는 그 편의성 및 효율성에도 불구하고 사용자의

사용기피로 인하여 널리 보급되지 않을 기능성이 있다.

3. 범죄에 관련된 문제

좁은 의미의 전자화폐의 경우에는 전통적인 화폐와 마찬가지로 화폐가치의 이전에 익명성이 보장되며 반드시 전자화폐 발행자의 관여가 필요한 것도 아니므로 범죄행위에 악용될 가능성을 배제할 수 없다. 세금의 회피 및 기타 불법적인 자금의 이전 시에 현금의 경우에는 막대한 양의 돈을 물리적으로 보관 및 운반함에 현실적인 어려움이 있으나 전자화폐의 경우에는 이러한 제약으로부터 자유로우므로 돈세탁 등의 범죄행위에 악용될 우려가 있다. 이에 대해 추후 심도 있는 논의가 필요할 것이며 익명성이 보장되는 전자화폐의 경우에는 저장금액의 상한을 규정하고 비정상적인 대규모의 자금의 이전 시에는 거래에 대한 기록을 남기는 등의 대비책을 고려해야 한다.

4. 전자화폐와 중앙은행과의 관계

지급결제 제도의 안정성과 효율성의 확보는 중앙은행의 기본적 임무이므로 대부분의 중앙은행들이 결제시스템의 구축 및 운영에 상당한 관심을 가지고 있으나 그 개입의 정도는 각 국가마다 역사적 문화적 배경의 차이에 따라 달라질 수 있다. 전자화폐를 통한 새로운 결제방식에 대하여도 중앙은행이 전자화폐의 신뢰성과 무결성의 확보 차원에서 대응 방안을 강구할 필요성이 있으나 그 개입의 정도에 대하여는 계속적인 논의가 필요하다. 기타 중앙은행의 시너리지(seigniorage)의 문제 및 전자화폐와 통화정책과의 관계에 대한 문제 등이 있다.

Ⅵ. 전자결제 시스템의 개선 방안

전자결제 시스템의 가장 큰 문제점은 보안성이다. 따라서 본 논문에서는 전자결제 시스템의 보안 방안을 위해 급속히 늘어나는 전자상거래의 안전을 위한 보안 프로그램을 개발한다. 또한, 일반적인 하드웨어와 소프트웨어에 전부 사용될 수 있는 통일성이 요구되는 방안을 개발한다.

1. 결제정보의 확신성

정보의 확신성이란 카드 사용자가 결제할 때 등록해야 하는 정보들로써 정보를 암호화함으로써 해결할 수 있다. 주어진 정보를 암호화하고 해독하는 암호 해독법은 비밀열쇠키법과 공개열쇠키법으로 분류된다. 비밀열쇠키법은 똑같은 패스워드로 암호화하고 해독하는 것을 말한다. 대표적인 흔글 같은 편집기가 이에 해당한다. 공개열쇠키법은 한 사람의 공개키와 비밀키를 합쳐져야만 해독이 가능한 방식이다. 이는 비밀키보다 안정적인 방식으로써 전자메일이 이에 해당한다.

2. 결제정보의 통일성

결제정보의 통일성이란 메시지의 내용이 보내는 사람으로부터 받는 사람한테 전달되는 과정에서 변경되지 않는 것을 보장해야 한다는 것이다. 이를 위해 전자 서명을 이용함으로써 결제정보의 통일성을 확보한다.

3. 카드 사용자의 인증 및 상점에 대한 인증

이 디지털 서명 방식은 누가 사인했는지 알 수 있도록 해주기 때문에 카드 사용자나 상점의 인증 과정에도 사용된다. 이는 카드 사용자나 상점, 두 쪽 모두 상대방이 인증된 사용자임을 확인해야만 안정된 거래를 할 수 있기 때문에 디지털 서명과 신임을 기반으로 해서 확인함으로써 인증 승인을 받는다.

4. 상호 이용성

상호 이용성은 하드웨어나 소프트웨어의 플랫폼에 상관없이 적용되어야 한다. 이것은 각각의 규약을 명확히 설정하고 메시지의 포맷을 정함으로써 얻어질 수 있다.

Ⅶ. 결론 및 향후과제

이상에서 살펴본 바와 같이 전자화폐의 개념과 다양한 전자화폐의 분류 및 현재 개발되어 운용되고 있는 전자화폐의 형태들에 대하여 간략하게 검토하여 보았다. 그리고 나아가 그러한 전자화폐를 발행, 운용함에 있어서 발행할 수 있는 문제점에 대하여 논의하여 보았다. 또한 전자결제 시스템의 개선 방안을 제시함으로써 보다 향상된 전자화폐의 안정성을 확보하였다.

전자화폐는 비교적 지속적으로 주목을 받는 영역으로써 인터넷의 폭발적인 보급과 더불어 인터넷을 이용한 다양한 상거래가 발행하면서 그 중요성이 계속적으로 인식되기에 이르렀다. 그러나 전자화폐와 같은 새로운 지급결제 수단의 개발 및 출현이 매우 빠른 속도로 진전되고 있으며 그러한 새로운 지급결제 수단이 갖는 국가경제 및 통화 정책에 미치는 영향력이 매우 클 것이다. 따라서 본 논문의 향후과제로는 전자화폐에 대한 보급의 선결조건으로써 결제의 확실성을 보장하기 위한 방안과 소비자 보호의 측면에서 전자화폐 사용자의 책임을 어느 정도로 제한할 것인지의 연구가 지속적으로 강구되어야 할 것이다.

참 고 문 헌

1. 김성희・김재경・장기진, 인터넷과 전자상거래, 무역경영사, 2000, pp.382～386.
2. 탁승호, 전자화폐와 결제시스템, 더뱅커사, 1996, pp.28～36.
3. 한국은행, 전자화폐의 영향과 대응방향 , 시사금융, Vol. 12-13, 시사금융사, 1996. 3, pp.64～72.
4. 강상우・강창구・김진규・김성옥, 전자화폐관련기술, 한남대학교논문집(자연) 28, 1998, pp.216～222.
5. Rich ard L. Field, “1996: Survey of th e Year's Development s in Electronic Cash Lawand The Laws affecting electronic Banking in the Unite States”, http://www.wcl.american.edu/journals/lawrev/Fieldtxt.htm, pp.5-15.

06. 김은기, 전자화폐의 법적문제, 상사법연구 제16권 제2호, 한국상사법학회, 1997, pp.94～102.
07. 한국은행 금융결제부 전자금융과, 전자화폐의 법률적 측면에 관한 BIS보고서, 1996,8., pp.13～22.
08. 한국은행, 전자화폐의 영향과 대응방안, 시사금융 Vol 12-13, 시사금융사, 1996, pp.8～18.
09. 이은영, 전자상거래와 소비자법, 전자상거래와 법정 대응(한국비교사법학회 창립4주년 기념학술대회 자료집), 1998. 10., pp.17～28.
10. http://dosan.skku.ac,kr/~sjkim/images/5_ksj.pdf, “암호 알고리즘과 암호 프로토콜”, 김승주・박성준・이임영・원동호
11. www.kupub.or.kr/faculty/yeomjf.html “전자화폐 시스템의 기반 기술”, 김은기
12. 손진화・박영태, 전자화폐의 법적 제문제에 관한 고찰, 국제상학 제13권 제1호, 한국국제상학회, 1998. 5., pp.70～80.

Abstract

A Plan of e-Settlement Study for Effective Improvement of e-Money Based on e-Commerce

Ahn, Byeong-tae · Lee, Chong-ha · Chung, Bhum-suk

The internet industry is gradually increasing according to the explosive explosion of internet and development of information communication industry. Specially, The payment method of settlement means is diversed with development of e-commerce. In this paper, we propose a settlement method using e-settlement in the network. and we suggest a security method for efficiency of e-money. Also, we propose a reform plan of e-settlement system.

Keyword : e-Commerce, e-Money, e-Settlement