(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년10월19일
(11) 등록번호 10-1073601
(24) 등록일자 2011년10월07일

(51) Int. Cl.
G06K 19/07 (2006.01) *G06Q 20/00* (2006.01)
(21) 출원번호 10-2010-0074082
(22) 출원일자 2010년07월30일
심사청구일자 2010년07월30일
(56) 선행기술조사문헌
JP2010055633 A

(73) 특허권자
한국과학기술원
대전 유성구 구성동 373-1
(72) 발명자
박규호
대전광역시 유성구 구성동 한국과학기술원 6-3208
박기웅
서울특별시 노원구 월계4동 500-11 8/5
(뒷면에 계속)
(74) 대리인
김학제, 문혜정

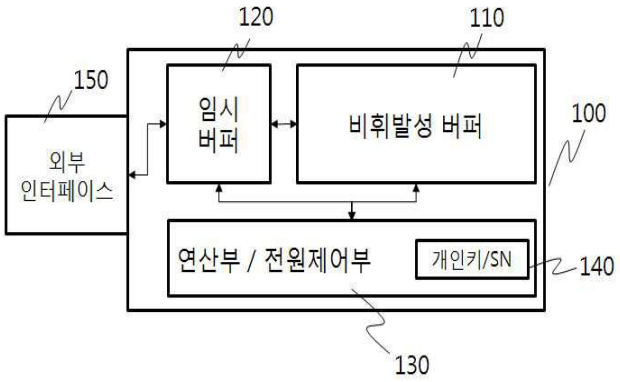
전체 청구항 수 : 총 7 항 심사관 : 김창주

(54) 전자 지불 매체 및 그를 이용한 오프라인 전자 지불시스템

(57) 요 약

본 발명은 1회 읽기만 가능한 메모리(One-Time Readable Memory)를 이용한 전자 지불 매체 및 그를 이용한 오프라인 전자 지불장치에 관한 것으로, 본 발명의 전자 지불 매체는 1회 읽기만 가능한 메모리이므로 정보의 유일성을 제공하여 화폐와 동일하게 사용될 수 있고, 온라인을 통한 인증절차 없이 전자 지불이 가능하여 신속한 처리 및 구매기관에서의 관리비용 및 시간을 절감할 수 있다.

대 표 도 - 도2



(72) 발명자

박영우

경기도 성남시 중원구 은행2동 708번지

정요원

경기도 안산시 상록구 본오2동 737-2 B01호

김철민

대전광역시 유성구 구성동 한국과학기술원 전자동 3243호

특허청구의 범위

청구항 1

1회 읽기만 가능한 메모리 소자(one-time readable memory device);

상기 메모리 소자 내의, 화폐 값을 나타내는 데이터를 포함하는 비활성 버퍼;

상기 메모리 소자 내의, 상기 비활성 버퍼로부터 읽어 들인 데이터를 임시로 저장하는 임시 버퍼;

상기 임시 버퍼에 대한 전원제어를 수행하고, 1회 읽기만 가능한 메모리 간의 상호인증을 위한 인증 연산을 수행하는 연산부/전원제어부;

상기 연산부/전원제어부 내에 저장되어 있는 1회 읽기만 가능한 메모리임을 입증하는 개인키 및 발권 일련번호(serial number); 및

외부장치와의 접속을 위한 외부 인터페이스부를 포함하는 전자 지불 매체(payment medium).

청구항 2

청구항 2은(는) 설정등록료 납부시 포기되었습니다.

제 1항에 있어서, 상기 임시 버퍼는 전원이 차단되면 데이터가 소거되는 휘발성 메모리 영역인 것을 특징으로 하는 전자 지불 매체.

청구항 3

청구항 3은(는) 설정등록료 납부시 포기되었습니다.

제 1항에 있어서, 상기 1회 읽기만 가능한 메모리임을 입증하는 개인키 및 발권 일련번호는 상기 1회 읽기만 가능한 메모리의 연산부 이외에는 읽힐 수 없도록 내부 정보 보호되어 있는 것을 특징으로 하는 전자 지불 매체.

청구항 4

제 1항에 있어서, 상기 화폐 데이터는 최소 화폐 단위를 나타내는 디지털 정보 블록의 일련의 스트링(string)으로 구성되고, 상기 스트링의 각각의 디지털 정보 블록은 발권날짜, 발권 일련번호, 및 상기 발권날짜 및 발권 일련번호의 디지털 서명을 포함하는 것을 특징으로 하는 전자 지불 매체.

청구항 5

청구항 5은(는) 설정등록료 납부시 포기되었습니다.

제 1항에 있어서, 상기 연산부/전원제어부의 인증 연산은 공개 키 암호화방식(RSA 방식)에 의해 수행되는 것을 특징으로 하는 전자 지불 매체.

청구항 6

제 1항에 있어서, 상기 전자 지불 매체는

화폐 값 및 송금 처리 상황을 디스플레이하는 표시부 ; 및

송금 모드 및 수금 모드 가운데 하나의 모드를 선택하기 위한 모드 버튼 및 확인버튼을 포함하는 키입력부를 더 포함하는 것을 특징으로 하는 전자 지불 매체.

청구항 7

하나 이상의 송금자의 전자 지불 매체; 및

하나 이상의 수금자의 전자 지불 매체를 포함하고,

상기 송금자의 전자 지불 매체 및 상기 수금자의 전자 지불 매체는 제 1항의 전자 지불 매체이고, 송금자의 전자 지불 매체의 외부 인터페이스부 및 수금자의 전자 지불 매체의 외부 인터페이스부가 서로 접속되면 오프라인 방식의 인증 연산을 거쳐 안전한 저장장치의 연결(secure mount)이 이루어지고, 전자 지불 매체의 1회 읽기만 가능한 특성으로 인해서 송금자에 의해 입력된 금액에 해당하는 디지털 정보가 송금자 전자 지불 매체에서 삭제되고, 수금자 전자 지불 매체로 이동되도록 구성되는 오프라인 전자 지불 시스템.

청구항 8

제 7항에 있어서, 상기 연산부/전원제어부의 인증 연산은 공개 키 암호화방식(RSA 방식)에 의해 수행되는 것을 특징으로 하는 오프라인 전자 지불 시스템.

청구항 9

제 8항에 있어서, 상기 전자 지불 매체 사이의 인증 연산은

송금자의 전자 지불 매체가 랜덤한 값 (Nonce-A)을 생성하여, 송금자 전자 지불 매체의 일련번호와 함께 수금자 전자 지불 매체로 정보를 전송하고;

수금자 전자 지불 매체는 송금자 전자 지불 매체로부터 수신한 랜덤값(Nonce-A값)과 일련번호 값에 자신의 1회 읽기만 가능한 메모리(One-Time Readable Memory)에 있는 개인키를 이용하여 디지털 서명을 생성하여 보내고, 수금자 전자 지불 매체도 랜덤값(Nonce-B)을 생성하여, 수금자 전자 지불 매체의 일련번호와 함께 수금자 전자 지불 매체로 정보를 전송하며;

송금자 전자 지불 매체 및 수금자 전자 지불 매체가 각각 상대방으로부터 수신한 정보를 전자 지불 매체의 발권자의 공개키를 이용하여 디지털 서명을 해독하였을 때, 자신이 보낸 정보와 일치하는 경우, 상대방 전자 지불 매체도 1회 기록 가능한 메모리라는 것을 확인하도록 되어 있는 것을 특징으로 하는 오프라인 전자 지불 시스템.

청구항 10

청구항 10은(는) 설정등록료 납부시 포기되었습니다.

제 7항에 있어서, 상기 연산부/전원제어부는 인증 연산의 원자성(atomicity)을 제공하도록 구성되는 것을 특징으로 하는 오프라인 전자 지불 시스템.

청구항 11

제 7항에 있어서, 상기 전자 지불 매체는

화폐 값 및 송금 처리 상황을 디스플레이하는 표시부 ; 및

송금 처리 수행을 위한 명령을 입력하기 위한 키입력부를 더 포함하고,

여기서 송금자의 전자 지불 매체와 수금자의 전자 지불 매체가 각자의 외부 인터페이스를 통해서 서로 연결되면, 수금자는 수금 모드를 누르고 대기하고, 송금자가 송금 모드를 누른 후 지불하고자 하는 금액을 입력하고 확인버튼을 누르면 전송 연산이 수행되어 해당 비용 만큼 지불이 이루어지도록 되어 있는 것을 특징으로

하는 오프라인 전자 지불 시스템.

명 세 서

기 술 분 야

[0001] 본 발명은 전자 지불 매체 및 그를 이용한 오프라인 전자 지불장치에 관한 것으로, 더욱 상세하게는 1회 읽기만 가능한 메모리(One-Time Readable Memory)를 이용하여, 온라인을 통한 인증 과정 없이 오프라인 전자 지불이 가능한 전자 지불 매체 및 그를 이용한 오프라인 전자 지불장치에 관한 것이다.

배 경 기 술

[0002] 인류 초기 상거래에서는 돌 또는 조개와 같은 화폐의 기능을 담당하는 교환 매체 및 주화가 사용되었으며, 경제 규모가 커지면서 화폐가 발명되어 사용되기 시작하였다. 지불 수단으로는 종이 화폐 또는 은행 수표와 같은 표시 화폐의 사용에 이어서 신용카드, 직불카드 등의 신용 지불 수단이 사용되었고, 최근에는 인터넷 사용의 증가와 정보통신기술의 발달로 전자 상거래가 활발하게 이용되면서 디지털 수표, 직불카드, 신용카드, 가치 저장 카드, 전자 현금(electronic cash) 등과 같은 다양한 형태의 전자 지불 수단들이 이용되고 있다.

[0003] 기존의 전자 지불 수단을 이용한 지불 방법을 살펴보면, 구매자가 네트워크를 통하여 지불 계좌가 개설된 금융기관(은행 또는 카드사)과 연결되어 소정의 인증과정을 거친 후 지불대금을 이체시켜 주는 방식으로 이루어지고 있다. 즉, 기존의 전자 지불 방식은 금융기관 서버에서 인증 처리를 하는 것을 기반으로 이루어지기 때문에, 지불 시 인증을 위해서 통신망을 통해서 지불 단말기와 서버가 접속되어 있어야 한다. 따라서 종래 방법으로는 단말기에서 서버로의 접속소요시간, 서버 처리 시간, 서버에서 단말기로의 전송시간 등으로 인해, 지불처리를 위해 많은 시간이 소요되고, 통신망에 접속하기 위한 인프라가 구축되어야 하므로 비용도 추가로 발생되는 문제가 있었다. 더욱이, 인터넷 상에서 전송되는 대금 처리 관련 데이터에 관한 보안상의 불완전함으로 인하여 전자 지불에 대한 불신을 증폭시켜 전자 지불의 활성화에 장애가 되고 있다.

[0004] 따라서 오프라인을 통한 인증 절차를 거치지 않고 현금처럼 편리하게 사용할 수 있는 전자 지불 매체의 개발이 요구되고 있다.

발명의 내용

해결하려는 과제

[0005] 본 발명은 상술한 본 발명이 속하는 기술 분야의 기술적 요구에 부응하기 위한 것으로, 본 발명의 하나의 목적은 온라인을 통하지 않고 전자적으로 지불이 가능한 전자 지불 매체를 제공하는 것이다.

[0006] 본 발명의 다른 목적은 온라인을 통하지 않고 전자적으로 지불이 가능한 전자 지불 시스템을 제공하는 것이다.

과제의 해결 수단

[0007] 상술한 목적을 달성하기 위한 본 발명의 하나의 양상은 1회 읽기만 가능한 메모리 소자(one-time readable memory device);

[0008] 상기 메모리 소자 내의, 화폐값을 나타내는 데이터를 포함하는 비활성 버퍼;

[0009] 상기 메모리 소자 내의, 상기 비활성 버퍼로부터 읽어 들인 데이터를 임시로 저장하는 임시 버퍼;

[0010] 상기 임시 버퍼에 대한 전원제어를 수행하고, 1회 읽기만 가능한 메모리 간의 상호인증을 위한 인증 연산을 수행하는 연산부/전원제어부;

[0011] 상기 연산부/전원제어부 내에 저장되어 있는 1회 읽기만 가능한 메모리임을 입증하는 개인키 및 발권 일련번호(serial number); 및

[0012] 외부장치와의 접속을 위한 외부 인터페이스부를 포함하는 전자 지불 매체(digital payment medium)에

관한 것이다.

[0013] 본 발명의 다른 구현예는 하나 이상의 송금자의 전자 지불 매체; 및

[0014] 하나 이상의 수금자의 전자 지불 매체를 포함하고,

[0015] 상기 송금자의 전자 지불 매체 및 상기 수금자의 전자 지불 매체는 상기의 1회 읽기만 가능한 전자 지불 매체이고, 송금자의 전자 지불 매체의 외부 인터페이스부 및 수금자의 전자 지불 매체의 외부 인터페이스부가 서로 접속되면 오프라인 방식의 인증 연산을 거쳐 안전한 저장장치의 연결(secure mount)이 이루어지고, 전자 지불 매체의 1회 읽기만 가능한 특성으로 인해서 송금자에 의해 입력된 금액에 해당하는 디지털 정보가 송금자 전자 지불 매체에서 삭제되고, 수금자 전자 지불 매체로 이동되도록 구성되는 오프라인 전자 지불 시스템에 관한 것이다.

발명의 효과

[0016] 본 발명의 다양한 구현예의 전자 지불 매체에서 1회 읽기만 가능한 메모리 (One-Time Readable Memory)에 저장되어 있는 화폐값에 대응되는 디지털 정보는 송금자의 전자 지불 매체로부터 독출되는 순간 하드웨어적으로 비가역적으로 삭제됨과 동시에 수금자의 전자 지불 매체로 복사가 아닌 이동되기 때문에, 저장된 정보는 유일성을 지니게 되어, 화폐로서의 역할을 수행할 수 있다. 따라서 본 발명의 전자화폐 및 전자 지불 시스템에 의하면 금융기관 및 네트워크를 이용하는 복잡한 인증 작업 없이 (Infra-less) 디지털 기반 거래를 편리하고 신뢰성 있는 방법으로 행할 수 있다. 더욱이, 본 발명의 전자 화폐는 일반 유가증권과 같이 사용될 수 있고, 더 나아가 DRM, 디지털 쿠폰, 일회용 음원 서비스 비용 지불 시에도 활용될 수 있다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 일실시예의 전자화폐를 구성하는 1회 읽기만 가능한 메모리의 동작 특성을 설명하기 위한 모식도이다.

도 2는 본 발명의 일실시예의 전자 지불 매체의 개략도이다.

도 3은 본 발명의 일실시예의 전자 지불 매체에 저장되는 화폐값을 나타내는 디지털 정보의 구조도이다.

도 4는 본 발명의 일실시예의 오프라인 전자 지불 장치에서의 전자 지불 매체들 사이의 연결을 설명하는 개략도이다.

도 5는 본 발명의 일실시예의 오프라인 전자 지불 장치를 이용한 전자 지불 과정을 설명하기 위한 모식도이다.

발명을 실시하기 위한 구체적인 내용

[0018] 이하에서 첨부 도면을 참조하여 본 발명에 대해서 더욱 상세하게 설명한다.

[0019] 본 발명에서 “1회 읽기만 가능한 메모리(One-Time Readable Memory)”란 여러 번 기록가능하고, 여러 번 읽을 수 있는 특성을 보장하는 일반적인 메모리와 다르게, 기록은 여러 번 가능하나, 읽기는 한 번만 가능한 메모리로 정의된다. 즉 도 1에 도시된 바와 같이, 기록(write) 연산을 통하여 기록을 하면 비휘발성 메모리와 같이 메모리가 보존되나, 해당 정보를 읽는 순간, 저장된 메모리는 안전하게 물리적으로도 복구가 되지 않도록 삭제가 되는 특성을 가지고 있는 메모리이다. 이와 같이 1회만 읽기가 가능한 메모리가 실현 가능한 이유는 읽기 연산 및 쓰기 연산에 있어서 원자성(Atomicity)을 칩 내부에서 보장해 주기 때문이다. 여기서 원자성(Atomicity)이란 하나의 연산이 쪼개어 질 수 없다는 의미를 갖는 것으로서, 중간에 끊이지 않고 한 번에 수행되는 연산의 특성을 의미한다. 즉 쓰기 연산을 위하여, 데이터를 입력하는 연산부터, 입력된 데이터가 소자에 기록이 되는 연산, 기록 완료 후 완료가 되는 연산까지, 중간에서 멈출 수 없는 하나의 연산으로 이루어지는 특징을 갖는다. 읽기 연산에 있어서도, 읽기를 위한 주소를 입력하는 연산부터, 입력된 주소 정보가 소자에 접근하여, 데이터를 가져오는 연산까지, 중간에서 멈출 수 없는 하나의 연산으로 수행되는 특징을 갖게 되어, 1회의 읽기만 가능한 메모리가 실현될 수 있는 것이다.

[0020] 본 발명에서 “오프라인 전자 지불 시스템(off-line digital payment system)”이란 신용카드, 기프티콘 처럼 거래 시에 온라인을 통한 인증이 필요하지 않고, 디지털 기반의 전자 지불 시스템 임에도 불구하고, 오

프라인으로 거래가 가능한 시스템으로 정의된다.

[0021] 도 2는 본 발명의 일실시예의 전자 지불 매체의 개략도이다. 도 2를 참조하면, 본 발명의 일실시예의 전자 지불 매체(100)는 기본적으로 1회 읽기만 가능한 메모리 소자(one-time readable memory device)로 구성되고, 상기 메모리 소자 내에 포함되는 화폐 값을 나타내는 데이터를 포함하는 비활성 버퍼(110); 상기 메모리 소자 내에 포함되는, 상기 비활성 버퍼(110)로부터 읽어 들인 데이터를 임시로 저장하는 임시 버퍼(120); 상기 임시 버퍼(120)에 대한 전원제어를 수행하고, 1회 읽기만 가능한 메모리 간의 상호인증을 위한 인증 연산을 수행하는 연산부/전원제어부(130); 상기 연산부/전원제어부(130) 내에 저장되어 있는 1회 읽기만 가능한 메모리임을 입증하는 개인키 및 발권 일련번호(serial number)(140); 및 외부장치와의 접속을 위한 외부 인터페이스부(150)를 포함한다.

[0022] 유가증권(화폐)이 상거래에서 지불 수단으로 통용될 수 있는 가장 큰 이유는, 각 지폐의 일련번호, 위조 방지 특성 등이 가미되어 유일성(Uniqueness)이 보장되기 때문이다. 이러한 유일성으로 사람들은 돈을 주고 받을 시에 온라인을 통한 확인 없이 거래가 가능한 것이다. 반면 디지털 쿠폰 또는 디지털 머니와 같은 전자 현금의 경우에는 복제가 용이하여 유일성을 보장하기 어렵기 때문에, 안전한 결재를 위해서 반드시 네트워크를 통한 온라인 인증과정을 거쳐야 한다.

[0023] 전자 화폐의 경우 화폐 값은 소정의 디지털 정보로 표현이 되는데, 디지털 정보는 0 또는 1로 표현되기 때문에, 원본과 100% 같은 복제가 가능하게 된다. 이러한 이유로 디지털 기반의 저장장치에서는 유일성을 보장하는 것이 원천적으로 불가능하다. 그러나 본 발명의 일구현예의 전자 지불 매체는 1회 읽기만 가능한 메모리 소자(one-time readable memory device)의 동작 특성으로 인해서 디지털 정보의 유일성을 제공하여 화폐와 동일하게 기능할 수 있다.

[0024] 본 발명의 1회 읽기만 가능한 메모리로 구성되는 전자 지불 매체는 하나의 반도체로 구성될 수 있고, 내부에는 비휘발성 버퍼(110), 임시 버퍼(120), 개인키/일련번호(140)를 저장하고 있는 연산부/전원제어부(130) 및 외부 인터페이스부(150)를 포함한다.

[0025] 본 발명에서 1회 읽기만 가능한 메모리 기반 디지털 거래가 가능하기 위해서는 다음과 같은 두 가지의 조건이 충족되어야 한다. 먼저 (1) 1회 읽기만 가능한 메모리는 저장된 정보에 대하여 한번만 읽기가 가능해야 하고, (2) 1회 읽기만 가능한 메모리에 저장된 정보는 1회 읽기만 가능한 메모리로만 이동이 가능해야 한다. 1회 읽기만 가능한 메모리가 아닌 곳에서 1회 읽기만 가능한 메모리로의 저장 또는 그 반대의 연산은 발권자(예. 한국조폐공사) 만이 가능하다.

[0026] 1회 읽기만 가능한 메모리는 저장된 정보에 대하여 한번만 읽기가 가능한데, 일반 메모리와 다른 연산 방식을 취하는 것을 특징으로 한다. 일반 메모리의 경우 (i) 특정 영역의 데이터에 대한 리드(read) 연산이 요청되면, (ii) 메모리로부터 해당하는 정보를 읽어 넘겨주게 된다. 이와 대조적으로, 1회 읽기만 가능한 메모리의 경우에는 (i) 특정 영역의 데이터에 대한 리드 연산이 요청되면(Read Request), (ii) 메모리로부터 임시로 읽어온 데이터를 칩 내부의 임시 버퍼에 저장하게 되고, (iii) 읽은 영역의 데이터를 0, 1 또는 무작위 데이터로 채우게 된다. 이때 (i) 내지 (iii)번의 트랜잭션은 원자성 있게 (Atomic) 진행되어, 비휘발성 버퍼로부터 읽혀진 화폐 값에 해당되는 디지털 정보는 원천적으로 소거되어야 한다. 한 번의 트랜잭션에 속한 여러 작용들이 하나의 단계의 연산으로 진행되고, 중간에 연산이 중단되지 않고 처리되는 원자성(atomicity)이 보장되어야 한다. 이와 같이, 1회 읽기만 가능한 메모리의 비휘발성 버퍼(110)로부터 독출되는 데이터는 삭제되고 바로 임시 버퍼에 저장되며, 임시 버퍼(120)에 있는 화폐값에 대응되는 디지털 정보는 지불이 이루어지면 전원이 차단되어 삭제된다.

[0027] 본 발명에서 이용되는 1회 읽기만 가능한 메모리에 저장된 메모리는 1회 읽기만 가능한 메모리로만 이동이 가능하다. 1회 읽기만 가능한 메모리에 저장된 메모리가 1회 읽기만 가능한 메모리에 저장된 메모리끼리만 정보 이동이 가능하기 위해서는, 1회 읽기만 가능한 메모리 사이의 상호 인증이 필요하다. 이러한 상호 인증은 상대방이 1회 읽기만 가능한 메모리임을 확인해야 하기 때문에 필요하고, 이러한 상호인증을 위해서 연산부/전원제어부(130)는 그 안에 저장된 개인키 및 일련번호를 이용하여 비대칭키 인증 연산을 수행한다.

[0028] 상거래에서 본 발명의 일구현예의 전자 지불 매체로 지불을 하는 경우에는 송금자의 전자 지불 매체와 수금자의 전가 지불 매체를 서로 연결해야 되는데, 상기와 같은 상호 인증을 통하여 서로가 1회 읽기만 가능한 메모리임을 확인한 후에야 연결이 되는 안전한 저장장치의 연결(Secure Mount) 기능을 제공한다. 비대칭키 연산이란 공개키, 개인키 두 개의 키를 이용하여 암호화 및 인증을 행하는 연산을 의미한다. 송금자 및 수금자는

공개키와 개인키의 두 가지 키를 가지게 된다. 암호화 방법으로는 해쉬 함수(hash function)를 이용한 인증(authentication) 프로토콜을 이용할 수 있다.

[0029] 이러한 인증 연산은 송금자의 전자 지불 매체 및 수금자의 전자 지불 매체가 모두 1회 읽기만 가능한 메모리로 구성된 정당하다고 인증된 전자 지불 매체라는 사실을 확인한다. 인증 연산에 의해서, 송금자와 수금자의 양자는 서로의 신원에 대해서 확신한다. 인증서와 디지털 서명 및 암호화의 사용은 결재의 안전성을 제공한다.

[0030] 여기서 1회 읽기만 가능한 메모리에 저장되어 있는 개인키 정보는 물리적으로 읽을 수 없는 구조를 가진다. 따라서 개인키가 저장되어 있는 메모리 영역은 메모리 내부의 연산부/전원제어부만이 읽을 수 있으며, 그 외의 모든 수단을 통해서라도, 메모리 내부 개인키 데이터를 읽을 수 없게 된다. 다만, 발권자는 해당하는 개인키를 알고 있기 때문에, 1회 읽기만 가능한 메모리가 아닌 곳에서 1회 읽기만 가능한 메모리로의 저장 또는 그 반대의 연산을 수행할 수 있게 된다.

[0031] 따라서 조폐공사와 같은 발권기관에서는 본 발명의 전자 지불 매체에 돈을 넣어줄 수 있다.

[0032] 본 발명에서 비휘발성 버퍼에 저장되는 화폐 값은 화폐의 최소단위(예컨대, 1원)에 해당되는 디지털 정보 블록이 이어진 일련의 스트링(string)의 개념이다. 예를 들면, 1원이 가장 작은 화폐 단위라고 가정하면, 7개의 디지털 정보 블록이 이어지면 7원이 되고, 세 개의 디지털 정보 블록이 이어지면 3원이 된다. 만약 전자 지불 매체에 7개의 디지털 정보 블록(7원)이 저장되어 있는 상태에서 3개의 디지털 정보 블록(3원)을 받게 되면, 10개의 디지털 정보 블록(10원)이 될 수 있다. 여기서 최소 화폐 단위에 해당되는 상기 스트링을 구성하는 하나의 디지털 정보 블록은, 도 3에 도시된 바와 같이, 발권날짜(10),일련번호(20), 및 발권자의 개인키를 이용하여 추출된 “발권날짜”와 “일련번호”의 정보의 디지털 서명(30)을 포함한다. 수금자는 발권자의 공개키를 이용하여, 진품 여부를 판별할 수 있다.

[0033] 비휘발성 버퍼(110)는 화폐 값을 나타내는 데이터가 저장되는 메모리 영역으로서, 전원이 차단되어도, 화폐 값 데이터가 그대로 유지가 되는 비휘발성 특성을 가진 메모리 영역이다. 임시 버퍼(120)는 전자 지불 매체를 이용해서 소정의 비용을 지불하는 경우에 수금자(수금자)에게 돈을 건네 줄 때 화폐값 데이터가 임시적으로 저장되는 곳으로, 이곳의 메모리는 전원이 차단되면 데이터가 소거되는 휘발성 메모리 영역으로 구성된다.

[0034] 연산부/전원제어부(130)는 본 발명의 전자 지불 매체를 이용해서 비용을 지불하는 경우에 양방의 전자 지불 매체가 1회 읽기만 가능한 메모리임을 인증하는 인증 연산을 수행하고, 임시 버퍼(120)로의 전원을 제어하는 역할을 수행한다. 본 발명의 전자 지불 매체가 화폐와 같이 통용되기 위해서 발권자(예컨대, 조폐공사)가 생성한 1회 읽기만 가능한 메모리임을 증명하기 위한 개인키/일련번호(serial number)가 저장되어 있어야 한다. 발권자가 생성한 1회 읽기만 가능한 메모리임을 증명하기 위한 개인키/일련번호는 상기 연산부/전원제어부(130) 내부에 저장되어 있는데, 연산부/전원제어부(130)에서만 내부의 일련번호와 개인키를 읽어와 연산을 수행할 수 있고, 외부에서는 다른 어떠한 방법으로도 내부의 개인키 및 일련번호 정보를 독출할 수 없도록 보호된다. 이와 같은 특성을 가진 메모리의 예로는 신뢰 플랫폼 모듈(Trusted Platform Module)을 예로 들 수 있다. 전자 지불 매체가 하나의 반도체로 집적되어 쉴딩되고, TPM에서 개발된 내부 정보 보호기술에 의해 보호되는 것이 필요하다.

[0035] 상기 전자 지불 매체는 화폐 값 및 송금 처리 상황을 디스플레이하는 표시부와 송금 모드 및 수금 모드 가운데 하나의 모드를 선택하기 위한 모드 버튼 및 확인버튼 등을 포함하는 키입력부를 더 포함할 수 있다.

[0036] 본 발명의 다른 양상은 이상에서 설명한 전자 지불 매체를 이용하는 오프라인 전자 지불 시스템에 관한 것이다. 본 발명의 전자 지불 매체에 의하면 화폐를 이용한 거래방법과 동일한 메커니즘이 디지털 기반으로 실현이 가능하게 된다.

[0037] 본 발명의 일구현예의 오프라인 전자 지불 시스템은 하나 이상의 송금자의 전자 지불 매체; 및 하나 이상의 수금자의 전자 지불 매체를 포함하고, 상기 송금자의 전자 지불 매체 및 상기 수금자의 전자 지불 매체는 위에서 설명한 1회 읽기만 가능한 메모리를 이용하는 전자 지불 매체이고, 송금자의 전자 지불 매체의 외부 인터페이스부 및 수금자의 전자 지불 매체의 외부 인터페이스부가 서로 접속되면 오프라인 방식의 인증 연산을 거쳐 안전한 저장장치의 연결(secure mount)이 이루어지고, 전자 지불 매체의 1회 읽기만 가능한 특성으로 인해서 송금자에 의해 입력된 금액에 해당하는 디지털 정보가 송금자 전자 지불 매체에서 삭제되고, 수금자 전자 지불 매체로 이동되도록 구성된다. 전자 지불 매체는 기존의 현금 또는 지갑과 같이 휴대될 수 있고, 비용 결재 시점포에 비치된 전자 지불 매체와 연결되어 비용 결재에 사용될 수 있다.

[0038] 도 4는 본 발명의 일실시예의 오프라인 전자 지불 장치에서의 전자 지불 매체들 사이의 연결을 설명하는 개략도이고, 도 5는 본 발명의 일실시예의 오프라인 전자 지불 장치를 이용한 전자 지불 과정을 설명하기 위한 모식도이다.

[0039] 도 4에 도시된 바와 같이, 본 발명의 오프라인 전자 지불 장치에서 송금자의 전자 지불 매체와 수금자의 전자 지불 매체 사이에 지불이 이루어지기 위해서는 송금자의 전자 지불 매체(400)와 수금자의 전자 지불 매체(450)가 서로 연결되어야 한다. 이러한 송금자의 전자 지불 매체(400)와 수금자의 전자 지불 매체(450)의 연결 방법은 디지털 정보의 전송이 가능한 연결이 가능하다면 특별히 제한되지 않는데, 일례로 도 4에 도시된 바와 같이 송금자의 전자 지불 매체(400)의 외부 인터페이스부와 수금자의 전자 지불 매체(450)의 외부 인터페이스부가 물리적으로 서로 체결 가능한 구조로 구성될 수 있다. 즉, 송금자의 전자 지불 매체(400)의 외부 인터페이스부의 철부(凸)와 수금자의 전자 지불 매체(450)의 외부 인터페이스부의 요홈(凹)이 서로 체결되도록 구성될 수 있다.

[0040] 상기 전자 지불 매체는, 도 5에 표시된 바와 같이, 화폐 값 및 송금 처리 상황을 디스플레이하는 표시부(410)와 송금 처리 수행을 위한 명령을 입력하기 위한 각종 버튼으로 구성되는 키입력부(420)를 더 포함할 수 있다. 여기서 송금자의 전자 지불 매체(400)와 수금자의 전자 지불 매체(450)가 각자의 외부 인터페이스를 통해서 서로 연결되면, 오프라인 방식의 인증과정을 거쳐 안전한 저장장치의 연결(Secure Mount)이 수행된다. 수금자는 수금 모드를 누르고 대기하고, 송금자가 송금 모드를 누른 후 지불하고자 하는 금액을 입력하고 확인버튼을 누르면 전송 연산이 수행되어 해당 비용의 지불이 이루어진다. 이때 금액이 송금자에서 수금자로 전송이 되는데, 1회 읽기만 가능한 메모리의 하드웨어적 특성으로 읽기를 수행한 순간 송금자의 메모리에 저장된 디지털 정보는 하드웨어적으로 소거되고, 수금자로 전달된다. 그러면 내부에서는 원자성 있게 전송 연산이 수행되며, 송금자의 전자 지불 매체에는 송금완료, 수금자의 전자 지불 매체에는 수금완료 표시가 되고, 이후 외부 인터페이스부를 서로 분리하게 되면 지불 과정이 완료된다.

[0041] 송금자 및 수금자 전자 지불 매체간 안전한 저장장치의 연결을 위한 인증 연산은 공개키 암호화방식(RSA 방식)에 의해 수행될 수 있으나, 반드시 이러한 방식으로 제한되는 것은 아니고, 공개키 암호화 방식 이외에 현재에 사용되거나 장래에 개발될 효율적인 암호화 방식을 이용할 수 있다.

[0042] 상기 오프라인 전자 지불 시스템에서는 1회 읽기만 가능한 메모리는 1회 읽기만 가능한 메모리끼리만 안전하게 연결이 되어야 하는데, 이를 확인하기 위해서 인증연산을 수행한다. 상기 전자 지불 매체 사이의 인증 연산을 예를 들어 보다 상세하게 설명하면 다음과 같다.

[0043] 1. 송금자의 전자 지불 매체는 랜덤한 값, Nonce-A를 생성하여, 송금자 전자 지불 매체의 일련번호(SN)와 함께 수금자의 전자 지불 매체로 정보{Nonce-A, SN}를 전송한다.

[0044] 2. 수금자 전자 지불 매체는 송금자 전자 지불 매체로부터 수신한 Nonce-A값과 SN값에 자신의 1회 읽기만 가능한 메모리에 있는 개인키를 이용하여 디지털 서명을 생성하여 송금자의 전자 지불 매체로 보내며, 수금자의 전자 지불 매체도 랜덤한 값, Nonce-B를 생성하여, 수금자 전자 지불 매체의 일련번호와 함께 수금자 전자 지불 매체로 정보{Nonce-B, SN + PR{Nonce-B, SN}}를 전송한다. 여기서, PR은 발권자가 생성한 1회 읽기만 가능한 메모리임을 증명하기 위한 개인키이다.

[0045] 3. 송금자 전자 지불 매체가 수금자 전자 지불 매체로부터 수신한 정보{PR{Nonce-B, SN}}를 발권자의 공개키를 이용하여, 디지털 서명을 해독하였을 때, 송금자 전자 지불 매체가 보낸 값과 일치하면, 이는 수금자 전자 지불 매체가 “발권자가 생성한 1회 읽기만 가능한 메모리임을 증명하기 위한 개인키”를 내부에 가지고 있다는 의미이므로, 수금자 전자 지불 매체가 1회 읽기만 가능한 메모리라는 것을 확인할 수 있다.

[0046] 4. 수금자 전자 지불 매체가 송금자 전자 지불 매체로부터 수신한 정보를 발권자의 공개키를 이용하여, 디지털 서명을 해독하였을 때, 수금자 전자 지불 매체가 보낸 값과 일치하면, 이는 송금자가 “발권자가 생성한 1회 읽기만 가능한 메모리임을 증명하기 위한 개인키”를 내부에 가지고 있다는 의미이므로, 송금자 전자 지불 매체가 1회 읽기만 가능한 메모리라는 것을 확인할 수 있다.

[0047] 상기 연산부/전원제어부는 인증 연산의 원자성(atomicity)을 제공하도록 구성되는데, 특정 영역의 데이터에 대한 리드 연산의 요청, 비휘발성 메모리로부터 임시로 읽어온 데이터의 임시 버퍼에의 저장 및 비휘발성 메모리에 저장된 데이터의 소거가 하나의 연산으로 수행되어야 하고, 중간에 연산이 중단된 경우, 자동으로 임시 버퍼(120)에 전원이 차단되어 진행이 되지 않아야 한다. 이를 위해서는 전자 지불 매체가 하나의 반도체로 집적되어 쉴딩(Shielding)되어야 한다.

[0048] 이상에서 1회 읽기만 가능한 메모리 소자를 이용한 전자 지불 매체(전자화폐)에 대해서 설명하였으나, 본 발명의 1회 읽기만 가능한 메모리 소자를 이용한 전자 지불 매체에서는 디지털 정보의 유일성 (Uniqueness)이 보장되어, 디지털 페이먼트, 디지털 쿠폰, DRM(Digital Right Management), 인증 서비스 등 기존 온라인 기반 보안 서비스가 오프라인으로 가능할 수 있게 된다. 예를 들어, AOD(Audio on Demand)서비스, VOD(Video on Demand)서비스, 웹 캐스팅 서비스 및 광고 서비스, 온라인 교육 컨텐츠 서비스, e-Book 관련 컨텐츠 서비스에서 보안 및 결재 수단으로 이용될 수 있다.

[0049] 이상에서 본 발명의 하나의 실시예를 들어 본 발명을 상세하게 설명하였으나, 이는 단지 예시를 위한 것으로, 본 발명은 본 발명의 정신 및 범위를 벗어나지 않은 범위 내에서 다양하게 변형 또는 변경 실시될 수 있을 것이다. 따라서 본 발명의 범위는 상기 실시예로 제한되는 것이 아니며, 첨부된 청구범위에 의해서만 정해져야 할 것이다.

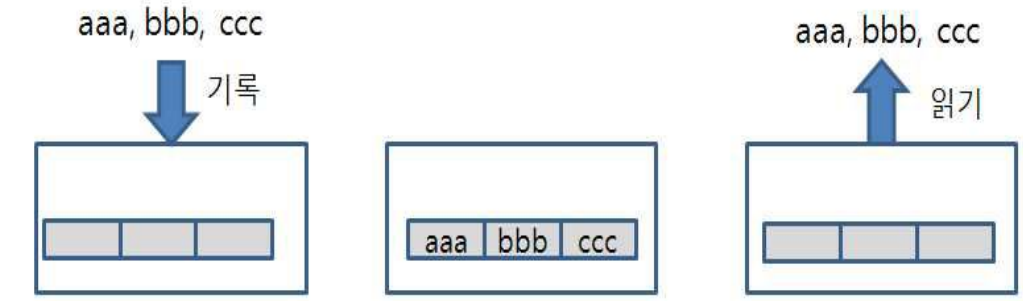
부호의 설명

[0050]

100: 전자 지불 매체
110: 비휘발성 버퍼
120: 임시 버퍼
130: 연산부/전원제어부
140:개인키/일련번호
150: 외부 인터페이스부
400: 송금자 전자 지불 매체
450: 수금자 전자 지불 매체

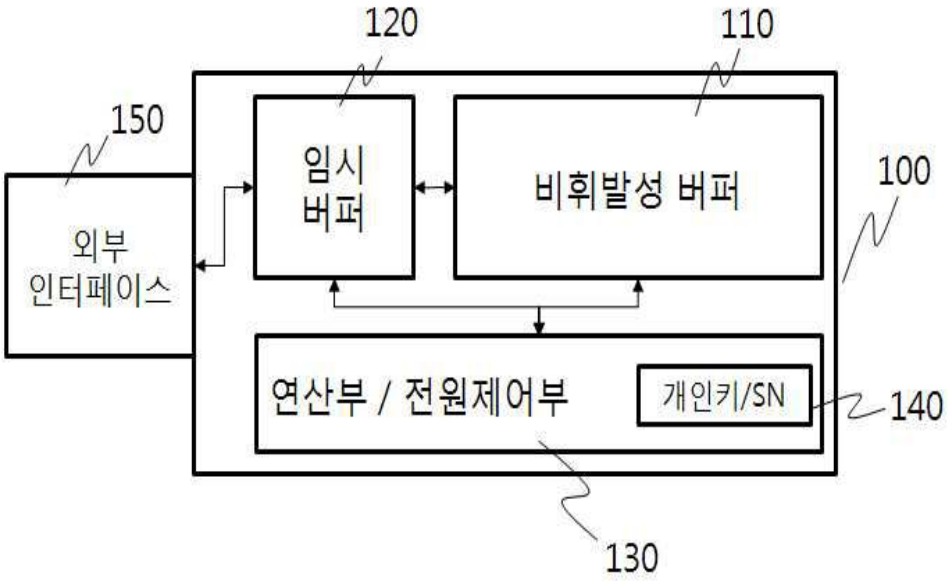
도면

도면1

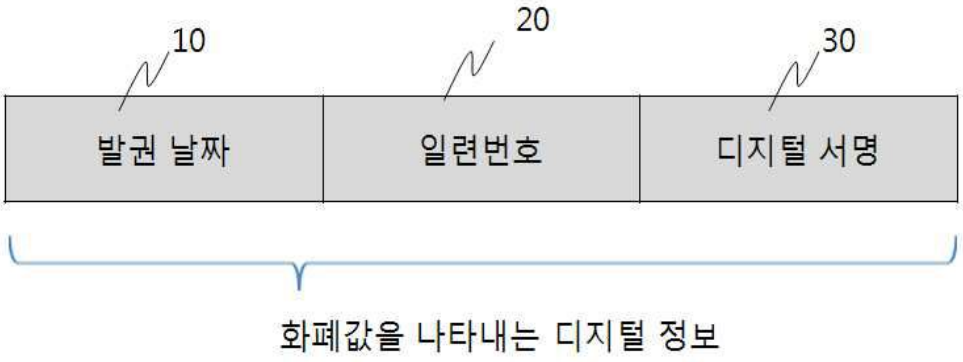


1회 읽기만 가능한 메모리(One-Time Readable Memory)

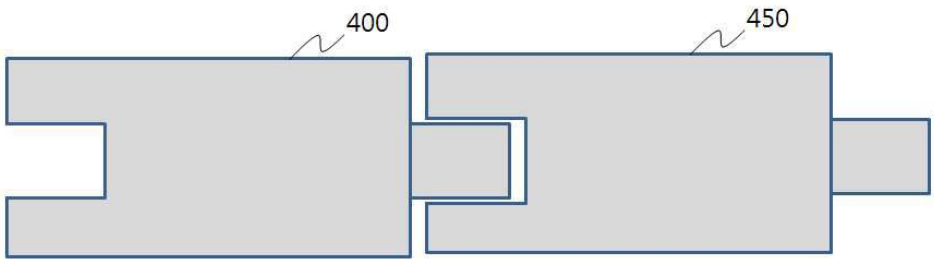
도면2


120
110
150
임시
버퍼
비휘발성 버퍼
100
외부
인터페이스
연산부 / 전원제어부
개인키/SN
140
130

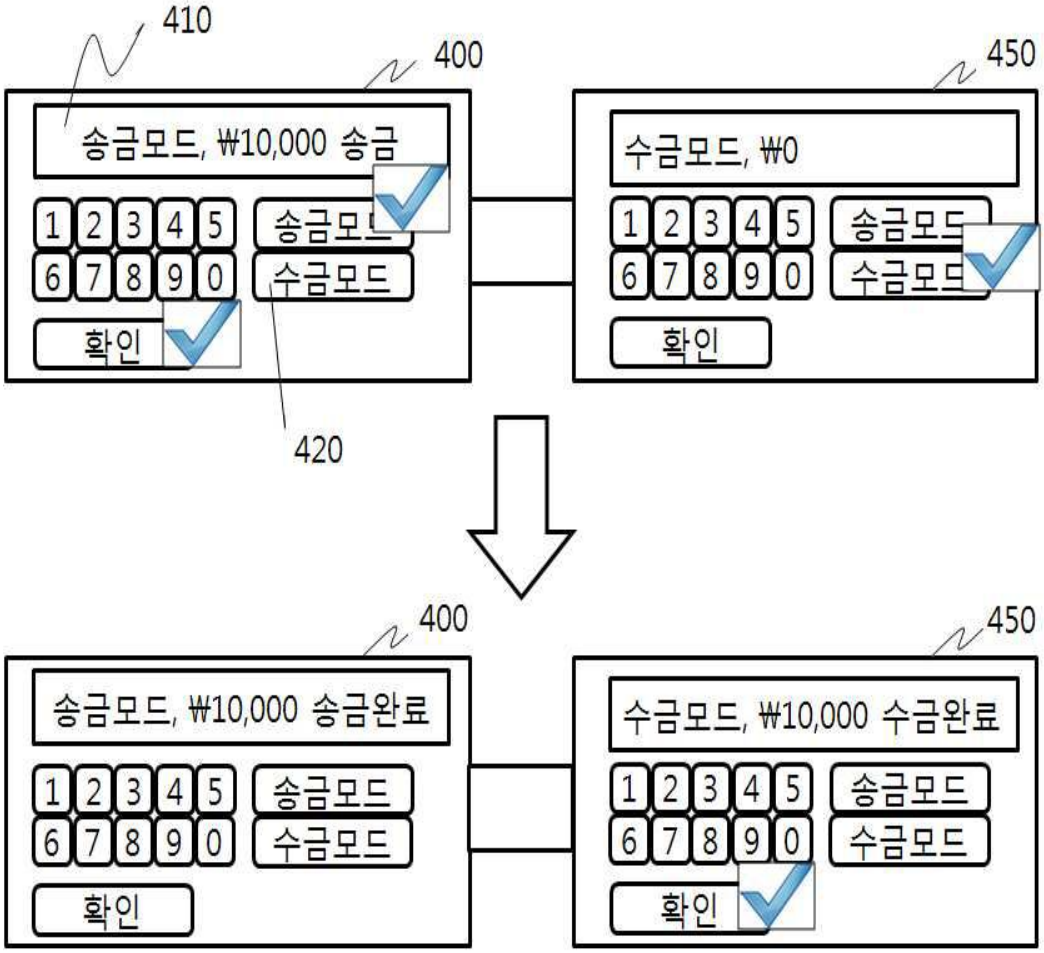
도면3


10
20
30
발권 날짜
일련번호
디지털 서명
화폐값을 나타내는 디지털 정보

도면4


400
450

도면5


410
400
450
송금모드, ₩10,000 송금
1 2 3 4 5
6 7 8 9 0
송금모드
수금모드
확인
수금모드, ₩0
송금모드
수금모드
확인
420
400
450
송금모드, ₩10,000 송금완료
수금모드, ₩10,000 수금완료