



(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。 Int. Cl.

G06Q 40/00G0 (2006.01)

G06Q 99/00 (2006.01)

(11) 공개번호

10-2007-0034603

(43) 공개일자

2007년03월28일

(21) 출원번호 10-2007-7001803

(22) 출원일자 2007년01월24일

심사청구일자 없음

번역문 제출일자 2007년01월24일

(86) 국제출원번호 PCT/US2005/023013

(87) 국제공개번호

WO 2006/004794

국제출원일자 2005년06월27일

국제공개일자

2006년01월12일

(30) 우선권주장

60/583,010

2004년06월25일

미국(US)

60/648,789

2005년02월01일

미국(US)

(71) 출원인

페퍼코인 아이엔씨

미합중국 매사추세츠주 02451 월섬 웨스트 스트리트 200

(72) 발명자

닉스, 로버트, 피.

미국 매사추세츠 01742 콩코드 벨크넵 스트리트 197

메사로비치, 알렉

미국 매사추세츠 02446 브록클린 하버드 애비뉴 51

슈왈츠, 씨오도르

미국 매사추세츠 01775 스토우 버취 힐 로드 19

샤호터, 제프리

미국 매사추세츠 01460 리틀턴 리차드 웨이 6

마스터스, 피터

미국 매사추세츠 02474 얼링턴 레이크힐 애비뉴 33

크로우포드, 찰스

미국 매사추세츠 02143 씨머빌 #1 스쿨 스트리트 12

몬다나로, 제이슨

미국 매사추세츠 01824 첼름스포트 샌드라 드라이브 10

리베스트, 로날드, 엘.

미국 매사추세츠 02476 얼링턴 아카데미 스트리트 41

미칼리, 실비오

미국 매사추세츠 02445 브록클린 체스트넛 힐 애비뉴 459

베르예론, 조셉

미국 매사추세츠 02114 보스톤 에스티. 게르망 스트리트 41

존날라가따, 바라프라사드

미국 매사추세츠 02458 뉴튼 펄 스트리트 72

(74) 대리인

특허법인아주

전체 청구항 수 : 총 36 항

(54) 지불 처리 방법 및 시스템

(57) 요약

지불 처리 시스템은 고객과 상인 사이에 저가의 판매 거래와 관련된 비용 데이터를 수집하는 하나의 거래 프로세서를 포함한다. 이러한 거래 프로세서는 수집된 비용 데이터를 나타내는 데이터를 상기 상인과 관련된 획득 금융 실체로 전달한다. 시스템은 또한 각각의 개별적인 저가의 판매 거래를 나타내는 데이터를 저장하는 다른 거래 프로세서를 포함한다. 저장된 데이터는 상인과 관련된 하나 이상의 금융 실체에 의해 액세스 가능하다.

대표도

도 1

특허청구의 범위

청구항 1.

지불 처리 시스템에 있어서,

고객과 상인 간에 저가의 판매 거래와 관련된 비용 데이터를 수집하도록 구성된 제 1거래 프로세서로서, 수집된 비용 데이터를 나타내는 데이터를 상기 상인과 관련된 획득 은행 실체에 전달하도록 추가로 구성되는, 제 1거래 프로세서와; 및

각각의 개별적인 저가의 판매 거래를 나타내는 데이터를 저장하도록 구성된 제 2거래 프로세서로서, 상기 저장된 데이터는 상기 상인과 관련된 하나 이상의 금융 실체에 의해 액세스 가능한, 제 2거래 프로세서를

포함하는 지불 처리 시스템.

청구항 2.

제 1항에 있어서,

상기 제 2거래 프로세서는 상기 고객과 상기 상인으로부터 떨어져 위치하는 지불 처리 시스템.

청구항 3.

제 1항에 있어서,

상기 제 1거래 프로세서는 상기 상인과 두명 이상의 고객 간에 저가의 판매 거래와 관련된 비용 데이터를 수집하도록 추가로 구성되는 지불 처리 시스템.

청구항 4.

제 1항에 있어서,

상기 제 1거래 프로세서는 두명 이상의 상인과 관련된 저가의 판매 거래와 관련된 비용 데이터를 수집하도록 추가로 구성되고, 상기 상인은 동일한 금융 실체와 관련되는 지불 처리 시스템.

청구항 5.

제 1항에 있어서,

상기 고객은 상기 저가의 판매 거래에 대해 사용시마다 지불을 기초로 하여 상기 상인에게 지불하는 지불 처리 시스템.

청구항 6.

제 1항에 있어서,

상기 고객은 상기 저가의 판매 거래에 대해 선불을 기초로 하여 상기 상인에게 지불하는 지불 처리 시스템.

청구항 7.

제 1항에 있어서,

상기 고객은 상기 저가의 판매 거래에 대해 청약을 기초로 하여 상기 상인에게 지불하는 지불 처리 시스템.

청구항 8.

제 1항에 있어서,

상기 고객은 상기 저가의 판매 거래에 대해 후불을 기초로 하여 상기 상인에게 지불하는 지불 처리 시스템.

청구항 9.

제 1항에 있어서,

각각의 개별적인 저가의 판매 거래를 나타내는 상기 저장된 데이터는 상기 획득 금융 실체에 의해 액세스 가능한 지불 처리 시스템.

청구항 10.

제 1항에 있어서,

각각의 개별적인 저가의 판매 거래를 나타내는 상기 저장된 데이터는 상기 고객과 관련된 상기 발급 금융 실체에 의해 액세스 가능한 지불 처리 시스템.

청구항 11.

제 1항에 있어서,

각각의 개별적인 저가의 판매 거래를 나타내는 상기 저장된 데이터는 상기 고객에 의해 액세스 가능한 지불 처리 시스템.

청구항 12.

제 1항에 있어서,

상기 제 1거래 프로세서는 고객 서비스를 제공하기 위하여 고객 요청을 상기 제 2거래 프로세서에 명령하도록 추가로 구성되는 지불 처리 시스템.

청구항 13.

제 1항에 있어서,

상기 제 1거래 프로세서는 상기 고객과 관련된 발급 금융 실체 내에 위치하는 지불 처리 시스템.

청구항 14.

제 1항에 있어서,

하나 이상의 저가의 판매 거래에 대한 지불의 조정을 기억하도록 구성되는 제 3거래 프로세서를 더 포함하는 지불 처리 시스템.

청구항 15.

제 14항에 있어서,

상기 제 3거래 프로세서는 획득 금융 실체 내에 위치하는 지불 처리 시스템.

청구항 16.

제 1항에 있어서,

상기 수집 비용 데이터를 제 3자를 위한 포맷으로 변환하도록 구성되는 제 4거래 프로세서를 더 포함하는 지불 처리 시스템.

청구항 17.

제 16항에 있어서,

상기 제 4거래 프로세서는 상기 제 1거래 프로세서를 포함하는 서버 내에 위치하는 지불 처리 시스템.

청구항 18.

제 1항에 있어서,

각각의 개별적인 저가의 판매 거래를 나타내는 상기 저장된 데이터는 하나 이상의 상기 거래와 관련된 계좌 번호의 일방향 해쉬를 포함하는 지불 처리 시스템.

청구항 19.

제 1항에 있어서,

저장된 데이터는 액세스를 위하여 암호해독되는 지불 처리 시스템.

청구항 20.

제 1항에 있어서,

하나 이상의 저가의 판매 거래는 가판대(kiosk) 디바이스에서 발생하는 지불 처리 시스템.

청구항 21.

제 1항에 있어서,

상기 고객과 제 2상인 간에 저가의 판매 거래와 관련된 비용 데이터를 수집하도록 구성된 제 3거래 프로세서를 더 포함하는 지불 처리 시스템.

청구항 22.

제 1항에 있어서,

상기 상인은 상기 고객에게 선호하는 처리를 제공하여, 상기 상인과의 장래의 거래를 조장하는 지불 처리 시스템.

청구항 23.

지불 처리 방법에 있어서,

제 1고객과 제 1상인 간에 제 1저가의 판매 거래를 나타내는 데이터를 수신하는 단계와,

상기 제 1저가의 판매 거래 비용과, 상기 고객과 상기 상인 간에 제 2저가의 판매 거래 비용을 수집하는 단계와,

상기 제 1저가의 판매 거래와 관련된 데이터가 상기 상인과 관련된 하나 이상의 금융 실체에 의해 액세스 가능하도록 상기 제 1저가의 판매 거래와 관련된 데이터를 저장하는 단계와,

수집 비용을 나타내는 데이터를 상기 상인과 관련된 획득 금융 실체에 전달하는 단계를 포함하는 지불 처리 방법.

청구항 24.

제 23항에 있어서,

상기 제 1고객과 관련된 저가의 판매 거래 비용과 제 2고객과 관련된 저가의 판매 거래 비용을 수집하는 단계를 더 포함하는 지불 처리 방법.

청구항 25.

제 23항에 있어서,

상기 제 1상인과 관련된 저가의 거래 비용과 제 2상인과 관련된 저가의 판매 거래 비용을 수집하는 단계를 더 포함하고, 상기 제 1 및 제 2상인은 상기 획득 금융 실체와 관련되는 지불 처리 방법.

청구항 26.

제 23항에 있어서,

상기 제 1저가의 판매 거래와 관련된 상기 저장된 데이터는 상기 획득 금융 실체에 의해 액세스 가능한 지불 처리 방법.

청구항 27.

제 23항에 있어서,

상기 제 1저가의 판매 거래와 관련된 상기 저장된 데이터는 상기 고객과 관련된 발급 금융 실체에 의해 액세스 가능한 지불 처리 방법.

청구항 28.

제 23항에 있어서,

상기 제 1저가의 판매 거래와 관련된 상기 저장된 데이터는 상기 고객에 의해 액세스 가능한 지불 처리 방법.

청구항 29.

제 21항에 있어서,

상기 제 1저가의 판매 거래와 관련된 데이터를 저장하는 단계는 상기 제 1저가의 판매 거래와 관련된 계좌 번호에 일방향 해쉬를 적용하는 단계를 포함하는 지불 처리 방법.

청구항 30.

컴퓨터 판독 가능한 매체 상에 존재하는 컴퓨터 프로그램 제품으로서, 저장된 복수의 지령을 구비하고, 상기 지령은 프로세서에 의한 실행시에, 상기 프로세서로 하여금,

제 1고객과 제 1상인 간에 제 1저가의 판매 거래를 나타내는 데이터를 수신하고,

상기 제 1저가의 판매 거래 비용과, 상기 고객과 상기 상인 간에 제 2저가의 판매 거래 비용을 수집하고,

상기 제 1저가의 판매 거래와 관련된 데이터가 상기 상인과 관련된 하나 이상의 금융 실체에 의해 액세스 가능하도록 상기 제 1저가의 판매 거래와 관련된 데이터를 저장하고,

수집 비용을 나타내는 데이터를 상기 상인과 관련된 획득 금융 실체에 전달하도록

하는 컴퓨터 프로그램 제품.

청구항 31.

제 30항에 있어서,

제 1고객과 관련된 저가의 판매 거래 비용과, 제 2고객과 관련된 저가의 판매 거래 비용을 수집하도록 하는 지령을 더 포함하는 컴퓨터 프로그램 제품.

청구항 32.

제 30항에 있어서,

상기 제 1상인과 관련된 저가의 거래 비용과, 제 2상인과 관련된 저가의 판매 거래 비용을 수집하도록 하는 지령을 더 포함하고, 상기 제 1 및 제 2상인은 상기 획득 금융 실체와 관련되는, 컴퓨터 프로그램 제품.

청구항 33.

제 30항에 있어서,

상기 제 1저가의 판매 거래와 관련된 상기 저장 데이터는 상기 획득 금융 실체에 의해 액세스 가능한 컴퓨터 프로그램 제품.

청구항 34.

제 30항에 있어서,

상기 제 1저가의 판매 거래와 관련된 상기 저장 데이터는 상기 고객과 관련된 발급 금융 실체에 의해 액세스 가능한 컴퓨터 프로그램 제품.

청구항 35.

제 30항에 있어서,

상기 제 1저가의 판매 거래와 관련된 상기 저장 데이터는 상기 고객에 의해 액세스 가능한 컴퓨터 프로그램 제품.

청구항 36.

제 30항에 있어서,

상기 제 1저가의 판매 거래와 관련된 데이터를 저장하는 단계는, 상기 제 1저가의 판매 거래와 관련된 계좌 번호에 일방향 해쉬를 적용하는 단계를 포함하는 컴퓨터 프로그램 제품.

명세서

기술분야

관련 출원

본 출원은 (a) 2004년 6월 25일 출원되었고, 발명이 명칭이 "소규모 지불 게이트웨이 방법 및 시스템"인 미국 가특허출원 제60/583,010호와, (b) 2005년 2월 1일 출원되었고, 발명이 명칭이 "소규모 거래 방법 및 시스템을 위한 예지 처리"인 미국 가특허출원 제60/648,789호를 우선권 주장한다.

본 명세서의 내용은 지불 처리에 관한 것으로, 보다 상세하게는 거래 비용을 낮추기 위하여 저가의 구매를 처리하는 것에 관한 것이다.

배경기술

신용카드 및 직불카드의 도입과, 시장에서 이들의 늘-증가하는 사용에 대해, 산업계 추세는 이들 도구가 더 많은 고객의 선호 대상이 되고 있음을 나타낸다. 2003년에, 처음으로 고객이 현금이나 수표에 기초한 지불 방법을 사용하는 것보다 전자 지불 방법을 사용하여 더 많이 지불하였다. 조사를 통해, 3,700만명 이상의 미국인이 5달러(\$ 이하)에 대해 카드를 사용하여 POS(point-of-sale) 구매를 행하였고, 카드를 사용하여 온라인 콘텐츠를 구매하는 미국인의 수는 1년도 안되어 400만명에서 1,400만명으로 증가하였다. 덧붙여, 무선 주파수 인식(RFID : radio frequency identification) 기술에 기초한 비접촉식 지불 카드는 전개 중이고, 이들 고객의 추세를 가속시킬 것이다.

물리적인 POS, 디지털, 및 모바일 시장에서 소규모 지불 금액은 경이적인 속도로 증가하고 있다. 미국에서 5달러 이하의 현금 지불로 1조3천억 달러 이상이 지불되고, 디지털 지불은 20%가 넘는 연평균 성장률(CAGR)로 30억 달러를 상회하고, 모바일 지불은 100%가 넘는 CAGR로 5억 달러를 상회하고, 전-세계적인 기회는 더 크다.

소규모 지불의 비즈니스 모델에 상인은 상당한 관심을 갖지만, 잠재적인 문제점이 소규모 지불에 기초한 이문이 있는 비즈니스의 제고를 방해할 수 있다. 예컨대, 높은 거래 처리비용은 비즈니스 수익성에 부정적인 충격을 가할 수 있다. 전형적인 거래 처리비용은 0.25 달러 + 거래의 2%가 될 수 있다. 1달러의 저가의 거래에 대해, 거래 처리비용은 0.27달러 즉 거래의 27%이다. 이것은 상인을 위한 이문이 있는 비즈니스를 지원하기 위한 상당한 거래 처리비용이다. 금융 산업 소식통은 거래에 대한 전체 처리비용이 0.2달러 내지 0.4달러이고, 산업계는 10달러 이하의 거래에 대해서는 돈을 잃을 것이라고 보고하였다.

거래 비용과 함께, 고객지원 비용은 수입과 수익에 상당한 충격을 가할 수 있다. 종래의 고객 서비스 비용은 전형적으로 전화 지원 건마다 5달러 내지 10달러, 그리고 비용청구를 초래하는 지불관련 지원에 관한 건당 15달러 내지 30달러이다. 높은 품질의 고객 지원을 제공하는 것은 비즈니스를 전개하고 성장시키는 중요한 부분이지만, 높은 고객 지원비용은 수익성을 낮출 수 있다.

고객 획득 비용은 평생 고객의 가치와 서로 관련되지 않을 수 있다. 상인은 고객을 유인하여 유지하기 위해 상당한 마케팅 지출을 초래할 수 있다. 예컨대, 비용은 컵 서비스 음식점을 위한 고객 당 광고에 2내지 4달러로부터 인터넷 비즈니스를 위한 고객 당 20내지 40달러에 이를 수 있다. 이들 문제점을 해결하기 위하여, 상인들은 빈번한 고객 구매를 구축하기 위한 유연하고 비용대비 효과가 큰 방식에 관심을 갖는다. 예컨대, 상인들은 강력한 새로운 제품 및 서비스를 생산하고, 다통이 없는 정책을 실현하거나, 통합된 로열티 및 보답 프로그램을 설정하거나, 또는 (간혹 제 3자 파트너와 함께) 목표로 정해진 판촉을 개시할 수 있다.

발명의 상세한 설명

본 발명의 하나의 양상에 따라, 지불 처리 시스템은 고객과 상인 간에 저가의 판매 거래와 관련된 비용 데이터를 수집하는 하나의 거래 프로세서를 포함한다. 이러한 거래 프로세서는 수집된 비용 데이터를 나타내는 데이터를 상인과 관련된 획득 금융 실체에 전달한다. 이 시스템은 또한 각각의 개별적인 저가의 판매 거래를 나타내는 데이터를 저장하는 다른 거래 프로세서를 포함한다. 저장된 데이터는 상인과 관련된 하나 이상의 금융 실체에 의해 액세스 가능하다.

일 실시예에 있어서, 제 2거래 프로세서는 고객과 상인으로부터 떨어져 위치할 수 있다. 제 1거래 프로세서는 다양한 유형의 수집을 수행할 수 있다. 예컨대, 이 프로세서는 상인과 적어도 두 고객 간에 저가의 판매 거래와 관련된 비용 데이터를 수집하거나, 또는 둘 이상의 상인에 관련된 저가의 판매 거래와 관련된 비용 데이터를 수집할 수 있다. 상인과 고객 사이에서 다양한 지불 방법론을 구현할 수 있다. 예컨대, 고객은 사용시마다 지불 기반, 선불 기반, 후불 기반, 또는 기타 유사한 기반으로 저가의 판매 거래에 대해 상인에게 지불할 수 있다. 각각의 개별적인 저가의 판매 거래를 나타내는 저장 데이터는, 고객과 관련된 획득 금융 실체 또는 발급 금융 실체와 같은 다양한 금융 실체에 의해 액세스가 가능하다. 각각의 개별

적인 저가의 판매 거래를 나타내는 저장 데이터는 또한 고객에 의해 액세스 가능하다. 고객 서비스의 제공을 위하여, 제 1 거래 프로세서는 고객 서비스를 제공하기 위해 고객의 요구를 제 2거래 프로세서에 명령할 수 있다. 각 프로세서는 다양한 위치에 위치할 수 있다. 예컨대, 제 1거래 프로세서는 고객과 관련된 발급 금융 실체에 위치할 수 있다. 지불 처리 시스템은 하나 이상의 저가의 판매 거래에 대한 지불의 조정을 기억하는 제 3거래 프로세서를 더 포함할 수 있다. 이러한 제 3거래 프로세서는 획득 금융 실체에 위치할 수 있다. 시스템은 수집 비용 데이터를 제 3자를 위한 포맷으로 변환하는 제 4거래 프로세서를 포함할 수도 있다. 이러한 제 4거래 프로세서는 제 1거래 프로세서를 포함하는 서버 내에 위치할 수 있다. 보안 방법은 지불 처리 시스템에 포함될 수 있다. 예컨대, 각각의 개별적인 저가의 판매 거래를 나타내는 저장된 데이터는 하나 이상의 거래와 관련된 계좌 번호의 일 방향 해쉬(one-way hash)를 포함할 수 있다. 따라서, 저장된 데이터는 액세스를 위하여 해독될 수 있다. 하나 이상의 저가의 판매 거래는 가판대 디바이스(kiosk device)에서 발생할 수 있다. 지불 처리 시스템은 고객과 다른 상인 간에 저가의 판매 거래와 관련된 비용 데이터를 수집하는 제 3 거래 프로세서를 포함할 수 있다. 일부 실시예에 있어서, 상기 상인은 상기 고객에게 선호하는 처리를 제공하여, 상기 상인과의 장래의 거래를 조장할 수 있다.

본 발명의 다른 양상에 따라, 지불을 처리하는 방법은 고객과 상인 간에 하나의 저가의 판매 거래를 나타내는 데이터를 수신하는 단계를 포함한다. 이러한 방법은 또한 고객과 상인 사이에서 저가의 판매 거래 비용과 다른 저가의 판매 거래 비용을 수집하는 단계를 포함한다. 더욱이, 이러한 방법은, 데이터가 상인과 관련된 하나 이상의 금융 실체에 의해 액세스될 수 있도록, 각 저가의 판매 거래와 관련된 데이터를 저장하는 단계를 포함한다. 이 방법은 또한 수집 비용을 나타내는 데이터를 상인과 관련된 획득 금융 실체에 전달하는 단계를 포함한다.

일 실시예에 있어서, 상기 방법은 또한 고객과 관련된 저가의 판매 거래 비용과 다른 고객과 관련된 저가의 판매 거래 비용을 수집하는 단계를 포함할 수 있다. 더욱이, 상기 방법은 한명의 상인과 관련된 저가의 거래 비용과 다른 상인과 관련된 저가의 판매 거래 비용을 수집하는 단계를 포함할 수 있는데, 두명의 상인 모두 획득 금융 실체와 관련된다.

본 발명의 다른 양상에 따라, 컴퓨터 판독 가능한 매체 상에 존재하는 컴퓨터 프로그램 제품은, 프로세서에 의해 실행될 때 프로세서로 하여금 고객과 상인 간에 저가의 판매 거래를 나타내는 데이터를 수신하도록 하는 지령을 구비한다. 추가적인 지령은 프로세서로 하여금 고객과 상인 간에 저가의 판매 거래 비용과 다른 저가의 판매 거래 비용을 수집하게 한다. 지령은 또한 프로세서로 하여금 각각의 저가의 판매 거래와 관련된 데이터를 저장하여, 이러한 데이터가 상인과 관련된 하나 이상의 금융 실체에 의해 액세스될 수 있도록 한다. 또한, 지령은 프로세서로 하여금 수집 비용을 나타내는 데이터를 상인과 관련된 획득 금융 실체에 보내게 한다.

일 실시예에 있어서, 컴퓨터 프로그램 제품은 한명의 고객과 관련된 저가의 판매 거래 비용과 다른 고객과 관련된 저가의 판매 거래 비용을 수집하도록 하는 추가적인 지령을 포함할 수 있다. 한명의 상인과 관련된 저가의 거래 비용과 다른 상인과 관련된 저가의 판매 거래 비용을 수집하게 하는 지령이 포함될 수 있다.

본 발명의 추가적인 장점 및 양상은, 본 발명을 실시하기 위해 고려되는 최상 모드의 단순한 도시를 통해 본 발명의 실시예가 도시되고 설명되는 다음의 상세한 설명으로부터 당업자에게는 자명해질 것이다. 여기에서 설명하는 바와 같이, 본 발명은 그 외의 다른 실시예가 가능하고, 다수의 세부 사항은 다양하게 명백한 측면에서, 본 발명의 사상으로부터 벗어남이 없이, 쉽게 변경할 수 있다. 따라서, 도면 및 명세서는 제한하는 것이 아니라 사실상 예시하는 것으로 간주되어야 한다.

실시예

도 1을 참조하면, 저가 구매의 거래 비용을 실제적으로 감소시키는 대규모 지불 시스템(10)이 도시되어 있다. 이러한 예시적인 예는 상인으로부터 상품 및/또는 서비스를 구매하는 고객을 포함한다. 획득 은행으로 알려진 금융 기관은 지불을 수납하기 위한 계좌를 상인에게 제공한다. 발급 은행으로 알려진 다른 금융 기관은 전자 지불을 하기 위한 도구(예, 신용카드, 직불카드, 선불카드 등)를 고객에게 제공한다. 카드 네트워크로도 알려진 조합은 발급 은행과 획득 은행 사이의 관계를 관리한다. 일부 장치에 있어서, 프로세서로 알려진 제 3자는 상인, 획득 은행, 발급 은행 및 조합 사이의 거래를 처리한다. 이러한 논의를 통해, 금융 서비스 기관(즉, 획득 은행, 발급 은행, 조합, 및 프로세서)은 FSI(financial service institute)로 언급될 수 있다.

상인, 획득 은행, 발급 은행, 프로세서, 및 조합으로 하여금 소규모 지불을 이용할 수 있게 하는 소규모 지불 애플리케이션을 만들어 배포함으로써, 신용카드 및 직불카드의 널리 퍼진 고객 신용 및 이에 대한 선호도를 적절히 활용할 수 있다. 그러한 목적을 위해, 소규모 거래 프로세서(12)는 상인과 통신하는 서버(14) 상에서 실행된다. 하드웨어, 소프트웨어, 또는 하드웨어와 소프트웨어의 결합으로 구현될 수 있는 소규모 거래 프로세서(12)는 기존의 지불 기반구조를 확장시킴으로써, 소규모 거래 처리에 대한 수입과 수익을 실질적으로 최적화하도록 설계된다.

일부 장치에 있어서, 소규모 거래 프로세서(12)는, 상인, 획득 은행, 발급 은행, 프로세서 및 조합으로 하여금 소규모 지불에 대해 성장하고 발전할 수 있도록 하는 확장 가능한 거래 처리 플랫폼이다. 소규모 지불을 효율적이고 경제적으로 운영함으로써, 소규모 거래 프로세서(12)는 관련 구매의 수집을 통해서 저가 구매의 거래 비용을 실질적으로 감소시킬 수 있다. 소규모 거래 프로세서(12)는 또한 고객으로 하여금 선호하는 지불 도구(예, 신용카드, 직불카드 등)를 통해 구매할 수 있도록 허용한다. 디지털, 모바일, 및 물리적인 POS 환경 내에서 작용함으로써, 소규모 거래 프로세서(12)의 운영은, 고객의 구매 경험에서 가시적인 변화가 전혀 없이, 신용카드 게이트웨이로서 상인의 구매 경험에 연속적으로 통합될 수 있다. 그 운영을 통해, 상인은, 사용시마다 지불, 선불(pre-paid), 청약(subscription), 및 후불(post-paid)의 잠재적인 비즈니스 모델의 혼합을 통해, 고객과의 수익이 있는 관계를 구축하기 위한 도구를 제공받는다. 소규모 거래 프로세서(12)는 또한 통합 청구서 고지 및 분쟁 해결을 통해 고객의 만족을 개선시킬 수 있고, 고객 서비스 비용을 낮출 수 있다. 더 낮은 거래 비용과 함께, 소규모 거래 프로세서(12)의 사용은 비용대비 효과가 큰 로열티, 판촉, 및 사기행위 관리 기술을 소규모 지불 시장에 제공한다.

소규모 거래 프로세서(12)는 지불 처리 시스템(10)에 포함된 다양한 당사자를 위한 이익을 제공한다. 예컨대, 전형적인 고객은 구매의 유연성을 원한다. 이들은 살 것, 구매하는 시간, 지불하는 방법에 대한 제어를 원한다. 하지만, 상인은 소규모 지불에 대한 카드 사용에 대해 빈번하게 제한을 부과하고, 궁극적으로는 고객이 희망하는 편리성을 제공하지 않을 수 있다. 상인은 고객이 자신들의 상품 및/또는 서비스를 구매하는 것을 쉽게 하기를 원한다. 하지만, 더 적은 거래에 대해, 카드 처리 및 고객 서비스 비용은 전부는 아니더라도 상인의 이익 중 상당 부분을 소비한다. 고객이 저가의 항목에 대해 지불하는데 그들의 선호하는 신용카드 또는 직불카드를 사용할 때, 상인의 이익은 사라질 수 있다.

소규모 거래 프로세서(12)는 고객에게는 실질적으로 눈에 띄지 않게 동작한다. 고객은 소프트웨어를 다운로드하거나, 제작을 만들거나 이에 사전 적립하거나, 또는 구매하기 위한 최소량을 소비할 필요가 없다. 그러나, 고객은 그들의 거래를 온라인으로 상대적으로 신속하게 재검토할 수 있다. 고객을 위해 지불 처리 시스템(10)은, 고객으로 하여금 그들이 이미 소유하고 있는 신용이 있고 선호하는 지불 메커니즘(카드)을 사용하여 소규모 구매를 행하는 것을 허용한다. 시스템은 고객에게 다양한 종류의 비즈니스 모델(예, 사용시마다 지불, 선불, 청약, 또는 후불)을 사용함으로써 구매하는 것과 함께, 저가의 디지털, 모바일, 및 물리적인 POS 상품 및 서비스에 대한 손쉬운 액세스를 제공한다.

부가적으로, 상인은 고객에게 바람직한 상품과 편익을 제공하기를 희망한다. 유연한 지불 선택사항을 제공함으로써, 지불 처리 시스템(10)은 편익을 제공한다. 상인은 또한 모든 구매에 대해 지불 선택의 넓은 배열을 제공하기를 바라지만, 비용이 드는 거래 처리 및 고객 서비스 수수료로 인해 상인은 소규모의 신용카드 및 직불카드 구매에 대해 수익면에서 방해를 받는다.

지불 처리 시스템(10)은 소규모 지불에 대한 수익이 있는 거래를 가능케 한다. 이러한 시스템은 소규모 및 소액지불과 관련된 두 가지 중요한 비용(거래 처리비용 및 고객 서비스 비용)을 감소시킨다. 지불 처리 시스템(10)은 수집 방법론을 통해 거래 비용을 다룬다. 상인으로 하여금 소규모 지불을 수집하고, 수집 설정값을 변경 및 조정하도록 허용함으로써, 이러한 시스템은 효율을 증가시킨다. 하나의 장치에 있어서, 지불 처리 시스템(10)의 일부는 (인터넷을 통해)온라인으로 구현된다. 이러한 장치에 있어서, 자동화된 고객 서비스가 제공되어, 해당 고객 서비스를 비교적 낮은 비용으로 전달한다. 지불 처리 시스템(10)은 또한 상인으로 하여금 고객 승낙을 최적화하는 비즈니스 모델을 제공하도록 허용한다.

상인에 대해, 지불 처리 시스템(10)은 저가의 상품과 서비스를 통해 상인이 상부-라인(수입)과 하부-라인(수익)을 모두 성장시키는 것을 돕는다. 이러한 시스템은 또한 예컨대, 사용시마다 지불, 청약, 선불 및 후불의 지불 구조를 지원함으로써 비즈니스 모델의 유연성을 제공한다. 부가적으로, 상인은 비용대비 효과가 큰 고객 자기 관리에 대한 비용 및 고객 만족의 이익을 제공받는다.

획득 은행 및 지불 프로세서는, 상인 고객의 요구에 부합하고 전체적인 거래 금액을 증가시키는 상품을 제공하는 것에 관심이 있을 수 있다. 그러나, 획득 은행 및 지불 프로세서는 전형적으로 소규모 지불에 대한 비용대비 효과가 큰 양도를 상인에게 제공할 수 없다. 전통적인 지불 처리와 관련된 고정되거나 변동하는 높은 수수료는 불균형하게 상인의 수익에 부정적인 영향을 미친다. 선불 카드 또는 최소 구매량의 사용을 구현하는 것과 같은 대안은 고객에 대해 경제적인 면이나 시간적인 면에서 방해를 줄 수 있다.

소규모 거래 프로세서(12)를 병합함으로써, 프로세서와 획득 은행은 상인을 위해 수익이 있는 비즈니스 모델을 가능케 할 수 있다. 상인은 소규모 및 소액 거래에 대해 바람직한 지불 도구(신용카드와 직불카드)를 수용하여, 유익하게 유지할 수 있다. 시스템을 통해 흐르는 새로운 등급의 거래에 대해, 처리량이 증가할 수 있고, 이를 통해 획득 은행과 프로세서를 위

한 수입이 증가할 수 있다. 일반적으로, 소규모 거래 프로세서(12)는 기존의 처리 시스템, 및 프로세서의 상인용 시스템에 통합될 수 있다. 획득 은행과 프로세서에 대해, 지불 처리 시스템(10)은 수입과 수익 모두를 유리하게 가져오는 거래 흐름을 증가시킬 수 있다.

발급 은행은 그들의 회원이 거래할 때마다 자사의 카드가 "자주 사용(top of wallet)" 카드가 되기를 희망한다. 하지만, 소규모 구매에 대해, 높은 처리 및 고객 서비스에 대한 비용은 (디지털 및 물리적인 면 모두에서) 상인이 신용카드와 직불카드를 수용하는 것을 방해한다. 결과적으로, 발급은행은 현금과 대안적인 지불 시스템에 대한 시장 점유율을 상실할 수 있다.

지불 처리 시스템(10)의 기능성에 대해, 발급 은행의 회원은 저가의 상품을 구매하는데 현금 대신에 카드를 사용하는 것에 대한 증가한 편리성을 인정할 수 있다. 구매 과정은 친숙하고 신속하며, 어떠한 계좌 등록도 필요로 하지 않는다. 수집 기능을 갖는 지불 처리 시스템(10)은 소규모 지불에 대한 발급 은행의 고객 서비스 비용을 감소시킬 수 있다. 종래의 일부 시스템에 있어서, 실시간 고객 서비스 응답은 특별히 낮은 수익의 소규모 지불에 대해, 건 당 10달러까지 비용이 상승할 수 있다. 소규모 지불에 대해 이러한 고가의 고객 서비스를 유지하는 것은 눈에 띄지 않을 정도로 적은 것일 수 있다. 지불 처리 시스템(10)은 특별히 소규모 지불을 위해 설계된 온라인 고객 자가-서비스를 제공할 수 있는데, 이는 비교적 낮은 비용으로 응답 서비스를 제공할 수 있다. 발급 은행에 대해, 지불 처리 시스템(10)은 현금 및 수표 소비를 카드 소비로 변환시킬 수 있어서, 거래의 흐름을 증가시킨다. 소규모 거래는 고객이 거래하는 빈도를 증가시켜, 자주 사용하는(top of wallet) 시장 점유율 수익을 고객이 사용하는 카드로부터 이루어지게 한다. 지불 처리 시스템(10)은 온라인 고객 자가 관리를 통해 비용을 줄인다. 부가적으로, 수집하는 경제의 일부 경제 측면은 비접촉식 지불 카드와 같은 소규모 지불 지향 발급 제품에 관한 상인의 새로운 발매에 대한 방해물을 제거한다.

일반적으로, 거래 처리에 대한 현재의 표준 수수료 구조는 수익이 있는 소규모 및 소액지불의 가능성을 방해한다. 응답이 없이, 카드 네트워크는 저가의 디지털 상품에 대해 신속히 전개되는 시장의 일부를 잃을 수 있다.

지불 처리 시스템(10)은 회원과 상인으로 하여금 낮은 가치의 항목에 대해 현금 대신에 카드 지불을 행하고 이를 수락하는 것을 가능케 할 수 있다. 고객은 증가된 편리성을 인정할 수 있는데, 왜냐하면 구매 과정이 친숙하고 비교적 신속하게 유지되고, (만약 필요하다면) 최소의 계좌 등록을 필요로 하기 때문이다. 지불 처리 시스템(10)은 소규모 지불에 대한 고객 서비스 비용을 줄임으로써 카드 조합 회원을 지원한다. 전형적으로, 종래의 실시간 고객 서비스 응답과 지불 수수료는 특히 낮은 이윤의 소규모 지불에 대해 매우 값비싸다. 대조적으로, 지불 처리 시스템(10)은, 비교적 낮은 비용으로 응답 고객 서비스를 전달하도록 설계된 직관적 온라인 고객 자가 서비스를 특히 소규모 지불을 위해 제공한다.

지불 처리 시스템(10)은 낮은 가치의 현금 및 수표 지불을 카드 지불로 전환시킴으로써 거래 흐름을 증가시킨다. 이러한 시스템은 또한 카드 지불 시스템을 경쟁 지불 형태의 입장으로부터 방어한다. 더욱이, 이윤이 있는 소규모 지불은 이러한 카드 네트워크 내에서 가능해진다.

도 2를 참조하면, 소규모 거래 프로세서(12)는 지불 처리 시스템(10) 내에서의 단일 당사자에 의해 소유되고 운영되는 소프트웨어 제품, 또는 하청을 받은 서비스로서 다수의 당사자에 의해 사용될 수 있는 제품으로 전개될 수 있다.

일반적으로, 소규모 거래 프로세서(12)는, 상인으로부터 지불 처리 시스템(10)으로 지불을 전달하기 위한 소규모 지불 게이트웨이를 제공하는 것과 같은 능력을 포함한다. 온라인 고객 자가 서비스는 또한 독립적으로 구현될 수 있거나 또는 기존 상인 서비스 인터페이스 내에서 구현될 수 있는 지불 처리 시스템(10)에 의해 제공될 수 있다. 지불 처리 시스템(10)은 또한, 수집 계산(예, 단일 상인으로부터의 수집 거래)을 지원하는 고객 계좌 프로세서(16) 및 상인 계좌 프로세서(18)를 포함한다. 부가적으로, 프로세서(12, 16 및 18)는 수집 파라미터를 조정하고, 상인으로 하여금 거래 비용, 교환 자격, 현금 흐름, 위험 비용, 및 고객 서비스를 실질적으로 최적화하도록 허용하는 능력을 제공한다. 프로세서(12, 16 및 18) 중 하나 이상은 발급 은행을 통해 수집을 수행하기 위한 기술을 포함할 수 있다.

지불 처리 시스템(10)의 설계의 유연성은 많은 금액의 거래 금융 및 처리 환경에서의 구현을 제공한다. 예컨대, 상인 계좌 프로세서(18)는 획득 은행과 획득 은행의 프로세서를 위한 상인 계좌 서비스를 제공하도록 설계될 수 있다. 고객 계좌 프로세서(18)는 또한 발급 은행과 발급 은행의 프로세서를 서비스 기능을 제공할 수 있다. 지불 처리 시스템(10)은 또한 FSI로 하여금 비용 효율적이고, 안전하며, 분산된 회계감사(auditing)를 통한 분산된 처리에 대한 제어를 유지하는 것을 가능케 하도록 구성할 수 있다.

지불 처리 시스템(10)의 설계는 범위성(scalability), 신뢰도 및 보안과 같은 설계 개념을 다룰 수 있다. 예컨대, 소규모 거래 프로세서(12)는 소규모 거래 경제의 상당 부분을 처리하기 위하여 1,000개 이상의 스케일 인수를 통해 설계할 수 있다.

범위성과 함께, 다수 레벨의 보안이 지불 처리 시스템(10) 내부 및 외부의 보안 사건 모두를 다루기 위하여 지불 처리 시스템(10) 내에서 구현될 수 있다. 확장 가능한 설계를 구현함으로써, 부가적인 기능은 상인 및 고객의 관심을 다루기 위하여 이후에 병합할 수 있다.

하나의 예시적인 장치인 도 3을 참조하면, 소규모 거래 프로세서(12), 고객 계좌 프로세서(16) 및 상인 계좌 프로세서(18)가 각 서버(14, 20 및 22)에 포함된다. 이 장치에 있어서, 서버(14, 20 및 22)는 각각 발급 은행, 획득 은행 및 상인 외부의 위치에 위치한다. 그러나, 다른 장치에서, 서버 및 프로세서는 다른 현장에 위치할 수 있다. 더욱이, 이러한 장치에 있어서, 아래에서 상세하게 기술하는 매크로 지불 프로세서(24)는 서버(14) 상에서 실행된다.

소규모 거래 프로세서(12)는 소액 거래를 처리하고, 공인, 포착, 판매, 신용 및 무효 거래를 위한 전통적인 지불 카드 게이트웨이 인터페이스를 제공한다. 소규모 거래 프로세서(12)는 상인의 금융 관리 및 지불 조정, 고객 서비스, 및 마케팅 관리를 위한 소액-거래 데이터를 저장한다. 소규모 거래 프로세서(12)는 또한 고객에게 상세한 자가 서비스 인터페이스를 제공한다. 소규모 거래 프로세서(12)는 상인의 위치에서 실행되도록 설계할 수 있거나, 또는 도면에 도시되는 바와 같이 소규모 거래 프로세서는 상인, 상인의 그룹 또는 FSI를 대표하여 제 3자 프로세서에 의해 실행될 수 있다.

고객 계좌 프로세서(16)는 고객 계좌의 집합에 대한 소규모 거래를 더 큰 거래로 수집한다. 고객 계좌 프로세서(16)는 고객의 자가 서비스를 위한 초기 인터페이스이고, 고객을 자가 서비스를 위한 적절한 소규모 거래 프로세서로 급송하는 고객 서비스를 위한 단일접속체계 포탈(single-signon portal)을 제공한다. 이러한 장치에 있어서, 고객 계좌 프로세서(16)는 발급 은행에서 서버(20) 상에서 실행된다. 대안적으로, 고객 계좌 프로세서(16)는 상인 또는 FSI의 그룹을 위한 제 3자 프로세서에 위치한 서버 상에서 실행될 수도 있다.

상인 계좌 프로세서(18)는 대규모 거래를 위한 지불을 각 개인의 소규모 거래(각각 집합되어 대규모 거래를 생성하는)으로 조정한다. 상인 계좌 프로세서(18)는 금융 산업의 수집된 양도 시스템과 상인의 개인적인 양도 시스템 사이의 인터페이스를 제공한다. 상술한 다른 프로세서와 유사하게 상인 계좌 프로세서(18)는 임의의 형태의 FSI를 대표하여 제 3자 프로세서에 의해 실행될 수 있다. 그러나, 이러한 예시적인 실시예에 있어서, 상인 계좌 프로세서(18)는 획득 은행에 위치한 서버(22) 상에서 실행된다.

매크로 지불 프로세서(24)는, 대규모 지불을 처리하는 제 3자 지불 프로세서에 대한 고객 계좌 프로세서(16)와 상인 계좌 프로세서(18)를 인터페이스 접속시킨다. 이러한 인터페이스를 제공하기 위하여, 매크로 지불 프로세서(24)는 데이터와 메시지를 제 3자 지불 프로세서에 의해 사용되는 하나 이상의 포맷으로 변환시킨다. 예컨대, First Data, Paymentech, Vital 등과 같은 제 3자 지불 프로세서를 위한 변환이 구현될 수 있다. 이러한 특정 장치에 있어서, 매크로 지불 프로세서(24)는 소규모 거래 프로세서(12)를 실행하는 서버(14) 상에서 실행된다. 그러나, 일부 장치에 있어서, 소액지불 프로세서(24)는 다른 위치(예, 상인의 위치)의 서버 상에서 실행될 수 있다.

도 4를 참조하면, 소규모 거래 프로세서(12), 고객 계좌 프로세서(16), 상인 계좌 프로세서(18), 및 매크로 지불 프로세서(24)에 의해 제공되는 기능의 일부를 나타내는 블록도가 제공되어 있다. 이러한 특정 구현에 있어서, 각 프로세서는 일부 유사한 구성요소를 포함한다. 특히, 프로세서(12, 16, 18 및 24) 각각은 거래 처리를 위해 분산된 처리 애플리케이션 프로그램 인터페이스(APIs : application program interfaces)를 구현하는 엔진 구성요소를 포함한다. 부가적으로, 각 프로세서는 거래 데이터를 제공하고 시스템의 상호작용형 사용을 허용하는 사용자 인터페이스와 리포팅 API 구성요소를 포함한다.

도 5를 참조하면, 도 4에 도시된 프로세서(12, 16, 18 및 24) 각각에 포함된 분산된 처리 엔진(26)을 나타내는 블록도가 도시되어 있다. 분산된 처리 엔진(26)은 메시지와 데이터를 다른 프로세서에 송신하고 다른 프로세서로부터 수신하기 위한 확장성 생성 언어(XML : extensible markup language) API(28)와 분산된 거래 라우터(30)를 포함한다. 분산된 처리 엔진(26)은 또한 저가의 거래의 소규모 금액을 수집하기 위한 수집 구성요소(32)를 포함한다. 수집 구성요소(32)는 다양한 유형의 수집을 계산하는 것을 지원할 수 있다. 예컨대, 저가의 거래는 고객 기반으로 수집될 수 있다. 발급 은행을 지원하기 위하여, 저가의 거래는 한명 이상의 상인을 기초로 수집될 수 있다. 분산된 처리 엔진(26)은 또한 개별 거래 및/또는 수집된 거래의 양도 및 조정을 지원하는 구성요소(34)를 포함한다. 부가적으로, 엔진(26)은 거래를 회계감사하고, 거래에 대한 보안과 거래와 관련된 데이터(예, 신용카드 번호, 계좌 번호 등)를 제공하는 것을 지원하기 위한 구성요소(36)를 포함한다.

상술한 구성요소와 함께, 소규모 거래 프로세서(12)에 병합된 분산된 처리 엔진은 추가적인 구성요소를 포함할 수 있다. 예컨대, 사용자에게 지불을 실행하는 다른 방법론을 제공하기 위한 개인화된 지불 구성요소(38)를 포함할 수 있다. 예컨대, 사용자는 선불, 청약, 후불, 사용분만큼 지불, 및/또는 로얄티에 기초한 지불 시스템과 같은 지불 방법론으로부터 선택할 수 있다. 소규모 거래 프로세서(12)와 함께, 지불 처리 시스템(10) 내의 다른 프로세서는 추가적인 구성요소를 포함할

수 있다. 예컨대, 고객 계좌 프로세서(16)는 지불 처리 시스템(10)에 대한 고객의 액세스를 허용하는 구성요소를 포함할 수 있다. 액세스를 제공함으로써, 고객은 하나 이상의 거래를 검토하기 위하여 적절한 소규모 거래 프로세서에 명령할 수 있다.

소규모 거래 프로세서(12)는, 고객의 구매 경험에서 있다하더라도 대체로 작은 변화를 가지고, 지불-카드 게이트웨이로서 상인의 구매 경험에 통합된다. 상인의 구매 경험의 임의의 시점에, 공인 및 양도(또는 거부)를 위해 지불 카드 게이트웨이 인터페이스에 거래가 제공된다. XML 지불 카드 게이트웨이 API를 가리킬 때, 상인은 유사한 지불 카드 거래 정보를 송신하고, 실질적으로 실시간 소액지불 공인 및 양도(또는 거부)를 수신한다. 실질적으로 고객의 구매 경험과 명백한 차이는 없다.

지불 카드 게이트웨이로서, 소규모 거래 프로세서(12)는 다양한 유형의 비즈니스 모델을 위한 지불을 처리할 수 있다. 예컨대, 지불 처리 시스템(10)은 고객이 선호하는 지불 도구(예, 신용카드, 직불카드, Paypal과 같은 지불 중개수단을 통해, 등)를 사용하여 구매를 행하는 것을 허용한다. 더욱이, 지불 처리 시스템(10)이 소규모 거래를 위해 유일하게 효율적인 처리를 제공하지만, 이러한 시스템은 또한 임의 크기의 거래를 처리할 수 있다.

프로세서(12,16,18 및 24)를 통해, 지불 처리 시스템(10)은 AVS, CVV2 검사, 사기행위 체크, 및 3D-Secure 확인과 같은 매크로 지불 거래 입증 처리에서의 정보를 소액지불 공인 제어 흐름에 전달한다. 이러한 정보를 처리하고, 특정 고객이 처리하도록 허용되어야 하는지에 대한 상인 레벨의 결정을 행하는 상인 소프트웨어는 전형적으로 유사한 방식으로 기능을 지속한다.

지불 처리 시스템(10)은, 실시간 소액지불 거래 처리를 실질적으로 네트워크의 변방으로 이동시키는 개방적이고 채택이 쉬운 기술을 제공하고, 동시에 오늘날 제작된 지불 카드 시스템과 완전한 호환성을 유지하면서, 종래 제작의 지불 카드 시스템의 범위를 확장시킨다.

지불 처리 시스템(10)은 다양한 유형의 고객 소프트웨어 시스템으로부터 전자 지불 거래를 수신한다. 예컨대, 거래는, 출석한 상거래의 물리적인 세상의 POS에서 동작하고, 카드제공 거래를 기존 지불 카드 네트워크에 집중시키도록 설계된 POS 디바이스로부터 수신될 수 있다. 출석하지 않은 상거래의 물리적인 세상의 POS에서 동작하고, 카드 제공 거래를 수행하는 가판대 디바이스는 전자 지불 거래를 제공할 수 있다. 이들 디바이스는 전형적으로 복잡한 그래픽 사용자 인터페이스(POS 디바이스와 비교하여)를 지원하는데, 왜냐하면 가판대 디바이스가 출석한 회계원으로부터의 지원이 거의 또는 전혀 없이 고객과 직접 상호 작용하도록 설계되기 때문이다. 지불 처리 시스템(10)은 또한 카드가 없는 거래를 행하는 인터넷 웹사이트 또는 웹페이지(또는 다른 유형의 전자상거래 시스템)로부터 전자 지불 거래를 수신할 수도 있다. 카드가 있거나 카드가 없는 거래의 결합을 수행하는 모바일 상거래 애플리케이션에 대한 모바일 인터페이스는 거래를 제공할 수 있다.

상술한 각 유형의 고객에 대해, 상인 애플리케이션을 지불 처리 시스템(10)에 인터페이스 접속시키기 위한 다양한 구조가 존재한다. 예컨대, 고객측의 맞춤화를 위하여, 고객을 지불 처리 시스템(10)에 적응시키는 비즈니스 로직은 고객 서버 또는 상인과 관련된 서버 내에서 코딩될 수 있다. 고객을 지불 처리 시스템(10)에 적응시키는 비즈니스 로직은 고객과, 시스템을 제어하는 제 3자 사이에 위치한 삽입 서버에서 구현할 수 있다. 고객을 지불 처리 시스템에 적응시키는 비즈니스 로직은 상인의 플러그인을 통해 지불 처리 시스템에 대한 서버측의 모듈(예, 플러그인 모듈)로서 구현할 수 있다. 또한 지불 처리 시스템(10)에 포함된 하나 이상의 프로세서(12,16,18 및 24)는 기존 지불 프로세서의 시스템에 투명하게 통합할 수 있다. 이러한 통합은, 이미 기존 지불 프로세서를 사용하고 있는 상인의 시스템에 대한 최소(또는 거의 없는) 변화를 포함할 수 있다. 일반적으로, 지불 처리 시스템(10)에 포함된 각 유형의 API는 이들 접근법 중 하나 이상을 수용할 수 있다.

지불 처리 시스템(10)에 의해 제공된 개인화된 지불 선택은 전형적으로 4가지 유형의 지불 모델, 즉 사용시마다 지불, 선불, 청약 및 후불을 구현한다. 지불 처리 시스템(10)은 단일 거래 처리 플랫폼 상에서 이들 각각의 모델을 지원한다. 지불 처리 시스템(10)은 또한 상인들이 하나 이상의 모델 하에서 동시에 운영하고 고객이 선호하는 구매 방법을 동적으로 선택할 수 있는 혼합 모델을 지원할 수 있다.

개인화된 지불 선택은 상인에게, 상인이 비즈니스 내의 지불로서 수용할 수 있는 "계좌 유형"의 집합을 한정할 수 있는 능력을 제공한다. 계좌 유형은 상인에게 특정될 수 있는데, 예컨대, 한명의 상인은 다운로드 음악을 위한 청약 계좌를 한정하는 다른 상인과는 달리, 전화 시간 동안 선불 계좌를 한정할 수 있다. 계좌 유형은 기초가 되는 "단위 유형"을 가질 수 있는데, 이러한 단위 유형은, 예컨대 미국 달러, 전화시간의 분, 게임 시간의 분, 또는 막대 사탕과 같은 이러한 유형의 계정 잔액의 단위 유형이다. 단위 유형의 확장 가능 집합은 로얄티 통화의 구현을 허용한다.

계좌 유형의 실제 예인 계좌는 전형적으로 고객이 소유하며, "도구"에 의해 보장된다. 도구는 고객을 확인하는 역할을 하고, 계좌에 대한 액세스를 인증하기 위한 중요한 기초가 될 수 있다. 도구의 예는 신용카드, 직불카드, 선물 카드, RFID에 기초한 스마트 카드, RFID에 기초한 모바일 토큰, 또는 웹사이트 계좌 식별자를 포함한다. 도구는 시스템 내에서 매크로 지불 기금의 원천이고, 실제 이러한 계좌를 위한 고객을 식별하는 유일한 토큰이 될 수 있다. 고객은 선택적으로 로그인(이름, 패스워드)을 가질 수 있고, 그 로그인을 하나 이상의 도구 및 도구와 관련된 계좌와 관련시킬 수 있다. 부록 A를 참조하면, 각 계좌에 포함될 수 있는 하나의 예시적인 집합의 정보가 도시되어 있다.

도 6을 참조하면, 흐름도(40)는, 개인화된 지불 선택을 기술하고, 상인과 소규모 거래 프로세서(12) 사이에서 뒤따르는 API 레벨의 상호 작용을 수반하는 일련의 동작을 나타낸다. 전형적인 거래를 개시하기 위하여, 고객은 도구를 상인에게 제공할 수 있다. 상인은 도구를 소규모 거래 프로세서(12)에 전달한다. 소규모 거래 프로세서(12)는 도구를 확인하고, 그 도구와 관련된 개인화된 지불 프로파일을 리턴시킨다. 프로파일은 도구와 함께 작용하기 위하여 한정된 계좌의 확장 가능 목록을, 새로운 계좌가 도구 프로파일에 어떻게 첨가될 수 있는지를 한정하는 파라미터와 함께 기술한다.

상인은, 고객의 선호도와 상인이 한정된 비즈니스 모델에 맞추어진 지불 경험을 고객에게 제공하기 위하여 프로파일 내의 정보를 사용한다. 고객은 필요대로 구매 거래를 완성하고, 상인은 선택된 지불 계좌에 의해 결정된 고객으로부터 기금을 포착한다. 전형적으로, API는 표준 지불 카드 거래에 대응하는 단일-계좌 구매와 같은 상호작용의 두 가지 스타일을 지원한다. 부가적으로, 복합, 복수 계좌의 구매가 지원될 수 있다. 예컨대, 복수 계좌의 구매는 미국 달러의 거래를 로얄티 포인트의 갱신과 결합시키거나, 또는 일본의 엔 거래를 자유 커피 갱신과 결합시킬 수 있다.

전형적으로, 각 지불 계좌는 구매 API의 공통 집합을 지원한다. 이것은 상인이 고객의 지불 선택과는 독립적인 방식으로 거래를 코딩하는 것을 허용한다. 전형적인 구매 요청의 목록은 부록 B에 도시되어 있다.

"사용시마다 지불" 모델에 있어서, 고객은 종료된 각 거래에 대해 지불한다. 상인의 관점으로부터, 이러한 모델은 유리한데, 왜냐하면 사용시마다 지불 모델이 고객 중에서 상당히 높은 취득율(take rate)을 제공하기 때문이다. 이러한 모델의 단순한 형태는 고객으로 하여금 상인의 제품을 구입하도록 조장하고, 신청은 상인의 제품에 대한 단위 가치 점수를 확립한다. 하지만, 사용시마다 지불 모델은 또한 상인에 대한 일부 도전을 포함한다. 예컨대, 고객이 "소규모 금액"의 고객이라면, 관계는 간혹 수익이 없을 수 있다. 거래 비용은 상당히 높을 수 있고, 관계는 간혹 익명으로 이루어진다. 사용시마다 지불 계좌에 대해 API 구매 요청에 부가하여, 지불 처리 시스템은 또한 두 가지 추가 요청(부록 C에 기술됨)을 지원할 수 있다.

"선불" 모델에 있어서, 고객은 거래 집합을 미리 구매한다. 고객이 상인과 함께 하나 이상의 거래에 관계하기 때문에, 상인의 관점으로부터 이러한 모델은 유리할 수 있고, 간혹 초기 관계를 넘을 수 있다. 고객에 대한 신용을 넘어설 위험은 낮아지는데, 왜냐하면 고객이 미리 지불하기 때문이다. 선불은 수량 할인, 선물 카드 및 계좌, 침대 계좌, 금융소외자에 도달하는 신청을 포함하는 관측 활동에 대한 플랫폼을 제공한다. 부가적으로, 선불 충전(top-up) 금액은 많은 소액 거래를 통해 거래 비용을 상환하도록 조정할 수 있다. 이러한 장점과 함께, 선불 모델은 또한 상인에 대한 도전을 부가한다. 예컨대, 취득율 대 사용당 지불이 낮은 비율은 사용당 지불을 올렛시키기 위하여 실질적인 판매 노력을 필요로 할 수 있다. 다른 잠재적인 도전은 수량 할인과 같은 동기를 제공할 필요가 있다. 상표가 붙은 선불 카드의 발급 비용은, POS에서 카드 발급 및 비용 청구를 위해 2 내지 3 달러, POS에서 카드 선반에 배포를 위해 15내지 40%, 2%의 거래 마다의 비용과, 고객 지원비용이다. 주에서 부가한 미청구 선불 기금의 복귀와 같이 새로 만들어지는 법규에 따르는 비용은 또 다른 도전이다. 부록 D에 기술된 바와 같이, 구매 요청에 부가하여 선불 계좌는 부가적인 요청을 지원한다.

"청약" 모델에 있어서, 고객은 지정된 시간 기간 동안 거래 집합을 미리 구매할 것을 약속한다. 상인의 관점으로부터, 이러한 모델의 일부 장점은 청약에 의한 구매에 대해 고객의 승낙이 상인에 대한 깊은 레벨의 약속(상인과 고객 사이의 더 깊은 관계를 초래할 수 있는)을 나타낸다는 사실을 포함할 수 있다. 이러한 고객은 상인을 위한 수입을 순환 발생시키는 원천이 될 수 있다. 고객에 대한 신용을 넘어서는 위험은 낮아진다.

청약 모델은 또한 상인에 대한 도전을 야기한다. 예컨대, 지속되는 금융 약속은 취득율을 낮출 수 있다. 취득율을 높이기 위하여, 상인은 제품 신청에 대한 상당한 할인에 의지할 수 있다. 청약 비즈니스 모델은 모든 제품 유형에 적용할 수 있는 것은 아니다. 부록 D에 나타난 바와 같이, 청약 계좌는 일부 추가적인 유형의 요청과 함께, 사용시마다 지불 요청에 의해 지원되는 요청을 사용할 수 있다.

"후불" 또는 "청구" 모델에 있어서, 상인은 사전 지불의 안전에 대한 보장 없이 고객의 거래를 수용한다. 지불을 안전하게 하는 것이 아니라, 상인은 대신에 주기적으로 거래에 대해 고객에게 청구한다. 상인의 관점에서, 이러한 모델이 유리한데,

왜냐하면 고객이 간혹 자유롭게 소비하고, 상인과 많은 수의 거래를 수행할 수 있기 때문이다. 고객은 상인에 대한 수입을 순환 발생시키는 원천이 될 수 있다. 이 모델은 상인에게 있어서 일부 고객이 그들의 계좌를 양호한 지위로 유지하는데 상당히 높게 동기 부여될 수 있다고 기대할 수 있는 서비스 신청(예, 주거 전화 또는 전력 서비스)에 맞추어진다.

상인에 대한 후불 도전은 미지불의 실질적인 위험에 대한 큰 신용 위험을 떠맡는 상인을 포함할 수 있다. 그러나, 이러한 위험은 후불 청구 기간을 비교적 짧게 유지함으로써 경감될 수 있다. 부가적으로, 이러한 모델은 많은 제품 항목에 대해 운영되는 것은 아니다. 후불 계좌는, 부록 E에 열거된 일부 부가적인 요청을 포함하여, 사용시마다 지불 요청에 의해 지원되는 모든 요청을 지원한다. 더욱이, 부록 F는 구매 및 계좌 API에 의해 사용되는 다양한 논의를 나타낸다.

도 7을 참조하면, 소규모 거래 프로세서(44,46), 고객 계좌 프로세서(48), 지불 처리 시스템(10)의 일부 실시예에 포함될 수 있는 매크로 지불 프로세서(50)의 상호작용을 설명하기 위한 블록도(42)가 도시되어 있다. 상술한 바와 같이, 상대적으로 저가의 거래를 하나의 큰 거래로 수집하는 것은 거래 비용을 줄이는 방법론을 제공한다. 일반적으로, 거래 수집은 많은 소규모 소액-거래를 하나의 대규모 매크로-거래로 전환하는 것을 포함한다. 수집함으로써, 매크로-거래를 처리하는 것과 관련된 고정 비용은 다수의 소액-거래 위로 분산될 수 있다. 도면에 도시된 바와 같이, 각 거래는 상인이 경험하는 3가지 상태를 통해 도시되는데, 이들 상태는, 회원 지불 증명서를 검사하고 거래에 필요한 기금을 예약하는 공인(또는 auth), 회원과의 거래를 완성하는 포착(또는 capt), 및 금융 기관을 지불에 의해 선회되는 거래에 조화되게 하는 마지막 양도(Settle) 메시지이다.

이러한 예에 있어서, 소규모 거래 프로세서(44,46)는 상인의 시스템으로부터 지불 카드 공인, 포착, 판매, 신용 및 무효 소액-거래의 스트림을 수신한다. 하지만, 다른 장치에서, 소규모 거래 프로세서(44,46)는 다수의 상인으로부터 소액-거래를 수신할 수 있다. 각 소규모 거래 프로세서(44 및 46)는 소액-거래를 더 적은 수의 매크로-거래로 수집하기 위하여 특정 지불 카드와 관련된 고객 계좌 프로세서(48)와 협력한다. 고객 계좌 프로세서(48)는 차례로 대규모 거래를 나타내는 데이터를 제 3자 지불 네트워크로 전달하기 위하여 매크로 지불 프로세서(50)를 사용한다. 이러한 특정 장치에 있어서, 상인 계좌 프로세서는 실시간 거래 흐름에 포함되지 않는다.

거래 수집의 비용 이익을 나타내기 위한 도시에로서, 상기 거래의 시퀀스가 순익을 내어 0.99 달러 비용에 대해 5개의 소액-거래를 야기했다고 간주한다. 만약 매크로-거래 레벨에서 거래 처리 수수료가 게이트웨이에 대해 0.10달러, 획득 은행에 대해 0.10달러, 그리고 교환을 위해 0.10달러 + 2%라면, 5개의 0.99달러 매크로-거래는 수수료로 1.60달러, 즉 거래 금액의 32%를 필요로 할 것이다. 대조적으로, 거래마다 0.05달러를 청구하는 지불 처리 시스템에 5개의 거래가 제공된다면, 5개의 소액-거래에 대한 전체 수수료는 0.55달러, 즉 거래 금액의 11%가 되어, 1.05달러, 즉 21%를 절약할 것이다.

수집 엔진을 병합하는 프로세서(44,46,48 및 50)를 구현함으로써, 소규모 거래 비즈니스 모델을 가능케하는 정책 집합이 구현된다. 수집을 구현함으로써 상인의 수익성은 거래 비용의 감소를 통해 증가할 수 있다. 그러나, 단지 비용을 최소화하는 것보다는, 일부 장치에 있어서, 수집은 다수의 인자의 균형을 이루는 방식으로 구현된다. 예컨대, 줄어드는 거래 비용(수집 시간을 증가시킴으로써) 사이의 절충을 수반하는 인자는 현금 흐름의 지연 및 사기행위 위험 회피와 같은 다른 인자의 균형을 이룰 수 있다. 실질적으로 이들 인자(예, 사기행위 및 사기행위 비율에 대한 상인의 비용을 고려하는)간의 절충을 최적화시킴으로써, 수집은 (예, 현금 흐름 지연, 위험이 있는 거래에 노출, 증가된 고객 서비스 비용 등을 감속시켜) 실질적으로 부정적인 충격이 없이 제공될 수 있다.

전형적으로, Visa 및 MasterCard와 같은 조합이 그들의 회원 획득 은행이 그들의 발급 은행에 지불하도록 요구하는 비용은 교환 분류에 따라 다르다. 교환 분류는 많은 규칙을 수반한다. Visa 및 MasterCard는 다양한 비율과 규칙을 갖는 80가지 이상의 교환 등급을 한정한다. 교환 분류는 거래별 기반으로 할당되고, 많은 인자에 의해 결정될 수 있다. 예컨대, 상인에 관련된 일부 인자는 상인의 비즈니스 범주(MCC 코드), 상인이 카드가 존재하는 비즈니스 또는 카드가 없는 비즈니스를 갖는지, 카드가 없는 비즈니스가 메일 순서/전화 순서 또는 전자 상거래인지, 출석하지 않은 판매 상황이 존재하는 지, 및/또는 조합이 이것을 특별 비율을 적용할만한 "새로 생성되는" 시장으로 간주하는 지를 포함할 수 있다. 다른 분류 인자는 사용된 고객의 지불 도구(예, 신용카드, 직불카드, 회사카드, 구매카드, 특별 상표가 부착된 카드, EBT 카드, 외국 발급자로부터의 카드, 등)와 관련될 수 있다. 거래의 거래-시간 세부사항 또한 하나의 인자가 될 수 있다. 예컨대, 이러한 인자의 예는, 유효한 카드 승인, 서명 또는 서명 지불 대 PIN 지불이 존재하는지, AVS 일치, CVV 일치 또는 Verified-By-Visa/Secure Code가 일치하는지, 주어진 간격 동안 거래가 충분히 적은지, 및/또는 거래에 대해 1달러 사전-공인이 존재하는 지를 들 수 있다. 유사하게, 거래의 사후-거래 세부사항은 인자가 될 수 있다. 예컨대, 공인과 포착 사이, 포착과 양도 사이, 또는 공인과 양도 사이의 경과 시간은 포착 금액과 동일한 공인 금액이거나, 또는 양도시 제공된 고객의 서비스 전화 번호 또는 웹사이트 주소와 같은 세부사항이다.

상인의 "최상"의 교환 분류의 요건 모두가 부합된다면, 거래는 전형적으로 "완전히 자격이 있다"라고 말할 수 있다. 교환 분류의 요건이 부합하지 않으면, 거래는 새로운 "중간-자격"의 교환 등급(현재, Visa EIRF 또는 MasterCard Merit 1)으로 등급이 낮아진다. 만약, 중간 자격 등급의 요건이 부합되지 않는다면, 거래는 "자격 없음"(현재, Visa Standard 또는 MasterCard Standard)으로 등급이 낮아진다. 특정 교환 등급은 중간의 중간-자격의 낮은 등급(예컨대, MasterCard Key Entry로)의 등급 강등은, 만약 거래에서의 유일한 결함이 손상된 트랙 승인이었다면, Merit 1 이전에 일어날 수 있다)을 가질 수 있다.

상인의 완전한 자격이 있는 교환 범주는 수집을 지원하기 위한 입력의 한 집합이다. 단일 라인의 비즈니스의 상인은 일반적으로 단일 교환 분류를 갖는다. 보다 더 복잡한 비즈니스를 갖는 사람들은 어떤 비즈니스 라인이 거래를 행하는 지에 따라 수 개의 분류를 가질 수 있지만, 전형적으로 이들 비즈니스 라인은 다른 상인 계좌를 갖는다. 지불 처리 시스템(10)의 수집 능력은 각 비즈니스가 수집 도중에 사용되는 별도의 프로파일을 유지하는 것을 허용함으로써 복잡한 비즈니스를 수용한다.

수집의 비용 이점은 고객의 구매 거동에 대한 두 가지 기본 측정값, 즉 얼마나 많이 구매하는 지, 그리고 얼마나 자주 구매하는 지에 의해 관리된다. 각 구매에 대한 고객의 소비량을 나타내는 구매량은 P_i 로 표시할 수 있고, 어떤 상인측에서 어떤 고객에 관한 구매 간의 시간적인 양을 나타내는 구매 도달 사이의 시간은 T_i 로 표시된다. 상인측에서 고객의 구매 거동은 금액과 도달 간의 시간의 시퀀스로 보여질 수 있다: $P_1...T_2...P_2...T_3...P_3...T_4...P_4...T_5...P_5$.

수집은, 매크로-공인과 매크로-포착/매크로-양도 사이의 타이밍을 최적화시킴으로써, 교환 분류와 더 많은 소액-거래를 기존의 "수집 윈도우" 내에 위치시키는 이익 사이의 절충을 실질적으로 최적화시킨다. 더욱이, 수집은 교환 등급 강등의 잠재적인 비용 충격에 대한 수집의 이익을 실질적으로 최적화시킨다.

부록 G를 참조하면, 상인이 수집을 제어하기 위하여 설정할 수 있는 파라미터를 기술하는 표가 제공된다. 지불 처리 시스템(10)은 상인에 의해 설정된 파라미터의 제어 하에서 거래별 기반의 수집을 실질적으로 최적화시킨다. 일부 장치에 있어서, 이들 파라미터는 복잡한 것으로 간주되지만, 디폴트 설정은 사용자가 수집 파라미터의 이해를 학습하거나 얻는 것을 필요로 하지 않고도 실질적으로 최적화된 수집 결과를 제공할 수 있다. 전형적으로, 지불 처리 시스템(10)은 조합 규칙을 따르는 단일 상인의 수집을 유지하면서, 조합 컴플라이언스 가이드라인 내에서 동작하는 수집을 수행한다.

도 8을 참조하면, 수집을 통해 지불 처리 시스템(52)은 보편적으로 많은 고객, 상인 및/또는 지불 공급자를 통해 저가의 거래를 수집할 수 있다. 지불 처리 시스템(52)은 보안 지불 처리 시스템을 유지하면서, 대부분의 소액-지불 처리를 지불 네트워크 코어로부터, 소규모 거래 프로세서(54,56), 고객 계좌 프로세서(58), 및 소액지불 프로세서(60)와 같은 분산된 프로세서로 이동시킴으로써 거래 수집을 확장시킨다.

지불 처리 시스템(52)은, 안전한 중앙집중 제어를 유지하면서, 지불 처리의 대규모 분산을 허용하는 암호학적으로 안전한 선택(CSS : cryptographically secure selection) 모듈을 포함할 수 있다. 이러한 장치에 있어서, CSS 모듈은 시스템 동작을 2개의 층으로 분리시킨다. 제 1층은 분산된 실시간 소액-지불 처리층으로, 여기에서 상인과 고객의 소액-지불 거래는 소규모 거래 프로세서(예, 소규모 거래 프로세서(54))에 기록된다. 제 2층은 비실시간으로 동작하고, 기존의 지불 네트워크에 인터페이스 연결되는 매크로-지불 및 분산된 제어 층이다.

전형적으로, 소액-지불 및 매크로-지불 층은 서로 연결된다. 예컨대, 실시간 거래를 제어하기 위한 정책은 소규모 거래 프로세서와 관련된 소액지불 층에 의해 (필요한 대로) 페치(fetch)되고, 그 층에 의해 저장된다. 이들 정책은 예컨대, 다수의 소액-지불 거래가 실시간 사기행위 검사결과를 전달하는 한, 이들 거래를 공인할 수 있다. 전형적으로, 소액-지불 층은 요약 양도 정보를 매크로-지불 층에 다시 전달하지만, 세부 소액-지불 기록은 비용이 낮은 소규모 거래 프로세서에 저장된다.

보안 제어를 강화하기 위하여, 지불 처리 시스템(52)은 암호학적으로 안전한 선택 모듈에 기초하여 프로토콜의 회계감사를 실현한다. 이러한 프로토콜을 사용하여, 매크로 지불 층은 상세한 소액-거래의 작은 부분집합을 시험할 수 있고, 적절한 지불 처리가 모든 소액-거래에서 발생하는 것을 보장할 수 있다. 이것은 비용 감축을 제공하면서 보안을 유지한다.

지불 처리 시스템(52)은 크기조정이 가능하고(scalable), 상당히 안전하게 동작하도록 설계된다. 시스템 내에서 실행되는 원리와 동작의 역할은 주의깊게 분할된다. 일부 장치에 있어서, 구성요소는 연합 공개키에 기초한 인증 시스템에 의해 인증된다. 은밀하게 유지되도록 지정된 정보는 송신되고 저장될 때 암호화되고, 인증할 필요가 있는 정보는 디지털 서명된다. 시스템은 증명서에 대해 그 사용을 제한하면서 엄격하게 제어하고, 증명서는 가벼운 철회 처리를 통해 철회할 수 있다.

암호학적으로 안전한 선택 과정은 계산을 지불 네트워크 중심으로부터 분산된 소규모 거래 프로세서(예, 소규모 거래 프로세서(54 및 56))로 이동시킴으로써 비용 이점을 제공한다. 지불 시스템의 중앙에서 지불을 처리하는 것은 전형적으로 상당히 중앙집중식 계산 및 통신 하부구조를 호출할 수 있는데, 이는 오히려 더 비싸질 수 있다. 소규모 거래 프로세서에서의 지불 처리는 상당히 값싼 상품의 하드웨어에서 수행될 수 있고, 통신은 전자 상거래 웹사이트에 국한될 수 있다. 암호학적으로 안전한 선택 모듈을 통해, 지불 처리 시스템(52)은 낮은 비용의, 크기 조정가능한 수집 하부구조를 제공하는데, 이 하부구조는 많은 수의 거래를 낮은 비용으로 처리할 수 있다.

전형적으로, 상인은 그들의 비즈니스를, 그들의 고객과 상호작용하는 레벨인 소액-거래 레벨로 관리한다. 지불 처리 시스템(52)은 제 3자 지불 네트워크 상호작용을 최적화하도록 시도하여, 일괄적인 매크로-레벨 거래에 관해 자금이 상인에게 흐르도록 한다. 시스템의 양도 및 조정은 자금 흐름을 일괄적인 매크로-거래로부터 개별적인 소액-거래로 맵핑한다. 양도 층은 American Express가 지불을 보류하는 동안 양도된 거래의 부분집합에 대해 Visa가 지불하는 부분 양도를 포함하는 다양한 인자를 처리할 수 있다. 발급 은행이 특정 고객의 불만과 관련된 상인과의 비용청구 처리를 개시할 수 있을 때의 비용청구와 같은 비용청구가 처리될 수 있다. 처리되는 다른 인자는 획득 은행 레벨과 소규모 거래 프로세서의 레벨 모두에서 상인 그룹 사이의 자금의 분할이다.

도 4를 다시 참조하면, 소규모 거래 프로세서(12)는, 지불 처리 시스템(10)이 조합에 의해 구동되는 중앙집중식 지불 처리 시스템과 관련된 규칙을 따르는 것을 보장하도록, 회계감사 및 제어 모듈(62)을 포함한다. 조합은 거의 모든 지불이 신뢰성이 있는 "제 3자 프로세서"에 의해 검사된다고 간주할 수 있는 컴플라이언스 규칙을 한정한다. 종래의 일부 시스템은 매크로-거래의 상당히 큰 비율을 검사할 수 있지만, 종래의 시스템이 매크로-거래의 큰 비율을 검사하도록 요구되었다면, 소액-거래를 처리하는 비용은 매크로-거래를 처리하는 비용과 동일할 것이고, 상인은 소규모 거래 시장에 진입할 수 없을 것이다.

회계감사 및 제어 모듈(62)은 회계감사 당사자가 모든 소액-거래를 검사하는 것을 필요로 하지 않고도, 소액-거래 처리 컴플라이언스에서 높은 레벨의 확신을 제공할 수 있다. 회계감사 및 제어 모듈(62)은, 2002년 4월 17일 출원되었고, 그 내용이 본 명세서에서 참조로서 병합된 PCT 특허출원(PCT/US02/12189호)에 기술된 암호학적으로 안전한 선택의 기술을 구현한다. 상기 PCT 특허출원의 내용은 부록 H에 제공된다. 암호학적으로 안전한 선택은 소액-거래의 부분집합이, 회계감사관이 전체 집합에 대해 결과를 신뢰할만하게 외삽할 수 있도록 하는 방식으로, 회계감사되는 것을 허용한다. 회계감사 및 제어 모듈(62)은 소규모 거래 프로세서(12)에서 작업의 대략 95%를, 그리고 다른 곳에서 작업의 대략 5%를 행하는 비용 부분으로 감시하는 포괄적인 컴플라이언스의 이익을 제공한다.

다양한 사건이 회계감사 및 제어 모듈(62)에 의해 검사된다. 예컨대, 이러한 모듈은 양도 일괄처리가 청구된 금액에 더해지는 지, 청구된 모든 거래가 공인되었는 지, 또는 이러한 일괄처리에 임의의 복제물이 존재하는 지를 검사할 수 있다. 더욱이, 회계감사 및 제어 모듈(62)은 교환 등급에 의해 요청된 각 소액-거래에서 AVS 일치, CVV 일치, Verified-By-Visa 일치의 적절한 정도가 존재하는 지를 결정할 수 있다. 교환 등급에 의해 지정된 경계 내에서 공인, 포착 및 양도 사이의 차이명과 같은 다른 사건이 검사될 수 있다. 회계감사 및 제어 모듈(62)은 확장가능하고, 다른 사건이 장래에 회계감사 되도록 허용한다.

도 9를 참조하면, 회계감사에 대한 초기 조건은, 상인이 그들의 거래에 시간 스탬프가 있는 공개 키 서명을 사용하여 서명함으로써 거래를 행할 때 구축된다. 공개-키 서명은 계산상 비용이 많이 든다. 머클 트리 기술은 N개의 공개 키 서명과 N개의 안전한 일방향 해쉬의 묶음을 메시지당 1개의 공개 키 서명, $2 \times N - 1$ 해쉬, 및 해쉬크기 $\times 1gN$ 바이트 이상으로 대체한다.

도면을 참조하면, 본 예에서, 상인에 의해 디지털 서명된 거래를 나타내는 머클 트리(64)($N=8$)가 도시되어 있다. 예컨대, T_{010} 과 $SIG_m(T_{010})$ 은, 모두 머클 트리에서 자매 해쉬값의 체인(v_{011}, v_{00}, v_1, v)을 갖는, 동일한 거래(T_{010})과 머클 트리의 뿌리의 디지털 서명($SIG_m(v)$)과 동등하다. 수령인은 $SIG_m(v)$ 를 검사하고, $v=H(H(v_{00}, H(T_{010}), v_{011}), v_1)$ 를 검사하는데, 이는 상인이 디지털 서명($SIG_m(T_{010})$)을 생성할 수 있었음을 증명한다, 즉 머클 트리 서명을 생성할 수 있었다면,

T_{010} 과 같은 특정 거래에 직접 서명할 수 있었을 것이다. 머클 트리 기술은 트리 내의 모든 N 개 항목에 걸쳐 하나의 서명($SIG_m(v)$)을 공유하고, 암호학적으로 안전한 해쉬(H)가 공개 키 서명보다는 계산하는데 실질적으로 값싸기 때문에 계산 비용이 대략 N 의 인자만큼 감소한다.

머클 트리 기술은 전형적으로 크기 N 의 묶음에서 서명의 묶음 처리를 호출한다. 지불 처리 시스템(10)은 수집 및 양도 방법론의 일부로서 소액-거래의 묶음을 제공하여, 이러한 기술이 애플리케이션의 거동을 변경하지 않고도 이들 개념 내에서 자연적으로 적용되게 된다. 머클 트리에서 각 소액-거래의 서명은 트리의 다른 요소를 페치(fetch)하지 않고도 개별적으로 검사할 수 있다. 이러한 기술은 실질적으로 공개 키 서명의 수를 상당히 감소시키지만, 대략 비대칭 암호의 신뢰도-범위성 장점 모두를 유지한다.

소규모 거래 프로세서(12)에서 시작하여, 소액-거래(T)의 포착 시간에, 소규모 거래 프로세서는 각 비트가 균일하게 $\{0,1\}$ 로 그려지는 상태로, 길이(n)의 무작위 비트 스트링(R)을 생성한다. 소규모 거래 프로세서(12)는 쌍(T,R)을 머클 트리 낙엽 서명($H_j(T,R)$)을 계산하는 머클 트리에 더한다. 주기적으로, 소규모 거래 프로세서(12)에 있어서의 상인의 소액-거래는 양도되고, 양도 시간 스탬프(S)로 타임 스탬핑되는데, 이 시간 스탬프(S)는 고객 계좌 프로세서(16)와 상인 계좌 프로세서(18)에 의해 생성되고, 머클 트리의 뿌리를 상인의 공개 키 서명으로 서명함으로써 완전한 머클 트리가 생성되어 실행된다. 상부 레벨의 머클 트리 서명($SIG_m(v)$)은 양도 전체값과 함께 고객 계좌 프로세서(16)와 상인 계좌 프로세서(18)로 전달된다. 이러한 서명은 묶음 내의 소액-거래 각각을 수행하고, 실질적으로 장래의 회계감사를 위하여 이들을 "고정"시킨다.

고객 계좌 프로세서(16) 또는 상인 계좌 프로세서(18)에 의한 후속적인 회계감사는 회계감사 질문(예, 특정한 날에 Visa 카드 거래의 전체 금액은 얼마나 되는지?)에 답하기 위하여 소규모 거래 프로세서(12)에 요청을 보내는 프로세서를 포함할 수 있다. 요청에 따라, 고객 계좌 프로세서(16) 및/또는 상인 계좌 프로세서(18)는 소규모 거래 프로세서가 계산한 결과에 대한 유효성의 증거로서 소규모 거래 프로세서(12)에 의해 리턴되어야 하는 소액 거래 회계감사 집합의 부분을 지정할 수 있다. 고객 계좌 프로세서(16) 및/또는 상인 계좌 프로세서(18)는 각 거래와 관련된 무작위 비트 스트링(R)에 적용될 선택 표준 쌍(마스크, 일치)의 목록을 제공함으로써 이러한 집합을 지정할 수 있다. 선택 표준 마스크 및 일치는 길이(n)의 비트 스트링이고, 마스크에 대한 R 의 비트-레벨 "AND"가 목록 내의 임의의 표준에 대한 일치와 동일하다면, 소액-거래가 복귀될 것이다. 이러한 메커니즘은 회계감사의 사실을 지원하는 회계감사된 소액-거래의 부분(p)의 선택을 허용하는데, 여기에서 p 는 이진 부분으로서 p 의 표현에서 1에 대응하는 1비트의 수로 마스크의 시퀀스를 선택함으로써 임의적으로 밀접하게 어림 계산된다.

소규모 거래 프로세서(12)는 회계감사 요청을 실행할 수 있고, 프로세서에서 각각의 소액-거래, 예컨대 특정한 날에 Visa-카드 거래의 합을 시험함으로써, 회계감사 질문에 대한 정확한 답을 리턴시킨다. 이러한 답에 따라, 소규모 거래 프로세서(12)는 이러한 선택 표준과 일치하는 소액-거래의 부분집합을 리턴시킬 수 있고, 이러한 부분집합은 소규모 거래 프로세서가 제공하는 답에 대한 증거로서 작용할 수 있다.

고객 계좌 프로세서(16) 및/또는 상인 계좌 프로세서(18)는, (a) 리턴된 소액-거래가 지불 처리 시스템(10)에서 이전에 행해진 것과 동일한 것임을 보장하기 위하여 이들 거래 상에서의 머클 서명을 확인함으로써, 그리고 (b) 회계감사된 집합 내의 결과를 $1/p$ 의 인자만큼 상승시키고, 이들 결과가 소규모 거래 프로세서(20)에 의해 리턴된 정확한 결과에 근접한지를 알아보기 위하여 시험함으로써, 소규모 거래 프로세서(12)의 결과를 확인한다. 만약 상승된 회계감사 결과가 근사적으로 충분히 접근하지 않았다고 판정되면, 고객 계좌 프로세서(16) 및/또는 상인 계좌 프로세서(18)는 새로운 선택 표준으로 동일한 요청을 보내면서 회계감사를 반복한다. 이러한 처리는 고객 계좌 프로세서(16) 및/또는 상인 계좌 프로세서(18)가 만족되거나, 또는 소규모 거래 프로세서(12)가 완전하게 회계감사 되었다고 결정할 때까지 반복될 수 있다. 성실한 상인에 대해, 통계는 고객 계좌 프로세서(16) 및/또는 상인 계좌 프로세서(18)가 합리적인 금액의 시간 내에서 부분 회계감사에 만족할 수 있음을 보장한다.

지불 처리 시스템(10)은 크기조정 가능하고 상당히 안전한 동작을 위해 설계된다. 시스템 내에서 실행되는 원리와 동작의 역할은 주의 깊게 분할된다. 신용 연합 구성요소는 지불 처리 시스템(10)을 위한 분산된 검증 당국이다. 이는 지불 처리 시스템(10) 내의 할당된 역할 내에서 시스템의 각 구성요소를 공인하기 위하여 공개 키 또는 다른 기술을 사용한다. 구성요소는 연합된 공개키에 기초한 공인 시스템에 의해 공인된다. 전형적으로, 비밀로 유지할 필요가 있는 정보는 송신되고 저장될 때 암호화된다. 따라서, 관리 경계에 걸쳐서 공인이 필요한 정보는 디지털 서명되고 회계감사될 수 있다. 지불 처리 시스템(10)은 증명서를 이들의 사용을 제한하면서 제어하고, 모든 증명서는 전형적으로 가벼운 철회 과정을 통해 철회할 수 있다.

전형적으로, 지불 처리 시스템(10)은 계좌 번호, CVV 코드, 트랙-1 또는 트랙-2 데이터를 소규모 거래 프로세서(12), 고객 계좌 프로세서(16) 또는 상인 계좌 프로세서(18)에 저장하지 않는다. 오히려, 계좌 번호의 일방향 해쉬가 데이터베이스에 저장된다. 일방향 해쉬는 또한 거래 수집을 위한 기초로서 사용된다. 지불 처리 시스템(10)에 있어서, 계좌 번호는 AUTH 거래 도중에(또는 SALE 거래의 AUTH 상태 도중에), 거의 실시간으로 사용할 수 있다. 만약 AUTH가 지속되면, 계좌번호는 추가 매크로-지불 시스템의 상호작용(-후속 포착, 신용 또는 적용한 특정 AUTH를 지정하기 위하여 AUTH를 통해 REFID가 리턴된 무효한 사용)을 위해 필요하지 않다. 만약 AUTH가 어떤 이유로 실패한다면, 시스템의 AUTH 프로토콜은 다시 새로운 AUTH를 시도하기 위한 계좌 번호를 제공하기 위하여 호출자를 필요로 할 것이다.

지불 처리 시스템(10) 내의 서버는 전형적으로 계좌번호, CVV 코드, 트랙-1, 또는 트랙-2 데이터를 저장장치에 저장하지 않는다. 부가적으로, 이러한 데이터는 전형적으로 데이터베이스에 기록되지 않을 뿐만 아니라, 새로운 텍스트로서 어떠한 서버 로그 파일에도 기록되지 않는다. 일부 장치에 있어서, 지불 처리 시스템(10)은 거래를 계좌번호와 만료일의 암호학적으로 안전한 일방향 해쉬 기능에 대해 일치시킴으로써 거래를 수집한다. 해쉬를 계산하기 위한 방법론은 SHA-1 암호학적으로 안전한 메시지의 요약 기능과 같은 기능을 구현할 수 있다.

상인 고객 서비스 목적을 위해, 지불 처리 시스템(10)은 새로운 텍스트에 계좌번호의 마지막 4자리 보유할 수 있다. 고객 서비스 랩(rebs)은 마지막 4자리를 볼 수 있고, 이들 자리와 일치하는 거래와 다른 거래 특성을 검색할 수 있다. 지불 처리 시스템(10)은 또한 상인 고객 서비스 표본이 신용카드 번호의 정확한 일치를 통해 거래를 검색하는 것을 허용한다. 내부적으로, 이러한 데이터베이스의 검사는 계좌번호의 일방향 해쉬에 기초하는데, 왜냐하면 계좌번호가 전형적으로 저장되지 않고, 일방향 해쉬로부터 잘 회복될 수 있기 때문이다.

지불 처리 시스템(10) 내의 매크로 지불 프로세서(24)는 소규모 지불 처리 서비스를 MPP 플러그-인을 통해 제 3자 지불 프로세서에 적응시킨다. 제 3자 지불 프로세서에 의해 계좌번호가 AUTH 시간에만 제공되도록 하는 AUTH 및 CAPT 처리가 지원될 때, MPP 플러그-인은 소규모 거래 프로세서(12)와 고객 계좌 프로세서(16)처럼 동작한다. 특히, 계좌번호는 AUTH 도중에 안전하게 지불 프로세서에 전달되고, 전형적으로 저장 장치에 보유되지 않는다. 그러나, 일부 제 3자 지불 프로세서가 각 CAPT 상호작용시에 제공될 계좌번호를 필요로 한다. 이러한 프로세서를 지원하기 위하여, 프로세서를 위한 MPP 플러그-인은 AUTH 시간에 계좌번호와 만료일을 암호화하고, 해독된 카드번호와 만료일을 포착 또는 신용 시간에 다시 제공한다.

일부 장치에 있어서, 암호 및 키 관리는 n-Cipher n-Shield와 같은 하드웨어 보안 모듈을 사용하여 구현된다. 이러한 시스템은 또한 AES-128과 같은 강력한 암호를 사용한다. 암호화된 카드번호는 전형적으로 AUTH와 CAPT 사이의 윈도우로서 한정될 수 있는 시간 기간 동안에만 유지된다. 현재의 신용카드 규칙은 이러한 윈도우를 대략 7일 내지 30일로 한정한다. 이러한 기간 이후, 지불 처리 시스템(10)은 암호화된 계좌정보를 삭제한다. 키는 하드웨어 보안 모듈에 의해 제공된 보안 설비와 같은 보안 설비를 사용하여 관리된다. HSM은 다수 층의 보안과 보안 키 관리 프로세서를 제공한다.

전형적으로, 소규모 지불은 상대적으로 저가에서 상대적으로 많은 금액이 발생한다. 지불 처리 시스템(10)은 상당히 크기 조정이 가능하고, 상당히 분산된 수 천 개의 소규모 거래 프로세서, 고객 계좌 프로세서, 상인 계좌 프로세서, 매크로-지불 프로세서, 발급 은행 서버, 획득 은행 서버 등을 포함하도록 크기를 조정할 수 있다. 지불 처리 시스템(10)은 또한 1000x를 넘는 범위성에 대해 크기를 조정할 수 있는데, 이러한 범위성은 점진적으로 크기 조정이 가능하다. 예컨대, 10-20x의 크기 조정 인자는 대규모 크기조정 인자(예, 100-200x, 1000-2000x 등)를 위해 시스템의 크기 조정에 앞서서 구현할 수 있다.

크기조정을 통해, 지불 처리 시스템(10)은 수 천 개의 분산된 서버 모두에서 거래 처리 고정을 투명하게 분할할 수 있다. 이러한 분할은 다수의 레벨로 발생한다. 예컨대 기능 분할에서는, 지불 처리 시스템(10)이 거래 처리의 다른 양상을 분리하도록 설계되어, 거래 처리가 별도의 서버 상에서 안전하고 효율적으로 실행될 수 있게 한다. 소액-거래 처리는 수집된 매크로-거래의 처리로부터 분리될 수 있다. 유사하게, 소액-거래 리포팅이 매크로-거래 리포팅으로부터 분리될 수 있다. 암호화될 필요가 있는 회원 데이터에 대한 장기간의 액세스를 필요로 하는 시스템 기능은, 그러한 액세스를 필요로 하지 않는 기능으로부터 분리된다. 이러한 구조는 고객 서비스 목적을 위한 고객의 안전한 인증을 고객의 서비스 데이터를 포함하는 소액-거래 기록으로부터 분리시킬 수 있다.

구성 경계 분할을 위하여, 지불 처리 시스템(10)의 구조는 지불 생태계를 구성하는 뚜렷한 구성 사이의 경계를 고려한다. 이들 구성은 상인(다수의 위치를 가질 수 있는), 획득 은행, 획득 은행의 프로세서, 발급 은행, 발급 은행의 프로세서, 및 각 거래가 다른 것과는 비밀을 유지하는 것을 필요로 하는 조합을 포함한다.

부하 분할을 위하여, 한명의 고객에 대한 거래는 전형적으로 다른 고객의 거래와 독립적이고, 많은 목적을 위하여 특정 지불 도구의 거래는 다른 것과는 독립적이다. 개별적인 지불 도구는 상대적으로 적은 거래를 갖는 경향이 있어서, 개별 고객의 거래의 실시간 처리에 대한 요구는 실제적이지 않고, 다른 고객의 거래 사이에 상당한 잠재적인 평행이 존재한다. 상인은 전형적으로 그들의 비즈니스와 관련된 거래의 통합된 관점을 필요로 하고, 이는 상당한 금액의 거래를 나타낼 수 있다. 상인은 전형적으로 그들의 비즈니스에 관해 시기 적절하고 신속한 정보를 희망하지만, 엄격한 실시간 정보를 위한 제한된 요건이 되는 경향이 있다.

도 10을 참조하면, 일부 장치에 있어서, 부하 분할을 실현하는 구성요소는 분산된 거래 라우터(66)이다. 전형적으로 지불 처리 시스템(10) 내의 대부분의 기능 모듈(예, 소규모 거래 프로세서, 고객 계좌 프로세서, 상인 계좌 프로세서, 등)은 하나 이상의 내장 라우터 구성요소를 포함한다. 이러한 라우터는 들어오거나 나가는 모든 메시지 트래픽을 조사한다.

라우터(66)는 어떤 노드가 요청 등을 처리해야하는 지를 결정하면서 XML 메시지의 신속한 검사와 같은 다양한 메시지 동작을 수행한다. 일 실시예에 있어서, AUTH 메시지는 지불 카드번호와 상인에 의해 분할된다. Auth에서 카드번호와 상인의 식별자를 찾아낸 후, 라우터(66)는 이러한 요청을 적절하게 처리할 수 있는 특정 서버를 찾기 위하여 관련 라우팅 테이블을 시험한다. 다른 실시예에 있어서, CAPT 메시지는 일치하는 AUTH의 시간에 회복되는 RefID에 의해 분할된다. 라우팅 테이블은 그후 RefID를 적절한 서버로 맵핑하기 위하여 사용된다.

메시지의 추가적인 애플리케이션 레벨의 분석에 관해 거래가 다른 위치에서 처리되어야 함을 나타내는 상황이 존재한다. 이러한 경우, 거래는 재라우팅되고, 라우터(66)는 새로운 방법을 결정한다. 일부 장치에 있어서, 라우팅은 적응적이어서, 거래가 대부분의 시간(예, 99%의 적절한 라우팅 비율)에 적절하게 라우팅된다.

라우터(66)는 또한 사기행위에 내성을 가질 수 있고, 라우팅 세트를 떠나거나 이로 들어오는 노드를 처리할 수 있다. 라우터(66)는 워밍 스페어(warm spare) 노드를 관리할 수 있고, 잠재적으로 실패한 노드를 상대적으로 짧은 시간 기간(예컨대, 1초 또는 2초) 내에 다른 노드로 대체할 수 있다.

라우터(66)는 또한 특정 서비스와 관련되는 도메인 이름의 집합을 관리함으로써 지형적이고 기능적인 분할을 처리할 수 있다. 도메인 이름을 관리함으로써, 라우터(66)는 이들 도메인 이름에 맵핑하는 큰 집합의 IP 어드레스 사이의 트래픽을 경감시킬 수 있다.

도 11을 참조하면, 로드 밸런서(LB : load balancer)(70)를 포함하는 하나의 예시적인 부하 분할된 처리 노드(68)가 도시되어 있다. 이 장치에 있어서, 로드 밸런서(70)는, "더미"("dumb") HTTP 로드 배런싱을 제공하는 종래의 HTTP/SSL 로드 밸런서이다. 이 장치에 있어서, 소규모 거래 프로세서 또는 고객 계좌 프로세서를 포함하는 노드는 거래 라우터를 통해 연결되고, 애플리케이션 레벨의 라우팅을 수행한다. 개별적인 소규모 거래 프로세서 또는 고객 계좌 프로세서 데이터베이스는 특정 엔진 거래에 따라 지불 카드번호에, 상인 계좌 식별자, 및/또는 상인 기준 식별자에 의해 초기에 분할될 수 있다.

소규모 거래 프로세서 및/또는 고객 계좌 프로세서 리포팅 및 고객-자가-서비스 노드는 전형적으로 거의 실시간으로 액세스되는 공통의 데이터베이스로부터 실행한다. 소규모 거래 프로세서 및 고객 계좌 프로세서 리포팅 부하는 지불 카드번호 및/또는 상인에 의해 분할될 수 있다. 하지만 이러한 리포팅은 더 낮은 우선권을 할당받을 수 있다.

일반적으로, 지불 처리 시스템(10)을 구현하는 구성은 전형적으로 시스템 내에서 고용인 특정 역할을 할당한다. 예컨대, 관리의 상점(또는 다른 비즈니스 시설) 내의 모든 동작에 대해 책임을 질 수 있지만, 주로 사용자를 관리하기 위하여 사용된다. 전형적으로, 상점 당 이들 사용자 중 한명만이 존재할 수 있다. 고객 서비스 부문은 요청을 다루고, 상인의 서비스에 대해 불평하는 사람과 같은 사용자를 포함할 수 있다. 이들은 지정된 데이터베이스 내에서 고객 서비스 분쟁을 개시하거나 해결할 수 있다. 금융 부문은 상점 계좌를 기억하는 사용자를 포함할 수 있고, 거래, 양도 및 지불을 변형 및 기억할 수 있다. 이러한 사용자는 또한 상점의 은행 계좌에 대한 지불 기록을 조정할 수 있다.

개별적인 사람들과 함께, 특정 처리(소프트웨어, 하드웨어, 또는 소프트웨어와 하드웨어의 결합으로 수행되는)는 또한 특정 동작을 수행하기 위한 구성에 의해 할당될 수도 있다. 예컨대, 거래 API는 거래 요청 문서를 소규모 지불 게이트웨이에 전달하기 위하여 수행할 수 있다. 각 요청 XML 문서에서, 어떤 상인 SDK 고객이 거래의 근원인지를 지정하는 증명서가 존재할 수 있다.

다른 할당 가능한 과정은 데이터 조회를 소규모 지불 게이트웨이 데이터베이스에 전달하기 위하여 실현할 수 있는 조회 API이다. 전형적으로, 이러한 조회 API 인터페이스는 상인 비즈니스 시스템을 지불 처리 시스템과 통합하기 위하여 사용

한다. 이러한 할당 가능한 처리로부터 각 XML 요청은 특정한 상인 애플리케이션을 지정한다. 또 다른 할당 가능한 처리는, 서버 구성 및 상인 애플리케이션 관리 문서를 소규모 지불 게이트웨이에 전달하기 위하여 실현할 수 있는 관리 API이다. 할당 가능한 이러한 처리로부터 각 XML 요청은, 지불의 조정 또는 수집 설정의 조정과 같은 상인 애플리케이션 상에서 수행될 특정한 상인 애플리케이션과 동작을 지정할 수 있다.

시스템과의 상호작용을 위해 사용자 인터페이스가 제공된다. 이들 사용자 인터페이스는 요약 리포트 제공, 거래 세부사항의 브라우징, 및 조회 거래와 같은 거래 기능을 상호작용 가능하게 지원한다. 사용자 인터페이스는 또한, 양도 요약 보고, 조회 양도, 및 양도 세부사항의 브라우징과 같은 양도 기능을 지원한다. 지불과 관련된 기능은 하나 이상의 사용자 인터페이스에 대해 지원된다. 예컨대, 지불 요약 보고, 지불 조회, 지불 세부사항의 브라우징, 지불의 조정과 관련된 동작을 제공할 수 있다.

또한, 사용자 인터페이스는 고객 서비스 요약 보고, 논쟁/서비스 메시지 작업흐름과 같은 고객 서비스 메시지를 제공하는 것을 지원할 수 있거나, 논쟁/서비스 메시지 세트를 브라우징하거나 또는 논쟁/서비스 메시지를 조회하는 것을 지원할 수 있다. 계좌 리포트를 생성하고, 새로운 계좌 유형을 생성 및 관리하고, 활성 계좌를 조회하고, 계좌 세부내용을 브라우징하는 계좌 관리 동작도 지원할 수 있다. 기본 사용자의 하우스키핑 역시 사용자 인터페이스를 제공받을 수 있다. 예컨대 이러한 기능은, 사용자 계좌 로그인 기능, 사용자 계좌 프로파일 관리 기능, 사용자 하위-계좌 관리 기능, 회계감사 사용자 활동, 등을 들 수 있다.

전형적으로, 조회 API는 사용자 인터페이스를 통해 사용 가능한 동일한 정보에 대한 상인의 프로그램의 액세스를 제공한다. 상인 및 FSI는 구현 데이터 조회와 시스템 관리를 유연한 상호작용형 체계를 통해 인터페이스 연결시킨다. 이러한 체계는, 웹 브라우저와 HTTP API에 대한 프로그램의 XML을 포함하는 다수의 방법론을 통해, 공통의 조회와 관리 코드에 대한 액세스를 가능케한다.

일반적으로, 이들 API는 조회 및 데이터 관리 구현으로 구성되는 비즈니스 로직 구성요소를 포함할 수 있다. API는 또한 작업 흐름을 구성하는 유틸리티 구성요소와, 데이터베이스 액세스(예, 객체 지향형 데이터 액세스 및 관계 데이터베이스 관리 시스템 액세스)와 데이터베이스의 이식 가능성을 가능케 하는 데이터 액세스 인터페이스를 포함할 수 있다.

저가의 거래에 대해 수익성이 있는 비즈니스를 운영하는 것은 상당한 압력을 비즈니스 운영의 많은 측면에 부가한다. 예컨대, 고객 서비스 상호작용의 비용은 사건당 5 내지 10달러가 될 수 있고, 많은 비즈니스에서 전체 고객 서비스 부담은 거래당 평균 0.50 달러 이상이 될 수 있다. 지불 처리 시스템(10)은 비용을 감소시키는 소규모 거래 프로세서에 기초한 고객 자가 서비스를 구현한다. 부가적으로, 지불 처리 시스템(10)은 상인의 상점에서 각 구매를 상술하는 온라인 청구서를 제공할 수 있다. 온라인 자가-서비스는 고객의 만족을 개선시키고, 통합 청구서의 제공 및 논쟁 해결을 통해 고객의 서비스 비용을 낮춘다.

청구서 내에서 각 소액-거래는 상인의 제어 하에, 특정 문제(예, 구매하였지만 부주의하게 삭제된 노래의 재 다운로드)를 해결할 수 있는 자동화된 논쟁 해결 소프트웨어 마법사를 포함할 수 있다. 이러한 마법사는 또한 다른 문제와 관련된 정보를 수집하고, 이러한 정보의 해결을 위한 상인 고객 서비스 요원에 전달한다. 부가적으로, 이러한 마법사는 또한, 상인의 제어 하의 정책을 통해, 논쟁의 거래에 대해 고객의 이전 이력에 의존하여 변할 수 있는 정책을 가지고, 신용을 발급함으로써 문제점을 해결할 수 있다.

일부 장치에 있어서, 지불 처리 시스템(10)은 고객이 하나 이상의 고객 계좌 프로세서 및 소규모 거래 프로세서와 인터페이스 접속하기 위한 인터페이스를 구현할 수 있다. 소규모 거래 프로세서와 관련된 이러한 인터페이스는 고객이 거래 기록을 조사하고, 논쟁을 개시 및 해결하고, 상인에 의해 한정된 금융 도구 계좌를 관리 및 생성하는 것을 허용한다.

도 12를 참조하면, 지불 처리 시스템(10)은 보안을 웹에 기초한 고객 자가 서비스에 제공하기 위한 다양한 방법론을 구현할 수 있다. 예컨대, 보안 로그인은 프린트된 신용카드 계산서에 대한 정보가 액세스를 얻기 위해 사용되는 것을 요구함으로써 제공될 수 있다. 다른 보안 구현에 있어서, 로그인은 상인에 관련된 웹에 기초한 애플리케이션에 의해 제어될 수 있다.

예컨대, 프린트된 계산서(72)에 대한 정보에 로그인하기 위하여, 고객은 자신의 신용카드 계산서를 찾는다. 청구 라인 항목 상에서 상인의 이름에 뒤이어, 8 또는 9개 문자열의 식별자가 제공된다. 이러한 예에 있어서, 문자열 "Z12A7B2G"은 "MYSTORE"로부터 26.41달러의 청구액 내에 포함된다. 이러한 문자열은 그래픽 사용자 인터페이스(GUI)(74)에 로그인하기 위하여 신용카드 사용자에게 의해 사용될 수 있다. 특히, 웹에 기초한 인터페이스에 대해 그들 자신을 확인하기 위하여,

이러한 문자열은 "Log in number"라고 라벨이 붙여진 필드에 입력된다. 부가적으로, 거래 금액 "Transaction total"이라 라벨이 붙여진 필드에 입력된다. 이 예에 있어서, 26.41 달러가 "Transaction total"에 입력된 후, "go"란 라벨이 붙은 그래픽 버튼이 선택된다.

유사한 방식으로, 고객 계좌 프로세서와 관련된 그래픽 사용자 인터페이스는 고객이 관련 정보에 액세스하는 것을 허용한다. GUI(74)와 유사하게, 고객은 프린트된 계산서로부터의 정보를 사용하여 안전하게 식별될 수 있다. 프린트된 계산서로부터의 문자열 및 전체 거래에 부가하여, 액세스를 얻기 위하여 다른 정보를 사용할 수 있다. 예컨대, 거래 날짜, 고객의 신용카드 번호의 마지막 4자리 또는 다른 유사한 유형의 정보가 액세스를 안전하게 제공하기 위하여 사용할 수 있다.

고객은 다양한 포털을 통한 액세스를 얻을 수 있다. 예컨대, 고객은 자신의 컴퓨터 시스템(또는 휴대전화, PDA 등과 같은 다른 디지털 디바이스)을 통한 액세스를 얻을 수 있다. 대안적으로, 고객은 상인의 시스템을 통해 서로 로그인할 수 있다.

일부 상황에 있어서, 상인은 이미 고객을 인증하였을 수 있고, 추가 인증을 필요로 함이 없이, 소액-거래 청구 기록에 대해 고객의 액세스를 제공할 수 있다. 지불 처리 시스템(10)은 상인이 고객에 전달할 수 있는 제한된 시간의 청구서 제공 증명서를 생성하는 API를 통해 이러한 액세스를 지원한다. 이러한 증명서는 "요금 URL"이고, 고객에게 그들의 소액-거래 청구 활동을 보여주는 특정 양의 시간 동안 유효할 수 있다. (고객 선택에 의해 또는 상인이 강제된 브라우저 재방향 설정에 의해) 요금 URL에 액세스하는 것은 고객에 의한 추가 인증을 필요로 하지 않고 고객에게 그들의 특정 요금을 부가할 수 있다.

전형적으로, 요금 URL은 제한된 시간(전형적으로 30분 이하) 동안 유효하다. 요금 URL이 만료되었지만, 상인에 대한 고객의 인증이 만료되지 않으면, 상인 시스템에 대해 고객에게 추가적인 시간을 제공하도록 요청함으로써, 요금 URL을 리프레쉬시킬 수 있는 메커니즘이 존재할 수 있다. 만약 고객이 더 이상 상인에게 인증받지 못한다면, 고객은 재로그인하여 새로운 요금 URL을 얻을 수 있다.

도 13을 참조하면, 액세스를 얻을 때, 고객은 매크로-거래로 수집된 소액-거래의 목록을 포함하는 GUI(76)를 제공받는다. 각 소액-거래는 추가 정보를 얻기 위하여 사용자가 선택 가능하다.

도 14를 참조하면, 예시적인 GUI(78)는 GUI(76)에 포함된 라인 항목으로부터 선택된 소액-거래와 관련된 추가 정보를 제공한다.

청구서 내의 각 소액-거래는 상인의 제어 하에, 특정 사용자 관련 문제(예, 구매하였지만 부주의하게 삭제된 노래의 재 다운로드)를 해결할 수 있는 자동화된 논쟁 해결 마법사를 포함할 수 있다. 이러한 마법사는 또한 다른 문제에 관한 정보를 수집하고, 이러한 정보의 해결을 위해 상인 고객 서비스 요원에게 전달한다. 추가적으로, 이러한 마법사는 신용을 고객에게 부여함으로써 문제를 해결할 수 있다. 문제를 해결하기 위한 정책은 상인에 의해 제어될 수 있고, 지불 처리 시스템(10) 내에 포함된 사기행위에 대한 기술에 의해 구동될 수 있다.

도 15 내지 도 17을 참조하면, 일련의 GUI(80, 82 및 84)가 일부 전형적인 사용자 상호작용을 나타낸다. 도 15를 참조하면, 고객은 "Customer Support Request"("고객 지원 요청") 링크를 선택하였고, 상인에 의해 한정된 GUI(80) 내의 잠재적인 요청 목록을 제공받는다. 도 16을 참조하면, 본 예에 있어서, "I lost this song"("이 곡을 분실했음") 링크를 선택함으로써, 사용자가 고객의 지원 요청내에서 대체물을 전달하는 것을 가능케 하는 GUI(82)가 제공된다. 도 17을 참조하면, 고객 지원 요원(아마도 상인과 관련이 되는)은 GUI(82)를 통해 확인된 문제와 관련되는 요청을 GUI(84)를 통해 제공받는다. 고객 지원 요원은 이러한 요청과 관련된 문제점을 해결할 수 있을 것이다. 해결시, 이메일이 고객에게 보내질 수 있다. 부가적으로, 고객의 온라인 청구서를 갱신할 수 있다.

도 18을 참조하여, 만약 거래가 단일 상인에 대해 수집되면, 대응하는 매크로-거래 내의 소액-거래는 동일한 상인과 관련이 있다. 이들 거래는 그 상인 이름으로 청구될 것이다. 상술한 바와 같이, 소액-거래는 상인의 그룹을 통해 수집될 수 있다. 따라서, 고객과 다수의 상인 간에 소액-거래가 수집될 수 있다. 부가적으로, 단일 상인과 고객 사이에 거래되는 다수의 소액-거래가 수집될 수 있다. 이들 다수의 소액-거래를 수집함으로써, 고객은 다른 상인과 관련하여 수집된 거래를 제공할 수 있다. 예컨대, 인쇄된 계산서(86)에 도시된 바와 같이, "SmallTab.com", 또는 "Bank Small Payment Service"와 같은 제 3자를 통해, 고객과 관련된 소액-거래의 수집에 기초하여 다수의 상인이 분류될 수 있다.

다수의 상인 모두에게 수집 데이터를 제공하는 것과 함께, 계산서(86)는 또한 제 3자 웹사이트에 액세스하는데 사용할 수 있는 식별 번호를 포함한다. 예컨대, 웹사이트(예, <http://smalltab.com>)에 액세스하여 식별번호에 입력함으로써,

1875766), 고객 서비스 GUI(88)가 제공될 수 있다. 이러한 예에 있어서, GUI(88)는 계산서(86)에 포함된 여러 상인의 목록과 그들의 대응하는 소계를 제공한다. 한명의 상인과 관련된 특정 링크를 선택함으로써, 그 상인과 관련된 개별 거래의 목록이 제공된다.

다수의 구현이 기술되었다. 그럼에도 불구하고, 다양한 변경이 이루어질 수 있음을 이해할 것이다. 따라서, 다른 구현 역시 다음의 청구범위의 범주 내에 든다.

산업상 이용 가능성

본 발명은 지불 처리 분야, 보다 상세하게는 거래 비용을 낮추기 위하여 저가의 구매를 처리하는 분야에 이용 가능하다.

부록

부록 A

계좌정보

정보	설명
계좌 ID	이 계좌에 대한 고유 ID.
도구	이러한 계좌와 관련된 지불 도구.
상인	만약 "보편적인 수집" 계좌가 아니라면, 이 계좌와 관련된 상인.
계좌 유형	이러한 계좌에 대해 동작이 어떻게 이루어지는 확인(아래의 프로세서를 참조).
계좌 데이터	소규모 거래 Suite 플러그-인에 의해 사용된 계좌를 위한 확장 데이터.
Ppcn 데이터	계좌와 관련된 내부 확장 데이터.
상태	계좌의 상태 : 계류중, 활성화중, 만료됨, 불가능, 또는 정지됨.
개방 auths	밸런스에 대해 허락 받았지만 아직 포착되지 않은 AUTH의 집합
Auth 밸런스	이 계좌 상의 개방AUTH(공인)된 금액의 진행중인 밸런스.
마지막 거래	계좌 내에서 마지막 거래의 데이터.
거래	이 계좌 내의 지불 거래.
계좌 사건	이 계좌 내의 미지불 거래.

부록 B

구매 요청

AUTH	잠재적인 구매에 대한 공인 요청
CAPTURE(포착)	기존 AUTH에 기초한 실제 구매의 확인
SALE(판매)	결합된 AUTH와 포착
VOID(무효)	최근 포착을 취소하고, 고객의 청구서에 거래를 보여주지 않는다.
CREDIT(신용)	초기 포착을 취소, 두 거래 모두 고객의 청구서 상에 별도로 보여짐
INQU(문의)	이 계좌에 대한 초기의 요청 상태에 관해 문의

부록 C

사용시마다 지불의 추가 요청

상태설정	가능, 불가능, 유효, 계류중 사이에서 사용시마다 지불 계좌의 상태 변경
전달	기존의 사용시마다 지불 계좌를 다른 신용카드(예, 기초가 되는 카드를 도난당하거나 만료된 경우 필요한)에 전달

부록 D

청약 추가 요청

생성	새로운 청약을 생성 & 기초가 되는 신용 계좌에 대한 교차 요금으로 이를 지원
취소	불완전한 청약을 취소, 벌지 못하는 임의의 밸런스를 기초가 되는 신용 계좌에 상환(CREDIT)
갱신	기존 청약 기간을 연장. 선불(일시 요금) 청약에 대해, 기초가 되는 계좌에 대한 교차 요금을 즉시 생성
조정	임의의 교차 요금을 생성함이 없이 청약 기간을 조정
상태설정	가능, 불가능, 유효, 계류중 사이에서 청약 계좌의 상태 변경
전달	기존의 청약을 다른 신용카드(예, 기초가 되는 카드가 도난당하거나 만료된 경우 필요한)에 전달

부록 E

후불 추가 요청

생성	새로운 후불 계좌를 생성
청구	지불 도구에 대한 청구서에 이 계좌에 대한 후불 요금을 청구
조정	예컨대, 지불 도구에 대한 청구서의 변경을 포함하여, 후불 계좌 기간을 조정
상태설정	가능, 불가능, 유효, 계류중 사이에서 계좌의 상태 변경
전달	기존의 후불 계좌를 다른 계좌에 전달

부록 F

API 논의

<u>요소</u>	<u>설명</u>
ACCT	신용카드/직불카드 계좌 번호
ACCTCLASS	계좌의 등급: 사용시마다 지불(디폴트), 선불, 청약, 후불
ACCTDATA	상인-특정 계좌 데이터를 위한 장소. 이 데이터는 Peppercoin 시스템에 의해 저장되고, 고객 프로그램과 서버측 확장 모두에게 사용가능하게 이루어진다.
ACCTENDDATE	이 날짜 이후 계좌는 더 이상 유효하지 않다(연장되지 않는 한)
ACCTID	이 계좌의 내부 ID: 계좌 문의에 의해 리턴되고, 후속 요청에서 사용된다.
ACCTINFO	계좌에 대한 요소 그룹화 정보: 조회 응답은 ACCTINFO 요소의 임의의 번호를 포함한다.
ACCTSTARTDATE	계좌가 유효해 지는 날짜
ACCTSTATUS	계좌의 상태; V3에서는 ACTV, PNDG, EXPD, DISA 중 하나.
ACCTTYPE	계좌의 유형. 계좌 유형은 API를 통해 동적으로 한정될 수 있다.
ACCTTYPELABEL	계좌 유형을 위한 라벨- 잠재적으로 사용자에게 제공.
AMT	금액

<u>요소</u>	<u>설명</u>
AMTDUE	사용시마다 지불 계좌를 위해, 공인되고 계류중인 포착 금액
AUTHBALANCE	선불 및 제한된 청약 계좌에 대해, 공인되었지만 아직 포착되지 않은 자원의 양
AUTHEXP	공인에 대한 만료 날짜/시간
AVSRESP	단지 권고를 위한 AVS 어드레스 응답
BALANCE	선불 및 제한된 청약 계좌에 대해, 포착을 위해 (어떠한 유닛이 한정되든)사용 가능한 자원의 금액
CHARGE	지불 스트림의 거동을 한정하는 복합 요소
CITY	회원의 시
COMMENT1	리포팅 목적만을 위한 사용자가 한정된 값
COMMENT2	리포팅 목적만을 위한 사용자가 한정된 값
COUNTRY	회원의 3문자 국가 코드
CURRENCY	금액의 화폐
CVV	신용 카드의 전면/후면의 3 또는 4 자리의 CVV/CVC 코드
CVVRESP	단지 권고를 위한 CVV 응답,
DEBIT	밸런스 조정을 나타내기 위하여 사용된 플래그(빈 요소)는 디폴트 신용카드 대신 직불카드인 것을 의미한다.
DEPOSIT	청약이 될 자원 스트림의 거동을 한정하는 복합 요소

DESCRIPTION	주문에서 항목의 설명
EDGEID	이러한 AUTH를 수행하는 Edge의 ID
EMAIL	회원의 이메일 어드레스
EXPDATE	신용카드의 만료일
GATEWAYRESPONSE	AUTH 실패를 보다 상세하게 기술하기 위한 선택적인 프로세서-특정 데이터
IMAGE	주문에서 항목을 위한 인터넷-액세스 가능한 URL

<u>요소</u>	<u>설명</u>
INQUIRESPONSE	조회 주제인 거래의 RESPONSE 객체를 포함하는 XML객체
MACCT	PPCN을 갖는 상인의 계좌 이름
NAME	주문에서 항목의 이름
NAMEONCARD	카드 상의 회원의 이름
OFFSET	청약 요금 기간의 만료 이전에 오프셋을 한정, 이 때 청약을 지원하기 위한 추가 요금 증분을 포착하기 위한 시도가 이루어진다.
OPERATOR	이러한 거래를 누가 실행하였는 지를 확인하기 위하여 app-s가 사용될 수 있는 식별 필드
ORDER	주문 메시지를 위한 상부 레벨 요소
ORDERINFO	주문 거래에서 구매한 사물과 관련된 정보를 포함
PERIOD	청약 지불 또는 자원 할당이 갱신되는 기간
POSMODE	POS 디바이스가 사용되는 모드
POSTAL	회원의 5 내지 9자의 우편 코드
PPCNDATA	Peppercoin에 의해 한정되고 Peppercoin-이 제공한 표준 프로세서에 의해 지원되는 계좌 데이터를 위한 장소
PRODUCTKEY	제품 등급
QUERYID	이러한 요청을 위한 상인의 ID. 이것이 계좌 조회(ACTQ)에 제공된다면, 이는 응답으로 리턴된다.
QUERY-PARAM	"BRIEF" 또는 "FULL"의 값을 취하는 선택적인 속성 RESPONSE를 갖는 빈 요소. 존재하지 않을 경우 응답은 BRIEF가 된다.
REFID	포착, 무효, 조회 거래 및 신용 거래를 위해 사용한 기준 ID.
REQUEST	고객으로부터 전달되는 기본 메시지; 정상적으로 상부레벨이지만 ORDER에 포함될 수 있다.
REQUESTID	이러한 요청을 위한 상인의 ID
RESPAMT	허락된 신용 금액
RESPMSG	주어진 응답 코드를 설명하는 메시지
RESPONSE	요청(또는 주문?)에 대한 응답; 정상적으로 상부레벨이지만 INQUIRESPONSE에 포함될 수 있다.
RESULT	성공 또는 실패를 나타내는 기본 응답 코드

<u>요소</u>	<u>설명</u>
SERVERID	거래 근원인 상인의 서버를 위한 식별 계좌
SERVERKEY	거래 근원인 상인의 서버를 위한 키/패스워드
STATE	회원의 주, 미국이라면 2문자 코드
STATUS	계좌 상태: ACTIVE, PENDING, EXPIRED, DISABLED 중 하나.
STREET1	회원의 거주지 주소(예, 12 Main St.)
STREET2	회원의 거주지 주소의 선택적인 두 번째 행
TRACK1	Track1로부터 카드 승인 데이터
TRACK2	Track2로부터 카드 승인 데이터
TRXTYPE	거래 유형; 수행될 동작을 확인하고, 어떤 주문 요소가 유효하고 및/또는 요구되는 지 암시적으로 결정한다.

부록 G

수집 파라미터

지능형 수집 파라미터	파라미터 설명
비즈니스 모델	이러한 특정 계좌의 비즈니스 모델: 사용시마다 지불, 선불, 청약, 후불

수용된 지불도구	이러한 비즈니스에 의해 수용된 지불 도구: Visa, MasterCard, American Express, Discover .
Visa와 MasterCard의 교환 분류	이러한 비즈니스에 대해 Visa와 MasterCard 거래를 위해 상인의 완전히 자격이 있는 교환 등급의 지능형 수집 시스템을 안내. 지능형 수집은, 완전히 자격이 있는 거래가 선택된 등급의 비율로 처리될 것이라고 간주하는 교환 자격을 최적화할 때 거래 레벨 사건을 자동적으로 고려한다. 지능형 수집은 비즈니스 레벨의 교환 자격 사건에 어떠한 가시성도 갖지 않는다; 여기서 잘못된 등급을 지정하는 것은 매크로-거래의 분류에 영향을 미치지 않을 것이지만, 수집의 부정확한 최적화를 야기할 것이다.
Visa와 MasterCard를 위한 획득자와 프로세서의 수수료	획득자와 프로세서에 대해 지불된 전체 처리 수수료는 비-수집 거래에 대해 지불하였다. 이들 수수료는 Visa와 MasterCard를 위한 교환 수수료에 더해진다.
American Express/ Discover 처리 수수료	American Express, Discover 및 다른 비(非)교환 기반 시스템에 대한 상인의 처리 수수료의 지능형 수집 시스템을 안내
자금 비용	년 단위를 기초로 한 자금의 비용. 이러한 금액은 재고 비용, 수집 원도의 확장 비용과 같은 금융 충격을 평가하는데 사용된다.
사기행위 비율	사기행위로 예상되는 거래의 예상 백분율
고객 서비스 비율	고객의 서비스 요청을 유발시킬 것으로 예상되는 거래의 예상되는 백분율

지능형 수집 파라미터	파라미터 설명
공인 금액 정책	각 거래에 대한 공인 금액을 계산하기 위한 정책을 설정. 선택사항은, 상인에 의해 결정된 고정된 금액; 상인의 비즈니스에서 평균 구매 거동에 의해 결정되거나, 특정 제품 등급에 대해 결정되는 동적인 금액; 과거에 이러한 상인으로부터 고객의 구매 거동의 분석을 기초로 한 동적인 금액; 또는 과거에 다른 비즈니스를 통해 이러한 고객의 구매 거동의 대략적인 분석에 기초한 동적인 금액을 포함한다. 교환 분류의 고려는 상인에 의해 한정되는 전체적인 최대값이 될 금액을 제한할 것이다.
공인 최대 윈도우 길이 정책	각 거래에 대한 수집 윈도우의 날짜 단위의 길이를 계산하기 위한 정책을 설정. 계산은 관찰된 거동을 교환 분류 최적화 고려사항에 대해 균형을 맞춘다. 윈도우 크기를 결정하기 위한 선택사항은: 상인에 의해 결정된 고정된 길이; 상인의 비즈니스에서 평균 구매 거동에 의해 결정되거나, 특정 제품 등급을 위해 결정되는 동적인 길이; 과거에 이러한 상인으로부터 고객의 구매 거동의 분석에 기초한 동적인 길이; 또는 과거의 다른 비즈니스를 통해 이러한 고객의 구매 거동의 대략적인 분석에 기초한 동적인 길이를 포함한다. 고객의 지불 도구에 특정한 교환 분류 고려사항은 상인에 의해 한정된 전체적으로 최대값이 될 계산 파라미터를 변경시킬 수 있다.
첫 번째 고객 정책	첫 번째 고객을 처리하기 위한 정책을 설정한다. 정책은: 첫 번째 고객을 수집하지 않는 것 또는 첫 번째 고객을 낮은 활동, 중간-활동 또는 높은 활동의 고객으로 취급하는 것을 포함한다.
수집 교환 등급 정책	수집 정책에 관해 이것이 가장 효율적이라고 결정할 경우, 수집 정책이 거래 교환 분류를 변경하는 것이 허용되는지의 여부를 제어한다. 등급 강등을 통한 절약은 임계값 효율 액수를 초과하여야 한다. 선택사항은 수집이 완전히 자격이 있는 교환 등급 내에 남아 있도록 강제하는 것, 등급 강등을 중간 자격의 등급이 되게 허용하는 것 또는 등급 강등이 자격이 없는 등급이 되게 허용하는 것을 포함한다.
최대 수집 거래 금액	수집된 매크로-거래의 최대값의 금액에 상한값을 부가한다.

지능형 수집 파라미터	파라미터 설명
최대 소액-거래 금액	수집된 매크로-거래 내에서 소액-거래의 최대 금액. 이 금액보다 많은 거래는 수집되지 않는다.
최대 소액-거래 계수값	수집된 매크로-거래 내에서 소액-거래의 최대수
최대 수집 윈도우 길이	수집 시간 날짜의 최대수. 실제 수집 시간은, 고객 구매 속도; 교환 자격에 기초한 제한; 동적인 비용/이익 분석; 및 다른 인자를 포함하는 많은 인자에 의해 감소될 수 있다.
주기적인 수집 윈도우 종료	매일, 주중의 특정한 날, 또는 월중의 특정한 날과 같은 주기적인 경계로 수집을 종료한다.
수집 Opt 입/출력	고객이 수집에 대해 Opt-입력 Opt-출력하도록 허용한다. Opt-입력이나 Opt-출력 중 어느 것이 디폴트인지 제어한다.
지불 도구 확인 정책	고객의 지불 도구가 수집 이전에 유효한 것을 보장한다. 지불 도구는 목표가 된 포착 금액 또는 1 달러에 대한 공인을 사용하여 확인된다. 이러한 설정은 기본적으로 이전의 공인을 필요로 하지 않는 수집 정책의 거동에 영향을 미친다.
확인 수명	종래의 지불 도구 확인의 날짜 단위의 수명. 이러한 날짜의 수보다 더 새로운 확인 정보를 가질 경우, 시스템은 확인을 재시행하지 않을 것이다. 이러한 설정이 거래 공인 거동에 영향을 미치지 않음을 주목해야 한다.
AVS 정책	AVS 일치가 모든 거래에 요구되는지를 제어한다.

CVV 정책	유효한 CVV 코드가 모든 거래를 제공받아야 하는 지를 제어한다.
최대 소액-거래 속도	속도 체크 기간 내에서 고객을 특정 수의 거래로 제한한다. 이러한 금액이 0이하라면, 속도는 체크되지 않는다.
속도 체크 기간	특정 기간: 제공된 옵션에 대해 매일, 또는 매시간 내에 거래 속도를 체크한다.
사기행위 점수 수집 차단	이러한 금액 이상의 사기행위 점수를 갖는 거래는 수집되지 않는다.
고객 서비스 점수 수집 차단	이러한 금액 이상의 고객 서비스 점수를 갖는 거래를 수집되지 않는다.

부록 H

PCT 출원 US02/12189

(발명의 명칭)

소액지불 거래를 위한 방법 및 시스템{METHOD AND SYSTEM FOR MICROPAYMENT TRANSACTIONS}

(기술분야)

관련 출원의 교차 참조

본 출원은 1) 2001년 4월 27일에 출원된 발명의 명칭이 "소액지불 거래를 위한 방법 및 시스템"인 미국 가출원 번호 60/287,251; 2) 2001년 7월 18일에 출원된 발명의 명칭이 "소액지불 거래를 위한 방법 및 시스템"인 미국 가출원 번호 60/306,257, 및 3) 2001년 12월 26일에 출원된 발명의 명칭이 "소액지불 거래를 위한 방법 및 시스템"인 미국 가출원 번호 60/344,205의 우선권의 이점을 주장한 것으로서, 이들 모두는 이하에 상세하게 설명된 바와 같이 본원에 전반적으로 병합되어 있다.

(배경기술)

전자 상거래 시스템의 성장이 전자 네트워크에 걸쳐서 실행되는 금융 거래 수를 급격하게 증가시켰다. 정보 검색 서비스와 같은 온라인 저가의 서비스에 대해서 파이낸싱(financing) 하는 간편한 방법을 제공함으로써, 소액지불은 새로운 형태의 전자 상거래를 실행할 수 있다. 소액지불은 초저가, 어떤 경우엔 페니의 프랙션(fraction)일 수 있지만, 매우 높은 볼륨으로 실행할 수 있다. 예로서, 정보 서비스 제공자는 자신들의 서비스를 소액으로 요금청구하길 원할 수 있다. 소액지불은 방문한 웹 페이지마다 또는 사용자에게 스트리밍되는 음악 또는 비디오의 매 분마다 지불하는 데 사용할 수 있다.

간단한 형태의 전자 지불 방식으로는 전자 수표가 있다. 전자 수표는 손으로 서명하는 것이 아니라 디지털적으로 서명하는 수표로 이루어진다. 디지털 서명은 수표의 수신자가 서명 당사자의 인증과 수표 내용의 무결성(예를 들어, 수표의 날짜와 금액) 둘 다를 검증하도록 한다. 공개 키 암호작성에 대한 문헌은 Rivest, R.L., Shamir, A., 및 Adleman, L.A.의 Communications of the ACM의 Vol. 21, No.2, 1978, S. 120-126에 발표한 "디지털 서명 획득 방법 및 공개 키 암호방식"에 서술된 RAS 방법과 같은 디지털 서명을 구현하기 위한 많은 방법을 제공한다. 널리 공지된 바와 같이, 공개 키 암호방식에서 각 당사자는 특정한 키 쌍을 이용한다. 각 쌍은 공개 키와 대응하는 사설(또는 비밀) 키를 포함한다. 공개 키를 공중이 이용할 수 있지만, 대응하는 사설 키는 공지되고 이 사설 키를 보호하고 비밀을 유지하는 소유자만 액세스할 수 있다. 대응하는 공개 키에 대한 지식 또는 발견으로부터 사설키를 계산적으로 도출하는 것은 불가능하다. 그러므로, 공개 키를 공중이 이용하여도 이에 정합하는 사설 키의 보안에는 위험이 없다. 소유자 이외에는 어떤 누구도 사설키에 접근할 수 없기 때문에, 공개 키 암호방식은 여러 당사자들이 비밀키를 공유하고 있는 시스템과 비교하여 보안성을 증가시킨다.

공개 키 암호방식에서, 비밀스럽게 메시지를 전송하길 원하는 송신자는 수신자의 공개키를 획득하고 이를 이용하여 메시지를 암호화한다. 암호화된 메시지의 수신시, 수신자는 자신의 정합하는 사설 키를 이용하여 이 메시지를 해독하고 원래 메시지를 판독한다. 정합하는 사설 키에 액세스함이 없이, 암호화된 메시지를 계산적으로 해독하는 것은 불가능하다.

공개 키 디지털 서명 방식에서, 메시지의 서명자는 자신의 사설 키를 메시지에 적용함으로써 자신의 디지털 서명을 생성한다. 따라서, 이 결과의 디지털 서명은 디지털 서명을 생성하는데 사용되는 특정 사설 키와 메시지 둘 다에 대해서 특정하게 된다. 이 메시지와 디지털 서명을 소유한 누구라도 서명자의 공개 키를 이용하여 디지털 서명의 인증을 검증할 수 있다.

해쉬 함수는 또한 많은 공개 키 디지털 서명 방식에 사용된다. 해쉬 함수는 메시지에 적용될 때 전형적으로 고정된 길이를 갖는 "해쉬 값"의 형태로 이 메시지의 디지털 "핑거프린트"를 생성하는 알고리즘이다. "일방향 충돌-회피"(또는 보안) 해쉬 함수는 해쉬 값으로부터 원래 메시지를 도출하거나 심지어 동일한 해쉬 값을 갖는 2개의 메시지를 구하는데 계산적으로 불가능한 해쉬 함수이다. 따라서, 메시지의 해쉬는 메시지에 대한 "핑거프린트" 식별에 따라서 양호하게 작동하는데, 왜냐하면 메시지에 대한 어떤 변화, 심지어 아주 작은 변화가 이루어진 경우조차도, 상이한 해쉬값을 지닌 메시지를 반드시 얻기 때문이다.

"해쉬와 사인" 방식의 디지털 서명 방식으로 해쉬 함수를 이용하는 것이 보편적이다. 이 방식으로 디지털 서명을 생성하기 위하여, 메시지의 송신자는 해쉬 함수를 메시지에 적용하여, 메시지에 대한 해쉬 값 또는 메시지 다이제스트를 계산한다. 그리고 나서, 송신자는 자신의 사설 키를 해쉬 값에 적용하여 이 메시지에 대한 자신의 디지털 서명을 획득한다.

디지털 서명의 인증뿐만 아니라, 메시지의 내용의 무결성은 서명을 생성하기 위하여 사용되는 해쉬 함수 및 송신자의 공개 키를 이용하여 검증할 수 있다. 수신자는 메시지에 대한 해쉬 값을 재계산하고 나서 이 해쉬 값과 송신자의 공개 키를 입력으로서 취하는 검증 절차를 적용함으로써, 메시지가 실제 송신자에 의해 서명되었다는 것을 검증할 수 있다. 검증 절차는 예를 들어 송신자의 공개 키를 해독 키로서 이용하고 해독이 메시지의 재계산된 해쉬 값을 산출하는 경우, 이 서명을 유효한 것으로 받아들이는 것이라고 일컬을 수 있다. 검증이 성공되면, 송신자가 메시지를 실제로 서명하고 서명된 후 메시지가 변경되지 않았다고 수신자는 신뢰할 수 있다.

전형적인 전자 수표 지불 방식에서, 사용자는 거래를 식별하는 데이터 조각에 디지털 서명을 제공함으로써, 거래에 대한 댓가를 상인에게 지불한다. 이 데이터는 특히, 사용자, 사용자의 은행 계좌 번호, 상인, 지불할 금액, 거래 시간, 및/또는 구입되는 정보, 서비스 또는 상품을 식별할 수 있다. 전형적으로, 상인은 수표를 은행에 보냄으로써, 사용자로부터 수신한 전자 수표를 예치한다.

전자 수표 방식에서 디지털 서명 능력은 디지털 인증서에 의해 지원될 수 있다. 디지털 인증서는 특정 개인이 인증서에 제공된 공개 키에 대응하는 사설 키를 유지한다고 단정하는 가장 보편적인 전자 문서이다. 바꿔 말하면, 인증서는 키 쌍을 특정 당사자와 상관시킨다. 인증서 자체가 신뢰성 있는 당국에 의해 디지털적으로 서명되기 때문에, 디지털 인증서는 통상, 기명된 당사자가 실제 인증서에 리스트된 공개 키를 소유하고 기명된 당사자가 대응하는 사설 키를 독점적으로 제어하는 증거로서 신뢰받는다. 디지털 인증서는 또한 당사자가 전자 지불을 서명하거나 다른 특정 작용을 수행하도록 하는 권한을 갖는다고 단정할 수 있다.

전자 수표상의 디지털 서명을 검증한 후, 은행은 적절한 금액을 상인에게 대변(credit)할 수 있고 적절한 금액을 사용자에게 차변(debit)할 수 있다. 은행은 또한 일임 매매 요금 또는 이외 다른 요금을 청구할 수 있다.

전자 지불 시스템 및 특히 소액지불 시스템은 많은 문제에 직면한다. 소액지불의 기본적인 문제는 소액지불을 위한 은행의 처리 비용이다. 빈번하게, 은행이 소액지불 거래를 취급하는데 드는 비용은 소액지불 자체의 값보다 몇 배 크다. 예를 들어, 신용 카드 거래를 처리하는데 드는 비용은 통상 약 25센트인 반면에, 전형적인 소액지불은 약 1센트 또는 1센트의 프랙션의 가격일 수 있다. 그러므로, 소액지불을 지원하기 위한 특단의 효율이 필요로 된다. 그렇지 않다면, 지불 메커니즘의 비용은 지불 가치를 훨씬 초과할 것이다.

그러므로, 소액지불 방식은 많은 작은 지불을 몇 개의 큰 지불로 수집시킴으로써 은행의 처리 비용을 감소시키고자 하였다. 다양한 수집 전략이 이용될 수 있다. 일부 소액지불 방식은 세션-레벨 수집(session-level aggregation)을 갖는다. 소정 "세션" 동안 사용자와 상인 간의 모든 지불은 단일의 큰 지불로 수집된다. 또 다른 전략은 글로벌 수집이다. 지불은 모든 사용자/상인 쌍에 걸쳐서 수집된다. 글로벌 수집은 유연성을 더욱 증가시키고 비용을 더욱 절감시킬 수 있다.

다수의 소액지불 방식은 종래 기술에 공지되어 있고, 조사는 예를 들어 Peter Wayner가 Academic Press, 1996에 발표한 "디지털 캐쉬: 네트워크상에서 상거래"의 문헌에서 찾아볼 수 있다. 현재 공지된 소액지불 방식은 Ronald L. Rivest와 Adi Shamir가 보안 프로토콜에 대한 네 번째 캠브리지 위크샵, Springer Verlag Apr. 1996에 발표한 2가지 간단한 소액지불 방식, 및 ("Ronald L. Rivest가 컴퓨터 사이언스의 강의 노트 vol. 1318, 페이지 307-314, Springer 1997의 금융 암호작성 '97의 회보 내의 "소액지불로서의 전자 복권 티켓"에 설명된) "전자 복권 방식"이 있다. 다른 공지된 소액지불 방식은 Manasse 등에 의한 "밀리센트", Riverst 및 Shamir에 의한 "마이크로민트, Anderson에 의한 "넷카드", Jutla 및 Yung에 의한 "페이트리", Hauser 등에 의한 "마이크로IKP", Jarecki 및 Odlyzko에 의한 확률적 폴링 방식, Wheeler에 의한 "베트를 사용한 거래"에 대한 제안, Pedersen에 의한 유사한 제안, 및 Lipton 및 Ostrovsky에 의한 효율적인 동전-던

지기에 의한 소액지불에 대한 관련 제안을 포함하지만, 이에 제한되지 않는다. Jerecki/Odlyzko의 확률적 폴링 방식은 Stanislaw Jajecski 및 Andrew M. Odlyzko가 1999년 12월 7일자로 발행하고, 명칭이 "효율적인 소액지불 시스템"인 미국 특허 번호 제5,999,919호에 게시되어 있다.

페이워드는 공개 키 디지털 서명 방식 및 일방향 해쉬 함수에 기초한 소액지불 시스템이다. 페이워드 시스템에서, 사용자는 은행으로부터 디지털 인증서를 수신하는데, 이 인증서는 사용자가 해쉬 값의 체인, 또는 "페이워드"(w_i)를 만들도록 한다. 이들 페이워드는 상인에 의해 은행으로부터 화폐로 태환될 수 있다. i -번째 페이워드는 다음 관계:

$w_i = h(w_{i+1})$ 에 의하여 $i+1$ 번째 페이워드와 관련되며, 여기서 h 는 일방향 해쉬 함수이다. 따라서, $h(w_{i+1})$ 로부터 w_{i+1} 를 도출하는 것이 계산적으로 실행 불가능하다. $i+1$ 번째 페이워드(w_{i+1})는 w_{i+1} 에서 해쉬 연산(h)을 수행함으로써, i -번째 페이워드(w_i)를 사용하여 상인에 의해 검증될 수 있다. 페이워드 방식에서, 사용자는 해쉬 값의 체인($w_0, w_1, \dots, w_n$)을 계산하고, 루트(root)(w_0)에 대한 자신의 디지털 서명을 상인에게 보냄으로써 전체 체인에 커미트(commit)한다. 그 후, 사용자는 페이워드를 연속하여 차례로($w_1, w_2, \dots, w_i, \dots$) 드러냄으로써 상인에게 각각의 연속적인 지불을 행한다. 체인 내의 각각의 연속적인 값은 이것이 페이워드 체인 내의 이전 값을 해쉬하였는지를 점검하기 위하여 그 값에 대해 해쉬 함수를 수행함으로써, 상인에 의해 검증될 수 있다.

페이워드는 상인이 소비자의 지불을 편리하게 수집시키도록 한다. k 의 소액지불이 행해진 후, 상인은 k 의 소액지불이 상당히 큰 충분한 소액지불을 구성한다고 느끼는 경우, k 센트(또는 각각의 소액지불을 나타내는 다른 적절한 화폐 단위)에 대해 은행에서 단일 예치를 행한다. 벤더는 단지 2개의 값(w_k), 및 w_0 의 사용자의 서명을 은행에 보고한다. 은행은 w_0 의 사용자의 서명을 검증하고, 이 연산이 실제로 w_0 를 산출하는지를 검증하기 위하여 w_k 에 해쉬 함수를 k 번 반복한다. 검증후, 은행은 벤더의 계좌에 k 센트를 지불하고, 사용자의 계좌에 k 센트를 청구하고, 임의로 다른 거래 요금을 청구한다.

페이워드는 상이한 사용자의 소액지불을 수집시킬 수 없다는 단점을 갖고 있다. 이것은 페이워드에서, 각 사용자가 자신의 해쉬-값 체인을 상인과 설정하기 때문이며, 상이한 해쉬-값 체인이 병합될 수 없기 때문이다. 밀리센트와 같은 많은 다른 소액지불 안은 또한 상이한 사용자/상인 쌍에 걸쳐 소액지불을 수집시킬 수 없다는 문제를 겪게 된다. 즉, 페이워드는 글로벌 수집이 아니라, 단지 세션-레벨 수집만을 제공한다.

Rivest에 의한 전자 복권 방식은 거래 비용을 절감시키기 위하여 소액지불을 수집시키는 또 다른 방법을 제공한다. 이 방식은 각각의 소액지불에 대한 선택 비율 또는 선택 확률($0 < s < 1$)에 기초하고; 평균하여, $1/s$ 의 소액지불 마다 단지 하나가 실제 지불을 위해 선택된다. 선택 비율은 고정되어 있고, 예측 가능하며, 고정되어 있다. 상인에게 제공된 각각의 소액지불에 대하여, 상인은 우선 페이워드 체인의 루트(w_0)에 대한 사용자의 서명을 검증하고, 제공된 해쉬 값(w_k)이 k 번 반복적으로 해쉬될 때 실제로 w_0 를 산출하는지를 검증한다. 그러한 경우, 상인은 사용자로부터 소액지불을 수용한다. 그 후, 상인은 소액지불이 은행에서 예치를 위해 선택되어야 하는지의 여부를 결정하기 위하여, 사용자와의 소정의 대화 프로토콜을 검토한다. 선택되지 않은 수표는 예치될 수 없으므로, 상인에게 가치가 없다: 따라서, 이는 사용자에게 의해 폐기된다. (대화 프로토콜을 통해) 선택되는 소액지불만이 지불을 수신하기 위하여, 상인에 의해 은행에 실제로 제공된다. 이 방식으로, 은행은 각각의 그리고 모든 소액지불을 처리하는 것이 아니라, 단지 $1/s$ 소액지불로부터 하나를 평균하여 처리해야 한다. 이로써 은행은 처리 비용은 상당히 절감된다. 이 프로세스를 상인에게 공정하게 하기 위하여, 각각의 선택된 소액지불에 대해, 상인은 원래 규정된 소액지불 금액보다 $1/s$ 배 더 큰 금액을 지불받게 된다. 바꿔 말하면, 은행은 소액지불의 액면가보다 $1/s$ 배의 값으로 조정되는 금액을 상인에게 지불한다.

이의 장점에도 불구하고, 전자 복권 방식은 사용자 및 상인이 예치를 위해 특정 소액지불을 선택해야 하는지를 결정하기 위하여 각각의 소액지불에 대해 대화를 해야 한다는 결점을 갖고 있다. 이러한 요건은 전자 지불 시스템을 상당히 저속화시키고, 어떤 경우에, 상기 방식은 실용적이지 않다.

상술한 이유로 인해, 소액지불의 글로벌 수집이 은행 처리 비용을 최소화할 수 있지만, 그와 동시에, 소액지불 선택 프로세스에서 사용자-상인 대화를 필요로 하지 않는 비-대화식 소액지불 방법 및 시스템이 필요하다.

게다가, 시간 제약을 소액지불 시스템 내로 통합시키는 것이 바람직하다. 예를 들어, 은행으로부터 지불을 수신하기 위하여, 임의의 지불 가능한 수표(즉, 예치를 위해 적절하게 선택되는 소액지불)를 적절한 시간 기간 내에 은행에서 예치하도록

상인에게 요청하는 시간 제약을 소액지불 시스템 내에 포함시키는 것이 유용할 것이다. 이 방식으로, 사용자는 너무 늦게, 즉, 거래에 대한 가능한 비용이 더 이상 자신의 예산이 아닐 때, 요금청구받지 않을 것이다. 이 유형의 제약은 또한 수표(C)에 대한 시간 정보가 정확한지를 검증하여, 시스템의 보안성을 강화시키는 여분의 인센티브를 상인에게 제공한다.

선택 프로세스에서의 사용자-상인 대화에 기인하는 비효율성 이외에, 확률적 소액지불 방식의 고유한 또 다른 문제점은 사용자가 실제로 소비하는 것을 초과하여 사용자에게 요금청구되는 위험성이다. 확률적 소액지불 방식에서 사용자는 어떤 경우에, 불행히도, (비록 적기는 하나) 자신이 실제로 소비한 것보다 더 많이 지불 가능한 확률을 처리해야 한다. 이와 같은 사건은 드물고, 이와 같은 드문 사건의 상대적인 영향은 행해진 소액지불의 수에 따라 상당히 절감될 수 있다. 그럼에도 불구하고, 아주 적지만, 과도하게 요금청구될 확률은 상기 방식을 광범위하게 수용하는데 있어서 상당한 장애가 될 수 있다. 이것은 통상적인 사용자가 일반적으로 위험성을 관리하는데 익숙하지 않기 때문이다.

상술한 이유로 인해, 은행 처리 비용을 최소화할 뿐만 아니라, 사용자가 결코 자신이 실제로 소비한 것을 초과하여 요금이 청구되지 않는 소액지불 방법 및 시스템이 필요하다.

최종적으로, 자신의 효율을 증가시키고자 하는 소액지불 시스템은 일반적으로 상인에 의한 지불을 위해 선택되었고 일반적으로 지불의 총수의 적은 프랙션만을 구성하는 그러한 지불에 대해서만 작동하여 은행에 호출한다. 그러나, 이와 같은 소액지불 시스템은 지불 선택 프로세스에 대한 제어 및 임의의 유연성을 은행에 제공하지 않는다. 이와 같은 제어는 은행의 위험성을 관리하는데 있어서 은행에 유용할 수 있다.

따라서, 선택 프로세스에서 사용자-상인 대화에 대한 필요성을 제거하고, 과도한 지불의 위험성을 사용자로부터 은행 또는 상인에게 시프트시킬 뿐만 아니라, 지불 선택 프로세스에 대한 제어 및 어떤 유연성을 은행에 제공하는 소액지불 방식이 사용될 수 있는 것이 바람직하다.

(발명의 상세한 설명)

본 발명은 하나 이상의 거래(T)에 대해 사용자(U)(또는 다른 지불인, 이하에서, "U" 또는 "사용자"라 칭함)가 상인(또는 다른 지불받는 사람, 이하에서, "M" 또는 "상인"이라 칭함)으로의 지불을 설정하도록 하는 확률적 소액지불 방식에 관한 것이다. 전형적으로, T는 본 발명에서 특징으로 하는 방식이 임의의 값의 T_V 에 적용 가능할지라도 초저가의 T_V 를 갖는다. 본 발명에서 특징으로 하는 소액지불 방식은 이와 같은 소액지불을 처리하는데 필요한 비용을 최소화함으로써, 시스템의 효율을 상당히 증가시킨다. 이하에서 설명하는 바와 같이, 다수의 부가적인 장점이 또한 제공된다.

본 발명의 제 1실시예에서, 수표를 수신하는 즉시, 그리고, 사용자와의 대화 없이, 지불을 위해 수표를 선택해야 하는지의 여부를 상인이 결정하도록 하는 소액지불 프로토콜이 제공된다. 종래 기술의 확률적 소액지불 방식과 달리, 이 실시예의 소액지불 프로토콜은 대화식 선택 프로토콜이 상인과 사용자 간에 생성될 때까지 확률 결정이 연기되는 것을 필요로 하지 않는다.

본 발명의 제 2실시예에서, 본 발명의 소액지불 방식은 시간 제약을 시스템 내에 통합하고, 이를 특정한 방식으로 사용한다. 이들 시간 제약은 지불을 위해 수표가 선택되도록 하기 위하여, 거래의 시간 및/또는 날짜에 관한 정보가 수표에 제공되고, 수표 상의 시간 정보가 소정의 기준을 충족하는 것을 필요로 한다.

본 발명의 제 3실시예에서, 사용자가 자신이 실제로 소비한 것을 초과하여 요금청구받는 임의의 위험성을 제거하는 선택적 예치 프로토콜이 제공된다.

최종적으로, 본 발명의 제 4실시예는 지불 프로세스에 대한 제어 및 유연성을 은행(또는 다른 제 3당사자 또는 브로커, 이하에서 "은행"이라 칭함)에 제공하는 연기된 선택 프로토콜을 특징으로 한다.

본 발명의 제 1실시예에 따른 소액지불 방식에서, 사용자(U)는 T에 관한 데이터 스트링(C)을 생성하기 위하여 거래(T)에 관한 기록을 사용한다. C는 사용자의 비밀 키를 사용하여, T에 대한 디지털 서명을 생성함으로써 서명되는 전자 수표일 수 있다. 사용자는 상인이 수표(C)를 수신하도록 한다. C의 수신시, 상인은 사용자에 의해 실질적으로 예측될 수 없는 아이템(V)을 C와 관련시킨다. 상인은 V를 C와 관련시키기 위하여 자신에게만 공지되어 있는 비밀 키(SI)를 사용할 수 있다. 예로서, V는 $SIG_M(C)$ 로 표시되고 공개 키 디지털 서명 방식으로 상인의 비밀 서명 키를 사용하여 상인에 의해 생성되는 C에 대한 상인의 디지털 서명일 수 있다.

그 후, 상인은 V가 특성(P)을 충족하는지를 결정한다. 바람직한 형태에서, 특성(P)은 소정의 수표(C)가 지불을 위해 선택되는 확률($0 < s < 1$)과 관련될 수 있다. 상인이 전자 수표(C)로부터 도출된 아이템(V)이 특성(P)을 충족하지 않는다고 결정한 경우, 상인은 단순히 수표(C)를 폐기하고, 은행은 결코 수표(C)를 알지 못한다. 상인이 아이템(V)(예를 들어, $SIG_M(C)$)이 특성(P)을 충족한다고 결정하는 경우, 상인은 V가 P를 충족하는지를 은행이 검증할 수 있도록 하는 정보(I)를 은행이 수신하도록 한다. 예를 들어, I는 V를 생성하는데 사용되는 상인의 비밀 키에 대응하는, 상인의 디지털 서명 방식에 대한 상인의 공개 키일 수 있다(또는 이 키를 포함할 수 있다). I의 수신시, 은행은 V가 특성(P)을 충족하는지를 독립적으로 검증하기 시작한다. 은행이 V가 실제로 특성(P)을 충족한다고 검증하는 경우, 은행은 상인, 또는 상인 이외의 제 4당사자, 또는 자신이 돈의 금액(A)을 수신하도록 한다. 금액(A)은 전형적으로 T_v 보다 더 크며, 하나의 형태에서, 확률(s)의 역수 및 T_v 의 곱과 관련될 수 있다. 금액(A)은 $A = [T_v * 1/s]$ 에 의해 제공될 수 있다.

본 발명의 제 1실시예에 따른, 거래(T)에 대한 지불을 설정하는 시스템은 제 1당사자(사용자 또는 다른 당사자), 제 2당사자(상인 또는 다른 당사자), 제 3당사자(은행 또는 다른 당사자), 및 제 4당사자 간에서 전자 데이터를 전송하는 통신 채널을 포함한다. 상기 시스템은 T로부터 도출된 데이터 스트링(C)을 입력하고 저장하기 위한 제 1당사자에 의해 동작되는 수단을 포함한다. 상기 시스템은 제 1당사자에 의해 실질적으로 예측될 수 없고 C의 적어도 일부와 관련되는 아이템(V)을 입력하고 저장하기 위한, C에 응답하고 제 2당사자에 의해 동작되는 수단을 더 포함한다. 상기 시스템은 V가 특성(P)을 충족하는지를 결정하기 위한, 제 2당사자에 의해 동작되는 수단을 포함한다. 상기 시스템은 V가 P를 충족하는지를 제 3당사자가 검증할 수 있도록 하는 정보(I)를 제 3당사자로 하여금 수신하도록 하기 위한, V가 P를 충족할 때 제 2당사자에 의해 선택적으로 동작되는 수단을 포함한다. 상기 시스템은 제 4당사자로 하여금 금액(A)을 수신하도록 하기 위한, V가 P를 충족할 때 제 3당사자에 의해 선택적으로 동작되는 수단을 더 포함한다.

본 발명의 제 2실시예에서, 시간 제약은 상술한 비-대화식 소액지불 프로토콜 내로 통합된다. 이 실시예에서, 사용자는 부분적으로 시간(t)에 의해 특징 지워지는 거래(T)에 대해 상인에게 지불을 설정할 수 있다. 전형적으로 시간(t)은 거래(T)가 발생하는 시간 및/또는 날짜를 나타낸다. 사용자는 T와 관련되는 데이터 스트링(C)을 생성한다. 이 실시예에서, C는 T의 시간(t)에 관한 정보를 포함해야 한다. 사용자는 상인이 t에 대한 정보를 포함하는 C, 또는 C의 적어도 일부를 수신하도록 한다. 상인은 사용자에게 의해 실질적으로 예측될 수 없는 아이템(V)을 C(또는 자신이 수신하였던 C의 부분)과 관련시킨다. 아이템(V)은 C에 대한 시간 정보, 예를 들어, 시간 정보를 포함하는 C의 적어도 일부의 (상인의 비밀 키를 사용하여 생성된) 상인의 디지털 서명의 함수이다. V는 또한 $G(C)$ 의 디지털 서명일 수 있고, 여기서 $G(C)$ 는 C의 함수, 또는 C를 사용한 알고리즘을 나타낸다. 예를 들어, $G(C)$ 는 C의 시간/날짜 정보(예를 들어, C의 정확하게 동일한 시간/날짜 정보, 또는 "반올림된" 시간/날짜 정보), 또는 C가 관련되는 거래(T)의 시간/날짜 정보를 리턴시키는 함수일 수 있다. 그 후, 상인은 V가 특성(P)을 충족하는지를 결정한다. V가 P를 충족하는 경우, 시간(t')에서 상인은 V가 P를 충족하는지를 은행이 검증할 수 있도록 하는 (예를 들어, V를 생성하는데 사용되는 상인의 비밀 키에 대응하는 상인의 공개 키를 포함할 수 있는) 정보(I)를 은행이 수신하도록 한다.

본 발명의 제 2실시예에서, 은행이 제 4당사자로 하여금 금액(A)을 수신하도록 하기 위하여, $t' - t$ 는 소정의 시간 간격보다 적어야 한다. 이것은 V가 P를 충족하는 요건 이외의, 또 다른 요건이다. 바꿔 말하면, 은행은 상인이 규정된 시간 한도인 (거래(T)가 발생했던) 시간(t)에 관한 정보를 포함하는 지불 가능한 수표를 제공하는 경우에만 상인의 계좌에 대변할 것이다. 예를 들어, 거래(T)가 날짜(i)에 발생한 경우, 상인은 날짜(i), 또는 날짜(i+1), 또는 날짜(i+n) 한도 내에 대응하는 수표(C)를 예치하는 것을 요청받을 수 있고, 여기서 n은 소정의 정수이다. 따라서, 프로토콜에서의 시간 제약은 적시의 예치를 요청할 수 있다. 적시의 예치를 요청하면 사용자가 너무 늦게 요금청구받지 않도록 함으로써 장점이 제공된다; 이것은 또한 은행이 "백-데이팅(back-dating)되는 수표로부터 발생하는 것과 같은 다른 형태의 위험성을 제어하도록 한다.

본 발명의 제 3실시예에서, 사용자가 결코 자신이 실제로 소비한 것보다 많이 요금청구받지 않도록 하는 선택적 예치 프로토콜이 제공된다. 하나 이상의 거래($T_i (i=1, \dots, n)$) 각각에 대하여, 사용자는 근원적인 확률적 지불 방식에 따라, (은행이 T_i 와 같은 거래를 처리하도록 하는데 필요한 비용의 단지 일부분의 가치가 있는) 액면가(TV_i)를 갖는 수표/소액지불(C_i)을 도출하도록 한다.

본 발명의 제 3실시예에서, 각각의 수표(C_i)는 바람직하게는, 1로부터 시작하는 점진적인 일련 번호(S_i)를 나타낸다. 일련 번호(S_i)는 바람직하게는, 사용자에게 의해 도출되는 시간-순서화된 연속적인 수표에서 다른 수표와 관련된 수표(C_i)의 위치

를 나타낸다. 제 3실시예에서, 사용자에게 대한 수집 차변 금액은 사용자에게 의해 실제로 소비된 수집 금액보다 결코 크지 않게 되며, 편의상 TV_{agg} 로 표시된다. 전형적으로, 사용자가 i -번째 수표를 기록할 때, 수집 금액(TV_{agg})은 자신의 수표의 수집 금액, 즉;

$TV_{agg}=TV_1+TV_2+...+TV_i$ 에 의해 제공된다.

예를 들어, 본 발명의 제 3실시예에서 특징으로 하는 소액지불 방식은 C_i 가 지불 가능한 것으로 인식되는 제 1수표이고 D_i 가 대응하는 차변 금액인 경우에, D_i 가 $TV_{agg}=TV_1+TV_2+...+TV_i$ 보다 크지 않도록 한다. 이러한 보증은 은행이 상인으로부터 수신하는 수표의 일련 번호를 추적하는 프로토콜을 통하여 성취된다. 사용자에게 차변하기 전, 은행은 순서화된 연속적인 수표 사이에서, 지불이 행해졌던 최종 수표에 대한 일련 번호(S_{max})를 결정해야 한다. 설명적인 경우에, 모든 거래는 동일한 값(TV)의 가치가 있다. 이 경우에, C_i 가 다음 지불 가능한 수표라면, 은행은 사용자가 금액($D_i=(S_i-S_{max})*TV$)으로 차변받도록 한다. 따라서, 금액(D_i)은 단지 최종 지불이 행해진 이래로 사용자가 기록했던 수표의 수만을 따르며, 수집 차변 금액은 S_i*TV 보다 크지 않게 된다.

최종적으로, 본 발명의 제 4실시예에서, 지불 프로세스에 대한 더 큰 제어 및 유연성을 은행에 제공하는 연기된 선택 프로토콜이 제공된다. 본 발명의 이전 실시예에서와 같이, 사용자는 값(TV_i)을 각각 갖는 하나 이상의 거래($T_i(i=1,...,n)$) 각각에 대하여 데이터 스트링 또는 "수표"(C_i)를 도출하고, 상인이 C_i 를 수신하도록 한다.

본 발명의 제 4실시예에서, 상인은 m 개의 리스트(L^k)와 자신이 수신하였던 수표(C_i)의 그룹을 특정하게 관련시키는데, 여기서 $k=1,...,m$ 이다. 각각의 리스트(L^k)는 데이터 스트링($C_1^k,...,C_{l_k}^k$)을 포함하는데, 여기서, l_k 는 소정의 리스트(L^k)에서 수표의 총수를 나타낸다. 따라서, n 이 모든 m 개의 리스트에서 수표의 총수라면, $\sum_{k=1}^m l_k=n$ 이다.

상인은 각각의 L^k 에 대해 커미트먼트(commitment)(CM^k)를 계산함으로써 m 개의 리스트(L^k)에 커미트한다. 커미트먼트(CM^k)는 바람직하게는, 해쉬 값($H(L^k)$)이며, 여기서, H 는 일방향 해쉬 함수이다. 상인은 은행이 커미트먼트(CM^k)($k=1,...,m$)를 수신하도록 한다.

(CM^k)($k=1,...,m$)의 수신시, 은행은 하나 이상의 정수 인덱스($i_1 i_2,...,i_r$)를 선택함으로써 본 발명의 제 4실시예에서 특징으로 하는 연기된 선택 프로토콜을 구현한다. r 의 값은 임의적이며, 은행까지이다. 은행은 상인이 선택된 인덱스($i_1 i_2,...,i_r$)를 수신하도록 한다.

선택된 인덱스($i_1 i_2,...,i_r$)의 수신에 응답하여, 상인은 $CM^{i1}, CM^{i2}...CM^{ir}$ 을 디커미트(de-commit)함으로써, $L^{i1},...L^{ir}$ 을 제 3당사자(예를 들어, 은행)에 나타낸다. (은행이거나, 은행 이외의 실체일 수 있는) 제 5당사자는 (상인이거나, 상인 이외의 실체일 수 있는) 제 4당사자로 하여금 대변 금액(CR)을 수신하도록 한다. 제 5당사자는 사용자가 차변 금액(D) 만큼 차변 받도록 한다.

바람직하게는, 대변 금액(CR)은 V^k 와 관련되며, 여기서 V^k 는 소정의 리스트(L^k)에 포함되는 모든 수표의 수집값을 나타내는데, 즉,

$V^k=TV_1^k+...+TV_{l_k}^k$ 이다.

대변 금액(CR)은 m 개의 리스트 모두에 포함된 모든 수표의 수집값에 의해 제공될 수 있는데, 즉,

$CR=V^1+...+V^k+...V^m=\sum_{k=1}^m V^k$ 이다.

이 경우에, 값(V^i)에 대한 커미트먼트는 목록에 대한 커미트먼트(CM^i)가 제공될 때 은행에 제공될 수 있다; 모든 값(V^i)은 은행이 자신의 인덱스를 규정함으로써 리스트 중 일부를 선택한 후 디커미트된다.

대안적으로, 대변 금액(CR)은 단지 그 인덱스가 은행으로부터 선택되었던 리스트에 포함되는 모든 수표의 수집값과 관련될 수 있다. 이러한 대변 금액(CR)은 은행이 단지 수표의 프랙션(r/m)만을 알고 있다는 사실을 반영하기 위하여, m/r (여기서, 정수 m 및 r 은 상기에 참조됨)와 같은 배율만큼의 막 언급된 수집값과 관련될 수 있다.

대응하는 차변 금액(D)은 여러 방식 중 하나에서 도출될 수 있다: D를 도출하는 방법의 선택은 CR을 계산하는 방법과 관련되거나 관련되지 않을 수 있다. 예를 들어, 값(D)은 그 인덱스가 은행에 의해 선택되어 상인에게 전달되는 인덱스와 정합하는 목록에 포함된 모든 수표의 수집값($V^{i1} + V^{i2} + \dots + V^{ir}$)과 관련될 수 있다; 예를 들어, 이 값은 m/r 과 같은 팩터만큼 스케일링된 이의 합산 값일 수 있다. 또는 값(D)은 대변 금액(CR)으로부터 도출될 수 있다; 예를 들어, 이 값은 대변 금액(CR)과 동일할 수 있다. 또는, 값(D)은 선택된 리스트 내에 포함된 수표의 일련 번호로부터 상술한 방식으로, 도출될 수 있다. 대부분의 애플리케이션에서, 다수의 상이한 사용자가 존재할 것이며, 각 사용자가 청구받을 금액은 선택된 리스트에서 그 사용자가 기록했던 수표에 따를 것이다. 각 사용자(U)에 대한 차변 금액(D_u)을 계산하는 바람직한 방법은 사용자(U)가 기록했던 수표의 일련 번호에 기초한 방법을 사용하는 것이다.

(도면의 간단한 설명)

본 발명은 첨부 도면과 함께 취해진 다음의 상세한 설명을 참조함으로써 더 충분하게 이해될 수 있다.

도 1은 본 발명은 제 1실시예에 따른, 소액지불을 위한 방법의 개요를 개략적인 흐름도 형태로 제공하는 도면.

도 2는 본 발명의 제 1실시예에 따른, 거래에 대한 지불을 설정하는 소액지불 시스템의 구성요소를 설명하는 개략적인 블록도를 제공하는 도면.

도 3은 본 발명의 제 2실시예에 따른, 소액지불 거래용 방법의 개요를 흐름도 형태로 제공하는 도면.

도 4는 사용자가 실제로 소비한 것을 초과하여 요금청구받을 위험성을 제거하는 선택적 예치 프로토콜을 포함하는, 본 발명의 제 3실시예에 따른 소액지불 거래를 위한 방법의 개요를 흐름도 형태로 제공하는 도면.

도 5는 본 발명의 제 3실시예에 따른, 거래에 대한 지불을 설정하는 소액지불 시스템의 구성요소를 설명하는 개략적인 블록도를 제공하는 도면.

도 6은 본 발명의 제 4실시예에 따른 소액지불 거래를 위한 방법의 개요를 흐름도 형태로 제공하는 도면.

도 7은 본 발명의 제 4실시예에 따른, 거래에 대한 지불을 설정하는 소액지불 시스템의 구성요소를 설명하는 개략적인 블록도를 제공하는 도면.

(실시예)

본 발명에서, 소액지불 방식의 효율 및 유연성을 증가시키는 방법 및 시스템이 제공된다.

본 발명에서, 소액지불 시스템은 적어도 제 1당사자, 제 2당사자, 및 제 3당사자를 포함한다. 본 발명의 하나의 형태에서, 제 1당사자는 지불인, 예를 들어, 소비자 또는 사용자를 나타낼 수 있다. 제 2당사자는 지불받는 사람, 예를 들어, 상품의 상인 또는 서비스의 벤더를 나타낼 수 있다. 제 3당사자는 브로커 또는 은행일 수 있다. 부가적인 당사자가 또한 포함될 수 있다. 어떤 상황에서, 단일 실체가 하나 이상의 당사자의 역할: 예를 들어, 제 2당사자 및 제 3당사자 둘 다의 역할을 할 수 있다. 일례는 사용자가 자신의 은행에 소액지불을 행하고자 하는 상황일 것이다. 대안적으로, 단일 실체가 제 2당사자 및 제 4당사자 둘 다의 역할을 할 수 있다.

참조의 용이함을 위하여, 다음에서, 각각, "제 1당사자"를 참조하기 위하여 용어 "사용자"를 사용할 수 있고, "제 2당사자"를 참조하기 위하여 용어 "상인"을 사용할 수 있으며, 제 3당사자 브로커를 참조하기 위하여 용어 "은행"을 사용할 수 있다. 그러나, 제 1당사자가 사용자일 필요가 없고, 제 2당사자가 상인일 필요가 없으며, 제 3당사자가 브로커 또는 은행일 필요가 없다는 것이 이해되어야 한다.

최종적으로, 부가적인 당사자가 또한 본 발명을 따른 소액지불 방식에 포함될 수 있다. 예를 들어, 제 3당사자는 (아마도 제 2당사자와 협동하는) 제 4당사자가 지불을 수신하도록 할 수 있다. 예를 들어, 제 1당사자는 요금징수소(toll booth)를 통과하는 자동차운전자의 지불 장치일 수 있고, 제 2당사자는 요금 징수소에서 장치일 수 있으며, 제 3당사자는 자동차운전자의 은행일 수 있고, 제 4당사자는 징수 요금 실체일 수 있다. 이 경우에, 자동차운전자는 요금징수소 장치에서 소액지불을 제공할 수 있고, 적절한 조건이 발생하면, 자동차운전자의 은행에 의해 요금 징수 실체로 지불이 행해질 수 있다. 다른 예로서, 제 5당사자가 포함될 수 있다: 제 3당사자는 제 5당사자가 제 4또는 제 2당사자에게 실제로 지불을 행하도록 할 수 있다. 예를 들어, 이전 예에 부연하면, 제 3당사자는 지불 장치의 제조자 또는 지불 장치를 제어하거나 임대하는 실체일 수 있고, 제 5당사자는 궁극적으로 제 4당사자에게 돈을 지불할 수 있는 자동차운전자의 은행일 수 있다. 동일한 제 5당사자, 또는 제 3당사자 또는 또 다른 제 6당사자는 실제로 그를 대신하여 제 1당사자 또는 또 다른 당사자에게 실제로 차변할 수 있다.

I. 비-대화식 소액지불 방식

본 발명의 제 1실시예에서, 소정의 지불이 선택되어야 하는지의 여부를 결정하기 위하여, 상인이 사용자와 대화할 필요성을 제거하는 소액지불 방식이 제공된다. 이 실시예에서, 사용자는 지불을 행하고자 할 때, 전자 문서 또는 "수표"를 생성하고, 상인이 수표를 수신하도록 한다. 이 실시예에서, 상인은 수표를 수신하는 즉시, 사용자의 계좌의 적절한 차변 및 상인의 계좌의 대변이 발생할 수 있도록 수표가 은행으로의 제공을 위해 선택되어야 하는지의 여부를 결정할 수 있다. 상인은 사용자와의 대화 없이 이와 같은 결정을 행할 수 있다. 종래 기술의 전자 복권 소액지불 방식의 경우와 달리, 사용자와 상인 간에 대화식 선택 프로토콜이 발생할 때까지 이와 같은 결정을 연기할 필요가 없다. 이 방식으로, 소액지불 프로세스의 효율이 상당히 강화된다.

본 발명의 제 1실시예에서, 사용자는 전형적으로 거래(T), 또는 일련의 이와 같은 거래로 이해 상인에게 돈을 지불할 필요가 있다. 거래는 전형적으로, 초저가, 예를 들어, 1센트 또는 1센트의 프랙션일 수 있는 거래 값(T_v)에 의해 특징지워진다. 따라서, 은행이 모든 단일 거래에 대한 지불을 처리한다면, 은행에서 거래 값 자체보다 처리 비용이 훨씬 더 많아 질 수 있다.

도 1은 본 발명의 제 1실시예에 따른, 소액지불 거리를 위한 방법의 개요를 개략적인 흐름도 형태로 제공한다. 사용자는 본 발명을 따른 소액지불 방식으로 지불을 행하고자 할 때, 데이터 스트링 또는 "전자 수표"(C)를 생성하여, C를 상인에게 전송하거나, 사용자가 C를 수신하도록 한다. 수표(C)는 전형적으로, 거래의 기록(T)으로부터 도출된다. 예를 들어, 수표(C)는 사용자의 비밀 키를 사용하여 거래에 대한 디지털 서명($SIG_U(T)$)을 생성함으로써 생성될 수 있다; 사용자에게 의한 이러한 서명은 상인에 의해 검증된다. 사용자의 서명($SIG_U(T)$)은 이 검증이 진행될 수 있도록 하는 T에 관한 충분한 정보를 포함하거나, 이러한 정보가 수반될 수 있다. 사용자는 또한 상인이 사용자의 디지털 서명의 검증을 가능하게 하는 디지털 인증서를 수신하도록 하거나, C에 통합하도록 할 수 있다 - 예를 들어, 디지털 인증서는 U의 디지털 서명을 검증하는데 사용될 U의 공개 키를 규정함. 각 수표(C)는 지불을 위해 선택되는 확률 또는 선택 비율(s)($0 < s < 1$)을 가질 수 있다.

상인은 자신의 비밀 키를 사용하여 생성되는, 사용자에게 의해 실질적으로 예측될 수 없는 아이템(V), 예를 들어, C에 대한 디지털 서명을 수표(C)와 관련시킨다. 그 후, 상인은 V가 어떠한 특성(P)을 충족하는지를 결정한다. 본 발명의 바람직한 실시예에서, V가 P를 충족할 확률은 선택 비율(s)과 동일하다. V가 실제로 P를 충족한다는 것을 상인이 확인한 경우, 상인은 V가 P를 충족하는지를 은행이 검증할 수 있도록 하는 정보(I)를 은행이 수신하도록 한다. 그렇지 않은 경우, 상인은 수표(C)를 폐기한다. I의 수신시, 은행은 존재한다면, 수표 상의 사용자의 서명을 검증할 수 있고, 서명이 검증되지 않으면 수표를 폐기한다. 은행은 예를 들어, 계좌가 여전히 양호한 상태인지(예를 들어, 관련 사용자의 디지털 인증서가 폐지되었는지)를 결정하는 것과 같은 은행에서 사용자의 계좌의 상태에 관한 것들에 대한 다른 테스트를 수행할 수 있다; 은행은 이와 같은 테스트가 통과되지 않은 경우 수표를 수신하지 않는 것을 선택할 수 있다. 그 후, 은행은 V가 P를 실제로 충족하는지를 검증하고, V가 P를 충족하는 경우에만 상인이 총액을 수신하도록 한다.

이제, 본 발명에서 특징으로 하는 소액지불 방식의 각 요소를 보다 상세히 참조하면, 본 발명에서 지불을 발생시키는 "거래"는 사용자가 상인에게 돈을 지불할 수 있는 광범위한 가능한 상황을 커버한다. 예를 들어, 사용자는 서비스, 정보, 또는 물

리적인 상품을 구매하기 위하여 사용자에게 돈을 지불할 수 있다. 대안적으로, 사용자는 예를 들어, 상인에게 기부를 행하기 위하여 임의의 구매를 행하지 않고, 상인에게 돈을 지불할 수 있다. 전형적인 거래(T)의 예로는 사용자가 정보 웹사이트, 웹 페이지마다 방문하는 것(각각의 방문된 웹 페이지가 단일 거래(T)를 나타냄), 또는 오디오/비디오 재료가 분마다 사용자에게 스트리밍되는 것(스트리밍되는 오디오/비디오 재료의 각각의 분이 단일 거래(T)를 나타냄)을 들 수 있지만, 이에 제한되지 않는다.

거래의 기록(T)은 거래의 설명적인 세부항목을 포함하는 데이터 스트링일 수 있다. 예를 들어, 기록(T)은 다음: 지불되는 금액; 만약 있다면, 구매될 상품의 설명; 사용자 및/또는 상인의 아이덴티티; 사용자 및/또는 상인의 공개 키; 사용자 및/또는 상인에 대한 디지털 인증서; 거래의 날짜와 시간; 은행 또는 금융 서비스 제공자와 같은 임의의 관련된 제 3당사자의 신분증명, 및 사용자의 계좌를 식별하는데 필요한 임의의 부가적인 정보 중 하나 이상을 규정할 수 있다. 거래는 이하에서, 거래를 나타내는 기록(T)으로 참조되는데, 즉, 어구 "거래(T)"는 거래를 나타내는 기록(T)을 참조하는데 사용될 것이다.

사용자에 의해 도출되는 데이터 스트링(C)은 전형적으로 거래에 대해 소정 액을 지불하는 사용자에게 의한 커밋먼트를 포함하는 전자 수표(종종 지불지시서라 칭함)를 나타낸다. 전형적으로, 수표(C)의 기명 액면가는 거래(T)에 대한 거래 값(T_v)이다. 다른 정보가 또한 수표(C)에 포함될 수 있다. 예를 들어, C는 거래(T), 또는 거래(T)의 적어도 일부, 또는 거래(T)의 표시를 포함할 수 있다. 본 발명의 바람직한 실시예에서, 데이터 스트링 또는 전자 수표(C), 또는 C의 적어도 일부가 인증된다. 인증은 종래 기술에 공지된 바와 같이, 다양한 방법에 의해 성취될 수 있다. 예를 들어, 수표(C)는 디지털 서명, 또는 메시지 인증 코드를 통하여 또는 인증된 세션에서 전송됨으로써 인증될 수 있다. 수표(C)는 예를 들어, 사용자의 요청시, 또는 사용자를 대신하여, 사용자 이외의 당사자에 의해 인증될 수 있다. 이러한 인증 방법은 사용자가 익명 구매를 행하고자 하는 상황에서 특히 유용하다. 종래 기술에 공지되어 있는 임의의 다른 인증 방식이 또한 본 발명의 범위 내에 존재한다.

사용자는 수표(C)를 생성할 때, 자신은 알고 있지만 상인에게는 공지되지 않은 비밀 정보를 사용할 수 있다. 전형적으로, 이 비밀 정보를 인지하지 못하는 사람의 경우에, 수표(C)를 생성하는 것이 계산적으로 실행 가능하지 않다. 본 발명의 바람직한 실시예에서, 수표(C)를 생성하는 프로세스는 공개 키 디지털 서명 시스템에서의 사용자에게 의한 디지털 서명의 생성과 관련되며, C를 생성하기 위해 사용자가 사용하는 비밀 정보는 이 시스템에서 사용자의 비밀 서명 키이다. 이 실시예에서, 데이터 스트링(C)은 편리하게는, $SIG_U(T)$ 로 표시된 이 시스템에서의 거래(T)에 대한 사용자의 디지털 서명을 포함한다.

$SIG_U(T)$ 는 사용자의 비밀 키를 사용하여 사용자에게 의해 생성된다. 사용자는 자신의 디지털 서명을 생성하기 위하여, 종래 기술에 공지되어 있는 디지털 서명 방식 중 어느 하나를 사용할 수 있다. 특히, 사용자의 디지털 서명 방식은 다음: 결정론적 서명 방식; 램덤화된 서명 방식; Shamir에 의해 제안된 바와 같은 아이덴티티 기반으로 한 서명 방식; 온라인 서명 방식; 오프라인 서명 방식; 및 지정된 검공기 방식을 포함할 수 있지만, 이에 제한되지 않는다. 스트링(C)은 또한 거래(T)에 관한 정보와 같은 다른 정보를 포함할 수 있다.

전자 수표(C)를 생성하였다면, 사용자는 상인이 C를 수신하도록 한다. 사용자가 상인으로 하여금 C를 수신하도록 할 수 있는 다양한 방식이 존재한다. 사용자는 단순히 수표(C)를 상인에게 전송할 수 있다. 대안적으로, 사용자는 수표(C)를 상인에게 전송하도록 다른 당사자에게 요청할 수 있다. 사용자는 상인이 상이한 시간에 상이한 부분에서 수표(C)를 수신하거나 수표에 접근하도록 할 수 있다. 예를 들어, 사용자는 임의의 거래(T)가 발생하기 전에, 초기에 사용자의 공개 키를 수신하거나 이 키에 접근하도록 할 수 있다. 그 후, 사용자는 상인이 나중에 C에 대한 사용자의 디지털 서명, C의 일부, 또는 T(또는 이의 일부)에 관련된 양을 수신하거나, 이들에 접근하도록 할 수 있다.

상인은 수표(C)가 접근 가능한지 아닌지, 즉, 수표(C)가 실제로 사용자에게 의해 서명되는지 아닌지, 및 수표(C)의 내용이 순전하고 완전한지 아닌지를 결정할 수 있다. 이를 성취하기 위하여, 상인은 수표(C)를 생성하는 사용자에게 특정되는 공개 검증 정보를 검토할 수 있다. 이 사용자-특정 공개 검증 정보는 C, 또는 더 일반적으로는, 예를 들어, 사용자가 소액지불을 행하는데 있어서 인증받아서, 사용자의 소액지불이 받아들여진다는 것을 증명하는 디지털 인증서를 생성하기 위하여 사용자가 사용하는 비밀 키에 대응하는 사용자의 공개 키일 수 있다. 목적 둘 다, 즉, 사용자가 소액지불을 행하도록 인정받았다는 것 및 소액지불 수표에서 사용자의 디지털 서명을 검증하기 위하여 소정의 공개 키가 사용되어야 한다는 것을 나타내기 위하여 동일한 디지털 서명이 사용될 수 있다. 상인은 수표(C)에 대한 디지털 서명이 인증되는지를, 즉, 실제로 사용자에게 의해 생성되는지를 점검하기 위하여, 사용자의 공개 키를 사용할 수 있다. 사용자가 아이덴티티 기반으로 한 디지털 서명 방식을 사용하는 경우, 공개 검증 정보는 사용자의 아이덴티티의 사양을 포함할 수 있다. 이와 같은 사용자-특정 공개 검증 정보는 상인에 의해 사용자로부터 직접 획득될 수 있다. 대안적으로, 이와 같은 공중 검증 정보는 상인에 의해 디지털 인증서, 또는 사용자에게 관한 공적으로 이용 가능한 정보(예를 들어, 공개 키의 공개된 디렉토리), 또는 수표(C)와 관련하여 또는 수표(C)의 부분으로서 사용자에게 의해 전송된 정보로부터 획득될 수 있다. 사용자-특정 공개 검증 정보는 일반인에게 이용 가능할 필요는 없다; 이 정보는 단지 상인(들) 및 은행에 이용 가능할 필요가 있다.

상인은 자신이 획득한 사용자-특정 공개 검증 정보의 인증을 점검하기 위한 단계를 취할 수 있다. 이러한 단계는 디지털 서명 및 사용자-특정 공개 검증 정보에 관한 다른 인증 정보를 검증하는 단계; 디지털 인증서에 대한 서명을 검증하는 단계; 디지털 인증서의 만기일을 점검하는 단계; 및 디지털 인증서가 폐지되었는지를 결정하는 단계를 포함할 수 있지만, 이에 제한되지 않는다. 상인은 또한 사용자가 실제로 전자 수표(C)를 기록하도록 인증받았는지를 디지털 인증서로부터 확인할 수 있다; 이는 예를 들어, 수표(C)의 금액, 계좌 번호, 일련 번호 또는 다른 정보에 대한 부가적인 점검을 포함할 수 있다.

상인은 사용자에게 의해 실질적으로 예측될 수 없는 아이템(V)을 자신이 수신한 모든 수표(C)와 관련시킨다. 예를 들어, 아이템(V)은 사용자가 C로부터 V를 도출하는 것이 계산적으로 실행 가능하지 않기 때문에, 즉, 사용자가 아이템(V)의 값을 도출하기 위하여 비실용적인 양의 계산을 수행할 필요가 있기 때문에, 사용자측에서는 실질적으로 예측할 수 없다. 본 발명의 하나의 실시예에서, 아이템(V)은 사용자에게 공지되어 있는 것이 아니라, 단지 상인에게 공지되어 있는 비밀 정보(SI)를 사용하여 C로부터 실행 가능하게 도출될 수 있다. 하나의 실시예에서, 비밀 정보(SI)는 공개 키 디지털 서명 방식의 상인의 비밀 키일 수 있다.

하나의 형태에서, 상인에 의해 C와 관련되는 아이템(V)은 편의상 $SIG_M(C)$ 로 표시되고, 공개 키 디지털 서명 방식으로 상인의 비밀 키를 사용하여 상인에 의해 생성되는 C에 대한 상인의 디지털 서명일 수 있다. 상인에 의해 사용되는 디지털 서명 방식은 C를 생성하기 위하여 사용자가 사용하는 서명 방식과 반드시 동일할 필요는 없고, 사용자의 서명 방식과 상이한 서명 방식일 것이다. 이 상황에서, C가 $SIG_u(T)$ 와 동일하거나, 이를 포함하는 경우, 아이템(V)은 $V=SIG_M(C)$ 에 의하여 제공될 수 있다. 따라서, $SIG_M(C)$ 는 사용자가 결코 상인의 비밀 서명 키를 인지할 수 없기 때문에, 사용자가 예측할 수 없는 양이다. 그러므로, 사용자가 예를 들어, 특정 거래(T)를 선택함으로써 자신의 원하는 임의의 방식으로 수표(C)를 제어할 수 있을지라도, $SIG_M(C)$ 는 사용자가 관련되는 한, 본질적으로 '랜덤'일 것이다. 본 발명의 다른 형태에서, V는 비밀 MAC 키를 사용하여 상인에 의해 계산되는 MAC(메시지 인증 코드) 값일 수 있다; 이 MAC 키는 사용자가 아니라, 상인 및 은행에 공지될 수 있다. 본 발명의 어떤 형태에서, C의 상인의 서명은 단지 (C에서의 날짜 및 시간, C에 포함된 랜덤 스트링, 또는 C에 포함된 일련 번호와 같은) C의 일부, 또는 C와 관련된 양의 MAC 또는 상인의 서명을 포함하도록 해석될 수 있다.

아이템(V)을 계산하는 단계는 반드시 시간적으로 사용자로부터 C를 수신하는 단계 다음에 수행될 필요는 없다. 예를 들어, 아이템(V)은 거래(T)에 관한 데이터 정보에 대한 상인의 디지털 서명일 수 있다. 상인은 C를 수신하기 전, 이 디지털 서명을 계산할 수 있다.

바람직한 실시예에서, 상인은 수신되었던 수표 중 어느 것이 지불을 위해 선택되어야 하는지를 결정하기 위하여 선택 절차를 사용한다. 상인은 단지 "선택된" 수표만을 은행에 전송하고, 임의의 선택되지 않은 수표를 은행에 전송하지 않는다. 사용자가 수표를 생성하는 시간에, 수표가 상인에 의해 선택될지 아닌지를 사용자가 결정하는 것이 계산적으로 실행 가능하지 않다. 실제로, 사용자는 자신이 궁극적으로 이와 같은 선택 절차를 습득하지 않을지라도, 상인이 선택 프로세스를 사용하고 사용자의 수표의 일부만을 은행에 전송한다는 것을 인지하거나 인지하지 못할 수 있다.

선택 절차의 부분으로서, 상인은 C와 관련된 아이템(V)이 특성(P)을 만족시키는지를 결정한다. 본 발명의 바람직한 실시예에서, 수표(C)가 지불을 위해 선택되는지 아닌지에 관한 결정은 V가 P를 충족하는지에 의해 정해진다.

바람직한 형태에서, 상인에 의해 사용되는 선택 절차는 각각의 선택된 수표에 대하여, 지불을 위해 선택되는 자신의 선택 비율 또는 "확률"을 추정할 수 있게 된다. 특히, 선택 절차는 모든 수표의 고정된 프랙션을 선택하기 위하여 추정되는 것일 수 있다 이 경우에, 특성(P)은 상수와 관련될 수 있고, 여기서 $0 < s < 1$ 이며, s는 소정의 소형지불이 실제 지불을 위해 선택될 확률이고, 이 확률은 고정되며 공지되어 있다. 대안적으로, V는 데이터 스트링(C)이나 이의 일부, 또는 기록(T)이나 이의 일부, 또는 데이터 스트링(C) 및 기록(T)의 조합으로부터 결정될 수 있는 확률로 P를 충족한다. 바꿔 말하면, 선택되는 수표의 프랙션은 수표(C)에서 사용자에게 의해 제공되는 파라미터에 따를 수 있다. 예를 들어, 이는 수표의 금액에 따를 수 있다. 대안적으로, 값(s)은 사용자의 공개 키를 사용자와 바인딩하는 사용자의 디지털 인증서 내에 규정될 수 있다. 대안적으로, 특성(P)은 아이템(V)의 값의 상수 프랙션에 대해 유지하게 될 수 있다. 대안적으로, 특성(P)은 V의 어떤 프랙션(F)에 대하여 유지하게 될 수 있고, 여기서 프랙션(F)은 데이터 스트링(C), 기록(T), C와 T의 부분, 또는 C와 T의 조합으로부터 결정될 수 있다. 대안적으로, 상인은 s 및/또는 특성(P)을 결정하는데 사용될 수 있는 정보를 은행으로부터 획득할 수 있다.

특성(P)은 미리, 즉, 거래(T)가 발생하기 전에 규정될 수 있고, 수표(C)는 T로부터 도출된다. 이와 같은 특성(P)의 예가 존재한다: "V의 최종 10 비트가 x보다 적은 수에 대응하고, 여기서 x는 상수이다." 대안적으로, 특성(P)은 거래(T), 또는 수표(C), 또는 이의 조합 내에 규정되거나, 이들로부터 획득될 수 있다. 이와 같은 특성(P)의 예가 존재한다: "V의 최종 10 비트는 C의 최종 10비트에 대응하는 수보다 적은 수에 대응한다." 선택 비율(s)이 결정되는 방식은 상기 방법의 조합, 또는 이의 변형을 포함할 수 있고, 이들은 당업자들에게는 명백할 것이다.

하나의 형태에서, 상인은 V가 P를 충족하는지를 결정하기 위하여 상인에게만 공지되어 있는 비밀 정보(SI)를 사용할 수 있다. 이와 같은 비밀 정보(SI)는 예를 들어, 공중-키 디지털 서명 방식인 상인의 비밀 키, 공개-키 암호방식의 상인의 비밀 키, 또는 공개-키 디지털 암호화 방식의 상인의 비밀 키를 포함할 수 있다. 바람직하게, 상인의 디지털 서명 알고리즘은 결정론적이어야 한다.

본 발명의 하나의 실시예에서, 특성(P)은 다음 형태:

$$F(V)=F(\text{SIG}_M(C))<s \text{ (1)을 취할 수 있고,}$$

여기서 F()는 입력으로 임의의 비트 스트링을 취하고, 출력으로서 0과 1 사이의 수를 리턴시키는 공중 함수를 나타내고, s는 0보다 크고 1보다 작은 상수이며 소액지불 방식에 대한 선택 비율, 즉, 소정의 수표(C)가 지불을 위해 선택되는 확률을 나타낸다(또는 적어도 결정한다). 하나의 예로서, F는 0 및 포인트를 프리-펜딩(pre-pending)하고, 그 결과를 이진수로서 해석함으로써 이진 입력 스트링(V)에 작용한다. 이 예에서, V가 입력 스트링 "011"이라면, F는 십진법 분수 3/8로서 해석되는 "0.011"를 산출하도록 V에 작용한다. 상술한 바와 같이, $\text{SIG}_M(C)$ 가 본질적으로 랜덤(예측될 수 없는) 수이기 때문에, $F(\text{SIG}_M(C))$ 가 또한 랜덤이며, 0과 1 사이의 충분히 긴 수이다. 따라서, $F(\text{SIG}_M(C))$ 는 비율(s)보다 적으므로, 본질적으로 사용자가 상인이 수신하도록 하는 모든 수표(C)의 프랙션(s)에 대하여 특성(P)이 충족된다. 다른 실시예에서, 함수(F)는 우선 해쉬 함수 또는 다른 결정론적 함수를 자신의 입력 값에 적용하고 나서, 0 및 포인트를 프리-펜딩하고, 그 결과를 이진수로서 해석함으로써 이전과 같이 진행한다. 다른 실시예에서, 특성(P)은 다음 형태:

$$F(V)=F(\text{SIG}_M(G(C)))<s \text{ (1')를 취할 수 있고,}$$

여기서 G()는 데이터 스트링을 생성하기 위하여 수표에 적용되는 함수를 나타낸다. 예를 들어, 함수(G)는 수표(C)의 일련 번호를 리턴시킬 수 있다.

지불을 위해 수표를 선택해야 하는지를 결정하기 위하여, 상인이 사용자와 대화할 필요가 없다는 것이 강조되어야 한다. 특성(P)이 식(1)에 따라 결정되는 경우에, 수표(C)가 지불 가능한지를 상인이 즉시 검증할 수 있다는 것이 용이하게 인지된다: 상인은 자신의 비밀 서명 키를 사용하여 $F(\text{SIG}_M(C))$ 를 용이하게 평가하고, $F(\text{SIG}_M(C))$ 를 선택 비율(s)과 비교할 수 있다. $F(\text{SIG}_M(C))$ 가 사용자에게 실질적으로 예측 불가능하다는 것이 중요하다; 이는 또한 충분히 정확한 수이어야 한다. 실제로 적합한 선택 비율, 예를 들어 1/128 또는 1/1024의 경우에, $\text{SIG}_M(C)$ 및 $F(\text{SIG}_M(C))$ 가 10-비트 길이이면 충분하다. 대신에, 전형적인 디지털 서명은 수백 비트의 길이이므로, 오버킬(overkill)을 나타낸다.

본 발명의 이 실시예에서, 상인은 일단 아이템(V)(예를 들어, $\text{SIG}_M(C)$)이 특성(P)을 충족한다고 상인 자신이 결정하였으면, V가 P를 충족하는지를 은행이 검증할 수 있도록 하는 정보에 은행이 접근하도록 한다. 본 발명의 전형적인 실시예에서, 정보(I)는 그 공중 키에 대한 상인의 인증서, 또는 $\text{SIG}_M(C)$ 를 생성하는데 사용되었던 비밀 키에 대응하는 상인의 공개 키를 포함할 수 있다. 정보(I)는 또한 C에 대한 상인의 디지털 서명, 즉, V 또는 $\text{SIG}_M(C)$ 을 포함할 수 있다. 상인은 수표(C)가 생성되기 전에도 정보의 일부는 은행에 의해 접근되도록 할 수 있다. 예를 들어, 상인은 과거의 자신의 인증서를 은행에 제공할 수 있고, 은행은 이를 저장할 수 있다. 전자 수표(C)로부터 도출된 아이템(V)이 특성(P)을 충족하지 않는다고 상인이 결정할 경우, 상인은 수표(C)를 간단히 폐기한다. 은행은 결코 수표(C)를 알지 못한다. 그러나, 수표가 적절하게 만들어진 경우, 지불을 위해 선택되지 않을지라도, 상인은 통상적으로 수표로 구매하고자 하는 상품/서비스를 사용자에게 제공한다. (C와 관련된) V가 특성(P)을 충족하는 수표(C)만이 상인에 의해 지불용으로 선택되어, 은행에 전달된다. 따라서, 은행은 사용자에 의해 행해진 소액지불의 프랙션에 대해서만 작동하게 된다.

은행이 사용자에 의해 생성되고 상인에 의해 수신되는 수표의 프랙션(s)만을 알고 있기 때문에, "손실" (선택되지 않은) 수표의 값을 고려하기 위하여 지불 금액의 조정이 행해질 필요가 있다. 이와 같은 조정을 행하는 하나의 방법에서, 예치를 위

해 은행으로 전달된 각 수표는 수표(C)의 기명 액면가(T_v)의 $1/s$ 의 값을 가지는 "소액지불"을 발생시킨다. s 가 가변일 때, 적용 가능한 s 는 C를 선택하는데 사용되는 절차와 관련된 s 이다. 예를 들어, s 가 $1/1000$ 이고 거래 값(T_v)이 1 센트라면, 평균하여, 1000개의 소액지불 중에서 단지 1개가 지불을 위해 선택되고, 1000개의 소액지불 중에서 999개는 폐기될 것이다. 1000 센트, 즉, \$10의 지불이 선택된 소액지불을 위해 행해질 것이다. 이 방식으로, 단지 각각의 1000개의 소액지불에 대하여, 평균하여, 단지 단일 처리 비용이 생성되어, 처리 비용이 상당히 절약되도록 한다.

은행은 상인으로부터 수신된 각각의 수표(C)에 대하여, 상인의 디지털 서명 방식에서의 상인의 공개 키와 같은 정보(I)를 사용하여 수표(C)가 실제로 지불을 위해 선택되었는지를 검증한다. 바꿔 말하면, 상인으로부터 수신된 각각의 수표(C)에 대하여, 은행은 또한 정보(I)를 사용하여 V가 특성(P)을 충족하는지를 검증한다. V가 실제로 특성(P)을 충족한다고 은행이 검증한 경우, 은행은 상인, 또는 상인 이외의 지정된 제 4당사자, 사용자, 또는 은행이 소액지불의 값에 대응하는 총액을 수신하도록 한다. 은행은 통상적으로 사용자의 계좌로부터, 그리고 상인의 계좌로 또는 어떤 지정된 제 4당사자의 계좌로 지불이 행해지도록 한다.

은행은 자유재량으로 및/또는 정책에 따라서, 사용자의 계좌가 연체되어 있는 경우, 사용자의 인증서가 취소되는 경우, 또는 상인 또는 사용자가 어떤 종류의 사기 미수의 혐의를 받는 경우와 같은 어떤 상황 하에서 수표에 대해 지불하는 것을 거절할 수 있다. 예를 들어, 은행은 상인이 동일한 수표를 두 번 제시하는 경우, 지불이 단지 한번 행해지도록 하기 위한 단계를 취할 수 있다. 은행이 이전에 처리되었던 수표에 대해 지불하는 것을 거절할 수 있다. 은행은 또한 사용자가 수표를 커버할 만큼 충분한 자금을 자신의 계좌에 예치할 때까지 수표를 지불에 대해 보류하도록 선택할 수 있다.

본 발명의 제 1실시예에서 특징으로 하는 소액지불은 네 당사자, 제 1당사자, 제 2당사자, 제 3당사자, 및 제 4당사자를 포함하며, 여기서 네 당사자 모두는 전적으로 별개이다. 일례로서, 제 1당사자는 요금징수소를 통과하는 사람일 수 있고, 제 2당사자는 요금징수소의 장치일 수 있으며, 제 3당사자는 사용자의 은행일 수 있고, 제 4당사자는 고속도로 소유자일 수 있다. 대안적으로, 제 1당사자는 노래를 다운로드하는 사용자일 수 있고, 제 2당사자는 노래의 제공자일 수 있으며, 제 3당사자는 사용자의 은행일 수 있고, 제 4당사자는 음악 배급자일 수 있다. 대안적으로, 제 3당사자는 제 1당사자(즉, 사용자)의 은행일 수 있고, 제 4당사자는 제 2당사자(상인)의 은행일 수 있다. 이 경우에, 제 2당사자는 자신의 이득을 위해, 사용자의 은행이 제 2당사자의 은행으로 지불을 행하도록 한다. 제 1, 제 2, 제 3, 및 제 4당사자 이외의 부가적인 당사자가 또한 본 발명의 소액지불 방식에 포함될 수 있다. 예를 들어, 제 1당사자(사용자)는 (특성(P)이 V에 대해 유지되는 경우) 아이템(V)을 사용자의 은행인 제 3당사자로 전달하는 장치인 제 2당사자로 수표(C)를 전송할 수 있다. 사용자의 은행(제 3당사자)은 제 5당사자인 수혜자의 이득을 위해, 수혜자의 은행인 제 4당사자에게 돈을 지불한다.

지불 금액은 수표의 기명 액면가(T_v) 및 이와 같은 수표가 지불을 위해 선택될 추정된 확률 둘 다에 따를 수 있다. 사용자의 계좌로부터, 그리고 상인의 계좌로의 지불 금액은 수표의 기명 액면가에 의해 제공되고, 이와 같은 수표가 선택될 추정된 확률의 역수($1/s$) 만큼 승산되고, 은행이 사용자 및 상인에게 청구할 수 있는 임의의 적용 가능한 은행 처리 요금만큼 조정될 수 있다.

상술한 바와 같이, 소액지불 방식은 저가 아이템, 예를 들어, 웹 아티클 또는 웹 페이지를 구매할 수 있도록 하는데 매우 유용하다. 종래 기술에서, 사용자가 저가 아이템을 구매할 수 있도록 하기 위하여 가입 방법이 광범위하게 사용되었다. 예를 들어, 웹 서비스에 가입함으로써, 사용자는 본질적으로 많은 미래의 저가 거래를 단일 소액지불로 수집시킨다. 그러나, 이 관행은 사용자가 현재 특정 아이템에는 관심이 있지만, 미래의 아이템에 접근하고자 하거나 접근할 필요가 있는지가 확실하지 않은 경우, 가입 가격이 사용자가 기꺼이 지불하는 것보다 더 많을 수 있기 때문에 사용자에게 최적적이지 아닐 수 있다. 결과적으로, 벤더는 사용자가 가입을 행하는 것(즉, "미리" 소액지불을 행하는 것)에 대해 결정할 수 있고, 자신의 희망하는 아이템을 포기할 수 있기 때문에 어떤 사업에 실패할 수 있다.

본 발명의 제 1실시예에서 특징으로 하는 확률적 소액지불 방식은 다음과 같이, 가입 및 개별적 판매를 브리징하는 방식으로 확장될 수 있다. 상인은 사용자에게 두 개의 옵션: 1) 사용자가 소정의 시간 간격 내에서 많은 아이템을 획득할 수 있도록 하는 가입(예를 들어, 가입은 일 년 동안 상인의 모든 웹 페이지에 접근하는 것을 소비자에게 제공할 수 있다), 및 2) 메뉴에서 고르는 개별적인 아이템을 사용자에게 제공할 수 있다. 사용자는 자신의 신고 가격(T_v)에 따라서, 개별적인 아이템만을 구매하도록 결정할 수 있다. 사용자는 T_v 의 액면가를 갖는 확률적 수표를 상인에게 지불하고, 상인은 사용자에게 원하는 아이템을 제공할 것이다. 그러나, 확률적 수표가 선택되어야 한다면, 수표는 실제로 상인이 훨씬 더 높은 금전 값, 예를 들어, $A = T_v * 1/s$ 을 수신하도록 할 것이며, 여기서, 개별적인 수표가 지불을 위해 선택될 확률이 $1/1000$ 인 경우에, $s=1/$

1000이다. 상인에 의해 수신되는 금액(A)은 상인의 가입 서비스의 비용을 초과하지 않을 것이다. 이 경우에, 사용자는 무료로 가입함으로써 보상받을 것이다. 가입의 비용이 A보다 높은 경우, 사용자는 상인으로부터 가입을 행하는 비용에 대해 신용으로 A를 획득함으로써 보상받을 수 있다.

가입 및 개별적 판매를 브리징하는 상술한 방법은 사용자에게 여러 추가적인 인센티브를 제공한다. 단지 간소화를 위하여, 모든 아이템이 동일한 비용(예를 들어, 1 센트)를 가지며, 가입 비용이 \$10이고, 확률적 수표가 1 센트의 액면가를 갖지만 근원적인 방식에서의 선택에 대한 확률이 1/1000이기 때문에 지불을 위해 선택시 결국 사용자에게 실제로 \$10을 요구한다고 가정하자. 그 후, 사용자는 평균하여, 자신의 수표의 1000 개중에서 단지 1개가 지불 가능하고, 자신이 실제로 \$10을 지불할 때, 또한 무료로 가입을 행한다는 것을 인지할 것이다. 따라서, 어떤 의미에서, 사용자는 자신이 가입을 행해야 하는지, 또는 자신이 메뉴에서 고르는 아이템에 대해 선택해야 하는지를 결정하지 않아도 된다: 사용자는 자신이 결국 무료로 아이템을 획득하게 되거나, 아이템에 대해 돈을 지불하지만, 결국은 무료로 가입하게 되기 때문에, 항상 메뉴에서 고르는 것을 선택한다. 이 방식에서, 사용자가 1000개의 1-센트 구매를 행하기 오래 전에, \$10 지불에 도달할지라도, 소액지불 방식은 항상 사용자에게 공정하고 매력이 있는 것처럼 보일 것이다. 이 프로세스는 상인에게도 매력이 있는 것처럼 보이는데, 그 이유는 상인이 그렇지 않았다면, 어쨌든 가입을 행하는 것을 고려하지 않는 고객을 잃을 수 있기 때문이다. 상인은 또한 사용자가 너무 많은 거래 상품을 획득하고 있다고 느끼면, 가입의 할당된 비용을 포함하도록 퍼-밸류(per-value)(Tv)를 1비트 상향으로 조정할 수 있다.

도 2는 본 발명의 하나의 실시예에 따른, 거래(T)에 대한 지불을 설정하는 소액지불 시스템(100)의 구성요소를 설명하는 개략적인 블록도를 제공한다. 시스템(100)은 사용자, 상인, 은행이 전자 데이터, 및 심지어 지불을 서로들 간에 전송하도록 하는 통신 수단(110)을 포함한다. 전자 데이터는 전자 수표를 나타내는 데이터 스트링, 또는 메시지를 나타내는 스트링을 포함할 수 있다. 하나의 실시예에서, 통신 수단(110)은 원격 서버로 접근하도록 할 수 있다. 통신 수단(110)은 모뎀, 및 네트워크 인터페이스 카드를 포함하지만, 이에 제한되지 않는, 종래 기술에 공지되어 있는 하나 이상의 네트워크 인터페이스를 포함할 수 있다. 통신 수단(110)은 상이한 네트워크 노드들 사이에서 데이터를 전달하도록 하는 버스, 예를 들어, 어드레스 버스(114) 및 데이터 버스(115)를 포함할 수 있다.

시스템(100)은 또한 제 1처리 수단(105), 및 제 2처리 수단(106)을 포함한다. 제 1및 제 2처리 수단은 컴퓨터 시스템, 예를 들어, DOS 또는 윈도우 운영 시스템을 실행하는 디지털 컴퓨터일 수 있고, 어드레스 버스(114) 및 데이터 버스(115)에 접속된다. 처리 수단(105 및 106) 각각은 전형적으로 데이터를 저장하는 저장 수단(121), 데이터를 입력하는 입력 수단(122), 및 시스템 명령을 구현하는 중앙 처리 장치("CPU")(123)를 포함한다. 저장 수단(121)은 컴퓨터 메모리, 및 하드 디스크, CD-ROM, 등과 같은 데이터 저장 장치를 포함할 수 있다. 입력 수단(122)은 종래 기술에 공지되어 있는 임의의 입력 장치, 예를 들어, 종래의 키보드일 수 있다.

거래(T)와 관련된 데이터 스트링(C)을 도출하고, 입력하여 저장하기 위한 제 1처리 수단(105)은 제 1당사자에 의해 동작된다. 아이템(V)을 C의 적어도 일부와 관련시키기 위한 제 2처리 수단(106)은 제 2당사자에 의해 동작되며 C에 응답한다. 제 2처리 수단(106)은 또한 V가 특성(P)을 충족하는지를 결정하도록 동작된다. 예를 들어, 한 세트의 명령이 제 2처리 수단(106)의 CPU(123)로 입력되어, CPU(123)가 C(또는 C의 일부)와 관련된 아이템(V)을 도출하도록 하고, V가 특성(P)을 충족하는지를 결정하도록 할 수 있다. 이것은 다음 단계가 CPU(123)에 의해 실행되도록 하기 위하여 충족되어야 하는 필요 조건, 즉, V가 P를 충족하는지를 제 3당사자가 검증할 수 있도록 하는 정보(I)를 제 3당사자(은행)에 전달하는 명령이다. CPU(123)는 V가 P를 충족할 때 선택적으로 동작하여, 정보(I)를 제 3당사자로 전송하도록 프로그램될 수 있다.

시스템(100)은 V가 P를 충족할 때 제 3당사자에 의해 선택적으로 동작하여, 제 4당사자가 총액을 수신하도록 하는 수단(140)을 포함한다. 그 수단(140)은 또한 V가 P를 충족할 때 선택적으로 동작되어, 제 4당사자에게 지불을 전달하도록 프로그램될 수 있는 CPU를 갖는 컴퓨터 시스템일 수 있다.

요약하면, 본 발명의 제 1실시예에서 특징으로 하는 소액지불 방식은 사용자-상인 대화의 필요성을 제거하고, 상당히 많은 수의 소액지불이 발생하는 시간 기간에 걸쳐 각각의 당사자가 거의 정확한 예측 값을 지불 또는 수신하도록 하면서, 처리 비용을 최소화한다.

II. 시간 제약을 포함하는 소액지불 시스템

상술한 제 1실시예에서 제공되는 비-대화식 구조 내에서 상이한 변형이 가능하다. 특히, 본 발명의 제 2실시예에서, 시간 제약을 통합할 수 있다. 상기 장에서 설명한 바와 같은 소액지불 방식은 상인이 지불 가능한 수표를 언제라도 예치하도록

할 수 있다. 그러나, 많은 경우에, 그 시간 정보가 관련 거래가 발생한 시간으로부터 소정의 시간 간격 내에 수표가 제공되어야 한다는 것을 나타내는 지불 가능한(즉, 적절하게 선택된) 수표를 상인이 제공하지 않는다면, 은행이 상인의 계좌에 대변하는 것을 거절하는 능력을 가지는 것이 유용하다.

본 발명의 제 2실시예에서, 사용자가 부분적으로 시간(t)에 의해 특징 지워지는 거래(T)에 대한 지불을 설정하도록 하는 소액지불 방식이 제공된다. 전형적으로, 시간(t)은 거래(T)가 발생한 시간 및/또는 날짜를 나타낸다. 도 3은 본 발명의 제 2실시예에 따른 소액지불 거래를 위한 방법의 개요를 흐름도 형태로 제공한다. 사용자는 T로부터 데이터 스트링을 도출하거나, 거래(T)로부터 전자 수표(C)를 도출한다. 제 2실시예에서, 수표(C), 또는 C가 관련되는 거래(T)는 상기 거래(T)의 시간에 관한 정보(IN)를 포함해야 한다.

사용자는 상인이 IN을 포함하는 C의 적어도 일부를 수신하도록 한다. C의 일부의 수신시 상인은 사용자에게 의해 실질적으로 예측될 수 없는 아이템(V)을 C와 관련시킨다. 본 발명의 이 실시예에서, 실질적으로 예측될 수 없는 아이템(V)은 T의 시간(t)에서 규정된다. 예를 들어, V는 공개 디지털 서명 방식의 상인의 비밀 키를 사용하여 생성될 수 있고, $SIG_M(C)$, 즉, t에 대한 정보를 포함하는 C의 부분 또는 C에 대한 상인의 디지털 서명에 의해 제공될 수 있다. 후자의 경우에, 더 정확하게는, $V = SIG_M((G(C)))$ 이고, 여기서, G는 C에 관한 시간 정보를 리턴시키는 C의 함수이다.

V가 충족해야 하는 특성(P)을 결정하기 위하여 소액지불 방식에서 파라미터(s) 및 함수(F 및 G)가 또한 사용된다. 파라미터(s) 및 함수(F 및 G)가 규정되는 방식뿐만 아니라, 특성(P)이 충족되어야 하는 방식은 이전 장에서 설명한 s, F 및 P를 규정하는 방법과 유사한 방식으로 변화할 수 있다. 예를 들어, 수표(C)(또는 C가 관련되는 거래(T))는 C와 관련된 적절한 값(V)으로 사용되어야 하는 특성(P)을 직접 규정할 수 있다. 예를 들어, 함수(F)는 특성(P)을 결정할 수 있고, 여기서, P는 다음:

$F(V) = F(SIG_M(C)) < s$ 에 의해 규정되고,

여기서, s는 0과 1 사이의 수이며, 소정 수표(C)가 상기 방식에서 지불을 위해 선택되는 확률을 나타낸다.

본 발명의 제 2실시예에서, 상인의 서명은 C 모두에 적용하기보다는 오히려, C의 함수(G)에만 적용할 수 있다. 즉, 특성(P)은 다음:

$F(V) = F(SIG_M(G(C))) < s$ 에 의해 제공될 수 있다.

다시, 함수(G)는 몇 가지 방식 중 하나로 규정될 수 있다. 예를 들어, 이 함수는 고정되거나, C에 의해 규정되거나, 대응하는 거래(T)에 의해 규정되거나, (예를 들어, 상인 또는 사용자의) 인증서에 의해 규정되거나, 은행에 의해 제공되는 다른 정보에서 규정될 수 있다.

특히 유용한 함수(G)는 C의 시간 정보(IN)를 리턴시키는 함수일 수 있다. 이 방식에서, (사용자에 의해 실질적으로 예측될 수 없는) 아이템(V)은 주로 거래(T)의 시간(t)의 함수이므로, 특성(P)은 주로 거래(T)의 시간(t)에 따른다. G에 의해 추출된 시간 정보가 t와 관련될 수 있지만, t와 일치할 필요는 없다는 점에 유의하라. 예를 들어, t는 T의 날짜, 시간 및 분을 규정할 수 있는 반면, G는 상이한 그레인러티(granularity)로 시간 표시를 리턴시킨다: 예를 들어, 이는 t 자체를 규정하지만, 날짜(또는 분이 아닌 날짜와 시간), 또는 t 이후의 다음 시간까지만을 규정할 수 있다. 본 발명의 제 2실시예에서, 상인에 의해 서명되는 값(G(C))은 항상 이 정보를 포함하도록 해석해야 한다.

V가 P를 충족한다고 결정하고(이것이 참인 경우에), 수표가 다른 테스트(예를 들어, 존재한다면, 사용자의 서명이 유효한지의 여부)를 통과한 후, 시간(t')에서 상인은 은행이 T의 시간(t)에 관한 일부 또는 모든 정보(IN)를 수신하도록 한다. 상인은 IN을 포함하는 수표(C)의 적어도 일부, 또는 C의 모두를 은행에 제공할 수 있다. 상인은 또한 V가 P를 충족하는지를 은행이 독립적으로 검증할 수 있도록 하는 정보(I)를 은행이 수신하도록 한다. 상인은 V가 계산되기도 전에 은행이 I의 부분을 수신하도록 할 수 있다. IN의 관련 부분을 수신한 후, 은행은 t'(즉, 상인이 은행에 수표를 제공했던 시간)이 t에 충분히 가까운지를 결정할 수 있다. 은행은 경과된 시간(|t'-t|)이 소정 금액보다 더 큰 경우, 수표(C)를 폐기할 수 있다. 수표(C)의 사용자 서명이 검증되지 않은 경우, 또는 사용자의 계좌가 연체되어 있는 경우, 또는 사용자 및/또는 상인이 사기 혐의를 받는 경우, 등과 같은 다른 조건이 유지되는 경우, 은행은 또한 자유재량으로 또는 정책에 따라서 지불을 거절하거나 연기할 수 있다.

I를 사용하여, 은행은 V가 P를 충족하는지를 독립적으로 검증한다. V가 실제로 P를 충족하고, ($|t'-t|$ 가 소정의 시간 간격보다 적은지 여부의 테스트와 같은) 모든 다른 테스트가 통과되는 경우에만, 은행은 상인이 총액을 수신하도록 한다. 소정의 시간 간격은 예를 들어, 하루, 일주, 또는 심지어 소정 수의 시간일 수 있다.

일례로서, 수표(C)가 관련되는 거래(T)가 날짜(i)에 발생하는 경우, 소액지불 시스템은 상인이 날짜(i) 한도, 또는 날짜(i+1) 한도, 또는 날짜(i+n) 한도까지 수표를 예치할 것을 요청하며, 여기서 n은 상인이 예치할 사업 감각을 만드는 날짜의 수를 나타내는 정수이다. 이 유형의 요건은 상인이 수신하는 수표의 시간 정확도를 검증하도록 하는 여분의 인센티브를 상인에게 제공하며, 이는 상인에게 부가된 보안 이점을 제공한다.

하나의 형태에서, 사용자가 상인으로 하여금 IN을 포함하는 C의 일부를 수신하도록 하는 시간을 t_1 이 나타내는 경우, 상인은 시간(t_1)이 미리 규정된 시간 제약 내에 존재하지 않으면 진행하는 것을 거절할 수 있다. 이와 같은 경우에, 상인은 요청된 "상품"(예를 들어, 상품, 서비스, 또는 정보)을 제공하는 것을 거절할 수 있다. 적시의 예치는 또한 사용자가 너무 늦게, 즉, 가능한 비용이 더 이상 사용자의 예산이 아닐 때, 요금청구받지 않도록 한다.

G(C)를 더 상세히 참조하면, G(C)는 C, 또는 C가 관련되는 거래(T)의 날짜 및/또는 시간 정보를 리턴시키는 함수일 수 있다. 예를 들어, 이와 같은 날짜가 2001.01.01인 경우, V는 $SIG_M(2001.01.01)$ 로 이루어질 수 있다. 이는 상인이 결코 이와 같은 날짜 이전에 서명하지 않았다면, 사용자에게 실질적으로 예측 불가능하다. 이 경우에, V가 충족해야 하는 특성(P)은 $SIG_M(2001.01.01)$ 또는 $F(SIG_M(2001.01.01))$ 을 C, C의 일부, C의 어떤 함수, 또는 미리-규정된 상수와 비교하는 것을 포함한다. 예를 들어, 하나의 이와 같은 특성(P)은 다음으로서 공식화될 수 있다: $SIG_M(2001.01.01)$ 의 선택된 m-비트 서브스트링이 C의 선택된 m-비트 서브스트링과 정합하는가?

V를 C와 관련시키는 상술한 방법이 다수의 장점을 갖는다는 점에 유의해야 한다. 특히, 상인은 2001년 1월 1일에 사용자로부터 C를 수신하기도 전에, $SIG_M(2001.01.01)$ 를 계산할 수 있다. 따라서, 일단 C가 그 날짜에 수신되었다면, 상인은 P가 필요한 특성(P)을 충족하는지를 훨씬 더 빨리 검증할 수 있다. 예를 들어, P가 $F(SIG_M(2001.01.01)) < s$ 로 이루어지는 경우, 어떤 고정된 수(s)에 대하여, P는 단지 V만을 따르며, 수표를 따르지 않는다. 따라서, 상인은 2001년 1월 1일 이전에도, P가 한번 유지되는지 및 모두에 대하여 유지되는지를 결정할 수 있다. P가 유지되는 경우, 상인은 (임의의 부가적인 검증 없이) 자신이 그 날짜를 수신하는 모든 수표를 지불을 위해, 은행으로 전달할 수 있다. P가 유지되지 않는 경우, 상인은 (임의의 부가적인 검증 없이) 자신이 그 날짜를 수신하는 모든 수표를 폐기할 것이다. 이 방식으로, 상인이 수행해야 할 서명의 수가 최소화된다.

대안적으로, 특성(P)은 $SIG_M(2001.01.01)$ 의 어떠한 m-비트(말하자면, 10-비트)가 사용자가 C에서 포함하는 소정의 10-비트 스트링과 정합하는지의 여부로 구성될 수 있다. 이 경우에, 특성이 V 및 수표(C) 둘 다를 따를지라도, P가 유지하는지를 결정하는 것은 거의 즉각적이다. 실제로, 디지털 서명의 계산이 다소 복잡할 수 있을지라도, 상인은 2001년 1월 1일 전에 또는 단지 한 번만 $SIG_M(2001.01.01)$ 를 계산하고 나서, 서명(또는 이의 임의의 소정 m-비트)을 저장할 필요가 있다.

이 방식으로, 수표마다 필요로 되는 상인의 수고가 단지 2개의 10-비트 스트링의 사소한 비교로만 이루어질 것이다. 이는 수표가 수신되기도 전에 소정의 수표가 지불을 위해 선택되는지를 은행이 독립적으로 검증할 수 있도록 하는 모든 정보(I)를 은행이 수신할 수 있도록 한다. 예를 들어, 상인은 2001년 1월 1일의 맨 처음에, 또는 그 이전에도, $SIG_M(2001.01.01)$ 를 전송하고 나서, 단지 2001년 1월 1일과 관련된 모든 수표를 은행에 전송할 수 있다. 그러나, 편리할지라도, 이는 악의가 있는 사용자가 2001년 1월 1일 동안 $SIG_M(2001.01.01)$ 의 소유권을 획득하고자 하면, 결코 지불을 위해 선택되지 않는 날짜를 수표에 기록할 수 있기 때문에, 상인에게 타산적이지 않을 수 있다. 당업자들에게는 명백한 (하루보다는 오히려 1시간의 시간 그레놀레리티를 사용하는 것과 같은) 이 방법의 다양한 변형이 존재한다.

하나의 형태에서, 본 발명의 제 2실시예는 상인이 값의 시퀀스(VL_i)를 도출함으로써, 수표(C)에 대한 시간/날짜 정보를 사용하여 (사용자에게 실질적으로 예측 불가능한) 아이템을 관련시키도록 한다. 상인은 적어도 하나가 거래(T)의 시간(t)과 소정의 방식으로 관련되는 시간의 시퀀스(t_i)($i=1, \dots, n$)와 관련된 값의 시퀀스(VL_i)를 도출한다. 예를 들어, 1보다 크고 보다 적은 하나 이상의 정수(m)의 경우에, $|t-t_m|$ 는 소정 금액, 예를 들어, 하루보다 적다. 대안적으로, 1과 n 사이의 하나 이상의 정수(m)의 경우에, $t-t_m$ (또는 t_m-t)는 둘 다 양이며, 하루보다 크지 않다. 사용자는 거래(T)의 시간(t)에 관한 정보를 포함하는 C의 적어도 일부를 상인이 수신하도록 한다.

그 후, 상인은 특성(P)이 C의 부분 및 값(VL_m) 사이에서 유지되는지, 또는 C의 부분 및 t_m과 관련된 값(VL_m)에 따른 양(Q) 사이에서 유지되는지를 결정한다. 그러한 경우, 상인은 특성(P)이 충족되는지를 은행이 검증할 수 있도록 하는 정보(I)를 은행이 수신하도록 하여, 은행이 적절한 대변 및 차변을 행할 수 있도록 한다.

하나의 형태에서, 상인은 해쉬 값의 체인을 발생시킴으로써, C의 데이터 정보를 사용하여 각 수표(C)에 (사용자에게 실질적으로 예측 불가능한) 아이템(V)을 관련시킬 수 있다. 이 형태에서, 상인은 값의 체인:

$w_0, w_1, \dots, w_n$ 을 발생시키고

여기서, $w_i = h(w_{i+1})$ 이고, h는 일방향 함수이며, w_0 를 자신의 공개 파일로 두고, 이를 디지털적으로 서명하거나, 그렇지 않으면, 이를 공개시킨다. 따라서, 상인은 w_{i+1} 를 i-번째 날짜/시간 유닛에 관련시킨다. 관련된 아이템(w_{i+1})은 상인이 이전 시간 유닛과 관련된 모든 아이템을 드러낼지라도, 예측될 수 없다. 처음 i의 이와 같은 아이템이 시간 유닛(i)에 의해 릴리스될 수 있을지라도, 단지 $w_i = h(w_{i+1})$ 만을 인지함으로써는 w_{i+1} 를 계산할 수 없기 때문에, w_{i+1} 는 실질적으로 예측될 수 없다. 상인이 시간/날짜 정보(i)를 갖는 수표(C)에 관련시키는 예측될 수 없는 아이템(V)은 w_{i+1} , 즉, 시간/날짜 정보의 i-번째 해쉬 인버스이다. 특성(P)은 다양한 방식으로 공식화될 수 있다. 일례로서, 특성(P)은 w_i 의 처음 10 비트가 C의 10개의 선택된 비트와 동일한 경우 충족될 수 있다. 상인은 정보(I) = w_i 를 단순히 릴리스함으로써 특성(P)이 유지되는지를 은행이 검증할 수 있도록 한다. 은행은 w_i 를 i번 해쉬하고 결과가 상인의 w_0 와 정합하는지를 확인함으로써 w_i 를 검증하고 나서, P가 유지되는지를 검증할 수 있다.

상인이 수표의 날짜/시간 정보와 관련된 예측 불가능한 아이템(V)을 사용하는 경우, 상인이 자신이 폐기했던 수표 및 자신이 소정의 날짜/시간 단위 동안 대변을 위해 파기했던 수표에 관한 임의의 정보를 숨기는 것이 더 바람직하다. 그 밖에, 악의가 있는 사용자는 값(V)을 조기에 발견하여, 예를 들어, 선택되지 않을 것이라고 자신이 인지하는 수표를 생성함으로써, 이 정보를 자신의 장점으로 사용할 수 있다. 상인이 소정의 날짜/시간 단위의 모든 "선택된" 지불 가능한 수표를 폐기하고 나서, 날짜/시간 단위 한도에서 모든 선택된 수표를 은행에 전송하는 것이 바람직하다. 이 방식으로, 악의가 있는 은행도 그가 상인에게 사기칠 수 있도록 사용자와 결탁할 수 없다. 사용자가 자유롭게 다양한 수표를 생성하고 이를 수표가 지불을 위해 선택된다고 판명될지를 결정하기 위하여 테스트하는 것을 어렵거나 불가능하게 하는 스마트 카드, 셀 전화, 또는 다른 장치들을 사용자가 사용하도록 요청함으로써 강화될 수 있다.

III. 사용자 위험성을 제거하는 선택적 예치 프로토콜을 포함하는 소액지불 시스템

이는 사용자가 미리 인지할 수 없고, 자신의 수표 중 어느 것이 지불을 위해 선택될지가 제어되지 않는 전형적인 확률적 지불 방식이다. 지금까지 설명된 바와 같이, 본 발명의 실시예에서, 사용자가 자신이 실제로 소비한 것을 초과하는 금액, 즉, 자신이 기록했던 수표의 총액을 초과하는 금액만큼 차변받게 될 수 있다. 종래의 확률적 지불 방식에서, 수표(C_i)가 확률(s)로 지불 가능하다고 선택되면, 사용자는 전형적으로 거래 값(TV_i)보다 더 많이 차변받는다: 많은 확률적 방식에서, 사용자는 예로서, 금액($TV_i * 1/s$)만큼 차변받는다. 따라서, 각각의 거래(T_i)가 동일한 값($TV_i = TV$)을 가지고, 불행히도 사용자의 처음 1/s 수표 중 (하나보다는 오히려) 2개 이상이 지불 가능한 경우, 사용자는 자신의 소비한 실제 금액의 적어도 두 배인 금액만큼 차변받을 것이다. s가 클 때, 이는 사용자의 거의 1/4에 대해 발생하는 것으로 예상할 수 있다.

본 발명의 제 3실시예에서는, 사용자 위험성 문제, 즉, 불행히도 사용자가 자신이 실제로 기록했던 수표의 총액보다 더 많이 요금청구받을 수 있는 확률 문제를 해결하는 선택적 예치 프로토콜을 특징으로 한다. 사용자 위험성 문제는 Rivest의 전자 복권 방식, 및 이전 장에서 제시된 소액지불 시스템과 같은 확률적 소액지불 방식에서 고유한 것이다. 예를 들어, 확률적 방식에 대한 선택 비율(s)이 1/1000일 수 있을지라도, 불행히도, 사용자의 처음 1000 번의 지불 중 한 번이라기보다는 오히려, 5번이 지불을 위해 선택되는 것이 발생할 수 있다. 사용자에게 과도하게 요금청구할 확률이 작고, 사용자 위험성의 상대적인 영향이 행해진 소액지불의 수에 따라 극적으로 감소되지만, 사용자 위험성은 확률적 소액지불 방식을 광범위하게 수용하는데 있어 상당한 장애가 될 수 있다. 이는 통상적인 사용자가 은행과 같은 더 큰 시설과 달리, 위험성을 관리하는데 익숙하지 않기 때문이다. 따라서, 이하에 설명된 본 발명의 제 3실시예의 방식은 근원적인 확률적 지불 방식을 개선시킨다.

도 4는 사용자가 과도하게 지불할 위험성을 제거하는 선택적 예치 프로토콜을 포함하는 본 발명을 따른 소액지불 거래를 위한 방법의 개요를 흐름도 형태로 제공한다. 이 실시예에서는, 사용자가 일련의 거래($T_i(i=1, \dots, n)$)에 대한 지불을 설정할 수 있도록 하는 방법 및 시스템을 특징으로 한다. 각각의 거래(T_i)는 전형적으로 초저가, 예를 들어, 1 센트 또는 1 센트의 프랙션의 거래 값(TV_i)에 의해 특징 지워진다. 따라서, 은행이 모든 단일 거래(T_i)에 대한 지불을 처리한다면, 은행에서 거래 값(TV_i) 자체보다 처리 비용이 훨씬 더 많아 질 수 있다.

따라서, 확률적 소액지불 방식(예를 들어, Riverst의 복권 방식, 또는 이전 장에서 설명한 방식 중 하나)은 각각의 T_i 에 대하여, 거래(T_i)에 대한 지불로서 상인에게 전송되는 수표/소액지불(C_i)을 발생시키기 위하여 사용될 수 있다. 그 후, 0보다 크고 1보다 적은 확률로, Riverst의 복권 방식으로 사용자와 상인의 대화에 의해, 또는 이전 장에서 설명한 방식에서와 같이 상인 혼자에 의해 비-대화식으로, C_i 가 지불을 위해 선택되는지가 결정될 수 있다.

도 4로부터 알 수 있는 바와 같이, 각각의 $C_i(i=1, \dots, n)$ 에 대하여, 사용자는 상인이 C_i 를 수신하도록 한다. 상인이 수신하는 각각의 C_i 에 대하여, 상인은 근원적인 확률적 방식에 따라, 그리고 어느 수표가 지불을 위해 선택될지를 사용자가 미리 예측하지 못하도록 하는 방식으로, C_i 가 선택되는지(즉, 지불 가능한지)를 결정한다. 예를 들어, 근원적인 확률적 방식은 상기 I 장에 설명된 방식일 수 있고, 이 경우에, 상인은 아이템(V_i)을 C_i 와 관련시키고, V_i 가 특성(P_i)을 충족하는지를 결정함으로써 확률을 결정할 것이다. 상인은 C_i 에 대한 사용자의 서명이 유효한지의 여부, 수표의 금액이 너무 많지 않은지의 여부, 등과 같은 다른 조건을 점검할 수 있다; 이러한 조건 중 일부는 사용자의 인증서에 규정될 수 있다. C_i 가 지불되지 않아도 된다고 상인이 결정하는 경우, 상인은 C_i 를 폐기한다. 상인이 C_i 가 지불 가능하다고 결정하는 경우, 상인은 선택된 C_i 가 지불 가능한지를 은행이 검증할 수 있도록 하는 정보(I_i)를 은행이 수신하도록 한다. 은행은 I_i 를 사용하여, C_i 가 지불 가능한지를 검증한다. C_i 가 지불 가능한 경우에만, 은행은 상인이 대변 금액(CR_i)을 수신하도록 하고, 사용자가 금액(D_i)만큼 차변받도록 한다.

본 발명의 제 3실시예에서, 은행은 사용자에게 차변된 총 금액 $D=D_1+D_2+\dots+D_i$ 이 사용자가 기록했던 수표의 총 수집값 $TV_{agg}=TV_1+TV_2+\dots+TV_i$ 보다 크지 않게 D_i 가 이루어지도록 해야 한다. 바꿔 말하면, 사용자가 $1 \leq i \leq n$ 인 임의의 정수 i 에 대하여, i 번째 거래에 참여한 후, 사용자가 차변받는 총 금액은 결코 자신의 상인으로부터 구매했던 거래($T_1, \dots, T_i$)의 수집값을 초과해서는 않된다.

바람직한 형태에서, 은행은 수표로부터의 일련 번호를 사용함으로써, $D=D_1+D_2+\dots+D_i$ 가 상기 T_{agg} 보다 크지 않도록 하는 방식으로 D_i 를 결정한다. 이 형태에서, 근원적인 확률적 지불 방식으로 사용자에 의해 발생된 다수의 수표($C_i(i=1, \dots, n)$) 각각은 일련 번호(S_i)를 포함한다. 이러한 일련 번호(S_i)는 바람직하게는 1에서 시작하는 연속적인 정수이다. 또한, i -번째 일련 번호는 바람직하게는, 다른 거래($T_1, \dots, T_{i-1}$, 및 $T_{i+1}, \dots, T_n$) 및 다른 수표($C_1, \dots, C_{i-1}$, 및 $C_{i+1}, \dots, C_n$)와 관련된 거래(T_i) 및 수표(C_i)의 시간 순서를 나타낸다.

일련 번호(S_i)는 거래(T_i) 및/또는 수표(C_i)와 관련된 인덱스(i)의 표시를 제공한다. 그러나, 순서화되지만 비-연속적인 일련 번호가 또한 사용될 수 있다. 예를 들어, 소정의 번호(P) 다음에, i -번째 수표를 i -번째 수표와 관련시킬 수 있다. 간소화를 위하여, 각각의 거래(T_i)가 동일한 거래 값($TV=TV_i$)을 갖는 경우가 먼저 설명될 것이다. 제 3실시예에는 또한 이하에 더 상세히 논의하는 바와 같이, 거래(T_i)가 상이한 값(TV_i)을 가질 수 있는 경우를 포함한다.

은행(또는 또 다른 제 5당사자)은 지불을 위해 선택되었던 수표의 일련 번호를 추적한다. 지불 가능한 수표(C_i)의 차변 금액(D_i)을 결정하기 위하여, 제 3/제 5당사자는 값(S_{max})을 사용하며, 여기서, S_{max} 는 지불을 위해 지금까지 제공되었던 가장 최근의 수표를 나타내는 일련 번호를 표시한다. 값(S_{max})은 일련 번호가 1에서 순차적으로 사용되는 경우에 0으로 초기화된다. 수표의 일련 번호가 순차적으로 순서화되기 때문에, S_{max} 는 지불을 위해 이전에 제공되었던 임의의 수표에 나타나는 가장 큰 일련 번호이다. 또한, S_{max} 는 일련 번호의 순차적인 순서로 인해, 현재 지불 가능한 수표(C_i)의 일련 번호(S_i)보다 적다. 도4에 도시된 바와 같이, 사용자는 (예를 들어, 제 5당사자에 의해) 이 수표에 대해 다음 금액:

$$D_i = (S_i - S_{\max}) * TV \quad (1)$$

만큼 차변받는다. 이는 사용자가 자신이 기록했던 모든 수표에 대해 차변받았던 총 금액(D)이 $S_i * TV$ 이라는 것을 따른다. 비-연속적인 일련 번호가 사용되는 경우, $D_i = \#(S_i - S_{\max}) * TV$ 를 규정할 수 있고, 여기서, $\#(S_i - S_{\max})$ 는 (S_i 를 포함하지만 $S_{\max}$ 를 제외하는) S_i 와 $S_{\max}$ 사이의 일련 번호의 수를 나타낸다.

금액 $D = D_1 + D_2 + \dots + D_{\max}$ 는 사용자가 발행한 모든 수표의 수집값을 나타낸다. i 번째 수표가 기록된 후, D 가 결코 $i * TV$ 이상이지 않기 때문에, 사용자가 과도한 지불을 행할 위험이 제거된다. 그 후, 미래의 소액지불을 처리하기 위하여, 은행은 $S_{\max}$ 의 값을 S_i 로 리셋하는데, 이는 상술한 바와 같이, 지금까지 은행에 의해 발견된 지불 가능한 가장 최근의 수표이다. 식(1)은 사용자가 궁극적으로 요구청구받는 양이 어느 수표가 궁극적으로 지불 가능하다고 판명되는지가 아니라, 단지 자신이 기록했던 수표의 수에 따른다는 것을 나타낸다; 사용자는 궁극적으로 자신이 기록했던 각각의 수표에 대해 적절한 금액을 청구받는다.

제 5당사자는 제 4당사자가 전형적으로 다음:

$$CR_i = TV * (1/s) \quad (2)$$

에 의해 제공되는 대변 금액(CR_i)을 수신하도록 할 수 있다. 근원적인 확률적 지불 방식에서 선택 비율(s)이 존재하면, 또한, 본 발명의 방법 및 시스템에서, 많은 수의 소액지불에 대해 평균될 때, 모든 $1/s$ 수표로부터 거의 단지 하나가 지불을 위해 선택된다. 따라서, 대변 금액은 또한, $1/s$ 수표의 완전히 수집된 값이기 때문에 상인에게 적합하며, 많은 수의 소액지불에 대한 평균이 행해질 때, 상인은 결국 정확한 금액을 수신하게 된다. 그러나, 결과적인 방식은 과도한 지불을 행할 위험성이 사용자로부터 은행으로 시프트되기 때문에, 사용자에게 훨씬 더 적합하다. 예를 들어, 선택 비율이 $s=1/1000$ 이고, 상인이 각각 1 센트의 가치가 있는 1,000개의 소액지불을 취급하면, 이들 1,000개의 소액지불 중 단지 하나가 선택되지만, 선택된 하나는 상인이 $1/s=1000$ 센트, 즉, \$10을 수신하도록 할 것이다. (1,000개의 소액지불 중) 하나 이상의 소액지불이 선택되면, 은행은 불행히도, \$10을 한 번 이상 지불해야 한다. 은행은 이 수표 및 또한 지불을 위해 선택되는 모든 이전 수표의 지불을 커버하기 위하여, 상술한 일련-번호 차변 방식에 따라서, 사용자가 총계를 충분히 지불할 때까지, 상인에게로의 수표에 대한 지불을 연기함으로써 어떠한 위험성을 상인에게 시프트하도록 선택할 수 있다.

본 발명의 이러한 제 3실시예에서, 사용자는 바람직하게는, 자신의 은행 계좌에 수표를 기록하도록 인증하는 인증서를 자신의 은행으로부터 획득할 수 있다. 이 인증서는 사용자의 공개 키를 규정할 수 있다; 이는 또한 사용자가 사용하도록 인증받은 최대 일련 번호, 및/또는 (수표가 가변 값을 가질 수 있는 경우) 수표의 최대 금액과 같은 다른 정보를 규정할 수 있다. 사용자는 자신이 기록한 각 수표와 함께 이 인증서를 전송하거나, 단지 자신이 이를 최근에 전송하지 않았던 상인에게 제공할 수 있다. 상인이 일정 양의 시간 동안 사용자 인증서를 캐시함으로써, 어떤 대역폭 절약이 성취될 수 있다.

본 발명의 이 실시예의 또 다른 변형에서, 사용자가 사용하도록 인증받은 최대 일련 번호(Y)는 페이워드 인증서가 특정 상인에게 Y 소액지불의 시퀀스를 인증하는 길이 Y 의 해쉬 체인의 루트를 규정하는 방식과 유사한 방식으로 길이(Y)의 해쉬 체인을 사용함으로써 규정될 수 있다. 그러나, 이 경우에, 인증받은 일련 번호를 지닌 수표는 임의의 상인에게 기록될 수 있다. 사용자는 자신이 일련 번호(i)를 갖는 수표를 기록하도록 인증받았다는 것을 입증하기 위하여 해쉬 체인의 i -번째 요소 및 인증서를 상인에게 제공할 수 있다. (해쉬 체인의 i -번째 요소는 i 번 연속적으로 해쉬될 때, 해쉬 체인의 루트를 산출하는 해쉬 체인의 요소인 것으로 규정된다.)

상인은 또한 사용자가 어느 버전의 프로토콜이 사용되는지에 따라서, 지불 프로토콜 중에 획득할 수 있거나 획득할 수 없는 디지털 인증서를 가질 수 있다. 지불 프로토콜이 실제로 비-대화식인 경우, 사용자는 이 인증서를 획득하기가 어려울 수 있다. 한편, 이 인증서는 지불 프로토콜에 필수적이지는 않다. 예를 들어, 사용자의 수표는 형태의 진술 "이 수표는 상인의 공개 키에 대한 유효한 인증서와 함께 예치되는 경우에만 유효하다", 등을 포함할 수 있고, 상인은 수표를 예치할 때 자신의 인증서를 은행에 제공할 수 있다.

여러 이유로 인해, 과도한 지불의 위험성을 사용자로부터 은행, 또는 상인으로 시프트시키는 것이 바람직하다. 우선, 수표가 $1/s$ 회 중에서 1회보다 상당히 더 자주 선택되는 확률은 작다. 따라서, 은행에 의한 과도한 지불은 거의 발생하지 않는다. 임의의 경우에, 각각의 이와 같은 과도한 지불의 금액은 그렇게 크지 않다. 은행은 또한 이와 같은 변형을 커버하기 위

하여, 계좌를 개설할 때, 각 사용자에게 고정 요금(예를 들어, 1/s에 비례하는 요금)을 부과하는 것과 같은 전략을 채용할 수 있다. 적당한 금액의 과도 지불에 대한 낮은 위험성이 개별적인 사용자를 성가시게 하고, 사용자가 본 발명에 제시된 것과 같은 확률적 소액지불 방식을 사용하지 않도록 할 있지만, 이와 같은 위험성은 일반적으로 은행을 성가시게 하지는 않을 것이다. 이는 은행이 실질적인 위험성을 관리하는데 익숙하기 때문이다. 단지 하나의 예로서, 은행에 의해 루틴으로 위험성은 사용자가 자신의 채무를 이행하지 않는 위험성이다. 따라서, 은행은 자신들이 위험성을 수용하고 관리함으로써 이득을 만들어낼 수 있는 지불 시스템을 지원하는데 제도적으로 매우 적합하다.

마찬가지로, 상인은 전형적으로 다수의 거래를 관리하는데 사용되며, 여기서 각 거래는 상품이 리턴되거나 사용자의 지불이 실현되지 않는 위험성과 같은, 어떤 관련 위험성을 갖는다. 따라서, 소액지불 방식에서 어떤 위험성을 수용하는 것이 또한 상인에게 수용 가능해야 한다. 따라서, 은행 및 상인은 예를 들어, 지불을 위해 선택된 소액지불 수표가 사용자의 계좌가 이를 커버할 충분한 자금을 포함할 때까지, 실제로 상인에게 지불되지 않는다는 것에 동의할 수 있다. 지불을 위해 선택되는 각 수표는 (상술한 일련-번호 방식에 따라 결정되는) 사용자의 지불이 이 수표 및 모든 이전에 큐잉된 수표를 커버하는데 충분할 때까지, 은행에서 "펜딩 큐(pending queue)"로 유지될 것이다.

두번째로, 얼마나 작은 간에, 은행에 의해 작은 거래당 요금이 징수되는 한, 과도 지불의 확률은 결국 점점 더 적어지는데, 즉, 소액지불 거래의 수가 증가함에 따라 위험성이 감소한다. 따라서, 은행에 대한 과도 지불의 확률은 은행이 일반적으로 단일 사용자에게 비하여, 훨씬 더 많은 양의 거래를 경험하기 때문에 통상적인 사람에 대한 확률에 비하여 더 작다.

사용자에 의한 과도 지불의 위험성을 제거하는 것 이외에, 본 발명의 제 3실시예에는 또한, 은행이 사기꾼을 처벌하거나, 이들이 임의의 실질적인 손상을 생성하기 전에, 시스템에서 추방할 수 있도록 한다. 이하에 보다 상세히 설명된 바와 같이, 본 발명은 은행으로 하여금 악의를 가진 사용자 및/또는 악의를 가진 상인이 사기치지 못하도록 하는 여러 특징을 포함한다. 예를 들어, 새로운 수표가 이전에 처리된 수표와 동일한 일련 번호를 가진다는 것을 은행이 인지하는 경우, 또는 새로운 수표의 일련 번호 및 시간이 이전에 처리된 수표에 대해 어쩐지 부적절한 경우, 또는 수표의 금액이 과도한 경우, 또는 다른 은행에 의해 규정되는 조건이 발생하는 경우, 은행은 수표를 수신하는 것을 거절할 수 있다. 은행은 적절하다고 간주할 때, 사용자에게 벌금을 부과할 수도 있고/있거나, 다른 징벌 조치를 취할 수 있다. 예를 들어, 은행은 통계치를 유지하고, 예를 들어, 인증서가 사용되는 경우 자신의 인증서를 폐지함으로써, 그의 지불 가능한 수표가 상술한 문제 중 어느 하나를 초래하는 사용자를 시스템으로부터 제외시킬 수 있다. 예를 들어, 수표는 모순되게 넘버링되고/되거나 날짜기입되는 경우, 또는 그의 수표가 예측된 것보다 더 자주 지불 가능한 사용자에게 속하는 경우 제외될 수 있다. 마찬가지로, 은행은 상술한 문제를 갖는 지불 수표, 또는 통계적으로 예측된 것보다 더 자주 지불 가능한 수표를 수신하는 품행이 좋지 못한 상인을 제외시킬 수 있다.

본 발명의 제 3실시예에서, 사용자는 일련 번호를 순서대로, 그리고, 반복 없이 사용하는 것을 요청받는다. 예를 들어, 일련 번호 1은 제 1수표에 사용되어야 하고, 일련 번호 2는 제 2수표에 사용되어야 하며, 이런 식으로 진행된다. 상술한 바와 같이, 이 방식에서, 사용자는 결코 자신이 사용한 것보다 많이 요금청구받지 않는다. 전형적으로, 소정 시간에, 최종적인 지불 가능한 수표 이후, 사용자는 지불을 위해 선택되지 않을 부가적인 거래를 위한 약간 더 많은 수표를 기록할 것이다. 따라서, 적어도 잠시 동안, 사용자는 자신이 실제로 소비한 것보다 더 적게 차변받고, 종종 자신이 차변받아야 하는 양, 즉, 최근의 수표가 실제로 지불 가능할 때의 양만큼 차변받을 것이다.

그러나, 부정직한 사용자는 자신이 실제로 소비했던 것보다 더 적은 양만큼 차변받도록 하는 방법을 찾아내기 위하여 일련 번호로 위험한 것을 하고자 할 수 있다. 하나의 방법이 일련 번호를 한번 이상 재사용하는 것이다. 사용자가 이를 행하는 경우, 양($S_i - S_{\max}$) 및 $(S_i - S_{\max}) * TV$ 에 의해 제공된 양이 실제 값에 비하여 감소될 것이다. 그러나, 이 종류의 사기는 지불 가능한 수표가 이전에 처리된 수표와 동일한 일련 번호를 갖는다는 것은 인지한 경우, 은행은 이와 같은 사기를 방지하도록 지정되는 징벌 조치를 취할 수 있기 때문에, 매우 유용하지는 않다. 예를 들어, 은행이 지불 가능한 수표에서 중복 일련 번호를 마주하게 되면, 은행은 사용자가 이 방법으로 사기치는 것이 비생산적으로 될 만큼 높은 금액을 사기치는 사용자에게 차변하도록 할 수 있다.

본 발명의 제 3실시예에서 특징으로 하는 소액지불 방식에서, 사용자는 자신의 수표 중 어느 것이 지불 가능한지를 예측할 수 없으므로, 제어할 수 없다. 따라서, 사용자가 동일한 일련 번호를 갖는 2개의 수표를 생성할 때마다, 비록 작을지라도, 이들 둘 다가 지불될 수 있는 가능성이 존재한다. 사기를 잡아내기 위한 페널티는 사용자가 사기에 의해 이득보기를 희망하는 것보다 더 많이 오프셋할 만큼 충분히 높게 설정될 수 있다.

여러 형태의 사기는 수표의 "백-데이팅" 등을 포함할 수 있다. 따라서, 상인 및 은행이 사용자가 동일한 것으로 보이는 임의의 2개의 수표(C 및 C')에 대하여, C의 일련 번호가 C'의 일련 번호보다 낮은 경우, C의 날짜/시간이 C'의 날짜/시간보다 이전인지를 점검하도록 하는 것이 중요하다.

사기치고 있는 사용자를 잡아내기 위한 상술한 메커니즘은 지불 거래 직후에, 자신의 수표 중 어느 것이 지불 가능한지를 사용자가 상인에게 말하지 않는 경우에 더 양호하게 동작한다. 실제로, 이러한 관점에서, 자신의 수표 중 어느 것이 지불 가능한지에 관해 가능한 한 사용자를 무시한 채로 유지하는 것이 바람직하다. 원칙적으로, 사용자는 실제로 얼마나 많은 수표가 기록되었는지를 모니터링할 수 있으므로, 공정한 차변에 대해 논쟁하지 않을 것이다. 그러나, 논쟁이 발생되었다면, 지불 가능한 수표의 일련 번호를 포함하는 차변된 금액의 증거를 제공하는 능력이 바람직할 것이다.

사기꾼을 찾아내서 제외시키는 상술한 메커니즘은 지불을 위한 수표(C_i)를 선택하는 기준이 단지 일련 번호(S_i)만을 따르는 경우, 개선될 수 있다. 이 방식으로, 수표가 지불 가능한 경우, 사기에 의해 동일한 일련 번호로 발생하는 임의의 다른 수표도 지불 가능하다. 예를 들어, 근원적인 확률적 지불 시스템이 이전 장에서 제시된 바와 같은 경우, 언제 수표가 지불 가능한지를 결정하는데 사용되는 (사용자에 의해 예측될 수 없는) 양(V_i)은 아마도 전체 C_i 의 상인의 서명보다는 오히려, 사용자의 계좌 번호 및/또는 이름과 함께, 단순히 S_i 만으로 이루어질 수 있다.

사용자가 돈을 더 적게 지불하고자 하는 다른 방식은 일련 번호를 이들의 사용 회수가 부적절한 시퀀스로 사용하는 것이다. 예를 들어, 악의가 있는 사용자는 S_{100} 이 지불 가능한 수표의 가장 낮은 일련 번호라는 것을 확신한다면, 자신이 사용하는 수표가 지불을 위해 선택되지 않을 것이라는 점을 확신하는 동시에, 자신이 동일한 일련 번호를 두 번 사용하는 것이 불잡힐 것이라는 점에 대해 근심하지 않도록 하기 위하여, 일련 번호(S_1 내지 S_{99})의 재사용을 시작하는 것에 대해 계획할 수 있다. 그러나, 이 종류의 게임 계획으로도, 악의가 있는 사용자는 불잡힐 많은 가능성을 여전히 갖는다. 이는 사용자가 나중에 1과 99 사이의 일련 번호를 재사용하는 경우, 사용자가 불법 수표가 지불되지 않도록 할 수 없기 때문이다. 이는 어떤 명확한 확률로 발생할 것이며, 그러한 경우에, 은행은 수표(C_{100})가 시간(t_{100})을 갖는 거래(T_{100})에 대해 지불 가능했다는 것 및 사용자가 그 시간이 t_{100} 보다 늦은 거래에 대해 S_{100} 보다 낮은 일련 번호를 갖는 수표를 생성했다는 것을 통지할 것이다. 다시, 은행에 의한 결과적인 제제에 의해, 사용자가 이 방식으로 사기치는 것이 비생산적이 될 수 있다. 이 종류의 스크리닝 메커니즘이 유연하게 동작하도록 하기 위하여, 각각의 수표가 자신이 지불될 거래의 시간 표시를 지니는 것, 및 선택 프로세스가 시작되기 전에, 상인이 잘못된 시간-표시를 지니는 수표를 무효한 것으로 무시하는 것이 바람직하다.

이러한 위조-방지 전략을 더 양호하게 지원하기 위하여, 은행은 예로서, 수표의 일련 번호만을 따르는 구성요소, 및 시간만을 따르는 구성요소 둘 다를 포함하도록 지적되는 선택 절차를 상인이 사용하는 것을 요청할 수 있다. 다른 구성요소는 전체 수표를 따를 수 있다. 본질적으로, 2개 이상의 선택 절차가 존재할 수 있고, 수표는 이들 중 어느 하나의 결과가 선택될 수표를 결정하는 경우 선택될 수 있다. 이와 같은 변형은 당업자들에게는 명백해야 한다.

악의가 있는 사용자(U')는 또한 U'에 의해 서명되고 M'에 의해 제공된 상품/서비스/정보에 대해 소비된 수표가 항상 지불 가능하도록 하기 위하여, 악의가 있는 상인(M')과 결탁할 수 있다. 이 방법에서, 간소화하기 위해 각각의 지불 값이 1 센트라고 가정하면, U'는 항상 은행에 의해 단지 1 센트 차변받는 반면, M'은 항상 1/s(즉, $s=1/1000$ 인 경우 \$10)을 차변받을 것이다. 그 후, U' 및 M'가 이들의 불법 수익을 공유할 수 있다: 실제로, U'는 자신이 (익명으로) 상인인체하는 경우, M'와 일치할 수 있다.

그럼에도 불구하고, U' 및 M'는 적당한 불법 이득을 만들 수 있다: 이들은 상술한 방법을 몇 번 반복함으로써 자신들의 불법 이득을 높이하고자 하는 경우, 시스템으로부터 제외될 것이다. 이는 특히, M'이 시스템에서 합법적인 이득을 갖는 경우에, 지불하는데 고가이다. 제외된 사용자 및 상인이 예를 들어, 새로운 아이덴티티로 시스템에 되돌아오기가 용이하지 않은 경우, 또는 제 1위치에서 시스템에 들어가는데 필요한 가격(예를 들어, 최초 인증서를 획득한 가격)이 충분히 높은 경우, 이 불법적인 게임은 거의 지불되지 않는다. 이는 사용자에게 부정적인 리턴이며, 관련 비용은 은행에 의해 용이하게 흡수될 것이다.

어쨌든, 이 종류의 사기는 제 1당사자가 보안 하드웨어를 사용함으로써 제거될 수 있다. 이러한 변조방지 구성요소는 예를 들어, 새로운 수표가 생성될 때마다 적절하게 증분시키고, 비밀 서명 키를 안전하게 유지하며 새로운 수표의 서명 구성요소를 생성할 책임이 있을 수 있다. 따라서, 악의가 있는 사용자가 자신의 상인 공범자에게 지불 가능한 수표를 생성하고자 시도하는 경우, 매 시도마다, 그 사용자는 또한 일련 번호를 증가시켜야 한다. 따라서, 일단 지불 가능한 수표가 생성되면,

상인은 소정의 금액을 지불받지만, 사용자는 또한 대응하는 적절한 금액을 차변받을 것이다. 본 명세서의 어딘가에서, 당사자가 이와 같은 동작의 적어도 일부를 수행하는 보안 하드웨어를 사용하고/하거나, 사용하도록 요청받을 수 있다는 점에 유의해야 한다. 이와 같은 보안 하드웨어는 특히, 스마트 카드 또는 이동 전화에 포함될 수 있다.

정직한 사용자가 악의가 있는 것처럼 보일 수 있는 확률이 낮게 존재하는데, 왜냐하면 그가 n 개의 수표를 기록한 후, 이들 중 n^* 보다 상당히 더 많은 것이 우연히 지불 가능해질 수 있다. 이 경우에, 그는 제외될 것이다. 적절한 파라미터 설정에 의하여, 이와 같은 사용자가 매우 적어질 것이다. 게다가, 이들이 의도하지 않게 은행에 손실을 입히는 것을 이들 사용자에게 통신하는 것이 가능하다. 예를 들어, 은행은 상당히 다수의 이들의 수표가 지불 가능한 것으로 발견되었다는 것을 드러내고, 동수의 이들의 수표가 실제로 지불 가능했던 이유를 설명하는 정보를 사용자에게 제공할 수 있다. 결과적으로, 이들 사용자는 상이한 조건 하에서 - 예를 들어, 사용자가 자신이 실제로 소비한 금액보다 더 큰 금액만큼 차변받는 위험성을 지니는 확률적 지불 시스템의 사용자로서 소액지불 시스템에 머무르는 것을 수용할 수 있다. 이와 같은 변화는 사용자와 은행 간의 원래 계약 내의 자동적인 특징으로서 통합될 수도 있다.

상술한 바와 같이, 은행은 자신이 이 수표(및 지불을 위해 선택되는 그 사용자로부터의 모든 이전의 수표)를 커버하는데 충분한 자금을 사용자로부터 수신할 때까지, 지불을 위해 선택된 수표의 지불을 연기함으로써, 통계적인 변형과 관련된 위험성 중 일부, 및 사용자의 사기와 관련된 위험성 중 일부를 상인에게 시프트시킬 수 있다. 상술한 바와 같이 본 발명을 따르면, 은행은 사용자가 기록했던 수표의 수에 따라 사용자로부터 계통적으로 자금을 수신할 것이며, 지불을 위해 선택되었던 수표를 상인으로부터 수신할 것이다. 사용자가 정직하고 수표를 자주 기록할 때, 이 방식에서 상인은 은행으로부터 지불을 오래 대기하지 않아야 한다. 또한, 은행이 각 수표의 완전한 값이 아니라, 다소 할인된 금액을 상인에게 지불하는 경우, 사용자의 계좌는 전형적으로, 사용자 지불 요금이 은행의 지급 요금을 다소 초과하기 때문에 전액(또는 거의 전액) 납입되어야 한다. 이 경우에, 상인은 짧은 지연 직후 또는 단지 짧은 지연 후, 지불을 예측해야 한다. 이 방식으로 상인에 대한 위험성을 감소시키는 것은 지불을 위해 선택된 사용자의 수표에 대해 행해진 지급이 사용자로부터 수령액을 초과할 임의의 위험성을 은행이 더 이상 가정하기 않기 때문에, 사용자 및 상인이 은행에 사기치기 위한 노력에 결탁하지 않도록 하는데 특히 유용한 방법일 수 있다. 이 변형이 채용되면, 은행이 사용자의 계좌와 관련된 "계류중인, 미지불" 수표의 총액을 사용자의 인증서에 표시하여, 이 계좌가 과도한 것처럼 보이는 경우에, 상인이 사용자의 수표를 수신하는 것을 결정할 수 있도록 하는 것이 유용할 수 있다.

본 발명의 제 3실시예의 방법 및 시스템은 또한 균일하고 고정된 거래 값을 갖지 않는 소액지불을 처리할 수 있도록 한다. 하나의 방법은 명시적으로 1-센트 수표의 번들로서 v 센트의 가치가 있는 수표를 연속적인 일련 번호로, 취급하는 것이다. 더 효율적인 방법은 사용자가 단일 일련 번호를 특징으로 하는 것이 아니라, (종점 S 및 $S+v-1$ 둘 다를 나타내는) 일련 번호 간격 $[S, S+v-1]$ 을 특징으로 하는 단일 수표를 기록하는 것이다. 이 수표가 지불 가능하면, 사용자는 $S+v-1-S_{\max}$ 센트 만큼 차변받고, 새로운 $S_{\max}$ 는 $S+v-1$ 이 될 것이다.

본 발명의 이러한 제 3실시예에서, 수표가 지불 가능한 것으로 결정되는 프로세스는 가변 값의 수표가 지원될 때, 수표의 값에 따를 수 있다. 즉, 단일 선택 확률(s) 대신, 0보다 큰 각각의 정수(v)에 대하여 선택 확률(s_v)이 존재하며, 이들 확률은 상이할 수 있다. 이 절차는 간단한 "단계 함수"의 형태를 사용할 수 있다: v 센트에 대한 수표는 v 가 100보다 적은 경우, 확률($1/100$)로 지불 가능하고, v 가 100 또는 그 이상인 경우 확률(1)로 지불 가능하다. 대안적으로, "램프 함수"가 사용될 수 있다: 수표는 v 가 많아야 1000인 경우, 확률($v/1000$)로 지불 가능하고, v 가 적어도 1000인 경우 확률(1)로 지불 가능하다. 그러나, 방식을 사용하는 것은 다양한 형태의 사기를 검출하는 은행의 능력과 역으로 상호작용하여, 이들은 주의하여 사용되어야 한다. 예를 들어, 은행은 단지 최대 일련 번호만 인지되었다면, 지금까지 상인에게 지불되었을 금액을 더 이상 용이하게 예측할 수 없다. 이 때문에, 선택 확률을 고정된 채로 유지하는 것이 바람직할 수 있다. 이 방향에서, 하나의 매력적인 방법은 은행이 자신의 허용된 일련 번호 세트, 자신의 최대 지불 가능한 크기, 및 자신의 선택 확률(s)을 각각 규정하는 두 개 이상의 인증서를 발부하는 것이다. 그 후, 본질적으로, 사용자는 자신의 파라미터 및 한도를 각각 지니지만, 자신의 선택 확률(s)을 각각 지닌 상이한 "수표장"의 세트를 갖는다.

동일하지 않은 거래 값 경우를 더 상세히 참조하면, 본 발명의 제 3실시예는 사용자가 다수의 n 개의 거래($T_1, T_2, \dots, T_n$)에 대한 지불을 선정하도록 하며, 여기서, 각 거래(T_i)는 부분적으로 정수 인덱스(i) 및 거래 값(TV_i)에 의해 특징 지워지며, 각각의 T_i 는 동일한 값으로 이루어지는 것이 아니지만, 각각의 TV_i 는 공통 단위 값(UV)의 배수로서 특징 지워질 수 있다. UV 는 예를 들어, 1 센트일 수 있다. 이 경우에, 각 데이터 스트링(C_i) 정수 인덱스(i), 및 T_i 의 값(TV_i)에 대한 정보를 포함한다. 상기 정보는 그 수표에 대한 "최초 일련 번호" 및 "최종 일련 번호"로 이루어진 한 쌍의 값(S_i, S_i+v_i-1)의 형태를 취

할 수 있다. 1과 n 사이의 모든 값에 대하여, S_i 는 순차적으로 순서화되고, 순서화된 연속적인 데이터 스트링(C_j)($j=1, \dots, n$) 내의 다른 데이터 스트링과 관련된 C_i 의 위치를 나타내는 프로그래시브 일련 번호이다. v_i 는 i 에 따른 정수이며, T_i 의 값 (TV_i)을 나타내고, $v_i = TV_i / (UV)$ 에 의해 제공된다.

상인은 어느 수표(C_j)가 지불 가능하도록 선택될지를 사용자가 미리 예측하지 못하도록 하는 방식으로 지불 가능한 것을 수신된 수표(C_j)($1 \leq j \leq n$)로부터 선택한다. 하나의 형태에서, 상인은 I 장에 설명된 방법, 즉, 사용자에게 실질적으로 예측 불가능한 (상인의 비밀 키를 사용하여 생성된 C_j 에 대한 상인의 디지털 서명과 같은) 아이템(V_j)을 C_j 와 관련시키는 것을 사용할 수 있다. 상인은 선택된 수표(C_j)가 지불 가능한지를 제 3당사자가 검증할 수 있도록 하는 정보(I_j)를 제 3당사자로 하여금 수신하도록 한다. 제 3당사자는 I_j 의 수신에 응답하여, 선택된 수표(C_j)가 실제로 지불 가능한지를 검증한다. C_j 가 지불 가능한 경우, 및 어떤 다른 조건이 또한 충족되는 경우에, 제 5당사자는 $S_{\max}$ 및 $v_{\max}$ 의 값을 결정하고, 여기서, $\max$ 는 $1 \leq \max \leq n$ 인 정수이며, $v_{\max} = TV_{\max} / (UV)$ 이다. $S_{\max}$ 는 지불을 위해 지금까지 선택된 임의의 수표의 최대의 최종 일련 번호를 나타낸다. 그 후, 제 5당사자는 (지불받는 사람이며, 상인 또는 또 다른 당사자일 수 있는) 제 4당사자가 수표 금액 (CR)을 수신하도록 한다. 제 5당사자는 제 1당사자가 D_i 와 관련된 차변 금액만큼 차변받도록 하며, 여기서 D_i 는 다음:

$(S_i + v_i - 1 - S_{\max}) * UV$ 에 의해 제공된다.

그 후, $S_{\max}$ 는 $S_i + v_i - 1$ 인 것으로 설정된다.

균일하지 않은 거래 값의 경우에 사기는 붙잡히고, 고정된 거래 값의 경우와 유사한 방법을 사용하여 처리된다. 예를 들어, 2개의 지불 가능한 수표, 즉, S 및 $S + v - 1$ 사이의 일련 번호(S')에 의해 특징 지워지는, 단일 센트에 대한 수표, 및 일련 번호 간격 [$S, S + v - 1$]에 의해 특징 지워지는, v 센트에 대한 또 다른 수표는 이 경우에, 사기의 증거로서 간주될 것이다. v 의 매우 높은 값에 대한 수표는 승인되지 않을 수 있는데, 즉, 지불이 거절될 수 있다. 그렇지 않으면, 악의가 있는 사용자가 지불 시스템에 참여하여, 거대한 금액에 대해 단일 수표를 기록하고, 상기 수표가 지불을 위해 선택되지 않는다고 판명되면, 결코 제 2수표를 생성하지 않을 것이다. 이 문제는 또한 그 사용자에게 대한 예측된 최대 "플로트(float)"를 커버할 만큼 충분히 큰 개시 요금과 같이, 사용자가 계좌를 개설할 때, "개시 요금"을 각 사용자에게 부과함으로써 처리될 수 있다. 여기서, "플로트"는 사용자가 기록하였지만 은행이 알지 못하는 수표에서의 예측된 최대 값이다. 본 발명의 어떤 형태의 경우에, 이 플로트는 사용자가 기록할 수 있는 수표의 최대 크기 곱하기 수표가 지불을 위해 선택될 확률의 역수로서 계산될 수 있다. 은행은 상술한 바와 같이, 자신이 이 수표(및 또한 지불을 위해 선택되었던, 사용자가 기록한 이전 수표)를 커버하는데 충분한 자금을 사용자로부터 수신할 때까지, 지불을 위해 선택된 수표에 대한 지불을 연기함으로써 사기치는 것을 방지할 수 있다.

하나의 형태에서, 사용자가 자신이 실제로 소비할 것보다 많이 요금청구받지 않도록 하는 제 3실시예의 방법 및 시스템이 I 장에 설명되었던 근원적인 확률적 지불 방식으로 구현될 수 있다. 이 경우에, 거래(T_i)($i=1, \dots, n$)에 대해 수표(C_i)의 수신 시 상인은 사용자에게 의해 실질적으로 예측될 수 없는 아이템(V_i), 예를 들어, 상인의 비밀 키를 사용하여 생성된, C_i , 또는 (T_i)의 일부에 대한 상인의 디지털 서명($SIG_M(C_i)$)을 수표(C_i)와 관련시킨다. 그 후, 상인은 V_i 가 어떤 특성(P_i), 예를 들어 다음 특성:

$F(SIG_M(C_i)) < s$ (3)을 충족하는지를 결정하는데,

여기서 F 는 비트 스트링에 대해 연산하고 0과 1 사이의 수를 리턴시키는 함수이며, s 는 선택 비율($0 < s < 1$)이다.

V_i 가 특성(P_i)을 충족한다라는 것을 상인이 발견하면, 상인은 V_i 가 P_i 를 충족하는지를 은행이 검증할 수 있도록 하는 정보 (I_i), 예를 들어, V_i 를 발생시키는데 사용되는 상인의 비밀 키에 대응하는 상인의 공개 키를 은행이 수신하도록 한다. V_i 가 P_i 를 충족하지 않으면, 상인은 수표(C_i)를 폐기한다. V_i 가 실제로 P_i 를 충족하고, V_i 가 은행의 자유재량으로 결정된 다른 조건을 충족한다라는 것을 은행이 발견하면, (은행, 또는 은행 이외의 실체일 수 있는) 제 5당사자는 (상인, 또는 상인 이외의 실체일 수 있는) 제 4당사자가 대변 금액(CR_i)을 수신하도록 한다. 제 5당사자는 또한 사용자가 차변 금액만큼 차변받도록 한다.

제 3실시예에서, 사용자에게 청구되는 금액(D_i)은 상인(또는 다른 실체)가 수신하는 금액(CR_i)과 반드시 동일하지는 않다. 그러나, 제 3실시예의 방법은 사용자가 차변받는 금액(D_i)이 결코 사용자가 자신의 수표를 기록함으로써, 총계로서 실제로 소비했던 금액보다 더 많지 않도록 하는 선택적 예치 프로토콜을 포함함으로써, 근원적인 확률적 지불 방식과 구별된다. 특히, 선택적 예치 프로토콜은 총계로서, 차변된 금액이 항상 대응하는 거래 값보다 더 크지 않도록 한다. 바꿔 말하면, 사용자는 결코 자신이 실제로 소비했던 것을 초과하여 요금청구받지 않게 된다.

도 5는 본 발명의 제 3실시예에 따른, 거래(T_i)에 대한 지불을 설정하는 소액지불 시스템(200)의 구성요소를 설명하는 개략적인 블록도를 제공한다. 시스템(200)은 사용자, 상인, 및 은행이 전자 데이터, 및 심지어 지불을 서로들 간에 전송하도록 하는 통신 수단(210)을 포함한다. 전자 데이터는 전자 수표를 나타내는 데이터 스트링, 또는 메시지를 나타내는 스트링을 포함할 수 있다. 하나의 실시예에서, 통신 수단(210)은 원격 서버로 접근하도록 한다. 통신 수단(210)은 모뎀 및 네트워크 인터페이스 카드를 포함하지만 이로 제한되지 않는 종래 기술에 공지된 하나 이상의 네트워크 인터페이스 장치를 포함할 수 있다. 하나 이상의 버스, 예를 들어, 어드레스 버스(214) 및 데이터 버스(215)는 여러 네트워크 노드들 사이에 데이터를 전달하기 위하여 제공될 수 있다.

시스템(200)은 또한 제 1처리 수단(205) 및 제 2처리 수단(206)을 포함한다. 제 1 및 제 2처리 수단은 컴퓨터 시스템, 예를 들어, DOS 또는 Windows 운영 시스템을 실행하는 디지털 컴퓨터일 수 있고 어드레스 버스(214) 및 데이터 버스(215)에 접속된다. 각 처리 수단(205 및 206)은 전형적으로 데이터를 저장하기 위한 저장 수단(221), 데이터를 입력하기 위한 입력 수단(222), 및 이 시스템 명령을 수행하는 중앙 처리 장치("CPU")(223)를 포함한다. 저장 수단(221)은 컴퓨터 메모리 및 하드 디스크, CD-ROM 등과 같은 데이터 저장 장치를 포함할 수 있다. 입력 수단(222)은 종래 기술에 공지된 입력 장치, 예를 들어, 종래의 키보드일 수 있다.

제 1처리 수단(205)은 거래 $T_i(i=1, \dots, n)$ 에 관련된 데이터 스트링(C_i)을 도출, 입력 및 저장하기 위하여 사용자에게 의해 동작되는데, 이 데이터 스트링(C_i)에는 수표($C_j(j=1, \dots, n)$)의 순서화된 연속값(ordered succession)에서 다른 수표에 대한 수표(C_i)의 위치를 나타내는 프로그래시브 일련 번호(S_i)가 포함된다. 제 2처리 수단(106)은 상인에 의해 동작되고 C_i 에 응답하여 아이템(V_i)을 C_i 와 관련시킨다. 제 2처리 수단(106)은 또한 V_i 가 특성(P_i)을 충족하는지를 결정하도록 동작된다. 예를 들어, 명령들의 세트는 제 2처리 수단(206)의 CPU(223)로 입력되어 이 CPU가 C_i (또는 C_i 의 일부)와 관련되는 아이템(V_i)을 도출하도록 하고 V_i 가 특성(P_i)을 충족하는지를 이 CPU(223)가 결정하도록 한다. 이는 제 2처리 수단(206)의 CPU(223)가 다음 단계, 즉 은행이 V_i 가 P_i 를 충족하는지를 검증하도록 정보(I_i)를 은행에 전달할 것을 명령하는 단계를 실행하기 위해선, 이는 충족되어야만 되는 필요 조건이다. 처리 수단(206)에서 CPU(223)는 V_i 가 P_i 를 충족할 때 선택적으로 동작되도록 프로그램 되어 정보(I_i)를 은행에 전송한다.

시스템(200)은 또한 V_i 가 P_i 를 충족할 때 은행(또는, 또 다른 제 5당사자)에 의해 선택적으로 동작되는 수단(240)을 포함하여, 제 4당사자(이는 상인 또는 또 다른 실체일 수 있다)가 총액을 수신하도록 한다. 이 수단(240)은 또한 V_i 가 P_i 를 충족할 때, 1) S_{max} 의 값을 결정, 여기서 S_{max} 는 지불된 마지막 수표의 일련 번호(지금까지 지불을 위하여 은행에 제출된 어떤 수표상의 일련 번호들 중 가장 큰 일련번호); 2) 제 4당사자에게 금액 CR 의 지불의 전달을 명령; 및 3) 사용자가 금액 (D)만큼 차변하도록 선택적으로 동작되도록 프로그램될 수 있는 CPU를 갖는 컴퓨터 시스템일 수 있다.

즉, 본 발명의 제 3실시예의 소액지불 시스템 및 방법은 사용자가 실제로 소비한 것을 초과하여 결코 요금청구받지 않도록 하는 메커니즘을 제공한다. 이 방식으로, 제 3실시예에서 제공된 시스템 및 방법은 소액지불 방식의 보편적인 수락을 실행시키는 주요한 요인인 사용자 수락을 크게 향상시킨다.

IV. 은행에 의해 제어되는 연기된 선택 프로토콜을 포함하는 소액지불 시스템

본 발명의 제 4실시예는 은행이 상인으로부터 하나 이상의 수표에 대한 커미트먼트를 수신할 때까지 지불 선택 프로세스를 연기하는 연기된 선택 프로토콜을 포함하는 확률적 소액지불 방식을 특징으로 한다. 이와 같은 연기된 선택 프로토콜을 성취하는 여러 방법들이 존재한다. 제 1(및 바람직한) 방법은 다음과 같다. 사용자는 소액지불 거래(T)로부터 도출되고 거래의 시간(t)의 적절한 표시를 제공하는 데이터 스트링 또는 "전자 수표" (C)를 생성하고 사용자가 지불하길 원할 때 상인에게 C 를 전송한다. 상인은 소정의 시간 간격(예를 들어, 소정의 날짜)에서 한 명 이상의 사용자로부터 수신한 수표(C_i

($i=1, \dots, n$)를 m 리스트 L^k (여기서 $k=1, \dots, m$)으로 그룹화한다. 여기서 m 은 임의적이지만 예를 들어 $1/s$ 와 동일하거나 거의 동일한 정수 일 수 있으며, s 는 원하는 선택 확률이다. 각 리스트는 m 개의 상호 배타적인 특성들($P_1, \dots, P_m$) 중 정확하게 한 특성을 충족하는 모든 수표를 포함하는 것이 바람직하다. 예를 들어, $m=1024$ 이면, 각 리스트 L^k ($k=1, \dots, m$)는 결정론적 해쉬 함수(H)에 따라서 해쉬된 그 날짜에 수신된 모든 수표를 포함하여 제 1의 10비트가 정수($k-1$)의 10-비트 2진 확장인 값을 산출한다. 각 리스트 L^k ($k=1, \dots, m$)는 l_k 개의 수표 ($C^k_1, \dots, C^k_{l_k}$)을 포함하며, 여기서 l_k 는 리스트 L^k 에서 데이터 스트링의 수를 표시한다. m 개의 리스트에 걸쳐서 합산될 때, l_k 는 본래 수신된 수표의 총수(n)까지 합산되는데, 즉 다음과 같다.

$$l_1 + \dots + l_k + \dots + l_m = n$$

상인은 L^k 에 대한 커미트먼트(CM^k)를 계산함으로써 각 리스트(L^k)에 커미트하고 은행이 CM^k ($k=1, \dots, m$)을 수신하도록 한다.

종래 기술에 공지된 바와 같이, 커미트먼트 방식은 메시지의 내용을 드러내지 않고 이 메시지에 커미트되면서 한 당사자가 메시지를 또 다른 당사자로 전달(deliver)하도록 하는 프로토콜이다. 이 프로토콜은 이들 당사자가 "잠겨진 상자(locked box)"에서 메시지를 전달하는 프로세스를 에뮬레이트하도록 하여, 전송자(이 경우에, 상인)는 수신자가 상자의 열쇠를 장차 제공받을 때까지 수신자(이 경우에, 은행)가 상자 내 메시지에 대해서 전혀 알지 못하도록 할 수 있다. 수신자가 이 메시지를 수신한 후엔, 수신자측에선 송신자가 박스 내 메시지를 변경하지 못하도록 할 수 있다. 커미트먼트 방식은 전형적으로 2개의 단계로 이루어진다. 제 1단계("커미트먼트 단계")는 잠겨진 박스의 전달(delivery)을 시뮬레이트 한다. 이 단계가 완료될 때, 수신자는 여전히 메시지를 알지 못하지만, 송신자는 더 이상 이를 변경할 수 없다. 제 2단계("디커미트먼트 단계")는 키의 전달(delivery)을 시뮬레이트 한다. 수신자는 현재 메시지를 알 수 있고 잠금해제된 박스 내 메시지가 실제로 송신자가 자신에게 커미트한 메시지인지를 검증할 수 있다.

바람직한 형태에서, L^k 에 대한 커미트먼트(CM^k)는 해쉬 값 $H(L^k)$ 일 수 있는데, 여기서 H 는 일방향충돌 회피 해쉬 함수이다. 그러므로, CM^k 로부터 L^k 를 계산적으로 도출할 수 없고, 또한 $H(L_1^k) = H(L_2^k)$ 가 되도록 2개의 상이한 스트링 (L_1^k 및 L_2^k)를 계산적으로 산출할 수 없다.

본 발명의 제 4실시예에서 특징으로 하는 연기된 선택 프로토콜에서, 특정 수표(C_i)가 지불을 위하여 선택되는지를 결정하기 위한 지불 선택 프로세스는 은행이 리스트(L^k)에 대한 상인의 커미트먼트(CM^k)($k=1, \dots, m$)을 수신할 때까지 연기된다. 이는 본 발명의 제 4실시예에서 설명된 소액지불 방식을 구별하는 특징이다. CM^k ($k=1, \dots, m$)의 수신시, 은행은 상인과 사용자에게 예측될 수 없는 방식으로 1 및 m 간의 하나의 인덱스(k)를 선택한다. 예를 들어, 은행은 해당 날짜(예를 들어, 2001. 01. 01)을 디지털적으로 서명하고 나서, 선택을 위하여 이 서명의 제 1의 10비트를 사용할 수 있다. 이 서명은 제 1의 10비트가 추출되기 전 해쉬될 수 있다. 은행의 서명은 공개(예를 들어, 웹 상에 게시된다) 되어, 모든 사람이 k 가 실제 그 날짜에 은행에 의해 선택된 인덱스라는 것을 검증할 수 있도록 한다. 선택된 인덱스 (k)는 지불 인덱스이다. 상인은 CM^k 을 수표 L^k 의 원래 리스트로 디커미트함으로써 응답한다. 대안적으로, 은행은 리스트(L^k)에 대해서 상인의 커미트먼트(CM^k)($k=1, \dots, m$)의 함수로서 인덱스(k)를 계산할 수 있다. 예를 들어, k 는 $CM^1 \dots CM^m$ 또는 $H(CM^1 \dots CM^m)$ 의 은행의 서명으로부터 추출될 수 있는데, 여기서 H 는 일방향 해쉬 함수이거나 어떤 소정의 함수(f)에 대한 $f(CM^1 \dots CM^m)$ 이다.

그 후, 은행은 모든 것이 적절한지를 검사한다. 예를 들어, 은행은 디커미트된 리스트 내의 수표가 실제로 해당 날짜에 대한 것인지, 리스트 내에 중복 수표가 존재하는지, 리스트 내의 모든 수표가 특성(P_k)을 만족하는지, 존재하는 경우 사용자 서명이 유효한지 등을 검증한다. 이들 조건들 중 어느것도 부합되지 않으면, 은행은 상인(또는 경우에 따라 사용자, 예를 들어, 은행은 사용자가 동일한 일련 번호를 가진 2개의 수표에 서명하였다는 것을 발견하였기 때문이다)에게 벌금이나 다른 징벌 조치를 취할 수 있다. 그렇지 않다면, 은행은 L^k 내의 수표의 수집값의 m 배를 상인에게 지불한다. 대안적으로, 은행은 검사된 리스트가 검사를 만족스럽게 통과하면 모든 리스트 내의 모든 수표의 총 금액을 상인에게 지불할 수 있다. 이들 지불의 일부는 또한, 사용자의 계정이 이들 수표를 커버하는데 불충분한 예금을 갖고 있는 경우 상술한 바와 같이 연기될 수 있다.

그 후, 수표가 L^k 에 속하는 사용자는 여러 가지 가능한 방식들 중 한 방식으로 차변받을 수 있다. 예를 들어, 이들 사용자는 (제 1실시예에서와 같이) 선택된 수표의 액면가로 그리고 (제 3실시예에서와 같이) 선택된 수표의 일련 번호에 따라서 m 배 차변받을 수 있다. 은행은 앞서의 실시예에 포함된 방식들로 정밀조사를 실시하거나 벌을 줄 수 있다. 은행은 또한 상인에게 부가적인 리스트를 디커미트하도록 요청하여 모든 것이 적절한지를 검증하거나 하나 이상의 지불 인덱스를 선택한다. 후자의 경우에, 은행은 L^k 내의 수표의 수집값의 m/r 배를 상인에게 지불할 수 있는데, 여기서 r 은 지불을 위하여 선택된 리스트의 수이다. 이 경우에, 선택 확률은 $1/m$ 이 아니라 r/m 이다. 대안적으로, 은행은 2개 이상의 리스트를 검사하고 나서 모든 리스트 내의 모든 수표에 대한 수집 금액을 상인에게 지불할 수 있다.

커미트먼트는 본 발명의 범위 내에서 재귀적으로 사용될 수 있다는 점에 유의하라. 예를 들어, 은행에 리스트(L^k) ($k=1,...,m$)에 대한 m 개의 커미트먼트(CM^k)($k=1,...,m$)를 전송하는 것이 아니라, 상인은 은행에 이들 m 개의 커미트먼트에 대한 커미트먼트를 전송할 수 있다. 예로서, 상인은 은행에 단일값($C=H(CM^1...CM^m)$)을 전송할 수 있는데, 여기서 H 는 일방향 해쉬 함수이다. 은행이 하나 (또는 그 이상) 인덱스(k)를 선택한 후, 상인은 우선 CM^k 가 무엇인지를 드러내도록 하기 위하여 C 를 디커미트하고 나서, 수표의 대응하는 리스트를 드러냄으로써 전과 같이 CM^k 를 디커미트할 수 있다. 예를 들어, $C=H(CM^1...CM^m)$ 이면, 상인은 모든 m 개의 커미트먼트($CM^1...CM^m$)를 드러냄으로써 CM^k 에 대한 정확한 값을 드러낼 수 있다. 은행은 동일한 값($C=H(CM^1...CM^m)$)이 산출되는 지를 점검하기 위하여 이들 m 값들을 일방향 해쉬하고 나서 CM^k 를 격리시키기 위하여 k 번째 커미트먼트를 검색할 수 있다. 물론, 상인은 또한 단일 커미트먼트(C)가 아니라 다수의 커미트먼트를 은행에 전송함으로써 m 개의 커미트먼트 ($CM^1...CM^m$)에 커미트할 수 있다. 예를 들어, 상인은 $CM^1...CM^{10}$ 에 커미트먼트, $CM^{10}...CM^{20}$ 에 제 2커미트먼트 등을 전송할 수 있다.

전형적으로, 단일값(V)(예를 들어, 어떤 일방향 해쉬 함수(h)에 대한 $V=h(V_1,...,V_m)$ 에 의해)에 의해 m 개의 값($V_1...V_m$)에 커미트하기 위하여, V_i 만을 디커미트하기 위하여 모든 $V_1...V_n$ 을 드러내며/전송하여야 한다. 이는 m 이 매우 크며 및/또는 V_i 가 매우 큰 경우 비실용적일 수 있다. 본 발명의 시스템에 사용될 커미트먼트에 대한 특정한 간편한 방법은 일반화된 Merkle 트리이다. "일반화된 Merkle 트리"란 모든 다른 값들에 디커미트함이 없이 이와 같은 값들 중 단지 한 값에 디커미트하도록 하는 m 개의 값들에 대한 커미트먼트를 의미한다.

일반화된 Merkle 트리의 특수한 경우는 본원에 참조된 Merkel에 허여된 미국 특허 4,309,569호에 서술된 널리 공지된 Merkle 트리 커미트먼트 방식이다. Merkle 트리를 구현하기 위한 한 가지 방식은 가능한 지향되지 않은 그래프(G)의 노드에 커미트될 값을 저장하는 것인데, 이들 에지의 일부는 비환식(및 전형적으로 트리형) 서브그래프(G')(바람직하게는 G 와 동일한 노드를 가짐)을 산출하기 위하여 지향될 수 있고 노드의 G' 의 디센던트(descendants)에 저장된 값들을 따른 값과 또한 가능한 부가적인 값을 따른 값을 각 노드에 저장하기 위하여 (예를 들어, 근원적인 일방향 해쉬 함수를 기반으로 한 가능한 가환식 일방향 해쉬를 사용함으로써) 하나 이상의 근원적인 일방향 해쉬 함수를 사용한다. 이 방식으로, 원래 값들 중 적어도 하나 이상을 변경시키면 근원적인 일방향 해쉬 함수들 중 한 함수에서 충돌이 발견되지 않는 한 높은 확률로 G' 의 루트 노드 중 하나 이상에 저장된 값들을 또한 변경시킨다. 이 방법을 사용하면, 루트 노드(들)에 저장된 값(들)은 그 그래프 노드에 저장된 원래 값에 대해 커미트먼트를 구성한다. 게다가, 어떤 제약들(이는 은행에 의해 나중에 점검될 수 있다)이 있을 수 있는데, 이들 제약들에 대해서 그래프에서 커미트된 각종 값들이 저장될 수 있다. 어쨌든, 상인은 일반화된 Merkle 트리를 사용하여 $CM^1...CM^m$ 에 커미트할 수 있다. 또한, 커미트먼트 CM^k 는 리스트(L^k)를 해시하는 일반화된 Merkle 트리에 의해 생성될 수 있다. 일반화된 Merkle 트리를 사용하면 커미트먼트를 사용하는 본 발명의 어떤 양상에서 발생될 수 있다.

상인은 커미트먼트 값($CM^1...CM^m$)(가능한 이들 자체는 하나 이상의 커미트먼트(C)에 의해 커미트된다), 이들 리스트 각각 내의 수집 금액과 같은 리스트($L^1...L^m$)에 관한 다른 양, 또는 이들 리스트 각각의 수표 수와 함께 은행에 전송하는데 유용한 것을 찾을 수 있다 라는 점에 유의하라. 이들 다른 양은 임의의 커미트먼트의 외부에서 통신될 수 있다. 예를 들어, 상인은 은행에 $CM^1...CM^m Q^1...Q^m$ 을 전송할 수 있는데, 여기서 Q^i 는 "클리어에서" L^i 양을 표시한다. 이는 예로서 은행이 부가적인 디커미트먼트 없이 각 리스트의 수집 양의 합을 평가하도록 한다.

연기된 선택 프로토콜을 포함하는 확률적 소액지불 방식을 구현하는 다른 관련된 방법이 존재한다. 이들 방법들에서, 지불 선택 프로세스는 은행이 상인으로부터 상인이 다수 사용자로부터 수신한 하나 이상의 수표에 대한 커미트먼트를 수신할

때까지 연기된다. 그 후, 은행은 공정하고 확률론적으로 커미트된 수표중 어느것이 지불될 수 있는지를 결정한다. 본 발명의 제 4실시예의 연기된 선택 프로토콜은 또한, 사기꾼이 어떤 실질적 손해를 일으키기 전 은행이 기만한 당사자들에게 벌을 주며/제거하도록 한다.

도 6은 본 발명의 제 4실시예에 따른 소액 지불 거래를 위한 방법의 개요도를 순서도 형태로 제공한다. 사용자는 소액지불 거래(T)로부터 도출되는 데이터 스트링 또는 "전자 책" (C)을 생성하고 사용자가 지불하길 원할 때 C를 상인에게 전송한다. 본 발명의 예시된 실시예에서, 다수의 거래 $T_i(i=1,...,n)$ 가 수반된다. 사용자 또는 사용자들은 각 거래(T_i)에 대해서 수표(C_i)를 도출하고 상인이 수표($C_i(i=1,...,n)$)을 수신하도록 한다.

상인은 사용자로부터 수신한 수표($C_i(i=1,...,n)$)를 m개의 리스트(L^k)로 그룹화하는데, 여기서 $k=1,...,m$ 이다. 각 리스트($L^k(k=1,...,m)$)는 l_k 데이터 스트링($C^k_1,...,C^k_{l_k}$)를 포함하는데, 여기서 l_k 는 소정의 리스트(L^k)에서 데이터 스트링의 수를 표시한다. m개의 리스트에 걸쳐서 합산될 때, l_k 는 본래 수신된 수표의 총 수(n)까지의 합이다. 즉 다음과 같다.

$$l_1 + ... + l_k + ... l_m = n$$

그 후, 상인은 L^k 에 대한 커미트먼트(CM^k)를 계산함으로써 각 리스트(L^k)에 커미트하고 은행이 각 k(즉, $k=1,...,m$ 에 대해)에 대해 CM^k 를 수신하도록 한다.

수표를 리스트로 그룹화하는 것은 상인과 은행에 의해 협정된 특정 규칙에 따라서 행해질 수 있다. 예를 들어, 수표(C)는 리스트(L^i)에 배치될 수 있는데, 여기서 i는 예를 들어 C의 일련 번호를 사용하거나 C로부터 일부 비트를 추출함으로써 또는 C의 해쉬로부터 일부 비트를 추출함으로써 C의 함수에 따라서 계산된다.

각 거래(T_i)는 거래 값(TV_i)에 의해 특정 지워지는 것이 바람직하다. 또한, 각 데이터 스트링(C_i)은 C_i 를 도출하는 거래(T_i)의 거래 값(TV_i)를 표시하는 데이터를 포함하는 것이 바람직하다. 따라서, 상인은 각 리스트(L^k)에 대한 수집값(V^k)을 결정할 수 있는데, 여기서 V^k 는 다음과 같이 제공된다.

$$V^k = TV^k_1 + ... + TV^k_{l_k}$$

바꿔 말하면, V^k 는 리스트(L^k) 내 모든 데이터 스트링($C^k_1,...,C^k_{l_k}$)의 수집값을 표시한다. 이 경우에, 상인은 또한 값들(L^k)에 커미트하는 것 이외에도 값(V^k)에 선택적으로 커미트할 수 있다. 즉, 상인은 부가적인 커미트먼트 ($CV=H(V^1, V^2,...,V^m)$)를 값들($V^1, V^2,...,V^m$)의 리스트에 제공할 수 있으며, 여기서 H는 일방향 해쉬 함수이다. CV를 디커미트함으로써, 상인은 리스트($V^1, V^2,...,V^m$)를 드러낸다.

제 4실시예에서 특징으로 하는 연기된 선택 프로토콜에서, 특정 수표(C_i)가 지불을 위하여 선택되는지를 결정하기 위한 지불 선택 공정은 은행이 리스트(L^k)에 대한 상인의 커미트먼트($CM^k(k=1,...,m)$)를 수신할 때까지 그리고 이 옵션이 선택되면 은행이 이 값(V^k)에 대한 커미트먼트(CV)를 수신할 때까지 연기된다. 이 집행연기는 제 4실시예에서 설명된 소액지불 방식을 구별하는 특징이다. $CM^k(k=1,...,m)$ (및 선택적인 커미트먼트(CV))의 수신시, 은행은 하나 이상의 정수 인덱스($i_1, i_2,..., i_r$)을 선택하고 상인이 선택된 인덱스($i_1, i_2,...,i_r$)을 수신하도록 한다. 본 발명의 제 4실시예에서, 정수 인덱스들($i_1,...,i_r$)의뱅크에 의한 선택은 수표가 지불을 위하여 선택되는지를 결정하는 선택 프로세스를 표시한다.

r의 값이 임의적이고 이 뱅크까지라는 점에 유의하여야 한다. 더 많은 시도된 사기의 발생률이 존재할 때, 또는 특정 상인에 대해 의심할 때, 더 큰 r값이 사용될 수 있다. 어떤 경우에, 은행은 심지어 상인에게 그 자신의 모든 커미트먼트(즉, $r=m$ 선택)을 디커미트하도록 요청할 수 있다. 통계적 증거에 기초하여 이와 같은 사용자를 나중에 제거하는 것이 아니라 동일한 일련 번호를 갖는 동일한 사용자로부터의 2개의 수표를 포착할 기회를 갖기 위하여 $r>1$ 을 선택하는 것이 권장된다.

인덱스($i_1, i_2, \dots, i_r$)의 수신시, 상인은 인덱스가 그가 수신한 인덱스($i_1, i_2, \dots, i_r$)에 대응하는 이들 커미트먼트(CM^k)를 디커미트한다. 바꿔 말하면, 상인은 ($CM^{i1}, CM^{i2}, \dots, CM^{ir}$)을 디커미트하는데, 즉 상인은 은행이 $CM^{i1}, CM^{i2}, \dots, CM^{ir}$ 각각에 대한 디커미트 스트링을 수신하도록 한다. 이로 인해, 상인은 각 $CM^k = H(L^k)$ 이면 은행($L^{i1}, L^{i2}, \dots, L^{ir}$)에 노출된다. 커미트먼트(CV)가 사전에 은행에 제공되면, 상인은 은행에 리스트($V^1, \dots, V^r$)를 드러낸다. 인덱스가 은행이 선택한 특정 인덱스에 정합하는 이들 리스트에 대해서, 은행은 리스트에 포함되는 데이터 스트링을 알 수 있으므로, 대응하는 수집 거래 값 또한 알 수 있다. CV가 또한 디커미트되면, 은행은 선택된 리스트만이 아니라 모든 리스트에 대한 상인의 요금청구된 수집 거래 값을 인지한다. 은행은 디커미트된 리스트에 대한 수집 거래 값을 재계산할 수 있고 이들 값을 CV의 디커미트먼트와 비교하여, 상인측의 사기를 점검한다. 이와 같은 점검은 또한 각 리스트가 단지 이 리스트에 포함되는데 적절한 수표를 포함하는지를 점검하고 하나 이상의 리스트에 나타내는 수표에 대한 점검을 포함할 수 있다.

본 발명의 제 4실시예에서 특징으로 하는 소액지불 방법 및 시스템에서 최종 단계로서, 제 5당사자(이는 은행일 수 있거나 은행 이외의 실체)는 지불 프로세스를 실행하는데, 즉 제 4당사자(이는 상인 또는 상인 이외의 실체일 수 있다)가 대변 금액(CR)을 수신하도록 한다. 어떤 경우에, 이와 같은 작용은 어떤 조건, 가령 수표의 크리에이터와 관련된 계정에 충분한 자금이 존재하는 것과 같은 조건이 충족될 때까지 연기될 수 있다. 제 5당사자는 또한 수표가 선택된 리스트($L^{i1}, L^{i2}, \dots, L^{ir}$) 중 하나 이상에 속하는 각 사용자가 차변 금액(D)에 의해 차변받을 수 있도록 한다.

바람직한 형태에서, 상인(또는 다른 제 4당사자 실체)에 의해 수신된 대변 금액(CR)은 m개의 리스트 모두에 포함된 모든 수표의 수집값(V)인 것이 바람직한데, 즉, 다음과 같다.

$$CR = V = V^1 + \dots + V^k + \dots + V^m$$

CR을 결정하는 이 방법을 구현하기 위하여, 선택적인 커미트먼트(CV)가 사용되어, CR이 CR의 디커미트먼트의 값들로부터 계산될 수 있도록 한다. 따라서, 은행(또는 다른 제 5당사자)에 의해 상인에게 지불되는 금액(CR)은 상인에 의해 수신되고 m개의 리스트(L^k)($k=1, \dots, m$)로 그룹화되는 모든 수표의 전체 수집값이다.

본 발명의 한 형태에서, 사용자(U)에게 요금청구된 차변 양(D_U)은 인덱스가 은행에 의해 선택된 인덱스에 대응하는 리스트에 포함되는 모든 사용자의 수표의 수집값과 관련된 값에 의해 제공된다. 예를 들어, 값(D_U)은 양(m/r)과 이 수집값을 스케일링함으로써 결정되는데, 선택 확률의 역수 $s=r/m$

$$D_U = (V^{i1}_U + V^{i2}_U + \dots + V^{ir}_U) * (m/r)$$

여기서, V^k_U 는 리스트 (L^k)에 포함되는 사용자 U의 수표의 총 수집값이다.

본 발명의 이 제 4실시예의 또 다른 버전에서, 각 수표(C_i)는 일련 번호(S_i)에 대한 정보를 포함한다. S_i 는 (각 사용자에게서) 1로부터 시작하여 순차적으로 순서화된 수표를 만든 사용자에게 발부된 프로그레시브 일련 번호이고 (이 사용자로부터) 데이터 스트링(C_i)의 순서화된 연속값에서 다른 데이터 스트링에 대한 데이터 스트링(C_i)의 위치를 나타낸다. S_i 는 또한 사용자가 이 상인과 관여되는 거래($T_1, \dots, T_{i-1}$ 및 $T_{i+1}, \dots, T_n$)에 대한 거래(T_i)의 시간 순서를 표시하는 것이 바람직하다.

본 발명의 이 형태에서, 차변 금액(D_U)은 은행에 의해 지불되도록 선택된 이들 리스트에 포함되는 각 수표에서 일련 번호(S_i)를 사용하여 결정된다. 각 거래(T_i)가 동일한 값(TV)을 갖는 경우에, 단일 수표(C_i)에 대응하는 차변 금액은 다음과 같이 제공된다.

$$(SN_i - S_{\max, U}) * TV$$

여기서 $S_{\max, U}$ 는 지금까지 지불을 위하여 처리되고 선택된 C_i 를 산출하는 사용자(U)로부터 가장 최근의 수표에 나타난 일련 번호를 표시한다. 더욱 상세한 설명은 사용자가 실제로 소비한 것을 초과하여 사용자가 요금청구 받을 위험성을 제거하

기 위하여 수표 상의 일련 번호의 사용에 관한 이전 III장에 제공된다. 바꿔 말하면, 수표의 r리스트가 이 제 4실시예에서 지불을 위하여 선택되면, 관련 선택 확률이 r/m 이라고 가정하여 수표는 본 발명의 제 3실시예에서 수표가 처리되는 방법과 유사하게 개별적으로 처리될 수 있다.

도 7은 다수의 n개의 거래($T_1, T_2, \dots, T_i, \dots, T_n$)에 대한 지불을 설정하기 위한 시스템(300)을 도시하는데, 각 T_i 는 값(TV_i)을 갖는다. 시스템(300)은 사용자, 상인, 은행, 및 제 4당사자 간에 데이터를 전송하기 위한 수단을 포함한다. 이 시스템(300)은 또한 제 1처리 수단(310), 제 2처리 수단(320), 제 3처리 수단(330) 및 제 4처리 수단(340)을 포함한다. 모두 4개의 처리 수단은 전형적으로 데이터를 저장하기 위한 저장 수단(351), 데이터를 입력하기 위한 입력 수단(352), 및 시스템 명령을 구현하는 CPU(353)를 포함한다.

제 1처리 수단(310)은 각 T_i 에 대한 데이터 스트링($C_i(1 \text{ in})$)을 도출, 입력 및 저장하기 위하여 사용자에게 의해 동작된다. 제 2처리 수단(320)은 상인에 의해 동작되고 m개의 리스트($L^k(k=1, \dots, m)$)로 상기 데이터 스트링($C_i(i=1, \dots, n)$)의 그룹을 특정하게 관련시키고 상기 리스트($L^k(k=1, \dots, m)$)를 입력하고 저장하기 위한 $C_i(i=1, \dots, n)$ 의 수신에 응답한다. 각 리스트(L^k)는 데이터 스트링($C^k_1, \dots, C^k_{l_k}$) 및 $\sum_{k=1}^m l_k = n$ 을 포함한다. 제 2처리 수단은 각 L^k 에 대한 커미트먼트(CM^k)를 계산하고 커미트먼트($CM^k(k=1, \dots, m)$)를 저장하기 위하여 상인에 의해 부가 동작된다.

이 제 3처리 수단(330)은 하나 이상의 정수 인덱스들($i_1, i_2, \dots, i_r$)을 선택하고 제 2당사자가 인덱스들($i_1, i_2, \dots, i_r$)을 수신하도록 하기 위하여 커미트먼트(CM^k)의 수신시 은행에 의해 동작되는데, 여기서 모든 r에 대해서 $1 \leq i_r \leq m$ 이다. 제 4처리 수단은 CM을 디커미트하기 위하여 인덱스($i_1, i_2, \dots, i_r$)의 수신시 상인에 의해 동작됨으로써, 은행에 ($L^{i_1}, \dots, L^{i_r}$)을 드러낸다.

시스템(300)은 사용자가 차변 금액(D)만큼 차변되도록 하고 제 4당사자로 하여금 대변 금액(CR)을 수신하도록 하기 위하여 $L^{i_1}, \dots, L^{i_r}$ 의 드러낼시 제 3당사자에 의해 동작되는 수단(370)을 포함한다.

본 발명의 제안된 실시예 각각에서, 셀 전화의 스마트 카드 또는 프로세서와 같은 변조 방지 하드웨어는 보안성을 제공하기 위하여 사용될 수 있다.

즉, 본 발명의 방법 및 시스템은 다음을 특징으로 한다. 1) 지불 선택 프로세스에서 사용자-상인 상호작용에 대한 필요성을 제거한다; 2) 시스템에 시간 제약을 통합시킨다; 3) 사용자에게 과도한 요금청구 위험성을 제거하는 선택적인 예치 프로토콜을 제공한다; 4) 지불 프로세스에 걸쳐서 유연성 및 제어를 은행에 제공하는 연가된 선택 프로토콜을 제공한다.

본 발명이 특히 특정 바람직한 실시예와 관련하여 도시되고 설명되었지만, 당업자는 형태 및 내용면에서 각종 변경을 첨부된 청구범위에 의해 규정된 바와 같은 본 발명의 원리 및 범위로부터 벗어남이 없이 행할 수 있다는 것을 이해하여야 한다.

(청구의 범위)

(청구항 1)

거래(T)에 대한 지불을 설정하는 방법에 있어서,

A. 제 1당사자는 T와 관련된 데이터 스트링(C)을 T로부터 도출하고, 제 2당사자로 하여금 상기 데이터 스트링(C)의 적어도 일부를 수신하도록 하는 단계;

B. 제 2당사자가 아이템(V)을 C의 적어도 일부분과 관련시키는 단계로서, V는 상기 제 1당사자에 의해 실질적으로 예측될 수 없는, 관련시키는 단계;

C. 상기 제 2당사자는 V가 특성(P)을 충족하는지를 결정하고, 충족될 경우 상기 제 2당사자는 V가 상기 특성(P)을 충족하는지를 제 3당사자로 하여금 검증하도록 하는 정보(I)를 상기 제 3당사자로 하여금 수신하도록 하는 단계;

D. 상기 제 3당사자는 I의 수신시, V가 상기 특성(P)을 충족하는지를 검증하는 단계; 및

E. 상기 제 3당사자는 V가 상기 특성(P)을 충족할 경우에만 제 4당사자로 하여금 금액(A)을 수신하도록 하는 단계를 포함하는 지불 설정 방법.

(청구항 2)

제 1항에 있어서, 상기 데이터 스트링(C)의 적어도 일부는 인증되는 지불 설정 방법.

(청구항 3)

제 1항에 있어서, 상기 제 2당사자가 V가 특성 P를 충족하는지를 결정하는 단계는, 상기 제 2당사자 및 상기 제 1당사자 사이의 상호작용을 필요로 하지 않는 지불 설정 방법.

(청구항 4)

제 2항에 있어서, 상기 데이터 스트링의 부분은, 상기 제 1당사자 대신에 제 5당사자에 의해 인증되는 지불 설정 방법.

(청구항 5)

제 1항에 있어서, 상기 제 1당사자가 T로부터 상기 데이터 스트링(C)을 도출하는 단계는, 상기 제 1당사자가 상기 제 1당사자의 비밀 키를 사용하여 T의 적어도 일부에 대한 디지털 서명을 생성하는 단계를 포함하는 지불 설정 방법.

(청구항 6)

제 5항에 있어서, 상기 제 1당사자의 디지털 서명은

(a) 결정론적 서명

(b) 랜덤화된 서명

(c) 오프-라인 서명

(d) 온-라인 서명; 및

(e) 아이덴티티 기반으로 한 서명(identity-based signature) 중 하나 이상을 포함하는 지불 설정 방법.

(청구항 7)

제 1항에 있어서, 상기 제 2당사자가 상기 아이템(V)을 C와 관련시키는 단계는, 상기 제 2당사자가 자신의 비밀 키를 사용하여 C의 적어도 일부에 대한 디지털 서명을 생성하는 단계를 포함하는 지불 설정 방법.

(청구항 8)

제 7항에 있어서, 상기 제 2당사자의 디지털 서명은 결정론적 서명인 지불 설정 방법.

(청구항 9)

제 1항에 있어서, 상기 데이터 스트링(C)은 상기 제 1당사자의 비밀 키를 사용하여 계산되는 상기 거래(T)의 적어도 일부에 대한 디지털 서명;

상기 제 1당사자의 비밀 키를 사용하여 계산되는 메시지 인증 코드; 및

iii) 전자 수표 중 하나 이상을 포함하는 지불 설정 방법.

(청구항 10)

제 1항에 있어서, 상기 아이템(V)은:

- a) 상기 제 2당사자의 비밀 키를 사용하여 계산되는 C에 대한 디지털 서명; 및
- b) 상기 제 2당사자에 공지된 비밀 키를 사용하여 계산된 메시지 인증 코드 값 중 하나 이상을 포함하는 지불 설정 방법.

(청구항 11)

제 1항에 있어서, 상기 제 2당사자는 상기 제 3당사자로 하여금 상기 정보 I를 수신하도록 하는 단계는:

- a) 상기 제 2당사자가 상기 제 3당사자에게 I를 전송하는 단계;
- b) 상기 제 2당사자는 제 5당사자가 상기 제 3당사자에게 I를 전송하도록 요청하는 단계; 및
- c) 상기 제 2당사자가 파일에 I를 게시하는 단계 및 상기 제 3당사자가 상기 파일로부터 I를 검색하는 단계 중 하나 이상을 포함하는 지불 설정 방법.

(청구항 12)

제 1항에 있어서, 상기 제 2당사자가 C를 수신한 후 C의 인증성 및 무결성을 점검하는 단계를 더 포함하는 지불 설정 방법.

(청구항 13)

제 12항에 있어서, 상기 제 2당사자가 상기 제 1당사자에 관련된 공개 검증 정보를 사용하여 C의 인증성 및 무결성을 점검하는 지불 설정 방법.

(청구항 14)

제 13항에 있어서, 상기 공개 검증 정보는, 공개 키 디지털 서명 방식에서 상기 제 1당사자의 비밀 키에 대응하는 상기 제 1당사자의 공개 키를 포함하는 지불 설정 방법.

(청구항 15)

제 13항에 있어서, 상기 제 2당사자가 상기 공개 검증 정보를 사용하는 단계는:

- (a) 상기 제 2당사자가 상기 제 1당사자로부터 상기 공개 검증 정보를 획득하는 단계;
- (b) 상기 제 2당사자가 상기 데이터 스트림(C)과 관련하여 상기 제 1당사자에 의해 전송되는 정보로부터 상기 공개 검증 정보를 획득하는 단계;
- (c) 상기 제 2당사자가 디지털 인증서로부터 상기 공개 검증 정보를 획득하는 단계; 및
- (d) 상기 제 2당사자가 공개적으로 이용 가능한 상기 제 1당사자에 관한 정보로부터 상기 공개 검증 정보를 획득하는 단계 중 하나 이상을 포함하는 지불 설정 방법.

(청구항 16)

제 1항에 있어서, 상기 제 2당사자 및 상기 제 4당사자는 동일한 지불 설정 방법.

(청구항 17)

제 1항에 있어서, 상기 제 2당사자 및 상기 제 3당사자는 동일한 지불 설정 방법.

(청구항 18)

제 1항에 있어서, V 는 $F(V) < s$ 인 경우에만 P 를 충족하고,

여기서 F 는 함수이며,

s 는 상수인 지불 설정 방법.

(청구항 19)

제 18항에 있어서, $0 < s < 1$ 인 지불 설정 방법.

(청구항 20)

제 18항에 있어서, F 는 입력으로서 임의의 비트 스트링을 취하고 출력으로서 0보다 크고 1보다 작은 수를 리턴시키는 공개 함수인 지불 설정 방법.

(청구항 21)

제 1항에 있어서, 상기 거래(T)는 부분적으로 거래 값(T_v)에 의해 특정 지워지는 지불 설정 방법.

(청구항 22)

제 21항에 있어서, 상기 제 4당사자에 의해 수신되는 금액은 T_v 보다 큰 지불 설정 방법.

(청구항 23)

제 20항에 있어서, 상기 거래(T)는 부분적으로 거래 값(T_v)에 의해 특정 지워지고 상기 제 4당사자에 의해 수신되는 상기 금액은 $(T_v * 1/s)$ 와 동일한 지불 설정 방법.

(청구항 24)

제 1항에 있어서,

(a) 상기 아이템(V)은 상기 데이터 스트링(C)에 관한 상기 제 2당사자의 디지털 서명을 포함하고;

(b) V 는 $F(V)$ 가 s 보다 작으면 상기 특성(P)을 충족하고, 여기서 F 는 비트 스트링 상에서 동작하고 출력으로서 0 및 1 사이의 수를 리턴시키는 공개 함수를 나타내는 지불 설정 방법.

(청구항 25)

제 1항에 있어서, 상기 데이터 스트링(C)은 T 에 관한 정보를 포함하고, 상기 정보는:

a) 상기 제 1당사자의 아이덴티티;

b) 상기 거래의 시간; 및

c) 상기 거래일 중 하나 이상을 포함하는 지불 설정 방법.

(청구항 26)

거래 값(T_v)을 갖는 거래(T)를 위하여 사용자(U)가 상인(M)에게 지불을 설정하는 방법에 있어서,

- A. 상기 사용자는 제 1디지털 서명 방식에 대한 공개 키 및 대응하는 비밀 키를 설정하고, C 를 포함하는 전자 수표를 생성하기 위하여 데이터 스트링 $C = \text{SIG}_U(T)$ 를 T 로부터 도출하는 단계로서, $\text{SIG}_U(T)$ 는 상기 제 1디지털 서명 방식에서 상기 거래(T)에 대한 사용자(U)의 디지털 서명을 나타내는, 설정 및 도출 단계;
- B. 상기 사용자는 상기 상인으로 하여금 상기 데이터 스트링(C)을 수신하도록 하는 단계;
- C. 상기 상인은 제 2디지털 서명 방식에 대해서 공개 키 및 대응하는 비밀 키를 설정하고, 상기 데이터 스트링(C)을 아이템 $V = \text{SIG}_M(C)$ 와 관련시키는 단계로서, $\text{SIG}_M(C)$ 는 상기 제 2디지털 서명 방식에서 상기 데이터 스트링(C)에 대한 상인(M)의 디지털 서명을 나타내는, 설정 및 관련시키는 단계;
- D. 상기 상인은 상기 값 $F(V) = F(\text{SIG}_M(C))$ 를 계산하는 단계로서, F 는 0 및 1사이의 수를 출력하도록 비트 스트링 상에서 동작하는 공개 함수를 나타내는, 계산 단계;
- E. 상기 상인은 $F(\text{SIG}_M(C))$ 를 상수와 비교하여 $F(V) < s$ 인지를 결정하도록 하고 만일 그렇다면, 은행으로 하여금 상기 상인의 상기 공개 키를 획득하도록 하는 단계;
- F. 상기 은행은 상기 상인의 공개 키를 사용하여 $F(\text{SIG}_M(C)) < s$ 인지를 검증하는 단계; 및
- G. $F(\text{SIG}_M(C)) < s$ 인 경우에만, 상기 은행은 상기 상인으로 하여금 금액 $A = [T_v * 1/s]$ 을 수신하도록 하는 단계를 포함하며,

여기서, s 는 0보다 크고 1보다 작은 상수이고, 전자 수표가 상기 은행에 제공하도록 선택될 확률을 나타내는 거래 값(T_v)을 갖는 거래(T)를 위하여 지불 설정 방법.

(청구항 27)

거래 T 에 대한 지불을 설정하는 시스템에 있어서,

- A. 제 1당사자, 제 2당사자, 제 3당사자, 및 제 4당사자 간에 데이터를 전송하는 통신 수단;
- B. T 와 관련된 데이터 스트링(C)을 도출, 입력, 및 저장하기 위하여 제 1당사자에 의해 동작되는 제 1처리 수단;
- C. 아이템(V)을 C 의 적어도 일부와 관련시키고 V 가 특성(P)을 충족하는지를 결정하기 위하여 상기 제 2당사자에 의해 동작되고 C 에 응답하는 제 2처리 수단으로서, V 는 상기 제 1당사자에 의해 실질적으로 예측될 수 없는 제 2처리 수단;
- D. V 가 P 를 충족할 때 상기 제 2당사자에 의해 선택적으로 동작되어, V 가 P 를 충족하는지를 상기 제 3당사자가 검증할 수 있도록 하는 정보 I 를 제 3당사자로 하여금 수신하도록 하는 수단; 및
- E. V 가 P 를 충족할 때 상기 제 3당사자에 의해 선택적으로 동작되어 제 4당사자로 하여금 금액(A)을 수신하도록 하는 수단을 포함하는 지불 설정 시스템.

(청구항 28)

거래(T)에 대한 지불을 설정하는 방법에 있어서,

- A. 제 1당사자가 데이터 스트링(C)의 적어도 일부를 제 2당사자로부터 수신하는 단계로서, 상기 데이터 스트링(C)은 T 와 관련되는, 수신 단계;

B. 상기 제 1당사자가 아이템(V)을 C의 적어도 일부와 관련시키는 단계로서, V는 상기 제 2당사자에 의해 실질적으로 예측될 수 없는, 관련시키는 단계; 및

C. 상기 제 1당사자는 V가 특성(P)을 충족하는지를 결정하고, 충족하는 경우에만, 상기 제 1당사자는 V가 상기 특성(P)을 충족하는지를 제 3당사자가 검증할 수 있도록 하는 정보(I)를 상기 제 3당사자가 수신하도록 함으로써, V가 P를 충족한다고 검증시, 상기 제 3당사자는 제 4당사자가 금액(A)을 수신할 수 있도록 하는 단계를 포함하는 지불 설정 방법.

(청구항 29)

거래(T)에 대한 지불을 설정하는 방법에 있어서,

A. 아이템(V)이 특성(P)을 충족하는지를 제 1당사자가 검증할 수 있도록 하는 정보(I)를 상기 제 1당사자가 제 2당사자로부터 수신하는 단계로서;

상기 아이템(V)은 제 3당사자에 의해 T로부터 도출되는 데이터 스트링(C)의 적어도 일부와 관련되며,

V는 상기 제 3당사자에 의해 실질적으로 예측될 수 없는, 수신 단계;

B. 상기 제 1당사자가 I의 수신시, V가 상기 특성(P)을 충족하는지를 검증하는 단계; 및

C. 상기 제 1당사자는 V가 상기 특성(P)을 충족하는 경우에만 제 4당사자로 하여금 금액(A)을 수신하도록 하는 단계를 포함하는 지불 설정 방법.

(청구항 30)

부분적으로 시간(T)에 의해 특징 지워지는 거래(T)에 대한 지불을 설정하는 방법에 있어서,

A. 제 1당사자는 T와 관련된 데이터 스트링(C)을 T로부터 도출하는 단계로서, C는 상기 t에 관한 정보(IN)를 포함하는, 도출 단계;

B. 상기 제 1당사자는 제 2당사자가 상기 데이터 스트링(C)의 적어도 일부를 수신하도록 하며, 상기 C의 적어도 일부는 정보(IN)를 포함하는, 수신 단계;

C. 상기 제 2당사자는 아이템(V)을 C의 적어도 일부와 관련시키는 단계로서, V는 상기 제 1당사자에 의해 실질적으로 예측될 수 없는, 관련시키는 단계;

D. 상기 제 2당사자는 V가 특성(P)을 충족하는지를 결정하고, 충족될 경우 시간 t'에서 상기 제 2당사자는 V가 상기 특성(P)을 충족하는지를 상기 제 3당사자로 하여금 검증할 수 있도록 하는 정보(IN) 및 정보(I)를 상기 제 3당사자로 하여금 수신하도록 하는 단계; 및

E. 상기 제 3당사자는 I의 수신시, V가 상기 특성(P)을 만족하는지를 검증하고,

F. 상기 제 3당사자는

a) V가 상기 특성(P)을 충족하고,

b) $|t'-t|$ 은 소정의 시간 간격보다 작은 경우에만 제 4당사자로 하여금 금액(A)을 수신하도록 하는 단계를 포함하는 지불 설정 방법.

(청구항 31)

제 30항에 있어서, 상기 소정 시간 간격 $|t'-t|$ 은 n일이며, n은 약 1 내지 약 7의 0이 아닌 정수인 지불 설정 방법.

(청구항 32)

제 30항에 있어서, 상기 소정 시간 간격 $|t'-t|$ 은 적어도 m 시간이며, m 은 약 1 내지 약 24시간의 0이 아닌 정수인 지불 설정 방법.

(청구항 33)

제 30항에 있어서, 단계 B에서 상기 제 1당사자는 상기 제 2당사자가 시간 $t_1 > t$ 에서 C의 상기 부분을 수신하도록 하고,

상기 제 2당사자는 $|t_1 - t|$ 가 소정 금액보다 적지 않은 한 T에 대한 지불로서 C를 수용하는 것을 거부하는 지불 설정 방법.

(청구항 34)

제 30항에 있어서,

상기 데이터 스트링(C)은 제 1당사자의 비밀 키를 사용하여 생성된 T의 적어도 일부에 대한 디지털 서명을 포함하는 지불 설정 방법.

(청구항 35)

제 30항에 있어서, V가 C의 적어도 일부에 정합하는 경우에만 V는 P를 충족하는 지불 설정 방법.

(청구항 36)

제 30항에 있어서, 상기 특성(P)은 C에 따르는 것이 아니라 V에 따른 지불 설정 방법.

(청구항 37)

제 30항에 있어서, V는 $F(V) < s$ 인 경우에만 P를 충족하고,

여기서 F는 함수이며,

s는 상수이고 $0 < s < 1$ 인 지불 설정 방법.

(청구항 38)

제 37항에 있어서, 상기 함수(F)의 값($F(V)$)은 상기 제 1당사자에 의해 실질적으로 예측될 수 없는 지불 설정 방법.

(청구항 39)

제 37항에 있어서, 상기 함수(F) 및 상기 상수(s) 중 적어도 하나는 C에서 규정되는 지불 설정 방법.

(청구항 40)

제 37항에 있어서, F는:

(a) 고정된 공개 함수;

(b) 입력으로서 임의의 비트 스트링을 취하고 출력으로서 0보다 크고 1보다 작은 수를 리턴시키는 공개 함수 중 하나인 지불 설정 방법.

(청구항 41)

제 30항에 있어서, V 는 제 2당사자의 비밀 키를 사용하여 계산되고 $SIG_M(C)$ 로서 표시되는 C 에 대한 디지털 서명을 포함하는 지불 설정 방법.

(청구항 42)

제 30항에 있어서, 제 4당사자가 금액(A)을 수신하는 단계 후, 상기 제 3당사자는 상기 제 1당사자로 하여금 상기 제 2당사자에 의해 제공되는 하나 이상의 거래($TS_i(i=1, \dots, n)$)에 자유 가입을 수신하도록 하는 단계를 더 포함하고, 모든 i ($i=1, \dots, n$)에 대해서 상기 거래(TS_i)는 부분적으로 시간(ts_i)에 의해 특징 지워지고 $|ts_i - t|$ 는 소정 금액보다 작은 지불 설정 방법.

(청구항 43)

제 30항에 있어서, 상기 아이템(V)은 :

- a) T 에 관련하고 C 에 포함되는 날짜 정보;
- b) C 에 포함되는 일련 번호;
- c) C 에 포함되는 스트링;
- d) C 의 랜덤 스트링 파트; 및
- e) C 에 따른 양 중 적어도 하나에 대한 디지털 서명을 포함하며,

여기서 V 는 제 2당사자의 비밀 키를 사용하여 계산되고 SIG_M 으로서 표시될 수 있는 지불 설정 방법.

(청구항 44)

제 30항에 있어서, 상기 아이템(V)은 $G(C)$ 의 디지털 서명을 포함하고, G 는 함수 및 알고리즘 중 적어도 하나를 표시하는 지불 설정 방법.

(청구항 45)

제 44항에 있어서, V 는 $F(V)=F(SIG_M(G(C)))<s$ 인 경우에만 P 를 충족하고,

여기서 F 는 함수를 표시하며,

s 는 상수 및 $0 < s < 1$ 을 표시하고,

상기 값 $F(V)$ 는 상기 제 1당사자에 의해 실질적으로 예측될 수 없는 지불 설정 방법.

(청구항 46)

제 44항에 있어서, $G(C)$ 는 T 및 C 중 적어도 하나 내에서 특정되는 지불 설정 방법.

(청구항 47)

제 44항에 있어서, $G(C)$ 는:

- (a) T의 서브스트링;
- (b) 상기 거래(T)의 상기 시간(t)에 관한 정보 F;
- (c) 상기 거래(T)가 발생하는 날짜에 관한 정보; 및
- (d) 상기 제 1당사자에 의해 선택되는 스트링(W) 중 하나 이상을 포함하는 지불 설정 방법.

(청구항 48)

제 47항에 있어서, 상기 스트링(W)은 T에 특정되고 랜덤하게 선택되는 지불 설정 방법.

(청구항 49)

제 47항에 있어서, $V = \text{SIG}_M(G(C))$ 는 C의 적어도 일부를 수신하기 전, 상기 제 2당사자에 의해 계산되도록 적응되는 지불 설정 방법.

(청구항 50)

제 44항에 있어서, $V = \text{SIG}_M(G(C))$ 의 적어도 일부 비트가 C의 적어도 일부 비트에 정합하면 상기 특성(P)이 충족되는 지불 설정 방법.

(청구항 51)

제 44항에 있어서, $V = \text{SIG}_M(G(C))$ 내의 선택된 m-비트 스트링이 C의 선택된 m-비트 스트링에 정합하면 상기 특성 P가 충족되며, 여기서 m은 소정의 양의 정수인 지불 설정 방법.

(청구항 52)

제 51항에 있어서, m은 약 10인 지불 설정 방법.

(청구항 53)

거래(T)에 대한 지불을 설정하는 방법에 있어서,

A. 제 1당사자는 T로부터 T와 관련된 데이터 스트링(C)을 도출하고,

제 2당사자가 상기 데이터 스트링(C)의 적어도 일부를 수신하도록 하는 단계;

B. 제 2당사자가 특성(P)이 C의 적어도 일부 및 C에 따르고 상기 제 1당사자에 의해 실질적으로 예측될 수 없는 양(Q) 사이에 유지되는지를 결정하고, 유지될 경우 상기 제 2당사자는 상기 특성(P)이 충족되는지를 제 3당사자로 하여금 검증할 수 있도록 하는 정보(I)를 상기 제 3당사자로 하여금 수신하도록 하는 단계;

C. 상기 제 3당사자는 I의 수신시, 상기 특성(P)이 충족되는지를 검증하는 단계; 및

D. 상기 특성(P)이 상기 C의 적어도 일부 및 Q 사이에 유지된다고 검증시에만, 상기 제 3당사자는 제 4당사자로 하여금 금액(A)을 수신하도록 하는 단계를 포함하는 지불 설정 방법.

(청구항 54)

제 53항에 있어서, 상기 양(Q)은 $G(C)$ 로서 표시될 수 있고, G는 함수 및 알고리즘 중 적어도 하나인 지불 설정 방법.

(청구항 55)

제 54항에 있어서, $G(C)$ 는:

- a) 상기 거래(T)가 발생하는 시간(t), 및
- b) 상기 거래(T)가 발생하는 날짜(d) 중 적어도 하나에 관한 정보를 포함하는 지불 설정 방법.

(청구항 56)

제 55항에 있어서, C 의 적어도 일부 비트는 $SIG_M(G(C))$ 의 적어도 일부 비트와 동일한 경우에만 상기 특성(P)이 유지되고, 여기서 $SIG_M(G(C))$ 는 상기 제 2당사자의 비밀 키를 사용하여 생성되는 $G(C)$ 에 대한 디지털 서명을 나타내는 지불 설정 방법.

(청구항 57)

시간(t)에 의해 부분적으로 특징 지워지는 거래(T)에 대한 지불을 설정하는 방법에 있어서,

- A. 제 1당사자는 T 와 관련되는 데이터 스트링(C)을 T 로부터 도출하는 단계
- B. 제 2당사자가 시간(t_i)($i=1, \dots, n$)의 순서와 관련된 값(VL_i)의 순서를 도출하는 단계로서, 1보다 크고 n 보다 작은 하나 이상의 정수 m 에 대해서, $|t - t_m|$ 은 소정 금액보다 작은, 도출 단계;
- C. 상기 제 1당사자는 상기 제 2당사자로 하여금 상기 데이터 스트링(C)의 적어도 일부를 수신하도록 하는 단계로서, 상기 부분은 상기 거래(T)의 시간(t)에 관한 정보를 포함하는, 수신 단계;
- D. 상기 제 2당사자는 특성(P)이 상기 C 의 부분과 t_m 과 관련된 상기 값(VL_m) 및 VL_m 에 따른 양(Q) 중 하나와의 사이에 유지되는지를 결정하는 단계;
- E. P 가 유지되면, 상기 제 2당사자는 상기 특성(P)이 충족되는지를 상기 제 3당사자로 하여금 검증할 수 있도록 하는 정보(I)를 제 3당사자로 하여금 수신하도록 하는 단계;
- F. 상기 제 3당사자는 I 의 수신시, Q 가 P 를 충족하는지를 검증하는 단계; 및
- G. 상기 제 3당사자는 Q 가 상기 특성(P)을 충족하는 경우에만, 제 4당사자로 하여금 금액(A)을 수신하도록 하는 단계를 포함하는 지불 설정 방법.

(청구항 58)

제 57항에 있어서, 상기 양(Q)은 $Q = F(SIG_M(V_m))$ 으로 제공되고, 여기서 F 는 함수를 표시하고 $SIG_M(V_m)$ 은 상기 제 2당사자의 비밀 키를 사용하여 생성된 V_m 의 디지털 서명을 표시하는 지불 설정 방법.

(청구항 59)

부분적으로 거래(t)에 의해 특징 지워지는 거래(T)에 대한 지불을 설정하는 방법에 있어서,

- A. 제 1당사자는 T 로부터 T 와 관련된 데이터 스트링(C)을 도출하는 단계로서, C 는 t 에 관한 정보를 포함하는, 도출 단계;
- B. 제 2당사자는 시간 단위(t_i)($i=1, \dots, n$)의 순서와 관련된 값(V_i)의 순서를 도출하는 단계로서;

여기서 인접 시간 단위(t_{i+1} 및 t_i)의 각 쌍은 시간 간격 $\Delta t_i = t_{i+1} - t_i$ 을 규정하고,

1보다 크고 n보다 작은 적어도 정수 m에 대해서, 상기 시간(t)은 시간 간격(Δt_m) 내에 있는, 도출 단계;

C. 상기 시간 간격(Δt_m)의 시작에서, 상기 제 2당사자는 V_m 과 관련된 값(Q_m)을 도출하는 단계로서, Q_m 은 상기 제 1당사자에 의해 실질적으로 예측될 수 없는, 도출 단계;

D. 상기 시간 간격(Δt_m) 동안,

a) 상기 제 1당사자는 상기 제 2당사자로 하여금 C의 적어도 일부를 수신하도록 하는 단계;

b) 상기 제 2당사자는 C의 상기 부분과 Q_m 사이에 유지되는지를 결정하고, 유지될 경우 상기 제 2당사자는 상기 특성(P)이 충족되는지를 제 3당사자가 검증할 수 있도록 하는 정보(I)를 상기 제 3당사자로 하여금 수신하도록 하는 단계;

E. 상기 제 3당사자는 I의 수신시, Q가 P를 충족하는지를 검증하는 단계; 및

F. 상기 제 3당사자는 Q가 상기 특성(P)을 충족하는 경우에만, 제 4당사자로 하여금 금액(A)을 수신하도록 하는 단계를 포함하는 지불 설정 방법.

(청구항 60)

제 59항에 있어서, 단계C는 단계 B 전에 발생되고, Q의 적어도 일부 비트가 C의 적어도 일부 비트에 정합하는 경우에만 상기 특성(P)은 충족되는 지불 설정 방법.

(청구항 61)

제 59항에 있어서, Q_i 는 $Q_i = F(\text{SIG}_M(V_i))$ 로 제공되고, 여기서 F는 함수를 표시하며, $\text{SIG}_M(V_i)$ 는 상기 제 2당사자의 비밀 키를 사용하여 생성되는 V_i 의 디지털 서명을 표시하는 지불 설정 방법.

(청구항 62)

제 59항에 있어서, 모든 $i=1, \dots, n$ 에 대해서, 시간 간격 $\Delta t_i = |t_{i+1} - t_i|$ 는 소정 시간 간격인 지불 설정 방법.

(청구항 63)

제 62항에 있어서, 상기 소정의 상수는 1일인 지불 설정 방법.

(청구항 64)

부분적으로 시간(t)에 의해 특징 지워지는 거래(T)에 대한 지불을 설정하는 방법에 있어서,

A. 제 1당사자는 T로부터 T와 관련된 데이터 스트링(C)을 도출하는 단계로서, C는 t에 관한 정보(F)를 포함하는, 도출 단계;

B. 제 2당사자는 시간 값($t_i(i=1, \dots, n)$)의 순서와 관련된 값($x_i(i=0, 1, \dots, n)$)의 순서를 도출하고 x_0 를 공개시키는 단계로서;

여기서 $i=0, 1, \dots, n-1$ 에 대해 $X_i = H(X_{i+1})$ 이고, Hsms 일방향 해쉬 함수이고;

인접 시간 값(t_{i+1} 및 t_i)의 각 쌍은 시간 간격 $\Delta t_i = t_{i+1} - t_i$ 을 규정하고;

1보다 크고 n보다 작은 적어도 정수 m에 대해서, 상기 시간(t)은 시간 간격(Δt_m)인, 도출 및 공개시키는 단계;

C. 상기 시간 간격(Δt_m) 동안, 상기 제 1당사자는 상기 제 2당사자로 하여금 C의 적어도 일부를 수신하도록 하는 단계로서, 상기 부분은 F를 포함하는, 수신하도록 하는 단계;

D. 상기 시간 간격(Δt_m) 동안, 상기 제 2당사자는 특성(P)이 Q_m 과 C의 상기 부분 사이에 유지되는지를 결정하고, 유지될 경우 상기 제 2당사자는 상기 특성(P)이 충족되는지를 제 3당사자로 하여금 검증하도록 하는 정보(I)를 상기 제 3당사자로 하여금 수신하도록 하는 단계;

E. 상기 제 3당사자는 I의 수신시, Q_m 이 P를 충족하는지를 검증하는 단계; 및

F. 상기 제 3당사자는 Q가 상기 특성(P)을 충족하는 경우에만, 제 4당사자로 하여금 금액(A)을 수신하도록 하는 단계를 포함하는 지불 설정 방법.

(청구항 65)

제 64항에 있어서, 상기 제 2당사자가 x_0 를 공개하는 단계는:

a) 공개 파일에 x_0 를 배치하는 단계; 및

b) 상기 제 2당사자의 비밀 키를 사용하여 x_0 를 디지털적으로 서명하고, 대응하는 공개 키를 공개 디렉토리에 배치하는 단계 중 하나 이상을 포함하는 지불 설정 방법.

(청구항 66)

제 64항에 있어서, 상기 시간 간격 $\Delta t_i = t_{i+1} - t_i$ 은 모든 $i=1, \dots, n$ 에 대한 소정의 상수인 지불 설정 방법.

(청구항 67)

부분적으로 시간(t)에 의해 특징 지워지는 거래(T)에 대한 지불을 설정하는 시스템에 있어서,

A. 제 1당사자, 제 2당사자, 제 3당사자 및 제 4당사자 간에 데이터를 전송하는 통신 수단;

B. T와 관련된 데이터 스트링(C)을 도출, 입력 및 저장하기 위하여 제 1당사자에 의해 동작되는 제 1처리 수단으로서, C는 시간(t)에 관한 정보(F)를 포함하는, 제 1처리 수단;

C. 아이템(V)을 C의 적어도 일부분과 관련시키고 V가 특성(P)을 충족하는지를 결정하기 위하여, 제 2당사자에 의해 동작되고 C에 응답하는 제 2처리 수단으로서, V는 상기 제 1당사자에 의해 실질적으로 예측될 수 없는, 제 2처리 수단;

D. V가 P를 충족할 때 상기 제 2당사자에 의해 선택적으로 동작되어, a) V가 P를 충족하는지 및 b) $|t' - t|$ 가 소정 금액보다 작은지를 제 3당사자가 검증할 수 있도록 하는 F 및 정보(I)를 상기 제 3당사자로 하여금 수신하도록 하는 수단; 및

E. V가 P를 충족할 때 상기 제 3당사자에 의해 선택적으로 동작되고 $|t' - t|$ 는 소정 금액보다 작게 되어 제 4당사자로 하여금 금액(A)을 수신하도록 하는 수단을 포함하는 지불 설정 시스템.

(청구항 68)

부분적으로 시간(t)에 의해 특징 지워지는 거래(T)에 대한 지불을 설정하는 방법에 있어서,

A. 아이템(V)이 특성(P)을 충족하는지를 상기 제 1당사자가 검증할 수 있도록 하는 정보(I)를 제 1당사자가 시간(t')에서 제 2당사자로부터 수신하는 단계로서, 상기 아이템(V)은 제 3당사자에 의해 T로부터 도출되고 t에 관한 정보를 포함하는 데이터 스트링(C)의 적어도 일부와 관련되고 V는 상기 제 3당사자에 의해 실질적으로 예측될 수 없는, 수신 단계;

B. 상기 제 1당사자가 I의 수신시, V가 상기 특성(P)을 충족하는지를 검증하는 단계; 및

C. 상기 제 1당사자는:

a) V가 상기 특성(P)을 충족하고,

b) $|t'-t|$ 가 소정 금액보다 작은 경우에만, 제 4당사자로 하여금 금액(A)을 수신하도록 하는 단계를 포함하는 지불 설정 방법.

(청구항 69)

부분적으로 시간(t)에 의해 특정 지워지는 거래(T)에 대한 지불을 설정하는 방법에 있어서,

A. 제 1당사자가 데이터 스트링(C)의 적어도 일부를 제 2당사자로부터 수신하는 단계로서, 상기 데이터 스트링(C)은 T와 관련되고, 상기 C의 일부는 t에 대한 정보를 포함하는, 수신 단계;

B. 상기 제 1당사자가 상기 C의 적어도 일부를 아이템(V)과 관련시키는 단계로서, V는 상기 제 2당사자에 의해 실질적으로 예측 불가능한, 관련시키는 단계; 및

C. 상기 제 1당사자는 V가 특성(P)을 충족하는지를 결정하고, 충족될 경우 시간(t')에서 상기 제 1당사자는 V가 특성(P)을 충족하는지를 상기 제 3당사자가 검증할 수 있도록 하는 정보(I)를 제 3당사자로 하여금 수신하도록 함으로써,

a) V가 P를 충족하고

b) $|t'-t|$ 가 소정 금액보다 적으면,

제 4당사자가 금액(A)을 수신할 수 있도록 하는 단계를 포함하는 지불 설정 방법.

(청구항 70)

1과 n 사이의 인덱스(i)가 부분적으로 거래 값(TV_i)에 의해 각각 특정 지워지는 각각의 T_i 와 관련될 수 있는 다수의 n개의 거래($T_1, T_2, \dots, T_i, \dots, T_n$)에 대해 지불을 설정하는 방법에 있어서,

A. 제 1당사자는 각각의 거래(T_i)에 대해 수표(C_i)를 생성하기 위하여 확률적 지불 방식을 사용하고 제 2당사자로 하여금 상기 C_i 를 수신하도록 하는 단계로서, C_i 는 상기 인덱스(i)의 표시를 포함하는, 사용 및 수신 단계;

B. 상기 제 2당사자는 어느 수표(C_j)가 지불 가능하도록 선택될지를 제 1당사자가 미리 예측하지 못하도록 하는 방식으로 지불 가능한 수표(C_j)($1 \leq j \leq n$)를 선택하는 단계;

C. 상기 제 2당사자는 선택된 수표(C_j)가 지불 가능한지를 제 3당사자가 검증할 수 있도록 하는 정보(I_j)를 제 3당사자로 하여금 수신하도록 하는 단계;

D. 상기 제 3당사자가 I_j 의 수신에 응답하여, 선택된 수표(C_j)가 지불 가능한지를 검증하는 단계; 및

E. C_j 가 지불 가능한 경우에만, 제 5당사자는 제 4당사자가 대변 금액(CR_j)을 수신하도록 하고, 상기 제 1당사자가 차변 금액(D_j) 만큼 차변받도록 하여, 모든 1과 n 사이의 인덱스(j), 및 지불 가능한 수표의 임의의 선택에 대하여, $D=D_1+D_2+\dots+D_j$ 가 $TV_{agg}=TV_1+TV_2+\dots+TV_j$ 보다 크지 않게 되도록 하는 단계를 포함하는 지불 설정 방법.

(청구항 71)

제 70항에 있어서, 각각의 차변 금액(D_j)은 1과 n 사이의 모든 인덱스(j)에 대하여, 적어도 부분적으로 TV_j 및 C_j 중 하나에 의해 결정되는 지불 설정 방법.

(청구항 72)

제 70항에 있어서, 각각의 차변 금액(D_j)은 T_j 와 관련된 상기 인덱스(j)에 따르는 지불 설정 방법.

(청구항 73)

제 72항에 있어서, 각각의 차변 금액(D_j)은 이전의 차변 금액(D_k)($1 \leq k \leq j \leq n$), 및 차변 금액(D_l)이 차변되었던 이전의 인덱스(l)($1 \leq l \leq j \leq n$) 중 적어도 하나에 따르는 지불 설정 방법.

(청구항 74)

제 70항에 있어서, 지불을 위해 선택되는 각각의 수표(C_j)에 대하여, 상기 제 5당사자가 인덱스(j)의 표시가 저장되도록 하는 단계를 더 포함하는 지불 설정 방법.

(청구항 75)

제 74항에 있어서, 지불 가능한 수표(C_j)의 각 차변 금액(D_j)은 지불 가능한 것으로 발견된 임의의 이전 수표 중 최종 저장된 인덱스(k)에 따르는 지불 설정 방법.

(청구항 76)

제 70항에 있어서, 상기 제 2당사자가 상기 제 3당사자로 하여금 정보(I_j)를 수신하도록 하는 상기 단계는:

- a) 상기 제 2당사자가 상기 제 3당사자에게 I_j 를 전송하는 단계;
- b) 상기 제 2당사자가, 제 3당사자에게 I_j 를 전송할 것을 제 5당사자에게 요청하는 단계; 및
- c) 상기 제 2당사자가 파일에 I_j 를 포스팅하고, 제 3당사자가 상기 파일로부터 I_j 를 회수하는 단계 중 하나 이상을 포함하는 지불 설정 방법.

(청구항 77)

1과 n 사이의 인덱스(i)가 부분적으로 거래 값(TV_i)에 의해 각각 특징 지워지는 각각의 T_i 와 관련될 수 있는 다수의 n개의 거래($T_1, T_2, \dots, T_i, \dots, T_n$)에 대해 지불을 설정하는 방법에 있어서,

A. 제 1당사자가 각각의 거래(T_i)로부터 T_i 와 관련된 데이터 스트링(C_i)을 도출하고, 제 2당사자로 하여금 상기 데이터 스트링을 수신하도록 하는 단계(C_i);

B. 상기 제 2당사자가 아이템(V_i)을 각각의 데이터 스트링(C_i)과 관련시키는 단계로서, V_i 는 상기 제 1사용자에 의해 실질적으로 예측될 수 없는, 관련시키는 단계;

C. 상기 제 2당사자는 V_i 가 특성(P_i)을 충족하는지를 결정하여, 만일 충족한다면, 상기 제 2당사자가 V_i 가 상기 특성(P_i)을 충족하는지를 상기 제 3당사자가 검증할 수 있도록 하는 정보(I_i)를 제 3당사자로 하여금 수신하도록 하는 단계;

D. 상기 제 3당사자는 I_i 의 수신에 응답하여, V_i 가 상기 특성(P_i)을 충족하는지를 검증하는 단계; 및

E. V_i 가 상기 특성(P_i)을 충족하는 경우에만, 제 5당사자는 제 4당사자가 대변 금액(CR_j)을 수신하도록 하고, 상기 제 1당사자가 차변 금액(D_j) 만큼 차변받도록 하는 단계를 포함하고,

상기 차변 금액(D_j)은 상기 대변 금액(CR_j)보다 적거나 이와 동일한 지불 설정 방법.

(청구항 78)

제 77항에 있어서, 1과 n 사이의 모든 인덱스(i)에 대하여, $D_1 + D_2 + \dots + D_i$ 이 $TV_1 + TV_2 + \dots + TV_i$ 보다 적거나 이와 동일한 지불 설정 방법.

(청구항 79)

제 77항에 있어서, 각각의 차변 금액(D_i)은 1과 n 사이의 모든 인덱스(i)에 대하여, 적어도 부분적으로 TV_i 및 C_i 중 하나에 의해 결정되는 지불 설정 방법.

(청구항 80)

제 77항에 있어서, 각각의 데이터 스트링(C_i)은 T_i 와 관련된 상기 인덱스(i)의 표시를 포함하는 지불 설정 방법.

(청구항 81)

제 80항에 있어서, 각각의 차변 금액(D_i)은 T_i 와 관련된 상기 인덱스(i)에 따르는 지불 설정 방법.

(청구항 82)

제 81항에 있어서, 각각의 차변 금액(D_i)은 또한 이전의 차변 금액(D_j), 및 차변 금액(D_k)이 차변되었던 이전의 인덱스(k) 중 적어도 하나에 따르는 지불 설정 방법.

(청구항 83)

제 82항에 있어서, 1과 n 사이의 모든 인덱스(i)에 대하여, $D_1 + D_2 + \dots + D_i$ 이 $TV_1 + TV_2 + \dots + TV_i$ 보다 적거나 이와 동일한 지불 설정 방법.

(청구항 84)

제 77항에 있어서, 상기 제 5당사자가 V_i 가 P_i 를 충족할 때마다 각 데이터 스트링(C_i)에 대해 정보(SN_i)가 저장되도록 하는 단계를 더 포함하는 지불 설정 방법.

(청구항 85)

제 84항에 있어서, SN_i 는 상기 제 1당사자에 의해 도출되는 데이터 스트링의 순서화된 연속값에서의 다른 데이터 스트링 ($C_1 \dots C_{i-1}$ 및 $C_{i+1} \dots C_n$)에 대해 상기 데이터 스트링(C_i)의 의 순서를 나타내는 프로그래시브 일련 번호인 지불 설정 방법.

(청구항 86)

제 84항에 있어서, 각각의 차변 금액(D_i)은 SN_i 를 사용하여 결정되는 지불 설정 방법.

(청구항 87)

제 84항에 있어서, 1과 n 사이의 모든 인덱스(i)에 대하여, $D_1 + D_2 \dots + D_i$ 이 $TV_1 + TV_2 + \dots + TV_i$ 보다 적거나 이와 동일한 지불 설정 방법.

(청구항 88)

제 84항에 있어서, 각각의 차변 금액(D_i)은 SN_i 를 사용하여 결정되는 지불 설정 방법.

(청구항 89)

값(TV)을 각각 갖는 다수의 동일한-가치의 거래($T_1, T_2, \dots, T_i, \dots, T_n$)에 대해 지불하는 방법에 있어서,

A. 제 1당사자는 각각의 거래(T_i)로부터 T_i 와 관련된 데이터 스트링(C_i)을 도출하고 제 2당사자는 상기 데이터 스트링(C_i)을 수신하도록 하는 단계로서;

상기 각각의 데이터 스트링(C_i)은 프로그래시브 일련 번호(S_i)를 포함하고, 상기 일련 번호는 1로부터 시작하여 순차적으로 순서화되고 데이터 스트링(C_j)($j=1, \dots, n$)의 순서화된 연속값에서의 다른 데이터 스트링에 대해 C_i 의 위치를 나타내는, 도출 및 수신하도록 하는 단계;

B. 제 2당사자가 아이템(V_i)을 C_i 와 관련시키는 단계로서, V_i 는 상기 제 1당사자에 의해 실질적으로 예측될 수 없는, 관련시키는 단계;

C. 상기 제 2당사자가 특성(P_i)이 C_i 와 V_i 사이에 유지되는지를 결정하고, 유지될 경우 상기 제 2당사자는 V_i 가 P_i 를 충족하는지를 제 3당사자가 검증할 수 있도록 하는 정보(I_i)를 제 3당사자로 하여금 수신하도록 하는 단계;

D. 상기 제 3당사자가 V_i 가 P_i 를 충족하는지를 검증하고, V_i 가 P_i 를 충족하는 경우에만:

a) 제 5당사자가 S_{max} 를 결정하는 단계로서, S_{max} 는 다음:

i) $1 \leq k \leq n$;

ii) C_k 가 C_i 를 수신하기 전에 제 2당사자에 의해 수신되고;

iii) 상기 제 3당사자가 V_k 가 P_k 를 충족하는지를 검증하고;

iv) 상기 제 1당사자가 0이 아닌 금액(D_k)만큼 차변받는 C_k 에 포함되는 임의의 일련 번호(S_k) 중 가장 큰 번호를 나타내는, 결정 단계;

b) 상기 제 5당사자가 상기 제 4당사자로 하여금 대변 금액(CR)을 수신하도록 하는 단계; 및

c) 상기 제 5당사자가 상기 제 1당사자가 차변 금액(D_i)만큼 차변받도록 하는 단계를 포함하며, D_i 는 $(S_i - S_{\max}) * TV$ 에 의해 제공되는 지불 방법.

(청구항 90)

제 89항에 있어서, $F(V_i) < s$ 인 경우에만, V_i 가 P_i 를 충족시키며,

여기서 s 는 상수이며, F 는 비트 스트링 상에서 동작하고 수를 리턴시키는 함수인 지불 방법.

(청구항 91)

제 90항에 있어서, 상기 제 4당사자가 수신하는 상기 대변 금액(CR)은 TV 및 $1/s$ 에 비례하는 지불 방법.

(청구항 92)

제 90항에 있어서, F 는 0과 1 사이의 수를 출력하도록 비트 스트링 상에서 동작하는 함수이며, s 는 0과 1 사이의 상수인 지불 방법.

(청구항 93)

값(TV_i)($i=1, \dots, n$)을 각각 갖는 다수의 거래(T_i)($i=1, \dots, n$)에 대해 사용자가 상인에게 지불을 설정하는 방법에 있어서,

A. 사용자(U)는 제 1디지털 서명 방식에 대한 공개 키 및 대응하는 비밀 키를 설정하고 데이터 스트링 $C = \text{SIG}_U(T_i)$ 를 각각의 T_i 로부터 도출하고 C_i 및 일련 번호(S_i)를 포함하는 전자 수표(CH_i)를 생성는 단계로서;

$\text{SIG}_U(T_i)$ 는 상기 제 1디지털 서명 방식에서 상기 거래(T_i)에 대한 사용자(U_i)의 디지털 서명을 나타내고;

S_i 는 상기 제 1당사자에 의해 도출되는 데이터 스트링(C_j)($j=1, \dots, n$)의 순서화된 연속값에서의 다른 데이터 스트링에 대한 상기 데이터 스트링(C_i)의 순서를 나타내는 프로그래시브 일련 번호인, 도출 단계;

B. 상기 사용자(U)는 상기 상인(M)이 C_i 및 S_i 을 수신하도록 하는 단계;

C. 상기 상인(M)은 제 2디지털 서명 방식에 대해서 공개 키 및 대응하는 비밀 키를 설정하고, 상기 데이터 스트링(C_i)을 아이템 $V = \text{SIG}_M(C_i)$ 과 관련시키는 단계로서, $\text{SIG}_M(C_i)$ 는 상기 제 2디지털 서명 방식에서 상기 데이터 스트링(C_i)에 대한 상인(M)의 디지털 서명을 나타내는, 설정 및 관련시키는 단계;

D. 상기 상인(M)은 상기 값 $F(V) = F(\text{SIG}_M(C))$ 를 계산하는 단계로서, F 는 0 및 1사이의 수를 출력하도록 비트 스트링 상에서 동작하는 공개 함수를 나타내는, 계산 단계;

E. 상기 상인(M)은 $F(\text{SIG}_M(C_i))$ 을 상수와 비교하여 $F(V) < s$ 인지를 결정하도록 하고, 만일 그렇다면, 은행이 상기 상인(M)의 상기 공개 키를 획득하도록 하는 단계;

F. 상기 은행은 상기 상인의 공개 키를 사용하여 $F(\text{SIG}_M(C_i)) < s$ 인지를 검증하는 단계; 및

G. $F(\text{SIG}_M(C)) < s$ 인 경우에만,

a) 제 5당사자가 $S_{\max}$ 를 결정하는 단계로서, $S_{\max}$ 는 지불이 행해졌던 상기 순서화된 연속값에서의 임의의 CH_j 에 포함된 가장 큰 일련 번호(S_j)를 나타내는, 결정 단계

b) 상기 제 5당사자는 제 4당사자로 하여금 대변 금액(CR)을 수신하도록 하는 단계; 및

c) 상기 제 5당사자는 상기 제 1당사자로 하여금 차변 금액(Di)만큼 차변하도록 하는 단계를 포함하는 지불 설정 방법.

(청구항 94)

제 93항에 있어서, 각각의 거래(T_i)($i=1, \dots, n$)는 동일한-가치여서, 모든 $i=1, \dots, n$ 에 대하여 $TV_i=TV$ 이며, D_i 는:

$D_i=(S_i-S_{\max})*TV$ 에 의해 제공되며, CR은:

$CR=TV*(1/s)$ 에 의해 제공되는 지불 설정 방법.

(청구항 95)

1과 n 사이의 인덱스(i)가 부분적으로 거래 값(TV_i)에 의해 각각 특징 지워지는 각각의 T_i 와 관련될 수 있는 거래 ($T_1, T_2, \dots, T_i, \dots, T_n$)에 대한 지불을 설정하는 시스템에 있어서,

A. 제 1당사자, 제 2당사자, 제 3당사자, 및 제 4당사자 간에 데이터를 전송하는 통신 수단;

B. 데이터 스트링(C_i)을 도출, 입력, 및 저장하기 위하여 제 1당사자에 의해 동작되는 제 1처리 수단(i 는 n보다 적거나 이와 동일하고 1보다 크거나 이와 동일함)으로서,

C_i 는 거래 T_i 와 관련되고,

C_i 는 수표(C_j)($j=1, \dots, n$)의 순서화된 연속값에서의 다른 수표에 대한 수표(C_i)의 위치를 나타내는 프로그래시브 일련 번호 (S_i)인, 제 1처리 수단;

C. 아이템(V_i)을 C_i 의 적어도 일부와 관련시키고 V 가 특성(P)을 충족하는지를 결정하기 위하여 상기 제 2당사자에 의해 동작되고, V_i 가 P_i 를 충족할 때, 상기 제 2당사자에 의해 선택적으로 동작되어, V_i 가 P_i 를 충족하는지를 상기 제 3당사자가 검증할 수 있도록 하는 정보(I_i)를 제 3당사자로 하여금 수신하도록 하는 제 2처리 수단으로서, V_i 는 상기 제 1당사자에 의해 실질적으로 예측될 수 없는, 제 2처리 수단;

D. V_i 가 P_i 를 충족할 때 상기 제 2당사자에 의해 선택적으로 동작되어 제 4당사자로 하여금 금액(CR_i)을 수신하도록 하고, 상기 제 1당사자가 금액(D_i)만큼 차변받도록 하는 수단을 포함하며, 1과 n 사이의 모든 인덱스(i)에 대하여, $D_1+D_2+\dots+D_i$ 이 $TV_1+TV_2+\dots+TV_i$ 보다 적은 지불 설정 시스템.

(청구항 96)

1과 n 사이의 인덱스(i)가 부분적으로 거래 값(TV_i)에 의해 각각 특징 지워지는 각각의 T_i 와 관련될 수 있는 다수의 n개의 거래($T_1, T_2, \dots, T_i, \dots, T_n$)에 대해 지불을 설정하는 방법에 있어서,

A. 제 1당사자가 각각의 거래(T_i)에 대해 데이터 스트링(C_i)의 적어도 일부를 제 2당사자로부터 수신하는 단계로서, 각각의 데이터 스트링(C_i)은 확률적 지불 방식을 사용하여 T_i 로부터 생성되는, 수신 단계;

B. 상기 제 1당사자는 수표(C_j)가 지불 가능한 것으로 선택될지를 제 5당사자 미리 예측하지 못하도록 하는 방식으로 예측 가능한 수표(C_j)(j 는 n보다 적거나 이와 동일하고 1보다 크거나 이와 동일함)를 선택하는 단계;

C. 각각의 선택된 수표(C_j)에 대하여, 상기 제 1당사자는 선택된 상기 수표(C_j)가 실제로 지불 가능한지를 제 3당사자가 검증할 수 있도록 하는 정보(I)를 제 3당사자로 하여금 수신하도록 함으로써, C_j 가 지불 가능하다고 검증시, 제 4당사자로 하여금 대변 금액(CR_j)을 수신하도록 하고, 상기 제 2당사자가 차변 금액(D_j) 만큼 차변받도록 하여, 모든 1과 n 사이의 인덱스(j), 및 지불 가능한 수표(C_j)의 임의의 선택에 대하여, $D=D_1+D_2+...+D_j$ 가 $TV_{agg}=TV_1+TV_2+...+TV_j$ 보다 크지 않게 되도록 하는 단계를 포함하는 지불 설정 방법.

(청구항 97)

1과 n 사이의 인덱스(i)가 부분적으로 거래 값(TV_i)에 의해 각각 특징 지워지고 대응하는 데이터 스트링(C_i)에 의해 표현될 수 있는 각각의 T_i 와 관련될 수 있는 다수의 n개의 거래($T_1, T_2, ..., T_i, ..., T_n$)에 대해 지불을 설정하는 방법에 있어서,

A. 제 1당사자는 수표(C_j)가 지불 가능한지를 상기 제 1당사자가 검증할 수 있도록 하는 정보(I_j)를 제 2당사자로부터 수신하는 단계로서,

상기 수표(C_j)는 상기 다수의 거래(T_i)($i=1, ..., n$) 중 대응하는 거래로부터 제 3당사자에 의해 도출되는 다수의 수표(C_i)($i=1, ..., n$)로부터 상기 제 2당사자에 의해 선택되고,

상기 수표(C_j)의 선택은 상기 제 3당사자에 의해서 실질적으로 예측될 수 없는, 상기 수신 단계;

B. 상기 제 1당사자가 I_j 의 수신시 C_j 가 실제로 지불 가능한지를 검증하는 단계; 및

C. 상기 제 1당사자는 제 4당사자로 하여금 대변 금액(CR_j)을 수신하도록 하고, 상기 제 3당사자가 차변 금액(D_j) 만큼 차변받도록 하는 단계를 포함하는 지불 설정 방법.

(청구항 98)

각각의 거래(T_i)가 단위 값(UV)의 배수인 거래 값(TV_i)에 의해 부분적으로 각각 특징 지워지는 다수의 n개의 거래($T_1, T_2, ..., T_i, ..., T_n$)에 대해 지불을 설정하는 방법에 있어서,

A. 제 1당사자는 각각의 거래(T_i)로부터 T_i 에 대응하는 데이터 스트링(C_i)을 도출하고, 제 2당사자가 C_i 를 수신하도록 하는 단계로서,

각 데이터 스트링(C_i)은 상기 정수 인덱스(i) 및 T_i 의 상기 값(TV_i)에 대한 정보를 벡터 형태($S_i, S_i + v_i - 1$)로 포함하며;

1과 n 사이의 모든 i에 대하여, S_i 는 순차적으로 순서화되고 데이터 스트링(C_j)($j=1, ..., n$)의 순서화된 연속값에서의 다른 데이터 스트링에 대한 C_i 의 위치를 나타내는 프로그래시브 일련 번호이고;

v_i 는 i에 따르며 T_i 의 TV_i 을 나타내는 정수이고, $v_i=TV_i/(UV)$ 에 의해 제공되는, 도출 및 수신하도록 하는 단계;

B. 상기 제 2당사자는 수표(C_j)가 지불 가능하도록 선택될지를 상기 제 1당사자가 미리 예측하지 못하도록 하는 방식으로 예측 가능한 수표(C_j)($1 \leq j \leq n$)를 선택하는 단계;

C. 상기 제 2당사자는 선택된 수표(C_j)가 지불 가능한지를 제 3당사자가 검증할 수 있도록 하는 정보(I_j)를 제 3당사자로 하여금 수신하도록 하는 단계;

D. 상기 제 3당사자가 I_j 의 수신에 응답하여, 선택된 수표(C_j)가 지불 가능한지를 검증하는 단계;

E. C_j 가 지불 가능한 경우에만:

a) 제 5당사자가 $S_{\max}$ 의 값을 결정하는 단계로서, $\max$ 는 $1 \leq \max \leq i \leq n$ 이도록 하는 정수이며, $v_{\max} = TV_{\max}/(UV)$ 이고, $S_{\max}$ 는 다음:

i) C_k 가 C_i 를 수신하기 전에 제 2당사자에 의해 수신되고;

ii) 상기 제 3당사자가 V_k 가 P_k 를 충족하는지를 검증하고;

iii) 상기 제 1당사자가 0이 아닌 금액(D_k)만큼 차변받는 C_k 에 포함되는 임의의 일련 번호(S_k)($1 \leq k \leq n$) 중 가장 큰 번호를 나타내는, 결정 단계;

b) 상기 제 5당사자는 제 4당사자로 하여금 대변 금액(CR)을 수신하도록 하는 단계; 및

c) 상기 제 5당사자는 상기 제 1당사자가 차변 금액(D_i) 만큼 차변받도록 하는 단계를 포함하며, D_i 는 $(S_i + v_i - 1 - S_{\max}) * UV$ 인 지불 설정 방법.

(청구항 99)

1과 n 사이의 인덱스(i)가 단위 값(UV)의 정배수인 거래 값(TV_i)에 의해 부분적으로 각각 특정 지워지는 각각의 T_i 와 관련 될 수 있는 다수의 n개의 거래($T_1, T_2, \dots, T_i, \dots, T_n$)에 대해 지불을 설정하는 방법에 있어서,

A. 제 1당사자는 각각의 거래(T_i)로부터 T_i 에 대응하는 데이터 스트링(C_i)을 도출하고, 제 2당사자가 C_i 를 수신하도록 하는 단계로서,

각 데이터 스트링(C_i)은 상기 정수 인덱스(i) 및 T_i 의 상기 값(TV_i)에 대한 정보를 벡터 형태($S_i, S_i + v_i - 1$)로 포함하며,

1과 n 사이의 모든 i에 대하여, S_i 는 순차적으로 순서화되고 데이터 스트링(C_j)($j=1, \dots, n$)의 순서화된 연속값에서의 다른 데이터 스트링에 대한 C_i 의 위치를 나타내는 프로그래시브 일련 번호이고,

v_i 는 i에 따르며 T_i 의 TV_i 을 나타내는 정수이고, $v_i = TV_i/(UV)$ 에 의해 제공되는, 도출 및 수신하도록 하는 단계;

B. 상기 제 2당사자가 상기 제 1당사자에 의해 실질적으로 예측될 수 없는 V_i 를 C_i 와 관련시키는 단계;

C. 상기 제 2당사자는 특성(P_i)이 C_i 와 V_i 사이에 유지되는지를 결정하고, 유지될 경우 상기 제 2당사자는 V_i 가 P_i 를 충족하는지를 제 3당사자가 검증할 수 있도록 하는 정보(I_i)를 수신하도록 하는 단계;

D. 상기 제 3당사자가 V_i 가 P_i 를 충족하는지를 검증하고;

V_i 가 P_i 를 충족하는 경우에만:

a) 제 5당사자가 $S_{\max}$ 의 값을 결정하는 단계로서,

$\max$ 는 $1 \leq \max \leq i \leq n$ 이도록 하는 정수이며, $v_{\max} = TV_{\max}/(UV)$ 이고, $S_{\max}$ 는 다음:

i) C_k 가 C_i 를 수신하기 전에 제 2당사자에 의해 수신되고;

ii) 상기 제 3당사자가 V_k 가 P_k 를 충족하는지를 검증하고;

iii) 상기 제 1당사자가 0이 아닌 금액(D_k)만큼 차변받는 C_k 에 포함되는 임의의 일련 번호(S_k)($1 \leq k \leq n$) 중 가장 큰 번호를 나타내는, 결정 단계;

b) 상기 제 5당사자는 제 4당사자로 하여금 대변 금액(CR)을 수신하도록 하는 단계; 및

c) 상기 제 5당사자는 상기 제 1당사자가 차변 금액(D_i) 만큼 차변받도록 하는 단계를 포함하며, D_i 는 $(S_i + v_i - 1 - S_{\max}) * UV$ 인 지불 설정 방법.

(청구항 100)

값(TV_i)을 각각 갖는 다수의 n 개의 거래(T_i)($i=1, \dots, n$)에 대한 지불을 설정하는 방법에 있어서,

a. 제 1당사자는 각각의 T_i 로부터 T_i 에 관련된 데이터 스트링(C_i)을 도출하고 제 2당사자가 상기 데이터 스트링(C_i)을 수신하도록 하는 단계;

b. 상기 제 2당사자는 상기 데이터 스트링(C_i)($i=1, \dots, n$)의 그룹과 m 개의 리스트(L^k)와 특정하게 관련시키는 단계로서, $k=1, \dots, m$ 이며;

각각의 리스트(L^k)는 데이터 스트링($C^k_1, \dots, C^k_{l_k}$)을 포함하고;

$\sum_{k=1}^m l_k = n$ 인, 관련시키는 단계;

c. 상기 제 2당사자가 각각의 L^k 에 대해 커미트먼트(CM^k)를 계산함으로써, L^k ($k=1, \dots, m$)를 커미트하고, 제 3당사자가 CM^k ($k=1, \dots, m$)를 수신하도록 하는 단계;

d. 상기 제 3당사자는 CM^k ($k=1, \dots, m$)의 수신에 응답하여, 하나 이상의 정수 인덱스($i_1, i_2, \dots, i_r$)를 선택하고, 상기 제 2당사자가 상기 인덱스($i_1, i_2, \dots, i_r$)를 수신하도록 하는 단계로서, $1 \leq i_r \leq m$ 인, 선택 및 수신하도록 하는 단계;

e. 상기 인덱스($i_1, i_2, \dots, i_r$)의 수신에 응답하여, 상기 제 2당사자는 $CM^{i_1}, CM^{i_2} \dots CM^{i_r}$ 를 디커미트함으로써, $L^{i_1}, \dots, L^{i_r}$ 을 드러내는 단계; 및

f. 제 5당사자는 제 4당사자로 하여금 대변 금액(CR)을 수신하도록 하고, 상기 제 1당사자가 차변 금액(D)만큼 차변받도록 하는 단계를 포함하는 지불 설정 방법.

(청구항 101)

제 100항에 있어서, 상기 L^k 에 대한 커미트먼트(CM^k)는 해쉬 값($H(L^k)$)이며, H 는 일방향 해쉬 함수인 지불 설정 방법.

(청구항 102)

제 100항에 있어서, 각각의 데이터 스트링(C_i)은 상기 거래 값(TV_i)을 나타내는 하나 이상의 비트를 포함하는 지불 설정 방법.

(청구항 103)

제 102항에 있어서, 단계(b) 후, 상기 제 2당사자가 각각의 리스트(L^k)와 대응하는 값(V^k)을 관련시키는 단계를 더 포함하며, V^k 는 리스트(L^k) 내의 모든 데이터 스트링($C^k_1, \dots, C^k_{l_k}$)의 수집값을 나타내고,

V^k 는 $V^k = TV^{k1} + \dots + TV^{kl_k}$ 에 의해 제공되는 지불 설정 방법.

(청구항 104)

제 103항에 있어서, 단계(c) 후, 상기 제 2당사자가 값의 리스트($V^1, \dots, V^m$)에 대한 커미트먼트(CV)를 계산하는 단계를 더 포함하고,

상기 커미트먼트(CV)는 ($V^1, \dots, V^m$)에 제 2당사자를 커미트하고,

CV는 해쉬 함수($H(V^1, \dots, V^m)$)이며,

H는 일방향 해쉬 함수이어서, CV를 디커미트함으로써, 상기 제 2당사자는 상기 제 3당사자에게 드러나는($V^1, \dots, V^m$) 지불 설정 방법.

(청구항 105)

제 100항에 있어서, 상기 제 4당사자에 의해 수신되는 상기 대변 금액(CR)은 $V = V^1 + \dots + V^k + \dots + V^m = \sum_{k=1}^m V^k$ 에 의해 제공되는 지불 설정 방법.

(청구항 106)

제 100항에 있어서, 상기 차변 금액(D)은 스케일 팩터와 승산되는 $D = V^{i1} + V^{i2} + \dots + V^{ir}$ 에 의해 제공되는 지불 설정 방법.

(청구항 107)

제 106항에 있어서, 상기 스케일 팩터는 m/r 인 지불 설정 방법.

(청구항 108)

제 100항에 있어서, 상기 각 데이터 스트링(C_i)은 정수(SN_i)를 표시하는 정보이고, SN_i 는 1로부터 시작하여 순차적으로 순서화되는 프로그레시브 일련 번호이고, 상기 일련 번호(SN_i)는 상기 다수의 n 거래(T_i)($i=1, \dots, n$)에서 다른 거래($T_1, \dots, T_{i-1}$ 및 $T_{i+1}, \dots, T_n$)에 대한 상기 거래(T_i)의 시간 순서를 표시하는 지불 설정 방법.

(청구항 109)

제 100항에 있어서, 상기 제 1당사자가 T_i 로부터 상기 데이터 스트링(C_i)을 도출하는 단계는 상기 제 1당사자가 자신의 비밀 키를 사용하여 T_i 의 적어도 일부에 대한 디지털 서명을 생성하는 단계를 포함하는 지불 설정 방법.

(청구항 110)

제 100항에 있어서, C_i 의 적어도 일부는 인증되는 지불 설정 방법.

(청구항 111)

제 100항에 있어서, C_i 는:

- a) T의 적어도 일부에 대한 디지털 서명;
- b) 메시지 인증 코드; 및
- c) 전자 책 중 하나 이상을 포함하는 지불 설정 방법.

(청구항 112)

제 100항에 있어서, 상기 제 5당사자 및 상기 제 3당사자는 동일한 지불 설정 방법.

(청구항 113)

제 100항에 있어서, 상기 제 2당사자, 상기 제 3당사자, 및 상기 제 5당사자는 동일한 지불 설정 방법.

(청구항 114)

제 100항에 있어서, 상기 제 2당사자 및 상기 제 3당사자는 동일한 지불 설정 방법.

(청구항 115)

다수의 n 거래($T_1, \dots, T_i, \dots, T_n$)에 대한 지불 설정 방법으로서, 각 거래(T_i)는 값(TV_i)을 갖는 지불 설정 방법에 있어서,

A. 각 T_i 에 대해서, 제 1당사자는 T_i 로부터 도출되는 데이터 스트링(C_i)을 제 2당사자로부터 수신하는 단계;

B. 상기 제 1당사자는 상기 데이터 스트링($C_i(i=1, \dots, n)$)의 그룹을 m 개의 리스트 L^k 와 특정하게 관련시키는 단계로서, 여기서 $k=1, \dots, m$ 이며;

각 리스트 L^k 는 데이터 스트링($C^k_1, \dots, C^k_{l_k}$) 이고,

$\sum_{k=1}^m l_k = n$ 인, 관련시키는 단계;

C. 상기 당사자는 각 L^k 에 대한 커미트먼트(CM^k)를 계산함으로써 $L^k(k=1, \dots, m)$ 에 커미트하고, 제 3당사자가 $CM^k(k=1, \dots, m)$ 을 수신하도록 함으로써, 상기 제 3당사자가 하나 이상의 정수 인덱스($i_1, i_2, \dots, i_r$)를 선택하도록 하는 단계로서, 여기서 $1 \leq i_r \leq m$ 인, 선택하도록 하는 단계;

D. 상기 인덱스($i_1, i_2, \dots, i_r$)의 수신시, 상기 제 1당사자는 $CM^{i_1}, CM^{i_2} \dots CM^{i_r}$ 을 디커미트함으로써, $L^{i_1} \dots L^{i_r}$ 을 상기 제 3당사자에게 드러내고, 상기 제 3당사자는 제 4당사자로 하여금 대변 금액(CR)을 수신하도록 하고 제 2당사자가 차변 금액(D) 만큼 차변받도록 하는 단계를 포함하는 지불 설정 방법.

(청구항 116)

다수의 n 거래($T_1, \dots, T_i, \dots, T_n$)에 대한 지불 설정 방법으로서, 각 거래(T_i)는 값(TV_i)을 갖고 T_i 로부터 도출되는 대응하는 데이터 스트링(C_i)으로 표시될 수 있고, 상기 데이터 스트링($C_i(i=1, \dots, n)$)의 그룹이 m 개의 리스트 $L^k(k=1, \dots, m)$ 와 관련되며, 각 리스트 L^k 는 데이터 스트링($C^k_1 \dots C^k_{l_k}$)($\sum_{k=1}^m l_k = n$)을 포함하는, 지불 설정 방법에 있어서,

- A. 제 1당사자가 m 개의 리스트 $L^k(k=1, \dots, m)$ 의 각각에 대한 커미트먼트(CM^k)를 제 2당사자로부터 수신하는 단계;
- B. 상기 제 1당사자는 $CM^k(k=1, \dots, m)$ 의 수신시 하나 이상의 정수 인덱스($i_1, i_2, \dots, i_r$)를 선택하고, 여기서 $1 \leq i_r \leq m$ 이며, 상기 제 2당사자가 상기 인덱스($i_1, i_2, \dots, i_r$)를 수신하도록 함으로써, $L^{i_1}, \dots, L^{i_r}$ 을 상기 제 1당사자에게 드러내도록 하기 위하여 상기 제 2당사자가 $CM^{i_1}, CM^{i_2}, \dots, CM^{i_r}$ 을 디커미트하도록 하는 단계; 및
- C. 상기 제 1당사자는 제 3당사자로 하여금 대변 금액(CR)을 수신하도록 하고 제 4당사자는 차변 금액(D)만큼 차변받도록 하는 단계를 포함하는 지불 설정 방법.

(청구항 117)

다수의 n 거래($T_1, T_2, \dots, T_i, \dots, T_n$)에 대한 지불 설정 시스템으로서, 각 T_i 는 값(TV_i)를 갖는, 지불 설정 시스템에 있어서,

- A. 제 1당사자, 제 2당사자, 제 3당사자, 및 제 4당사자 간에 데이터를 전송하기 위한 통신 수단;
- B. 각 T_i 에 대해 데이터 스트링($C_i(1 \leq i \leq n)$)을 도출, 입력, 및 저장하기 위하여 상기 제 1당사자에 의해 동작되는 제 1처리 수단;
- C. 상기 데이터 스트링 $C_i(i=1, \dots, n)$ 의 그룹을 m 개의 리스트 $L^k(k=1, \dots, m)$ 와 특정하게 관련시키고, 상기 리스트 $L^k(k=1, \dots, m)$ 를 입력하고 저장하기 위하여 제 2당사자에 의해 동작되고 $C_i(i=1, \dots, n)$ 의 수신에 응답하는 제 2처리 수단으로서;

각 리스트 L^k 는 데이터 스트링($C^k_1, \dots, C^k_{l_k}$)을 포함하고,

$$\sum_{k=1}^m l_k = n \text{이며,}$$

상기 제 2처리 수단은 각 L^k 에 대한 커미트먼트(CM^k)를 계산하고 상기 커미트먼트(CM^k)($k=1, \dots, m$)를 입력하고 저장하기 위하여 상기 제 2당사자에 의해 부가적으로 동작되는, 제 2처리 수단;

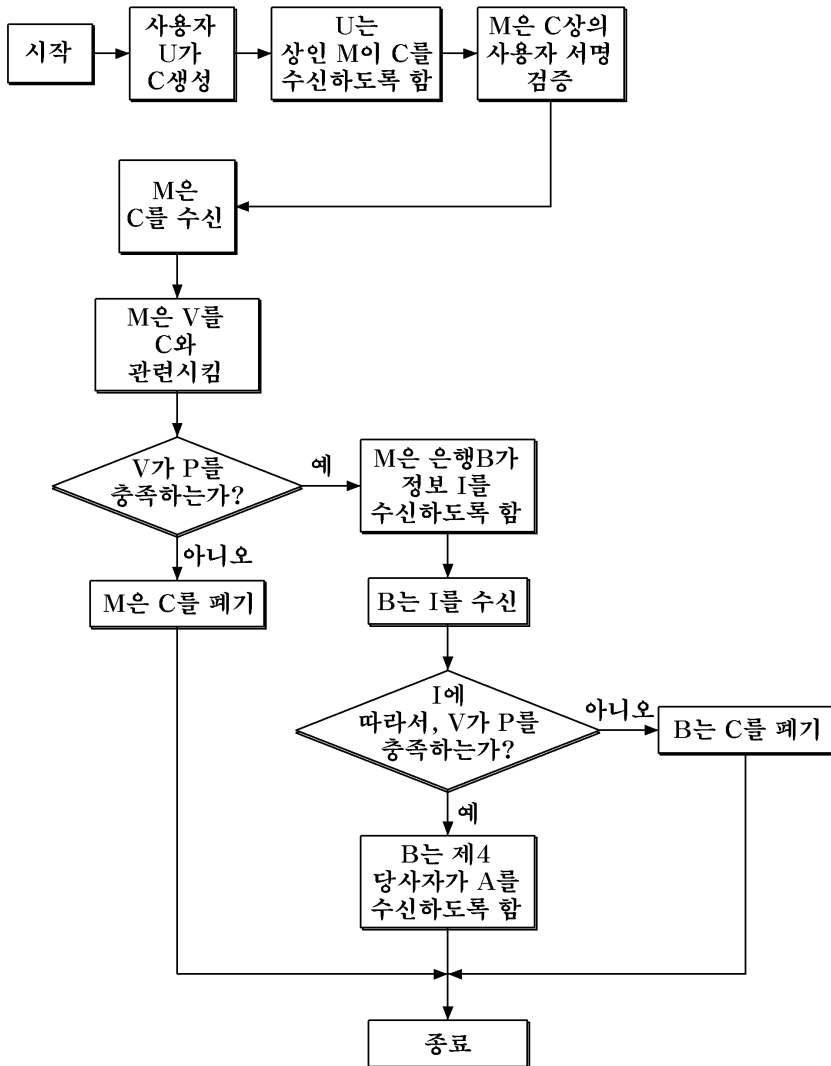
D. 하나 이상의 정수 인덱스($i_1, i_2, \dots, i_r$)를 선택하고 상기 제 2당사자가 상기 인덱스($i_1, i_2, \dots, i_r$)를 수신하도록 하기 위하여 상기 커미트먼트(CM^k)의 수신시 상기 제 3당사자에 의해 동작되는 제 3처리 수단으로서,

여기서 모든 r 에 대해서 $1 \leq i_r \leq m$ 인 제 3처리 수단;

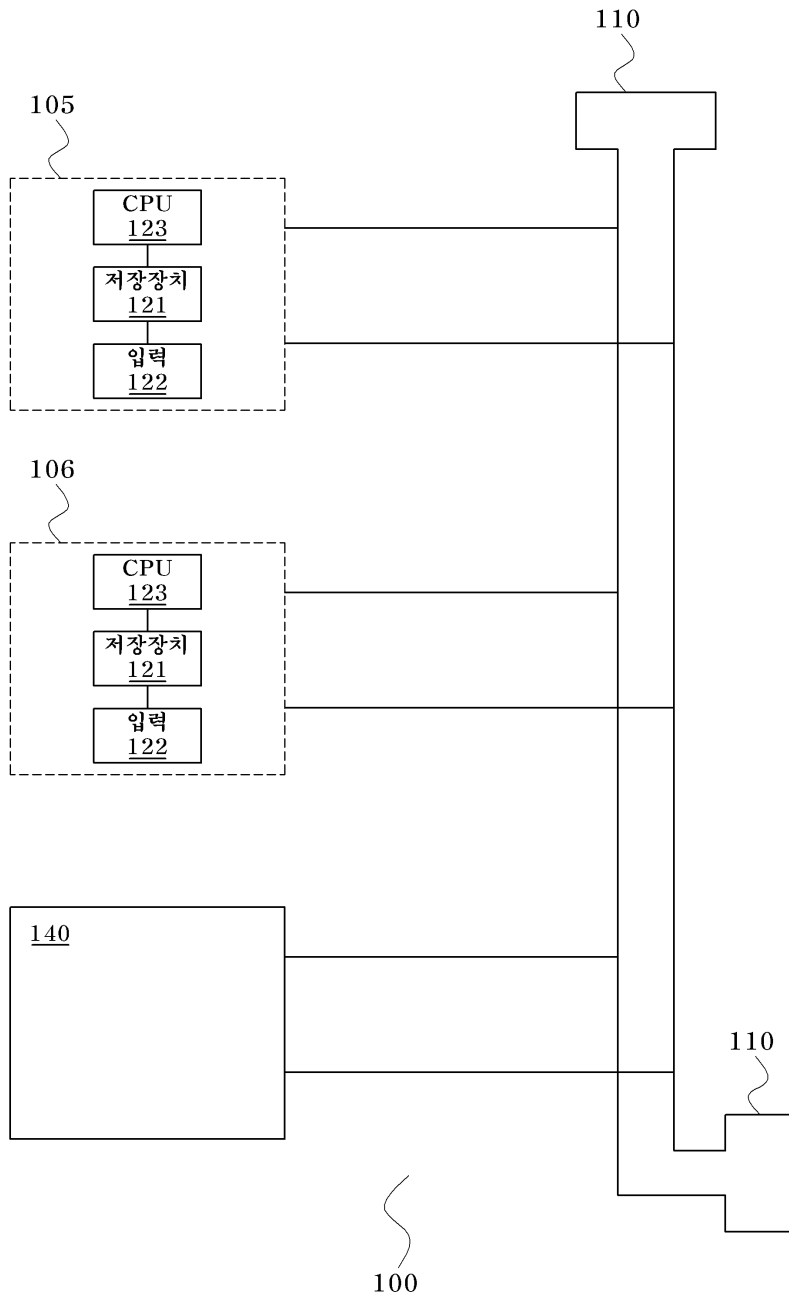
E. CM을 디커미트하기 위하여 상기 인덱스($i_1, i_2, \dots, i_r$)의 수신시 상기 제 2당사자에 의해 동작됨으로써, 상기 제 3당사자에 드러내는 제 4처리 수단; 및

F. 상기 제 1당사자가 차변 금액(D) 만큼 차변받도록 하고 제 4당사자로 하여금 대변 금액(CR)을 수신하도록 하기 위하여 $L^{i_1}, \dots, L^{i_r}$ 을 드러낼 때 상기 제 3당사자에 의해 동작되는 수단을 포함하는 지불 설정 시스템.

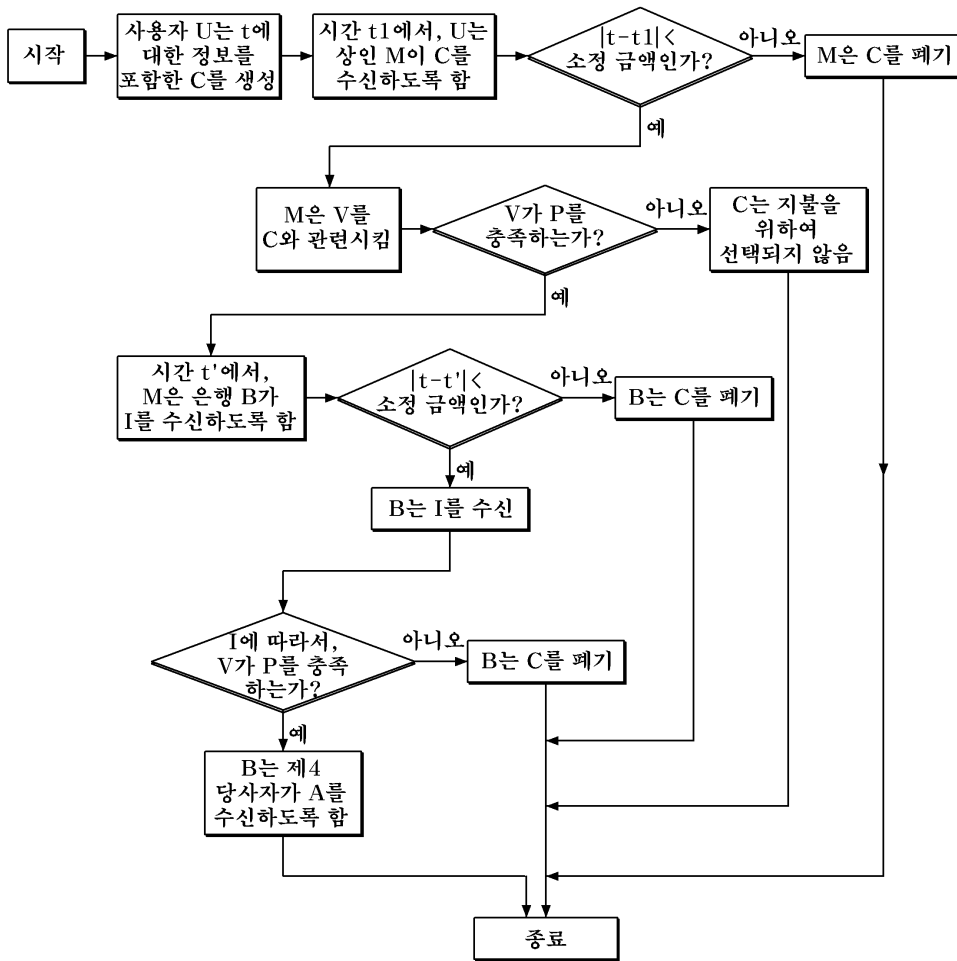
[도 1]



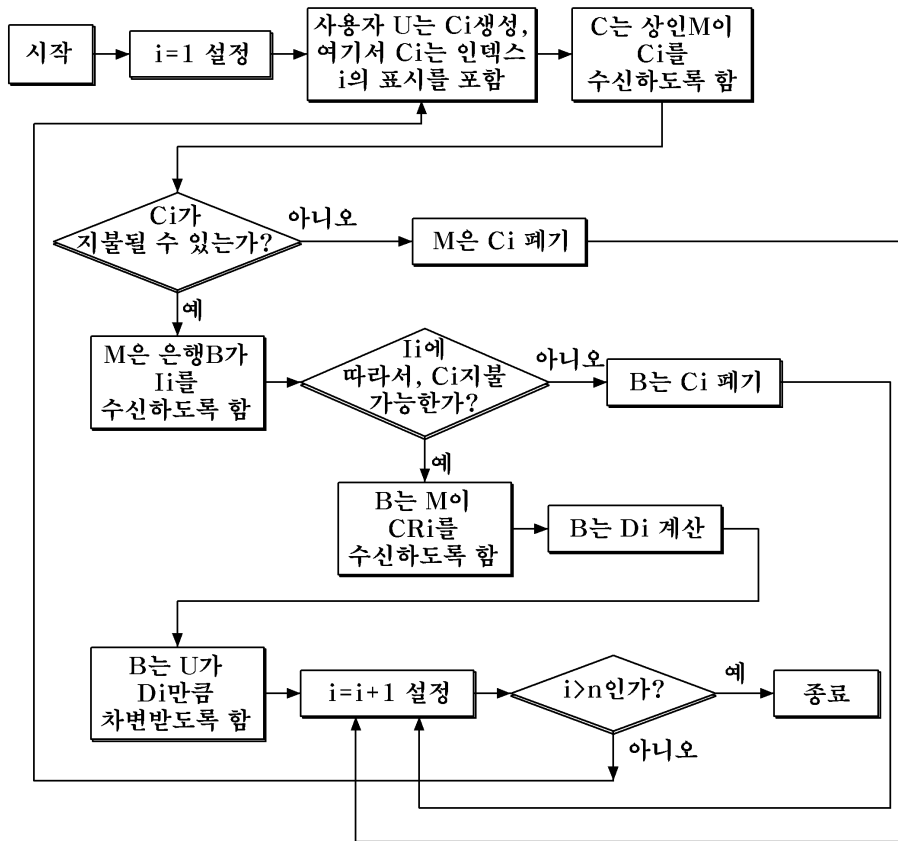
[도 2]



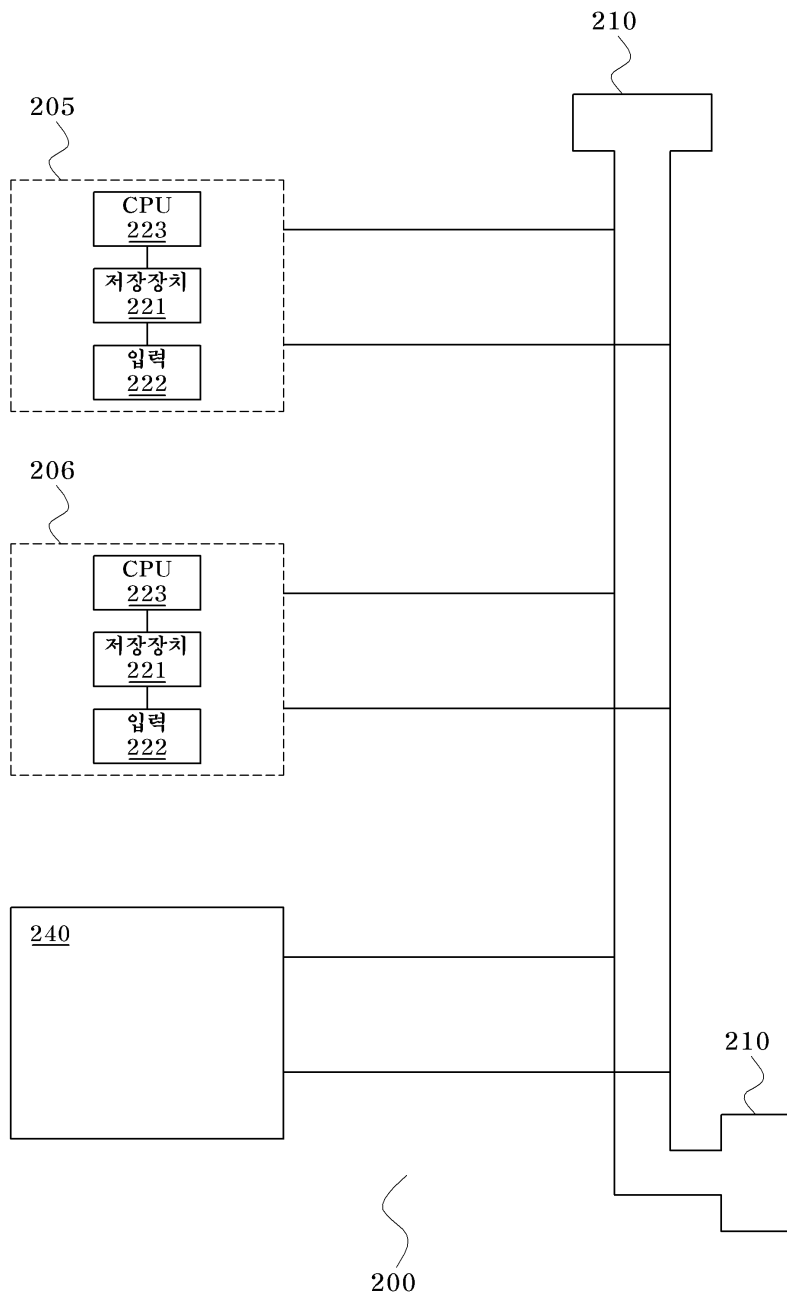
[도 3]



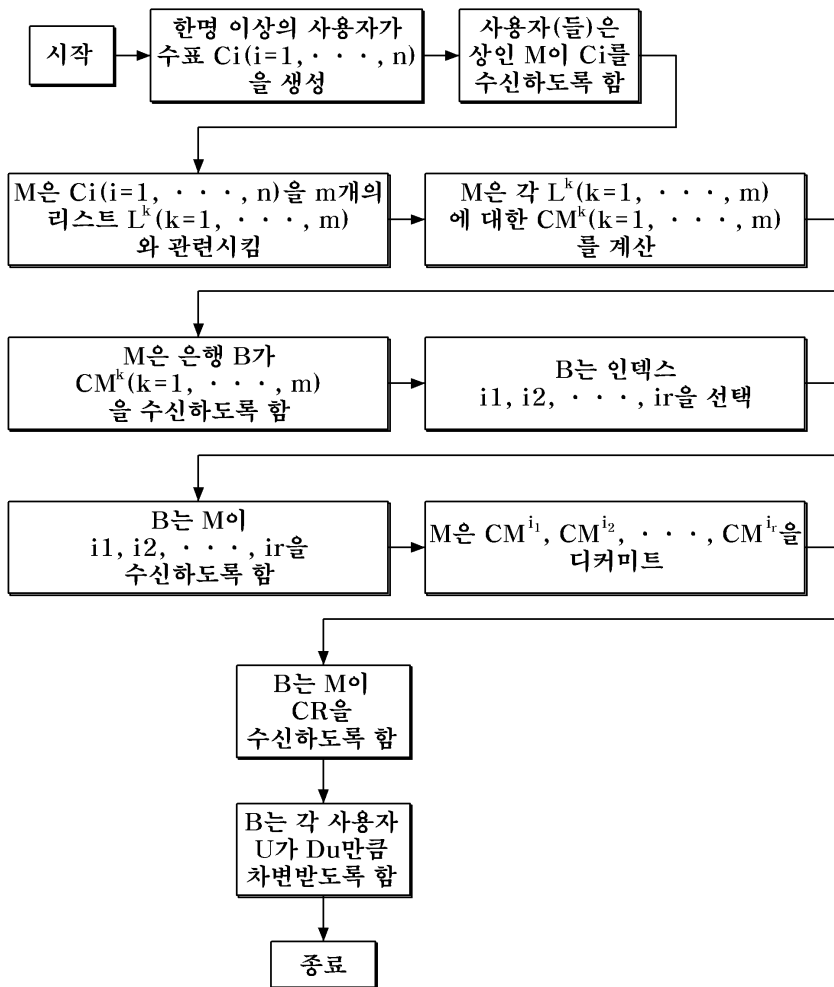
[도 4]



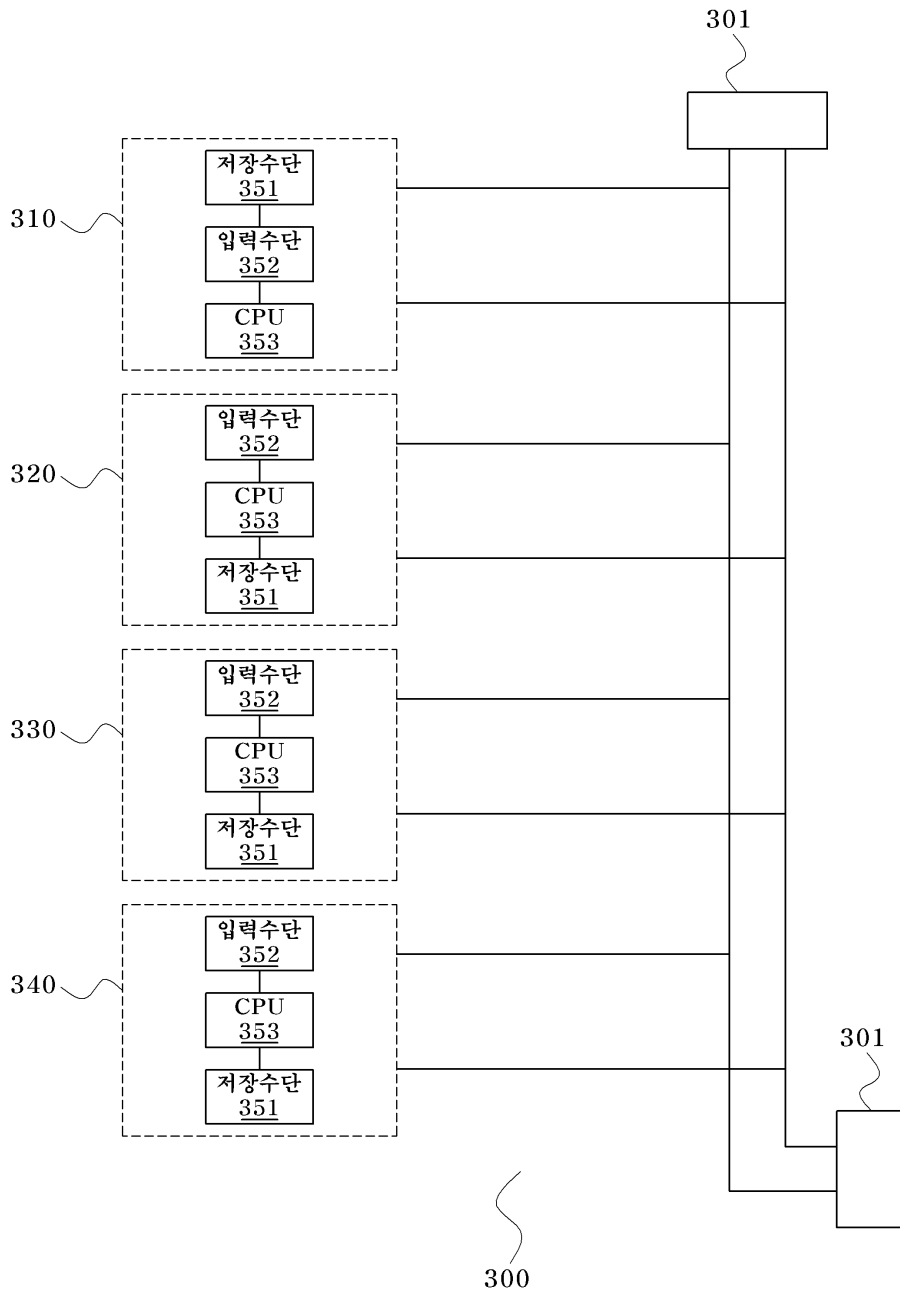
[도 5]



[도 6]



[도 7]



도면의 간단한 설명

도 1은 대규모 지불 시스템을 나타내는 블록도.

도 2는 거래 비용을 줄이기 위하여 도 1에 도시된 대규모 지불 시스템 내에서 프로세서의 분산을 나타내는 블록도.

도 3은 분산된 프로세서를 포함하는 서버의 위치를 나타내는 블록도.

도 4는 분산된 프로세서 내에 포함된 기능 모듈을 나타내는 블록도.

도 5는 분산된 프로세서 내에 포함될 수 있는 기능 모듈을 나타내는 블록도.

도 6은 저가의 거래과 관련된 동작을 나타내는 흐름도.

도 7은 분산된 프로세서 중에서 실행되는 단일 상인과 관련된 동작을 나타내는 블록도.

도 8은 분산된 프로세서 중에서 실행되는 다수의 상인과 관련된 동작을 나타내는 블록도.

도 9는 머클 트리(Merkle tree)를 나타내는 블록도.

도 10은 각 분산된 프로세서 내에 포함될 수 있는 라우터를 나타내는 블록도.

도 11은 분산된 프로세서의 노드를 나타내는 블록도.

도 12는 대금 청구서와 그래픽 사용자 인터페이스의 일부를 나타내는 도면.

도 13은 거래 브레이크다운(transaction breakdown)을 제공하는 그래픽 사용자 인터페이스를 나타내는 도면.

도 14는 개별적인 거래를 확인하는 그래픽 사용자 인터페이스를 나타내는 도면.

도 15는 고객 서비스와 관련된 그래픽 사용자 인터페이스를 나타내는 도면.

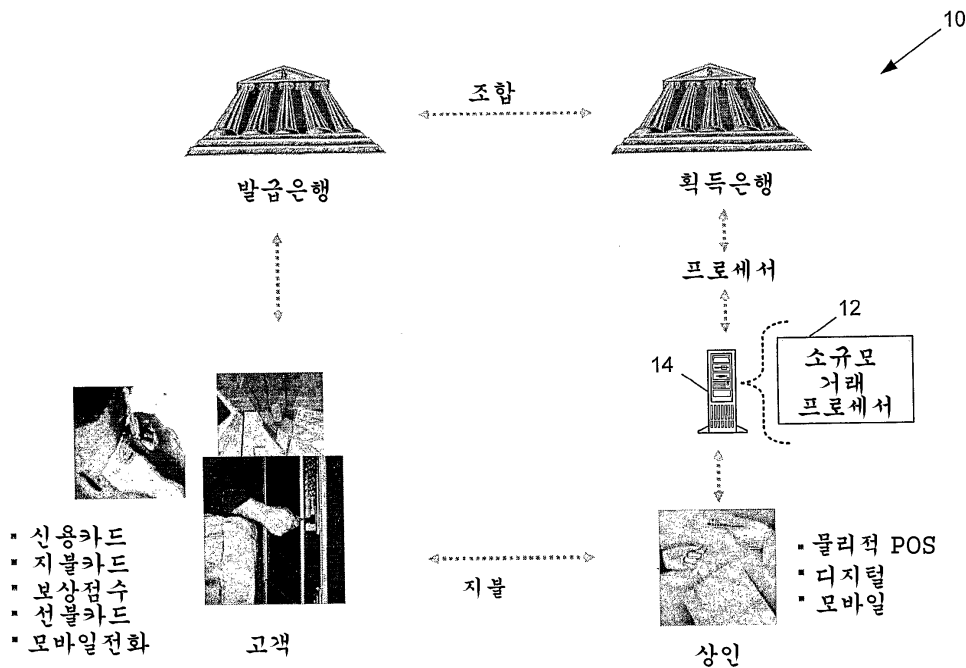
도 16은 고객으로부터 서비스 요청을 수신하는 것과 관련된 그래픽 사용자 인터페이스를 나타내는 도면.

도 17은 고객의 요청을 서비스 공급자에 제공하는 그래픽 사용자 인터페이스를 나타내는 도면.

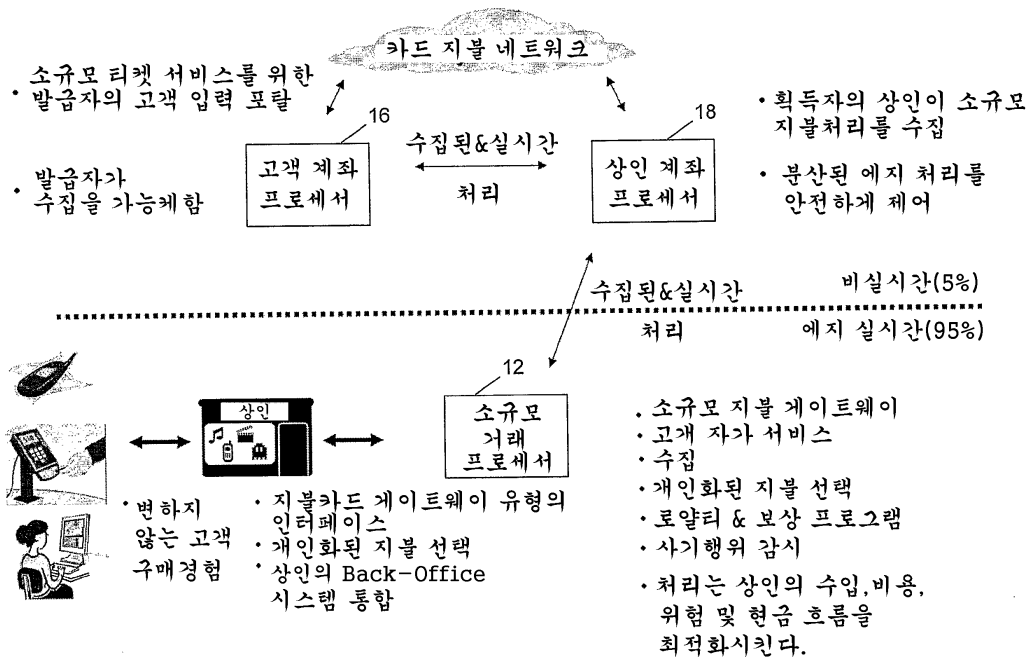
도 18은 수집된 저가의 거래 정보를 나타내는 그래픽 사용자 인터페이스를 나타내는 도면.

도면

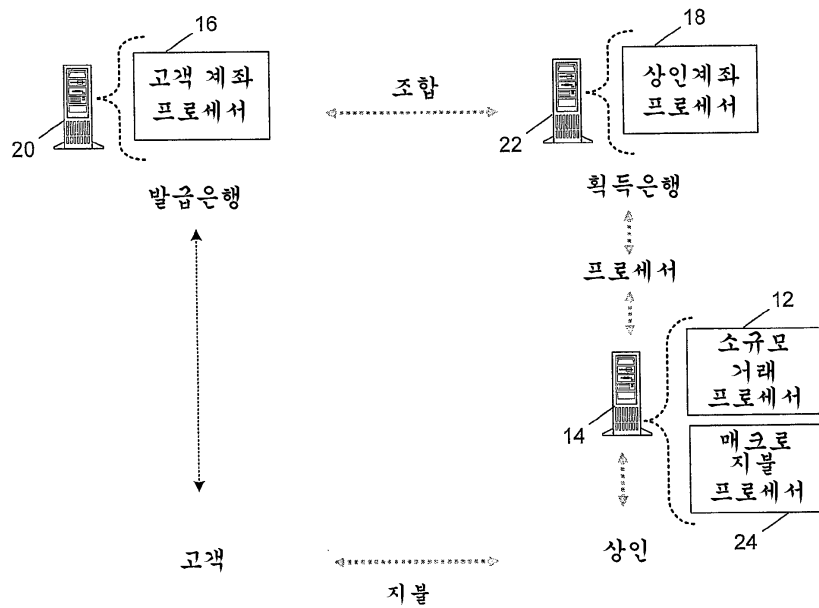
도면1



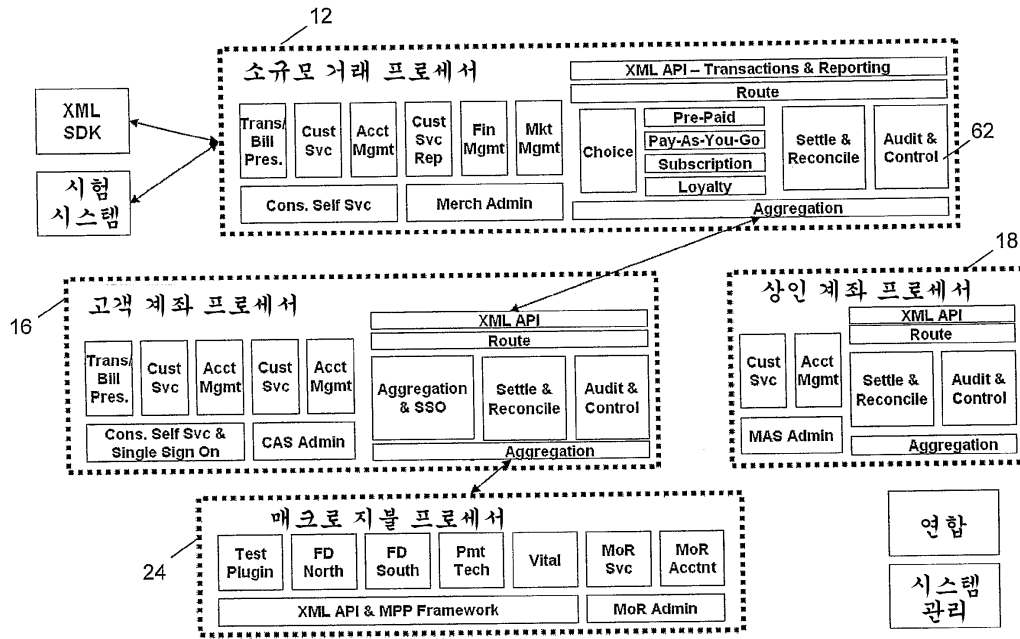
도면2



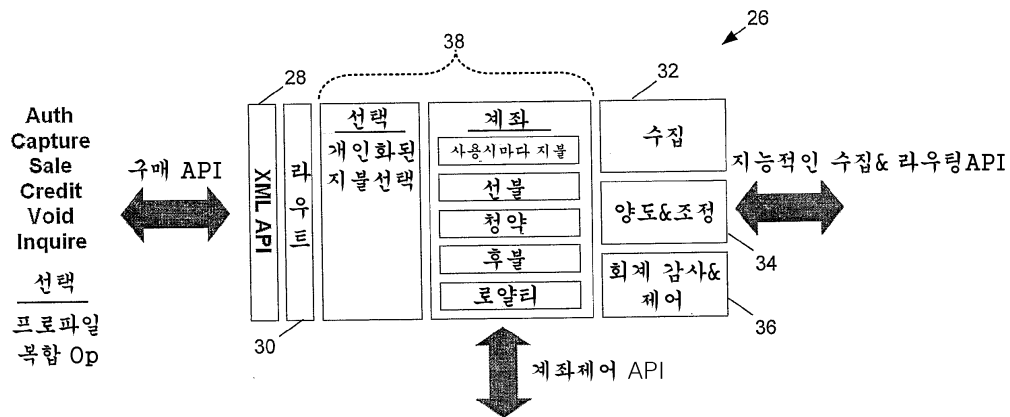
도면3



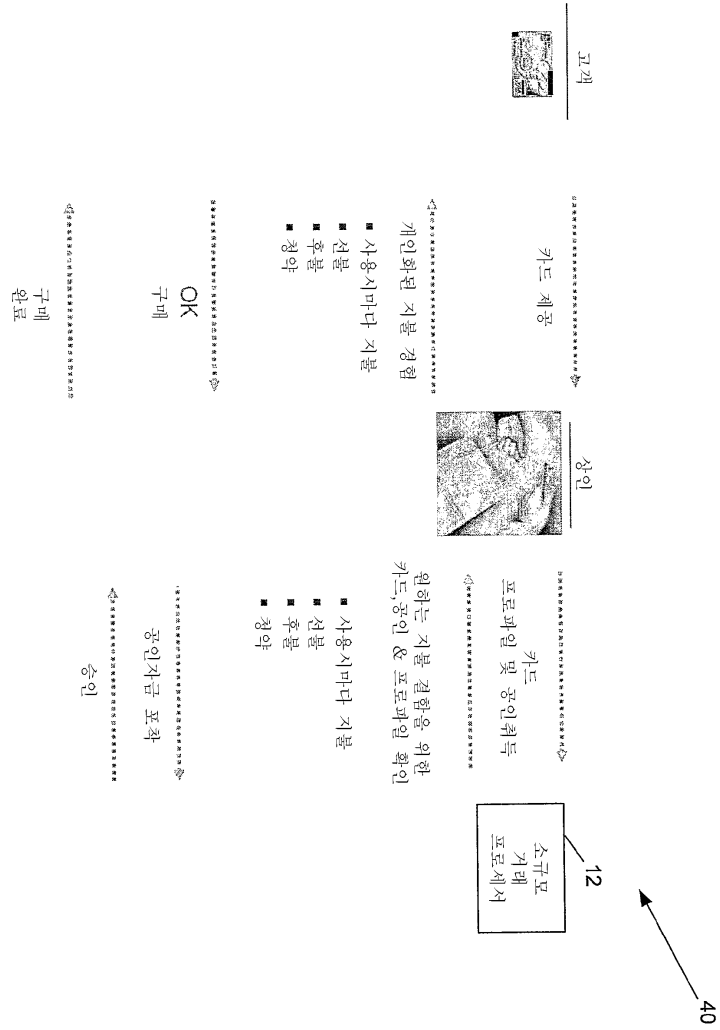
도면4



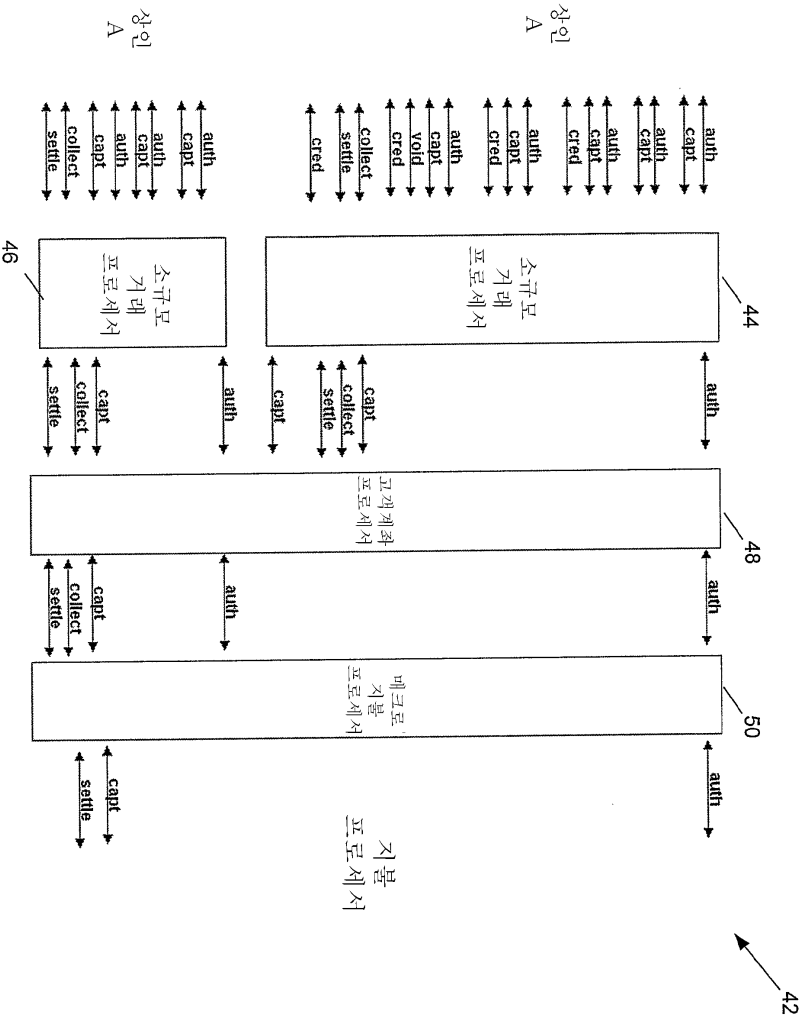
도면5



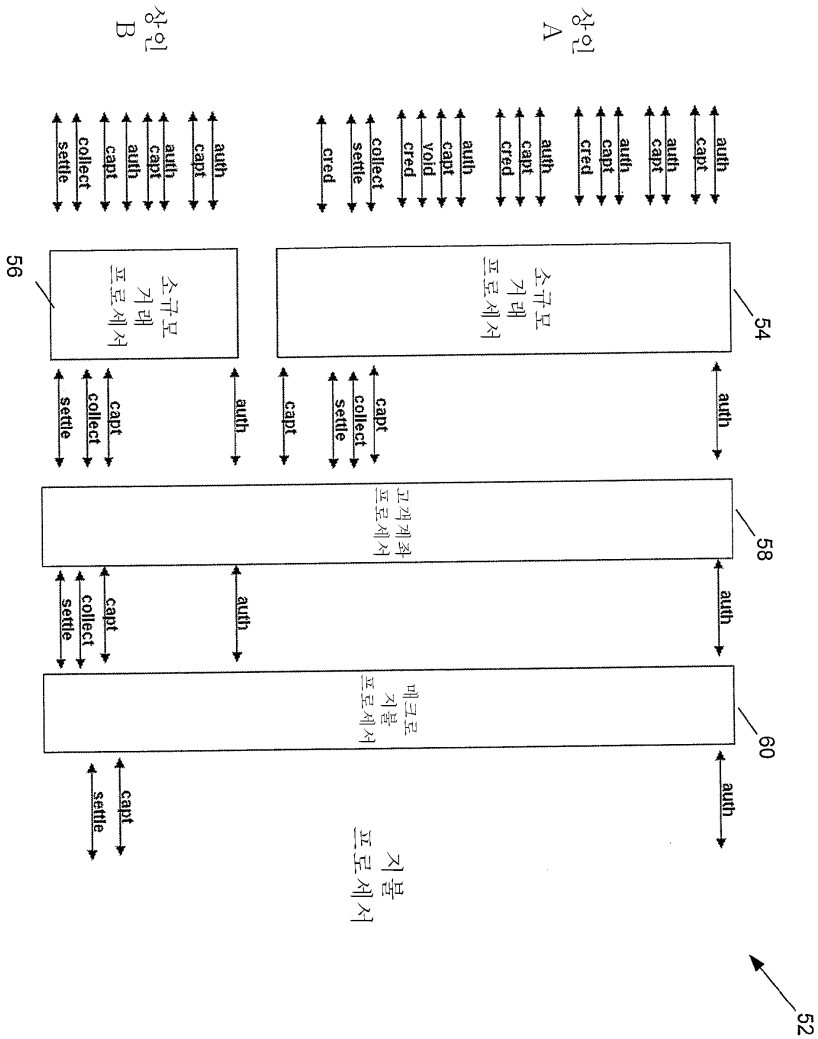
도면6



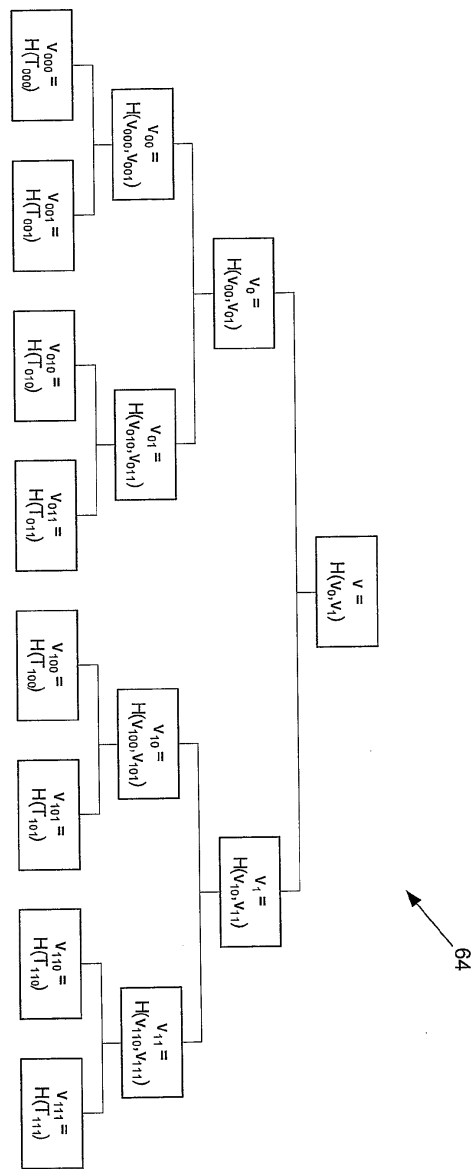
도면7



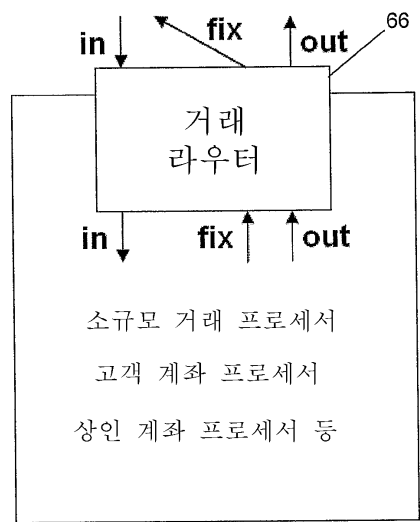
도면8



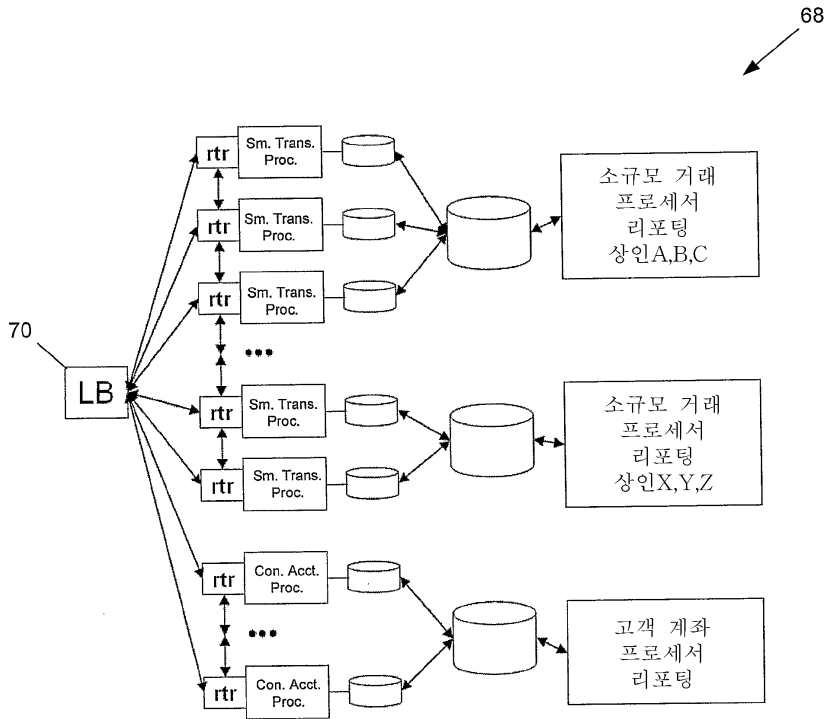
도면9



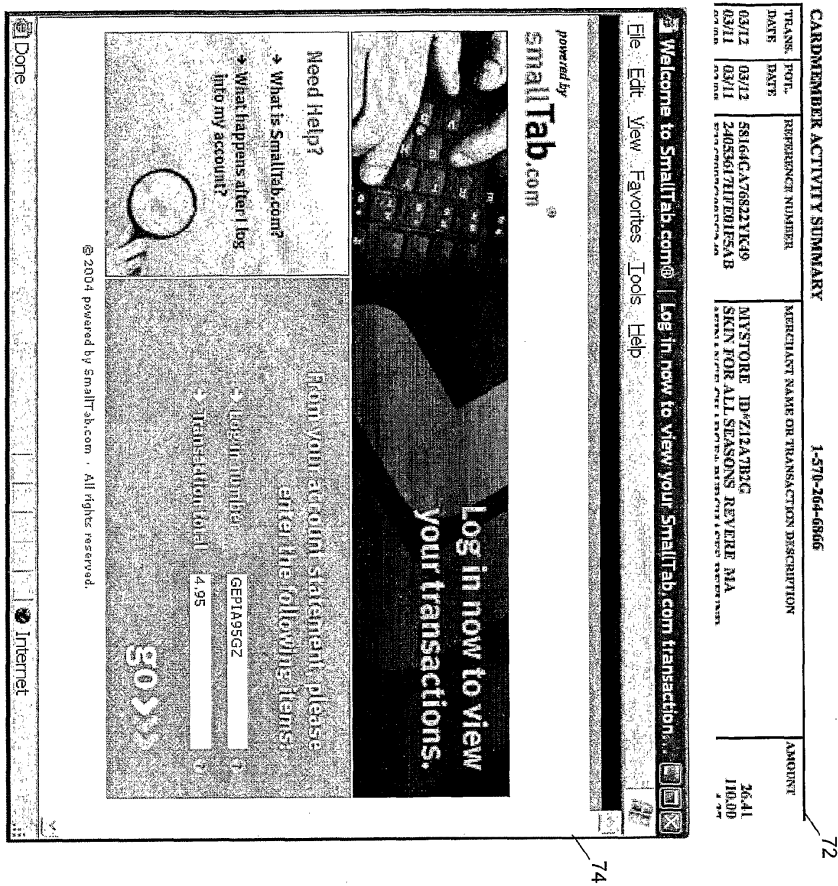
도면10



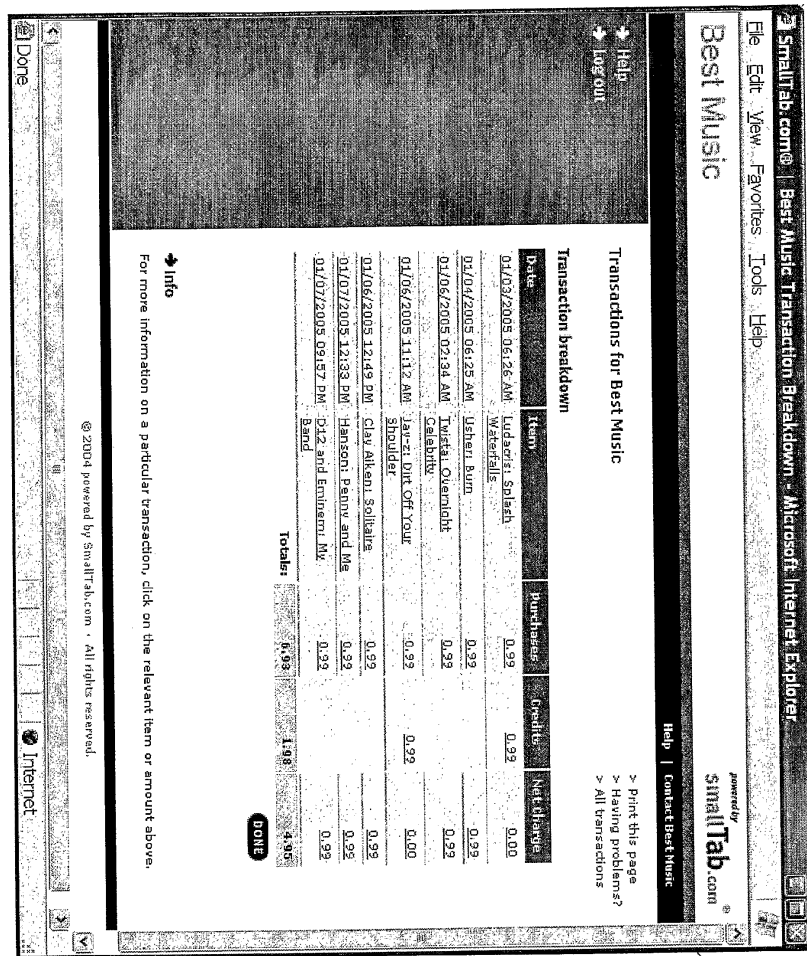
도면11



도면12

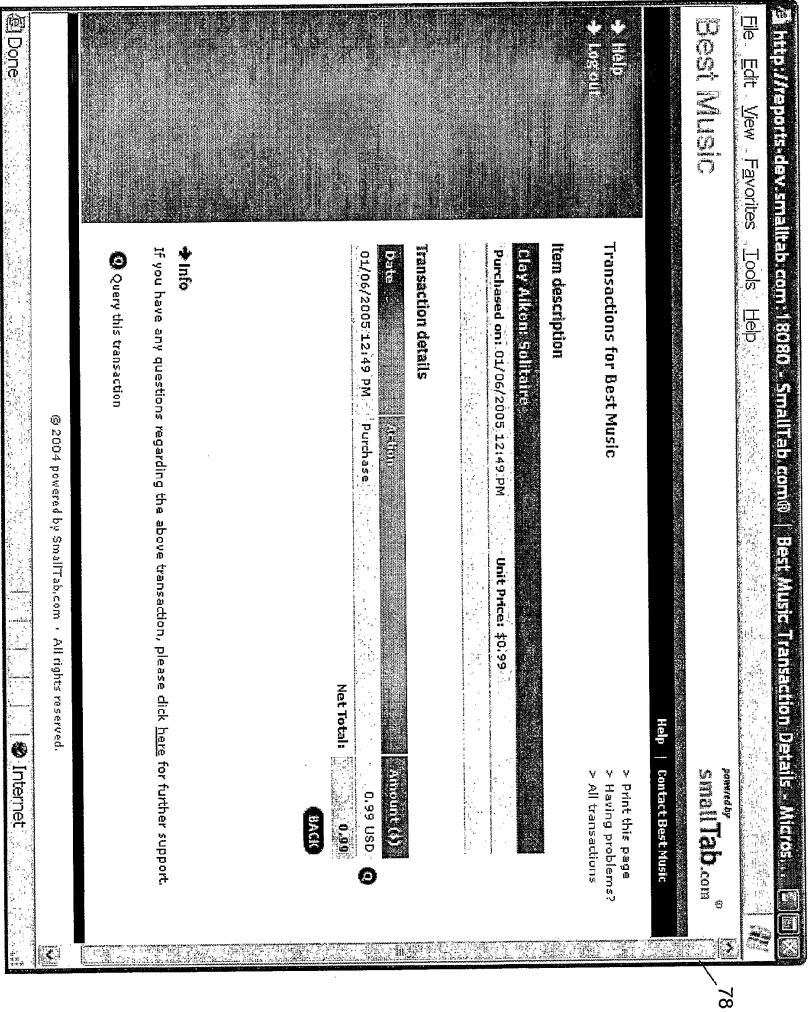


도면13

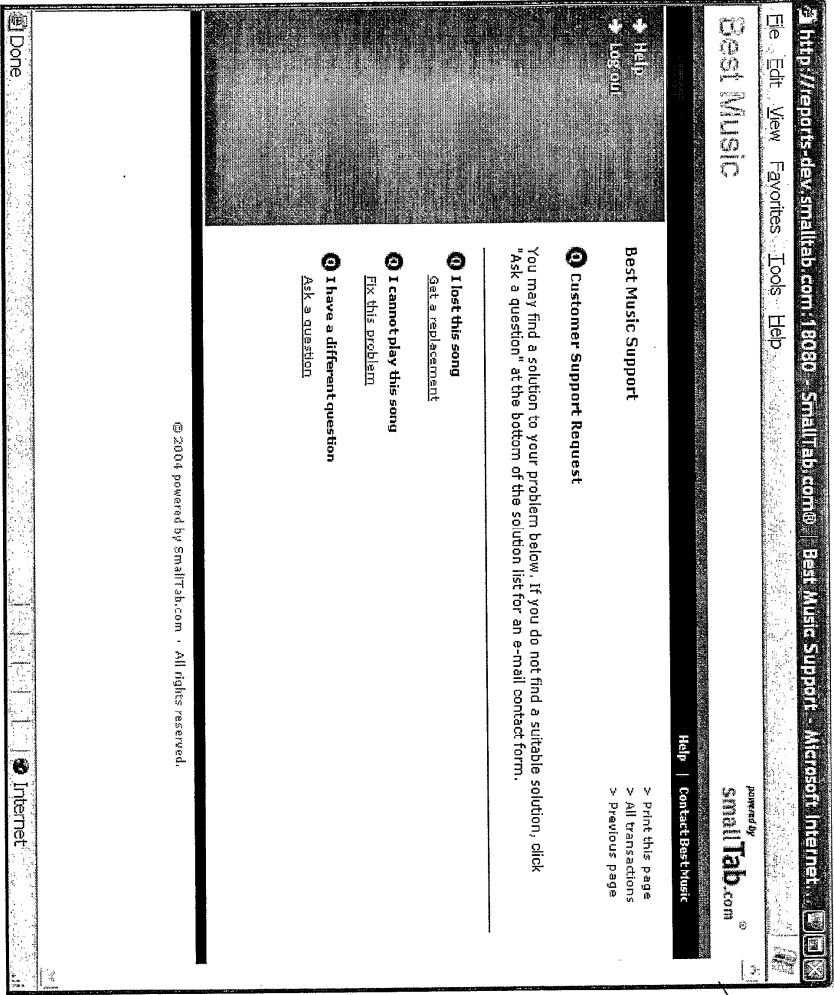


76

도면14

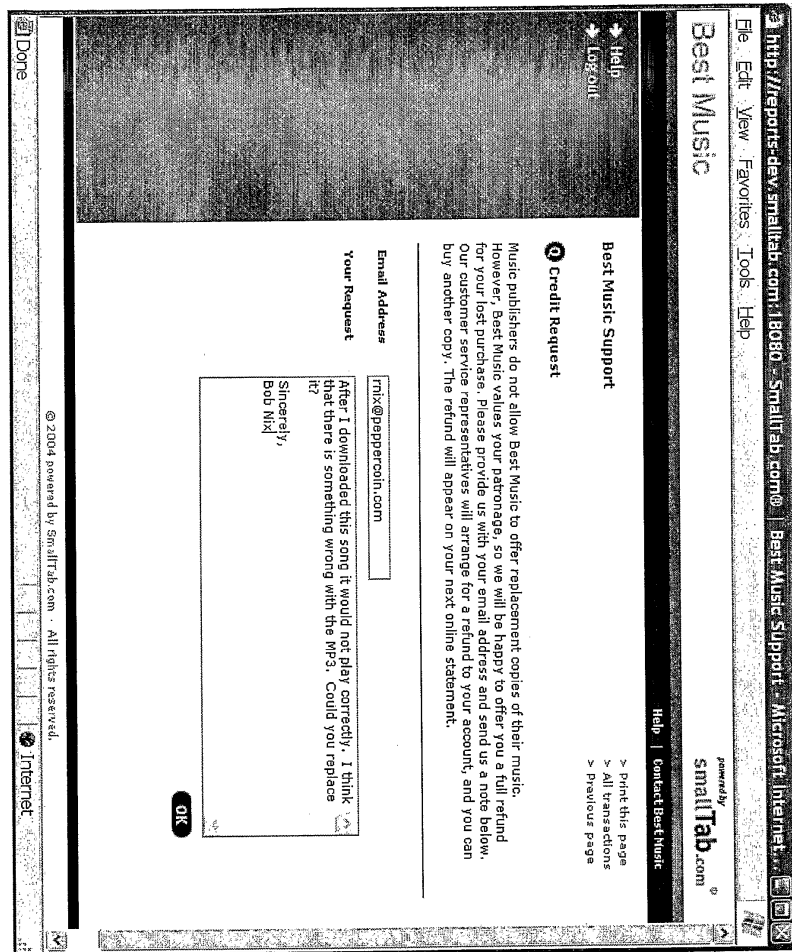


도면15



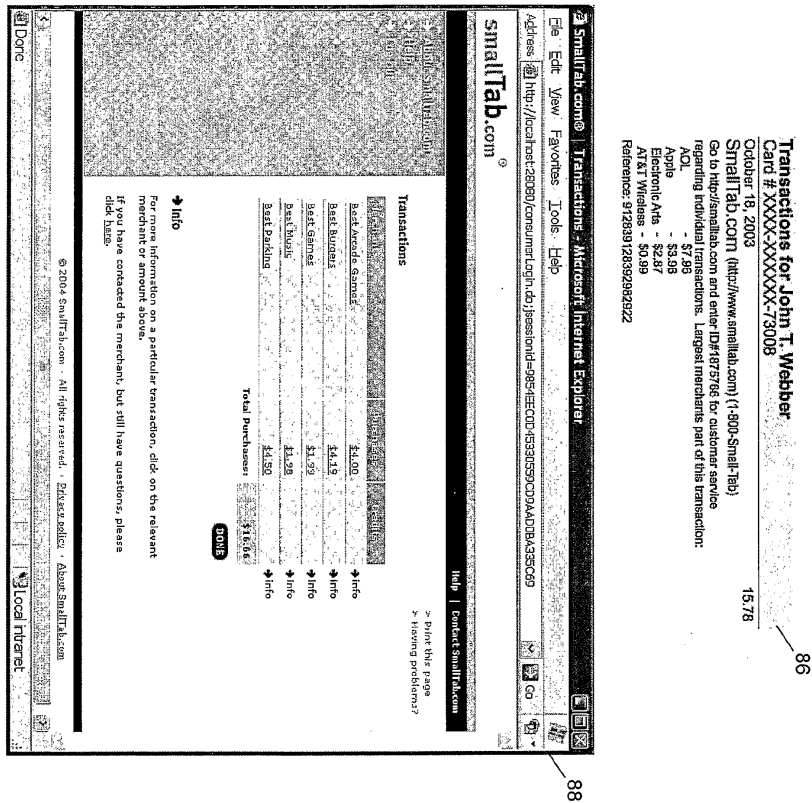
80

도면16



82

도면17



도면18

