(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0029064
(43) 공개일자 2025년03월04일

(51) 국제특허분류(Int. Cl.)
G06Q 20/38 (2012.01) *G06Q 20/20* (2012.01)
G06Q 20/32 (2012.01) *G06Q 20/36* (2012.01)
G06Q 20/40 (2012.01) *H04L 9/08* (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
G06Q 20/3829 (2013.01)
G06Q 20/202 (2013.01)
(21) 출원번호 10-2024-7042746
(22) 출원일자(국제) 2023년06월14일
심사청구일자 없음
(85) 번역문제출일자 2024년12월24일
(86) 국제출원번호 PCT/IL2023/050615
(87) 국제공개번호 WO 2023/248213
국제공개일자 2023년12월28일
(30) 우선권주장
294174 2022년06월21일 이스라엘(IL)

(71) 출원인
나약스 리미티드
이스라엘 헤르츨리야 아릭 아인슈타인 스트리트 3
(72) 발명자
벤-아비, 데이비드
이스라엘 4659071 헤르츨리야 아릭 아인슈타인 스트리트 3
로젠호이츠, 가이
이스라엘 4659071 헤르츨리야 아릭 아인슈타인 스트리트 3
(74) 대리인
특허법인(유)남아이피그룹

전체 청구항 수 : 총 17 항

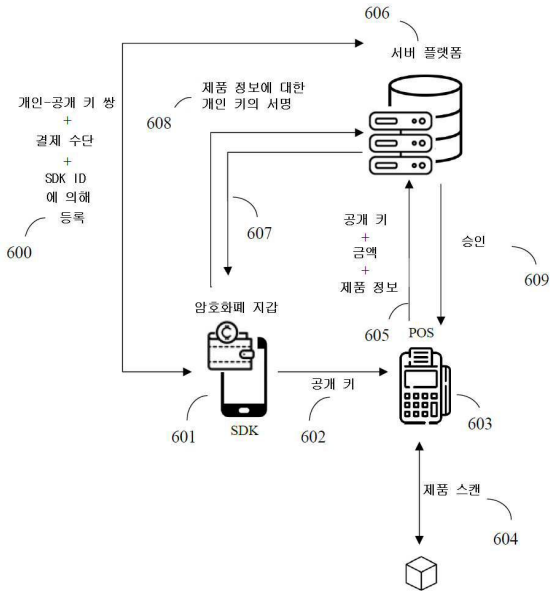
(54) 발명의 명칭 **결제 유효성을 검증하기 위한 시스템, 디바이스 및 방법**

(57) 요 약

하나 이상의 유형의(tangible) 컴퓨터-판독가능 비-일시적 저장 매체를 포함하는 결제 단말로서, 하나 이상의 유형의 컴퓨터-판독가능 비-일시적 저장 매체는 결제 유효성을 검증하기 위한 프로그램 명령들을 포함하며, 하나 이상의 프로세서들에 의한 프로그램 명령들의 실행은, 결제 단말로 하여금: 무선 디바이스에 위치한

(뒷면에 계속)

대 표 도 - 도6



SDK(software development kit)에 의해 발행된 결제 토큰을 수신하게 하고 — 결제 토큰은 고객 식별 정보 및 공개-개인 키 쌍 키들의 쌍의 제1 공개 키를 포함함 —; 트랜잭션 정보 메시지를 포함하는 결제 요청을 생성하고 상기 제1 결제 요청 메시지 및 상기 결제 토큰을 적어도 하나의 데이터베이스에 저장되도록 적어도 하나의 백-엔드 플랫폼에 송신하게 하고; 그리고 상기 적어도 하나의 백-엔드 플랫폼에 의해 생성된 결제 승인에 기반하여 상기 적어도 하나의 백-엔드 플랫폼으로부터 결제 및 트랜잭션 확인 메시지를 수신하게 하고, 상기 제1 공개 키의 소유권을 검증하는 것은 상기 서명된 트랜잭션 정보 메시지의 공개 키와 결제 토큰의 상기 공개 키의 비교에 기반하여 적어도 하나의 백-엔드 플랫폼에서 행해진다.

(52) CPC특허분류
G06Q 20/204 (2013.01)
G06Q 20/3223 (2013.01)
G06Q 20/326 (2023.05)
G06Q 20/3278 (2013.01)
G06Q 20/367 (2020.05)
G06Q 20/3825 (2013.01)
G06Q 20/3827 (2013.01)
G06Q 20/4012 (2020.05)
H04L 9/0861 (2013.01)

명 세 서

청구범위

청구항 1

무선 디바이스에 의해 실행되는, 결제 유효성(payment validity)을 검증하기 위한 방법으로서,

암호화폐 지갑(crypto wallet)에 의해 공개-개인 키 쌍(Public-Private key pair)을 생성하는 단계;

상기 공개-개인 키 쌍의 공개 키를 포함하는 결제 토큰을 생성하는 단계;

판매 지점(point of sale)의 결제 단말에 상기 결제 토큰을 송신하는 단계 – 상기 결제 단말은 상기 결제 토큰 및 결제의 트랜잭션(transaction) 정보 메시지를 포함하는 결제 요청을 생성하고 그 후 상기 결제 요청을 적어도 하나의 백-엔드 플랫폼(back-end platform)으로 송신하도록 구성됨 –;

상기 트랜잭션 정보 메시지에 기반하여 상기 적어도 하나의 백-엔드 플랫폼에 의해 트랜잭션 검증 메시지를 생성하는 단계;

상기 결제 토큰의 상기 공개 키와 연관된 디바이스에 상기 트랜잭션 검증 메시지를 제공하는 단계;

상기 공개-개인 키 쌍의 개인 키로 상기 트랜잭션 검증 메시지에 서명하고 상기 서명된 트랜잭션 검증 메시지를 상기 적어도 하나의 백-엔드 플랫폼으로 전송하는 단계;

상기 적어도 하나의 백-엔드 플랫폼에 의해, 상기 결제 단말에 의해 생성된 결제 요청 메시지 내에 포함된 상기 공개 키에 대하여 상기 무선 디바이스에 의해 서명된 상기 트랜잭션 검증 메시지의 공개 키를 비교하여, 상기 제1 공개 키의 소유권을 검증하는 단계;

적어도 하나의 금융 기관(financing entity)의 고객 플랫폼으로 상기 결제를 승인하는 단계;

상기 적어도 하나의 백-엔드 플랫폼으로부터 트랜잭션 확인 메시지를 전송함으로써, 상기 결제 단말, 무선 디바이스, 및 상기 고객 플랫폼 중 어느 하나에 상기 적어도 하나의 백-엔드 플랫폼에 의한 결제 검증 결과를 통지하는 단계를 포함하는,

결제 유효성을 검증하기 위한 방법.

청구항 2

제1 항에 있어서,

상기 결제 토큰의 상기 고객 식별 정보는, 상기 적어도 하나의 백-엔드 플랫폼 내에 저장된 난수(random number), 고객과 연관된 정보의 해시 값, 고유한 일련 번호 중 적어도 하나인,

결제 유효성을 검증하기 위한 방법.

청구항 3

제1 항에 있어서,

상기 트랜잭션 정보 메시지는 결제 금액(payment due), 제품 리스트, 판매자 ID 중 적어도 하나를 포함하는,

결제 유효성을 검증하기 위한 방법.

청구항 4

제1 항에 있어서,

상기 결제 토큰을 생성하는 단계는,

난수인 개인 키를 생성하는 단계;

상기 개인 키를 해싱함으로써 공개 키를 생성하는 단계;

고객 연락처 정보, 무선 디바이스 ID, 결제 정보, 지리적 위치(geolocation), 및 고객 ID 번호 중 적어도 하나를 포함하는 고객 식별 정보를 해싱하는 단계;

상기 고객 식별 정보의 해시 값 및 상기 공개 키를 이용하여 상기 결제 토큰을 구성하는 단계를 포함하는,

결제 유효성을 검증하기 위한 방법.

청구항 5

결제 단말로서,

상기 결제 단말은 결제 유효성을 검증하기 위한 프로그램 명령들을 포함하는 하나 이상의 유형의 컴퓨터-판독가능 비-일시적 저장 매체를 포함하고, 하나 이상의 프로세서들에 의한 상기 프로그램 명령들의 실행은 상기 결제 단말로 하여금:

무선 디바이스에 위치된 SDK(software development kit)에 의해 발행된 결제 토큰을 수신하게 하고 — 상기 결제 토큰은 암호화폐 지갑에 의해 생성된 공개-개인 키들의 쌍의 공개 키를 포함함 —;

상기 결제 토큰 및 트랜잭션 정보 메시지를 포함하는 결제 요청을 생성하게 하고, 그리고 상기 결제 요청을 적어도 하나의 백-엔드 플랫폼으로 송신하게 하고; 그리고

상기 적어도 하나의 백-엔드 폴랫폼에 의해 생성된 결제 승인에 기반하여 상기 적어도 하나의 백-엔드 플랫폼으로부터 결제 및 트랜잭션 확인 메시지를 수신하게 하고, 상기 공개 키의 소유권을 검증하는 것은, 상기 무선 디바이스의 공개-개인 키 쌍의 개인 키에 의해 서명된 트랜잭션 검증 메시지의 공개 키와 상기 결제 단말에 의해 생성된 상기 결제 요청에 포함된 공개 키의 비교에 기반하여 적어도 하나의 백-엔드 플랫폼에 의해 행해지는,

결제 단말.

청구항 6

제5 항에 있어서,

하나 이상의 프로세서들에 의해 상기 프로그램 명령들을 실행하는 것은 상기 결제 단말로 하여금:

RFID(Radio Frequency Identification) 통신, 단거리 라디오 통신 및 NFC(Near Field Communication) 중 적어도 하나를 통해 상기 결제 토큰을 수신하게 하는,

결제 단말.

청구항 7

제5 항에 있어서,

상기 결제 토큰은: 상기 적어도 하나의 백-엔드 플랫폼에 저장된 난수, 사용자와 연관된 정보의 해시 값, 고유한 일련 번호 중 적어도 하나를 포함하는 고객 식별 정보를 포함하는,

결제 단말.

청구항 8

제5 항에 있어서,

상기 트랜잭션 정보 메시지는: 결제 금액, 제품 리스트, 및 판매자 ID 중 적어도 하나를 포함하는,

결제 단말.

청구항 9

하나 이상의 유형의(tangible) 컴퓨터-판독가능 비-일시적 저장 매체를 포함하는 무선 디바이스로서,

상기 비-일시적 저장 매체에는 결제 유효성을 검증하기 위한 프로그램 명령들을 포함하는 애플리케이션이 설치되어 있고, 하나 이상의 프로세서들에 의한 상기 프로그램 명령들의 실행은:

암호화폐 지갑에 의해 공개-개인 키 쌍을 생성하는 것;

상기 공개-개인 키 쌍의 공개 키를 포함하는 결제 토큰을 생성하는 것;

상기 판매 지점의 결제 단말에 상기 결제 토큰을 송신하는 것;

상기 결제 단말로부터 트랜잭션 정보 메시지를 수신하는 것;

적어도 하나의 백-엔드 플랫폼으로부터 트랜잭션 검증 메시지를 수신하는 것;

상기 결제 단말로부터 수신된 트랜잭션 정보 메시지와, 상기 적어도 하나의 백-엔드 플랫폼에 의해 생성된 상기 트랜잭션 검증 메시지의 비교에 기반하여, 상기 공개-개인 키 쌍의 개인 키로 상기 트랜잭션 검증 메시지에 서명하고, 상기 서명된 트랜잭션 검증 메시지를 상기 적어도 하나의 백-엔드 플랫폼으로 전송하는 것; 및

상기 서명된 트랜잭션 검증 메시지의 공개 키와 상기 적어도 하나의 백-엔드 플랫폼에 의한 상기 결제 토큰의 비교에 기반하여 상기 공개 키의 소유권을 검증한 후 트랜잭션 확인을 수신하는 것을 초래하는,

무선 디바이스.

청구항 10

제9 항에 있어서,

상기 결제 토큰은: 상기 적어도 하나의 백-엔드 플랫폼에 저장된 난수, 고객과 연관된 정보의 해시 값 중 적어도 하나로 구성된 고객 식별 정보를 포함하는,

무선 디바이스.

청구항 11

제9 항에 있어서,

상기 저장 매체의 상기 프로그램 명령들은 하나 이상의 프로세서들에 의해 실행될 때:

검증될 각각의 결제 전에 결제 토큰을 생성하는 것을 초래하는,

무선 디바이스.

청구항 12

제9 항에 있어서,

상기 저장 매체의 상기 프로그램 명령들은 하나 이상의 프로세서들에 의해 실행될 때:

상기 적어도 하나의 백-엔드 플랫폼에 고객을 처음 등록할 때 개인-공개 쌍을 생성하는 것을 초래하는,

무선 디바이스.

청구항 13

제9 항에 있어서,

상기 저장 매체의 상기 프로그램 명령들은 하나 이상의 프로세서들에 의해 실행될 때:

상기 결제 토큰에서 사용하기 위해 기존의 공개-개인 키 쌍을 임포팅(importing)하는 것을 초래하는,

무선 디바이스.

청구항 14

제9 항에 있어서,

상기 저장 매체의 상기 프로그램 명령들은 하나 이상의 프로세서들에 의해 실행될 때:

상기 무선 디바이스를 잠금해제 하는 것, 상기 무선 디바이스의 지리적 위치가 결제 단말의 알려진 지리적 위치의 미리 결정된 범위 내에 있을 때, 서명될 트랜잭션이 미리 설정된 허용한도(pre-set allowance)를 초과하지 않는지 여부의 이벤트들 중 적어도 하나의 이벤트 시, 상기 트랜잭션 검증 메시지에 서명하는 것을 초래하는,

무선 디바이스.

청구항 15

제14 항에 있어서,

상기 알려진 지리적 위치의 상기 미리 결정된 범위는 상기 알려진 지리적 위치의 중심으로부터 0 내지 5미터인,

무선 디바이스.

청구항 16

제9 항에 있어서,

상기 저장 매체의 상기 프로그램 명령들은 하나 이상의 프로세서들에 의해 실행될 때:

난수인 개인 키를 생성하는 것;

상기 개인 키를 해싱함으로써 공개 키를 생성하는 것;

고객 식별 정보 해싱하는 것;

상기 고객 식별 정보의 해시 값 및 상기 공개 키를 이용하여 상기 결제 토큰을 구성하는 것을 초래하는,

무선 디바이스.

청구항 17

제10 항에 있어서,

상기 고객 식별 정보는: 고객 연락처 정보, 무선 디바이스 ID, 결제 정보, 지리적 위치, 및 고객 ID 번호 중 적어도 하나를 포함하는,

무선 디바이스.

발명의 설명

기 술 분 야

[0001] [001] 본 명세서에서 설명된 일부는 일반적으로 결제 유효성(payment validity)을 검증하기 위한 방법들, 시스템들, 및 장치에 관한 것이다. 보다 상세하게는, 본 개시내용은 금융 트랜잭션(financial transaction)들의 검증에 관한 것이다.

배 경 기 술

[0002] [002] 결제 카드들, 이를테면 예를 들어, 신용 카드들 또는 직불 카드들은 사기(fraud)에 취약하지만 고객들 및 비즈니스들 둘 모두에게 매우 이익이 된다는 것은 널리 알려져 있다.

[0003] [003] 결제 카드 소지자들을 위한 안전한 구매 환경의 형성 및 사기 방지는 20세기에 결제 카드들이 확립된 이래로 이 분야에서의 많은 노력들의 목표였다.

[0004] [004] EMV(Eourepay, Visa, Mastercard) 표준은 카드 발급자에 의한 검증을 위해 판매자 POS(point of sale)로부터 결제 카드 번호와 4-자리 PIN 번호의 안전한 송신을 통해 카드 소지자 신원의 검증을 가능하게 한다. 결제 카드 번호와 4-자리 PIN, 유효 날짜의 세부사항들이 인가되지 않은 사람에게 노출되면, 이 사람은 상품 및 서비스들을 구매하기 위해 그 신용 카드를 이용할 수 있다.

[0005] [005] 따라서, 위에 언급된 결함들을 해결하기 위한 보다 안전한 시스템 및 방법이 필요하다.

발명의 내용

[0006] [006] 결제 유효성을 검증하기 위한 시스템, 방법, 및 제품과 관련된 본 발명이 이하에서 단지 예시에 의해 설명된다.

[0007] [007] 현재 개시된 청구내용의 양상에 따르면, 본 발명은, 하나 이상의 유형의(tangible) 컴퓨터-판독가능 비-

일시적 저장 매체를 포함하는 결제 단말을 포함할 수 있고, 이 저장 매체는 결제 유효성을 검증하기 위한 프로그램 명령들을 포함하며, 하나 이상의 프로세서들에 의한 프로그램 명령들의 실행은, 결제 단말로 하여금: 무선 디바이스에 위치한 SDK(software development kit)에 의해 발행된 결제 토큰을 수신하게 하고 – 결제 토큰은 공개-개인 키 쌍(Public-Private key pair)의 공개 키를 포함함 –; 트랜잭션 정보 메시지를 포함하는 결제 요청을 생성하고 상기 결제 요청 및 상기 결제 토큰을 적어도 하나의 데이터베이스에 저장되도록 적어도 하나의 백-엔드 플랫폼(back-end platform)에 송신하게 하고; 그리고 상기 적어도 하나의 백-엔드 플랫폼에 의한 결제 승인에 기반하여 상기 적어도 하나의 백-엔드 플랫폼으로부터 결제 및 트랜잭션 확인 메시지를 수신하게 하고, 상기 공개 키의 소유권을 검증하는 것은 상기 적어도 하나의 백-엔드 플랫폼에 의한, 무선 디바이스 내의 개인 키에 의해 서명된 트랜잭션 정보 메시지의 공개 키와 결제 토큰의 상기 공개 키의 비교에 기반한다.

[0008] [008] 예를 들어, 상기 저장 매체의 상기 프로그램 명령들은: 상기 결제를 개시한 무선 디바이스에 상기 트랜잭션 정보 메시지의 해시 값을 송신하는 것을 포함하고, 트랜잭션 확인은, 무선 디바이스가 상기 트랜잭션 정보 메시지의 상기 해시 값에 대하여 트랜잭션 검증 메시지를 비교한 후에 수신된다.

[0009] [009] 예를 들어, 상기 저장 매체의 상기 프로그램 명령들은, 실행될 때, RFID(Radio Frequency Identification) 통신, 단거리 라디오 통신 및 NFC(Near Field Communication) 중 적어도 하나를 통해 상기 결제 토큰을 수신하는 것을 초래한다.

[0010] [010] 예를 들어, 상기 결제 토큰의 상기 고객 식별 정보는 상기 적어도 하나의 백-엔드 플랫폼에 저장된 난수(random number), 사용자와 연관된 정보의 해시 값, 고유한 일련 번호 중 적어도 하나를 포함한다.

[0011] [011] 예를 들어, 상기 트랜잭션 정보는 결제 금액(payment due), 제품 리스트, 및 판매자 ID 중 하나 이상을 포함한다.

[0012] [012] 일 실시예는 결제 유효성을 검증하기 위한 방법을 포함할 수 있으며, 이 방법은: 무선 디바이스에 의해 공개-개인 키 쌍을 제공하는 단계; 상기 무선 디바이스가 고객 식별 정보 및 상기 공개-개인 키 쌍의 공개 키를 포함하는 결제 토큰을 생성하는 단계; 상기 무선 디바이스가 판매 지점(point of sale)의 결제 단말에 상기 결제 토큰을 제공하는 단계; 상기 결제 단말이 결제의 트랜잭션 정보 메시지를 포함하는 제1 결제 요청 메시지를 생성하고 결제 요청 메시지 및 상기 결제 토큰을 적어도 하나의 백-엔드 플랫폼으로 송신하는 단계; 상기 트랜잭션 정보 메시지로부터 상기 적어도 하나의 백-엔드 플랫폼에 의해 트랜잭션 검증 메시지를 생성하는 단계; 상기 결제 토큰의 상기 공개 키와 연관된 디바이스에 트랜잭션 검증 메시지 제공하는 단계; 상기 공개-개인 키 쌍의 개인 키로 상기 트랜잭션 검증 메시지에 서명하고 서명된 트랜잭션 검증 메시지를 상기 적어도 하나의 백-엔드 플랫폼으로 전송하는 단계; 상기 적어도 하나의 백-엔드 플랫폼에 의해, 무선 디바이스 내의 개인 키에 의해 서명된 제2 트랜잭션 정보에 의해 제공된 제2 공개 키를 상기 제1 공개 키에 대하여 비교함으로써 상기 제1 공개 키의 소유권을 검증하는 단계; 적어도 하나의 금융 기관(financing entity)의 고객 플랫폼을 이용하여 상기 트랜잭션을 승인하는 단계; 상기 적어도 하나의 백-엔드 플랫폼이 상기 적어도 하나의 백-엔드 플랫폼으로부터 트랜잭션 확인 메시지를 전송함으로써, 상기 결제 단말, 무선 디바이스, 및 상기 고객 플랫폼에 결제 검증 결과를 통지하는 단계를 포함한다.

[0013] [013] 예를 들어, 상기 결제 토큰의 상기 고객 식별 정보는, 상기 적어도 하나의 백-엔드 플랫폼에 저장된 난수, 사용자와 연관된 정보의 해시 값, 고유한 일련 번호 중 적어도 하나이다.

[0014] [014] 예를 들어, 상기 트랜잭션 정보는 결제 금액, 제품 리스트, 판매자 ID 중 하나 이상을 포함한다.

[0015] [015] 예를 들어, 상기 결제 토큰은: 난수인 개인 키를 생성하는 것; 상기 개인 키를 해싱하여 공개 키를 생성하는 것; 고객 연락처 정보, 무선 디바이스 ID, 결제 정보, 지리적 위치(geolocation), 및 고객 ID 번호 중 적어도 하나를 포함하는 고객 식별 정보를 해싱하는 것; 상기 공개 키와 소비자 식별 정보의 해시 값을 이용하여 상기 결제 토큰을 구성하는 것에 의해 생성된다.

[0016] [016] 다른 하나의 실시예는 하나 이상의 유형의 컴퓨터-판독가능 비-일시적 저장 매체를 포함하는 무선 디바이스를 포함할 수 있으며, 이 저장 매체에는 결제 유효성을 검증하기 위한 프로그램 명령들을 포함하는 애플리케이션이 설치되어 있고, 하나 이상의 프로세서들에 의한 프로그램 명령들의 실행은: 공개-개인 키 쌍을 제공하는 것; 상기 공개-개인 키 쌍의 공개 키를 포함하는 결제 토큰을 생성하는 것; 상기 판매 지점의 결제 단말에 상기 결제 토큰을 제공하는 것; 상기 결제 단말로부터 트랜잭션 정보 메시지를 수신하는 것; 적어도 하나의 백-엔드 플랫폼으로부터 트랜잭션 검증 메시지를 수신하는 것; 트랜잭션 검증 메시지와 트랜잭션 정보 메시지의 비교에 기반하여, 상기 공개-개인 키 쌍의 개인 키로 상기 트랜잭션 검증 메시지에 서명하고, 이를 상기 적어도 하나의

백-엔드 플랫폼으로 전송하는 것; 서명된 트랜잭션 메시지의 공개 키와 상기 결제 토큰의 비교에 기반하여 상기 공개 키의 소유권을 검증한 후 트랜잭션 확인을 수신하는 것을 초래하고, 상기 트랜잭션 확인은 적어도 하나의 금융 기관의 고객 플랫폼으로 상기 트랜잭션을 승인한 후 수신된다.

[0017] [017] 예를 들어, 상기 결제 토큰은 고객 식별 정보를 포함하고, 고객 식별 정보는 상기 적어도 하나의 백-엔드 플랫폼에 저장된 난수, 사용자와 연관된 정보의 해시 값 중 적어도 하나를 포함한다.

[0018] [018] 예를 들어, 상기 저장 매체의 상기 프로그램 명령들은, 실행될 때, 검증될 각각의 결제 전에 결제 토큰을 생성하는 것을 초래한다.

[0019] [019] 예를 들어, 상기 저장 매체의 상기 프로그램 명령들은, 실행될 때, 상기 적어도 하나의 백-엔드 플랫폼에 고객이 처음 등록할 때 개인-공개 쌍을 생성하는 것을 초래한다.

[0020] [020] 예를 들어, 상기 저장 매체의 상기 프로그램 명령들은, 실행될 때, 상기 결제 토큰에서 사용하기 위해 기존의 공개-개인 키 쌍을 임포팅(importing)하는 것을 초래한다.

[0021] [021] 예를 들어, 상기 저장 매체의 상기 프로그램 명령들은, 실행될 때: 상기 무선 디바이스를 잠금해제하는 것, 상기 무선 디바이스의 지리적 위치가 결제 단말의 지리적 위치와 유사한 때, 및 서명될 트랜잭션이 미리 설정된 금액 허용한도(pre-set money allowance)를 초과하지 않음 중 적어도 하나의 이벤트시, 상기 트랜잭션 검증 메시지에 서명하는 것을 초래한다.

[0022] [022] 예를 들어, 상기 저장 매체의 상기 프로그램 명령들은, 실행될 때: 난수인 개인 키를 생성하는 것; 상기 개인 키를 해싱하여 공개 키를 생성하는 것; 고객 연락처 정보, 무선 디바이스 ID, 결제 정보, 지리적 위치, 및 고객 ID 번호 중 적어도 하나를 포함하는 고객 식별 정보를 해싱하는 것; 고객 식별 정보의 해시 값 및 상기 공개 키를 이용하여 상기 결제 토큰을 구성하는 것의 결과를 가져온다.

[0023] [023] 본 발명의 다양한 목적들, 피처들, 및 양상들은 본 발명의 바람직한 실시예들에 대한 이하의 상세한 설명과 첨부 도면들에서 더욱 명확해질 것이며, 도면들에서 유사한 번호들은 유사한 구성요소들을 나타낸다.

도면의 간단한 설명

[0024] [024] 본 명세서에 개시된 청구대상을 더 잘 이해하고 실제로 이것이 수행될 수 있는 방법을 예시하기 위해, 이제 첨부 도면들을 참조하여, 단지 제한적이지 않은 예로서, 실시예들이 설명될 것이며, 도면들에서:

[025] 도 1은 일부 예시적인 실시예들에 따른, 결제 유효성을 검증하기 위한 시스템의 블록도를 예시한다.

[026] 도 2는 일부 예시적인 실시예들에 따른, 결제 유효성을 검증하기 위한 방법의 흐름도를 예시한다.

[027] 도 3은 일부 예시적인 실시예들에 따른, 결제 유효성을 검증하기 위한 방법의 흐름도를 예시한다.

[028] 도 4는 일부 예시적인 실시예들에 따른, 결제 유효성을 검증하기 위한 방법의 흐름도를 예시한다.

[029] 도 5는 일부 예시적인 실시예들에 따른 제조 제품을 예시한다.

[030] 도 6은 일부 예시적인 실시예들에 따른, 결제 유효성을 검증하기 위한 시스템의 블록도를 예시한다.

발명을 실시하기 위한 구체적인 내용

[0025] [031] 다음의 상세한 설명에서는, 일부 실시예의 철저한 이해를 제공하기 위해 다양한 특정 세부사항들이 설명된다. 그러나, 일부 실시예들이 이러한 특정 세부사항들 없이도 실시될 수 있음이 당업자들에 의해 이해될 것이다. 다른 경우들에 있어서, 논의를 모호하게 하지 않기 위해 공지된 방법들, 절차들, 구성 요소들, 유닛들 및/또는 회로들은 상세히 설명되지 않았다.

[0026] [032] 예를 들어, "프로세싱", "컴퓨팅", "계산", "결정", "확립", "분석", "검사" 등과 같은 용어들을 이용하여 본 명세서에서 이루어진 논의들은 컴퓨터의 레지스터들 및/또는 메모리들 내의 물리적(예를 들어, 전자적) 수량들로 표현되는 데이터를 컴퓨터의 레지스터들 및/또는 메모리들 또는 동작들 및/또는 프로세스들을 수행하기 위한 명령들을 저장할 수 있는 다른 정보 저장 매체 내의 물리량들로서 유사하게 표현되는 다른 데이터로 조작 및/또는 변환하는 컴퓨터, 컴퓨팅 플랫폼, 컴퓨팅 시스템 또는 다른 전자 컴퓨팅 디바이스들의 동작(들) 및/또는 프로세스(들)를 지칭할 수 있다.

[0027] [033] 본 명세서에서 사용되는 바와 같이, 용어들 "복수"("plurality" and "a plurality")는, 예를 들어, "다

수" 또는 "2개 이상"을 포함한다. 예를 들어, "복수의 항목들"은 2개 이상의 항목들을 포함한다.

[0028] [034] "일 실시예", "실시예", "예시적인 실시예", "다양한 실시예들" 등에 대한 지칭들은 그렇게 설명된 실시예(들)가 특정의 특징, 구조 또는 특성을 포함할 수 있음을 나타내지만, 모든 실시예가 반드시 특정의 특징, 구조 또는 특성을 포함한다는 것을 나타내지는 않는다. 추가로, "일 실시예에서"라는 문구의 반복된 사용은, 동일한 실시예를 지칭할 수도 있지만, 반드시 동일한 실시예를 지칭하는 것은 아니다.

[0029] [035] 본 명세서에서 사용되는 바와 같이, 달리 명시되지 않는 한, 공통 객체를 설명하기 위한 서수 형용사들 "제1", "제2", "제3" 등의 사용은 단지 유사한 객체들의 상이한 예들이 지칭되고 있음을 나타낼 뿐이며, 이렇게 설명된 객체들이 시간적, 공간적, 순위적 또는 임의의 다른 방식으로 주어진 순서를 따라야 함을 의미하도록 의도된 것은 아니다.

[0030] [036] 본 명세서에서 사용되는 "회로"라는 용어는 ASIC(Application Specific Integrated Circuit), 집적 회로, 전자 회로, 프로세서(공유, 전용 또는 그룹) 및/또는 설명된 기능을 제공하는 하나 이상의 소프트웨어 또는 펌웨어 프로그램들, 조합 논리 회로 및/또는 다른 적절한 하드웨어 구성 요소들을 실행하는 메모리(공유, 전용 또는 그룹)를 지칭하거나, 그 일부이거나, 이를 포함할 수 있다. 일부 예시적인 실시예들에서, 회로는 하나 이상의 소프트웨어 또는 펌웨어 모듈에 구현될 수 있거나 회로와 연관된 기능들이 하나 이상의 소프트웨어 또는 펌웨어 모듈들에 의해 구현될 수 있다. 일부 예시적인 실시예들에서, 회로는 하드웨어에서 적어도 부분적으로 동작 가능한 논리를 포함할 수 있다.

[0031] [037] "로직"이라는 용어는, 예를 들어, 컴퓨팅 장치의 회로부에 임베딩된 컴퓨팅 로직 및/또는 컴퓨팅 장치의 메모리에 저장된 컴퓨팅 로직을 지칭할 수 있다. 예를 들어, 로직은 컴퓨팅 기능들 및/또는 동작들을 수행하기 위해 컴퓨팅 로직을 실행하도록 컴퓨팅 장치의 프로세서에 의해 액세스가능할 수 있다. 일 예에서, 로직은 다양한 유형들의 메모리 및/또는 펌웨어, 예컨대, 다양한 칩들 및/또는 프로세서들의 실리콘 블록들에 임베딩될 수 있다. 로직은 다양한 회로, 예를 들어, 무선 회로, 수신기 회로, 제어 회로, 송신기 회로, 트랜시버 회로, 프로세서 회로 등에 포함되거나 그 일부로서 구현될 수 있다. 일 예에서, 로직은 랜덤 액세스 메모리, 판독-전용 메모리, 프로그래밍 가능 메모리, 자기 메모리, 플래시 메모리, 영구 메모리 등을 포함하는 휘발성 메모리 및/또는 비휘발성 메모리에 내장될 수 있다. 로직은, 예컨대 로직을 실행하기 위해 필요에 따라, 하나 이상의 프로세서들에 결합된 메모리, 예컨대 레지스터들, 스택(stuck), 버퍼들 등을 사용하여 하나 이상의 프로세서들에 의해 실행될 수 있다.

[0032] [038] 이하에서 사용되는 "모듈"이라는 용어는 실행 중인 커널 환경을 확장하기 위한 코드를 포함하는 오브젝트 파일이다.

[0033] [039] 본 명세서에서 사용되는 바와 같이, 이하에서 사용되는 "소프트웨어 엔진"이라는 용어는 실행 중인 커널 환경을 확장하기 위한 코드를 포함하는 오브젝트 파일이다.

[0034] [040] 이하에서 사용되는 "디지털 지갑"이라는 용어는 소프트웨어 및 정보 구성 요소 모두이다. 디지털 지갑들은 클라이언트-측 상에 저장될 수 있다. 디지털 지갑들은 예를 들어, 스마트폰들의 NFC(Near Field Communication)를 사용하여 스마트폰을 터치함으로써 상점의 결제 단말에 결제를 전송할 수 있다.

[0035] [041] 이하에서 사용되는 "로열티 클럽 고객"이라는 용어는 로열티 클럽을 제공하고 로열티-기반 모바일 서비스, 예를 들어, 그의 고객 기반을 위한 로열티 카드 애플리케이션을 운영하는 B2B(business to business) 고객이다.

[0036] [042] 이하에서 사용되는 "백-엔드 플랫폼"이라는 용어는 디지털 지갑 서비스들을 관리 및 제어하고 선택된 제3자 시스템들 및 디지털 지갑 모듈 및/또는 디지털 지갑 엔진 및/또는 디지털 지갑 SDK와 상호 작용하도록 구성된 디지털 지갑 시스템의 클라우드 플랫폼, 백-엔드 서버이다.

[0037] [043] 이하에서 사용되는 "디지털 지갑 SDK"라는 용어는 디지털 지갑 모듈 및/또는 디지털 지갑 엔진을 포함할 수 있다. 디지털 지갑 SDK는 맞춤형 모바일 애플리케이션에 내에 상주하고 통합된 디지털 지갑 소프트웨어 프로그램의 프론트-엔드(front-end)이다. 디지털 지갑 SDK는 고객의 모바일 애플리케이션을 통해 최종-사용자의 프론트-엔드 결제 상호작용을 관리할 수 있다. 디지털 지갑 SDK는 디지털 지갑 플랫폼을 대신하여 벤더 POS의 POS 단말과 통신하기 위해 NFC 프로토콜을 사용할 수 있다.

[0038] [044] 이하에서 사용되는 "CRM(customer relationship manager) API(application programming interface)"라는 용어는 CRM과 통신하도록 구성된 API이다. CRM은 하나 이상의 고객 리워드 프로그램들을 관리하도록 구성된

다.

[0039] [045] 이하에서 사용되는 "결제 단말"이라는 용어는 예를 들어, 최종-사용자가 고객 모바일 애플리케이션을 사용하여 결제 트랜잭션을 소비하기로 결정한 때 다양한 결제 트랜잭션들이 이루어질 수 있는 특정 판매자 및/또는 벤더 및/또는 샵 등의 신용 카드 단말을 포함할 수 있다.

[0040] [046] 이하에서 사용되는 바와 같은 "고객 플랫폼"이라는 용어는 예를 들어, 디지털 지갑 플랫폼을 통한 결제들의 제공을 위해 디지털 지갑과 연계하도록 구성된 파트너 고객의 기술 플랫폼을 포함할 수 있다. 백-엔드 기술 플랫폼은 고객 및/또는 파트너가 선택한 결제 구성에 따라 디지털 지갑 SDK뿐만 아니라 고객 모바일 애플리케이션과도 통신한다. 예를 들어, 이 플랫폼은 클라우드 기반으로, 예를 들어 Amazon Web Services(AWS) 및/또는 Microsoft AZURE에서 실행될 것이다.

[0041] [047] 이하에서 사용된 바와 같은 "암호화폐 지갑 모듈(cryptowallet module)"이라는 용어는 공개 키로부터 생성된 개개의 암호화폐 지갑 어드레스와 함께 랜덤 개인-공개 키 쌍들을 생성하고 저장하도록 구성된 애플리케이션 또는 SDK를 지칭할 수 있다. 암호화폐 지갑 모듈은 Ethereum 블록체인 및 Bitcoin, Solana, Cardano, Polkadot, Avalanche 등과 같은 다른 유사한 블록체인 네트워크들과 같은 적어도 하나의 블록체인 네트워크와 상호작용하도록 추가로 구성될 수 있다.

[0042] [048] "해시 값"이라는 용어는, 임의의 길이의 입력을 받아서 이를 고정된 길이로 변환하는 수학적 함수의 출력을 지칭하며, 따라서 입력에 무시할 만한 차이가 있더라도 출력에 대해 완전히 상이한 해시 값이 초래되지만 동일한 입력에 해시 함수를 적용하는 것은 항상 동일한 해시 값을 초래한다. 해시 값들은 메시지들의 내용을 검증하는 데 사용된다. 내용이 변경될 때, 새 메시지의 해시 값은 오리지널 메시지와 상이하게 될 것이다.

[0043] [049] 이하에서 사용되는 바와 같이, "결제 토큰"이라는 용어는, 예를 들어 Rivest-Shamir-Adleman - 'RSA' 알고리즘과 같은 알려진 공개-개인 알고리즘들로 암호화된 사용자를 고유하게 식별하는 정보를 포함하도록 구성된, 결제 토큰으로 불리는 고유한 플레이스홀더를 포함할 수 있다.

[0044] [050] 일부 실시예들에서, 결제 토큰은 사용자가 소유한 블록체인 네트워크 상의 어드레스를 나타내는 공개 키 및 예를 들어, 이름, 연락처 정보, 모바일 디바이스 메타데이터, 시간, 지리적 위치 데이터 등과 같은 기타 식별 정보로 구성될 수 있다.

[0045] [051] 예를 들어, 사용자의 고유 식별가능 정보가 다음을 포함하는 간단한 JSON 포맷으로 파싱(parsing)되면:

[0046] [052] {"address" : "0xb794f5ea0ba39494ce839613fffba74279579268", "name" = "John Smith"}, 결제 토큰은 이하의 암호화된 스트링을 포함할 수 있다.

[0047] [053]NjX1HoGdktQHFF5hJ0Psy+SJmOhCTEgcYFVvpJCwuoR6TDQjmTMJI6G+/lCf2mWYswjCz/6pSW/90EQmzp6Xiv4x8maycBsVwNIPa2t4dcWAGK0D9n5mkUaA2tz+pk1FrOYq4ttrLZc7pNzCaDpcNyOa8ZEnwAA7TSqNfsvqXfw=.

[0048] [054] 다른 예시적인 구현에서, 식별가능한 정보만 암호화되고 공개 어드레스는 JSON 파일에서 있는 그대로 파싱된다. 여기서, 식별 스트링은: "name : John Smith"이고, JSON 파일은 다음과 같이 판독될 것이다:

[0049] [055] {"address":"0xb794f5ea0ba39494ce839613fffba74279579268", "idInfo":"XFftAh5RGXtlzJ622+vrg2nUBozV97KdyHRL300xBIGdiCRzf4h+bsxbYGFqCxHzLp4HidpJAc3PvzjPwE1AuQ=="}

[0050] [056] 위의 내용은 본 명세서에서 사용된 용어를 명확히 하기 위한 예일 뿐이다. 실제로, 결제 토큰의 해시된 부분이 각각의 사용에서 고유하게 유지되는 것을 보장하기 위해, 백-엔드 플랫폼의 데이터베이스에 또한 저장되는 일회용 난수를 포함하여, 부가적인 파라미터들이 결제 토큰에 포함될 수 있다.

[0051] [057] 이하에서 사용되는 바와 같은 "모바일 애플리케이션"이라는 용어는 고객의 무선 디바이스 상에 설치된 적어도 하나의 애플리케이션, 예를 들어, 로열티 클럽 애플리케이션, 전자-지갑 애플리케이션 등을 포함할 수 있다. 고객 애플리케이션은 디지털 지갑 SDK를 포함할 수 있고, 디지털 지갑 플랫폼 및 고객 플랫폼과 상호작용할 수 있다. 고객 모바일 애플리케이션은 예를 들어 iOS 및/또는 Android와 무선 디바이스 운영 시스템에서 실행되도록 구성될 수 있다.

[0052] [058] 일부 예시적인 실시예들은 web3 생태계 개념 및 블록체인 기술을 기반으로 구축될 수 있다. 예를 들어, web3 생태계 개념 및 블록체인 기술은 안전하고 투명하고, 그리고 탈중앙화된(decentralized) 결제 시스템을 확립한다. 블록체인의 사용은 고객들 및 기업들로 하여금 중개자(intermediary)들 없이 암호화폐 지갑들을 통해 예를 들어, Bitcoin, 및 Ethereum과 같은 암호화폐를 직접 교환할 수 있게 한다. 결제는 검증되고 익명으로,

분산 원장(distributed ledger)에 등록되며, 예를 들어, 그 사본이 암호화폐 지갑 상에 저장될 수 있다.

[0053] [059] 예를 들어, 암호화폐 지갑과 그 자금의 소유권 검증은 개인-공개 키들을 사용하여 달성될 수 있고, 기본 가정은 암호화폐 지갑의 소유자만이 개인 키에 대한 액세스를 가질 수 있어서, 공개 키를 고유 지갑 식별자로서 사용할 수 있게 한다는 것이다.

[0054] [060] Bitcoin 블록체인이 처음 구현된 지 10년이 넘었지만, 이 기술은 고객 결제 방법으로 채택되는 데 어려움을 겪고 있으며 대부분 투기적 투자 채널로 남아 있다.

[0055] [061] 블록체인 기술 및 암호화폐가 전통적인 중앙화된 결제 수단 및 법정 통화(legal tender)에 대한 실행 가능한 대안이 되는 목적을 왜 아직까지 달성하지 못하고 있는지에는 많은 이유들이 존재한다.

[0056] [062] 예를 들어, 그러한 이유 중 일부는 블록체인 설계에 내재된 에너지 비효율성들과 관련이 있다. 다른 이유는 자금 세탁 활동들을 위한 플랫폼이 되는 트랜잭션들의 익명성과 관련이 있고, 또 다른 이유는 트랜잭션 검증자들에게 부과되는 높은 트랜잭션 수수료(fee)들과 관련이 있다.

[0057] [063] 본 개시내용의 실시예들은 민감한 신용 카드 정보의 전달을 처리하기 위한 복잡한 표준들의 사용을 피하는, 결제 유효성을 검증하기 위한 시스템들, 장치들, 및 방법들과 관련될 수 있다. 예를 들어, 민감한 신용 카드 번호들을 송신하거나 사용하는 대신, 공개 키들을 프로세싱하고 소유권 및 결제들을 검증하도록 구성된 판매 시점 단말들과 함께 암호화 공개-개인 키 인증을 사용하는 것은, 비용절감 및 더욱 단순한 시스템들에 이르게 할 수 있는데, 그 이유는 민감한 신용 카드 정보의 전달을 처리하는 복잡한 표준들(예컨대, EMV)의 사용이 이제 회피될 수 있기 때문이다.

[0058] [064] 다른 실시예들은 공개 고유 고객 식별자의 소유권 검증을 가능하게 하는 시스템들, 장치들, 및 방법들과 관련될 수 있다. 예를 들어, 공개-개인 암호화의 특성으로 인해, 소유권을 증명하기 위해 신용 카드 번호, 유효 기간, CVC 숫자들, 및 4-자리 PIN과 같은 민감한 비밀 정보를 송신할 이유가 없다. 대신, 공개 키는 부가 정보와 함께 송신될 수 있지만, 본 개시내용은 고객으로 하여금 송신된 공개 키의 소유권을 증명할 수 있게 하는 장치들, 시스템들, 및 방법들을 소개한다.

[0059] [065] 그러나, 일부 실시예들은 또한 블록체인-관련 수수료 비용들 없이 암호화폐 지갑들 기반의 결제 검증을 가능하게 하도록 구성될 수 있다. 블록체인 기반 결제들은 안전하다고 여겨질 수 있지만, 결제 검증 목적들로 각각의 결제를 공개 분산 원장에 레코딩해야 한다는 것이 비효율적으로 여겨질 수 있다. 본 개시내용을 이용하면, 블록체인 네트워크 클라이언트들로서 이미 암호화폐 지갑들에 대한 액세스를 갖는 많은 대중은 그들의 암호화폐 지갑들을 사용하여 상품 및 서비스들을 살 수 있지만, 암호화폐 트랜잭션들과 연관된 수수료들이 전혀 없으며 프라이버시 우려들도 없는데, 이들의 구매가 분산 공개 원장에 공개되지 않을 것이기 때문이다.

[0060] [066] 유리하게도, 디바이스들 및 그 안의 시스템들의 구성은 사용자에게 단일 액션만을 요구하면서도 다중-요소 인증에서 결제 계좌의 소유권을 인증할 수 있게 한다.

[0061] [067] 예를 들어, 사용자가 체크아웃(checkout)시 자신의 스마트폰의 NFC(Near Field Communication) 칩을 결제 단말 디바이스에 가까이 가져갈 때, 그는 단일 액션을 수행한다. SDK(Software Development Kit)를 포함하는 애플리케이션은 사용자를 나타내는 공개 키를 갖는 결제 토큰을 결제 단말로 전송해야 하며, 이 결제 토큰은 체크아웃 정보와 함께 결제 단말로부터 서버로 중계(relay)될 것이다. 수신된 결제 토큰 및 사용자 데이터베이스 내의 공개 키를 교차 참조하여 이를 사용자와 연관시킨 후, 서버는 사용자와 미리 연동된(pre-associated) 스마트폰으로 트랜잭션 정보를 중계할 수 있다.

[0062] [068] 사전 설정된 컨디션들이 실현되면(예컨대, 스마트폰 화면이 잠금해제되고, 스마트폰의 지리적 위치가 결제 단말과 유사하면), SDK는 공개 키에 대응하는 개인 키를 사용하여 이전에 수신된 트랜잭션 메시지에 서명해야 하고, 서명된 트랜잭션 메시지를 서버로 다시 반환해야 한다. 그런 다음 서버는 수신된 서명된 메시지를 복호화(decrypt)할 수 있고, 서명된 메시지의 다수의 파라미터들을 데이터베이스 엔트리와 비교할 수 있다. 다수의 파라미터들은 다음 중 적어도 하나를 포함할 수 있다: 서명된 메시지로부터 유도된 공개 키 및 결제 토큰과 함께 이전에 수신된 공개 키; 서명된 메시지의 내용 및 결제 단말로부터 수신된 트랜잭션 정보; 결제 단말로부터 수신된 결제 토큰의 사용자 정보 및 최초 등록시 수집된 사용자 정보.

[0063] [069] 알 수 있듯이, 사용자는 단일 액션만을 수행하도록 요구되었지만, 두 가지 상이한 관점들로부터 공개-개인 인증의 특성들을 활용한 다중-요소 인증에서 사용자의 신원 및 트랜잭션이 검증되었다. 제1 관점은 결제 토큰의 공개 키들을 등록 동안 제공된 공개 키와 비교할 때이다. 제2 관점은 결제 토큰 공개 키를 대응하는 개인

키에 의해 서명된 메시지와 비교할 때이다.

[0064] [070] 본 발명의 예시적인 실시예를 도시한 도 1을 먼저 참조하면, 결제 유효성을 검증하기 위한 시스템(10)이 도시된다. 시스템(10)은 적어도 하나의 고객 무선 디바이스(100), 백-엔드 플랫폼(110), 적어도 하나의 결제 단말(120), 및 금융 기관(130)의 고객 플랫폼(131)을 포함할 수 있다.

[0065] [071] 일부 예시적인 실시예들에서, 무선 디바이스(100)는 프로세서(101), NFC 통신 스위트(102), 인터넷 모뎀(103), 암호화폐 지갑 애플리케이션(104), 디지털 지갑 SDK(105), 결제 토큰 저장 모듈(106)을 포함할 수 있다. 프로세서(101)는 암호화폐 지갑 모듈(104) 및 디지털 지갑 SDK(105)을 포함할 수 있는 모바일 애플리케이션(107) 중 적어도 하나를 실행하도록 구성될 수 있다. 모바일 애플리케이션(107)은 예를 들어 Ethereum 블록체인과 같은 블록체인 네트워크와 상호작용하도록 구성될 수 있다.

[0066] [072] 일부 예시적 실시예들에서, 암호화폐 지갑(104)은 적어도 하나의 공개-개인 키 쌍들(108)을 포함할 수 있고, 결제 토큰 저장 모듈(106)은 적어도 하나의 결제 토큰(109)을 포함한다.

[0067] [073] 일부 예시적 실시예들에서, 인터넷 모뎀(103)은 60Ghz, 5G, 6G, WiFi, 셀룰러 통신 프로토콜들 중 어느 하나, IEEE 811 프로토콜들 중 어느 하나 등과 같은 일반적인 무선 통신 프로토콜들을 사용할 수 있다.

[0068] [074] 일부 예시적 실시예들에서, 판매자 POS의 결제 단말(120)은 예를 들어, 프로세싱 회로부(121), NFC 통신 스위트(122), 인터넷 모뎀(123), 적어도 하나의 결제 요청 메시지(126)를 생성하기 위한 트랜잭션 생성기 모듈(124), 및 결제 토큰 트랜시버 모듈(125)을 포함할 수 있다.

[0069] [075] 예를 들어, 프로세싱 회로부(121)는 결제 토큰 트랜시버 모듈(125), 및 트랜잭션 생성기 모듈(124)을 포함하는 애플리케이션을 실행하도록 구성될 수 있다.

[0070] [076] 결제 단말(120)은 백-엔드 플랫폼(110) 및 고객 무선 디바이스(100)와 디지털 통신할 수 있다.

[0071] [077] 예를 들어, 백-엔드 플랫폼(110)은 하나 이상의 결제 단말들(120), 고객 무선 디바이스들(100), 및 다양한 금융 기관들(130)의 고객 플랫폼(131)과 디지털 통신할 수 있다. 백-엔드 플랫폼(110)은 트랜잭션 데이터베이스(111), 메시지 생성기 모듈(112), 고객 데이터베이스(116) 프로세싱 회로부(도시되지 않음)를 포함할 수 있으며, 이 프로세싱 회로부는 결제 토큰 복호화 모듈(113), 메시지 서명 복호화 모듈(114), 및 트랜잭션 검증 모듈(115)의 기능들을 수행하도록 구성될 수 있다.

[0072] [078] 도 2를 참조하면, 일부 실시예들의 예시적인 구현이 다음 방법으로부터 이해될 것이다. 명확성을 위해, 구조적 컴포넌트들은 도 1에 참조번호들로 참조되지만, 이 방법은 본 발명의 다른 실시예들로 수행될 수 있다.

[0073] [079] 결제 유효성을 검증하기 위한 방법은: 예를 들어, 고객 무선 디바이스(100) 상에 설치된 모바일 애플리케이션(107)을 사용하여 공개-개인 키 쌍(108)(텍스트 박스(201))을 제공하는 단계를 포함할 수 있다.

[0074] [080] 일부 예시적인 실시예들에서, 사용자가 모바일 애플리케이션에 서명하면, 커맨드가 암호화폐 지갑 모듈(104)에 전달되며, 이 모듈은 공개 키와 개인 키를 포함할 수 있는 공개-개인 키 쌍 (108)(도 1)을 생성하도록 구성될 수 있다. 일부 실시예들에서, 공개-개인 키 쌍(108)(도 1)의 공개 키는 적어도 하나의 블록체인 네트워크를 준수하는 프로세스에서 암호화폐 지갑 어드레스를 생성하는 데 사용될 수 있다.

[0075] [081] 일부 다른 예시적인 실시예들에서, 공개-개인 키 쌍(108)(도 1)이 각각의 결제를 검증하기 전에 생성될 수 있다. 또 다른 실시예들에서, 사용자가 모바일 애플리케이션(107)에 처음 등록할 때 공개-개인 키 쌍(108)이 생성될 수 있다. 다른 실시예들에서, 사용자는 기존의 공개-개인 키 쌍을 암호화폐 지갑 모듈(104)(도 1)로 임포팅할 수 있다.

[0076] [082] 일부 예시적인 실시예들에서, 방법은 고객 무선 디바이스(100)(도 1)에 설치될 수 있는 모바일 애플리케이션(107)(도 1)에 의한 결제 유효성 검증(텍스트 박스(202))을 위해 결제 토큰(109)을 생성하는 단계로 진행될 수 있다. 일부 실시예들에서, 공개 키 및/또는 암호화폐 지갑 어드레스 및/또는 임의의 다른 사용자 식별 정보는 결제 토큰을 생성하기 위해 결제 단말(120)(도 1)로 전달될 수 있다.

[0077] [083] 일부 예시적인 실시예들에서, 결제 토큰(109)(도 1)은 고객 무선 디바이스와 연관된 사용자 ID 및 공개 키를 포함한다.

[0078] [084] 다른 예시적인 실시예들에서, 결제 토큰(109)(도 1)은 디지털 지갑 SDK(105)(도 1)에 의해 생성될 수 있

으며 결제 토큰 저장 데이터베이스(106)(도 1) 내에 저장될 수 있다.

[0079] [085] 일부 실시예들에서, 디지털 지갑 SDK(105)(도 1)는 암호화폐 지갑 모듈(104)(도 1)로부터 공개-개인 키 쌍(108)(도 1)의 공개 키를 리트리브(retrieve)하고 그후, 이를 이용하여 결제 토큰(109)(도 1)을 생성할 수 있다. 이 실시예에서, 공개-개인 키 쌍 108(도 1)의 개인 키는 고객 무선 디바이스(100)(도 1) 상의 데이터베이스 내에 안전하게 저장된 상태로 유지될 수 있으며, 공개-개인 키 쌍(108)(도 1)의 공개 키는 나중에 백-엔드 플랫폼(110)(도 1) 상의 고객 데이터베이스(116)(도 1), 및 결제 단말(120)(도 1) 상에 포워딩되어 저장될 수 있다.

[0080] [086] 일부 예시적인 실시예들에서, 방법은 고객 무선 디바이스(100)(도 1)의 결제 토큰(109)(도 1)을 결제 단말(120)(도 1)에 제공하는 단계로 진행될 수 있다(텍스트 박스(203)). 일부 실시예들에서, 결제 토큰은 다음 중 적어도 하나를 통해 고객 무선 디바이스(100)(도 1)로부터 결제 단말(120)(도 1)로 전송될 수 있다: NFC 라디오(102)(도 1) 및/또는 인터넷 모뎀(103)(도 1)(예컨대, LTE, GSM, WIFI, 블루투스 라디오).

[0081] [087] 일부 예시적인 실시예들에서, 방법은 트랜잭션 정보를 제공하는 단계(텍스트 박스(204))로 진행될 수 있다. 예를 들어, 결제 단말(120)(도 1)의 프로세싱 회로부(121)(도 1)는 결제 요청(126)(도 1)을 생성하도록 구성될 수 있으며, 이 결제 요청은 예를 들어, 결제 금액, 제품 리스트, 및/또는 판매자 ID와 같은 트랜잭션 정보 메시지 및 결제 토큰(109)(도 1)을 포함할 수 있다. 결제 요청(126)은 인터넷 모뎀(123)(도 1)을 통해 고객 무선 디바이스(100)에 의해 제공되는 백-엔드 플랫폼(110)(도 1)으로 전송될 수 있다.

[0082] [088] 다음은 예시적인 예이다: 제품들을 스캐닝할 때, 이들의 가격 및 다른 정보가 결제 단말(120)(도 1)에 의해 페치된다. 결제 요청과 관련된 정보는 고객이 자신의 무선 디바이스(100)(도 1)를 결제 단말(120)(도 1)에 어태치 및/또는 더 가까이 가져가고, NFC 통신을 통해 자신의 결제 토큰(109)(도 1)을 결제 단말(120)(도 1)에 제공한 후에, 결제 단말(120)(도 1)에 디스플레이될 수 있다. 결제 단말(120)(도 1)은 트랜잭션 정보 메시지를 포함하는 결제 요청(126)(도 1)을 요약하여 제공할 수 있다. 예를 들어, 트랜잭션 정보는 결제 금액, 판매자 ID를 포함할 수 있다. 일부 실시예들에서, 결제 단말(120)(도 1)은 메시지에 서명하기 전에 검증을 위해 트랜잭션 정보 메시지 및/또는 그 해시 값을 또한 고객 무선 디바이스(100)(도 1)에 전송하도록 구성될 수 있다.

[0083] [089] 일부 예시적인 실시예들에서, 방법은 결제 요청 메시지의 트랜잭션 정보 메시지 및 결제 토큰(109)(도 1) 데이터를 해석하고 저장하는 단계로 진행될 수 있다(텍스트 박스(205)). 예를 들어, 해석은 결제 토큰 복호화 모듈(113)(도 1)에 의해 행해질 수 있고 저장은 백-엔드 플랫폼(110)(도 1) 상의 트랜잭션 데이터베이스(111) 내에 행해질 수 있다.

[0084] [090] 일부 예시적인 실시예들에서, 결제 토큰(109)(도 1)이 서비스 제공자와 연관된 공개 키로 암호화될 수 있고, 결제 토큰(109)(도 1)은 결제 토큰 복호화 모듈(113)(도 1)에 의해 페치된 대응하는 개인 키로 복호화될 수 있다.

[0085] [091] 일부 예시적인 실시예들에서, 방법은 금융 기관(130)(도 1)을 이용하여 트랜잭션을 승인하는 단계로 진행될 수 있다(텍스트 박스(206)). 예를 들어, 트랜잭션 정보 및 고객의 신원은 금융 기관(130)(도 1)의 고객 플랫폼(131)(도 1)으로 디지털 방식으로 포워딩될 수 있다. 일부 예시적인 실시예들에서, 고객은 금융 기관(130)이 발급한 신용 카드, 은행 계좌를 보유하고 있으며, 그리고/또는 고객은 금융 기관(130)(도 1)에 의해 관리되는 고객 로열티 프로그램의 회원이다.

[0086] [092] 예를 들어, 이를테면 예를 들어, 고객이 트랜잭션을 커버하기에 충분한 신용 또는 자산을 가지고 있는지 여부와 같은 미리 정의된 규칙들을 트랜잭션이 준수하는지 검증한 후, 금융 기관(130)(도 1)은 미리 정의된 코드 메시지를 반환하여 트랜잭션을 확인할 수 있다.

[0087] [093] 일부 예시적인 실시예들에서, 트랜잭션 정보 메시지는 예를 들어, 구매된 제품이 적격 제품들의 리스트에 리스팅되어 있는지 여부 및/또는 판매자가 적격 비즈니스들의 특정 리스트에 리스팅되어 있는지 여부와 같은 다양한 규칙들에 대하여 비교될 수 있다.

[0088] [094] 일부 예시적인 실시예들에서, 방법은 백-엔드 플랫폼(110)(도 1)에 의해 트랜잭션 검증 메시지를 생성하고 이를 대응하는 결제 토큰(109)(도 1)과 연관된 고객에게 제공하는 단계로 진행될 수 있다(텍스트 박스(207)).

[0089] [095] 예를 들어, 트랜잭션 검증 메시지는 판매자 ID 및 결제 금액을 포함할 수 있는 결제와 관련된 정보를 포함한다. 트랜잭션 검증 메시지는 메시지 생성기 모듈(112)(도 1)에 의해 생성될 수 있고, 예를 들어 고객과 연

관된 어드레스(이를테면, 예를 들어, 모바일 애플리케이션(107)(도 1)이 고객의 무선 디바이스(100)(도 1)에 설치될 수 있음), 전화번호 및/또는 이메일 어드레스로 전송될 수 있다.

[0090] [096] 일부 예시적인 실시예들에서, 방법은 트랜잭션 검증 메시지에 서명하고 이를 복호화를 위해 백-엔드 플랫폼(110)(도 1)으로 전송하는 단계로 진행될 수 있다(텍스트 박스(208)). 예를 들어, 트랜잭션의 세부사항들은 메시지에 서명하기 전에 모바일 애플리케이션(107)(도 1)의 사용자 인터페이스를 사용하여 고객의 확인(예컨대, 확인 버튼을 누름)을 위해 고객에게 제시될 수 있다.

[0091] [097] 다른 예로, 디지털 지갑 SDK는 컨디션들 또는 규칙들 중 적어도 하나를 충족하면 메시지에 서명하는 단계로 진행될 수 있다. 예를 들어, 규칙들은, 제2 메시지의 해시 값이 이 트랜잭션과 연관하여 결제 단말로부터 이전에 수신된 제1 메시지의 해시 값과 매칭되는 것에 대한 규칙, 고객 무선 디바이스가 잠금해제된 때에 대한 규칙, 및 무선 디바이스의 지리적 위치가 결제 단말의 알려진 지리적 위치의 미리 결정된 범위 내에 있는지 여부에 대한 규칙, 서명될 트랜잭션이 고객 또는 그의 대리인에 의해 설정된 정기 허용금액을 초과하지 않는지 여부에 대한 규칙 등을 포함할 수 있다.

[0092] [098] 일부 실시예들에서, 상기 알려진 지리적 위치의 미리 결정된 범위는 알려진 지리적 위치의 중심으로부터 0 내지 5미터이다.

[0093] [099] 일부 예시적인 실시예들에서, 트랜잭션 검증 메시지는 공개-개인 키 쌍의 개인 키로 서명되어 백-엔드 플랫폼(110)(도 1)으로 다시 전송될 수 있다.

[0094] [0100] 일부 예시적인 실시예들에서, 메시지 복호화 모듈(114)(도 1)은 고객과 연관된 공개 키로, 서명된 트랜잭션 검증 메시지를 복호화할 수 있다.

[0095] [0101] 다른 실시예에서, 메시지 복호화 모듈(114)(도 1)은 서명된 트랜잭션 검증 메시지의 내용, 및 개인 키에 대응하는 공개 키 – 이 공개 키는 해당 개인 키를 노출하지 않고도 메시지 전체에 서명하기 위해 사용될 수 있음 – 를 유도하기 위해 적절한 알고리즘을 적용할 수 있다. 개인 키에 의해 서명된 메시지를 복호화하는 프로세스는, 예를 들어, EIP 712 Ethereum 표준에 따를 수 있다. 물론, 동일한 결과를 달성하기 위해 다른 적절한 알고리즘들이 고려될 수 있다.

[0096] [0102] 일부 예시적인 실시예들에서, 방법은 트랜잭션 검증 메시지의 서명자의 신원 및 트랜잭션의 유효성을 검증하는 단계로 진행될 수 있다(텍스트 박스(209)). 예를 들어, 트랜잭션 검증 모듈(115)(도 1)은 결제 단말로부터 이전에 수신된 트랜잭션 정보 메시지에 대하여 복호화된 검증 메시지를 비교할 수 있다. 매칭이 발견되면, 트랜잭션 정보를 이용하여, 메시지에 서명한 사람의 신원이 검증되는데, 그 이유는 수신된 서명된 메시지가 '고객'의 개인 키를 사용하여 서명될 수 있고 트랜잭션 데이터베이스(111)(도 1)로부터의 고객의 공개 키를 이용하여 복호화될 수 있기 때문이다.

[0097] [0103] 또 다른 예에서, 트랜잭션 검증 모듈(115)(도 1)은 복호화된 서명된 메시지로부터의 검증 메시지 및 공개 키 파라미터들을 트랜잭션 데이터베이스(111)(도 1)로부터의 동일한 것들에 대하여 비교할 수 있다.

[0098] [0104] 일부 예시적인 실시예들에서, 방법은 트랜잭션 결과들을 통지하는 단계로 진행될 수 있다(텍스트 박스(210)). 예를 들어, 백-엔드 플랫폼(110)(도 1)은 트랜잭션 확인 메시지를 전송하여 소비자, 판매자, 및 금융기관(130)(도 1)에 결제 유효성 검증의 결과를 통지할 수 있고, 따라서 상품, 서비스들 및 자금의 교환을 허용하거나 검증되지 않은 트랜잭션을 방지할 수 있다.

[0099] [0105] 이 방법은 상이한 순서로 또는 동시에 수행될 수 있다는 점을 이해해야 하며, 따라서 위에 설명된 방법 동작의 순서는 중요하지 않다.

[0100] [0106] 일부 예시적 실시예들에 따른 결제 토큰을 생성하기 위한 방법의 흐름도 설명인 도 3을 참조한다. 일부 예시적인 실시예들에서, 이 방법은 고객 무선 디바이스(100)(도 1)에 설치된 모바일 애플리케이션(107)(도 1)에 포함된 디지털 지갑 SDK(105)(도 1)에 의해 수행될 수 있다. 일부 다른 실시예들에서는, 다음 방법이 결제 단말(120)(도 1)에 의해 수행될 수 있다.

[0101] [0107] 일부 실시예들에서, 고객 무선 디바이스(100)의 암호지갑 모듈(104)은 랜덤 공개-개인 키 쌍(108)을 생성하고 저장할 수 있다.

[0102] [0108] 일부 예시적인 실시예들에서, 방법은 공개 키를 생성하는 데 사용되는 알고리즘에 대한 입력으로 적절할 수 있는 난수를 생성하여 개인 키(를 생성하는 단계(텍스트 박스(301))로 시작할 수 있다.

[0103] [0109] 일부 예시적인 실시예들에서, 방법은 예를 들어 Elliptic Curve Digital Signature Algorithm과 같은 알고리즘을 사용하여 개인 키를 해싱하여 개인 키에 기반하여 공개 키를 생성하는 단계(텍스트 박스(302))로 진행될 수 있다.

[0104] [0110] 일부 예시적인 실시예들에서, 방법은, 문자들의 세트를 암호화폐-지갑 어드레스로서 식별하기 위해 사용되는 미리 결정된 포맷으로 공개 키를 포맷함으로써, 공개 키의 지갑 어드레스를 생성하는 단계(텍스트 박스(303))로 진행될 수 있다. 예를 들어, 공개 키의 마지막 20바이트를 추출하고 시작부에 '0x'를 추가한다.

[0105] [0111] 일부 예시적인 실시예들에서, 방법은 고유한 고객 식별 정보를 페치하고 해싱하는 단계(텍스트 박스(304))로 진행될 수 있다. 일부 실시예에서, 식별 정보는 다음 중 적어도 하나를 포함할 수 있다: 소비자 연락처 정보(예컨대, 이름, 전화번호, 이메일), 무선 디바이스 ID(예컨대, IMEI 번호), 결제 정보(예컨대, 은행 계좌, 신용 카드), 지리적 위치, 및 소비자 ID 번호.

[0106] [0112] 일부 예시적인 실시예들에서, 백-엔드 플랫폼(110)(도 1)은 고유한 난수를 생성하고, 고유한 난수를 사용자 데이터베이스에 저장한 후 이를 결제 토큰을 구성할 때 논스(nonce)로서 포함시키기 위해 안전하게 전송할 수 있다. 이 피처는 식별 정보에 변경이 없었을 경우 동일한 결제 토큰들이 생성되는 것을 방지할 수 있다.

[0107] [0113] 이 방법은 고유한 사용자 정보의 해시 값 및 공개 키를 포함하는 결제 토큰을 구성하는 것으로 진행될 수 있다(텍스트 박스(305)). 일부 실시예들에서, 공개 키 또는 암호화폐-지갑 어드레스는, 소비자 식별 정보의 해시 값을 사용하여, 백-엔드 플랫폼(110)에서 판독가능한 공통의 적합한 데이터 구조, 이를테면 예를 들어, JSON 파일로 구조화될 수 있다.

[0108] [0114] 일부 예시적인 실시예들에 따른 서비스를 위한 초기 사용자 등록을 위한 방법의 흐름도 예시인 도 4를 참조한다. 일부 예시적인 실시예들에서, 이 방법은 고객 무선 디바이스(100)(도 1)에 설치된 모바일 애플리케이션(107)(도 1)에 포함될 수 있는 디지털 지갑 SDK(105)(도 1)에 의해 수행될 수 있다.

[0109] [0115] 일부 예시적인 실시예들에서, 방법은 디지털 지갑 SDK(105)(도 1) 및 암호화폐-지갑(텍스트 박스(401))을 사용하여 랜덤 공개-개인 키 쌍(108)(도 1)을 생성하고 저장하는 단계로 시작될 수 있고, 사용자 개인 정보로부터 입력을 수신하는 단계로 진행될 수 있다(텍스트 박스(402)). 예를 들어, 개인 정보는 이름, 전화번호, 어드레스, 이메일 어드레스, 생일, 및/또는 얼굴 사진 중 적어도 하나를 포함할 수 있다.

[0110] [0116] 일부 예시적인 실시예들에서, 이 방법은 무선 디바이스 고유 식별자 및 메타데이터를 페치하는 단계(텍스트 박스(403))로 진행될 수 있다. 이 정보는: 디지털 지갑 SDK를 실행하는 무선 디바이스의 IMEI 번호, 디바이스 모델, 운영 시스템 버전, 및 SDK 버전 중 적어도 하나를 포함할 수 있다.

[0111] [0117] 일부 예시적인 실시예들에서, 방법은 결제 정보의 입력을 수신하는 단계로 진행될 수 있다(텍스트 박스(404)). 이 정보는 다음 중 적어도 하나를 포함할 수 있다: 신용 카드 정보, 은행 계좌 번호, 로열티 프로그램 정보.

[0112] [0118] 일부 실시예들에서, 결제 정보는 무선 디바이스 상에 설치된 금융 기관의 애플리케이션, 이를테면, 예를 들어, 은행 모바일 애플리케이션, 로열티 프로그램 모바일 애플리케이션 등에 대한 인터페이스를 통해 수신될 수 있다.

[0113] [0119] 일부 실시예들에서, 금융 기관의 웹사이트에 로그인할 때 무선 디바이스에 설치된 브라우저에 대한 인터페이스를 통해 결제 정보가 수신될 수 있다.

[0114] [0120] 선택적으로, 백-엔드 플랫폼으로부터 논스를 요청하고 수신한다(텍스트 박스(405)).

[0115] [0121] 예를 들어, 백-엔드 플랫폼(110)의 공개 키로 개인 정보, 디바이스 정보, 결제 정보, 및 논스를 포함하는 정보를 암호화 한다(텍스트 박스(406)).

[0116] [0122] 일부 예시적인 실시예들에서, 방법은 암호화된 정보 및 디지털 지갑 SDK(105)(도 1)에 의해 생성된 공개 키를 백-엔드 플랫폼(110)(도 1)으로 송신하는 단계, 요구되는 개인 키로 암호화된 정보를 복호화하고 모든 정보를 백-엔드 플랫폼(110)(도 1) 내의 고객 데이터베이스(116)(도 1)에 저장하는 단계로 진행될 수 있다(텍스트 박스(407)).

[0117] [0123] 일부 실시예에서, 방법은 결제 정보와 연관된 금융 기관(130)(도 1)을 이용하여 신용에 대해 사용자를 승인하는 단계(텍스트 박스(408))를 더 포함한다. 예를 들어, 은행 계좌 정보가 입력되었을 때, 백-엔드 플랫폼(110)(도 1)은 은행의 연관된 고객 플랫폼(131)(도 1)에 질의하여 그 사용자에 의해 요청된 트랜잭션들을 은

행이 커버할 것인지 그리고 어떤 규칙들에 따를 것인지(예컨대, 국내 트랜잭션들만 허용)를 확인할 수 있다.

[0118] [0124] 일부 예시적인 실시예들에서, 방법은, 승인된 및/또는 등록된 사용자에 대한 사용자 ID를 생성하는 단계, 사용자에 의해 제공된 공개-개인 쌍(108)(도 1)의 공개 키로 이를 암호화하는 단계, 및 공개-개인 쌍(108)(도 1)의 적절한 개인 키로 복호화하기 위해, 암호화된 사용자 ID를 사용자의 무선 디바이스(100)(도 1)로 송신하는 단계, 및 장래의 트랜잭션들에서 결제 토큰(109)으로서 사용하기 위해 결제 토큰 저장소(106)(도 1) 내에 공개 키와 함께 저장하는 단계를 포함할 수 있다.

[0119] [0125] 일부 실시예들에서, 사용자 ID는 적어도 하나의 난수, 고유한 일련 번호, 특정 순서로 정렬된 사용자 정보의 해시 값을 포함할 수 있다.

[0120] [0126] 이제 일부 예시적인 실시예들에 따른 제조 제품(500)의 개략적인 예시인 도 5를 참조한다. 제품(500)은 적어도 하나의 컴퓨터 프로세서에 의해 실행될 때 적어도 하나의 프로세싱 회로(121)(도 1)가 결제 유효성을 검증하기 위한 하나 이상의 프로그램 명령들을 구현하고/구현하거나 도 1 내지 도 4를 참조하여 상술한 바와 같은 하나 이상의 동작들, 통신들 및/또는 기능들을 수행, 트리거링(triggering) 및/또는 구현하게 할 수 있도록 동작 가능한 프로세싱 디바이스(520)에 의해 구현된 컴퓨터-실행 가능 명령들(530)을 포함할 수 있는 하나 이상의 유형의 컴퓨터-판독 가능 비일시적 저장 매체(510)를 포함할 수 있다. "비일시적 기계-판독 가능 매체"라는 문구는 일시적인 전파 신호를 제외한 모든 컴퓨터-판독가능 매체를 포함하도록 의도된다.

[0121] [0127] 일부 예시적인 실시예들에서, 제품(500) 및/또는 기계-판독가능 저장 매체(510)는 휘발성 메모리, 비휘발성 메모리, 제거 가능 또는 제거 불능 메모리, 소거 가능 또는 소거 불능 메모리, 기입 가능 또는 재기입 가능 메모리 등을 포함하여 데이터를 저장할 수 있는 하나 이상의 유형의 컴퓨터-판독가능 저장 매체를 포함할 수 있다. 예를 들어, 기계-판독 가능 저장 매체(510)는 예를 들어, RAM, DRAM, ROM, 프로그래밍 가능 ROM(PROM: programmable ROM), 소거 가능 프로그래밍 가능 ROM(EPROM: erasable programmable ROM), 전기적 소거 가능 프로그래밍 가능 ROM(EEPROM: electrically erasable programmable ROM), 플래시 메모리, 하드 디스크 드라이브(HDD: hard disk drive), 솔리드-스테이트 디스크 드라이브(SDD: solid-state disk drive), 퓨젼(fusion) 드라이브 등과 같은 임의의 유형의 메모리를 포함할 수 있다. 컴퓨터 판독가능 저장 매체들은 통신 링크, 예컨대, 모뎀, 라디오, 또는 네트워크 접속을 통해 반송파 또는 다른 전파 매체에 구현된 데이터 신호들에 의해 반송되는 컴퓨터 프로그램을 원격 컴퓨터로부터 요청 컴퓨터로 다운로드하거나 전송하는 것과 관련된 임의의 적합한 매체들을 포함할 수 있다.

[0122] [0128] 일부 예시적인 실시예들에서, 프로세싱 디바이스(520)는 로직을 포함할 수 있다. 로직은 기계에 의해 실행되는 경우 기계로 하여금 본원에 설명된 방법, 프로세스 및/또는 동작들을 수행하게 할 수 있는 명령들, 데이터 및/또는 코드를 포함할 수 있다. 기계는 예를 들어 임의의 적합한 프로세싱 플랫폼, 컴퓨팅 플랫폼, 컴퓨팅 디바이스, 프로세싱 장치, 컴퓨팅 시스템, 프로세싱 시스템, 컴퓨터, 프로세서 등을 포함할 수 있으며, 하드웨어, 소프트웨어, 펌웨어 등의 임의의 적합한 조합을 사용하여 구현될 수 있다.

[0123] [0129] 일부 예시적인 실시예들에서, 프로세싱 디바이스(520)는 소프트웨어, 펌웨어, 소프트웨어 모듈, 애플리케이션, 프로그램, 서브루틴, 명령들, 명령 세트, 컴퓨팅 코드, 워드들, 값들, 심볼들 등으로서 구현될 수 있다. 명령들(540)은 소스 코드, 컴파일된 코드, 해석된 코드, 실행 가능 코드, 정적 코드, 동적 코드 등과 같은 임의의 적합한 유형의 코드를 포함할 수 있다. 명령들은 프로세서에 특정 기능을 수행하도록 명령하기 위해 사전 정의된 컴퓨터 언어, 방식 또는 신택스(syntax)에 따라 구현될 수 있다. 명령들은 C, C++, C#, Java, Python, BASIC, Mat lab, 어셈블리 언어, 기계 코드 등과 같은 임의의 적절한 하이-레벨, 로우-레벨, 객체-지향, 비주얼(visual), 컴파일되고/컴파일되거나 인터프리팅된 프로그래밍 언어들을 사용하여 구현될 수 있다.

[0124] [0130] 본 발명의 예시적 실시예를 도시한 도 6을 참조한다. 본 명세서에 묘사된 예시적인 프로세스는 SDK(601)가 암호화폐-지갑으로부터의 개인-공개 키 쌍과 같은 고객 정보(600), 신용 카드 정보와 같은 결제 수단, 및 고유 식별자일 수 있는 SDK ID를 수집하여 서버 플랫폼(606)으로 전송하는 것을 포함할 수 있는 등록 단계(600)로 시작할 수 있다.

[0125] [0131] 고객이 스캔된 제품들(604)을 구매하기 위해 POS(603)에 접근할 때, 고객은 SDK(601)를 갖는 디바이스를 디스플레이할 수 있으며, 이는 결제 토큰 내의 공개 키를 POS(603)의 결제 단말로 송신하는 것을 초래할 수 있다.

[0126] [0132] 프로세스는 POS가 서버 플랫폼(606)에 공개 키와 트랜잭션 정보 메시지(예컨대, 총 결제 금액)(605)를

포함할 수 있는 결제 요청을 전송하는 단계로 진행될 수 있다.

[0127] [0133] 프로세스는 서버 플랫폼(606)이 결제 토큰 또는 공개 키에 의해 식별된 SDK(601), 트랜잭션 정보 메시지에 의해 이전에 제공된 그러한 세부사항들을 포함할 수 있는 트랜잭션 검증 메시지(607)를 전송하는 단계로 진행될 수 있다.

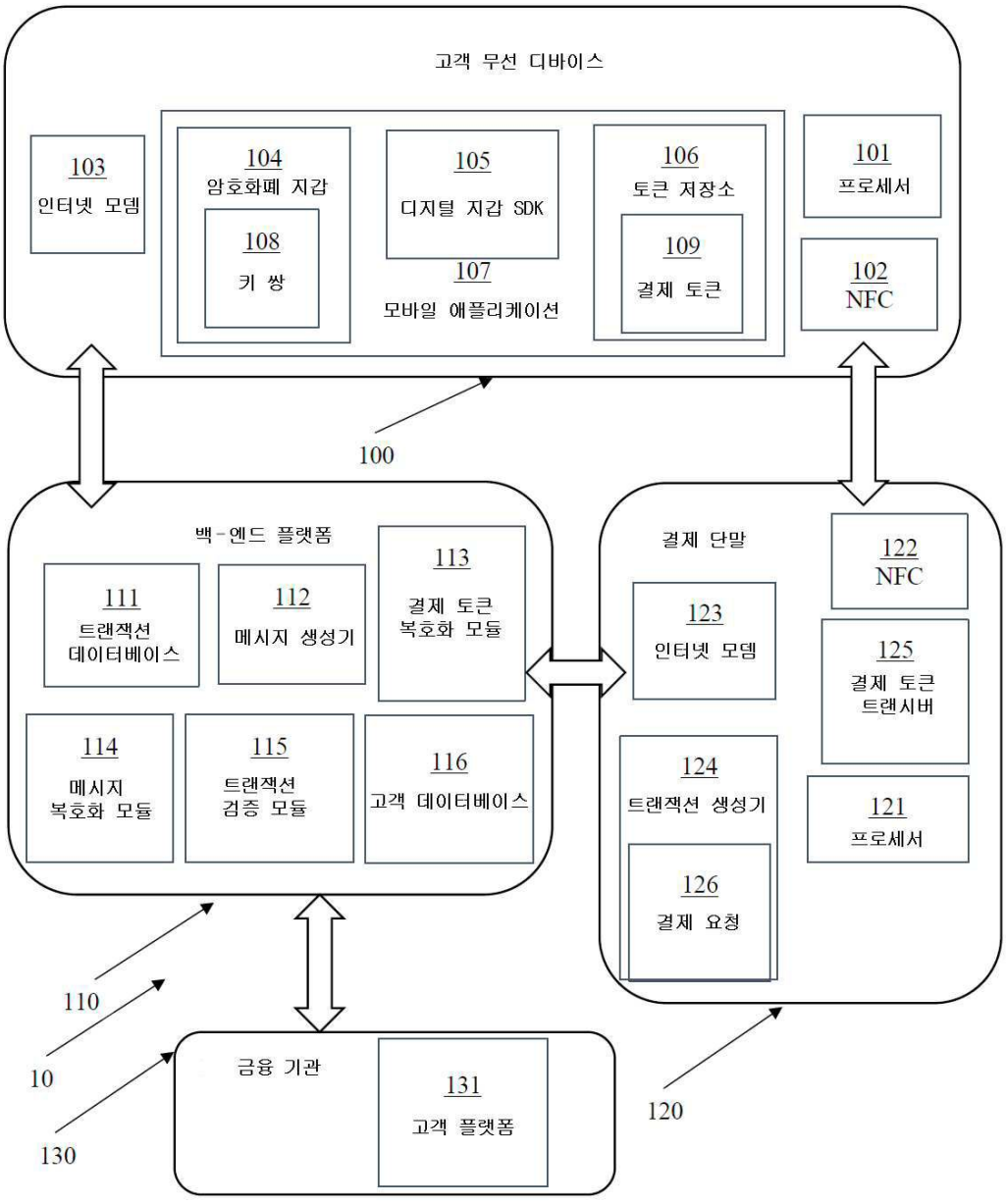
[0128] [0134] 프로세스는 고객 승인 후 SDK(601)가 트랜잭션 검증 메시지에 서명하고 이를 서버 플랫폼(606)으로 송신(608)하는 단계로 진행될 수 있다.

[0129] [0135] 프로세스는 서버 플랫폼(606)이, SDK(601)가 서명한 트랜잭션 검증 메시지와 POS(603)에 의해 제공된 트랜잭션 정보 메시지 사이의 정보의 비교에 기반하여 결제를 검증하는 단계로 진행될 수 있다.

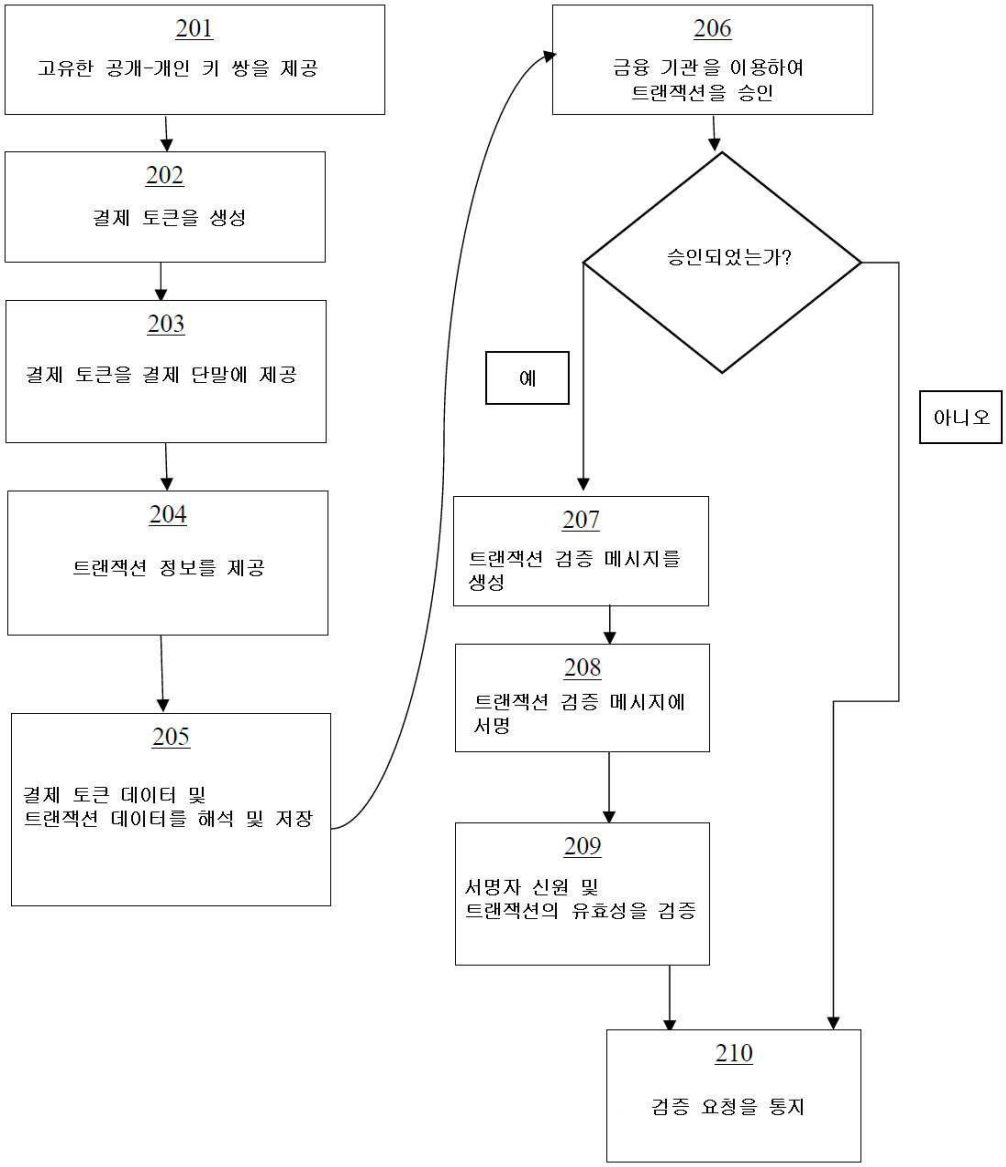
[0130] [0136] 프로세스는 서버 플랫폼(606)이 POS 609에 결제 승인 또는 거부를 통지하는 단계로 진행될 수 있다. 위에 설명된 청구대상은 단지 예시로서 제공되며 제한하는 것으로 해석되어서는 안 된다. 예시되고 설명된 예시적인 실시예들 및 애플리케이션들을 따르지 않고, 이하의 청구항들에 제시된 본 발명의 진정한 사상과 범위를 벗어나지 않고, 본원에 설명된 주제에 대해 다양한 수정들 및 변경들이 이루어질 수 있다.

도면

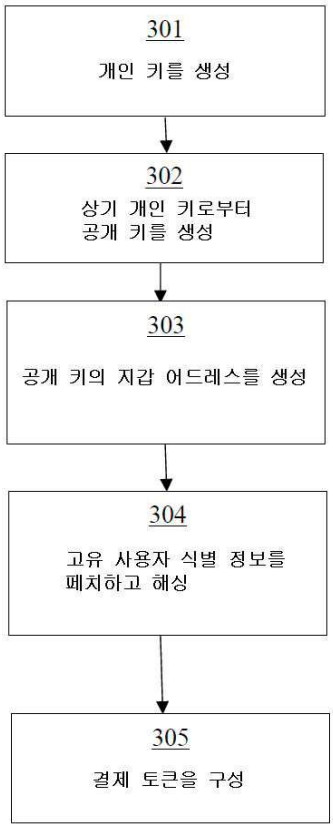
도면1



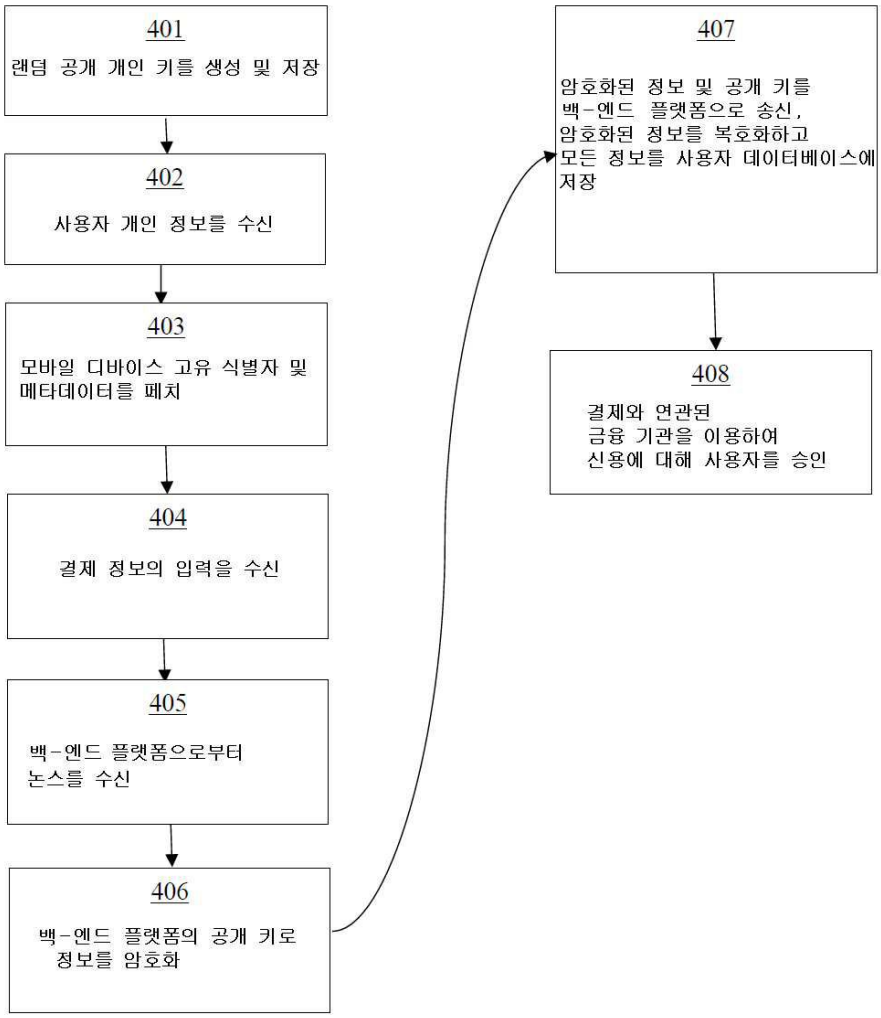
도면2


201
고유한 공개-개인 키 쌍을 제공
202
결제 토큰을 생성
203
결제 토큰을 결제 단말에 제공
204
트랜잭션 정보를 제공
205
결제 토큰 데이터 및
트랜잭션 데이터를 해석 및 저장
206
금융 기관을 이용하여
트랜잭션을 승인
승인되었는가?
예
아니오
207
트랜잭션 검증 메시지를
생성
208
트랜잭션 검증 메시지에
서명
209
서명자 신원 및
트랜잭션의 유효성을 검증
210
검증 요청을 통지

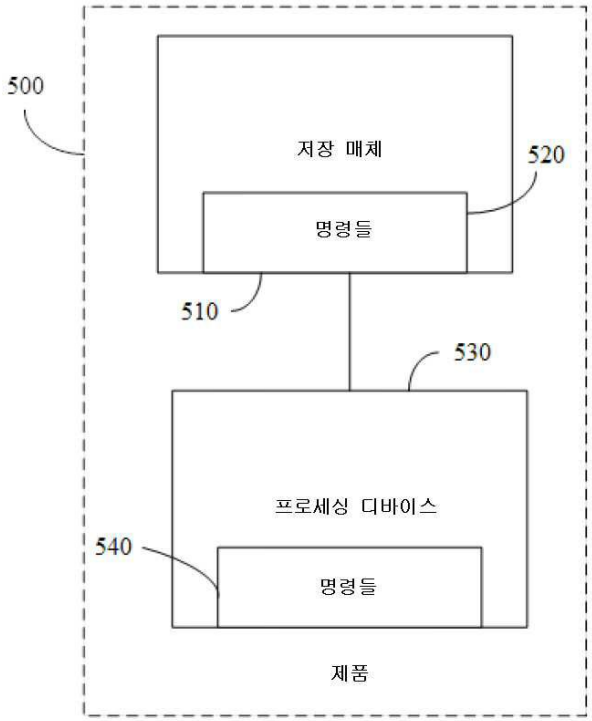
도면3


301
개인 키를 생성
302
상기 개인 키로부터
공개 키를 생성
303
공개 키의 지갑 어드레스를 생성
304
고유 사용자 식별 정보를
페치하고 해싱
305
결제 토큰을 구성

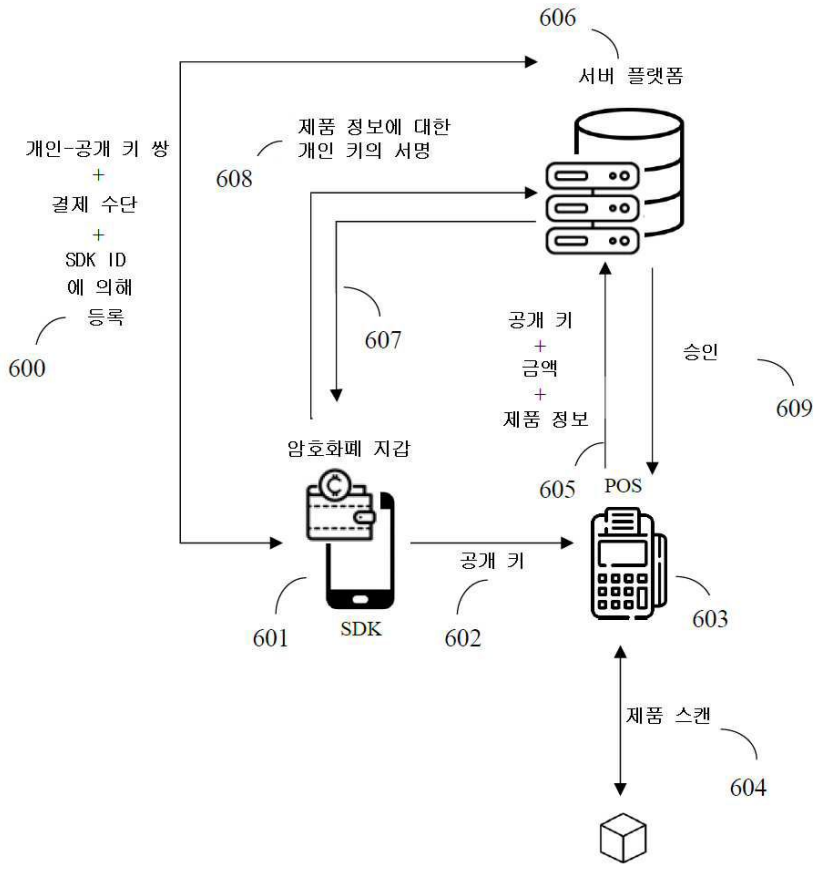
도면4


401
랜덤 공개 개인 키를 생성 및 저장
402
사용자 개인 정보를 수신
403
모바일 디바이스 고유 식별자 및 메타데이터를 페치
404
결제 정보의 입력을 수신
405
백-엔드 플랫폼으로부터 논스를 수신
406
백-엔드 플랫폼의 공개 키로 정보를 암호화
407
암호화된 정보 및 공개 키를 백-엔드 플랫폼으로 송신, 암호화된 정보를 복호화하고 모든 정보를 사용자 데이터베이스에 저장
408
결제와 연관된 금융 기관을 이용하여 신용에 대해 사용자를 승인

도면5


500
저장 매체
520
명령들
510
530
프로세싱 디바이스
540
명령들
제품

도면6


606
서버 플랫폼
개인-공개 키 쌍
+
결제 수단
+
SDK ID
에 의해
등록
600
제품 정보에 대한
개인 키의 서명
608
607
공개 키
+
금액
+
제품 정보
승인
609
암호화폐 지갑
605
POS
공개 키
601
SDK
602
603
제품 스캔
604