(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2021 년 11 월 25 일 (25.11.2021)

WIPO | PCT

(10) 국제공개번호
WO 2021/235838 A1

(51) 국제특허분류:
G06Q 20/38 (2012.01) *G06F 21/62* (2013.01)
G06Q 20/36 (2012.01) *H04L 9/08* (2006.01)

(21) 국제출원번호: PCT/KR2021/006232

(22) 국제출원일: 2021 년 5 월 18 일 (18.05.2021)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2020-0059799 2020 년 5 월 19 일 (19.05.2020) KR

(71) 출원인: 삼성전자 주식회사 (**SAMSUNG ELECTRONICS CO., LTD.**) [KR/KR]; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR).

(72) 발명자: 박찬준 (**PARK, Chanjoon**); 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). 김예원 (**KIM, Yewon**); 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). 제성민 (**JE, Seongmin**); 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR).

(74) 대리인: 권혁록 등 (**KWON, Hyuk-Rok** et al.); 03173 서울시 종로구 새문안로 5길 19, 11층, Seoul (KR).

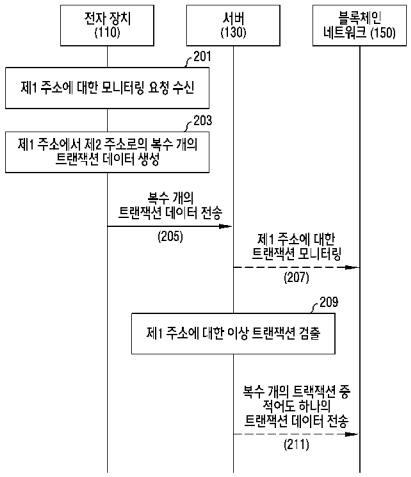
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:
— 국제조사보고서와 함께 (조약 제21조(3))

(54) **Title:** ELECTRONIC DEVICE USING BLOCKCHAIN AND OPERATION METHOD THEREOF

(54) **발명의 명칭:** 블록체인을 이용하는 전자 장치 및 동작 방법



110 ... Electronic device
130 ... Server
150 ... Blockchain network
201 ... Receive monitoring request for first address
203 ... Generate multiple pieces of transaction data from first address to second address
205 ... Transmit multiple pieces of transaction data
207 ... Monitor transaction for first address
209 ... Detect abnormal transaction for first address
211 ... Transmit at least one piece of transaction data from among multiple transactions

(57) Abstract: An embodiment according to the present disclosure provides an electronic device comprising a communication circuit, a security memory, and at least one processor connected to the communication circuit and the security memory, wherein the at least one processor is configured to: generate a first key pair including a first public key and a first private key, wherein the first private key is stored in the security memory; generate a first address on the basis of the first public key; generate a second key pair including a second public key distinct from the first public key and a second private key distinct from the first private key; generate a second address on the basis of the second public key; and generate transaction data for multiple transactions transferring an unused transaction output value of the first address from the first address to the second address on the basis of a digital signature through the first private key. Various other embodiments inferred from the specification are also possible.

(57) 요약서: 본 개시에 따른 일 실시 예는 통신회로, 보안 메모리 및 상기 통신회로 및 상기 보안 메모리와 연결되는 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는 제1 공개 키(public key) 및 제1 개인 키(private key)를 포함하는 제1 키 쌍을 생성하고, 상기 제1 개인 키는 상기 보안 메모리에 저장되며, 상기 제1 공개 키에 기반하여 제1 주소를 생성하고, 상기 제1 공개 키와 구별되는 제2 공개 키 및 상기 제1 개인 키와 구별되는 제2 개인 키를 포함하는 제2 키 쌍을 생성하고, 상기 제2 공개 키에 기반하여 제2 주소를 생성하고, 상기 제1 개인 키를 통한 디지털 서명에 기반하여 상기 제1 주소의 미사용 트랜잭션 출력 값을 상기 제1 주소로부터 상기 제2 주소로 이전시키는 복수 개의 트랜잭션들에 대한 트랜잭션 데이터를 생성하도록 설정되는 전자 장치가 개시된다. 이 외에도 명세서를 통해 파악되는 다양한 실시 예가 가능하다.

WO 2021/235838 A1

명세서

발명의 명칭: 블록체인을 이용하는 전자 장치 및 동작 방법

기술분야

[1] 본 개시에 따른 다양한 실시 예들은, 블록체인을 이용하여 거래를 수행하는 전자 장치에 관한 것이다.

배경기술

[2] 블록체인(blockchain)은 데이터를 특정 단위의 블록으로 만들어 유효한 네트워크 상에서 체인 형태로 연결하는 데이터 저장 기술이다. 블록체인 노드(node)는 중앙 서버에 의해 관리되지 않으며, 개별적인 분산 공공 장부를 갖는다. 암호화폐의 거래 내역은 분산 공공 장부에 기재되고, 모든 블록체인 네트워크 상의 노드는 동일한 거래 내역 데이터를 보유할 수 있다. 이에 따라 블록체인 노드에 저장된 데이터에 대한 개별적인 위조 및 변조는 어렵다.

[3] 최근에는 블록체인 기술에 기반하여 다양한 암호화폐(예: 비트코인(bitcoin), 이더리움(ethereum))가 등장하고 있다. 암호화폐를 통해 가상 거래를 수행하는 경우에, 거래 내용이 담긴 신규 블록이 생성될 수 있다. 생성된 블록은 블록체인 네트워크 상에 있는 모든 참여자에게 전송되고, 특정 알고리즘에 기반하여 승인된 블록만이 블록체인 노드에 저장되어 거래가 완료될 수 있다.

[4] 사용자는 가상 거래에서의 자산인 암호화폐를 보호하기 위하여 지갑(wallet)을 보유할 수 있다. 암호화폐 지갑은 사용자의 키를 저장하고 관리할 수 있다. 가상 거래의 거래 내용에 대한 데이터는 사용자의 키를 이용해 전자 서명되어 블록체인 노드에 저장될 수 있다.

[5] 사용자의 키는 개인 키(private key) 및 공개 키(public key)를 포함하는 키 쌍(key pair)으로 구성될 수 있다. 사용자에게 고유하게 부여된 개인 키로부터 공개 키가 생성되고, 공개 키로부터 해시함수를 이용하여 어드레스(address)가 생성될 수 있다.

발명의 상세한 설명

기술적 과제

[6] 암호화폐 지갑은 오프라인에서 작동하는 콜드월렛(cold wallet) 및 온라인에서 작동하는 핫월렛(hot wallet)으로 구분될 수 있다. 콜드월렛은 오프라인 환경인 하드웨어 장치 내부에서 트랜잭션 내역을 생성하고, 전자 서명 과정이 수행되도록 구성될 수 있다. 콜드월렛은 하드월렛(hard wallet)이라고도 언급될 수 있으며, 암호화(예: 개인 식별 번호, Personal Identification Number)되어 있으며 바이러스나 백도어 프로그램에 영향을 받지 않도록 설계되어 보안성이 높은 것으로 평가된다. 높은 보안성을 갖는 콜드월렛은 가격이 비싸고 사용 절차가 복잡하다는 단점이 있다.

[7] 핫월렛은 온라인 상에서의 실시간 거래가 가능하다는 점에서 높은 편의성을

가지고 있으나, 온라인 환경에서 거래가 수행되므로 외부로부터 개인 키가 해킹될 위험이 있다. 외부로부터 개인 키가 해킹되는 경우, 사용자의 암호화폐에 대하여 임의의 거래가 발생할 수 있다. 예를 들어, 공격자가 온라인 서버에 저장된 개인 키를 탈취하여 암호화폐에 대한 전송 권한을 획득할 수 있다. 다만, 사용자는 외부에 의한 거래 발생을 실시간으로 확인하기 어렵고, 거래 내용이 블록체인 네트워크에 전송된 이후에는 암호화폐에 대한 소유권이 완전히 이전되므로 탈취된 암호화폐를 되찾을 수 없다.

[8] 따라서, 본 개시에 따른 다양한 실시 예들은 온라인 상에서의 거래를 모니터링하여 해킹을 방지하는 전자 장치를 제공하고자 한다.

과제 해결 수단

[9] 일 실시 예에서의 전자 장치는 통신회로, 보안 메모리 및 상기 통신회로 및 상기 보안 메모리와 연결되는 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는 제1 공개 키(public key) 및 제1 개인 키(private key)를 포함하는 제1 키 쌍을 생성하고, 상기 제1 개인 키는 상기 보안 메모리에 저장되며, 상기 제1 공개 키에 기반하여 제1 주소를 생성하고, 상기 제1 공개 키와 구별되는 제2 공개 키 및 상기 제1 개인 키와 구별되는 제2 개인 키를 포함하는 제2 키 쌍을 생성하고, 상기 제2 공개 키에 기반하여 제2 주소를 생성하고, 상기 제1 개인 키를 통한 디지털 서명에 기반하여 상기 제1 주소의 미사용 트랜잭션 출력 값을 상기 제1 주소로부터 상기 제2 주소로 이전시키는 복수 개의 트랜잭션들에 대한 트랜잭션 데이터를 생성하도록 설정될 수 있다.

[10] 일 실시 예에서의 전자 장치의 동작 방법은 제1 공개 키 및 제1 개인 키를 포함하는 제1 키 쌍을 생성하는 동작, 상기 제1 개인 키는 보안 메모리에 저장됨, 상기 제1 공개 키에 기반하여 제1 주소를 생성하는 동작, 상기 제1 공개 키와 구별되는 제2 공개 키 및 상기 제1 개인 키와 구별되는 제2 개인 키를 포함하는 제2 키 쌍을 생성하는 동작, 상기 제2 공개 키에 기반하여 제2 주소를 생성하는 동작, 및 상기 제1 개인 키를 통한 디지털 서명에 기반하여 상기 제1 주소의 미사용 트랜잭션 출력 값을 상기 제1 주소로부터 상기 제2 주소로 이전시키는 복수 개의 트랜잭션들에 대한 트랜잭션 데이터를 생성하는 동작을 포함할 수 있다.

[11] 일 실시 예에서의 서버는 통신회로 및 상기 통신회로와 연결되는 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는 전자 장치로부터 상기 통신회로를 통해서 수신된 제1 주소의 미사용 트랜잭션 출력 값을 상기 제1 주소로부터 제2 주소로 이전시키는 복수 개의 트랜잭션에 대한 트랜잭션 데이터를 저장하고, 상기 제1 주소에 대한 트랜잭션을 모니터링하고, 상기 제1 주소에 대한 이상 트랜잭션이 검출되면 상기 복수 개의 트랜잭션 중 적어도 하나의 트랜잭션에 대한 트랜잭션 데이터를 블록체인 네트워크로 전송하도록 설정될 수 있다.

발명의 효과

[12] 본 개시의 다양한 실시 예에 따르면 복수 개의 트랜잭션을 생성하는 전자 장치를 통해, 외부로부터 생성된 트랜잭션을 무효화하여 해킹을 방지할 수 있다.

도면의 간단한 설명

[13] 도 1은 일 실시 예에 따른 전자 장치, 서버 및 블록체인 네트워크를 포함하는 트랜잭션 시스템의 구성을 나타낸다.

[14] 도 2는 일 실시 예에 따른 트랜잭션 시스템의 동작 흐름도를 도시한다.

[15] 도 3은 일 실시 예에 따른 전자 장치의 동작 흐름도를 도시한다.

[16] 도 4는 일 실시 예에 따른 이상 트랜잭션을 검출한 서버의 동작 흐름도를 도시한다.

[17] 도 5는 일 실시 예에 따른 전자 장치에서 운용되는 REE 및 TEE의 블록도를 도시한다.

[18] 도 6a는 일 실시 예에 따른 전자 장치의 제1 UI 상태를 도시한다.

[19] 도 6b는 일 실시 예에 따른 전자 장치의 제2 UI 상태를 도시한다.

[20] 도 6c는 일 실시 예에 따른 전자 장치의 제3 UI 상태를 도시한다.

[21] 도 6d는 일 실시 예에 따른 전자 장치의 제4 UI 상태를 도시한다.

[22] 도 6e는 일 실시 예에 따른 전자 장치의 제5 UI 상태를 도시한다.

[23] 도 6f는 일 실시 예에 따른 전자 장치의 제6 UI 상태를 도시한다.

[24] 도 7은 일 실시 예에 따른 해킹 방지 트랜잭션을 생성하는 전자 장치의 UI 상태를 도시한다.

[25] 도 8은 일 실시 예에 따른 복수 개의 트랜잭션을 생성하는 전자 장치의 UI 상태를 도시한다.

[26] 도 9는 일 실시 예에 따른 트랜잭션 전송이 완료된 후 트랜잭션 시스템의 동작 흐름도를 도시한다.

[27] 도 10은 다양한 실시 예들에 따른 네트워크 환경 내의 전자 장치의 블록도를 도시한다.

[28] 도 11은 다양한 실시 예들에 따른 프로그램을 예시하는 블록도를 도시한다.

발명의 실시를 위한 형태

[29] 도 1은 일 실시 예에 따른 전자 장치, 서버 및 블록체인 네트워크를 포함하는 트랜잭션 시스템의 구성을 나타낸다.

[30] 도 1을 참조하면, 트랜잭션 시스템(100)은 전자 장치(110), 서버(130) 및 블록체인 네트워크(150)를 포함할 수 있다.

[31] 일 실시 예에서, 전자 장치(110)(예: 도 10의 전자 장치(1001))는 통신회로(112)(예: 도 10의 통신 모듈(1090)), 보안 메모리(114)(예: 도 10의 메모리(1030)), 프로세서(116)(예: 도 10의 프로세서(1020)) 및 디스플레이(118)(예: 도 10의 표시 장치(1060))를 포함할 수 있다. 일 실시 예에서, 통신회로(112)는 전자 장치(110)와 외부 전자 장치(예: 서버(130))간의 통신

채널을 수립하고 데이터를 전송 및 수신할 수 있다. 예를 들어, 통신회로(112)는 트랜잭션을 수행하는 전자 장치(110)의 트랜잭션 데이터를 서버(130)에 전송할 수 있다.

[32] 일 실시 예에서, 전자 장치(110)는 비대칭키 암호 방식(예: 공개키 암호 방식 public-key cryptography)으로 키 쌍(key pair)을 생성할 수 있다. 키 쌍은 개인 키(private key) 및 공개 키(public key)를 포함할 수 있다. 일 실시 예에서, 보안 메모리(114)는 생성된 개인 키를 저장할 수 있다. 일 실시 예에서, 보안 메모리(114)는 보안 환경(security environment)을 제공하는 하드웨어 형태의 메모리를 의미할 수 있다. 예를 들어, 보안 메모리(114)는 전자 장치(110) 에 내장된 형태이거나, 전자 장치(110)에 별도로 삽입 가능한 장치(예: 마이크로 SD 카드)의 형태일 수 있다. 예를 들어, 보안 메모리(114)는 일반 메모리와 하드웨어적으로 분리되는 메모리를 의미할 수 있다. 또 다른 실시 예에서, 보안 메모리(114)는 보안 환경을 제공하도록 암호화된 소프트웨어 형태의 메모리를 의미할 수도 있다. 예를 들어, 보안 메모리(114)는 일부 구성(예: TEE)을 통해서만 데이터에 접근할 수 있도록, 데이터를 암호화하여 저장하는 소프트웨어의 형태일 수도 있다. 예를 들어, 보안 메모리(114)는 일반 메모리와 동일한 메모리(예: 도 10의 메모리(1030)) 상에서 구현되지만 소프트웨어적(예: 메모리 주소)으로 분리되는 보안 메모리 영역에 저장되는 소프트웨어 형태일 수 있다.

[33] 일 실시 예에서, 디스플레이(118)는 전자 장치(110)의 외부(예: 사용자)로 정보를 시각적으로 제공할 수 있다. 예를 들어, 디스플레이(118)는 전자 장치(110)의 트랜잭션 생성 정보, 잔액 정보, 트랜잭션 전송 지연 정보 및 트랜잭션 전송 완료 정보 중 적어도 하나의 정보를 외부로 제공할 수 있다.

[34] 일 실시 예에서, 프로세서(116)는 루트 시드(root seed)에 기반하여 키 쌍을 생성할 수 있다. 예를 들어, 프로세서(116)는 해킹 방지 트랜잭션을 수행하는 경우에, 프로세서(116)는 새로운 루트 시드에 기반하여 개인 키를 생성하고, 개인 키에 기반하여 공개 키를 생성할 수 있다. 프로세서(116)는 공개 키에 대하여 해시 함수를 통해 어드레스를 생성할 수 있다.

[35] 일 실시 예에서, 서버(130)는 통신회로(132), 메모리(134) 및 프로세서(136)를 포함할 수 있다. 일 실시 예에서, 통신회로(132)는 서버(130)와 외부 장치(예: 전자 장치(110), 블록체인 네트워크(150))간의 통신 채널을 수립하여 데이터를 전송 및 수신할 수 있다. 예를 들어, 통신회로(132)는 전자 장치(110)로부터 수신한 트랜잭션 데이터를 블록체인 네트워크(150)에 전송할 수 있다. 전송된 트랜잭션 데이터는 블록체인 노드(152)에 저장될 수 있다.

[36] 일 실시 예에서, 프로세서(136)는 통신회로(132)를 통해 전자 장치(110)로부터 데이터를 수신할 수 있다. 일 실시 예에서, 프로세서(136)는 전자 장치(110)로부터 수신된 데이터에 포함된 구분 플래그를 식별할 수 있다. 일 실시 예에서, 프로세서(136)는 데이터에 포함된 구분 플래그에 기반하여 수신된 데이터를 블록체인 네트워크(150)에 전송할지 여부를 결정할 수 있다. 예를 들어,

수신된 데이터에 특정 구분 플래그가 포함된 경우(또는, 포함된 구분 플래그의 값이 제1 구분 값인 경우)에, 프로세서(136)는 수신된 데이터를 메모리(134)에 저장할 수 있다. 다른 예를 들어, 수신된 데이터에 특정 구분 플래그가 포함되지 않은 경우 (또는, 포함된 구분 플래그의 값이 상기 제1 구분 값과 구별되는 제2 구분 값인 경우)에, 프로세서(136)는 수신된 데이터를 블록체인 네트워크(150)에 전송할 수 있다. 일 실시 예에서, 구분 플래그는 데이터 패킷에 포함되는 구분 값을 의미할 수 있다. 예를 들어, 전자 장치(110)로부터 수신된 데이터 패킷의 일부 비트에 대하여 제1 구분 값 “1”을 포함하는 경우에는, 프로세서(136)는 수신된 데이터를 메모리(134)에 저장할 수 있다. 다른 예를 들어, 수신된 데이터 패킷의 일부 비트에 대하여 제2 구분 값 “0”을 포함하는 경우에는, 프로세서(136)는 수신된 데이터를 블록체인 네트워크(150)에 전송할 수 있다.

[37] 도 1은 전자 장치(110)에서 생성한 데이터가 서버(130)를 통해 블록체인 네트워크(150)로 전송되는 트랜잭션 시스템만을 도시하고 있으나, 또 다른 실시 예에서, 전자 장치(110)에서 생성된 데이터의 일부는 블록체인 네트워크(150)로 직접 전송될 수도 있다. 예를 들어, 전자 장치(110)는 특정 구분 플래그를 포함하지 않는 트랜잭션 데이터를 블록체인 네트워크(150)에 직접 전송할 수 있다. 다른 예를 들어, 전자 장치(110)는 특정 구분 플래그를 포함하는 트랜잭션 데이터를 서버(130)에 전송할 수 있다. 특정 구분 플래그를 포함하는 트랜잭션 데이터를 수신한 서버(130)는 블록체인 네트워크(150)를 모니터링할 수 있다. 서버(130)는 블록체인 네트워크(150)에서 이상 트랜잭션이 검출되면, 특정 구분 플래그를 포함하는 트랜잭션 데이터를 블록체인 네트워크(150)에 전송할 수 있다. 또 다른 예를 들어, 전자 장치(110)는 특정 구분 플래그를 포함하는 트랜잭션 데이터를 메모리(예: 보안 메모리(114))에 저장할 수 있다. 서버(130)는 블록체인 네트워크(150)에서 이상 트랜잭션이 검출되면, 전자 장치(110)에 특정 구분 플래그를 포함하는 트랜잭션 데이터를 블록체인 네트워크(150)로 전송할 것을 요청할 수 있다.

[38] 도 2는 일 실시 예에 따른 트랜잭션 시스템의 동작 흐름도를 도시한다.

[39] 도 2를 참조하면, 전자 장치(110)는 동작 201에서 제1 주소에 대한 모니터링 요청을 수신할 수 있다. 예를 들어, 전자 장치(110)는 디스플레이(예: 도 1의 디스플레이(118))에 대한 터치 입력을 통해 제1 주소에 대한 모니터링 요청을 수신할 수 있다. 다만, 또 다른 실시 예에서, 전자 장치(110)가 제1 주소에 대한 모니터링 요청을 수신하지 않는 경우에도, 서버(130)는 다양한 임의의 설정에 따라 모니터링을 개시할 수 있다. 예를 들어, 서버(130)는 전자 장치(110)에 대한 사용자의 설정, 전자 장치(110) 및/또는 서버(예: 도 1의 서버(130)) 내 임의의 설정에 따라 모니터링을 개시할 수도 있다.

[40] 일 실시 예에서, 전자 장치(110)는 동작 203에서 제1 주소에서 제2 주소로의 복수 개의 트랜잭션에 대한 트랜잭션 데이터를 생성할 수 있다. 일 실시 예에서, 제1 주소는 외부 해킹에 대한 모니터링이 수행될 주소를 의미하고, 제2 주소는

외부에 의한 도난을 방지하기 위한 해킹 방지 주소를 의미할 수 있다. 제1 주소 및 제2 주소는 서로 상이한 루트 시드에 기반하여 생성된 주소를 의미할 수 있다. 일 실시 예에서, 전자 장치(110)는 트랜잭션 데이터에 기반하여 수수료를 계산할 수 있다. 예를 들어, 전자 장치(110)는 2.1BTC를 가진 미사용 트랜잭션 출력 값(Vin)을 갖는 제1 주소에서 제2 주소로 1.9BTC를 전송(Vout)하고, 제1 주소로 0.05BTC를 전송(Vout)하는 트랜잭션 데이터를 생성할 수 있다. 전자 장치(110)는 Vin 및 Vout에 기반하여 트랜잭션 데이터의 수수료가 0.15BTC임을 계산할 수 있다. 또 다른 실시 예에서, 전자 장치(110)는 복수 개의 트랜잭션에 대하여 서로 다른 수수료 정보를 포함하도록 트랜잭션 데이터를 생성할 수 있다. 예를 들어, 전자 장치(110)는 2.1BTC를 가진 미사용 트랜잭션 출력 값(Vin)을 갖는 제1 주소에서 제2 주소로 1.9BTC를 전송(Vout)하는 제1 트랜잭션 데이터를 생성할 수 있다. 제1 트랜잭션 데이터는 0.2BTC의 수수료 정보를 포함할 수 있다. 전자 장치(110)는 2.1BTC를 가진 미사용 트랜잭션 출력 값(Vin)을 갖는 제1 주소에서 제2 주소로 2.05BTC를 전송(Vout)하는 제2 트랜잭션 데이터를 생성할 수 있다. 제2 트랜잭션 데이터는 0.05BTC의 수수료 정보를 포함할 수 있다.

[41] 일 실시 예에서, 전자 장치(110)는 동작 205에서 복수 개의 트랜잭션에 대한 트랜잭션 데이터를 서버(130)로 전송할 수 있다. 일 실시 예에서, 서버(130)는 수신된 복수 개의 트랜잭션에 대한 트랜잭션 데이터를 메모리(134)에 저장할 수 있다. 일 실시 예에서, 복수 개의 트랜잭션은 구분 플래그를 포함할 수 있다. 일 실시 예에서, 구분 플래그가 포함된 복수 개의 트랜잭션에 대한 트랜잭션 데이터를 수신함에 따라, 서버(130)는 제1 주소에 대하여 모니터링 상태로 결정할 수 있다. 예를 들어, 제1 주소가 모니터링 상태인 경우에, 제1 주소는 서버(130) 및/또는 전자 장치(110)의 보안 환경을 제공하는 보안 메모리(예: 도 1의 보안 메모리(114))에서 관리됨에 따라 임의의 상태 변경이 불가능할 수 있다.

[42] 일 실시 예에서, 서버(130)는 동작 207에서 제1 주소에 대한 트랜잭션을 모니터링할 수 있다. 일 실시 예에서, 서버(130)는 블록체인 네트워크(150)에 전송되는 트랜잭션 데이터의 입력 값을 모니터링할 수 있다. 예를 들어, 서버(130)는 사용자의 미사용 트랜잭션 출력 값(unspent transaction output, UTXO)을 포함하는 어드레스 목록을 저장할 수 있다. 서버(130)는 블록체인 네트워크(150)에 전송되는 트랜잭션 데이터의 입력 값과 사용자의 미사용 트랜잭션 출력 값을 포함하는 어드레스를 비교할 수 있다. 트랜잭션 데이터의 입력 값과 사용자의 미사용 트랜잭션 출력 값이 동일한 경우에, 서버(130)는 해당 트랜잭션 데이터를 외부 해킹에 의한 트랜잭션 데이터로 판단할 수 있다. 또 다른 예를 들어, 서버(130)는 사용자의 미사용 트랜잭션 출력 값의 트랜잭션 ID 정보 및 트랜잭션의 출력 인덱스 값(Vout)을 저장할 수 있다. 서버(130)는 블록체인 네트워크(150)에 전송되는 트랜잭션 데이터의 트랜잭션 ID 정보 및 트랜잭션의 출력 인덱스 값과 사용자의 미사용 트랜잭션 출력 값의 트랜잭션 ID 정보 및 트랜잭션의 출력 인덱스 값을 비교할 수 있다. 트랜잭션 ID 정보 및

트랜잭션의 출력 인덱스 값이 서로 동일한 경우에, 서버(130)는 해당 트랜잭션 데이터가 외부 해킹에 의한 트랜잭션 데이터로 판단할 수 있다.

[43] 일 실시 예에서, 동작 207은 동작 205 이후에 순차적으로 실행되거나, 동작 205와 병렬적으로 실행될 수 있다. 예를 들어, 서버(130)는 전자 장치(110)로부터 복수 개의 트랜잭션 데이터를 수신한 시점 이후에 트랜잭션을 모니터링할 수 있다. 또 다른 예를 들어, 서버(130)는 전자 장치(110)로부터 복수 개의 트랜잭션 데이터를 수신함과 동시에 트랜잭션을 모니터링할 수 있다.

[44] 일 실시 예에서, 서버(130)는 동작 209에서 제1 주소에 대한 이상(또는, 비정상) 트랜잭션을 검출할 수 있다. 예를 들어, 서버(130)는 모니터링 상태인 제1 주소에 대하여 출금을 요청하는 이상 트랜잭션을 검출하면, 외부에 의한 해킹이 발생하였음을 식별할 수 있다.일 실시 예에서, 서버(130)는 동작 211에서 복수 개의 트랜잭션 중 적어도 하나의 트랜잭션에 대한 트랜잭션 데이터를 블록체인 네트워크(150)에 전송할 수 있다. 예를 들어, 서버(130)는 제1 주소에 대한 이상 트랜잭션의 수수료 정보를 확인하고, 해당 수수료 정보보다 높은 수수료 정보를 포함하는 제1 주소에서 제2 주소로의 트랜잭션 데이터를 블록체인 네트워크(150)에 전송할 수 있다.

[45] 도 2는 전자 장치(110)에서 생성한 데이터가 서버(130)를 거쳐 블록체인 네트워크(150)로 전송되는 흐름도를 도시하고 있으나, 또 다른 실시 예에서, 전자 장치(110)는 생성한 데이터를 블록체인 네트워크(150)로 직접 전송할 수도 있다. 예를 들어, 전자 장치(110)는 제1 주소에서 제2 주소로의 복수 개의 트랜잭션에 대한 트랜잭션 데이터를 생성하여 메모리(예: 도 1의 보안 메모리(114))에 저장할 수 있다. 전자 장치(110)는 트랜잭션 데이터의 생성 여부만을 포함하는 데이터를 서버(130)에 전송할 수 있다. 서버(130)는 제1 주소에 대한 이상 트랜잭션을 검출함에 따라, 전자 장치(110)에 특정 조건을 만족하는 트랜잭션 데이터(예: 이상 트랜잭션보다 높은 수수료 정보를 포함하는 트랜잭션 데이터)를 서버(130)로 전송할 것을 요청하거나, 블록체인 네트워크(150)로 전송할 것을 요청할 수 있다.

[46] 도 3은 일 실시 예에 따른 전자 장치의 동작 흐름도를 도시한다. 도 3의 설명과 관련하여 전술한 내용과 대응되거나 동일 또는 유사한 내용은 생략될 수 있다.

[47] 일 실시 예에서, 도 3에 도시된 동작 301 내지 동작 307은 전자 장치(110)(예: 도 1의 전자 장치(110))의 프로세서(예: 도 1의 프로세서(116))에서 수행하는 것으로 이해될 수 있다.

[48] 도 3을 참조하면, 일 실시 예에 따른 전자 장치(110)는 동작 301에서 제1 키 쌍(key pair)을 생성할 수 있다. 일 실시 예에서, 전자 장치(110)는 루트 시드에 기반하여 제1 키 쌍을 생성할 수 있다. 제1 키 쌍은 제1 개인 키 및 제1 공개 키를 포함할 수 있다. 일 실시 예에서, 상기 루트 시드에 기반하여 계층 결정적 지갑(hierarchical deterministic wallet, HD wallet)이 생성될 수 있다. 계층 결정적 지갑은 HMAC-SHA512 알고리즘을 통해서 마스터 개인 키 및 마스터

체인코드를 생성할 수 있다. 계층 결정적 지갑은 상기 HMAC-SHA512를 통해 획득한 512비트의 해시된 값에서 왼쪽 256비트를 마스터 개인 키로 사용하고, 오른쪽 256비트를 마스터 체인코드로 사용할 수 있다. 일 실시 예에서, 마스터 공개 키는 타원곡선 함수를 이용하여 상기 마스터 개인 키로부터 획득될 수 있다. 계층 결정적 지갑은 트리 구조에서 생성된 키를 포함하고, 부모 키(예: 마스터 키)로부터 복수 개의 자식 키가 생성되고, 상기 복수 개의 자식 키로부터 복수 개의 손자 키가 생성될 수 있다. 일 실시 예에서, 루트 시드에 기반하여 개인 키, 공개 키 및 블록체인 주소가 유도될 수 있다.

[49] 일 실시 예에서, 상기 제1 개인 키는 보안 환경을 제공하는 전자 장치(110)의 보안 영역(예: 도 1의 보안 메모리(114))에 저장될 수 있다.

[50] 일 실시 예에서, 전자 장치(110)는 동작 303에서 제1 공개 키에 기반하여 제1 주소를 생성할 수 있다. 예를 들어, 전자 장치(110)는 제1 공개 키에 대하여 보안해시 알고리즘(SHA, Secure Hash Algorithm)을 통해 해시 값(제1 공개 키 해시)을 산출하고, 산출된 해시 값에 대하여 지정된 인코딩(예: Base58Check 인코딩)을 통해 주소를 생성할 수 있다. 생성된 주소는 제1 주소를 의미할 수 있다.

[51] 일 실시 예에서, 전자 장치(110)는 동작 305에서 제2 키 쌍(key pair)을 생성할 수 있다. 일 실시 예에서, 전자 장치(110)는 동작 307에서 제2 공개 키에 기반하여 제2 주소를 생성할 수 있다. 동작 305 및 동작 307에 대한 설명은 동작 301 및 동작 303의 설명에 대응할 수 있다.

[52] 일 실시 예에서, 전자 장치(110)는 동작 309에서 제1 개인 키를 통한 디지털 서명에 기반하여 제1 주소에서 제2 주소로의 복수 개의 트랜잭션에 대한 트랜잭션 데이터를 생성할 수 있다. 일 실시 예에서, 복수 개의 트랜잭션에 대한 트랜잭션 데이터는 서로 다른 수수료 정보를 포함할 수 있다. 또 다른 실시 예에서, 복수 개의 트랜잭션에 대한 수수료는 트랜잭션 데이터에 기반하여 계산될 수도 있다. 일 실시 예에서, 전자 장치(110)는 제1 주소에서 제2 주소로의 복수 개의 트랜잭션에 대한 트랜잭션 데이터에 대하여 제1 주소와 연관된 제1 개인 키를 통해 암호화할 수 있다. 예를 들어, 제1 개인 키를 통해 암호화된 트랜잭션 데이터의 무결성을 검증하기 위하여, 블록체인 노드(예: 도 1의 블록체인 노드(152))는 제1 개인 키와 키 쌍을 이루는 제1 공개 키를 통해 복호화할 수 있다. 일 실시 예에서, 전자 장치(110)는 복수 개의 트랜잭션에 대한 트랜잭션 데이터에 구분 플래그를 포함하도록 설정할 수 있다. 또 다른 실시 예에서, 전자 장치(110)는 복수 개의 트랜잭션에 대한 트랜잭션 데이터에 대하여 특정 구분 값(예: 제1 구분 값 “1” 또는 제2 구분 값 “0”)을 갖는 구분 플래그를 포함하도록 설정할 수도 있다.

[53] 일 실시 예에서, 전자 장치(110)는 동작 311에서 복수 개의 트랜잭션에 대한 데이터를 서버(130)에 전송할 수 있다. 일 실시 예에서, 전자 장치(110)는 제1 개인 키를 통해 암호화된 복수 개의 트랜잭션 데이터를 서버(130)에 전송할 수

있다.

[54] 도 4는 일 실시 예에 따른 이상 트랜잭션을 검출한 서버의 동작 흐름도를 도시한다. 도 4에 도시된 동작들은 도 2의 동작 209와 관련될 수 있다. 도 4의 설명과 관련하여 전술한 내용과 대응되거나 동일 또는 유사한 내용은 생략될 수 있다.

[55] 일 실시 예에서, 도 4에 도시된 동작 401 내지 동작 405는 서버(예: 도 1의 서버(130))의 프로세서(예: 도 1의 프로세서(136))에서 수행하는 것으로 이해될 수 있다.

[56] 도 4를 참조하면, 서버(130)는 동작 401에서 이상 트랜잭션의 수수료 정보를 확인할 수 있다. 일 실시 예에서, 트랜잭션 데이터는 트랜잭션 ID 정보, 트랜잭션 입력 값(예: 이전 트랜잭션 ID, 보내는 사람의 전자 서명) 및 트랜잭션 출력 값(예: 송금 금액, 수수료 정보, 받는 사람의 어드레스) 중 적어도 하나를 포함할 수 있다. 예를 들어, 서버(130)는 모니터링 상태인 제1 주소에서 2.1BTC를 가진 미사용 트랜잭션 출력 값(Vin)을 제2 주소로 1.98BTC를 전송(Vout)하는 이상 트랜잭션 데이터를 검출할 수 있다. 서버(130)는 이상 트랜잭션의 수수료 정보가 0.12BTC임을 확인할 수 있다.

[57] 일 실시 예에서, 서버(130)는 동작 403에서 복수 개의 트랜잭션 중 이상 트랜잭션보다 높은 수수료 정보를 포함하는 트랜잭션을 확인할 수 있다. 일 실시 예에서, 트랜잭션의 수수료 정보는 블록체인 네트워크(150)의 노드(예: 도 1의 블록체인 노드(152))에 전송되는 속도에 대응될 수 있다. 예를 들어, 트랜잭션의 수수료 정보가 0.2BTC인 제1 트랜잭션 데이터는 트랜잭션의 수수료 정보가 0.05BTC인 제2 트랜잭션 데이터보다 블록체인 노드(152)에 먼저 전송될 수 있다. 일 실시 예에서, 서버(130)는 이상 트랜잭션의 수수료 정보와 메모리(134)에 저장된 제1 주소에서 제2 주소로의 복수 개의 트랜잭션의 수수료 정보를 비교할 수 있다. 예를 들어, 서버(130)는 제1 트랜잭션이 이상 트랜잭션의 수수료 정보(0.12BTC)보다 큰 수수료 정보(0.2BTC)를 포함하고, 제2 트랜잭션이 이상 트랜잭션의 수수료 정보보다 작은 수수료 정보(0.05BTC)를 포함하는 것을 확인할 수 있다.

[58] 일 실시 예에서, 서버(130)는 동작 405에서 확인된 트랜잭션 데이터를 블록체인 네트워크(150)로 전송할 수 있다. 일 실시 예에서, 확인된 트랜잭션은 복수 개의 트랜잭션 중 이상 트랜잭션의 수수료 정보보다 높은 수수료 정보를 포함하는 트랜잭션을 의미할 수 있다. 예를 들어, 서버(130)는 복수 개의 트랜잭션 중 0.2BTC 수수료 정보를 포함하는 제1 트랜잭션 데이터를 블록체인 네트워크로 전송할 수 있다. 또 다른 실시 예에서, 복수 개의 트랜잭션 중 이상 트랜잭션보다 높은 수수료 정보를 포함하는 트랜잭션 데이터가 없는 것으로 확인되는 경우에, 서버(130)는 전자 장치(예: 도 1의 전자 장치(110))에 알림을 전송할 수도 있다.

[59] 도 5는 일 실시 예에 따른 전자 장치에서 운용되는 REE 및 TEE의 블록도를 도시한다.

[60] 도 5를 참조하면, 전자 장치(예: 도 1의 전자 장치(110))는 복수의 보안 레벨을 가진 실행 환경을 운용할 수 있다. 예를 들어, 복수의 보안 레벨을 가진 실행 환경은 REE(rich execution environment)(510) 및 TEE(trusted execution environment)(520)를 포함할 수 있다. REE(510)는 제1 보안 레벨을 가진 제1 실행 환경이고, TEE(520)는 제1 보안 레벨보다 높은 제2 보안 레벨을 가진 제2 실행 환경을 의미할 수 있다.

[61] 일 실시 예에서, REE(510)는 클라이언트 어플리케이션(512), TEE 클라이언트 API(514), Rich OS 컴포넌트(516) 및 REE 통신 에이전트(518)를 포함할 수 있다. 일 실시 예에서, 클라이언트 어플리케이션(512)은 전화, 메시지, 결제, 알람, 브라우저 또는 카메라와 같은 기능을 수행할 수 있는 하나 이상의 어플리케이션을 포함할 수 있다. 일 실시 예에서, TEE 클라이언트 API(514)는 TEE(520)에 접근이 허용되는 API로, REE(510)와 TEE(520)의 어플리케이션 간에 데이터를 교환할 수 있도록 설계된 인터페이스를 의미할 수 있다. 일 실시 예에서, Rich OS 컴포넌트(516)는 REE 통신 에이전트(518)를 포함하고, REE 통신 에이전트(518)를 통해 메시지 통신을 처리할 수 있다.

[62] 일 실시 예에서, TEE(520)는 높은 보안 레벨이 요구되는 데이터를 보안 환경 내에 저장하고 관리할 수 있다. 일 실시 예에서, 보안을 필요로 하는 데이터가 메모리에 저장되는 경우에, 메모리는 TEE를 통해서만 접근할 수 있는 설정 영역을 포함할 수 있다. 상기 설정 영역은 일반 메모리에 대하여 특정 메모리 주소를 포함하는 영역을 의미할 수 있다. 예를 들어, 상기 설정 영역은 루트 시드 및/또는 루트 시드에 기반하여 생성된 개인 키를 저장할 수 있다. 또 다른 실시 예에서, 보안을 필요로 하는 데이터가 메모리에 저장되는 경우에, 상기 데이터는 Trusted OS에서만 복호화 가능하도록 암호화하여 저장될 수도 있다. 예를 들어, 루트 시드 및/또는 루트 시드에 기반하여 생성된 개인 키는 Trusted OS에서만 복호화 가능하도록 암호화되어 일반 메모리에 저장될 수 있다. 일 실시 예에서, TEE(520)는 REE(510)와 하드웨어적으로 분리될 수 있다. 다른 실시 예에서, TEE(520)와 REE(510)는 동일한 하드웨어에 의해 구현되지만 소프트웨어적으로 분리될 수도 있다.

[63] 일 실시 예에서, TEE(520)는 신뢰 어플리케이션(522), TEE 내부 API(524), Trusted OS 컴포넌트(526) 및 모니터(528)를 포함할 수 있다. 일 실시 예에서, 신뢰 어플리케이션(522)은 DRM(digital rights management), 보안, 결제 또는 생체 정보 저장과 같은 기능을 수행할 수 있는 하나 이상의 어플리케이션을 포함할 수 있다. 일 실시 예에서, 모니터(528) 및 Trusted OS 컴포넌트(526)는 REE 통신 에이전트(518)로부터 수신된 메시지(예: SMC(secure monitor call))를 신뢰 어플리케이션(522)으로 전달할 수 있다. 일 실시 예에서, 모니터(528) 및 Trusted OS 컴포넌트(526)는 SMC 처리 함수를 호출하고, 신뢰 어플리케이션(522)을 실행할 수 있다. 일 실시 예에서, 신뢰 어플리케이션(522)은 SMC에 대응하여 보안 메모리(532)에 접근할 수 있다. 일 실시 예에서, TEE 내부 API(524)는

TEE(520)의 기본 소프트웨어가 동작할 수 있도록 제공되는 인터페이스를 의미할 수 있다.

[64] 일 실시 예에서, 하드웨어 플랫폼(530)은 보안 메모리(532)를 적어도 일부의 구성으로 포함할 수 있다. 일 실시 예에서, 하드웨어 플랫폼(530)은 Rich OS 컴포넌트(516)와 통신할 수 있으나, 보안 메모리(532)는 Trusted OS 컴포넌트(526)와만 통신할 수 있다. 일 실시 예에서, 보안 메모리(532)는 루트 시드 및/또는 루트 시드에 기반하여 생성된 개인 키를 저장할 수 있다. 일 실시 예에서, 개인 키가 저장된 보안 메모리(532)는 시스템 접근 권한을 제한할 수 있다. 예를 들어, 보안 메모리(532)는 사용자의 생체 인증 또는 PIN 번호 인증이 수행되는 경우에만 데이터(예: 개인 키)에 접근을 허용하도록 설정될 수 있다.

[65] 도 6a는 일 실시 예에 따른 전자 장치의 제1 UI 상태를 도시한다. 도 6b는 일 실시 예에 따른 전자 장치의 제2 UI 상태를 도시한다. 도 6c는 일 실시 예에 따른 전자 장치의 제3 UI 상태를 도시한다. 도 6d는 일 실시 예에 따른 전자 장치의 제4 UI 상태를 도시한다. 도 6e는 일 실시 예에 따른 전자 장치의 제5 UI 상태를 도시한다. 도 6f는 일 실시 예에 따른 전자 장치의 제6 UI 상태를 도시한다. 도 6a 내지 도 6f의 설명과 관련하여 전술한 내용과 대응되거나 동일 또는 유사한 내용은 생략될 수 있다.

[66] 도 6a를 참조하면, 전자 장치(110)(예: 도 1의 전자 장치(110))는 디스플레이(118)(예: 도 1의 디스플레이(118))를 통해 블록체인 월렛을 포함하는 제1 UI(600)를 제공할 수 있다. 제1 UI는 블록체인 잔액 정보(예: “예상 총 잔액”) 및 제1 주소 정보(예: “BTC 계좌 1”)(602)를 포함하는 블록체인 월렛을 표시할 수 있다. 일 실시 예에서, 블록체인 월렛은 적어도 하나의 주소 정보를 포함할 수 있고, 블록체인 잔액 정보는 적어도 하나의 주소 정보의 잔액을 합산한 금액 정보를 의미할 수 있다. 일 실시 예에서, 전자 장치(110)는 제1 주소 정보(602)를 표시하는 영역에 대한 터치 입력(604)을 수신할 수 있다.

[67] 도 6b를 참조하면, 전자 장치(110)는 디스플레이(118)를 통해 제1 주소에 대한 제어 화면을 포함하는 제2 UI(610)를 제공할 수 있다. 제2 UI는 제1 주소의 설정을 변경할 수 있는 객체를 포함할 수 있다. 일 실시 예에서, 전자 장치(110)는 제1 주소의 설정을 변경할 수 있는 객체 영역에 대한 터치 입력(612)을 수신할 수 있다.

[68] 도 6c를 참조하면, 전자 장치(110)는 디스플레이(118)를 통해 제1 주소의 설정 목록을 표시하는 제3 UI(620)를 제공할 수 있다. 일 실시 예에서, 제1 주소의 설정 목록은 “계좌 이름 편집”, “모니터링 계좌 설정” 및 “계좌 삭제” 중 적어도 하나를 포함할 수 있다. 일 실시 예에서, 전자 장치(110)는 제1 주소를 모니터링 계좌로 설정하는 터치 입력(622)을 수신할 수 있다.

[69] 도 6d를 참조하면, 전자 장치(110)는 디스플레이(118)를 통해 제2 주소를 만들기 위한 루트 시드(634)에 대한 복원 코드(예: 니모닉 코드)를 표시하는 제4 UI(630)를 제공할 수 있다. 일 실시 예에서, 전자 장치(110)는 제2 주소를 만들기

위한 루트 시드(634)를 생성하기 위하여 니모닉 코드(mnemonic code)(632)를 생성할 수 있다. 전자 장치(110)는 랜덤하게 128bits의 시퀀스를 생성할 수 있다. 전자 장치(110)는 시퀀스에 대하여 SHA 256 해시 함수를 이용하여 획득한 해시 값의 4bits를 체크섬으로 만들어 시퀀스의 끝에 추가할 수 있다. 전자 장치(110)는 체크섬이 추가된 시퀀스를 11bits의 단위로 자르고 미리 정의된 단어로 치환하여 니모닉 코드(632)를 생성할 수 있다. 도 6d는 단어가 중복되는 12개의 니모닉 코드(632)를 도시하고 있으나, 니모닉 코드는 서로 다른 단어로만 구성될 수도 있고, 24개의 단어로 구성될 수도 있다. 일 실시 예에서, 전자 장치(110)는 니모닉 코드(632)에 기반하여 루트 시드를 생성할 수 있고, 생성된 루트 시드에 기반하여 개인 키 및 공개 키를 생성할 수 있다. 일 실시 예에서, 전자 장치(110)는 외부(예: 사용자)에 니모닉 코드(632)를 별도로 기록해둘 것을 지시하는 알림을 표시할 수도 있다.

[70] 도 6e를 참조하면, 전자 장치(110)는 디스플레이(118)를 통해 제2 주소 생성이 완료된 제5 UI(640)를 제공할 수 있다. 일 실시 예에서, 제2 주소는 공개 키에 대하여 해시 함수를 통해 생성된 어드레스를 의미할 수 있다. 일 실시 예에서, 전자 장치(110)는 제2 주소 생성 과정이 완료하였음을 확인하는 터치 입력(642)을 수신할 수 있다.

[71] 도 6f를 참조하면, 전자 장치(110)는 디스플레이(118)를 통해 블록체인 월렛을 포함하는 제6 UI(650)를 제공할 수 있다. 제6 UI는 블록체인 잔액 정보(예: “예상 총 잔액”), 제1 주소 정보(예: “BTC 계좌 1”) 및 제2 주소 정보(예: “BTC 계좌 2(해킹 방지 계좌)”)(652)를 포함하는 블록체인 월렛을 표시할 수 있다. 도 6a 내지 도 6f는 이상 트랜잭션이 검출되는 경우 이를 무효화하기 위하여 해킹 방지 계좌만을 생성하는 UI만을 도시하고 있으나, 또 다른 실시 예에서 전자 장치(110)는 해킹 방지 계좌를 생성하고, 이어서 해킹 방지 트랜잭션을 생성하는 과정을 진행할 수도 있다.

[72] 도 7은 일 실시 예에 따른 해킹 방지 트랜잭션을 생성하는 전자 장치의 UI 상태를 도시한다.

[73] 도 7을 참조하면, 전자 장치(110)는 제1 주소의 미사용 트랜잭션 출력 값을 제1 주소로부터 제2 주소로 이전시키는 해킹 방지 트랜잭션을 생성하는 UI(700)를 표시할 수 있다. 일 실시 예에서, UI(700)의 “Recipient Address”는 제2 주소를 의미할 수 있다. 일 실시 예에서, 해킹 방지 트랜잭션은 수수료(fee) 정보의 설정 및/또는 변경을 통해 생성될 수 있다. 예를 들어, 송금 금액(amount) 및 수수료(fee) 정보를 설정하는 일반적인 트랜잭션과 달리, 해킹 방지 트랜잭션은 제1 주소의 미사용 트랜잭션 출력 값 전체를 제2 주소로 이전하는 트랜잭션이므로 사용자에 의해 수수료 정보만이 변경되어 설정될 수 있다. 제1 주소에 대한 총 잔액이 0.3012BTC인 경우에, 사용자가 해킹 방지 트랜잭션의 수수료를 0.001084BTC로 설정하면 송금 금액은 총 잔액에서 수수료를 제외한 0.300116BTC로 설정될 수 있다. 일 실시 예에서, 전자 장치(110)는 제1 주소에

대한 해킹 방지 트랜잭션을 복수 개 생성할 수 있고, 복수 개의 트랜잭션은 서로 다른 수수료 정보를 포함할 수 있다. 일 실시 예에서, 해킹 방지 트랜잭션의 수수료 정보는 블록체인 네트워크(예: 도 1의 블록체인 네트워크(150))의 메모리 풀에 대기중인 트랜잭션의 수수료 정보 시세를 고려하여 자동으로 설정될 수도 있다.

[74] 일 실시 예에서, 전자 장치(110)는 해킹 방지 트랜잭션에 대하여 확인하는 터치 입력(702)을 수신함에 따라, 사용자 인증(712)을 수행하기 위한 UI(710)를 표시할 수 있다. 일 실시 예에서, 해킹 방지 트랜잭션의 생성은 개인 키에 기반한 암호화 및 생체 인증 및/또는 PIN 번호 인증을 포함하는 사용자 인증을 통해 완료될 수 있다. 생체 인증 및/또는 PIN 번호 인증을 수행함에 따라 트랜잭션의 유효성 및 진위성이 증가할 수 있다. 일 실시 예에서, 전자 장치(110)는 생체 인증 및/또는 PIN 번호 인증이 수행되는 경우에만 보안 메모리(예: 도 1의 보안 메모리(114))에 저장된 데이터(예: 개인 키)에 접근할 수 있다.

[75] 도 8은 일 실시 예에 따른 복수 개의 트랜잭션을 생성하는 전자 장치의 UI 상태를 도시한다.

[76] 도 8의 상황 (a), (b) 및 (c)를 참조하면, 전자 장치(110)는 서로 다른 수수료 정보를 포함하는 해킹 방지 트랜잭션 생성 UI를 표시할 수 있다. 도 8의 상황 (a)는 해킹 방지 트랜잭션의 수수료(fee) 정보가 0.001084BTC로 설정된 UI(800)를 도시하고 있다. 도 8의 상황 (b)는 해킹 방지 트랜잭션의 수수료 정보가 0.000735BTC로 설정된 UI(810)를 도시하고 있다. 도 8의 상황 (c)는 해킹 방지 트랜잭션의 수수료 정보가 0.002397BTC로 설정된 UI(820)를 도시하고 있다. 일 실시 예에서, 도 8의 상황 (a) 내지 (c)와 같이 서로 다른 수수료 정보를 포함하는 복수 개의 해킹 방지 트랜잭션 생성 UI가 각각의 UI를 통해 표시되는 경우에는, 적어도 두 번 이상의 사용자 인증으로 해킹 방지 트랜잭션의 생성이 완료될 수 있다. 또 다른 실시 예에서, 서로 다른 수수료 정보를 포함하는 복수 개의 해킹 방지 트랜잭션 생성 UI가 하나의 UI를 통해 표시되는 경우에는, 한 번의 사용자 인증으로 해킹 방지 트랜잭션의 생성이 완료될 수 있다.

[77] 일 실시 예에서, 전자 장치(110)는 도 2의 동작 205와 같이 상황 (a) 내지 (c)를 통해 생성된 3개의 해킹 방지 트랜잭션을 서버(130)에 전송할 수 있다. 일 실시 예에서, 서버(130)는 도 4의 동작 401와 같이 제1 주소에 대한 이상 트랜잭션을 검출하면, 이상 트랜잭션의 수수료 정보를 확인할 수 있다. 일 실시 예에서, 서버(130)는 이상 트랜잭션의 수수료 정보보다 높은 수수료 정보를 포함하는 해킹 방지 트랜잭션의 트랜잭션 데이터를 블록체인 네트워크(150)에 전송할 수 있다. 예를 들어, 서버(130)는 제1 주소에 대한 이상 트랜잭션의 수수료 정보가 0.0014BTC로 설정되었음을 확인할 수 있다. 서버(130)는 이상 트랜잭션의 수수료 정보보다 높은 수수료 정보를 포함하는 해킹 방지 트랜잭션을 확인할 수 있다. 서버(130)는 상황 (a) 내지 (c)를 통해 생성된 3개의 해킹 방지 트랜잭션 중 상황 (c)를 통해 생성된 해킹 방지 트랜잭션이 이상 트랜잭션의 수수료 정보보다

높은 수수료 정보를 포함함을 확인할 수 있다. 서버(130)는 상황 (c)를 통해 생성된 해킹 방지 트랜잭션의 트랜잭션 데이터를 블록체인 네트워크(150)에 전송할 수 있다.

[78] 일 실시 예에서, 서버(130)는 이상 트랜잭션의 수수료 정보보다 높은 수수료 정보를 포함하는 해킹 방지 트랜잭션이 복수 개인 경우에는, 더 낮은 수수료 정보를 포함하는 해킹 방지 트랜잭션의 트랜잭션 데이터를 블록체인 네트워크(150)에 전송할 수 있다. 예를 들어, 서버(130)는 제1 주소에 대한 이상 트랜잭션의 수수료 정보가 0.0009BTC로 설정되었음을 확인할 수 있다. 서버(130)는 상황 (a) 내지 (c)를 통해 생성된 3개의 해킹 방지 트랜잭션 중 상황 (a) 및 (c)를 통해 생성된 해킹 방지 트랜잭션이 이상 트랜잭션의 수수료 정보보다 높은 수수료 정보를 포함함을 확인할 수 있다. 서버(130)는 상황 (a) 및 (c)를 통해 생성된 해킹 방지 트랜잭션 중 낮은 수수료 정보를 포함하는 상황 (a)를 통해 생성된 해킹 방지 트랜잭션의 트랜잭션 데이터를 블록체인 네트워크(150)에 전송할 수 있다. 일 실시 예에서, 해킹 방지 트랜잭션의 트랜잭션 데이터가 블록체인 네트워크(150)로 전송됨에 따라, 제1 주소의 전액은 제2 주소로 송금됨에 따라 트랜잭션이 완료될 수 있다.

[79] 도 9는 일 실시 예에 따른 트랜잭션 전송이 완료된 후 트랜잭션 시스템의 동작 흐름도를 도시한다. 도 9의 동작 901은 도 2의 동작 211에 대응될 수 있다. 따라서, 도 9의 설명과 관련하여 전술한 내용과 대응되거나 동일 또는 유사한 내용은 생략될 수 있다.

[80] 도 9를 참조하면, 서버(130)는 동작 901에서 복수 개의 트랜잭션 중 적어도 하나의 트랜잭션 데이터를 블록체인 네트워크(150)에 전송할 수 있다. 일 실시 예에서, 적어도 하나의 트랜잭션 데이터가 블록체인 네트워크(150)에 전송됨에 따라, 제1 주소에 대한 미사용 트랜잭션 출력 값은 소멸될 수 있다. 예를 들어, 도 8의 상황 (a) 내지 (c)를 통해 생성된 3개의 해킹 방지 트랜잭션 중 상황 (c)를 통해 생성된 해킹 방지 트랜잭션의 트랜잭션 데이터가 블록체인 네트워크(150)에 전송되는 경우에, 제1 주소에 대한 미사용 트랜잭션 출력 값은 소멸되므로 상황 (a) 및 (b)를 통해 생성된 나머지 2개의 해킹 방지 트랜잭션은 유효하지 않은 트랜잭션에 해당할 수 있다.

[81] 일 실시 예에서, 서버(130)는 동작 903에서 제2 주소에 대한 트랜잭션 완료 알림을 전자 장치(110)에 전송할 수 있다. 일 실시 예에서, 제2 주소에 대한 트랜잭션 완료 알림은 제1 주소에 대한 미사용 트랜잭션 출력 값의 소멸 정보를 포함할 수 있다. 일 실시 예에서, 제2 주소에 대한 트랜잭션 완료 알림에 응답하여, 전자 장치(110)는 제2 주소에 대한 모니터링 요청을 수신할 수 있다.

[82] 일 실시 예에서, 전자 장치(110)는 동작 905에서 제3 키 쌍(key pair)을 생성할 수 있다. 일 실시 예에서, 전자 장치(110)는 새로운 루트 시드에 기반하여 제3 키 쌍을 생성할 수 있다. 제3 키 쌍은 제3 개인 키 및 제3 공개 키를 포함할 수 있다. 일 실시 예에서, 제3 개인 키는 보안 환경을 제공하는 전자 장치(110)의 보안

영역(예: 도 1의 보안 메모리(114))에 저장될 수 있다.

[83] 일 실시 예에서, 전자 장치(110)는 동작 907에서 제3 공개 키에 기반하여 제3 주소를 생성할 수 있다. 일 실시 예에서, 전자 장치(110)는 동작 909에서 제2 개인 키를 통한 디지털 서명에 기반하여 제2 주소에서 제3 주소로의 복수 개의 트랜잭션 데이터를 생성할 수 있다. 일 실시 예에서, 전자 장치(110)는 동작 911에서 복수 개의 트랜잭션 데이터를 서버(130)에 전송할 수 있다.

[84] 도 10은 다양한 실시 예들에 따른 네트워크 환경 내의 전자 장치의 블록도를 도시한다.

[85] 도 10을 참조하면, 네트워크 환경(1000)에서 전자 장치(1001)는 제 1 네트워크(1098)(예: 근거리 무선 통신 네트워크)를 통하여 전자 장치(1002)와 통신하거나, 또는 제 2 네트워크(1099)(예: 원거리 무선 통신 네트워크)를 통하여 전자 장치(1004) 또는 서버(1008)와 통신할 수 있다. 일 실시 예에 따르면, 전자 장치(1001)는 서버(1008)를 통하여 전자 장치(1004)와 통신할 수 있다. 일 실시 예에 따르면, 전자 장치(1001)는 프로세서(1020), 메모리(1030), 입력 장치(1050), 음향 출력 장치(1055), 표시 장치(1060), 오디오 모듈(1070), 센서 모듈(1076), 인터페이스(1077), 햅틱 모듈(1079), 카메라 모듈(1080), 전력 관리 모듈(1088), 배터리(1089), 통신 모듈(1090), 가입자 식별 모듈(1096), 또는 안테나 모듈(1097)을 포함할 수 있다. 어떤 실시 예에서는, 전자 장치(1001)에는, 이 구성요소들 중 적어도 하나(예: 표시 장치(1060) 또는 카메라 모듈(1080))가 생략되거나, 하나 이상의 다른 구성 요소가 추가될 수 있다. 어떤 실시 예에서는, 이 구성요소들 중 일부들은 하나의 통합된 회로로 구현될 수 있다. 예를 들면, 센서 모듈(1076)(예: 지문 센서, 홍채 센서, 또는 조도 센서)은 표시 장치(1060)(예: 디스플레이)에 임베디드된 채 구현될 수 있다

[86] 프로세서(1020)는, 예를 들면, 소프트웨어(예: 프로그램(1040))를 실행하여 프로세서(1020)에 연결된 전자 장치(1001)의 적어도 하나의 다른 구성요소(예: 하드웨어 또는 소프트웨어 구성요소)을 제어할 수 있고, 다양한 데이터 처리 또는 연산을 수행할 수 있다. 일 실시 예에 따르면, 데이터 처리 또는 연산의 적어도 일부로서, 프로세서(1020)는 다른 구성요소(예: 센서 모듈(1076) 또는 통신 모듈(1090))로부터 수신된 명령 또는 데이터를 휘발성 메모리(1032)에 로드하고, 휘발성 메모리(1032)에 저장된 명령 또는 데이터를 처리하고, 결과 데이터를 비휘발성 메모리(1034)에 저장할 수 있다. 일 실시 예에 따르면, 프로세서(1020)는 메인 프로세서(1021)(예: 중앙 처리 장치 또는 어플리케이션 프로세서), 및 이와는 독립적으로 또는 함께 운영 가능한 보조 프로세서(1023)(예: 그래픽 처리 장치, 이미지 시그널 프로세서, 센서 허브 프로세서, 또는 커뮤니케이션 프로세서)를 포함할 수 있다. 추가적으로 또는 대체적으로, 보조 프로세서(1023)은 메인 프로세서(1021)보다 저전력을 사용하거나, 또는 지정된 기능에 특화되도록 설정될 수 있다. 보조 프로세서(1023)는 메인 프로세서(1021)와 별개로, 또는 그 일부로서 구현될 수

있다.

[87] 보조 프로세서(1023)는, 예를 들면, 메인 프로세서(1021)가 인액티브(예: 슬립) 상태에 있는 동안 메인 프로세서(1021)를 대신하여, 또는 메인 프로세서(1021)가 액티브(예: 어플리케이션 실행) 상태에 있는 동안 메인 프로세서(1021)와 함께, 전자 장치(1001)의 구성요소들 중 적어도 하나의 구성요소(예: 표시 장치(1060), 센서 모듈(1076), 또는 통신 모듈(1090))와 관련된 기능 또는 상태들의 적어도 일부를 제어할 수 있다. 일 실시 예에 따르면, 보조 프로세서(1023)(예: 이미지 시그널 프로세서 또는 커뮤니케이션 프로세서)는 기능적으로 관련 있는 다른 구성 요소(예: 카메라 모듈(1080) 또는 통신 모듈(1090))의 일부로서 구현될 수 있다.

[88] 메모리(1030)는, 전자 장치(1001)의 적어도 하나의 구성요소(예: 프로세서(1020) 또는 센서 모듈(1076))에 의해 사용되는 다양한 데이터를 저장할 수 있다. 데이터는, 예를 들어, 소프트웨어(예: 프로그램(1040)) 및, 이와 관련된 명령에 대한 입력 데이터 또는 출력 데이터를 포함할 수 있다. 메모리(1030)는, 휘발성 메모리(1032) 또는 비휘발성 메모리(1034)를 포함할 수 있다.

[89] 프로그램(1040)은 메모리(1030)에 소프트웨어로서 저장될 수 있으며, 예를 들면, 운영 체제(1042), 미들 웨어(1044) 또는 어플리케이션(1046)을 포함할 수 있다.

[90] 입력 장치(1050)는, 전자 장치(1001)의 구성요소(예: 프로세서(1020))에 사용될 명령 또는 데이터를 전자 장치(1001)의 외부(예: 사용자)로부터 수신할 수 있다. 입력 장치(1050)는, 예를 들면, 마이크, 마우스, 키보드, 또는 디지털 펜(예: 스타일러스 펜)을 포함할 수 있다.

[91] 음향 출력 장치(1055)는 음향 신호를 전자 장치(1001)의 외부로 출력할 수 있다. 음향 출력 장치(1055)는, 예를 들면, 스피커 또는 리시버를 포함할 수 있다. 스피커는 멀티미디어 재생 또는 녹음 재생과 같이 일반적인 용도로 사용될 수 있고, 리시버는 착신 전화를 수신하기 위해 사용될 수 있다. 일 실시 예에 따르면, 리시버는 스피커와 별개로, 또는 그 일부로서 구현될 수 있다.

[92] 표시 장치(1060)는 전자 장치(1001)의 외부(예: 사용자)로 정보를 시각적으로 제공할 수 있다. 표시 장치(1060)는, 예를 들면, 디스플레이, 홀로그램 장치, 또는 프로젝터 및 해당 장치를 제어하기 위한 제어 회로를 포함할 수 있다. 일 실시 예에 따르면, 표시 장치(1060)는 터치를 감지하도록 설정된 터치 회로(touch circuitry), 또는 상기 터치에 의해 발생되는 힘의 세기를 측정하도록 설정된 센서 회로(예: 압력 센서)를 포함할 수 있다.

[93] 오디오 모듈(1070)은 소리를 전기 신호로 변환시키거나, 반대로 전기 신호를 소리로 변환시킬 수 있다. 일 실시 예에 따르면, 오디오 모듈(1070)은, 입력 장치(1050)를 통해 소리를 획득하거나, 음향 출력 장치(1055), 또는 전자 장치(1001)와 직접 또는 무선으로 연결된 외부 전자 장치(예: 전자 장치(1002))(예: 스피커 또는 헤드폰))를 통해 소리를 출력할 수 있다.

[94] 센서 모듈(1076)은 전자 장치(1001)의 작동 상태(예: 전력 또는 온도), 또는 외부의 환경 상태(예: 사용자 상태)를 감지하고, 감지된 상태에 대응하는 전기 신호 또는 데이터 값을 생성할 수 있다. 일 실시 예에 따르면, 센서 모듈(1076)은, 예를 들면, 제스처 센서, 자이로 센서, 기압 센서, 마그네틱 센서, 가속도 센서, 그립 센서, 근접 센서, 컬러 센서, IR(infrared) 센서, 생체 센서, 온도 센서, 습도 센서, 또는 조도 센서를 포함할 수 있다.

[95] 인터페이스(1077)는 전자 장치(1001)가 외부 전자 장치(예: 전자 장치(1002))와 직접 또는 무선으로 연결되기 위해 사용될 수 있는 하나 이상의 지정된 프로토콜들을 지원할 수 있다. 일 실시 예에 따르면, 인터페이스(1077)는, 예를 들면, HDMI(high definition multimedia interface), USB(universal serial bus) 인터페이스, SD카드 인터페이스, 또는 오디오 인터페이스를 포함할 수 있다.

[96] 연결 단자(1078)는, 그를 통해서 전자 장치(1001)가 외부 전자 장치(예: 전자 장치(1002))와 물리적으로 연결될 수 있는 커넥터를 포함할 수 있다. 일 실시 예에 따르면, 연결 단자(1078)는, 예를 들면, HDMI 커넥터, USB 커넥터, SD 카드 커넥터, 또는 오디오 커넥터(예: 헤드폰 커넥터)를 포함할 수 있다.

[97] 햅틱 모듈(1079)은 전기적 신호를 사용자가 촉각 또는 운동 감각을 통해서 인지할 수 있는 기계적인 자극(예: 진동 또는 움직임) 또는 전기적인 자극으로 변환할 수 있다. 일 실시 예에 따르면, 햅틱 모듈(1079)은, 예를 들면, 모터, 압전 소자, 또는 전기 자극 장치를 포함할 수 있다.

[98] 카메라 모듈(1080)은 정지 영상 및 동영상을 촬영할 수 있다. 일 실시 예에 따르면, 카메라 모듈(1080)은 하나 이상의 렌즈들, 이미지 센서들, 이미지 시그널 프로세서들, 또는 플래시들을 포함할 수 있다.

[99] 전력 관리 모듈(1088)은 전자 장치(1001)에 공급되는 전력을 관리할 수 있다. 일 실시 예에 따르면, 전력 관리 모듈(388)은, 예를 들면, PMIC(power management integrated circuit)의 적어도 일부로서 구현될 수 있다.

[100] 배터리(1089)는 전자 장치(1001)의 적어도 하나의 구성 요소에 전력을 공급할 수 있다. 일 실시 예에 따르면, 배터리(1089)는, 예를 들면, 재충전 불가능한 1차 전지, 재충전 가능한 2차 전지 또는 연료 전지를 포함할 수 있다.

[101] 통신 모듈(1090)은 전자 장치(1001)와 외부 전자 장치(예: 전자 장치(1002), 전자 장치(1004), 또는 서버(1008))간의 직접(예: 유선) 통신 채널 또는 무선 통신 채널의 수립, 및 수립된 통신 채널을 통한 통신 수행을 지원할 수 있다. 통신 모듈(1090)은 프로세서(1020)(예: 어플리케이션 프로세서)와 독립적으로 운영되고, 직접(예: 유선) 통신 또는 무선 통신을 지원하는 하나 이상의 커뮤니케이션 프로세서를 포함할 수 있다. 일 실시 예에 따르면, 통신 모듈(1090)은 무선 통신 모듈(1092)(예: 셀룰러 통신 모듈, 근거리 무선 통신 모듈, 또는 GNSS(global navigation satellite system) 통신 모듈) 또는 유선 통신 모듈(1094)(예: LAN(local area network) 통신 모듈, 또는 전력선 통신 모듈)을 포함할 수 있다. 이들 통신 모듈 중 해당하는 통신 모듈은 제 1

네트워크(1098)(예: 블루투스, WiFi direct 또는 IrDA(infrared data association) 같은 근거리 통신 네트워크) 또는 제 2 네트워크(1099)(예: 셀룰러 네트워크, 인터넷, 또는 컴퓨터 네트워크(예: LAN 또는 WAN)와 같은 원거리 통신 네트워크)를 통하여 외부 전자 장치와 통신할 수 있다. 이런 여러 종류의 통신 모듈들은 하나의 구성 요소(예: 단일 칩)으로 통합되거나, 또는 서로 별도의 복수의 구성 요소들(예: 복수 칩들)로 구현될 수 있다. 무선 통신 모듈(1092)은 가입자 식별 모듈(1096)에 저장된 가입자 정보(예: 국제 모바일 가입자 식별자(IMSI))를 이용하여 제 1 네트워크(1098) 또는 제 2 네트워크(1099)와 같은 통신 네트워크 내에서 전자 장치(1001)를 확인 및 인증할 수 있다.

[102] 안테나 모듈(1097)은 신호 또는 전력을 외부(예: 외부 전자 장치)로 송신하거나 외부로부터 수신할 수 있다. 일 실시 예에 따르면, 안테나 모듈은 서브스트레이트(예: PCB) 위에 형성된 도전체 또는 도전성 패턴으로 이루어진 방사체를 포함하는 하나의 안테나를 포함할 수 있다. 일 실시 예에 따르면, 안테나 모듈(1097)은 복수의 안테나들을 포함할 수 있다. 이런 경우, 제 1 네트워크(1098) 또는 제 2 네트워크(1099)와 같은 통신 네트워크에서 사용되는 통신 방식에 적합한 적어도 하나의 안테나가, 예를 들면, 통신 모듈(1090)에 의하여 상기 복수의 안테나들로부터 선택될 수 있다. 신호 또는 전력은 상기 선택된 적어도 하나의 안테나를 통하여 통신 모듈(1090)과 외부 전자 장치 간에 송신되거나 수신될 수 있다. 어떤 실시 예에 따르면, 방사체 이외에 다른 부품(예: RFIC)이 추가로 안테나 모듈(1097)의 일부로 형성될 수 있다.

[103] 상기 구성요소들 중 적어도 일부는 주변 기기들간 통신 방식(예: 버스, GPIO(general purpose input and output), SPI(serial peripheral interface), 또는 MIPI(mobile industry processor interface))를 통해 서로 연결되고 신호(예: 명령 또는 데이터)를 상호간에 교환할 수 있다.

[104] 일 실시 예에 따르면, 명령 또는 데이터는 제 2 네트워크(1099)에 연결된 서버(1008)를 통해서 전자 장치(1001)와 외부의 전자 장치(1004)간에 송신 또는 수신될 수 있다. 전자 장치(1002, 1004) 각각은 전자 장치(1001)와 동일한 또는 다른 종류의 장치일 수 있다. 일 실시 예에 따르면, 전자 장치(1001)에서 실행되는 동작들의 전부 또는 일부는 외부 전자 장치들(1002, 1004 또는 1008) 중 하나 이상의 외부 장치들에서 실행될 수 있다. 예를 들면, 전자 장치(1001)가 어떤 기능이나 서비스를 자동으로, 또는 사용자 또는 다른 장치로부터의 요청에 반응하여 수행해야 할 경우에, 전자 장치(1001)는 기능 또는 서비스를 자체적으로 실행시키는 대신에 또는 추가적으로, 하나 이상의 외부 전자 장치들에게 그 기능 또는 그 서비스의 적어도 일부를 수행하라고 요청할 수 있다. 상기 요청을 수신한 하나 이상의 외부 전자 장치들은 요청된 기능 또는 서비스의 적어도 일부, 또는 상기 요청과 관련된 추가 기능 또는 서비스를 실행하고, 그 실행의 결과를 전자 장치(1001)로 전달할 수 있다. 전자 장치(1001)는 상기 결과를, 그대로 또는 추가적으로 처리하여, 상기 요청에 대한

응답의 적어도 일부로서 제공할 수 있다. 이를 위하여, 예를 들면, 클라우드 컴퓨팅, 분산 컴퓨팅, 또는 클라이언트-서버 컴퓨팅 기술이 이용될 수 있다.

[105] 도 11은 다양한 실시예에 따른 프로그램을 예시하는 블록도를 도시한다.

[106] 도 11은 다양한 실시 예에 따른 프로그램(1040)을 예시하는 블록도(1100)이다. 일 실시 예에 따르면, 프로그램(1040)은 전자 장치(1001)의 하나 이상의 리소스들을 제어하기 위한 운영 체제(1042), 미들웨어(1044), 또는 상기 운영 체제(1042)에서 실행 가능한 어플리케이션(1046)을 포함할 수 있다. 운영 체제(1042)는, 예를 들면, Android™, iOS™, Windows™, Symbian™, Tizen™, 또는 Bada™를 포함할 수 있다. 프로그램(1040) 중 적어도 일부 프로그램은, 예를 들면, 제조 시에 전자 장치(1001)에 프리로드되거나, 또는 사용자에 의해 사용 시 외부 전자 장치(예: 전자 장치(1002 또는 1004), 또는 서버(1008))로부터 다운로드되거나 갱신될 수 있다.

[107] 운영 체제(1042)는 전자 장치(1001)의 하나 이상의 시스템 리소스들(예: 프로세스, 메모리, 또는 전원)의 관리(예: 할당 또는 회수)를 제어할 수 있다. 운영 체제(1042)는, 추가적으로 또는 대체적으로, 전자 장치(1001)의 다른 하드웨어 디바이스, 예를 들면, 입력 장치(1050), 음향 출력 장치(1055), 표시 장치(1060), 오디오 모듈(1070), 센서 모듈(1076), 인터페이스(1077), 햅틱 모듈(1079), 카메라 모듈(1080), 전력 관리 모듈(1088), 배터리(1089), 통신 모듈(1090), 가입자 식별 모듈(1096), 또는 안테나 모듈(1097)을 구동하기 위한 하나 이상의 드라이버 프로그램들을 포함할 수 있다.

[108] 미들웨어(1044)는 전자 장치(1001)의 하나 이상의 리소스들로부터 제공되는 기능 또는 정보가 어플리케이션(1046)에 의해 사용될 수 있도록 다양한 기능들을 어플리케이션(1046)으로 제공할 수 있다. 미들웨어(1044)는, 예를 들면, 어플리케이션 매니저(1101), 윈도우 매니저(1103), 멀티미디어 매니저(1105), 리소스 매니저(1107), 파워 매니저(1109), 데이터베이스 매니저(1111), 패키지 매니저(1113), 커넥티비티 매니저(1115), 노티피케이션 매니저(1117), 로케이션 매니저(1119), 그래픽 매니저(1121), 시큐리티 매니저(1123), 통화 매니저(1125), 또는 음성 인식 매니저(1127)를 포함할 수 있다.

[109] 어플리케이션 매니저(1101)는, 예를 들면, 어플리케이션(1046)의 생명 주기를 관리할 수 있다. 윈도우 매니저(1103)는, 예를 들면, 화면에서 사용되는 하나 이상의 GUI 자원들을 관리할 수 있다. 멀티미디어 매니저(1105)는, 예를 들면, 미디어 파일들의 재생에 필요한 하나 이상의 포맷들을 파악하고, 그 중 선택된 해당하는 포맷에 맞는 코덱을 이용하여 상기 미디어 파일들 중 해당하는 미디어 파일의 인코딩 또는 디코딩을 수행할 수 있다. 리소스 매니저(1107)는, 예를 들면, 어플리케이션(1046)의 소스 코드 또는 메모리(1030)의 메모리의 공간을 관리할 수 있다. 파워 매니저(1109)는, 예를 들면, 배터리(1089)의 용량, 온도 또는 전원을 관리하고, 이 중 해당 정보를 이용하여 전자 장치(1001)의 동작에 필요한 관련 정보를 결정 또는 제공할 수 있다. 일 실시 예에 따르면, 파워 매니저(1109)는

전자 장치(1001)의 바이오스(BIOS: basic input/output system)(미도시)와 연동할 수 있다.

[110] 데이터베이스 매니저(1111)는, 예를 들면, 어플리케이션(1046)에 의해 사용될 데이터베이스를 생성, 검색, 또는 변경할 수 있다. 패키지 매니저(1113)는, 예를 들면, 패키지 파일의 형태로 배포되는 어플리케이션의 설치 또는 갱신을 관리할 수 있다. 커넥티비티 매니저(1115)는, 예를 들면, 전자 장치(1001)와 외부 전자 장치 간의 무선 연결 또는 직접 연결을 관리할 수 있다. 노티피케이션 매니저(1117)는, 예를 들면, 지정된 이벤트(예: 착신 통화, 메시지, 또는 알람)의 발생을 사용자에게 알리기 위한 기능을 제공할 수 있다. 로케이션 매니저(1119)는, 예를 들면, 전자 장치(1001)의 위치 정보를 관리할 수 있다. 그래픽 매니저(1121)는, 예를 들면, 사용자에게 제공될 하나 이상의 그래픽 효과들 또는 이와 관련된 사용자 인터페이스를 관리할 수 있다.

[111] 시큐리티 매니저(1123)는, 예를 들면, 시스템 보안 또는 사용자 인증을 제공할 수 있다. 통화(telephony) 매니저(1125)는, 예를 들면, 전자 장치(1001)에 의해 제공되는 음성 통화 기능 또는 영상 통화 기능을 관리할 수 있다. 음성 인식 매니저(1127)는, 예를 들면, 사용자의 음성 데이터를 서버(1008)로 전송하고, 그 음성 데이터에 적어도 일부 기반하여 전자 장치(1001)에서 수행될 기능에 대응하는 명령어(command), 또는 그 음성 데이터에 적어도 일부 기반하여 변환된 문자 데이터를 서버(1008)로부터 수신할 수 있다. 일 실시 예에 따르면, 미들웨어(1144)는 동적으로 기존의 구성요소를 일부 삭제하거나 새로운 구성요소들을 추가할 수 있다. 일 실시 예에 따르면, 미들웨어(1044)의 적어도 일부는 운영 체제(1042)의 일부로 포함되거나, 또는 운영 체제(1042)와는 다른 별도의 소프트웨어로 구현될 수 있다.

[112] 어플리케이션(1046)은, 예를 들면, 홈(1151), 다이얼러(1153), SMS/MMS(1155), IM(instant message)(1157), 브라우저(1159), 카메라(1161), 알람(1163), 컨택트(1165), 음성 인식(1167), 이메일(1169), 달력(1171), 미디어 플레이어(1173), 앨범(1175), 와치(1177), 헬스(1179)(예: 운동량 또는 혈당과 같은 생체 정보를 측정), 또는 환경 정보(1181)(예: 기압, 습도, 또는 온도 정보 측정) 어플리케이션을 포함할 수 있다. 일 실시 예에 따르면, 어플리케이션(1046)은 전자 장치(1001)와 외부 전자 장치 사이의 정보 교환을 지원할 수 있는 정보 교환 어플리케이션(미도시)을 더 포함할 수 있다. 정보 교환 어플리케이션은, 예를 들면, 외부 전자 장치로 지정된 정보 (예: 통화, 메시지, 또는 알람)를 전달하도록 설정된 노티피케이션 릴레이 어플리케이션, 또는 외부 전자 장치를 관리하도록 설정된 장치 관리 어플리케이션을 포함할 수 있다. 노티피케이션 릴레이 어플리케이션은, 예를 들면, 전자 장치(1001)의 다른 어플리케이션(예: 이메일 어플리케이션(1169))에서 발생된 지정된 이벤트(예: 메일 수신)에 대응하는 알림 정보를 외부 전자 장치로 전달할 수 있다. 추가적으로 또는 대체적으로, 노티피케이션 릴레이 어플리케이션은 외부 전자 장치로부터 알림 정보를

수신하여 전자 장치(1001)의 사용자에게 제공할 수 있다.

[113] 장치 관리 어플리케이션은, 예를 들면, 전자 장치(1001)와 통신하는 외부 전자 장치 또는 그 일부 구성 요소(예: 표시 장치(1060) 또는 카메라 모듈(1080))의 전원(예: 턴-온 또는 턴-오프) 또는 기능(예: 표시 장치(1060) 또는 카메라 모듈(1080)의 밝기, 해상도, 또는 포커스)을 제어할 수 있다. 장치 관리 어플리케이션은, 추가적으로 또는 대체적으로, 외부 전자 장치에서 동작하는 어플리케이션의 설치, 삭제, 또는 갱신을 지원할 수 있다.

[114] 본 문서에 개시된 다양한 실시 예들에 따른 전자 장치는 다양한 형태의 장치가 될 수 있다. 전자 장치는, 예를 들면, 휴대용 통신 장치 (예: 스마트폰), 컴퓨터 장치, 휴대용 멀티미디어 장치, 휴대용 의료 기기, 카메라, 웨어러블 장치, 또는 가전 장치를 포함할 수 있다. 본 문서의 실시 예에 따른 전자 장치는 전술한 기기들에 한정되지 않는다.

[115] 본 문서의 다양한 실시 예들 및 이에 사용된 용어들은 본 문서에 기재된 기술적 특징들을 특정한 실시 예들로 한정하려는 것이 아니며, 해당 실시 예의 다양한 변경, 균등물, 또는 대체물을 포함하는 것으로 이해되어야 한다. 도면의 설명과 관련하여, 유사한 또는 관련된 구성요소에 대해서는 유사한 참조 부호가 사용될 수 있다. 아이템에 대응하는 명사의 단수 형은 관련된 문맥상 명백하게 다르게 지시하지 않는 한, 상기 아이템 한 개 또는 복수 개를 포함할 수 있다. 본 문서에서, "A 또는 B", "A 및 B 중 적어도 하나",“A 또는 B 중 적어도 하나,””A, B 또는 C," "A, B 및 C 중 적어도 하나,”및 “A, B, 또는 C 중 적어도 하나"와 같은 문구들 각각은 그 문구들 중 해당하는 문구에 함께 나열된 항목들 중 어느 하나, 또는 그들의 모든 가능한 조합을 포함할 수 있다. "제 1", "제 2", 또는 "첫째" 또는 "둘째"와 같은 용어들은 단순히 해당 구성요소를 다른 해당 구성요소와 구분하기 위해 사용될 수 있으며, 해당 구성요소들을 다른 측면(예: 중요성 또는 순서)에서 한정하지 않는다. 어떤(예: 제 1) 구성요소가 다른(예: 제 2) 구성요소에, “기능적으로” 또는 “통신적으로”라는 용어와 함께 또는 이런 용어 없이, “커플드” 또는 “커넥티드”라고 언급된 경우, 그것은 상기 어떤 구성요소가 상기 다른 구성요소에 직접적으로(예: 유선으로), 무선으로, 또는 제 3 구성요소를 통하여 연결될 수 있다는 것을 의미한다.

[116] 본 문서에서 사용된 용어 "모듈"은 하드웨어, 소프트웨어 또는 펌웨어로 구현된 유닛을 포함할 수 있으며, 예를 들면, 로직, 논리 블록, 부품, 또는 회로 등의 용어와 상호 호환적으로 사용될 수 있다. 모듈은, 일체로 구성된 부품 또는 하나 또는 그 이상의 기능을 수행하는, 상기 부품의 최소 단위 또는 그 일부가 될 수 있다. 예를 들면, 일 실시 예에 따르면, 모듈은 ASIC(application-specific integrated circuit)의 형태로 구현될 수 있다.

[117] 본 문서의 다양한 실시 예들은 기기(machine)(예: 전자 장치(1001)) 의해 읽을 수 있는 저장 매체(storage medium)(예: 내장 메모리(1036) 또는 외장 메모리(1038))에 저장된 하나 이상의 명령어들을 포함하는 소프트웨어(예:

프로그램(1040))로서 구현될 수 있다. 예를 들면, 기기(예: 전자 장치(1001))의 프로세서(예: 프로세서(1020))는, 저장 매체로부터 저장된 하나 이상의 명령어들 중 적어도 하나의 명령을 호출하고, 그것을 실행할 수 있다. 이것은 기기가 상기 호출된 적어도 하나의 명령어에 따라 적어도 하나의 기능을 수행하도록 운영되는 것을 가능하게 한다. 상기 하나 이상의 명령어들은 컴파일러에 의해 생성된 코드 또는 인터프리터에 의해 실행될 수 있는 코드를 포함할 수 있다. 기기로 읽을 수 있는 저장매체는, 비일시적(non-transitory) 저장매체의 형태로 제공될 수 있다. 여기서, '비일시적'은 저장매체가 실재(tangible)하는 장치이고, 신호(signal)(예: 전자기파)를 포함하지 않는다는 것을 의미할 뿐이며, 이 용어는 데이터가 저장매체에 반영구적으로 저장되는 경우와 임시적으로 저장되는 경우를 구분하지 않는다.

[118] 일 실시 예에 따르면, 본 문서에 개시된 다양한 실시 예들에 따른 방법은 컴퓨터 프로그램 제품(computer program product)에 포함되어 제공될 수 있다. 컴퓨터 프로그램 제품은 상품으로서 판매자 및 구매자 간에 거래될 수 있다. 컴퓨터 프로그램 제품은 기기로 읽을 수 있는 저장 매체(예: compact disc read only memory (CD-ROM))의 형태로 배포되거나, 또는 어플리케이션 스토어(예: 플레이 스토어™)를 통해 또는 두개의 사용자 장치들(예: 스마트폰들) 간에 직접, 온라인으로 배포(예: 다운로드 또는 업로드)될 수 있다. 온라인 배포의 경우에, 컴퓨터 프로그램 제품의 적어도 일부는 제조사의 서버, 어플리케이션 스토어의 서버, 또는 중계 서버의 메모리와 같은 기기로 읽을 수 있는 저장 매체에 적어도 일시 저장되거나, 임시적으로 생성될 수 있다.

[119] 다양한 실시 예들에 따르면, 상기 기술한 구성요소들의 각각의 구성요소(예: 모듈 또는 프로그램)는 단수 또는 복수의 개체를 포함할 수 있다. 다양한 실시 예들에 따르면, 전술한 해당 구성요소들 중 하나 이상의 구성요소들 또는 동작들이 생략되거나, 또는 하나 이상의 다른 구성요소들 또는 동작들이 추가될 수 있다. 대체적으로 또는 추가적으로, 복수의 구성요소들(예: 모듈 또는 프로그램)은 하나의 구성요소로 통합될 수 있다. 이런 경우, 통합된 구성요소는 상기 복수의 구성요소들 각각의 구성요소의 하나 이상의 기능들을 상기 통합 이전에 상기 복수의 구성요소들 중 해당 구성요소에 의해 수행되는 것과 동일 또는 유사하게 수행할 수 있다. 다양한 실시 예들에 따르면, 모듈, 프로그램 또는 다른 구성요소에 의해 수행되는 동작들은 순차적으로, 병렬적으로, 반복적으로, 또는 휴리스틱하게 실행되거나, 상기 동작들 중 하나 이상이 다른 순서로 실행되거나, 생략되거나, 또는 하나 이상의 다른 동작들이 추가될 수 있다.

청구범위

[청구항 1] 전자 장치에 있어서,
통신회로;
보안 메모리; 및
상기 통신회로 및 상기 보안 메모리와 연결되는 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는:
제1 공개 키(public key) 및 제1 개인 키(private key)를 포함하는 제1 키 쌍을 생성하고, 상기 제1 개인 키는 상기 보안 메모리에 저장되며,
상기 제1 공개 키에 기반하여 제1 주소를 생성하고,
상기 제1 공개 키와 구별되는 제2 공개 키 및 상기 제1 개인 키와 구별되는 제2 개인 키를 포함하는 제2 키 쌍을 생성하고
상기 제2 공개 키에 기반하여 제2 주소를 생성하고,
상기 제1 개인 키를 통한 디지털 서명에 기반하여, 상기 제1 주소의 미사용 트랜잭션 출력 값을 상기 제1 주소로부터 상기 제2 주소로 이전시키는 복수 개의 트랜잭션들에 대한 트랜잭션 데이터를 생성하도록 설정되는, 전자 장치.

[청구항 2] 청구항 1에 있어서,
상기 복수 개의 트랜잭션들에 대한 상기 트랜잭션 데이터는 서로 다른 수수료 정보를 포함하는 것을 특징으로 하는, 전자 장치.

[청구항 3] 청구항 2에 있어서,
서버를 통해 상기 제1 주소에 대한 이상 트랜잭션이 검출되면, 상기 복수 개의 트랜잭션들 중 상기 이상 트랜잭션의 수수료 정보보다 높은 수수료 정보를 포함하는 트랜잭션에 대한 트랜잭션 데이터가 상기 블록체인 네트워크로 전송되는 것을 특징으로 하는, 전자 장치.

[청구항 4] 청구항 1에 있어서,
상기 적어도 하나의 프로세서는:
상기 복수 개의 트랜잭션들 중 적어도 하나의 트랜잭션에 대한 트랜잭션 데이터가 상기 블록체인 네트워크로 전송됨에 응답하여, 디스플레이를 통해 상기 제2 주소에 대한 트랜잭션 완료 알림을 표시하도록 설정되는, 전자 장치.

[청구항 5] 청구항 4에 있어서,
상기 적어도 하나의 프로세서는:
상기 제2 주소에 대한 모니터링 요청에 응답하여, 제3 공개 키 및 제3 개인 키를 포함하는 제3 키 쌍을 생성하고, 상기 제3 개인 키는 상기 보안 메모리에 저장되며,
상기 제3 공개 키에 기반하여 제3 주소를 생성하도록 설정되는, 전자 장치.

[청구항 6] 청구항 5에 있어서,
상기 적어도 하나의 프로세서는, 상기 제2 개인 키를 통한 디지털 서명에 기반하여 상기 제2 주소로부터 상기 제3 주소에 대한 복수 개의 트랜잭션들을 생성하도록 설정되는, 전자 장치.

[청구항 7] 청구항 1에 있어서,
상기 복수 개의 트랜잭션들은 구분 플래그를 포함하는 것을 특징으로 하는, 전자 장치.

[청구항 8] 청구항 1에 있어서,
상기 적어도 하나의 프로세서는, 새로운 루트 시드(root seed)를 생성하고, 상기 새로운 루트 시드에 기반하여 상기 제2 키 쌍을 생성하도록 설정되는, 전자 장치.

[청구항 9] 청구항 1에 있어서,
디스플레이를 더 포함하고,
상기 적어도 하나의 프로세서는,
상기 제2 주소에 대한 정보를 상기 디스플레이를 통해서 표시하고,
상기 복수 개의 트랜잭션들에 대한 수수료 정보를 설정하는 사용자 인터페이스를 표시하며,
상기 사용자 인터페이스를 통해서 입력된 수수료 정보에 기초하여 상기 복수 개의 트랜잭션들을 생성하는, 전자 장치.

[청구항 10] 전자 장치의 동작 방법에 있어서,
제1 공개 키(public key) 및 제1 개인 키(private key)를 포함하는 제1 키 쌍을 생성하는 동작, 상기 제1 개인 키는 보안 메모리에 저장됨;
상기 제1 공개 키에 기반하여 제1 주소를 생성하는 동작;
상기 제1 공개 키와 구별되는 제2 공개 키 및 상기 제1 개인 키와 구별되는 제2 개인 키를 포함하는 제2 키 쌍을 생성하는 동작;
상기 제2 공개 키에 기반하여 제2 주소를 생성하는 동작; 및
상기 제1 개인 키를 통한 디지털 서명에 기반하여, 상기 제1 주소의 미사용 트랜잭션 출력 값을 상기 제1 주소로부터 상기 제2 주소로 이전시키는 복수 개의 트랜잭션들에 대한 트랜잭션 데이터를 생성하는 동작을 포함하는 동작 방법.

[청구항 11] 청구항 10에 있어서,
상기 복수 개의 트랜잭션들에 대한 상기 트랜잭션 데이터는 서로 다른 수수료 정보를 포함하는 것을 특징으로 하는, 동작 방법.

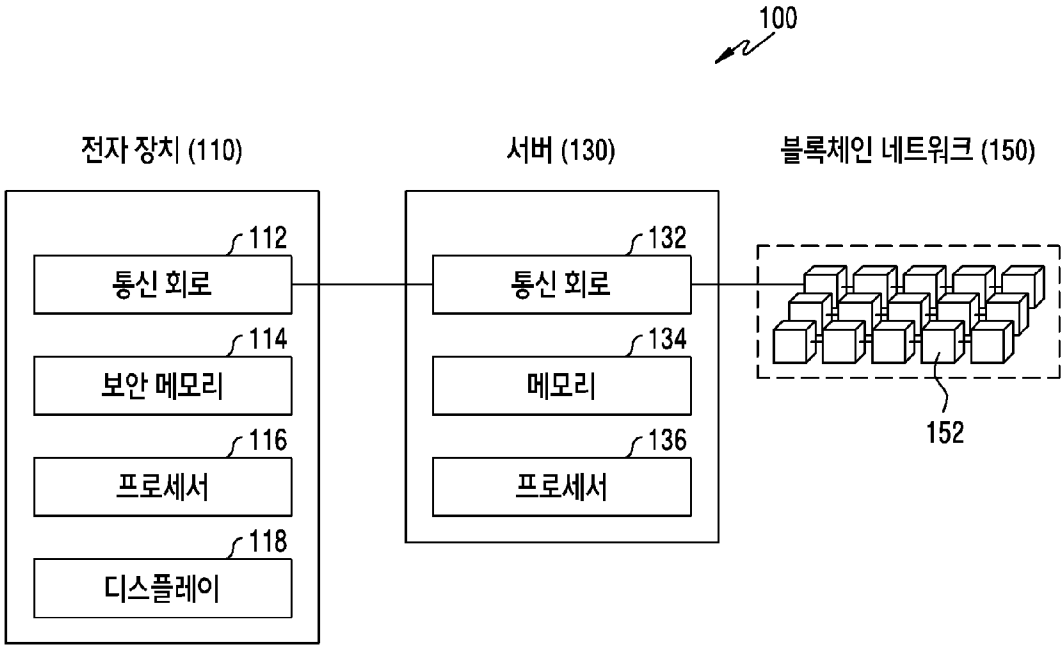
[청구항 12] 청구항 11에 있어서,
서버를 통해 상기 제1 주소에 대한 이상 트랜잭션이 검출되면, 상기 복수 개의 트랜잭션들 중 상기 이상 트랜잭션의 수수료 정보보다 높은 수수료 정보를 포함하는 트랜잭션에 대한 트랜잭션 데이터가 상기 블록체인 네트워크로 전송되는 것을 특징으로 하는, 동작 방법.

[청구항 13] 청구항 10에 있어서,
상기 복수 개의 트랜잭션들 중 적어도 하나의 트랜잭션에 대한 트랜잭션 데이터가 상기 블록체인 네트워크로 전송됨에 응답하여, 디스플레이를 통해 상기 제2 주소에 대한 트랜잭션 완료 알림을 표시하는 동작을 더 포함하는, 동작 방법.

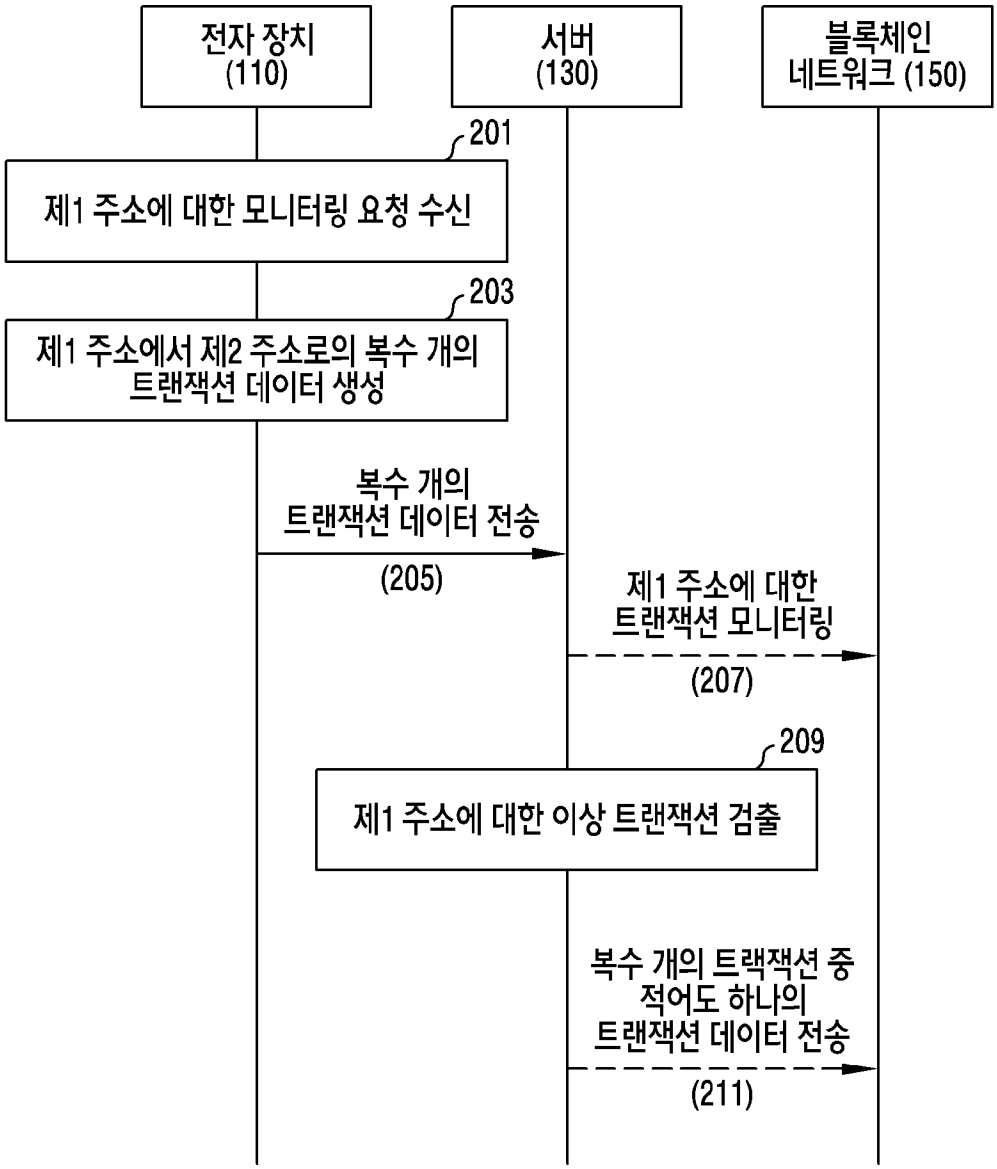
[청구항 14] 청구항 13에 있어서,
상기 제2 주소에 대한 모니터링 요청에 응답하여, 제3 공개 키 및 제3 개인 키를 포함하는 제3 키 쌍을 생성하는 동작, 상기 제3 개인 키는 상기 보안 메모리에 저장됨;
상기 제3 공개 키에 기반하여 제3 주소를 생성하는 동작을 더 포함하는, 동작 방법.

[청구항 15] 청구항 14에 있어서,
상기 제2 개인 키를 통한 디지털 서명에 기반하여 상기 제2 주소로부터 상기 제3 주소에 대한 복수 개의 트랜잭션들을 생성하는 동작을 더 포함하는, 동작 방법.

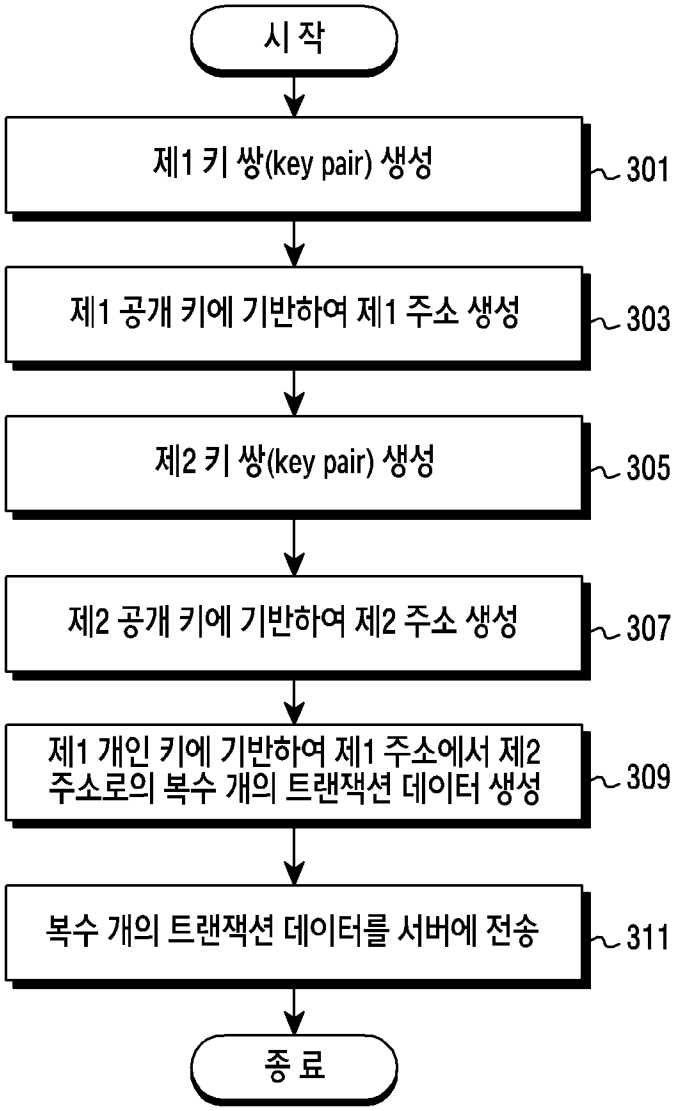
[도1]


100
전자 장치 (110)
서버 (130)
블록체인 네트워크 (150)
112
통신 회로
114
보안 메모리
116
프로세서
118
디스플레이
132
통신 회로
134
메모리
136
프로세서
152

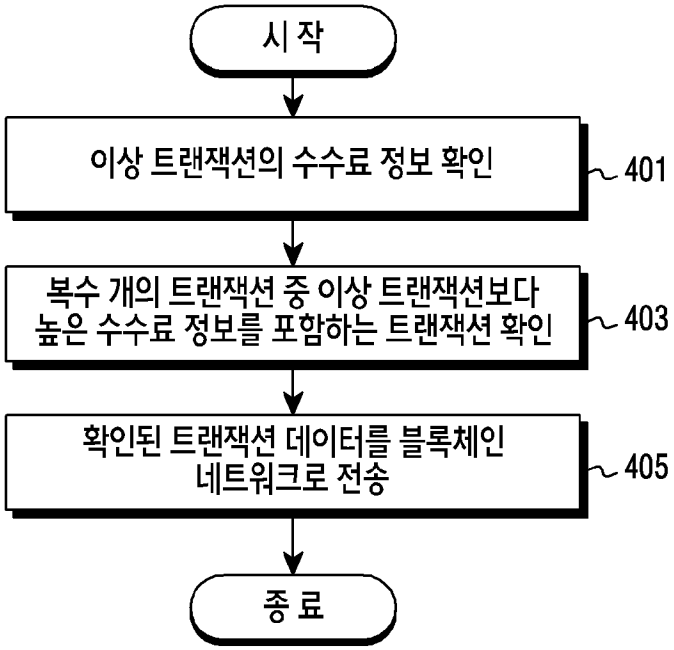
[도2]


전자 장치 (110)
서버 (130)
블록체인 네트워크 (150)
201
제1 주소에 대한 모니터링 요청 수신
203
제1 주소에서 제2 주소로의 복수 개의 트랜잭션 데이터 생성
복수 개의 트랜잭션 데이터 전송
(205)
제1 주소에 대한 트랜잭션 모니터링
(207)
209
제1 주소에 대한 이상 트랜잭션 검출
복수 개의 트랙잭션 중 적어도 하나의 트랜잭션 데이터 전송
(211)

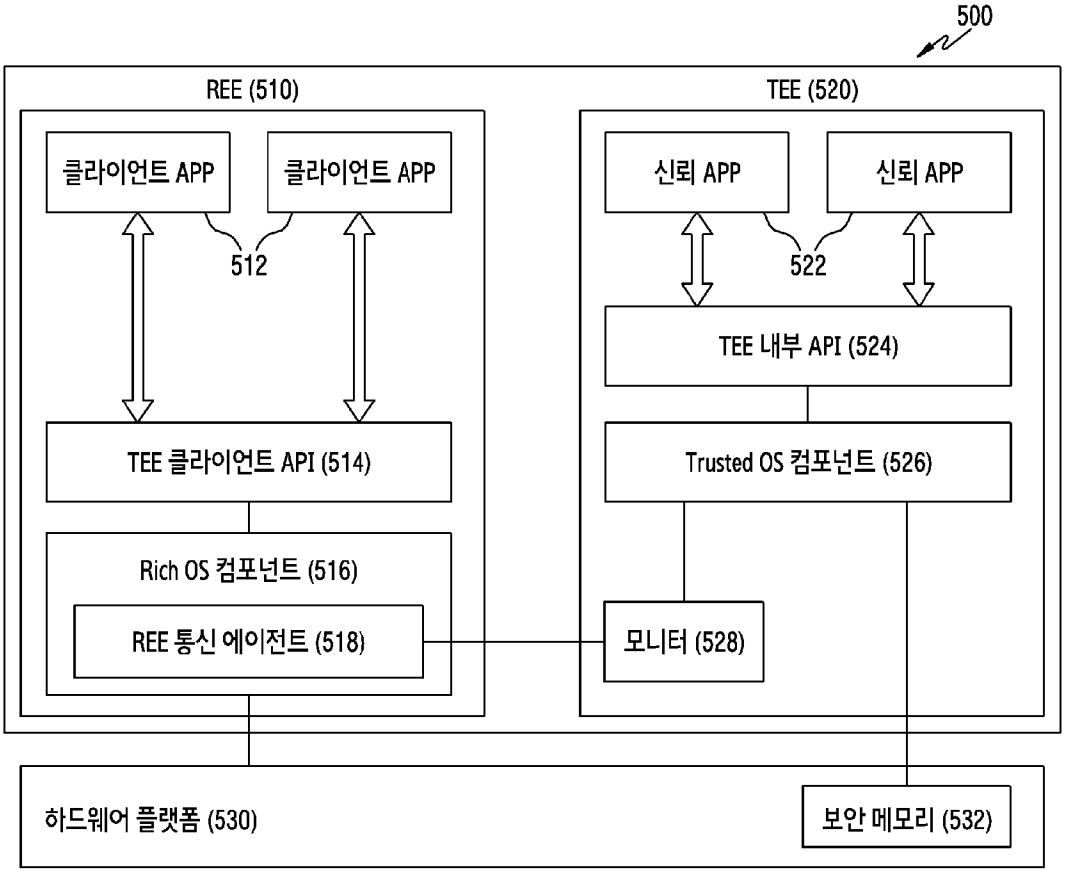
[도3]


시 작
제1 키 쌍(key pair) 생성
301
제1 공개 키에 기반하여 제1 주소 생성
303
제2 키 쌍(key pair) 생성
305
제2 공개 키에 기반하여 제2 주소 생성
307
제1 개인 키에 기반하여 제1 주소에서 제2 주소로의 복수 개의 트랜잭션 데이터 생성
309
복수 개의 트랜잭션 데이터를 서버에 전송
311
종 료

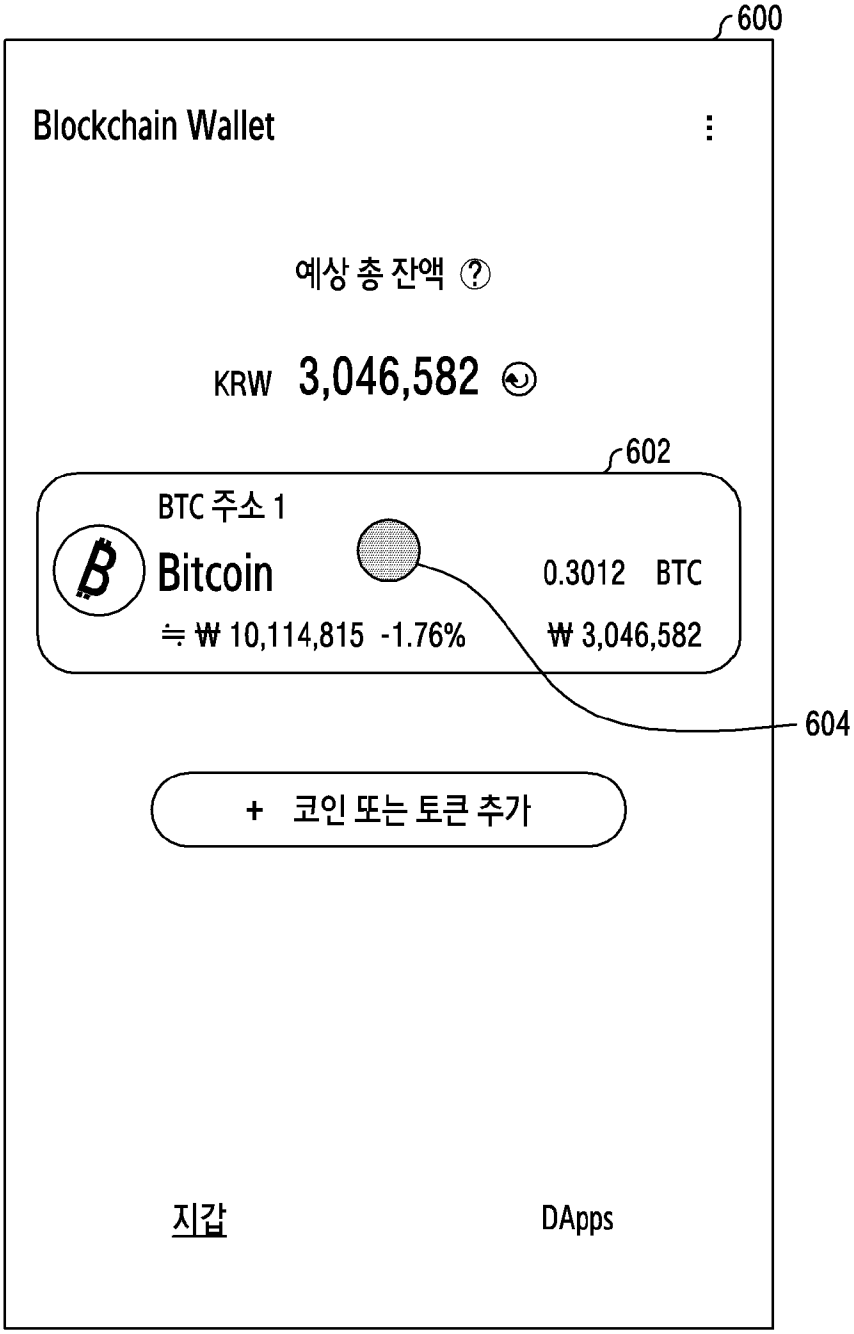
[도4]


시 작
이상 트랜잭션의 수수료 정보 확인
401
복수 개의 트랜잭션 중 이상 트랜잭션보다 높은 수수료 정보를 포함하는 트랜잭션 확인
403
확인된 트랜잭션 데이터를 블록체인 네트워크로 전송
405
종 료

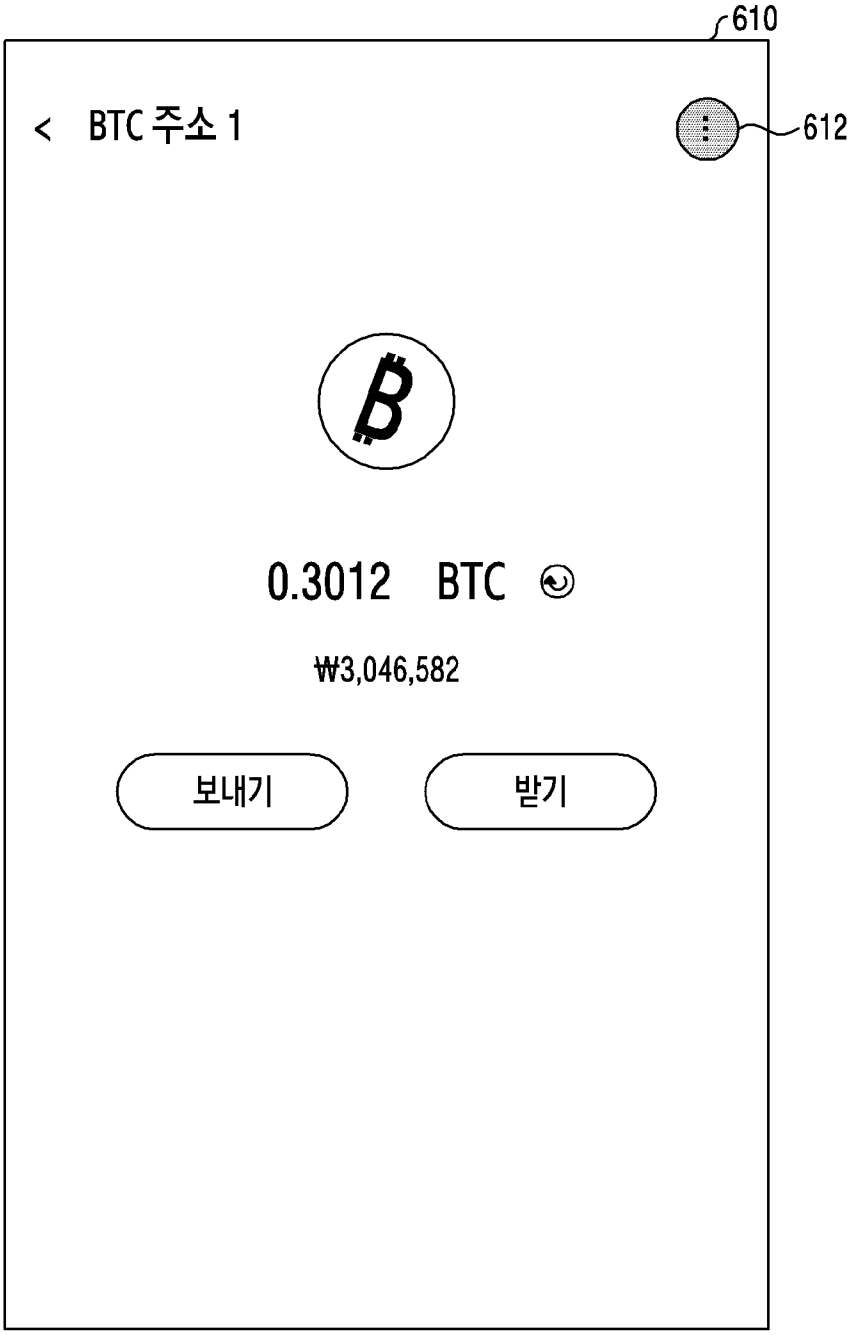
[도5]


500
REE (510)
TEE (520)
클라이언트 APP
클라이언트 APP
512
신뢰 APP
신뢰 APP
522
TEE 내부 API (524)
TEE 클라이언트 API (514)
Trusted OS 컴포넌트 (526)
Rich OS 컴포넌트 (516)
REE 통신 에이전트 (518)
모니터 (528)
하드웨어 플랫폼 (530)
보안 메모리 (532)

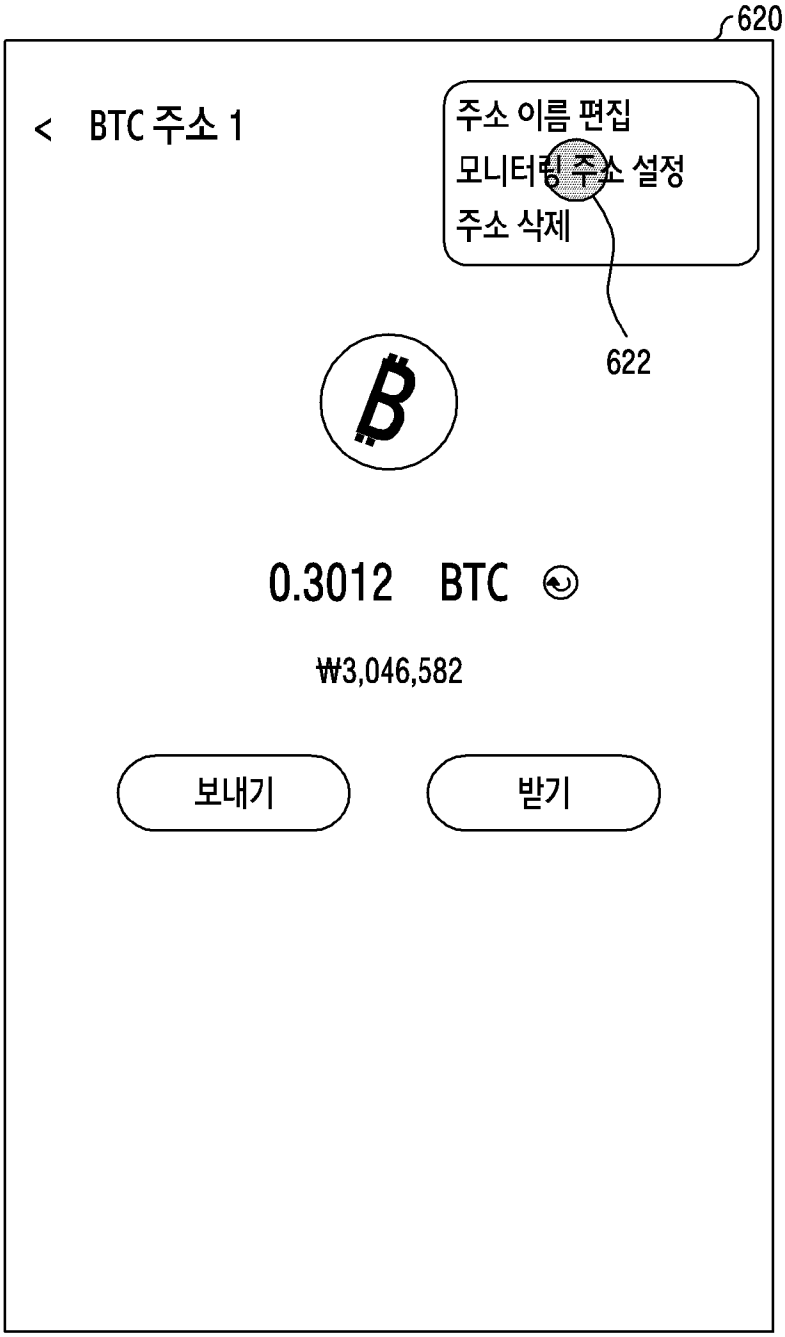
[도6a]


600
Blockchain Wallet
예상 총 잔액
KRW 3,046,582
602
BTC 주소 1
Bitcoin
0.3012 BTC
≒ ₩ 10,114,815 -1.76%
₩ 3,046,582
604
+ 코인 또는 토큰 추가
지갑
DApps

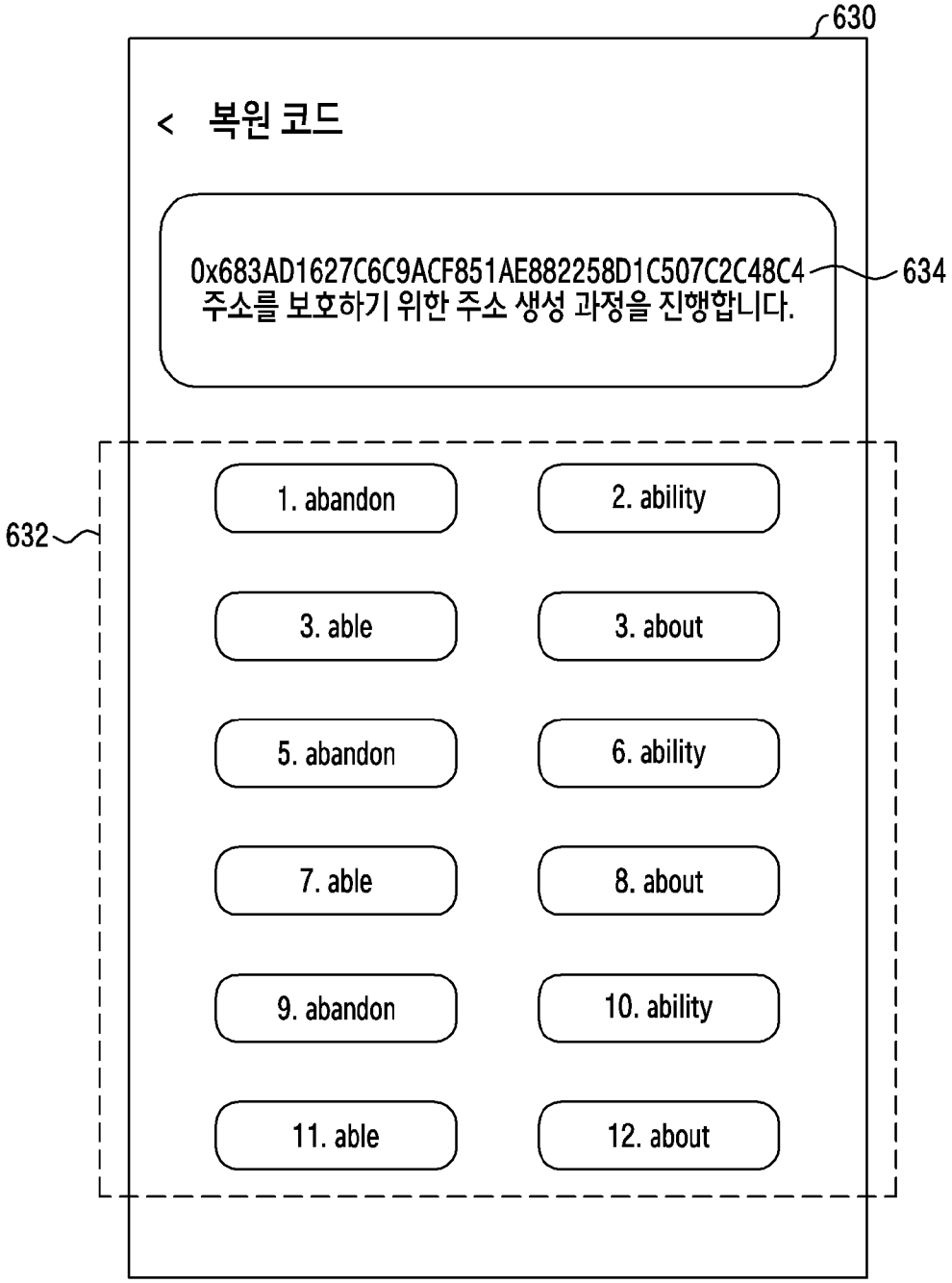
[도6b]



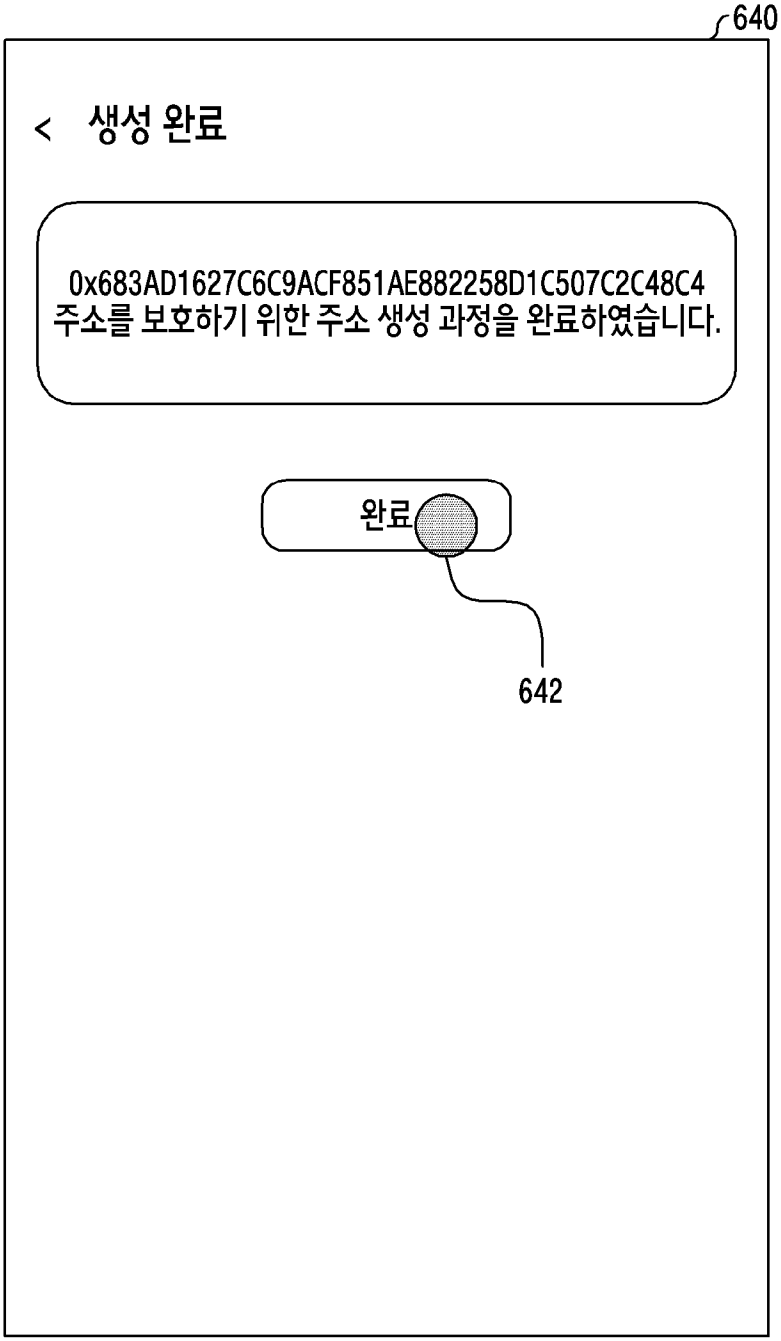
[도6c]


620
< BTC 주소 1
주소 이름 편집
모니터링 주소 설정
주소 삭제
622
0.3012 BTC
₩3,046,582
보내기
받기

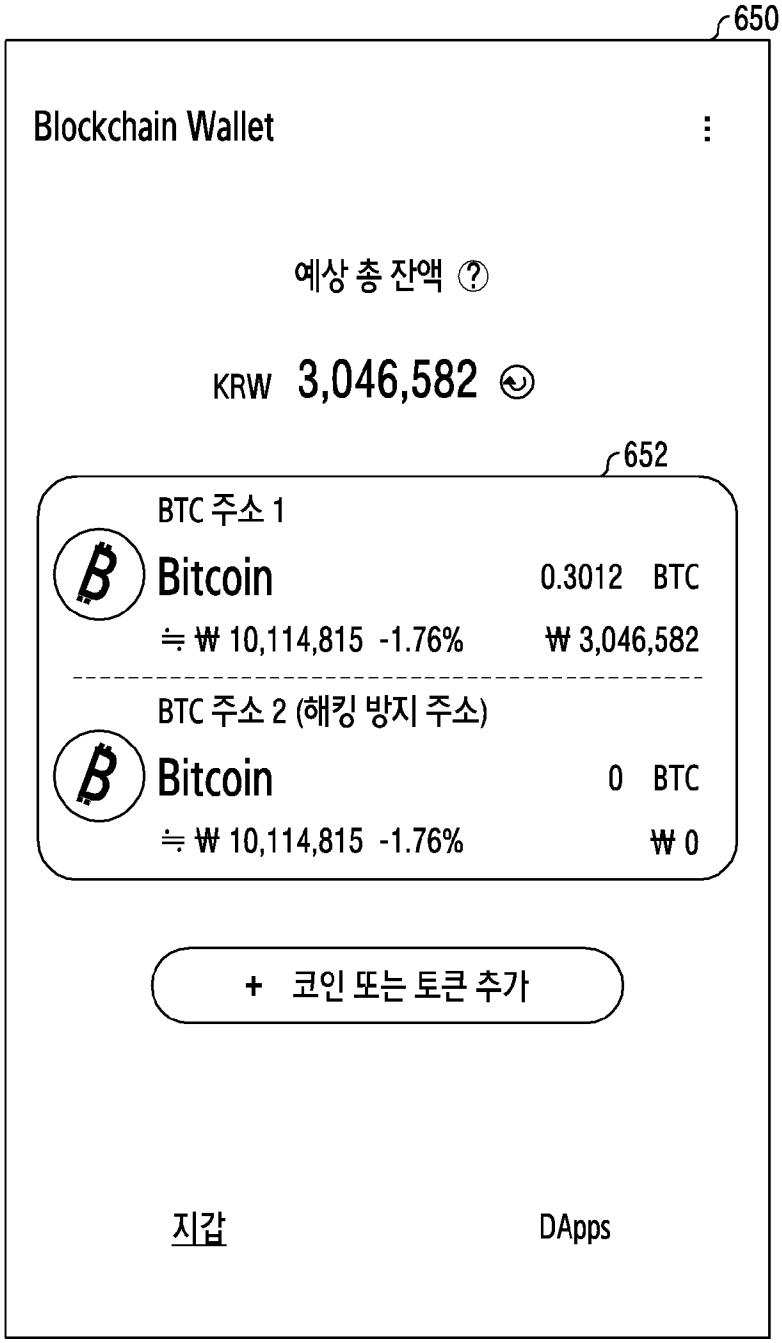
[도6d]


630
< 복원 코드
0x683AD1627C6C9ACF851AE882258D1C507C2C48C4
주소를 보호하기 위한 주소 생성 과정을 진행합니다.
634
632
1. abandon
2. ability
3. able
3. about
5. abandon
6. ability
7. able
8. about
9. abandon
10. ability
11. able
12. about

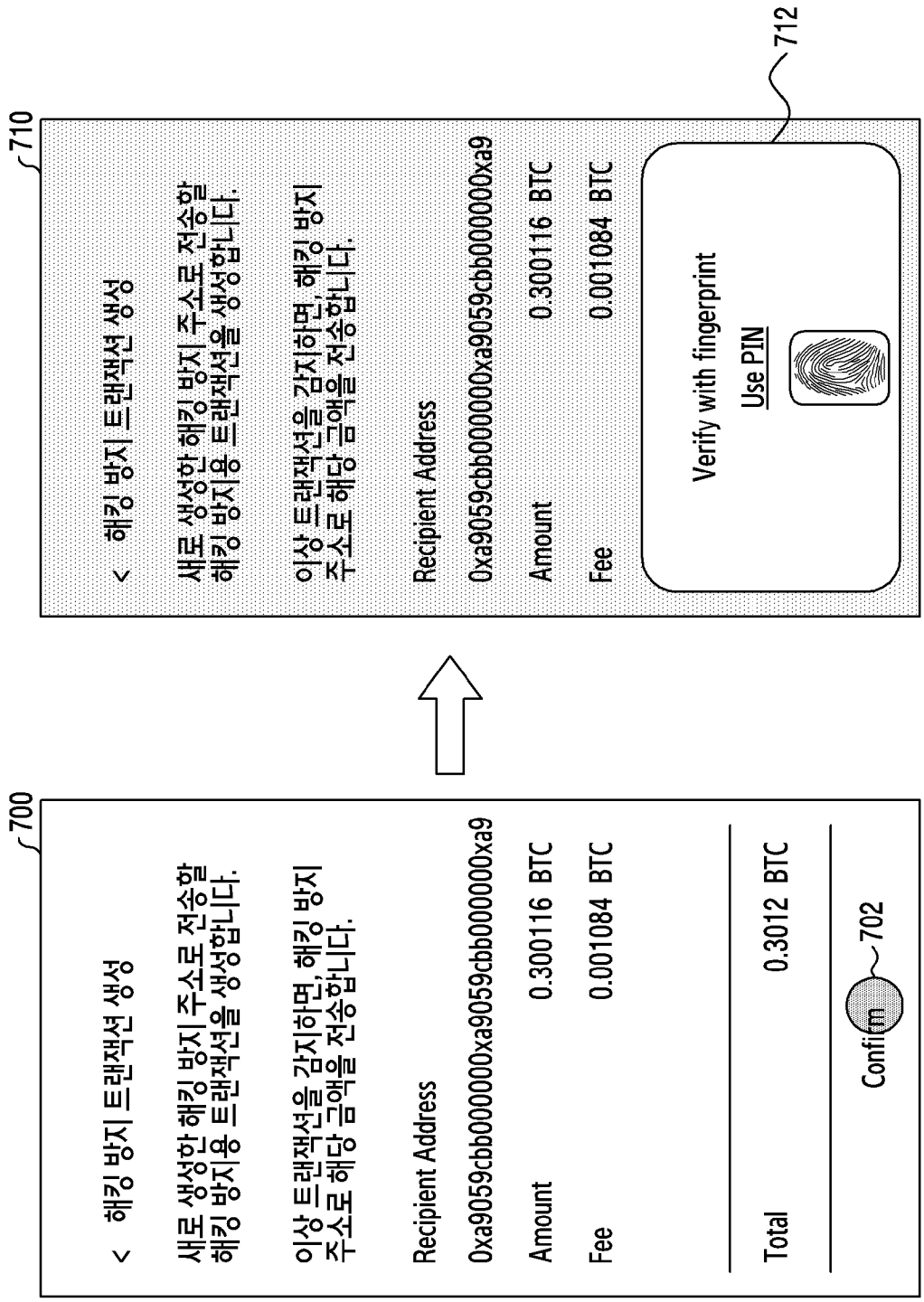
[도6e]


640
< 생성 완료
0x683AD1627C6C9ACF851AE882258D1C507C2C48C4
주소를 보호하기 위한 주소 생성 과정을 완료하였습니다.
완료
642

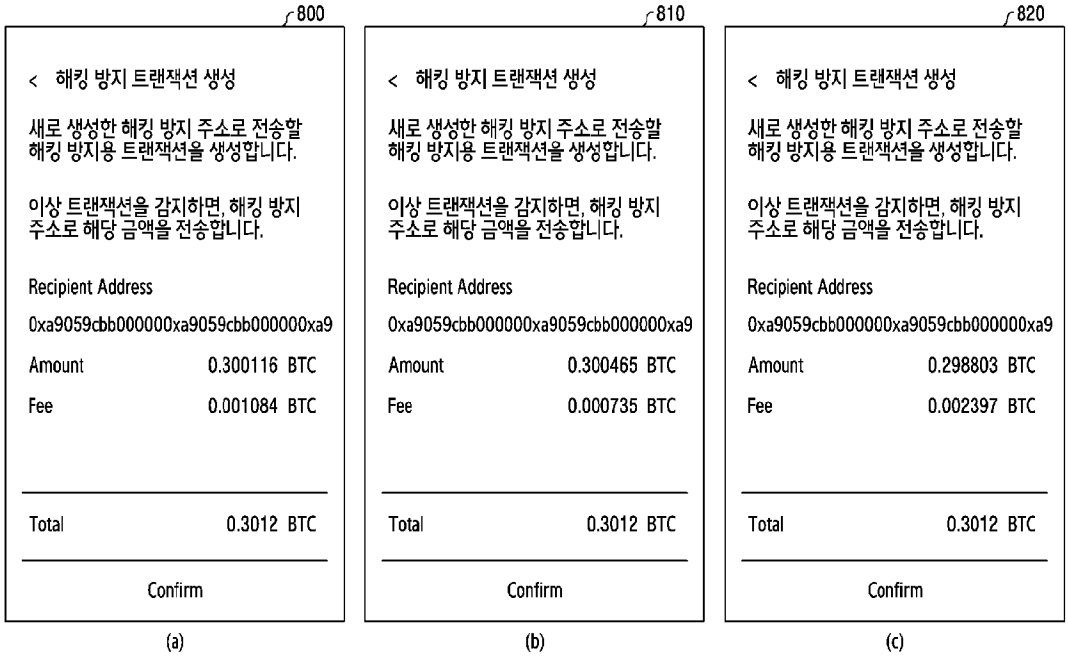
[도6f]


650
Blockchain Wallet
예상 총 잔액
KRW 3,046,582
652
BTC 주소 1
Bitcoin
0.3012 BTC
≒ ₩ 10,114,815 -1.76%
₩ 3,046,582
BTC 주소 2 (해킹 방지 주소)
Bitcoin
0 BTC
≒ ₩ 10,114,815 -1.76%
₩ 0
+ 코인 또는 토큰 추가
지갑
DApps

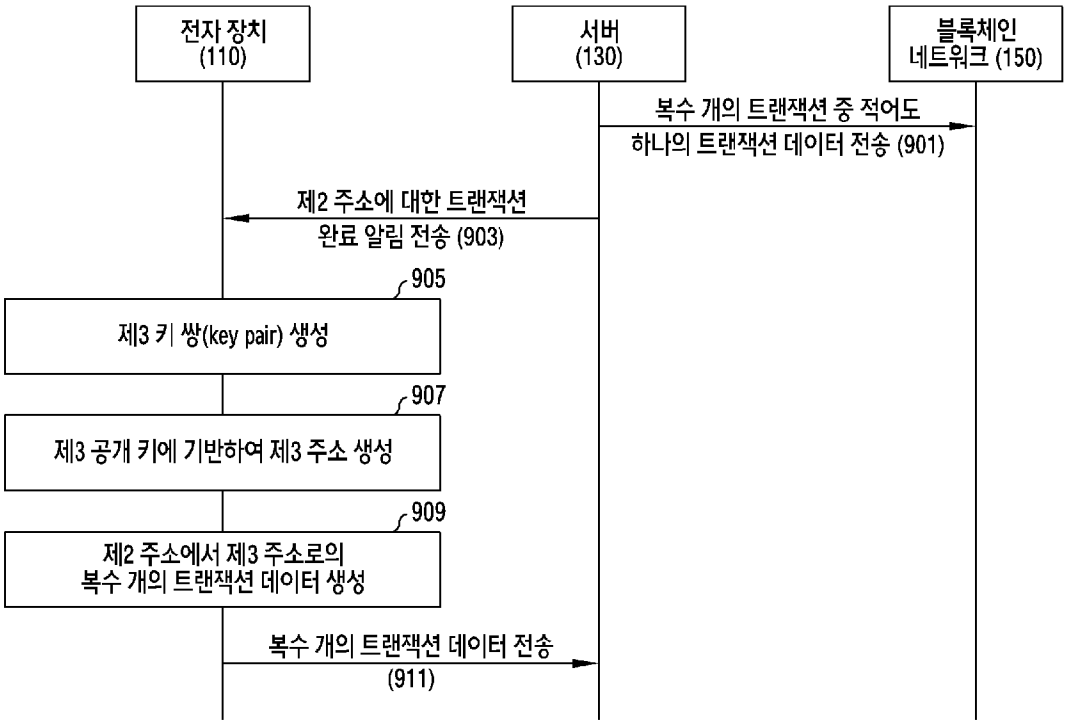
[도7]


700
< 해킹 방지 트랜잭션 생성
새로 생성한 해킹 방지 주소로 전송할
해킹 방지용 트랜잭션을 생성합니다.
이상 트랜잭션을 감지하면, 해킹 방지
주소로 해당 금액을 전송합니다.
Recipient Address
0xa9059cbb000000xa9059cbb000000xa9
Amount 0.300116 BTC
Fee 0.001084 BTC
Total 0.3012 BTC
Confirm
702
710
< 해킹 방지 트랜잭션 생성
새로 생성한 해킹 방지 주소로 전송할
해킹 방지용 트랜잭션을 생성합니다.
이상 트랜잭션을 감지하면, 해킹 방지
주소로 해당 금액을 전송합니다.
Recipient Address
0xa9059cbb000000xa9059cbb000000xa9
Amount 0.300116 BTC
Fee 0.001084 BTC
Verify with fingerprint
Use PIN
712

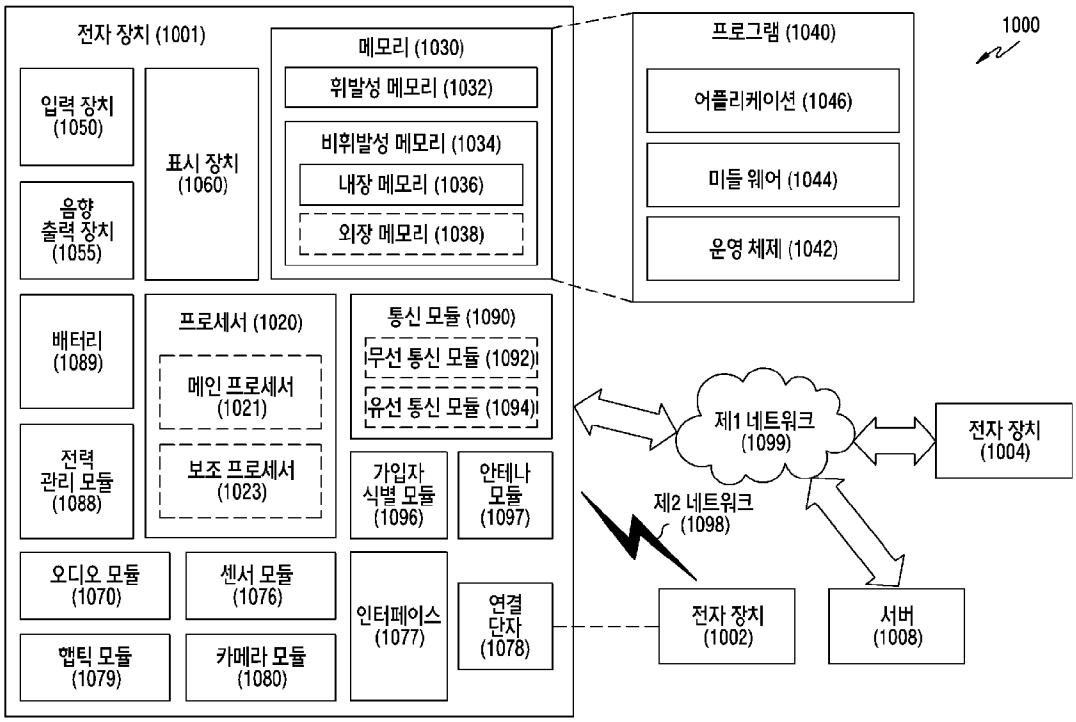
[도8]


800
< 해킹 방지 트랜잭션 생성
새로 생성한 해킹 방지 주소로 전송할 해킹 방지용 트랜잭션을 생성합니다.
이상 트랜잭션을 감지하면, 해킹 방지 주소로 해당 금액을 전송합니다.
Recipient Address
0xa9059cbb000000xa9059cbb000000xa9
Amount 0.300116 BTC
Fee 0.001084 BTC
Total 0.3012 BTC
Confirm
(a)
810
< 해킹 방지 트랜잭션 생성
새로 생성한 해킹 방지 주소로 전송할 해킹 방지용 트랜잭션을 생성합니다.
이상 트랜잭션을 감지하면, 해킹 방지 주소로 해당 금액을 전송합니다.
Recipient Address
0xa9059cbb000000xa9059cbb000000xa9
Amount 0.300465 BTC
Fee 0.000735 BTC
Total 0.3012 BTC
Confirm
(b)
820
< 해킹 방지 트랜잭션 생성
새로 생성한 해킹 방지 주소로 전송할 해킹 방지용 트랜잭션을 생성합니다.
이상 트랜잭션을 감지하면, 해킹 방지 주소로 해당 금액을 전송합니다.
Recipient Address
0xa9059cbb000000xa9059cbb000000xa9
Amount 0.298803 BTC
Fee 0.002397 BTC
Total 0.3012 BTC
Confirm
(c)

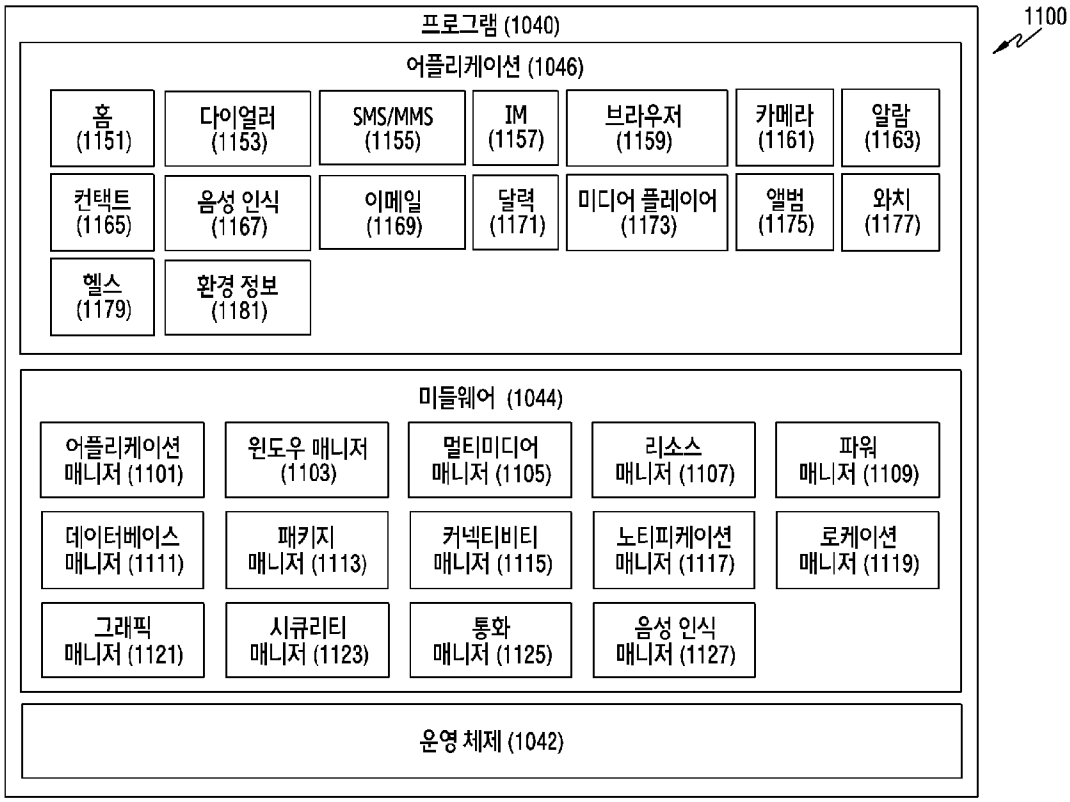
[도9]


전자 장치 (110)
서버 (130)
블록체인 네트워크 (150)
복수 개의 트랜잭션 중 적어도 하나의 트랜잭션 데이터 전송 (901)
제2 주소에 대한 트랜잭션 완료 알림 전송 (903)
905
제3 키 쌍(key pair) 생성
907
제3 공개 키에 기반하여 제3 주소 생성
909
제2 주소에서 제3 주소로의 복수 개의 트랜잭션 데이터 생성
복수 개의 트랜잭션 데이터 전송 (911)

[도10]


1000
전자 장치 (1001)
입력 장치 (1050)
음향 출력 장치 (1055)
표시 장치 (1060)
메모리 (1030)
휘발성 메모리 (1032)
비휘발성 메모리 (1034)
내장 메모리 (1036)
외장 메모리 (1038)
프로그램 (1040)
어플리케이션 (1046)
미들 웨어 (1044)
운영 체제 (1042)
배터리 (1089)
전력 관리 모듈 (1088)
프로세서 (1020)
메인 프로세서 (1021)
보조 프로세서 (1023)
통신 모듈 (1090)
무선 통신 모듈 (1092)
유선 통신 모듈 (1094)
가입자 식별 모듈 (1096)
안테나 모듈 (1097)
오디오 모듈 (1070)
센서 모듈 (1076)
햅틱 모듈 (1079)
카메라 모듈 (1080)
인터페이스 (1077)
연결 단자 (1078)
제1 네트워크 (1099)
제2 네트워크 (1098)
전자 장치 (1004)
전자 장치 (1002)
서버 (1008)

[도11]


1100
프로그램 (1040)
어플리케이션 (1046)
홈 (1151)
다이얼러 (1153)
SMS/MMS (1155)
IM (1157)
브라우저 (1159)
카메라 (1161)
알람 (1163)
컨택트 (1165)
음성 인식 (1167)
이메일 (1169)
달력 (1171)
미디어 플레이어 (1173)
앨범 (1175)
와치 (1177)
헬스 (1179)
환경 정보 (1181)
미들웨어 (1044)
어플리케이션 매니저 (1101)
윈도우 매니저 (1103)
멀티미디어 매니저 (1105)
리소스 매니저 (1107)
파워 매니저 (1109)
데이터베이스 매니저 (1111)
패키지 매니저 (1113)
커넥티비티 매니저 (1115)
노티피케이션 매니저 (1117)
로케이션 매니저 (1119)
그래픽 매니저 (1121)
시큐리티 매니저 (1123)
통화 매니저 (1125)
음성 인식 매니저 (1127)
운영 체제 (1042)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2021/006232

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/38(2012.01)i; **G06Q 20/36**(2012.01)i; **G06F 21/62**(2013.01)i; **H04L 9/08**(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q 20/38(2012.01); G06F 17/30(2006.01); G06Q 20/02(2012.01); G06Q 20/06(2012.01); G06Q 20/36(2012.01); G06Q 40/02(2012.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models: IPC as above
Japanese utility models and applications for utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & keywords: 키 쌍(key pairs), 제1 주소(first address), 제2 주소(second address), 트랜잭션(transaction), 이전(transfer)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2018-0240107 A1 (BLACK GOLD COIN, INC.) 23 August 2018 (2018-08-23) See paragraphs [0115], [0162]-[0167] and [0182]-[0190].	1-15
Y	KR 10-2019-0137070 A (ALIBABA GROUP HOLDING LIMITED) 10 December 2019 (2019-12-10) See paragraphs [0017]-[0018], [0024] and [0038] and claims 10 and 13.	1-15
Y	KR 10-2019-0065824 A (BIZMODELINE CO., LTD.) 12 June 2019 (2019-06-12) See paragraphs [0261] and [0291].	2-3,9,11-12
Y	US 2018-0039667 A1 (CHICAGO MERCANTILE EXCHANGE INC.) 08 February 2018 (2018-02-08) See paragraph [0119] and claims 1, 6, 8 and 10.	9
A	US 2019-0180273 A1 (INTERCONTINENTAL EXCHANGE HOLDINGS, INC.) 13 June 2019 (2019-06-13) See entire document.	1-15

☐ Further documents are listed in the continuation of Box C.

☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 August 2021	**27 August 2021**
Name and mailing address of the ISA/KR **Korean Intellectual Property Office** **Government Complex-Daejeon Building 4, 189 Cheongsa-ro, Seo-gu, Daejeon 35208** Facsimile No. **+82-42-481-8578**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2021/006232

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2018-0240107	A1	23 August 2018	AU	2015-389877	A1	19 October 2017
				AU	2018-100482	A4	07 June 2018
				BR	112017020562	A2	03 July 2018
				CA	2980818	A1	06 October 2016
				CN	107710258	A	16 February 2018
				EP	3073670	A1	28 September 2016
				EP	3073670	B1	02 September 2020
				HK	1244098	A1	27 July 2018
				MX	2017012445	A	28 September 2018
				RU	2017134723	A	04 April 2019
				RU	2017134723	A3	25 June 2019
				US	2016-0283941	A1	29 September 2016
				WO	2016-156954	A1	06 October 2016
KR	10-2019-0137070	A	10 December 2019	AU	2019-204019	A1	19 December 2019
				AU	2019-204019	B2	28 May 2020
				AU	2020-210283	A1	20 August 2020
				AU	2020-210283	B2	13 May 2021
				BR	112019011776	A2	13 April 2021
				CA	3045632	A1	29 November 2019
				CN	108898483	A	27 November 2018
				EP	3593306	A1	15 January 2020
				JP	2020-524826	A	20 August 2020
				MX	2019006758	A	20 January 2020
				PH	12019501309	A1	24 February 2020
				RU	2019117942	A	10 December 2020
				RU	2019117942	A3	10 December 2020
				RU	2739482	C2	24 December 2020
				SG	11201905270	A	30 January 2020
				TW	202004634	A	16 January 2020
				US	2019-0370798	A1	05 December 2019
				WO	2019-231955	A1	05 December 2019
KR	10-2019-0065824	A	12 June 2019		None		
US	2018-0039667	A1	08 February 2018	EP	3494535	A1	12 June 2019
				US	10417217	B2	17 September 2019
				US	2019-0340170	A1	07 November 2019
				WO	2018-026883	A1	08 February 2018
US	2019-0180273	A1	13 June 2019	CA	3034098	A1	20 August 2019
				EP	3528190	A1	21 August 2019
				SG	10201901461	A	27 September 2019

국 제 조 사 보 고 서

국제출원번호
PCT/KR2021/006232

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06Q 20/38(2012.01)i; **G06Q 20/36**(2012.01)i; **G06F 21/62**(2013.01)i; **H04L 9/08**(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06Q 20/38(2012.01); G06F 17/30(2006.01); G06Q 20/02(2012.01); G06Q 20/06(2012.01); G06Q 20/36(2012.01); G06Q 40/02(2012.01)

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 키 쌍(key pairs), 제1 주소(first address), 제2 주소(second address), 트랜잭션(transaction), 이전(transfer)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	US 2018-0240107 A1 (BLACK GOLD COIN, INC.) 2018.08.23 단락 115, 162-167, 182-190 참조.	1-15
Y	KR 10-2019-0137070 A (알리바바 그룹 홀딩 리미티드) 2019.12.10 단락 17-18, 24, 38 및 청구항 10, 13 참조.	1-15
Y	KR 10-2019-0065824 A (주식회사 비즈모델라인) 2019.06.12 단락 261, 291 참조.	2-3,9,11-12
Y	US 2018-0039667 A1 (CHICAGO MERCANTILE EXCHANGE INC.) 2018.02.08 단락 119 및 청구항 1, 6, 8, 10 참조.	9
A	US 2019-0180273 A1 (INTERCONTINENTAL EXCHANGE HOLDINGS, INC.) 2019.06.13 전체 문서 참조.	1-15

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☑ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌
"D" 본 국제출원에서 출원인이 인용한 문헌
"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌
"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌
"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌
"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌
"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌
"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.
"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.
"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2021년08월27일(27.08.2021)	**2021년08월27일(27.08.2021)**

ISA/KR의 명칭 및 우편주소	심사관
대한민국 특허청 **(35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사)**	**박혜련**
팩스 번호 **+82-42-481-8578**	전화번호 **+82-42-481-3463**

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2021/006232

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 2018-0240107 A1	2018/08/23	AU 2015-389877 A1	2017/10/19
		AU 2018-100482 A4	2018/06/07
		BR 112017020562 A2	2018/07/03
		CA 2980818 A1	2016/10/06
		CN 107710258 A	2018/02/16
		EP 3073670 A1	2016/09/28
		EP 3073670 B1	2020/09/02
		HK 1244098 A1	2018/07/27
		MX 2017012445 A	2018/09/28
		RU 2017134723 A	2019/04/04
		RU 2017134723 A3	2019/06/25
		US 2016-0283941 A1	2016/09/29
		WO 2016-156954 A1	2016/10/06
KR 10-2019-0137070 A	2019/12/10	AU 2019-204019 A1	2019/12/19
		AU 2019-204019 B2	2020/05/28
		AU 2020-210283 A1	2020/08/20
		AU 2020-210283 B2	2021/05/13
		BR 112019011776 A2	2021/04/13
		CA 3045632 A1	2019/11/29
		CN 108898483 A	2018/11/27
		EP 3593306 A1	2020/01/15
		JP 2020-524826 A	2020/08/20
		MX 2019006758 A	2020/01/20
		PH 12019501309 A1	2020/02/24
		RU 2019117942 A	2020/12/10
		RU 2019117942 A3	2020/12/10
		RU 2739482 C2	2020/12/24
		SG 11201905270 A	2020/01/30
		TW 202004634 A	2020/01/16
		US 2019-0370798 A1	2019/12/05
		WO 2019-231955 A1	2019/12/05
KR 10-2019-0065824 A	2019/06/12	없음	
US 2018-0039667 A1	2018/02/08	EP 3494535 A1	2019/06/12
		US 10417217 B2	2019/09/17
		US 2019-0340170 A1	2019/11/07
		WO 2018-026883 A1	2018/02/08
US 2019-0180273 A1	2019/06/13	CA 3034098 A1	2019/08/20
		EP 3528190 A1	2019/08/21
		SG 10201901461 A	2019/09/27