

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일

2019년 6월 6일 (06.06.2019)



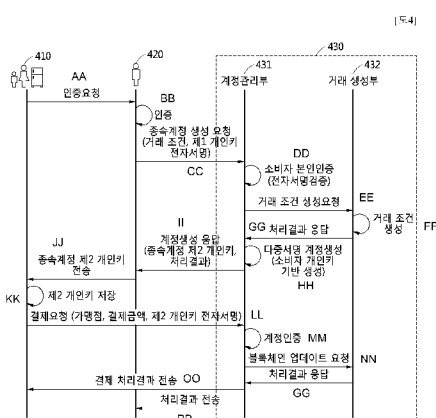
(10) 국제공개번호

WO 2019/107654 A1

- (51) 국제특허 분류: (씨 6안 20/06 (2012.01) G06Q 20/36 (2012.01)
- (21) 국제출원번호: P(17) 120 17/0 15097
- (22) 국제출원일: 2017년 12월 20일 (20. 12.2017)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보: 10-2017-0161354 2017년 11월 29일 (29. 11.2017) KR
- (71) 출원인: 신한카드 주식회사 (SHINHAN CARD CO., LTD.) [KR/KR]; 04551 서울시 중구 을지로 100, 에이동 (을지로 2가, 파인에비뉴), Seoul (KR).
- (72) 발명자: 김정수 (KIM, Jung Soo); 04551 서울시 중구 을지로 100, Seoul (KR). 조문일 (CHO, Moon II); 04551 서울시 중구 을지로 100, Seoul (KR). 김치헌 (KIM, Chy Heon); 04551 서울시 중구 을지로 100, Seoul (KR). 김영환 (KIM, Young Hwan); 22766 인천시 서구 비치니스로 10, 534 동 3002호, bcheon (KR). 김학범 (KIM, Hak Bum); 12145 경기도 남양주시 늘을로 71, 1504 동 102호, Gyeonggi-do (KR). 정승채 (CHUNG, Seung Chi); 06735 서울시 서초구 남부순환로 347길 18, Seoul (KR).
- (74) 대리인: 특허법인 무한 (PATENT & I&Y 이_ ; 06144 서울시 강남구 언주로 560, 8층 (역삼동, 진영빌딩), 360111 (101).
- (81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): JP, KR, CN, AU, AT, DE, CH, US, CA, MX, BR, AR, CO, EC, EE, EG, ES, FI, GB, GL, GE, GR, HU, IL, IN, IT, JP, KR, MA, MD, MY, NZ, PE, PT, RU, SA, SG, ST, SY, TH, TN, TR, TW, UA, ZM, ZW.
- (84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): JP, KR, CN, AU, AT, DE, CH, US, CA, MX, BR, AR, CO, EC, EE, EG, ES, FI, GB, GL, GE, GR, HU, IL, IN, IT, JP, KR, MA, MD, MY, NZ, PE, PT, RU, SA, SG, ST, SY, TH, TN, TR, TW, UA, ZM, ZW.

(54) Title: CREDIT VIRTUAL MONEY GENERATION DEVICE AND CREDIT VIRTUAL MONEY MANAGEMENT DEVICE

(54) 발명의 명칭: 여신 가상화폐 생성 장치 및 여신 가상화폐 관리 장치



(57) Abstract: Provided is a virtual money generation device comprising: a blockchain generation unit for generating a blockchain, which includes virtual money generated according to a payment history; an account management unit for managing multi-signatures of a plurality of accounts sharing the blockchain; and a transaction generation unit for storing a transaction condition corresponding to each of the plurality of accounts, and proceeding with payments using the blockchain according to the transaction condition.

(57) 요약서: 소비자의 신용(credit) 한도에 따라 생성되는 가상화폐를 포함하는 블록체인을 생성하고, 결제 내역에 따라 상기 블록체인을 업데이트하는 블록체인 생성부, 상기 블록체인을 공유하는 복수의 계정들의 다중서명(multi-signature)을 관리하는 계정관리부 및 상기 복수의 계정 각각에 대응하는 거래 조건을 저장하고, 상기 거래 조건에 따라 상기 블록체인을 이용한 결제를 진행하는 거래 생성부를 포함하는 가상화폐 생성 장치가 제공된다.

- 431 ... Account management unit
- 432 ... Account generation unit
- AA ... Request authentication
- BB ... Authenticate
- CC ... Request generation of sub-account (transaction condition, first private key electronic signature)
- DD ... Authenticate identity of consumer (verify electronic signature)
- EE ... Request generation of transaction condition
- FF ... Generate transaction condition
- GG ... Respond to processing result
- HH ... Generate multi-signature account (generate on basis of consumer private key)
- II ... Response to account generation (sub-account second private key, processing result)
- JJ ... Transmit sub-account second private key
- KK ... Store second private key
- LL ... Request payment (franchise, payment amount, second private key electronic signature)
- MM ... Authenticate account
- NN ... Request blockchain update
- OO ... Transmit payment processing result
- PP ... Transmit processing result



WO 19/107654 A1



공개:

— 국제조사 보고서 와 함께 (조약 제21조(3))

명세서

발명의 명칭: 여신 가상화폐 생성 장치 및 여신 가상화폐 관리 장치 기술분야

- [1] 이하의 설명은 여신 가상화폐를 생성하는 장치 및 여신 가상화폐를 관리하는 장치에 관한 것이다. 보다 구체적으로, 여신 가상화폐를 이용하는 사용자 단말 및 여신 가상화폐를 발행하고, 관리하는 카드사 서버에 연관된다.

배경기술

- [2] 종래의 신용거래는 소비자, 가맹점 및 카드회사 사이를 연결하는 VAN사(Value Added Network) 또는 PG사(Payment Gateway)를 통해 결제가 진행되었다. 따라서 종래 방식은 VAN사 또는 PG사 각각이 거래를 중개하고, 중개된 거래 횟수에 따라 수수료를 취득하였기 때문에 VAN사 및 PG사를 거치지 않는 새로운 결제 프로세스가 개발되지 않는 이상 신용카드 가맹점들의 수수료를 인하하기 어렵다는 한계가 존재한다.
- [3] 한편, 최근에는 계좌이체 방식의 앱(APP: Application)투 앱 결제로써 VAN사 또는 PG사가 없는 거래 프로세스를 구현하고 가맹점 수수료를 낮추고자 하는 시도가 있으나, 계좌이체 방식은 신용거래가 아니라는 한계가 존재한다. 따라서 기존의 신용카드 사용 및 신용으로 결제하고자 하는 소비자들에게는 앱투 앱 결제를 통해서만 통장 잔액 내에서만 소비가 가능하다는 아쉬움이 존재할 수 있다.
- [4] 또한, 미래에는 사람뿐만 아니라 사물 단말을 통해서도 자동 결제하는 시대가 도래할 예정이다. 그러나 현재 신용카드 거래는 사람 또는 사람이 제어하는 사용자 단말을 통해서만 가능하다는 한계가 존재한다.
- [5] 대한민국 공개특허 제 10-2016-0132307호에는 암호화폐를 이용한 송금 방법이 개시된다. 구체적으로, 대상특허는 피어투 피어(peer-to-peer) 네트워크를 통해 상호 연결된 거래소 컴퓨터 장치들이 암호화폐를 각자의 전자지갑으로 이체하고, 해당 암호화폐를 법정화폐와 교환하도록 하여 사용자 간의 편리한 계좌이체를 구현하는 구성을 개시하고 있다.

발명의 상세한 설명

과제 해결 수단

- [6] 일측에 따르면, 프로세서를 포함하는 가상화폐 생성 장치가 제공된다. 상기 가상화폐 생성 장치는 상기 프로세서에 의해 구현되는, 소비자의 신용(credit) 한도에 따라 생성되는 가상화폐를 포함하는 블록 체인을 생성하고, 결제 내역에 따라 상기 블록 체인을 업데이트하는 블록 체인 생성부, 상기 블록 체인을 공유하는 복수의 계정들의 다중서명(multi-signature)을 관리하는 계정관리부 및 상기 복수의 계정 각각에 대응하는 거래 조건을 저장하고, 상기 거래 조건에 따라 상기 가상화폐를 이용한 결제를 진행하는 거래 생성부를 포함할 수 있다.

- [7] 일실시에에 따르면, 상기 계정관리부는 상기 소비자의 사용자 단말에 관한 주계정 및 상기 소비자에 연관되는 적어도 하나의 종속계정 각각의 다중서명을 관리할 수 있다.
- [8] 다른 일실시에에 따르면, 상기 가상화폐 생성 장치는 상기 사용자 단말로 부터 제1종속계정에 대한 생성 요청을 수신하는 통신부를 더 포함할 수 있다. 또한, 상기 계정관리 부는 상기 사용자 단말에 저장된 제1개인키를 인증하고, 상기 인증의 결과에 따라 상기 제1종속계정의 생성 여부를 결정할 수 있다.
- [9] 또 다른 일실시에에 따르면, 상기 계정관리 부는 상기 제1개인키가 인증된 경우에 상기 제1종속계정을 생성하고, 상기 제1개인키를 이용하여 상기 제1종속계정의 다중서명을 생성할 수 있다.
- [10] 또 다른 일실시에에 따르면, 상기 계정관리 부는 상기 제1개인키로 부터 유도된 복수의 제2개인키를 생성하고, 상기 복수의 제2개인키 중 하나를 시스템 키로서 저장하고, 상기 복수의 개인키 중 하나를 상기 주계정에 대한 사용자 단말로 전송하고, 상기 복수의 개인키 중 하나를 상기 제1종속계정에 대한 단말로 전송할 수 있다.
- [11] 또 다른 일실시에에 따르면, 상기 통신부는 상기 주계정의 제1개인키를 이용한 전자서명 및 상기 제1종속계정에 대한 거래 조건을 상기 제1종속계정에 대한 생성 요청으로서 수신할 수 있다. 상기 거래 생성부는 상기 제1개인키가 인증된 경우에 상기 제1종속계정에 대한 거래 조건을 저장하고, 상기 거래 조건은 상기 제1종속계정의 유효기간, 사용권 한 및 결제권 한 중 적어도 하나를 포함할 수 있다.
- [12] 또 다른 일실시에에 따르면, 상기 소비자의 사용자 단말은 상기 주계정에 대한 제1개인키를 저장하고, 상기 적어도 하나의 종속계정 각각에 대한 백업키들을 저장하고, 상기 백업키들은 상기 제1개인키로부터 유도된 것을 특징으로 할 수 있다.
- [13] 다른 일측에 따르면, 새로운 종속계정의 생성을 요청하는 사용자 단말이 제공된다. 상기 사용자 단말은 단말로 부터 블록 체인을 공유하기 위한 인증 요청을 수신하는 통신부, 상기 블록 체인을 이용하기 위한 주계정의 제1개인키를 암호화하여 저장하는 메모리 및 지정된 조건에 따라 상기 단말을 인증하고, 상기 인증의 결과에 따라 새로운 종속계정의 생성을 요청하는 메시지를 생성하는 프로세서를 포함할 수 있다. 상기 새로운 종속계정의 생성을 요청하는 메시지는 상기 주계정의 제1개인키를 이용한 전자서명 및 상기 새로운 종속계정에 대한 거래 조건을 포함하고, 상기 블록 체인은 소비자의 신용 한도에 따라 생성되는 가상화폐를 포함할 수 있다.
- [14] 일실시에에 따르면, 상기 프로세서는 사용자 입력에 따라 상기 종속계정의 유효기간, 사용권 한 및 결제권 한 중 적어도 하나를 포함하는 상기 거래 조건을 결정할 수 있다.
- [15] 다른 일실시에에 따르면, 상기 통신부는 상기 새로운 종속계정의 생성을

요청하는 메시지를 상기 블록 체인을 관리하는 카드사 서버로 전송하고, 상기 카드사 서버는 상기 제1개인키가 인증된 경우에 상기 새로운 종속계정에 대한 거래 조건을 저장하고, 상기 제1개인키로부터 유도된 복수의 제2개인키 중 적어도 두 개를 상기 사용자 단말로 전송할 수 있다.

- [16] 또 다른 일실시예에 따르면, 상기 통신부는 카드사 서버로부터 상기 새로운 종속계정에 대한 계정생성 응답 메시지를 수신하고 상기 프로세서는 상기 계정생성 응답 메시지로 부터 상기 새로운 종속계정에 대한 복수의 제2개인키를 추출할 수 있다.
- [17] 또 다른 일실시예에 따르면, 상기 통신부는 상기 새로운 종속계정에 대한 복수의 제2개인키 중 하나를 상기 단말의 개인키로서 상기 단말로 전송하고 상기 프로세서는 상기 복수의 제2개인키 중 하나를 상기 새로운 종속계정에 대한 백업키로서 상기 메모리에 저장할 수 있다.
- [18] 또 다른 일실시예에 따르면, 상기 프로세서는 사용자 입력에 응답하여 상기 새로운 종속계정에 대한 계정삭제 메시지 및 결제취소 메시지 중 하나를 생성하고, 상기 계정삭제 메시지 및 상기 결제취소 메시지 각각은 상기 메모리에 저장된 제2개인키에 기초한 전자서명을 포함하고, 상기 통신부는 상기 계정삭제 메시지 및 상기 거래취소 메시지 중 하나를 상기 카드사 서버로 전송하고, 상기 카드사 서버는 상기 종속계정에 대해 저장된 시스템키를 이용하여 상기 전자서명을 검증하고, 상기 검증의 결과에 따라 상기 종속계정을 삭제하거나, 상기 종속계정에 연관되는 결제를 취소할 수 있다.
- [19] 또 다른 일실시예에 따르면, 상기 메모리는 카드사 서버로부터 배포된 가상화폐 어플리케이션을 포함하고, 상기 프로세서는 상기 통신부를 통해 상기 가상화폐 어플리케이션을 이용하여 접속하는 소비자 단말과 상기 블록 체인에 연관되는 가상화폐를 이용한 신용 결제를 처리할 수 있다.
- [20] 또 다른 일측에 따르면, 종속계정을 생성하는 프로그램을 수록한 컴퓨터 판독 가능한 기록 매체가 제공된다. 상기 프로그램은 블록 체인을 이용하기 위한 주계정의 제1개인키를 암호화하여 저장하는 명령어 세트, 지정된 조건에 따라 상기 종속계정에 연관되는 단말을 인증하는 명령어 세트, 상기 인증의 결과에 따라 상기 종속계정의 생성을 요청하는 메시지를 상기 블록 체인을 관리하는 카드사 서버로 전송하는 명령어 세트 및 상기 카드사 서버로부터 상기 종속계정에 대한 계정생성 응답 메시지를 수신하는 명령어 세트를 포함할 수 있다.
- [21] 일실시예에 따르면, 상기 프로그램은 상기 계정생성 응답 메시지로 부터 상기 종속계정에 대한 복수의 제2개인키를 추출하는 명령어 세트 및 상기 복수의 제2개인키 중 하나를 상기 종속계정에 연관되는 단말의 개인키로서 전송하는 명령어 세트를 포함할 수 있다.
- [22] 또 다른 일측에 따르면, 블록 체인을 공유하는 복수의 계정 중 제1계정에 연관되는 단말로 부터 상기 블록 체인을 이용한 결제 요청 메시지를 수신하는

통신부 및 프로세서를 포함하는 가상화폐 관리 장치가 제공된다. 상기 가상화폐 관리 장치는 상기 프로세서에 의해 구현되는 소비자의 신용(credit) 한도에 따라 생성되는 가상화폐를 포함하는 상기 블록 체인을 생성하고, 결제 내역에 따라 상기 블록 체인을 업데이트하는 블록 체인 생성부 및 상기 결제 요청 메시지와 상기 제1 계정에 대응하는 거래 조건을 확인하여 거래 승인 여부를 관리하는 거래 관리부를 포함할 수 있다.

- [] 일실시예에 따르면, 상기 거래 관리부는 상기 결제 요청 메시지에 포함되는 가맹점 정보, 결제금액 및 전자서명 중 적어도 하나를 상기 거래 조건과 비교하여 거래 승인 여부를 결정하고 상기 거래 조건은 상기 제1 계정의 사용권 한, 상기 제1 계정의 결제 권한 및 상기 제1 계정의 백업키를 포함할 수 있다.
- [24] 다른 일실시예에 따르면, 상기 결제 요청 메시지에 포함되는 거래 유형 정보가 할부 거래에 대응하는 경우, 상기 거래 관리부는 상기 거래 조건에 포함되는 결제 한도를 할부된 전체 금액만큼 차감할 수 있다.
- [] 또 다른 일실시예에 따르면, 상기 거래 관리부는, 소정 기간 이후에 상기 제1 계정에 대응하는 할부 대금의 입금 여부를 확인하고, 상기 입금 결과에 따라 상기 거래 조건에 포함되는 결제 한도의 일부를 복원할 수 있다.
- [26] 또 다른 일실시예에 따르면, 상기 결제 요청 메시지에 포함되는 거래 유형 정보가 할부 거래에 대응하는 경우, 상기 거래 관리부는 상기 거래 조건을 이용하여 상기 제1 계정이 할부 가능 계정인지 여부를 확인할 수 있다.
- [] 또 다른 일실시예에 따르면, 상기 거래 관리부는 상기 제1 계정에 연관되는 식별값을 확인하고, 상기 식별값이 나타내는 정보에 따라 상기 결제 요청 메시지에 상응하는 송금 처리 또는 결제 처리를 진행하는 것을 특징으로 할 수 있다.

2735

도면의 간단한 설명

- [28] 도 1은 여신 가상화폐를 이용하여 결제가 진행되는 과정을 전체적으로 도시하는 예시도이다.
- [29] 도 2는 일실시예에 따른 가상화폐 생성 장치를 나타내는 블록도이다.
- [30] 도 3은 다른 일실시예에 따른 가상화폐 생성 장치의 동작 과정을 설명하는 예시도이다.
- [31] 도 4는 여신 가상화폐를 이용한 결제 과정을 도시하는 흐름도이다.
- [32] 도 5는 일실시예에 따라 주계정에 연관되는 사용자 단말이 종속계정의 생성을 요청하는 과정을 설명하는 흐름도이다.
- [33] 도 6a 및 도 6b는 또 다른 일실시예에 따른 가상화폐 생성 장치가 다중서명 계정을 생성하는 과정을 설명하는 예시도이다.
- [34] 도 7은 일실시예에 따른 가상화폐 관리 장치를 나타내는 블록도이다.
- 발명의 실시를 위한 최선의 형태**

- [35] 실시예들에 대한 특정한 구조적 또는 기능적 설명들은 단지 예시를 위한 목적으로 개시된 것으로서, 다양한 형태로 변경되어 실시될 수 있다. 따라서, 실시예들은 특정한 개시형태로 한정되는 것이 아니며, 본 명세서의 범위는 기술적 사상에 포함되는 변경, 균등물, 또는 대체물을 포함한다.
- [36] 제1 또는 제2 등의 용어를 다양한 구성요소들을 설명하는데 사용될 수 있지만, 이런 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 해석되어야 한다. 예를 들어, 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소는 제1 구성요소로 도 명명될 수 있다.
- [37] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다.
- [38] 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 기재된 특징, 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함으로 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.
- [39] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 해당 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.
- [40] 이하, 실시예들을 첨부된 도면들을 참조하여 상세하게 설명한다. 첨부 도면을 참조하여 설명함에 있어, 도면 부호에 관계없이 동일한 구성요소는 동일한 참조부호를 부여하고, 이에 대한 중복되는 설명은 생략하기로 한다.
- [41] 용어의 설명
- [42] 이하의 설명에서, 블록 체인이란 거래 정보 각각을 하나의 블록으로 생성하고, 생성된 블록들을 차례차례 연결한 거래 장부를 나타낸다. 블록 체인 기술을 이용하여 비트코인(bitcoin)과 같은 암호화된 가상화폐들이 생성될 수 있다. ..비트코인..이란 2009년 1월 사토시 나카모토에 의해 개발되어 소스코드 (source code)가 공개된 암호화 페(cryptocurrency)이며, 오늘날 이용되고 있는 가상화폐 의 한 종류이다.
- [43] 이하의 실시예들이 새롭게 제안하는 여신 가상화폐 (credit virtual currency)는 사용자의 신용 한도에 기반하여 발행된 가상화폐를 나타낼 수 있다. 여신 가상화폐에 상응하는 결제 대금의 납부 여부에 따라 여신 가상화폐가 갖는 결제 한도가 복원될 수도 있고, 제한될 수도 있을 것이다.
- [44] 도 1은 여신 가상화폐를 이용하여 결제가 진행되는 과정을 전체적으로

도시하는 예시도 이다. 도 1을 참고하면, 여신 가상화폐 거래관리 시스템 (40)이 도시된다. 예시적으로, 여신 가상화폐 거래관리 시스템 (40)은 가상화폐 생성 장치(111) 및 가상화폐 관리 장치(112)를 포함할 수 있다. 도 1에서는 이해를 돕기 위해 여신 가상화폐 거래관리 시스템 (40)이 개별적인 기능에 따라 두 개의 장치(111, 112)로 구현되는 경우에 대해 설명되나, 이는 다른 실시예의 범위를 제한하거나 한정하는 것으로서 해석되어서는 안 될 것이다. 이를테면, 여신 가상화폐 거래관리 시스템 (40) 자체가 기능적 분리 없이 하나의 프로세서를 통해 구현되는 실시예 또한 발명의 권리범위에 포함될 것이다.

[45] 여신 가상화폐 거래관리 시스템 (40)은 각각의 소비자들에 대응하는 사용자 단말에 여신 가상화폐 (120)를 발급할 수 있다. 구체적으로, 여신 가상화폐 거래관리 시스템 (40)에 포함되는 가상화폐 생성 장치(111)가 각각의 사용자 단말에 여신 가상화폐 (120)를 발급할 수 있다. 가상화폐 생성 장치(111)는 블록 체인에 기반하여 특정 소비자의 신용(credit) 한도에 따라 생성되는 가상화폐를 발행할 수 있다. 구체적으로, 가상화폐 생성 장치(111)는 상기 가상화폐를 포함하는 블록 체인을 생성하고, 상기 소비자의 결제 내역에 따라 상기 블록 체인을 업데이트할 수 있다.

[46] 일실시예로서, 제1 소비자는 자신이 이용하는 제1 사용자 단말(131)을 통해 가상화폐 생성 장치(111)로부터 여신 가상화폐 (120)를 발급받을 수 있다. 예시적으로, 가상화폐 생성 장치(111)는 실물 신용카드를 관리하는 카드사 서버 형태로 구현될 수 있다. 또한, 제1 사용자 단말(131)은 카드사 서버가 미리 배포한 어플리케이션을 통해 가상화폐 생성 장치(111)와 데이터 통신을 수행하고, 여신 가상화폐 (120)를 발급받을 수 있다.

[47] 다른 일실시예로서, 제1 소비자와 제2 소비자들은 여신 가상화폐 (120)를 이용하여 소비자 간의 피어투피어(peer to peer) 형태의 거래를 수행할 수 있다. 제1 소비자는 제1 사용자 단말(131) 내의 전자지갑에 저장된 여신 가상화폐 (120)를 전달하는 형태로, 제2 사용자 단말(132)에 여신 가상화폐 (120)를 송금할 수 있다.

[48] 또 다른 일실시예로서, 제1 소비자 또는 제2 소비자 각각은 자신의 사용자 단말(131, 132)을 이용하여 제1 가맹점 단말(141)과 여신 가상화폐 (120)를 이용한 신용 거래를 진행할 수 있다. 구체적으로, 제1 소비자 또는 제2 소비자 각각은 자신의 사용자 단말(131, 132) 내의 전자지갑에 저장된 여신 가상화폐 (120)를 이용하여 제1 가맹점 단말(141)과 신용 결제를 진행할 수 있다. 일실시예로서, 제1 가맹점 단말(141)은 실제 가맹점에 배치된 2세대 어센더 3세대 단말이나 카드 결제 단말과 같은 형태로 구현될 수 있다. 다른 일실시예로서, 제1 가맹점 단말(141)은 온라인 상으로 운영되는 인터넷 쇼핑 사이트 등의 가맹점 서버와 같은 형태로 구현될 수도 있을 것이다.

[49] 또 다른 일실시예로서, 제1 가맹점 단말(141)은 카드사 서버로부터 배포된 가상화폐 어플리케이션을 실행하는 스마트폰, 스마트패드, 컴퓨터 및 휴대용

- 랩탑(laptop) 컴퓨터와 같은 단말로 구현될 수 있다. 보다 구체적으로, 제1 가맹점 단말(141)은 제1 소비자 또는 제2 소비자의 사용자 단말(131, 132)에 설치된 가상화폐 어플리케이션을 통하여 앱 투 앱 거래를 실행할 수 있다. 제1 가맹점 단말(141)은 사용자 단말(131, 132) 내의 가상화폐 어플리케이션으로부터 여신 가상화폐 (120)를 전달 받는 형태로 결제를 수행할 수 있다.
- [50] 신용 거래 서비스를 이용한 제1 소비자는 제1 사용자 단말(131)을 이용하여 여신 가상화폐 (120)를 통한 결제 대금을 가상화폐 관리 장치(112)에게 정산할 수 있다. 위와 같은 정산 과정에는 원화와 같은 실물 법정화폐가 이용될 수 있다. 상기 대금 정산 절차는 여신 가상화폐 (120)를 이용한 신용 거래와는 독립적으로 카드사와 소비자 사이의 계약에 따라 기설정된 시간 간격으로 수행될 수 있다. 다시 말하여, 대금 정산 절차는 여신 가상화폐 (120)를 이용한 신용 거래가 완료된 시점으로 부터 소정 시간 이후에 진행될 수 있다.
- [51] 또 다른 일실시예로서, 제1 가맹점과 제2 가맹점 각각은 소비자와 마찬가지로 여신 가상화폐 (120)를 이용하여 가맹점 간의 피어투 피어 형태의 거래를 수행할 수도 있다. 예시적으로, 제2 가맹점은 기업 간의 전자상 거래를 지원하는 B2B(Business To Business) 서버를 나타낼 수 있다. 또는, 제2 가맹점은 기업 간의 거래를 지원하는 B2B 가맹점의 결제 단말을 나타낼 수도 있다. 제1 가맹점은 제1 가맹점 단말(141) 내의 전자지갑에 저장된 여신 가상화폐 (120)를 전달하는 형태로, 제2 가맹점 단말(142)에 여신 가상화폐 (120)를 송금할 수 있다.
- [52] 제1 가맹점 단말(141) 및 제2 가맹점 단말(142) 각각은 전자지갑 내에 저장된 여신 가상화폐 (120)에 기반하여 가상화폐 관리 장치(112)로 여신 가상화폐 (120)의 환전 요청 메시지를 전송할 수 있다.
- [53] 본 실시예의 여신 가상화폐 거래관리 시스템 (no) 은 소비자의 신용을 기반으로 한 여신 가상화폐 (120)를 발행하고, 발행된 여신 가상화폐 (120)를 이용하여 소비자와 가맹점 사이뿐만 아니고, 소비자간 및 가맹점 간의 신용 거래를 지원할 수 있다. 이하에서는, 가상화폐 생성 장치가 하나의 소비자에 대한 복수의 종속계정을 생성하고, 블록 체인을 공유하는 신용 거래 서비스를 제공하는 과정에 대해 추가적인 도면과 함께 보다 자세히 설명된다.
- [54] 도 2는 일실시예에 따른 가상화폐 생성 장치를 나타내는 블록도 이다. 도 2를 참조하면, 가상화폐 생성 장치(200)는 통신부 (2W), 블록 체인 생성부 (220), 계정관리부 (230) 및 거래 생성부 (240)를 포함할 수 있다. 통신부 (210)는 사용자 단말로 부터 제1 종속계정에 대한 생성 요청을 수신할 수 있다. 상기 사용자 단말은 소비자의 주계정에 대응하는 단말(mobile terminal)을 나타낼 수 있다. 또한, 상기 사용자 단말에는 가상화폐 생성 장치(200)를 관리하는 카드사에 의해 배포된 어플리케이션이 설치되어 있고, 상기 소비자는 사용자 단말을 통해 가상화폐 생성 장치(200)에 대한 계정인증을 미리 수행할 수 있다.
- [55] 본 실시예의 여신 가상화폐는 복수의 다중계정을 통해 공유될 수 있다. 구체적으로, 소비자가 직접적으로 결제를 진행하는 하나의 주계정과, 상기

주계정의 인증을 통해 생성되며 소비자의 가족 또는 소비자에 연관되는 사물 단말을 통해 결제가 수행되는 복수의 종속 계정이 가상화폐를 공유하며 블록 체인을 업데이트할 수 있다.

- [56] 블록 체인 생성부(220)는 소비자의 신용 한도에 따라 생성되는 가상화폐를 포함하는 블록 체인을 생성할 수 있다. 또한, 블록 체인 생성부(220)는 결제 내역에 따라 상기 블록 체인을 업데이트할 수 있다. 블록 체인에 대한 구체적인 설명은 기술 분야에 있는 전문가에게는 straight forward 한 사항이므로 자세한 설명은 생략하기로 한다.
- [57] 계정관리 부(230)는 블록 체인을 공유하는 복수의 계정들의 다중서명(multi-signature)을 관리할 수 있다. 예시적으로, 다중서명에는 개인키에 기반한 전자서명, 시스템키에 기반한 전자서명 및 백업키에 기반한 전자서명 중 적어도 하나가 포함될 수 있다. 구체적으로, 계정관리 부(230)는 소비자의 사용자 단말에 관한 주계정 및 상기 소비자에 연관되는 적어도 하나의 종속 계정 각각의 다중서명을 관리할 수 있다. 일실시예로서, 상기 소비자에 연관되는 적어도 하나의 종속 계정은 주계정 소유자의 가족 또는 회사직원과 같은 연관 인물에 의해 관리되는 계정일 수 있다.
- [58] 다른 일실시예로서, 상기 소비자에 연관되는 적어도 하나의 종속 계정은 주계정 소유자가 보유하고 있는 사물 단말에 연관되는 계정일 수 있다. 구체적으로, 사물 단말은 IoT(Internet Of Things) 단말과 같이 자동화된 데이터 통신 기능을 갖는 기계 단말로서, 스마트 센서, 자동차, 냉장고 및 세탁기 등과 같이 주계정 소비자가 이용하는 전자기기 중 하나의 형태로 구현될 수 있다.
- [59] 거래 생성부(240)는 복수의 계정 각각에 대응하는 거래 조건을 저장할 수 있다. 예시적으로, 거래 생성부(240)는 주계정에 대응하는 제1 거래 조건, 제1 종속 계정에 대응하는 제2 거래 조건 및 제2 종속 계정에 대응하는 제3 거래 조건 각각을 저장할 수 있다. 앞서 설명한, 주계정과 두 개의 종속 계정에 대한 거래 조건들의 설명은 이해를 돕기 위한 예시적 기재일 뿐, 발명의 사상이 위와 같은 예시로 제한되거나 한정되는 것은 아니다. 이를테면, 하나의 주계정만의 거래 조건이 저장되는 실시예 또는 하나의 주계정과 열 개의 종속 계정의 거래 조건이 각각 저장되는 실시예와 같은 다양한 변형이 가능할 것이다. 또한, 거래 생성부(240)는 거래 조건에 따라 블록 체인을 이용한 결제를 진행할 수 있다. 이하에서는 추가적인 도면과 함께 다중계정 각각의 다중서명 계정과 거래 조건들이 관리되는 과정이 설명된다.
- [60] 도 3은 다른 일실시예에 따른 가상화폐 생성 장치의 동작 과정을 설명하는 예시도이다. 도 3을 참조하면, 가상화폐 생성 장치(300)는 계정관리부(3W), 거래 생성부(320) 및 블록 체인 생성부(330)를 포함할 수 있다. 제1 소비자(341)는 자신에 연관되는 복수의 계정을 통해 가족, 지인과 같은 사람뿐만 아니라 전자기기와 같은 IoT 단말들과 여신 가상화폐를 공유할 수 있다.
- [61] 도 3의 실시예에서, 제1 소비자(341)는 자신이 이용하는 주계정과 함께 네 개의

종속계정을 이용할 수 있다. 네 개의 종속계정은 각각 제1 소비자(341)의 가족(342), 제1 소비자(341)의 자동차(343), 제1 소비자(341)의 냉장고(344) 및 제1 소비자(341)의 세탁기(345)에 연관될 수 있다.

- [62] 제1 소비자(341)는 사용자 단말을 이용하여 가상화폐 생성 장치(300)로 제1 종속계정에 대한 생성 요청을 전송할 수 있다. 구체적으로, 제1 소비자(341)는 주계정의 제1 개인키를 이용한 전자서명 및 상기 제1 종속계정에 대한 거래 조건을 상기 제1 종속계정에 대한 생성요청으로서 가상화폐 생성 장치(300)로 전송할 수 있다.
- [63] 본 실시예에서 제1 종속계정은 소비자(341)의 가족(342)에 연관되는 계정을 의미할 수 있다. 이 경우에, 계정관리부(자0)는 사용자 단말에 저장된 제1 개인키를 인증할 수 있다. 또한, 계정관리부(310)는 인증의 결과에 따라 제1 종속계정의 생성 여부를 결정할 수 있다.
- [64] 보다 구체적으로, 계정관리부(자0)는 제1 개인키가 인증된 경우에 제1 소비자(341)에 대한 제1 종속계정을 생성할 수 있다. 상기 제1 종속계정은 제2 다중서명 계정을 포함하고, 상기 제2 다중서명 계정은 제1 개인키를 이용하여 유도된(由比애) 개인키 중 적어도 하나를 포함할 수 있다.
- [65] 이 경우에, 거래 생성부(320)는 제1 소비자(341)에 대한 제1 개인키가 인증된 경우, 제1 종속계정에 대한 제2 거래 조건을 저장할 수 있다. 구체적으로, 제2 거래 조건은 제1 종속계정의 유효기간, 사용권한 및 결제권한 중 적어도 하나를 포함할 수 있다.
- [66] 위와 같은 원리에 기초하여, 가상화폐 생성 장치(300)는 제1 소비자(341)의 가족(342), 제1 소비자(341)의 자동차(343), 제1 소비자(341)의 냉장고(344) 및 제1 소비자(341)의 세탁기(345) 각각에 대한 종속계정들을 생성할 수 있다. 구체적으로, 제1 소비자(341)의 가족(342)에 연관되는 제1 종속계정은 제2 다중서명 계정 및 제2 거래 조건에 연관되고, 제1 소비자(341)의 자동차(343)에 연관되는 제2 종속계정은 제3 다중서명 계정 및 제3 거래 조건에 연관된다. 또한, 제1 소비자(341)의 냉장고(344)에 연관되는 제3 종속계정은 제4 다중서명 계정 및 제4 거래 조건에 연관되고, 제1 소비자(341)의 세탁기(345)에 연관되는 제4 종속계정은 제5 다중서명 계정 및 제5 거래 조건에 연관될 수 있다.
- [67] 본 실시예에 따른 가상화폐 생성 장치(300)는 주계정의 관리하에 운영되는 다중사용자 계정을 생성할 수 있다. 또한, 가상화폐 생성 장치(300)는 각각의 종속계정에 대응하는 거래 조건들을 관리함으로써 서로 다른 권한을 갖는 복수의 계정을 지원하는 효과를 사용자에게 제공할 수 있다. 이를테면, 자동차(343)에 연관되는 제2 종속계정은 카센터 또는 주유소와 같은 유형의 가맹점 내에서만 거래가 가능하도록 제한하는 제3 거래 조건이라든가, 미성년자인 가족(342)에 연관되는 제1 종속계정은 주계정의 결제 한도와 다른 월 30만원의 결제 한도를 갖도록 하는 제2 거래 조건과 같은 서비스를 제공할 수 있다.

- [68] 도 4는 여신 가상화폐 를 이용한 결제 과정을 도시하는 흐름도 이다. 도 4를 참조하면 , 소비자의 종속 계정에 연관되는 단말(산 0), 소비자의 주 계정에 연관되는 사용자 단말(420) 및 가상화폐 생성 장치(430) 상호 간에 데이터 통신을 통해 여신 가상화폐를 발행하고 , 상기 여신 가상화폐를 이용하여 결제를 진행하는 과정이 도시된다.
- [69] 종속 계정에 연관되는 단말(410)은 블록 체인을 공유하는 새로운 종속 계정을 생성하기 위해 주 계정에 연관되는 사용자 단말(420)로 인증 요청 메시지를 전송할 수 있다. 단말(산 0)은 소비자의 가족이 이용하는 단말 또는 전자기 기로 구현되는 1(付 단말과 같은 형태로 구현될 수 있다. 단말(410)에는 가상화폐를 발행하는 카드사가 배포한 어플리케이션이 미리 설치되어 있을 수 있다. 어플리케이션의 설치 과정은 소비자의 가족이나 회사 직원과 같은 종속 계정 소유자의 선택으로 진행되거나 , 단말 제조사 , 주 계정 소유자 본인의 선택 등 다양한 방법으로 진행될 수 있다. 이 경우에 , 주 계정에 연관되는 사용자 단말(420)은 이미 카드사 서버에 대해 계정인증 및 생성을 마친 상태일 수 있다.
- 「 이 주 계정에 연관되는 사용자 단말(420)은 종속 계정 생성 요청 메시지에 응답하여 종속 계정에 연관되는 단말(산 0)을 인증할 수 있다. 상기 인증이 성공된 경우 , 사용자 단말(420)은 종속 계정에 대한 거래 조건 및 주 계정의 제1 개인키로 생성된 전자서명을 포함하는 종속 계정 생성 요청을 가상화폐 생성 장치(430)로 전송할 수 있다.
- 「 1] 가상화폐 생성 장치(430)의 계정관리부(431)는 수신한 전자서 명을 검증하여 사용자 단말(420)에 관한 주 계정을 인증할 수 있다. 상기 주 계정이 인증된 경우 , 계정관리 부(431)는 거래 생성부(432)로 종속 계정에 대한 거래 조건의 생성을 요청할 수 있다. 상기 거래 조건은 생성될 종속 계정에 대한 유효기 간, 사용권 한, 결제권 한 등을 포함하며 , 상기 거래 조건은 블록 체인에 저장될 수 있도록 전달된다 .
- 「 2] 거래 생성부(432)로부터 결과를 수신한 계정관리 부(431)는 주 계정의 제1 개인키로부터 유도한 개인키를 기반으로 종속 계정의 다중서명 계정을 생성할 수 있다. 또한, 거래 생성부(432)는 통신부를 통해 생성된 종속 계정의 제2 개인키와 처리 결과를 계정생성에 대한 응답 메시지로 사용자 단말(420)에 전송할 수 있다. 또한, 사용자 단말(420)은 종속 계정에 연관되는 단말(410)로 제2 개인키를 전송할 수 있다. 단말(410) 내의 메모리에 제2 개인키가 저장되면서 종속 계정 생성 절차가 종료될 수 있다.
- 「 3] 소비자의 가족 또는 사물 단말은 종속 계정을 이용하여 가상화폐를 이용한 결제 요청 메시지를 가상화폐 생성 장치(430)로 전송할 수 있다. 이 경우에 , 계정관리 부(431)는 종속 계정에 대한 결제 요청 메시지에 응답하여 종속 계정을 응답하고 , 거래를 처리할 수 있다. 계정관리 부(431)는 거래 생성부(432)로 결제 내역에 따른 블록 체인 업데이트를 요청할 수 있다. 거래 생성부(432)은 이에 응답하여 처리 결과를 계정관리 부(431)로 전달할 수 있다.

- 「4」 단말(410) 또는 사용자 단말(420) 각각에는 가상화폐를 발행하는 카드사 서버로부터 배포된 가상화폐 어플리케이션이 설치될 수 있다. 또한, 각각의 가상화폐 어플리케이션은 단말(410) 또는 사용자 단말(420)의 식별값을 나타내는 데이터 필드를 포함할 수 있다. 상기 식별값에 따라 가상화폐 생성 장치(430)는 신용 거래에 연관되는 주체가 법인인지, 가맹점인지, 개인인지 여부를 확인할 수 있다. 일실시예로서, 가상화폐 생성 장치(430)는 가상화폐를 이용한 거래 요청 메시지가 개인과 개인 사이의 메시지라면, 가상화폐를 이용한 송금 처리를 수행할 수 있다. 다른 일실시예로서, 가상화폐 생성 장치(430)는 가상화폐를 이용한 거래 요청 메시지가 법인이나 가맹점과 개인 사이의 메시지라면, 가상화폐를 이용한 결제 처리를 수행할 수 있다.
- 「5」 계정관리부(431)는 사용자 단말(420) 또는 단말(410)로 처리 결과를 전송할 수 있다.
- 「6」 도 5는 일실시예에 따라 주계정에 연관되는 사용자 단말이 종속계정의 생성을 요청하는 과정을 설명하는 흐름도이다. 도 5를 참조하면, 주계정에 연관되는 사용자 단말이 종속계정을 생성하는 방법은 블록체인을 이용하기 위한 주계정의 제1개인키를 암호화하여 저장하는 단계(5W), 지정된 조건에 따라 상기 종속계정에 연관되는 단말을 인증하는 단계(520), 상기 인증의 결과에 따라 상기 종속계정의 생성을 요청하는 메시지를 상기 블록체인을 관리하는 카드사 서버로 전송하는 단계(530) 및 상기 카드사 서버로부터 상기 종속계정에 대한 계정생성 응답 메시지를 수신하는 단계(540)를 포함할 수 있다.
- 「7」 단계(510)에서 주계정에 연관되는 사용자 단말은 블록체인을 이용하기 위한 주계정의 제1개인키를 암호화하여 저장할 수 있다. 예시적으로, 사용자 단말 내의 메모리는 블록체인을 이용하기 위한 주계정의 제1개인키를 암호화하여 저장할 수 있다. 상기 제1개인키는 상기 사용자 단말에 대한 인증 결과에 기반하여 카드사 서버로부터 수신된 개인키를 나타낼 수 있다. 또한, 상기 제1개인키에 상응하는 제1시스템키는 가상화폐를 발급하고 관리하는 카드사 서버에 저장될 수 있다.
- 「8」 단계(520)에서 사용자 단말에 포함되는 프로세서는 지정된 조건에 따라 종속계정에 연관되는 단말을 인증할 수 있다. 이를테면, 상기 프로세서는 상기 종속계정에 연관되는 단말에 대해 주계정 소비자에 대한 주민등록번호, 실물 신용카드 번호, 실물 신용카드 비밀번호 및 휴대폰 번호 등과 같은 식별키(identification key)를 요구하고, 수신된 식별키 값을 검증하는 방식으로 상기 단말을 인증할 수 있다. 종속계정에 연관되는 단말을 인증하는 과정에 대해서는 기술 분야에 널리 알려진 방식과 같이 다양한 변형이 가능할 것이다. 이를테면, 실물 신용카드의 유효기간 검증 또는 실물 신용카드의 CVC(Card Validation Code) 번호 검증과 같은 다양한 실시예로서 사용자 단말이 종속계정에 연관되는 단말을 인증할 수 있다.
- 「9」 단계(530)에서 사용자 단말에 포함되는 프로세서는 단계(520)에서의 인증의

결과에 따라 새로운 종속계정의 생성을 요청하는 메시지를 생성할 수 있다. 예시적으로, 상기 새로운 종속계정의 생성을 요청하는 메시지는 상기 주계정의 제1 개인키를 이용한 전자서명 및 상기 새로운 종속계정에 대한 거래 조건을 포함할 수 있다. 구체적으로, 프로세서는 사용자 입력에 따라 상기 종속계정의 유효기간, 사용권한 및 결제권한 중 적어도 하나를 포함하는 상기 거래 조건을 결정할 수 있다. 소비자는 주계정에 상응하는 사용자 단말을 통해 제1 종속계정의 유효기간을 1년으로 설정하거나, 제2 종속계정이 패스트푸드와 같은 요식업 업종 가맹점에 대해서만 결제권한을 갖는 것과 같은 각각의 거래 조건을 설정함으로써 동일한 가상화폐를 공유하는 복수의 계정들의 각각의 개별적인 거래 환경을 정의할 수 있다. 위와 같은 거래 조건은 오늘날 기술 분야에서 널리 이용되는 이른바 스마트 계약(smart contract) 형태로 구현될 수도 있을 것이다.

- [80] 또한, 사용자 단말의 통신부는 상기 새로운 종속계정의 생성을 요청하는 메시지를 블록체인을 관리하는 카드사 서버로 전송할 수 있다. 상기 블록체인은 소비자의 신용 한도에 따라 생성되는 가상화폐를 포함할 수 있다. 통신부는 통신 인터페이스를 포함하는 통신 모듈의 형태로 구현될 수 있다. 이를테면, 통신 인터페이스는 WLAN(Wireless LAN), WiFi(Wireless Fidelity) Direct, DLNA(Digital Living Network Alliance), Wibro(Wireless broadband), Wimax(World Interoperability for Microwave Access), HSDPA(High Speed Downlink Packet Access) 등의 무선 인터넷 인터페이스와 블루투스(Bluetooth™), RFID(Radio Frequency Identification), 적외선 통신(Infrared Data Association; IrDA), UWB(Ultra Wideband), ZigBee, NFC(Near Field Communication) 등의 근거리 통신 인터페이스를 포함할 수 있다. 뿐만 아니라, 통신 인터페이스는 외부와 통신을 수행할 수 있는 모든 인터페이스(예를 들어, 유선 인터페이스)를 나타낼 수 있다.
- [81] 단계(540)에서 사용자 단말은 상기 카드사 서버로부터 상기 종속계정에 대한 계정생성 응답 메시지를 수신할 수 있다. 구체적으로, 사용자 단말에 포함되는 프로세서는 계정생성 응답 메시지로 부터 상기 새로운 종속계정에 대한 복수의 제2 개인키를 추출할 수 있다. 상기 통신부는 상기 새로운 종속계정에 대한 복수의 제2 개인키 중 하나를 종속계정에 연관되는 단말의 개인키로서 상기 단말로 전송할 수 있다. 또한, 프로세서는 상기 복수의 개인키 중 하나를 새로운 종속계정에 대한 백업키로서 사용자 단말 내의 메모리에 저장할 수 있다.
- [82] 본 실시예에 다른 사용자 단말을 이용하여, 소비자는 자신의 주계정에 기초하여 인증된 복수의 종속계정을 생성할 수 있다. 또한, 소비자는 결제 수단으로 자신의 신용에 기반하여 여신 가상화폐를 공유하는 종속계정을 생성하면서, 거래 조건에 기반하여 각각의 종속계정들의 개별적인 거래 환경을 관리하는 것 또한 가능하여 다중사용자 계정을 관리하는 편의성이 극대화되는 효과를 기대할 수 있다.
- [83] 도 6a 및 도 6b는 또 다른 일실시예에 따른 가상화폐 생성 장치가 다중서명

계정을 생성하는 과정을 설명하는 예시도이다. 도 6a을 참조하면, 제1 소비자에 대응하는 다중서명 계정을 생성하는 가상화폐 생성 장치(610)의 동작이 도시된다. 본 실시예에 따른 가상화폐 생성 장치(610)는 계정관리부(611)와 거래 생성부(612)를 포함할 수 있다. 제1 소비자(621)는 자신이 직접 관리하는 주계정뿐만 아니라, 제1 소비자의 가족(622) 및 제1 소비자의 IoT 단말(623) 각각이 이용하는 두 개의 종속계정을 추가 생성할 수 있다.

- [84] 제1 소비자(621)의 사용자 단말 내의 전자지갑에는 주계정에 대한 제1 개인키(631)가 저장된다. 제1 개인키(631)는 주계정에 대한 인증이 완료된 이후에 가상화폐 생성 장치(610)로부터 발급된 키를 나타낼 수 있다. 가상화폐 생성 장치(610)는 제1 개인키(631)에 대응하는 제1 시스템 키(632)를 계정관리부(611) 내의 다중서명 계정에 저장할 수 있다. 또한, 가상화폐 생성 장치(610)는 제1 개인키(631)에 대응하는 제1 백업키(633)를 발급하여, 제1 백업키(633)를 주계정에 연관되는 사용자 단말로 전송할 수 있다. 제1 소비자(621)는 제1 백업키(633)를 USB(Universal Serial Bus)와 같은 범용 저장장치에 보관하는 방식으로, 제1 개인키(631)가 삭제되거나 분실되는 경우를 대비할 수 있다. 제1 개인키(631)가 삭제되거나 분실된 경우, 제1 소비자(621)의 사용자 단말은 제1 백업키(633)를 가상화폐 생성 장치(6W)에 전송함으로써 제1 시스템키(632)와의 인증을 통해 여신 가상화폐를 통한 결제를 진행하거나 계정을 삭제하는 것과 같은 관리 행위를 지속할 수 있다.
- [85] 또한, 계정관리부(611)는 주계정의 사용자 단말로 부터 새로운 종속계정의 생성 요청이 수신되면, 제1 개인키(631)에 의한 전자서명을 검증할 수 있다. 제1 개인키(631)에 의한 전자서명이 인증된 경우, 계정관리부(611)는 각각의 종속계정을 생성할 수 있다. 일실시예로서, 계정관리부(611)는 제1 개인키(631)로부터 유도된 복수의 제2 개인키(641, 642, 643)를 생성할 수 있다. 구체적으로, 계정관리부(611)는 복수의 제2 개인키 중 하나를 제2 시스템 키(642)로 저장하고, 복수의 제2 개인키 중 하나를 주계정에 대한 사용자 단말로 제2 백업키(643)로서 전송하고, 복수의 제2 개인키 중 하나를 제1 종속계정에 대한 단말의 개인키(641)로서 전송할 수 있다.
- [86] 위와 같은 원리로, 계정관리부(611)는 제1 개인키(631)에 의한 전자서명을 검증하여, 제3 개인키(651), 제3 시스템키(652) 및 제3 백업키(653)를 생성할 수도 있다. 제3 시스템 키(652)는 제1 소비자의 IoT 단말(623)과 연관되며 계정관리부(611) 내의 다중서명 계정 내에 저장될 수 있다. 또한, 제3 개인키(651)는 제1 소비자의 IoT 단말(623) 내의 전자지갑에 단말에 대한 개인키로서 저장될 수 있다.
- [87] 본 실시예에서는 계정관리부(611)가 종속계정에 대한 단말로 개인키(641)를 전송하는 과정이 설명되나, 주계정에 대한 사용자 단말이 두 개의 개인키를 수신하고, 그 중 하나를 종속계정에 대한 단말로 전송하는 실시예 또한 구현 가능할 것이다. 이 경우에, 계정관리부(611)는 제1 개인키(631)가 인증된 경우에,

새로운 종속 계정 각각에 대한 거래 조건을 저장하고 , 제 1 개인키 (631)로부터 유도된 복수의 제2 개인키 중 적어도 두 개의 주계정에 대한 사용자 단말로 전송할 수 있다.

- [88] 이 경우에 , 주계정에 연관되는 소비자의 사용자 단말은 주계정에 대한 제 1 개인키(631)를 저장하고 , 복수의 종속 계정에 대한 백업키(643, 653) 또한 함께 저장할 수 있다. 상기 백업키들(643, 653)은 제 1 개인키 (631)로부터 유도된 것을 특징으로 할 수 있다. 이에 따라, 소비자는 종속 계정들에 대한 백업키들(643, 653)에 기반하여 개별 종속 계정 각각에 대한 거래 중단, 결제 취소, 개인키 폐기와 같은 계정관리를 안정적으로 수행할 수 있다. 또한, 카드사 서버는 제 1 개인키 (631)에 기반하여 생성된 복수의 종속 계정에 대한 백업키(643, 653)를 검증할 수 있어, 소비자가 해당 종속 계정에 대한 관리 능력을 갖는 주계정의 사용자라는 것을 안전하면서도 용이하게 확인하는 효과를 가질 수 있다.
- [89] 일 실시 예로서 , 주 계정에 연관되는 사용자 단말의 프로세서는 사용자 입력에 응답하여 상기 새로운 종속 계정에 대한 계정삭제 메시지 및 결제취소 메시지 중 하나를 생성할 수 있다. 예를 들어, 소비자가 제 1 소비자의 가족(622)에 대한 제 1 종속 계정을 삭제하고자 하는 경우에 , 상기 계정삭제 메시지 및 상기 결제취소 메시지 각각은 사용자 단말의 메모리 에 저장된 제2 백업키(643)에 기초한 전자서 명을 포함할 수 있다. 또한, 제2 백업키(643)는 제 1 종속 계정의 단말이 저장하고 있는 제2 개인키(641)로부터 유도된 키를 나타낼 수 있다. 사용자 단말의 통신부는 상기 계정삭제 메시지 및 상기 거래취소 메시지 중 하나를 계정관리부(611)로 전송할 수 있다. 계정관리부(611)는 제 1 종속 계정에 대해 저장된 제2 시스템 키(642)를 이용하여 상기 전자서 명을 검증하고 , 상기 검증의 결과에 따라 제 1 종속 계정을 삭제하거나 , 제 X종속 계정에 연관되는 결제를 취소할 수 있다.
- [90] 다른 일 실시 예로서 , 계정관리 부(611)는 제 1 개인키 (631)로부터 유도된 하나의 제3 개인키를 생성하고, 생성된 제3 개인키를 주계정에 대한 사용자 단말에 제3 백업키(653)로서 전송할 수 있다. 또한, 계정관리부(610)는 제3 백업키(653)에 기반하여 복수의 제3 개인키를 생성하고 , 복수의 제3 개인키 중 하나를 제3 시스템 키(652)로서 저장하고 , 복수의 제3 개인키 중 하나를 제2 종속 계정에 대한 단말의 개인키(651)로서 전송할 수 있다.
- [91] 도 해를 참조하면 , 주 계정에 대한 제 1 개인키 (631)와 독립적으로 , 복수의 종속 계정에 대한 백업키(643, 653)가 별도로 관리되는 실시 예가 개시된다. 나머지 구성요소들에 대해서는 도 6a와 함께 기재된 설명이 그대로 적용될 수 있으므로 중복되는 설명은 생략한다 . 주 계정을 관리하는 제 1 소비자 (621)는 자신의 사용자 단말 내의 전자지갑에 주계정에 대한 제 1 개인키 (631)만을 저장할 수 있다. 이 경우에, 제 1 소비자 (621)는 복수의 종속 계정 각각에 대한 백업키(643, 653)를 별도의 USB나 저장 토큰과 같은 저장 매체에 보관하여 비상 사태를 대비할 수 있다. 이를 테면, 제 1 소비자 (621)가 사용자 단말을 분실한 경우에 , 제 1

개인키(631)를 잃어버릴 가능성이 존재한다. 그러나, 이 경우에 제1 소비자 (621)는 주계정의 개인키가 재발행되기 이전까지 별도 보관된 백업키(643, 653)들을 이용하여 종속계정에 대한 계정 삭제, 결제 취소 등의 관리를 지속하는 효과를 가질 수 있다.

- [92] 도 7은 일실시예에 따른 가상화폐 관리 장치를 나타내는 블록도 이다. 도 7을 참조하면, 가상화폐 관리 장치(700)는 통신부 (기0), 블록체인 생성부(720) 및 거래 관리부 (730)를 포함할 수 있다. 통신부 (710)는 블록체인을 공유하는 복수의 계정 중 제1 계정에 연관되는 단말로 부터 상기 블록체인을 이용한 결제 요청 메시지를 수신할 수 있다. 도 7에 도시되지는 않았지만, 가상화폐 관리 장치(700)는 프로세서를 포함하며, 블록체인 생성부(720) 및 거래 관리부 (730) 각각은 프로세서에 의해 적어도 일시적으로 구현될 수 있다.
- [93] 블록체인 생성부(720)는 소비자의 신용(credit) 한도에 따라 생성되는 가상화폐를 포함하는 상기 블록체인을 생성하고, 결제 내역에 따라 상기 블록체인을 업데이트할 수 있다.
- [94] 거래 관리부(730)는 상기 결제 요청 메시지와 상기 제1 계정에 대응하는 거래 조건을 확인하여 거래 승인 여부를 관리할 수 있다. 거래 관리부 (730)는 결제 요청 메시지에 포함되는 가맹점 정보, 결제금액 및 전자서명 중 적어도 하나를 상기 거래 조건과 비교하여 거래 승인 여부를 결정할 수 있다. 상기 거래 조건은 동일한 소비자의 다중계정일지라도, 각각의 주계정 또는 종속계정 별로 상이한 거래 조건이 설정될 수 있다. 구체적으로, 거래 조건은 상기 제1 계정의 사용권 한, 상기 제1 계정의 결제권한 및 상기 제1 계정의 백업키를 포함할 수 있다.
- [95] 일실시예로서 결제 요청 메시지에 포함되는 거래 유형 정보가 할부 거래에 대응하는 경우, 거래 관리부 (730)는 상기 거래 조건에 포함되는 결제 한도를 할부된 전체 금액만큼 차감할 수 있다. 또한, 거래 관리부 (730)는 소정 기간 이후에 상기 제1 계정에 대응하는 할부 대금의 입금 여부를 확인하고, 상기 입금 결과에 따라 상기 거래 조건에 포함되는 결제 한도의 일부를 복원할 수 있다.
- [96] 예시적으로, 전체적으로 120만원의 결제 한도를 갖는 제1 종속계정이 존재하는 경우가 있을 수 있다. 이 경우에, 제1 종속계정을 이용하여 5개월 할부로 100만원의 결제가 발생된 경우에, 거래 관리부 (730)는 상기 제1 종속계정의 결제 한도를 20만원으로 계산할 수 있다. 1개월 뒤에 할부금에 상응하는 20만원이 입금되었다면, 거래 관리부 (730)는 종전의 20만원에서 입금된 20만원 만큼의 결제 한도를 복원하는 방식으로 상기 제1 종속계정의 결제 한도를 40만원 만큼 복원할 수 있다. 위와 같은 방식으로, 가상화폐 관리 장치(700)는 각각의 종속계정에 대한 할부 거래를 지원하며, 할부 거래에 상응하도록 결제 한도를 관리할 수 있다.
- [97] 다른 일실시예로서 결제 요청 메시지에 포함되는 거래 유형 정보가 할부 거래에 대응하는 경우, 거래 관리부 (730)는 상기 거래 조건을 이용하여 상기 제1

계정이 할부 가능 계정인지 여부를 확인할 수 있다. 예를 들어, 주계정의 소비자에 의해 특정 종속계정에 대해서는 할부 거래가 불가하도록 거래 조건이 설정되는 경우가 있을 수 있다. 이 경우에, 거래 관리부 (730)는 결제 요청 메시지에 응답하여 해당 종속계정이 할부 가능한 계정인지 여부를 미리 확인하는 방식으로 각각의 종속계정을 관리할 수 있다.

- [98] 이상에서 설명된 실시예들은 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치, 방법 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서 (digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

- [99] 소프트웨어는 컴퓨터 프로그램 (computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로 (collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

- [100] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 컴퓨터 판독 가능 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어

당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD 와 같은 광기록 매체(optical media), 솔롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

- [101] 이상과 같이 실시예들이 비록 한정된 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기를 기초로 다양한 기술적 수정 및 변형을 적용할 수 있다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

청구 범위

- [청구 항 1] 프로세서를 포함하고, 상기 프로세서에 의해 구현되는 :
 소비자의 신용(credit) 한도에 따라 생성되는 가상화폐를 포함하는
 블록 체인을 생성하고, 결제 내역에 따라 상기 블록 체인을 업데이트 하는
 블록 체인 생성부 ;
 상기 블록 체인을 공유하는 복수의 계정들의 다중서명(multi-signature)을
 관리하는 계정관리부 ; 및
 상기 복수의 계정 각각에 대응하는 거래 조건을 저장하고, 상기 거래
 조건에 따라 상기 가상화폐를 이용한 결제를 진행하는 거래 생성부
 를 포함하는 가상화폐 생성 장치.
- [청구 항 2] 제1항에 있어서,
 상기 계정관리부는 상기 소비자의 사용자 단말에 관한 주계정 및 상기
 소비자에 연관되는 적어도 하나의 종속계정 각각의 다중서명을 관리하는
 가상화폐 생성 장치.
- [청구 항 3] 제2항에 있어서,
 상기 사용자 단말로 부터 제1 종속계정에 대한 생성 요청을 수신하는
 통신부
 를 더 포함하고,
 상기 계정관리부는 상기 사용자 단말에 저장된 제1 개인키를 인증하고,
 상기 인증의 결과에 따라 상기 제1 종속계정의 생성 여부를 결정하는
 가상화폐 생성 장치.
- [청구 항 4] 제3항에 있어서,
 상기 계정관리부는 상기 제1 개인키가 인증된 경우에 상기 제1
 종속계정을 생성하고, 상기 제1 개인키를 이용하여 상기 제1 종속계정의
 다중서명을 생성하는 가상화폐 생성 장치.
- [청구 항 5] 제4항에 있어서,
 상기 계정관리부는 상기 제1 개인키로 부터 유도된 복수의 제2 개인키를
 생성하고, 상기 복수의 제2 개인키 중 하나를 시스템 키로서 저장하고,
 상기 복수의 개인키 중 하나를 상기 주계정에 대한 사용자 단말로
 전송하고, 상기 복수의 개인키 중 하나를 상기 제1 종속계정에 대한
 단말로 전송하는 가상화폐 생성 장치.
- [청구 항 6] 제3항에 있어서,
 상기 통신부는 상기 주계정의 제1 개인키를 이용한 전자서명 및 상기 제1
 종속계정에 대한 거래 조건을 상기 제1 종속계정에 대한 생성 요청으로서
 수신하고,
 상기 거래 생성부는 상기 제1 개인키가 인증된 경우에 상기 제1
 종속계정에 대한 거래 조건을 저장하고, 상기 거래 조건은 상기 제1

- 종속계정의 유효기간, 사용권 한 및 결제권 한 중 적어도 하나를 포함하는 가상화폐 생성 장치.
- [청 구 항 7] 제2항에 있어서,
상기 소비자의 사용자 단말은 상기 주계정에 대한 제1개인키를 저장하고, 상기 적어도 하나의 종속계정 각각에 대한 백업키들을 저장하고,
상기 백업키들은 상기 제1개인키로부터 유도된 것을 특징으로 하는 가상화폐 생성 장치.
- [청 구 항 8] 단말로 부터 블록 체인을 공유하기 위한 인증 요청을 수신하는 통신부;
상기 블록 체인을 이용하기 위한 주계정의 제1개인키를 암호화하여 저장하는 메모리; 및
지정된 조건에 따라 상기 단말을 인증하고, 상기 인증의 결과에 따라 새로운 종속계정의 생성을 요청하는 메시지를 생성하는 프로세서를 포함하고,
상기 새로운 종속계정의 생성을 요청하는 메시지는 상기 주계정의 제1개인키를 이용한 전자서명 및 상기 새로운 종속계정에 대한 거래 조건을 포함하고,
상기 블록 체인은 소비자의 신용 한도에 따라 생성되는 가상화폐를 포함하는 사용자 단말.
- [청 구 항 9] 제8항에 있어서,
상기 프로세서는 사용자 입력에 따라 상기 종속계정의 유효기간, 사용권 한 및 결제권 한 중 적어도 하나를 포함하는 상기 거래 조건을 결정하는 사용자 단말.
- [청 구 항 10] 제8항에 있어서,
상기 통신부는 상기 새로운 종속계정의 생성을 요청하는 메시지를 상기 블록 체인을 관리하는 카드사 서버로 전송하고,
상기 카드사 서버는 상기 제1개인키가 인증된 경우에 상기 새로운 종속계정에 대한 거래 조건을 저장하고, 상기 제1개인키로부터 유도된 복수의 제2개인키 중 적어도 두 개를 상기 사용자 단말로 전송하는 것을 특징으로 하는 사용자 단말.
- [청 구 항 11] 제10항에 있어서,
상기 통신부는 카드사 서버로부터 상기 새로운 종속계정에 대한 계정생성 응답 메시지를 수신하고,
상기 프로세서는 상기 계정생성 응답 메시지로 부터 상기 새로운 종속계정에 대한 복수의 제2개인키를 추출하는 사용자 단말.
- [청 구 항 12] 제8항에 있어서,
상기 메모리는 카드사 서버로부터 배포된 가상화폐 어플리케이션을 포함하고, 상기 프로세서는 상기 통신부를 통해 상기 가상화폐

- 어플리케이션을 이용하여 접속하는 소비자 단말과 상기 블록 체인에
연관되는 가상화폐를 이용한 신용 결제를 처리하는 사용자 단말.
- [청구항 13] 제 11항에 있어서,
상기 통신부는 상기 새로운 종속계정에 대한 복수의 제2 개인키 중
하나를 상기 단말의 개인키로서 상기 단말로 전송하고,
상기 프로세서는 상기 복수의 제2 개인키 중 하나를 상기 새로운
종속계정에 대한 백업키로서 상기 메모리에 저장하는 사용자 단말.
- [청구항 14] 제 13항에 있어서,
상기 프로세서는 사용자 입력에 응답하여 상기 새로운 종속계정에 대한
계정삭제 메시지 및 결제취소 메시지 중 하나를 생성하고,
상기 계정삭제 메시지 및 상기 결제취소 메시지 각각은 상기 메모리에
저장된 제2 개인키에 기초한 전자서명을 포함하고,
상기 통신부는 상기 계정삭제 메시지 및 상기 거래취소 메시지 중 하나를
상기 카드사 서버로 전송하고,
상기 카드사 서버는 상기 종속계정에 대해 저장된 시스템키를 이용하여
상기 전자서명을 검증하고, 상기 검증의 결과에 따라 상기 종속계정을
삭제하거나, 상기 종속계정에 연관되는 결제를 취소하는 사용자 단말.
- [청구항 15] 종속계정을 생성하는 프로그램을 수록한 컴퓨터 판독 가능한 기록
매체에 있어서, 상기 프로그램은 :
블록 체인을 이용하기 위한 주계정의 제1 개인키를 암호화하여 저장하는
명령어 세트;
지정된 조건에 따라 상기 종속계정에 연관되는 단말을 인증하는 명령어
세트;
상기 인증의 결과에 따라 상기 종속계정의 생성을 요청하는 메시지를
상기 블록 체인을 관리하는 카드사 서버로 전송하는 명령어 세트; 및
상기 카드사 서버로부터 상기 종속계정에 대한 계정생성 응답 메시지를
수신하는 명령어 세트
를 포함하는 컴퓨터 판독 가능한 기록 매체.
- [청구항 16] 제 15항에 있어서,
상기 프로그램은,
상기 계정생성 응답 메시지로 부터 상기 종속계정에 대한 복수의 제2
개인키를 추출하는 명령어 세트; 및
상기 복수의 제2 개인키 중 하나를 상기 종속계정에 연관되는 단말의
개인키로서 전송하는 명령어 세트
를 포함하는 컴퓨터 판독 가능한 기록 매체.
- [청구항 17] 블록 체인을 공유하는 복수의 계정 중 제1 계정에 연관되는 단말로부터
상기 블록 체인을 이용한 결제 요청 메시지를 수신하는 통신부; 및
프로세서를 포함하고, 상기 프로세서에 의해 구현되는 :

소비자의 신용 (credit) 한도에 따라 생성되는 가상화폐를 포함하는 상기 블록 체인을 생성하고, 결제 내역에 따라 상기 블록 체인을 업데이트하는 블록 체인 생성부; 및

상기 결제 요청 메시지와 상기 제 1 계정에 대응하는 거래 조건을 확인하여 거래 승인 여부를 관리하는 거래 관리부를 포함하는 가상화폐 관리 장치.

[청 구 항 18]

제 17 항에 있어서,

상기 거래 관리부는 상기 결제 요청 메시지에 포함되는 가맹점 정보, 결제금액 및 전자서명 중 적어도 하나를 상기 거래 조건과 비교하여 거래 승인 여부를 결정하고,

상기 거래 조건은 상기 제 1 계정의 사용권 한, 상기 제 1 계정의 결제권 한 및 상기 제 1 계정의 백업키를 포함하는 가상화폐 관리 장치.

[청 구 항 19]

제 18 항에 있어서,

상기 결제 요청 메시지에 포함되는 거래 유형 정보가 할부 거래에 대응하는 경우, 상기 거래 관리부는 상기 거래 조건에 포함되는 결제 한도를 할부된 전체 금액만큼 차감하는 가상화폐 관리 장치.

[청 구 항 20]

제 19 항에 있어서,

상기 거래 관리부는, 소정 기간 이후에 상기 제 1 계정에 대응하는 할부 대금의 입금 여부를 확인하고, 상기 입금 결과에 따라 상기 거래 조건에 포함되는 결제 한도의 일부를 복원하는 가상화폐 관리 장치.

[청 구 항 21]

제 18 항에 있어서,

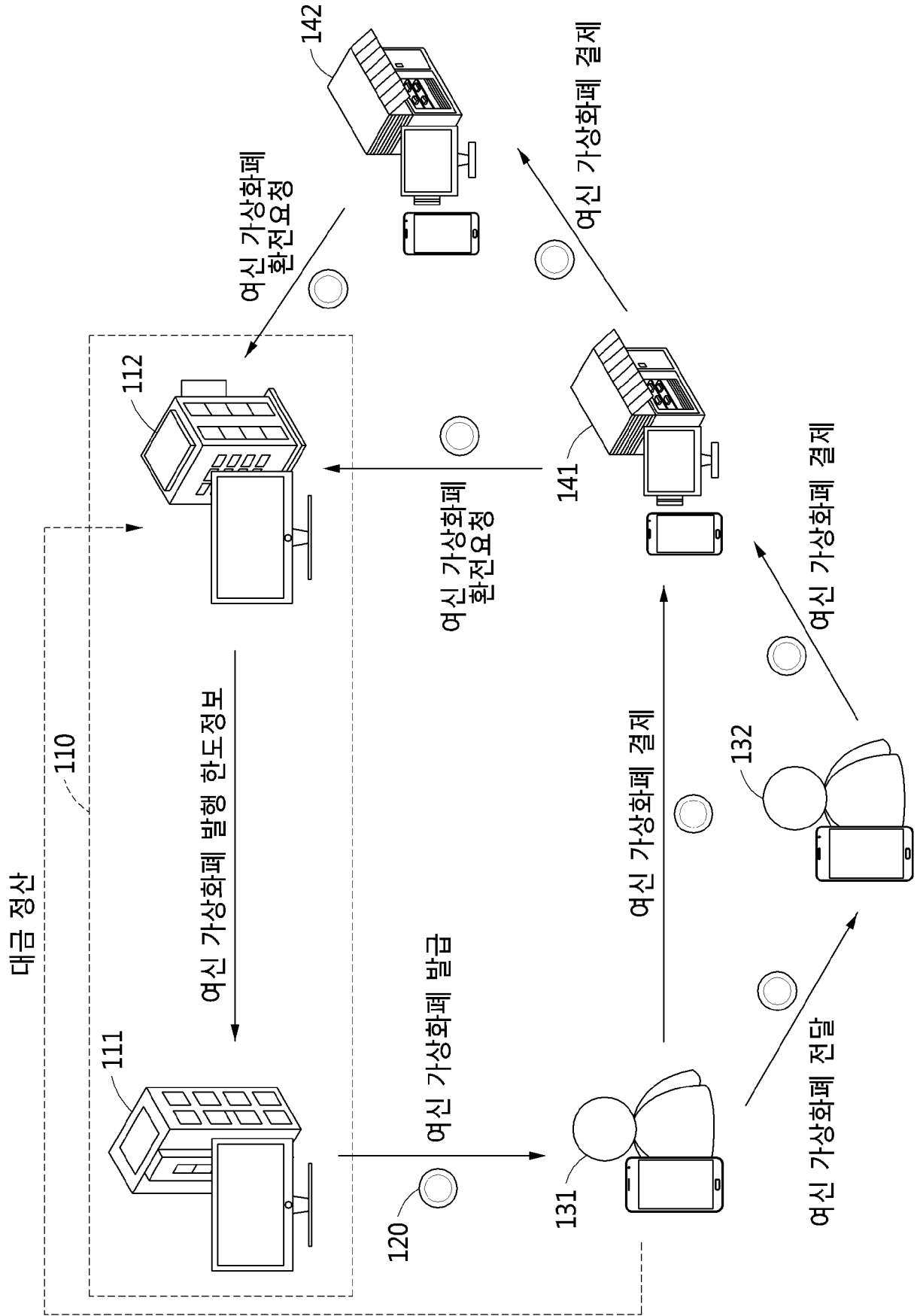
상기 결제 요청 메시지에 포함되는 거래 유형 정보가 할부 거래에 대응하는 경우, 상기 거래 관리부는 상기 거래 조건을 이용하여 상기 제 1 계정이 할부 가능 계정인지 여부를 확인하는 가상화폐 관리 장치.

[청 구 항 22]

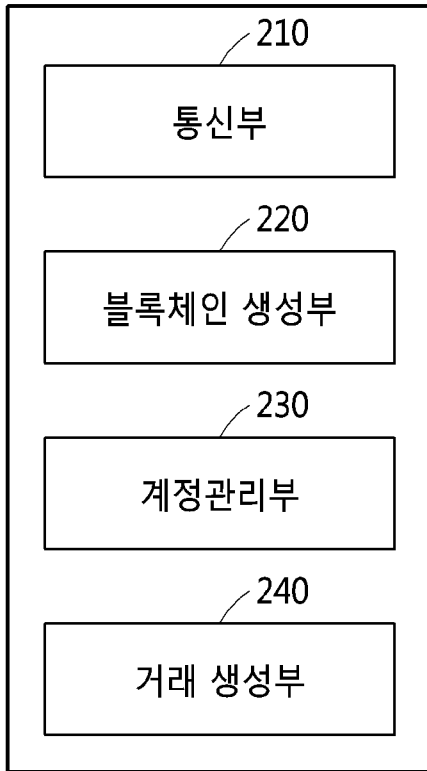
제 17 항에 있어서,

상기 거래 관리부는 상기 제 1 계정에 연관되는 식별값을 확인하고, 상기 식별값이 나타내는 정보에 따라 상기 결제 요청 메시지에 상응하는 송금 처리 또는 결제 처리를 진행하는 것을 특징으로 하는 가상화폐 관리 장치.

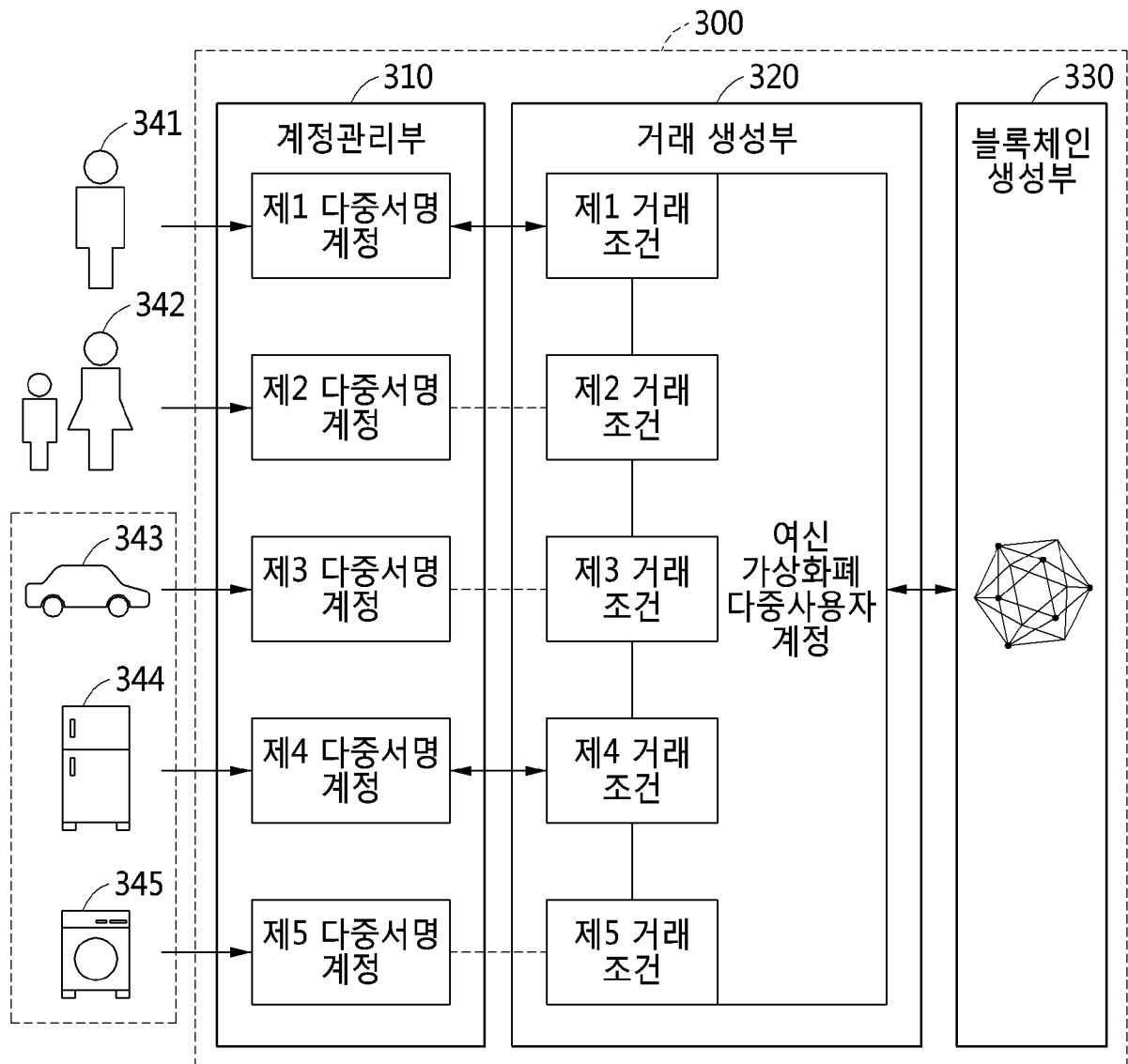
[도 1]



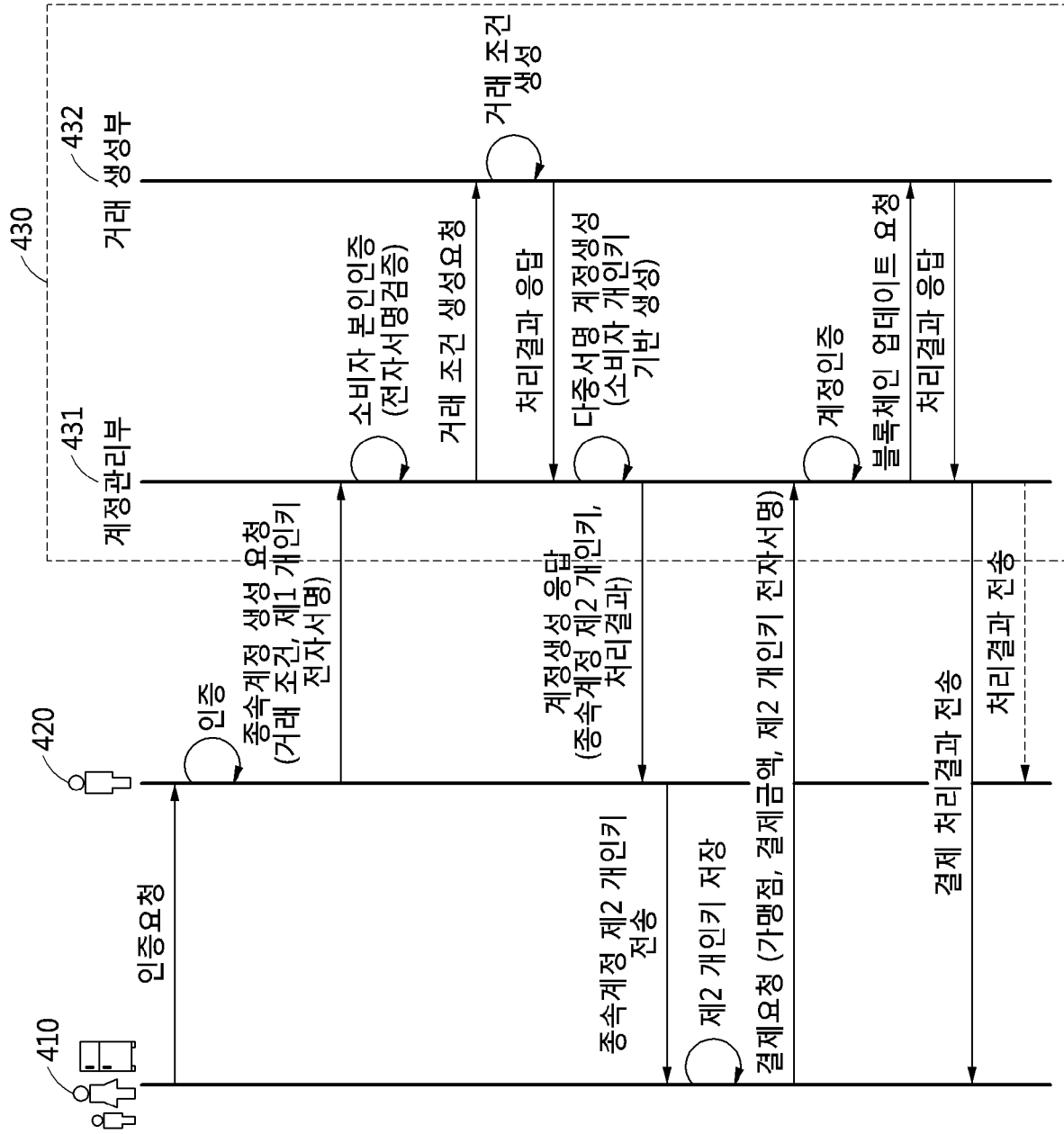
[도2]

200

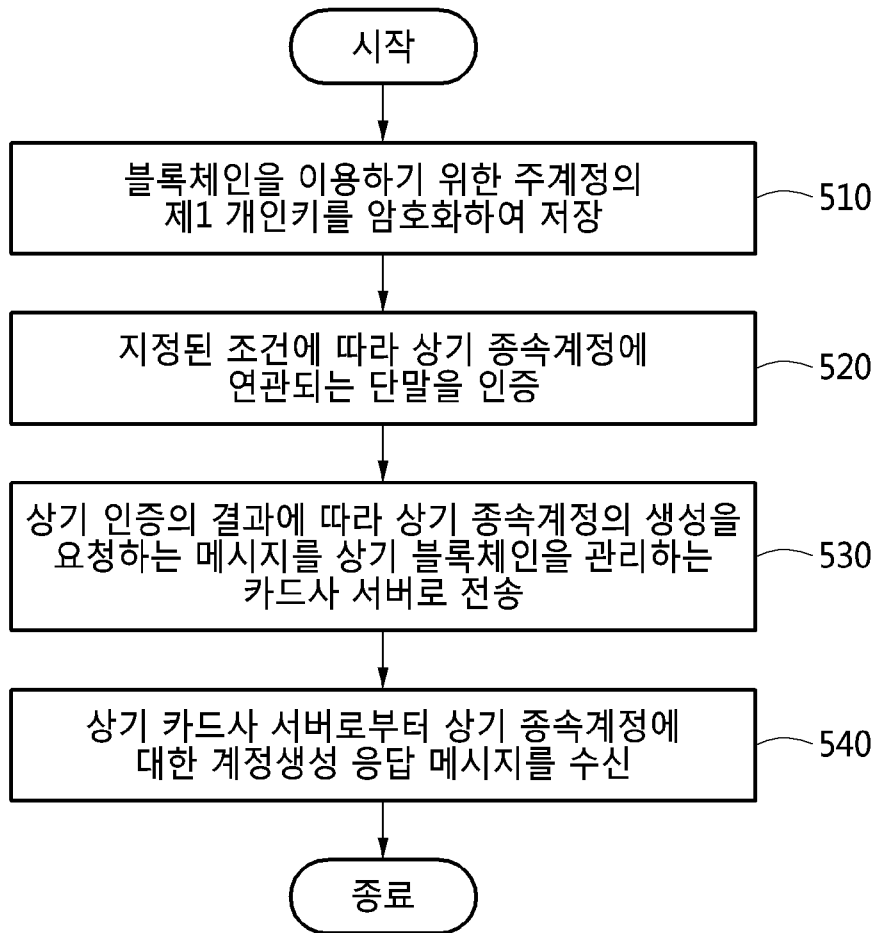
[도3]



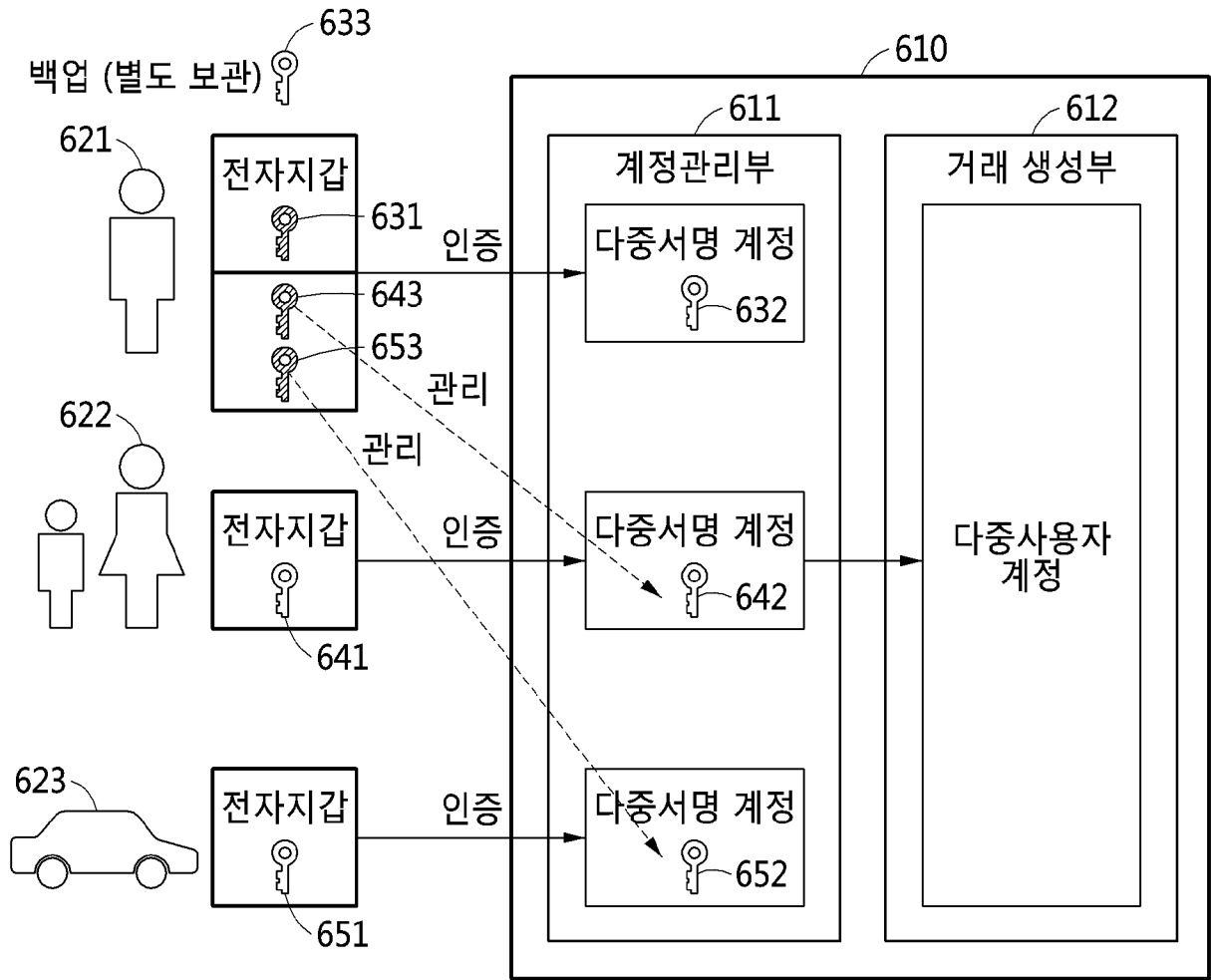
[도4]



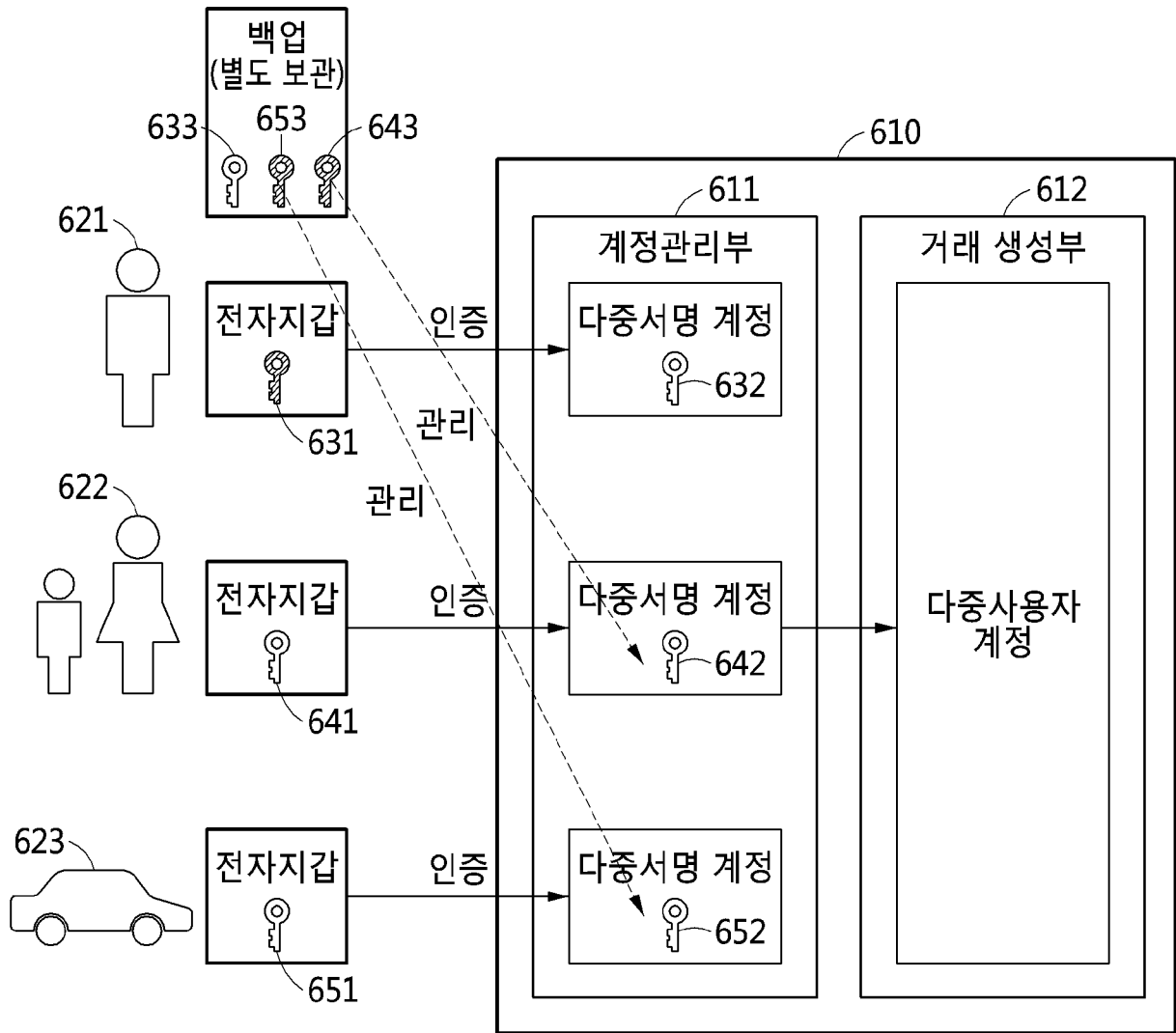
[도5]



[도6a]

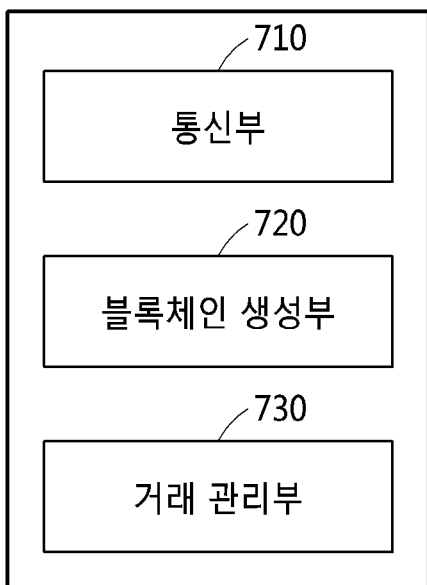


[도6b]



[도7]

700



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2017/015097

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/06(2012.01)i, G06Q 20/36(2012.01)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 20/06; G06Q 20/36; G06Q 20/34; G06Q 20/14; G06Q 20/38; H04L 9/32; G06Q 40/04

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: virtual currency, blockchain, multi-signature, account, transaction

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2017-0103385 A1 (DIGITAL ASSET HOLDINGS) 13 April 2017 See paragraphs [5]-[8], [35]-[98], [119]-[121].	1,17,18,22
Y		2-16,19-21
Y	US 2017-0330279 A1 (PONZONE, Hector Jose Maximiliano) 16 November 2017 See paragraphs [279]-[284]; claim 1; and figure 1.	2-16
Y	KR 10-2016-0086171 A (WISECARE) 19 July 2016 See paragraphs [2], [22]-[32]; claim 1; and figure 1.	19-21
A	KR 10-1799343 B1 (COINPLUG, INC.) 22 November 2017 See paragraphs [92]-[116]; claim 1; and figures 6-9.	1-22
A	KR 10-2017-0099155 A (COINPLUG, INC.) 31 August 2017 See paragraphs [38]-[68]; claim 1; and figures 1-3.	1-22



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

"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

28 AUGUST 2018 (28.08.2018)

Date of mailing of the international search report

28 AUGUST 2018 (28.08.2018)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex Daejeon Building 4, 189, Cheongsa-ro, Seo-gu,
Daejeon, 35208, Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2017/015097

Patent document cited in search report	Publication date	Patent family member	Publication date
US 2017-0103385 A1	13/04/2017	AU 2016-246428 A1	22/12/2016
		AU 2016-246428 B2	09/11/2017
		CA 02981586 A1	13/10/2016
		SG 11201707962 A	30/10/2017
		US 2016-0292680 A1	06/10/2016
		US 2017-0103390 A1	13/04/2017
		US 2017-0103391 A1	13/04/2017
		WO 2016-164310 A1	13/10/2016
		US 2017-0330279 A1	16/11/2017
AU 2015-346038 A1	19/05/2016		
EP 3218864 A1	20/09/2017		
IL 252263 A	31/07/2017		
WO 2016-077833 A1	19/05/2016		
KR 10-2016-0086171 A	19/07/2016	KR 10-1733682 B1	11/05/2017
KR 10-1799343 B1	22/11/2017	US 2017-0330180 A1	16/11/2017
KR 10-2017-0099155 A	31/08/2017	KR 10-1780634 B1	21/09/2017

소 발 명 이 속 하 는 기 술 분 류 (국 제 특 허 분 류 (11 번))
0)6(? 20/06(2012.01)1, 0)6(? 20/36(2012.01)1

B. 조사된 분야

조사된 최소 문헌 (국 제 특 허 분 류 를 기 재)
0060 20/06 ; 0060 20/36 ; G06E) 20/34 ; G06E) 20/14 ; G06E) 20/38 ; H04L 9/32 ; 0060 40/04

조사된 기술 분야에 속하는 최소 문헌 이외의 문헌
한국 등록 실용신 안공보 및 한국 공개 실용신 안공보 : 조사된 최소 문헌란에 기재된 IPC
일본 등록 실용신 안공보 및 일본 공개 실용신 안공보 : 조사된 최소 문헌란에 기재된 IPC

국제 조사에 이용된 전산 데이터베이스 (데이터베이스의 명칭 및 검색어 (해당하는 경우))
eKOMPASS (특허청 내부 검색 시스템) & 키워드 : 가상화폐 , 블록체인 , 다중서명 , 계정 , 거래

€. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	US 2017-0103385 A1 (DIGITAL ASSET HOLDINGS) 2017.04.13 단락 [5]-[8], [35]-[98], [119]-[121] 참조.	1, 17, 18, 22
Y		2-16, 19-21
Y	US 2017-0330279 A1 (HECTOR JOSE MAXIMILIANO PONZONE) 2017.11.16 단락 [279]-[284]; 청구항 1; 및 도면 1 참조.	2-16
Y	KR 10-2016-0086171 A (주식회사 와이즈케어) 2016.07.19 단락 [2], [22]-[32]; 청구항 1; 및 도면 1 참조.	19-21
A	KR 10-1799343 B1 (주식회사 코인플러그) 2017.11.22 단락 [92]-[116]; 청구항 1; 및 도면 6-9 참조.	1-22
A	KR 10-2017-0099155 A (주식회사 코인플러그) 2017.08.31 단락 [38]-[68]; 청구항 1; 및 도면 1-3 참조.	1-22

추가 문헌이 C(계속)에 기재되어 있습니다. | 3/4 대응 특허에 관한 별지를 참조하십시오.

*: 인용된 문헌의 특별 카테고리 :
 “G” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌
 “G” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌
 “I” 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
 “U” 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.
 “V” 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

국 제 조 사 의 실 제 완 료 일 : 2018년 08월 28일 (28.08.2018)
국 제 조 사 보 고 서 발 송 일 : 2018년 08월 28일 (28.08.2018)

IS쵸/101의 명칭 및 우편주소
대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-481-8578

심사관
강민정
전화번호 +82-42-481-813 1



국제조사 보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
狀 2017-0103385 쇼	2017/04/13	새 2016-246428 신	2016/12/22
		새 2016-246428 82	2017/11/09
		CA 02981586 신	2016/10/13
		80 11201707962 쇼	2017/10/30
		狀 2016-0292680 신	2016/10/06
		狀 2017-0103390 신	2017/04/13
		狀 2017-0103391 신	2017/04/13
		비 2016-164310 신	2016/10/13
狀 2017-0330279 쇼	2017/11/16	새 2015-346038 신	2017/07/06
		새 2015-346038 신	2016/05/19
		프 3218864 신	2017/09/20
		比 252263 쇼	2017/07/31
		비 2016-077833 신	2016/05/19
KR 10-2016-0086171 A	2016/07/19	KR 10-1733682 B1	2017/05/11
KR 10-1799343 B1	2017/11/22	US 2017-0330180 A1	2017/11/16
KR 10-2017-0099155 A	2017/08/31	KR 10-1780634 B1	2017/09/21