

명세서

발명의 명칭: 거래에서 사용자 정보를 식별하는 방법 및 이러한 방법을 수행하는 장치

기술분야

- [1] 본 발명은 거래에서 사용자 정보를 식별하는 방법 및 이러한 방법을 수행하는 장치에 관한 것이다. 보다 상세하게는 가상 자산의 이동에 있어서 가상 자산을 보내고 받는 사용자에게 대한 정보를 식별하기 위한 거래에서 사용자 정보를 식별하는 방법 및 이러한 방법을 수행하는 장치에 관한 것이다.

배경기술

- [2] FATF(Financial Action Task Force) AML(Anti Money Laundering) 관련 트레블룰(travel rule) 조항은 아래와 같이 거래자의 신원을 확인을 규정하고 있다. A거래소 및 B 거래소는 송신인 a 및 수신인 b에 대한 ID(identifier) 정보 및 트랜잭션에 대한 페어(pair) 정보를 데이터베이스화 해야 한다. 그래야 추후 테러 자금 및 자금세탁 관련 정황이 있을 경우 검찰 또는 경찰이 각 거래소에 해당 정보의 조회를 요청해서 자금을 추적하고 제재를 가할 수 있기 때문이다.
- [3] 권고 15안 7(b)항에 따르면 자금을 보내는 VASP(Virtual Asset Service Provider)는 보내는 사람의 정보와 함께 받는 사람의 정보를 보유하고 있어야 하며 규제 당국이 정보를 요청할 경우 이를 제출할 수 있어야 한다. 자금을 받는 VASP도 받는 사람의 정보와 함께 보내는 사람의 정보를 보유하고 있어야 하며, 규제 당국이 정보를 요청할 경우 이를 제출할 수 있어야 한다.
- [4] 따라서, 이러한 규정을 만족시키기 위한 기술에 대한 연구가 필요하다.

발명의 상세한 설명

기술적 과제

- [5] 본 발명은 상술한 문제점을 모두 해결하는 것을 그 목적으로 한다.
- [6] 또한, 본 발명은, 가상 자산 거래에서 송금 사용자와 수금 사용자에게 대한 정보를 식별하는 방법을 제공하는 것을 목적으로 한다.
- [7] 또한, 본 발명은, 가상 자산 거래에서 송금 사용자와 수금 사용자에게 대한 정보를 식별하되, 보다 간단한 절차로 가상 자산 거래를 단순화시키기 위한 방법을 제공하는 것을 목적으로 한다.

기술적 해결방법

- [8] 상기 목적을 달성하기 위한 본 발명의 대표적인 구성은 다음과 같다.
- [9] 본 발명의 일 실시예에 따르면, 거래에서 사용자 정보를 식별하는 방법은, O-VASP(originator virtual asset service provider)가 송금 정보를 기반으로 제1 사용자 확인 트랜잭션을 B-VASP으로 전송하는 단계, 상기 O-VASP가 상기 B-VASP(beneficiary virtual asset service provider)로부터 제2 사용자 확인 트랜잭션을 수신하는 단계와 상기 O-VASP가 상기 송금 정보를 기반으로 생성된

- 가상 거래 자산을 수급자 사용자 지갑으로 전송하는 단계를 포함할 수 있다.
- [10] 한편, 상기 제1 사용자 확인 트랜잭션은 송금 사용자 장치에 의해 입력된 수급 사용자 식별 정보를 포함하고, 상기 B-VASP는 상기 제1 사용자 확인 트랜잭션 상의 수급 사용자 식별 정보와 상기 B-VASP 상에 저장된 수급 사용자 식별 정보의 동일성 여부를 판단할 수 있다.
- [11] 또한, 상기 제2 사용자 확인 트랜잭션은 수급 사용자 장치에 의해 입력된 송금 사용자 식별 정보를 포함하고, 상기 O-VASP는 상기 제2 사용자 확인 트랜잭션 상의 송금 사용자 식별 정보와 상기 O-VASP 상에 저장된 송금 사용자 식별 정보의 동일성 여부를 판단할 수 있다.
- [12] 본 발명의 다른 실시예에 따르면, 거래에서 사용자 정보를 식별하는 O-VASP(originator virtual asset service provider)는 상기 B-VASP(beneficiary virtual asset service provider)와 통신하기 위한 통신부, 상기 통신부와 동작 가능하게(operatively) 연결된 프로세서를 포함하되, 상기 프로세서는 송금 정보를 기반으로 제1 사용자 확인 트랜잭션을 B-VASP으로 전송하고, 상기 B-VASP로부터 제2 사용자 확인 트랜잭션을 수신하고, 상기 송금 정보를 기반으로 생성된 가상 거래 자산을 수급자 사용자 지갑으로 전송하록 구현될 수 있다.
- [13] 한편, 상기 제1 사용자 확인 트랜잭션은 송금 사용자 장치에 의해 입력된 수급 사용자 식별 정보를 포함하고, 상기 B-VASP는 상기 제1 사용자 확인 트랜잭션 상의 수급 사용자 식별 정보와 상기 B-VASP 상에 저장된 수급 사용자 식별 정보의 동일성 여부를 판단할 수 있다.
- [14] 또한, 상기 제2 사용자 확인 트랜잭션은 수급 사용자 장치에 의해 입력된 송금 사용자 식별 정보를 포함하고, 상기 O-VASP는 상기 제2 사용자 확인 트랜잭션 상의 송금 사용자 식별 정보와 상기 O-VASP 상에 저장된 송금 사용자 식별 정보의 동일성 여부를 판단할 수 있다.

발명의 효과

- [15] 본 발명에 의하면, 가상 자산 거래에서 송금 사용자와 수급 사용자에 대한 정보가 식별될 수 있다.
- [16] 또한, 본 발명에 의하면, 가상 자산 거래에서 송금 사용자와 수급 사용자에 대한 정보를 식별하되, 보다 간단한 절차로 가상 자산 거래가 단순화될 수 있다.

도면의 간단한 설명

- [17] 도 1은 기존의 가상 자산의 이동 방법을 나타낸 개념도이다.
- [18] 도 2는 본 발명의 실시예에 따른 가상 자산 거래 시스템을 나타낸 개념도이다.
- [19] 도 3은 본 발명의 실시예에 따른 해시화 방법이 개시된다.
- [20] 도 4는 본 발명의 실시예에 따른 해시값 비교를 수행하는 방법을 나타낸 개념도이다.
- [21] 도 5는 본 발명의 실시예에 따른 해시화 방법을 나타낸 개념도이다.

- [22] 도 6은 본 발명의 실시예에 따른 입력 정보 입력 방법을 나타낸 개념도이다.
- [23] 도 7은 본 발명의 실시예에 따른 가상 자산 전송의 단순화를 위한 방법을 나타낸 개념도이다.
- [24] 도 8은 본 발명의 실시예에 따른 가상 자산 전송의 단순화를 위한 방법을 나타낸 개념도이다.
- [25] 도 9는 본 발명의 실시예에 따른 가상 자산 전송의 단순화를 위한 방법을 나타낸 개념도이다.
- [26] 도 10은 본 발명의 실시예에 따른 송금 사용자 및 수금 사용자에게 대한 정보를 저장하는 방법이 개시된다.
- [27] 도 11은 본 발명의 실시예에 따른 가상 자산 전송 방법을 나타낸 개념도이다.
- [28] 도 12는 본 발명의 실시예에 따른 가상 자산 전송 방법을 나타낸 개념도이다.
- [29] 도 13은 본 발명의 실시예에 따른 가상 자산의 전송 방법을 나타낸 개념도이다.

발명의 실시를 위한 형태

- [30] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이러한 실시예는 당업자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의 다양한 실시예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 본 명세서에 기재되어 있는 특정 형상, 구조 및 특성은 본 발명의 정신과 범위를 벗어나지 않으면서 일 실시예로부터 다른 실시예로 변경되어 구현될 수 있다. 또한, 각각의 실시예 내의 개별 구성요소의 위치 또는 배치도 본 발명의 정신과 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 행하여 지는 것이 아니며, 본 발명의 범위는 특허청구범위의 청구항들이 청구하는 범위 및 그와 균등한 모든 범위를 포괄하는 것으로 받아들여져야 한다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 구성요소를 나타낸다.
- [31] 이하에서는, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있도록 하기 위하여, 본 발명의 여러 바람직한 실시예에 관하여 첨부된 도면을 참조하여 상세히 설명하기로 한다.
- [32]
- [33] 도 1은 기존의 가상 자산의 이동 방법을 나타낸 개념도이다.
- [34] 도 1에서는 종래의 가상 자산의 송금 VASP에서 수금 VASP로의 전달 방법이 개시된다.
- [35] 이하, 본 발명의 실시예에서 송금 VASP는 O(originator)-VASP, 수금 VASP는 B(beneficiary)-VASP라는 용어로 표현될 수 있다. O-VASP는 송금 절차를 위한 거래소, B-VASP는 수금 절차를 위한 거래소일 수 있다.
- [36] 도 1을 참조하면, 송금 사용자(100)는 O-VASP(120) 상에서 O-VASP의 통합 지갑(140)을 통해 B-VASP의 수금 사용자의 개인 지갑(160)으로 가상 자산을

전달하게 된다. 이때 통합 지갑(140)은 송금 사용자(100)의 개인 지갑이 아닌 O-VASP(120)에서 통합적으로 사용되는 출금 지갑으로서 개인의 특징이 불가능한 지갑이다.

- [37] 기존의 O-VASP(120)는 송금 사용자(100)부터 수금 사용자의 개인 지갑 정보 및 송금되는 가상 자산에 대한 정보를 가지고 O-VASP의 통합 지갑(140)을 통해 가상 자산을 수금 사용자에게 송금하였다. 즉, 기존의 O-VASP(120)는 해킹의 위험성 및 관리의 효율성을 위해 별도의 통합 계좌를 통해 블록체인 거래를 수행했다.
- [38] 하지만, 이러한 가상 자산 전송 방법은 FATF(Financial Action Task Force)의 트래블 룰(travel rule)을 따르지 못하는 것이다. 트래블 룰 상에서는 O-VASP와 B-VASP 각각에서 송금 사용자와 수금 사용자를 식별할 수 있는 송금 사용자 식별 정보(예를 들어, 송금 사용자 이름) 및 수금 사용자 식별 정보(예를 들어, 수금 사용자 이름)가 획득되어야 한다.
- [39] 트래블 룰을 따라야 하되, 현재 법규 하에서는 아래와 같은 제약 사항이 존재한다. 현재 거래소 사이에 회원 정보가 공유될 수 없다. 외부의 사업자가 고객 데이터베이스 접근 권한을 가질 경우, 개인정보보호법에 저촉된다. 따라서, 송금 사용자의 거래소(O-VASP)와 수금 사용자의 거래소(B-VASP) 사이에서 트랜잭션과 관련된 송금 사용자 식별 또는 수금 사용자 식별 정보를 취득하여 트래블 룰을 만족시키기 위한 연구가 필요하다.
- [40] 이하, 본 발명의 실시예에서는 설명의 편의상 송금 또는 수금이라는 용어를 사용하나, 송금은 송신(또는 전송), 수금은 수신(또는 입금)이라는 용어로 표현될 수 있다.
- [41] 또한, 이하, 본 발명의 실시예에서는 설명의 편의상 송금 사용자, 수금 사용자라는 용어를 사용하나 송금 사용자는 송금 사용자 장치, 수금 사용자는 수금 사용자 장치를 포함하는 의미로 사용될 수 있다.
- [42]
- [43] 도 2는 본 발명의 실시예에 따른 가상 자산 거래 시스템을 나타낸 개념도이다.
- [44] 도 2에서는 AML(Anti Money Laundering)을 위한 트래블 룰은 준수하기 위해 VASP 간의 상대 사용자 정보를 확인하기 위한 시스템이 개시된다.
- [45] 도 2를 참조하면, 가상 자산 거래 시스템은 송금 사용자 장치(200), 수금 사용자 장치(205), O-VASP(210), B-VASP(220), 가상 자산 교환 네트워크(230), KYC(know your customer) 엔진(240, 270), 트랜잭션 레코드(250, 280), AML 엔진(260, 290)을 포함할 수 있다.
- [46] 송금 사용자 장치(200)는 가상 자산을 송금하는 송금 사용자의 장치일 수 있다. 송금 사용자는 오리지네이터(originator)라는 용어로 표현될 수 있다.
- [47] 수금 사용자 장치(205)는 가상 자산을 수금하려는 수금 사용자의 장치일 수 있다. 수금 사용자는 베니피셔리(beneficiary)라는 용어로 표현될 수 있다.
- [48] O-VASP(210)는 송금 사용자와 관련된 가상 자산 송금 서버(또는 가상 자산

- 송금 노드, 가상 자산 송금 거래소)일 수 있다. 송금 사용자는 O-VASP(210)를 통해 가상 자산을 송금할 수 있다.
- [49] B-VASP(220)는 수금 사용자와 관련된 가상 자산 수금 서버(또는 가상 자산 수금 노드, 가상 자산 수금 거래소)일 수 있다. 수금 사용자는 B-VASP(220)를 통해 가상 자산을 수금할 수 있다.
- [50] 가상 자산 교환 네트워크(또는 암호 화폐 교환 네트워크)(Cryptocurrency(virtual asset) Exchange Network)(230)는 가상 자산과 관련된 트랜잭션(transaction)을 원장에 기록하고 블록을 생성하는 노드로 구성된 네트워크일 수 있다.
- [51] 가상 자산 교환 네트워크(230)는 후술할 제1 사용자 확인 트랜잭션(201), 제2 사용자 확인 트랜잭션(202) 및 가상 자산 전송 트랜잭션(203)을 송신 또는 수신하기 위한 트랜잭션일 수 있다.
- [52] KYC 엔진(engine)(240, 270)은 KYC(know your customer)와 같은 절차를 통해 O-VASP(210) 및 B-VASP(220) 각각에서 사용자의 정보를 획득하고 관리하기 위해 구현될 수 있다. O-VASP(210)의 KYC 엔진(engine) (240)은 O-VASP(210)와 관련된 송금 사용자 및/또는 수금 사용자에 대한 정보를 획득하여 관리하고, B-VASP(220)의 KYC 엔진(engine)(270)은 B-VASP(220)와 관련된 송금 사용자 및/또는 수금 사용자에 대한 정보를 획득하여 관리할 수 있다.
- [53] 트랜잭션 레코드(transaction record)(250, 280)는 O-VASP(210) 및 B-VASP(220) 각각에서 발생하는 트랜잭션 정보를 획득하고 관리하기 위해 구현될 수 있다. O-VASP(210)의 트랜잭션 레코드는 O-VASP(210)에서 발생하는 트랜잭션 정보를 획득하여 관리하고, B-VASP(220)의 트랜잭션 레코드는 B-VASP(220)에서 발생하는 트랜잭션 정보를 획득하여 관리할 수 있다.
- [54] AML 엔진(260, 290)은 본 발명의 실시예에 따른 거래에서 사용자 정보를 식별하기 위해 구현될 수 있다. AML 엔진(260, 290)은 송금 정보 및 수금 정보에 대한 해시화를 수행하기 위해 구현될 수 있다. 해시 정보는 송금 사용자와 수금 사용자 간의 상호 확인을 위해 활용될 수 있다. AML 엔진(260, 290)은 KYC 엔진(240, 270)과 연결된 송금 사용자, 수금 사용자의 정보를 획득하여 해시 정보를 생성할 수 있고, 해시 정보를 교환하여 송금 사용자 수금 사용자 간의 확인 절차가 수행될 수 있다.
- [55] 해시화 방법 및 해시 정보를 기반으로 송금 사용자와 수금 사용자 간의 상호 확인을 수행하는 구체적인 방법은 후술된다.
- [56] 우선 송금 사용자가 수금 사용자에게 가상 자산을 전송하기 위한 거래를 요청할 수 있다.
- [57] 송금 사용자는 송금 사용자 장치(200)를 통해 수금 사용자 지갑 주소(To_{wallet}), 거래량(또는 송금량)(Value), 송금 사용자 식별 정보(예를 들어, 이름)(To_{info}) 등을 입력할 수 있다. O-VASP(210)는 통합 지갑 주소($From_{wallet}$), 수금 사용자 장치 지갑 주소(To_{wallet}), 거래량(또는 송금량)(Value), 수금 사용자 식별 정보(예를 들어, 이름)(To_{info})를 송금 정보로서 생성하고, 송금 정보를 기반으로 가상 자산

전송을 위한 가상 자산 전송 트랜잭션(203)을 생성할 수 있다.

- [58] 가상 자산 전송 트랜잭션(203)은 수금 사용자, 송금 사용자에게 대한 확인 절차를 위한 제1 사용자 확인 트랜잭션(201) 및 제2 사용자 확인 트랜잭션(202)의 전송을 위해 일시적으로 펜딩될 수 있다(Pending Trust). 펜딩된 가상 전송 트랜잭션(203)은 해시값 기반 사용자 확인 절차(제1 사용자 확인 트랜잭션(201) 및 제2 사용자 확인 트랜잭션(202))의 완료 이후 전송될 수 있다.
- [59] 이후, O-VASP(210)와 B-VASP(220) 사이에서 해시값 기반 사용자 확인 절차(제1 사용자 확인 트랜잭션(201) 및 제2 사용자 확인 트랜잭션(202))가 수행될 수 있다. 해시값 기반 사용자 확인 절차는 전술한 트래블 룰을 만족시키기 위한 송금 사용자 및 수금 사용자에게 대한 확인 절차일 수 있다.
- [60] 제1 사용자 확인 트랜잭션(201)은 송금 사용자에게 의해 입력된 수금 사용자 식별 정보가 정확한지 여부에 대해 확인 절차이고, 제2 사용자 확인 트랜잭션(202)은 수금 사용자에게 의해 입력된 송금 사용자 식별 정보가 정확한지 여부에 대해 확인 절차일 수 있다. 제1 사용자 확인 트랜잭션(201) 및 제2 사용자 확인 트랜잭션(202)을 통해 O-VASP(210)는 수금 사용자 정보를 획득할 수 있고, B-VASP(220)는 송금 사용자 정보를 획득할 수 있어서 트래블 룰을 만족시킬 수 있다.
- [61] 이하, 구체적인 제1 사용자 확인 트랜잭션(201) 및 제2 사용자 확인 트랜잭션(202)의 전송 방법이 개시된다.
- [62] O-VASP(210)는 해시값을 생성하여 제1 사용자 확인 트랜잭션(201)(Tx₁ (value=0, hash(To_{info})))을 B-VASP(220)로 송신할 수 있다 제1 사용자 확인 트랜잭션(201)은 송금 정보를 해시화한 정보를 포함하고 수금 사용자에게 대한 확인을 위해 사용될 수 있다. 제1 사용자 확인 트랜잭션(201)에서 전송되는 가상 자산은 없으므로 value=0이고, 송금 사용자에게 의해 입력된 수금 사용자 식별 정보(To_{info})는 해시화되어 hash(To_{info})일 수 있다.
- [63] 해시화시 무작위 공격의 난이도를 높이기 위해 두 거래소(O-VASP, B-VASP)가 동일하게 생성할 수 있는 난수값을 추가하여 해시값을 생성할 수 있다.
- [64] O-VASP(210)는 O-VASP(210)를 이용하는 송금 사용자 식별 정보는 이미 KYC 엔진(240, 270)을 통해 획득하고 있고, 수금 사용자 식별 정보도 송금 사용자에게 의해 입력된 수금 사용자 식별 정보를 통해 획득할 수 있다.
- [65] 제1 사용자 확인 트랜잭션(201)은 가상 자산 교환 네트워크를 통해 B-VASP(220)로 전달될 수 있다.
- [66] B-VASP(220)는 제1 사용자 확인 트랜잭션(201)을 수신하고, 제1 사용자 확인 트랜잭션(201)에 포함되는 수금 사용자 식별 정보의 해시값(hash(To_{info}))과 B-VASP(220)에 저장된 수금 사용자 식별 정보의 해시값을 비교하여 송금 사용자에게 의해 입력된 수금 사용자 식별 정보가 정확한지 여부를 확인할 수 있다.
- [67] 구체적으로 B-VASP(220)의 AML 엔진(260, 290)은 제1 사용자 확인

트랜잭션(201)에 포함되는 수금 사용자의 개인 지갑 주소(To_{wallet})에 대한 정보를 기반으로 KYC 엔진(240, 270)을 통해 수금 사용자 식별 정보($KYC(To_{wallet})$)를 획득할 수 있다. 이후, 수금 사용자 식별 정보($KYC(To_{wallet})$)는 해시화되어 $hash(KYC(To_{wallet}))$ 되고, 제1 사용자 확인 트랜잭션(201)에 포함되는 해시값($hash(To_{info})$)과 동일한지 여부가 판단될 수 있다. 해시값 비교를 통해 정보의 동일성을 판단하기 위해 두 거래소(O-VASP, B-VASP)에서 동일한 해시 함수가 사용될 수 있고, 추가적으로 두 거래소(O-VASP, B-VASP)가 동일하게 생성할 수 있는 난수값을 추가하여 보안성을 강화시킬 수 있다.

- [68] 개인 정보($KYC(To_{wallet})$)를 해시화한 $hash(KYC(To_{wallet}))$ 은 제1 해시값(B-VASP)이라는 용어로 표현되고 제1 사용자 확인 트랜잭션에 포함되는 해시값($hash(To_{info})$)은 제1 해시값(O-VASP)이라는 용어로 표현될 수 있다.
- [69] 제1 해시값(B-VASP)과 제1 해시값(O-VASP)이 동일하다는 의미는 송신 사용자에게 의해 특정된 수신 사용자 식별 정보가 정확하다는 것을 의미할 수 있다.
- [70] 제1 해시값(O-VASP)과 제1 해시값(B-VASP)이 동일하지 않은 경우, 수금 사용자의 확인 실패를 지시하는 제2 사용자 확인 트랜잭션(실패)(202)가 O-VASP(210)로 전송될 수 있다. 제2 사용자 확인 트랜잭션(실패)(202)는 제1 사용자 확인 트랜잭션(201)에 의해 지시된 수금 사용자 식별 정보($KYC(To_{wallet})$)를 더 포함하여 전송할 수도 있다.
- [71] 반대로, 제1 해시값(O-VASP)과 제1 해시값(B-VASP)이 동일한 경우, 수금 사용자에게 송금 사용자 식별 정보를 요청하고, 송금 사용자 식별 정보를 해시화한 정보를 포함하는 제2 사용자 확인 트랜잭션(성공)(202)가 O-VASP(210)로 전송될 수 있다. 기존에 송금 사용자와 수금 사용자 간의 거래가 있었을 경우 수금 사용자에게 별도의 송금 사용자 식별 정보를 요청하지 않을 수도 있다. 초기 거래이거나 비정상 거래로 판단되는 경우, 수금 사용자에게 별도의 송금 사용자 식별 정보를 요청하여 수금 사용자가 송금 사용자를 식별 가능한지 여부가 확인될 수 있다. 이러한 단순화된 가상 자산 전송 방법은 후술된다.
- [72] 제2 사용자 확인 트랜잭션(성공)(202)은 O-VASP(210) 상에서 송금 사용자의 확인을 위해 활용될 수 있다. 제2 사용자 확인 트랜잭션(성공)(202)에 포함된 해시화된 송금 사용자 식별 정보와 O-VASP(210)의 KYC 엔진(240) 상에 저장된 송금 사용자 식별 정보를 해시화한 결과가 비교될 수 있다.
- [73] 제2 사용자 확인 트랜잭션(성공)(202)에 포함된 해시화된 송금 사용자 식별 정보는 제2 해시값(B-VASP)이고 O-VASP(210)의 KYC 엔진(240)을 통해 획득된 송금 사용자 식별 정보를 해시화한 결과는 제2 해시값(O-VASP)일 수 있다. 제2 해시값(B-VASP)과 제2 해시값(O-VASP)이 동일하다는 의미는 수신 사용자에게 의해 특정된 송신 사용자 식별 정보가 정확하다는 것을 의미할 수 있다.
- [74] O-VASP(210)에서 제2 해시값(B-VASP)과 제2 해시값(O-VASP)의 비교 결과

동일한 해시값인 경우, 펜딩된 가상 자산 전송 트랜잭션(203)이 전송되어 가상 자산이 송신 사용자로부터 수신 사용자에게 전달될 수 있다. 가상 자산의 전송 전 송신 사용자의 잔고에 대해 확인하여 정상 거래 가능 여부에 대한 확인이 수행될 수 있다. 완료된 가상 자산 전송 트랜잭션(203)에 대한 정보는 O-VASP(210), B-VASP(220)에 저장될 수 있다. O-VASP(210)는 송신 사용자로부터 수신한 수신 사용자 식별 정보(예를 들어, 지갑 주소, 이름, 거래소)를 저장하고 B-VASP(220)는 수신 사용자로부터 입력받은 송신 사용자 식별 정보(예를 들어, 지갑 주소, 이름, 거래소)를 저장할 수 있다.

- [75] 즉, 거래 전에 O-VASP(210)는 송신 사용자에 대한 정보만을 보관하였고, B-VASP(220)는 수신 사용자에 대한 정보만을 보관하였다. 거래 후에는 O-VASP(210)는 송신 사용자로부터 수신 사용자 식별 정보를 입력받아 별도로 저장할 수 있고, B-VASP(220)는 수신 사용자로부터 송신 사용자 식별 정보를 입력받아 별도로 저장할 수 있다.
- [76]
- [77] 도 3은 본 발명의 실시예에 따른 해시화 방법이 개시된다.
- [78] 도 3에서는 전술한 제1 해시값(O-VASP), 제1 해시값(B-VASP), 제2 해시값(O-VASP), 제2 해시값(B-VASP)를 생성하기 위한 방법이 개시된다.
- [79] 도 3을 참조하면, 해시화(또는 해시 암호화) 알고리즘은 단방향 암호화 방법이다. 따라서, 해시값만 가지고 다시 원 데이터로 복구하는 것은 원칙적으로 불가능하다. 데이터의 아주 작은 변화로 해시값이 변화하기 때문에 해시값은 정보의 일치 여부를 확인하기 위해 사용될 수 있다. 예를 들어 사용자의 비밀번호가 서버에 저장시 서버 데이터가 유출되면 사용자의 비밀번호 페어가 유출되기 때문에 보안에 큰 문제가 발생한다. 이러한 보안 문제를 해결하기 위해 해시화된 비밀번호(해시)가 서버에 저장되고, 사용자가 로그인을 위해 비밀번호(입력)를 입력하면 동일한 해시 함수로 해시화하여 비밀번호(입력)의 해시값과 비밀번호(해시)를 비교하여 암호의 일치 여부가 확인된다.
- [80] 해시알고리즘으로 MD5, SHA-1, SHA-256, SHA-512와 같은 알고리즘이 사용될 수 있다. 하지만 해시 함수의 종류가 알려지고, 입력해야 하는 값의 필드를 알게 되면 무차별 공격으로 입력값을 알아낼 가능성이 존재하기 있기 때문에 보완이 필요하다.
- [81] 따라서 본 발명의 실시예에서는 평문에 임의의 문자열인 솔트(salt)를 추가하여 해시값을 생성하는 방법이 사용된다. 솔트값(salt value)을 이용해서 미리 만들어둔 원문과 해시의 조합을 비교하는 레인 보우 어택(rainbow attack)에 대한 방어가 가능하다.
- [82] 구체적으로 본 발명에서는 서로 다른 VASP(O-VASP, B-VASP)가 동일하게 생성할 수 있는 salt(random value)를 해싱하여 더 높은 보안이 유지될 수 있다. 두 VASP는 해시에 사용되는 솔트(salt), 반복 횟수 등에 대한 사전 합의가 수행될 수 있다. 솔트 값은 고객의 정보와 생성 시간에 기반한 OTP(one time password)와

같은 알고리즘으로 생성될 수 있다.

- [83] 제1 해시값(O-VASP)(310)과 제2 해시값(B-VASP)(320)은 동일한 해시 함수 및 솔트값을 기반으로 생성되고, 마찬가지로 제2 해시값(O-VASP)(350), 제2 해시값(B-VASP)(360)은 동일한 해시 함수 및 솔트값을 기반으로 생성될 수 있다.
- [84]
- [85] 도 4는 본 발명의 실시예에 따른 해시값 비교를 수행하는 방법을 나타낸 개념도이다.
- [86] 도 4에서는 제1 해시값(O-VASP), 제1 해시값(B-VASP)의 비교 및 제2 해시값(O-VASP), 제2 해시값(B-VASP)의 비교를 통해 정보의 동일성을 비교하기 위한 방법이 개시된다.
- [87] 도 4의 상단을 참조하면, 제1 해시값(O-VASP)(410), 제1 해시값(B-VASP)(450)의 비교를 수행하는 방법이 개시된다.
- [88] 전술한 바와 같이 O-VASP 상에서 송금 정보로서 O-VASP의 통합 지갑 주소(From_{wallet}), 수금 사용자 지갑 주소(To_{wallet}), 거래량(또는 송금량)(Value), 수금 사용자 식별 정보(예를 들어, 이름)(To_{info})(400)가 생성될 수 있다.
- [89] 제1 해시값(O-VASP)(410)는 수금 사용자 식별 정보(예를 들어, 이름)(To_{info})(400)에 대한 해시값일 수 있다. 제1 해시값(O-VASP)(410)는 제1 사용자 확인 트랜잭션(420)에 포함되어 B-VASP로 전송될 수 있다.
- [90] B-VASP로 전송되는 제1 사용자 확인 트랜잭션(420)은 O-VASP의 통합 지갑 주소(From_{wallet}), 수금 사용자 지갑 주소(To_{wallet})(430) 또는 거래량(또는 송금량)(Value)에 대한 정보를 더 포함할 수 있다.
- [91] B-VASP는 제1 사용자 확인 트랜잭션(420)에 포함되는 수금 사용자 지갑 주소(To_{wallet})(430)를 기반으로 수금 사용자 장치에 대응되는 수금 사용자 식별 정보(440)를 KYC 엔진을 통해 획득할 수 있다.
- [92] 즉, 송금 사용자 장치에 의해 입력되어 해시화된 수금 사용자 식별 정보를 해시화한 값이 제1 해시값(O-VASP)(410)이고, B-VASP의 KYC엔진을 통해 획득된 수금 사용자 식별 정보(440)를 해시화한 값이 제1 해시값(B-VASP)(450)일 수 있다. 이해의 편의상 다른 용어로, 제1 해시값(O-VASP)(410)는 제1 수금 사용자 식별 정보(해시), 제1 해시값(B-VASP)는 제2 수금 사용자 식별 정보(해시)라는 용어로도 표현될 수 있다.
- [93] 제1 수금 사용자 식별 정보(해시)(제1 해시값(O-VASP)(410))와 제2 수금 사용자 식별 정보(해시)(제1 해시값(B-VASP)(450))는 동일한 해시 함수 및 난수값(솔트값)을 기반으로 해시화된 값일 수 있다. 제1 수금 사용자 식별 정보(해시)와 제2 수금 사용자 식별 정보(해시)의 비교를 통해 송금 사용자가 입력한 수금 사용자 식별 정보와 B-VASP 상의 수금 사용자 식별 정보가 동일한지 여부가 판단될 수 있다.
- [94] 도 4의 하단을 참조하면, 제2 해시값(O-VASP)(495), 제2

해시값(B-VASP)(470)의 비교를 수행하는 방법이 개시된다.

- [95] 전술한 바와 같이 제1 해시값(O-VASP)(410)과 제1 해시값(B-VASP)(450)이 동일한 경우, 수급 사용자에게 송금 사용자 식별 정보를 요청하고, 송금 사용자 식별 정보(460)를 해시화하여 포함한 제2 사용자 확인 트랜잭션(성공)(480)을 O-VASP로 전송할 수 있다.
- [96] 제2 사용자 확인 트랜잭션(성공)(480)은 해시화된 송금 사용자 식별 정보(480), 송금 사용자를 특정하기 위한 정보가 포함될 수 있다. 해시화된 송금 사용자 식별 정보가 제2 해시값(B-VASP)(470)이다. 송금 사용자를 특정하기 위한 정보는 후술할 송금 사용자 장치의 개인 지갑 주소(490) 및/또는 제1 사용자 확인 트랜잭션의 트랜잭션 ID에 대한 정보를 포함할 수 있다. 도 4에서는 설명의 편의상 송금 사용자 지갑 주소(490)로 송금 사용자를 특정하는 것으로 가정한다.
- [97] 예를 들어, O-VASP는 제2 사용자 확인 트랜잭션(성공)(480) 상에 포함된 송금 사용자 지갑 주소(490)를 기반으로 KYC 엔진을 통해 송금 사용자에게 대응되는 송금 사용자 식별 정보(475)를 결정하고 송금 사용자 식별 정보(475)를 해시화하여 제2 해시값(O-VASP)(495)를 생성할 수 있다.
- [98] 즉, 수급 사용자에게 의해 입력되어 해시화된 송금 사용자 식별 정보(460)를 해시화한 값이 제2 해시값(B-VASP)(470)이고, O-VASP의 KYC엔진을 통해 획득된 송금 사용자 식별 정보(475)를 해시화한 값이 제2 해시값(O-VASP)(495)일 수 있다.
- [99] 이해의 편의상 다른 용어로, 제2 해시값(B-VASP)(470)은 제1 송금 사용자 식별 정보(해시), 제2 해시값(O-VASP)(495)는 제2 송금 사용자 식별 정보(해시)라는 용어로도 표현될 수 있다. 제1 송금 사용자 식별 정보(해시)와 제2 송금 사용자 식별 정보(해시)는 동일한 해시 함수 및 난수값(솔트값)을 기반으로 해시화될 수 있다. 제1 송금 사용자 식별 정보(해시)와 제2 송금 사용자 식별 정보(해시)의 비교를 통해 수급 사용자가 입력한 송금 사용자 식별 정보와 B-VASP 상의 송금 사용자 식별 정보가 동일한지 여부가 판단될 수 있다.
- [100] 위와 같은 해시값 비교 절차를 통해 송금 사용자의 수급 사용자 특정 여부 및 수급 사용자의 송금 사용자 특정 여부가 확인될 수 있고, O-VASP와 B-VASP는 송금 사용자 식별 정보 및 수급 사용자 식별 정보를 획득하고 트래블 룰을 만족시킬 수 있다.
- [101]
- [102] 도 5는 본 발명의 실시예에 따른 해시화 방법을 나타낸 개념도이다.
- [103] 도 5에서는 송금 사용자 장치 및 수급 사용자 장치에 의해 입력된 정보에 대한 해시화를 수행하기 위한 방법이 개시된다.
- [104] 도 5를 참조하면, 해시화를 수행함에 있어, 해시값은 작은 데이터의 변화에 민감하게 변화하여 일부 입력 실수가 발생하는 경우, 가상 자산의 전송이 실패할 수 있다.
- [105] 따라서, 송금 사용자 장치 및/또는 수급 사용자 장치에 의해 발생될 수 있는

일부 입력 오류에 의한 문제를 해결하기 위한 방법이 필요하다. 설명의 편의상 송금 사용자 장치 및 수금 사용자 장치에 의해 입력된 송금 정보 또는 수금 정보를 입력 정보라는 용어로 표현한다.

- [106] 본 발명에서는 입력 오류로 인한 가상 자산 전송 실패를 최소화하기 위해 입력 정보에 대한 표준화 절차가 수행될 수 있다.
- [107] 예를 들어, 공식 명칭 이외에 편의성 등을 목적으로 축약어, 별명과 같이 일반적으로 사용되는 명칭이 존재하거나 사명을 변경한 경우가 존재할 수 있다. 예를 들어, IBM은 International Business Machines Corporation, 국제사무기기회사, IBM corp 등으로 여러가지 명칭이 통용되고 있다.
- [108] 이러한 경우, 해시 알고리즘은 입력 정보 상의 작은 데이터의 변화만으로 완전히 다른 값을 나타내는 특징이 있어 해시화 이후 입력 정보가 유사한지 여부에 대한 확인이 불가능하다. 따라서, 입력 정보(500)는 표준 입력 정보(520)로 변환되고, 표준 입력 정보(520)가 해시 함수를 통해 해시값으로 변화되어 전송한 제1 해시값(O-VASP), 제1 해시값(B-VASP), 제2 해시값(O-VASP), 제2 해시값(B-VASP)가 생성될 수 있다.
- [109] 입력 정보(500)를 표준 입력 정보(520)로 변환하기 위해 표준 변환 테이블(510)이 사용될 수 있다. 표준 변환 테이블(510)은 송금 사용자 또는 수금 사용자에게 의해 또는 송금 사용자 또는 수금 사용자에게 의해 제공된 정보에 의해 생성될 수 있다.
- [110] 입력 정보(500)에 대해 표준 변환 테이블(510)이 존재하는 경우 표준 변환 테이블(510)을 통해 입력되는 입력 정보(500)는 표준 입력 정보(510)로 변환될 수 있고, 표준 입력 정보(510)가 해시화되어 해시값이 생성될 수 있다.
- [111] 또는, 본 발명의 실시예에 따르면, 입력 오류로 인한 가상 자산 전송 실패를 최소화하기 위해 입력 정보(500)를 다변환하여 다변화된 입력 정보가 해시값으로서 전송될 수도 있다.
- [112] 예를 들어, 입력 정보(500)가 입력 정보 다변화 엔진(530)으로 입력되고, 입력 정보 다변화 엔진(530)을 통해 복수개의 후보 입력 정보(540)가 생성될 수 있다. 입력 정보(500)와 복수개의 후보 입력 정보(540)는 복수의 해시값(0: hash[입력 정보], 1: hash[후보 입력 정보2], 2: hash[후보 입력 정보2], ..., n: hash[후보 입력 정보n])으로 생성되어 전송될 수 있다.
- [113] 입력 정보 다변화 엔진(530)은 발음을 기반으로 유사 발음으로 혼동이 오는 입력 정보({지현, 지연}, {수연, 수현} 등)에 대한 발음 규칙, 이전 입력 오류 정보 등을 기반으로 생성될 수 있고, 이러한 정보를 기반으로 한 기계 학습을 통해 생성될 수도 있다.
- [114]
- [115] 도 6은 본 발명의 실시예에 따른 입력 정보 입력 방법을 나타낸 개념도이다.
- [116] 도 6에서는 송금 사용자 및 수금 사용자에게 의한 입력 정보의 직접 입력이 없이 입력 정보를 생성하기 위한 방법이 개시된다.

- [117] 도 6을 참조하면, 송금 사용자와 수금 사용자가 다른 매체를 통해 입력 정보를 입력하기 위한 방법이 개시된다.
- [118] QR(quick response) 코드와 같은 식별 정보를 이용한 입력 정보 입력 방법이 사용될 수 있다.
- [119] 송금 사용자는 수금 사용자에게 송금을 위한 QR 코드(송금)(600)를 요청할 수 있고, QR 코드(송금)(600)은 수금 사용자 식별 정보 및/또는 수금 사용자 지갑 정보가 포함될 수 있다.
- [120] 송금 사용자 장치는 O-VASP 상에서 QR 코드(송금)(600)를 인식시켜 송금 정보를 생성할 수 있고, 이러한 경우 송금 사용자에게 의한 별도의 송금 정보의 입력은 필요하지 않을 수 있다.
- [121] 반대로 수금 사용자 장치도 송금 사용자 장치로 수금을 위한 QR 코드(수금)(620)를 요청할 수 있고, QR 코드(수금)(620)은 송금 사용자 식별 정보 및/또는 송금 사용자 지갑 정보가 포함될 수 있다.
- [122] 수금 사용자는 B-VASP 상에서 QR 코드(수금)(620)을 인식시켜 수금 정보를 생성할 수 있고, 이러한 경우 수금 사용자에게 의한 별도의 수금 정보의 입력은 필요하지 않을 수 있다.
- [123] 또는, 메시지를 이용한 입력 정보의 입력 방법이 사용될 수 있다.
- [124] 송금 사용자는 수금 사용자에게 송금을 위한 송금 정보(메신저)(650)를 메시지를 통해 요청할 수 있고, 송금 정보(메신저)(650)는 수금 사용자 식별 정보 및/또는 수금 사용자 장치 지갑 정보가 포함될 수 있다. 예를 들어, 송금 정보(메신저)(650)는 메신저 상의 클릭을 통해 획득될 수 있는 정보일 수 있다.
- [125] 송금 사용자는 O-VASP 상에 송금 정보(메신저)(650) 입력하여 송금 정보를 생성할 수 있고, 이러한 경우 송금 사용자에게 의한 별도의 송금 정보의 입력은 필요하지 않을 수 있다.
- [126] 반대로 수금 사용자는 송금 사용자로 수금을 위한 수금 정보(메신저)(670)를 메시지를 통해 요청할 수 있고, 수금 정보(메신저)(670)는 송금 사용자 식별 정보 및/또는 송금 사용자 지갑 정보가 포함될 수 있다. 수금 정보(메신저)(670)는 메신저 상의 클릭을 통해 획득될 수 있는 정보일 수 있다.
- [127] 수금 사용자는 B-VASP 상에 수금 정보(메신저)(670)를 입력하여 수금 정보를 생성할 수 있고, 이러한 경우 수금 사용자에게 의한 별도의 수금 정보의 입력은 필요하지 않을 수 있다.
- [128] 이러한 QR 코드(송금, 수금), 송금 정보(메신저), 수금 정보(메신저)는 상대 VASP 또는 상대 사용자만 인식할 수 있는 형태로 암호화하여 전송될 수 있다. 예를 들어, QR 코드(송금, 수금), 송금 정보(메신저), 수금 정보(메신저)는 거래소의 공개키로 암호화되어 거래소 개인키로만 QR 코드(송금, 수금), 송금 정보(메신저), 수금 정보(메신저)에 대한 확인이 가능하도록 구현될 수도 있다.
- [129]
- [130] 도 7은 본 발명의 실시예에 따른 가상 자산 전송의 단순화를 위한 방법을

나타낸 개념도이다.

- [131] 도 7에서는 송금 사용자 및 수금 사용자에게 대한 확인의 주체를 변경하여 가상 자산 전송 절차를 단순화하기 위한 방법이 개시된다.
- [132] 도 7을 참조하면, 제1 사용자 확인 트랜잭션의 전송시 송금 정보로서 송금 사용자 식별 정보도 추가적으로 포함하여 전송될 수 있다.
- [133] 전송한 바와 같이 제1 해시값(O-VASP)과 제1 해시값(B-VASP)이 동일하다면, 수금 사용자는 송금 사용자 식별 정보를 입력하여 O-VASP로 전송하여 송금 사용자를 특정할 수 있다. 만약, 수금 사용자에게 의한 송금 사용자에게 대한 특정이 실패하는 경우, 제2 해시값(O-VASP)과 제2 해시값(B-VASP)이 동일하지 않아서 가상 자산 전송이 실패할 수 있다. 가상 자산 전송이 실패하는 경우, 제1 사용자 확인 트랜잭션의 전송부터 다시 시작해야 할 수 있고, 입력 오류로 인한 불필요한 블록체인 네트워크의 혼잡도를 높일 수 있다.
- [134] 따라서, 별도의 블록체인 네트워크 상에서의 전송없이 B-VASP 상의 확인 절차를 입력 오류로 인한 문제를 해결하기 위해 제1 사용자 확인 트랜잭션(710)의 전송시 송금 정보로서 송금 사용자 식별 정보(해시)(720)도 추가적으로 포함하여 전송될 수 있다. 송금 사용자 식별 정보(해시)(720)는 적용한 송금 사용자 식별 정보에 해시함수를 적용한 값일 수 있다.
- [135] B-VASP 상에서 수금 사용자가 입력한 송금 사용자 식별 정보(입력)(해시)(725)와 제1 사용자 확인 트랜잭션(710)에 포함된 송금 사용자 식별 정보(해시)(720)를 비교하여 수금 사용자로 입력 오류 여부에 대해 미리 알려줄 수 있다. 이러한 방법을 통해 불필요한 블록체인 상의 트랜잭션이 방지되고, 수금 사용자의 입력 오류가 정정될 수도 있다.
- [136] 또한, 제1 사용자 확인 트랜잭션(710)의 전송시 송금 사용자에게 의한 수금 사용자 식별 정보의 입력 오류가 발생할 수도 있다. 이러한 경우, 송금 사용자는 제1 사용자 확인 트랜잭션을 전송하는 절차부터 다시 시작해야 한다. 반복 절차를 방지하기 위해 아래와 같은 단순화된 가상 자산 전송 절차가 수행될 수도 있다.
- [137] 송금 사용자에게 의해 수금 사용자 식별 정보에 대한 입력 오류가 발생된 경우, 제1 해시값(O-VASP)과 제1 해시값(B-VASP)이 동일할 수 없고, 수금 사용자의 확인 실패를 지시하는 제2 사용자 확인 트랜잭션(실패)가 O-VASP로 전송될 수 있다.
- [138] 송금 사용자의 수금 사용자 식별 정보에 대한 입력 오류를 정정하기 위해 제2 사용자 확인 트랜잭션(실패)(730)는 수금 사용자 식별 정보를 해시화한 수금 사용자 식별 정보(해시)(740)를 포함할 수 있다.
- [139] O-VASP 상에서 송금 사용자에게 입력 오류로 인한 수금 사용자 식별 정보의 재입력을 요청할 수 있다. 송금 사용자에게 의해 재입력된 수금 사용자 식별 정보(재입력)을 해시화한 수금 사용자 식별 정보(재입력)(해시)(745)와 제2 사용자 확인 트랜잭션(실패)(730)에 포함된 수금 사용자 식별 정보(해시)(740)가

비교되어 동일성 여부를 판단할 수 있다. 이러한 절차를 통해 계속되는 송금 사용자의 수금 사용자 식별 정보에 대한 입력 오류로 인한 불필요한 제1 사용자 확인 트랜잭션의 전송을 방지할 수 있다.

- [140] 임계 개수의 재입력 횟수 내에 송금 사용자에게 의해 정확한 수금 사용자 식별 정보(입력)(해시)(745)가 입력되는 경우, 펜딩된 가상 자산 전송 트랜잭션이 전송될 수 있다. 즉, 송금 사용자가 수금 사용자 장치 식별 정보의 입력 오류를 발생시키 경우에도 O-VASP 단에서 입력된 오류가 정정되는 경우, 다시 제1 사용자 확인 트랜잭션의 전송없이 펜딩된 가상 자산 전송 트랜잭션(770)을 바로 전송하도록 절차가 단순화될 수 있다.
- [141] 구체적으로 임계 개수의 재입력 횟수 내에 송금 사용자에게 의해 정확한 수금 사용자 식별 정보가 입력되는 경우, 펜딩된 가상 자산 전송 트랜잭션이 바로 전송되기 위해서는 제2 사용자 확인 트랜잭션(실패)에 수금 사용자에게 의해 생성된 송금 사용자 식별 정보(입력)(해시)(725)가 포함되어 O-VASP의 KYC를 기반으로 획득된 송금 사용자 식별 정보(해시)(720)와 동일성이 확인된 경우에 진행될 수도 있다. 또는 제2 사용자 확인 트랜잭션(실패)(730)에 B-VASP 상에서 수금 사용자에게 의해 생성된 송금 사용자 식별 정보(입력)(해시)(725)가 제1 사용자 확인 트랜잭션(720)(710)에 포함된 송금 사용자 식별 정보(해시)와의 동일성이 확인되었음을 식별하는 정보가 포함된 경우에도 임계 개수의 재입력 횟수 내에 송금 사용자에게 의해 정확한 수금 사용자 식별 정보가 입력된 후 펜딩된 가상 자산 전송 트랜잭션(770)이 바로 전송될 수 있다.
- [142] 또한 본 발명의 실시예에 따르면 입력하는 상대 사용자의 식별 정보가 재입력 횟수 제한을 넘게 틀릴 경우, 개인정보의 등급이 높은 사용자에게 이름, 생년월일, 전화번호, 주소 등과 같은 높은 수준의 추가 사용자 식별 정보의 입력을 요청하고, 추가 사용자 식별 정보를 기반으로 한 해시값의 동일성을 확인할 수 있다.
- [143] 위와 같은 단순화된 가상 자산 전송 절차는 선택적으로 사용되어 가상 자산 전송시 오류 입력시 트랜잭션의 재전송 없이 입력 오류를 정정할 수 있다. 단순화된 가상 자산 전송 절차는 블록체인 네트워크의 혼잡도, 거래량 등을 고려하여 선택적으로 수행될 수 있다.
- [144]
- [145] 도 8은 본 발명의 실시예에 따른 가상 자산 전송의 단순화를 위한 방법을 나타낸 개념도이다.
- [146] 도 8에서는 송금 사용자와 수금 사용자 간의 기존 거래 내역이 존재하는 경우 단순화된 가상 자산 전송 절차가 개시된다.
- [147] 도 8을 참조하면, 단순화된 가상 자산 전송 절차의 가능 여부를 판단한다(단계 S800).
- [148] 송금 사용자와 수금 사용자 간의 기존 거래 내역이 존재하는 경우, 전송한 제1 사용자 확인 트랜잭션 및 제2 사용자 확인 트랜잭션 없이 단순화된 가상 자산

전송 절차가 수행될 수 있다. 다른 표현으로 가상 자산 전송 트랜잭션이 트러스트 펜딩(trust pending) 상태가 아닌 트러스트(trust) 상태로 바로 설정되어 전송될 수 있다.

- [149] 구체적으로 송금 사용자는 기존에 거래를 한 수금 사용자를 선택할 수 있다. 기존 거래로 인해 O-VASP에는 수금 사용자 식별 정보가 저장되어 있고, 이러한 수금 사용자 식별 정보를 확인할 수 있어 거래를 물을 만족한다.
- [150] B-VASP는 가상 자산 전송 트랜잭션을 수신하고, 수금 사용자의 송금 사용자에 대한 확인을 위한 절차를 생략하거나 별도의 트랜잭션 없이 B-VASP 상에서만 수금 사용자의 송금 사용자에 대한 확인을 위한 절차를 수행할 수 있다.
- [151] 예를 들어, 송금 사용자 장치의 지갑 주소가 거래소 지갑이 아닌 특정된 지갑 주소인 경우, 가상 자산 전송 트랜잭션을 기반으로 송금 사용자 식별 정보를 획득할 수 있어 별도의 송금 사용자에 대한 확인 절차가 수행되지 않을 수 있다.
- [152] 또는 단순화된 가상 자산 전송 절차를 수행시 가상 자산 전송 트랜잭션 상에 해시화된 송금 사용자 식별 정보가 포함될 수 있다. 수금 사용자의 기존 거래 상대방에 대한 정보를 해시화하여 해시화된 송금 사용자 식별 정보와 비교하여 동일한 송금 사용자가 특정되는 경우, 가상 자산 전송이 유효화될 수 있다.
- [153] 또는 이러한 단순화된 가상 자산 전송 절차를 수행시 가상 자산 전송 트랜잭션 상에 해시화된 송금 사용자 식별 정보가 포함될 수 있다. 수금 사용자가 기존의 거래 상대방 중 송금 사용자를 선택하는 경우 해시화하여 해시화된 송금 사용자 식별 정보와 비교하여 가상 자산 전송이 유효화될 수 있다.
- [154] 마찬가지로 거래 완료 이후 O-VASP 및 B-VASP 상에는 송금 사용자, 수금 사용자 간의 거래에 대한 내역이 저장될 수 있다(단계 S810).
- [155] 단순화된 가상 자산 전송 절차의 가능하지 않은 경우, 전술한 가상 자산 전송 절차를 통해 가상 자산 전송이 이루어질 수 있다.
- [156]
- [157] 도 9는 본 발명의 실시예에 따른 가상 자산 전송의 단순화를 위한 방법을 나타낸 개념도이다.
- [158] 도 9에서는 송금 사용자 식별 정보가 B-VASP 상에 미리 제공된 경우, 단순화된 가상 자산 전송 절차가 개시된다.
- [159] 도 9를 참조하면, 수금 사용자가 송금 사용자 식별 정보(900)를 B-VASP에 미리 제공한 경우, 또는 송금 사용자가 송금 사용자 식별 정보(900)를 B-VASP에 미리 제공한 경우, 제1 사용자 확인 트랜잭션(910)을 수신한 이후, 수금 사용자로 송금 사용자 식별 정보의 요청 없이 제2 사용자 확인 트랜잭션(920)이 전송될 수 있다.
- [160] 이러한 방법을 통해 수금 사용자에게 송금 사용자에 대한 식별을 요청하지 않아서 가상 자산 전송 절차가 보다 단순화될 수 있다.
- [161]
- [162] 도 10은 본 발명의 실시예에 따른 송금 사용자 및 수금 사용자에 대한 정보를 저장하는 방법이 개시된다.

- [163] 도 10을 참조하면, 전술한 바와 같이 송금 사용자의 잔고를 확인하여 정상 거래가 가능한지 확인한 후 가상 자산 전송 트랜잭션이 전송될 수 있다.
- [164] 가상 전송 트랜잭션이 전송되어 완료된 거래에 대해서 트랜잭션 정보에 더하여 O-VASP(1000) 상에는 수금 사용자(또는 B-VASP)에 의해 입력된 송금 사용자와 관련된 정보(지갑 주소, 이름, 거래소)에 대한 정보가 저장되고, B-VASP(1050) 상에는 송금 사용자(또는 O-VASP)에 의해 입력된 수금 사용자와 관련된 정보(지갑 주소, 이름, 거래소)에 대한 정보가 저장될 수 있다.
- [165]
- [166] 도 11은 본 발명의 실시예에 따른 가상 자산 전송 방법을 나타낸 개념도이다.
- [167] 도 11에서는 가상 자산 전송시 송금 사용자 장치를 특정하기 위한 방법이 개시된다.
- [168] 도 11을 참조하면, O-VASP에서 송금 사용자로부터 송금 요청을 받으면, O-VASP의 통합 지갑에서 송금이 이루어지는 것이 일반적이다. 통합 지갑은 O-VASP의 지갑으로서 개인을 특정할 수 없는 지갑이다. B-VASP 상에서 수금을 받는 수금 지갑은 수금하는 수금 사용자의 구분을 위해 수금 사용자마다 설정된 개인 지갑일 수 있다.
- [169] 이러한 경우, O-VASP의 통합 지갑을 통해 송금 거래가 발생할 경우, 통합 지갑의 주소 정보로는 송금 사용자를 특정할 수 없다는 문제가 발생한다. 따라서, 기존 거래소의 통합된 통합 지갑과 수금을 위해 수금 사용자 별로 존재하는 개인 지갑을 유지하면서 신원 확인 절차를 거치는 방법으로 해시값 이외에도 이전 트랜잭션 정보나 고객을 특정할 수 있는 주소가 추가적으로 트랜잭션에 포함될 수 있다.
- [170] 예를 들어, 송금 사용자의 특정을 위해 이전 트랜잭션 정보를 추가하는 방법은 아래와 같다.
- [171] (1) 이전 트랜잭션 정보 추가 방법(1100)
- [172] 제1 사용자 확인 트랜잭션의 생성 이후, 제2 사용자 확인 트랜잭션에 제1 사용자 확인 트랜잭션의 트랜잭션ID가 포함될 수 있다. 이러한 제1 사용자 확인 트랜잭션의 트랜잭션ID를 기반으로 O-VASP 상에서 송금 사용자에 대한 특정이 가능하다. 이후, 가상 자산 전송 트랜잭션에는 제2 사용자 확인 트랜잭션의 트랜잭션 ID가 포함되어 제2 사용자 확인 트랜잭션과 관련된 가상 자산 전송입을 특정하여 송금 사용자에 대한 특정이 가능하다.
- [173] (2) 송금 사용자 개인 지갑 정보 추가 방법(1150)
- [174] 또 다른 예로, 송금 사용자의 특정을 위해 송금 사용자의 개인 지갑에 대한 정보가 제1 사용자 확인 트랜잭션에 추가로 포함될 수 있다.
- [175] O-VASP의 지갑 주소뿐만 아니라 송금 사용자의 개인 지갑에 대한 정보가 제1 사용자 확인 트랜잭션에 포함되어 송금 사용자에 대한 특정이 가능할 수 있다.
- [176] 제2 사용자 확인 트랜잭션 상에서는 송금 사용자의 개인 지갑을 특정함으로써 O-VASP 상에서는 송금 사용자를 특정할 수 있다.

- [177] 가상 자산 전송 트랜잭션에도 송금 사용자의 개인 지갑에 대한 정보가 포함되어 송금 사용자에 대한 특정이 가능할 수 있다.
- [178]
- [179] 도 12는 본 발명의 실시예에 따른 가상 자산 전송 방법을 나타낸 개념도이다.
- [180] 도 12에서는 다양한 가상 자산 전송에 대한 실시예가 개시된다.
- [181] 도 12를 참조하면, 제1 가상 자산 전송 방법(1210), 제2 가상 자산 전송 방법(1220), 제3 가상 자산 전송 방법(1230), 제4 가상 자산 전송 방법(1240)이 개시된다.
- [182] 제1 가상 자산 전송 방법(1210)은 송금 사용자의 개인 지갑 및 수금 사용자의 개인 지갑을 이용한 가상 자산 전송이다. 송금 사용자의 개인 지갑 및 수금 사용자의 개인 지갑이 사용되는 경우, 별도의 송금 사용자의 특정 이슈가 발생하지 않고, 송금 사용자의 개인 지갑 주소 및 수금 사용자의 개인 지갑 주소를 기반으로 제1 사용자 확인 트랜잭션, 제2 사용자 확인 트랜잭션, 가상 자산 전송 트랜잭션이 발생할 수 있다.
- [183] 제2 가상 자산 전송 방법(1220)은 O-VASP의 통합 지갑을 통해 거래가 이루어지는 경우, 제2 사용자 확인 트랜잭션에 제1 사용자 확인 트랜잭션의 트랜잭션 ID를 추가하여 O-VASP 상에서 송금 사용자에 대한 특정이 가능하도록 할 수 있다.
- [184] 제3 가상 자산 전송 방법(1230)은 O-VASP의 통합 지갑을 통해 거래가 이루어지는 경우, 제1 사용자 확인 트랜잭션에 송금 사용자의 개인 지갑에 대한 정보를 추가하여 전송할 수 있다. 제2 사용자 확인 트랜잭션에서 송금 사용자의 개인 지갑을 기반으로 송금 사용자를 특정하여 송금 사용자에 대한 확인을 수행하고, 가상 자산 전송 트랜잭션은 O-VASP의 통합 지갑에서 이루어질 수 있다.
- [185] 제4 가상 자산 전송 방법(1240)은 제1 사용자 확인 트랜잭션 및 제2 사용자 확인 트랜잭션이 개인 지갑을 기반으로 이루어지고 가상 자산 전송 트랜잭션은 O-VASP의 통합 지갑을 통해 이루어지는 방법이다. 즉, 트랜잭션 상에 별도의 정보 추가없이 송신 주소에 송금 사용자의 개인 지갑 주소, 수신 주소에 수금 사용자의 개인 지갑 주소가 직접적으로 사용되어 제1 사용자 확인 트랜잭션 및 제2 사용자 확인 트랜잭션을 기반으로 한 송금 사용자 확인, 수금 사용자 확인 절차가 수행될 수 있다.
- [186]
- [187] 도 13은 본 발명의 실시예에 따른 가상 자산의 전송 방법을 나타낸 개념도이다.
- [188] 도 13에서는 서로 다른 블록체인 네트워크를 활용한 가상 자산 전송 방법이 개시된다.
- [189] 도 13을 참조하면, 특정 블록체인(예를 들어, 비트코인, 이더리움)은 트랜잭션 전송 수수료가 높고 트랜잭션의 확정을 위한 시간이 오래 걸린다는 한계가 있다. 또한 데이터의 전송에서 메인넷의 특성에 따라서 설계가 변경되어야 한다.

- [190] 따라서, 제1 사용자 확인 트랜잭션 및 제2 사용자 확인 트랜잭션을 전송하는 블록체인 네트워크와 가상 자산을 전송하기 위한 블록체인 네트워크가 별도로 설정될 수 있다.
- [191] 제1 사용자 확인 트랜잭션 및 제2 사용자 확인 트랜잭션을 전송하는 블록체인 네트워크는 제1 블록체인 네트워크(1310) 또는 블록체인 네트워크(사용자 확인)이라는 용어로 표현되고, 가상 자산 전송 트랜잭션을 전송하는 블록체인 네트워크는 제2 블록체인 네트워크(1320) 또는 블록체인 네트워크(가상 자산 전송)이라는 용어로 표현될 수 있다.
- [192] 서로 다른 블록체인 네트워크를 사용하기 위해서 제1 블록체인 네트워크(1310) 상에서 사용자 확인을 진행시 가상 자산 전송을 위한 송금 사용자, 수금 사용자의 제2 블록체인 네트워크(1320) 상의 지갑 주소에 대한 정보(wallet(from), wallet(to))가 전달될 수 있다.
- [193] Tx1 (From = wallet(O-VASP), To = wallet(B-VASP), data = {hash(to), wallet(from), wallet(to), Currency})
- [194] 또한, 제2 블록체인 네트워크(1320) 상에서 가상 자산을 거래하기 위해 제1 블록체인 네트워크(1310) 상에서 트랜잭션에 대한 정보(제1 사용자 확인 트랜잭션 및 제2 사용자 확인 트랜잭션)(예를 들어, Txid(Tx2))가 포함될 수 있다.
- [195] Tx3 (From = wallet(O-VASP), To = wallet(to), data = {hash(to), Txid(Tx2)})
- [196] 제1 블록체인 네트워크(1310) 상에서 트랜잭션에 대한 정보는 제1 사용자 확인 트랜잭션 정보 및/또는 제2 사용자 확인 트랜잭션 정보가 선택적으로 포함될 수 있다.
- [197]
- [198] 이상 설명된 본 발명에 따른 실시예는 다양한 컴퓨터 구성요소를 통하여 실행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수 있다. 컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM 및 DVD와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical medium), 및 ROM, RAM, 플래시 메모리 등과 같은, 프로그램 명령어를 저장하고 실행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령어의 예에는, 컴파일러에 의하여 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용하여 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위하여 하나 이상의 소프트웨어 모듈로 변경될 수 있으며, 그 역도 마찬가지이다.

- [199] 이상에서 본 발명이 구체적인 구성요소 등과 같은 특정 사항과 한정된 실시예 및 도면에 의하여 설명되었으나, 이는 본 발명의 보다 전반적인 이해를 돕기 위하여 제공된 것일 뿐, 본 발명이 상기 실시예에 한정되는 것은 아니며, 본 발명이 속하는 기술분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정과 변경을 꾀할 수 있다.
- [200] 따라서, 본 발명의 사상은 상기 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 또는 이로부터 등가적으로 변경된 모든 범위는 본 발명의 사상의 범주에 속한다고 할 것이다.