(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2018 년 5 월 3 일 (03.05.2018)

WIPO | PCT

(10) 국제공개번호
WO 2018/080205 A1

(51) 국제특허분류:
G06Q 20/36 (2012.01) *G06Q 40/02* (2012.01)
G06Q 20/38 (2012.01) *G06Q 40/04* (2012.01)
G06Q 20/06 (2012.01)

(21) 국제출원번호: PCT/KR2017/011937

(22) 국제출원일: 2017 년 10 월 26 일 (26.10.2017)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2016-0140163 2016 년 10 월 26 일 (26.10.2016) KR

(71) 출원인: 주식회사 코인플러그 (COINPLUG, INC.) [KR/KR]; 13558 경기도 성남시 분당구 성남대로331번길 8, 801호, Gyeonggi-do (KR).

(72) 발명자: 송주한 (SONG, Joo Han); 13558 경기도 성남시 분당구 느티로 22, A동 2114호, Gyeonggi-do (KR). 홍재우 (HONG, Jay Wu); 03336 서울시 은평구 연서로 149, 1203호, Seoul (KR). 어준선 (UHR, Joon Sun); 13558 경기도 성남시 분당구 느티로 22, B동 1710호, Gyeonggi-do (KR).

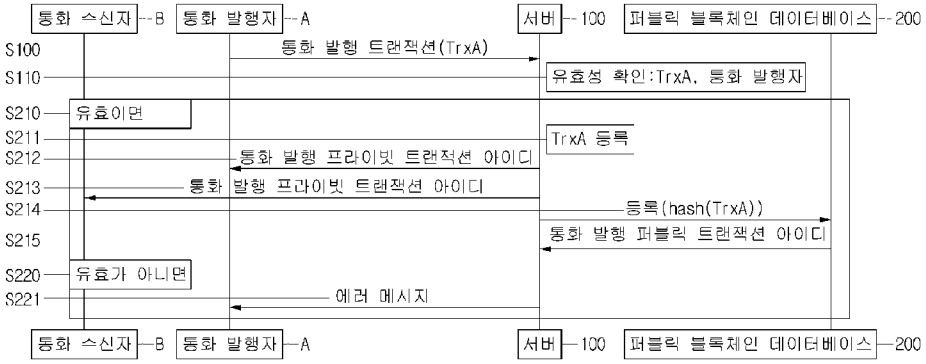
(74) 대리인: 특허법인 수 (SU INTELLECTUAL PROPERTY); 06134 서울시 강남구 강남대로 94길 34, 6층 (역삼동, 케이앤와이빌딩), Seoul (KR).

(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, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK,

WO 2018/080205 A1

(54) **Title:** METHOD FOR ISSUING CURRENCY AND MAKING PAYMENT USING UTXO-BASED PROTOCOL AND SEVER USING SAME

(54) **발명의 명칭:** UTXO 기반 프로토콜을 사용하여 통화를 발행 및 지급 결제하는 방법과 이를 이용한 서버



100 ... Server
200 ... Public blockchain database
S100 ... Currency issuing transaction (TrxA)
S110 ... Confirm validity: TrxA, currency issuer
S210 ... If valid
S211 ... Register TrxA
S212 , S213 ... Currency issuance private transaction ID
S214 ... Register (hash(TrxA))
S215 ... Currency issuance public transaction ID
S220 ... If invalid
S221 ... Error message
A ... Currency issuer
B ... Currency receiver

(57) **Abstract:** The present invention relates to a method for issuing a currency comprising the steps of: (a) confirming the validity of a currency issuing transaction and a currency issuer, when the currency issuing transaction for issuing the currency from the currency issuer is obtained, the currency issuing transaction including (i) currency receiver information, (ii) issued amount of the currency, (iii) a public key of the currency issuer, and (iv) a signature value of the currency issuer signing the (i), (ii), and (iii) with a private key of the currency issuer; and (b) registering the currency issuing transaction or a hash value thereof on a public blockchain database, and obtaining a currency issuance public transaction ID indicating location information of the currency issuing transaction or the hash value thereof on the public blockchain database, when the currency issuing transaction and the currency issuer are deemed valid.

[다음 쪽 계속]

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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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))

(57) 요약서: 본 발명은 통화를 발행하는 방법에 있어서, (a) 통화 발행자로부터 상기 통화 발행을 위한 (i) 통화 수신자 정보, (ii) 상기 통화의 발행량, (iii) 상기 통화 발행자의 퍼블릭 키 및 (iv) 상기 통화 발행자의 프라이빗 키로 상기 (i), (ii), 및 (iii) 을 서명한 상기 통화 발행자의 서명값을 포함하는 통화 발행 트랜잭션이 획득되면, 상기 통화 발행 트랜잭션 및 상기 통화 발행자의 유효 여부를 확인하는 단계, 및 (b) 상기 통화 발행 트랜잭션과 상기 통화 발행자가 유효이면, 상기 통화 발행 트랜잭션 또는 이의 해쉬값을 퍼블릭 블록체인 데이터베이스에 등록하고, 상기 통화 발행 트랜잭션 또는 이의 해쉬 값의 상기 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 통화 발행 퍼블릭 트랜잭션 아이디를 획득하는 단계를 포함하는 방법이 제공된다.

명세서

발명의 명칭: UTXO 기반 프로토콜을 사용하여 통화를 발행 및 지급 결제하는 방법과 이를 이용한 서버

기술분야

[1] UTXO 기반 프로토콜을 사용하여 통화를 발행 및 지급 결제하는 방법과 이를 이용한 서버에 관한 것으로, 보다 상세하게는, (a) 통화 발행자로부터 상기 통화 발행을 위한 (i) 통화 수신자 정보, (ii) 상기 통화의 발행량, (iii) 상기 통화 발행자의 퍼블릭 키 및 (iv) 상기 통화 발행자의 프라이빗 키로 상기 (i), 상기 (ii), 상기 (iii)을 서명한 상기 통화 발행자의 서명값을 포함하는 통화 발행 트랜잭션이 획득되면, 상기 통화 발행 트랜잭션 및 상기 통화 발행자의 유효 여부를 확인하고, (b) 상기 확인 결과 유효이면, 상기 통화 발행 트랜잭션에 대한 해쉬 값을 퍼블릭 블록체인 데이터베이스에 등록하며, 상기 퍼블릭 블록체인 데이터베이스에 등록된 해쉬 값의 상기 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 통화 발행 퍼블릭 트랜잭션 아이디를 획득하는 방법과 이를 이용하는 서버에 관한 것이며, 더 나아가 특정 사용자가 통화를 지급 결제하는 방법 및 이를 이용하는 서버에 관한 것이다.

배경기술

[2] 일반적으로 통화는 유통 수단이나 지불 수단으로서 기능하는 교환 수단으로, 국가가 공식적으로 지정하여 쓰는 돈, 다시 말해 지불 및 상업적 유통 단위를 뜻한다. 또한, 특정 단체 내에서만 사용되는 특정 교환 수단도 하나의 통화일 수 있을 것이다.

[3] 그리고, 국가 단위에서 볼 경우, 중앙은행은 통화를 발행하거나 관리하며, 시중은행들은 중앙은행에서 발행된 통화를 사용하게 된다.

[4] 이때, 시중은행에서의 은행간 자금 결제는 중앙은행의 결제 시스템을 통해 이루어지며, 실제 현금의 이동을 수반하지는 않는다. 즉, 중앙은행에 개설되어 있는 각 은행들의 계정에서 은행별 결제금액을 입금 또는 출금하는 방식으로 결제가 이루어지고 있다.

[5] 그러나, 이러한 결제 시스템에서는 은행의 업무 종료 이후, 중앙은행과 시중은행들은 하루 동안 발생된 자금의 지급 결제에 대하여 매일 정산하여야 하는 불편함이 있다.

[6] 또한, 정산시 방대한 지급 결제에 대한 자료를 확인하여야 하는 어려움이 있으며, 정산 결과에 오류가 있을 경우 이를 확인하는데 많은 시간이 소요되는 등의 문제점이 있다.

[7] 또한, 결제 시스템의 해킹이나 시중은행의 해킹에 의한 기록 데이터의 복사 또는 위/변조가 발행할 경우 이를 확인하는 데 많은 시간과 노력이 소모되는 등의 문제점이 있다.

발명의 상세한 설명

기술적 과제

[8] 본 발명은 상술한 문제점들을 모두 해결하는 것을 그 목적으로 한다.

[9] 또한, 본 발명은 가상 화폐의 블록체인에 통화의 발행 또는 지급 결제에 대한 정보를 등록하여 복사 또는 위/변조가 불가능하도록 하는 방법 및 서버를 제공하는 것을 다른 목적으로 한다.

[10] 또한, 본 발명은 통화 발행이나 통화의 지급 결제 등의 정보를 해쉬 함수와 암호화 기술을 이용하여 보안이 보장되고 위/변조가 불가능하도록 하는 방법 및 서버를 제공하는 것을 또 다른 목적으로 한다.

[11] 또한, 본 발명은 가상 화폐의 블록체인에 통화의 발행이나 지급 결제에 대한 정보를 등록함으로써 통화의 중복 지급 등의 문제점을 미연에 방지할 수 있도록 하는 방법 및 서버를 제공하는 것을 또 다른 목적으로 한다.

[12] 또한, 본 발명은 중앙은행과 시중은행 간의 정산 절차를 진행하지 않아도 항상 정산된 최신의 정산 정보를 확인할 수 있도록 하는 방법 및 서버를 제공하는 것을 또 다른 목적으로 한다.

과제 해결 수단

[13] 상기 목적을 달성하기 위한 본 발명의 대표적인 구성은 다음과 같다.

[14] 본 발명의 일 실시예에 따르면, 통화를 발행하는 방법에 있어서, (a) 통화 발행자로부터의 상기 통화 발행을 위한 (i) 통화 수신자 정보, (ii) 상기 통화의 발행량, (iii) 상기 통화 발행자의 퍼블릭 키 및 (iv) 상기 통화 발행자의 프라이빗 키로 상기 (i), 상기 (ii), 상기 (iii)을 서명한 상기 통화 발행자의 서명 값을 포함하는 통화 발행 트랜잭션이 획득되면, 서버는, 상기 통화 발행 트랜잭션 및 상기 통화 발행자의 유효 여부를 확인하는 단계; 및 (b) 상기 통화 발행 트랜잭션과 상기 통화 발행자가 유효이면, 상기 서버는, (i) 상기 통화 수신자 정보, (ii) 상기 통화의 발행량, (iii) 상기 통화 발행자의 퍼블릭 키 및 (iv) 상기 통화 발행자의 서명 값을 포함하는 상기 통화 발행 트랜잭션 또는 상기 통화 발행 트랜잭션에 대한 해쉬 값을 퍼블릭 블록체인 데이터베이스에 등록하거나 등록하도록 지원하고, 상기 퍼블릭 블록체인 데이터베이스에 등록된 상기 통화 발행 트랜잭션 또는 상기 통화 발행 트랜잭션에 대한 해쉬 값의 상기 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 통화 발행 퍼블릭 트랜잭션 아이디를 획득하거나 획득하도록 지원하는 단계를 포함하는 방법이 제공된다.

[15] 또한, 본 발명의 일 실시예에 따르면, 통화의 지급을 결제하는 방법에 있어서, (a) 특정 사용자로부터 상기 통화의 지급 결제를 위한 (i) 이전에 적어도 일부 미사용된 적어도 하나 이상의 제1 통화 사용 트랜잭션 아이디, (ii) 통화 수신자 정보, (iii) 지급 결제 금액, (iv) 상기 특정 사용자의 퍼블릭 키 및 (v) 상기 특정 사용자의 프라이빗 키로 상기 (i), 상기 (ii), 상기 (iii), 상기 (iv)를 서명한 상기 특정 사용자의 서명 값을 포함하는 제2 통화 사용 트랜잭션이 획득되면, 서버는,

상기 제2 통화 사용 트랜잭션의 상기 특정 사용자의 밸런스를 참조하여 상기 제2 통화 사용 트랜잭션의 지급 결제 방식을 확인하는 단계; 및 (b) (i) 상기 특정 사용자의 밸런스가 상기 지급 결제 금액 이상이어서 상기 제2 통화 사용 트랜잭션의 지급 결제 방식이 "즉시 지급 결제"로 확인되면, 상기 서버는, 상기 특정 사용자의 서명 값이 유효한지를 판단하여 유효일 경우, 상기 제2 통화 사용 트랜잭션 또는 상기 제2 통화 사용 트랜잭션에 대한 해쉬 값을 퍼블릭 블록체인 데이터베이스에 등록하거나 등록하도록 지원하고, 상기 퍼블릭 블록체인 데이터베이스에 등록된 상기 제2 통화 사용 트랜잭션 또는 상기 제2 통화 사용 트랜잭션의 해쉬 값의 상기 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 제2 통화 사용 퍼블릭 트랜잭션 아이디를 획득하거나 획득하도록 지원하거나, (ii) 상기 특정 사용자의 밸런스가 상기 지급 결제 금액 미만이어서 상기 제2 통화 사용 트랜잭션의 지급 결제 방식이 "지연 지급 결제"로 확인되면, 상기 서버는, 상기 특정 사용자의 서명 값이 유효한지를 판단하여 유효일 경우, 상기 제2 통화 사용 트랜잭션을 저장부에 저장한 상태에서, 적어도 하나 이상의 타 사용자에 의해 지급 결제되며 상기 특정 사용자를 수취인으로 하는 적어도 하나 이상의 제3 통화 사용 트랜잭션이 소정의 상계 처리 조건을 만족하면, 상기 제2 통화 사용 트랜잭션과 상기 제3 통화 사용 트랜잭션들을 상계 처리하며, 상계 처리된 상기 제2 통화 사용 트랜잭션 또는 상기 제2 통화 사용 트랜잭션의 해쉬 값과 상기 제3 통화 사용 트랜잭션 또는 상기 제3 통화 사용 트랜잭션의 해쉬 값을 상기 퍼블릭 블록체인 데이터베이스에 등록하거나 등록하도록 지원하며, 상기 퍼블릭 블록체인 데이터베이스에 등록된 상기 제2 통화 사용 트랜잭션 또는 상기 제2 통화 사용 트랜잭션의 해쉬 값과 상기 제3 통화 사용 트랜잭션 또는 상기 제3 통화 사용 트랜잭션의 해쉬 값의 상기 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 제2 통화 사용 퍼블릭 트랜잭션 아이디와 제3 통화 사용 퍼블릭 트랜잭션 아이디를 획득하거나 획득하도록 지원하는 단계를 포함하는 방법이 제공된다.

[16] 또한, 본 발명의 일 실시예에 따르면, 통화를 발행하는 서버에 있어서, 통화 발행자로부터의 상기 통화 발행을 위한 (i) 통화 수신자 정보, (ii) 상기 통화의 발행량, (iii) 상기 통화 발행자의 퍼블릭 키 및 (iv) 상기 통화 발행자의 프라이빗 키로 상기 (i), 상기 (ii), 상기 (iii)을 서명한 상기 통화 발행자의 서명 값을 포함하는 통화 발행 트랜잭션을 획득하는 통신부; 및 상기 획득된 상기 통화 발행 트랜잭션 및 상기 통화 발행자의 유효 여부를 확인하여 유효이면, (i) 상기 통화 수신자 정보, (ii) 상기 통화의 발행량, (iii) 상기 통화 발행자의 퍼블릭 키 및 (iv) 상기 통화 발행자의 서명 값을 포함하는 상기 통화 발행 트랜잭션 또는 상기 통화 발행 트랜잭션에 대한 해쉬 값을 퍼블릭 블록체인 데이터베이스에 등록하거나 등록하도록 지원하고, 상기 퍼블릭 블록체인 데이터베이스에 등록된 상기 통화 발행 트랜잭션 또는 상기 통화 발행 트랜잭션에 대한 해쉬 값의 상기 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 통화 발행

퍼블릭 트랜잭션 아이디를 획득하거나 획득하도록 지원하는 프로세서를 포함하는 것을 특징으로 하는 서버가 제공된다.

[17] 또한, 본 발명의 일 실시 예에 따르면, 통화의 지급을 결제하는 서버에 있어서, 특정 사용자로부터 상기 통화의 지급 결제를 위한 (i) 이전에 적어도 일부 미사용된 적어도 하나 이상의 제1 통화 사용 트랜잭션 아이디, (ii) 통화 수신자 정보, (iii) 지급 결제 금액, (iv) 상기 특정 사용자의 퍼블릭 키 및 (v) 상기 특정 사용자의 프라이빗 키로 상기 (i), 상기 (ii), 상기 (iii), 상기 (iv)를 서명한 상기 특정 사용자의 서명 값을 포함하는 제2 통화 사용 트랜잭션을 획득하는 통신부: 및 상기 획득된 상기 제2 통화 사용 트랜잭션의 상기 특정 사용자의 밸런스를 참조하여 상기 제2 통화 사용 트랜잭션의 지급 결제 방식을 확인하여, 상기 특정 사용자의 밸런스가 상기 지급 결제 금액 이상이어서 상기 제2 통화 사용 트랜잭션의 지급 결제 방식이 "즉시 지급 결제"로 확인되면, 상기 특정 사용자의 서명 값이 유효한지를 판단하여 유효일 경우, 상기 제2 통화 사용 트랜잭션 또는 상기 제2 통화 사용 트랜잭션에 대한 해쉬 값을 퍼블릭 블록체인 데이터베이스에 등록하거나 등록하도록 지원하고, 상기 퍼블릭 블록체인 데이터베이스에 등록된 상기 제2 통화 사용 트랜잭션 또는 상기 제2 통화 사용 트랜잭션의 해쉬 값의 상기 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 제2 통화 사용 퍼블릭 트랜잭션 아이디를 획득하거나 획득하도록 지원하도록 하는 프로세스, 및 상기 특정 사용자의 밸런스가 상기 지급 결제 금액 미만이어서 상기 제2 통화 사용 트랜잭션의 지급 결제 방식이 "지연 지급 결제"로 확인되면, 상기 특정 사용자의 서명 값이 유효한지를 판단하여 유효일 경우, 상기 제2 통화 사용 트랜잭션을 저장부에 저장한 상태에서, 적어도 하나 이상의 타 사용자에 의해 지급 결제되며 상기 특정 사용자를 수취인으로 하는 적어도 하나 이상의 제3 통화 사용 트랜잭션이 소정의 상계 처리 조건을 만족하면, 상기 제2 통화 사용 트랜잭션과 상기 제3 통화 사용 트랜잭션들을 상계 처리하며, 상계 처리된 상기 제2 통화 사용 트랜잭션 또는 상기 제2 통화 사용 트랜잭션의 해쉬 값과 상기 제3 통화 사용 트랜잭션 또는 상기 제3 통화 사용 트랜잭션의 해쉬 값을 상기 퍼블릭 블록체인 데이터베이스에 등록하거나 등록하도록 지원하며, 상기 퍼블릭 블록체인 데이터베이스에 등록된 상기 제2 통화 사용 트랜잭션 또는 상기 제2 통화 사용 트랜잭션의 해쉬 값과 상기 제3 통화 사용 트랜잭션 또는 상기 제3 통화 사용 트랜잭션의 해쉬 값의 상기 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 제2 통화 사용 퍼블릭 트랜잭션 아이디와 제3 통화 사용 퍼블릭 트랜잭션 아이디를 획득하거나 획득하도록 지원하는 프로세스를 수행하는 프로세서를 포함하는 것을 특징으로 하는 서버가 제공된다.

[18] 이 외에도, 본 발명의 방법을 실행하기 위한 컴퓨터 프로그램을 기록하기 위한 컴퓨터 판독 가능한 기록 매체가 더 제공된다.

발명의 효과

[19] 본 발명에 의하면, 다음과 같은 효과가 있다.

[20] 본 발명은 가상 화폐의 블록체인에 통화의 발행 및 지급 결제 정보를 등록하여 복사 또는 위/변조가 불가능하도록 하여 통화의 발행 및 지급 결제 정보에 대한 신뢰성 및 보안성을 향상시킬 수 있다.

[21] 또한, 본 발명은 통화의 발행 및 지급 결제 정보를 해쉬 함수와 암호화 기술을 이용하여 보안이 보장되고 위/변조가 불가능하도록 하여 통화의 발행 및 지급 결제 정보에 대한 신뢰성 및 보안성을 향상시킬 수 있다.

[22] 또한, 본 발명은 가상 화폐의 블록체인에 통화의 발행 및 지급 결제에 대한 정보를 등록함으로써 통화의 중복 지급 등의 문제점을 미연에 방지할 수 있게 된다.

[23] 또한, 본 발명은 중앙은행과 시중은행 간의 정산 절차를 진행하지 않아도 항상 정산된 최신의 정산 정보를 확인할 수 함으로써 사용자들의 편의성을 향상시킬 수 있다.

도면의 간단한 설명

[24] 도 1은 본 발명의 일 실시예에 따라 통화를 발행하는 서버를 개략적으로 도시한 것이고,

[25] 도 2는 본 발명의 일 실시예에 따라 통화를 발행하는 방법을 개략적으로 도시한 것이고,

[26] 도 3은 본 발명의 일 실시예에 따른 통화를 발행하는 방법에서 통화를 발행하는 통화 발행자를 등록하는 방법을 개략적으로 도시한 것이고,

[27] 도 4A는 본 발명의 일 실시예에 따라 통화를 즉시 지급 결제하는 방법을 개략적으로 도시한 것이고,

[28] 도 4B는 본 발명의 일 실시예에 따라 통화를 지연 지급 결제하는 방법을 개략적으로 도시한 것이다.

발명의 실시를 위한 형태

[29] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 당 업자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의 다양한 실시예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시예에 관련하여 본 발명의 정신 및 범위를 벗어나지 않으면서 다른 실시예로 구현될 수 있다. 또한, 각각의 개시된 실시예 내의 개별 구성요소의 위치 또는 배치는 본 발명의 정신 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 본 발명의 범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다. 도면에서 유사한 참조부호는 여러

측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다.

[30] 이하, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있도록 하기 위하여, 본 발명의 바람직한 실시예들에 관하여 첨부된 도면을 참조하여 상세히 설명하기로 한다.

[31] 또한, 본 명세서에서 "특정"이라는 단어로 제한되는 단어는 행위의 주요 주체와 관련된 개념이고, "관련"이라는 단어로 제한되는 단어는 상기 주요 주체 이외의 다른 주체와 연관된 개념이며, 이하 상세설명에서는 문맥에 의해 각 개념의 구별이 가능하므로 "특정"과 "관련"은 편의상 생략될 수 있다. 다만, 청구항에서는 "특정" 및 "관련"을 삽입하여 의미가 명확히 이해되도록 하였다.

[32] 도 1은 본 발명의 일 실시예에 따라 통화를 발행하는 서버를 개략적으로 도시한 것으로, 서버(100)는 통신부(110)와 프로세서(120)를 포함할 수 있다. 동일한 참조 부호를 이용하여 나타낸 것은 설명의 편의를 위한 것일 뿐, 이들 개별 장치들이 동일하다는 의미로 의도된 것은 아니다. 그리고, 본 발명의 다른 실시예에서의 방법은 서버를 상이하게 구성하여 해당 방법을 수행하거나 동일한 서버(100)를 통해 해당 방법을 수행할 수도 있다.

[33] 구체적으로, 서버(100)는 전형적으로 컴퓨팅 장치(예컨대, 컴퓨터 프로세서, 메모리, 스토리지, 입력 장치 및 출력 장치, 기타 기존의 컴퓨팅 장치의 구성요소들을 포함할 수 있는 장치; 라우터, 스위치 등과 같은 전자 통신 장치; 네트워크 부착 스토리지(NAS) 및 스토리지 영역 네트워크(SAN)와 같은 전자 정보 스토리지 시스템과 컴퓨터 소프트웨어(즉, 컴퓨팅 장치로 하여금 특정의 방식으로 기능하게 하는 인스트럭션들)의 조합을 이용하여 원하는 시스템 성능을 달성하는 것일 수 있다.

[34] 이와 같은 컴퓨팅 장치의 통신부(110)는 연동되는 타 컴퓨팅 장치와 요청과 응답을 송수신할 수 있는 바, 일 예시로서 그러한 요청과 응답은 동일한 TCP 세션에 의하여 이루어질 수 있지만, 이에 한정되지는 않는바, 예컨대 UDP 데이터그램으로서 송수신될 수도 있을 것이다.

[35] 또한, 컴퓨팅 장치의 프로세서(120)는 MPU(Micro Processing Unit) 또는 CPU(Central Processing Unit), 캐쉬 메모리(Cache Memory), 데이터 버스(Data Bus) 등의 하드웨어 구성을 포함할 수 있다. 또한, 운영체제, 특정 목적을 수행하는 애플리케이션의 소프트웨어 구성을 더 포함할 수도 있다.

[36] 먼저, 도 2를 참조하여 본 발명의 일 실시예에 따른 통화를 발행하는 방법을 도 1의 서버를 통해 설명하면 다음과 같다.

[37] 특정 국가의 중앙은행이나 특정 단체의 통화 관리 주체 등을 포함하는 통화 발행자(A)가 통화를 발행하기 위하여 통화 발행 트랜잭션(TrxA)을 단말을 통해 생성하여 전송하면(S100), 서버(100)는 통신부(110)를 통해 통화 발행 트랜잭션(TrxA)를 획득하게 된다.

[38] 이때, 통화 발행 트랜잭션(TrxA)은 (i) 통화의 수신자 정보, (ii) 통화의 발행량, (iii) 통화 발행자의 퍼블릭 키(public key) 및 (iv) 통화 발행자의 프라이빗

키(private key)로 (i) 통화의 수신자 정보, (ii) 통화의 발행량, (iii) 통화 발행자의 퍼블릭 키를 서명한 통화 발행자의 서명 값을 포함할 수 있다. 그리고, 통화의 수신자 정보는 발행되는 통화의 수신자에 대한 정보로 통화 사용자로 등록된 특정 사용자의 퍼블릭 키 일 수 있으며, 통화 수신자의 퍼블릭 키와 통화 발행자의 퍼블릭 키는 사전에 서버(100)에 등록된 것이거나, 필요에 따라 해당 시점에 서버(100)에 등록할 수도 있으며, 등록 정보는 프라이빗 키와 퍼블릭 키를 가진 발행자 또는 사용자가 자신의 퍼블릭 키를 서버(100)에 등록한 것으로, 이에 대한 설명은 다른 동작에서 설명한다. 또한, 통화 발행자(A)는 통화 수신자(B)에 대한 정보로서 통화 수신자(B)의 퍼블릭 키를 사전에 가지고 있을 수 있다.

[39] 그리고, 일 예로, 통화 발행 트랜잭션(TrxA)은 1. 지급 결제 방식, 2. 이전의 트랜잭션 아이디, 3. 수신자, 4. 발행 금액, 5. 발행자 퍼블릭 키, 6. 발행자 서명 값의 데이터 포맷을 가질 수 있으나, 반드시 이에 한정되는 것은 아니다.

[40] 이때, 상기 "1. 결제 방식"은 "즉시 지급 결제"와 "지연 지급 결제"를 포함할 수 있으며, "즉시 지급 결제"는 통화 관련 트랜잭션을 바로 처리하도록 하는 것이고 "지연 지급 결제"는 소정의 조건이 만족할 때까지 통화 관련 트랜잭션의 처리를 지연하는 것일 수 있다. 일 예로, "지연 지급 결제"는 지급을 위한 금액이 부족할 경우 유동성 문제를 해결하기 위하여 자신의 밸런스보다 많은 금액에 대한 지급 결제를 할 경우 이후 자신이 수취하는 금액들과 상계 처리할 수 있도록 하는 것이다. 하지만, 통화의 발행자는 새로운 통화를 발생시키는 기관 또는 이에 준하는 당사자이므로 통화의 발행에서는 "지연 지급 결제"가 발생되지 않으므로 "즉시 지급 결제"가 디폴트로 설정되거나, 통화 발행 트랜잭션에 지급 결제 방식에 대한 데이터 포맷을 포함하지 않도록 할 수도 있다. 그리고, 상기 "2. 이전의 트랜잭션 아이디"는 해당 발행자 또는 사용자의 밸런스에 대한 정보를 포함하는 것으로 통화와 관련하여 이전에 생성 또는 거래된 트랜잭션이 등록된 프라이빗 블록체인 데이터베이스 또는 퍼블릭 블록체인 데이터베이스 상위 위치 정보를 나타내는 프라이빗 트랜잭션 아이디 또는 퍼블릭 트랜잭션 아이디로, 통화의 발행에서는 새로운 통화의 생성이므로 이전의 트랜잭션 아이디는 없을 수 있다. 또한, 상기 "3. 수신자"는 발행되는 통화를 수신할 통화 수신자의 퍼블릭 키(PubB)일 수 있으며, 상기 "4. 발행 금액"은 발행하고자 하는 통화량일 수 있으며, 상기 "5. 발행자 퍼블릭 키"는 발행자가 등록한 퍼블릭 키(PubA)일 수 있으며, 상기 "6. 발행자 서명값"은 통화 발행자가 프라이빗 키로 서명한 1, 2, 3, 4, 5의 서명값(SignPrivA(1, 2, 3, 4, 5))일 수 있다.

[41] 그러면, 서버(100)의 프로세서(120)는 통신부(110)를 통해 획득된 (i) 통화 수신자 정보, (ii) 통화의 발행량, (iii) 통화 발행자의 퍼블릭 키 및 (iv) 통화 발행자의 서명 값을 포함하는 통화 발행 트랜잭션(TrxA)와 통화 발행자의 유효 여부를 확인한다(S110). 이때, 서버(100)의 프로세서(120)는 통화 발행 트랜잭션(TrxA)의 데이터 포맷의 유효 여부, 통화 수신자의 유효 여부, 통화 발행자의 퍼블릭 키의 유효 여부 및 통화 발행자의 서명 값의 유효 여부를

확인하여 통화 발행 트랜잭션(TrxA)의 유효 여부를 확인하게 된다. 일 예로, 통화 발행자(A)의 서명 값에 대해 통화 발행자의 퍼블릭 키를 사용하여 획득한 통화 수신자, 통화 발행자의 퍼블릭 키가 통화 발행 트랜잭션(TrxA)에 포함된 값과 일치하는 지를 확인하여 통화 수신자 및 통화 발행자의 퍼블릭 키에 대한 유효 여부를 확인할 수 있다. 또한, 통화 발행자의 서명 값을 통화 발행자의 퍼블릭 키를 사용하여 검증함으로써 통화 발행자의 서명 값에 대한 유효 여부를 확인할 수 있을 뿐만 아니라, 통화 발행자의 퍼블릭 키를 통해 유효한 통화 발행자인지를 확인할 수 있다.

[42] 그리고, 서버(100)는 확인 결과(S110) 유효한 것으로 판단되면(S210), (i) 통화 수신자 정보, (ii) 통화의 발행량, (iii) 통화 발행자의 퍼블릭 키 및 (iv) 통화 발행자의 서명 값을 포함하는 통화 발행 트랜잭션(TrxA)을 프라이빗 블록체인 데이터베이스에 등록하거나 등록하도록 지원하고(S211), 프라이빗 블록체인 데이터베이스에 등록된 통화 발행 트랜잭션(TrxA)의 프라이빗 블록체인 데이터베이스 상의 위치 정보를 나타내는 통화 발행 프라이빗 트랜잭션 아이디(PrivTxid)를 통화 발행자(A) 및 통화 수신자(B) 중 적어도 일부에게 제공하거나 제공하도록 지원할 수 있다(S212, S213). 하지만, 서버(100)는 확인 결과(S110) 유효가 아니면(S220), 통화 발행자(A)에게 에러 메시지를 포함하는 실패를 나타내는 응답을 제공하거나 제공하도록 지원할 수 있다(S221). 다만, 본 발명은 아래에서 언급할 퍼블릭 블록체인 데이터베이스(200)에 등록하는 것이 필수적인 것이고 프라이빗 블록체인 데이터베이스에 등록하는 것이 필수적인 것은 아닐 수도 있을 것이다.

[43] 한편, 서버(100)는 유효한 확인 결과에 대응하여, (i) 통화 수신자 정보, (ii) 통화의 발행량, (iii) 통화 발행자의 퍼블릭 키 및 (iv) 통화 발행자의 서명 값을 포함하는 통화 발행 트랜잭션(TrxA)에 해쉬 함수를 적용하여 생성한 해쉬 값(hash(TrxA))을 퍼블릭 블록체인 데이터베이스(200)에 등록하거나 등록하도록 지원한다(S214). 이때, 해쉬 값 생성을 위한 해쉬 함수는 MD4 함수, MD5 함수, SHA-0 함수, SHA-1 함수, SHA-224 함수, SHA-256 함수, SHA-384 함수, SHA-512 함수 및 HAS-160 함수를 포함할 수 있으나, 이에 한정되지 않음은 통상의 기술자가 알 수 있을 것이다. 예를 들어 Triple SHA256도 가능할 것이다.

[44] 이후, 서버(100)는 퍼블릭 블록체인 데이터베이스(200)에 등록된 해쉬 값의 퍼블릭 블록체인 데이터베이스(200) 상의 위치 정보를 나타내는 통화 발행 퍼블릭 트랜잭션 아이디(PubTxid)를 획득하거나 획득하도록 지원할 수 있다(S215). 또한, 서버(100)는 통화 발행 퍼블릭 트랜잭션 아이디(PubTxid)에 대응되는 OP 메시지를 퍼블릭 블록체인 데이터베이스(200)로부터 획득할 수 있다.

[45] 앞서 언급하였듯이, 상기에서는 서버(100)가 통화 발행 트랜잭션을 프라이빗 블록체인 데이터베이스와 퍼블릭 블록체인 데이터베이스를 이용하여 등록하였지만, 퍼블릭 블록체인 데이터베이스만을 이용하는 경우도 상정할

수도 있다.

[46] 즉, 통화 발행 트랜잭션(TrxA)과 통화 발행자(A)가 유효일 경우, 서버(100)는 (i) 통화 수신자 정보, (ii) 통화의 발행량, (iii) 통화 발행자의 퍼블릭 키 및 (iv) 통화 발행자의 서명값을 포함하는 통화 발행 트랜잭션(TrxA) 또는 통화 발행 트랜잭션에 대한 해쉬값(hash(TrxA))을 퍼블릭 블록체인 데이터베이스(200)에 등록하거나 등록하도록 지원하고, 퍼블릭 블록체인 데이터베이스(200)에 등록된 통화 발행 트랜잭션(TrxA) 또는 통화 발행 트랜잭션에 대한 해쉬값(hash(TrxA))의 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 통화 발행 퍼블릭 트랜잭션 아이디(PubTxid)를 획득하거나 획득하도록 지원할 수도 있다. 그리고, 서버(100)는 획득된 통화 발행 퍼블릭 트랜잭션 아이디를 통화 발행자(A) 및 통화 수신자(B) 중 적어도 일부에게 제공하거나 제공하도록 지원할 수 있다.

[47] 다음으로, 도 3을 참조하여 통화 발행자(A)를 등록하는 과정을 설명하면 다음과 같다.

[48] 통화 발행자(A)의 퍼블릭 키(PubA)에 의한 발행자 등록 요청이 획득되면(S300), 서버(100)는, 통화 발행자(A)의 유효 여부를 확인하여 통화 발행자(A)가 유효할 경우(S310), 랜덤 논스(random nonce)(RN)를 통화 발행자(A)에게 전달하거나 전달하도록 지원할 수 있다(S311). 그리고, 통화 발행자(A)가 유효하지 않을 경우(S320), 일 예로 타인의 명의를 도용한 사람일 경우, 서버(100)는 통화 발행자(A)에게 발행자 확인 실패를 나타내는 응답을 제공하거나 제공하도록 지원할 수 있다(S321). 다만, 발행자(A)가 유효한지 판단하기 위한 방법은 이에 한정되지 않으며, 가령 타임스탬프 등을 이용하여 발행자(A)의 유효성을 판단할 수도 있을 것이다. 참고로, 아래에서는 랜덤 논스를 이용하여 유효성을 판단하는 것으로 예를 들어 설명한다.

[49] 통화 발행자(A)가 단말에서 프라이빗 키(PrivA)와 퍼블릭 키(PubA)를 생성한 상태에서, 통화를 발행하기 위한 발행자로 등록하기 위하여 퍼블릭 키(PubA)를 서버(100)로 전송하면, 서버(100)는 획득되는 퍼블릭 키의 통화 발행자(A)가 유효한지를 확인한다. 이때, 통화 발행자(A)의 유효 여부는 공개 키 기반(PKI: Public Key Infrastructure) 인증서를 이용하거나 통화 발행자(A)의 신분 증명 정보를 이용할 수 있으나, 이에 한정되는 것은 아니다. 일 예로, 공개 키 기반 인증서인 공인인증서, OPSign 인증서 등을 통해 특정 발행자를 확인하거나, 주민번호, 여권, 법인 등록 번호, 사업자 등록 번호 등과 같이 개인, 은행 또는 단체의 신분을 증명할 수 있는 신분 증명 정보를 통해 통화 발행자를 확인할 수 있다.

[50] 이후, 랜덤 논스(RN)를 통화 발행자(A)의 프라이빗 키로 서명한 랜덤 논스 서명값(SignPrivA(RN))이 획득되면(S312), 서버(100)는, 랜덤 논스 서명 값이 유효한 서명 값인지를 통화 발행자(A)의 퍼블릭 키를 사용하여 검증한다. 즉, 서버(100)는 통화 발행자의 퍼블릭 키를 사용하여 랜덤 논스 서명 값으로부터 랜덤 논스(RN)를 확인하고, 확인된 랜덤 논스(RN)가 통화 발행자에게 전달된

랜덤 논스(RN)와 일치하는지를 확인하여 일치할 경우 유효한 서명인 것으로 검증한다.

[51] 그리고, 서버(100)는 통화 발행자(A)로부터 획득된 서명 값이 유효한 것일 경우(S330), 랜덤 논스, 랜덤 논스 서명 값 및 통화 발행자의 퍼블릭 키를 포함하는 발행자 등록 트랜잭션(RN, SignPrivA(RN), PubA)을 프라이빗 블록체인 데이터베이스에 등록하거나 등록하도록 지원하며(S331), 프라이빗 블록체인 데이터베이스에 등록된 발행자 등록 트랜잭션의 프라이빗 블록체인 데이터베이스 상의 위치 정보를 나타내는 발행자 등록 프라이빗 트랜잭션 아이디(PrivTxid)를 포함하는 등록이 성공했음을 나타내는 응답을 통화 발행자(A)에게 제공하거나 제공하도록 지원할 수 있다(S332).

[52] 그러나, 서버(100)는 통화 발행자(A)로부터 획득된 서명 값이 유효하지 않을 경우, 통화 발행자(A)에게 서명 값 확인 실패를 나타내는 메시지를 포함하는 응답을 제공하거나 제공하도록 지원할 수 있다(S341).

[53] 또한, 서버(100)는 통화 발행자의 서명 값이 유효한 경우, 랜덤 논스, 랜덤 논스 서명 값 및 통화 발행자의 퍼블릭 키에 대한 해쉬 값(hash(RN, SignPrivA(RN), PubA))을 퍼블릭 블록체인 데이터베이스(200)에 등록하거나 등록하도록 지원하고(S333), 퍼블릭 블록체인 데이터베이스(200)에 등록된 해쉬 값의 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 발행자 등록 트랜잭션 아이디(PubTxid)를 획득하거나 획득하도록 지원할 수 있다(S334).

[54] 상기에서는 서버(100)가 통화 발행자(A)의 발행자 등록 트랜잭션을 프라이빗 블록체인 데이터베이스와 퍼블릭 블록체인 데이터베이스를 이용하여 등록하였지만, 이와는 달리 퍼블릭 블록체인 데이터베이스만을 이용할 수도 있다.

[55] 즉, 서버(100)는 통화 발행자의 서명 값이 유효한 경우, 랜덤 논스, 랜덤 논스 서명 값 및 통화 발행자의 퍼블릭 키를 포함하는 발행자 등록 트랜잭션(RN, SignPrivA(RN), PubA) 또는 발행자 등록 트랜잭션에 대한 해쉬 값(hash(RN, SignPrivA(RN), PubA))을 퍼블릭 블록체인 데이터베이스(200)에 등록하거나 등록하도록 지원하고(S333), 퍼블릭 블록체인 데이터베이스(200)에 등록된 발행자 등록 트랜잭션 또는 발행자 등록 트랜잭션에 대한 해쉬 값의 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 발행자 등록 퍼블릭 트랜잭션 아이디(PubTxid)를 획득하거나 획득하도록 지원할 수 있다. 그리고, 서버(100)는 획득된 발행자 등록 퍼블릭 트랜잭션 아이디를 통화 발행자(A)에게 제공하거나 제공하도록 지원할 수 있다.

[56] 다음으로, 도 4A와 4B를 참조하여 본 발명의 일 실시예에 따른 통화의 지급을 결제하는 방법을 설명하면 다음과 같다. 다음의 설명에서 도 2의 본 발명의 일 실시예에 따른 통화를 발행하는 방법에서와 유사한 부분은 도 2의 설명으로부터 이해 가능하므로 상세한 설명을 생략한다.

[57] 통화의 지급을 결제하기 위하여, 특정 사용자(C)로부터 통화의 지급 결제를

위한 제2 통화 사용 트랜잭션(TrxC)이 특정 사용자(C)의 단말로부터 송신되면 서버(100)는 이를 통신부(110)를 통해 수신한다(S400).

[58] 이때, 제2 통화 사용 트랜잭션(TrxC)은 (i) 이전에 적어도 일부 미 사용된 적어도 하나 이상의 제1 통화 사용 트랜잭션 아이디, (ii) 통화 수신자 정보, (iii) 지급 결제 금액, (iv) 특정 사용자의 퍼블릭 키 및 (v) 특정 사용자의 프라이빗 키로 (i) 이전에 적어도 일부 미 사용된 적어도 하나 이상의 제1 통화 사용 트랜잭션 아이디, (ii) 통화 수신자 정보, (iii) 지급 결제 금액, (iv) 특정 사용자의 퍼블릭 키를 서명한 특정 사용자의 서명 값을 포함할 수 있다. 그리고, 이전에 적어도 일부 미 사용된 적어도 하나 이상의 제1 통화 사용 트랜잭션 아이디는 통화 발행자나 타 사용자들로부터 특정 사용자가 수취한 지급 결제에 대하여 사용 금액이 남은 통화 관련 트랜잭션으로, 특정 사용자(c)가 소유한 모든 제1 통화 사용 트랜잭션의 미사용 금액을 합한 금액은 특정 사용자의 현재 밸런스일 수 있다. 그리고, 통화 수신자 정보는 지급 결제되는 통화의 수신자에 대한 정보로 통화 사용자로 등록된 사용자들 중 지급 결제되는 통화를 수취하는 통화 수신자의 퍼블릭 키 일 수 있으며, 통화 수신자의 퍼블릭 키와 특정 사용자(C)의 퍼블릭 키는 사전에 서버(100)에 등록된 것이거나, 필요에 따라 해당 시점에 서버(100)에 등록할 수도 있으며, 등록 정보는 프라이빗 키와 퍼블릭 키를 가진 발행자 또는 사용자가 자신의 퍼블릭 키를 서버(100)에 등록한 것으로, 이에 대한 설명은 다른 동작에서 설명한다. 또한, 특정 사용자(C)는 통화 수신자에 대한 정보로서 통화 수신자의 퍼블릭 키를 사전에 가지고 있을 수 있다.

[59] 그리고, 일 예로, 제2 통화 사용 트랜잭션(TrxC)은 1. 지급 결제 방식, 2. 제1 통화 사용 트랜잭션 아이디, 3. 수신자, 4. 사용 금액, 5. 잔금, 6. 잔금 소유자 정보, 7. 특정 사용자의 퍼블릭 키, 8. 특정 사용자의 서명 값을 포함하는 데이터 포맷을 가질 수 있다.

[60] 이때, “1. 결제 방식”은 “즉시 지급 결제”와 “지연 지급 결제”를 포함할 수 있으며, “즉시 지급 결제”는 통화 관련 트랜잭션을 바로 처리하도록 하는 것이고 “지연 지급 결제”는 소정의 조건이 만족할 때까지 통화 관련 트랜잭션의 처리를 지연하는 것일 수 있다. 일 예로, “지연 지급 결제”는 지급을 위한 금액이 부족할 경우 유동성 문제를 해결하기 위하여 자신의 밸런스보다 많은 금액에 대한 지급 결제를 할 경우 이후 자신이 수취하는 금액들과 상계 처리할 수 있도록 하는 것이다. 그리고, “2. 제1 통화 사용 트랜잭션 아이디”는 특정 사용자(C)의 밸런스에 대한 정보를 포함하는 것으로 통화와 관련하여 이전에 수취한 통화 사용 트랜잭션이 등록된 프라이빗 블록체인 데이터베이스 또는 퍼블릭 블록체인 데이터베이스 상위 위치 정보를 나타내는 프라이빗 트랜잭션 아이디 또는 퍼블릭 트랜잭션 아이디로, 통화의 발행자 또는 타 사용자들로부터 지급 결제 받은 통화 사용 트랜잭션 및 일부 미 사용된 금액을 포함하는 통화 사용 트랜잭션의 정보에 관한 것일 수 있으며, 특정 사용자(C)가 소유한 모든 제1 통화 사용 트랜잭션의 잔금을 합한 금액은 현재 특정 사용자(C)가 소유한 밸런스가 될

수 있다. 또한, "3. 수신자"는 지급 결제되는 통화를 수취할 통화 수신자의 퍼블릭 키(PubB)일 수 있으며, "4. 사용 금액"은 지급 결제하고자 하는 금액일 수 있으며, "5. 잔금"은 특정 사용자(C)의 밸런스에서 지급 결제 이후 남는 금액으로 지급 결제에 의해 잔금이 없거나 부(-)의 값을 가질 수도 있으며, "6. 잔금 소유자 정보"는 "5. 잔금"에 대한 소유자 정보로 본 실시예에서는 특정 사용자(C)의 퍼블릭 키로 잔금이 없을 경우 정보가 없을 수도 있으며, "7. 특정 사용자의 퍼블릭 키"는 지금 결제를 하려고 하는 특정 사용자(C)의 퍼블릭 키일 수 있으며, "8. 특정 사용자의 서명 값"은 특정 사용자(C)가 프라이빗 키로 서명한 1, 2, 3, 4, 5, 6, 7의 서명 값(SignPrivC(1, 2, 3, 4, 5, 6, 7))일 수 있다.

[61] 그러면, 서버(100)는 특정 사용자(C)의 밸런스를 참조하여 제2 통화 사용 트랜잭션의 지급 결제 방식을 확인한다. 이때, 특정 사용자(C)가 소유한 밸런스가 지급 결제 금액 이상이면 "즉시 지급 결제"로 확인하며, 특정 사용자(C)가 소유한 밸런스가 지급 결제 금액 미만이면 "지연 지급 결제"로 확인할 수 있다. 또한, 제2 통화 사용 트랜잭션에 포함된 지급 결제 방식에 따라 "즉시 지급 결제"와 "지연 지급 결제"로 확인할 수 있으며, 특히 제2 통화 사용 트랜잭션에 포함된 지급 결제 방식에는 "즉시 지급 결제"로 입력되었지만 특정 사용자(C)가 소유한 밸런스가 지급 결제 미만일 경우에는 "지연 지급 결제"로 판단할 수 있다.

[62] 이때, 제2 통화 사용 트랜잭션(TrxC)가 "즉시 지급 결제"로 확인되면(S410), 서버(100)는 제2 통화 사용 트랜잭션(TrxC)의 특정 사용자(C)의 서명 값이 유효한지를 판단하여 유효일 경우(S430), 제2 통화 사용 트랜잭션(TrxC)을 프라이빗 블록체인 데이터베이스에 등록하고(S431), 프라이빗 블록체인 데이터베이스에 등록된 제2 통화 사용 트랜잭션(TrxC)의 프라이빗 블록체인 데이터베이스 상의 위치 정보를 나타내는 제2 통화 사용 프라이빗 트랜잭션 아이디(PrivTxid)를 특정 사용자(C) 및 통화 수신자 중 적어도 일부에게 제공하거나 제공하도록 지원할 수 있다(S432). 하지만, 서버(100)는 확인 결과 유효한 서명 값이 아니면(S440), 특정 사용자(C)에게 에러 메시지를 포함하는 실패를 나타내는 응답을 제공하거나 제공하도록 지원할 수 있다(S441).

[63] 또한, 서버(100)는 유효한 확인 결과에 대응하여, 제2 통화 사용 트랜잭션(TrxC)의 해쉬 값(hash(TrxC))을 퍼블릭 블록체인 데이터베이스(200)에 등록하거나 등록하도록 지원할 수 있다(S433). 이후, 서버(100)는 퍼블릭 블록체인 데이터베이스(200)에 등록된 해쉬 값의 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 제2 통화 사용 퍼블릭 트랜잭션 아이디(PubTxid)를 획득하거나 획득하도록 지원할 수 있다(S434). 그리고, 서버(100)는 제2 통화 사용 퍼블릭 트랜잭션 아이디(PubTxid)에 대응되는 OP 메시지를 퍼블릭 블록체인 데이터베이스(200)로부터 획득할 수도 있다.

[64] 상기에서는 서버(100)가 특정 사용자(C)의 제2 통화 사용 트랜잭션(TrxC)을 프라이빗 블록체인 데이터베이스와 퍼블릭 블록체인 데이터베이스를 이용하여

등록하였지만, 프라이빗 블록체인 데이터베이스를 사용하지 않고 퍼블릭 블록체인 데이터베이스만을 이용할 수도 있다.

[65] 즉, 서버(100)는 지급 결제 방식이 "즉시 지급 결제'이며 특정 사용자(C)의 서명이 유효한 제2 통화 사용 트랜잭션(TrxC) 또는 제2 통화 사용 트랜잭션의 해쉬 값(hash(TrxC))을 퍼블릭 블록체인 데이터베이스(200)에 등록하거나 등록하도록 지원하고, 퍼블릭 블록체인 데이터베이스에 등록된 제2 통화 사용 트랜잭션(TrxC) 또는 제2 통화 사용 트랜잭션의 해쉬 값(hash(TrxC))의 퍼블릭 블록체인 데이터베이스(200) 상의 위치 정보를 나타내는 제2 통화 사용 퍼블릭 트랜잭션 아이디(PubTxid)를 획득하거나 획득하도록 지원할 수 있다. 그리고, 서버(100)는 획득된 제2 통화 사용 퍼블릭 트랜잭션 아이디(PubTxid)를 특정 사용자(C) 및 통화 수신자 중 적어도 일부에게 제공하거나 제공하도록 지원할 수 있다.

[66] 이와는 달리, 제2 통화 사용 트랜잭션(TrxC)가 “지연 지급 결제”로 확인되면(S420), 서버(100)는 제2 통화 사용 트랜잭션(TrxC)의 특정 사용자(C)의 서명 값이 유효한지를 판단하여 유효일 경우(S450), 제2 통화 사용 트랜잭션(TrxC)을 네팅(netting) 데이터베이스, 저장부, 메모리 등의 기록 장치에 저장한다(S451). 하지만, 서버(100)는 확인 결과 유효한 서명 값이 아니면(S460), 특정 사용자(C)에게 에러 메시지를 포함하는 실패를 나타내는 응답을 제공하거나 제공하도록 지원할 수 있다(S461).

[67] 그리고, 제2 통화 사용 트랜잭션(TrxC)을 저장 장치에 저장한 상태에서, 적어도 하나 이상의 타 사용자(D)에 의해 지급 결제되며 특정 사용자(C)를 수취인으로 하는 적어도 하나 이상의 제3 통화 사용 트랜잭션(TrxD)이 획득되면(S452), 서버(100)는 획득되는 제3 통화 사용 트랜잭션(TrxD)과 제2 통화 사용 트랜잭션(TrxC)이 상계 조건을 만족하는 지를 확인한다. 이때, 제3 통화 사용 트랜잭션(TrxD)은 특정 사용자(C)를 수취인으로 하되 '지연 지급 결제"로 저장 장치에 저장된 통화 사용 트랜잭션일 수 있으며, 이 경우 서버(100)는 "지연 지급 결제"로 저장된 제3 통화 사용 트랜잭션(TrxD)이 상계 처리되면 이에 대응하여 제2 통화 사용 트랜잭션(TrxC)에 대한 상계 처리를 수행할 수 있다. 또한, 서버(100)는 상계 조건으로, 제3 통화 사용 트랜잭션(TrxD)이 획득될 경우 상계 처리를 수행하며, 상계 처리에 의해 특정 사용자(C)의 밸런스가 "0" 이상의 값을 가지는 지를 판단한다.

[68] 한편, 획득된 제3 통화 사용 트랜잭션(TrxD)에 의해 상계 조건을 만족하지 않으면(S480), 서버는 획득된 제3 통화 사용 트랜잭션(TrxD)을 기록 매체에 저장하고, 다른 제3 통화 사용 트랜잭션이 획득되기를 기다린다(S481).

[69] 이러한 상태에서, 적어도 하나 이상의 제3 통화 사용 트랜잭션(TrxD)에 의해 상계 조건을 만족하면(S470), 즉, 다수의 제3 통화 사용 트랜잭션(TrxD)에 의해 수취할 금액이 제2 통화 사용 트랜잭션(TrxC)에 의해 지급할 금액보다 많아질 경우 또는 다수의 제3 통화 사용 트랜잭션(TrxD)에 의해 수취할 금액과 제2 특정

사용자(C)의 밸런스의 합산 금액이 제2 통화 사용 트랜잭션(TrxC)에 의해 지급할 금액보다 많아질 경우, 서버(100)는 제2 통화 사용 트랜잭션(TrxC)과 적어도 하나 이상의 제3 통화 사용 트랜잭션(TrxD)을 상계 처리한다. 이때, 다수의 제3 통화 사용 트랜잭션(TrxD)은 특정 타 사용자에 의해 생성된 다수의 통화 트랜잭션, 다수의 타 사용자에 의해 생성된 다수의 통화 트랜잭션, 또는 다수의 타 사용자에 의해 다수로 생성되는 각각의 타 사용자에 의해 다수 개로 생성된 통화 트랜잭션 일 수 있다.

[70] 또한, 특정 사용자(C)와 다수의 타 사용자들이 각각 "지연 지급 결제"로 된 통화 사용 트랜잭션의 지급자인 사용자와 수취인으로 연결되어 순환 고리를 형성할 경우, 서버(100)는 특정 사용자(C)와 다수의 타 사용자들 간의 "지연 지급 결제"로 순환 고리를 형성하며 연결된 모든 통화 사용 트랜잭션을 상계 처리할 수 있다. 물론, "지연 지급 결제"로 확인되는 임의의 통화 사용 트랜잭션이 다른 통화 사용 트랜잭션과의 지급 결제 금액 차이에 의해 상계 조건을 만족하지 않을 경우에는 임의의 통화 사용 트랜잭션의 상계 처리 조건, 즉, 또 다른 통화 사용 트랜잭션에 의해 임의의 통화 사용 트랜잭션이 상계 처리 조건을 만족하면, 서버(100)는 순환 고리를 형성하는 "지연 지급 결제"인 모든 통화 사용 트랙잭션을 상계 처리할 수 있다.

[71] 일 예로, 사용자A는 사용자B에게 "지연 지급 결제"로 통화 사용 트랜잭션A를 생성하며, 사용자B는 사용자C에게 "지연 지급 결제"로 통화 사용 트랜잭션B를 생성하며, 사용자C는 사용자D에게 "지연 지급 결제"로 통화 사용 트랜잭션C를 생성하며, 사용자D는 사용자A에게 "지연 지급 결제"로 통화 사용 트랜잭션D를 생성하여 사용자A, 사용자B, 사용자C, 및 사용자D 사이에 서로 지급자와 수취인으로 하는 순환 고리가 형성될 경우, 서버(100)는 사용자A, 사용자B, 사용자C 및 사용자D에 의해 생성된 통화 사용 트랜잭션A, 통화 사용 트랜잭션B, 통화 사용 트랜잭션C 및 통화 사용 트랜잭션D를 상계 처리할 수 있다. 물론, "지연 지급 결제"인 각각의 통화 사용 트랜잭션에서의 지급 결제 금액이 일치하여야 하는 조건이 만족되어야 하며, 만약 지급 결제 금액들이 일치하지 않을 경우에는 "지연 지급 결제"인 각각의 통화 사용 트랜잭션이 또 다른 통화 사용 트랜잭션에 의해 상계 처리 조건을 만족하여 순화 고리 형태를 이루는 각각의 "지연 지급 결제"인 통화 사용 트랜잭션이 상계 처리 조건을 만족하면 상계 처리를 수행할 수 있다.

[72] 그리고, 서버(100)는 상계 처리된 제2 통화 사용 트랜잭션(TrxC)과 적어도 하나 이상의 제3 통화 사용 트랜잭션(TrxD)을 프라이빗 블록체인 데이터베이스에 등록하거나 등록하도록 지원하며(S471), 프라이빗 블록체인 데이터베이스에 등록된 제2 통화 사용 트랜잭션(TrxC)과 적어도 하나 이상의 제3 통화 사용 트랜잭션(TrxD)의 프라이빗 블록체인 데이터베이스 상의 위치 정보를 나타내는 제2 통화 사용 프라이빗 트랜잭션 아이디(PrivTxid)와 제3 통화 사용 프라이빗 트랜잭션 아이디(PrivTxid)를 특정 사용자(C), 통화 수신자, 및 적어도 하나

이상의 타 사용자(D) 중 적어도 일부에게 제공하거나 제공하도록 지원할 수 있다(S472, S473). 이때, 기록 매체에 저장된 정보, 즉, 제2 통화 사용 트랜잭션(TrxC)과 획득된 적어도 하나 이상의 제3 통화 사용 트랜잭션(TrxD)은 삭제할 수 있다.

[73] 또한, 서버(100)는 상계 처리된 제2 통화 사용 트랜잭션(TrxC)의 해쉬값(hash(TrxC))과 적어도 하나 이상의 제3 통화 사용 트랜잭션(TrxD) 각각의 해쉬값(hash(TrxD))을 퍼블릭 블록체인 데이터베이스(200)에 등록하거나 등록하도록 지원할 수 있다(S474). 즉, 서버(100)는 상계 처리된 모든 통화 사용 트랜잭션에 대한 정보를 퍼블릭 블록체인 데이터베이스(200)에 등록하거나 등록하도록 지원할 수 있다. 이후, 서버(100)는 퍼블릭 블록체인 데이터베이스(200)에 등록된 해쉬값(hash(TrxC), hash(TrxD))의 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 제2 통화 사용 퍼블릭 트랜잭션 아이디(Txid)와 적어도 하나 이상의 제3 통화 사용 퍼블릭 트랜잭션 아이디(Txid)를 획득하거나 획득하도록 지원할 수 있다(S475). 그리고, 서버(100)는 제2 통화 사용 퍼블릭 트랜잭션 아이디(Txid)와 적어도 하나 이상의 제3 통화 사용 퍼블릭 트랜잭션 아이디(Txid)에 각각 대응되는 OP 메시지를 퍼블릭 블록체인 데이터베이스(200)로부터 획득할 수 있다.

[74] 상기에서는 서버(100)가 상계 처리된 특정 사용자(C)의 제2 통화 사용 트랜잭션(TrxC)과 타 사용자(D)의 제3 통화 사용 트랜잭션(TrxD)을 프라이빗 블록체인 데이터베이스와 퍼블릭 블록체인 데이터베이스를 이용하여 등록하였지만, 이와는 달리 퍼블릭 블록체인 데이터베이스만을 이용할 수도 있다.

[75] 즉, 서버(100)는 상계 처리된 제2 통화 사용 트랜잭션(TrxC) 또는 제2 통화 사용 트랜잭션의 해쉬값(hash(TrxC))과 적어도 하나 이상의 제3 통화 사용 트랜잭션(TrxD) 또는 제3 통화 사용 트랜잭션의 해쉬값(hash(TrxD))을 퍼블릭 블록체인 데이터베이스(200)에 등록하거나 등록하도록 지원하고, 퍼블릭 블록체인 데이터베이스에 등록된 제2 통화 사용 트랜잭션(TrxC) 또는 제2 통화 사용 트랜잭션의 해쉬값(hash(TrxC))과 제3 통화 사용 트랜잭션(TrxD) 또는 제3 통화 사용 트랜잭션의 해쉬값(hash(TrxD))의 퍼블릭 블록체인 데이터베이스(200) 상위 위치 정보를 나타내는 제2 통화 사용 퍼블릭 트랜잭션 아이디(Txid)와 제3 통화 사용 퍼블릭 트랜잭션 아이디(Txid)를 획득하거나 획득하도록 지원할 수 있다. 그리고, 서버(100)는 획득된 제2 통화 사용 퍼블릭 트랜잭션 아이디(Txid)와 제3 통화 사용 퍼블릭 트랜잭션 아이디(Txid)를 특정 사용자(C), 통화 수신자 및 적어도 하나 이상의 타 사용자(D) 중 적어도 일부에게 제공하거나 제공하도록 지원할 수 있다.

[76] 그리고, 서버(100)가 통화 사용자인 특정 사용자를 등록하는 과정을 설명하면 다음과 같다. 특정 사용자의 등록 또한 도 3에서의 통화 발행자의 등록과 같은 방법을 수행하는 것으로 유사한 부분은 도 3에서의 설명으로 이해 가능하므로

생략한다.

[77] 특정 사용자(C)의 퍼블릭 키에 의한 사용자 등록 요청이 획득되면, 서버(100)는, 특정 사용자(C)의 유효 여부를 확인하여 특정 사용자(C)가 유효할 경우 랜덤 논스를 특정 사용자(C)에게 전달하거나 전달하도록 지원할 수 있다. 그리고, 특정 사용자(C)가 유효하지 않을 경우, 서버(100)는 특정 사용자(C)에게 사용자 확인 실패를 나타내는 응답을 제공하거나 제공하도록 지원할 수 있다.

[78] 한편, 유효한 사용자일 경우, 랜덤 논스를 특정 사용자의 프라이빗 키로 서명한 랜덤 논스 서명값이 획득되면, 서버(100)는, 랜덤 논스 서명값이 정상적으로 서명되었는지를 특정 사용자의 퍼블릭 키를 사용하여 검증한다.

[79] 그리고, 서버(100)는 특정 사용자(C)로부터 획득된 서명값이 유효한 것일 경우, 랜덤 논스, 랜덤 논스 서명값 및 특정 사용자의 퍼블릭 키를 포함하는 사용자 등록 트랜잭션을 프라이빗 블록체인 데이터베이스에 등록하거나 등록하도록 지원하고, 프라이빗 블록체인 데이터베이스에 등록된 사용자 등록 트랜잭션의 프라이빗 블록체인 데이터베이스 상의 위치 정보를 나타내는 사용자 등록 프라이빗 트랜잭션 아이디(PrivTxid)를 특정 사용자(C)에게 제공하거나 제공하도록 지원할 수 있다.

[80] 그러나, 서버(100)는 특정 사용자(C)로부터 획득된 서명값이 유효하지 않을 경우, 특정 사용자(111)에게 서명값 확인 실패를 나타내는 응답을 제공하거나 제공하도록 지원할 수 있다.

[81] 또한, 서버(100)는 특정 사용자(C)의 서명값이 유효한 경우, 랜덤 논스, 랜덤 논스 서명값 및 특정 사용자의 퍼블릭 키에 대한 해쉬값을 퍼블릭 블록체인 데이터베이스에 등록하거나 등록되도록 지원하고, 퍼블릭 블록체인 데이터베이스에 등록된 해쉬값의 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 사용자 등록 퍼블릭 트랜잭션 아이디(Txid)를 획득하거나 획득하도록 지원할 수 있다.

[82] 상기에서는 서버(100)가 특정 사용자의 사용자 등록 트랜잭션을 프라이빗 블록체인 데이터베이스와 퍼블릭 블록체인 데이터베이스를 이용하여 등록하였지만, 이와는 달리 퍼블릭 블록체인 데이터베이스만을 이용할 수도 있다.

[83] 즉, 서버(100)는 특정 사용자와 서명값이 유효할 경우, 사용자 등록 트랜잭션 또는 사용자 등록 트랜잭션의 해쉬값을 퍼블릭 블록체인 데이터베이스에 등록하거나 등록하도록 지원하고, 퍼블릭 블록체인 데이터베이스 상의 해쉬값의 등록 위치 정보를 나타내는 사용자 등록 퍼블릭 트랜잭션 아이디(Txid)를 획득하거나 획득하도록 지원할 수 있다. 그리고, 획득된 사용자 등록 퍼블릭 트랜잭션 아이디(Txid)를 특정 사용자에게 전송하거나 전송하도록 지원할 수 있다.

[84] 한편, 상기에서 설명한 통화 수신자(B), 통화 사용자(C), 통화 사용자(D)는 시중 은행일 수도 있으며, 일반 개인일 수도 있을 것이다.

[85] 또한, 이상 설명된 본 발명에 따른 실시예들은 다양한 컴퓨터 구성요소를 통하여 수행될 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 것들이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 상기 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[86] 이상에서 본 발명이 구체적인 구성요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나, 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명이 상기 실시예들에 한정되는 것은 아니며, 본 발명이 속하는 기술분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형을 꾀할 수 있다.

[87] 따라서, 본 발명의 사상은 상기 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등하게 또는 등가적으로 변형된 모든 것들은 본 발명의 사상의 범주에 속한다고 할 것이다.

[88]

청구범위

[청구항 1] 통화를 발행하는 방법에 있어서,

(a) 통화 발행자로부터의 상기 통화 발행을 위한 (i) 통화 수신자 정보, (ii) 상기 통화의 발행량, (iii) 상기 통화 발행자의 퍼블릭 키 및 (iv) 상기 통화 발행자의 프라이빗 키로 상기 (i), 상기 (ii), 상기 (iii)을 서명한 상기 통화 발행자의 서명값을 포함하는 특정 통화 발행 트랜잭션이 획득되면, 서버는, 상기 특정 통화 발행 트랜잭션 및 상기 통화 발행자의 유효 여부를 확인하는 단계; 및

(b) 상기 특정 통화 발행 트랜잭션과 상기 통화 발행자가 유효이면, 상기 서버는, (i) 상기 통화 수신자 정보, (ii) 상기 통화의 발행량, (iii) 상기 통화 발행자의 퍼블릭 키 및 (iv) 상기 통화 발행자의 서명값을 포함하는 상기 특정 통화 발행 트랜잭션 또는 상기 특정 통화 발행 트랜잭션에 대한 해쉬값을 퍼블릭 블록체인 데이터베이스에 등록하거나 상기 서버에 연동된 타 장치로 하여금 상기 퍼블릭 블록체인 데이터베이스에 등록하도록 지원하고, 상기 퍼블릭 블록체인 데이터베이스에 등록된 상기 특정 통화 발행 트랜잭션 또는 상기 특정 통화 발행 트랜잭션에 대한 해쉬값의 상기 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 특정 통화 발행 퍼블릭 트랜잭션 아이디를 획득하거나 상기 타 장치로 하여금 상기 퍼블릭 블록체인 데이터베이스로부터 획득하도록 지원하는 단계;

를 포함하는 것을 특징으로 하는 방법.

[청구항 2] 제1항에 있어서,

상기 (b) 단계에서,

상기 특정 통화 발행 트랜잭션과 상기 통화 발행자가 유효이면, 상기 서버는, (i) 상기 통화 수신자 정보, (ii) 상기 통화의 발행량, (iii) 상기 통화 발행자의 퍼블릭 키 및 (iv) 상기 통화 발행자의 서명값을 포함하는 상기 특정 통화 발행 트랜잭션을 추가적으로 프라이빗 블록체인 데이터베이스에 등록하거나 상기 타 장치로 하여금 상기 프라이빗 블록체인 데이터베이스에 등록하도록 지원하고, 상기 프라이빗 블록체인 데이터베이스에 등록된 상기 특정 통화 발행 트랜잭션의 상기 프라이빗 블록체인 데이터베이스 상의 위치 정보를 나타내는 특정 통화 발행 프라이빗 트랜잭션 아이디를 상기 통화 발행자 및 상기 통화 수신자 중 적어도 일부에게 제공하거나 상기 타 장치로 하여금 상기 통화 발행자 및 상기 통화 수신자 중 적어도 일부에게 제공하도록 지원하는 것을 특징으로 하는 방법.

[청구항 3] 제1항에 있어서,

상기 (a) 단계에서,

상기 서버는,
상기 특정 통화 발행 트랜잭션의 데이터 포맷의 유효 여부, 상기 통화 수신자의 유효 여부, 상기 통화 발행자의 퍼블릭 키의 유효 여부 및 상기 통화 발행자의 서명값의 유효 여부를 확인하되, 상기 통화 발행자의 서명값을 기등록된 상기 통화 발행자의 퍼블릭 키를 사용하여 검증함으로써 상기 통화 발행자의 서명값에 대한 유효 여부를 확인하여 상기 특정 통화 발행 트랜잭션의 유효 여부를 확인하는 것을 특징으로 하는 방법.

[청구항 4] 제1항에 있어서,
상기 (a) 단계에서,
상기 서버는,
상기 통화 발행자의 서명 값을 사전에 등록된 상기 통화 발행자의 퍼블릭 키를 사용하여 검증함으로써 상기 통화 발행자의 서명값에 대한 유효 여부를 확인하는 것을 특징으로 하는 방법.

[청구항 5] 제1항에 있어서,
상기 (a) 단계 이전에,
(a01) 상기 통화 발행자의 퍼블릭 키에 의한 발행자 등록 요청이 획득되면, 상기 서버는, 상기 통화 발행자의 유효 여부를 확인하여 상기 통화 발행자가 유효할 경우 특정 랜덤 논스를 상기 통화 발행자에게 전달하거나 상기 타 장치로 하여금 상기 통화 발행자에게 전달하도록 지원하는 단계; 및
(a02) 상기 특정 랜덤 논스를 상기 통화 발행자의 프라이빗 키로 서명한 특정 랜덤 논스 서명값이 획득되면, 상기 서버는, 상기 특정 랜덤 논스 서명값이 유효한 서명 값인지를 상기 통화 발행자의 퍼블릭 키를 사용하여 검증하고 검증이 완료되면 상기 특정 랜덤 논스, 상기 특정 랜덤 논스 서명값 및 상기 통화 발행자의 퍼블릭 키를 포함하는 발행자 등록 트랜잭션 또는 상기 발행자 등록 트랜잭션에 대한 해쉬값을 상기 퍼블릭 블록체인 데이터베이스에 등록하거나 상기 타 장치로 하여금 상기 퍼블릭 블록체인 데이터베이스에 등록하도록 지원하고, 상기 퍼블릭 블록체인 데이터베이스에 등록된 상기 발행자 등록 트랜잭션 또는 상기 발행자 등록 트랜잭션에 대한 해쉬값의 상기 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 발행자 등록 퍼블릭 트랜잭션 아이디를 획득하거나 상기 타 장치로 하여금 상기 퍼블릭 블록체인 데이터베이스로부터 획득하도록 지원하는 단계를 더 포함하는 것을 특징으로 하는 방법.

[청구항 6] 제5항에 있어서,
상기 (a02) 단계에서,
상기 서버는,

상기 특정 랜덤 논스, 상기 특정 랜덤 논스 서명값 및 상기 통화 발행자의 퍼블릭 키를 포함하는 상기 발행자 등록 트랜잭션을 추가적으로 프라이빗 블록체인 데이터베이스에 등록하거나 상기 타 장치로 하여금 상기 프라이빗 블록체인 데이터베이스에 등록하도록 지원하고, 상기 프라이빗 블록체인 데이터베이스에 등록된 상기 발행자 등록 트랜잭션의 상기 프라이빗 블록체인 데이터베이스 상의 위치 정보를 나타내는 발행자 등록 프라이빗 트랜잭션 아이디를 상기 통화 발행자에게 제공하거나 상기 타 장치로 하여금 상기 통화 발행자에게 제공하도록 지원하는 것을 특징으로 하는 방법.

[청구항 7] 제5항에 있어서,
상기 (a01) 단계에서,
상기 서버는,
상기 통화 발행자의 공개키 기반 인증서를 이용하거나 상기 통화 발행자의 신분 증명 정보를 이용하여 상기 통화 발행자의 유효 여부를 확인하는 것을 특징으로 하는 방법.

[청구항 8] 통화의 지급을 결제하는 방법에 있어서,
(a) 특정 사용자로부터 상기 통화의 지급 결제를 위한 (i) 이전에 적어도 일부 미사용된 적어도 하나 이상의 제1 통화 사용 트랜잭션 아이디, (ii) 통화 수신자 정보, (iii) 특정 지급 결제 금액, (iv) 상기 특정 사용자의 퍼블릭 키 및 (v) 상기 특정 사용자의 프라이빗 키로 상기 (i), 상기 (ii), 상기 (iii), 상기 (iv)를 서명한 상기 특정 사용자의 서명값을 포함하는 제2 통화 사용 트랜잭션이 획득되면, 서버는, 상기 제2 통화 사용 트랜잭션의 상기 특정 사용자의 밸런스를 참조하여 상기 제2 통화 사용 트랜잭션의 지급 결제 방식을 확인하는 단계; 및
(b) (i) 상기 특정 사용자의 밸런스가 상기 특정 지급 결제 금액 이상이어서 상기 제2 통화 사용 트랜잭션의 지급 결제 방식이 "즉시 지급 결제"로 확인되면, 상기 서버는, 상기 특정 사용자의 서명값이 유효한지를 판단하여 유효일 경우, 상기 제2 통화 사용 트랜잭션 또는 상기 제2 통화 사용 트랜잭션에 대한 해쉬값을 퍼블릭 블록체인 데이터베이스에 등록하거나 상기 서버에 연동된 타 장치로 하여금 상기 퍼블릭 블록체인 데이터베이스에 등록하도록 지원하고, 상기 퍼블릭 블록체인 데이터베이스에 등록된 상기 제2 통화 사용 트랜잭션 또는 상기 제2 통화 사용 트랜잭션의 해쉬값의 상기 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 제2 통화 사용 퍼블릭 트랜잭션 아이디를 획득하거나 상기 타 장치로 하여금 상기 퍼블릭 블록체인 데이터베이스로부터 획득하도록 지원하거나, (ii) 상기 특정 사용자의 밸런스가 상기 특정 지급 결제 금액 미만이어서 상기 제2 통화 사용 트랜잭션의 지급 결제 방식이 "지연 지급 결제"로 확인되면, 상기 서버는,

상기 특정 사용자의 서명값이 유효한지를 판단하여 유효일 경우, 상기 제2 통화 사용 트랜잭션을 저장부에 저장한 상태에서, 적어도 하나 이상의 타 사용자에 의해 지급 결제되며 상기 특정 사용자를 수취인으로 하는 적어도 하나 이상의 제3 통화 사용 트랜잭션이 소정의 상계 처리 조건을 만족하면, 상기 제2 통화 사용 트랜잭션과 상기 제3 통화 사용 트랜잭션들을 상계 처리하며, 상계 처리된 상기 제2 통화 사용 트랜잭션 또는 상기 제2 통화 사용 트랜잭션의 해쉬값과 상기 제3 통화 사용 트랜잭션 또는 상기 제3 통화 사용 트랜잭션의 해쉬값을 상기 퍼블릭 블록체인 데이터베이스에 등록하거나 상기 타 장치로 하여금 상기 퍼블릭 블록체인 데이터베이스에 등록하도록 지원하며, 상기 퍼블릭 블록체인 데이터베이스에 등록된 상기 제2 통화 사용 트랜잭션 또는 상기 제2 통화 사용 트랜잭션의 해쉬값과 상기 제3 통화 사용 트랜잭션 또는 상기 제3 통화 사용 트랜잭션의 해쉬값의 상기 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 제2 통화 사용 퍼블릭 트랜잭션 아이디와 제3 통화 사용 퍼블릭 트랜잭션 아이디를 획득하거나 상기 타 장치로 하여금 상기 퍼블릭 블록체인 데이터베이스로부터 획득하도록 지원하는 단계를 포함하는 것을 특징으로 하는 방법.

[청구항 9] 제8항에 있어서,

상기 제1 통화 사용 트랜잭션 아이디가, 상기 제1 통화 사용 트랜잭션의 상기 프라이빗 블록체인 데이터베이스 상의 위치 정보를 나타내는 제1 통화 사용 프라이빗 트랜잭션 아이디인 경우,

상기 (b) 단계에서,

(i) 상기 특정 사용자의 밸런스가 상기 특정 지급 결제 금액 이상이어서 상기 제2 통화 사용 트랜잭션의 지급 결제 방식이 "즉시 지급 결제"로 확인되면, 상기 서버는, 상기 특정 사용자의 서명값이 유효한지를 판단하여 유효일 경우, 상기 제2 통화 사용 트랜잭션을 추가적으로 상기 프라이빗 블록체인 데이터베이스에 등록하고, 상기 프라이빗 블록체인 데이터베이스에 등록된 상기 제2 통화 사용 트랜잭션의 상기 프라이빗 블록체인 데이터베이스 상의 위치 정보를 나타내는 제2 통화 사용 프라이빗 트랜잭션 아이디를 상기 특정 사용자 및 상기 통화 수신자 중 적어도 일부에게 제공하거나 상기 타 장치로 하여금 상기 특정 사용자 및 상기 통화 수신자 중 적어도 일부에게 제공하도록 지원하거나, (ii) 상기 특정 사용자의 밸런스가 상기 특정 지급 결제 금액 미만이어서 상기 제2 통화 사용 트랜잭션의 지급 결제 방식이 "지연 지급 결제"로 확인되면, 상기 서버는, 상기 특정 사용자의 서명값이 유효한지를 판단하여 유효일 경우, 상계 처리된 상기 제2 통화 사용 트랜잭션과 상기 제3 통화 사용 트랜잭션을 추가적으로 상기 프라이빗 블록체인 데이터베이스에 등록하거나 상기 타 장치로 하여금 상기 프라이빗 블록체인

데이터베이스에 등록하도록 지원하며, 상기 프라이빗 블록체인 데이터베이스에 등록된 상기 제2 통화 사용 트랜잭션과 상기 제3 통화 사용 트랜잭션의 상기 프라이빗 블록체인 데이터베이스 상의 위치 정보를 나타내는 제2 통화 사용 프라이빗 트랜잭션 아이디와 제3 통화 사용 프라이빗 트랜잭션 아이디를 상기 특정 사용자, 상기 통화 수신자, 및 적어도 하나 이상의 상기 타 사용자 중 적어도 일부에게 제공하거나 상기 타 장치로 하여금 상기 특정 사용자, 상기 통화 수신자, 및 적어도 하나 이상의 상기 타 사용자 중 적어도 일부에게 제공하도록 지원하는 것을 특징으로 하는 방법.

[청구항 10] 제8항에 있어서,
상기 제2 통화 사용 트랜잭션은, 상기 특정 지급 결제 금액을 지급한 이후의 잔금 및 상기 잔금의 소유주 정보를 더 포함하는 것을 특징으로 하는 방법.

[청구항 11] 제8항에 있어서,
상기 제2 통화 사용 트랜잭션은, 상기 "즉시 지급 결제" 또는 "지연 지급 결제"를 포함하는 지급 결제 방식을 더 포함하며,
상기 (b) 단계에서,
상기 서버는, 상기 제2 통화 사용 트랜잭션의 지급 결제 방식이 "즉시 지급 결제"이지만 상기 특정 사용자의 밸런스가 상기 특정 지급 결제 금액 미만일 경우에는 상기 제2 통화 사용 트랜잭션의 지급 결제 방식이 "지연 지급 결제"인 것으로 판단하는 것을 특징으로 하는 방법.

[청구항 12] 제8항에 있어서,
상기 소정의 상계 처리 조건은,
상기 제3 통화 사용 트랜잭션이 획득될 경우 상기 상계 처리를 수행하며, 상기 상계 처리에 의해 상기 특정 사용자의 밸런스가 "0" 이상의 값을 가지는 조건인 것을 특징으로 하는 방법.

[청구항 13] 제8항에 있어서,
상기 (a) 단계 이전에,
(a01) 상기 특정 사용자의 퍼블릭 키에 의한 사용자 등록 요청이 획득되면, 상기 서버는, 상기 특정 사용자의 유효 여부를 확인하여 상기 특정 사용자가 유효할 경우 특정 랜덤 논스를 상기 특정 사용자에게 전달하거나 상기 타 장치로 하여금 상기 특정 사용자에게 전달하도록 지원하는 단계; 및
(a02) 상기 특정 랜덤 논스를 상기 특정 사용자의 프라이빗 키로 서명한 특정 랜덤 논스 서명값이 획득되면, 상기 서버는, 상기 특정 랜덤 논스 서명값이 유효한 서명인지를 상기 특정 사용자의 퍼블릭 키를 사용하여 검증하고 검증이 완료되면 상기 특정 랜덤 논스, 상기 특정 랜덤 논스 서명값 및 상기 특정 사용자의 퍼블릭 키를 포함하는 특정 사용자 등록

트랜잭션 또는 상기 특정 사용자 등록 트랜잭션에 대한 해쉬값을 상기 퍼블릭 블록체인 데이터베이스에 등록하거나 상기 타 장치로 하여금 상기 퍼블릭 블록체인 데이터베이스에 등록하도록 지원하고, 상기 퍼블릭 블록체인 데이터베이스에 등록된 상기 특정 사용자 등록 트랜잭션 또는 상기 특정 사용자 등록 트랜잭션에 대한 해쉬값의 상기 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 특정 사용자 등록 퍼블릭 트랜잭션 아이디를 획득하거나 상기 타 장치로 하여금 상기 퍼블릭 블록체인 데이터베이스로부터 획득하도록 지원하는 단계를 더 포함하는 것을 특징으로 하는 방법.

[청구항 14] 제13항에 있어서,

상기 (a02) 단계에서,

상기 서버는,

상기 특정 랜덤 논스, 상기 특정 랜덤 논스 서명값 및 상기 특정 사용자의 퍼블릭 키를 포함하는 상기 특정 사용자 등록 트랜잭션을 추가적으로 프라이빗 블록체인 데이터베이스에 등록하거나 상기 타 장치로 하여금 상기 프라이빗 블록체인 데이터베이스에 등록하도록 지원하고, 상기 프라이빗 블록체인 데이터베이스에 등록된 상기 특정 사용자 등록 트랜잭션의 상기 프라이빗 블록체인 데이터베이스 상의 위치 정보를 나타내는 특정 사용자 등록 프라이빗 트랜잭션 아이디를 상기 특정 사용자에게 제공하거나 상기 타 장치로 하여금 상기 특정 사용자에게 제공하도록 지원하는 것을 특징으로 하는 방법.

[청구항 15] 통화를 발행하는 서버에 있어서,

통화 발행자로부터의 상기 통화 발행을 위한 (i) 통화 수신자 정보, (ii) 상기 통화의 발행량, (iii) 상기 통화 발행자의 퍼블릭 키 및 (iv) 상기 통화 발행자의 프라이빗 키로 상기 (i), 상기 (ii), 상기 (iii)을 서명한 상기 통화 발행자의 서명값을 포함하는 특정 통화 발행 트랜잭션을 획득하는 통신부; 및

상기 획득된 상기 특정 통화 발행 트랜잭션 및 상기 통화 발행자의 유효 여부를 확인하여 유효이면, (i) 상기 통화 수신자 정보, (ii) 상기 통화의 발행량, (iii) 상기 통화 발행자의 퍼블릭 키 및 (iv) 상기 통화 발행자의 서명값을 포함하는 상기 특정 통화 발행 트랜잭션 또는 상기 특정 통화 발행 트랜잭션에 대한 해쉬값을 퍼블릭 블록체인 데이터베이스에 등록하거나 상기 서버에 연동된 타 장치로 하여금 상기 퍼블릭 블록체인 데이터베이스에 등록하도록 지원하고, 상기 퍼블릭 블록체인 데이터베이스에 등록된 상기 특정 통화 발행 트랜잭션 또는 상기 특정 통화 발행 트랜잭션에 대한 해쉬값의 상기 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 특정 통화 발행 퍼블릭 트랜잭션 아이디를 획득하거나 상기 타 장치로 하여금 상기 퍼블릭

블록체인 데이터베이스로부터 획득하도록 지원하는 프로세서;
를 포함하되,
상기 프로세서는,
상기 특정 통화 발행 트랜잭션의 데이터 포맷의 유효 여부, 상기 통화 수신자의 유효 여부, 상기 통화 발행자의 퍼블릭 키의 유효 여부 및 상기 통화 발행자의 서명값의 유효 여부를 확인하되, 상기 통화 발행자의 서명값을 기등록된 상기 통화 발행자의 퍼블릭 키를 사용하여 검증함으로써 상기 통화 발행자의 서명값에 대한 유효 여부를 확인하여 상기 특정 통화 발행 트랜잭션의 유효 여부를 확인하는 것을 특징으로 하는 서버.

[청구항 16] 제15항에 있어서,
상기 프로세서는,
상기 특정 통화 발행 트랜잭션과 상기 통화 발행자가 유효이면, (i) 상기 통화 수신자 정보, (ii) 상기 통화의 발행량, (iii) 상기 통화 발행자의 퍼블릭 키 및 (iv) 상기 통화 발행자의 서명값을 포함하는 상기 특정 통화 발행 트랜잭션을 추가적으로 프라이빗 블록체인 데이터베이스에 등록하거나 상기 타 장치로 하여금 상기 프라이빗 블록체인 데이터베이스에 등록하도록 지원하고, 상기 프라이빗 블록체인 데이터베이스에 등록된 상기 특정 통화 발행 트랜잭션의 상기 프라이빗 블록체인 데이터베이스 상의 위치 정보를 나타내는 특정 통화 발행 프라이빗 트랜잭션 아이디를 상기 통화 발행자 및 상기 통화 수신자 중 적어도 일부에게 제공하거나 상기 타 장치로 하여금 상기 통화 발행자 및 상기 통화 수신자 중 적어도 일부에게 제공하도록 지원하는 것을 특징으로 하는 서버.

[청구항 17] 제15항에 있어서,
상기 프로세서는,
(i) 상기 통화 발행자의 퍼블릭 키에 의한 발행자 등록 요청이 획득되면, 상기 통화 발행자의 유효 여부를 확인하여 상기 통화 발행자가 유효할 경우 특정 랜덤 논스를 상기 통화 발행자에게 전달하거나 상기 타 장치로 하여금 상기 통화 발행자에게 전달하도록 지원하며, (ii) 상기 특정 랜덤 논스를 상기 통화 발행자의 프라이빗 키로 서명한 특정 랜덤 논스 서명값이 획득되면, 상기 특정 랜덤 논스 서명값이 유효한 서명 값인지를 상기 통화 발행자의 퍼블릭 키를 사용하여 검증하고 검증이 완료되면 상기 특정 랜덤 논스, 상기 특정 랜덤 논스 서명값 및 상기 통화 발행자의 퍼블릭 키를 포함하는 발행자 등록 트랜잭션 또는 상기 발행자 등록 트랜잭션에 대한 해쉬값을 상기 퍼블릭 블록체인 데이터베이스에 등록하거나 상기 타 장치로 하여금 상기 퍼블릭 블록체인 데이터베이스에 등록하도록 지원하고, 상기 퍼블릭 블록체인

데이터베이스에 등록된 상기 발행자 등록 트랜잭션 또는 상기 발행자 등록 트랜잭션에 대한 해쉬값의 상기 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 발행자 등록 퍼블릭 트랜잭션 아이디를 획득하거나 상기 타 장치로 하여금 상기 퍼블릭 블록체인 데이터베이스로부터 획득하도록 지원하는 것을 특징으로 하는 서버.

[청구항 18] 제17항에 있어서,
상기 프로세서는,
상기 특정 랜덤 논스, 상기 특정 랜덤 논스 서명값 및 상기 통화 발행자의 퍼블릭 키를 포함하는 상기 발행자 등록 트랜잭션을 추가적으로 프라이빗 블록체인 데이터베이스에 등록하거나 상기 타 장치로 하여금 상기 프라이빗 블록체인 데이터베이스에 등록하도록 지원하고, 상기 프라이빗 블록체인 데이터베이스에 등록된 상기 발행자 등록 트랜잭션의 상기 프라이빗 블록체인 데이터베이스 상의 위치 정보를 나타내는 발행자 등록 프라이빗 트랜잭션 아이디를 상기 통화 발행자에게 제공하거나 상기 타 장치로 하여금 상기 통화 발행자에게 제공하도록 지원하는 것을 특징으로 하는 서버.

[청구항 19] 통화의 지급을 결제하는 서버에 있어서,
특정 사용자로부터 상기 통화의 지급 결제를 위한 (i) 이전에 적어도 일부 미사용된 적어도 하나 이상의 제1 통화 사용 트랜잭션 아이디, (ii) 통화 수신자 정보, (iii) 특정 지급 결제 금액, (iv) 상기 특정 사용자의 퍼블릭 키 및 (v) 상기 특정 사용자의 프라이빗 키로 상기 (i), 상기 (ii), 상기 (iii), 상기 (iv)를 서명한 상기 특정 사용자의 서명값을 포함하는 제2 통화 사용 트랜잭션을 획득하는 통신부: 및
상기 획득된 상기 제2 통화 사용 트랜잭션의 상기 특정 사용자의 밸런스를 참조하여 상기 제2 통화 사용 트랜잭션의 지급 결제 방식을 확인하여, 상기 특정 사용자의 밸런스가 상기 특정 지급 결제 금액 이상이어서 상기 제2 통화 사용 트랜잭션의 지급 결제 방식이 "즉시 지급 결제"로 확인되면, 상기 특정 사용자의 서명값이 유효한지를 판단하여 유효일 경우, 상기 제2 통화 사용 트랜잭션 또는 상기 제2 통화 사용 트랜잭션에 대한 해쉬값을 퍼블릭 블록체인 데이터베이스에 등록하거나 상기 서버에 연동된 타 장치로 하여금 상기 퍼블릭 블록체인 데이터베이스에 등록하도록 지원하고, 상기 퍼블릭 블록체인 데이터베이스에 등록된 상기 제2 통화 사용 트랜잭션 또는 상기 제2 통화 사용 트랜잭션의 해쉬값의 상기 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 제2 통화 사용 퍼블릭 트랜잭션 아이디를 획득하거나 상기 타 장치로 하여금 상기 퍼블릭 블록체인 데이터베이스로부터 획득하도록 지원하도록 하는 프로세스, 및 상기 특정 사용자의 밸런스가 상기 특정 지급 결제 금액 미만이어서 상기 제2

통화 사용 트랜잭션의 지급 결제 방식이 "지연 지급 결제"로 확인되면, 상기 특정 사용자의 서명값이 유효한지를 판단하여 유효일 경우, 상기 제2 통화 사용 트랜잭션을 저장부에 저장한 상태에서, 적어도 하나 이상의 타 사용자에 의해 지급 결제되며 상기 특정 사용자를 수취인으로 하는 적어도 하나 이상의 제3 통화 사용 트랜잭션이 소정의 상계 처리 조건을 만족하면, 상기 제2 통화 사용 트랜잭션과 상기 제3 통화 사용 트랜잭션들을 상계 처리하며, 상계 처리된 상기 제2 통화 사용 트랜잭션 또는 상기 제2 통화 사용 트랜잭션의 해쉬값과 상기 제3 통화 사용 트랜잭션 또는 상기 제3 통화 사용 트랜잭션의 해쉬값을 상기 퍼블릭 블록체인 데이터베이스에 등록하거나 상기 타 장치로 하여금 상기 퍼블릭 블록체인 데이터베이스에 등록하도록 지원하며, 상기 퍼블릭 블록체인 데이터베이스에 등록된 상기 제2 통화 사용 트랜잭션 또는 상기 제2 통화 사용 트랜잭션의 해쉬값과 상기 제3 통화 사용 트랜잭션 또는 상기 제3 통화 사용 트랜잭션의 해쉬값의 상기 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 제2 통화 사용 퍼블릭 트랜잭션 아이디와 제3 통화 사용 퍼블릭 트랜잭션 아이디를 획득하거나 상기 타 장치로 하여금 상기 퍼블릭 블록체인 데이터베이스로부터 획득하도록 지원하는 프로세스를 수행하는 프로세서;

를 포함하는 것을 특징으로 하는 서버.

[청구항 20] 제19항에 있어서,

상기 제1 통화 사용 트랜잭션 아이디가, 상기 제1 통화 사용 트랜잭션의 상기 프라이빗 블록체인 데이터베이스 상의 위치 정보를 나타내는 프라이빗 제1 통화 사용 트랜잭션 아이디인 경우,

상기 프로세서는,

(i) 상기 특정 사용자의 밸런스가 상기 특정 지급 결제 금액 이상이어서 상기 제2 통화 사용 트랜잭션의 지급 결제 방식이 "즉시 지급 결제"로 확인되면, 상기 특정 사용자의 서명값이 유효한지를 판단하여 유효일 경우, 상기 제2 통화 사용 트랜잭션을 추가적으로 상기 프라이빗 블록체인 데이터베이스에 등록하고, 상기 프라이빗 블록체인 데이터베이스에 등록된 상기 제2 통화 사용 트랜잭션의 상기 프라이빗 블록체인 데이터베이스 상의 위치 정보를 나타내는 제2 통화 사용 프라이빗 트랜잭션 아이디를 상기 특정 사용자 및 상기 통화 수신자 중 적어도 일부에게 제공하거나 상기 타 장치로 하여금 상기 특정 사용자 및 상기 통화 수신자 중 적어도 일부에게 제공하도록 지원하는 프로세스, 및 상기 특정 사용자의 밸런스가 상기 특정 지급 결제 금액 미만이어서 상기 제2 통화 사용 트랜잭션의 지급 결제 방식이 "지연 지급 결제"로 확인되면, 상기 특정 사용자의 서명값이 유효한지를 판단하여 유효일 경우, 상계 처리된 상기 제2 통화 사용 트랜잭션과 상기 제3 통화 사용

트랜잭션을 추가적으로 프라이빗 블록체인 데이터베이스에 등록하거나 상기 타 장치로 하여금 상기 프라이빗 블록체인 데이터베이스에 등록하도록 지원하며, 상기 프라이빗 블록체인 데이터베이스에 등록된 상기 제2 통화 사용 트랜잭션과 상기 제3 통화 사용 트랜잭션의 상기 프라이빗 블록체인 데이터베이스 상의 위치 정보를 나타내는 제2 통화 사용 프라이빗 트랜잭션 아이디와 제3 통화 사용 프라이빗 트랜잭션 아이디를 상기 특정 사용자, 상기 통화 수신자, 및 적어도 하나 이상의 상기 타 사용자 중 적어도 일부에게 제공하거나 상기 타 장치로 하여금 상기 특정 사용자, 상기 통화 수신자, 및 적어도 하나 이상의 타 사용자 중 적어도 일부에게 제공하도록 지원하는 프로세스를 수행하는 것을 특징으로 하는 서버.

[청구항 21] 제19항에 있어서,

상기 프로세서는,

(i) 상기 특정 사용자의 퍼블릭 키에 의한 특정 사용자 등록 요청이 획득되면, 상기 특정 사용자의 유효 여부를 확인하여 상기 특정 사용자가 유효할 경우 특정 랜덤 논스를 상기 특정 사용자에게 전달하거나 상기 타 장치로 하여금 상기 특정 사용자에게 전달하도록 지원하며, (ii) 상기 특정 랜덤 논스를 상기 특정 사용자의 프라이빗 키로 서명한 특정 랜덤 논스 서명값이 획득되면, 상기 특정 랜덤 논스 서명값이 유효한 서명인지를 상기 특정 사용자의 퍼블릭 키를 사용하여 검증하고 검증이 완료되면 상기 특정 랜덤 논스, 상기 특정 랜덤 논스 서명값 및 상기 특정 사용자의 퍼블릭 키를 포함하는 특정 사용자 등록 트랜잭션 또는 상기 특정 사용자 등록 트랜잭션에 대한 해쉬값을 상기 퍼블릭 블록체인 데이터베이스에 등록하거나 상기 타 장치로 하여금 상기 퍼블릭 블록체인 데이터베이스에 등록하도록 지원하고, 상기 퍼블릭 블록체인 데이터베이스에 등록된 상기 특정 사용자 등록 트랜잭션 또는 상기 특정 사용자 등록 트랜잭션에 대한 해쉬값의 상기 퍼블릭 블록체인 데이터베이스 상의 위치 정보를 나타내는 특정 사용자 등록 퍼블릭 트랜잭션 아이디를 획득하거나 상기 타 장치로 하여금 상기 퍼블릭 블록체인 데이터베이스로부터 획득하도록 지원하는 것을 특징으로 하는 서버.

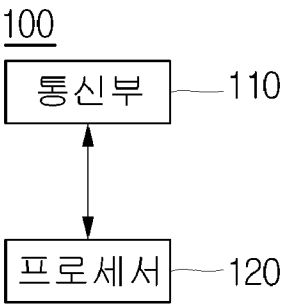
[청구항 22] 제21항에 있어서,

상기 프로세서는,

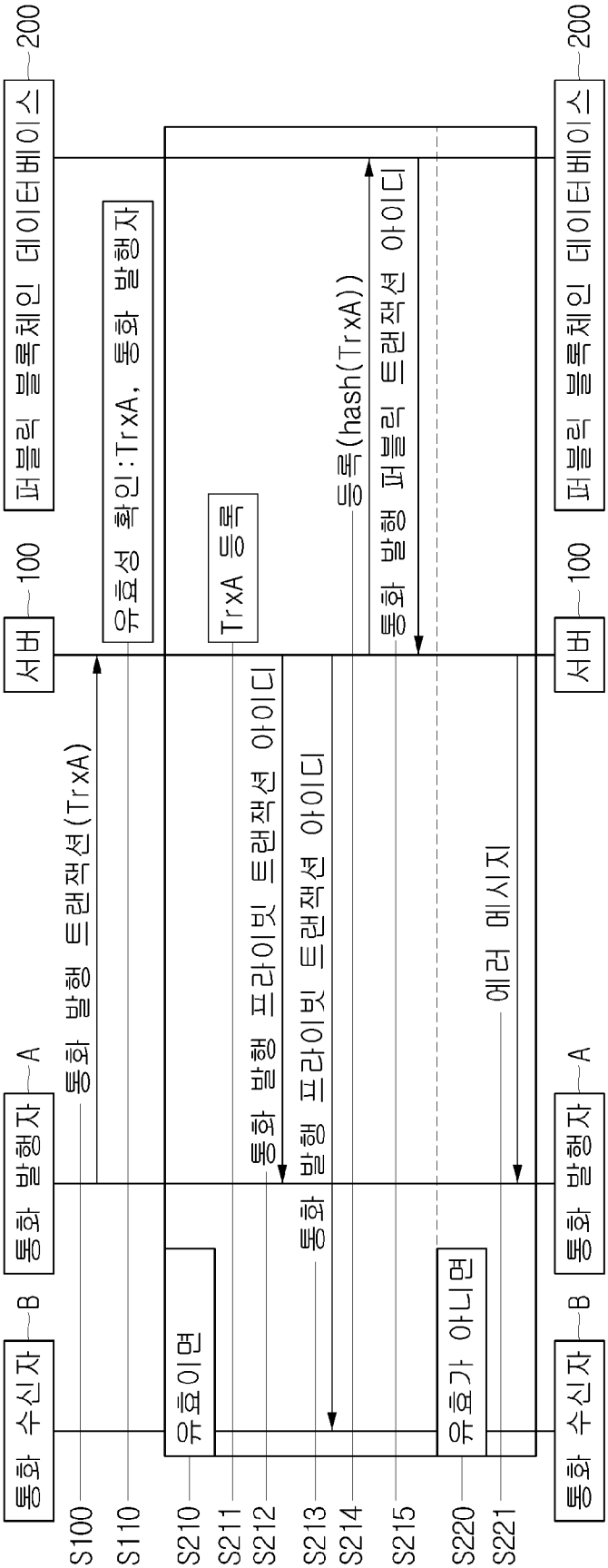
상기 특정 랜덤 논스, 상기 특정 랜덤 논스 서명값 및 상기 특정 사용자의 퍼블릭 키를 포함하는 상기 특정 사용자 등록 트랜잭션을 추가적으로 프라이빗 블록체인 데이터베이스에 등록하거나 상기 타 장치로 하여금 상기 프라이빗 블록체인 데이터베이스에 등록하도록 지원하고, 상기 프라이빗 블록체인 데이터베이스에 등록된 상기 특정 사용자 등록

트랜잭션의 상기 프라이빗 블록체인 데이터베이스 상의 위치 정보를 나타내는 특정 사용자 등록 프라이빗 트랜잭션 아이디를 상기 특정 사용자에게 제공하거나 상기 타 장치로 하여금 상기 특정 사용자에게 제공하도록 지원하는 것을 특징으로 하는 서버.

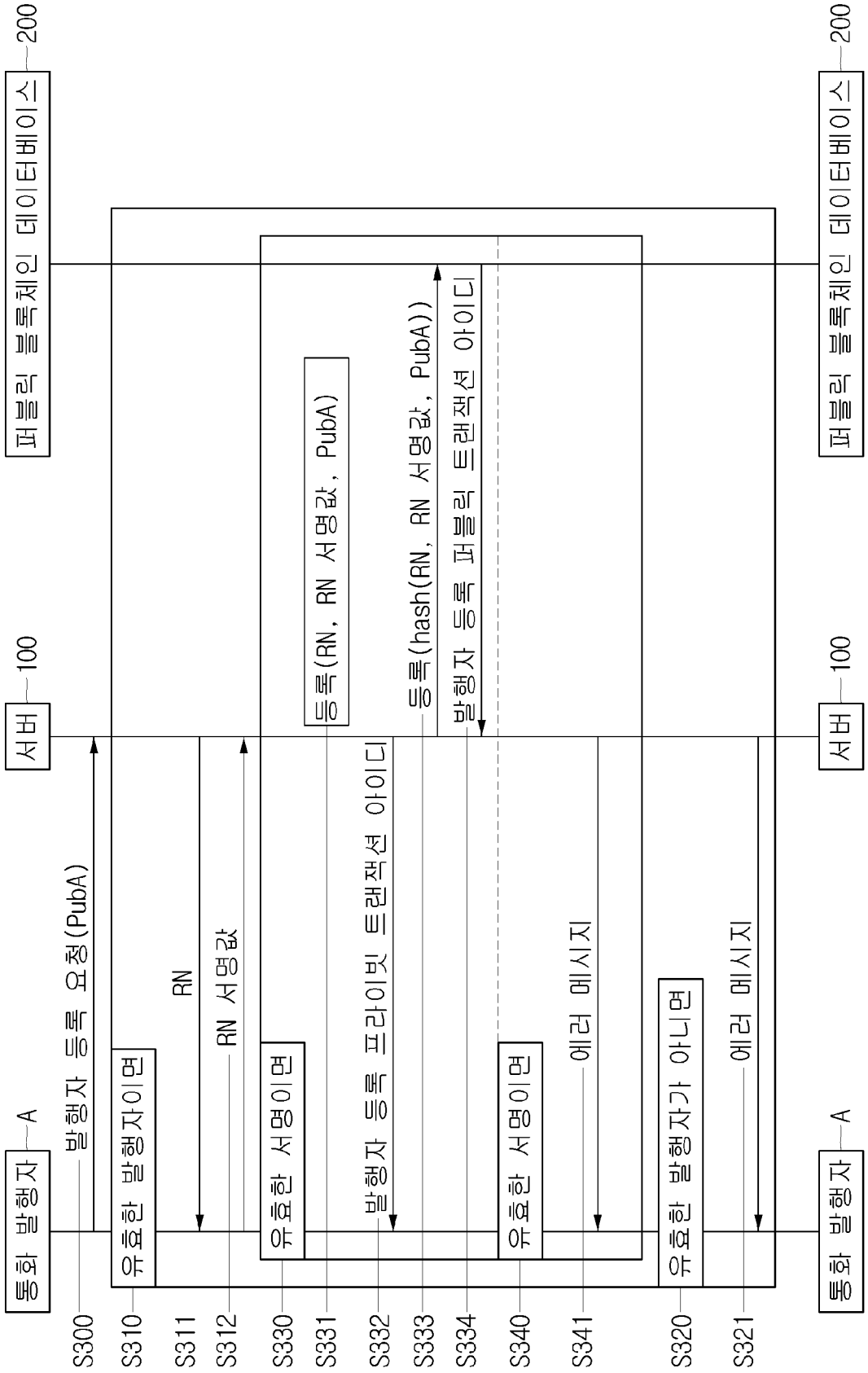
[도1]



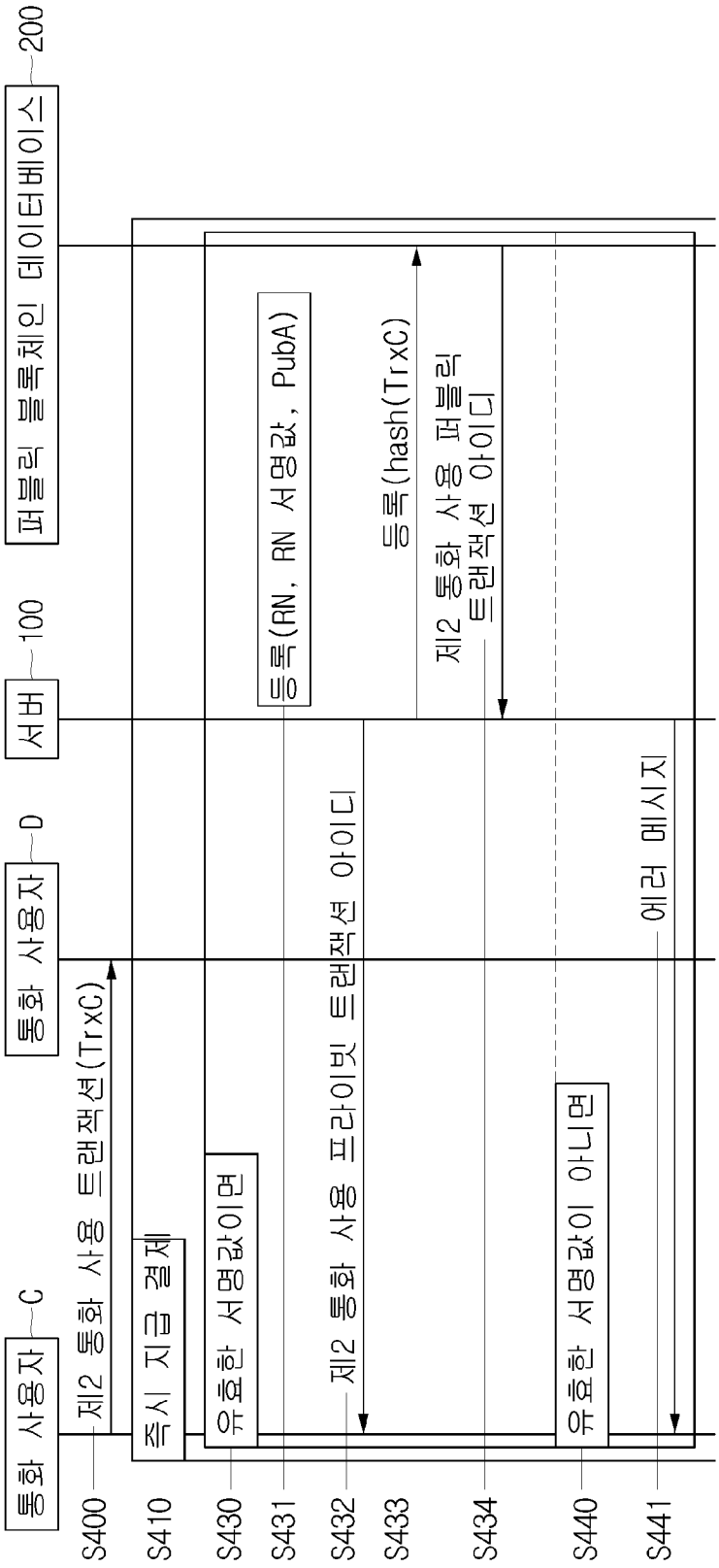
[도2]


퍼블릭 블록체인 데이터베이스 200
서버 100
통화 발행자 A
통화 수신자 B
통화 발행 트랜잭션(TrxA)
유효성 확인:TrxA, 통화 발행자
TrxA 등록
통화 발행 프라이빗 트랜잭션 아이디
통화 발행 프라이빗 트랜잭션 아이디
등록(hash(TrxA))
통화 발행 퍼블릭 트랜잭션 아이디
에러 메시지
유효이면
유효가 아니면
S100
S110
S210
S211
S212
S213
S214
S215
S220
S221

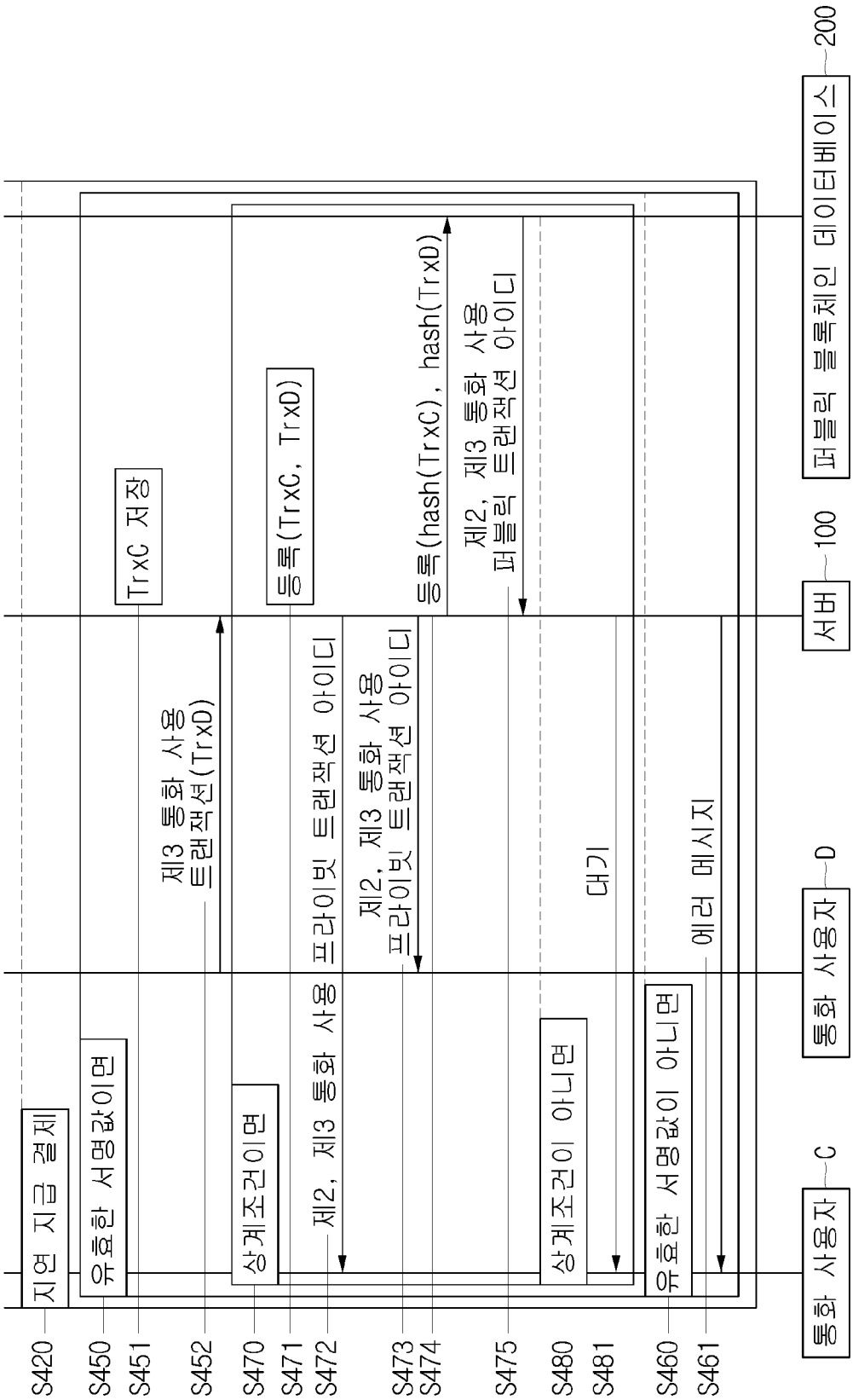
[도3]


통화 발행자 A
서버 100
퍼블릭 블록체인 데이터베이스 200
발행자 등록 요청(PubA)
유효한 발행자이면
RN
RN 서명값
유효한 서명이면
등록(RN, RN 서명값, PubA)
발행자 등록 프라이빗 트랜잭션 아이디
등록(hash(RN, RN 서명값, PubA))
발행자 등록 퍼블릭 트랜잭션 아이디
유효한 서명이면
에러 메시지
유효한 발행자가 아니면
에러 메시지
S300
S310
S311
S312
S330
S331
S332
S333
S334
S340
S341
S320
S321

[도4a]


통화 사용자 C
통화 사용자 D
서버 100
퍼블릭 블록체인 데이터베이스 200
S400
제2 통화 사용 트랜잭션(TrxC)
S410
즉시 지급 결제
S430
유효한 서명값이면
S431
등록(RN, RN 서명값, PubA)
S432
제2 통화 사용 프라이빗 트랜잭션 아이디
S433
등록(hash(TrxC)
S434
제2 통화 사용 퍼블릭 트랜잭션 아이디
S440
유효한 서명값이 아니면
S441
에러 메시지

[도4b]


통화 사용자 C
통화 사용자 D
서버 100
퍼블릭 블록체인 데이터베이스 200
지연 지급 결제
유효한 서명값이면
TrxC 저장
제3 통화 사용 트랜잭션(TrxD)
상계조건이면
등록(TrxC, TrxD)
제2, 제3 통화 사용 프라이빗 트랜잭션 아이디
등록(hash(TrxC), hash(TrxD))
제2, 제3 통화 사용 프라이빗 트랜잭션 아이디
상계조건이 아니면
대기
유효한 서명값이 아니면
에러 메시지
S420
S450
S451
S452
S470
S471
S472
S473
S474
S475
S480
S481
S460
S461

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2017/011937

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/36(2012.01)i, G06Q 20/38(2012.01)i, G06Q 20/06(2012.01)i, G06Q 40/02(2012.01)i, G06Q 40/04(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 20/36; G06Q 20/02; H04L 9/30; H04L 9/32; G06Q 20/38; G06Q 20/06; G06Q 40/02; 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: currency, issue, payment, payment, block chain, database, registration, location, ID

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	KR 10-1575030 B1 (INDUSTRY-ACADEMIC COOPERATION FOUNDATION, CHOSUN UNIVERSITY) 07 December 2015 See claims 1, 4, 8 and figures 1-3.	1-2,4 3,5-22
Y	KR 10-1637854 B1 (COINPLUG, INC.) 08 July 2016 See claims 1, 6, 9 and figure 1.	1-2,4
Y	"Data Forgery Detection in Private Block Chain Using Public Block Chain"., Internet post., 05 August 2016., <URL: https://github.com/Kangmo/blitz/wiki/퍼블릭-블록체인을-활용한-프라이빗-블록체인의-데이터-위변조-탐지>. See pages 1-2.	2,4
A	"The Reason Why Block Chain Could Be Fatal to Your Business", CIO Korea., 07 September 2016, <URL: http://www.ciokorea.com/news/31161>. See pages 1-3.	1-22
A	"Tree Signatures", Blockstream., Internet post., 24 August 2015., <URL: https://blockstream.com/2015/08/24/treesignatures.html>. See pages 1-5.	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	Date of mailing of the international search report
17 JANUARY 2018 (17.01.2018)	**18 JANUARY 2018 (18.01.2018)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. +82-42-481-8578	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2017/011937

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The invention of group 1: claims 1 to 7 and 15 to 18 relate to currency issuing,
The invention of group 2: claims 8 to 14 and 19 to 22 relate to payment and settlement of a currency.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☒ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2017/011937

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-1575030 B1	07/12/2015	NONE	
KR 10-1637854 B1	08/07/2016	WO 2017-065389 A1	20/04/2017

국 제 조 사 보 고 서

국제출원번호
PCT/KR2017/011937

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06Q 20/36(2012.01)i, G06Q 20/38(2012.01)i, G06Q 20/06(2012.01)i, G06Q 40/02(2012.01)i, G06Q 40/04(2012.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
G06Q 20/36; G06Q 20/02; H04L 9/30; H04L 9/32; G06Q 20/38; G06Q 20/06; G06Q 40/02; G06Q 40/04

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: 통화, 발행, 지급, 결제, 블록체인, 데이터베이스, 등록, 위치, 아이디

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y A	KR 10-1575030 B1 (조선대학교산학협력단) 2015.12.07 청구항 1,4,8 및 도면 1-3 참조.	1-2,4 3,5-22
Y	KR 10-1637854 B1 (주식회사 코인플러그) 2016.07.08 청구항 1,6,9 및 도면 1 참조.	1-2,4
Y	'퍼블릭 블록체인을 활용한 프라이빗 블록체인의 데이터 위변조 탐지'. 인터넷 게시물. 2016.08.05. <URL: https://github.com/Kangmo/blitz/wiki/퍼블릭-블록체인을-활용한-프라이빗-블록체인의-데이터-위변조-탐지>. 페이지 1-2 참조.	2,4
A	'블록체인이 당신의 기업에 치명적일 수 있는 이유', CIO Korea. 2016.09.07. <URL: http://www.ciokorea.com/news/31161>. 페이지 1-3 참조.	1-22
A	'Tree Signatures', Blockstream. 인터넷 게시물. 2015.08.24. <URL: https://blockstream.com/2015/08/24/treesignatures.html>. 페이지 1-5 참조.	1-22

☐ 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

"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
2018년 01월 17일 (17.01.2018)	2018년 01월 18일 (18.01.2018)

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

심사관
김연경
전화번호 +82-42-481-3325

국 제 조 사 보 고 서

국제출원번호
PCT/KR2017/011937

제2기재란 일부 청구항을 조사할 수 없는 경우의 의견(첫 번째 용지의 2의 계속)

PCT 제17조(2)(a)의 규정에 따라 다음과 같은 이유로 일부 청구항에 대하여 본 국제조사보고서가 작성되지 아니하였습니다.

1. ☐ 청구항:
이 청구항은 본 기관이 조사할 필요가 없는 대상에 관련됩니다. 즉,

2. ☐ 청구항:
이 청구항은 유효한 국제조사를 수행할 수 없을 정도로 소정의 요건을 충족하지 아니하는 국제출원의 부분과 관련됩니다. 구체적으로는,

3. ☐ 청구항:
이 청구항은 종속청구항이나 PCT규칙 6.4(a)의 두 번째 및 세 번째 문장의 규정에 따라 작성되어 있지 않습니다.

제3기재란 발명의 단일성이 결여된 경우의 의견(첫 번째 용지의 3의 계속)

본 국제조사기관은 본 국제출원에 다음과 같이 다수의 발명이 있다고 봅니다.

제1군 발명: 청구항 제1항 내지 제7항 및 제15항 내지 제18항은 통화 발행에 관한 것이고,
제2군 발명: 청구항 제8항 내지 제14항 및 제19항 내지 제22항은 통화의 지급 결제에 관한 것입니다.

1. ☐ 출원인이 모든 추가수수료를 기간 내에 납부하였으므로, 본 국제조사보고서는 모든 조사 가능한 청구항을 대상으로 합니다.

2. ☒ 추가수수료 납부를 요구하지 않고도 모든 조사 가능한 청구항을 조사할 수 있었으므로, 본 기관은 추가수수료 납부를 요구하지 아니하였습니다.

3. ☐ 출원인이 추가수수료의 일부만을 기간 내에 납부하였으므로, 본 국제조사보고서는 수수료가 납부된 청구항만을 대상으로 합니다. 구체적인 청구항은 아래와 같습니다.

4. ☐ 출원인이 기간 내에 추가수수료를 납부하지 아니하였습니다. 따라서 본 국제조사보고서는 청구범위에 처음 기재된 발명에 한정되어 있으며, 해당 청구항은 아래와 같습니다.

이의신청에 관한 기재

☐ 출원인의 이의신청 및 이의신청료 납부(해당하는 경우)와 함께 추가수수료가 납부되었습니다.

☐ 출원인의 이의신청과 함께 추가수수료가 납부되었으나 이의신청료가 보정요구서에 명시된 기간 내에 납부되지 아니하였습니다.

☐ 이의신청 없이 추가수수료가 납부되었습니다.

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2017/011937

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-1575030 B1	2015/12/07	없음	
KR 10-1637854 B1	2016/07/08	WO 2017-065389 A1	2017/04/20