

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2019년 4월 25일 (25.04.2019) **WIPO | PCT**

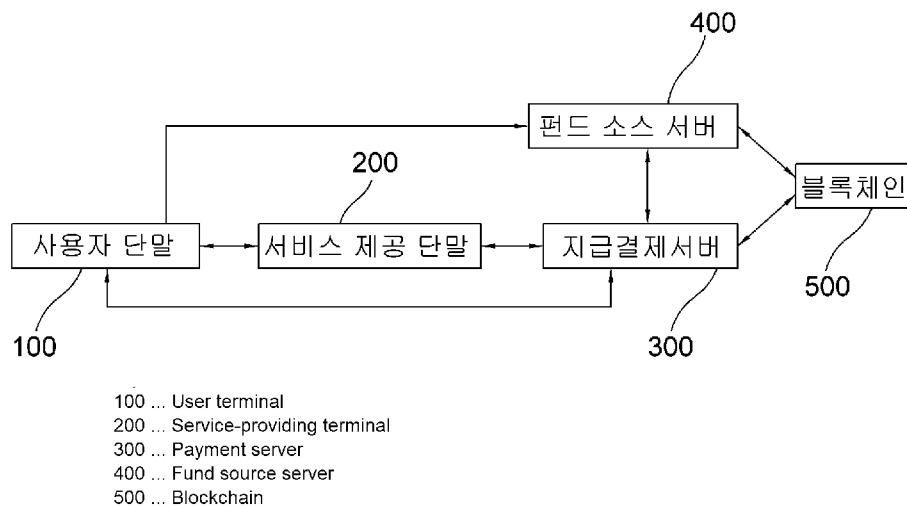


(10) 국제공개번호
WO 2019/078622 A1

- (51) 국제특허분류: *G06Q 20/38* (2012.01) *G06Q 20/02* (2012.01)
G06Q 20/34 (2012.01)
- (21) 국제출원번호: PCT/KR2018/012284
- (22) 국제출원일: 2018년 10월 17일 (17.10.2018)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2017-0134454 2017년 10월 17일 (17.10.2017) KR
10-2018-0076091 2018년 6월 29일 (29.06.2018) KR
- (71) 출원인: 주식회사 코인플러그 (COINPLUG, INC.) [KR/KR]; 13558 경기도 성남시 분당구 성남대로331번길 8, 801호, Gyeonggi-do (KR).
- (72) 발명자: 어준선 (UHR, Joon Sun); 13558 경기도 성남시 분당구 느티로 22, B동 1710호, Gyeonggi-do (KR). 서문규 (SUH, Moon Gju); 06707 서울시 서초구 명달로 33, 102동 602호, Seoul (KR). 홍재우 (HONG, Jay Wu); 03336 서울시 은평구 연서로 149, 1203호, Seoul (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, 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 국내 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), 유

(54) Title: BLOCKCHAIN-BASED PAYMENT METHOD, AND PAYMENT SERVER USING SAME

(54) 발명의 명칭: 블록체인 기반의 결제 방법 및 이를 이용한 지급 결제 서버



(57) Abstract: The present invention relates to a payment method and a payment server using same, the payment method comprising: when order request information, comprising one or more of user identification information and order information, is acquired, acquiring from a blockchain a push token ID corresponding to the user identification information contained in the order request information; generating an order ID corresponding to the order request information; registering, in the blockchain, transaction data comprising at least one from among the order ID and order information; transmitting the push token ID and signature request information to a user terminal; when a signature value is acquired from the user terminal, and if the signature value is valid following authentication, transmitting, to a fund source server, approval request information comprising one or more from among a payment means token ID, the order ID, and order request information; when approval result information is acquired from the fund source server, registering the approval result information in the blockchain; and transmitting, to a service terminal, approval completion information corresponding to the approval result information.

럼 (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 사용자 식별 정보, 및 주문 정보 중 적어도 하나 이상을 포함하는 주문 요청 정보가 획득되면, 주문 요청 정보에 포함된 사용자 식별 정보에 대응하는 푸시 토큰 아이디를 블록체인으로부터 획득하고, 주문 요청 정보에 대응하는 주문 아이디를 생성하며, 주문 아이디와 주문 정보 중 적어도 하나를 포함하는 트랜잭션 데이터를 블록체인에 등록하고, 푸시 토큰 아이디와 서명 요청 정보를 사용자 단말로 전송하며, 사용자 단말로부터의 서명값이 획득되면, 서명값을 검증하여 유효일 경우, 지급 수단 토큰 아이디, 주문 아이디, 및 주문 요청 정보 중 적어도 하나 이상을 포함하는 승인 요청 정보를 펀드 소스 서버로 전송하고, 펀드 소스 서버로부터의 승인 결과 정보가 획득되면, 승인 결과 정보를 블록체인에 등록하며, 승인 결과 정보에 대응한 승인 완료 정보를 서비스 단말로 전송하여 주는 결제 방법 및 이를 이용한 지급 결제 서버에 관한 것이다.

명세서

발명의 명칭: 블록체인 기반의 결제 방법 및 이를 이용한 지급 결제 서버

기술분야

- [1] 본 발명은 블록체인 기반의 결제 방법 및 이를 이용한 지급 결제 서버에 관한 것으로, 보다 상세하게는, 사용자 식별 정보, 및 주문 정보 중 적어도 하나 이상을 포함하는 주문 요청 정보가 획득되면, 주문 요청 정보에 포함된 사용자 식별 정보에 대응하는 푸시 토큰 아이디를 블록체인으로부터 획득하고, 주문 요청 정보에 대응하는 주문 아이디를 생성하며, 주문 아이디와 주문 정보 중 적어도 하나를 포함하는 트랜잭션 데이터를 블록체인에 등록하고, 푸시 토큰 아이디와 서명 요청 정보를 사용자 단말로 전송하며, 사용자 단말로부터의 서명값이 획득되면, 서명값을 검증하여 유효일 경우, 지급 수단 토큰 아이디, 주문 아이디, 및 주문 요청 정보 중 적어도 하나 이상을 포함하는 승인 요청 정보를 펀드 소스 서버로 전송하고, 펀드 소스 서버로부터의 승인 결과 정보가 획득되면, 승인 결과 정보를 블록체인에 등록하며, 승인 결과 정보에 대응한 승인 완료 정보를 서비스 단말로 전송하여 주는 결제 방법 및 이를 이용한 지급 결제 서버에 관한 것이다.

배경기술

- [2] 인터넷 온라인 쇼핑몰 및 오프라인 상점에서의 신용카드 사용자가 증가하면서 신용카드는 현금과 함께 중요한 결제 수단으로 자리잡고 있다.
- [3] 종래에 신용카드를 이용한 결제 시스템은 도 1과 같이 나타내어질 수 있다. 도 1에서의 카드 결제의 흐름은 다음과 같다.
- [4] 우선, 사용자가 특정 상품 또는 서비스를 구매하기 위하여 쇼핑몰, 일 예로, 온라인 쇼핑몰 또는 오프라인 쇼핑몰과 같은 서비스 제공자(10)에게 구매 요청을 하고, 온라인 인증사(20), 일 예로, 신용카드 인증 제공자에게 카드 번호를 입력한다.
- [5] 그러면, 온라인 인증사(20)는 카드사(30)에 카드 번호의 인증을 요청하고, 카드사(30)로부터 카드 번호의 인증 결과를 전달받는다. 인증 결과가 성공적이면, 온라인 인증사(20)는 서비스 제공자(10)에게 인증번호를 전달하고, 쇼핑몰인 서비스 제공자(10)는 암호화된 카드 번호와 인증번호를 결제 대행사(PG사; payment gateway사)(40)에 전달하며, 결제 대행사(40)는 이를 VAN사(50)에 전달하고, VAN사(50)는 이를 다시 카드사(30)에 전달하는 연쇄적인 전달이 이루어진다. 그리고 카드사(30)로부터 나온 승인결과가 다시 VAN사(50)에 전달되고, VAN사(50)로부터 결제 대행사(40)에, 결제 대행사(40)로부터 서비스 제공자(10)에게 전달되어, 최종적인 승인 결과를 사용자가 전달받게 된다.

- [6] 종래의 이와 같은 일반적인 결제 방식은 결제 대행사와 VAN사를 통해 서비스 제공자와 카드사 사이의 카드 결제에 대한 동작이 수행되므로 시스템이 복잡할 뿐만 아니라 각각의 결제 중개사에 의한 수수료도 증가하게 되는 문제점이 있다.
- [7] 또한, 최근에는 서비스 제공자에 의해 제공되는 서비스는 다양한 플랫폼에 의해 이루어지고 있다. 즉, 서비스 제공자는 pc나 모바일을 위한 웹 기반 서비스, iOS, AOS 등을 이용한 앱 기반 서비스, iOS, AOS, 윈도우 등을 이용한 POS 기반 서비스 등을 제공하고 있다. 따라서, 이러한 다양한 플랫폼을 수용하기 위하여 PHP, JAVA, Ruby, Python, Node.js, ASP, Object C, MFC 등의 개발언어와 서비스 환경을 제공하기 위한 결제 인터페이스 제공자(60)가 서비스 제공자와 결제 대행사 사이에서 결제 인터페이스를 제공하고 있다.
- [8] 하지만, 이러한 종래의 카드 결제 시스템에서는 결제 인터페이스 제공자, 결제 대행사, VAN사 등에 의한 결제 대행 수수료에 의해 서비스 제공자가 부담하여야 하는 카드 결제 수수료, 인터페이스 연동 이용수수료, 결제 대행사 이용 수수료, 카드 결제 수수료 등이 증가될 뿐만 아니라, 카드사가 결제 중개사들에게 지급하여야 하는 수수료 등도 증가되는 문제점이 있다.

발명의 상세한 설명

기술적 과제

- [9] 본 발명은 상술한 문제점들을 모두 해결하는 것을 그 목적으로 한다.
- [10] 또한, 본 발명은 카드 사용에 대한 승인 과정에서 수수료를 최소화하는 것을 다른 목적으로 한다.
- [11] 또한, 본 발명은 카드 사용에 관한 트랜잭션을 블록체인에 등록하고 관리함으로써 카드 사용 정보의 위변조가 불가능하도록 하는 것을 또 다른 목적으로 한다.
- [12] 또한, 본 발명은 카드 사용의 승인에서 VAN사나 PG사를 이용하지 않고 블록체인을 이용함으로써 시스템을 간소화할 수 있을 뿐만 아니라 유지 비용을 절감할 수 있도록 하는 것을 또 다른 목적으로 한다.

과제 해결 수단

- [13] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따르면, 블록체인 기반의 결제 방법에 있어서, (a) 사용자의 지급 수단에 대응되는 지급 수단 토큰 아이디, 상기 사용자를 식별하기 위한 사용자 식별 정보, 상기 사용자의 사용자 단말에 설치된 앱에 대응되는 푸시 토큰 아이디, 및 상기 사용자의 퍼블릭 키를 블록체인에 등록한 상태에서, 서비스 제공 단말로부터 사용자 단말의 구매 및 지불 정보에 대응하는 주문 요청 정보 - 상기 주문 요청 정보는 사용자 식별 정보, 및 주문 정보 중 적어도 하나 이상을 포함함 - 가 획득되면, 지급 결제 서버가, 상기 주문 요청 정보에 포함된 상기 사용자 식별 정보에 대응하는 상기 푸시 토큰 아이디를 상기 블록체인으로부터 획득하거나 상기 지급 결제 서버에 연동되는 타 장치를 통해 상기 푸시 토큰 아이디를 상기 블록체인으로부터

획득하도록 지원하고, 상기 주문 요청 정보에 대응하는 주문 아이디를 생성하며, 상기 주문 아이디와 상기 주문 정보 중 적어도 하나를 포함하는 트랜잭션 데이터를 상기 블록체인에 등록하거나 상기 지급 결제 서버에 연동되는 타 장치를 통해 상기 트랜잭션 데이터를 상기 블록체인에 등록하도록 지원하고, 상기 푸시 토큰 아이디와 서명 요청 정보를 상기 사용자 단말로 전송하거나 상기 지급 결제 서버에 연동되는 타 장치 또는 상기 서비스 단말을 통해 상기 푸시 토큰 아이디와 상기 서명 요청 정보를 상기 사용자 단말로 전송하도록 지원하는 단계; (b) 상기 사용자 단말로부터의 서명값이 획득되면, 상기 지급 결제 서버가, 상기 서명값을 검증하거나 상기 지급 결제 서버에 연동되는 타 장치를 통해 상기 서명값을 검증하도록 지원하고, 상기 서명값이 유효일 경우, 상기 지급 수단 토큰 아이디, 상기 주문 아이디, 및 상기 주문 요청 정보 중 적어도 하나 이상을 포함하는 승인 요청 정보를 펀드 소스 서버로 전송하거나 상기 결제 지원 서버와 연동하는 타 장치를 통해 상기 승인 요청 정보를 상기 펀드 소스 서버로 전송하도록 지원하는 단계; 및 (c) 상기 펀드 소스 서버로부터의 승인 결과 정보가 획득되면, 상기 결제 지원 서버가, 상기 승인 결과 정보를 상기 블록체인에 등록하거나 상기 결제 지원 서버에 연동되는 타 장치를 통해 상기 승인 결과 정보를 상기 블록체인에 등록하도록 지원하며, 상기 승인 결과 정보에 대응한 승인 완료 정보를 상기 서비스 단말로 전송하거나 상기 결제 지원 서버에 연동되는 타 장치를 통해 상기 승인 완료 정보를 상기 서비스 단말로 전송하도록 지원하는 단계; 를 포함하는 결제 방법이 제공된다.

- [14] 또한, 본 발명의 일 실시예에 따르면, 블록체인 기반의 결제를 수행하는 지급 결제 서버에 있어서, 사용자의 지급 수단에 대응되는 지급 수단 토큰 아이디, 상기 사용자를 식별하기 위한 사용자 식별 정보, 상기 사용자의 사용자 단말에 설치된 앱에 대응되는 푸시 토큰 아이디, 및 상기 사용자의 퍼블릭 키를 블록체인에 등록한 상태에서, 서비스 제공 단말로부터 사용자 단말의 구매 및 지불 정보에 대응하는 주문 요청 정보 - 상기 주문 요청 정보는 사용자 식별 정보, 및 주문 정보 중 적어도 하나 이상을 포함함 - 를 획득하는 통신부; 및 상기 주문 요청 정보에 포함된 상기 사용자 식별 정보에 대응하는 상기 푸시 토큰 아이디를 상기 블록체인으로부터 획득하거나 상기 지급 결제 서버에 연동되는 타 장치를 통해 상기 푸시 토큰 아이디를 상기 블록체인으로부터 획득하도록 지원하고, 상기 주문 요청 정보에 대응하는 주문 아이디를 생성하며, 상기 주문 아이디와 상기 주문 정보 중 적어도 하나를 포함하는 트랜잭션 데이터를 상기 블록체인에 등록하거나 상기 지급 결제 서버에 연동되는 타 장치를 통해 상기 트랜잭션 데이터를 상기 블록체인에 등록하도록 지원하고, 상기 푸시 토큰 아이디와 서명 요청 정보를 상기 사용자 단말로 전송하거나 상기 지급 결제 서버에 연동되는 타 장치 또는 상기 서비스 단말을 통해 상기 푸시 토큰 아이디와 상기 서명 요청 정보를 상기 사용자 단말로 전송하도록 지원하는 프로세스와, 상기 사용자 단말로부터의 서명값이 획득되면, 상기 서명값을 검증하거나 상기 지급 결제

서버에 연동되는 타 장치를 통해 상기 서명값을 검증하도록 지원하고, 상기 서명값이 유효일 경우, 상기 지급 수단 토큰 아이디, 상기 주문 아이디, 및 상기 주문 요청 정보 중 적어도 하나 이상을 포함하는 승인 요청 정보를 펀드 소스 서버로 전송하거나 상기 결제 지원 서버와 연동하는 타 장치를 통해 상기 승인 요청 정보를 상기 펀드 소스 서버로 전송하도록 지원하는 프로세스와, 상기 펀드 소스 서버로부터의 승인 결과 정보가 획득되면, 상기 승인 결과 정보를 상기 블록체인에 등록하거나 상기 결제 지원 서버에 연동되는 타 장치를 통해 상기 승인 결과 정보를 상기 블록체인에 등록하도록 지원하며, 상기 승인 결과 정보에 대응한 승인 완료 정보를 상기 서비스 단말로 전송하거나 상기 결제 지원 서버에 연동되는 타 장치를 통해 상기 승인 완료 정보를 상기 서비스 단말로 전송하도록 지원하는 프로세스를 수행하는 프로세서; 를 포함하는 지급 결제 서버가 제공된다.

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

발명의 효과

- [16] 본 발명에 의하면, 다음과 같은 효과가 있다.
- [17] 본 발명은 카드 사용에 대한 승인 과정에서 수수료를 최소화할 수 있다.
- [18] 또한, 본 발명은 카드 사용에 관한 트랜잭션을 블록체인에 등록하고 관리함으로써 카드 사용 정보의 위변조가 불가능하도록 할 수 있다.
- [19] 또한, 본 발명은 카드 사용의 승인에서 VAN사나 PG사를 이용하지 않고 블록체인을 이용함으로써 시스템을 간소화할 수 있을 뿐만 아니라 유지 비용을 절감할 수 있다.

도면의 간단한 설명

- [20] 도 1은 종래의 카드 결제 시스템을 개략적으로 도시한 것이고,
- [21] 도 2는 본 발명의 일 실시예에 따른 블록체인 기반의 결제 시스템을 개략적으로 도시한 것이고,
- [22] 도 3은 본 발명의 일 실시예에 따른 블록체인 기반의 결제 방법을 개략적으로 도시한 것이고,
- [23] 도 4와 도 5는 본 발명의 일 실시예에 따른 블록체인 기반의 결제 방법에서 결제와 관련한 트랜잭션을 블록체인에 등록하는 다른 실시예를 개략적으로 도시한 것이고,
- [24] 도 6은 본 발명의 일 실시예에 따른 블록체인 기반의 결제 방법에서 지불 정보를 등록하는 방법을 개략적으로 도시한 것이다.

발명의 실시를 위한 최선의 형태

- [25] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 당업자가 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.

- [26] 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.
- [27] 도 2는 본 발명의 일 실시예에 따른 블록체인 기반의 결제 시스템을 개략적으로 도시한 것으로, 시스템은 사용자 단말(100), 서비스 제공 단말(200), 지급 결제 서버(300), 및 펀드 소스 서버(400)를 포함할 수 있다.
- [28] 먼저, 사용자 단말(100)은 사용자에게 서비스되는 정보를 표시하여 주며 결제를 위한 정보의 입력 및 표시를 위한 디바이스로, PC, 모바일 컴퓨터, PDA/EDA, 휴대 전화, 스마트폰, 태블릿 등을 포함할 수 있다. 그리고, 사용자 단말(100)은 이에 한정되지 않으며, 유무선 통신 기능을 가진 휴대용 게임기, 디지털 카메라, 개인 내비게이션 등의 모든 통신 디바이스를 포함할 수 있다. 또한, 사용자 단말(100)은 정보의 송수신을 지원하는 통신부와 정보를 처리하는 프로세서를 포함할 수 있다. 이에 더하여, 사용자 단말(100)은 지급 결제 서버(300) 또는 서비스 제공 단말(200)에서 제공하는 사용자 인터페이스인 앱(APP; application)을 포함할 수 있다.
- [29] 다음으로, 서비스 제공 단말(200)은 사용자가 사용할 수 있는 다양한 서비스를 제공하여 주는 것으로, 정보의 송수신을 지원하는 통신부와 정보를 처리하는 프로세서를 포함할 수 있다. 또한, 서비스 제공 단말(200)은 사용자 단말(100)에 의한 구매 및 지불 정보에 대응되는 주문 요청 정보를 생성하여 사용자의 결제 펀드 소스에 대응되는 지급 수단에 따른 결제를 수행하는 단말로, 오프라인 쇼핑물의 결제 단말 또는 온라인 쇼핑물의 결제 서버를 포함할 수 있으며, 오프라인 쇼핑물의 결제 단말 또는 온라인 쇼핑물의 결제 서버와 연동하여 사용자에게 제공된 서비스 또는 물품에 대한 결제를 수행하는 서버를 포함할 수 있다. 이에 더하여, 서비스 제공 단말(200)은 온라인 또는 오프라인에서 서비스 제공 또는 제품의 구매에 대응하는 비용을 사용자 소유의 펀드 소스에 대응하는 지급 수단을 이용하여 결제할 수 있도록 하는 모든 단말을 포함할 수 있다.
- [30] 다음으로, 지급 결제 서버(300)는 블록체인 기반의 결제를 수행하는 것으로, 통신부와 프로세서를 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 지급 결제 서버(300)를 통해 해당 방법을 수행할 수도 있다. 또한, 지급 결제 서버(300)는 블록체인의 각각의 노드에 대응하는 서버이거나, 블록체인의 노드를 관리하는 서버 또는 트랜잭션 서버일 수 있다.

[31] 구체적으로, 지급 결제 서버(300)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 시스템)와 컴퓨터 소프트웨어(즉, 컴퓨팅 장치로 하여금 특정의 방식으로 기능하게 하는 인스트럭션들)의 조합을 이용하여 원하는 시스템 성능을 달성하는 것일 수 있다.

[32] 이와 같은 컴퓨팅 장치의 통신부는 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.

[33] 또한, 컴퓨팅 장치의 프로세서는 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.

[34] 다음으로, 펀드 소스 서버(400)는 통신부와 프로세서를 포함할 수 있으며, 사용자의 지급 수단 사용에 대한 승인 및 서비스 제공자의 정산에 대한 서비스를 제공하여 줄 수 있다. 이때, 정산에 대한 서비스는 지급 결제를 위한 매입, 청구, 및 정산을 포함할 수 있다. 그리고, 펀드 소스 서버(400)는 사용자가 지급 결제에 사용하고자 하는 펀드 소스를 관리하는 서버일 수 있으나, 이에 한정되는 것은 아니며, 펀드 소스에 대응되는 지급 수단에 대한 승인 서비스를 제공하는 모든 서버를 포함할 수 있다. 또한, 펀드 소스 서버(400)는 지급 결제 서버(300)와의 통신을 통해 지급 수단 사용에 필요한 각종 정보의 확인 동작을 수행할 수 있다. 이때, 펀드 소스는 사용자의 은행 계좌, 신용카드, 상품권, 멤버쉽카드, 쿠폰, 포인트 등을 포함할 수 있으나, 이에 한정되지 않으며, 지급 결제가 가능한 모든 가치 보유 장치 또는 정보를 포함할 수 있으며, 지급 수단은 펀드 소스에 대응하여 펀드 소스를 인식할 수 있도록 하는 장치 또는 정보일 수 있다.

[35] 구체적으로, 펀드 소스 서버(400)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 시스템)와 컴퓨터 소프트웨어(즉, 컴퓨팅 장치로 하여금 특정의 방식으로 기능하게 하는 인스트럭션들)의 조합을 이용하여 원하는 시스템

성능을 달성하는 것일 수 있다.

- [36] 이와 같이 구성된 시스템을 통해 본 발명의 일 실시예에 따른 블록체인 기반의 결제 시스템에서 결제를 수행하는 방법을 도 3을 참조하여 설명하면 다음과 같다.
- [37] 먼저, 사용자의 지불 정보, 일 예로, 사용자의 지급 수단에 대응되는 지급 수단 토큰 아이디, 사용자를 식별하기 위한 사용자 식별 정보, 사용자의 사용자 단말(100)에 설치된 앱에 대응되는 푸시 토큰 아이디, 및 사용자의 퍼블릭 키가 블록체인(500)에 등록된 상태에서, 사용자가 온라인 또는 오프라인에서 서비스 이용 또는 제품 구매 등에 따른 비용을 결제하기 위하여 서비스 제공 단말(200)로 사용자의 펀드 소스에 따른 지급 수단에 대응하는 사용자 식별 정보를 입력하거나 제공하여 주문 정보에 대한 결제를 요청하면(S1), 서비스 제공 단말(200)은 사용자에게 의해 주문된 서비스 또는 제품들에 대한 정보인 주문 정보를 저장하고, 사용자 식별 정보와 주문 정보를 포함하는 주문 요청 정보를 지급 결제 서버(300)로 전송하거나 서비스 제공 단말(200)에 연동되는 타 장치로 하여금 주문 요청 정보를 지급 결제 서버(300)로 전송하도록 지원한다(S2). 이때, 주문 정보는 상품명, 상품 수량, 단가, 가격 등과 같이 사용자가 구매하거나 이용한 제품 또는 서비스에 대한 상세 정보를 포함할 수 있다. 또한, 사용자 식별 정보는 사용자의 식별을 위하여 사용자 별로 주어지는 고유 정보로서, 사용자 아이디, 주민번호, 사용자 단말 아이디, 사용자 단말의 아이피 주소, 사용자 단말의 MAC 어드레스, 전화번호, 및 이들 각각의 해시값 중 적어도 하나 이상을 포함할 수 있다. 또한, 블록체인(500)은 다수의 블록체인으로 구성될 수 있으며, 블록체인(500)이 제1 블록체인과 제2 블록체인으로 구성될 경우, 지불 정보는 제1 블록체인에 등록되며, 지불 정보에 해시함수를 적용하여 생성한 제1 해시값과 제1 해시값과 매칭되는 적어도 하나의 이웃 해시값을 연산한 제1 대표 해시값 또는 제1 대표 해시값을 가공한 값이 제2 블록체인에 등록될 수 있다.
- [38] 그러면, 지급 결제 서버(300)는 서비스 제공 단말(200)로부터 획득되는 주문 요청 정보의 사용자 식별 정보에 대응하는 푸시 토큰 아이디를 블록체인(500)으로부터 획득하거나 지급 결제 서버(300)에 연동되는 타 장치로 하여금 사용자 식별 정보에 대응하는 푸시 토큰 아이디를 블록체인(500)으로부터 획득하도록 지원한다(S3)(S4). 일 예로, 지급 결제 서버(300)는 사용자 식별 정보에 대응하는 블록체인 트랜잭션 아이디를 확인하며, 블록체인 트랜잭션 아이디를 이용하여 블록체인(500)에 등록된 지불 정보 트랜잭션을 획득하며, 획득된 지불 정보 트랜잭션에 포함된 푸시 토큰 아이디를 확인하게 된다.
- [39] 한편, 블록체인(500)이 다수의 블록체인으로 구성될 수 있으며, 블록체인(500)이 제1 블록체인과 제2 블록체인으로 구성될 경우, 지급 결제 서버(300)는 주문 요청 정보에 포함된 사용자 식별 정보를 참조하여 제2 블록체인으로 부터 제1 대표 해시값 또는 제1 대표 해시값을 가공한 값을

획득하거나 지급 결제 서버(300)에 연동되는 타 장치로 하여금 제2 블록체인으로부터 제1 대표 해시값 또는 제1 대표 해시값을 가공한 값을 획득하도록 지원하며, 제1 대표 해시값 또는 제1 대표 해시값을 가공한 값과 관련되어 제1 블록체인에 등록된 머클 트리 정보 및 리프 노드 정보를 획득하거나 지급 결제 서버(300)에 연동되는 타 장치로 하여금 머클 트리 정보 및 리프 노드 정보를 획득하도록 지원한다. 그리고, 지급 결제 서버(300)는 획득된 머클 트리 정보 및 리프 노드 정보를 참조하여 제1 블록체인으로부터 푸시 토큰 아이디를 획득하거나 지급 결제 서버(300)에 연동되는 타 장치로 하여금 푸시 토큰 아이디를 획득하도록 지원할 수 있다.

[40] 그리고, 지급 결제 서버(300)는 주문 요청 정보에 대응하는 주문 아이디를 생성하고, 적어도 생성된 주문 아이디와 주문 정보 중 적어도 하나를 포함하는 트랜잭션 데이터를 블록체인(500)에 등록하거나 지급 결제 서버(300)에 연동되는 타 장치를 통해 트랜잭션 데이터가 블록체인(500)에 등록하도록 지원한다(S5). 이때, 지급 결제 서버(300)는 주문 정보들을 리프노드로 한 머클트리를 연산하며, 연산된 머클트리의 루트 해시값 또는 루트 해시값을 가공한 값을 주문 아이디로 생성한다.

[41] 한편, 상기에서는 트랜잭션 데이터를 블록체인(500)에 등록하였으나, 블록체인(500)이 다수로 이루어질 수 있으며, 일 예로, 블록체인(500)이 제1 블록체인과 제2 블록체인으로 구성될 경우, 지급 결제 서버(300)가 트랜잭션 데이터를 제1 블록체인과 제2 블록체인에 등록하는 과정을 상세히 설명하면 다음과 같다.

[42] 지급 결제 서버(300)는 트랜잭션 데이터를 제1 블록체인에 등록하거나 지급 결제 서버(300)에 연동되는 타 장치로 하여금 제1 블록체인에 등록하도록 한다.

[43] 그리고, 제2 블록체인에 소정의 해시값을 등록하기 위한 트리거링 조건이 만족되면, 지급 결제 서버(300)는 트랜잭션 데이터에 해시합수를 적용하여 생성한 제2 해시값과 제2 해시값에 매칭되는 적어도 하나의 이웃 해시값을 연산함으로써 머클 루트인 제2 대표 해시값 또는 제2 대표 해시값을 가공한 값을 생성한다.

[44] 또한, 지급 결제 서버(300)는 생성된 제2 대표 해시값 또는 제2 대표 해시값을 가공한 값을 제2 블록체인에 등록하거나 지급 결제 서버(300)에 연동되는 타 장치 또는 제1 블록체인으로 하여금 제2 대표 해시값 또는 제2 대표 해시값을 가공한 값을 제2 블록체인에 등록하도록 할 수 있다.

[45] 한편, 지급 결제 서버(300)는 제2 해시값과 적어도 하나의 이웃 해시값을 소정의 데이터 구조로 저장하여 관리할 수 있다. 여기서, 데이터 구조는 다양할 수 있는 데, 일 예로 머클 트리(merkle tree) 구조가 될 수도 있다.

[46] 즉, 지급 결제 서버(300)는 제2 해시값이 특정 리프 노드에 할당된 머클 트리(merkle tree)를 생성하거나 생성하도록 지원할 수 있고, 트리거링 조건이 만족되면, 제2 해시값과 매칭되는 적어도 하나의 다른 리프 노드에 할당된

해시값을 연산하여 생성되는 머클 루트인 제2 대표 해시값 또는 제2 대표 해시값을 가공한 값을 제2 블록체인에 등록하거나 지급 결제 서버(300)에 연동되는 타 장치 또는 제1 블록체인으로 하여금 제2 블록체인에 등록하도록 지원할 수 있다.

- [47] 좀더 구체적으로 설명하면, (x1) 지급 결제 서버(300)는, (i) 제2 해시값과 (ii) 제2 해시값이 할당된 노드의 형제 노드에 할당된 해시값을 연산하거나 지급 결제 서버(300)에 연동된 타 장치로 하여금 연산하도록 지원하고, 연산값에 대한 해시값을 노드의 부모 노드에 할당하거나 지급 결제 서버(300)에 연동된 타 장치로 하여금 부모 노드에 할당하도록 지원할 수 있다. (x2) 만일, 부모 노드가 머클 트리의 루트 노드이면, 부모 노드에 할당된 해시값이 제2 대표 해시값 또는 제2 대표 해시값을 가공한 값이 된다. (x3) 반면, 부모 노드가 머클 트리의 루트 노드가 아니면, 지급 결제 서버(300)는, 부모 노드에 할당된 해시값을 제2 해시값으로 하여 (x1) 내지 (x3)를 반복하여 수행한다.
- [48] 그리고, 지급 결제 서버(300)는 최종적으로 머클 트리의 루트 노드에 할당된 해시값을 제2 대표 해시값 또는 제2 대표 해시값을 가공한 값으로서 제2 블록체인에 등록하거나 지급 결제 서버(300)에 연동된 타 장치 또는 제1 블록체인으로 하여금 제2 블록체인에 등록하도록 지원한다. 이때, 제2 대표 해시값을 가공한 값은, 예를 들어, 제2 대표 해시값에 hex 연산이 수행된 결과값일 수 있다.
- [49] 한편, 지급 결제 서버(300)가 제2 해시값과 적어도 하나의 이웃 해시값을 소정의 제1-1 데이터 구조로 저장하고, 이후 제1-1 데이터 구조와 동일한 형태의 제1-2 데이터 구조를 저장하여 관리하는 경우, 제1-1 데이터 구조와 제1-2 데이터 구조는 체인 형태로 연결될 수 있다.
- [50] 특히, 상술한 예에서와 같이 제1-1 데이터 구조 및 제1-2 데이터 구조가 머클 트리인 경우, 제1-1 데이터 구조의 루트값 또는 루트값의 해시값이 제1-2 데이터 구조의 첫번째 리프 노드에 할당될 수 있다.
- [51] 또한, 제1-2 데이터 구조를 생성할 때는 제1-1 데이터 구조에 대한 검증이 이루어짐으로써 데이터 integrity가 좀더 보장될 수 있다. 제1-2 데이터 구조의 검증에 대해서는 후술하기로 한다.
- [52] 또한, 체인 형태로 연결된 적어도 하나의 머클 트리 중 첫번째 머클 트리의 경우, 첫번째 머클 트리의 첫번째 리프 노드에는 텍스트, 숫자, 또는 기호로 이루어진 소정의 메시지 데이터의 해시값 또는 이를 가공한 값이 할당될 수 있다. 예를 들어, 머클 트리 생성시 지급 결제 서버(300)에 의해 최초로 부여된 입력 메시지의 해시값이 할당될 수 있다.
- [53] 도 4 및 도 5는 본 발명의 일 실시예에 따라 생성된 머클 트리의 예를 도시한 것이다.
- [54] 도 4에서는 리프 노드의 개수가 4개인 머클 트리가 도시된다. 도시된 머클 트리는 첫번째 머클 트리이기 때문에(tree_id=0), 첫번째 리프 노드인 h0

노드에는 소정의 메시지 데이터의 해시값 (sha256(coinplug_unique_message))이 할당되었음을 알 수 있다. 기록 데이터에 대한 등록 요청이 있는 경우, 지급 결제 서버(300)는 현재 구성 중인 머클 트리의 가장 마지막 리프 노드의 다음 리프 노드를 생성하여 제2 해시값 또는 제2 해시값을 가공한 값을 할당하거나 할당하도록 지원한다. 예를 들어, 도 4의 머클 트리에서 두번째 리프 노드인 h1 노드까지 값 할당이 완료된 상태에서 새로운 리프 노드를 생성하여야 하는 경우, 다음 리프 노드인 h2 노드를 생성하여 제2 해시값 또는 제2 해시값을 가공한 값(sha256(input2))을 할당할 수 있다. 또한, 지급 결제 서버(300)는 (i) h2 노드에 할당된 제2 해시값과 (ii) h2 노드의 형제 노드인 h3 노드에 할당된 해시값을 연산하거나 연산하도록 지원할 수 있다. 연산값에 대한 해시값은 h2 노드와 h3 노드의 부모 노드(h23 노드)에 할당된다. 부모 노드(h23 노드)가 머클 트리의 루트 노드가 아니므로 지급 결제 서버(300)는 h23 노드에 할당된 해시값을 제2 해시값으로 하여 상기 과정을 반복하여 수행할 수 있다. 즉, h23 노드에 할당된 해시값을 제2 해시값으로 하고, h23 노드에 할당된 해시값과 h01 노드에 할당된 해시값을 연산하여 h23 노드와 h01 노드의 부모 노드(h0123 노드)에 할당할 수 있다. 이때, h0123 노드가 머클 트리의 루트 노드이므로 지급 결제 서버(300)는, h0123 노드에 할당된 해시값을 가공한 값(hex(h{node_index}))을 제2 블록체인에 등록하거나 지급 결제 서버(300)에 연동된 타 장치 또는 제1 블록체인으로 하여금 제2 블록체인에 등록하도록 지원할 수 있다

- [55] 한편, 전술한 트리거링 조건이란, (i) 소정의 개수만큼 결제와 관련한 트랜잭션이 생성되는 조건, (ii) 소정 시간이 경과하는 조건, (iii) 제1 블록체인에서 블록이 생성되는 조건, (iv) 서비스 특성에 대한 조건 중 적어도 하나를 포함할 수 있다.
- [56] 한편, 예를 들어, 결제와 관련한 트랜잭션이 머클 트리의 리프 노드 수만큼 획득되면 지급 결제 서버(300)는 머클 트리를 생성하고, 머클 트리의 루트값을 제2 블록체인에 등록하거나 지급 결제 서버(300)에 연동된 타 장치로 하여금 등록하도록 지원할 수 있다.
- [57] 또한, 지급 결제 서버(300)는 소정 시간 단위로 전술한 머클 트리의 루트값을 생성할 수 있다(상기 (ii) 조건). 이 경우 지급 결제 서버(300)는 소정의 시간이 경과되면 그때까지의 입력값을 이용하여 머클 트리를 생성하고 머클 트리의 루트값을 제2 블록체인에 등록하거나 지급 결제 서버(300)에 연동된 타 장치 또는 제1 블록체인으로 하여금 제2 블록체인에 등록하도록 지원할 수 있다.
- [58] 그런데, 이 경우에는 소정 시간이 경과하였음에도 머클 트리의 특정 해시값이 할당된 노드의 형제 노드에 값이 할당되지 않을 수 있다. 이처럼 트리거링 조건이 만족되었음에도 제2 해시값이 할당된 노드의 형제 노드에 해시값이 할당되어 있지 않은 경우, 지급 결제 서버(300)는, 형제 노드에 소정의 해시값을 할당하거나 할당하도록 지원하여 전술한 방식으로 머클 트리의 루트값이 산출되도록 할 수 있다. 예를 들어, 지급 결제 서버(300)는 제2 해시값을 복제하여

형제 노드에 할당하거나 할당하도록 지원할 수 있다.

- [59] 그리고, 서비스 특성이란, 결제와 관련한 트랜잭션을 발행한 발행자가 제공한 비용 정보, 결제 관련 트랜잭션 등록이 이루어지는 시간대 정보, 결제 관련 트랜잭션 등록 서비스가 이루어지는 지역 정보, 결제 관련 트랜잭션 등록 요청을 한 회사 타입 정보 중 적어도 일부가 될 수 있다. 다만, 여기서 기재한 것에 한정할 것은 아니고, 통상적으로 인정되는 차등적 서비스가 제공될 수 있는 다양한 조건 정보를 포함한다.
- [60] 한편, 새로운 머클 트리 생성이 시작되고, 결제 관련 트랜잭션이 없는 상태에서 트리거링 조건이 만족되면, 지급 결제 서버(300)는, 소정의 메시지 데이터가 첫번째 리프 노드와 두번째 리프 노드에 할당된 머클 트리를 생성하거나 생성하도록 지원하고, 머클 트리의 루트값 또는 이를 가공한 값을 제2 블록체인에 등록하거나 지급 결제 서버(300)에 연동된 타 장치 또는 제1 블록체인으로 하여금 제2 블록체인에 등록하도록 지원할 수 있다. 이 경우에는 리프 노드 2개짜리 머클 트리가 생성될 수도 있는 것이다.
- [61] 또한, 전술한 것처럼 지급 결제 서버(300)가 제2 해시값과 적어도 하나의 이웃 해시값을 소정의 제1-1 데이터 구조로 저장하고, 이후 제1-1 데이터 구조와 동일한 형태의 제1-2 데이터 구조를 저장하여 관리하는 경우, 제1-1 데이터 구조와 제1-2 데이터 구조는 체인 형태로 연결될 수 있다. 특히, 제1-1 데이터 구조 및 제1-2 데이터 구조가 머클 트리인 경우, 제1-1 데이터 구조의 루트값 또는 루트값의 해시값이 제1-2 데이터 구조의 첫번째 리프 노드에 할당될 수 있다.
- [62] 도 5는 본 발명의 일 실시예에 따라 제1-2 데이터 구조로서 생성된 머클 트리를 도시한 도면이다.
- [63] 도 5를 참조하면, 도 4의 머클 트리(tree_id=0)의 루트값(hex(h0123))이 새로운 머클 트리의 첫번째 리프 노드(h4 노드)에 할당되었음을 알 수 있다(sha256(input4)). 본 발명은 이와 같이 트랜잭션 발생시 생성되는 복수의 데이터 구조를 연결함으로써 중간에 데이터가 변조가 발생하는 경우라도 쉽게 트래킹이 가능하여 데이터 integrity를 향상시키는 장점을 가진다.
- [64] 다시, 도 3을 참조하면, 지급 결제 서버(300)는 푸시 토큰 아이디와 서명 요청 정보를 사용자 단말(100)로 전송하거나, 서비스 제공 단말(200)을 통해 푸시 토큰 아이디와 서명 요청 정보가 사용자 단말(100)로 전송되도록 한다(S6)(S7). 이때, 서명 요청 정보에는 주문 정보 또는 검증 확인값을 포함할 수 있다.
- [65] 그러면, 사용자 단말(100)은 푸시 토큰 아이디에 대응하는 결제 요청된 펀드 소스에 해당하는 앱을 실행하고, 사용자에게 검증 확인값에 대한 전자 서명을 요청하거나, 주문 정보에 대한 확인과 전자 서명에 대한 요청 정보를 표시하여 주며(S8), 사용자가 전자 서명 요청을 확인하거나 주문 정보가 자신이 주문한 내용과 일치하는 것을 확인한 후, 비밀번호, PIN 코드, 지문, 및 생체 정보 중 적어도 하나를 포함하는 자신이 설정한 확인 정보를 입력하면, 사용자 단말(100)은 사용자에게 의해 입력되는 확인 정보가 사용자에게 의해 기설정된 확인

정보와 일치하는 지를 확인한다.

- [66] 그리고, 사용자에게 의해 입력된 확인 정보가 기설정된 확인 정보와 일치할 경우, 사용자 단말(100)은 검증 확인값 또는 주문 정보에 대한 사용자 서명값을 생성하여(S9) 지급 결제 서버(300)로 전송하거나 서비스 제공 단말(200)을 통해 지급 결제 서버(300)로 전송되도록 지원한다(S10). 일 예로, 사용자 단말(100)은 사용자에게 의해 입력된 확인 정보가 기설정된 확인 정보와 일치할 경우 저장된 사용자의 프라이빗 키에 대한 접근이 허용되며, 그에 따라 사용자의 프라이빗 키로 검증 확인값 또는 주문 정보를 서명한 사용자 서명값을 생성하며, 생성된 사용자 서명값을 지급 결제 서버(300)로 전송하여 주거나 서비스 제공 단말(200)을 통해 지급 결제 서버(300)로 전송되도록 한다.
- [67] 그러면, 지급 결제 서버(300)는 사용자 단말(100)로부터의 검증 확인값 또는 주문 정보를 서명한 사용자 서명값을 획득하며, 획득된 사용자 서명값이 유효한지를 확인하거나 지급 결제 서버(300)에 연동된 타 장치로 하여금 서명값이 유효한지를 확인하도록 지원한다(S11). 일 예로, 지급 결제 서버(300)는 사용자 식별 정보에 대응하여 블록체인(500)에 등록된 사용자의 퍼블릭 키를 획득하며, 획득된 퍼블릭 키를 이용하여 사용자 서명값이 유효한지를 확인한다. 즉, 지급 결제 서버(300)는 퍼블릭 키를 이용하여 서명값으로부터 주문 정보 또는 검증 확인값을 추출하며, 서명값으로부터 추출된 주문 정보 또는 검증 확인값이 서명 요청 정보에 포함된 주문 정보 또는 검증 확인값과 일치하는지를 확인하여 서명값의 유효 여부를 판단할 수 있다.
- [68] 한편, 블록체인(500)은 제1 블록체인과 제2 블록체인으로 구성될 수 있으며, 퍼블릭 키는 제1 블록체인에 등록되고, 제2 블록체인에는 퍼블릭 키의 해시값을 리프 노드로 한 머클 트리의 루트 해시값이 등록될 수 있다. 이 경우, 지급 결제 서버(300)는 사용자 식별 정보에 대응하여 제2 블록체인에 등록된 루트 해시값을 확인하고, 제2 블록체인에서 확인된 루트 해시값에 대응하여 제1 블록체인에 등록된 머클 트리 정보 및 리프 노드 정보를 확인하며, 머클 트리 정보 및 리프 노드 정보를 참조하여 제1 블록체인에 등록된 퍼블릭 키를 확인하거나 타 장치로 하여금 확인하도록 지원할 수 있다.
- [69] 다시 도 3을 참조하면, 지급 결제 서버(300)는 사용자 서명값이 유효한 것으로 판단되면, 사용자 식별 정보에 대응하는 지급 수단 토큰 아이디를 블록체인(500)으로부터 획득하고, 지급 수단 토큰 아이디, 주문 아이디, 및 주문 요청 정보 중 적어도 하나 이상을 포함하는 승인 요청 정보를 펀드 소스 서버(400)로 전송하거나 결제 지원 서버(300)와 연동하는 타 장치를 통해 승인 요청 정보를 펀드 소스 서버(400)로 전송하도록 지원한다(S12). 이때, 블록체인(300)이 다수의 블록체인으로 구성되며, 일 예로, 제1 블록체인에 지급 수단 토큰 아이디가 등록되며, 제2 블록체인에 지급 수단 토큰 아이디에 대응되는 루트 해시값이 등록된 경우에도 지급 결제 서버(300)는 상기에서와 같은 방법에 의해 루트 해시값을 이용하여 지급 수단 토큰 아이디를 획득할 수

있다.

- [70] 그러면, 펀드 소스 서버(400)는 승인 요청 정보에 포함된 지급 수단 토큰 아이디의 유효성을 확인하며, 주문 정보를 검증하고, 검증 결과에 대응하는 승인 결과를 지급 결제 서버(300)로 전송하거나 타 장치로 하여금 전송하도록 지원한다(S13). 이때, 펀드 소스 서버(400)는 블록체인(500)을 통한 주문 정보를 참조하여 머클 트리에 의한 루트 해시값을 생성하고, 승인 요청 정보에 포함된 주문 아이디와 비교하여 주문 정보를 검증할 수 있다.
- [71] 그리고, 지급 결제 서버(300)는 펀드 소스 서버(400)로부터 승인 결과가 획득되면, 주문 요청에 대한 승인 결과 정보를 블록체인(500)에 등록하거나 타 장치로 하여금 등록하도록 지원하고, 승인 완료 정보를 서비스 제공 단말(200) 또는 사용자 단말(100)로 전송하거나 지급 결제 서버(300)에 연동되는 타 장치로 하여금 승인 완료 정보를 전송하도록 지원한다(S14)(S15). 이때, 지급 결제 서버(300)는 블록체인(500)에 등록된 승인 결과 정보의 블록체인(500) 상의 위치 정보를 나타내는 승인 결과 트랜잭션 아이디를 획득하고, 승인 결과 트랜잭션 아이디를 승인 결과 정보에 포함할 수 있다.
- [72] 또한, 블록체인(500)은 제1 블록체인과 제2 블록체인으로 구성될 수 있으며, 지급 결제 서버(300)는 승인 결과 정보를 제1 블록체인에 등록하거나 지급 결제 서버(300)에 연동되는 타 장치로 하여금 제1 블록체인에 등록하도록 지원하고, 제2 블록체인에 소정의 해시값을 등록하기 위한 트리거링 조건이 만족되면, 지급 결제 서버(300)는 승인 결과 정보에 해시함수를 적용하여 생성한 제3 해시값과 제3 해시값에 매칭되는 적어도 하나의 이웃 해시값을 연산함으로써 머클 루트인 제3 대표 해시값 또는 제3 대표 해시값을 가공한 값을 생성하며, 생성된 제3 대표 해시값 또는 제3 대표 해시값을 가공한 값을 제2 블록체인에 등록하거나 지급 결제 서버(300)에 연동되는 타 장치 또는 제1 블록체인으로 하여금 제3 대표 해시값 또는 제3 대표 해시값을 가공한 값을 제2 블록체인에 등록하도록 할 수 있다. 이에 대한 상세한 설명은 트랜잭션 데이터를 등록하는 과정으로부터 용이하게 확인할 수 있으므로 생략하기로 한다.
- [73] 한편, 상기와 같은 방법에 의해 주문 정보들에 대한 결제를 수행하며, 펀드 소스 서버(400)로부터의 정산 데이터 요청 정보가 획득되면(S21), 결제 지원 서버(300)는, 정산 데이터 요청 정보에 대응하는 트랜잭션 데이터를 참조하여 블록체인(500)으로부터 정산 요청된 주문 정보를 포함하는 정산 데이터를 획득하거나 결제 지원 서버(300)에 연동되는 타 장치로 하여금 정산 데이터를 블록체인(500)으로부터 획득하도록 지원하며(S22)(S23), 블록체인(500)으로부터 획득된 정산 데이터를 펀드 소스 서버(400)로 전송하거나 지급 결제 서버(300)에 연동되는 타 장치를 통해 펀드 소스 서버(400)로 전송하도록 지원함으로써(S24) 펀드 소스 서버(400)로 하여금 정산 데이터를 참조하여 비용을 정산하도록 한다. 이때, 비용의 정산은 매입, 청구의 개념도 포함할 수 있다. 또한, 블록체인(500)이 제1 블록체인과 제2 블록체인으로 구성된 경우에도, 제2 대표 해시값 또는 제2

대표 해시값을 가공한 값, 즉, 루트 해시값을 이용하여 상기에서와 같은 방법에 의해 정산 데이터를 확인할 수 있다.

- [74] 즉, 결제 지원 서버(300)는, 정산 데이터 요청 정보에 대응하는 트랜잭션 데이터를 참조하여 제2 블록체인으로부터 제2 대표 해시값 또는 제2 대표 해시값을 가공한 값을 획득하거나 지급 결제 서버(300)에 연동된 타 장치로 하여금 제2 대표 해시값 또는 제2 대표 해시값을 가공한 값을 획득하도록 지원하고, 제2 대표 해시값 또는 제2 대표 해시값을 가공한 값과 관련되어 제1 블록체인에 등록된 머클 트리 정보 및 리프 노드 정보를 획득하거나 지급 결제 서버(300)에 연동된 타 장치로 하여금 머클 트리 정보 및 리프 노드 정보를 획득하도록 지원하며, 머클 트리 정보 및 리프 노드 정보를 참조하여 제1 블록체인으로 부터 정산 요청된 주문 정보를 포함하는 정산 데이터를 획득하거나 결제 지원 서버(300)에 연동되는 타 장치로 하여금 정산 데이터를 제1 블록체인으로 부터 획득하도록 지원하며, 제1 블록체인으로 부터 획득된 정산 데이터를 펀드 소스 서버(400)로 전송하거나 결제 지원 서버(300)에 연동되는 타 장치를 통해 정산 데이터를 펀드 소스 서버(400)로 전송하도록 지원함으로써 펀드 소스 서버(400)로 하여금 정산 데이터를 참조하여 비용을 정산하도록 할 수 있다.
- [75] 그리고, 상기에서의 사용자의 지급 수단에 대응되는 지급 수단 토큰 아이디, 상기 사용자를 식별하기 위한 사용자 식별 정보, 상기 사용자의 사용자 단말에 설치된 앱에 대응되는 푸시 토큰 아이디, 및 상기 사용자의 퍼블릭 키를 포함하는 지불 정보를 블록체인(500)에 등록하는 방법을 도 6을 참조하여 설명하면 다음과 같다.
- [76] 먼저, 사용자가 사용하고자 하는 펀드 소스를 등록하기 위하여 사용자 단말(100)에 설치된 펀드 소스에 대응되는 앱을 통해 펀드 소스 서버(400)에 접속한 상태에서, 사용자 단말(100)이 지불 정보 등록을 위한 개인 정보, 사용자 식별 정보, 지급 수단 정보, 및 퍼블릭 키 등을 포함하는 사용자 인증 및 지불 정보 등록 요청을 펀드 소스 서버(400)로 전송하거나 사용자 단말(100)에 연동되는 타 장치를 통해 펀드 소스 서버(400)로 전송하도록 지원한다(S31). 이때, 개인 정보는 사용자의 성명, 생년월일, 사용자 아이디, 주민번호, 사용자 단말 아이디, 사용자 단말의 아이피 주소, 사용자 단말의 MAC 어드레스, 및 전화번호 중 적어도 어느 하나 이상을 포함할 수 있으며, 사용자 식별 정보는 개인 정보 중 특정 개인 정보로서 사용자의 식별을 위하여 사용자 별로 주어지는 고유 정보일 수 있다. 그리고, 지급 수단 정보는 펀드 소스를 이용한 비용 지급을 위한 결제 수단에 대한 정보일 수 있다. 일 예로, 지급 수단은 카드, 상품권, 포인트, 멤버십 카드, 디지털 전자 지갑 등을 포함할 수 있으며, 지급 수단 정보는 이들을 식별할 수 있도록 하는 식별 정보, 즉, 발급 주체인 펀드 소스 정보, 유효 기간, 사용자 정보 등을 포함할 수 있다.
- [77] 이때, 사용자 단말(100)은 사용자의 개인 정보, 사용자 식별 정보를 사용자가

입력하도록 하는 것과는 달리, 사용자 단말(100)의 저장부로부터 추출하여 전송하여 줄 수도 있다.

- [78] 그러면, 펀드 소스 서버(400)는 사용자 단말(100)로부터 개인 정보, 사용자 식별 정보, 지급 수단 정보, 및 퍼블릭 키 등을 포함하는 사용자 인증 및 지불 정보 등록 요청 정보를 획득하고, 사용자 인증을 수행한다(S32). 이때, 사용자 인증은 아이디/패스워드에 의한 인증, 스마트카드나 생체인식에 의한 인증, 공개키기반의 전자서명을 이용한 인증, 공인인증서를 이용한 인증 등 다양한 방법에 의해 수행될 수 있다.
- [79] 또한, 펀드 소스 서버(400)는 지급 수단에 대한 검증을 수행한다. 이때, 지급 수단에 대한 검증은 사용자 단말(100)로부터 전송된 지급 수단 정보가 등록된 지급 수단 원장 정보와 일치하는지를 확인함으로써 수행될 수 있다.
- [80] 이후, 펀드 소스 서버(400)는 인증된 사용자에게 대한 지불 정보를 생성한다(S33). 이때, 지불 정보는 지급 수단 토큰 아이디, 사용자 식별 정보, 푸시 토큰 아이디, 및 퍼블릭 키를 포함할 수 있다. 그리고, 지급 수단 토큰 아이디는 지급 수단 정보의 노출을 방지하기 위하여 지급 수단을 토큰화한 것이며, 푸시 토큰 아이디는 사용자 단말(100)에 설치된 펀드 소스 관련 앱을 호출할 수 있는 토큰 아이디일 수 있다.
- [81] 그리고, 펀드 소스 서버(400)는 생성된 지불 정보에 대한 등록 요청을 지급 결제 서버(300)로 전송하거나 펀드 소스 서버(400)에 연동되는 타 장치로 하여금 지불 정보 등록 요청을 지급 결제 서버(300)로 전송하도록 지원할 수 있다(S34).
- [82] 그러면, 지급 결제 서버(300)는 펀드 소스 서버(400)로부터의 지불 정보 등록 요청에 대응하여 지급 수단 토큰 아이디, 사용자 식별 정보, 푸시 토큰 아이디, 및 퍼블릭 키를 포함하는 지불 정보를 블록체인(500)에 등록하며(S35)(S36), 지불 정보 등록 완료에 대한 정보를 펀드 소스 서버(400)로 전송하거나 지급 결제 서버(300)에 연동되는 타 장치로 하여금 지불 정보 등록 완료 신호를 펀드 소스 서버(400)로 전송하도록 지원할 수 있다(S37).
- [83] 이때, 블록체인(500)은 다수의 블록체인으로 구성될 수 있으며, 일 예로, 블록체인(500)이 제1 블록체인과 제2 블록체인으로 구성될 경우, 지급 결제 서버(300)는 지불 정보를 제1 블록체인에 등록하거나 지급 결제 서버(300)에 연동되는 타 장치로 하여금 제1 블록체인에 등록하도록 지원하고, 제2 블록체인에 소정의 해시값을 등록하기 위한 트리거링 조건이 만족되면, 지급 결제 서버(300)는 지불 정보에 해시함수를 적용하여 생성한 제1 특정 해시값과 제1 특정 해시값에 매칭되는 적어도 하나의 이웃 해시값을 연산함으로써 머클 루트인 제1 대표 해시값 또는 제1 대표 해시값을 가공한 값을 생성하며, 생성된 제1 대표 해시값 또는 제1 대표 해시값을 가공한 값을 제2 블록체인에 등록하거나 지급 결제 서버(300)에 연동되는 타 장치 또는 제1 블록체인으로 하여금 제1 대표 해시값 또는 제1 대표 해시값을 가공한 값을 제2 블록체인에 등록하도록 할 수 있다.

- [84] 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.
- [85] 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.
- [86] 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.

청구범위

- [청구항 1] 블록체인 기반의 결제 방법에 있어서,
- (a) 사용자의 지급 수단에 대응되는 지급 수단 토큰 아이디, 상기 사용자를 식별하기 위한 사용자 식별 정보, 상기 사용자의 사용자 단말로 설치된 앱에 대응되는 푸시 토큰 아이디, 및 상기 사용자의 퍼블릭 키를 블록체인에 등록한 상태에서, 서비스 제공 단말로부터 사용자 단말의 구매 및 지불 정보에 대응하는 주문 요청 정보 - 상기 주문 요청 정보는 사용자 식별 정보, 및 주문 정보 중 적어도 하나 이상을 포함함 - 가 획득되면, 지급 결제 서버가, 상기 주문 요청 정보에 포함된 상기 사용자 식별 정보에 대응하는 상기 푸시 토큰 아이디를 상기 블록체인으로부터 획득하거나 상기 지급 결제 서버에 연동되는 타 장치를 통해 상기 푸시 토큰 아이디를 상기 블록체인으로부터 획득하도록 지원하고, 상기 주문 요청 정보에 대응하는 주문 아이디를 생성하며, 상기 주문 아이디와 상기 주문 정보 중 적어도 하나를 포함하는 트랜잭션 데이터를 상기 블록체인에 등록하거나 상기 지급 결제 서버에 연동되는 타 장치를 통해 상기 트랜잭션 데이터를 상기 블록체인에 등록하도록 지원하고, 상기 푸시 토큰 아이디와 서명 요청 정보를 상기 사용자 단말로 전송하거나 상기 지급 결제 서버에 연동되는 타 장치 또는 상기 서비스 단말을 통해 상기 푸시 토큰 아이디와 상기 서명 요청 정보를 상기 사용자 단말로 전송하도록 지원하는 단계;
- (b) 상기 사용자 단말로부터의 서명값이 획득되면, 상기 지급 결제 서버가, 상기 서명값을 검증하거나 상기 지급 결제 서버에 연동되는 타 장치를 통해 상기 서명값을 검증하도록 지원하고, 상기 서명값이 유효일 경우, 상기 지급 수단 토큰 아이디, 상기 주문 아이디, 및 상기 주문 요청 정보 중 적어도 하나 이상을 포함하는 승인 요청 정보를 펀드 소스 서버로 전송하거나 상기 결제 지원 서버와 연동하는 타 장치를 통해 상기 승인 요청 정보를 상기 펀드 소스 서버로 전송하도록 지원하는 단계; 및
- (c) 상기 펀드 소스 서버로부터의 승인 결과 정보가 획득되면, 상기 결제 지원 서버가, 상기 승인 결과 정보를 상기 블록체인에 등록하거나 상기 결제 지원 서버에 연동되는 타 장치를 통해 상기 승인 결과 정보를 상기 블록체인에 등록하도록 지원하며, 상기 승인 결과 정보에 대응한 승인 완료 정보를 상기 서비스 단말로 전송하거나 상기 결제 지원 서버에 연동되는 타 장치를 통해 상기 승인 완료 정보를 상기 서비스 단말로 전송하도록 지원하는 단계;
- 를 포함하는 것을 특징으로 하는 결제 방법.
- [청구항 2] 제1항에 있어서,
- (d) 상기 펀드 소스 서버로부터의 정산 데이터 요청 정보가 획득되면,

상기 결제 지원 서버는, 상기 정산 데이터 요청 정보에 대응하는 상기 주문 정보를 포함하는 정산 데이터를 상기 블록체인으로부터 획득하거나 상기 결제 지원 서버에 연동되는 타 장치를 통해 상기 정산 데이터를 상기 블록체인으로부터 획득하도록 지원하며, 상기 블록체인으로부터 획득된 상기 정산 데이터를 상기 펀드 소스 서버로 전송하거나 상기 결제 지원 서버에 연동되는 타 장치를 통해 상기 정산 데이터가 상기 펀드 소스 서버로 전송되도록 지원함으로써 상기 펀드 소스 서버로 하여금 상기 정산 데이터를 참조하여 비용을 정산하도록 하는 단계; 를 더 포함하는 것을 특징으로 하는 결제 방법.

[청구항 3] 제1항에 있어서,
상기 (a) 단계에서,
상기 결제 지원 서버는, 상기 주문 정보를 리프노드로 한 머클트리를 연산하며, 상기 연산된 머클트리의 루트 해시값 또는 상기 루트 해시값을 가공한 값을 상기 주문 아이디로 생성하는 것을 특징으로 하는 결제 방법.

[청구항 4] 제1항에 있어서,
상기 사용자 식별 정보는,
상기 사용자의 식별을 위하여 사용자 별로 주어지는 고유 정보로서,
사용자 아이디, 주민번호, 사용자 단말 아이디, 사용자 단말의 아이피 주소, 사용자 단말의 MAC 어드레스, 전화번호, 및 이들 각각의 해시값 중 적어도 하나 이상을 포함하는 것을 특징으로 하는 결제 방법.

[청구항 5] 제1항에 있어서,
상기 (a) 단계에서,
상기 지급 결제 서버가, 상기 서명 요청 정보에, 상기 주문 정보 또는 검증 확인값을 포함하여 상기 사용자 단말로 하여금 상기 사용자의 프라이빗 키를 이용하여 상기 주문 정보 또는 상기 검증 확인값을 서명하도록 요청하며,
상기 (b) 단계에서,
상기 지급 결제 서버가, 상기 블록체인에 등록된 상기 사용자의 퍼블릭 키를 이용하여 상기 서명값으로부터 상기 주문 정보 또는 상기 검증 확인값을 추출하며, 상기 서명값으로부터 추출된 상기 주문 정보 또는 상기 검증 확인값이 상기 서명 요청 정보에 포함된 상기 주문 정보 또는 상기 검증 확인값과 일치하는지를 확인하여 상기 사용자 서명값의 유효 여부를 판단하는 것을 특징으로 하는 결제 방법.

[청구항 6] 제1항에 있어서,
상기 (a) 단계 이전에,
상기 펀드 소스 서버로부터의 지불 정보 - 상기 지불 정보는 상기 사용자 단말의 사용자 인증 및 지불 정보 등록 요청에 대응하여 상기 펀드 소스 서버가 사용자 인증을 수행한 사용자에게 대응되는 정보인 상기 지급 수단

토큰 아이디, 상기 사용자 식별 정보, 상기 푸시 토큰 아이디, 및 상기 퍼블릭 키를 포함함 - 등록 요청이 획득되면, 상기 지급 결제 서버가, 상기 지불 정보를 상기 블록체인에 등록하거나 상기 결제 지원 서버에 연동되는 타 장치를 통해 상기 지불 정보를 상기 블록체인에 등록하도록 지원하는 단계;

를 더 포함하는 것을 특징으로 하는 결제 방법.

[청구항 7]

블록체인 기반의 결제를 수행하는 지급 결제 서버에 있어서, 사용자의 지급 수단에 대응되는 지급 수단 토큰 아이디, 상기 사용자를 식별하기 위한 사용자 식별 정보, 상기 사용자의 사용자 단말에 설치된 앱에 대응되는 푸시 토큰 아이디, 및 상기 사용자의 퍼블릭 키를 블록체인에 등록한 상태에서, 서비스 제공 단말로부터 사용자 단말의 구매 및 지불 정보에 대응하는 주문 요청 정보 - 상기 주문 요청 정보는 사용자 식별 정보, 및 주문 정보 중 적어도 하나 이상을 포함함 - 를 획득하는 통신부; 및

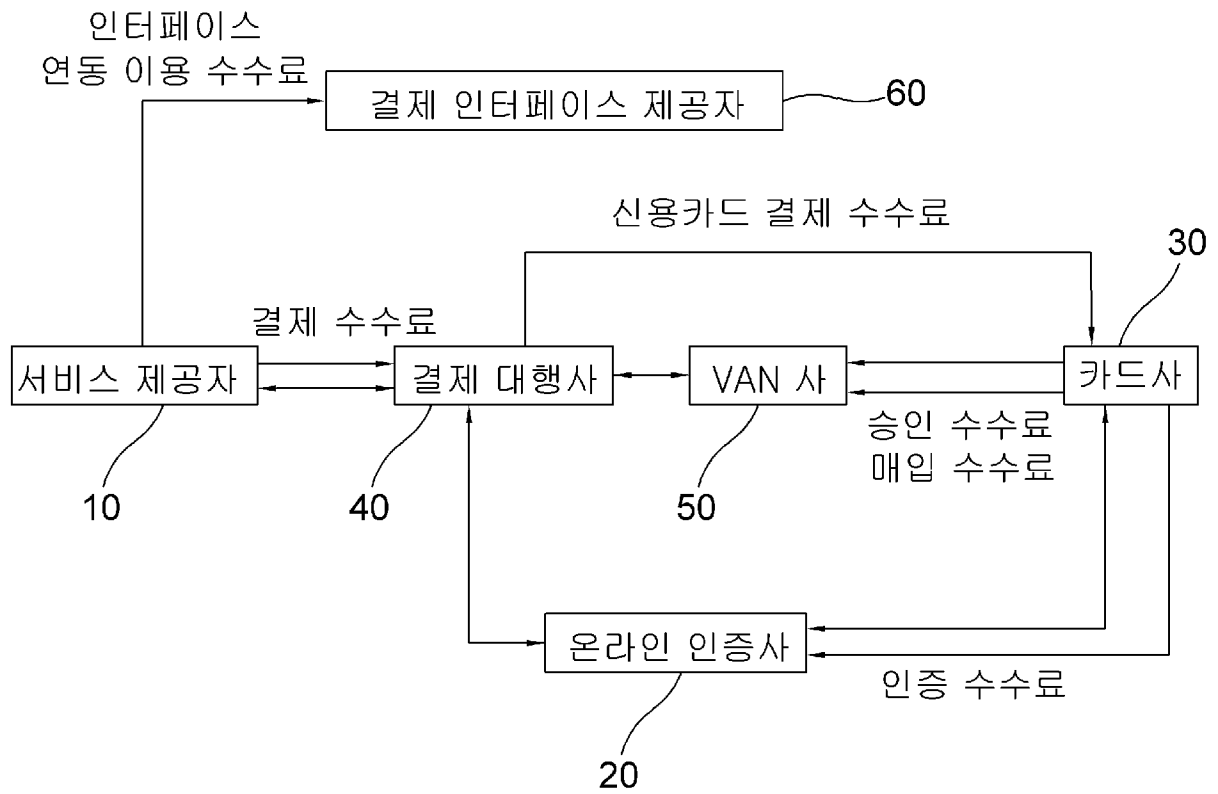
상기 주문 요청 정보에 포함된 상기 사용자 식별 정보에 대응하는 상기 푸시 토큰 아이디를 상기 블록체인으로부터 획득하거나 상기 지급 결제 서버에 연동되는 타 장치를 통해 상기 푸시 토큰 아이디를 상기 블록체인으로부터 획득하도록 지원하고, 상기 주문 요청 정보에 대응하는 주문 아이디를 생성하며, 상기 주문 아이디와 상기 주문 정보 중 적어도 하나를 포함하는 트랜잭션 데이터를 상기 블록체인에 등록하거나 상기 지급 결제 서버에 연동되는 타 장치를 통해 상기 트랜잭션 데이터를 상기 블록체인에 등록하도록 지원하고, 상기 푸시 토큰 아이디와 서명 요청 정보를 상기 사용자 단말로 전송하거나 상기 지급 결제 서버에 연동되는 타 장치 또는 상기 서비스 단말을 통해 상기 푸시 토큰 아이디와 상기 서명 요청 정보를 상기 사용자 단말로 전송하도록 지원하는 프로세스와, 상기 사용자 단말로부터의 서명값이 획득되면, 상기 서명값을 검증하거나 상기 지급 결제 서버에 연동되는 타 장치를 통해 상기 서명값을 검증하도록 지원하고, 상기 서명값이 유효일 경우, 상기 지급 수단 토큰 아이디, 상기 주문 아이디, 및 상기 주문 요청 정보 중 적어도 하나 이상을 포함하는 승인 요청 정보를 펀드 소스 서버로 전송하거나 상기 결제 지원 서버와 연동하는 타 장치를 통해 상기 승인 요청 정보를 상기 펀드 소스 서버로 전송하도록 지원하는 프로세스와, 상기 펀드 소스 서버로부터의 승인 결과 정보가 획득되면, 상기 승인 결과 정보를 상기 블록체인에 등록하거나 상기 결제 지원 서버에 연동되는 타 장치를 통해 상기 승인 결과 정보를 상기 블록체인에 등록하도록 지원하며, 상기 승인 결과 정보에 대응한 승인 완료 정보를 상기 서비스 단말로 전송하거나 상기 결제 지원 서버에 연동되는 타 장치를 통해 상기 승인 완료 정보를 상기 서비스 단말로 전송하도록 지원하는 프로세스를

수행하는 프로세서;
를 포함하는 것을 특징으로 하는 지급 결제 서버.

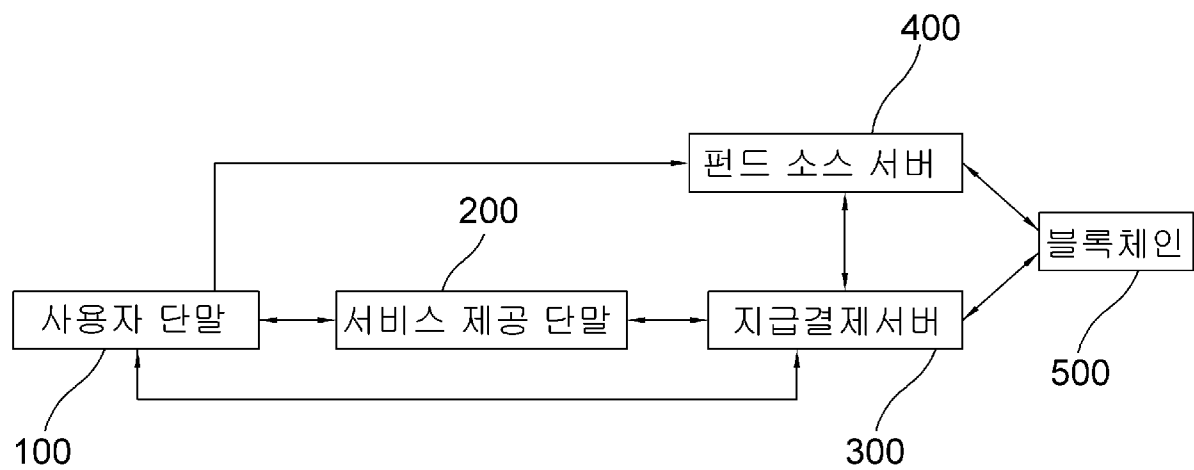
- [청구항 8] 제7항에 있어서,
상기 프로세서는,
상기 펀드 소스 서버로부터의 정산 데이터 요청 정보가 획득되면, 상기 정산 데이터 요청 정보에 대응하는 상기 주문 정보를 포함하는 정산 데이터를 상기 블록체인으로부터 획득하거나 상기 결제 지원 서버에 연동되는 타 장치를 통해 상기 정산 데이터를 상기 블록체인으로부터 획득하도록 지원하며, 상기 블록체인으로부터 획득된 상기 정산 데이터를 상기 펀드 소스 서버로 전송하거나 상기 결제 지원 서버에 연동되는 타 장치를 통해 상기 정산 데이터가 상기 펀드 소스 서버에 전송되도록 지원함으로써 상기 펀드 소스 서버로 하여금 상기 정산 데이터를 참조하여 비용을 정산하도록 하는 프로세스를 더 수행하는 것을 특징으로 하는 지급 결제 서버.
- [청구항 9] 제7항에 있어서,
상기 프로세서는,
상기 주문 정보를 리프노드로 한 머클트리를 연산하며, 상기 연산된 머클트리의 루트 해시값 또는 상기 루트 해시값을 가공한 값을 상기 주문 아이디로 생성하는 것을 특징으로 하는 지급 결제 서버.
- [청구항 10] 제7항에 있어서,
상기 사용자 식별 정보는,
상기 사용자의 식별을 위하여 사용자 별로 주어지는 고유 정보로서, 사용자 아이디, 주민번호, 사용자 단말 아이디, 사용자 단말의 아이피 주소, 사용자 단말의 MAC 어드레스, 전화번호, 및 이들 각각의 해시값 중 적어도 하나 이상을 포함하는 것을 특징으로 하는 지급 결제 서버.
- [청구항 11] 제7항에 있어서,
상기 프로세서가,
상기 서명 요청 정보에, 상기 주문 정보 또는 검증 확인값을 포함하여 상기 사용자 단말로 하여금 상기 사용자의 프라이빗 키를 이용하여 상기 주문 정보 또는 상기 검증 확인값을 서명하도록 요청하며,
상기 블록체인에 등록된 상기 사용자의 퍼블릭 키를 이용하여 상기 서명값으로부터 상기 주문 정보 또는 상기 검증 확인값을 추출하며, 상기 서명값으로부터 추출된 상기 주문 정보 또는 상기 검증 확인값이 상기 서명 요청 정보에 포함된 상기 주문 정보 또는 상기 검증 확인값과 일치하는지를 확인하여 상기 사용자 서명값의 유효 여부를 판단하는 것을 특징으로 하는 지급 결제 서버.
- [청구항 12] 제7항에 있어서,
상기 프로세서가,

상기 펀드 소스 서버로부터의 지불 정보 - 상기 지불 정보는 상기 사용자 단말의 사용자 인증 및 지불 정보 등록 요청에 대응하여 상기 펀드 소스 서버가 사용자 인증을 수행한 사용자에게 대응되는 정보인 상기 지급 수단 토큰 아이디, 상기 사용자 식별 정보, 상기 푸시 토큰 아이디, 및 상기 퍼블릭 키를 포함함 - 등록 요청이 획득되면, 상기 지불 정보를 상기 블록체인에 등록하거나 상기 결제 지원 서버에 연동되는 타 장치를 통해 상기 지불 정보를 상기 블록체인에 등록하도록 지원하는 프로세스를 더 수행하는 것을 특징으로 하는 지급 결제 서버.

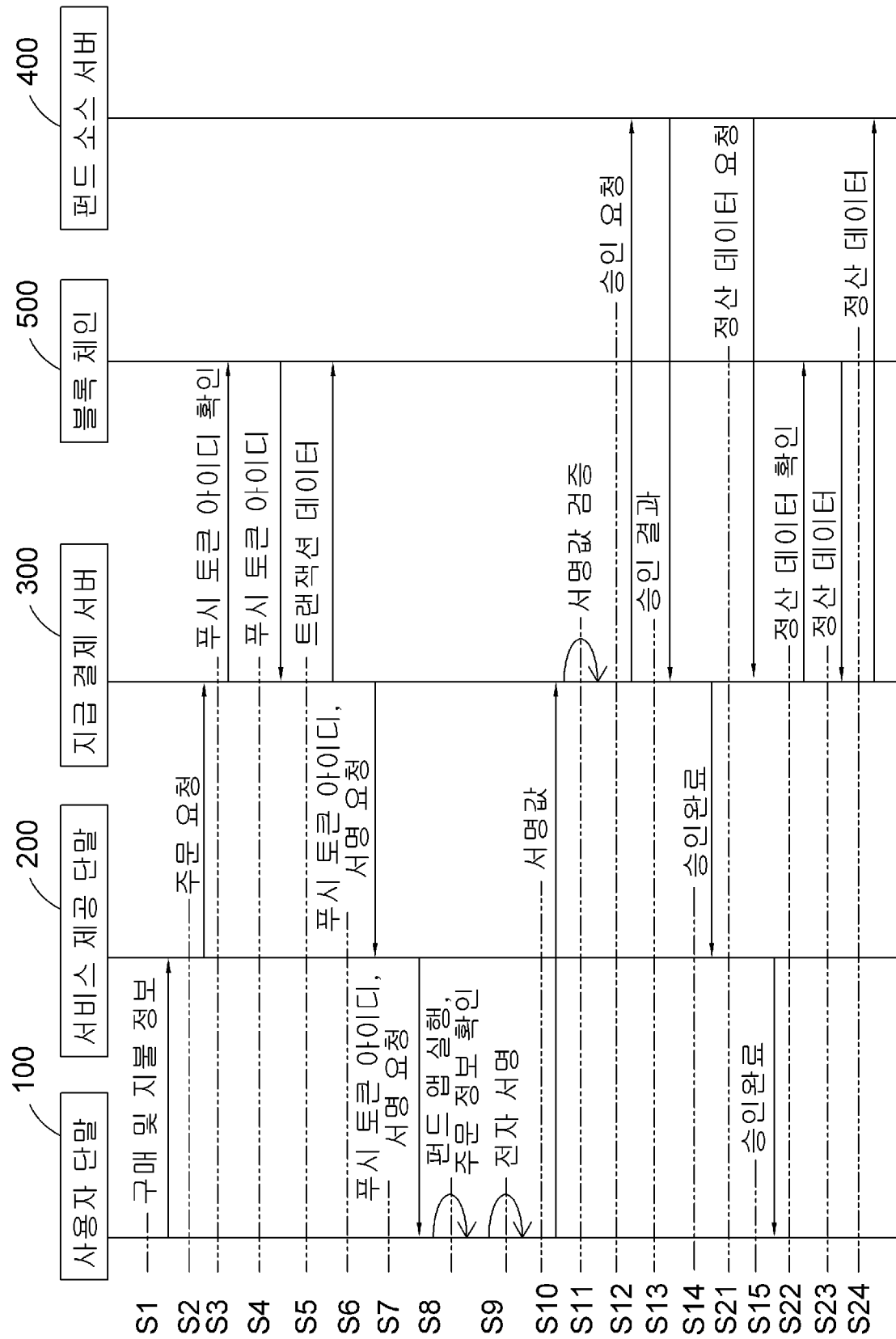
[도1]



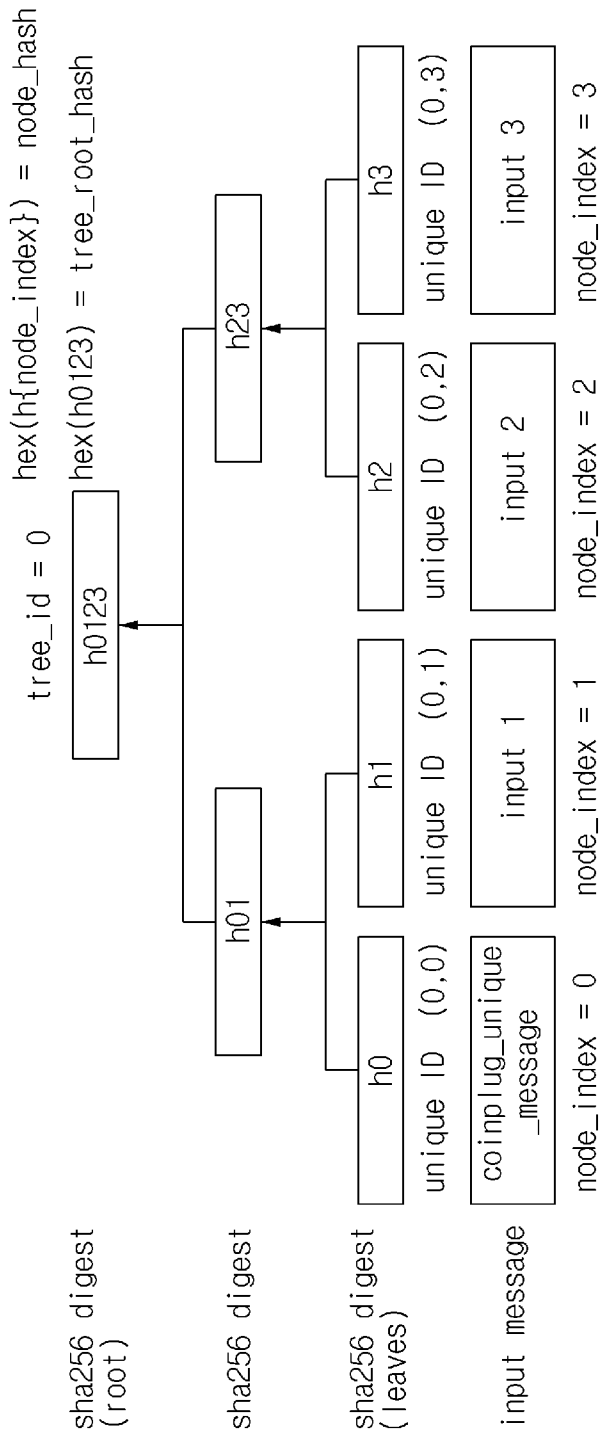
[도2]



[도3]



[4]



Input0 = coinplug_unique_message
Input1 = RN+SigPrivate(RN)+PubA (= User A registration)

input2 = TrxA

input3 = delta_0

h0 = sha256(input0)

h1 = sha256(input1)

h2 = sha256(input2)

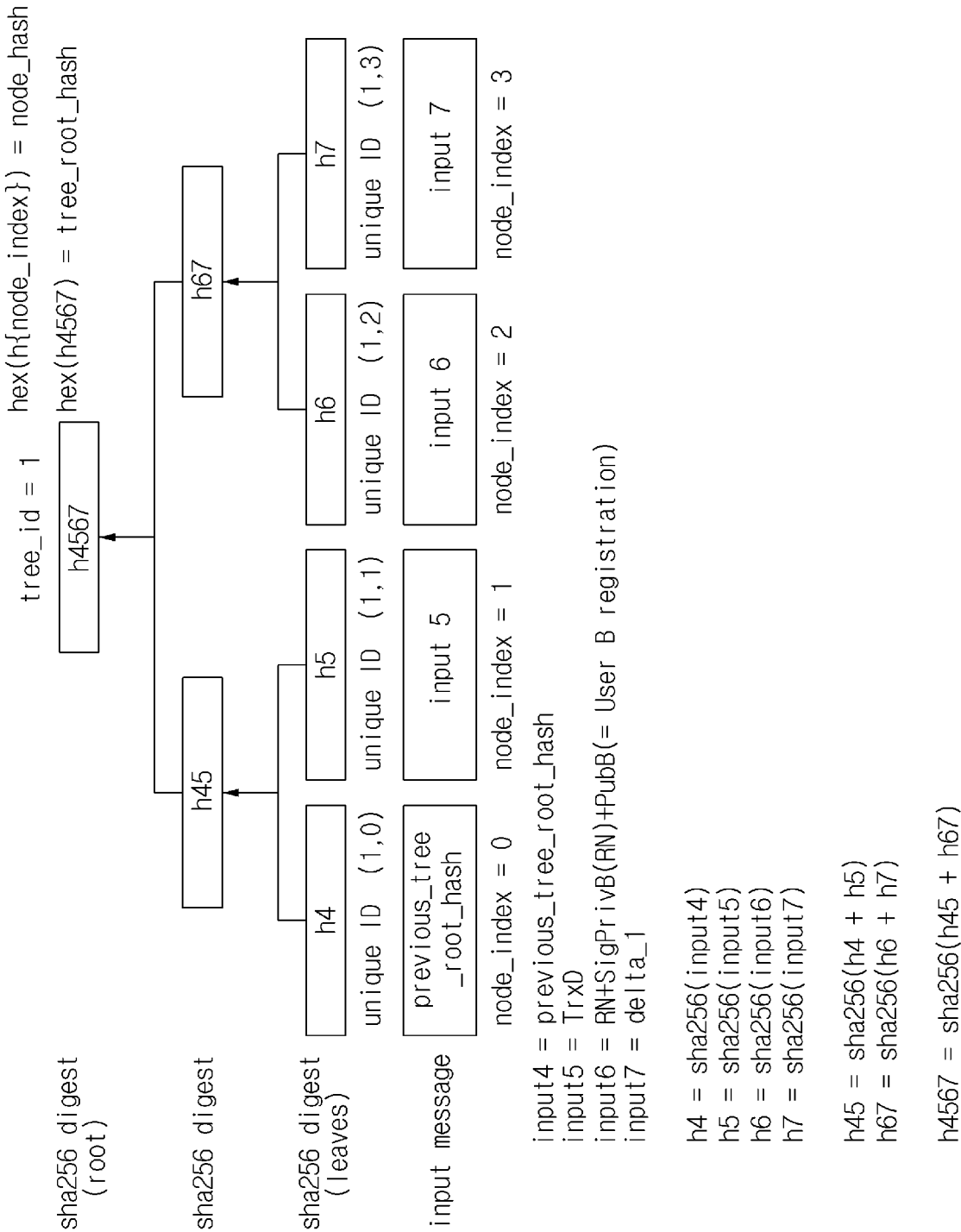
h3 = sha256(input3)

h01 = sha256(h0 + h1)

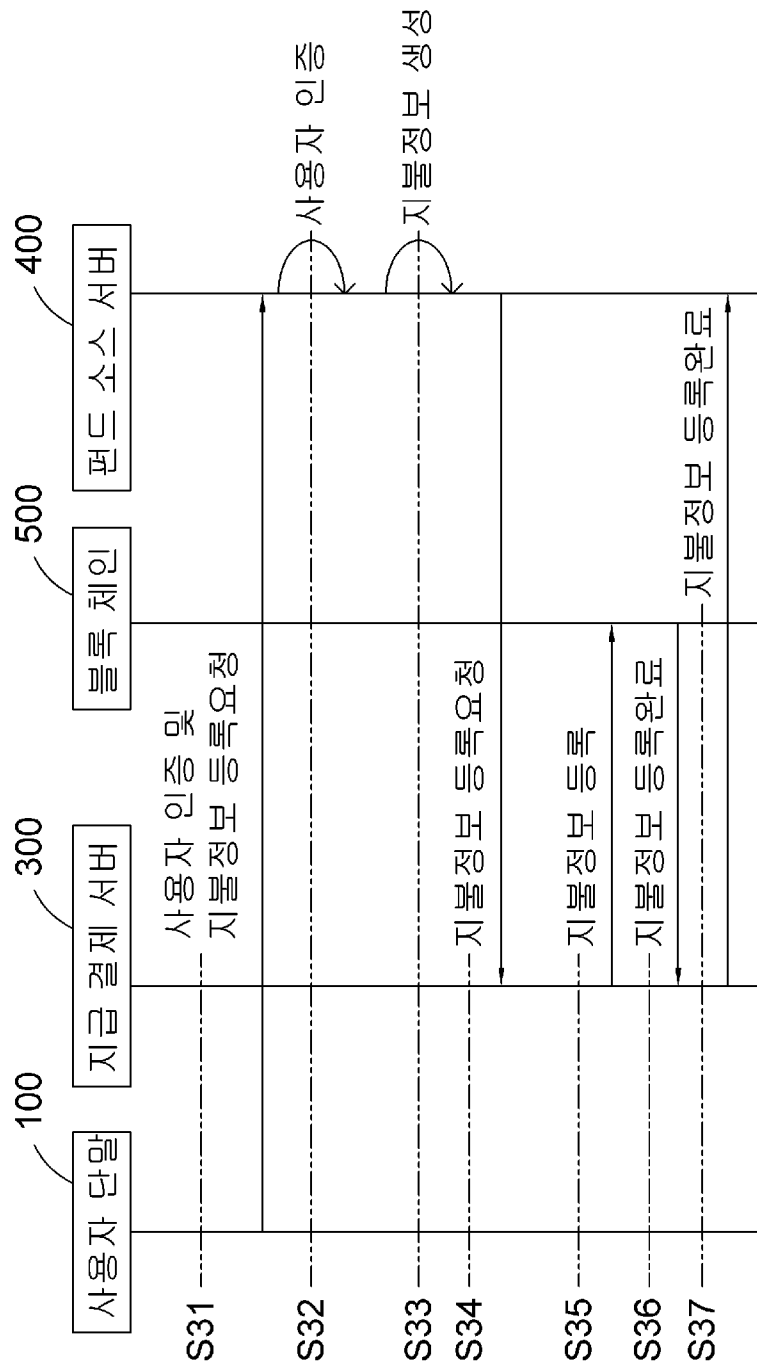
h23 = sha256(h2 + h3)

h0123 = sha256(h01 + h23)

[Fig. 5]



[도6]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2018/012284

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/38(2012.01)i, G06Q 20/34(2012.01)i, G06Q 20/02(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 20/38; G06F 21/33; G06F 21/45; G06Q 20/06; G06Q 20/22; G06Q 20/40; H04L 9/06; H04L 9/08; G06Q 20/34; G06Q 20/02

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: blockchain, order, token, ID, signature, verification, approval

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 10-2017-0091069 A (BIZMODEL LINE CO., LTD.) 08 August 2017 See paragraphs [0102]-[0104], [0132], claims 1-2 and figure 1.	1-5,7-11 6,12
Y	KR 10-1780636 B1 (COINPLUG, INC.) 21 September 2017 See paragraphs [0068], [0086], [0110], claims 1, 12 and figure 1.	1-5,7-11
Y	"Blockchain Technical Overview", Theloop., 15 March 2017. <URL: https://blog.theloop.co.kr/2017/03/15/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8-%EA%B8%B0%EC%88%A0-%EA%B0%9C%EC%9A%94/ >. See pages 1-3.	1-5,7-11
Y	KR 10-1701131 B1 (RAPI INC.) 13 February 2017 See paragraphs [0059]-[0068], claims 1, 11 and figures 1, 9.	3,9
A	KR 10-1680260 B1 (COINPLUG, INC.) 29 November 2016 See claims 1, 12 and figure 1.	1-12



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

31 JANUARY 2019 (31.01.2019)

Date of mailing of the international search report

01 FEBRUARY 2019 (01.02.2019)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex Daejeon Building 4, 189, Cheongsu-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/KR2018/012284

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2017-0091069 A	08/08/2017	KR 10-2012-0110926 A KR 10-2018-0030975 A	10/10/2012 27/03/2018
KR 10-1780636 B1	21/09/2017	US 2017-0330179 A1	16/11/2017
KR 10-1701131 B1	13/02/2017	NONE	
KR 10-1680260 B1	29/11/2016	CA 3008705 A1 KR 10-1723405 B1 US 2018-0294977 A1 WO 2017-171165 A1 WO 2018-008800 A1	05/10/2017 06/04/2017 11/10/2018 05/10/2017 11/01/2018

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06Q 20/38(2012.01)i, G06Q 20/34(2012.01)i, G06Q 20/02(2012.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06Q 20/38; G06F 21/33; G06F 21/45; G06Q 20/06; G06Q 20/22; G06Q 20/40; H04L 9/06; H04L 9/08; G06Q 20/34; G06Q 20/02

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: 블록체인, 주문, 토큰, 아이디, 서명, 검증, 승인

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y A	KR 10-2017-0091069 A (주식회사 비즈모델라인) 2017.08.08 단락 [0102]-[0104],[0132], 청구항 1-2 및 도면 1 참조.	1-5,7-11 6,12
Y	KR 10-1780636 B1 (주식회사 코인플러그) 2017.09.21 단락 [0068],[0086],[0110], 청구항 1,12 및 도면 1 참조.	1-5,7-11
Y	‘블록체인 기술 개요’, theloop. 2017.03.15. <URL: ">https://blog.theloop.co.kr/2017/03/15/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8-%EA%B8%B0%EC%88%A0-%EA%B0%9C%EC%9A%94/> . 페이지 1-3 참조.	1-5,7-11
Y	KR 10-1701131 B1 (주식회사 라피) 2017.02.13 단락 [0059]-[0068], 청구항 1,11 및 도면 1,9 참조.	3,9
A	KR 10-1680260 B1 (주식회사 코인플러그) 2016.11.29 청구항 1,12 및 도면 1 참조.	1-12

☐ 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

“T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

“X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

“L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

“Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

“O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

“&” 동일한 대응특허문헌에 속하는 문헌

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

국제조사의 실제 완료일

2019년 01월 31일 (31.01.2019)

국제조사보고서 발송일

2019년 02월 01일 (01.02.2019)

ISA/KR의 명칭 및 우편주소



대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)

팩스 번호 +82-42-481-8578

심사관

강민정

전화번호 +82-42-481-8131



국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2017-0091069 A	2017/08/08	KR 10-2012-0110926 A KR 10-2018-0030975 A	2012/10/10 2018/03/27
KR 10-1780636 B1	2017/09/21	US 2017-0330179 A1	2017/11/16
KR 10-1701131 B1	2017/02/13	없음	
KR 10-1680260 B1	2016/11/29	CA 3008705 A1 KR 10-1723405 B1 US 2018-0294977 A1 WO 2017-171165 A1 WO 2018-008800 A1	2017/10/05 2017/04/06 2018/10/11 2017/10/05 2018/01/11