(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2024 년 6 월 6 일 (06.06.2024)

WIPO | PCT

(10) 국제공개번호
WO 2024/117830 A1

(51) 국제특허분류:
G06F 21/31 (2013.01) *G06Q 20/36* (2012.01)
G06F 21/44 (2013.01)

(21) 국제출원번호: PCT/KR2023/019610

(22) 국제출원일: 2023 년 11 월 30 일 (30.11.2023)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2022-0164357 2022 년 11 월 30 일 (30.11.2022) KR
10-2023-0169284 2023 년 11 월 29 일 (29.11.2023) KR

(71) 출원인: 히포크랏다오 아이앤씨 (**HIPPOCRATDAO INC.**) [PA/PA]; 308-5200 피소 17, 피에이치 파이낸셜 파크 타워, 블러바드 코르타 델 에스타, Piso 17 (PA).

(72) 발명자; 겸

(71) 출원인: 최현섭 (**CHOI, Hyun Sub**) [KR/KR]; 04375 서울특별시 용산구 백범로99길 40, 102동 2304호, Seoul (KR).

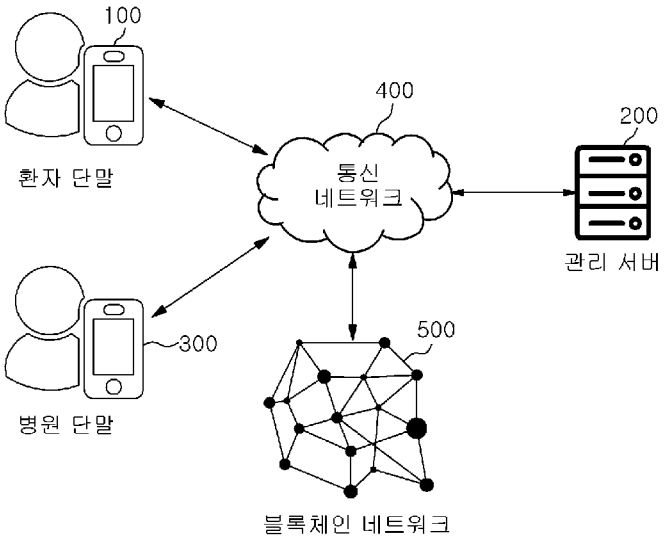
(74) 대리인: 이강욱 (**LEE, Kang Wook**); 06096 서울특별시 강남구 봉은사로 469, 에스-타워, 12층, Seoul (KR).

(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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

WO 2024/117830 A1

(54) **Title:** METHOD AND DEVICE FOR SUPPORTING SECURE MEDICAL DATA TRANSACTIONS ON BASIS OF BLOCKCHAIN IN COMMUNICATION SYSTEM

(54) **발명의 명칭:** 통신 시스템에서 블록 체인에 기반하여 보안성을 가진 의료 데이터 거래를 지원하기 위한 방법 및 장치



100 ... Patient terminal
200 ... Management server
300 ... Hospital terminal
400 ... Communication network
500 ... Blockchain network

(57) **Abstract:** The present invention relates to a method and device for supporting secure medical data transactions on the basis of blockchain in a communication system. Specifically, the present invention relates to a method and device for increasing security of party verification with respect to medical data by verifying an identity of an individual user trading medical data with a medical institution, through a double transaction history in a blockchain network.

[다음 쪽 계속]

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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 통신 시스템에서 블록 체인에 기반하여 보안성을 가진 의료 데이터 거래를 지원하기 위한 방법 및 장치에 관한 것이다. 구체적으로, 본 발명은 의료 데이터를 의료 기관과 거래하는 개인 사용자의 신원 확인에 대하여 블록 체인 네트워크에서 이중의 거래 내역을 통해 증명함으로써 의료 데이터에 대한 당사자 확인의 보안성을 높이기 위한 방법 및 장치에 관한 것이다.

명세서

발명의 명칭: 통신 시스템에서 블록 체인에 기반하여 보안성을 가진 의료 데이터 거래를 지원하기 위한 방법 및 장치

기술분야

[1] 본 발명은 통신 시스템에서 블록 체인에 기반하여 보안성을 가진 의료 데이터 거래를 지원하기 위한 방법 및 장치에 관한 것이다. 구체적으로, 본 발명은 의료 데이터를 의료 기관과 거래하는 개인 사용자의 신원 확인에 대하여 블록 체인 네트워크에서 이중의 거래 내역을 통해 증명함으로써 의료 데이터에 대한 당사자 확인의 보안성을 높이기 위한 방법 및 장치에 관한 것이다.

배경기술

[2] 데이터 거래에서 신원 인증의 중요성은 상당히 높다. 신원 인증은 거래의 모든 단계에서 중추적인 역할을 수행하며, 특히 데이터가 민감하고 가치가 높은 분야에서 그 중요성은 더욱 강조된다. 신원 인증은 데이터 거래 프로세스의 보안을 강화하는 핵심 요소이다. 거래 당사자들이 서로의 정체성을 확실히 알고 있을 때, 데이터의 무단 접근, 도용, 및 사기 같은 위험들을 크게 줄일 수 있다.

[3] 기존의 중앙집중식 신원 인증 시스템은 여러 가지 취약점을 가지고 있다. 이러한 시스템들은 단일 실패 지점(Single Point of Failure)을 가지며, 사용자의 개인 데이터 보호와 통제에 있어서 한계를 가지고 있다. 의료 데이터의 경우, 그 가치와 민감성 때문에 특히 더 높은 수준의 보안과 개인의 통제가 필요하다. 하지만 현재 대부분의 의료 데이터는 병원이나 기타 의료 기관의 중앙 서버에 저장되며, 환자는 자신의 의료 데이터에 대한 완전한 통제권을 가지고 있지 않는다. 이로 인해 개인의 데이터 주권에 대한 요구가 증가하고 있으며, 이는 의료 데이터 사이언스의 발전에도 장애가 되고 있다.

[4] 본 발명의 다양한 실시 예들은 디지털 신원 확인과 관련하여, 비트코인 기반의 분산형 신원증명(Decentralized Identity, DID) 시스템 및 이를 통한 의료 데이터 거래에 대한 새로운 방식을 제공한다. 본 발명의 주된 목적은 기존 중앙집중식 신원 인증 시스템의 한계를 극복하고, 사용자에게 개인 데이터에 대한 더 큰 통제력과 보안을 제공하는 것이다. 이를 위해 비트코인 기반의 DID 시스템을 사용하여 사용자가 자신의 디지털 신원을 소유하고 통제할 수 있도록 한다. 본 발명의 다양한 실시 예들은 ECDH(Elliptic Curve Diffie-Hellman) 암호화 방식을 통해 안전한 데이터 교환을 가능하게 하며, AES-GCM(Advanced Encryption Standard Galois/Counter Mode)을 사용하여 데이터의 무결성과 기밀성을 보장한다. 더 나아가, 본 발명의 다양한 실시 예들은 환자 개인이 자신의 의료 데이터를 효과적으로 관리하고, 이를 필요에 따라 다른 기관이나 개인과 안전하게 공유할 수 있는 새로운 방식을 제공한다. 이를 통해 환자는 자신의 의료 데이터를 이용해 경제적인 가치를 창출하거나, 더 나은 의료 서비스를 받을 수 있는 기회를 가질 수

있다. 비트코인 레이어 2 솔루션을 통해 소액의 의료 데이터 거래도 빠르고 효율적으로 처리될 수 있다. 이 모든 것은 사용자의 개인 정보 보호와 데이터 주권을 강화하는 동시에, 의료 데이터 사이언스와 연구의 발전을 촉진하는 것을 목표로 한다.

발명의 상세한 설명

기술적 과제

[5] 본 발명은 전술한 문제점을 해결하기 위하여 다음과 같은 해결 과제를 목적으로 한다.

[6] 본 발명은 통신 시스템에서 블록 체인에 기반하여 보안성을 가진 의료 데이터 거래를 지원하기 위한 방법 및 장치의 제공을 목적으로 한다.

[7] 본 발명은 의료 데이터를 의료 기관과 거래하는 개인 사용자의 신원 확인에 대하여 블록 체인 네트워크에서 이중의 거래 내역을 통해 증명함으로써 의료 데이터에 대한 당사자 확인의 보안성을 높이기 위한 방법 및 장치의 제공을 목적으로 한다.

[8] 본 발명은 기존의 중앙 집중형 신원 인증 시스템이 내포하는 보안 취약점과 단일 실패 지점의 위험의 문제를 해결하기 위해 탈중앙화된 신원 인증 방식을 도입하여 보안성과 신뢰성을 크게 향상시킨 방법 및 장치의 제공을 목적으로 한다.

[9] 본 발명은 사용자가 자신의 데이터와 신원에 대한 직접적인 관리 및 통제를 할 수 있는 방법 및 장치의 제공을 목적으로 한다.

[10] 본 발명은 데이터 보호 및 개인 정보 보호에 대한 규제 요구사항을 충족시키면서, 사용자 및 조직의 법적 위험을 감소시킬 수 있는 방법 및 장치의 제공을 목적으로 한다.

[11] 본 발명은 복잡한 중간 과정을 제거하고 직접적인 데이터 교환 및 관리 메커니즘을 구축하여 빠르고 효율적인 데이터 거래 및 관리를 가능하게 할 수 있는 방법 및 장치의 제공을 목적으로 한다.

[12] 본 발명은 확장성 높은 비트코인 레이어 2 솔루션을 통해 이를 해결함으로써, 더 많은 사용자들이 저렴한 비용으로 데이터 거래에 참여할 수 있는 방법 및 장치의 제공을 목적으로 한다.

[13] 본 발명은 데이터의 암호화 및 복호화 과정에서의 보안성을 강화하기 위해 본 발명은 ECDH(Elliptic Curve Diffie-Hellman)과 같은 첨단 암호화 기술을 활용하여 데이터의 안전한 전송을 보장할 수 있는 방법 및 장치의 제공을 목적으로 한다.

과제 해결 수단

[14] 본 발명의 다양한 실시 예들에 따르면, 통신 시스템에서 서버의 동작 방법에 있어서, 상기 서버는 송수신기, 메모리, 프로세서를 포함하고, 환자 단말과 상기 서버의 제1 암호화폐 지갑의 정보 및 상기 환자 단말의 제2 암호화폐 지갑의 정보를 상기 송수신기에 의하여 교환하는 단계; 상기 제1 암호화폐 지갑으로부터 상기 제2 암호화폐 지갑으로 설정된 양의 암호화폐 및 OP_RETURN을 전송하는

2개의 로직과 관련된 하나의 트랜잭션 정보를 블록체인 네트워크에게 상기 송수신기에 의하여 전송하는 단계; 병원 단말로부터 상기 제1 암호화폐 지갑에서 상기 2개의 로직과 관련된 상기 트랜잭션 정보의 요청 메시지를 상기 송수신기에 의하여 수신하는 단계 - 상기 환자 단말의 탈중앙화 신원 정보(Decentralized Identifier, DID)은 상기 제1 암호화폐 지갑의 제1 주소 및 상기 제2 암호화폐 지갑의 제2 주소를 포함함 -; 상기 병원 단말에게 상기 2개의 로직과 관련된 상기 제1 암호화폐 지갑의 상기 트랜잭션 정보를 포함하는 응답 메시지를 상기 송수신기에 의하여 전송하는 단계를 포함하고, 상기 제1 암호화폐 지갑의 제1 주소 및 상기 제2 암호화폐 지갑의 제2 주소에 설정된 양의 암호화폐 및 OP_RETURN을 전송하는 2개의 로직과 관련된 하나의 트랜잭션 정보가 공통적으로 존재함에 기반하여 상기 DID의 유효함이 증명되고, 상기 OP_RETURN은 트랜잭션 생성 시 상기 서버의 서명 데이터가 예정된 위치에 상기 서명 데이터를 삽입하지 않고 비우거나 또는 서명 데이터 대신 다른 데이터를 삽입한 정보인 방법이 제공된다.

[15] 본 발명의 다양한 실시 예들에 따르면, 통신 시스템에서 환자 단말의 동작 방법에 있어서, 상기 환자 단말은 송수신기, 메모리, 프로세서를 포함하고, 서버와 상기 서버의 제1 암호화폐 지갑의 정보 및 상기 환자 단말의 제2 암호화폐 지갑의 정보를 상기 송수신기에 의하여 교환하는 단계; 상기 제1 암호화폐 지갑으로부터 상기 제2 암호화폐 지갑으로 설정된 양의 암호화폐 및 OP_RETURN을 수신하는 2개의 로직과 관련된 하나의 트랜잭션 정보를 블록체인 네트워크에게 상기 송수신기에 의하여 전송하는 단계; 각 통신 인스턴스에 대하여 ECIES(Elliptic Curve Integrated Encryption Scheme) 방식에 기반하여 무작위 개인 키 및 무작위 공개 키의 키 쌍을 상기 프로세서에 의하여 생성하는 단계; 상기 환자 단말의 상기 무작위 개인 키 및 병원 단말의 공개 키로부터 계산되는 ECDH(Elliptic Curve Diffie-Hellman) 공유 키를 사용하여 상기 환자 단말의 의료 데이터를 상기 프로세서에 의하여 암호화하는 단계; 상기 환자 단말의 무작위 공개 키와 함께 상기 암호화된 의료 데이터를 상기 병원 단말에게 상기 환자 단말의 탈중앙화 신원 정보(Decentralized Identifier, DID)에 기반하여 상기 송수신기에 의하여 전송하는 단계를 포함하고, 상기 DID는 상기 제1 암호화폐 지갑의 제1 주소 및 상기 제2 암호화폐 지갑의 제2 주소를 포함하고, 상기 제1 암호화폐 지갑의 제1 주소 및 상기 제2 암호화폐 지갑의 제2 주소에 설정된 양의 암호화폐 및 OP_RETURN을 전송하는 2개의 로직과 관련된 하나의 트랜잭션 정보가 공통적으로 존재함에 기반하여 상기 DID의 유효함이 증명되고, 상기 OP_RETURN은 트랜잭션 생성 시 상기 서버의 서명 데이터가 예정된 위치에 상기 서명 데이터를 삽입하지 않고 비우거나 또는 서명 데이터 대신 다른 데이터를 삽입한 정보인 방법이 제공된다.

[16] 본 발명의 다양한 실시 예들에 따르면, 통신 시스템에서 서버에 있어서, 송수신기, 메모리, 프로세서를 포함하고, 프로세서는 본 발명의 다양한 실시 예들에 따른 서버의 동작 방법을 수행하도록 구성된 서버가 제공된다.

[17] 본 발명의 다양한 실시 예들에 따르면, 통신 시스템에서 환자 단말에 있어서, 송수신기, 메모리, 프로세서를 포함하고, 프로세서는 본 발명의 다양한 실시 예들에 따른 환자 단말의 동작 방법을 수행하도록 구성된 서버가 제공된다.

발명의 효과

[18] 본 발명은 통신 시스템에서 블록 체인에 기반하여 보안성을 가진 의료 데이터 거래를 지원하기 위한 방법 및 장치를 제공할 수 있다.

[19] 본 발명은 의료 데이터를 의료 기관과 거래하는 개인 사용자의 신원 확인에 대하여 블록 체인 네트워크에서 이중의 거래 내역을 통해 증명함으로써 의료 데이터에 대한 당사자 확인의 보안성을 높이기 위한 방법 및 장치를 제공할 수 있다.

[20] 본 발명은 기존의 중앙 집중형 신원 인증 시스템이 내포하는 보안 취약점과 단일 실패 지점의 위험의 문제를 해결하기 위해 탈중앙화된 신원 인증 방식을 도입하여 보안성과 신뢰성을 크게 향상시킨 방법 및 장치를 제공할 수 있다.

[21] 본 발명은 사용자가 자신의 데이터와 신원에 대한 직접적인 관리 및 통제를 할 수 있는 방법 및 장치를 제공할 수 있다.

[22] 본 발명은 데이터 보호 및 개인 정보 보호에 대한 규제 요구사항을 충족시키면서, 사용자 및 조직의 법적 위험을 감소시킬 수 있는 방법 및 장치를 제공할 수 있다.

[23] 본 발명은 복잡한 중간 과정을 제거하고 직접적인 데이터 교환 및 관리 메커니즘을 구축하여 빠르고 효율적인 데이터 거래 및 관리를 가능하게 할 수 있는 방법 및 장치를 제공할 수 있다.

[24] 본 발명은 확장성 높은 비트코인 레이어 2 솔루션을 통해 이를 해결함으로써, 더 많은 사용자들이 저렴한 비용으로 데이터 거래에 참여할 수 있는 방법 및 장치를 제공할 수 있다.

[25] 본 발명은 데이터의 암호화 및 복호화 과정에서의 보안성을 강화하기 위해 본 발명은 ECDH(Elliptic Curve Diffie-Hellman)과 같은 첨단 암호화 기술을 활용하여 데이터의 안전한 전송을 보장할 수 있는 방법 및 장치를 제공할 수 있다.

[26] 본 발명의 효과는 이상에서 언급된 것들에 한정되지 않으며, 언급되지 아니한 다른 효과들은 아래의 기재로부터 당해 기술분야에 있어서의 통상의 지식을 가진 자가 명확하게 이해할 수 있을 것이다.

도면의 간단한 설명

[27] 도 1은 본 발명의 다양한 실시 예들에 따른 통신 시스템을 도시한다.

[28] 도 2는 본 발명의 다양한 실시 예들에 따른 환자 단말, 병원 단말의 구성에 대한 블록도를 도시한다.

[29] 도 3은 본 발명의 다양한 실시 예들에 따른 서버의 구성에 대한 블록도를 도시한다.

[30] 도 4는 본 발명의 다양한 실시 예들에 따른 서버의 동작 방법의 일 예를 도시한다.

[31] 도 5는 본 발명의 다양한 실시 예들에 따른 환자 단말의 동작 방법의 일 예를 도시한다.

[32] 도 6은 본 발명의 다양한 실시 예들에 따른 비트코인에 기록되는 ION DID의 일 예를 도시한다.

[33] 도 7는 본 발명의 다양한 실시 예들에 따른 OP_RETURN을 활용한 개인 신원 인증 내역 기록의 일 예를 도시한다.

[34] 도 8은 본 발명의 다양한 실시 예들에 따른 의료 데이터의 수집 및 활용 생태계의 일 예를 도시한다.

[35] 도 9는 본 발명의 다양한 실시 예들에 따른 데이터 활용과 보호의 적정한 균형의 일 예를 도시한다.

[36] 도 10은 본 발명의 다양한 실시 예들에 따른 신원 인증(ION), 소액 송수신 및 결제(Lightning Network), 자산 발행(Taro) 및 더 다양한 스마트 컨트랙트 (BIP-119, Liquid Network, RGB 등) 등 Bitcoin의 탈중앙성과 보안성 위에서 확장성을 실현하는 기술의 일 예를 도시한다.

[37] 도 11은 본 발명의 다양한 실시 예들에 따른 API 모델과 데이터 상호호환성에 대한 인센티브의 일 예를 도시한다.

[38] 도 12는 본 발명의 다양한 실시 예들에 따른 QR코드 인식만으로 간편하게 로그인, 인증, 자산 및 데이터 송수신하는 과정의 일 예를 도시한다.

[39] 도 13은 본 발명의 다양한 실시 예들에 따른 선택적 데이터 공유의 일 예를 도시한다.

[40] 도 14는 본 발명의 다양한 실시 예들에 따른 데이터 지갑과 연동하여 데이터를 활용한 부가 서비스의 일 예를 도시한다.

[41] 도 15는 본 발명의 다양한 실시 예들에 따른 실제 환자의 데이터를 데이터 지갑으로 발급하는 기능의 일 예를 도시한다.

[42] 도 16은 본 발명의 다양한 실시 예들에 따른 의료 연구자의 신뢰할 수 있는 연구를 위해 의료 데이터를 선별된 환자로부터 생성하는 과정의 일 예를 도시한다.

[43] 도 17은 본 발명의 다양한 실시 예들에 따른 데이터 활용의 일 예를 도시한다.

[44] 도 18은 본 발명의 다양한 실시 예들에 따른 데이터에 대한 보상 증가 및 개인정보 침해 위험의 감소에 따른 데이터 공유에 대한 동의 증가의 일 예를 도시한다.

[45] 도 19는 본 발명의 다양한 실시 예들에 따른 거버넌스 프로토콜의 일 예를 도시한다.

[46] 도 20은 본 발명의 다양한 실시 예들에 따른 데이터 수집 및 보상 시스템의 일 예를 도시한다.

[47] 도 21은 본 발명의 다양한 실시 예들에 따른 데이터 수집 및 활용에 따른 보상 시스템의 일 예를 도시한다.

발명의 실시를 위한 형태

[48] 이하, 첨부한 도면을 참고로 하여 본 발명의 실시 예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시 예에 한정되지 않는다.

[49]

[50] 도 1은 본 발명의 다양한 실시 예들에 따른 통신 시스템을 도시한다.

[51] 도 1을 참고하면, 본 발명의 다양한 실시 예들에 따른 통신 시스템은 환자 단말(100), 관리 서버(200), 병원 단말(300), 유/무선 통신 네트워크(400), 블록 체인 네트워크(500)를 포함한다.

[52] 환자 단말(100)은 본인 명의의 의료 데이터를 병원에 제공할 수 있는 환자에 의하여 운영되는 단말이다. 환자 단말(100)은, 유/무선 통신 네트워크(400)를 통하여 관리 서버(200), 병원 단말(300), 블록체인 네트워크(500)에게 정보를 전송하고 또한 정보를 수신할 수 있는 전자 장치이다. 환자 단말(100)은 컴퓨터, 셀룰러 폰, 스마트 폰 및 태블릿 컴퓨터 등과 같이, 정보를 입력할 수 있는 입력 장치, 정보를 출력할 수 있는 출력 장치, 정보를 저장할 수 있는 메모리, 정보의 송수신을 수행할 수 있는 송수신부, 정보의 연산을 수행할 수 있는 적어도 하나의 프로세서를 포함하는 전자 장치일 수 있다.

[53] 관리 서버(200)는 환자와 병원간 의료 데이터 거래를 수행할 수 있는 플랫폼을 제공하는 사업자에 의하여 운영되는 서버이다. 관리 서버(200)는 유/무선 통신 네트워크(400)를 통하여 환자 단말(100), 병원 단말(300), 블록체인 네트워크(500)에게 정보를 전송하고 또한 정보를 수신할 수 있는 전자 장치이다. 서버(200)는 정보를 저장할 수 있는 메모리, 정보의 송수신을 수행할 수 있는 송수신부, 정보의 연산을 수행할 수 있는 적어도 하나의 프로세서를 포함하는 전자 장치일 수 있다.

[54] 병원 단말(300)은 환자 단말(100)로부터 의료 데이터를 수집하고 보상을 지급할 수 있는 병원에 의하여 운영되는 단말이다. 병원 단말(300)은, 유/무선 통신 네트워크(400)를 통하여 환자 단말(100), 관리 서버(200), 블록체인 네트워크(500)에게 정보를 전송하고 또한 정보를 수신할 수 있는 전자 장치이다. 병원 단말(300)은 컴퓨터, 셀룰러 폰, 스마트 폰 및 태블릿 컴퓨터 등과 같이, 정보를 입력할 수 있는 입력 장치, 정보를 출력할 수 있는 출력 장치, 정보를 저장할 수 있는 메모리, 정보의 송수신을 수행할 수 있는 송수신부, 정보의 연산을 수행할 수 있는 적어도 하나의 프로세서를 포함하는 전자 장치일 수 있다.

[55] 유/무선 통신 네트워크(400)는, 환자 단말(100), 관리 서버(200), 병원 단말(300), 블록 체인 네트워크(500)가 서로 신호 및 데이터를 송수신할 수 있는 통신 경로를 제공한다. 유/무선 통신 네트워크(400)는 특정한 통신 프로토콜에 따른 통신 방식에 한정되지 않으며, 구현 예에 따라 적절한 통신 방식이 사용될 수 있다. 예를 들어, 인터넷 프로토콜(internet protocol, IP) 기초의 시스템으로 구성되는 경우 유/무선 통신 네트워크(400)는 유무선 인터넷망으로 구현될 수 있으며, 환자

단말(100), 관리 서버(200), 병원 단말(300), 블록 체인 네트워크(500)가 이동 통신 단말로서 구현되는 경우 유/무선 통신 네트워크(400)는 셀룰러 네트워크 또는 WLAN(wireless local area network) 네트워크와 같은 무선망으로 구현될 수 있다.

[56] 블록 체인 네트워크(500)는 블록 체인 기술에 기반하여 동작하는 복수의 노드들을 의미한다. 여기서, 블록 체인 기술은 블록이 체인 형태로 연결된 저장 구조를 사용하여 관리 대상이 되는 데이터를 블록 체인 네트워크를 구성하는 복수의 노드들에 저장하는 분산 저장 기술이다. 블록 체인 네트워크(500)는 환자 단말(100), 관리 서버(200), 병원 단말(300) 등 블록 체인 네트워크를 구성하는 노드 중 적어도 하나로부터 전달된 트랜잭션을 사전 결정된 합의 알고리즘에 기초하여 블록 형태로 저장할 수 있다. 블록 형태로 저장되는 데이터는 블록 체인 네트워크(500)를 구성하는 복수의 노드들에 의해 공유될 수 있다. 도 1에서는 블록 체인 네트워크(500)를 별도의 분리된 엔티티로서 표현하였지만, 본 발명의 다양한 실시 예들에 따르면 블록 체인 네트워크(500)는 관리 서버(200)에 포함된 형태로 구현될 수도 있다. 블록 체인 네트워크(500)는 구현 형태에 따라서 임의의 노드들이 합의 동작을 수행할 수 있는 퍼블릭 블록 체인 네트워크 또는 사전 결정된 노드만이 합의 동작을 수행할 수 있는 프라이빗 블록 체인 네트워크를 포함할 수 있다.

[57] 본 발명의 다양한 실시 예들에 따른 블록 체인 네트워크(500)에서 수행되는 합의 알고리즘은: PoW(Proof of Work) 알고리즘, PoS(Proof of Stake) 알고리즘, DPoS(Delegated Proof of Stage) 알고리즘, PBFT(Practical Byzantine Fault Tolerance) 알고리즘, DBFT(Delegated Byzantine Fault Tolerance) 알고리즘, RBFT(Redundant Byzantine Fault Tolerance) 알고리즘, Sieve 알고리즘, Tendermint 알고리즘, Paxos 알고리즘, Raft 알고리즘, PoA(Proof of Authority) 알고리즘 및/또는 PoET(Proof of Elapsed Time) 알고리즘을 포함할 수 있다.

[58] 본 발명의 다양한 실시 예들에 따르면, 블록 체인 네트워크(500)에서의 노드들은 계층 구조에 따른 블록 체인 코어 패키지에 의해 동작할 수 있다. 상기 계층 구조는: 블록 체인 네트워크(500)에서 다뤄지는 데이터의 구조를 정의하고 데이터를 관리하는 데이터 계층, 블록의 유효성을 검증하고 블록을 생성하는 마이닝을 수행하고 마이닝 과정에서 채굴자에게 지급되는 수수료의 처리를 담당하는 합의 계층, 스마트 컨트랙트를 처리 및 실행시키는 실행 계층, P2P 네트워크 프로토콜, 해시 함수, 전자서명, 인코딩 및 공통 저장소를 구현 및 관리하는 공통 계층, 및 다양한 어플리케이션이 생성, 처리 및 관리되는 응용 계층을 포함할 수 있다.

[59]

[60] 도 2는 본 발명의 다양한 실시 예들에 따른 환자 단말, 병원 단말의 구성에 대한 블록도를 도시한다.

[61] 도 2를 참고하면, 본 발명의 다양한 실시 예들에 따른 환자 단말(100), 병원 단말(300)은 입력 장치(110), 출력 장치(120), 송수신기(130), 메모리(140) 및 프로세서(150)를 포함한다.

[62] 입력 장치(110)는, 프로세서(150)와 연결되고 정보 등을 입력할 수 있다. 일 실시 예에 따라서, 입력 장치(110)는 송수신기(130)를 통해 유/무선 통신 네트워크(400)로 연결된 다른 장치로부터 수신한 정보 등을 입력할 수 있다. 입력 장치(110)는 터치 디스플레이, 키 패드, 키보드 등을 포함할 수 있다.

[63] 출력 장치(120)는, 프로세서(150)와 연결되고 정보 등을 영상/음성 등의 형태로 출력할 수 있다. 일 실시 예에 따라서, 출력 장치(120)는 송수신기(130)를 통해 유/무선 통신 네트워크(400)로 연결된 다른 장치로부터 수신한 정보 등을 출력할 수 있다. 출력 장치(120)는 디스플레이, 스피커 등을 포함할 수 있다.

[64] 송수신기(130)는, 프로세서(150)와 연결되고 신호를 전송 및/또는 수신한다. 송수신기(130)의 전부 또는 일부는 송신기(transmitter), 수신기(receiver), 또는 트랜시버(transceiver)로 지칭될 수 있다. 송수신기(130)는 유선 접속 시스템 및 무선 접속 시스템들인 IEEE(institute of electrical and electronics engineers) 802.xx 시스템, IEEE Wi-Fi 시스템, 3GPP(3rd generation partnership project) 시스템, 3GPP LTE(long term evolution) 시스템, 3GPP 5G NR(new radio) 시스템, 3GPP2 시스템, 블루투스(bluetooth) 등 다양한 무선 통신 규격 중 적어도 하나를 지원할 수 있다.

[65] 메모리(140)는, 입력 장치(110), 출력 장치(120), 송수신기(130)와 연결되고, 입력 장치(110)를 통해 입력된 정보, 송수신기(130)의 통신을 통해 수신한 정보 등을 저장할 수 있다. 또한, 메모리(140)는, 프로세서(150)와 연결되고 프로세서(150)의 동작을 위한 기본 프로그램, 응용 프로그램, 설정 정보, 프로세서(150)의 연산에 의하여 생성된 정보 등의 데이터를 저장할 수 있다. 메모리(140)는 휘발성 메모리, 비휘발성 메모리 또는 휘발성 메모리와 비휘발성 메모리의 조합으로 구성될 수 있다. 그리고, 메모리(140)는 프로세서(150)의 요청에 따라 저장된 데이터를 제공할 수 있다.

[66] 프로세서(150)는, 본 발명에서 제안한 절차 및/또는 방법들을 구현하도록 구성될 수 있다. 프로세서(150)는 환자 단말(100), 병원 단말(300)의 전반적인 동작들을 제어한다. 예를 들어, 프로세서(150)는 송수신기(130)를 통해 정보 등을 전송 또는 수신한다. 또한, 프로세서(150)는 메모리(140)에 데이터를 기록하고, 읽는다. 또한, 프로세서(150)는 입력 장치(110)를 통해 정보를 입력 받는다. 또한, 프로세서(150)는 출력 장치(120)를 통해 정보를 출력한다. 프로세서(150)는 적어도 하나의 프로세서(processor)를 포함할 수 있다.

[67]

[68] 도 3은 본 발명의 다양한 실시 예들에 따른 서버의 구성에 대한 블록도를 도시한다.

[69] 도 3을 참고하면, 본 발명의 다양한 실시 예들에 따른 관리 서버(200)는 송수신기(210), 메모리(220) 및 프로세서(230)를 포함한다.

[70] 송수신기(210)는, 프로세서(230)와 연결되고 신호를 전송 및/또는 수신한다. 송수신기(210)의 전부 또는 일부는 송신기(transmitter), 수신기(receiver), 또는 트랜시버(transceiver)로 지칭될 수 있다. 송수신기(210)는 유선 접속 시스템 및 무

선 접속 시스템들인 IEEE(institute of electrical and electronics engineers) 802.xx 시스템, IEEE Wi-Fi 시스템, 3GPP(3rd generation partnership project) 시스템, 3GPP LTE(long term evolution) 시스템, 3GPP 5G NR(new radio) 시스템, 3GPP2 시스템, 블루투스(bluetooth) 등 다양한 무선 통신 규격 중 적어도 하나를 지원할 수 있다.

[71] 메모리(220)는, 송수신기(220)와 연결되고, 송수신기(220)의 통신을 통해 수신한 정보 등을 저장할 수 있다. 또한, 메모리(220)는, 프로세서(230)와 연결되고 프로세서(230)의 동작을 위한 기본 프로그램, 응용 프로그램, 설정 정보, 프로세서(230)의 연산에 의하여 생성된 정보 등의 데이터를 저장할 수 있다. 메모리(220)는 휘발성 메모리, 비휘발성 메모리 또는 휘발성 메모리와 비휘발성 메모리의 조합으로 구성될 수 있다. 그리고, 메모리(220)는 프로세서(230)의 요청에 따라 저장된 데이터를 제공할 수 있다.

[72] 프로세서(230)는, 본 발명에서 제안한 절차 및/또는 방법들을 구현하도록 구성될 수 있다. 프로세서(230)는 관리 서버(200)의 전반적인 동작들을 제어한다. 예를 들어, 프로세서(230)는 송수신기(210)를 통해 정보 등을 전송 또는 수신한다. 또한, 프로세서(230)는 메모리(220)에 데이터를 기록하고, 읽는다. 프로세서(230)는 적어도 하나의 프로세서(processor)를 포함할 수 있다.

[73]

[74] 도 4는 본 발명의 다양한 실시 예들에 따른 서버의 동작 방법의 일 예를 도시한다. 도 4의 실시 예에서, 서버는 송수신기, 메모리, 프로세서를 포함한다.

[75] 도 4를 참조하면, S401 단계에서, 서버는 환자 단말과 상기 서버의 제1 암호화폐 지갑의 정보 및 상기 환자 단말의 제2 암호화폐 지갑의 정보를 상기 송수신기에 의하여 교환한다.

[76] S402 단계에서, 서버는 상기 제1 암호화폐 지갑으로부터 상기 제2 암호화폐 지갑으로 설정된 양의 암호화폐 및 OP_RETURN을 전송하는 2개의 로직과 관련된 하나의 트랜잭션 정보를 블록체인 네트워크에게 상기 송수신기에 의하여 전송한다.

[77] S403 단계에서, 서버는 병원 단말로부터 상기 제1 암호화폐 지갑에서 상기 2개의 로직과 관련된 상기 트랜잭션 정보의 요청 메시지를 상기 송수신기에 의하여 수신한다. 상기 환자 단말의 탈중앙화 신원 정보(Decentralized Identifier, DID)은 상기 제1 암호화폐 지갑의 제1 주소 및 상기 제2 암호화폐 지갑의 제2 주소를 포함한다.

[78] S404 단계에서, 서버는 상기 병원 단말에게 상기 2개의 로직과 관련된 상기 제1 암호화폐 지갑의 상기 트랜잭션 정보를 포함하는 응답 메시지를 상기 송수신기에 의하여 전송한다.

[79] 상기 제1 암호화폐 지갑의 제1 주소 및 상기 제2 암호화폐 지갑의 제2 주소에 설정된 양의 암호화폐 및 OP_RETURN을 전송하는 2개의 로직과 관련된 하나의 트랜잭션 정보가 공통적으로 존재함에 기반하여 상기 DID의 유효함이 증명된다.

[80] 상기 OP_RETURN은 트랜잭션 생성 시 상기 서버의 서명 데이터가 예정된 위치에 상기 서명 데이터를 삽입하지 않고 비우거나 또는 서명 데이터 대신 다른 데이터를 삽입한 정보이다.

[81] 본 발명의 다양한 실시 예들에 따르면, 상기 OP_RETURN은 상기 서명 데이터 대신 상기 서버에 의하여 생성된 상기 환자 단말의 상기 DID를 포함할 수 있다.

[82] 본 발명의 다양한 실시 예들에 따르면, 상기 환자 단말 및 상기 병원 단말은 상기 서버에 의하여 탈중앙화 신원 정보(Decentralized Identifier, DID)가 관리될 수 있다.

[83] 본 발명의 다양한 실시 예들에 따르면, 상기 환자 단말과 상기 병원 단말 간 의료 데이터 전송의 보안과 관련하여, 공유 키 생성을 위해 ECIES(Elliptic Curve Integrated Encryption Scheme) 및 ECDH(Elliptic Curve Diffie-Hellman)를 사용하여 상기 환자 단말과 상기 병원 단말 간 개인 키를 공유하지 않고도 데이터 암호화 및 복호화가 상기 프로세서에 의하여 수행될 수 있다. 또한, 데이터 무결성과 기밀성을 보장하기 위해 상기 환자 단말과 상기 병원 단말 간 상기 의료 데이터의 전송 전에 상기 의료 데이터를 암호화하기 위한 AES-GCM(Advanced Encryption Standard Galois/Counter Mode)가 상기 프로세서에 의하여 수행될 수 있다.

[84] ECIES(Elliptic Curve Integrated Encryption Scheme)는 대칭 암호화와 비대칭 암호화의 장점을 결합한 하이브리드 암호화 시스템이다. 이는 특히 스마트 카드나 모바일 장치와 같이 계산 리소스가 제한된 환경에서 안전한 데이터 전송에 널리 사용된다. ECIES 작동 방식에 대한 개요는 다음과 같다.

[85] (1) 키 쌍 생성: 수신자는 타원 곡선 공개-개인 키 쌍을 생성합니다. 개인 키는 비밀로 유지되는 반면, 공개 키는 잠재적인 발신자와 공유됩니다.

[86] (2) (발신자에 의한) 암호화 프로세스: 수신자의 공개 키를 가지고 있는 발신자는 이 메시지를 위해 특별히 임시 타원 곡선 키 쌍을 생성한다. 그런 다음 발신자는 수신자의 공개 키와 임시 개인 키를 사용하여 ECDH(Elliptic Curve Diffie-Hellman)를 사용하여 공유 비밀을 계산한다. 이 공유 비밀은 대칭 암호화 및 MAC(Message Authentication Code, 메시지 인증 코드) 키를 파생하는 데 사용된다. 보낸 사람은 대칭 암호화 키를 사용하여 메시지를 암호화한다. 무결성 및 인증을 위해 암호화된 메시지에 대해 MAC이 계산된다. MAC 및 보낸 사람의 임시 공개 키와 함께 암호화된 메시지가 받는 사람에게 전송된다.

[87] (3) (수신자에 의한)복호화 과정: 수신자는 자신의 개인 키와 발신자의 임시 공개 키를 사용하여 발신자와 동일한 공유 비밀을 계산한다. 이 공유 비밀에서 수신자는 동일한 대칭 암호화 및 MAC 키를 생성한다. 수신자는 메시지의 무결성과 신뢰성을 보장하기 위해 MAC를 확인한다. MAC이 유효하면 수신자는 대칭 키를 사용하여 메시지를 해독한다.

[88] ECIES의 장점은 다음과 같다.

[89] (1) 보안: 공개 키 암호화의 보안(보안 키 교환을 위한)과 대칭 암호화의 효율성을 결합한다.

[90] (2) 효율성: 타원 곡선 암호화는 RSA와 같은 다른 공개 키 시스템에 비해 더 작은 키 크기를 허용하므로 계산 속도가 빨라지고 리소스 사용량이 줄어든다.

[91] (3) 유연성: ECIES는 다양한 타원 곡선, 대칭 암호화 방식 및 MAC 알고리즘과 함께 사용할 수 있으므로 다양한 보안 요구 사항에 적응할 수 있다.

[92] ECIES는 작은 메시지를 암호화하거나 키 캡슐화(대규모 데이터 세트의 대칭 암호화에 사용되는 암호화 키)에 특히 효과적이다. 이는 많은 최신 암호화 프로토콜 및 시스템의 중요한 구성 요소로서 강력하고 효율적인 통신 보안 수단을 제공한다.

[93] ECDH(Elliptic Curve Diffie-Hellman)는 두 당사자가 안전하지 않은 채널을 통해 공유 비밀을 설정할 수 있도록 하는 핵심 합의 프로토콜이다. 타원곡선 암호화를 응용한 것이다. ECDH 작동 방식에 대한 기본 개요는 다음과 같다.

[94] (1) 키 생성: 각 당사자는 개인 키(무작위로 선택한 숫자)와 공개 키(개인 키에서 계산되는 타원 곡선의 점)라는 자체 키 쌍을 생성한다.

[95] (2) 공개 키 교환: 당사자들은 공개 키를 서로 교환한다. 이 교환은 안전할 필요가 없다. 공개 키는 비밀이 아니다.

[96] (3) 공유 비밀 계산: 각 당사자는 상대방의 공개 키와 자신의 개인 키를 결합하여 공유 비밀을 계산한다. 이는 타원 곡선의 속성과 Diffie-Hellman 문제의 수학을 사용하여 수행된다. ECDH의 장점은 양 당사자가 동일한 공유 비밀에 독립적으로 도달한다는 것이다. 한쪽의 공개키와 상대방의 개인키를 결합하면 상대방의 공개키와 첫 번째 개인키를 결합한 것과 같은 값이 나오기 때문이다.

[97] (4) 공유비밀의 활용: 그런 다음 공유 비밀을 사용하여 대칭 암호화 알고리즘을 사용하여 추가 통신을 암호화할 수 있다.

[98] ECDH는 보안 웹 통신을 위한 SSL/TLS와 다양한 보안 메시징 애플리케이션을 비롯한 다양한 암호화 프로토콜에서 널리 사용된다. ECDH의 강점은 현재 기술로는 해결하기 어려운 타원곡선 이산대수 문제를 기반으로 한다는 점이다. 이로 인해 ECDH는 특히 처리 능력과 대역폭이 중요한 환경에서 안전한 키 교환을 위한 강력한 선택이 된다. 모든 암호화 프로토콜과 마찬가지로 ECDH의 보안은 안전한 타원 곡선 선택 및 다양한 유형의 암호화 공격에 대한 보호를 포함하여 적절한 구현에 달려 있다.

[99] AES-GCM(Advanced Encryption Standard Galois/Counter Mode)은 민감한 데이터를 보호하기 위해 널리 사용되는 암호화 알고리즘이다. AES(Advanced Encryption Standard) 알고리즘과 GCM(Galois/Counter Mode) 작동을 결합한다. 주요 특징에 대한 개요는 다음과 같다.

[100] (1) AES(Advanced Encryption Standard, 고급 암호화 표준): AES는 대칭 키 암호화 알고리즘이다. 즉, 데이터 암호화 및 암호 해독에 동일한 키를 사용한다. 이는 보안 강도와 효율성으로 인해 전 세계적으로 안전한 데이터 암호화의 사실상 표준이 되었다. AES는 128, 192, 256비트의 키 크기를 지원한다.

[101] (2) GCM(Galois/Counter Mode, 갈루아/카운터 모드): GCM은 대칭 키 암호화 블록 암호의 작동 모드이다. 암호화를 통한 기밀성(confidentiality)과 데이터 신뢰성을 통한 무결성(integrity)을 모두 제공하는 스트림 암호화 모드이다. GCM은 암호화 프로세스를 병렬화하는 방식으로 블록 암호를 기반으로 작동하여 긴 메시지의 처리 속도를 높인다.

[102] (3) AES와 GCM의 조합: AES-GCM은 AES 알고리즘과 GCM 모드를 결합하여 데이터를 효율적으로 암호화하고 인증하는 시스템을 만든다. 이 조합은 AES 암호화를 통한 기밀성과 GCM의 인증 기능을 통한 인증된 무결성을 제공한다.

[103] (4) 기능: AES-GCM에서 데이터는 데이터 블록(일반적으로 128비트 크기)에 대한 일련의 작업을 통해 암호화된다. GCM 모드는 각 블록에 카운터를 적용하여 각 블록이 고유 키로 암호화되도록 한다. 또한 GCM은 데이터에 대한 무결성 검사를 제공하는 인증 태그(암호화 체크섬 유형)를 계산한다.

[104] (5) 장점:

[105] 효율성: 병렬 데이터 블록을 처리하는 기능으로 인해 처리량이 높은 환경에 적합하다.

[106] 보안: 강력한 데이터 기밀성과 무결성을 제공한다.

[107] 유연성: AES와 함께 가장 일반적으로 사용되지만 다양한 블록 암호화 알고리즘과 함께 사용할 수 있다.

[108] (6) 애플리케이션: AES-GCM은 TLS(Transport Layer Security, 전송 계층 보안) 및 IPSec(Internet Protocol Security, 인터넷 프로토콜 보안)과 같은 보안 통신 프로토콜에 널리 사용된다. 또한 파일 암호화, 보안 데이터 전송, VPN(Virtual Private Networks, 가상 사설망) 등 암호화와 데이터 무결성이 모두 필요한 다양한 애플리케이션에도 사용된다.

[109] 구현 고려 사항: AES-GCM의 올바른 구현은 보안에 매우 중요하다. 키 또는 nonce(한 번 사용되는 숫자)를 잘못 관리하면 암호화 보안이 손상될 수 있다. AES-GCM은 AES 암호화의 장점과 GCM 작동 모드의 추가 보안 및 성능 이점을 결합하여 최신 암호화 요구 사항에 맞는 강력하고 효율적인 선택이다.

[110]

[111] 본 발명의 다양한 실시 예들에 따르면, 통신 시스템에서 서버에 있어서, 송수신기, 메모리, 프로세서를 포함하고, 프로세서는 도 4의 실시 예에 따른 서버의 동작 방법을 수행하도록 구성된 서버가 제공된다.

[112]

[113] 본 발명의 다양한 실시 예들에 따르면, 도 4의 실시 예에 따른 서버의 동작 방법을 수행하도록 구성되며, 컴퓨터 판독 가능한 저장 매체에 기록된 컴퓨터 프로그램이 제공된다.

[114]

[115] 도 5는 본 발명의 다양한 실시 예들에 따른 환자 단말의 동작 방법의 일 예를 도시한다. 도 5의 실시 예에서, 환자 단말은 송수신기, 메모리, 프로세서를 포함한다.

[116] 도 5를 참조하면, S501 단계에서, 환자 단말은 서버와 상기 서버의 제1 암호화폐 지갑의 정보 및 상기 환자 단말의 제2 암호화폐 지갑의 정보를 상기 송수신기에 의하여 교환한다.

[117] S502 단계에서, 환자 단말은 상기 제1 암호화폐 지갑으로부터 상기 제2 암호화폐 지갑으로 설정된 양의 암호화폐 및 OP_RETURN을 수신하는 2개의 로직과 관련된 하나의 트랜잭션 정보를 블록체인 네트워크에게 상기 송수신기에 의하여 전송한다.

[118] S503 단계에서, 환자 단말은 각 통신 인스턴스에 대하여 ECIES(Elliptic Curve Integrated Encryption Scheme) 방식에 기반하여 무작위 개인 키 및 무작위 공개 키의 키 쌍을 상기 프로세서에 의하여 생성한다.

[119] S504 단계에서, 환자 단말은 상기 환자 단말의 상기 무작위 개인 키 및 병원 단말의 공개 키로부터 계산되는 ECDH(Elliptic Curve Diffie-Hellman) 공유 키를 사용하여 상기 환자 단말의 의료 데이터를 상기 프로세서에 의하여 암호화한다.

[120] S505 단계에서, 환자 단말은 상기 환자 단말의 무작위 공개 키와 함께 상기 암호화된 의료 데이터를 상기 병원 단말에게 상기 환자 단말의 탈중앙화 신원 정보(Decentralized Identifier, DID)에 기반하여 상기 송수신기에 의하여 전송한다.

[121] 상기 DID는 상기 제1 암호화폐 지갑의 제1 주소 및 상기 제2 암호화폐 지갑의 제2 주소를 포함한다.

[122] 상기 제1 암호화폐 지갑의 제1 주소 및 상기 제2 암호화폐 지갑의 제2 주소에 설정된 양의 암호화폐 및 OP_RETURN을 전송하는 2개의 로직과 관련된 하나의 트랜잭션 정보가 공통적으로 존재함에 기반하여 상기 DID의 유효함이 증명된다.

[123] 상기 OP_RETURN은 트랜잭션 생성 시 상기 서버의 서명 데이터가 예정된 위치에 상기 서명 데이터를 삽입하지 않고 비우거나 또는 서명 데이터 대신 다른 데이터를 삽입한 정보이다.

[124]

[125] 본 발명의 다양한 실시 예들에 따르면, 상기 OP_RETURN은 상기 서명 데이터 대신 상기 서버에 의하여 생성된 상기 환자 단말의 상기 DID를 포함할 수 있다.

[126] 본 발명의 다양한 실시 예들에 따르면, 상기 환자 단말 및 상기 병원 단말은 상기 서버에 의하여 탈중앙화 신원 정보(Decentralized Identifier, DID)가 관리될 수 있다.

[127] 본 발명의 다양한 실시 예들에 따르면, 상기 환자 단말과 상기 병원 단말 간 상기 의료 데이터의 전송의 보안과 관련하여, 공유 키 생성을 위해 ECIES(Elliptic Curve Integrated Encryption Scheme) 및 ECDH(Elliptic Curve Diffie-Hellman)를 사용하여 상기 환자 단말과 상기 병원 단말 간 개인 키를 공유하지 않고도 데이터 암호화 및 복호화가 수행될 수 있다. 데이터 무결성과 기밀성을 보장하기 위해

상기 환자 단말과 상기 병원 단말 간 상기 의료 데이터의 전송 전에 상기 의료 데이터를 암호화하기 위한 AES-GCM(Advanced Encryption Standard Galois/Counter Mode)가 수행될 수 있다.

[128]

[129] 본 발명의 다양한 실시 예들에 따르면, 통신 시스템에서 환자 단말에 있어서, 송수신기, 메모리, 프로세서를 포함하고, 프로세서는 도 5의 실시 예에 따른 서버의 동작 방법을 수행하도록 구성된 서버가 제공된다.

[130] 본 발명의 다양한 실시 예들에 따르면, 도 5의 실시 예에 따른 환자 단말의 동작 방법을 수행하도록 구성되며, 컴퓨터 판독 가능한 저장 매체에 기록된 컴퓨터 프로그램이 제공된다.

[131]

[132] 비트코인 DID와 데이터 거래 기술에 관하여 설명한다.

[133] 블록체인: Bitcoin, ION, Lightning, Liquid

[134] 암호학: ECDSA, ECDH, ECIES, AES-GCM, PBKDF2, SHA256

[135] 이하, Hippocrat Bitcoin DID, Hippocrat data economy에 대하여 설명한다.

[136] 본 발명의 다양한 실시 예들에서, Hippocrat은 관리 서버(200)의 운영자로서, 환자와 병원간 의료 데이터 거래를 수행할 수 있는 플랫폼을 제공하는 사업자에 대한 예시적 명칭에 해당한다. 즉, 본 발명의 다양한 실시 예들에서, Hippocrat은 관리 서버(200), 또는, 관리 서버(200)의 운영자, 또는, 환자와 병원간 의료 데이터 거래를 수행할 수 있는 플랫폼을 제공하는 사업자, 또는, 본 발명의 다양한 실시 예들로 치환하여 해석될 수 있다.

[137]

[138]

[139] 1. Hippocrat Bitcoin DID

[140] 1.1. 기존 플랫폼의 인증 체계

[141] 기존 플랫폼의 인증 체계에는 크게 3명의 참여자가 있다.

[142] 신원의 주권자인 개인(환자(Patient)로 예시를 들 수 있다.) 위 개인의 신원을 증명해주는 증명 기관(증명기관은 의료 데이터의 거래 플랫폼에 대한 운영자 등이 될 수 있으며, 이러한 증명 기관의 예시적 명칭으로서 Hippocrat으로 예시를 들 수 있다.) 위 개인의 신원을 확인하려는 외부 기관(병원(Hospital)로 예시를 들 수 있다.)

[143]

[144] 인증이 요청될 수 있는 예시 상황을 들어보겠다. 예를 들어, 환자는 희귀질환 환자로, 의학적으로 연구 가치가 아주 높은 유전체 데이터를 보유하고 있다. 이에 병원은 연구를 위해 위 환자의 유전체 데이터를 구매하고자 한다. 이러한 거래가 플랫폼 상에서 이루어지기 위해서는 환자는 거래가 이루어지는 플랫폼에 등록된 신원(및 데이터)가 자신의 것이 맞다는 것을 증명해야 한다.

[145] 기존의 플랫폼은 증명 기관, 예를 들어, 중앙화된 데이터베이스에 환자의 신원 정보를 저장한다. 환자는 신원증명 데이터를 보유하지도 관리하지도 않는다. 병원 역시 중앙화된 데이터베이스를 통해 환자의 신원 증명을 확인할 수 있다. 이처럼 기존의 인증 체계는 보안적으로도 위험하고(중앙화된 데이터베이스라는 단일 실패 지점 존재), 개인의 데이터 주권이 존재하지 않는다.

[146]

[147] 1.2. Hippocrat DID 인증 체계

[148] Hippocrat의 인증 체계에는 마찬가지로 3명의 참여자가 있다. 신원의 주권자이자 이를 DID로 직접 소유하는 개인(예를 들어, 환자)이 있다. 위 DID가 Hippocrat이 발급한 것임을 증명해주는 탈중앙화 데이터베이스(예를 들어, Bitcoin)가 있다. 개인의 DID 및 탈중앙화 데이터베이스를 확인하려는 외부 기관(예를 들어, 병원)이 있다.

[149] 인증이 요청되는 예시 상황은 앞서 1.1과 동일하다고 전제하겠다. 먼저, DID는 개인이 직접 신원 증명 데이터를 소유하는 것이다. DID는 W3C에서 정한 표준에 따라 크게 3가지로 구성된다.

[150] Id: 해당 DID의 고유한 식별자이다.

[151] Key Pair: 공개 키-비밀 키로 이루어진다.

[152] Service: DID에 들어갈 신원 데이터이다.

[153] DID는 공개 키-비밀 키라는 비대칭 키 구조의 ECDSA을 활용하여 신원을 증명한다.

[154] 비밀 키는 중앙화된 데이터베이스가 아닌 개인이 직접 소유하며(예를 들어, 로컬 디바이스의 디스크), 해당 비밀 키를 기반으로 서명을 생성한다. 반면, 공개 키는 DID에 공개되어 기록된다. 위의 비밀 키로 생성된 서명은 공개 키로 인증이 가능하다. 따라서, 특정 개인이 해당 DID의 소유자가 자신임을 인증할 때에는, 자신만의 고유한 비밀 키로 서명을 생성한 후, 신원 증명 여부를 확인하고자 하는 상대방이 DID에 공개되어 있는 자신의 공개 키로 해당 서명이 유효함을 확인하는 방식으로 이루어질 수 있다. 즉, 개인이 온전히 신원 데이터의 소유자가 되어 데이터 주권을 높임과 동시에 단일 실패 지점에 대한 우려를 지울 수 있다.

[155] ION DID는 이러한 표준을 준수하는 비트코인 레이어 2 DID 서비스이다. DID 생성 시 레이어 2인 ION 네트워크에서 작업 증명을 수행한 후, 1만 개의 DID를 배치 단위로 비트코인 메인넷에 기록한다. ION은 Microsoft와 Block과 같이 기술력이 높고 비트코인에 대한 이해도가 높은 빅테크의 주요 개발자들이 기여 중인 오픈소스이다. 이에 본 발명의 다양한 실시 예들은 ION DID를 활용하고 직접 해당 오픈소스에 기여하고자 한다.

[156] 하지만, ION DID만으로는 부족하다. 예를 들면, ION DID의 서비스, 즉 개인의 신원 증명 데이터에는 본 발명의 다양한 실시 예들에 따라서 ION DID를 발급했다는 증명이 필요하다(물론, 표식만 남길 뿐 개인의 데이터와 비밀 키는 개인이 저장한다). 당연히 본 발명의 다양한 실시 예들에 따른 중앙화된 데이터베이스에

는 아무것도 저장하지 않는 방식으로 수행된다. 만약 그 곳에 단순히, 예시적으로,“특정 플랫폼 사업자(예를 들어, Hippocrat)이 발급한 DID입니다” 라는 문장을 넣는 것으로 충분하지 않다. ION DID는 해당 id를 가진 DID의 소유자가 개인 키를 들고 있는 이의 소유라는 것만 증명할 수 있다. 즉, 악의적인 공격자가 위 내용을 그대로 복사하여 포함시키는 새로운 ION DID를 만들고 개인 키를 로컬에 소유하며 서명을 한다면, 본 발명의 다양한 실시 예들에 따라서 발급한 ION DID의 진위 여부를 구분할 수 없게 된다. 이를 위해서 신원 증명의 경우, 인증 가능한 탈중앙화 데이터베이스를 활용해야 한다.

[157] Hippocrat은 탈중앙화된 시스템인 비트코인을 인증 가능한 탈중앙화 데이터베이스로 활용할 수 있다. 기술적인 프로세스는 다음과 같다.

[158] 1. Patient 및 Hippocrat의 비트코인 지갑을 생성한다.

[159] 2. Hippocrat의 비트코인 지갑에서 OP_RETURN*과 Patient 비트코인 지갑에 설정된 양, 예를 들어, 극소량의 비트코인을 전송하는 2개의 로직을 하나의 트랜잭션으로 전송한다.

[160] 3. Patient의 ION DID에 Patient 및 Hippocrat의 비트코인 지갑 주소를 포함시킨다.

[161] 4. Hospital은 Patient ION DID에 포함된 Patient 및 Hippocrat의 비트코인 주소에 2의 트랜잭션 기록이 존재하는지 확인한다.

[162] 5. 이를 통해 Patient ION DID가 Hippocrat이 발급한 유효한 DID임을 확인할 수 있다.

[163]

[164] 도 6은 본 발명의 다양한 실시 예들에 따른 비트코인에 기록되는 ION DID의 일 예를 도시한다.

[165] OP_RETURN은 비트코인 블록에 작은 크기의 데이터를 저장할 수 있는 기술이다. 비트코인 역시 공개 키-비밀 키 서명 인증 구조(Elliptic Curve Digital Signature Algorithm, ECDSA)를 사용하는데, 트랜잭션 생성시 서명에 필요한 데이터를 넣지 않아 의도적으로 유효하지 않은 트랜잭션을 생성한다. 굳이 수수료를 내면서 유효하지 않은 트랜잭션을 생성하는 이유는 위의 서명에서 넣지 않은 서명 데이터의 크기만큼 자유롭게 데이터를 저장할 수 있기 때문이다. 여기에, “Hippocrat이 발급한 DID입니다” 역시 넣을 수 있다. 이처럼 비트코인 블록체인을 Hippocrat DID 인증 체계의 탈중앙화 데이터베이스로 활용함으로써, 높은 수준의 무결함과 검열저항성을 실현할 수 있다. 제안된 방법을 통해 악의적인 공격자가 환자가 아님에도 위 내용을 포함하여 가짜 ION DID를 생성할 경제적 유인이 사라질 수 있다. ION DID에는 진짜 환자의 비트코인 지갑 주소가 들어가 있기 때문이다.

[166] 설사 악의적인 공격자가 비트코인 지갑 주소만 자신의 비트코인 주소로 수정하여 ION DID를 만들었다 하더라도 비트코인 블록체인 상에서 Hippocrat의 OP_RETURN 트랜잭션 내역이 없기 때문에 가짜임이 드러난다.

[167] ION DID 및 비트코인 블록에 기록되는 트랜잭션의 일 예시는 도 6과 같다.

[168]

[169] 도 7는 본 발명의 다양한 실시 예들에 따른 OP_RETURN을 활용한 개인 신원 인증 내역 기록의 일 예를 도시한다.

[170] (1) DID 발급자(트랜잭션 인풋)은 본 발명의 다양한 실시 예들에 따른 DID 관리자의 지갑이며 트랜잭션 수수료를 부담한다.

[171] (2) DID 레지스트리(Tx 아웃풋 1)은 OP_RETURN에 humanDid라고 표식을 한다.

[172] (3) DID 소유자(Tx 아웃풋 2)는 DID 소유자이며, 본 발명의 다양한 실시 예들에 따른 데이터 지갑에서의 OP_RETURN 트랜잭션과 함께 있으면 휴먼의 환자임이 증명될 수 있다. 여러 명의 소유자에게 한 번에 발급이 가능한 구조이다(예를 들어, Tx 아웃풋 3, Tx 아웃풋 4, Tx 아웃풋 5, ...).

[173] 도 7은 OP_RETURN을 활용한 Hippocrat 인증 내역 기록(예를 들어, 비트코인 블록 익스플로러)의 일 예시를 도시한다. 이처럼, 본 발명은 현존하는 DID 중에서도 높은 수준의 보안성과 확장성을 확보하는 DID를 제공할 수 있다.

[174]

[175] 2. Hippocrat data economy

[176] 2.1. 블록체인 데이터 경제 구축을 위한 기술적 이슈

[177] 본 발명의 다양한 실시 예들에 따른 비트코인 DID를 기반으로 구현하고자 하는 서비스는 바로 탈중앙화 데이터 거래 시장이다. 환자의 의료 데이터는 상당히 높은 가치를 가지고 있음에도 불구하고, 환자들이 직접 보유 및 관리하는 경우가 드물고, 따라서 수익을 창출하는 일도 아직 많지 않은 상황이다. 이러한 의료 데이터는 각 병원의 중앙화된 서버에 저장되어 관리되어 있다. 이 때문에 환자의 마이데이터 주권도, 의료 데이터 사이언스의 발전에도 큰 걸림돌이 되고 있다.

[178] 이러한 점을 해결하기 위해 본 발명의 다양한 실시 예들은 다음과 같은 데이터 거래 시장을 구현한다.

[179] (1) 환자인 Alice는 자신의 의료 데이터를 병원으로부터 가져온다.

[180] (2) 병원의 연구원인 Bob은 Alice의 의료 데이터의 메타 데이터를 확인하고, 1 BTC에 구매하겠다는 의사를 전달한다.

[181] (3) Alice가 동의 시, Bob은 1 BTC을 Hippocrat DID에 적힌 Alice의 비트코인 주소로 송금한다.

[182] (4) Alice는 비트코인에 입금을 확인한 후 자신의 의료 데이터를 암호화하여 전송한다.

[183] (5) Bob은 암호화된 데이터를 수신받은 후 복호화한다.

[184]

[185] 여기서 기술적 이슈는 2가지이다. 데이터의 암호화/복호화 및 안전한 송수신 확장성 높은 비트코인 결제 솔루션과 관련하여, 본 발명의 다양한 실시 예들은 DIDComm 표준에 따라 ECDH 기반 다중 서명 기술을 통해 안전하게 데이터를

암호화/복호화하여 송수신한다. 또한, 확장성 높은 비트코인 결제를 위해 Liquid 및 Lightning 네트워크를 통한 결제 솔루션을 제공한다.

[186]

[187] 2.2. 보안성: 암호학적으로 안전한 데이터 전송 및 저장 기술

[188] ECDH(Elliptic Curve Diffie-Hellman)는 ECDSA(Elliptic Curve Digital Signature Algorithm)와 마찬가지로 Elliptic Curve를 기반으로 생성되는 비대칭 키 페어를 활용한다. ECDH의 DH(Diffie-Hellman)는 디피-헬먼으로, 키 교환 알고리즘을 활용하여 2개의 비대칭 키 페어로 하나의 공유 키를 계산한다. 즉, 본 발명의 다양한 실시 예들에 따른 DID 보유자 2명이 각자의 비밀 키를 공유하지 않으면서 암호화에 사용할 수 있는 공유 키를 만들 수 있다.

[189] 프로세스는 아래와 같다.

[190] (1) Alice가 Bob에게 의료 데이터를 전송하는 상황이다.

[191] (2) Alice와 Bob은 본 발명의 다양한 실시 예들에 따른 DID의 보유자로, EC로 생성된 비대칭 키 페어를 보유하고 있다(각자의 공개 키는 DID에 공개되어 있고, 비밀 키는 각자만 알고 있다).

[192] (3) Alice는 Bob의 공개 키와 자신의 비밀 키로 공유 키 A를 계산한다.

[193] (4) Bob은 Alice의 공개 키와 자신의 비밀 키로 공유 키 B를 계산한다.

[194] (5) 위와 같은 방식으로 계산 시, 공유 키 A = 공유 키 B가 된다.

[195] (6) 이러한 공유 키는 1개의 대칭 키다.

[196] (7) Alice는 대칭 키 암호화 알고리즘 표준인 AES-GCM을 활용하여 데이터를 암호화한다.

[197] (8) Bob은 계산한 공유 키로 데이터를 복호화한다.

[198] 이러한 방식을 통해 비대칭적으로 각각의 비밀 키를 보유하지만 대칭적으로 공유 키를 계산하게 된다. 설사 공유 키가 탈취되더라도, 각자의 비밀 키는 탈취되지 않는 장점이 있다.

[199] 하지만 실제 통신에 있어서는, 굳이 Alice가 자신의 비밀 키로 직접 공유 키 A를 연산할 필요까지는 없다. 데이터 암호화 전달을 위한 표준 프레임워크인 ECIES를 사용하면 된다. 즉, 다음과 같은 방법으로 수행하면 된다.

[200] (1) Alice는 통신 1회마다 EC 기반의 랜덤 키 페어를 생성한다.

[201] (2) Alice는 자신의 랜덤 개인 키와 Bob의 고정 공개 키로 공유 키를 계산한다.

[202] (3) Alice는 공유 키로 데이터를 암호화하면서 전송할 때, 1에서 생성한 랜덤 공개 키와 함께 전송한다.

[203] (4) Bob은 수신 받은 랜덤 공개 키와 자신의 고정 비밀 키로 공유 키를 계산하여 데이터를 복호화 한다.

[204] 이처럼 보안을 위해 송신 측은 자신의 고정 비밀 키가 아닌 일회용 랜덤 비밀 키를 사용하여 보안성을 더 높이고 있다. 결론적으로, ECDH를 활용하는 ECIES(Elliptic Curve Integrated Encryption Scheme) 암호화 통신 프레임워크를 사용하여, 본 발명의 다양한 실시 예들의 데이터 거래 시장에서 순수한 Peer-to-Peer

의 데이터 전송을 DID 키를 통해 안전하고 편리하게 구현할 수 있다. 이러한 암호화 기술은 본 발명의 다양한 실시 예들에 따른 데이터 지갑의 니모닉을 암호화할 때에도 활용되어, 편의성과 보안성을 모두 추구할 수 있다.

[205]

[206] 2.3. 확장성: 비트코인 Layer2를 통한 확장성 높은 결제

[207] 비트코인은 가장 탈중앙화되고 신뢰도가 높은 블록체인이지만, 많은 거래를 위한 확장성은 아직 부족하다. 트랜잭션이 완료되는 데에 평균 10분 이상이 소요되고, 수수료도 1 USD 이상 요구된다. 만약 의료 데이터가 충분히 가치가 큰 경우에는 메인넷을 활용하여 결제되어도 괜찮겠지만, 소액의 가치를 가진 의료 데이터를 빈번하게 거래하기 위해서는 확장성이 높은 솔루션이 필수적이다.

[208] 이에 본 발명의 다양한 실시 예들은 비트코인 메인넷 결제 솔루션에 더해, 레이어 2 솔루션들을 지원한다. 이러한 솔루션에는 리퀴드와 라이트닝 네트워크가 있다.

[209] 리퀴드 네트워크는 비트코인 코어 개발자들이 설립한 블록스트림에서 구현한 사이드체인 기반의 비트코인 레이어2 솔루션이다. 사이드체인이란 일종의 독립된 블록체인으로서 자체 합의 과정과 알고리즘을 기반으로 하지만, 레이어 1의 암호화폐(예를 들어, 비트코인)를 해당 사이드체인에 페그 및 언페그하는 방식을 사용한다. 즉, 리퀴드의 경우, 메인넷 비트코인과 리퀴드 비트코인 간의 전환(페그 및 언페그)가 가능하여, 리퀴드 네트워크에서는 리퀴드 비트코인을 활용한다. 이러한 리퀴드 네트워크는 DPOS 와 유사하게 15개의 노드 중 11개의 노드가 합의가 될 때 블록을 생성하고, 이에 더해 페그 및 언페그를 실행한다. HSMs(hardware security modules)에 저장하는 키를 사 용함으로써 보안성을 확보한다. 또한, 이더리움의 ERC20과 같은 토큰을 발행할 수 있도록 하여 비트코인 기반의 토큰 이코노미를 구현할 수 있다.

[210] 라이트닝 네트워크는 현재 비트코인 레이어 2 솔루션으로 가장 많이 채택되고 있는 솔루션으로, 비트코인의 멀티시그 지갑을 활용한 스테이트 채널 솔루션이다. Alice와 Bob이 비트코인을 라이트닝 네트워크로 전송하기 위해서는, 양측의 비밀 키 서명이 모두 있어야 트랜잭션을 생성할 수 있는 2-of-2 멀티시그 지갑을 생성한다. 이후 Alice와 Bob은 연결된 라이트닝 채널에서 상대방에게 비트코인을 전송할 때, 각자의 비밀 키로 서명된 불완전 트랜잭션을 생성한다. 이렇게 할 경우, 상대방은 전송된 트랜잭션에 자신의 서명만이 있으면 비트코인 메인넷에서 해당 트랜잭션이 실행될 수 있기 때문에 악의적으로 장부를 조작할 가능성이 사라진다. 이처럼 라이트닝 네트워크에서 무수히 많은 불완전 트랜잭션을 생성한 후, 최종적으로 계산된 잔고를 멀티시그 지갑 서명을 통해 온체인 트랜잭션 한 개로 기록한다. 악의적인 사용자가 자신에게 유리한 과거의 불완전 트랜잭션을 서명하려고 하는 등 공격 시나리오가 이외에도 있지만 해시타임락을 통해 방지할 수 있다.

[211] 이처럼 본 발명의 다양한 실시 예들은 안전한 데이터 송수신 및 비트코인 기반 결제 솔루션 지원을 통해, 의료 데이터 토큰 이코노미를 구축할 수 있다.

[212]

[213] 도 8은 본 발명의 다양한 실시 예들에 따른 의료 데이터의 수집 및 활용 생태계의 일 예를 도시한다.

[214] 지난 2018년 시작된 HUM 프로젝트는 투명하게 환자 데이터를 수집하고 활용할 수 있는 환경을 구축하여 의료 서비스의 개인화에 기여하겠다는 비전과 함께 출발하였다. 2020년에는 파트너 개발 법인인 Humanscape Inc.를 통해 레어노트를 출시하였고 지금까지 약 3만 명의 희귀질환 환자를 대상으로 환자 데이 터를 확보했다. 이 과정에서 환자들의 다양한 건강 데이터 수집 내역이 블록체인에 기록되었고 현재까지 7,200건 이상의 트랜잭션이 발생하였다. 추가로 2020년에는 임신·육아 서비스 마미톡, 2022년에는 임상연구 데이터 플랫폼 레어데이터를 차례로 출시하면서 데이터의 생성과 활용 과정에서 생길 수 있는 문제들을 더욱 잘 이해하게 되었다. 하지만, '건강 데이터의 수집 및 활용 생태계'가 본연의 의미대로 자리 잡으려면 아래 3가지 항목을 충족할 수 있어야 한다.

[215] (1) 환자 중심의 데이터 활용 환경 구축

[216] (2) 탈중앙 거버넌스 및 개방형 협력 구조

[217] (3) 환자뿐만 아니라 거버넌스 참여자들까지 고려한 지속가능한 인센티브 모델

[218] 이러한 과정을 통해 프로젝트 팀은 기존 HUM 프로젝트 백서를 통해 밝힌 거버넌스와 목표의 한계를 넘어서는 새로운 구조의 청사진이 필요하다. 실제로, 파트너 개발 법인 Humanscape Inc.의 한두가지 서비스 외에는 전세계적으로 블록체인에 기반을 두고 건강 데이터를 유의미하게 활용하는 사례를 찾기 어렵다. 데이터 생성이 가능하거나 이미 많은 데이터를 수집하고 있는 주요 조직과 기관이, 특정 민간 회사에서 주도권을 지니고 있는 블록체인 프로젝트에 선뜻 참여하기 어려운 이해관계를 구성하고 있기 때문이다. 이에 본 발명의 다양한 실시 예들에서, HUM 프로젝트 팀은 Hippocrat이라는 새로운 정체성을 가지고 '건강 데이터 수집·활용 생태계 구축'을 위한 청사진을 제시한다. Hippocrat이란 '히포크라테스의 정당'이라는 의미로, 고대 그리스 의학자 히포크라테스의 이름을 따랐다.

[219]

[220] 본 발명의 다양한 실시 예들에서 제공하는 인센티브 모델과 거버넌스는 더욱 개방적이고 탈중앙화된 프로토콜상에서 정보 주체가 헬스케어 데이터에 대한 자기 주권을 가지도록 하고, 의료 기관과 헬스케어 데이터를 활용하는 기관들이 원활하게 협력하도록 도울 수 있다. 이는 정보 주체를 개인정보 침해로부터 보호하고, 개인과 기관 간의 신뢰를 구축하며, 데이터의 활용을 촉진하여 건강을 증진하고 삶의 질을 높일 수 있는 다양한 혁신을 일으킬 수 있다.

[221] 예를 들어, 환자는 개인정보 침해의 위험은 최소화하면서 자신의 헬스케어 데이터를 활용하여 맞춤형 건강 관리를 받을 수도 있고 데이터 활용으로부터 발생하는 수익을 기대할 수도 있다. 제약사나 헬스케어 서비스 제공자는 환자의 충분

한 동의 하에 데이터를 확보하여 이를 더 효율적인 임상시험 대상자 스크리닝이나 정밀 의료 서비스를 개발하는 데 활용할 수 있다. 병원 등 의료 기관은 정보 주체가 요구하는 높은 수준의 데이터 권리를 충족시키면서도, 스스로 데이터 생성에 기여했음을 입증하여 지속가능한 데이터 제공을 위한 보상을 기대할 수 있다.

[222] 헬스케어 데이터를 얻으려면 공공 보건의료 체계와 그 지속가능성이 중요하다. 본 발명의 다양한 실시 예들에서 제시하는 의료 데이터의 거래 방식의 활성화는 개별 이해관계자에게 이익이 될 뿐만 아니라, 각 정보 주체가 속한 국가의 공공 보건의료 체계에 기부되는 재원의 증가를 도울 수 있다. 이처럼 본 발명의 다양한 실시 예들은 정보 주체 및 개별 이해관계자의 권리를 강화하는 것은 물론, 전 세계의 더 많은 환자와 생태계 내 이해관계자가 건강한 삶을 누리는 미래에 기여할 수 있다.

[223]

[224] 헬스케어 데이터의 정의와 분류 기준은 다양하다. 이하, 본 발명의 다양한 실시 예들에서 사용되는 헬스케어 데이터의 분류 방법과 그 개념을 설명한다.

[225]

[226] 개인의 식별가능성에 대한 분류

[227] 미국을 비롯한 대부분 주요 국가는 개인의 식별가능성을 데이터 분류의 중요한 기준으로 포함하고 있다. 특히 의료 데이터의 식별가능성은 개인 정보 침해의 위험이 있기에 이를 방지하는 것도 중요하지만, 가치 있는 다양한 데이터를 결합해 환자와 개인의 건강을 개선하는 새로운 혁신을 이끌어 내는 데 활용되기도 한다. 따라서 개인정보 보호와 활용 사이에서 적정선을 유지할 수 있는 섬세한 접근이 필요하다. 이러한 접근 방식을 따르고 있는 가장 대표적인 방법은 미국의 HIPPA/HITECH 방법이다. 이 방법은 의료정보(Health Information)의 보호와 활용에 관한 기초적인 원칙을 제시하며 의료정보를 아래 3가지로 분류하고 있다. 이 분류에 포함되지 않는 의료정보도 기본적으로는 개인정보 보호 관련 일반법을 따른다.

[228] [표1]

데이터 종류	식별가능성	환자의 활용 동의 필요	연구 목적 활용
보호의료정보(PHI)	O	O	IRB 심사 후 가능
비식별의료정보(DHI)	X	X	자유롭게 가능
한정데이터세트(LDS)	X(다소 완화된 조건 적용)	X (연구 등 목적은 면제)	데이터 재식별 금지 합의서 제출 및 IRB 심사 후 가능

[229] 보호의료정보(Protected health information, PHI)보호의료정보는 HIPPA가 적용되는 의료 기관, 지불 기관, 의료 관련 기관에서 생성, 수집, 전송, 보관되는

개인의 (1) 과거, 현재, 미래의 물리적, 정신적 건강 상태, (2) 건강보험 정보, (3) 의료비 지출 상황 등에 대한 정보 로서 개인이 식별되는 의료정보(individually identifiable health information)라고 정의된다.

[230] 보호의료정보는 공익 등 일부 예외적인 경우를 제외하면 치료 외 목적으로는 환자의 동의를 받아야만 활용, 정정, 반출할 수 있도록 규정되어 있다. 연구 기관 등은 연구 목적으로 기관생명윤리위원회(Institutional review board, IRB)를 거쳐 보호의료정보를 활용할 수 있다.

[231]

[232] 비식별의료정보(De-identified health information, DHI)

[233] 비식별의료정보는 1) 세이프하버(Safe harbor) 방식과 2) 전문가 판단 방식 두 가지에 의해 인정된다. 세이프하버 방식은 아래 18가지 유형의 식별자를 제거하는 방식을 말한다. 전문가 판단 방식의 주체는 식별가능성 또는 식별방법에 관하여 통계, 과학 분야의 적절한 지식과 전문성을 갖춘 사람이다. 해당 정보가 다른 정보와 결합하더라도 개인을 식별할 수 있는 리스크가 매우 적다고 판단하고, 그 이유와 결과를 문서로 기록해야 인정될 수 있다.

[234] HIPAA에서 규정한 기관들은 비식별의료정보를 자유롭게 사용하거나 공개할 수 있도록 규정되어 있다. 만약 이러한 조치에도 불구하고 식별가능한 것으로 판단될 경우, 보호의료정보(PHI)로 간주된다.

[235]

[236] 개인 식별자 유형의 예시는 다음과 같다: 이름, 주소, 개인에 대한 날짜(생년월일, 보험 가입일, 보험 해지일, 사망일 등), 전화번호, 자동차 등록 번호, 팩스 번호, 기기 시리얼 번호 및 식별 정보, 이메일 주소, 온라인 접속 주소(URLs), 사회보장 번호(SSN), 인터넷 접속(IP) 주소, 의료 기록 숫자, 생물학적 지문 또는 성문), 건강보험 정보, 개인 식별 가능성이 있는 사 진, 계좌 정보, 재식별가능 정보로 제안된 정보, 인증/자격 정보, 그 밖에 인지 가능성이 있는 정보

[237]

[238] 한정데이터세트(Limited data sets, LDS)

[239] 한정데이터세트는 세이프하버 방식을 따른 비식별의료정보(De-identified Health Information, DHI)처럼 의료정보에서 식별자를 제거한 정보라는 점에서는 유사하나, 좀 더 완화된 기준이 적용되어 일부 날짜 정보(생년월일, 입원일, 퇴원일 등) 및 우편번호, 거주지(주, 시)정도의 정보를 포함할 수 있다.

[240] 연구자 등 정보 이용자에게 데이터 남용을 방지하고자 하는 내용을 담은 데이터 재식별 금지 합의서를 제출하게 하고, 특정 목적(연구, 공중 보건, 의료 서비스 제공)으로 정보를 활용하는 경우 환자의 동의가 없어도 IRB를 거친 뒤에 활용할 수 있다고 규정하고 있다. 즉, 정보 이용자에게 재식별 책임을 부과하고 그 대 신 정보의 가치 있는 활용을 좀 더 용이하게 한 유형이다.

[241]

[242] 데이터 내용에 대한 분류

[243] 개인의 식별가능성 외에도 데이터를 분류하는 기준은 구조화 가능 여부, 생성 주체 및 방식, 활용 목적, 대상물의 종류 등 다양하다. 하지만 본 발명의 다양한 실시 예들에서는 엄밀하게 구분되는 분류 기준을 적용하거나 모든 유형을 상세히 설명하는 것보다는 활용 가치 측면에서 중요한 의미를 가지는 대표적인 유형들을 선별하여 소개하고, 각각의 데이터가 활용되는 방식에 대한 이해를 돕는 것 무게 중심을 두고자 한다.

[244]

[245] 임상 데이터 (Clinical data)

[246] 가장 대표적인 헬스케어 데이터로, 병원 등 의료 기관이 진단, 투약, 검사, 수술 등을 진행하면서 생성되는 환자 정보를 포함하는 유형이다. 따라서 구조화된 검사 수치 데이터부터 자연어로 작성된 의무 기록, 의료 영상 및 이미지(X-ray, CT, MRI, 초음파, 내시경 등)까지 매우 다양한 세부 항목이 존재한다.

[247] 이러한 정보를 전자적으로 저장하면 EMR(Electronic Medical Record)이라 하고, 나아가 여러 곳에 저장되어 있는 한 개인의 의료 정보 총체를 EHR(Electronic Health Record)이라 한다. 임상 데이터는 대부분 생성 시점에는 보호의료정보(PHI)에 해당하며 법에 의해 의료 기관이 안전하게 보관할 의무와 책임을 가지고 환자 외에 다른 기관이 이 데이터에 접근하고 활용하는 것은 엄격히 금지되고 있다.

[248] 임상 데이터에서 파생되는 데이터로는 의료 기관에서 보험 기관에 비용 청구를 할 때 제출하는 정보를 기반으로 한 청구 데이터가 있다. 여기에는 환자의 개인 정보, 진단명, 투약 정보, 검사 정보 등이 포함된다. 한국의 경우 단일 보험 체제를 채택하고 있어, 건강보험심사평가원과 국민건강보험공단은 전국민의 데이터를 기반으로 공공 데이터를 구축하여 공개하고 있다(보건의료빅데이터 개방시스템, 국민건강보험자료 공유 서비스 등).

[249]

[250] 오믹스 데이터 (Omics data)

[251] 유전체(genome), 전사체(transcriptome), 단백질체(proteome), 대사체(metabolome), 마이크로바이옴 (microbiome) 등 생체 물질을 포괄하는 총체적인 개념의 데이터 세트를 말한다. 이 생체 물질은 개인마다 고유의 특성을 가지고 있어, 이에 대한 데이터를 대규모로 축적하고 분석할 경우 개인 맞춤형 의료가 가능해질 것으로 기대되고 있다.

[252] 유전체 데이터는 가장 대표적인 오믹스 데이터로, 마치 암호문처럼 알파벳 A,T,G,C를 조합하여 개인의 특성을 결정짓는 DNA에 기록된 유전 정보를 염기서열로 표현한 데이터를 말한다. 실제로 유전체 데이터를 분 석하는 것은 마치 암호문을 해독하는 것과 같은데, 특정 자리의 단일 혹은 복수의 염기가 무엇인지에 따라 개인간에 어떠한 차이를 만드는지 등을 분석해 내는 것이 주된 과제이다. 특히 희귀질환의 원인은 약 80% 이상이 유전자 변이이기 때문에 발병의 원인이 되는 유전자를 알아내기 위한 암호 해독이 중요하다.

[253] 최근에는 머신러닝과 빅데이터 분석 기술의 발전으로, 유전체 및 다양한 생체 물질 데이터를 임상 데이터와 함께 활용하여 복합적으로 분석할 수 있게 되었다. 이를 통해 질환을 조기에 진단하고, 치료 반응 예측과 측정에 사용되는 표지자 (바이오마커)를 발견하는 데 활용되고 있다.

[254]

[255] 사람 유래 건강 데이터 (Person-generated health data, PGHD)

[256] 외부 기관에 의존하지 않고 환자 또는 개인이 소지한 웨어러블 디바이스, 휴대폰 등의 다양한 센서로부터 생성되는 데이터 또는 소셜 서비스 등에 스스로 올린 포스팅이나 설문 등을 포함하는 데이터를 말한다. 이러한 데이터들은 병원에 방문하지 않고도 일상생활에서 상시로 수집될 수 있다는 특징이 있다.

[257] 사람 유래 건강 데이터는 질환과 다소 무관해 보일 수 있지만 임상 데이터 및 다른 데이터와 결합하면 질환과 관련된 새로운 발견이 이루어질 가능성이 있다. 실제로 최근 신약 임상시험에서도 실제임상자료(Real- world data, RWD)로써 PGHD를 적극 활용하는 시도들이 계속되는 추세이다.

[258]

[259] 건강의 사회적 결정 요인(Social Determinants of Health, SDOH)

[260] 건강의 사회적 결정 요인은 인구 통계 정보, 사회·정치적 요건, 기후·환경 등 태생적으로 결정되는 사회·경제적인 외부 요인 중 건강에 영향을 미치는 데이터를 말한다. SDOH 데이터를 실제로 활용하는 사례로는 Gravity Project가 있다. 이 프로젝트에서는 사회·경제적 요인 (교육, 직업, 가정, 소득, 사회 안전), 물리적 환경, 건강(흡연, 식습관, 알코올, 성생활), 보건의료(의료 기관 접근성)를 주요 요인으로 규정하고 건강에 미치는 영향을 분석하는 것을 목표로 하고 있다.

[261]

[262] 연구 데이터 (Research data)

[263] 의약학 및 생명과학 관련 실험실이나 제약사 및 병원에서 신약 등의 새로운 치료법을 개발할 때 생성되는 데이터에 해당한다. 대표적으로 임상시험 및 연구 결과로 나오는 데이터가 있다. 이미 생성되어 있는 임상 데이터나 오믹스 데이터 등도 연구 목적으로 재활용하거나 수집되는 경우 연구 데이터라고 할 수 있다.

[264] 연구 데이터는 연구 진행에 필요한 참가자를 충분히 확보하기 위해 다양한 기관과 협력하는 것이 필수적이다. 서로 다른 언어를 사용하는 사람들 사이의 의사소통이 쉽지 않듯, 서로 다른 기관이 동일한 데이터에 대해서 명칭이나 단위 등을 다르게 사용한다면 연구 과정에서 소통과 협력이 어려울 것이다. 따라서 연구 데이 터는 대체로 잘 구조화되어 있고 공동으로 연구를 수행하는 기관 간에는 통일된 규칙하에 수집된다. 서로 다른 병원 내의 데이터들을 대상으로 한 통합적 분석이나 다양한 연구를 통해 축적된 환자 데이터의 통합적 분석을 위해 공통 데이터 모델(Common data model, CDM)과 같은 표준화 노력도 지속되고 있다.

[265] 연구 데이터는 대체로 과학적으로 엄밀하고 체계적으로 수집될 수 있도록 설계되고 학계와 심사 기관에 의해 검증된다. 또한 연구를 실시하기 전에 데이터 수

집 대상과 수집 방법의 적법성, 적합성을 IRB 등 심의위원회에 의해 심사를 받기에 데이터의 품질이 높다는 점이 특징이다.

[266]

[267] 그 밖에도 개인의 결제 정보와 같이 그 자체로는 건강과 큰 관련은 없지만, 다른 헬스케어 데이터와 결합되어 분석되었을 때 유의미하게 활용될 수 있는 데이터가 있다. 예를 들어 개인의 정기적인 피트니스 센터 결제 내역이 있다고 할 때, 결제 정보는 그 자체로만 보면 건강과 관련이 없어 보일 수 있다. 하지만 어떤 건강 관련 수치가 개선되거나 악화될 경우, 이를 결제 정보와 연관시켜 분석함으로써 개인의 건강 지표의 변화를 예측해 볼 수 있다.

[268] 이와 같이 데이터는 다른 종류의 데이터와 결합되었을 때 더 가치가 높아질 수 있다. 따라서, 어떤 데이터를 일반적으로 알려진 헬스케어 데이터와 결합되었을 때 가치 있게 활용할 수 있을지 알아내는 것이 앞으로의 중요한 과제이다.

[269]

[270] 도 9는 본 발명의 다양한 실시 예들에 따른 데이터 활용과 보호의 적정한 균형의 일 예를 도시한다.

[271] 이처럼 데이터는 건강 수준을 향상시키고 질환 치료의 새로운 돌파구를 만들어내는 데 활용되고 있다. 하지만 지금까지 천문학적으로 투자된 금액과 빅데이터 활용 기술이 약속한 이상에 비해 실제 성과는 그에 못 미치는 것도 사실이다. 이에 대한 주요 이유는 1. 신뢰할 수 있고 2. 장기적으로 수집되고 3. 상호 연결된 데이터가 충분하지 않다는 것이다. 즉, AI나 빅데이터 기술보다도 그 밑바탕이 되는 데이터의 질과 양적인 문제를 해결하는 것이 의료 혁신의 핵심이다. 이하, 충분한 크기의, 질 높은 의료 데이터 확보를 위해 해결해야 하는 과제에는 무엇이 있는지 설명한다.

[272]

[273] 1. 데이터 보호와 활용의 균형

[274] 유형 1.

[275] 개인의 의료정보는 민감한 개인정보 중 하나로, 전 세계적으로 법에 의해 매우 엄격하게 보호될 수 있도록 규정되는 추세이다. 가장 흔한 보호 조치는 가명화 및 익명화이고, 이렇게 비식별화 조치가 취해진 데이터는 개인을 식별하는 것이 현실적으로 매우 어렵거나 불가능하여 개인정보 유출이나 남용에 의한 피해를 줄일 수 있게 된다. 안전하게 익명화 또는 가명화 되었다고 판단된 비식별화 된 데이터는 신약 및 새로운 치료법 개발 등을 위한 연구 등 일부 목적에 한해서 자유롭게 활용될 수 있다. 이와 같이 주요 국가들은 개인 식별의 위험을 최소화한 상태에서 데이터가 더 가치 있게 활용될 수 있는 법률을 제정하고 있다.

[276] 하지만 이러한 개인정보 보호 조치가 정보의 활용을 통한 가치 창출 측면에서 한계로 작용하는 것은 불가피하다. 데이터는 서로 결합되었을 때 더 풍부하게 분석될 수 있고 새로운 가치 창출이 용이해질 수 있다. 하지만 가명화 된 데이터는 데이터 값이 추상화 또는 범주화 된다. 예를 들면 33세는 30대로, 87kg은 80-90kg

나 90kg 로 표현되는 식이다. 이는 실제 수치와 차이가 있기 때문에, 데이터의 활용 목적에 따라 부적합할 수 있다. 또한 데이터를 결합하면 개별 데이터세트만으로는 할 수 없었던 일이 가능해지는 경우가 많은데, 데이터 익명화는 데이터 결합을 매우 어렵게 만든다.

[277] 따라서, 데이터 활용과 보호의 적정한 균형을 이루는 것이 중요하다.

[278]

[279] 2. 적절한 동의 확보 방법과 사후 통제권 제공

[280] 앞에서 설명한 바와 같이 현재 환자로부터 별도의 동의를 받지 않고도 활용할 수 있는 데이터는 그 활용 목적 이 연구, 통계 작성 등 일부 목적으로만 한정되어 있고, 활용되는 데이터 또한 그 품질이 훼손되는 문제가 있다. 이러한 문제없이 데이터를 최대한 있는 그대로 확보하려면 환자 등 정보 주체로부터 수집하려는 데이 터 항목과 활용 목적, 활용 조건에 대해 알리고 동의를 받아야만 한다.

[281] 유형 1. 동의 확보 과정의 문제

[282] 이렇게 동의를 얻는 것은 데이터를 활용하려는 기관 입장에서 적법성을 갖추기 위한 최소한의 요건이다. 그 때문에 기관 입장에서는 최대한 제약 없이 데이터를 활용할 수 있는 조건으로 환자의 동의를 받고자 할 것이다. 이는 반대로 말하면 정보 주체를 충분히 보호하지 못하는 방식으로 동의를 받게 될 수도 있다는 것이다. 실제로 EU(판례: 독일소비자단체연합 대 플래닛49 사건)와 한국의 사법 기관(판례: 경품 응모권 1mm 글씨 고지 사건)에서는 미리 선택된 체크박스를 통한 동의와 같은 수동적 동의나 정보 주체가 인식하기 어려운 방식으로 수집하는 동의는 유효한 동의가 아니라고 판단하고 있다.

[283] 그렇지만 그러한 '불충분한 동의'의 이유가 꼭 기관의 불순한 의도 때문만은 아닐 수 있다. 서비스 이용 약관 및 개인정보 보호 정책에 대한 고지 내용이 방대하고 어려운 용어들로 작성되어 대부분의 사람들이 그 내용을 이해하기 어렵다는 점 때문일 수도 있다. 또한 개인정보를 철저히 보호하고자 내용을 세분화하여 동의를 받는 형식 자체가 역설적으로 개인에게는 번거롭게 느껴질 수도 있고, 이 때문에 약관 등의 내용이 환자 본인에게 최선인지 확인하는 노력을 들이기보다 무신경하게 동의나 비동의를 해버릴 수도 있다. 이와 같이 기관이 개인정보를 보다 철저히 보호하려는 의도였다고 하더라도 결과적으로는 불충분한 동의가 될 수 있다.

[284] 한편, 환자 입장에서 데이터가 활용되었을 때 본인에게 어떤 이익이 있는지, 이 과정에서의 잠재적인 위험은 무엇이 있는지에 대한 이해의 정도도 동의 확보에 영향을 주는 요인이 될 수 있다. 즉, 데이터 활용으로 인한 개인적 이익이 크다고 기대될수록, 데이터의 리스크에 대한 이해 수준이 높을수록 충분한 동의를 받을 가능성이 커질 것이다.

[285] 따라서, 강요가 아니라 정보 주체의 판단 하에 동의를 얻는 것이 중요하다.

[286]

[287] 유형 2.

[288] 미국 보건복지부(HHS)는 2020년 1월 20일 커먼룰(Common Rule)을 개정하면서 충분한 고지를 전제로 한 포괄적 동의를 받으면, 식별 가능하고 연구 목적이 아닌 경우에도 추가 동의 없이 데이터를 이차적으로 활용하는 것을 허용하였다. 이는 특별한 위험 요소가 없다면 매번 환자로부터 동의를 받아야 하는 비용과 시간을 절약함으로써 연구의 효율과 데이터의 활용 가치를 높이는 순기능을 이끌어내기 위함이다. 또한 데이터를 수집한 이후에야 합리적인 사용 목적을 고민할 수 있는 경우가 많기 때문에 다소 포괄적인 목적으로 동의를 받아 데이터를 수집하는 것이 효율적일 수 있다.

[289] 하지만 이런 경우 환자에게 모든 데이터 활용 및 공개 이력에 대한 접근성과, 데이터 활용 동의를 철회할 수 있는 권리도 함께 제공하는 것이 중요하다. 혹은 일단 데이터부터 수집하되, 실제 활용이 이루어지는 시점에 환자가 더 세부적인 내용을 확인하고 활용에 대한 동의를 하거나(Opt-in), 동의를 한 이후에도 언제든지 철회 (Opt-out) 할 수 있는 동적 동의(Dynamic-consent) 시스템을 제공하는 방법도 있다.

[290] 이와 같이 사전에 충분한 동의를 받고 사후에도 데이터를 통제할 수 있는 권한을 보장하는 것은 개인정보를 보호하면서도 데이터 활용으로 가치를 창출할 수 있도록 하는 매우 중요한 요소이다. 이를 실현할 경우 정 보의 투명성과 시스템의 신뢰 측면에서 긍정적인 경험을 제공할 수 있을 것이고, 이는 점차 당연한 기대치로 작용하여 법적 측면을 떠나 기관 입장에서도 환자와 사용자 확보를 위해 필수적으로 고려해야 할 요인으로 작용할 것이다. 따라서 환자, 데이터를 활용하려는 기관, 환자 대신 데이터를 관리해 주는 기관 모두의 입장에서 충분한 동의 기반의 데이터 관리와 활용을 가능케 하는 솔루션이 필요하다.

[291]

[292] 3. 데이터 공유에 인센티브 부족

[293] 주요 국가들은 환자의 데이터 자기결정권 실현을 통해 개인정보 보호와 데이터 활용의 균형을 이루기 위하여 관련 법을 제정하고 있다. 그 대표적인 사례가 미국의 21세기 치료법(21st Century Cures Act)이다. 이 법에서는 의료 기관에 저장된 환자의 의료정보가 상호 호환되도록 하고 환자가 원하는 애플리케이션에서 의료정보에 접근, 교류, 활용할 수 있도록 하고 있다. 이를 준수하지 않을 경우 건당 백만 달러 이하의 벌금이 부과된다.

[294] 하지만 여전히 많은 의료 기관은 전자적으로 읽고 활용하기 어려운 형태로 데이터를 공유하고 있다. 그 외 기업이나 연구자에게는 환자에게 동의를 받더라도 데이터를 공유할 수 없도록 법적으로 제한되어 있거나 그러한 법이 적용되지 않는 국가라 할지라도 데이터 보호를 이유로 데이터 제공을 꺼리는 것은 전 세계 공통 적인 현상이다.

[295] 한국의 경우도 보건복지부에서 의료 분야의 마이데이터 법제화와 시범 서비스인 마이헬스웨이를 추진 중인데, 최근 보도된 바에 따르면 환자의 정보 전송 요구에 대해 의료 기관의 참여를 강제하지 않고 개인과 환자에 대한 서비스 질 향

상을 목표로 자발적 참여를 유도하겠다고 한 바 있다. 또한 의료 기관 외에 민간 기업은 2024년 이후에 참여가 가능하도록 하여 엄밀한 의미의 데이터 자기결정권 실현과는 아직 거리가 먼 상황이다.

[296] 이처럼 법적인 의무나 처벌에 의해 데이터 자기결정권을 실현하는 것은 한계가 있다. 더 이상적인 것은 생태계 내 이해관계자들의 자발적인 동기에 의해서 데이터 자기결정권이 실현되는 것이다. 하지만 미국 국립 의학 아카데미의 조사 결과에 따르면 의료 기관 경영진들은 데이터 공유에 대한 경제적인 동인은 부족한 반면 데이터를 외부에 공유함으로써 경쟁력을 잃게 되는 것에 대해 우려하고 있다고 응답했다. 실제로 데이터 구조화 및 표준화, 품질 관리, 데이터 보관 등 데이터 공유를 위한 조치들은 주로 데이터를 생성하는 의료 기관의 비용과 전문성이 수반되는 일들인 반면 그 이득은 오히려 데이터를 활용하는 기관이 보게 될 가능성이 높다. 이와 같은 인센티브 불균형으로 인해 데이터 생성 기관의 자발적인 동참이 쉽지 않은 상황이다.

[297]

[298] 데이터 공유를 위해 필요한 조치들

[299] (1) 데이터 구조화 및 표준화

[300] 임상 데이터의 경우 비정형 텍스트 형식에 사용하는 용어도 일관되지 않은 경우가 많은데 이를 컴퓨터가 읽고 이해할 수 있도록 구조화하는 작업

[301] 데이터 공유를 통해 여러 사람이 협력하기 용이하도록 데이터 종류, 용어, 형식의 표준화를 위한 추가 작업

[302] 중복 데이터의 존재 여부 확인 및 결합 가능한 데이터의 발견을 위한 검색 메타데이터 추가 작업

[303] (2) 품질 관리

[304] 여러 질환을 동시에 가진 환자가 보험 청구에 필요한 진단명만 넣은 것, 수기 작성 과정에서 의도치 않게 정보가 누락되거나 잘못된 정보가 입력된 사항들 검수 및 정정

[305] 측정 장비의 정확도 문제, 장비 사용의 숙련도에 따라 결과가 일관되지 않은 문제 해결 노력

[306] (3) 데이터 보관

[307] 1인당 최대 200GB 정도에 이르는 유전체 데이터 보관 및 관리

[308] 재분석이 용이하면서도 적은 용량으로 데이터를 보관, 관리, 전송하는 기술

[309]

[310] 4. 데이터 권리에 대한 이해와 신뢰할 수 있는 기록의 부재

[311] 인센티브와 함께 고려해야 하는 점은 데이터에 대한 권리의 공감대 형성이다. 데이터의 자기결정권이 정보 주체인 환자에게 있어야 한다는 사실에는 큰 이견이 없다. 하지만 인센티브와 밀접하게 연관된 개념 인 소유권은 그리 단순하지 않다. 소유권이라는 개념은 일반적으로 부동산이나 물건 같은 유형물의 재화 에만 적용되는 개념이다. 무형물에 배타적 권리를 부여하는 개념으로는 저작권, 특

허와 같은 지적 재산권이 있으나 이 권리는 창작의 노력이 들어가야 인정된다. 따라서, 정보나 데이터 그 자체가 아닌 편집의 노력이 들어간 데이터베이스의 경우에만 배타적 권리인 저작권이 인정되고 있다.

[312] 환자의 의료 데이터가 생성되기까지는 수많은 노력이 필요하다. 일차적으로 의료 전문가와 의료 기관의 장비를 통해 측정되는 단순 데이터 그 자체뿐만 아니라, 진단명이나 양성·음성 여부와 같이 전문성에 기초한 판단이나 해석에 의해 생성되는 데이터도 많다. 또한 데이터가 공유되어 의미 있게 활용되려면 앞에서 언급한 조치들을 취해야 한다. 경우에 따라서는 서로 다른 데이터를 결합하는 노력도 추가로 필요하다. 이 모든 과정을 통해 만들어진 데이터세트는 적지 않은 비용과 의료 전문가의 상당한 전문성을 통해 편집된 결과이다.

[313] 또한 의료 데이터는 의료보험 제도나 공공 재원이 투입되어 만들어진 의료 시스템에 의해 뒷받침되어 공공성을 지니고 있다는 점도 간과할 수 없다. 따라서 특정 주체에게 배타적인 수익권과 사용권을 보장하는 것 보다는, 비경합성, 즉 한 주체가 소비한다고 해서 다른 주체가 소비할 기회가 줄어들지 않는 특성을 보장하는 것이 정보 주체 당사자뿐만 아니라 공공에 더 이익이 되고 데이터를 더 활발하게 활용할 수 있다.

[314] 이러한 소유권, 데이터 공유와 활용에 대한 이력들이 신뢰할 수 있는 방식으로 기록되고, 이 기록에 모든 이해 관계자가 자유롭게 접근하고 활용할 수 있는 방법이 아직은 부재한 상황이다.

[315]

[316] 도 10은 본 발명의 다양한 실시 예들에 따른 신원 인증(ION), 소액 송수신 및 결제(Lightning Network), 자산 발행(Taro) 및 더 다양한 스마트 컨트랙트 (BIP-119, Liquid Network, RGB 등) 등 Bitcoin의 탈중앙성과 보안성 위에서 확장성을 실현하는 기술의 일 예를 도시한다.

[317] 앞서 신약 개발 등 보건과 의료의 발전을 위해 필요한 헬스케어 데이터는 어떤 것이 있는지 설명하였다. 좋은 품질의 데이터를 충분히 확보하기 위해서는 개인정보의 보호와 활용의 균형, 충분한 동의 확보, 데이터 공유를 위한 인센티브, 데이터 권리에 대한 이해와 신뢰할 수 있는 기록 등과 같은 과제를 해결해야 한다.

[318] 본 발명의 다양한 실시 예들은 상술한 과제들을 해결하기 위해 개방형 표준과 Bitcoin 레이어 위에서 환자의 데이터 자기결정권과 탈중앙 거버넌스, 그리고 지속 가능한 인센티브 모델을 통해 헬스케어 데이터를 위한 협력 프로토콜을 제안한다. 이하, 이러한 목표를 실현하기 위한 방법에 대하여 설명한다.

[319]

[320] 환자의 데이터 자기주권 실현

[321] 현재까지 많은 인터넷 기업의 비즈니스 모델은 기업 내부 서버에 축적된 사용자들의 데이터를 활용하여 더 좋은 광고 알고리즘을 개발하고 수익성 높은 광고 상품을 만드는 것이라 할 수 있다. 이러한 비즈니스 모델 은 사용자가 편리하고

저렴하게 서비스를 사용할 수 있게 했지만 그 반대급부로 사용자는 자신의 정보와 데이터에 대한 주권을 상당 부분 포기해야 했다.

[322] 비영리 글로벌조직 마이데이터 글로벌(mydata.org)은 이러한 문제의식에 대한 해답으로 '마이데이터'라는 이름의 개념을 제안하고 다음과 같이 정의하였다. 이는 신원의 영역으로 확장되어 개인 신원과 데이터에 대한 주권을 가지고 인터넷을 사용할 수 있게 하는 자기주권신원(Self soverign identity, SSI)이라는 기술 분야의 탄생 배경이 되었다.

[323] (1) 개인 데이터의 관리 및 처리에 있어 현재 조직 중심적 체계(organization-centric system)를 사람 중심적 체계(human-centric system)로 바꾸고자 하는 새로운 실천적 운동

[324] (2) 개인이 접근하고 통솔할 수 있는 자원으로서의 개인데이터

[325] 본 발명의 다양한 실시 예들은 마이데이터 및 자기주권신원과 동일한 철학을 공유하며 이를 헬스케어 분야에서 실현하는 것에 집중한다. 특히 헬스케어 분야에서 개인을 충분히 보호하면서도 데이터의 합리적인 활용이 가능하 게 하기 위해서는 정보 주체에 의한 결정이 꼭 필요하다. 이것이 실현된다면 인터넷과 디지털 기술의 혁신이 헬스케어 분야에서도 비로소 가속화될 수 있다.

[326]

[327] 인센티브와 개방형 협력으로 데이터 생태계

[328] 헬스케어 데이터의 생성에서부터 부가가치가 더해지고 활용되기까지는 환자와 같은 정보 주체뿐만 아니라 의료 기관, 공공 기관, 기업 등 다양한 이해관계자의 협력이 수반된다. 이 모든 과정에서는 부가가치를 생산하기 위한 비용이 투입된다. 따라서 각 이해관계자의 동기를 충족시킬 수 있는 적절한 인센티브(금전적 보상 혹은 부가가치가 더해진 서비스 등)가 없다면 이 협력은 지속될 수 없을 것이다.

[329] 본 발명의 다양한 실시 예들은 정보 주체의 자기결정권에 의해 데이터가 거래 및 활용되도록 하고, 이 과정에서 금전적 보상이 발생할 경우 정보 주체를 포함하여 데이터의 생성과 가공 과정에 기여한 이해관계자에게도 보상이 배분되는 프로토콜을 제공한다. 또한 데이터의 생성부터 활용까지 유통 과정의 모든 정보는 투명하고 위·변조 위험 없이 블록체인에 기록되므로 제3자의 신뢰에 의존하지 않고도 충분히 협력할 수 있는 환경이 마련된다.

[330] 이러한 프로토콜도 특정 중앙화된 주체에 의해 결정되는 것이 아니라 개방형 협력 체계에 의해 결정된다. 사용자들이 사용하는 도구와 서비스는 개방형 표준과 오픈소스로 개발되고, 정책과 표준은 공개적인 토론과 거버넌스 참여 구성원들의 투표로 결정된다. 이러한 방식을 통해 인류의 건강 증진을 위한 글로벌 단위의 협력을 가능케 할 수 있다.

[331]

[332] 도 11은 본 발명의 다양한 실시 예들에 따른 API 모델과 데이터 상호호환성에 대한 인센티브의 일 예를 도시한다.

[333] 해시: 데이터의 무결성 보장

[334] 사람들이 블록체인에 의료 데이터 그 자체를 기록하는 것으로 오해를 하는 경우가 많다. 블록체인은 위의 설명과 같이 동일한 내용의 복사본을 끊임없이 유지하는 데 비용이 들기 때문에 필연적으로 많은 데이터를 담을 수 없다. 따라서 블록체인은 자산이나 신원과 같이 정말 중요한 데이터에 대해 신뢰할 수 있는 저장소가 꼭 필요한 최소한의 정보를 담는 목적으로 사용되어야 적합하다.

[335] 이는 부동산 등기부에 남겨지는 기록을 생각해 보면 이해가 쉽다. 부동산 등기부에서는 부동산의 소유권을 명확히 판단하기 위한 현재와 과거의 기록을 확인할 수 있다. 우리는 실제 부동산을 주고받지 않고도 등기부의 기록만을 변경함으로써 실질적인 소유권도 변경할 수 있다. 본 발명의 다양한 실시 예들도 의료 데이터의 정보 주체, 담고 있는 의료 정보의 내용, 생성 주체, 데이터의 실제 위치, 공유 대상 등의 유통 이력을 기록하는 데 블록 체인을 사용한다.

[336] 그렇다면 실제 데이터의 내용 자체가 블록체인에 올라가는 것은 아니므로 블록체인이 데이터 내용을 위·변조하는 것은 막지 못할 것이라고 생각하실 수도 있다. 여기서 '해시 함수'라는 암호 기술이 필요하다. 해시 함수는 입력하는 데이터에 아주 사소한 변화만 발생하더라도 그 결과값(해시값)이 전혀 달라진다는 특징이 있다. 예를 들어, 원본 파일을 입력했을 때 57이 나와서 이를 블록체인에 기록해 두었는데, 내가 받은 데이터의 해시값이 블록체인에 기록된 해시값과 다르게 58이라면 원본 파일이 위·변조되었다고 확신할 수 있다. 원본 데이터에서 글자 하나만 바뀌어도, 공백 하나만 추가되어도 전혀 다른 해시값이 나온다. 이러한 방법을 통해서 블록체인에 실제 데이터를 기록하지 않고도 원본 데이터의 위·변조 여부를 확인하고 거래를 할 수 있다.

[337] [표2]

입력 데이터	해시값 (SHA-256 해시 함수 사용)
Hippocrat	174ae7c5faf856241800d4156a303d97252b1a015c141b4022b9e0b87712f9f5
Hippocrat	ec4a395e1d365143981a6f2474971f94f033e3eac1f4c7777833668f350abf3a
Hippo crat	30583e5b90579f8eb47ab12aa5bd3753bfbd73d18c4512ef9525e4beef5869f4
Hippocrat1	b8fa3200c96fa507857bf7850b8e32e73ecd253ba3c69b22ea57af410d98c618

[338] 자기주권신원과 마이데이터자기주권신원(Self Sovereign Identity, SSI)은 인터넷에서 개인의 신원을 나타내기 위해 제안된 새로운 모델이며 이를 실현하기 위한 기술인 탈중앙화신원증명(Decentralized Identifier, DID)과 검증가능한 자격증

명 (Verifiable Credentials, VC)은 2022년 7월, W3C에 의해 웹 표준으로 채택되었다.

[339] 자기주권신원 기술은 개인이 어떤 기업을 믿고(혹은 서비스를 사용하기 위해 어쩔 수 없이 약관에 동의하고) 자신의 정보를 위탁하여 대신 관리하도록 하는 것이 아니라, 정보 주체가 자신의 정보 통제권을 완전히 유지하는 상태에서 기업이 정보 주체에게 정보 접근과 이용에 대한 동의를 구하도록 한다.

[340] 그러면 꼭 필요한 정보만 정보 주체가 주도적으로 공유하고 그 활용을 통제하는 식으로 패러다임을 바꿀 수 있다. 또한 이전에는 해커가 중앙화된 서버를 한 번만 해킹하면 수십에서 수백만에 이르는 개인 정보를 탈취할 수 있었지만, 이제는 한 번에 한 명에 대해서만 공격이 가능하므로 해킹 동기를 떨어뜨리며 결과적으로 개인 정보가 더욱 효과적으로 보호되는 환경을 만들 수 있다.

[341] Hippocrat은 자기주권신원 기술을 기반으로 정보 주체가 개인의 신원 정보뿐만 아니라 의료 데이터까지 포함하여 자기결정권을 행사할 수 있는 마이데이터 개념을 실현할 수 있다.

[342] 마이데이터 모델은 지나치게 복잡도가 높아지는 API 모델과 데이터 상호호환성에 대한 인센티브가 없는 플랫폼 모델의 문제를 해결할 수 있다

[343]

[344] DID: 자기주권신원을 위한 식별자

[345] 지금까지 인터넷상에서 우리의 신원은 특정 기업이 제공하는 서비스 서버 내 계정의 형태로만 식별할 수 있었다. 그 때문에 새로운 서비스에 가입할 때마다 새로운 계정을 만들어야 하고, 본인 인증이 필요한 경우 서비스마다 매번 같은 과정을 반복해야 하는 불편함이 있었다. 그래서 구글이나 페이스북 같은 대규모 서비스의 계정으로 로그인하는 방법이 널리 채택됐지만, 이는 하나의 서버에 개인정보가 과중하게 몰리는 결과로 이어져 해킹 시의 리스크를 심화시켰다. 또한 특정 서비스에 대한 의존도가 높아질수록, 해당 기업의 정책에 위배된다고 '판단'되었을 때 계정이 언제든지 정지되거나 제한될 위협에서 취약해진다. 이는 최근 미국의 간편 결제 서비스 Paypal이 자사 정책에 부합하지 않는 사용자의 계정에 2,500달러를 '벌금'으로 부과할 수 있다는 정책을 시도한 사례에서 단적으로 드러난다.

[346] DID는 이러한 문제에 대한 솔루션을 제공한다. DID는 제3자의 도움 없이 수학과 암호학을 기반으로 생성하 여 인터넷 어디서든 자유롭게 사용할 수 있는 자신만의 고유한 ID(신원 식별자)이다. 이는 우주에 존재하는 모든 원자에 고유 번호를 부여하고 그중 하나를 무작위로 선택하여 해당 고유 번호로부터 생성된 아이디와 이를 통제할 수 있는 암호(개인 키)를 할당 받는 것과 같다. 그리고 개인 계정과 그 계정에 연결된 개인 정보는 블록체인에 기록되는데, 이를 조회하고 통제할 수 있는 권한은 개인 키를 소유한 사용자에게만 주어진다. 이를 통해 우리는 정부나 기업의 도움이나 통제에서 벗어나 자유롭게 나의 신원을 생성하고 관리할 수 있다. 이 방법은 특히 높은 수준의 개인정보 보호를 요구하는 의료 분야에

서 탁월하게 쓰일 수 있으며, 신원에 대한 기록과 그 통제 권한 역시 블록체인에 연결된 모든 컴퓨터와 인터넷이 사라지지 않는 한 안전하게 지킬 수 있으므로 본 발명의 다양한 실시 예들에 필요한 자기주권신원을 실현할 수 있다.

[347] DID는 어떤 블록체인에 기록되느냐에 따라 여러 종류가 존재하는데, 본 발명의 다양한 실시 예들은 Bitcoin을 기반으로 하는 ION을 사용한다. ION은 Microsoft와 Block이 주요 지원자인 오픈소스 DID 프로토콜로, 하나의 Bitcoin상 기록에 1만개의 DID 기록을 담을 수 있다. 이러한 특징은 Bitcoin의 견고한 탈중앙성과 보안 위에 충분한 확장성이 필요한 본 발명의 다양한 실시 예들에 적합하다.

[348]

[349] VC(검증가능한 자격증명): 나를 증명하는 모든 것

[350] 출생증명서, 대학 졸업장, 여권, 운전면허증, 사원증, 피트니스 센터 이용권, 병원 등록 카드, 처방전 등은 나에 대한 특정 사실을 설명하고 증명한다. 예를 들어 약국에 가서 처방전을 제시하면, 내가 어떤 질병으로 인해 어떤 약을 어느 병원의 어느 의사에 의해 처방받았는지 설명하고 증명할 수 있다. 이를 통해 약사는 이 처방이 적절하다는 것을 신뢰하고 약을 제조할 수 있다. 그리고 약국으로부터 받은 약제비 영수증을 통해 실제로 처방받은 약을 받았음을 증명할 수 있다. 이러한 서류를 모아 보험사에 제출하면 증명된 기록을 바탕으로 보험금을 받을 수 있다.

[351] 검증가능한 자격증명(Verifiable Credential, VC)은 이렇게 나에 대한 특정 사실을 설명하고 증명하는 구체적인 정보들을 말한다. VC에 담기는 정보는 발급자(발급자의 DID), 자격증명의 주체(정보 주체의 DID), 그리고 증명하고자 하는 주장(나이, 관계, 진단명 등), 이 자격증명을 보관하는 보유자(보유자의 DID. 보통은 정보 주체와 보유자가 동일하나 미성년자 자녀가 정보 주체인 경우 보호자가 보유자일 수 있다)로 구성된다. 그리고 이 정보들은 모두 누가 발급했는지, 조작되지는 않았는지, 만료되거나 해지되지는 않았는지 등을 검증할 수 있다.

[352] 처음 예시에서 언급한 전통적인 물리적 자격증명은 모두 위조의 가능성이 있으며, 인터넷으로 검증하기 어려운 내용이 많았다. 이를 해결하고자 서명이나 홀로그램 같은 증명 장치나 검증 기관이 별도로 존재했지만, 개인정보 보호 측면에서 불완전하였고, 글로벌 단위로 인터넷상에서 사용하기에는 비용이나 기술 면에서 한계가 많았다. VC는 누구나 투명하게 검증할 수 있는 블록체인상에 발급되어 인터넷상에서 훨씬 빠른 속도로 검증이 가능하며 비용도 크게 절감된다. 이러한 가능성을 바탕으로 DID와 VC는 미국 국토안보부 (US Department of Homeland Security) 등으로부터 자금을 지원받아 개발되었고 2022년 7월에 개방형 글로 벌 표준으로 채택되었다.

[353]

[354] 본 발명의 다양한 실시 예들이 제시하는 협력적인 헬스케어 데이터 생태계를 실현하는 데에도 VC는 필수적인 요소이다. 어떤 환자에 대한 데이터를 중개인

없이도 검증할 수 있다면 데이터의 유통과 활용 과정에서 발생하는 마찰이 최소화되어 더 활발한 생태계가 만들어질 수 있다.

[355]

[356] 안전한 헬스케어 데이터 교환

[357] 앞서 설명했듯이 블록체인은 자산이나 신원에 대한 등기부처럼 중요성이 높고 신뢰할 수 있는 저장소가 반드시 필요한 최소한의 정보를 담는 목적으로 사용되어야 적합하다. 그런데 의료 데이터의 일부는 신원정보로서 VC 형태로 블록체인상에 기록될 수도 있지만, 수백 GB의 유전체 데이터에서 수 TB에 달할 수 있는 PGHD(참고)의 경우 블록체인에 저장하는 것은 현실적이지 않으며 그만큼 많은 복사본이 꼭 필요한 것은 아니다.

[358] 본 발명의 다양한 실시 예들은 DIDComm 표준에 따라 ECDH(Elliptic Curve Diffie-Helman) 기반 다중 서명 기술을 활용하는 데이터 암호화 전달을 위한 표준 프레임워크인 ECIES(Elliptic Curve Integrated Encryption Scheme)을 통해 데이터를 주고받을 수 있게 한다. 이러한 기술을 이용하면 중개자의 서버를 별도로 거치지 않고, 데이터 교환을 위해 명시적으로 연결된 두 당사자 외에는 데이터를 열어볼 수 없도록 데이터가 안전하게 암호화·복호화되어 교환된다. 이것이 의미하는 바는 환자가 다른 기관에 의존하지 않고도 대용량의 데이터를 의료 기관 및 데이터 활용 기관과 직접 안전하게 교환할 수 있고, 개인정보 유출 위험 없이 데이터의 유통 경로가 매우 효율적으로 개선될 수 있다는 것이다. 이에 적절한 인센티브 장치를 결합하면 데이터 거래가 가능해진다.

[359] 이외에도 파일을 분산하여 저장하고 공유하기 위한 프로토콜인 IPFS(InterPlanetary File System)를 활용하는 방법도 고려할 수 있다. 어떤 파일이 IPFS 네트워크에 올라오면 여러 노드에 분산되어 저장되며, 분산된 파일을 연결하는 역할을 하는 고유 식별자 CID(Content IDentifier)가 파일의 해시값으로부터 만들어진다. 환자에 대한 특정 대용량 데이터세트를 환자의 공개 키로 암호화하여 IPFS에 올리고 그 CID를 VC에 담아 발급하면, 이후 환자가 그 데이터를 다른 기관에 공유할 때 그 기관은 CID가 변경되지 않았는지를 확인함으로써 원본과 동일한 파일임을 확신할 수 있다.

[360] 상기에 설명한 방법 외에도 안전한 데이터 교환은 다양한 방식으로 구현될 수 있으며, 본 발명의 다양한 실시 예들이 채택할 방식은 이에 한정되지 않는다. 본 발명의 다양한 실시 예들은 상술한 예시 외에도 다양한 솔루션에 적용할 수 있음은 물론이다.

[361]

[362] 도 12는 본 발명의 다양한 실시 예들에 따른 QR코드 인식만으로 간편하게 로그인, 인증, 자산 및 데이터 송수신하는 과정의 일 예를 도시한다.

[363] 데이터 지갑: 데이터

[364] 본 발명의 다양한 실시 예들에 따른 데이터 지갑은 정보 주체가 자신의 신원과 기관으로부터 받은 데이터, 그리고 데이터 공유 보상 등으로 획 득한 자산을 관

리하는 데이터 지갑이다. 데이터 지갑에서 개인의 데이터를 보관하는 방식은 원본 데이터 자체를 보관하는 것이 아니라 그 데이터에 접근할 수 있는 카드키나 영수증을 보관하는 것과 유사하다. 마치 지갑에 현금이나 신용 카드뿐만 아니라 신분증, 멤버십 카드, 티켓, 헌혈증, 카드키, 영수증 등을 보관했다가 필요할 때마다 꺼내 쓰는 것과 같다. 지갑을 분실하면 그 안에 있는 것도 함께 잃어버리듯 지갑은 지갑 소유자에게 온전한 통제권이 있으며, 바꿔 말하면 온전한 책임 또한 지갑 소유자에게 있다. 데이터 지갑도 마찬가지이다.

[365] 이하, 본 발명의 다양한 실시 예들에 따른 데이터 지갑에서 제공하는 핵심 기능을 설명한다. 핵심 기능 대부분은 개방형 표준과 오픈소스를 기반으로 구현되는데 이는 바퀴를 새로 발명하는 대신, 이미 충분히 검증된 기술을 기반으로 본 발명의 다양한 실시 예들이 해결하려는 문제에 초점을 둔 부가가치를 더하는 데 집중하기 위함이다. 이러한 방식은 새로운 소프트웨어에서 발생할 수 있는 의도적/비의도적 결함을 최소화하면서도 개방형 표준에서 지속되는 개선과 혁신을 그대로 누릴 수 있다는 장점이 있다. 더불어 최종 구현된 데이터 지갑 애플리케이션도 오픈소스로 공개될 예정인데, 이는 본 발명의 다양한 실시 예들에 따른 데이터 지갑에서 새로 작성한 코드를 누구나 투명하게 검증할 수 있게 해 신뢰성을 제공하고, 이를 기반으로 새로운 개선과 혁신을 쌓아 올리는 가능성을 차단하지 않기 위함이다. 또한 이러한 방식은 본 발명의 다양한 실시 예들에 따른 데이터 지갑에 담은 자산과 데이터를 사용자가 선호하는 다른 데이터 지갑 애플리케이션을 통해 접근하는 것을 허용한다.

[366]

[367] 개인 키 생성 및 관리

[368] 본 발명의 다양한 실시 예들에 따른 데이터 지갑의 가장 기본적인 기능은 자신의 자산과 데이터 그리고, 신원 식별자 DID에 접근하고 관리하는 데 필요한 개인 키를 안전하게 생성하고 보관하는 것이다. 본 발명의 다양한 실시 예들에 따른 데이터 지갑은 BIP39 표준을 따르므로 Bitcoin 지갑 대부분의 개인 키, 그리고 이를 복구하기 위한 니모닉 코드(Mnemonic code) 생성 방식과 그 보안성이 동일하다. 따라서 본 발명의 다양한 실시 예들에 따른 데이터 지갑은 Bitcoin 지갑 기능을 기본적으로 제공한다. 개인 키 보관의 추가적인 보안을 위해 기기의 TEE(Trusted execution environment) 등을 활용할 수도 있다.

[369]

[370] 연결, 인증, 로그인

[371] 자신의 DID가 생성되면 이를 통해 중개자 없이 데이터에 접근하는 기관과 P2P로 연결할 수 있다. 이 사이에 오가는 모든 데이터와 메시지는 종단 간 암호화되어 당사자 외에는 그 내용을 볼 수 없다. 이러한 방식을 이용하면 통신 과정에서 발생하는 개인정보 노출 위험을 최소화할 수 있다.

[372] 최초 연결은 보통 기관의 애플리케이션이나 웹 사이트에서 연결을 위한 QR코드를 스캔하거나 버튼을 누른 후, 사용자가 연결하려는 대상에 대한 정보와 요청

권한 및 데이터 등을 확인한 후 승인하는 방식으로 이뤄진다. 이렇게 한 번만 연결하면 어느 한쪽에서 종료하지 않는 이상 신뢰 관계로 기억되어 연결이 유지된다.

[373] 헬스케어 상황을 생각해 보면 일반적으로 병원은 최초 방문 시 신규 환자로 등록해야 한다. 이때 환자는 등록 버튼을 누르고 본인 데이터 지갑으로 QR코드를 스캔하면 본인임을 확인할 수 있는 이름, 주민등록번호, 사진, 성별 등 법정 신원에 대한 공유 요청을 받는다. 환자가 이를 승인하면 병원 측 담당자가 환자의 데이터 지갑으로부터 환자 본인임을 확인한 후 환자 등록이 이뤄진다.

[374] 이러한 방식은 로그인이나 다른 인증 수단을 대체하기 때문에 사용자가 연결하려는 서비스마다 아이디와 암 호를 생성하고 기억해야 하는 불편함을 해소한다. 또한 QR코드 인식만으로 간편하게 로그인, 인증, 자산 및 데이터 송수신 등을 할 수 있다. 그 뿐만 아니라 데이터 지갑 애플리케이션 자체에 PIN, 생체인식 등 추가적인 보안 수단을 개인 키와 조합하면 사실상 멀티팩터 인증(Multi-factor Authentication, MFA)으로서 일반적인 로그인 방식보다 훨씬 높은 수준의 보안성을 갖출 수 있다.

[375] 도 12를 참조하면, 본 발명의 다양한 실시 예들에 따른 데이터 지갑을 통해, QR코드 인식만으로 간편하게 로그인, 인증, 자산 및 데이터 송수신을 할 수 있다.

[376]

[377] 도 13은 본 발명의 다양한 실시 예들에 따른 선택적 데이터 공유의 일 예를 도시한다.

[378] 데이터(VC) 관리

[379] 데이터 지갑을 통해 병원과 같은 상대방과 연결된 상태에서는 사용자가 요청할 때마다 혹은 상대방이 필요하다고 판단할 때마다 각종 증명서 혹은 데이터를 사용자에게 전송할 수 있다. 본 발명의 다양한 실시 예들에 따른 데이터 지갑에서 주로 전송하는 대상은 검증가능한 자격증명(Verifiable Credential, VC) 형태로 발급되는 데이터이다.

[380] 전형적인 시나리오로는 병원에서 의무기록과 같은 데이터를 발급할 때 환자 본인임을 확인하는 인증 절차를 거친 뒤, 환자의 데이터 지갑 DID에 VC 형태로 발급하는 것이다. 그러면 데이터 지갑에 데이터가 발급되었으며 이를 승인하겠냐는 알림과 메시지가 도착하고, 승인 후에는 데이터를 확인할 수 있게 된다. 일반적인 클라우드 스토리지와 달리, 데이터는 모두 사용자의 암호키에 의해 암호화되어 저장된다.

[381] 이렇게 발급된 데이터는 필요한 곳에 제시할 수 있다. 예를 들어 데이터를 활용한 건강 관리 서비스를 이용하려면 환자에게 서비스를 제공하기 위해 특정 데이터에 접근이 필요하다며, QR코드 스캔을 요청한다. 환자가 QR코드를 스캔하면 어떤 데이터를 활용하는지 서비스 제공자에 대한 상세 정보와 이용 조건 등을 확인할 수 있고, 이를 승인하면 서비스 제공자에게 데이터를 공유한다. 그러면 서비스 제공자는 해당 데이터의 해시가 발급자가 제공한 데이터의 해시와 동일한

지, 발급자는 신뢰할 수 있는 기관인지 등을 검증한다. 검증을 마치면 환자에게 필요한 서비스가 제공된다. 다소 복잡해 보이지만, 이 모든 과정은 자동화된 소프트웨어가 빠른 속도로 처리하기 때문에 환자는 일반적인 간편 인증 과정처럼 느낄 것이다.

[382] 경우에 따라 데이터 전체를 공유하지 않고 원하는 데이터만 선택해서 공유할 수 있다. 심지어 개인정보가 노출될 수 있는 데이터를 상대방에게 공유하지 않고도 목적을 달성할 수 있다. 본인이 자녀의 법정 대리인(보호자)임을 증명해야 하는 상황을 예로 들어볼 수 있다. 우선 본인 데이터 지갑에 자녀에 대한 정보와 자녀와의 관계가 담긴 정보가 보관되어 있어야 한다. 병원 담당자는 본인에게 자녀의 보호자가 맞는지 확인하 고자 QR코드를 스캔해 달라고 요청할 것이다. QR코드를 스캔하고 승인하면 시스템은 이름, 생년월일, 성별, 주소 등 개인정보는 노출하지 않은 채 해당 환자의 보호자로 등록되어 있는지 여부만 확인하고 맞다 틀리다 결과만 알려준다. 이러한 방법을 영지식 증명(Zero-knowledge proof)이라고 한다. 병원 담당자는 개인정보가 아니라 실제 보호자인지만 확인하면 되기 때문에 목적을 달성할 수 있다.

[383]

[384] 도 14는 본 발명의 다양한 실시 예들에 따른 데이터 지갑과 연동하여 데이터를 활용한 부가 서비스의 일 예를 도시한다.

[385] 동의(서명) 관리

[386] 동의 자체는 기존 방식도 큰 문제가 없다. 이미 위의 인증, 로그인, 데이터 관리에서 사용자가 동의 버튼을 누르면 되는 것으로 설명했고, 이는 기존 방식과 비슷하다.

[387] 차이점은 데이터 지갑에서는 이미 동의한 내역을 한 번에 확인할 수 있고, 더 이상 상대방에게 권한을 주고 싶지 않은 경우에는 언제든지 철회할 수 있다는 것이다. 기존 방식은 일일이 해당 서비스를 방문해야 하고, 동의 철회는 대체로 쉽지 않으며, 심지어는 별도 서류를 작성해야 하는 등 번거롭다. 이와 달리, 데이터 지갑은 동의 이후에도 사용자에게 정보에 대한 자기결정권을 최대한으로 제공한다.

[388] 또한 사용자가 공유하겠다고 동의한 모든 데이터에는 사용자의 암호키로 일종의 워터마크와 같은 서명을 남길 수 있다. 이를 활용하면 특정 기관이 보유한 데이터에 워터마크가 없는 경우, 해당 기관은 해당 데이터를 어떻게 적법하게 가졌는지 증명해야 한다. 이로써 정보 주체의 데이터가 더 안전한 방식으로 유통될 수 있게 된다.

[389] 한편, 기존 방식의 본질적인 문제는 사용자가 약관의 내용을 읽고 동의한다는 문구를 표시하고, 이에 대한 증거로 동의 버튼을 누르도록 강요하는 동의 확보 방법에 있다. 이는 정보 주체보다 서비스를 제공하는 기업을 보호하기 위한 것에 가깝다. 서비스 약관 및 프라이버시 정책 등은 내용이 너무 길고 복잡하기 때문

에 현실적으로 사용자가 모든 내용을 면밀히 읽고 불합리한 조항이 있는지 검토하기란 어렵다. 불충분한 동의가 발생할 수밖에 없는 이유이기도 하다.

[390] 이를 해결하기 위해 본 발명의 다양한 실시 예들은 정보 주체를 충분히 보호하면서도 합리적으로 활용하는 데 문제가 없는 정책에 대한 표준화된 라이센스를 도입한다. 만약 여러 서비스가 같은 정보보호 정책을 갖추고, 자세히 읽어보지 않아도 모든 내용이 동일하다는 것을 신뢰할 수 있다면 사용자는 여러 서비스를 쓰더라도 한 번만 제대로 읽어보면 될 것이다. 그 다음부터는 동일한 정보보호 정책 라이센스를 사용한다는 것만 확인하 면 그저 동의 버튼만 누르거나 또는 사용자가 원하면 자동으로 동의하도록 설정할 수도 있을 것이다. 이는 사용자 편의성, 사용자 보호, 기업의 동의 확보율 등 모든 측면에서 도움이 될 것이다.

[391] 만약 표준에 존재하지 않거나 기존에 사용자가 동의한 적이 없는 조항이 담긴 정책의 경우, 동의를 별도로 받아야 하는 약관으로 분리할 수 있다. 이러한 경우, 사용자는 변경되거나 새로운 내용만 확인하면 되기에 더욱 확신을 갖고 동의 여부를 결정할 수 있게 된다. 이러한 라이센스는 탈중앙 거버넌스 프레임워크에서 관리되어 신뢰성을 갖출 수 있다.

[392]

[393] 관리

[394] 헬스케어 데이터는 글로벌 단위로 수집되고 활용되어야 그 잠재력이 최대한으로 발휘될 수 있다. 데이터 수집과 활용은 정보 주체에게 그 정보를 활용해 생긴 부가 서비스를 제공하는 것으로 이뤄질 수도 있지만, 당장 제공할 서비스가 없는 경우에는 적절한 보상을 하는 편이 보편적이고 효율적일 수 있다. 그러한 측면에서 인터넷을 통해 글로벌 단위로 데이터가 빠르고 저렴하게 전송될 수 있는 자산을 지원하고, 이를 데이터 지갑을 통해 주고받으며 보관할 수 있어야 한다.

[395] 이에 가장 적합한 자산은 Bitcoin과 달러와 연동된 Stablecoin일 것이다. 특히 Lightning 네트워크의 발전 덕분에 수십 달러 이내의 돈은 0.0x 달러도 안 되는 수수료만으로도 전 세계 어디로든 신용카드 결제할 때와 같은 속도로 전송할 수 있다. 또한 Taproot와 Taro와 같은 기술의 발전으로 Bitcoin 네트워크를 통해서도 Stablecoin 전송이 가능해질 예정이다.

[396] 본 발명의 다양한 실시 예들에 따른 데이터 지갑을 활용한다면 사용자나 기업이 선호하는 자산의 형태로 데이터 수집 및 활용을 통한 글로벌 단위의 보상이 가능하다. 본 발명의 다양한 실시 예들에 따른 데이터 지갑은 BIP-39 표준에 호환되도록 구현할 예정이므로 HPO 토큰, 이더리움 등 기타 알트코인도 필요하다면 지원할 수 있다.

[397]

[398] 백업과 복원

[399] 데이터 지갑에는 개인의 귀중한 자산과 데이터가 보관되므로 이를 안전하게 백업하고 복원하는 방법도 중요하다. 사용자는 기본적으로 BIP-39에 의해 데이터 지갑 생성 과정에서 표시된 니모닉 코드(Mnemonic code)를 안전한 곳에 기록해

둠으로써 백업할 수 있다. 그런데 이러한 방식은 다소 생소하고 대부분은 개인이 온전히 책임져야 하는 방식이 부담스러울 수 있다. 이를 위해 니모닉 코드를 사용자가 설정한 추가 암호로 암호화해 iCloud나 Google Drive 등 평소 사용하는 개인 클라우드 저장소에 저장하는 방식을 지원할 예정이다.

[400] 이러한 방식은 일반적으로 거액의 자산을 보관하는 데이터 지갑에는 부적합하지만, 본 발명의 다양한 실시 예들에 따른 데이터 지갑의 사용자 대부분이 니모닉 코드 자체를 분실할 위험을 해소할 수 있으므로 적절한 트레이드-오프일 수 있다. 물론 사용자가 개인 클라우드 저장소에 보관하지 않고, 더 안전한 방법을 선택할 수도 있다. 앞서 설명했듯이 Bitcoin 지갑 관련 표준을 준수해 개발할 예정이므로 다중서명 지갑(Multi-sig wallet), Passphrase 추가와 같은 Bitcoin 지갑의 보안성을 높이는 방법은 거의 동일하게 구현할 수 있다.

[401]

[402] 본 발명의 다양한 실시 예들에 따른 데이터 지갑의 애플리케이션들

[403] 본 발명의 다양한 실시 예들에 따른 데이터 지갑과 연동해 데이터를 활용한 부가 서비스를 제공하거나 데이터에 대해 보상을 하는 서비스를 탐색할 수 있는 디렉터리인 데이터 지갑 애플리케이션이 제공될 수 있다. 각 서비스가 어떤 데이터를 요청하는지, 어떤 서비스와 보상을 주는지 미리 살펴보고 데이터 지갑의 활용도를 높일 수 있다.

[404]

[405] 도 15는 본 발명의 다양한 실시 예들에 따른 실제 환자의 데이터를 데이터 지갑으로 발급하는 기능의 일 예를 도시한다.

[406] 알림

[407] 필수적인 고지 내용이나 동의 요청을 사용자가 적시에 확인하려면 알림 기능이 필요하다. 효과적으로 사용 자의 주의를 끌 수 있도록 동의와 서명이 필요할 때만 기기의 시스템 알림 기능을 활용할 것이다.

[408]

[409] 대리인, 후견인

[410] 일반적으로는 지갑 소유자와 정보 주체가 동일하지만, 많은 환자가 건강이나 기술 이해도 등의 이유로 스스로 데이터 지갑을 관리하기 어려울 수 있다. 이러한 경우에는 타인이 환자를 대신해 동의와 데이터 공유에 대한 의사 결정을 할 수 있도록 데이터 지갑 수준에서 대리인을 지정하는 기능을 제공할 수 있다. 이때, 대 리인 자격을 가진 지갑 사용자는 정보 주체의 데이터를 지갑에 대신 보관하고 통제할 수 있는 권한을 가질 수 있다.

[411] 이러한 대리인은 보호자와 같은 개인뿐만 아니라 단체가 될 수도 있다. 또한 이 기능을 확장하면 환자가 사망했을 때 환자의 자산과 데이터를 후견인이 넘겨받을 수 있도록 구현할 수도 있다. 각국 법률에서 이러한 방식이 허용되는지는 추가적인 확인이 필요하지만, 대리인과 후견인에 대한 신원 인증은 앞서 설명한 검증가능한 자격증명(VC)을 통해 전자적 방식으로 구현이 가능하다.

[412]

[413] 로그

[414] 데이터 지갑을 사용해 발생한 모든 활동은 이후 감사가 가능하도록 로그정보를 암호화해 사용자 기기에 저장할 수 있다. 이렇게 저장된 로그정보는 만약 사고나 오류가 발생했을 때, 책임 소재나 원인 파악 등을 면밀히 분석하는 데 활용할 수 있다.

[415]

[416] 데이터 발급 및 활용

[417] 데이터 발급

[418] 데이터 발급 기관은 검증가능한 자격증명(VC)의 형태로 데이터를 발급할 수 있다. 이를 위해서는 지갑과 DID 생성이 필요하다. 또한 기관 내부 시스템에 데이터 발급 SDK를 통합해야 한다. 그러면 기본적인 데이터 발급을 위한 준비가 완료된다.

[419] 데이터는 정보 주체로부터 요청을 받아 각 건별로 발급하거나 내부 관리자 페이지에서 발급 대상의 DID를 입력해 일괄 발급도 가능하다. 두 방법 모두 기관 내부 데이터를 VC 형태로 발급할 수 있도록 데이터 모델을 변환해야 한다. 현재 JSON-LD와 JWT 두 가지 구문 표현을 사용해 VC를 발급할 수 있으며, 모든 데이터를 이러한 데이터 모델로 변환하지 않고 앞서 언급한 IPFS 등 보안 데이터 저장소(SDS)에 데이터 파일을 정보 주체의 공개 키로 암호화해 업로드 후 생성된 해시값을 VC에 포함하는 방법도 있다. 이때 VC에 포함되는 데이터는 schema.org에 정의된 스키마를 활용할 경우 다양한 서비스에 호환되는 형태로 표현할 수 있는데, 이미 Health와 Medical 등 헬스케어 관련 스키마가 정의되어 있어 이를 기반으로 자주 사용되는 VC 템플릿을 제공하고 이를 재사용하도록 유도하는 방식으로 데이터 지갑을 통해 교환되는 데이터의 호환성을 높일 수 있다. 또한 본 발명의 다양한 실시 예들에서 자주 사용되는 VC 스키마를 정의해 거버넌스 프레임워크에 의해 관리하는 방식도 채택할 수 있다.

[420]

[421] 도 16은 본 발명의 다양한 실시 예들에 따른 의료 연구자의 신뢰할 수 있는 연구를 위해 의료 데이터를 선별된 환자로부터 생성하는 과정의 일 예를 도시한다.

[422] 상술한 기능들은 임상연구 데이터 관리 프로그램인 Raredata에 최초로 적용되어 데이터 발급 SDK와 함께 실제 환자의 데이터를 데이터 지갑으로 발급하는 기능으로 제공될 수 있다. SDK는 다른 영리/비영리 제품에도 별도 계약 없이 자유롭게 통합될 수 있다.

[423] 임상연구 데이터 관리 프로그램인 Raredata는 본 발명의 다양한 실시 예들에 따른 생태계에 신뢰할 수 있는 고품질 데이터를 공급할 수 있다. Raredata의 주요 고객인 의료 연구자는 신뢰할 수 있는 연구를 위해 다양하고 방대한 고품질의 데이터를 선별된 환자로부터 생성한다. 특히 임상연구 대부분은 데이터의 대표성을 위해 여러 기관의 연구자가 협력해 데이터를 구축한다. 이 과정에서 필연적으로

데이터의 종류, 용어, 수집 방법 등이 체계적으로 구조화된다. 또한 연구 결과의 재 현가능성이 중요하므로 데이터의 의도적인 조작에 대한 동기는 최소화된다. 이러한 메커니즘을 통해 VC를 통한 데이터 유통 과정뿐만 아니라 원천 데이터의 신뢰성도 확보할 수 있게 된다.

[424] VC에 포함되는 또 다른 중요한 정보는 발급된 데이터가 거래되었을 때 발급 기관의 몫으로 배분될 수수료율이다. 지금까지 데이터 발급 기관은 기관 외부로 반출된 데이터에 대한 몫을 청구할 방법이 현실적으로 없었다. VC를 활용한다면 모든 데이터는 환자의 결정이 있어야 유통될 수 있고, 환자 동의하에 유료로 거래된 데이터에 대한 금액은 환자와 발급 기관에 자동으로 배분된다. 이를 통해 데이터 발급 기관은 데이터 발급 수수료 외에 데이터 활용으로 발생하는 인센티브를 확보할 수 있다. 이러한 메커니즘은 발급 기관으로 하여금 보다 신뢰할 수 있고 활용하기 좋은 데이터를 준비하고 발급하는 데 동기 부여가 된다.

[425]

[426] 도 17은 본 발명의 다양한 실시 예들에 따른 데이터 활용의 일 예를 도시한다.

[427] 데이터 활용

[428] 인공지능 헬스케어 솔루션을 개발하거나 이미 개발된 솔루션을 활용해 데이터 기반 헬스케어 서비스를 제공하는 기관, 또는 임상시험에 적합한 참여자를 스크리닝 하려는 등의 목적을 가진 기관은 본 발명의 다양한 실시 예들을 통해 충분한 동의가 이뤄져 신뢰할 수 있는 데이터를 활용할 수 있다. 이를 위해선 우선 데이터 활용 기관에서 사용할 데이터 지갑과 DID를 준비한다. 그리고 데이터 활용 SDK를 기관 내부 서비스에 통합해야 한다. 그러면 데이터 활용을 위한 준비가 완료된다.

[429] 데이터 활용을 위해선 정보 주체의 DID와 활용 기관의 DID를 연결하는 작업이 필요하다. 이는 일반적으로 정보 주체에게 로그인, 인증, 연결 등의 목적으로 QR 코드 스캔을 요청하고, 정보 주체가 이를 스캔 후 동의하는 과정으로 이뤄진다. 활용 기관은 모든 정보를 한 번에 요청할 필요는 없으며, 초기 단계에서는 기본적인 서비스 이용에 필요한 정보만 요청하고, 더 높은 수준의 사용자 동의가 필요한 정보는 별도로 요청하는 방법으로 데이터를 확보할 수 있다. 이러한 방법을 활용하면 사용자 전환이 이뤄지는 퍼널별로 적합한 데이터를 확보할 수 있다. 동의를 확보할 때 정보 주체에게 전달해야 할 정보는 활용 기관의 정보, 요청하는 권한의 내용, 어떤 데이터를 어떤 조건으로 활용하고자 하는지 등을 포함한다. 이는 기존의 이용 약관, 개인정보 보호 정책 등 데이터 수집과 활용을 위한 법적 고지문을 제시하고 동의받는 단계에 해당한다. 차이점은 활용 기관이 거버넌스 프레임워크에 의해 인증된 표준화된 약관을 채택할 수 있다는 점이다. 이러한 방식의 장점은 데이터 지갑의 동의(서명) 관리에서도 설명했듯이 정보 주체 입장에서는 매번 법적 고지문을 세세히 확인하는 노력을 들일 필요가 없다는 것이고, 기관 입장에서는 국가별, 상황별로 적합한 컴플라이언스 요건을 갖춘 라이센스

를 채택하면 된다는 것이다. 이는 법률 검토를 위한 비용과 시간을 크게 절감하고, 충분한 동의를 확보하는 데 한층 수월할 것이다.

[430] 데이터 활용 기관은 CompliantData SDK를 통해 Hippocrat DAO의 표준화된 프로토콜과 라이센스를 이용할 수 있다.

[431]

[432] 도 18은 본 발명의 다양한 실시 예들에 따른 데이터에 대한 보상 증가 및 개인정보 침해 위험의 감소에 따른 데이터 공유에 대한 동의 증가의 일 예를 도시한다.

[433] 상술한 기능들은 희귀질환 환자를 위한 서비스 Rarenote에 최초로 적용되어 데이터 활용 SDK 와 함께 실제 환자가 자신의 데이터 지갑에 보관된 데이터를 통해 건강 관리 및 커뮤니티 서비스를 이용할 수 있다. SDK는 다른 영리/비영리 제품에도 별도 계약 없이 자유롭게 통합될 수 있다.

[434] Rarenote는 본 발명의 다양한 실시 예들에 따른 생태계에 환자가 데이터 지갑을 활용할 수 있는 사용처를 제공할 수 있다. Rarenote는 희귀질환, 난치암 등 치료제에 대한 접근이 어려운 질환 환자에게 충분한 동의를 받아 확보한 데이터를 기반으로 신뢰할 수 있는 맞춤 정보와 건강 관리 솔루션, 커뮤니티 경험을 제공한다. 나아가 환자가 서비스 사용 과정에서 생성한 환자 유래 건강 데이터와 지갑을 통해 제출한 임상 데이터 등을 통합하고, 이를 제약사와 같은 또 다른 데이터 수요기관에서 활용하기 좋은 형태로 가공한다면 부가가치가 높은 데이터 판매가 가능해질 수 있다. 이 과정은 환자의 동의를 기반으로 하며, 발생한 수익은 환자와 데이터 발급 기관에 배분되는 보상의 원천이 되어 지속가능한 데이터 보상과 활용을 가능하게 한다.

[435] 이 시나리오를 구현하려면 데이터 활용 및 보상에 대한 조건이 환자가 동의하는 내용에 포함된다. 특히 개인정보 공개 수준에 따라 데이터는 보호의료정보, 비식별의료정보, 한정데이터세트 또는 식별의료정보, 익명의료정보, 가명의료정보 등으로 나뉠 수 있다. 일반적으로 높은 수준의 개인정보와 더 많은 정보를 요구할수록 보상 금액이 커지지만, 환자가 개인정보를 보호하고자 거절할 가능성 또한 높아진다. 이에 따라 데이터 활용 기관은 환자를 설득할 수 있는 꼭 필요한 데이터만 확보하려 노력할 것이다. 또한 데이터는 생성 과정에서 공공 재원이 많이 투입되기 때문에 가명 또는 익명정보일수록, 과학적 연구 목적으로 활용될수록, 공공의 목적으로 배분되는 보상의 비율이 커지게끔 설계할 수 있다. 이러한 메커니즘은 공공 보건의료 서비스의 품질을 높이는 데 기여할 수 있다.

[436] 데이터에 대한 보상이 클수록, 개인정보 침해에 대한 위험이 적을수록 데이터 공유에 대한 동의를 받을 수 있는 가능성이 커질 수 있다.

[437]

[438] 도 19는 본 발명의 다양한 실시 예들에 따른 거버넌스 프로토콜의 일 예를 도시한다.

[439] 거버넌스 및 DAO

[440] COVID-19를 통해 인류의 건강이 비단 한 국가나 인종이 아닌 글로벌 단위로 협력해야 함을 확인된 바 있다. 따라서, 본 발명의 다양한 실시 예들은 특정 국가나 기관에 종속되지 않은, 개방적이며 탈중앙 협력 메커니즘을 지향한다. 이에 가장 개방적이며 탈중앙화된 블록체인인 Bitcoin과 Lightning, Liquid 등의 레이어 네트워크 및 프로토콜을 기반으로 Hippocrat 프로토콜을 구현하고자 하며, 스마트 컨트랙트(Smart Contract)를 포함한 모든 소프트웨어는 개방형 표준과 오픈소스로 개발된다.

[441] 이하 본 발명의 다양한 실시 예들에 따른 정책에 관한 초기 제안과 이러한 정책을 수립하는 과정에서의 접근 과정을 설명한다. 정책별 구체적인 거버넌스 프로토콜은 명문화되어 검증할 수 있는 형태로 게시된다.

[442]

[443] 도 20은 본 발명의 다양한 실시 예들에 따른 데이터 수집 및 보상 시스템의 일 예를 도시한다.

[444] 거버넌스 참여 자격

[445] 기본적인 거버넌스 참여에는 특별한 자격이 필요 없다. 포럼을 통한 정책 의견 개진, 오픈소스 코드 개선 제안 등은 누구나 자유롭게 할 수 있다. 합의 방식은 IETF(Internet engineering task force. 국제인터넷 표준화기구)에서 취하는 Rough consensus 를 채택할 예정이다. 단, 표준 정책 채택, 기관 인증 심사, 프로토콜 소스 코드 수정 권한 보유자 선정, DAO 재정 및 관련 지갑 관리 보유자 선정 등 명확한 역할과 책임이 필요한 일부 권한은 DAO 구성원 간의 합의에 의해 선출된 단일 혹은 복수의 구성원에 부여될 수 있다. 또한 일부 권한은 지갑 소유자가 특정 질환 환자인지, 의료 기관 담당자인지 등 특정 이해관계자임을 증명할 수 있는 VC 보유 여부에 따라 달라진다. 이에 따라 특정 이해관계자의 의사가 비중 있게 다뤄질 수 있도록 한다.

[446] 일부 소수에게 권한이 집중되어 남용되는 것을 막기 위해 권한별로 이해관계가 분산된 다수의 구성원이 권한을 가질 수 있으며, 이들 사이에 충분한 합의가 이뤄지는 방식으로 결정하게 된다. 이러한 권한은 당사자의 DID로 DAO 혹은 기존 권한 보유자로부터 해당 권한에 대한 VC를 발급받은 것으로 증명될 수 있다. 대체로 이러한 권한은 정책에 의해 만료일이 있으며, 갱신되지 않을 경우 권한은 만료된다.

[447]

[448] DAO의 역할

[449] 기본적으로 본 발명의 다양한 실시 예들은 오픈소스와 자발적인 개방형 협력의 형태로 소프트웨어와 정책 개발이 이뤄지지만, 본 발명의 다양한 실시 예들의 주요 요소인 데이터 지갑과 SDK 등을 개발하고 표준 정책의 초안을 작성하는 경우에는 책임과 역할이 체계적으로 정의된 조직이 있을 때 보다 효율적일 수 있다. 이를 위해 커뮤니티 중 일부는 Hippocrat DAO(Decentralized autonomous organization)에 속해 기여할 수 있다.

[450] Hippocrat DAO는 탈중앙화된 구조와 자율적으로 운영되는 조직을 지향한다. 이를 위해 최대한 많은 일을 스마트 콘트랙트에 의해 운영되도록 구현하지만, 기술적 또는 법적 한계로 모든 일이 가능하진 않을 수 있다. 그러한 경우에는 역할과 책임이 분명한 체계를 기반으로 사람에 의해 운영되는 조직과 구성원이 필요하다. 따라서 DAO에서 필요로 하는 전문성과 경험이 있는 경우에는 DAO에 소속되어 일함으로써 거버넌스에 참여할 수 있다. DAO는 본 발명의 다양한 실시예들에 따른 생태계의 성장에 도움을 줄 수 있는 이들로 구성되어 특정 개인이나 기관으로부터 자유로운 체계를 갖출 것이다.

[451]

[452] DAO 트레저리 관리

[453] 데이터 활용 SDK를 통해 금전적 보상을 제공하고 거래되는 데이터의 경우, 거래 금액의 10%는 프로토콜 수 수료로 DAO의 수입이 된다. DAO는 이 수입과 Hippocrat Foundation으로부터 받은 토큰이 보관된 트레저리 (Treasury) 관리 권한을 선출된 이들에게 부여하고, 이를 통해 필요한 수입과 비용이 관리되도록 한다.

[454] 이러한 권한이 필요한 이유는 데이터 거래에서 발생하는 인센티브 배분처럼 스마트 콘트랙트에 의해 자동으로 이뤄지는 경우도 있지만, 스마트 콘트랙트로 표현할 수 없는 계약과 거래도 존재하기 때문이다. 그리고 스마트 콘트랙트 또한 최초에는 사람에 의해 설계되는 것이므로 그 과정에도 이들이 함께 참여한다. 이는 전통적인 조직 체계의 비용 집행을 위한 의사 결정 프로세스와 유사하게 이뤄진다. 대신 모든 의사 결정은 투명하게 기록되고 공개된다.

[455] 한편 거래하는 데이터의 유형이 개인 식별가능성이 적고, 공익성이 높은 경우에는 프로토콜 수수료와 별도로 공공 보건의료 재원을 위한 추가 공제가 이뤄진다. 이 공공 보건의료 재원 공제로 적립된 금액은 DAO의 운영 예산과는 따로 관리되며, 국가별 공공 보건의료 기관에 기부하는 목적으로만 사용될 수 있다. 이는 최소 10%에서 시작해 개인 식별가능성이 적고, 공익성이 높을수록 최대 30%까지 부과될 수 있다. 이렇게 적립된 재원은 국가별 공공 보건의료 기관과의 원활한 협력을 가능하게 할 것이다.

[456]

[457] 도 21은 본 발명의 다양한 실시 예들에 따른 데이터 수집 및 활용에 따른 보상 시스템의 일 예를 도시한다.

[458] 표준 법적 고지문 관리

[459] DAO에서는 데이터 활용자가 정보 주체에게 제시하고 동의를 구할 때 사용할 수 있는 이용 약관 및 개인정보 보호 정책 등의 법적 고지문을 국가별, 데이터 활용 목적별로 표준화해 제공한다. 데이터 활용자가 이 표준화된 법적 고지문 중 적절한 항목을 데이터 활용 SDK를 통해 선택하면, 정보 주체는 데이터 지갑을 통해 데이터를 공유할 때 이를 확인할 수 있다. 만약 다양한 국적의 정보 주체를 대상으로 하는 경우에는 각 정보 주체의 국적에 맞는 법적 고지문이 표시된다.

[460] DAO는 국가별, 상황별로 데이터 활용자가 데이터를 잘 활용하면서도 정보 주체를 보호할 수 있도록 법적 고지문을 작성할 책임이 있다. 이렇게 작성된 법적 고지문은 탈중앙 저장소에 보관되고, 각 파일의 해시값을 표준 약관 레지스트리에 등록해 본 발명의 다양한 실시 예들의 표준으로 인증한다. 데이터 활용자가 채택한 법적 고지문이 표준 약관 레지스트리에 등록되어 있으면 정보 주체는 인증되었다는 사실을 확인할 수 있다. 또한 동일한 해시값을 가지는 항목에 대해서는 향후 추가 조치 없이 자동으로 동의하도록 설정할 수 있다. 모든 약관의 기본값이 동의로 되어있는 것은 아니지만, 이러한 방식을 통해 사용자는 최초 한 번만 내용을 파악하고, 이 후에는 같은 내용을 반복해서 검토하지 않아도 된다. 데이터 활용자 또한 충분한 동의를 효율적으로 확보할 수 있게 된다. 이것이 바로 표준화의 이점이다.

[461] 만약 법적 고지문에 변경이 필요하다면 데이터 표준 약관을 관리하는 권한을 가진 거버넌스 참여자간의 컨센서스를 통해 가능하다. 이는 포럼처럼 의사록이 공개되고, 변경안이 충분히 합의된 경우에만 실제 레지스트리에 반영될 수 있다. 또한 데이터 활용의 공익성과 개인 식별가능성에 따른 공공재원 배분율 또한 위와 같은 절차에 의해 정해진다.

[462]

[463] 데이터 발급 인증 관리

[464] 데이터 활용 기관이 어떤 데이터를 활용할 때, 그 데이터가 실제 유효한 기관으로부터 발급되었는지 궁금할 수 있다. 그래서 데이터 발급 기관의 데이터 지갑에는 발급 기관에 대한 필수 정보가 VC 형태로 기록되어 있어야 한다. 예를 들어 병원의 경우, 병원명, 주소, 등록 번호, 발급 담당자명, 이메일 주소, 연락처 등이 포함된다. 또한 데이터가 거래되었을 때 데이터 발급자의 몫으로 배분될 수수료율도 함께 포함되어야 한다. 이러한 정보는 별도 요청과 정보 공유 과정 없이도 공개적으로 조회할 수 있다.

[465] 그런데 제3자 입장에서는 이러한 정보를 있는 그대로 신뢰할 수 없다. 따라서 본 발명의 다양한 실시 예들은 DAO를 통해 발급 기관에 대한 인증 절차와 인증 기관을 조회할 수 있는 레지스트리를 운영한다. 기관 인증 심사를 통해 이 정보를 검증하고, 검증이 완료된 경우에는 인증된 기관의 레지스트리에 해당 기관의 DID 주소가 추가된다. 데이터 활용 SDK는 검증하려는 VC의 발급 기관이 이 레지스트리에 포함된 경우, '인증됨'이라는 값을 알려준다. 이를 통해 활용 기관은 별도 확인 절차 없이 해당 기관의 정보가 유효함을 신뢰하고 활용할 수 있다.

[466]

[467] 본 발명의 다양한 실시 예들에 따른 데이터 지갑 애플리케이션 관리

[468] 본 발명의 다양한 실시 예들에 따른 데이터 지갑은 사용자가 본인의 데이터를 활용한 데이터 지갑 애플리케이션을 탐색할 수 있는 디렉터리인 Hippocrat Apps를 제공한다. 이러한 애플리케이션에는 걸음 수 측정과 같은 서비스부터 디지털 치료제까지 다양한 유형이 존재할 수 있다. 사용자는 이곳에서 각 애플리케이션

이 제공하는 데이터 활용 서비스나 데이터 보상, 데이터 활용 조건 등을 살펴볼 수 있다. 이를 통해 각 애플리케이션은 정보 주체에게 본인의 서 비스를 알리고 유입시킬 기회를 얻을 수 있다.

[469] Hippocrat Apps에 표시되려면 DAO를 통해 게시 신청을 해야 하며, 관리 권한을 가진 거버넌스 참여자가 심사를 진행한 후 Hippocrat Apps에 표시되는 것을 결정할 수 있다. 게시 리스트와 정책은 Github 등을 통해 오픈소스로 관리되며 신청부터 심사, 노출 결정까지 투명하게 기록된다. 이 외에 DAO에 의해 심사되지 않는 리스트는 규격에 맞게 정보를 올리면 별도 심사 없이 게시될 수 있다.

[470]

[471] 관리

[472] 본 발명의 다양한 실시 예들에 따른 데이터 지갑과 SDK, 웹사이트 등, 프로토콜의 공식 소프트웨어 프로그램 소스코드는 주로 DAO에 의해 관리된다. 이는 기본적으로 개방형 표준과 오픈소스로 개발되지만, 제3자의 기여에만 의존할 경우 개발 효율이 떨어지거나 지속가능한 개발이 이뤄지지 않을 수 있다. 소스코드 관리 권한은 다수의 구성원에게 부여되며, 일부 권한의 경우 구성원 간 합의가 이뤄져야 실행할 수 있도록 관리된다.

[473] 상기 언급된 영역 외에도 다양한 이해관계자 간 합의를 토대로 개발되고 공지가 필요한 안건은 무엇이든 거버넌스에 의해 논의되고 결정될 수 있다.

[474]

[475] 인센티브 모델

[476] 본 발명의 다양한 실시 예들과 관련된 이해관계자는 크게 사용자와 거버넌스 참여자로 구분된다. DAO를 비롯한 거버넌스 참여자는 좋은 프로토콜을 설계해 프로토콜이 잘 운영되고 발전한 것에 대한 인센티브를, 사용자는 프로토콜을 사용함으로써 자기 문제가 해결되거나 경제적 이익을 얻게 되는 인센티브를 기대할 것이다. 한 사람이 두 역할을 하는 경우도 있지만, 어떠한 상황에서는 역할이 분명히 구분된다. 따라서 인센티브 모델도 역할별로 구분해야 혼란스럽지 않고, 각 역할의 동기에 잘 부합하도록 설계할 수 있다.

[477] 본 발명의 다양한 실시 예들은 신뢰할 수 있고 지속가능한 토큰 이코노미를 위해 주요 국가의 규제를 준수하고자 하며, 현재 미국, 유럽, 한국 등 주요 국가에서 진행 중인 디지털 자산에 대한 최종 법제화 내용에 기반한 커뮤니티와의 컨센서스를 통해 인센티브 모델을 결정할 수 있다.

[478] 적극적인 거버넌스 참여자는 특정 정책이나 이슈에 대해 자신의 주장과 의견이 프로토콜 차원에서 반영되도록 안건을 제안하고 다른 거버넌스 참여자를 설득하고자 노력할 것이다. 하지만 모든 참여자에게 이 정도 수준의 참여를 위한 전문성과 여력을 기대하기는 어려울 수 있다. 이러한 경우에는 자신의 이해관계를 잘 대변하는 주장과 안건에 투표로 지지를 표명할 수 있다.

[479] 사용자에게는 프로토콜 상에서 서로가 제공하는 가치를 효율적으로 교환하는 데 쓸 화폐가 필요하다. 이를 위해 본 발명의 다양한 실시 예들은 프로토콜 네이

티브 토큰인 HPO뿐만 아니라, 글로벌 단위의 탈중앙 생태계와 법정 화폐 기반 생태계 각각에서 가장 널리 채택되는 Bitcoin과 달러와 연동된 Stablecoin 또한 사용자 간 가치 교환을 위한 화폐로 사용한다.

[480] 본 발명의 다양한 실시 예들의 사용자별 인센티브 정책의 초기 제안은 다음과 같다. 이 내용은 새로운 인센티브 정책 제안과 투표에 의해 변경될 수 있다.

[481] 1. 정보 주체 (Data subject)

[482] 정보 주체는 데이터의 활용 및 거래 내용을 확인하고 결정할 권한이 있다. 자신의 데이터를 활용한 서비스를 인센티브로 누릴 수 있고, 데이터를 공유하는 대가로 데이터 활용자가 제시하는 경제적 보상을 인센티브로 받을 수도 있다. 그러면 프로토콜 수수료와 공공 보건의료 재원 목적의 공제를 제외한 나머지를 정보 주체와 데이터 발급자가 배분율에 따라 나눠 가진다. 하지만 어떤 조건에서도 가장 많은 몫은 정보 주체가 받는 것을 원칙으로 해, 전체 보상 중 최소 40%에서 최대 90%가 정보 주체에게 돌아간다.

[483] 2. 데이터 발급자 (Data issuer)

[484] 데이터 발급자는 데이터가 생성되는 데 필요한 비용과 전문성을 제공하며, 데이터 발급 시 정보 주체와 데이터 발급자 간에 보상 배분율을 정하는 권한을 가진다. 정보 주체가 결정한 데이터 거래로부터 경제적 이익이 발생하는 경우, 데이터 발급자는 이 배분율에 따른 보상을 인센티브로 받게 된다. 단, 데이터 발급자는 정보 주체가 가져가는 몫의 절반 이하로만 배분율을 정할 수 있다. 이 상한선 내에서는 데이터 발급자가 자율적으로 배분율을 정할 수 있지만, 정보 주체가 다른 데이터 발급 기관의 배분율이 더 합리적이라고 판단할 경우에는 발급 기관을 변경할 동기가 생긴다. 즉, 병원과 같은 발급 기관 입장에서는 환자가 다른 병원으로 이탈하는 일이 발생한다. 하지만 특정 기관에서만 발급할 수 있는 데이터일수록 발급 기관의 몫이 더 커지도록 배분율이 정해질 가능성이 크다. 본 발명의 다양한 실시 예들은 이러한 시장 메커니즘에 의해 적정 배분율이 결정되도록 한다.

[485] 3. 데이터 활용자(Data user)

[486] 데이터 활용자는 정보 주체에게 매력적인 서비스나 경제적 보상을 제시해 데이터 수집 및 활용 동의를 확보하게 된다. 이때, 프로토콜이 제공하는 표준화된 법적 고지문을 사용하면 컴플라이언스 비용을 최소화하고, SDK를 활용해 데이터 수집 및 활용을 효율적으로 할 수 있다. 법적 고지문에서 수집하고 활용하려는 데이터의 공익성이 높을수록, 개인 식별가능성이 적을수록, 공공 재원으로 배분되는 몫이 커진다. 공공 재원은 정보 주체의 국적에 따라 구분하여 관리되며 각국 정부 또는 공공 보건의료 기관에 기부된다. 이를 통해 글로벌 제약사나 헬스케어 서비스 제공자는 각국에서 의학 연구와 같은 공익성 데이터를 활용할 때 공공 기관으로부터 적절한 협조를 기대할 수 있다.

[487]

[488] HPO 토큰

[489] HPO 토큰은 본 발명의 다양한 실시 예들에 따른 생태계에서 데이터 수요자가 정보 주체에게 데이터 공유에 대한 대가로 보상을 지급하기 위해 구매 후 사용된다.

[490]

[491] 기대 효과

[492] 지금까지 개인은 자신의 정보에 대한 온전한 주권을 가질 방법이 없었다. 특히 최근 10년간은 거대 인터넷 플랫폼이 성장하며 이들에게 개인의 정보가 집중되는 현상이 심화하였고, 이로부터 비롯된 대규모 정보 유출 사고, 부가가치 독점 등에 대한 부작용 또한 심화하였다. 이에 대한 해결책으로 시작된 마이데이터와 자기주권신원 운동은 다시금 정보 주체에게 그 주권을 돌려주는 데 기여할 것이다.

[493] 특히 의료 분야는 이러한 문제와 중요성이 더욱 크다. 개인을 보호하려는 목적뿐만 아니라, 산업의 발전과 개인이 누릴 수 있는 실리적인 효익 측면에서도 정보 주체가 주권을 확보하는 것은 중요하다. 이를 중심으로 정보 주체를 둘러싼 이해관계자의 동기가 충족되어 서로 효율적인 협력이 이뤄지는 것도 필요하다. 본 발명의 다양한 실시 예들은 이를 실현할 것이며 기대 효과를 요약하면 다음과 같다.

[494]

[495] [표3]

기대 효과	기존 방식	본 발명(Hippocrat)
데이터 관리 및 통합	기관 중심	정보 주체 중심
환자 동의 확보 및 관리	어려움	쉬움
인센티브 교환	어려움	쉬움
데이터 위·변조	가능	불가능
의료정보 반출 형식	비전자적(종이 출력, CD 등)	전자적(VC)
중복 데이터 수집	빈번함	최소화

[496] 본 발명의 다양한 실시 예들을 통해 각 이해관계자들이 활용할 수 있는 예시는 다음과 같다.환자, 정보 주체

[497] 의료정보 인증

[498] 데이터 지갑 애플리케이션으로 병원에 비치된 등록 및 접수 QR코드를 스캔하면, 저장되어 있는 법정 신원정보로 쉽고 안전하게 본인을 인증하고 환자 등록 카드를 발급받아 데이터 지갑에 보관한다. 환자 등록 카드 에는 진단명, 검사 결과, 처방 약 등의 정보가 기록되어 이후 병원 접수, 보험금 신청 시 관련된 정보를 제출할 수 있다. 또한, 공항 및 특정 공공시설에서 백신 접종 여부를 확인할 때 애플리케이션에 보관된 백신 패스를 제시할 수 있다. 이렇게 의료 정보 제출과 인

증이 필요한 상황에서도 불필요한 개인정보는 노출하지 않으면서 필요한 의료 정보만 간편하게 전달할 수 있다.

[499]

[500] 데이터 수익화

[501] 제약사 및 헬스케어 서비스 제공자는 부가가치를 더한 신약과 서비스를 개발하기 위해 데이터 수집에 대한 비용을 지불할 용의가 충분하다. 특히 병원으로부터 생성된 임상 데이터뿐만 아니라, 소셜 네트워크, 쇼핑, 피트니스, 모빌리티 등 개인 기기를 통해 사용하는 서비스에서 생성된 환자 데이터도 헬스케어 목적으로 활용되는 사례가 늘어나고 있다. 따라서 다양한 기관과 기업이 자신의 데이터를 활용할 수 있도록 허용하는 대가로 받는 보상 빈도와 규모도 점점 늘어날 것이다. 데이터는 이미 공유했더라도 다른 대상에게 동일하게 공유할 수 있으므로 지속적인 수익화가 가능하다. 환자는 본 발명의 다양한 실시 예들에 따른 데이터 지갑을 통해 데이터 거래를 승인하고, 그 대가로 받은 보상을 데이터 지갑에서 모아 관리할 수 있다.

[502]

[503] 맞춤형 건강 관리

[504] 환자는 비용을 지불하더라도 건강과 삶의 질을 개선할 수 있는 건강 관리 서비스를 사용할 용의가 충분하다. 환자 본인의 데이터 지갑에 저장된 헬스케어 데이터를 활용하는 서비스를 제공할 수 있도록 허용하여 맞춤화된 건강 관리 서비스를 누릴 수 있게 된다.

[505]

[506] 제약사 및 헬스케어 서비스 제공자

[507] 충분한 동의 기반 데이터 확보

[508] 환자로부터 충분한 동의를 확보한 데이터의 경우, 강도 높은 비식별화 처리로 인해 데이터 훼손이 최소화되고, 다른 데이터세트와의 결합을 통해 새로운 발견이 가능해진다. 또한 법에서 보장된 비식별화 데이터의 활용 목적보다 더 다양한 목적과 상업화를 전제로 한 활용을 가능하게 하여금 보다 혁신적이고 도전적인 시도를 가능하게 한다. 그뿐만 아니라 환자로부터 직접 받았던 동의를 데이터로 공유받기 때문에, 중간자 역할을 하는 기업에 쓰는 비용을 절감하거나 환자에게 더 매력적인 보상을 제시하여 데이터 확보 가능성을 높일 수 있다.

[509]

[510] 임상시험 참여자 스크리닝

[511] 환자의 데이터 지갑에 이미 발급된 데이터를 활용하면 임상시험에 적합한 환자를 스크리닝하는 단계가 훨씬 효율적으로 진행된다. 예를 들어 임상시험에 관심 있는 환자가 임상시험 모집 공고에 첨부된 QR코드를 스캔하면, 데이터 지갑에 저장된 데이터를 토대로 그 즉시 참여 가능 여부가 표시되고 참여 의사를 전달할 수 있다. 특히 임상시험 선정 및 제외 조건은 비공개로 이뤄지는 경우가 많은데,

영지식 증명을 활용하면 이러한 조건과 환자의 개인정보는 비공개로 유지된 상태에서 적합 여부만을 확인할 수 있게 된다.

[512]

[513] 맞춤형 헬스케어 서비스 개발

[514] 헬스케어 서비스 개발 기관은 환자 중심으로 통합된 임상 데이터를 비롯해 다양한 헬스케어 데이터가 보관된 데이터 지갑을 통해 개인 맞춤형 서비스 개발을 위한 데이터를 글로벌 단위로 확보할 수 있다. 개발 단계를 지나 상업화 단계에서도 복잡한 회원 가입 없이 지갑만 연결하면 그 즉시 맞춤화 서비스를 제공할 수 있어 사용자의 구매 전환율을 높이고, 국가별로 표준화된 법적 고지문으로 컴플라이언스 이슈는 최소화하면서 글로벌 비즈니스를 운영할 수 있다.

[515]

[516] 병원 등 의료 기관

[517] 환자정보 발급 효율화

[518] 미국 등 주요 국가 정부 기관이 의료 기관에 보관된 데이터를 외부에 전자적 형태로 반출할 수 있도록 법제화하는 조치에 효과적으로 대응할 수 있다. 본 발명의 다양한 실시 예들에 따른 데이터 지갑, 데이터 발급 SDK가 적용된 Raredata를 이용하 면 클릭 몇 번만으로 수집된 데이터를 전자적 형태로 발급할 수 있다. 이를 통해 추가 비용 없이 규제를 준수하고, 환자의 데이터 자기주권 친화적인 시스템을 통해 환자 만족도를 높일 수 있다.

[519]

[520] 데이터 수익화

[521] 환자의 데이터 지갑으로 데이터를 발급할 때 의료 기관의 디지털 서명이 기록되어 외부로 반출된 이후에도 발급된 데이터의 유통 경로를 추적할 수 있고, 환자를 통해 유상으로 제3자에게 공유된 경우 그 일부가 의료 기관으로 자동 배분된다. 이를 통해 데이터 발급과 관리를 위해 투자된 전문 장비와 인력에 대한 비용을 회수하고, 데이터 활용 활성화를 통한 추가 수익을 기대할 수 있다.

[522]

[523] 임상연구 활성화

[524] 제약사 등 스폰서 없이 의료 기관 자체적으로 실시하는 임상 연구의 경우, 예산의 한계로 인해 활성화되기 어렵다. 또한 임상연구 진행을 위해 환자의 동의와 데이터를 수집하는 비용과 시간이 적지 않게 든다. 만약 환자의 데이터 지갑에 다른 임상연구로부터 발급된 데이터가 있다면, 이를 환자의 동의를 받아 활용하는 식으로 중복 데이터 수집에 드는 환자와 연구진의 시간과 노력 그리고 비용을 절감할 수 있게 된다. 스폰서 없이도 더욱 다양한 연구가 활성화될 수 있다.

[525]

[526] 공공 보건 의료기관

[527] 공공 데이터 구축 및 활용 활성화

[528] All of US와 같이 공공 보건의료 기관 주도로 공익을 위해 실시하는 연구 또한 정보 주체로부터 데이터를 직접 수집하면 그 시간과 비용을 크게 절감할 수 있어 한정된 공공 예산을 더욱 효율적으로 쓸 수 있게 된다. 이렇게 수집된 데이터는 공익적 목적의 데이터세트로 가공하여 다시 공공 보건의료의 발전을 촉진하는 데 도움이 된다.

[529]

[530] 공공 보건의료 재정 확보

[531] 공익적 목적으로 개인 식별가능성이 낮은 데이터가 거래될 경우, 해당 정보 주체 국적의 공공 보건의료 기관에 기부되는 목적의 재원으로 적립된다. 이를 통해 정보 주체의 권리와 보건의료 데이터 공공성의 균형을 실현하고, Hippocrat과 각 국가 기관과의 긍정적인 협력 관계를 유지하게 된다.

[532]

[533] 하드웨어를 이용하여 본 발명의 실시 예를 구현하는 경우에는, 본 발명을 수행하도록 구성된 ASICs(application specific integrated circuits) 또는 DSPs(digital signal processors), DSPDs(digital signal processing devices), PLDs(programmable logic devices), FPGAs(field programmable gate arrays) 등이 본 발명의 프로세서(505)에 구비될 수 있다.

[534] 한편, 상술한 방법은, 컴퓨터에서 실행될 수 있는 프로그램으로 작성 가능하고, 컴퓨터 판독 가능 매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다. 또한, 상술한 방법에서 사용된 데이터의 구조는 컴퓨터 판독 가능한 저장 매체에 여러 수단을 통하여 기록될 수 있다. 본 발명의 다양한 방법들을 수행하기 위한 실행 가능한 컴퓨터 코드를 포함하는 저장 디바이스를 설명하기 위해 사용될 수 있는 프로그램 저장 디바이스들은, 반송파(carrier waves)나 신호들과 같이 일시적인 대상들은 포함하는 것으로 이해되지는 않아야 한다. 상기 컴퓨터 판독 가능한 저장 매체는 마그네틱 저장매체(예를 들면, 롬, 플로피 디스크, 하드 디스크 등), 광학적 판독 매체(예를 들면, 시디롬, DVD 등)와 같은 저장 매체를 포함한다.

[535] 이상에서 설명된 실시 예들은 본 발명의 구성요소들과 특징들이 소정 형태로 결합된 것들이다. 각 구성요소 또는 특징은 별도의 명시적 언급이 없는 한 선택적인 것으로 고려되어야 한다. 각 구성요소 또는 특징은 다른 구성요소나 특징과 결합되지 않은 형태로 실시될 수 있다. 또한, 일부 구성요소들 및/또는 특징들을 결합하여 본 발명의 실시 예를 구성하는 것도 가능하다. 발명의 실시 예들에서 설명되는 동작들의 순서는 변경될 수 있다. 어느 실시 예의 일부 구성이나 특징은 다른 실시 예에 포함될 수 있고, 또는 다른 실시 예의 대응하는 구성 또는 특징과 교체될 수 있다. 특허청구범위에서 명시적인 인용 관계가 있지 않은 청구항들을 결합하여 실시 예를 구성하거나 출원 후의 보정에 의해 새로운 청구항으로 포함시킬 수 있음은 자명하다.

[536] 본 발명이 본 발명의 기술적 사상 및 본질적인 특징을 벗어나지 않고 다른 형태로 구체화될 수 있음은 본 발명이 속한 분야 통상의 기술자에게 명백할 것이다. 따라서, 상기 실시 예는 제한적인 것이 아니라 예시적인 모든 관점에서 고려되어야 한다. 본 발명의 권리범위는 첨부된 청구항의 합리적 해석 및 본 발명의 균등한 범위 내 가능한 모든 변화에 의하여 결정되어야 한다.

산업상 이용가능성

[537] 본 발명은 의료 데이터를 의료 기관과 거래하는 개인 사용자의 신원 확인에 대하여 블록 체인 네트워크에서 이중의 거래 내역을 통해 증명함으로써 의료 데이터에 대한 당사자 확인의 보안성을 높이기 위한 방법 및 장치에 관한 것으로서, 존의 중앙 집중형 신원 인증 시스템이 내포하는 보안 취약점과 단일 실패 지점의 위험의 문제를 해결하기 위해 탈중앙화된 신원 인증 방식을 도입하여 보안성과 신뢰성을 크게 향상시키고 사용자가 자신의 데이터와 신원에 대한 직접적인 관리 및 통제를 할 수 있어, 의료 데이터 관리 분야에서 산업상 이용 가능성이 기대된다.

청구범위

[청구항 1] 통신 시스템에서 서버의 동작 방법에 있어서, 상기 서버는 송수신기, 메모리, 프로세서를 포함하고,
환자 단말과 상기 서버의 제1 암호화폐 지갑의 정보 및 상기 환자 단말의 제2 암호화폐 지갑의 정보를 상기 송수신기에 의하여 교환하는 단계;
상기 제1 암호화폐 지갑으로부터 상기 제2 암호화폐 지갑으로 설정된 양의 암호화폐 및 OP_RETURN을 전송하는 2개의 로직과 관련된 하나의 트랜잭션 정보를 블록체인 네트워크에게 상기 송수신기에 의하여 전송하는 단계;
병원 단말로부터 상기 제1 암호화폐 지갑에서 상기 2개의 로직과 관련된 상기 트랜잭션 정보의 요청 메시지를 상기 송수신기에 의하여 수신하는 단계 - 상기 환자 단말의 탈중앙화 신원 정보(Decentralized Identifier, DID)은 상기 제1 암호화폐 지갑의 제1 주소 및 상기 제2 암호화폐 지갑의 제2 주소를 포함함 -;
상기 병원 단말에게 상기 2개의 로직과 관련된 상기 제1 암호화폐 지갑의 상기 트랜잭션 정보를 포함하는 응답 메시지를 상기 송수신기에 의하여 전송하는 단계를 포함하고,
상기 제1 암호화폐 지갑의 제1 주소 및 상기 제2 암호화폐 지갑의 제2 주소에 설정된 양의 암호화폐 및 OP_RETURN을 전송하는 2개의 로직과 관련된 하나의 트랜잭션 정보가 공통적으로 존재함에 기반하여 상기 DID의 유효함이 증명되고,
상기 OP_RETURN은 트랜잭션 생성 시 상기 서버의 서명 데이터가 예정된 위치에 상기 서명 데이터를 삽입하지 않고 비우거나 또는 서명 데이터 대신 다른 데이터를 삽입한 정보인,
방법.

[청구항 2] 제1 항에 있어서,
상기 OP_RETURN은 상기 서명 데이터 대신 상기 서버에 의하여 생성된 상기 환자 단말의 상기 DID를 포함하는,
방법.

[청구항 3] 제1 항에 있어서,
상기 환자 단말 및 상기 병원 단말은 상기 서버에 의하여 탈중앙화 신원 정보(Decentralized Identifier, DID)가 관리되는,
방법.

[청구항 4] 제1 항에 있어서,
상기 환자 단말과 상기 병원 단말 간 의료 데이터 전송의 보안과 관련하여,

공유 키 생성을 위해 ECIES(Elliptic Curve Integrated Encryption Scheme) 및 ECDH(Elliptic Curve Diffie-Hellman)를 사용하여 상기 환자 단말과 상기 병원 단말 간 개인 키를 공유하지 않고도 데이터 암호화 및 복호화가 상기 프로세서에 의하여 수행되고,

데이터 무결성과 기밀성을 보장하기 위해 상기 환자 단말과 상기 병원 단말 간 상기 의료 데이터의 전송 전에 상기 의료 데이터를 암호화하기 위한 AES-GCM(Advanced Encryption Standard Galois/Counter Mode)가 상기 프로세서에 의하여 수행되는,

방법.

[청구항 5] 통신 시스템에서 환자 단말의 동작 방법에 있어서, 상기 환자 단말은 송수신기, 메모리, 프로세서를 포함하고,

서버와 상기 서버의 제1 암호화폐 지갑의 정보 및 상기 환자 단말의 제2 암호화폐 지갑의 정보를 상기 송수신기에 의하여 교환하는 단계;

상기 제1 암호화폐 지갑으로부터 상기 제2 암호화폐 지갑으로 설정된 양의 암호화폐 및 OP_RETURN을 수신하는 2개의 로직과 관련된 하나의 트랜잭션 정보를 블록체인 네트워크에게 상기 송수신기에 의하여 전송하는 단계;

각 통신 인스턴스에 대하여 ECIES(Elliptic Curve Integrated Encryption Scheme) 방식에 기반하여 무작위 개인 키 및 무작위 공개 키의 키 쌍을 상기 프로세서에 의하여 생성하는 단계;

상기 환자 단말의 상기 무작위 개인 키 및 병원 단말의 공개 키로부터 계산되는 ECDH(Elliptic Curve Diffie-Hellman) 공유 키를 사용하여 상기 환자 단말의 의료 데이터를 상기 프로세서에 의하여 암호화하는 단계;

상기 환자 단말의 무작위 공개 키와 함께 상기 암호화된 의료 데이터를 상기 병원 단말에게 상기 환자 단말의 탈중앙화 신원 정보(Decentralized Identifier, DID)에 기반하여 상기 송수신기에 의하여 전송하는 단계를 포함하고,

상기 DID는 상기 제1 암호화폐 지갑의 제1 주소 및 상기 제2 암호화폐 지갑의 제2 주소를 포함하고,

상기 제1 암호화폐 지갑의 제1 주소 및 상기 제2 암호화폐 지갑의 제2 주소에 설정된 양의 암호화폐 및 OP_RETURN을 전송하는 2개의 로직과 관련된 하나의 트랜잭션 정보가 공통적으로 존재함에 기반하여 상기 DID의 유효함이 증명되고,

상기 OP_RETURN은 트랜잭션 생성 시 상기 서버의 서명 데이터가 예정된 위치에 상기 서명 데이터를 삽입하지 않고 비우거나 또는 서명 데이터 대신 다른 데이터를 삽입한 정보인,

방법.

[청구항 6] 제5 항에 있어서,

상기 OP_RETURN은 상기 서명 데이터 대신 상기 서버에 의하여 생성된 상기 환자 단말의 상기 DID를 포함하는,
방법.

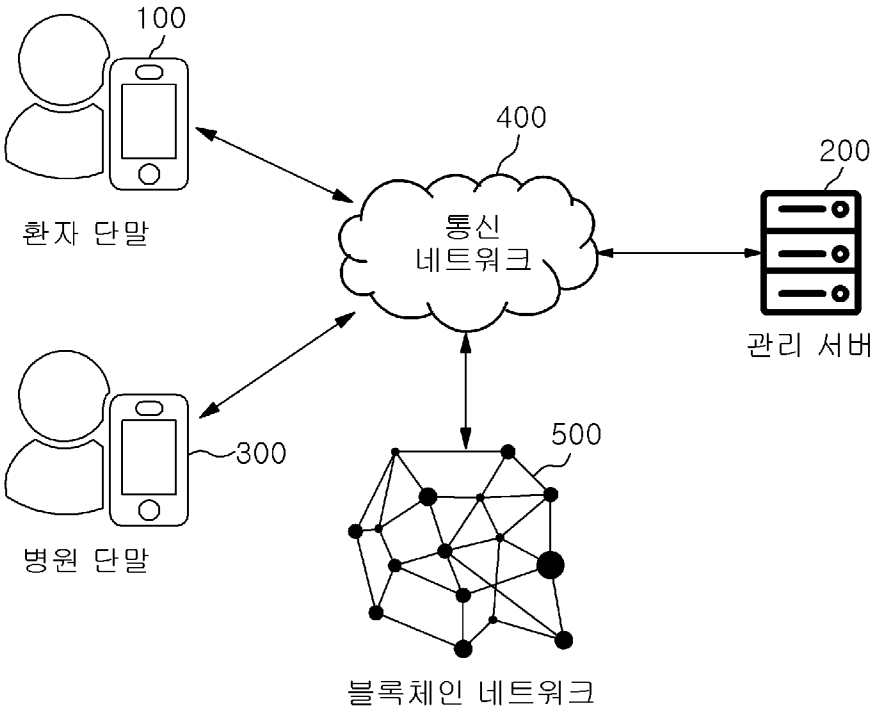
[청구항 7] 제5 항에 있어서,
상기 환자 단말 및 상기 병원 단말은 상기 서버에 의하여 탈중앙화 신원 정보(Decentralized Identifier, DID)가 관리되는,
방법.

[청구항 8] 제5 항에 있어서,
상기 환자 단말과 상기 병원 단말 간 상기 의료 데이터의 전송의 보안과 관련하여,
공유 키 생성을 위해 ECIES(Elliptic Curve Integrated Encryption Scheme) 및 ECDH(Elliptic Curve Diffie-Hellman)를 사용하여 상기 환자 단말과 상기 병원 단말 간 개인 키를 공유하지 않고도 데이터 암호화 및 복호화가 수행되고,
데이터 무결성과 기밀성을 보장하기 위해 상기 환자 단말과 상기 병원 단말 간 상기 의료 데이터의 전송 전에 상기 의료 데이터를 암호화하기 위한 AES-GCM(Advanced Encryption Standard Galois/Counter Mode)가 수행되는,
방법.

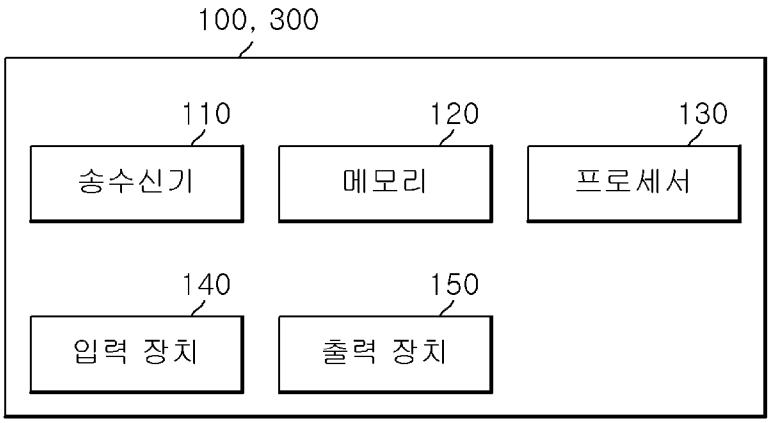
[청구항 9] 통신 시스템에서 서버에 있어서,
송수신기;
메모리; 및
프로세서를 포함하고,
상기 프로세서는 제1 항 내지 제4 항 중 어느 한 항의 방법을 수행하도록 구성된,
서버.

[청구항 10] 통신 시스템에서 환자 단말에 있어서,
송수신기;
메모리; 및
프로세서를 포함하고,
상기 프로세서는 제5 항 내지 제8 항 중 어느 한 항의 방법을 수행하도록 구성된,
환자 단말.

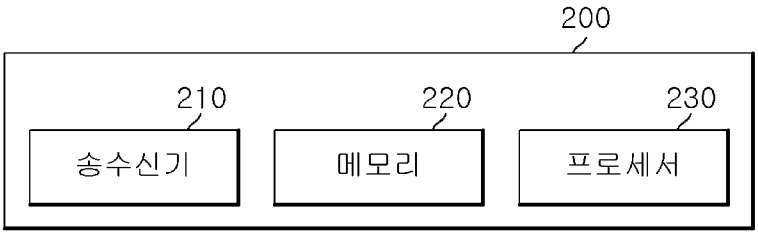
[도1]


100
환자 단말
400
통신
네트워크
200
관리 서버
300
병원 단말
500
블록체인 네트워크

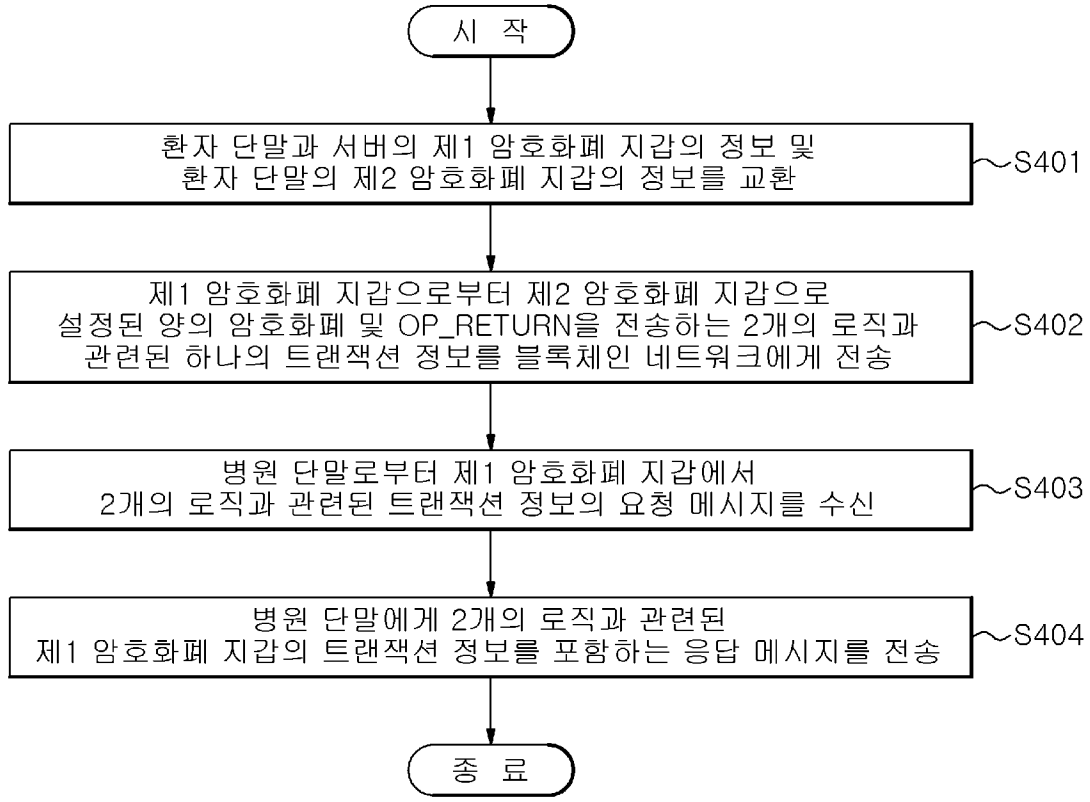
[도2]


100, 300
110
송수신기
120
메모리
130
프로세서
140
입력 장치
150
출력 장치

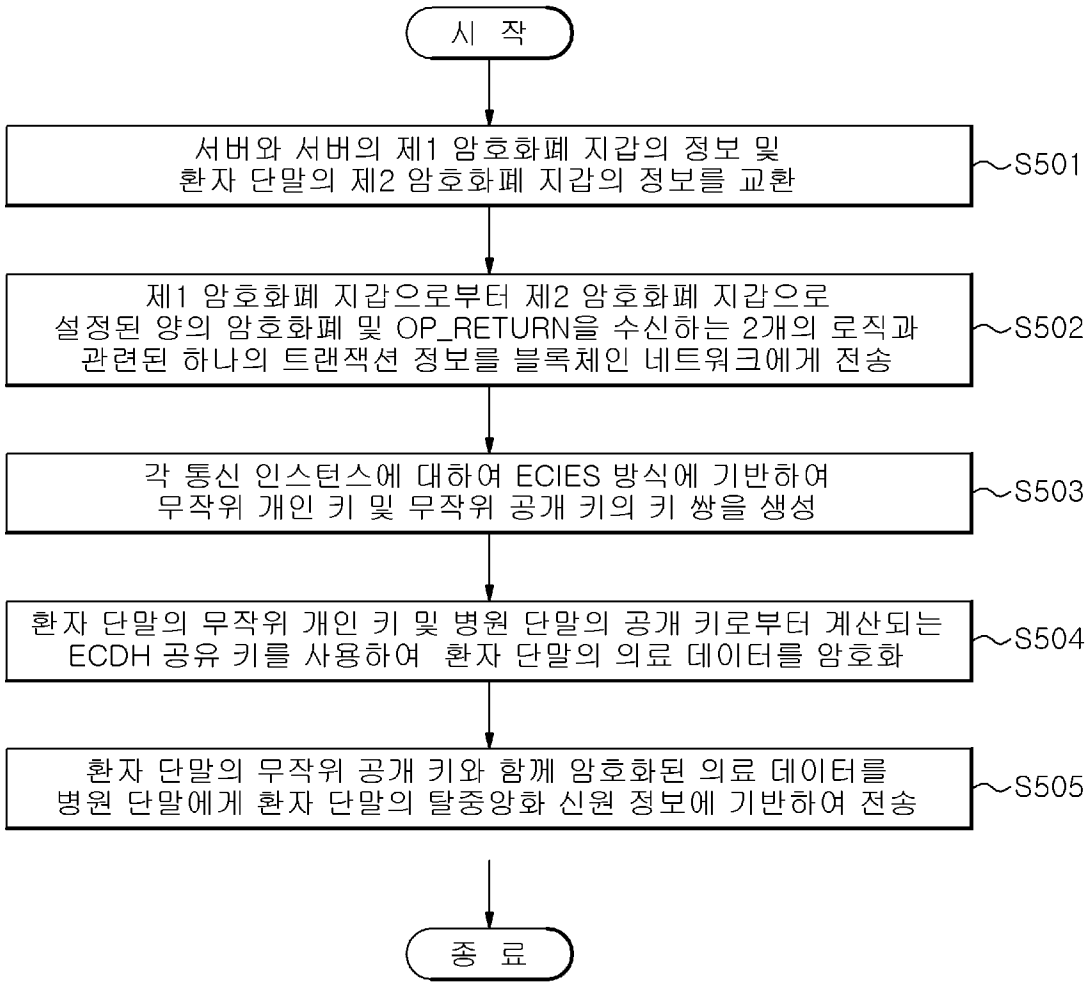
[도3]


200
210
송수신기
220
메모리
230
프로세서

[도4]


시 작
환자 단말과 서버의 제1 암호화폐 지갑의 정보 및
환자 단말의 제2 암호화폐 지갑의 정보를 교환
S401
제1 암호화폐 지갑으로부터 제2 암호화폐 지갑으로
설정된 양의 암호화폐 및 OP_RETURN을 전송하는 2개의 로직과
관련된 하나의 트랜잭션 정보를 블록체인 네트워크에게 전송
S402
병원 단말로부터 제1 암호화폐 지갑에서
2개의 로직과 관련된 트랜잭션 정보의 요청 메시지를 수신
S403
병원 단말에게 2개의 로직과 관련된
제1 암호화폐 지갑의 트랜잭션 정보를 포함하는 응답 메시지를 전송
S404
종 료

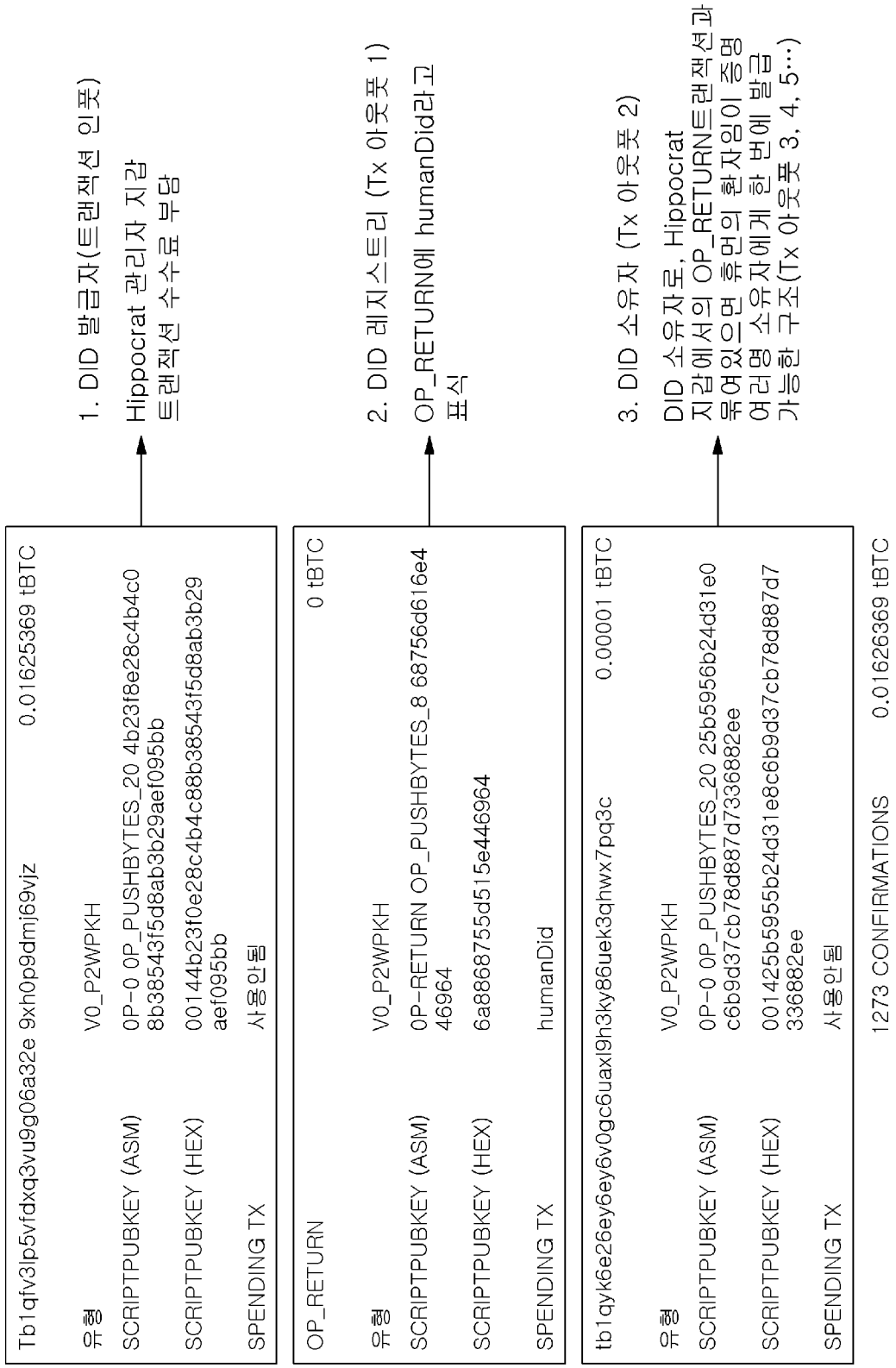
[도5]


시 작
서버와 서버의 제1 암호화폐 지갑의 정보 및
환자 단말의 제2 암호화폐 지갑의 정보를 교환
S501
제1 암호화폐 지갑으로부터 제2 암호화폐 지갑으로
설정된 양의 암호화폐 및 OP_RETURN을 수신하는 2개의 로직과
관련된 하나의 트랜잭션 정보를 블록체인 네트워크에게 전송
S502
각 통신 인스턴스에 대하여 ECIES 방식에 기반하여
무작위 개인 키 및 무작위 공개 키의 키 쌍을 생성
S503
환자 단말의 무작위 개인 키 및 병원 단말의 공개 키로부터 계산되는
ECDH 공유 키를 사용하여 환자 단말의 의료 데이터를 암호화
S504
환자 단말의 무작위 공개 키와 함께 암호화된 의료 데이터를
병원 단말에게 환자 단말의 탈중앙화 신원 정보에 기반하여 전송
S505
종 료

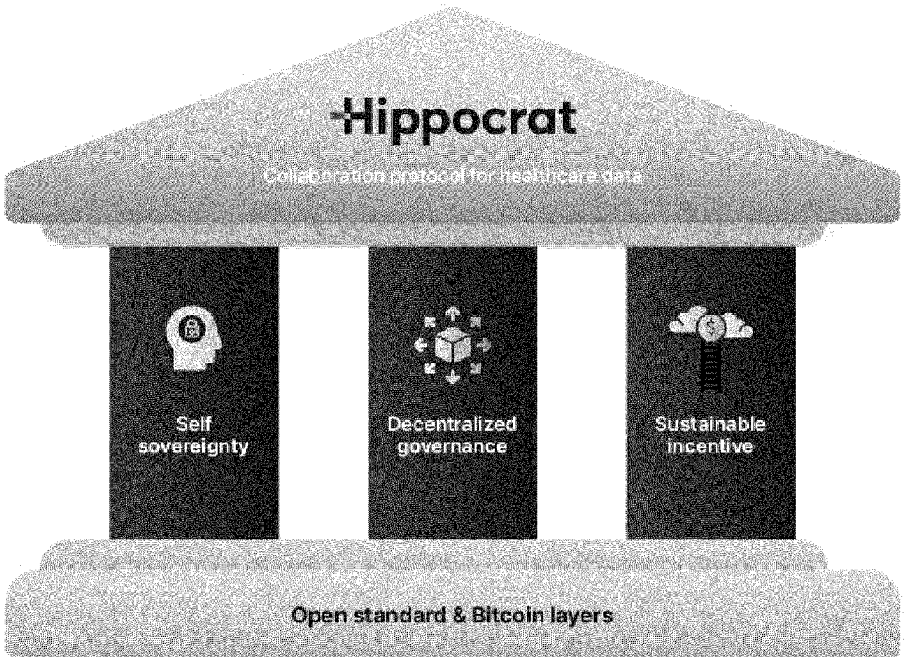
[도6]


```
"@Context" : "http://w3id.org/did-resolution/v1",
"didDocument" : {
  "id" : "did:ion:EiCawIuzvfHIW-mPt8mk1NmJGnJILgzrjJ3YYy3VtcDLw",
  "@context" : [
    "http://www.w3.org/ns/did/v1",
    {
  ],
  "service" : [
    {
      "id" : "#tb1qyk6e26ey6v0qc6uax19h3ky86uek3qhwx7pq3c",
      "type" : "humanscape admin willet",
      "serviceEndpoint" : "https://blockstream.info/testnet/address/tb1qsww2x6w2mjmdfv31cr6gxzxfalykrxxsqprpp7"
    },
    {
      "id" : "tb1qsww2x6w2mjmdfv31cr6gxzxfalykrxxsqprpp7",
      "type" : "humanscape admin wallet",
      "serviceEndpoint" : "https://blockstream.info/testnet/address/tb1qyk6e26ey6v0qc6uax19h3ky86uek3qhwx7pq3c"
    },
    {
      "id" : "#humanscape0patient0id",
      "type" : "humanscape patient data",
      "serviceEndpoint" : "https://ipfs.io/ipfs/bafybeialzikkahbkmyjegm5tgus3m4izqntr647pf7uqvhglossdop5fau"
    }
  ],
```

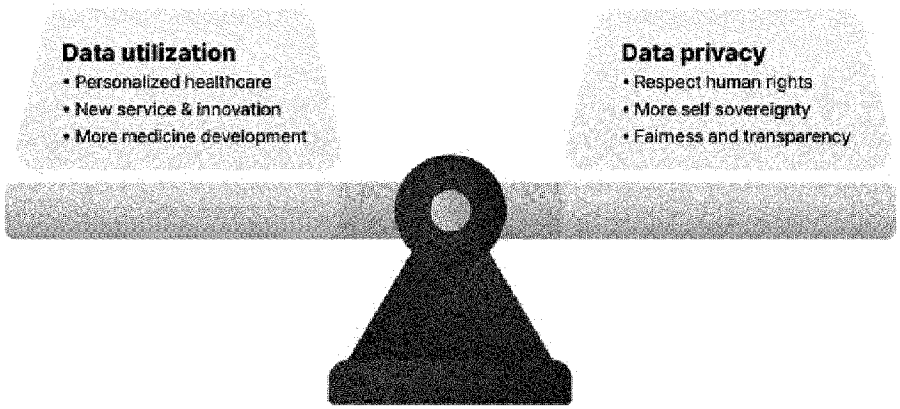
[도7]


Tb1qfv3lp5vfdxq3vu9g06a32e 9xh0p9dmj69vjz 0.01625369 tBTC
유형 V0_P2WPKH
SCRIPTPUBKEY (ASM) 0P-0 0P_PUSHBYTES_20 4b23f8e28c4b4c0 8b38543f5d8ab3b29aef095bb
SCRIPTPUBKEY (HEX) 00144b23f0e28c4b4c88b38543f5d8ab3b29 aef095bb
SPENDING TX 사용안됨
1. DID 발급자(트랜잭션 인풋)
Hippocrat 관리자 지갑
트랜잭션 수수료 부담
OP_RETURN 0 tBTC
유형 V0_P2WPKH
SCRIPTPUBKEY (ASM) 0P-RETURN OP_PUSHBYTES_8 68756d616e4 46964
SCRIPTPUBKEY (HEX) 6a8868755d515e446964
SPENDING TX humanDid
2. DID 레지스트리 (Tx 아웃풋 1)
OP_RETURN에 humanDid라고
표식
tb1qyk6e26ey6ey6v0gc6uaxl9h3ky86uek3qhwx7pq3c 0.00001 tBTC
유형 V0_P2WPKH
SCRIPTPUBKEY (ASM) 0P-0 0P_PUSHBYTES_20 25b5956b24d31e0 c6b9d37cb78d887d7336882ee
SCRIPTPUBKEY (HEX) 001425b5955b24d31e8c6b9d37cb78d887d7 336882ee
SPENDING TX 사용안됨
3. DID 소유자 (Tx 아웃풋 2)
DID 소유자로, Hippocrat
지갑에서의 OP_RETURN트랜잭션과
묶여있으면 휴먼의 환자임이 증명
여러명 소유자에게 한 번에 발급
가능한 구조(Tx 아웃풋 3, 4, 5…)
1273 CONFIRMATIONS 0.01626369 tBTC

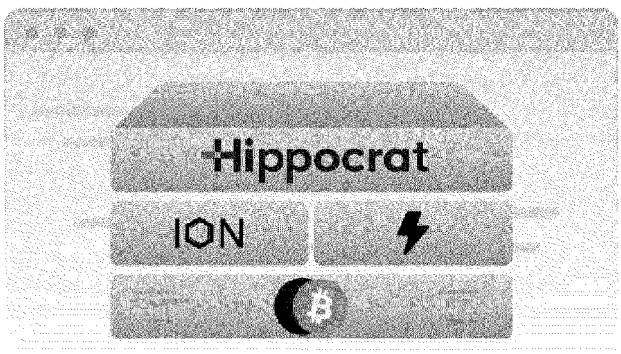
[도8]


Hippocrat
Collaboration protocol for healthcare data
Self sovereignty
Decentralized governance
Sustainable incentive
Open standard & Bitcoin layers

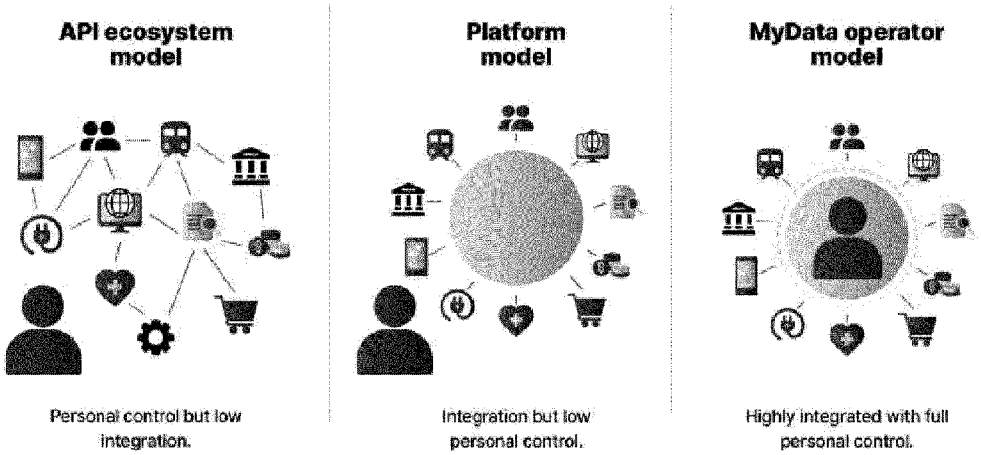
[도9]


Data utilization
• Personalized healthcare
• New service & innovation
• More medicine development
Data privacy
• Respect human rights
• More self sovereignty
• Fairness and transparency

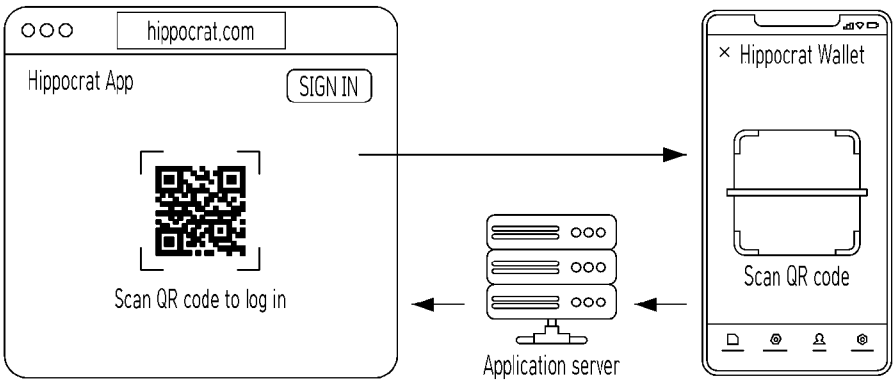
[도10]


Hippocrat
ION

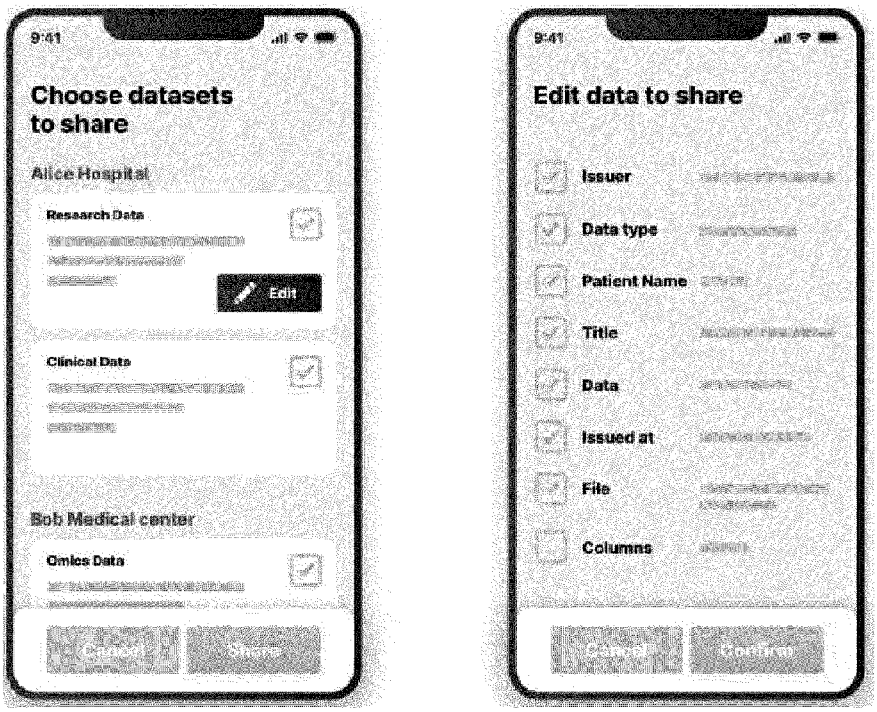
[도11]


API ecosystem model
Platform model
MyData operator model
Personal control but low integration.
Integration but low personal control.
Highly integrated with full personal control.

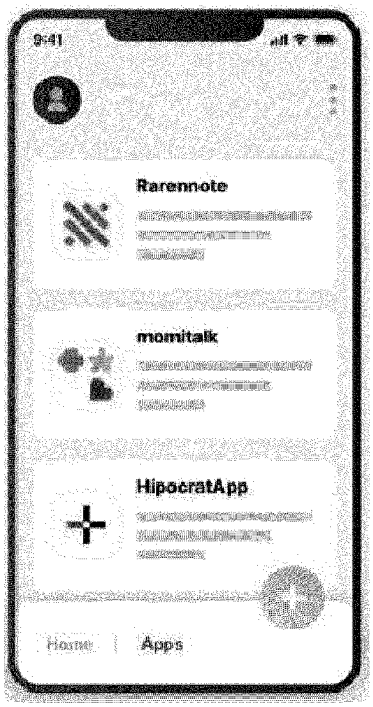
[도12]


hippocrat.com
Hippocrat App
SIGN IN
Scan QR code to log in
Application server
Hippocrat Wallet
Scan QR code

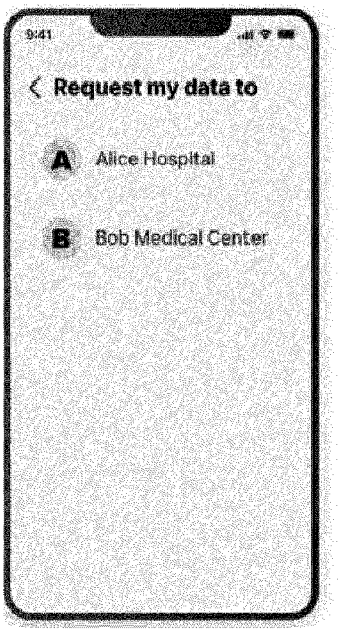
[도13]

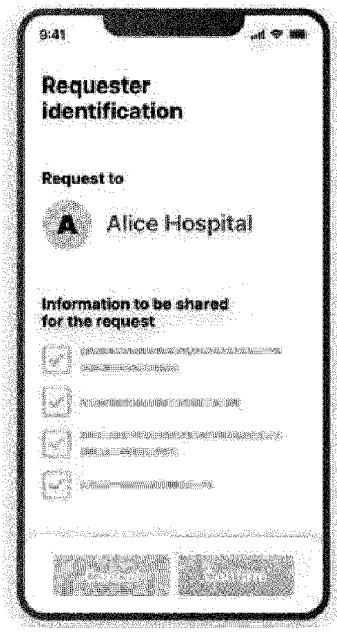

9:41
Choose datasets to share
Alice Hospital
Research Data
Edit
Clinical Data
Bob Medical center
Omics Data
Cancel
Share
9:41
Edit data to share
Issuer
Data type
Patient Name
Title
Data
Issued at
File
Columns
Cancel
Continue

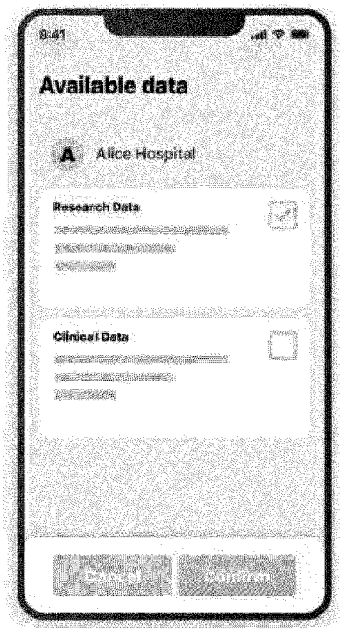
[도14]


9:41
Rarenote
momitalk
HipocratApp
Home
Apps

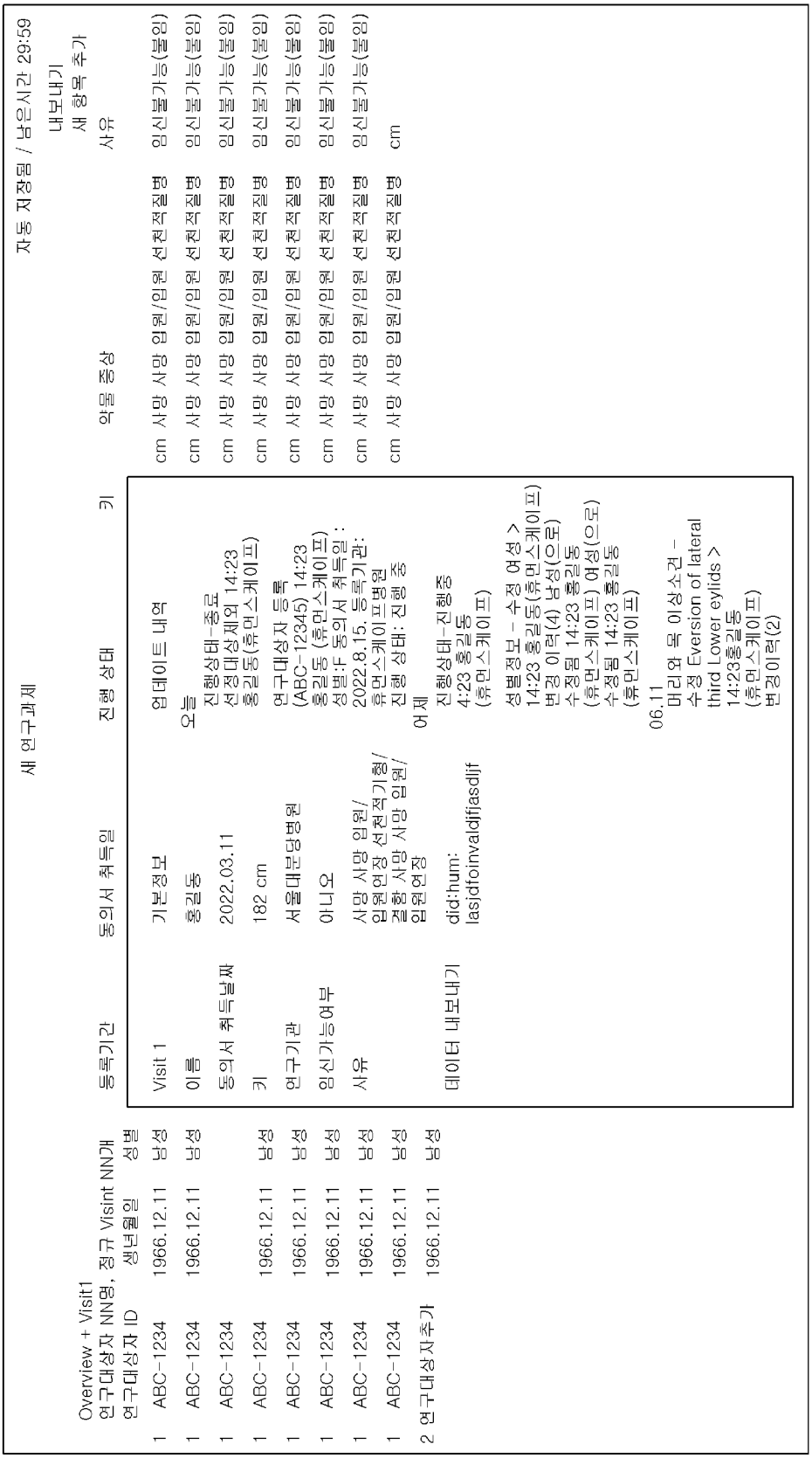
[도15]


9:41
Request my data to
A Alice Hospital
B Bob Medical Center

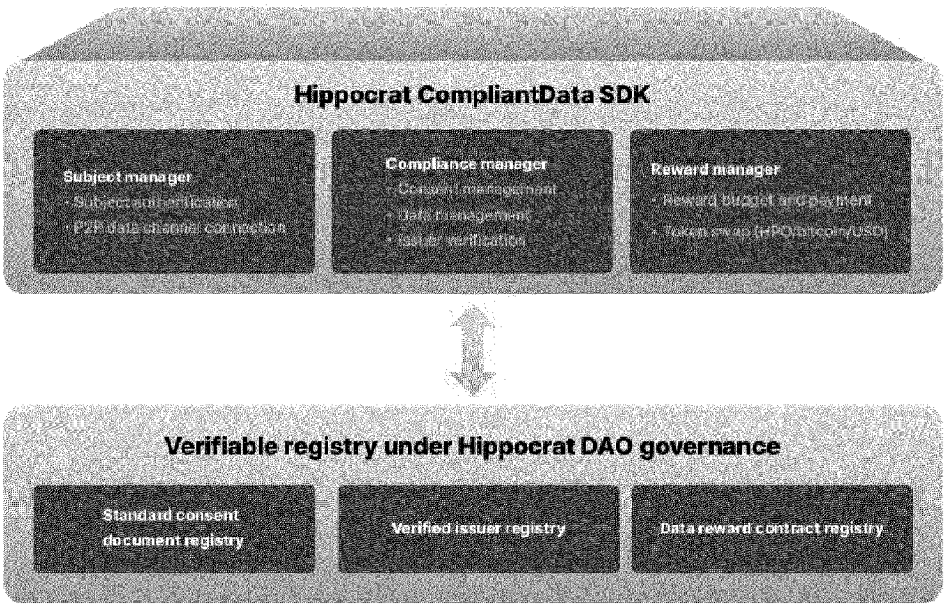

9:41
Requester identification
Request to
A Alice Hospital
Information to be shared for the request


9:41
Available data
A Alice Hospital
Research Data
Clinical Data

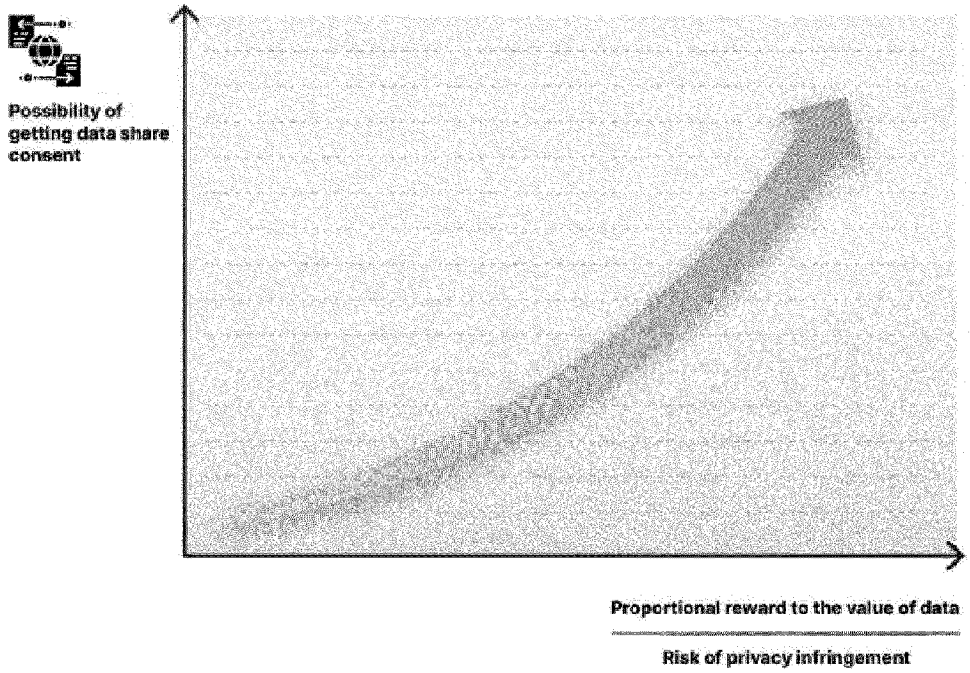
[도16]


새 연구과제
자동 저장됨 / 남은시간 29:59
내보내기
새 항목 추가
Overview + Visit1
연구대상자 NN명, 정규 Visint NN개
연구대상자 ID
생년월일
성별
등록기간
동의서 취득일
진행 상태
키
약물 증상
사유
1 ABC-1234 1966.12.11 남성
1 ABC-1234 1966.12.11 남성
1 ABC-1234
1 ABC-1234 1966.12.11 남성
1 ABC-1234 1966.12.11 남성
1 ABC-1234 1966.12.11 남성
1 ABC-1234 1966.12.11 남성
1 ABC-1234 1966.12.11 남성
2 연구대상자추가 1966.12.11 남성
Visit 1
이름
동의서 취득날짜
키
연구기관
임신가능여부
사유
데이터 내보내기
기본정보
홍길동
2022.03.11
182 cm
서울대분당병원
아니오
사망 사망 입원/
입원연장 선천적기형/
질환 사망 사망 입원/
입원연장
did:hum:
lasjdfoinvaldjfjasdljf
업데이트 내역
오늘
진행상태-종료
선정대상제외 14:23
홍길동(휴먼스케이프)
연구대상자 등록
(ABC-12345) 14:23
홍길동 (휴먼스케이프)
성별:F 동의서 취득일 :
2022.8.15. 등록기관:
휴먼스케이프병원
진행 상태: 진행 중
어제
진행상태-진행중
4:23 홍길동
(휴먼스케이프)
성별정보 - 수정 여성 >
14:23 홍길동(휴먼스케이프)
변경 이력(4) 남성(으로)
수정됨 14:23 홍길동
(휴먼스케이프) 여성(으로)
수정됨 14:23 홍길동
(휴먼스케이프)
06.11
머리와 목 이상소견 -
수정 Eversion of lateral
third Lower eylids >
14:23홍길동
(휴먼스케이프)
변경이력(2)
cm 사망 사망 입원/입원 선천적질병 임신불가능(불임)
cm 사망 사망 입원/입원 선천적질병 임신불가능(불임)
cm 사망 사망 입원/입원 선천적질병 임신불가능(불임)
cm 사망 사망 입원/입원 선천적질병 임신불가능(불임)
cm 사망 사망 입원/입원 선천적질병 임신불가능(불임)
cm 사망 사망 입원/입원 선천적질병 임신불가능(불임)
cm 사망 사망 입원/입원 선천적질병 임신불가능(불임)
cm 사망 사망 입원/입원 선천적질병 임신불가능(불임)
cm 사망 사망 입원/입원 선천적질병 cm

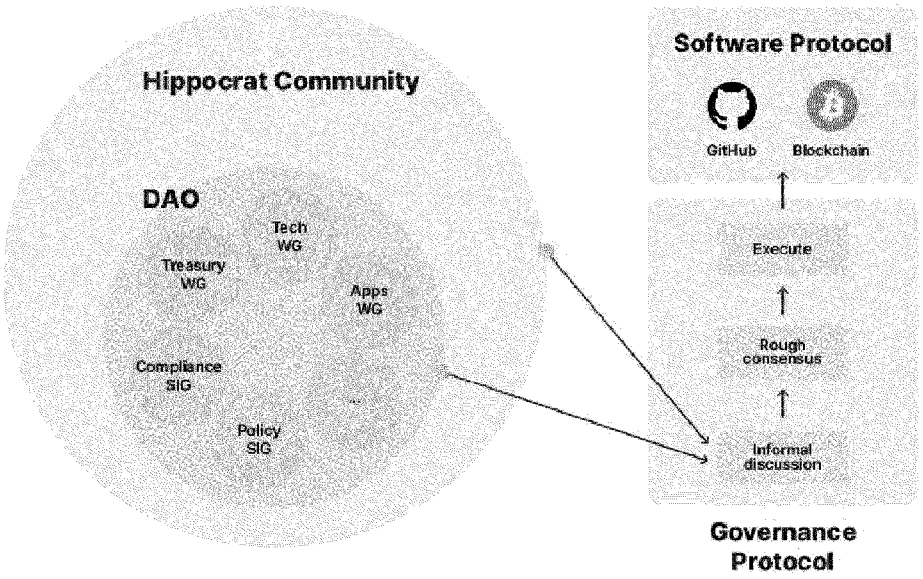
[도17]


Hippocrat CompliantData SDK
Subject manager
Compliance manager
Reward manager
Verifiable registry under Hippocrat DAO governance
Standard consent document registry
Verified issuer registry
Data reward contract registry

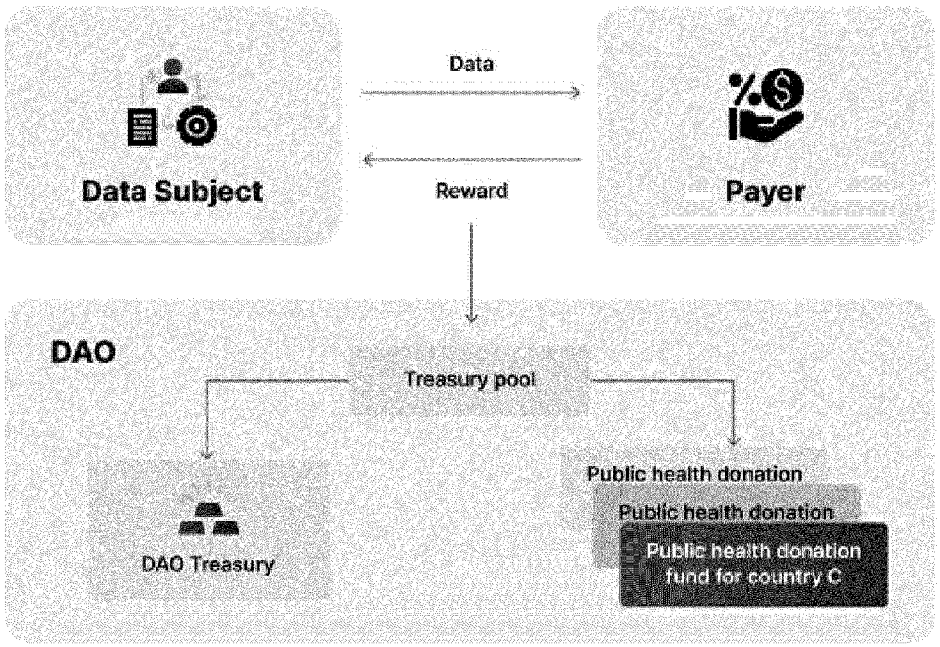
[도18]


Possibility of getting data share consent
Proportional reward to the value of data
Risk of privacy infringement

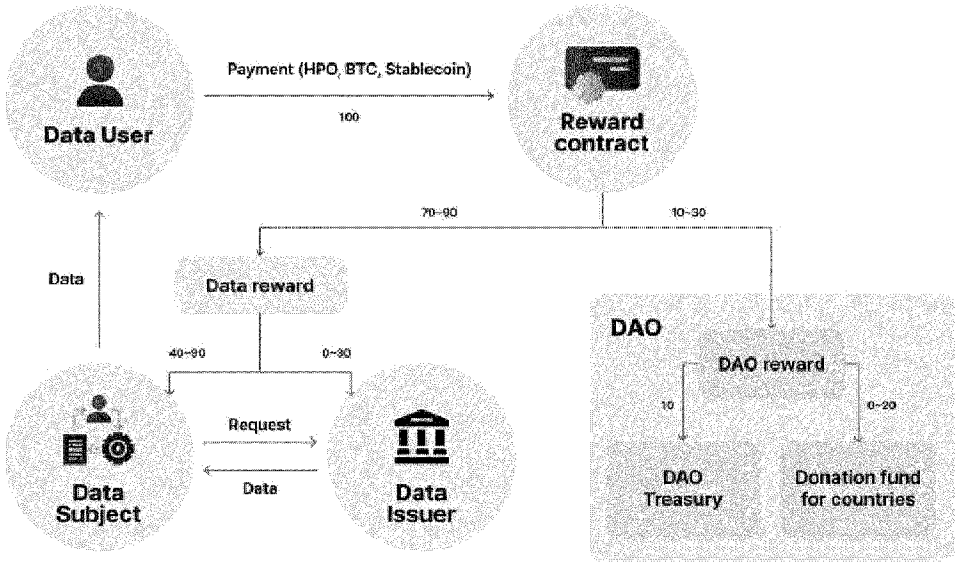
[도19]


Hippocrat Community
DAO
Tech WG
Treasury WG
Apps WG
Compliance SIG
Policy SIG
Software Protocol
GitHub
Blockchain
Execute
Rough consensus
Informal discussion
Governance Protocol

[도20]


Data Subject
Data
Reward
Payer
DAO
Treasury pool
DAO Treasury
Public health donation
Public health donation
Public health donation fund for country C

[도21]


Data User
Payment (HPO, BTC, Stablecoin)
100
Reward contract
70~90
10~30
Data
Data reward
DAO
DAO reward
40~90
0~30
10
0~20
Request
Data
Data Subject
Data Issuer
DAO Treasury
Donation fund for countries

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2023/019610

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/31(2013.01)i; **G06F 21/44**(2013.01)i; **G06Q 20/36**(2012.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/31(2013.01); G06F 21/60(2013.01); G06F 21/72(2013.01); H04L 29/06(2006.01); H04L 9/06(2006.01); H04L 9/32(2006.01)

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

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

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

eKOMPASS (KIPO internal) & keywords: 블록 체인(blockchain), 보안(security), 의료(medical), 거래(transaction), 서버(server), 환자(patient), 암호화폐(cryptocurrency), 지갑(wallet), OP_RETURN, 로직(logic), 병원(hospital), 탈중앙화 신원 정보(Decentralized Identifier, DID), 주소(address), 응답(response), 메시지(message), 유효함(validity), 서명(signature), ECIES(Elliptic Curve Integrated Encryption Scheme), 무작위(random), ECDH(Elliptic Curve Diffie-Hellman), 개인 키(private key), 공개 키(public key), 공유 키(shared key)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2021-0344507 A1 (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 04 November 2021 (2021-11-04) See paragraphs [0111]-[0175]; and figures 3-5.	1-10
A	US 2019-0213333 A1 (ALAN HEALTH AND SCIENCE D/B/A ONPACEPLUS) 11 July 2019 (2019-07-11) See paragraphs [0012], [0026], [0031]-[0034], [0037] and [0047]; claims 1-2; and figures 1-7.	1-10
A	KR 10-2022-0006097 A (NCHAIN HOLDINGS LIMITED) 14 January 2022 (2022-01-14) See paragraphs [0034]-[0044]; claims 1-3; and figure 2.	1-10
A	KR 10-2020-0140916 A (AMAZON TECHNOLOGIES, INC.) 16 December 2020 (2020-12-16) See paragraphs [0122]-[0124].	1-10

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
05 March 2024	**05 March 2024**

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2023/019610

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-1799343 B1 (COINPLUG, INC.) 22 November 2017 (2017-11-22) See paragraphs [0063], [0067], [0071] and [0088]-[0089]; and claims 1 and 3.	1-10

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2023/019610

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2021-0344507 A1	04 November 2021	CN 111527489 A	11 August 2020
		EP 3799684 A2	07 April 2021
		EP 3799684 A4	09 June 2021
		SG 11202013204 A	28 January 2021
		US 11063770 B1	13 July 2021
		US 11271754 B2	08 March 2022
		WO 2020-098845 A2	22 May 2020
		WO 2020-098845 A3	21 January 2021
US 2019-0213333 A1	11 July 2019	CN 111201605 A	26 May 2020
		CN 111201605 B	03 August 2021
		JP 2020-537345 A	17 December 2020
		JP 7060683 B2	26 April 2022
		TW 201926665 A	01 July 2019
		TW I754105 B	01 February 2022
		US 10903258 B2	26 January 2021
		US 11055419 B2	06 July 2021
		US 2019-0109163 A1	11 April 2019
		WO 2019-075152 A1	18 April 2019
KR 10-2022-0006097 A	14 January 2022	CN 113950801 A	18 January 2022
		EP 3966997 A1	16 March 2022
		EP 3966997 B1	07 February 2024
		GB 2583767 A	11 November 2020
		JP 2022-532578 A	15 July 2022
		SG 11202112441 A	30 December 2021
		US 2022-0094542 A1	24 March 2022
		WO 2020-229947 A1	19 November 2020
KR 10-2020-0140916 A	16 December 2020	CA 3098836 A1	07 November 2019
		CA 3098836 C	05 September 2023
		CN 112470425 A	09 March 2021
		CN 112470425 B	10 June 2022
		EP 3788741 A1	10 March 2021
		JP 2021-521718 A	26 August 2021
		JP 7205031 B2	17 January 2023
		KR 10-2229739 B1	22 March 2021
		US 10909250 B2	02 February 2021
		US 2019-0342079 A1	07 November 2019
		WO 2019-212773 A1	07 November 2019
KR 10-1799343 B1	22 November 2017	US 11568396 B2	31 January 2023
		US 2017-0330180 A1	16 November 2017

국 제 조 사 보 고 서

국제출원번호
PCT/KR2023/019610

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 21/31(2013.01)i; **G06F 21/44**(2013.01)i; **G06Q 20/36**(2012.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06F 21/31(2013.01); G06F 21/60(2013.01); G06F 21/72(2013.01); H04L 29/06(2006.01); H04L 9/06(2006.01); H04L 9/32(2006.01)

조사된 기술분야에 속하는 최소문헌 이외의 문헌

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

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

eKOMPASS(특허청 내부 검색시스템) & 키워드: 블록 체인(blockchain), 보안(security), 의료(medical), 거래(transaction), 서버(server), 환자(patient), 암호화폐(cryptocurrency), 지갑(wallet), OP_RETURN, 로직(logic), 병원(hospital), 탈중앙화 신원 정보(Decentralized Identifier, DID), 주소(address), 응답(response), 메시지(message), 유효함(validity), 서명(signature), ECIES(Elliptic Curve Integrated Encryption Scheme), 무작위(random), ECDH(Elliptic Curve Diffie-Hellman), 개인 키(private key), 공개 키(public key), 공유 키(shared key)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	US 2021-0344507 A1 (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 2021.11.04 단락 [0111]-[0175]; 및 도면 3-5	1-10
A	US 2019-0213333 A1 (ALAN HEALTH AND SCIENCE D/B/A ONPACEPLUS) 2019.07.11 단락 [0012], [0026], [0031]-[0034], [0037], [0047]; 청구항 1-2; 및 도면 1-7	1-10
A	KR 10-2022-0006097 A (엔체인 홀딩스 리미티드) 2022.01.14 단락 [0034]-[0044]; 청구항 1-3; 및 도면 2	1-10
A	KR 10-2020-0140916 A (아마존 테크놀로지스, 인크.) 2020.12.16 단락 [0122]-[0124]	1-10

☑ 추가 문헌이 C(계속)에 기재되어 있습니다.

☑ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

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

국제조사의 실제 완료일	국제조사보고서 발송일
2024년03월05일(05.03.2024)	**2024년03월05일(05.03.2024)**

ISA/KR의 명칭 및 우편주소

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

팩스 번호 **+82-42-481-8578**

심사관

양정록

전화번호 **+82-42-481-5709**

국 제 조 사 보 고 서

국제출원번호
PCT/KR2023/019610

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-1799343 B1 (주식회사 코인플러그) 2017.11.22 단락 [0063], [0067], [0071], [0088]-[0089]; 및 청구항 1, 3	1-10

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2023/019610

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 2021-0344507 A1	2021/11/04	CN 111527489 A	2020/08/11
		EP 3799684 A2	2021/04/07
		EP 3799684 A4	2021/06/09
		SG 11202013204 A	2021/01/28
		US 11063770 B1	2021/07/13
		US 11271754 B2	2022/03/08
		WO 2020-098845 A2	2020/05/22
		WO 2020-098845 A3	2021/01/21
US 2019-0213333 A1	2019/07/11	CN 111201605 A	2020/05/26
		CN 111201605 B	2021/08/03
		JP 2020-537345 A	2020/12/17
		JP 7060683 B2	2022/04/26
		TW 201926665 A	2019/07/01
		TW I754105 B	2022/02/01
		US 10903258 B2	2021/01/26
		US 11055419 B2	2021/07/06
		US 2019-0109163 A1	2019/04/11
		WO 2019-075152 A1	2019/04/18
KR 10-2022-0006097 A	2022/01/14	CN 113950801 A	2022/01/18
		EP 3966997 A1	2022/03/16
		EP 3966997 B1	2024/02/07
		GB 2583767 A	2020/11/11
		JP 2022-532578 A	2022/07/15
		SG 11202112441 A	2021/12/30
		US 2022-0094542 A1	2022/03/24
		WO 2020-229947 A1	2020/11/19
KR 10-2020-0140916 A	2020/12/16	CA 3098836 A1	2019/11/07
		CA 3098836 C	2023/09/05
		CN 112470425 A	2021/03/09
		CN 112470425 B	2022/06/10
		EP 3788741 A1	2021/03/10
		JP 2021-521718 A	2021/08/26
		JP 7205031 B2	2023/01/17
		KR 10-2229739 B1	2021/03/22
		US 10909250 B2	2021/02/02
		US 2019-0342079 A1	2019/11/07
		WO 2019-212773 A1	2019/11/07
KR 10-1799343 B1	2017/11/22	US 11568396 B2	2023/01/31
		US 2017-0330180 A1	2017/11/16