【서지사항】

【서류명】 특허출원서

【출원구분】 특허출원

【출원인】

【성명】 장우영

【특허고객번호】 4-2024-072963-6

【발명의 국문명칭】 블록체인을 기반으로한 구매 영수증 관리 시스템 및 그 방법

【발명의 영문명칭】 BLOCKCHAIN-BASED PURCHASE RECEIPT MANAGEMENT SYSTEM AND METHOD

【발명자】

【성명】 장우영

【특허고객번호】 4-2024-072963-6

【발명자】

【성명】 임현성

【특허고객번호】 4-2024-074376-7

【발명자】

【성명】 한수연

【특허고객번호】 4-2024-074481-1

【발명자】

【성명】 SHURENGEREL SERGELEN

【특허고객번호】 6-2024-079036-9

【출원언어】 국어

【우선권 주장】

【출원국명】 KR

【출원번호】 10-2024-0149101

【출원일자】 2024.10.28

【증명서류】 우선권증명서류의 전자적 교환에 의한 첨부생략

【심사청구】 청구

【기술이전희망】

【양도】 희망

【전용 실시권】 희망

【통상 실시권】 희망

【개인정보 제공동의】 동의

【기술이전 대가】 유상

【취지】 위와 같이 특허청장에게 제출합니다.

출원인 장우영 (서명 또는 인)

【수수료】

【출원료】	0	면	46,000 원
【가산출원료】	33	면	0 원
【우선권주장료】	1	건	18,000 원
【심사청구료】	8	항	574,000 원

【합계】 638,000원

【감면사유】 개인(70%감면)[1]

【감면후 수수료】 204,000 원

【발명의 설명】

【발명의 명칭】

블록체인을 기반으로한 구매 영수증 관리 시스템 및 그 방법{BLOCKCHAIN-BASED PURCHASE RECEIPT MANAGEMENT SYSTEM AND METHOD}

【기술분야】

【0001】 본 발명은 블록체인 기술과 대체 불가능한 토큰(NFT) 시스템을 활용하여 소비자의 물품 소유권을 디지털화하고, 이를 안전하게 관리함으로써 소유권 증명, A/S 요청, 보험 청구, 중고 거래 등에서 신뢰성과 효율성을 제공할 수 있는 블록체인을 기반으로 한 구매 영수증 관리 시스템 및 그 방법에 관한 것이다.

【발명의 배경이 되는 기술】

【0002】 기존의 구매 영수증 관리 방식은 종이 영수증이나 디지털 파일 형태로 구매 내역을 저장하지만, 분실, 훼손, 위·변조의 위험이 크다는 한계가 있다. 특히, 종이 영수증은 시간이 지나면서 보관이 어려워지고, 디지털 파일 또한 관리 및 신뢰성 측면에서 한계를 드러낸다. 이러한 문제로 인해 구매 영수증을 증빙 자료로 활용하기 어려워, 소비자와 서비스 제공자 간의 신뢰를 저해한다.

【0003】 또한, 현재의 시스템은 구매 기록과 제품의 소유권 정보를 연결하지 않기 때문에, 중고 거래나 분쟁 상황에서 소유권을 명확히 증명하기 어렵다. 이러한 한계는 제품 소유권 증명의 부재로 이어지며, 중고 거래 시장에서 사기나 분쟁이 발생하는 주요 원인으로 작용한다. 결과적으로, 거래의 안전성과 신뢰성이 크게

저하되는 문제가 발생한다.

【0004】 더욱이, 중고 거래 시장에서는 제품의 진위 여부와 소유권 이력을 확인할 신뢰할 만한 수단이 부족하다. 이로 인해 거래 과정에서 사기와 분쟁의 위험이 증가하며, 이는 소비자와 판매자 모두에게 불편과 손해를 초래한다.

【0005】 또한, 보험 청구나 A/S 요청 과정에서도 구매 증빙 자료를 효율적으로 제출하기 어렵고, 구매 기록이 분실되거나 훼손되면 소비자는 정당한 권리를 주장하기 어려운 상황에 직면하게 되므로 이로 인해 불필요한 갈등이 발생할 수 있다.

【0006】 위와 같은 문제를 해결하기 위해 최근 블록체인 기술이 도입되고 있지만, 이 역시 근본적인 한계를 가진다. 블록체인 지갑의 경우 사용자가 개인키(Private Key)를 직접 관리해야 하며, 이를 분실하거나 유출할 경우 복구가 불가능하다. 이는 사용자가 키 관리에 대한 부담을 느끼게 하고, 실수로 자산을 잃는 사례를 유발하며, 결과적으로 블록체인 기술의 대중화를 저해하는 요인으로 작용한다.

【0007】 또한, 블록체인 지갑 사용에는 기술적 진입장벽이 높다. 지갑 생성 및 관리를 위한 기본 지식이 부족한 사용자들은 복잡한 인터페이스와 네트워크 지연, 거래 수수료 등의 문제로 불편함을 느낀다. 특히, 다수의 블록체인 네트워크와 연동될 경우 각 네트워크의 상이한 규칙과 관리 방식으로 인해 사용이 더욱 어려워지며, 이는 일반 사용자들에게 큰 부담으로 작용한다.

【0008】 따라서, 종이 영수증 및 디지털 파일 기반의 기존 구매 영수증 관리 방식과 블록체인 지갑 관리의 문제점을 해결할 새로운 시스템이 필요하다. 구매 물품의 소유권을 명확히 증명하고 거래의 투명성을 보장하며, 블록체인 지갑 관리 기능을 사용자 친화적으로 개선함으로써, 소비자와 서비스 제공자 모두에게 신뢰할 수 있는 솔루션을 제공해야 할 필요성이 있다.

【선행기술문헌】

【특허문헌】

【0009】**(특허문헌 0001)** 공개특허공보 제2023-0112290호

(특허문헌 0002) 등록특허공보 제10-2044747호

【발명의 내용】

【해결하고자 하는 과제】

【0010】 본 발명의 목적은, 상술한 문제점을 해결할 수 있는 블록체인을 기반으로 한 구매 영수증 관리 시스템 및 그 방법을 제공함에 있다.

【0011】 먼저, 기존의 구매 영수증 관리 방식의 문제점을 극복하고 구매 영수증을 블록체인을 기반으로 관리하여 구매 영수증의 분실, 훼손, 위·변조의 위험이 줄일 수 있도록 하는 것을 일 목적으로 한다.

【0012】 또한, 블록체인 지갑 관리의 어려움을 개선함으로써 구매 물품의 소유권을 명확히 하여 거래의 투명성을 보장하고, 블록체인 지갑관리 기능을 사용자

가 쉽게 접근하여 사용할 수 있도록 하는 것을 또 다른 목적으로 한다.

【과제의 해결 수단】

【0013】 상기 목적을 달성하기 위해, 본 발명에 따른 블록체인을 기반으로 한 구매 영수증 관리 시스템(10)은 사용자의 SNS 계정을 인증하는 SNS 연동모듈, SNS 계정 정보를 기반으로 접근 권한을 확인하는 계정연동모듈, 상기 사용자의 접근 권한에 따라 블록체인 네트워크 상에 배포된 NFT형태의 영수증에 관한 소유권 이전 및 구매 기록을 관리하는 스마트 컨트랙트 처리모듈을 포함할 수 있다.

【0014】 또한, 스마트 컨트랙트 처리모듈은 구매 거래 조건을 코드화하여, 거래 조건이 충족되었을 때 영수증의 소유권을 자동으로 이전할 수도 있다.

【0015】 또한, 스마트 컨트랙트 처리모듈은 사용자가 업로드한 종이 형태의 구매 영수증 이미지를 NFT 형태의 데이터로 변환할 수도 있고, NFT 형태의 데이터로 변환하는 과정에서 OCR 기능을 적용할 수도 있다.

【0016】 또한, 본 발명에 따른 블록체인을 기반으로 한 구매 영수증 관리 시스템(10)은 보안 강화를 위해 사용자 또는 시스템이 설정한 시간 동안만 블록체인 지갑의 특정된 작업에만 제한적으로 사용할 수 있도록 하는 임시키를 생성하여 임시키 발행모듈을 더 포함할 수 있다.

【0017】 다음으로 본 발명에 따른 블록체인을 기반으로 한 구매 영수증 관리 방법은 블록체인을 기반으로 한 구매 영수증 관리 시스템에 로그인하는 단계, 사용자의 SNS 계정을 인증하는 단계, SNS 계정 정보를 기반으로 접근 권한을 확인하는

단계, 상기 사용자의 접근 권한에 따라 블록체인 네트워크 상에 배포된 NFT 형태의 영수증에 관한 소유권 이전 및 구매 기록을 관리하는 단계를 포함할 수 있다.

【0018】 또한, 사용자가 종이 형태의 구매 영수증 이미지를 업로드하면 NFT 형태의 데이터로 변환하는 단계 및 변환하는 단계에서 OCR 기능을 적용하여 동작되도록 구현할 수 있다.

【발명의 효과】

【0019】 본 발명에 따르면, 다음과 같은 효과가 달성될 수 있다.

【0020】 먼저, 본 발명은 기존의 구매 영수증 관리 방식의 문제점을 극복하고 구매 영수증을 블록체인을 기반으로 관리하여 구매 영수증의 분실, 훼손, 위·변조의 위험이 줄일 수 있다.

【0021】 또한, 본 발명은 블록체인 지갑 관리의 어려움을 개선함으로써 블록체인 지갑관리 기능을 사용자가 쉽게 접근하여 사용할 수 있고, 구매 물품의 소유권을 명확히 하여 거래의 투명성을 보장할 수 있다.

【0022】 또한, 본 발명은 임시키 사용, SNS 인증 기반 접근 제한, 멀티팩터 인증, 고유 식별자와 지갑 주소 매핑 정보 저장에 강력한 암호화 기술로 저장 등을 적용하여 보안을 강화할 수 도 있다.

【도면의 간단한 설명】

【0023】 도 1은 본 발명의 실시예에 따른 블록체인을 기반으로 한 구매 영수증 관리 시스템을 도시하는 개략도이다.

도 2는 본 발명의 실시예에 따른 블록체인을 기반으로 구매 영수증 관리하는 방법을 나타내는 흐름을 도시하는 순서도이다.

【발명을 실시하기 위한 구체적인 내용】

【0024】 본 발명은 블록체인을 기반으로 한 구매 영수증 관리 시스템 및 그 방법에 관한 것으로, SNS 계정 연동을 통해 사용자를 인증하고, 블록체인 지갑을 생성 및 관리하며, 구매 영수증 데이터를 블록체인에 저장하고 검증하는 시스템이다.

【0025】 또한, 본 발명은 IPFS를 이용한 구매 영수증 데이터의 분산 저장, 거래 물품의 소유권 및 진위를 확인하는 스마트 컨트랙트, 다중 디바이스에서 동일 지갑 주소를 관리하는 통합 관리 모듈, 오프라인 인증(QR 코드, NFC)을 통한 거래 검증 기능을 포함한다.

【0026】 더욱이, 사용자가 개인키를 분실했을 때 SNS 계정을 이용한 지갑 복구 기능과 거래 이력, 소유권 변경 내역을 실시간으로 관리 및 조회할 수 있는 기능을 제공한다. 이를 통해 거래의 신뢰성을 강화하고, 중고거래 과정에서의 안전성과 투명성을 확보할 수 있다.

【0027】 본 발명은 상기와 같은 기술적 특징을 구현하기 위해 이하에서는 첨부된 도면을 참조하여 본 발명의 바람직한 실시 예를 상세히 설명하기로 한다. 그러나, 본 발명의 실시 예들은 여러 가지 다른 형태로 변형될 수 있으며, 본 발명의 범위가 아래에서 상술하는 실시예들로 인해 한정되는 것으로 해석되어서는 안된다.

【0028】도 1은 본 발명의 실시예에 따른 블록체인을 기반으로 한 구매 영수증 관리 시스템(10)을 도시하는 개략도이다.

【0029】먼저, 본 발명은 구매 영수증을 관리하기 위해 블록체인 지갑을 사용하는데 일반적인 사용자에게 장애요소가 되는 개인키(Private Key)를 직접 관리의 어려움을 해결하기 위해 사용자의 SNS 계정을 이용한다.

【0030】이를 위해 도 1에 도시된 SNS 연동모듈(11)은 사용자 SNS 계정을 이용하여 블록체인 지갑을 생성하기 위해서 SNS 계정을 사용하여 사용자를 인증하는 역할을 수행한다.

【0031】SNS 계정을 사용하여 사용자를 인증하는 과정은 OPEN API를 활용하여 SNS 서버(20)로부터 사용자의 SNS 계정 정보를 받아오고, 이를 통해 사용자를 인증한 후 블록체인 지갑을 생성하기 위한 것이다. 여기서 SNS 계정은 카카오톡, 인스타그램, 페이스북, 구글 등 다양한 소셜 네트워크 서비스 계정을 포함할 수 있고, 사용자를 인증하는 절차는 다음과 같다.

【0032】예를 들어, 인스타그램의 경우, 인스타그램 그래프 API를 통해 사용자의 프로필 정보와 고유 ID(예를 들어, I000001)를 가져올 수 있다. 이 정보는 인스타그램 계정을 통해 인증된 사용자를 식별하는 데 사용된다.

【0033】또한, 카카오톡의 경우, 카카오 로그인 API를 사용하여 사용자가 카카오톡 계정으로 로그인하게 할 수 있다. 카카오는 사용자 정보(닉네임, 프로필 사진, 이메일 등)와 함께 고유한 사용자 ID(예를 들어, K000001)를 제공한다. 이를

통해 사용자가 카카오톡 계정으로 로그인하는 것을 확인하고 인증할 수 있다.

【0034】SNS 서비스들은 각기 다른 방식으로 인증 기능을 제공하며, 각각의 SNS 서비스는 인증 기능을 통해 사용자가 자신의 SNS 계정을 이용하여 웹사이트나 애플리케이션에 로그인할 수 있다. 이때, OPEN API를 활용하면, 특정 SNS 계정으로 로그인한 사용자의 인증 정보를 가져올 수 있다.

【0035】SNS 계정과 블록체인 지갑을 연동하는 과정에서 중요한 부분은 보안이다. 이를 위해 SNS 로그인 과정에서 OAuth 2.0 인증 방식을 사용하여 SNS 로그인 정보를 받아옴으로써, 사용자의 비밀번호나 중요한 정보를 직접적으로 처리하지 않고, SNS 플랫폼에서 제공하는 인증 토큰을 통해 로그인 절차를 처리한다. 이렇게 하면 사용자의 민감한 정보가 유출되지 않으며, 보안이 강화된다.

【0036】SNS 연동모듈(11)이 OPEN API를 통해 SNS 로그인 정보를 받아오고, 사용자가 SNS 계정으로 인증되면 지갑생성모듈(12)은 블록체인 지갑을 생성한다.

【0037】블록체인 지갑을 생성하는 과정은 사용자가 블록체인 네트워크(30)에서 자산을 안전하게 관리하고 거래를 수행할 수 있도록 하는 중요한 절차이다.

【0038】블록체인 지갑 주소를 생성하기 위해서는 개인키(Private Key)와 공개키(Public Key) 쌍을 생성해야 한다. 이 과정은 블록체인 네트워크(30)에서 안전하게 거래를 수행할 수 있게 해주는 기본적인 요소이다.

【0039】개인키는 사용자가 자신의 자산을 관리하고 거래를 승인하는 데 필요한 중요한 정보이다. 이 키는 외부에 노출되거나 유출되면 안 되며, 안전하게 보

관해야 한다.

【0040】 공개키는 다른 사용자들이 해당 지갑으로 자산을 송금할 수 있게 해주는 주소이다. 공개키는 공개되어도 안전하며, 거래가 발생하는 블록체인 네트워크(30)에서 자산 송수신을 처리하는 데 사용된다.

【0041】 개인키와 공개키 쌍을 생성하는 방법은 다양한 방법이 있지만, 일반적인 방식은 블록체인 플랫폼에서 제공하는 라이브러리(예를 들면, 이더리움과 같은 블록체인에서는 자주 사용되는 JavaScript 라이브러리인 web3.js와 ethers.js 등)나 API를 사용하는 것이다.

【0042】 보다 구체적으로 설명하면, ECDSA(Elliptic Curve Digital Signature Algorithm) 암호화 알고리즘을 이용하여 랜덤하게 생성하는 방식과 BIP-39(Bitcoin Improvement Proposal 39) 표준에 따라 니모닉(Mnemonic) 문구를 제시하며 생성하는 방식으로 구분할 수 있으며, 이러한 생성방식에는 블록체인 플랫폼에서 제공하는 web3.js와 ethers.js 등의 라이브러리가 필요에 따라 선택적으로 사용될 수도 있다.

【0043】 블록체인 지갑을 랜덤하게 생성하는 방식은 ECDSA 암호화 알고리즘을 사용해 완전히 랜덤한 방식으로 생성된 개인키를 기반으로 공개키와 지갑 주소를 생성하는 방식이다. 이 방식은 블록체인 지갑을 생성하는데 있어 가장 일반적으로 사용되는 방식이며, 이에 대한 설명은 당업자에게 널리 알려져 있어 이에 대한 설명은 생략한다.

【0044】다음으로 BIP-39 표준에 따라 니모닉 문구를 제시하며 생성하는 방식은 사람이 기억하기 쉬운 단어(니모닉 문구)를 조합하여 지갑을 복구하거나 관리할 수 있도록 하는 방식이다.

【0045】일반적으로 BIP-39 표준에 따라 니모닉 문구를 제시하며 생성하는 방식은 랜덤 시드를 생성하고 이를 기반으로 니모닉 문구를 생성한다. 다음으로, 니모닉 문구를 다시 입력하여 동일한 시드를 복구한다. 마지막으로 시드에서 개인키를 생성하고, 공개키와 지갑 주소를 파생한다.

【0046】본 발명에 따른 블록체인 지갑생성 방법은 BIP-39 표준에 따라 니모닉 문구를 제시하며 생성하는 방식과는 달리 랜덤시드를 사용하지 않는 대신 SNS ID를 이용하여 생성된 초기 시드를 바탕으로 개인키, 공개키, 및 지갑주소를 생성하는 점에서 차이가 있고, 그 이후의 절차는 BIP-39 표준에 따라 니모닉 문구를 제시하며 생성하는 방식과 동일하므로 이하에서는 SNS ID를 이용하여 초기 시드를 생성하는 과정에 대해서만 설명하기로 한다.

【0047】본 발명의 실시예에 따르면, 지갑생성모듈(12)은 사용자의 SNS ID (예: "user123@kakao.com")를 입력값으로 사용하여 니모닉 문구를 생성할 수 있다.

【0048】사용자가 SNS ID를 입력(또는 사용자가 선택하거나 로그인한 SNS에 대해 SNS 연동모듈(11)이 SNS API를 통해 자동 수집한 ID)하면, 지갑생성모듈(12)은 입력된 SNS ID를 해싱(Hashing) 또는 키 파생 함수(예: PBKDF2, HMAC)를 통해 변환하면 암호화된 시드 값을 생성하게 된다.

【0049】이 때, 사용자의 SNS ID만 사용하면 해당 데이터가 유출될 경우, 다른 사람이 동일한 해시 값을 생성할 수 있으므로 이를 방지하기 위해, 사용자 입력 사항; 시스템(10)에 의해 부여되는 Secret Key(임의의 문구 또는 번호의 조합); 휴대폰 번호; 또는 본 발명에 따른 시스템(10)에 로그인 하기 위한 ID; 본 발명에 따른 시스템(10)이 사용자에게 부여한 고유 식별자(예를 들어, B000001와 같은 형태의 숫자 또는 문자의 조합); 중의 어느 하나 또는 이들 간의 조합을 추가하여 해시 값을 생성함으로써 초기 시드를 생성할 수 있고, 이하에서는 특별한 언급이 없는 한 Secret Key는 보안을 향상시킬 목적으로 사용되는 이들 모두를 포함하는 집합적인 용어로 사용된다.

【0050】예를 들어, SNS ID가 ‘user123@kakao.com’이고, Secret Key는 ‘X1y2Z3SecretKey2024!’인 경우 해시값은 다음과 같이 생성된다.

【0051】해시 값 = SHA-256("user123@kakao.comX1y2Z3SecretKey2024!")

【0052】256비트 길이의 결과 : e3f2a45b...

【0053】여기서, SHA-256은 입력 데이터를 256비트(32바이트) 길이의 고정된 해시 값으로 변환하는 암호화 해시 함수로써, 입력값이 같으면 항상 고정된 256비트 길이의 동일한 출력값을 생성하고, 출력값에서 원래 입력값을 되돌릴 수 없는 특징이 있다.

【0054】이와 같이, 본 발명에 따른 시스템(10)이 내부적으로 관리하는 고유하고 비밀스러운 값인 Secret Key를 추가하여 SNS ID가 유출되어도 해시 값을 예측

할 수 없도록 하여 보안을 강화할 수 있다.

【0055】 Secret Key는 일반적으로 사용자나 외부에 공개되지 않으며, Secret Key는 전역 Secret Key와 사용자별 Secret Key가 있다.

【0056】 전역 Secret Key는 모든 사용자에게 동일한 값이 적용될 수 있도록 하는 초기 시드를 생성하는 시스템(10)에 부여되는 Secret Key이고, 사용자별 Secret Key는 각 사용자에게 고유하게 부여된 Secret Key이다.

【0057】 본 발명에서는 초기 시드를 생성할 때, 전역 Secret Key 또는 사용자별 Secret Key를 동시에 적용할 수도 있고, 이들 중 어느 하나를 선택적으로 적용할 수도 있고, 사용자마다 다르게 설정할 수도 있으며 이에 한정되지는 않는다.

【0058】 다음으로, 생성된 초기 시드를 BIP-39 표준에 따라 니모닉 문구로 변환한다.

【0059】 니모닉 문구는 초기 시드를 사람이 읽을 수 있는 형태로 변환한 결과물이며, 니모닉 문구만 저장하면, 이를 기반으로 초기 시드를 복구하여 개인키를 분실한 경우에 사용할 수도 있으므로 니모닉 문구는 사용자에게 제시하여 사용자가 이를 저장하여 개인키를 복구할 수 있도록 한다.

【0060】 다음으로, 생성된 초기 시드를 BIP-39 표준에 따라 니모닉 문구로 변환하고, 사용자가 니모닉 문구를 저장하면 지갑생성모듈(12)은 니모닉 문구를 이용하여 시드를 다시 생성한다. 재 생성된 시드는 초기 시드와 동일한 값이다.

【0061】지갑생성모듈(12)은 재생성된 시드를 이용하여 사용자의 SNS ID와 연결된 개인키를 생성하고, 공개키와 지갑 주소를 생성한다.

【0062】블록체인 지갑 주소 생성 과정에서 web3.js나 ethers.js와 같은 라이브러리를 사용하여 개인키와 공개키 쌍을 생성할 수 있다. 이 라이브러리들은 이더리움 블록체인과의 상호작용을 간편하게 만들어주는 도구들로, 지갑 생성뿐만 아니라 블록체인 거래, 스마트 계약 실행 등 여러 기능을 지원한다.

【0063】개인키와 공개키 쌍이 생성된 후, 생성된 지갑 주소는 블록체인 네트워크(30)에 기록된다. 이때 중요한 점은 개인키는 오프체인(사용자 기기 등)에 저장되며, 공개키 또는 지갑주소는 블록체인 상에서 사용되거나 다른 사용자와 공유된다. 사용자는 공개키 또는 지갑주소를 통해 다른 사람에게 자산을 송금할 수 있다.

【0064】지갑생성모듈(12)에 의해 블록체인 지갑이 생성되면, 계정연동모듈(13)은 SNS ID와 블록체인 지갑 주소를 연결하여 데이터베이스의 형태로 구성되는 저장모듈(14)에 저장한다.

【0065】SNS 계정을 활용한 사용자 인증과 블록체인 지갑 생성을 통해, 사용자는 보다 간편하고 안전하게 블록체인 지갑을 생성하고 관리할 수 있게 된다. OPEN API를 통해 SNS 로그인 정보를 받아오고, 이를 기반으로 지갑을 생성하는 시스템(10)은 사용자의 진입 장벽을 낮추고, 블록체인 기술의 접근성을 높이는 데 중요한 역할을 한다.

【0066】본 발명에 따른 다른 실시예로, 사용자 입력 데이터(SNS ID)만 사용하면 해당 데이터가 유출되면 다른 사람이 동일한 해시 값을 생성할 수 있으므로 이를 방지하기 위해, 사용자 입력 사항; 시스템(10)에 의해 부여되는 Secret Key(임의의 문구 또는 번호의 조합); 휴대폰 번호; 또는 본 발명에 따른 시스템(10)에 로그인 하기 위한 ID; 본 발명에 따른 시스템(10)이 사용자에게 부여한 고유 식별자; 중의 어느 하나 또는 이들 간의 조합을 추가하여 해시 값을 생성함으로써 초기 시드를 생성할 수 있다.

【0067】예를 들어, SNS ID가 ‘user123@kakao.com’이고, Secret Key는 ‘X1y2Z3SecretKey2024!’인 경우 해시값은 다음과 같이 생성된다.

【0068】해시 값 = SHA-256("user123@kakao.comX1y2Z3SecretKey2024!")

【0069】256비트 길이의 결과 : e3f2a45b...

【0070】여기서, SHA-256은 입력 데이터를 256비트(32바이트) 길이의 고정된 해시 값으로 변환하는 암호화 해시 함수로써, 입력값이 같으면 항상 고정된 256비트 길이의 동일한 출력값을 생성하고, 출력값에서 원래 입력값을 되돌릴 수 없다.

【0071】이와 같이, 본 발명에 따른 시스템(10)이 내부적으로 관리하는 고유하고 비밀스러운 값인 Secret Key를 추가하여 SNS ID가 유출되어도 해시 값을 예측할 수 없도록 하여 보안을 강화할 수 있다.

【0072】Secret Key는 일반적으로 사용자나 외부에 공개되지 않으며, Secret Key는 전역 Secret Key와 사용자별 Secret Key가 있다.

【0073】전역 Secret Key는 모든 사용자에게 동일한 값이 적용될 수 있도록 하는 초기 시드를 생성하는 시스템(10)에 부여되는 Secret Key이고, 사용자별 Secret Key는 각 사용자에게 고유하게 부여된 Secret Key이다.

【0074】본 발명에서는 초기 시드를 생성할 때, 전역 Secret Key 또는 사용자별 Secret Key를 동시에 적용할 수도 있고, 이들 중 어느 하나를 선택적으로 적용할 수도 있고, 사용자마다 다르게 설정할 수도 있으며 이에 한정되지는 않는다.

【0075】블록체인 지갑 생성에 사용된 Secret Key는 사용자에 의해 설정된 값일 수도 있고, 본 발명에 따른 시스템(10)에 의해 로그인하기 위한 사용자가 설정한 ID 또는 시스템이 부여한 고유 식별자일 수도 있으며, SNS 계정 연동 과정에서 OPEN API를 통해 수신한 SNS 계정의 사용자 고유 식별자일 수도 있다. 또한, 이들 중 어느 하나를 선택적으로 적용할 수도 있고, 사용자마다 다르게 설정할 수도 있으며 이에 한정되지는 않는다.

【0076】다만, 어떠한 정보가 Secret Key로 이용되었는지에 대한 정보만을 데이터베이스에 저장할 뿐, Secret Key 자체는 저장하지 않음으로써 사용자가 만든 블록체인 관련 정보에 대한 보안을 담보할 수 있도록 한다.

【0077】지갑생성모듈(12)에 의해 블록체인 지갑 생성에 사용된 Secret Key는 사용자의 기기에 별도로 저장될 수도 있고, 사용자의 요청 또는 허가가 있는 경우 데이터베이스를 포함하는 저장모듈(14)에 저장되어 블록체인 지갑의 개인키를 복구할 수 있는 기능을 제공할 수도 있다.

【0078】또한, 저장모듈에 저장되는 정보로는 블록체인 지갑 생성에 사용된 Secret Key에 해당되는 사용자 입력 사항; 시스템에 의해 부여되는 Secret Key(임의의 문구 또는 번호의 조합); 휴대폰 번호; 또는 본 발명에 따른 시스템(10)에 로그인 하기 위한 ID; 본 발명에 따른 시스템이 사용자에게 부여한 고유 식별자; 등이 있다.

【0079】또한, 사용자의 블록체인 지갑에 대한 관리도 중요한데, 지갑의 개인키는 사용자가 직접 관리해야 하며, 복구 기능이 제공되는 것이 바람직하다.

【0080】이를 위해 본 발명은 계정연동모듈(13)을 포함하여 구성되고, 계정연동모듈(13)은 사용자의 SNS ID로 로그인하는 것을 허용함으로써 본 발명에 따른 시스템(10)에 접속한 사용자가 블록체인 지갑에 접속하여 자산의 확인 및 거래를 할 수도 있고, 분실된 키를 복구할 수 있도록 한다.

【0081】본 발명에 의한 실시예에 따르면, 사용자가 제 1 로그인 과정을 거쳐 블록체인 지갑에 접속하면 사용자 ID와 블록체인 지갑 주소를 연결하여, 해당 사용자의 지갑 주소를 조회하고 관리할 수 있도록 한다.

【0082】사용자에 의한 제 1 로그인 과정은 본 발명에 따른 시스템(10)에 로그인하기 위한 사용자 ID와 패스워드의 입력을 통해 수행된다. 이에 더해, OTP 입력 또는 회원 가입시 저장한 전화번호에 기반한 추가 인증(예: SMS OTP)을 더 요구하여 보안을 강화할 수도 있다.

【0083】본 발명에 의한 다른 실시예에 따르면, 사용자는 블록체인 지갑 생성에 사용된 SNS ID와 블록체인 지갑 주소가 연결되는 구조로 형성된 데이터베이스를 활용하여 블록체인 지갑 생성에 사용된 SNS ID로 본 발명에 따른 시스템(10)에 로그인할 수 있다.

【0084】SNS ID로 로그인하는 과정에서 회원 가입시 저장한 전화번호에 기반한 추가 인증(예: SMS OTP) 또는 OTP 입력을 더 요구함으로써 본 발명에 따른 시스템(10)에 접속하기 위한 사용자 ID와 패스워드를 분실해도 편리하게 접속할 수 있고, 더불어 보안을 강화할 수도 있다.

【0085】SNS ID로 로그인 한 경우에는 사용자 ID와 패스워드로 로그인 한 경우와 동일한 권한을 부여함으로써 블록체인 지갑에 접속하여 안전하게 자산을 조회하고 관리할 수 있게 된다.

【0086】본 발명은 SNS 계정을 통한 개인키 복구 기능을 제공할 수 있는 복구모듈(15)을 포함하여 구성된다.

【0087】본 발명의 실시 예에 따르면, 사용자가 개인키를 분실한 경우에도 사용자가 별도로 저장하고 있는 니모닉 문구(블록체인 지갑을 생성 과정에서 생성됨) 또는 블록체인 지갑 생성에 사용된 SNS ID 및 Secret Key를 이용하여 개인키를 복구할 수 있다.

【0088】먼저, 사용자가 보관하고 있는 니모닉 문구를 이용하여 개인키를 복구하는 과정은 다음과 같다.

【0089】개인키 복구를 위해 사용자가 보관하고 있는 니모닉 문구를 입력하면 지갑생성모듈(12)은 시드를 다시 생성한다. 이 때, 생성된 시드는 분실한 개인키를 생성할 때 생성된 초기 시드와 동일한 값이다.

【0090】지갑생성모듈(12)은 개인키 복구과정에서 다시 생성된 시드를 이용하여 개인키를 복구하고, 개인키를 사용자에게 제공한다.

【0091】다음으로, 블록체인 지갑 생성에 사용된 SNS ID 및 Secret Key를 이용하여 개인키를 복구하는 과정은 다음과 같다.

【0092】블록체인 지갑 생성에 사용된 Secret Key가 어떤 종류의 정보인지는 시스템(10)의 데이터베이스를 포함하는 저장모듈(14)에 저장되어 있으므로 복구모듈(15)은 사용자에게 순차적으로 블록체인 지갑 생성에 사용된 Secret Key와 관련된 정보의 종류를 제시하며 사용자의 입력을 대기한다.

【0093】사용자가 정확한 정보를 입력하면 복구모듈(15)은 다음 단계로 진행하여 추가적인 정보를 입력받고, 개인키 복구에 필요한 모든 정보가 수집되면 이를 지갑생성모듈(12)로 전송한다.

【0094】지갑생성모듈(12)은 복구모듈(15)로부터 수신한 정보를 바탕으로 시드를 다시 생성한다. 이 때, 생성된 시드는 분실한 개인키를 생성할 때 생성된 초기 시드와 동일한 값이다.

【0095】지갑생성모듈(12)은 개인키 복구과정에서 다시 생성된 시드를 이용하여 개인키를 복구하고, 개인키를 사용자에게 제공한다.

【0096】개인키를 복구하는 과정에서 보안 강화를 위해 본 발명에 따른 시스템(10)에 회원 가입을 위해 저장한 전화번호에 기반한 추가 인증(예: SMS OTP) 또는 OTP 입력을 더 요구할 수도 있고, SNS 연동모듈(11)을 통해 제공되는 SNS 인증 기능을 부가하여 OPEN API를 활용함으로써 특정 SNS 계정으로 로그인한 사용자의 인증 정보를 가져와 사용자 인증을 수행하고 개인키 복구 과정을 진행할 수도 있으며, 이들 중 어느 하나를 선택적으로 적용할 수도 있고, 모두를 적용하여 개인키 과정을 진행할 수 있으나 이에 한정되지는 않는다.

【0097】개인키 복구 기능은 사용자가 블록체인 지갑을 안전하게 관리하고, 실수나 사고로 인해 개인키를 잃어버렸을 때도 문제없이 자산을 보호할 수 있도록 돕는 중요한 기능이다. SNS 계정 연동, OPEN API, Secret Key 등을 통해 안전하고 효율적으로 개인키 복구를 제공하며, 개인키를 외부 시스템에 저장하지 않고도 복구가 가능하도록 설계할 수 있다. 이를 통해 사용자 경험을 개선하고, 보안을 강화하며, 블록체인 기술을 더욱 안전하고 실용적으로 활용할 수 있다.

【0098】블록체인 지갑을 생성할 때 최초로 생성된 개인키를 사용자가 저장하는 단계에서 지갑생성모듈(12)은 개인키를 사용자가 지정한 단말기에 저장하는 것 이외에 다른 저장 방법을 제공할 수 있다.

【0099】예를 들면, 비공개키를 파편화하여 개인키를 여러 조각으로 나누어 분산 저장하고, 각 조각을 복구할 수 있는 SNS 인증과 결합된 재조합 기능 제공하도록 하는 것이다.

【0100】개인키를 파편화하여 분산 저장하고, 이를 SNS 인증과 결합된 재조

합 기능을 통해 복구하는 기술은 보안성과 접근성을 동시에 확보하기 위한 솔루션이다.

【0101】이를 구현하기 위해 생성된 개인키를 SSSS(Shamir's Secret Sharing Scheme) 알고리즘을 통해 n개의 조각으로 분할하고, 각 조각에 고유한 ID를 부여해 추적 및 관리 가능하도록 설계한다.

【0102】이렇게 분할된 조각은 분산 저장되고, SNS와 연동하여 저장할 수도 있고, 다중 저장소를 활용할 수도 있다.

【0103】SNS와 연동된 저장방식으로는 분할된 각 조각을 사용자가 연동한 SNS 계정(예: Google Drive, iCloud, Dropbox)의 개인 이메일에 암호화된 형태로 저장한다. 저장을 위해 SNS 연동모듈(11)이 연동한 SNS 계정의 OPEN API를 통해 사용자 인증 후, 안전하게 조각을 업로드한다.

【0104】또한, 다중 저장소를 활용하여 동일한 조각을 여러 저장소에 중복 저장하거나, 조각을 분리하여 다양한 저장소에 배포하여 저장할 수도 있다. 예를 들면, 한 조각은 Google Drive에 저장하고, 다른 조각은 로컬 장치 또는 별도의 클라우드 서버에 저장할 수 있다. 저장되는 각 조각은 별도의 암호화 키로 다시 암호화하여 저장할 수 있다.

【0105】다음으로 분할된 조각을 복구하기 위해 사용자가 개인키 복구를 요청하면, 시스템(10)은 연동된 SNS 계정 정보를 확인한다. SNS API를 통해 사용자 인증 후, 복구 가능한 조각에 접근할 수 있다.

【0106】조각을 모아 재조합하여 복구를 하기 위해서는 SSSS(Shamir's Secret Sharing Scheme) 알고리즘에서 필요한 최소 개수(t)의 조각을 수집하고, 수집된 조각을 SSSS 알고리즘을 통해 원래 개인키를 복원한다. 조각은 네트워크를 통해 암호화된 형태로 전달되며, 로컬 환경에서만 복호화 및 복구한다.

【0107】복구 요청 시, 추가 인증 절차를 적용(예: SMS OTP, 생체 인증 등)하고, 조각이 네트워크를 통해 이동할 때는 SSL 또는 TLS와 같은 암호화 프로토콜 사용한다.

【0109】다음으로 본 발명에 따른 블록체인을 기반으로 한 구매 영수증 관리 시스템(10)은 스마트 컨트랙트와 연계되어 자동으로 구매 영수증을 관리하고, 소유권 이전 및 관리가 가능하다.

【0110】스마트 컨트랙트(Smart Contract)는 블록체인 상에서 특정 조건이 충족되면 자동으로 실행되는 디지털 계약이다. 탈중앙화된 네트워크에서 동작하며, 계약 내용과 실행 결과가 모두 블록체인에 기록되어 신뢰성과 투명성을 보장한다.

【0111】구매 주문의 조건을 코드화하여 특정 조건이 충족될 때 자동으로 결제를 실행한다. 예를 들면, 배송 확인에 따라 대금을 자동으로 지급하거나, 구매 조건에 따라 대금을 분할 지급 및 각 단계별 자동 결제하는 등의 처리를 수행할 수 있다.

【0112】중개자 없이 계약 조건을 수행할 수 있는 특징을 가지며, 금융 거래, 물류, 인증 등 다양한 분야에서 활용된다.

【0113】스마트 컨트랙트가 작성되면 블록체인 네트워크(30)에 배포되고, 스마트 컨트랙트를 배포하면 고유한 컨트랙트 주소가 생성되며, 이를 통해 호출 및 실행이 가능하다.

【0114】NFT(Non-Fungible Token, 대체 불가능한 토큰)는 블록체인 상에서 고유성과 대체 불가능성을 가지는 디지털 자산이다.

【0115】각각의 NFT는 고유한 ID와 메타데이터를 가지며, 이를 통해 소유권, 진품 여부, 이력 등을 블록체인에 안전하게 기록할 수 있고, 디지털 아트, 게임 아이템, 부동산 등 다양한 자산을 표현하고 거래하는 데 사용되며, 스마트 컨트랙트와 연계되어 자동으로 소유권 이전 및 관리가 가능하다.

【0116】스마트 컨트랙트는 NFT를 발행하고 거래하는 데 사용되며, NFT는 스마트 컨트랙트의 실행을 통해 고유한 디지털 자산으로서의 특성을 갖게 되므로 스마트 컨트랙트와 NFT는 긴밀하게 연결된다.

【0117】IPFS(InterPlanetary File System)는 데이터를 중앙 서버가 아닌 분산 네트워크에 저장하는 분산형 파일 저장 시스템(10)이다. 데이터를 고유한 해시 값으로 식별하고, 이를 통해 파일의 무결성과 안전성을 보장한다. 블록체인의 저장 한계를 보완하여 NFT의 메타데이터나 대용량 데이터를 저장하는 데 활용되며, 파일이 네트워크 내 여러 노드에 분산되어 있어 데이터의 유실 위험을 줄이고 빠른 접

근성을 제공한다.

【0118】스마트 컨트랙트는 자동화된 계약 실행을 통해 거래의 신뢰성을 보장하며, NFT는 제품 소유권과 구매 내역을 블록체인 상에 안전하게 기록한다. 또한, IPFS를 활용하면 영수증이나 데이터가 분산형 네트워크에 안전하게 저장되어 A/S, 소유권 이전, 거래 이력 검증과 같은 후속 작업을 효율적으로 처리할 수 있다.

【0119】본 발명의 실시 예에 따르면, 본 발명의 시스템(10)이 블록체인 네트워크(30), 스마트 컨트랙트, NFT, 및 IPFS를 연계하여 구매 영수증을 관리할 수 있고, 소유권 이전 및 관리가 가능하다.

【0120】또한, 스마트 컨트랙트와 OPEN API를 연동하여 구매 내역을 자동으로 관리하는 시스템(10)은 블록체인 기술과 디지털화된 계약의 장점을 결합해 구매 데이터를 안전하게 저장하고 효율적으로 관리할 수 있다.

【0121】OPEN API는 외부 애플리케이션과 블록체인 네트워크(30) 간의 통신을 가능하게 하는 인터페이스이고, 이를 통해 사용자는 블록체인 네트워크(30)에 연결하여 스마트 컨트랙트를 생성, 관리, 실행할 수 있으며, OPEN API는 인증 키(API Key)와 보안 프로토콜(Hmac-SHA256 등)을 통해 안전한 데이터 통신을 보장한다.

【0123】본 발명의 실시예에 따르면, 본 발명의 시스템(10)은 스마트 컨트랙트 처리모듈(16)을 포함한다. 스마트 컨트랙트 처리모듈(16)은 본 발명에서 생성된 사용자의 지갑주소와 영수증을 연결시켜 주는 역할을 수행하며, 도 3에 도시된 바와 같이 다음과 같은 과정를 거쳐 구매 영수증을 관리하게 된다.

【0124】(S1) 물품 구매 및 영수증 발행 과정:

【0125】본 발명의 실시 예에 따르면, 사용자 A가 온라인 쇼핑몰에서 전자제품을 구매하고, 구매가 완료되면, 쇼핑몰의 스마트 컨트랙트가 작동하여 구매 정보를 기반으로 디지털 영수증을 NFT 형태로 발행하여 스마트 컨트랙트 처리모듈(16)로 전송한다.

【0126】온라인 쇼핑몰에서 발급하는 디지털 영수증을 사용자 A가 직접 받는 경우, 사용자 A가 쇼핑몰로부터 받은 NFT 형태의 디지털 영수증을 스마트 컨트랙트 처리모듈(16)을 포함하는 본 발명의 시스템(10)에 업로드한다.

【0127】(S2) IPFS 저장 과정:

【0128】온라인 쇼핑몰 또는 사용자 A로부터 영수증 NFT를 수신한 스마트 컨트랙트 처리모듈(16)은 영수증 NFT를 IPFS 저장 처리모듈(17)로 전송하여 IPFS에 저장되도록 한다. IPFS 저장 처리모듈(17)은 IPFS에서 반환된 해시 값을 스마트 컨트랙트 처리모듈(16)로 전송한다.

【0129】온라인 쇼핑몰 또는 사용자 A로부터 수신한 영수증 NFT에는 구매 내역(제품명, 구매 일시, 가격)과 함께 제품의 소유권 정보가 기록된다.

【0130】IPFS(InterPlanetary File System)는 분산형 파일 저장 시스템(10)으로, 영수증 데이터를 안전하게 보관할 수 있고, 콘텐츠 주소를 지정할 수 있어 파일 내용을 기반으로 고유한 해시를 생성하며, 이 고유한 해시 값이 CID(Content Identifier)이며, IPFS에서 데이터를 찾기 위한 주소 역할을 하여 데이터를 식별하고 접근할 수 있게 한다. 또한, 데이터를 여러 노드에 분산 저장하여 가용성을 높일 수 있고, 동일한 내용의 파일은 한 번만 저장되어 효율성을 높일 수 있는 저장 방식이다.

【0131】(S3) 블록체인에 데이터 기록 과정:

【0132】스마트 컨트랙트 처리모듈(16)은 IPFS 저장 처리모듈(17)로부터 IPFS에서 반환된 해시 값을 수신하여 블록체인 네트워크(30)에 기록한다. 이 과정에서 스마트 컨트랙트가 사용되어 해시 값과 관련 메타데이터(예: 지갑주소(또는 사용자 ID), 타임스탬프)를 저장한다.

【0133】생성된 스마트 컨트랙트는 블록체인 네트워크(30)에 기록된다. 이 과정에서 모든 트랜잭션이 암호화되고 분산 저장되어 데이터의 무결성과 투명성을 보장하며, 기록된 데이터는 시간 순서대로 정렬되며, 각 데이터는 고유한 식별자를 가지므로 추적이 용이하다.

【0134】블록체인에 저장된 스마트 컨트랙트는 디지털 영수증 역할을 한다. 사용자 A는 자신의 지갑을 통해 언제든지 구매 내역에 접근할 수 있으며, 이를 A/S 요청, 보험 청구, 중고 거래 등의 증빙 자료로 활용할 수 있다

【0135】(S4) 소유권 이전 및 검증 과정:

【0136】사용자 A가 해당 제품을 사용하다가 사용자 B에게 중고로 판매하기로 결정하면, 사용자 A는 스마트 컨트랙트 기반 거래 플랫폼에서 제품과 함께 영수증 NFT를 사용자 B에게 전송한다.

【0137】스마트 컨트랙트는 거래 조건(예: 사용자 B가 대금을 지불했는지)을 확인한 뒤, 대금 결제와 동시에 영수증 NFT의 소유권을 사용자 B에게 이전한다.

【0138】사용자 B는 블록체인에 기록된 거래 내역과 NFT 정보를 통해 제품의 진품 여부와 소유권 이력을 확인할 수 있다.

【0139】(S5) A/S 및 보증 과정:

【0140】제품에 문제가 발생하면, 사용자 B는 영수증 NFT의 메타데이터를 통해 IPFS에 저장된 원본 영수증을 확인하고, 제조사에 A/S를 요청한다.

【0141】제조사는 블록체인에서 영수증 NFT의 소유권 정보를 검증하여 사용자 B가 정당한 소유자인지 확인한 뒤, 서비스를 제공한다.

【0142】본 발명의 다른 실시 예에 따르면, 구매 영수증이 종이 형태인 경우는 NFT 형태의 영수증이 아니므로 사용자에 의해 스캔 또는 촬영한 종이 영수증 이미지를 NFT 형태의 데이터로 변환할 필요가 있다. 이를 위해 본 발명의 스마트 컨트랙트 처리모듈(16)은 사용자가 업로드한 종이 영수증 이미지를 NFT 형태의 데이터로 변환하는 기능을 수행할 수 있다.

【0143】이미지를 NFT 형태의 데이터로 변환하는 과정에서 OCR 기능을 적용하여 영수증에 기록된 문자 또는 이미지를 판독하고, 판독된 정보를 기반으로 구매 내역(제품명, 구매 일시, 가격)과 함께 제품의 소유권 정보를 기록할 수도 있다.

【0144】이 후, 스마트 컨트랙트 처리모듈(16)은 NFT 형태의 데이터로 변환된 영수증을 IPFS 저장 처리모듈(17)로 전송하여 IPFS에 저장되도록 한다.

【0145】그 이후의 동작은 앞선 실시예의 “(S2) IPFS 저장 과정” 이후와 동일하므로 이에 대한 설명은 생략하기로 한다.

【0147】본 발명의 보안 강화를 위한 실시예에 따르면, 일정 시간만 사용가능한 1회용 임시키를 사용하도록 설정할 수 있다. 이를 위해 본 발명은 임시키 발행모듈(18)을 더 포함하여 구성된다.

【0148】임시키 발행모듈(18)은 사용자가 기존 개인키를 사용하지 않고도 일정 시간 동안 지갑을 안전하게 사용할 수 있도록 한다. 이를 위해 HMAC(Hash-based Message Authentication Code)와 같은 암호화 방식을 사용해 기존 개인키와 시간 데이터를 조합해 임시키를 생성하며, 생성된 임시키를 통해 임시 공개키와 지갑 주소를 파생한다. 이러한 방식은 ECDSA와 같은 비대칭 암호화 알고리즘을 사용하며, 사용 기한과 권한을 제한하여 보안성을 확보한다.

【0149】임시키는 사용 기한(예: 1시간, 24시간)을 명확하게 설정하고, 이를 블록체인 네트워크(30)나 메타데이터에 기록하여 유효 기간 동안만 활성화된다. 또

한, 임시키는 특정 작업(예: 거래 승인, 소액 결제, 잔액 확인 등)에 한정된 권한만 부여되므로 과도한 사용 권한으로 인한 보안 리스크를 최소화한다. 임시키는 지갑 애플리케이션과 연동되며, 사용자가 본 발명에 따른 시스템(10)에 접속하기 위한 앱 또는 PC 프로그램을 실행하여 로그인한 후 “임시키 발행” 버튼을 눌러 생성할 수 있고, 생성된 키는 OPEN API를 통해 블록체인 네트워크(30)에 등록된다.

【0150】블록체인 네트워크(30)는 거래 요청 시 임시키의 유효성(유효 기간, 권한 범위 등)을 검증하고, 이를 통해 불법 사용을 차단한다. 사용자 역시 거래 승인 시 SNS 인증, 생체 인증과 같은 추가 인증 절차를 통해 본인임을 확인한다. 임시키는 사용자 기기에 암호화된 형태로 저장되며, 모바일 환경에서는 Android KeyStore나 iOS Secure Enclave를 사용해 안전하게 관리된다. 또한, 재사용을 방지하기 위해 임시키는 1회성으로 설계되며, 사용 후 즉시 폐기되거나 네트워크에 기록되어 재사용이 차단된다.

【0151】예를 들어, 사용자가 지갑 애플리케이션에서 임시키 발행을 요청하면 SNS 인증이나 생체 인증을 통해 본인 확인이 이루어진다. 이후 임시키가 생성되고 블록체인 네트워크(30)에 등록되며, 사용자는 임시키를 통해 소액 결제나 거래 승인 등의 특정 작업을 수행할 수 있다. 유효 기간이 지나면 네트워크는 해당 키를 자동으로 비활성화한다. 이를 통해 개인키를 직접 노출하지 않고도 안전하게 지갑을 사용할 수 있으며, 개인키 분실 시에도 임시 접근 권한을 제공하여 사용자 편의성과 보안성을 동시에 높일 수 있다.

【0153】본 발명의 보안 강화를 위한 다른 실시예에 따르면, SNS 인증에 기반하여 접근을 제한할 수도 있다. 사용자가 블록체인 지갑에 접근하려면 먼저 SNS 인증 절차를 거쳐야 한다. 시스템(10)은 사용자의 SNS 계정 정보를 기반으로 접근 권한을 확인하며, 인증이 성공한 경우에만 매핑된 지갑 주소를 반환한다. 이를 통해 접근 권한이 없는 사용자나 비인가자의 접근을 방지할 수 있어 보안성을 높인다.

【0154】본 발명의 보안 강화를 위한 또 다른 실시예에 따르면, 멀티팩터 인증을 적용하여 보안을 강화할 수 도 있다. 추가적인 보안을 위해 로그인 과정에서 OTP(일회용 비밀번호)나 생체 인증과 같은 멀티팩터 인증(MFA)을 적용한다. 사용자가 새로운 디바이스에서 접근하려고 시도할 경우, 시스템(10)은 추가 인증 절차를 요구해 불법 접근을 방지한다. 이를 통해 인증된 사용자만이 지갑에 안전하게 접근할 수 있도록 보호한다.

【0155】본 발명의 보안 강화를 위한 또 다른 실시예에 따르면, 본 발명에 따른 시스템(10)이 사용자에게 부여한 고유 식별자와 지갑 주소 매핑 정보를 AES 알고리즘과 같은 강력한 암호화 기술을 사용해 저장한다. 암호화된 데이터는 저장모듈(14)에 기록되지만, 복호화되지 않은 상태로만 보관되므로 외부 공격이나 데이터 유출 시에도 정보의 노출을 최소화할 수 있다.

【0156】본 발명의 보안 강화를 위한 또 다른 실시예에 따르면, 개인키 노출 방지를 위해 지갑 주소를 불러오는 과정에서도 개인키는 사용자의 로컬 디바이스에서만 관리되는 것을 원칙으로 한다. 개인키는 저장모듈(14)에 저장되지 않으며, 오

직 사용자의 디바이스에 안전하게 보관된다. 이를 통해 중앙화된 시스템(10)에서 발생할 수 있는 개인키 유출 위험을 원천적으로 차단하고 사용자의 자산을 보호한다. 다만, 개인키 복구를 목적으로 사용자의 요청이나 허가에 의해 개인키를 파편화시켜 분산 저장하는 경우는 예외로 한다.

【0157】이상 본 발명의 바람직한 실시 예를 참조하여 설명하였지만, 당 업계에서 통상의 지식을 가진 자라면 이하의 청구범위에 기재된 본 발명의 사상 및 영역을 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

【부호의 설명】

【0158】10 : 구매 영수증 관리 시스템

11 : SNS 연동모듈

12 : 지갑생성모듈

13 : 계정연동모듈

14 : 저장모듈

15 : 복구모듈

16 : 스마트 컨트랙트 처리모듈

17 : IPFS 저장 처리모듈

18 : 임시키 발행모듈

20 : SNS 서버

30 : 블록체인 네트워크

【청구범위】

【청구항 1】

사용자의 SNS 계정을 인증하는 SNS 연동모듈,

SNS 계정 정보를 기반으로 접근 권한을 확인하는 계정연동모듈,

상기 사용자의 접근 권한에 따라 블록체인 네트워크 상에 배포된 NFT형태의 영수증에 관한 소유권 이전 및 구매 기록을 관리하는 스마트 컨트랙트 처리모듈을 포함하는 것을 특징으로 하는 블록체인을 기반으로 한 구매 영수증 관리 시스템.

【청구항 2】

제1항에 있어서,

상기 스마트 컨트랙트 처리모듈은 구매 거래 조건을 코드화하여, 거래 조건이 충족되었을 때 영수증의 소유권을 자동으로 이전하는 것을 특징으로 하는 블록체인을 기반으로 한 구매 영수증 관리 시스템.

【청구항 3】

제1항에 있어서,

상기 스마트 컨트랙트 처리모듈은 상기 사용자가 업로드한 종이 형태의 구매 영수증 이미지를 NFT 형태의 데이터로 변환하는 것을 특징으로 하는 블록체인을 기반으로 한 구매 영수증 관리 시스템.

【청구항 4】

제3항에 있어서,

상기 스마트 컨트랙트 처리모듈은 NFT 형태의 데이터로 변환하는 과정에서 OCR 기능을 적용하는 것을 특징으로 하는 블록체인을 기반으로 한 구매 영수증 관리 시스템.

【청구항 5】

제1항에 있어서,

상기 사용자 또는 상기 시스템이 설정한 시간 동안만 블록체인 지갑의 특정된 작업에만 제한적으로 사용할 수 있도록 하는 임시키를 생성하여 임시키 발행모듈을 더 포함하는 것을 특징으로 하는 블록체인을 기반으로 한 구매 영수증 관리 시스템.

【청구항 6】

블록체인을 기반으로 한 구매 영수증 관리 방법에 있어서,

블록체인을 기반으로 한 구매 영수증 관리 시스템에 로그인하는 단계,

사용자의 SNS 계정을 인증하는 단계,

SNS 계정 정보를 기반으로 접근 권한을 확인하는 단계,

상기 사용자의 접근 권한에 따라 블록체인 네트워크 상에 배포된 NFT 형태의 영수증에 관한 소유권 이전 및 구매 기록을 관리하는 단계를 포함하는 것을 특징으로 하는 방법.

【청구항 7】

제6항에 있어서,

상기 사용자가 종이 형태의 구매 영수증 이미지를 업로드하면 NFT 형태의 데이터로 변환하는 단계를 더 포함하는 것을 특징으로 하는 방법.

【청구항 8】

제7항에 있어서,

상기 변환하는 단계에서 OCR 기능을 적용하는 것을 특징으로 하는 방법.

【요약서】

【요약】

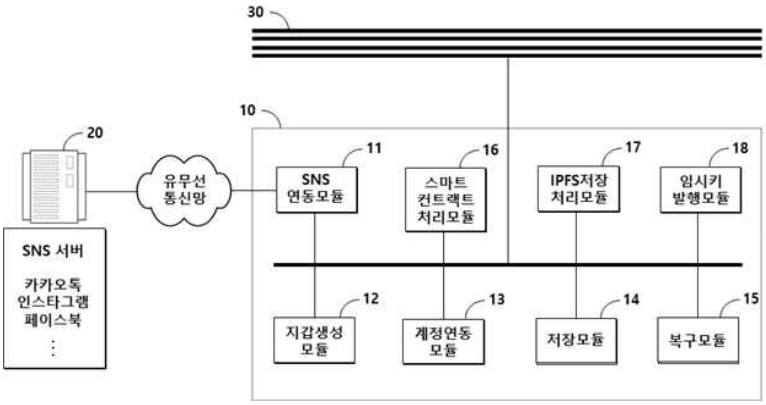
본 발명은 블록체인을 기반으로 한 구매 영수증 관리 시스템 및 그 방법에 관한 것으로, 블록체인 기술과 대체 불가능한 토큰(NFT) 시스템을 활용하여 소비자의 물품 소유권을 디지털화하고, 이를 안전하게 관리함으로써 소유권 증명, A/S 요청, 보험 청구, 중고 거래 등에서 신뢰성과 효율성을 제공할 수 있다.

【대표도】

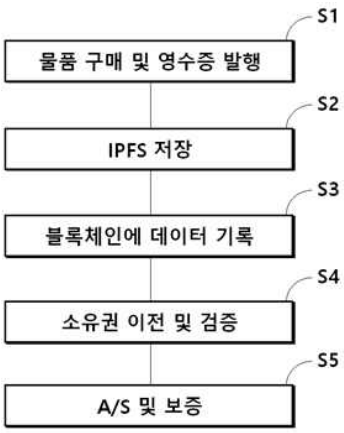
도 1

【도면】

【도 1】


30
10
20
유무선 통신망
SNS 서버
카카오톡
인스타그램
페이스북
SNS 연동모듈
11
스마트 컨트랙트 처리모듈
16
IPFS저장 처리모듈
17
임시키 발행모듈
18
지갑생성 모듈
12
계정연동 모듈
13
저장모듈
14
복구모듈
15

【도 2】


S1
물품 구매 및 영수증 발행
S2
IPFS 저장
S3
블록체인에 데이터 기록
S4
소유권 이전 및 검증
S5
A/S 및 보증