



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0051135
(43) 공개일자 2020년05월13일

(51) 국제특허분류(Int. Cl.)
G06Q 20/36 (2012.01) G06Q 20/06 (2012.01)
G06Q 20/38 (2012.01)
(52) CPC특허분류
G06Q 20/367 (2013.01)
G06Q 20/065 (2013.01)
(21) 출원번호 10-2018-0134080
(22) 출원일자 2018년11월04일
심사청구일자 없음

(71) 출원인
김성일
서울특별시 송파구 송파대로 111, 204동 1122호
(문정동, 파크하비오푸르지오)
(72) 발명자
김성일
서울특별시 송파구 송파대로 111, 204동 1122호
(문정동, 파크하비오푸르지오)

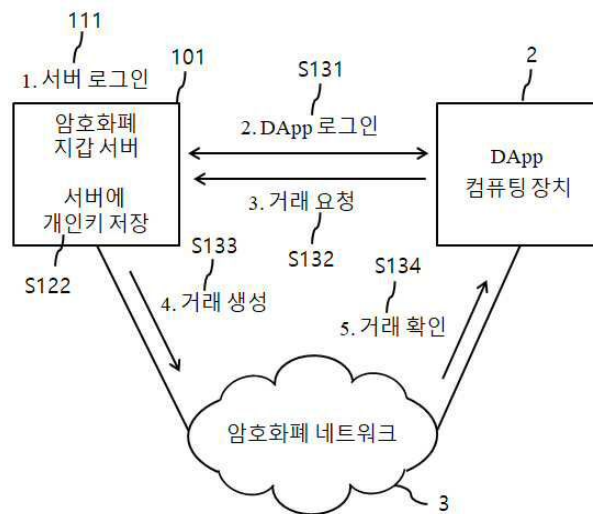
전체 청구항 수 : 총 2 항

(54) 발명의 명칭 암호화폐 지갑서버를 통해 DApp 서비스에 로그인하는 방법 및 이를 위한 암호화폐 지갑서버

(57) 요약

본 발명은, 블록체인 네트워크와 DApp 서비스를 제공하는 DApp 컴퓨팅 장치에 연결되고 사용자 계정으로 로그인하는 암호화폐 지갑 서버를 통해 상기 DApp 서비스를 이용하는 방법에 있어서, 상기 암호화폐 지갑 서버가 상기 사용자 계정에 대한 암호화폐 지갑을 생성하기 위해 계정이름을 포함하여 개인키(프라이빗키)를 생성하고 저장하는 암호화폐 지갑 생성 단계와; 상기 사용자 계정이 상기 DApp 서비스를 사용하기 위해 상기 암호화폐 지갑서버가 상기 DApp 서비스의 로그인을 DApp 컴퓨팅 장치에 요청하여 로그인하는 단계;를 포함하고, 상기 지갑서버가 상기 사용자 계정의 상기 개인키를 독점적으로 관리하기 때문에 상기 사용자 계정이 상기 개인키에 접근할 수 없도록 이루어진 것을 특징으로 한다.

대표도 - 도2



(52) CPC특허분류
G06Q 20/3829 (2013.01)

명세서

청구범위

청구항 1

블록체인 네트워크와 DApp 서비스를 제공하는 DApp 컴퓨팅 장치에 연결되고 사용자 계정으로 로그인하는 암호화폐 지갑 서버를 통해 상기 DApp 서비스를 이용하는 방법에 있어서,

상기 암호화폐 지갑 서버가 상기 사용자 계정에 대한 암호화폐 지갑을 생성하기 위해 계정이름을 포함하여 개인키(프라이빗키)를 생성하고 저장하는 암호화폐 지갑 생성 단계와;

상기 사용자 계정이 상기 DApp 서비스를 사용하기 위해 상기 암호화폐 지갑서버가 상기 DApp 서비스의 로그인을 DApp 컴퓨팅 장치에 요청하여 로그인하는 단계;를 포함하고,

상기 암호화폐 지갑서버가 상기 사용자 계정의 상기 개인키를 독점적으로 관리하기 때문에 상기 사용자 계정이 상기 개인키에 접근할 수 없도록 이루어진 것을 특징으로 하는, 암호화폐 지갑서버를 통해 DApp 서비스를 이용하는 방법

청구항 2

DApp 컴퓨팅 장치가 제공하는 DApp 서비스를 이용하기 위해 처리부와 데이터를 저장하는 저장부와 암호화폐 네트워크와 연결된 통신부를 포함하고 사용자 계정으로 로그인하는 암호화폐 지갑 서버에 있어서,

상기 사용자 계정에 대한 암호화폐 지갑을 생성하기 위해 계정이름을 포함하여 개인키(프라이빗키)를 생성하고,

상기 사용자 계정이 상기 DApp 서비스를 이용하기 위해, DApp 컴퓨팅 장치에게 상기 사용자 계정으로 로그인을 요청하는 상기 처리부와;

상기 지갑 서버의 로그인에 필요한 상기 사용자 계정의 정보와 상기 계정이름과 상기 계정이름과 연결된 상기 개인키를 저장하는 저장부와;

상기 DApp 컴퓨팅 장치와 상기 암호화폐 네트워크에 연결되어 있는 통신부;를 포함하고,

상기 처리부가 상기 사용자 계정의 상기 개인키를 독점적으로 관리하기 때문에 상기 사용자 계정이 상기 개인키를 접근할 수 없도록 처리하는 것을 특징으로 하는, 암호화폐 지갑서버

발명의 설명

기술 분야

[0001]

본 발명은 암호화폐 지갑서버의 암호화폐 지갑으로 DApp 서비스를 이용하는 방법 및 이를 위한 암호화폐 지갑서버에 관한 것으로서, 구체적으로 상기 암호화폐 지갑서버가 사용자 계정의 개인키를 사용자가 볼 수 없도록 이를 비밀리에 관리하는 상태에서 상기 사용자 계정이 DApp 서비스에 로그인하는 방법 및 이를 위한 암호화폐 지갑서버를 제공한다.

배경 기술

[0002]

많은 사람들이 이오스(EOS), 비트코인(Bitcoin), 이더리움(Ethereum) 및 라이트코인(lite coin) 등의 암호화폐들(cryptocurrencies)의 사용률이 증가하고 이제 이런 암호화폐의 이용범위가 DApp 서비스로 넓어지고 있다. 또한 EOS나 이더리움과 같은 DApp(Decentralized application), 즉 분산 어플리케이션을 실행할 수 있는 DApp 플랫폼이 일반화되면서 사용자는 여러 회사가 제공한 다양한 DApp 서비스를 이용할 수 있게 되었고, EOS의 DApp 서비스는 <https://dappradar.com/eos-dapps>에서 확인할 수 있다.

- [0003] 이런 DApp 서비스는 과 같이 이를 누구나 사용할 수 있다. 하지만 아이폰의 어플리케이션과 달리, DApp 서비스는 분산된 p2p 네트워크의 블록체인에서 사용하도록 프로그래밍 된 분산 어플리케이션을 말하고 이 때문에 이들은 분명한 차이가 존재한다. 이런 DApp은 스마트컨트랙트(smart contract)라고도 불린다.
- [0004] EOS 및 이더리움은 암호화폐 DApp 플랫폼으로서 다양한 회사들이 이들 네트워크에서 동작하는 DApp 서비스를 개발하여 이를 이미 제공하고 있다. 현재 EOS에서 DApp 서비스를 이용하기 위해서는 스캐터(scatter), 미원 지갑(meet.one wallet) 및 Nova 지갑 등을 설치하고 사용자의 개인키를 상기 지갑에 등록한 후에 DApp 서비스에 로그인하여 이를 이용한다.
- [0005] 하지만 모든 종류의 암호화폐 지갑은 사용자의 개인키를 사용자 자신이 관리한다. 즉 이런 지갑은 사용자의 개인키를 지갑의 비밀번호 등으로 상기 개인키를 암호화하여 사용자 단말에 저장한다. 즉 암호화폐 지갑의 개인키를 사용자가 직접 관리하는 것이다. 이 때문에 만일 사용자가 암호화폐 지갑의 개인키를 분실하거나 실수로 지갑을 삭제한 상태에서 상기 사용자가 자신의 개인키를 분실했다면, 상기 사용자는 자신의 암호화폐를 찾을 방법이 전혀 없다. 즉 사용자가 암호화폐 지갑의 개인키를 분실하면 자신의 암호화폐를 분실하게 되는 단점이 발생했다.
- [0006] 이와 달리 기존의 암호화폐 거래소는 사용자를 대신하여 거래소의 서버가 상기 사용자의 비밀키를 보관하고, 이를 사용자가 볼 수 없도록 비밀리에 관리한다. 하지만 이들 거래소는 거래소의 사용자 계정으로 DApp 서비스에 로그인하여 상기 DApp 서비스를 이용하는 방법을 제공하지는 못한다.

선행기술문헌

특허문헌

- [0007] (특허문헌 0001) 한국특허출원번호 10-2018-0047101: 블록체인 기반의 암호화폐와 전자지갑 관리 시스템

발명의 내용

해결하려는 과제

- [0008] 본 발명은 상기와 같은 문제점을 해결하기 위해 창안한 것으로, 암호화폐 지갑서버의 상기 사용자 계정이 DApp 서비스에 로그인하여 이를 이용하는 방법 및 암호화폐 지갑서버를 제공한다.
- [0009] 본 발명은 암호화폐 지갑서버가 상기 개인키를 비밀리에 보관하면서 DApp 서비스에 로그인하는 방법 및 암호화폐 지갑서버를 제공한다.

과제의 해결 수단

- [0010] 상기한 목적을 달성하기 위해서 본 발명은, 블록체인 네트워크와 DApp 서비스를 제공하는 DApp 컴퓨팅 장치에 연결되고 사용자 계정으로 로그인하는 암호화폐 지갑 서버를 통해 상기 DApp 서비스를 이용하는 방법에 있어서, 상기 암호화폐 지갑 서버가 상기 사용자 계정에 대한 암호화폐 지갑을 생성하기 위해 계정이름을 포함하여 개인키(프라이빗키)를 생성하고 저장하는 암호화폐 지갑 생성 단계와; 상기 사용자 계정이 상기 DApp 서비스를 사용하기 위해 상기 암호화폐 지갑서버가 상기 DApp 서비스의 로그인을 DApp 컴퓨팅 장치에 요청하여 로그인하는 단계;를 포함하고, 상기 지갑서버가 상기 사용자 계정의 상기 개인키를 독점적으로 관리하기 때문에 상기 사용자 계정이 상기 개인키에 접근할 수 없도록 이루어진 것을 특징으로 한다.

발명의 효과

- [0011] 본 발명은 상기와 같은 문제점을 해결하기 위해 창안한 것으로, 암호화폐 지갑서버의 상기 사용자 계정이 DApp 서비스에 로그인하여 이를 이용하는 방법을 제공하는 효과가 있다.
- [0012] 본 발명은 암호화폐 지갑서버가 상기 개인키를 비밀리에 보관하면서 DApp 서비스에 로그인하는 방법 및 암호화폐 지갑서버를 제공하는 효과가 있다.

도면의 간단한 설명

- [0013] 도 1는 기존 암호화폐 지갑을 이용하여 DApp 서비스를 이용하는 간략한 구성도 및 작업 흐름
- 도 2는 본 발명의 일 실시예에 따른 암호화폐 지갑서버의 사용자 계정으로 DApp 서비스를 이용하는 간략한 구성도 및 작업 흐름
- 도 3은 본 발명의 일 실시예에 따른 암호화폐 지갑서버(101)에서 제공하는 지갑 서비스를 이용하기 위한 흐름도
- 도 4는 본 발명의 일 실시예에 따른 암호화폐 지갑서버가 제공하는 지갑서비스 중에서 계정이름을 생성하는 단말 화면(201)의 예
- 도 5은 본 발명의 일 실시예에 따른 암호화폐 지갑서버에 사용자 계정이 DApp 서비스를 이용하는 흐름도
- 도 6는 본 발명의 일 실시예에 따른 지갑 서비스의 사용자 계정으로 로그인하기 위한 DApp 서비스의 화면(150)의 예
- 도 7은 본 발명의 일 실시예에 따른 지갑 서비스에서 DApp 서비스를 이용하기 위한 시스템

발명을 실시하기 위한 구체적인 내용

- [0014] 이하 첨부된 도면을 참조하여 본 발명을 용이하게 실시할 수 있는 바람직한 일 실시예를 상세히 설명한다. 다만, 본 발명의 바람직한 일 실시예에 대한 동작 원리를 상세하게 설명함에 있어 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 상세한 설명을 생략한다. 이는 불필요한 설명을 생략함으로써 본 발명의 핵심을 흐리지 않고 더욱 명확히 전달하기 위함이다. 또한 본 발명은 일 실시예에 의해 제한하거나 한정하는 것은 아니며, 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낼 수 있다.
- [0015] 본 명세서에서 사용하는 용어는 일 실시예를 설명하기 위해 사용된 것으로, 본 발명을 이것에 한정하려는 의도가 아니고, 단수의 표현은 문맥상 명백하게 다르게 의미하지 않는 한, 복수의 표현을 포함할 수 있다.
- [0016] 본 명세서에서 암호화폐 네트워크는 다수의 노드들(nodes)이 피어투피어(peer-to-peer, p2p) 네트워크를 구성하고 이 노드들의 합의에 의해 거래들이 블록체인에 기록하고 블록을 주기적으로 추가하여 업데이트한다. 여기서 블록체인은 분산 원장(distributed ledger)이라고 부르기도 한다. 상기 블록체인은 방향성 비순환 그래프(Directed Acyclic Graph, DAG) 기술을 이용하는 분산원장 등을 포함할 수 있다. 여기서 상기 노드들은 블록생산자(block producers), 또는 검증인들(validators) 등 다양한 이름으로 불릴 수 있지만 모두 블록체인을 유지 및 관리하고 P2P 네트워크를 유지하는 역할을 한다.
- [0017] 본 명세서에서 암호화폐는 p2p 네트워크에서 분산된 다수의 노드들(nodes)의 합의에 의해서 거래들을 처리하여 상대방에게 상기 암호화폐를 유무선으로 전송할 수 있는 임의의 기술에 의한 전자화폐를 말한다. 상기 암호화폐는 EOS, 이더리움(ethereum), 비트코인(bitcoin) 등과 같이 p2p 네트워크에서 블록체인에 거래를 기록하여 이들을 코인을 거래할 수 있다. 상기 거래는 개인키(private key)를 포함한 암호화폐 지갑이 디지털 사인하여 소유권을 입증하고 이를 암호화폐 네트워크에 전파시키면 상기 거래에 대한 검증 후에 이를 블록체인에 포함시켜서 거래를 완료한다.
- [0018] 본 명세서에서 암호화폐 지갑은 암호화폐를 보관 및 관리를 할 수 있는 암호화폐를 위한 지갑으로 암호화폐를 보내고 받을 수 있도록 공개키와 개인키를 저장하여 거래에 디지털 사인을 한다. 본 명세서에서 개인키를 저장한다는 것은 암호화폐 지갑에 상기 개인키를 생성하여 상기 암호화폐 지갑을 사용할 수 있는 상태로 만드는 것일 수 있다.
- [0019] 도 1는 기존 암호화폐 지갑을 이용하여 DApp 서비스를 이용하는 간략한 구성도 및 작업 흐름을 보여준다.
- [0020] 도 1의 기존 암호화폐 지갑에서 DApp 서비스를 이용하는 방법을 보여주고, 이것은 암호화폐 지갑(1)과 DApp 컴퓨팅장치(2)와 암호화폐 네트워크(3)로 구성된다. 예를 들면 상기 암호화폐 지갑(1)은 스캐터 지갑 및 Nova 지갑과 같은 EOS 지갑일 수 있고, 또한 이더리움이나 트론 등과 같은 암호화폐 지갑일 수 있다.
- [0021] 상기 암호화폐 지갑(1)은 사용자 단말에서 해당하는 컴퓨팅 프로그램에 의해서 동작하는 것일 수 있다. 예로 DApp 서비스를 이용하기 위한 EOS 지갑은 일반적으로 설치 후 상기 지갑에 가입을 할 때 비밀번호만 입력하고 사용자 계정(이것은 id 등과 같이 사용자를 구별하기 위한 목적의 계정정보임)을 입력하지 않는다. 이것은 이 지갑은 해당 단말 사용자만 이를 이용하기 때문이다. 즉 사용자 단말에 자신의 개인키(private key)를 저장하여 암호화폐 지갑을 사용하기 때문에 상기 지갑은 사용자 계정으로 사용자를 구분하지 않는다. 이런 때문에 단말에

서 사용하는 암호화폐 지갑은 회원관리가 전혀 필요가 없다.

- [0022] 사용자는 상기 암호화폐 지갑을 설치 후 로그인을 위한 비밀번호를 입력한 후에 상기 지갑을 사용하기 위한 개인키를 저장(16)하여 상기 지갑을 이용할 수 있다. 이때 상기 개인키는 일반적으로 상기 지갑의 로그인에 사용된 비밀번호나 12단어나 24 단어의 시드(seed) 등으로 암호화되어서 사용자 단말에 저장된다. 본 명세서에서 이런 암호화폐 지갑을 단말 지갑이라 부르겠다. 그리고 단말 지갑에서 상기 개인키의 저장(16)이 완료되면, 이제 단말 지갑의 사용자는 DApp 컴퓨팅 장치(2)가 제공하는 DApp 서비스에 로그인을 이용할 수 있다. 본 명세서에서 DApp 서비스는 사용자가 단말의 화면을 통해 DApp 서비스를 이용할 수 있도록 제공될 수 있다.
- [0023] 이런 상태에서 상기 사용자가 상기 DApp 서비스를 이용하려면, 상기 사용자는 상기 DApp 컴퓨팅장치(2)가 제공하는 DApp 서비스에 로그인을 해야 한다. 상기 사용자가 상기 DApp 서비스에 로그인을 요청하면 상기 단말 지갑이 이 요청을 승인하면 사용자 계정이 상기 DApp 서비스에 로그인(12)이 된다.
- [0024] EOS에는 이미 갬블링과 게임 등과 같은 아주 많은 DApp 서비스가 이미 서비스를 시작했다. 사용자는 이미 Scatter과 같은 EOS의 단말 지갑을 사용하여 상기 DApp 서비스에 로그인하여 상기 DApp 서비스를 이용하고 있다.
- [0025] 상기 DApp 서비스에 로그인 후 상기 사용자가 상기 DApp 서비스에서 특정한 거래를 요청을 선택하면, DApp 컴퓨팅장치(2)는 상기 단말 지갑(1)으로 상기 특정한 거래를 요청(13)을 전송한다. 상기 거래의 요청을 받은 상기 단말 지갑(1)은 이를 검증한 후에 특정 거래(14)를 생성하여 이를 암호화폐 네트워크(3)로 전파시킨다. 이때 상기 거래는 상기 단말 지갑(1)에 저장된 개인키로 디지털 서명을 포함하여 상기 거래(14)를 생성한다. 상기 전파된 거래(14)는 암호화폐 네트워크(3)의 노드들의 검증을 거친 후에 블록체인에 기록된다. 그리고 DApp 컴퓨팅장치(2)가 상기 블록체인에 기록된 거래를 확인(15)한다.
- [0026] 본 발명에서 DApp 컴퓨팅장치(2)는 상기 암호화폐 네트워크(3)와 상기 지갑(1)과 통신으로 연결되어 있고, 또한 상기 DApp 컴퓨팅장치(2)는 상기 암호화폐 네트워크(2)의 일부일 수 있다. 따라서 상기 DApp 컴퓨팅 장치(2)는 상기 네트워크(2)의 노드로 참여하여 p2p 네트워크를 유지하고 거래를 블록체인에 기록하는 노드로서의 역할을 담당할 수 있다. 본 명세서에서 상기 DApp 컴퓨팅 장치(2)는 암호화폐 네트워크(3)를 구성하는 노드 또는 상기 노드 역할을 하지 않는 서버 또는 단말 또는 이들의 조합으로 구성될 수 있다. 따라서 DApp 서비스는 암호화폐 네트워크에서 동작하는 스마트컨트랙트(smart contract) 그리고 서버 또는 단말에서 동작하는 임의의 프로그램밍 프로그램, 또는 이들의 조합에 의해 동작하는 임의의 프로그램으로 구성될 수 있다.
- [0027] 도 2는 본 발명의 일 실시예에 따른 암호화폐 지갑서버의 사용자 계정으로 DApp 서비스를 이용하는 간략한 구성도 및 작업 흐름을 보여준다.
- [0028] 본 발명에 의한 암호화폐 지갑서버(101)은 DApp 컴퓨팅장치(2)와 암호화폐 네트워크(3)와 통신망으로 연결된다. 사용자는 상기 암호화폐 지갑서버에서 제공하는 지갑서비스를 이용하기 위해 사용자 계정(일반적으로 id와 같이 사용자 계정을 구분할 수 있는 사용자 정보)을 입력하고 상기 지갑 서비스의 회원으로 가입하여 상기 사용자 계정으로 상기 지갑서비스에 로그인(111)할 수 있다.
- [0029] 그리고 상기 지갑서버(101)는 상기 사용자가 상기 지갑서비스에서 제공하는 암호화폐 지갑을 사용하기 위해 사용자의 개인키(private key)를 생성 및 저장하고 이를 상기 사용자가 볼 수 없도록 비공개로 관리한다. 상기 지갑서버에 상기 개인키를 등록하여 사용자는 상기 지갑서비스에서 해당하는 지갑을 이용할 수 있다. 이때 상기 지갑서버(101)는 사용자의 개인키를 독점적으로 관리하고, 상기 사용자는 이에 접근할 수 없다. 본 명세서에 개인키에 접근할 수 없다는 것은 사용자가 지갑서버(101)에서 제공한 지갑서비스에서 개인키의 생성 단계를 포함한 모든 상태에서 자신의 개인키를 확인하거나 볼 수 없도록 구성되었다는 것을 의미한다. 상기 사용자 계정은 상기 지갑서비스에 개인키를 등록한 후 상기 지갑서비스를 사용할 수 있다.
- [0030] 사용자가 상기 지갑서비스에 로그인(111)을 한 후, DApp 컴퓨팅장치에서 제공한 DApp 서비스를 이용하기 위해서는 상기 DApp 서비스에 다시 로그인(S131)을 해야 한다. 상기 DApp 서비스의 로그인(S131)은 상기 지갑 서비스의 사용자 계정 등의 사용자 정보 또는 개인키를 바탕으로 사용자를 구분할 수 있도록 구성될 수 있다. 상기 지갑서버(101)는 사용자를 사용자 계정으로 구분하여 해당하는 서비스를 제공할 수 있다.
- [0031] 여기서 상기 지갑 서비스는 사용자가 사용자 단말에서 이용할 수 있고 암호화폐 네트워크와 연결된 임의의 형태의 서비스를 말하며, 사용자 단말은 스마트폰 및 노트북 등을 포함할 수 있다. 도 4는 계정이름 생성에 대한 상기 지갑 서비스를 단말화면에 보인 예이다.

- [0032] 도 3은 본 발명의 일실시예에 따른 암호화폐 지갑서버(101)에서 제공하는 지갑 서비스를 이용하기 위한 흐름도를 보여준다.
- [0033] 본 발명은 사용자가 사용자 계정으로 지갑서버(101)가 제공하는 지갑서비스에 가입하는 단계(S121)와; 상기 사용자 계정에 대한 **계정이름**을 포함하여 개인키를 생성하여 이를 상기 지갑 서버(101)에 저장하여 암호화폐 지갑을 활성화하는 단계(S122)를 포함하여 구성할 수 있다. 이를 통해서 상기 사용자는 암호화폐 지갑을 사용할 수 있다. 본 발명은 암호화폐 지갑을 사용하기 위해서 계정이름과 이에 해당하는 개인키를 생성하여 등록한 후에 상기 지갑서버가 제공하는 지갑서비스를 이용할 수 있다. 상기 지갑서비스는 DApp 서비스에 로그인하여 DApp 서비스를 이용하고 암호화폐의 입출금 서비스 등을 제공하도록 구성할 수 있다.
- [0034] 본 발명의 암호화폐 지갑서버(101)가 제공하는 지갑서비스는 사용자의 공개키 대신에 사용할 수 있는 계정이름을 포함하고, 상기 공개키에 해당하는 개인키를 생성한 후에 이를 상기 지갑서버의 저장부에 저장한다.
- [0035] 참고로, 암호화폐는 비대칭 암호를 사용하고, 이것은 공개키(public key)와 개인키(private key)로 구성된다. 암호화폐 지갑에 개인키를 저장하면 상기 개인키와 짝이 되는 공개키는 바로 생성할 수 있다. 그리고 암호화폐 지갑이 거래를 발생시킬 때 상기 거래를 상기 개인키로 디지털 사인을 해서 소유권을 입증한다. 상기 디지털 사인된 거래는 암호화폐 네트워크로 전파되고, 암호화폐 네트워크는 해당하는 공개키로 상기 거래를 검증한 후에 이를 블록체인에 기록한다.
- [0036] 암호화폐 네트워크에서 상대방에게 암호화폐를 전송할 때 상대방의 공개키로 상기 암호화폐를 전송하는 것이 일반적이다. 예로 들면, 이더리움의 공개키는 0x0caff12817de13aB5195E706Dc3E9CdF90A010a6 와 같이 매우 길기 때문에 이를 사용자가 기억할 수 없다. 이런 이유 때문에 EOS 등에서는 상기 공개키 대신에 사용자가 기억하기 쉬운 계정이름으로 이체 거래를 할 수 있다. 이는 공개키에 해당하는 상기 계정이름을 블록체인에 기록하고 상기 공개키 대신에 계정이름으로 암호화폐를 거래하는 방법이다. 예를 들면, EOS, steemit 등과 같은 암호화폐를 전송할 때 공개키 대신에 상기 계정이름을 사용하여 이체할 수 있다. EOS를 예를 들면 계정이름은 일반적으로 12자 길이로 abcdefghij12와 같이 만들 수 있다.
- [0037] 도 4는 본 발명의 일실시예에 따른 암호화폐 지갑서버가 제공하는 지갑서비스 중에서 계정이름을 생성하는 단말 화면(201)의 예를 보여준다.
- [0038] EOS의 지갑인 scatter 지갑 등에 비밀키를 등록할 때 상기 계정이름도 같이 등록한다. EOS에서 키 등록은 1) 계정이름과 2) 개인키를 입력하여 암호화폐 지갑에 이를 저장 또는 등록하여 상기 지갑을 활성화하는 과정이다. 즉 상기 도면은 EOS의 지갑에서 개인키 등록과정 중에서 계정이름을 사용자가 입력(202)하는 화면의 예를 보여준다.
- [0039] 상기 계정이름은 공개키를 대신하여 상대방에게 EOS 토큰을 보내는 주소 등으로 사용된다. 본 발명에 따른 지갑 서버는 상기 계정이름을 사용자로부터 입력받아 이를 계정 서비스에 사용할 수 있다. 본 발명에서 상기 계정이름은 상기 지갑서버가 임의의 계정이름을 생성하거나 도 4와 같이 사용자가 입력한 것을 사용하도록 구성할 수 있다. 상기 도면은 사용자가 계정이름을 단말의 화면(201)로부터 입력받는 예를 보여준다.
- [0040] 본 발명에서 계정이름을 포함하여 개인키를 생성한다는 것은 암호화폐 지갑에 개인키를 생성하는 과정에 계정이름을 포함하는 것을 말한다. 이와 같이 상기 계정이름을 블록체인에 기록하여, 상기 개인키에서 발생된 공개키 대신에 상기 계정이름을 암호화폐 네트워크에서 사용할 수 있다.
- [0041] 도 5은 본 발명의 일실시예에 따른 암호화폐 지갑서버에 사용자 계정이 DApp 서비스를 이용하는 흐름도를 보여준다.
- [0042] 지갑서버(101)의 지갑서비스에 로그인(111)한 사용자 계정은 DApp 컴퓨팅 장치(2)가 제공하는 DApp 서비스 (사이트)에 로그인(S131)한 후에 상기 DApp 서비스를 이용할 수 있다. 상기 사용자 계정이 상기 DApp 서비스에 로그인하기 위해, 상기 DApp 컴퓨팅장치(2)는 상기 DApp 서비스에 로그인(S131)을 위한 정보를 상기 지갑서버(101)로부터 받아서 로그인을 처리할 수 있다.
- [0043] 도 5의 흐름도와 같이, 본 발명은 지갑서버(101)가 제공하는 지갑서비스에 로그인한 사용자 계정이 DApp 컴퓨팅 장치(2)가 제공하는 DApp 서비스에 로그인(S131)하는 단계와; 상기 지갑서버(101)가 DApp 컴퓨팅장치(2)로부터 거래를 요청을 받는 단계(S132)와; 상기 지갑서버(101)가 상기 거래를 생성하여 암호화폐 네트워크(3)에 전파하는 단계(S133)와; DApp 서비스에서 상기 거래를 암호화폐 네트워크를 통해 확인하는 단계(S134)를 더 포함하여 구성될 수 있다.

- [0044] 상기 도 3과 도 5도의 흐름도를 이용하여 도 2에 보인 본 발명에 의한 DApp 서비스를 이용하기 위한 간략한 작업흐름을 설명하면 다음과 같다.
- [0045] 사용자가 암호화폐 지갑서버(101)가 제공하는 지갑 서비스에 사용자 계정 및 자신의 정보를 입력하여 회원으로 가입을 한다. 상기 지갑서버는 사용자 계정으로 사용자를 구분하여 회원관리를 하고 해당하는 서비스를 제공할 수 있다. 상기 사용자 계정이 상기 지갑 서비스에서 암호화폐 지갑을 이용하기 위해서, 상기 지갑서버(101)는 상기 사용자 계정의 개인키를 저장하며 상기 저장은 해당 지갑에 개인키를 등록하는 것을 말할 수 있다. 이때 상기 지갑서버는 상기 개인키에 해당하는 공개키와 연결된 계정이름을 포함하여 저장할 수 있다. 이를 통해 상기 지갑서버(101)에서 상기 사용자 계정의 지갑 생성이 완료되고, 상기 사용자 계정은 자신의 계정 정보를 이용하여 상기 지갑서비스에 로그인(111)을 하여 지갑서비스를 이용할 수 있다. 즉 상기 사용자 계정의 지갑이 상기 지갑서버(101)에 생성되면, 상기 사용자 계정은 DApp 컴퓨팅장치(2)가 제공하는 DApp 서비스에 로그인(S131)하여 자신의 지갑을 이용할 수 있다.
- [0046] 상기 지갑서비스에 로그인(111)한 사용자 계정이 DApp 컴퓨팅장치(2)가 제공하는 DApp 서비스에 로그인(S131)하는 과정에 대한 일실시예는 아래와 같다.
- [0047] 도 5의 흐름도와 같이, 상기 지갑서비스의 상기 사용자 계정이 상기 DApp 서비스에서 로그인(S131)을 요청하면, 상기 지갑서버는 상기 요청에 대한 결과를 상기 DApp 컴퓨팅장치로 전송하여 로그인을 완료(S131)할 수 있다. 구체적인 예를 들면, 상기 로그인 요청을 받으면, 상기 DApp 컴퓨팅장치(2)는 이를 위한 로그인 화면을 제공하고 사용자 계정에 의해 로그인이 선택되면, 지갑서버(101)가 DApp 컴퓨팅 장치(2)에게 미리 정해진 형태로 로그인을 요청하고, 상기 DApp 컴퓨팅 장치(2)에서 상기 요청에 대한 결과를 상기 지갑서버(101)에 전송하여 상기 로그인을 완료(S131)하도록 이루어질 수 있다. 상기 로그인 요청은 상기 사용자의 계정 정보 또는 사용자 계정의 비밀키를 디지털 사인하여 이를 인증할 수 있다.
- [0048] 이와 달리, 본 발명에서 상기 사용자 계정의 DApp 서비스의 로그인(S131)은 DApp 컴퓨팅 장치(2)에서 상기 지갑서버(101)로 로그인을 요청하고, 상기 지갑서버가 이에 대한 결과를 제공하여 상기 DApp 컴퓨팅 장치에서 상기 로그인(S131)을 처리할 수도 있다.
- [0049] 상기 사용자 계정이 상기 DApp 서비스에 로그인(S131)을 완료하면, 상기 사용자 계정은 상기 DApp 서비스가 제공하는 다양한 서비스를 이용할 수 있다. 만일 상기 사용자 계정이 상기 DApp 서비스에서 특정한 거래를 요청하면 DApp 컴퓨팅장치는 이를 상기 지갑서버(101)에 이를 요청(S132)하도록 구성될 수 있다.
- [0050] 이 경우, 상기 지갑서버(101)는 상기 거래에 대한 요청을 받고 상기 요청이 검증을 통과하면, 상기 지갑서버에 저장된 개인키로 상기 거래를 생성(S133)하여 이를 암호화폐 네트워크(3)로 전파시키도록 구성될 수 있다. 그 후 전파된 상기 거래는 상기 DApp 컴퓨팅장치(2)가 이를 확인(S134)하고 상기 사용자 계정을 위한 해당 작업을 진행한다.
- [0051] 도 6는 본 발명의 일 실시예에 따른 지갑 서비스의 사용자 계정으로 로그인하기 위한 DApp 서비스의 화면(150)의 예를 보여준다.
- [0052] 상기 도면은 지갑서버(101)에서 제공하는 지갑 서비스에 이미 로그인(111)한 상태의 사용자 계정이 DApp 서비스의 화면(150)에서 DApp 서비스에 로그인(S131)하는 방법의 한 예를 보여준다. 구체적으로 상기 사용자 계정이 상기 로그인 버튼(152)을 선택하면, 상기 사용자 계정이 상기 DApp 서비스에 로그인(S131)하기 위한 창이 사용자의 단말에 생성되고, 해당 사용자가 이를 선택하면 상기 사용자 계정이 상기 DApp 서비스에 로그인(S131)이 되도록 구성된다.
- [0053] 이와 다른 로그인(S131) 방법의 예를 들면, 사용자 계정이 사용자 단말의 지갑서비스에 있는 DApp 서비스의 로그인 버튼을 누르면 지갑서버(101)가 상기 DApp 컴퓨팅장치에 이에 대한 로그인 요청을 하여 이를 완료하도록 구성할 수 있다.
- [0054] 본 발명은, 블록체인 네트워크(3)와 DApp 서비스를 제공하는 DApp 컴퓨팅 장치(2)에 연결되고 사용자 계정으로 로그인하는 암호화폐 지갑 서버(101)를 통해 상기 DApp 서비스를 이용하는 방법에 있어서, 상기 암호화폐 지갑서버(101)가 상기 사용자 계정에 대한 암호화폐 지갑을 생성하기 위해 계정이름을 포함하여 개인키(프라이빗 키)를 생성하고 저장하는 암호화폐 지갑 생성 단계(S122)와; 상기 사용자 계정이 상기 DApp 서비스를 사용하기 위해 상기 지갑서버가 상기 DApp 서비스의 로그인을 DApp 컴퓨팅 장치에 요청하여 로그인하는 단계(S131);를 포함하고, 상기 암호화폐 지갑서버(101)가 상기 사용자 계정의 상기 개인키를 독점적으로 관리하기 때문에 상기

사용자 계정이 상기 개인키에 접근할 수 없도록 이루어진 것을 특징으로 한다.

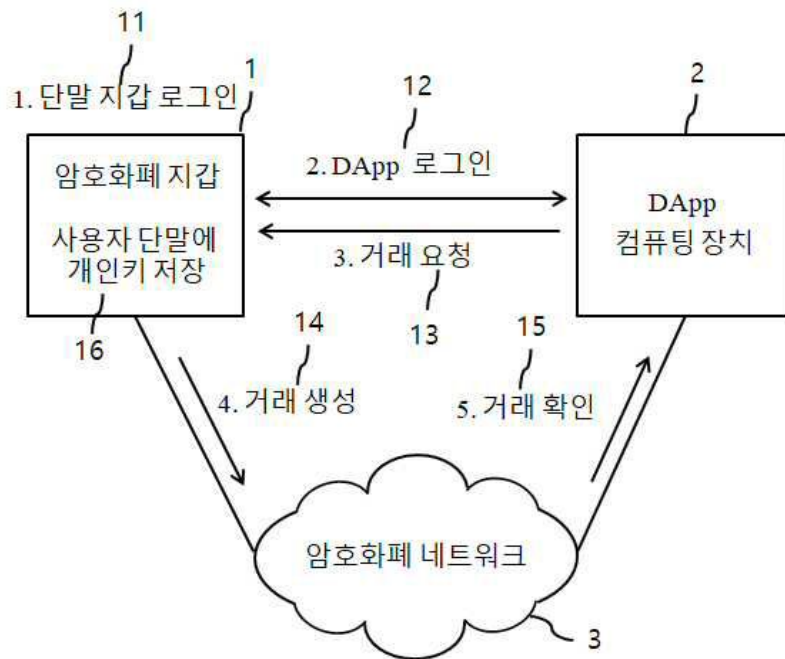
- [0055] 본 발명에서 상기 지갑서버(101)가 상기 서버의 저장부에 상기 사용자 계정 및 이와 관련된 정보를 저장하여 상기 사용자 계정에 대한 회원관리를 하는 것을 특징으로 한다.
- [0056] 본 발명에서 상기 DApp 서비스의 로그인은 상기 지갑서버가 상기 DApp 컴퓨팅장치에 상기 사용자 계정의 정보를 보내서 인증하거나 사용자 계정의 비밀번호를 디지털 사인하여 이를 인증하는 것을 특징으로 한다.
- [0057] 도 7은 본 발명의 일실시예에 따른 지갑 서비스에서 DApp 서비스를 이용하기 위한 시스템을 보여준다.
- [0058] 본 발명에 의한 암호화폐 지갑서버(161)은 처리부(161a)와; 저장부(161b)와; 통신부(161c)로 구성되고, 상기 통신부(161c)는 암호화폐 네트워크(3)와 DApp 컴퓨팅장치(2)와 통신으로 연결된다. 상기 지갑서버(162)와 상기 컴퓨팅장치(2)는 암호화폐 네트워크와 그 외의 통신네트워크로 서로 연결될 수 있다.
- [0059] 본 발명은, DApp 컴퓨팅 장치(2)가 제공하는 DApp 서비스를 이용하기 위해 처리부(161a)와 데이터를 저장하는 저장부(161b)와 암호화폐 네트워크와 연결된 통신부(161c)를 포함하고 사용자 계정으로 로그인하는 암호화폐 지갑 서버(161)는, 상기 사용자 계정에 대한 암호화폐 지갑을 생성하기 위해 계정이름을 포함하여 개인키(프라이빗키)를 생성하고, 상기 사용자 계정이 상기 DApp 서비스를 이용하기 위해, DApp 컴퓨팅 장치(2)에게 상기 사용자 계정으로 로그인을 요청하는 상기 처리부(161a)와; 상기 지갑 서버(161)의 로그인에 필요한 상기 사용자 계정의 정보와 상기 계정이름과 상기 계정이름과 연결된 상기 개인키를 저장하는 저장부(161b)와;
- [0060] 상기 DApp 컴퓨팅 장치와 상기 암호화폐 네트워크에 연결되어 있는 통신부(161c);를 포함하고, 상기 처리부(161a)가 상기 사용자 계정의 상기 개인키를 독점적으로 관리하기 때문에 상기 사용자 계정이 상기 개인키를 접근할 수 없도록 처리하는 것을 특징으로 한다.
- [0061] 본 발명에서 상기 처리부(161a)는 상기 계정이름과 연결된 사용자 계정의 상기 개인키를 생성할 때 상기 사용자 계정이 볼 수 없도록 상기 개인키를 비밀리에 생성하도록 이루어진 것을 특징으로 한다.
- [0062] 본 발명에 의한 암호화폐 지갑서버는 DApp 컴퓨팅장치(2)가 제공하는 DApp 서비스에 로그인하거나 연동하여 상기 DApp 서비스를 이용할 수 있는 임의의 기능 또는 구성을 가진 서버 또는 서버의 묶음일 수 있다.
- [0063] 이상에서 설명한 본 발명은, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 있어 본 발명의 기술적 사상을 벗어나지 않는 장소 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시 예 및 첨부된 도면에 의해 한정되는 것이 아니다. 그러나 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등 내지 대체를 포함하는 것으로 이해되어야 한다.

부호의 설명

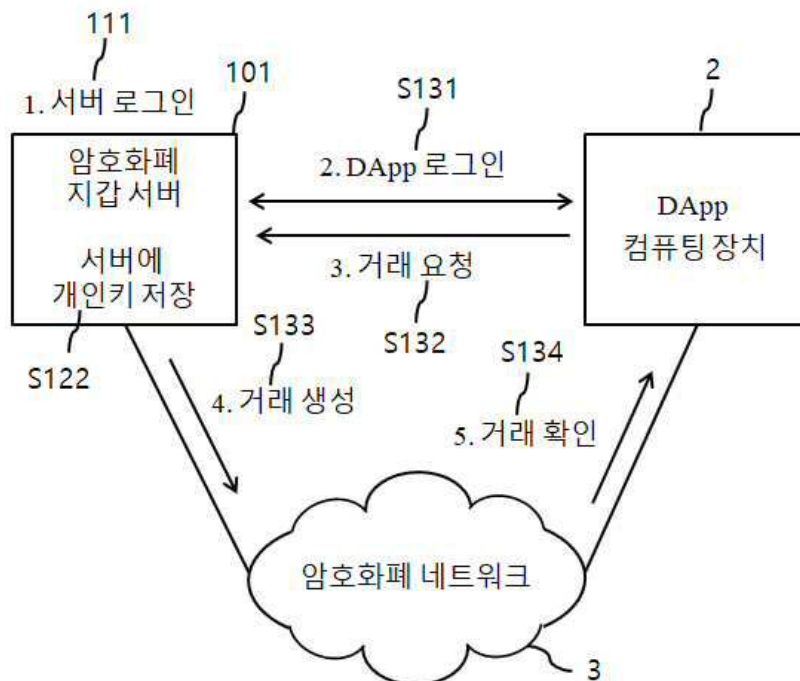
- [0064] 1, 161: 암호화폐 지갑, 2: DApp 컴퓨팅장치, 3: 암호화폐 네트워크, 101: 암호화폐 지갑서버, 150: DApp 서비스의 화면, 161a: 처리부, 161b: DB부, 161c: 통신부, 162: 통신 네트워크, 201: 지갑서비스의 화면, 202:계정이름 입력박스, 203: 계정이름 생성 확인버튼

도면

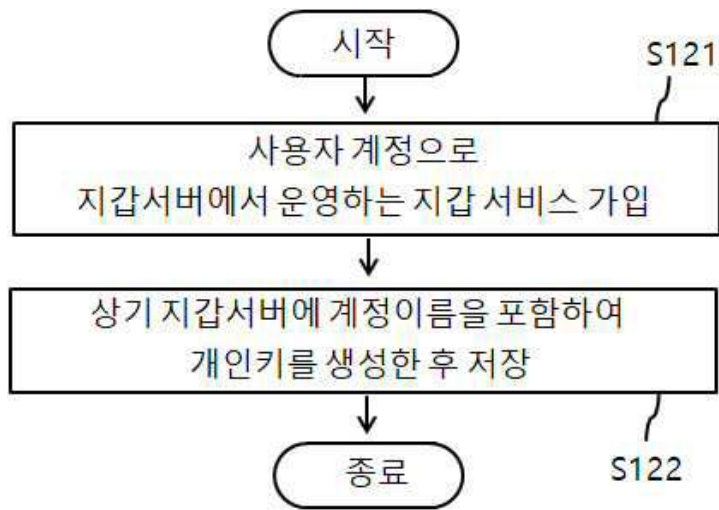
도면1



도면2



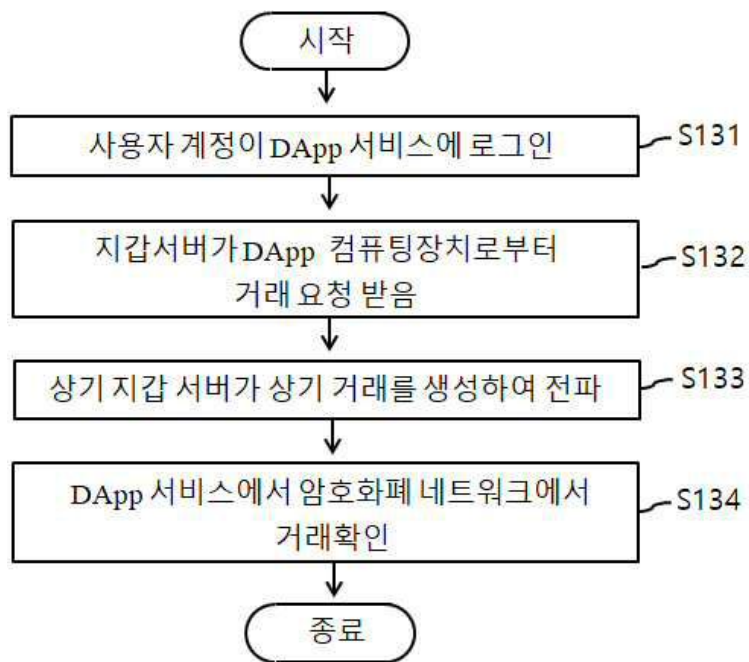
도면3



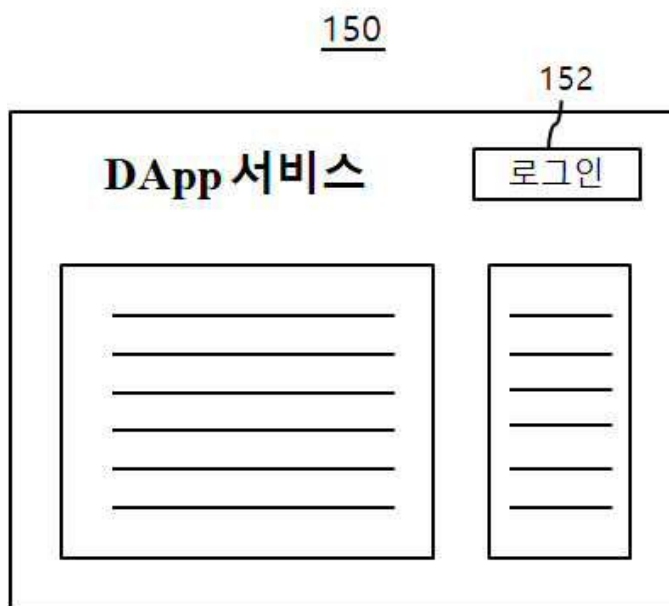
도면4



도면5



도면6



도면7

