



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0048458
(43) 공개일자 2020년05월08일

(51) 국제특허분류(Int. Cl.)

G06Q 20/36 (2012.01)

(52) CPC특허분류

G06Q 20/3678 (2013.01)

G06Q 20/3674 (2013.01)

(21) 출원번호 10-2018-0130572

(22) 출원일자 2018년10월30일

심사청구일자 없음

(71) 출원인

서강대학교산학협력단

서울특별시 마포구 백범로 35 (신수동, 서강대학교)

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

박수용

서울특별시 마포구 독막로18길 5, 101동 1001호(상수동, 상수두산위브아파트)

박재용

서울특별시 송파구 송이로33길 7(문정동)

(뒷면에 계속)

(74) 대리인

특허법인충현

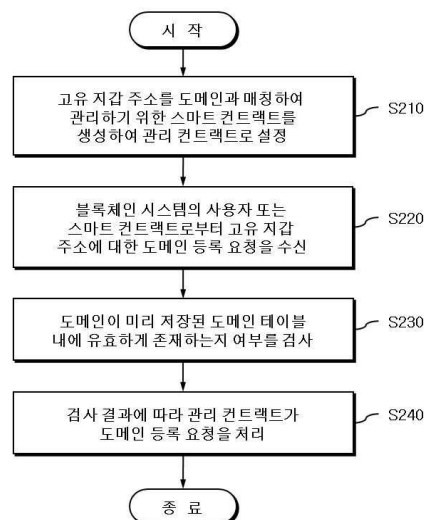
전체 청구항 수 : 총 17 항

(54) 발명의 명칭 **블록체인 시스템의 지갑 주소를 관리하는 방법 및 도메인에 기반한 트랜잭션을 처리하는 방법**

(57) 요약

블록체인(blockchain) 시스템의 지갑 주소를 관리하거나 이를 이용하여 트랜잭션을 처리하는 기술에 관한 것으로, 블록체인 시스템의 고유 지갑 주소를 관리하는 방법은, 고유 지갑 주소를 그에 대응하는 도메인(domain)과 매칭하여 관리하기 위한 스마트 컨트랙트(smart contract)를 생성하여 관리 컨트랙트로 설정하고, 관리 컨트랙트가 블록체인 시스템의 사용자 또는 스마트 컨트랙트로부터 고유 지갑 주소에 대한 도메인 등록 요청을 수신하고, 도메인이 미리 저장된 도메인 테이블 내에 유효하게 존재하는지 여부를 검사하며, 검사 결과에 따라 도메인 등록 요청을 처리한다.

대표도 - 도2



(72) 발명자

인호

서울특별시 용산구 이촌로88길 15, 3동 106호(이촌동, 왕궁아파트)

정종욱

서울특별시 성북구 인촌로 44(안암동3가)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711070410

부처명 과학기술정보통신부

연구관리전문기관 정보통신기술진흥센터(IITP)

연구사업명 정보통신기술인력양성(정보화)

연구과제명 적응형 블록체인 플랫폼 기술 개발 및 전문 인력 양성

기 여 율 1/1

주관기관 서강대학교 산학협력단

연구기간 2018.01.01 ~ 2018.12.31

명세서

청구범위

청구항 1

블록체인(blockchain) 시스템의 고유 지갑 주소를 관리하는 방법에 있어서,

고유 지갑 주소를 그에 대응하는 도메인(domain)과 매칭하여 관리하기 위한 스마트 컨트랙트(smart contract)를 생성하여 관리 컨트랙트로 설정하는 단계;

상기 관리 컨트랙트가 블록체인 시스템의 사용자 또는 스마트 컨트랙트로부터 고유 지갑 주소에 대한 도메인 등록 요청을 수신하는 단계;

상기 관리 컨트랙트가 상기 도메인이 미리 저장된 도메인 테이블 내에 유효하게 존재하는지 여부를 검사하는 단계; 및

상기 검사 결과에 따라 상기 관리 컨트랙트가 상기 도메인 등록 요청을 처리하는 단계;를 포함하는 고유 지갑 주소의 관리 방법.

청구항 2

제 1 항에 있어서,

상기 도메인 등록 요청을 처리하는 단계는,

상기 검사 결과, 상기 도메인이 상기 도메인 테이블 내에 유효하게 중복하여 존재하는 경우 상기 관리 컨트랙트가 상기 도메인 등록 요청을 거부하는 응답을 전송하는 것을 특징으로 하는 고유 지갑 주소의 관리 방법.

청구항 3

제 1 항에 있어서,

상기 도메인 등록 요청을 처리하는 단계는,

상기 도메인 등록 요청이 동시에 복수 개 수신된 경우 상기 검사 결과와 무관하게 상기 관리 컨트랙트가 상기 도메인 등록 요청을 거부하는 응답을 전송하는 것을 특징으로 하는 고유 지갑 주소의 관리 방법.

청구항 4

제 1 항에 있어서,

상기 도메인 등록 요청을 처리하는 단계는,

상기 검사 결과, 상기 도메인이 상기 도메인 테이블 내에 유효하게 중복하여 존재하지 않는 경우 상기 관리 컨트랙트가 상기 도메인 등록 요청에 따라 상기 도메인과 상기 고유 지갑 주소를 매칭하여 상기 도메인 테이블에 저장함으로써 등록 성공을 나타내는 응답을 전송하는 것을 특징으로 하는 고유 지갑 주소의 관리 방법.

청구항 5

제 4 항에 있어서,

상기 도메인 등록 요청을 처리하는 단계는,

상기 도메인과 상기 고유 지갑 주소를 매칭하여 상기 도메인 테이블에 저장하되, 등록이 이루어지는 시간 정보 및 상기 도메인의 유효 상태를 더 포함하여 저장하는 것을 특징으로 하는 고유 지갑 주소의 관리 방법.

청구항 6

제 5 항에 있어서,

상기 도메인 테이블은,

상기 도메인을 포함하는 정보를 키(key) 값으로 하는 해시 테이블(hash table)인 것을 특징으로 하는 고유 지갑 주소의 관리 방법.

청구항 7

제 1 항에 있어서,

상기 관리 컨트랙트가 블록체인 시스템의 사용자의 요청에 따라 상기 도메인 테이블에 저장된 도메인을 변경하거나 점유를 해제하는 명령을 수행하는 것을 특징으로 하는 고유 지갑 주소의 관리 방법.

청구항 8

제 7 항에 있어서,

상기 도메인 테이블에 저장된 도메인의 점유가 해제된 경우 상기 관리 컨트랙트가 해당 도메인에 대한 도메인 등록 요청시 새로운 고유 지갑 주소를 매칭하여 저장하는 명령을 수행하는 것을 특징으로 하는 고유 지갑 주소의 관리 방법.

청구항 9

블록체인(blockchain) 시스템의 트랜잭션을 처리하는 방법에 있어서,

송신자가 송신자 또는 수신자 중 적어도 하나의 고유 지갑 주소에 대응하는 도메인(domain)을 사용하여 트랜잭션을 생성하는 단계;

고유 지갑 주소를 그에 대응하는 도메인과 매칭하여 관리하는 관리 컨트랙트로 설정된 스마트 컨트랙트(smart contract)가 생성된 상기 트랜잭션으로부터 상기 도메인에 대한 조회 요청을 수신하는 단계;

상기 스마트 컨트랙트가 상기 조회 요청에 따라 미리 저장된 도메인 테이블을 검색하는 단계; 및

상기 검색 결과에 따라 상기 스마트 컨트랙트가 상기 도메인에 대응하는 고유 지갑 주소를 획득하여 상기 트랜잭션을 처리하는 단계;를 포함하는 트랜잭션의 처리 방법.

청구항 10

제 9 항에 있어서,

상기 도메인 테이블을 검색하는 단계는,

상기 미리 저장된 도메인 테이블 내에 상기 도메인이 존재하지 않는 경우 상기 트랜잭션을 무효화하는 것을 특징으로 하는 트랜잭션의 처리 방법.

청구항 11

제 9 항에 있어서,

상기 도메인 테이블을 검색하는 단계는,

상기 미리 저장된 도메인 테이블 내에 상기 도메인이 존재하는 경우 상기 도메인에 대응하는 고유 지갑 주소가 여전히 유효한지 여부를 검사하는 단계를 더 포함하는 트랜잭션의 처리 방법.

청구항 12

제 11 항에 있어서,

상기 고유 지갑 주소가 여전히 유효한지 여부를 검사하는 단계는,

상기 도메인에 대응하는 고유 지갑 주소가 만료되었거나 점유가 해제된 경우 유효하지 않는 것으로 판단하는 것을 특징으로 하는 트랜잭션의 처리 방법.

청구항 13

제 11 항에 있어서,

상기 고유 지갑 주소가 여전히 유효한지 여부를 검사하는 단계는,

상기 도메인에 대응하는 고유 지갑 주소가 유효하지 않는 것으로 판단한 경우 상기 트랜잭션을 무효화하는 것을 특징으로 하는 트랜잭션의 처리 방법.

청구항 14

제 9 항에 있어서,

상기 도메인 테이블을 검색하는 단계는,

상기 미리 저장된 도메인 테이블 내에 상기 도메인이 존재하되 도메인에 대응하는 고유 지갑 주소가 복수 개인 경우 복수 개의 고유 지갑 주소 중 가장 최근에 등록된 유효한 값을 획득하는 것을 특징으로 하는 트랜잭션의 처리 방법.

청구항 15

제 9 항에 있어서,

상기 트랜잭션을 처리하는 단계는,

상기 도메인에 대응하는 유효한 고유 지갑 주소가 획득된 경우 수신자가 사람이면 송금을 처리하는 것을 특징으로 하는 트랜잭션의 처리 방법.

청구항 16

제 9 항에 있어서,

상기 트랜잭션을 처리하는 단계는,

상기 도메인에 대응하는 유효한 고유 지갑 주소가 획득된 경우 수신자가 컨트랙트이면 실행 및 처리를 진행하는 것을 특징으로 하는 트랜잭션의 처리 방법.

청구항 17

제 1 항 내지 제 16 항 중에 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

발명의 설명

기술 분야

[0001] 본 발명은 블록체인 데이터의 관리 기술에 관한 것으로서, 보다 구체적으로 블록체인 시스템의 지갑 주소를 도메인을 이용하여 관리하는 데이터 처리 방법, 이러한 도메인에 기반하여 블록체인 트랜잭션을 처리하는 장치, 방법 및 이를 기록한 기록매체에 관한 것이다.

배경 기술

[0002] 블록체인(blockchain)은 관리 대상 데이터를 '블록'이라고 하는 소규모 데이터들이 P2P(peer-to-peer) 방식을 기반으로 생성된 체인 형태의 연결고리 기반 분산 데이터 저장환경에 저장되어 누구도 임의로 수정할 수 없고 누구나 변경의 결과를 열람할 수 있는 분산 컴퓨팅 기술 기반의 데이터 위변조 방지 기술 이다.

[0003] 블록에는 해당 블록이 발견되기 이전에 사용자들에게 전파되었던 모든 거래 내역이 기록되어 있고, 이것은 P2P 방식으로 모든 사용자에게 똑같이 전송되므로 거래 내역을 임의로 수정하거나 누락시킬 수 없다. 블록은 발견된 날짜와 이전 블록에 대한 연결고리를 가지고 있으며 이러한 블록들의 집합을 블록체인이라 칭한다.

[0004] 기존에 전자화폐로 거래할 때 중앙 서버에 거래 기록을 보관하는 것과는 달리, 블록체인은 모든 사용자에게 거래 기록을 보여주며 서로 비교해 위조를 막는다.

[0005] 한편, 스마트 컨트랙트(smart contract) 또는 스마트 계약은 블록체인 기반으로 체결하는 계약을 말한다. 이러한 스마트 컨트랙트는 이더리움(Ethereum)에서 처음 도입되었으며, 현재는 에이다, NEO, Qtum, EOS, 플레이코인

등의 암호화폐에도 적용된 상태이다.

선행기술문헌

특허문헌

- [0006] (특허문헌 0001) 한국특허공개공보 제2018-0085570호, "블록 체인을 이용하여 데이터를 관리하는 장치 및 방법", 2018년07월27일 공개

발명의 내용

해결하려는 과제

- [0007] 본 발명이 해결하고자 하는 기술적 과제는, 종래의 블록체인 기술에서 사용되는 사용자 또는 스마트 컨트랙트의 지갑 주소는 인코딩 또는 해싱을 기반으로 한 무의미한 주소를 가짐으로 인해 사용자로 하여금 기억, 식별 및 입력이 매우 불편하다는 문제를 해결하고, 스마트 컨트랙트 사용, 작성 및 분석의 난이도가 증가하는 약점을 극복하며, 잘못된 입력으로 인해 야기되는 치명적인 실수를 방지하고자 한다.

과제의 해결 수단

- [0008] 상기 기술적 과제를 해결하기 위하여, 본 발명의 일 실시예에 따른 블록체인(blockchain) 시스템의 고유 지갑 주소를 관리하는 방법은, 고유 지갑 주소를 그에 대응하는 도메인(domain)과 매칭하여 관리하기 위한 스마트 컨트랙트(smart contract)를 생성하여 관리 컨트랙트로 설정하는 단계; 상기 관리 컨트랙트가 블록체인 시스템의 사용자 또는 스마트 컨트랙트로부터 고유 지갑 주소에 대한 도메인 등록 요청을 수신하는 단계; 상기 관리 컨트랙트가 상기 도메인이 미리 저장된 도메인 테이블 내에 유효하게 존재하는지 여부를 검사하는 단계; 및 상기 검사 결과에 따라 상기 관리 컨트랙트가 상기 도메인 등록 요청을 처리하는 단계;를 포함한다.
- [0009] 일 실시예에 따른 고유 지갑 주소의 관리 방법에서, 상기 도메인 등록 요청을 처리하는 단계는, 상기 검사 결과, 상기 도메인이 상기 도메인 테이블 내에 유효하게 중복하여 존재하는 경우 상기 관리 컨트랙트가 상기 도메인 등록 요청을 거부하는 응답을 전송할 수 있다.
- [0010] 일 실시예에 따른 고유 지갑 주소의 관리 방법에서, 상기 도메인 등록 요청을 처리하는 단계는, 상기 도메인 등록 요청이 동시에 복수 개 수신된 경우 상기 검사 결과와 무관하게 상기 관리 컨트랙트가 상기 도메인 등록 요청을 거부하는 응답을 전송할 수 있다.
- [0011] 일 실시예에 따른 고유 지갑 주소의 관리 방법에서, 상기 도메인 등록 요청을 처리하는 단계는, 상기 검사 결과, 상기 도메인이 상기 도메인 테이블 내에 유효하게 중복하여 존재하지 않는 경우 상기 관리 컨트랙트가 상기 도메인 등록 요청에 따라 상기 도메인과 상기 고유 지갑 주소를 매칭하여 상기 도메인 테이블에 저장함으로써 등록 성공을 나타내는 응답을 전송할 수 있다. 또한, 상기 도메인 등록 요청을 처리하는 단계는, 상기 도메인과 상기 고유 지갑 주소를 매칭하여 상기 도메인 테이블에 저장하되, 등록이 이루어지는 시간 정보 및 상기 도메인의 유효 상태를 더 포함하여 저장할 수 있다. 나아가, 상기 도메인 테이블은, 상기 도메인을 포함하는 정보를 키(key) 값으로 하는 해시 테이블(hash table)로 구현될 수 있다.
- [0012] 일 실시예에 따른 고유 지갑 주소의 관리 방법에서, 상기 관리 컨트랙트가 블록체인 시스템의 사용자의 요청에 따라 상기 도메인 테이블에 저장된 도메인을 변경하거나 점유를 해제하는 명령을 수행할 수 있다. 또한, 상기 도메인 테이블에 저장된 도메인의 점유가 해제된 경우 상기 관리 컨트랙트가 해당 도메인에 대한 도메인 등록 요청시 새로운 고유 지갑 주소를 매칭하여 저장하는 명령을 수행할 수 있다.
- [0013] 상기 기술적 과제를 해결하기 위하여, 본 발명의 다른 실시예에 따른 블록체인(blockchain) 시스템의 트랜잭션을 처리하는 방법은, 송신자가 송신자 또는 수신자 중 적어도 하나의 고유 지갑 주소에 대응하는 도메인(domain)을 사용하여 트랜잭션을 생성하는 단계; 고유 지갑 주소를 그에 대응하는 도메인과 매칭하여 관리하는 관리 컨트랙트로 설정된 스마트 컨트랙트(smart contract)가 생성된 상기 트랜잭션으로부터 상기 도메인에 대한 조회 요청을 수신하는 단계; 상기 스마트 컨트랙트가 상기 조회 요청에 따라 미리 저장된 도메인 테이블을 검색하는 단계; 및 상기 검색 결과에 따라 상기 스마트 컨트랙트가 상기 도메인에 대응하는 고유 지갑 주소를 획득하여 상기 트랜잭션을 처리하는 단계;를 포함한다.

- [0014] 다른 실시예에 따른 트랜잭션의 처리 방법에서, 상기 도메인 테이블을 검색하는 단계는, 상기 미리 저장된 도메인 테이블 내에 상기 도메인이 존재하지 않는 경우 상기 트랜잭션을 무효화할 수 있다.
- [0015] 다른 실시예에 따른 트랜잭션의 처리 방법에서, 상기 도메인 테이블을 검색하는 단계는, 상기 미리 저장된 도메인 테이블 내에 상기 도메인이 존재하는 경우 상기 도메인에 대응하는 고유 지갑 주소가 여전히 유효한지 여부를 검사하는 단계를 더 포함할 수 있다. 또한, 상기 고유 지갑 주소가 여전히 유효한지 여부를 검사하는 단계는, 상기 도메인에 대응하는 고유 지갑 주소가 만료되었거나 점유가 해제된 경우 유효하지 않는 것으로 판단할 수 있다. 나아가, 상기 고유 지갑 주소가 여전히 유효한지 여부를 검사하는 단계는, 상기 도메인에 대응하는 고유 지갑 주소가 유효하지 않는 것으로 판단한 경우 상기 트랜잭션을 무효화할 수 있다.
- [0016] 다른 실시예에 따른 트랜잭션의 처리 방법에서, 상기 도메인 테이블을 검색하는 단계는, 상기 미리 저장된 도메인 테이블 내에 상기 도메인이 존재하되 도메인에 대응하는 고유 지갑 주소가 복수 개인 경우 복수 개의 고유 지갑 주소 중 가장 최근에 등록된 유효한 값을 획득할 수 있다.
- [0017] 다른 실시예에 따른 트랜잭션의 처리 방법에서, 상기 트랜잭션을 처리하는 단계는, 상기 도메인에 대응하는 유효한 고유 지갑 주소가 획득된 경우 수신자가 사람이면 송금을 처리할 수 있다.
- [0018] 다른 실시예에 따른 트랜잭션의 처리 방법에서, 상기 트랜잭션을 처리하는 단계는, 상기 도메인에 대응하는 유효한 고유 지갑 주소가 획득된 경우 수신자가 컨트랙트이면 실행 및 처리를 진행할 수 있다.
- [0019] 한편, 이하에서는 상기 기재된 고유 지갑 주소의 관리 방법 및 트랜잭션의 처리 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

발명의 효과

- [0020] 본 발명의 실시예들은, 사용자는 복잡한 지갑 주소 대신에 사용자가 정의한 쉬운 단어들로 이루어진 도메인을 이용하여 주소의 기억, 식별 및 입력을 용이하게 수행할 수 있으므로 블록체인 시스템 사용이 보다 편리해지며, 스마트 컨트랙트의 사용, 작성 및 분석이 수월해지고 오타로 인한 치명적인 실수를 감소시킬 수 있다는 장점을 갖는다.

도면의 간단한 설명

- [0021] 도 1은 종래의 블록체인 플랫폼들이 사용하는 지갑 주소를 예시한 도면이다.
- 도 2는 본 발명의 일 실시예에 따른 블록체인(blockchain) 시스템의 고유 지갑 주소를 관리하는 방법을 도시한 흐름도이다.
- 도 3은 본 발명의 일 실시예에 따른 도 2의 고유 지갑 주소의 관리 방법을 도메인 신청 및 할당 절차에 따라 도시한 도면이다.
- 도 4는 본 발명의 다른 실시예에 따른 블록체인(blockchain) 시스템의 트랜잭션을 처리하는 방법을 도시한 흐름도이다.
- 도 5는 본 발명의 다른 실시예에 따른 도 4의 트랜잭션 처리 과정에서의 도메인 관리 컨트랙트의 내부 동작 방식을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0022] 본 발명의 실시예들을 설명하기에 앞서, 종래의 블록체인 시스템에서 사용하는 지갑 주소로부터 이들이 내포하고 있는 문제점들을 검토한 후, 이들 문제점을 해결하기 위해 본 발명의 실시예들이 채택하고 있는 기술적 수단을 순차적으로 소개하도록 한다.
- [0023] 도 1은 종래의 블록체인 플랫폼들이 사용하는 지갑 주소를 예시한 도면이다.
- [0024] 사용자(사람) 및 스마트 컨트랙트는 자기 자신임을 나타내는 식별자(identifier, ID)의 역할을 하는 고유 지갑 주소를 갖고 있으며, 그 주소를 통해 트랜잭션을 처리할 수 있다. 현재 비트코인, 이더리움 등의 블록체인 플랫폼들은 수학적, 암호학적 알고리즘을 이용해 생성된 16진수 혹은 숫자+알파벳 조합으로 이루어진 긴 자리의 값을 사용자 및 스마트 컨트랙트의 지갑 주소로 사용하고 있다.
- [0025] 도 1에 예시된 바를 통해 확인할 수 있듯이, 지갑 주소는 인코딩(부호화) 혹은 해싱(임의의 길이를 가진 데이터

를 특정한 길이의 데이터로 변환해주는 기술)을 기반으로 한 무의미한 주소를 가지게 된다. 따라서, 이러한 현재의 블록체인 기술은 다음과 같은 문제점을 갖는다.

- [0026] 첫째, 기존의 블록체인 시스템들에서 스마트 컨트랙트 혹은 사용자의 식별자는 인코딩 및 해시값으로 이루어진 지갑 주소인데, 사용자에게 이러한 주소는 기억, 식별 및 입력이 매우 불편하다.
- [0027] 둘째, 또한 기존의 주소는 스마트 컨트랙트 사용, 작성 및 분석의 난이도를 높이고, 오타로 인한 치명적인 실수를 야기할 수 있다.
- [0028] 따라서, 이상의 문제점 인식에 기초하여 기존의 지갑 주소를 대체하는, 식별 및 입력이 간단하며 분석이 간단한 도메인(domain) 시스템이 필요하다. 여기서, 도메인이란 고유의 지갑 주소를 대체할 수 있는 일종의 별칭(alias)에 해당하는 것으로, 사용자에게 의해 쉽게 인식/기억/식별/입력될 수 있도록 구성되는 것이 바람직하다.
- [0029] 이하에서는 도면을 참조하여 본 발명의 실시예들을 구체적으로 설명하도록 한다. 다만, 하기의 설명 및 첨부된 도면에서 본 발명의 요지를 흐릴 수 있는 공지 기능 또는 구성에 대한 상세한 설명은 생략한다. 덧붙여, 명세서 전체에서, 어떤 구성 요소를 '포함'한다는 것은, 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라, 다른 구성요소를 더 포함할 수 있는 것을 의미한다.
- [0030] 본 발명에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 실시된 특징, 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.
- [0031] 특별히 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미이다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미인 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.
- [0032] 도 2는 본 발명의 일 실시예에 따른 블록체인(blockchain) 시스템의 고유 지갑 주소를 관리하는 방법을 도시한 흐름도로서, 인코딩 및 해시값으로 이루어진 스마트 컨트랙트 및 사용자들의 종래의 식별하기 어려운 지갑 주소 대신에, 사용자 편의를 위해 지갑 주소에 매칭되는 식별이 용이한 도메인을 생성, 조회 및 관리하는 기술적 수단을 제안하고 있다.
- [0033] S210 단계에서, 고유 지갑 주소를 그에 대응하는 도메인(domain)과 매칭하여 관리하기 위한 스마트 컨트랙트(smart contract)를 생성하여 관리 컨트랙트로 설정한다. 즉, 블록체인의 탈중앙화 성향에 맞추어, 도메인 테이블을 관리하는 특수한(그리고 유일한) 스마트 컨트랙트를 생성한다.
- [0034] S220 단계에서, 관리 컨트랙트는 블록체인 시스템의 사용자 또는 스마트 컨트랙트로부터 고유 지갑 주소에 대한 도메인 등록 요청을 수신한다.
- [0035] S230 단계에서, 상기 관리 컨트랙트는 상기 도메인이 미리 저장된 도메인 테이블 내에 유효하게 존재하는지 여부를 검사한다. 여기서, 도메인 테이블은 (도메인, 등록 날짜, 유효상태, 원래의 지갑 주소)의 정보를 가질 수 있다. 또한, 이 테이블은 도메인과 그 외 정보들을 키(key) 값으로 하는 해시 테이블(해시를 색인으로 사용하는 테이블)로서, 저장할 수 있는 정보량은 거의 무한하게 확장 가능하다.
- [0036] S240 단계에서, 상기 검사 결과에 따라 상기 관리 컨트랙트는 상기 도메인 등록 요청을 처리한다.
- [0037] 이 과정에서는, 상기 검사 결과, 상기 도메인이 상기 도메인 테이블 내에 유효하게 중복하여 존재하는 경우 상기 관리 컨트랙트가 상기 도메인 등록 요청을 거부하는 응답을 전송할 수 있다. 또한, 이 과정에서는, 상기 도메인 등록 요청이 동시에 복수 개 수신된 경우 상기 검사 결과와 무관하게 상기 관리 컨트랙트가 상기 도메인 등록 요청을 거부하는 응답을 전송할 수 있다.
- [0038] 반면, 상기 검사 결과, 상기 도메인이 상기 도메인 테이블 내에 유효하게 중복하여 존재하지 않는 경우 상기 관리 컨트랙트가 상기 도메인 등록 요청에 따라 상기 도메인과 상기 고유 지갑 주소를 매칭하여 상기 도메인 테이블에 저장함으로써 등록 성공을 나타내는 응답을 전송할 수 있다.
- [0039] 즉, 도메인 관리 스마트 컨트랙트를 통해 사용자들은 지갑의 주소에 상응하는 도메인을 사용자가 임의로 정의할

수 있으며, 중복 혹은 동시 생성은 거부 처리로 막을 수 있다. 또한, 사용자들은 이러한 관리 컨트랙트를 통해 도메인의 변경 및 점유 해제가 가능한데, 점유가 해제된 도메인은 다른 지갑 주소로 등록될 수 있으며, 이전의 점유자와 구분하기 위해 등록 날짜 정보도 도메인 테이블에 함께 기록하는 것이 바람직하다. 한편, 각각의 지갑 주소는 1개 이상의 도메인에 매칭될 수 있다.

[0040] 도 3은 본 발명의 일 실시예에 따른 도 2의 고유 지갑 주소의 관리 방법을 도메인 신청 및 할당 절차에 따라 도시한 도면이다.

[0041] 도 3을 참조하면, 먼저 ① 사용자(사람) 또는 스마트 컨트랙트(10)가 도메인 관리 컨트랙트(20)에게 도메인 등록을 요청한다. 그러면, ② 도메인 관리 컨트랙트(20)는 도메인 테이블(25) 내에서 중복 여부를 조회한다. ③ 만약, 도메인 테이블(25) 내에서 해당 도메인이 중복되지 않는 경우 도메인 테이블(25)에 도메인 정보를 등록한다. 반면, 해당 도메인이 중복되는 경우 혹은 동시 신청된 경우에는 도메인 등록 요청을 거절한다. 이제, ④ 도메인 관리 컨트랙트는 요청자에게 결과를 반환하게 된다.

[0042] 요약하건대, 관리 컨트랙트(20)가 도메인 등록 요청을 처리하는 과정은, 도메인 테이블(25)에 대한 검사 결과, 해당 도메인이 상기 도메인 테이블(25) 내에 유효하게 중복하여 존재하지 않는 경우 상기 관리 컨트랙트(20)가 상기 도메인 등록 요청에 따라 상기 도메인과 상기 고유 지갑 주소를 매칭하여 상기 도메인 테이블(25)에 저장함으로써 등록 성공을 나타내는 응답을 전송하게 된다.

[0043] 또한, 상기 도메인 등록 요청을 처리하는 과정은, 상기 도메인과 상기 고유 지갑 주소를 매칭하여 상기 도메인 테이블에 저장하되, 등록이 이루어지는 시간 정보 및 상기 도메인의 유효 상태를 더 포함하여 저장하는 것이 바람직하다. 이때, 상기 도메인 테이블(25)은, 상기 도메인을 포함하는 정보를 키(key) 값으로 하는 해시 테이블(hash table)로 구현될 수 있다.

[0044] 이상과 같은 구조를 채택함으로써, 본 발명의 실시예들에 따른 고유 지갑 주소의 관리 방법은, 관리 컨트랙트(20)가 블록체인 시스템의 사용자의 요청에 따라 도메인 테이블(25)에 저장된 도메인을 변경하거나 점유를 해제하는 명령을 수행할 수 있다. 따라서, 만약 도메인 테이블(25)에 저장된 도메인의 점유가 해제된 경우 상기 관리 컨트랙트(20)가 해당 도메인에 대한 도메인 등록 요청시 새로운 고유 지갑 주소를 매칭하여 저장하는 명령을 수행할 수 있게 된다.

[0045] 이제 이상에서 소개한 도메인 테이블을 이용하여 블록체인 시스템의 트랜잭션을 보다 용이하게 처리하는 과정을 제안하도록 한다.

[0046] 도 4는 본 발명의 다른 실시예에 따른 블록체인(blockchain) 시스템의 트랜잭션을 처리하는 방법을 도시한 흐름도이다. 사용자 및 스마트 컨트랙트가 도메인을 사용해 트랜잭션을 처리하면, 블록체인 시스템은 도메인 관리 스마트 컨트랙트에서 도메인을 조회해서 상응하는 지갑 주소로 트랜잭션을 처리하게 된다. 블록체인의 특성상 도메인 관리 스마트 컨트랙트 역시 모든 노드에서 같은 값으로 동기화 되므로 도메인 테이블의 무결성은 보장될 수 있다.

[0047] S410 단계에서, 송신자는 송신자 또는 수신자 중 적어도 하나의 고유 지갑 주소에 대응하는 도메인(domain)을 사용하여 트랜잭션을 생성한다.

[0048] S420 단계에서, 관리 컨트랙트는 생성된 상기 트랜잭션으로부터 상기 도메인에 대한 조회 요청을 수신한다. 이때 관리 컨트랙트는 고유 지갑 주소를 그에 대응하는 도메인과 매칭하여 관리하도록 설정된 스마트 컨트랙트(smart contract)를 의미한다.

[0049] S430 단계에서, 상기 스마트 컨트랙트는 상기 조회 요청에 따라 미리 저장된 도메인 테이블을 검색한다. 이 과정에서 상기 미리 저장된 도메인 테이블 내에 상기 도메인이 존재하지 않는 경우 상기 트랜잭션을 무효화할 수 있다. 반면, 상기 미리 저장된 도메인 테이블 내에 상기 도메인이 존재하는 경우 상기 도메인에 대응하는 고유 지갑 주소가 여전히 유효한지 여부를 검사하는 단계를 더 포함할 수 있다. 이때, 고유 지갑 주소가 여전히 유효한지 여부를 검사하는 과정은 상기 도메인에 대응하는 고유 지갑 주소가 만료되었거나 점유가 해제된 경우 유효하지 않는 것으로 판단할 수 있다. 또한, 상기 도메인에 대응하는 고유 지갑 주소가 유효하지 않는 것으로 판단한 경우 상기 트랜잭션을 무효화할 수 있다. 나아가, 도메인 테이블을 검색하는 과정에서는, 상기 미리 저장된 도메인 테이블 내에 상기 도메인이 존재하되 도메인에 대응하는 고유 지갑 주소가 복수 개인 경우 복수 개의 고유 지갑 주소 중 가장 최근에 등록된 유효한 값을 획득할 수 있다.

[0050] S440 단계에서, 상기 검색 결과에 따라 상기 스마트 컨트랙트가 상기 도메인에 대응하는 고유 지갑 주소를 획득

하여 상기 트랜잭션을 처리한다. 이 과정에서, 상기 도메인에 대응하는 유효한 고유 지갑 주소가 획득된 경우 수신자가 사람이면 송금을 처리하고, 수신자가 컨트랙트이면 실행 및 처리를 진행할 수 있다.

[0051] 도 5는 본 발명의 다른 실시예에 따른 도 4의 트랜잭션 처리 과정에서의 도메인 관리 컨트랙트의 내부 동작 방식을 설명하기 위한 도면이다.

[0052] S501 단계에서 송신자(33)가 송신자(33) 또는 수신자(35), 혹은 양자(33, 35) 모두의 지갑 주소 대신에 도메인을 사용하여 트랜잭션을 생성한다. S502 단계에서 트랜잭션(40)은 관리 컨트랙트(20)에게 도메인의 조회를 요청한다. 그러면, S503 단계에서 관리 컨트랙트(20)는 S502 단계를 통해 전달받은 도메인을 도메인 테이블(25)에서 검색한다. 이때, 매칭되는 도메인이 없다면 처리에 실패하고, 매칭되는 도메인이 존재할 경우 이에 대한 처리에 성공하여 S504 단계를 통해 각각의 응답을 수행한다.

[0053] 다음으로, S505 단계에서 관리 컨트랙트(20)는 S504 단계를 통해 반환받은 수신자의 지갑 주소가 여전히 유효한지 검사한다. 점유 해제 또는 도메인 만료 등의 이유로 주소가 유효하지 않은 경우에는 처리에 실패하고, 여전히 해당 지갑 주소가 유효하다면 처리에 성공하여 S506 단계를 통해 각각의 응답을 수행한다.

[0054] S507 단계에서 관리 컨트랙트(20)는 요청된 도메인과 매칭되는 지갑 주소를 트랜잭션(40)에 반환한다. 이전 과정들에서 처리에 실패한 경우, 트랜잭션은 무효화된다.

[0055] 이제, S508 단계에서, 앞서 반환받은 수신자의 주소를 이용해 트랜잭션을 처리한다. 수신자가 사람이면 송금이 이루어지고, 수신자가 컨트랙트라면 실행 및 처리가 이루어지며, S509 단계를 통해 각각의 처리 응답을 수행한다. 트랜잭션의 처리에 따라, 지갑의 잔고가 증가하거나 컨트랙트의 상태가 업데이트 된다. 이때 오류가 발생하여 처리에 실패하면 트랜잭션 처리 과정은 무효화될 수 있다.

[0056] 마지막으로, S510 단계를 통해 송신자(33)는 트랜잭션 처리의 결과를 반환받는다.

[0057] 상기된 본 발명의 실시예들에 따르면, 사용자는 복잡한 지갑 주소 대신에 사용자가 정의한 쉬운 단어들로 이루어진 도메인을 이용하여 주소의 기억, 식별 및 입력을 용이하게 수행할 수 있으므로 블록체인 시스템 사용이 보다 편리해지며, 스마트 컨트랙트의 사용, 작성 및 분석이 수월해지고 오타로 인한 치명적인 실수를 감소시킬 수 있다는 장점을 갖는다. 따라서, 본 발명의 실시예들은 블록체인 거래소 또는 블록체인 지갑 등 스마트 컨트랙트가 동작하는 블록체인 기반 시스템에 널리 적용 가능하다.

[0058] 한편, 본 발명의 실시예들은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.

[0059] 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등을 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술 분야의 프로그래머들에 의하여 용이하게 추론될 수 있다.

[0060] 이상에서 본 발명에 대하여 그 다양한 실시예들을 중심으로 살펴보았다. 본 발명에 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

부호의 설명

[0061] 10: 사용자 / 컨트랙트

20: 관리 컨트랙트

25: 도메인 테이블

33: 송신자

35: 수신자

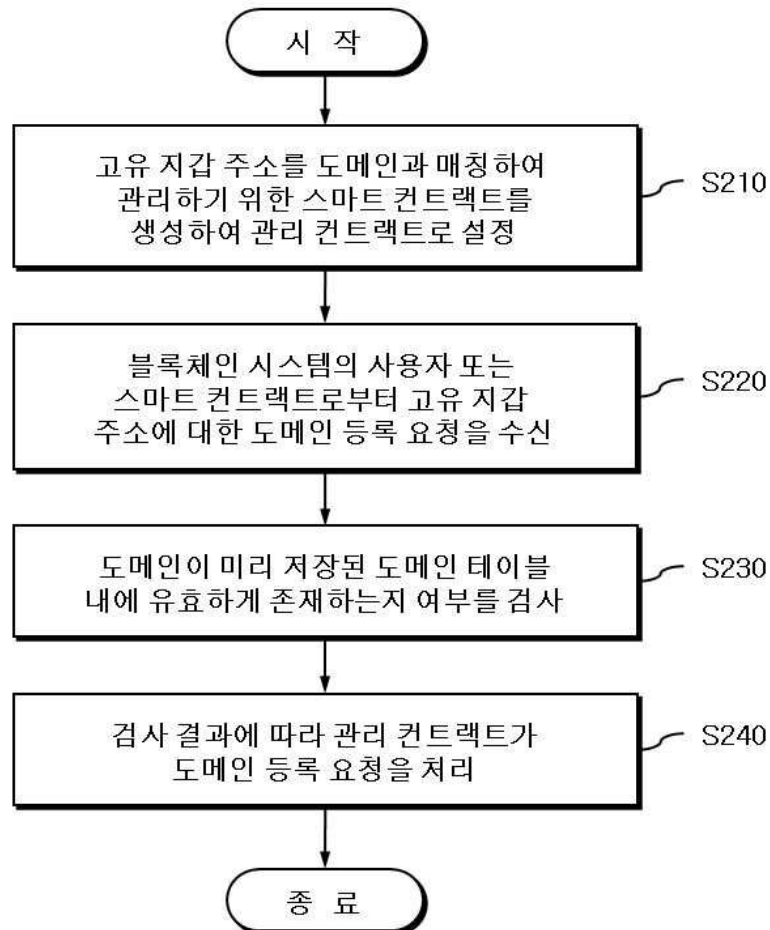
40: 트랜잭션

도면

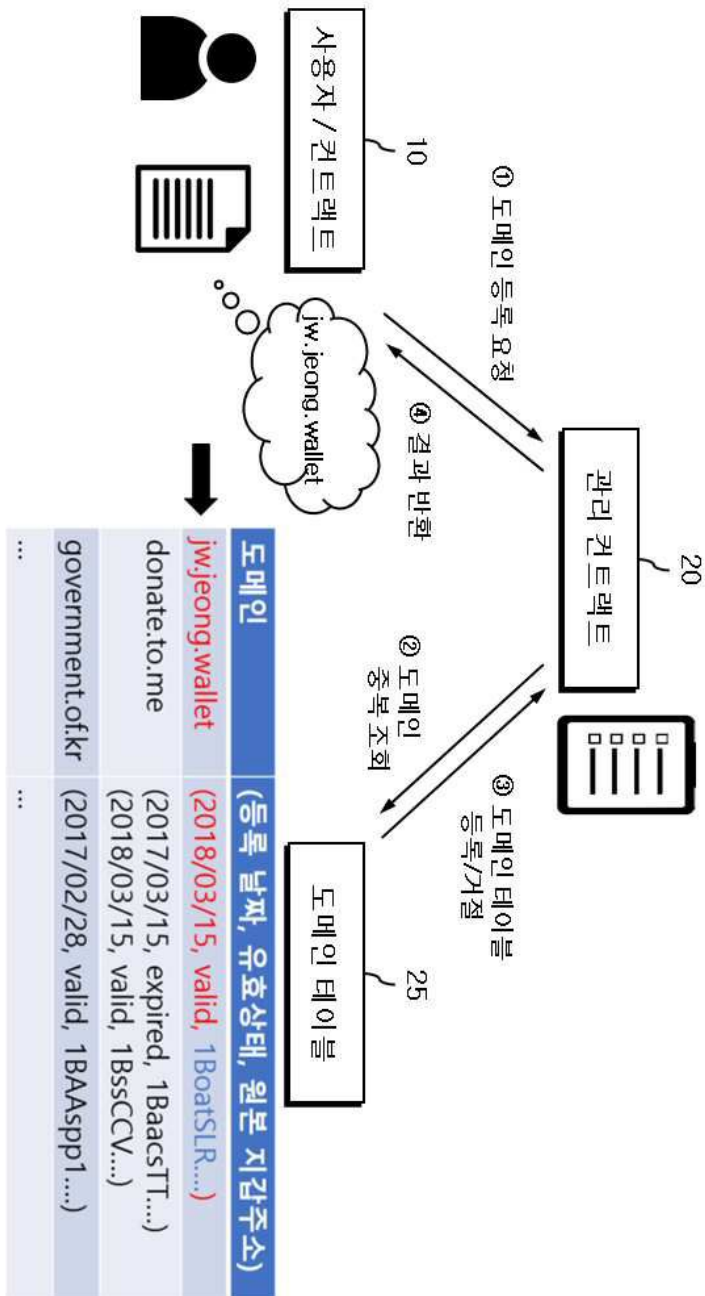
도면1

유형	지갑 주소의 예
비트코인	1BoatSLRHtKNgkdXEobR76b53LEtTpyT
	1aa5cmqmvQq8YQTEqcTmW7dfBNuFwgdCD
이더리움	0xEC19F701c32311C7818d70B77db793C60c325Cf3
	0xa3054515d24c1aF9429e8B18DF7b2f8ECc1Dc2f4
NEO	AKDVzYGLczmykdtRaejgvWeZrvdkVEvQ1X
	AFpzNPxukXV84hm3AuVeeMi4vAcWGqiEFB

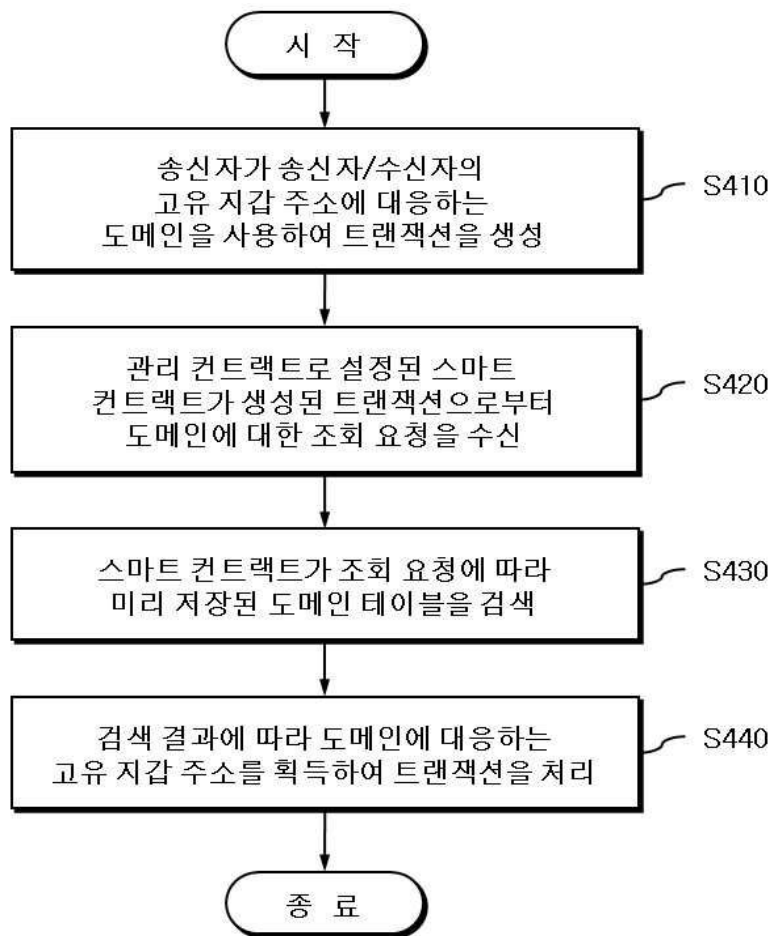
도면2



도면3



도면4



도면5

