



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0086501
(43) 공개일자 2023년06월15일

(51) 국제특허분류(Int. Cl.)

G06Q 20/38 (2012.01) G06Q 20/06 (2012.01)
G06Q 20/36 (2012.01) H04L 29/08 (2006.01)
H04L 9/08 (2006.01) H04L 9/32 (2006.01)

(52) CPC특허분류

G06Q 20/3825 (2013.01)
G06Q 20/065 (2013.01)

(21) 출원번호 10-2021-0175188

(22) 출원일자 2021년12월08일

심사청구일자 2021년12월08일

(71) 출원인

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

인호

서울특별시 용산구 서빙고로 35, 102동 1705호(한강로3가, 용산시티파크1단지)

최지혁

서울특별시 강동구 천호대로 1239, 110동 803호(길동, GS강동자이아파트)

(74) 대리인

윤귀상

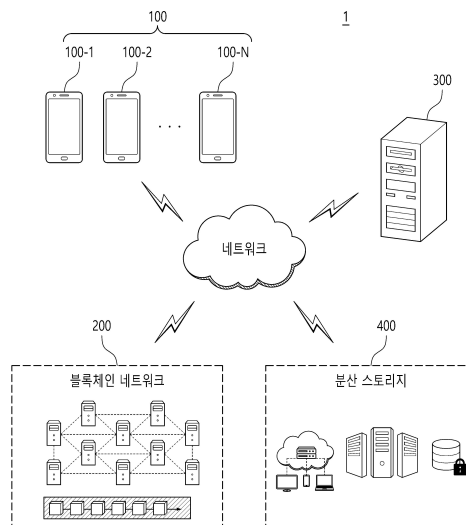
전체 청구항 수 : 총 13 항

(54) 발명의 명칭 **블록체인 기반 공유자산 거래 시스템의 제어방법, 이를 수행하기 위한 기록매체 및 시스템**

(57) 요약

공유자산의 감정결과가 포함된 원본 보증서를 전송하고, 원본 보증서에 공유자의 서명이 입력된 보증서를 전송하는 공유자 측에 마련된 복수의 공유자 단말기; 토큰을 발행하며, 토큰이 저장되는 전자지갑을 생성하는 블록체인 네트워크; 및 복수의 공유자 단말기로부터 서명이 입력된 보증서를 수신하고, 블록체인 네트워크에 서명이 입력된 보증서와 토큰의 거래 요청 신호를 포함한 트랜잭션을 전송하는 전자지갑 관리 서버;를 포함하는 블록체인 기반 공유자산 거래 시스템을 제공한다.

대표도 - 도1



(52) CPC특허분류

G06Q 20/367 (2020.05)
 G06Q 20/38215 (2013.01)
 H04L 67/104 (2022.05)
 H04L 67/1097 (2022.05)
 H04L 9/0825 (2013.01)
 H04L 9/3247 (2013.01)
 H04L 9/50 (2022.05)
 H04L 2209/56 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711152671
과제번호	2021-0-00177-002
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	데이터경제를위한블록체인기술개발
연구과제명	스마트 컨트랙트의 개발-배포-실행의 전주기적 취약점 및 신뢰성 오류 개선 기술개발
발	
기 여 율	1/1
과제수행기관명	고려대학교산학협력단
연구기간	2021.04.01 ~ 2025.12.31

명세서

청구범위

청구항 1

공유자산을 토큰화하여 거래하는 블록체인 기반 공유자산 거래 시스템에 있어서,

공유자산의 감정결과가 포함된 원본 보증서를 전송하고, 상기 원본 보증서에 공유자의 서명이 입력된 보증서를 전송하는 공유자 측에 마련된 복수의 공유자 단말기;

상기 원본 보증서를 수신하여 스마트컨트랙트 블록에 저장하고, 상기 스마트컨트랙트 블록을 기초로 토큰을 발행하며, 상기 토큰이 저장되는 전자지갑을 생성하는 블록체인 네트워크; 및

상기 복수의 공유자 단말기로부터 서명이 입력된 보증서를 수신하고, 상기 블록체인 네트워크에 상기 서명이 입력된 보증서와 토큰의 거래 요청 신호를 포함한 트랜잭션을 전송하는 전자지갑 관리 서버;를 포함하는 블록체인 기반 공유자산 거래 시스템.

청구항 2

제 1항에 있어서,

상기 원본 보증서가 저장되는 분산 스토리지를 더 포함하되, 상기 분산 스토리지는 로컬스토리지, IPFS 및 클라우드를 포함하고, 상기 적어도 어느 하나의 공유자 단말기에 의해 로컬스토리지, IPFS 및 클라우드 중 어느 하나로 선택되는 블록체인 기반 공유자산 거래 시스템.

청구항 3

제 1항에 있어서,

상기 전자지갑 관리 서버는,

상기 공유자가 2명인 경우, 제1 공유자 측의 공유자산의 지분정보와 제1 공유자 측의 서명이 입력된 보증서를 제1 공유자 측에 마련된 공유자 단말기로부터 수신하여 제1 트랜잭션을 생성하고, 제1 공유자 측의 공유자산의 지분정보와 제1 공유자 측의 서명이 입력된 상기 보증서를 제2 공유자 측에 마련된 공유자 단말기에 전송하며, 제2 공유자 측에 마련된 공유자 단말기로부터 제2 공유자 측의 공유자산의 지분정보와 제2 공유자 측의 서명이 입력된 보증서를 수신하여 제2 트랜잭션을 생성하는 트랜잭션 생성부;

제1 트랜잭션과 제2 트랜잭션을 결합하는 트랜잭션 결합부; 및

상기 트랜잭션 결합부에 의해 결합된 트랜잭션을 상기 블록체인 네트워크에 전송하는 통신부;를 포함하는 블록체인 기반 공유자산 거래 시스템.

청구항 4

제 3항에 있어서,

상기 트랜잭션 생성부는,

상기 공유자가 2명 초과인 경우, 모든 공유자 측의 트랜잭션을 생성하도록 상기 트랜잭션을 생성하는 과정을 반복 수행하고,

상기 트랜잭션 결합부는,

상기 트랜잭션 생성부에 의해 생성된 복수개의 트랜잭션을 결합하는 블록체인 기반 공유자산 거래 시스템.

청구항 5

제 3항 또는 제 4항에 있어서,

상기 서명은 상기 원본 보증서에 개인키로 입력되고, 상기 복수의 공유자 단말기는 공개키를 상기 블록체인 네트워크에 전송하는 블록체인 기반 공유자산 거래 시스템.

청구항 6

제 5항에 있어서,

상기 블록체인 네트워크는,

상기 트랜잭션 결합부에 의해 결합된 트랜잭션을 공개키로 복호화하고, 복호화된 보증서와 상기 스마트컨트랙트 블록에 저장된 보증서를 비교하여 동일한지 여부를 검증하며, 동일한 경우 토큰의 거래를 위한 트랜잭션을 실행하여 구매자의 지갑주소로 상기 토큰을 전송하는 블록체인 기반 공유자산 거래 시스템.

청구항 7

제 1항에 있어서,

상기 적어도 어느 하나의 공유자 단말기는,

미리 설정된 지식재산권 범위에서만 구매자에게 권리가 이전되도록 지식재산권 범위가 선택되는 블록체인 기반 공유자산 거래 시스템.

청구항 8

공유자산을 토큰화하여 거래하는 블록체인 기반 공유자산 거래 시스템의 제어방법에 있어서,

공유자산의 감정결과가 포함된 원본 보증서를 전송하고, 상기 원본 보증서에 공유자의 서명이 입력된 보증서를 전송하는 단계;

블록체인 네트워크가 상기 원본 보증서를 수신하여 스마트컨트랙트 블록에 저장하고, 상기 스마트컨트랙트 블록을 기초로 토큰을 발행하며, 상기 토큰이 저장되는 전자지갑을 생성하는 단계; 및

상기 서명이 입력된 보증서를 수신하고, 상기 블록체인 네트워크에 상기 서명이 입력된 보증서와 토큰의 거래 요청 신호를 포함한 트랜잭션을 전송하는 단계;를 포함하는 블록체인 기반 공유자산 거래 시스템의 제어방법.

청구항 9

제 8항에 있어서,

상기 서명이 입력된 보증서를 수신하고, 상기 블록체인 네트워크에 상기 서명이 입력된 보증서와 토큰의 거래 요청 신호를 포함한 트랜잭션을 전송하는 단계는,

상기 공유자가 2명인 경우, 제1 공유자 측의 공유자산의 지분정보와 제1 공유자 측의 서명이 입력된 보증서를 제1 공유자 측에 마련된 공유자 단말기로부터 수신하여 제1 트랜잭션을 생성하는 단계;

제1 공유자 측의 공유자산의 지분정보와 제1 공유자 측의 서명이 입력된 상기 보증서를 제2 공유자 측에 마련된 공유자 단말기에게 전송하는 단계;

제2 공유자 측에 마련된 공유자 단말기로부터 제2 공유자 측의 공유자산의 지분정보와 제2 공유자 측의 서명이

입력된 보증서를 수신하여 제2 트랜잭션을 생성하는 단계;

제1 트랜잭션과 제2 트랜잭션을 결합하는 단계; 및

결합된 제1 트랜잭션과 제2 트랜잭션을 상기 블록체인 네트워크에 전송하는 단계;를 포함하는 블록체인 기반 공유자산 거래 시스템의 제어방법.

청구항 10

제 9항에 있어서,

상기 서명이 입력된 보증서를 수신하고, 상기 블록체인 네트워크에 상기 서명이 입력된 보증서와 토큰의 거래 요청 신호를 포함한 트랜잭션을 전송하는 단계는,

상기 공유자가 2명 초과인 경우, 모든 공유자 측의 트랜잭션을 생성하도록 상기 트랜잭션을 생성하는 과정을 반복 수행하는 단계;

상기 생성된 복수개의 트랜잭션을 결합하는 단계; 및

결합된 트랜잭션을 상기 블록체인 네트워크에 전송하는 단계;를 포함하는 블록체인 기반 공유자산 거래 시스템의 제어방법.

청구항 11

제 9항 또는 제 10항에 있어서,

상기 서명은 상기 원본 보증서에 개인키로 입력되고, 복수의 공유자 단말기는 공개키를 상기 블록체인 네트워크에 전송하는 블록체인 기반 공유자산 거래 시스템의 제어방법.

청구항 12

제 11항에 있어서,

상기 결합된 제1 트랜잭션과 제2 트랜잭션을 공개키로 복호화하는 단계;

복호화된 보증서와 상기 스마트컨트랙트 블록에 저장된 보증서를 비교하여 동일한지 여부를 검증하는 단계; 및

동일한 경우 토큰의 거래를 위한 트랜잭션을 실행하여 구매자의 지갑주소로 상기 토큰이 전송되는 단계;를 포함하는 블록체인 기반 공유자산 거래 시스템의 제어방법.

청구항 13

제 8항 내지 제 12항 중 어느 하나의 항에 따른 상기 블록체인 기반 공유자산 거래 시스템의 제어방법을 수행하기 위한 컴퓨터 프로그램이 기록된 컴퓨터로 판독 가능한 저장 매체.

발명의 설명

기술 분야

[0001] 본 발명은 블록체인 기반 공유자산 거래 시스템의 제어방법, 이를 수행하기 위한 기록매체 및 시스템에 관한 것으로, 보다 상세하게는, 공유자산을 토큰화하여 거래하는 블록체인 기반 공유자산 거래 시스템의 제어방법, 이를 수행하기 위한 기록매체 및 시스템에 관한 것이다.

배경 기술

[0002] 블록체인(blockchain)은 관리 대상 데이터를 '블록'이라고 불리는 소규모 데이터들이 피어 투 피어(P2P, peer-

to-peer) 방식을 기반으로 생성된 체인 형태의 연결고리 기반 분산 데이터 저장환경에 저장되는 분산 컴퓨팅(distributed computing) 기술 기반의 데이터 대변 방지 기술이다. 블록체인에서 개별의 트랜잭션(transaction)은 탈중앙화된(decentralized) 전자장부에 쓰이기 때문에 블록체인 소프트웨어를 실행하는 사용자들의 컴퓨터에서 서버가 운영되어 중앙은행 없이 개인 간의 자유로운 거래가 가능하다.

- [0003] 복수의 공유자가 지분비율별로 공유하는 토큰화된 공유자산을 거래하기 위해서는 모든 공유자의 동의가 필요하다. 따라서, 모든 공유자가 개인키로 서명하고, 블록체인 네트워크에서 이를 유효한 것으로 검증하여야만 토큰화된 공유자산을 거래할 수 있는 블록체인 기반 공유자산 거래 시스템이 필요한 실정이다.

선행기술문헌

특허문헌

- [0004] (특허문헌 0001) KR 10-1914668호

발명의 내용

해결하려는 과제

- [0005] 본 발명이 해결하고자 하는 기술적 과제는 블록체인 서버에서 공유자산을 토큰화하고, 블록체인 서버와 연동되는 마켓 서버에서 토큰을 거래할 수 있는 블록체인 기반 공유자산 거래 시스템의 제어방법, 이를 수행하기 위한 기록매체 및 시스템을 제공하는 것이다.

- [0006] 또한, 본 발명이 해결하고자 하는 기술적 과제는 모든 공유자가 개인키로 서명해야 토큰을 거래할 수 있는 블록체인 기반 공유자산 거래 시스템의 제어방법, 이를 수행하기 위한 기록매체 및 시스템을 제공하는 것이다.

과제의 해결 수단

- [0007] 본 발명의 일측면은, 공유자산을 토큰화하여 거래하는 블록체인 기반 공유자산 거래 시스템에 있어서, 공유자산의 감정결과가 포함된 원본 보증서를 전송하고, 상기 원본 보증서에 공유자의 서명이 입력된 보증서를 전송하는 공유자 측에 마련된 복수의 공유자 단말기; 상기 원본 보증서를 수신하여 스마트컨트랙트 블록에 저장하고, 상기 스마트컨트랙트 블록을 기초로 토큰을 발행하며, 상기 토큰이 저장되는 전자지갑을 생성하는 블록체인 네트워크; 및 상기 복수의 공유자 단말기로부터 서명이 입력된 보증서를 수신하고, 상기 블록체인 네트워크에 상기 서명이 입력된 보증서와 토큰의 거래 요청 신호를 포함한 트랜잭션을 전송하는 전자지갑 관리 서버;를 포함할 수 있다.

- [0008] 또한, 상기 원본 보증서가 저장되는 분산 스토리지를 더 포함하되, 상기 분산 스토리지는 로컬스토리지, IPFS 및 클라우드를 포함하고, 상기 적어도 어느 하나의 공유자 단말기에 의해 로컬스토리지, IPFS 및 클라우드 중 어느 하나로 선택되는 것을 포함할 수 있다.

- [0009] 또한, 상기 전자지갑 관리 서버는, 상기 공유자가 2명인 경우, 제1 공유자 측의 공유자산의 지분정보와 제1 공유자 측의 서명이 입력된 보증서를 제1 공유자 측에 마련된 공유자 단말기로부터 수신하여 제1 트랜잭션을 생성하고, 제1 공유자 측의 공유자산의 지분정보와 제1 공유자 측의 서명이 입력된 상기 보증서를 제2 공유자 측에 마련된 공유자 단말기에게 전송하며, 제2 공유자 측에 마련된 공유자 단말기로부터 제2 공유자 측의 공유자산의 지분정보와 제2 공유자 측의 서명이 입력된 보증서를 수신하여 제2 트랜잭션을 생성하는 트랜잭션 생성부; 제1 트랜잭션과 제2 트랜잭션을 결합하는 트랜잭션 결합부; 및 상기 트랜잭션 결합부에 의해 결합된 트랜잭션을 상기 블록체인 네트워크에 전송하는 통신부;를 포함할 수 있다.

- [0010] 또한, 상기 트랜잭션 생성부는, 상기 공유자가 2명 초과인 경우, 모든 공유자 측의 트랜잭션을 생성하도록 상기 트랜잭션을 생성하는 과정을 반복 수행하고, 상기 트랜잭션 결합부는, 상기 트랜잭션 생성부에 의해 생성된 복수개의 트랜잭션을 결합할 수 있다.

- [0011] 또한, 상기 서명은 상기 원본 보증서에 개인키로 입력되고, 상기 복수의 공유자 단말기는 공개키를 상기 블록체인 네트워크에 전송하는 것을 포함할 수 있다.

- [0012] 또한, 상기 블록체인 네트워크는, 상기 트랜잭션 결합부에 의해 결합된 트랜잭션을 공개키로 복호화하고, 복호

화된 보증서와 상기 스마트컨트랙트 블록에 저장된 보증서를 비교하여 동일한지 여부를 검증하며, 동일한 경우 토큰의 거래를 위한 트랜잭션을 실행하여 구매자의 지갑주소로 상기 토큰을 전송하는 것을 포함할 수 있다.

[0013] 또한, 상기 적어도 어느 하나의 공유자 단말기는, 미리 설정된 지식재산권 범위에서만 구매자에게 권리가 이전 되도록 지식재산권 범위가 선택될 수 있다.

[0014] 본 발명의 다른 일측면은, 공유자산을 토큰화하여 거래하는 블록체인 기반 공유자산 거래 시스템의 제어방법에 있어서, 공유자산의 감정결과가 포함된 원본 보증서를 전송하고, 상기 원본 보증서에 공유자의 서명이 입력된 보증서를 전송하는 단계; 블록체인 네트워크가 상기 원본 보증서를 수신하여 스마트컨트랙트 블록에 저장하고, 상기 스마트컨트랙트 블록을 기초로 토큰을 발행하며, 상기 토큰이 저장되는 전자지갑을 생성하는 단계; 및 상기 서명이 입력된 보증서를 수신하고, 상기 블록체인 네트워크에 상기 서명이 입력된 보증서와 토큰의 거래 요청 신호를 포함한 트랜잭션을 전송하는 단계;를 포함할 수 있다.

[0015] 또한, 상기 서명이 입력된 보증서를 수신하고, 상기 블록체인 네트워크에 상기 서명이 입력된 보증서와 토큰의 거래 요청 신호를 포함한 트랜잭션을 전송하는 단계는, 상기 공유자가 2명인 경우, 제1 공유자 측의 공유자산의 지분정보와 제1 공유자 측의 서명이 입력된 보증서를 제1 공유자 측에 마련된 공유자 단말기로부터 수신하여 제1 트랜잭션을 생성하는 단계; 제1 공유자 측의 공유자산의 지분정보와 제1 공유자 측의 서명이 입력된 상기 보증서를 제2 공유자 측에 마련된 공유자 단말기에게 전송하는 단계; 제2 공유자 측에 마련된 공유자 단말기로부터 제2 공유자 측의 공유자산의 지분정보와 제2 공유자 측의 서명이 입력된 보증서를 수신하여 제2 트랜잭션을 생성하는 단계; 제1 트랜잭션과 제2 트랜잭션을 결합하는 단계; 및 결합된 제1 트랜잭션과 제2 트랜잭션을 상기 블록체인 네트워크에 전송하는 단계;를 포함할 수 있다.

[0016] 상기 서명이 입력된 보증서를 수신하고, 상기 블록체인 네트워크에 상기 서명이 입력된 보증서와 토큰의 거래 요청 신호를 포함한 트랜잭션을 전송하는 단계는, 상기 공유자가 2명 초과인 경우, 모든 공유자 측의 트랜잭션을 생성하도록 상기 트랜잭션을 생성하는 과정을 반복 수행하는 단계; 상기 생성된 복수개의 트랜잭션을 결합하는 단계; 및 결합된 트랜잭션을 상기 블록체인 네트워크에 전송하는 단계;를 포함할 수 있다.

[0017] 또한, 상기 서명은 상기 원본 보증서에 개인키로 입력되고, 복수의 공유자 단말기는 공개키를 상기 블록체인 네트워크에 전송할 수 있다.

[0018] 또한, 상기 결합된 제1 트랜잭션과 제2 트랜잭션을 공개키로 복호화하는 단계; 복호화된 보증서와 상기 스마트컨트랙트 블록에 저장된 보증서를 비교하여 동일한지 여부를 검증하는 단계; 및 동일한 경우 토큰의 거래를 위한 트랜잭션을 실행하여 구매자의 지갑주소로 상기 토큰이 전송되는 단계;를 포함할 수 있다.

[0019] 본 발명의 또 다른 일측면은, 컴퓨터로 판독 가능한 저장 매체에는 블록체인 기반 공유자산 거래 시스템의 제어방법을 수행하기 위한 컴퓨터 프로그램이 기록될 수 있다.

발명의 효과

[0020] 상술한 본 발명의 일 측면에 따르면, 모든 공유자가 개인키로 서명해야만 토큰이 거래될 수 있으므로, 해킹으로 인한 사고를 방지할 수 있으며, 자산상실 우려가 감소될 수 있는 효과가 존재한다.

도면의 간단한 설명

[0021] 도1은 본 발명의 일 실시예에 따른 블록체인 기반 공유자산 거래 시스템을 나타내는 개념도이다.

도2는 전자지갑 관리 서버의 제어 블록도이다.

도3은 본 발명의 일 실시예에 따른 블록체인 기반 공유자산 거래 시스템의 제어방법을 나타낸 전체적인 흐름도이다.

도4는 공유자 측이 개인키로 서명을 하는 과정을 나타낸 도면이다.

도5는 트랜잭션을 생성하는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0022] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 당업자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의 다양한 실시예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있

는 특정 형상, 구조 및 특성은 일 실시예와 관련하여 본 발명의 정신 및 범위를 벗어나지 않으면서 다른 실시예로 구현될 수 있다. 또한, 각각의 개시된 실시예 내의 개별 구성요소의 위치 또는 배치는 본 발명의 정신 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 본 발명의 범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다.

[0023] 이하, 도면들을 참조하여 본 발명의 바람직한 실시예들을 보다 상세하게 설명하기로 한다.

[0025] 도1은 본 발명의 일 실시예에 따른 블록체인 기반 자산 거래 시스템을 나타내는 개념도이다.

[0026] 블록체인 기반 공유자산 거래 시스템(1)은 복수의 공유자 단말기(100), 블록체인 네트워크(200), 전자지갑 관리 서버(300) 및 분산 스토리지(400)를 포함할 수 있다.

[0027] 블록체인 기반 공유자산 거래 시스템(1)은 공유자산의 감정결과가 포함된 원본 보증서를 기초로 자산을 토큰화할 수 있다. 자산을 토큰화하는 것은, 자산을 거래할 수 있는 교환권을 생성하는 것을 의미할 수 있다. 토큰의 가격은 공유자산의 감정결과가 포함된 원본 보증서를 기초로 결정될 수 있다.

[0028] 이 때, 자산은 실물 자산과 디지털자산을 포함할 수 있다. 실물 자산은 부동산, 예술품, 명품 등을 포함할 수 있고, 디지털 자산은 이미지, 오디오가 담긴 파일, 암호화폐, 특허, 상표권, 저작권, 퍼블리시티권 등의 산업재산권, 게임 아이템, 게임 캐릭터 등을 포함하는 것으로서, 교환 가치가 있는 전자 문서 등을 더 포함할 수 있으나, 이에 한정되는 것은 아니다.

[0029] 복수의 공유자 단말기(100)는 본 발명의 블록체인 기반 공유자산 거래 시스템(1)을 이용하고자 하는 공유자가 보유한 데스크탑 PC, 랩탑 PC, 스마트폰 또는 태블릿PC 등의 컴퓨팅 장치일 수 있다.

[0030] 복수의 공유자 단말기(100)는 전문가 단말기로부터 공유자산에 대한 감정평가 정보, 판매자의 소유권 증명 정보 및 전문가의 보증 서명 정보를 담은 보증서를 수신할 수 있다. 전문가 단말기가 공유자산에 대한 감정평가를 수행하고, 보증서를 생성하는 것으로 전술하였으나, 전문가가 공유자산에 대한 감정평가를 수행하고, 보증서를 생성하여 전문가 단말기에 입력할 수 있는 것은 물론이다.

[0031] 또한, 전문가 단말기는 복수의 공유자 단말기(100)로부터 전문가의 개인 정보, 자격증 및 경력 정보 열람을 요청할 수 있는 신호를 수신할 수 있다. 전문가 단말기는 전문가의 개인정보, 자격증 및 경력 정보를 복수의 공유자 단말기(100)에 송신할 수 있다. 또한, 발급기관의 서버가 전문가의 자격증 및 경력 정보를 복수의 공유자 단말기(100)에 송신하도록 발급기관의 서버를 더 포함할 수 있다.

[0032] 복수의 공유자 단말기(100)는 공유자산의 감정결과와 공유자의 지분정보가 포함된 원본 보증서를 블록체인 네트워크(200)에 전송하고, 복수의 공유자 단말기(100)는 원본 보증서의 공유자들의 서명이 입력된 보증서를 블록체인 네트워크(200) 및 전자지갑 관리 서버(300)에 전송한다. 이 때, 지분 정보는 미리 설정된 공유자의 지분비율일 수 있고, 복수의 공유자의 지분비율의 합은 100%이다.

[0033] 분산 스토리지(400)는 복수의 공유자 단말기(100)로부터 자산에 대한 보증서를 수신하여 저장할 수 있다.

[0034] 분산 스토리지(400)는 자산의 보증서를 파일로서 저장하고, 파일은 이미지 파일이나 오디오 파일일 수 있다. 이 때, 이미지 파일은 JPEG, BMP, TIFF의 형식으로 저장될 수 있고, 오디오 파일은 WAV, MP3, MIDI, PTX, M4A의 형식으로 저장될 수 있다. 다만, 이와 같은 형식에 한정하는 것은 아니다.

[0035] 분산 스토리지(400)는 로컬스토리지, IPFS, 클라우드로 마련될 수 있다. 이 때, 적어도 어느 하나의 공유자 단말기(100)는 자산의 파일을 로컬스토리지, IPFS, 클라우드 중 어느 하나에 저장될 수 있도록 전송할 수 있다. 로컬스토리지는 URL 또는 P2P 방식(PEER-TO-PEER)으로 파일을 수신할 수 있고, IPFS는 GATEWAY를 거친 URL과 고유한 해시값으로 파일을 수신할 수 있으며, 클라우드는 URL 또는 P2P 방식(PEER-TO-PEER)으로 파일을 수신할 수 있다. 여기서, 로컬스토리지는 키(KEY)와 값(VALUE)의 쌍 형태로 데이터가 저장되는 브라우저를 의미하고, IPFS(21)(Inter Planetary File System)는 분산형 파일 시스템에 데이터를 저장하고 공유하기 위한 프로토콜을 의미하며, 클라우드는 데이터, 소프트웨어 및 다양한 컴퓨터 자원 등을 사용자가 소유하고 있는 PC나 스마트폰 같은 하드웨어에 두지 않고 인터넷을 통해 접근할 수 있도록 하는 것을 의미할 수 있다.

[0036] 이 때, 분산 스토리지(400)는 적어도 어느 하나의 공유자 단말기(100)로부터 공유자산의 파일을 전송받아 파일

로 저장하거나 암호화된 URL 주소를 생성해 URL 주소로 저장할 수 있다. 또한, 분산 스토리지(400)는 파일에 포함된 자산정보와 메타데이터를 전송할 수도 있다. 파일에 포함된 자산정보는 자산의 보증서 파일의 크기, 생성일시, URL 주소 등을 포함할 수 있다. 메타데이터는 오디오 파일로 마련된 자산이 가진 파장, 진동수, 자산이 가진 색상, 생김새, 픽셀, 작품명, 작가명, 작품이 저장된 링크, 경로 및 과거 거래이력 등을 의미할 수 있다. 적어도 어느 하나의 공유자 단말기(100)에 의해 로컬스토리지, IPFS 및 클라우드 중 어느하나로 선택된다.

[0037] 블록체인 네트워크(200)는 복수개의 노드로 구성되고, 자산을 관리하는 서비스를 제공한다. 분산스토리지(400) 또는 복수의 공유자 단말기(100)로부터 자산의 보증서를 수신하여 안전하게 보관할 수 있다. 또한, 복수의 공유자 단말기(100), 분산스토리지(400) 및 전자지갑 관리 서버(300)는 블록체인 네트워크(200)의 복수개의 노드 중 하나의 노드로서 참여할 수 있다. 이 때, 복수 개 노드는 복수개의 공유자 단말기(100)를 통해 제출된 자산의 토큰화를 위한 트랜잭션(Transaction)에 대한 스마트컨트랙트를 실행하고, 이를 하나 이상의 블록에 기록할 수 있다.

[0038] 또한, 블록체인 네트워크(200)는 스마트컨트랙트 블록을 기초로 자산을 토큰화하여 토큰을 발행한다. 토큰은 대체가능(Fungible)토큰과 대체불가능(Non-Fungible) 토큰으로 분류될 수 있다. 대체가능 토큰은 동일한 타입의 다른 토큰과 교환이 가능하지만 대체불가능 토큰은 동일한 타입의 다른 토큰과 교환이 불가능하다는 특징이 있다. 본 발명의 토큰은 블록체인 네트워크의 ERC-721, ERC-1155 표준의 대체불가능 토큰(NFT: Non Fungible Token)으로 이루어질 수 있으나, 이에 한정하는 것은 아니다.

[0039] 이 때, 스마트컨트랙트 블록에 기록되는 정보는 기본정보와 확장정보로 구성될 수 있다. 기본정보는 공유자의 정보, 실물자산인지 디지털 자산인지여부를 나타내는 자산종류일 수 있다. 확장정보는 자산의 생성일자, 자산의 보증서 내용, 자산의 보증기관의 정보, 자산의 소유권 분할여부, 소유권 분할 비율정보 또는 자산에 부여된 지식재산권 정보를 포함할 수 있다.

[0040] 예를 들면, 블록체인 네트워크(200)는 실물자산이 부동산인 경우, 기본 정보로서 판매자 정보를 스마트컨트랙트 블록에 기록할 수 있다. 또한, 블록체인 네트워크(200)는 확장 정보로서 부동산 계약서의 계약자, 계약서 파일의 해시값, 계약서 페이지 수, 계약일, 계약자의 서명, 계약서 파일의 생성일자, 계약서 파일 또는 매도인/매수인의 계약서의 서명 이미지가 저장된 경로정보를 스마트컨트랙트 블록에 기록할 수 있고, 이를 기초로 토큰을 생성할 수 있다.

[0041] 또 다른 예로, 블록체인 네트워크(200)는 디지털자산이 음원과 같은 저작권인 경우, 기본 정보로서 판매자 정보를 포함할 수 있다. 또한, 블록체인 네트워크(200)는 확장 정보로서 MP3파일의 해시값, 음원의 가수, 해당 음원의 작곡/작사가, 해당 음원의 생성일자, 수익비율, 보증서 또는 보증기관정보를 포함할 수 있고, 이를 스마트컨트랙트 블록에 기록할 수 있으며, 이를 기초로 토큰을 생성할 수 있다.

[0042] 또한, 블록체인 네트워크(200)는 온라인 전자지갑을 생성할 수 있다. 전자지갑은 토큰을 저장하고 인출할 수 있도록 공유자의 각각의 고유의 개인 은행 계좌 역할로서 전자 은행 계좌처럼 작동될 수 있는 것이다. 이 때, 전자지갑은 통합 API가 제공되어 METAMASK, Klay, MyCrypto 등의 웹 지갑 어플리케이션과 연동되는 것일 수 있다.

[0043] 전자지갑 관리 서버(300)는 복수의 공유자 각각의 전자지갑을 총괄하여 관리할 수 있는 서버이다. 전자지갑 관리 서버(300)는 복수의 공유자 단말기(100)로부터 공유자의 서명이 입력된 보증서를 수신하고, 블록체인 네트워크(200)에 공유자의 서명이 입력된 보증서와 토큰의 거래 요청 신호를 포함한 트랜잭션을 전송한다.

[0044] 블록체인 네트워크(200)는 수신한 트랜잭션이 유효한지 검증하고, 검증결과 유효한 경우 토큰의 거래를 위한 트랜잭션을 실행하여 구매자의 지갑주소로 토큰을 전송한다.

[0045] 이 때, 적어도 어느 하나의 공유자 단말기(100)는 미리 설정된 지식재산권 범위에서만 구매자에게 공유자산의 권리가 이전되도록 지식재산권의 범위가 공유자로부터 선택될 수 있다. 미리 설정된 지식재산권의 범위는 복제권, 공연권, 방송권, 전송권, 전시권, 배포권, 대여권 및 2차적 저작물의 작성권을 포함할 수 있고, 예시를 들었을 뿐, 이에 한정되는 것은 아니다.

[0047] 도2는 전자지갑 관리 서버의 제어 블록도이다.

[0048] 전자지갑 관리 서버(300)는 통신부(310), 제어부(320) 및 저장부(30)를 포함할 수 있다.

[0049] 통신부(310)는 복수의 공유자 단말기(100)와 통신하여 공유자의 서명이 입력된 보증서를 수신하고, 블록체인 네

트위크(200)와 통신하여 트랜잭션을 전송할 수 있다.

- [0050] 제어부(320)는 공유자의 서명이 입력된 보증서를 이용하여 토큰의 거래 요청에 대한 트랜잭션을 생성한다. 제어부(320)는 트랜잭션 생성부(321) 및 트랜잭션 결합부(322)를 포함할 수 있다.
- [0051] 트랜잭션 생성부(321)는 복수의 공유자가 2명인 경우, 제1 공유자 측의 공유자산의 지분정보와 제1 공유자 측의 서명이 입력된 보증서를 제1 공유자 측에 마련된 공유자 단말기(100)부터 수신하여 제1 트랜잭션을 생성한다. 또한, 트랜잭션 생성부(321)는 제1 공유자 측의 공유자산의 지분정보와 제1 공유자 측의 서명이 입력된 보증서를 제2 공유자 측에 마련된 공유자 단말기(100)에게 전송하고, 제2 공유자 측에 마련된 공유자 단말기(100)로부터 제2 공유자 측의 공유자산의 지분정보와 제2 공유자 측의 서명이 입력된 보증서를 수신하여 제2 트랜잭션을 생성한다.
- [0052] 트랜잭션 결합부(322)는 제1 트랜잭션과 제2 트랜잭션을 결합한다.
- [0053] 통신부(310)는 트랜잭션 결합부(322)에 의해 결합된 트랜잭션을 블록체인 네트워크(200)에 전송한다. 저장부(330)는 트랜잭션 생성부(321)에 의해 생성된 트랜잭션을 저장하고, 트랜잭션 결합부(322)에 의해 결합된 트랜잭션을 저장할 수 있다.
- [0054] 또한, 공유자가 2명 초과인 경우, 트랜잭션 생성부(321)는 모든 공유자 측의 트랜잭션을 생성하도록 공유자 측의 공유자산의 지분정보와 서명이 입력된 보증서를 기초로 상기에서 설명한 트랜잭션을 생성하는 과정을 반복 수행한다. 트랜잭션 결합부(322)는 트랜잭션 생성부(321)에 의해 생성된 복수개의 트랜잭션을 결합한다. 통신부(310)는 결합된 트랜잭션을 블록체인 네트워크(200)에 전송한다.
- [0056] 도3은 본 발명의 일 실시예에 따른 블록체인 기반 공유자산 거래 시스템의 제어방법을 나타낸 전체적인 흐름도이다.
- [0057] 본 발명의 일 실시예에 따른 블록체인 기반 공유자산 거래 시스템의 제어방법은 도1에 블록체인 기반 공유자산 거래 시스템(1)과 실질적으로 동일한 구성상에서 진행되므로, 도1의 블록체인 기반 공유자산 거래 시스템(1)과 동일한 구성요소에 대해 동일한 도면 부호를 부여하고, 반복되는 설명은 생략하기로 한다.
- [0058] 복수의 공유자 단말기(100)는 블록체인 네트워크(200)에 공유자산의 원본 보증서를 전송한다. 블록체인 네트워크(200)는 원본 보증서를 스마트컨트랙트 블록에 저장한다. 블록체인 네트워크(200)는 스마트컨트랙트를 기초로 토큰을 발행하고, 전자지갑을 생성한다. 이 때, 발급되는 토큰의 가격은 보증서에 기재된 자산의 가격정보일 수 있다.
- [0059] 복수의 공유자 단말기(100)는 원본 보증서에 지분정보와 서명을 입력한다. 복수의 공유자 단말기(100)는 지분정보와 서명이 입력된 보증서를 전자지갑 관리 서버(300)에 전송한다.
- [0060] 전자지갑 관리 서버(300)는 모든 공유자 측의 트랜잭션을 생성하고, 생성된 모든 트랜잭션을 결합한다. 또한, 전자지갑 관리 서버(300)는 결합된 트랜잭션을 블록체인 네트워크(200)에 전송한다.
- [0061] 블록체인 네트워크(200)는 수신한 트랜잭션을 검증하며, 검증결과 유효한 것으로 판단하면 트랜잭션을 실행하여 구매자의 지갑주소로 토큰을 전송한다.
- [0063] 도4는 공유자 측이 개인키로 서명을 하는 과정을 나타낸 도면이다.
- [0064] 복수의 공유자가 3명인 경우, 토큰의 거래에 대한 트랜잭션의 검증이 유효하지 않은 경우의 일 예시를 나타낸 도면이다.
- [0065] 제1 공유자는 개인키1을 소유하고, 제2 공유자는 개인키2를 소유하며, 제2 공유자는 개인키3을 소유한다. 제1 공유자의 공유자산의 지분비율은 40%이고, 제2 공유자의 지분비율은 30%이며, 제3 공유자의 지분비율은 30%이다. 복수의 공유자가 공유자산을 판매자에게 거래하기 위해서는 제1 공유자 내지 제3 공유자 모두의 개인키로 서명된 보증서가 존재하여야 한다. 도4를 참조하면, 원본 보증서에 제1 공유자와 제2 공유자의 개인키로 서명(Signed)이 입력되었으나, 제3 공유자의 서명은 입력되지 않았다. 트랜잭션 생성부(321)는 제1 공유자의 제1 트랜잭션을 생성하고, 제2 공유자의 제2 트랜잭션을 생성한다. 트랜잭션 결합부(322)는 제1 트랜잭션과 제2 트랜잭션을 결합하며, 통신부(310)는 결합된 트랜잭션을 블록체인 네트워크(200)에 전송한다. 이 때, 제1 공유

자 단말기와 제2 공유자 단말기는 블록체인 네트워크(200)에 자신의 공개키를 전송한다.

- [0066] 블록체인 네트워크(200)는 트랜잭션 결합부(322)에 의해 결합된 트랜잭션을 공개키로 복호화한다. 복호화된 보증서에는 제1 공유자의 지분비율인 40%와 제1 공유자의 개인키 및 제2 공유자의 지분비율인 30%와 제2 공유자의 개인키가 기재되어 있다. 제3 공유자의 개인키 서명은 기재되어 있지 않다. 스마트컨트랙트 블록에 저장된 보증서에는 제1 공유자의 지분비율 40%, 제2 공유자의 지분비율 30% 및 제3 공유자의 지분비율 30%이 기재되어 있다.
- [0067] 블록체인 네트워크(200)는 복호화된 보증서와 스마트컨트랙트 블록에 저장된 보증서를 비교하여, 지분비율 및 공유자의 개인정보 등 보증서의 내용이 동일한지 및 해당 지분 비율에 공유자의 개인키의 서명이 있는지 여부를 검증한다.
- [0068] 복호화된 보증서에는 제3 공유자의 개인키 서명이 기재되어 있지 않은바, 블록체인 네트워크(200)는 트랜잭션이 유효하지 않은 것으로 판단한다. 따라서, 블록체인 네트워크(200)는 전자지갑에 존재하는 토큰을 구매자의 지갑 주소로 전송하지 않는다.
- [0070] 도5는 트랜잭션을 생성하는 도면이다.
- [0071] 복수의 공유자가 3명인 경우, 토큰의 거래에 대한 트랜잭션을 생성하여 블록체인 네트워크(200)에 트랜잭션을 전송하는 과정을 나타내었다.
- [0072] Tx는 트랜잭션을 의미하고, Pk는 공개키를 의미하며, Sk는 개인키(비밀키)를 의미하고, Sig는 개인키로 서명하였음을 의미한다. Verify는 블록체인 네트워크(200)에서 트랜잭션을 검증하는 것을 의미하며, True는 검증결과, 트랜잭션이 유효함을 의미한다.
- [0073] 트랜잭션 생성부(321)는 제1 공유자 측의 공유자산의 지분정보(50%)와 제1 공유자 측의 서명(Sk1)이 입력된 보증서를 제1 공유자 측에 마련된 공유자 단말기로부터 수신하여 제1 트랜잭션을 생성한다. 이 때, 통신부(310)는 제1 트랜잭션을 제2 공유자 측에 마련된 공유자 단말기로 전송한다. 또한, 통신부(310)는 제2 공유자 측에 마련된 공유자 단말기(100)로부터 제2 공유자 측의 공유자산의 지분정보(30%)와 제2 공유자 측의 서명(Sk2)이 입력된 보증서를 수신한다. 트랜잭션 생성부(321)는 수신한 보증서를 기초로 제2 트랜잭션을 생성한다.
- [0074] 또한, 통신부(310)는 제1 트랜잭션과 제2 트랜잭션을 제3 공유자 측에 마련된 공유자 단말기로 전송한다. 또한, 통신부(310)는 제3 공유자 측에 마련된 공유자 단말기(100)로부터 제3 공유자 측의 공유자산의 지분정보(20%)와 제3 공유자 측의 서명(Sk3)이 입력된 보증서를 수신한다. 트랜잭션 생성부(321)는 수신한 보증서를 기초로 제3 트랜잭션을 생성한다.
- [0075] 트랜잭션 결합부(322)는 제1 트랜잭션 내지 제3 트랜잭션을 결합하여 하나의 트랜잭션을 생성한다. 트랜잭션 결합부(322)에 의해 생성된 하나의 트랜잭션에는 모든 공유자 측의 지분정보, 서명정보가 포함된다. 통신부(310)는 트랜잭션 결합부(322)에 의해 결합된 트랜잭션을 블록체인 네트워크(200)에 전송한다. 또한, 제1 공유자 측, 제2 공유자 측 및 제3 공유자 측에 마련된 공유자 단말기(100)가 블록체인 네트워크(200)에 공유자 각각의 공개키를 전송한다.
- [0076] 블록체인 네트워크(200)는 트랜잭션 결합부(322)에 의해 결합된 트랜잭션을 공개키로 복호화한다. 복호화된 보증서에는 제1 공유자의 지분비율인 50%와 제1 공유자의 개인키로 된 서명 및 제2 공유자의 지분비율인 30%와 제2 공유자의 개인키로 된 서명이 기재되어 있다. 제3 공유자의 지분비율인 20%와 제3 공유자의 개인키로 된 서명이 기재되어 있다. 스마트컨트랙트 블록에 저장된 보증서에는 제1 공유자의 지분비율 50%, 제2 공유자의 지분비율 30% 및 제3 공유자의 지분비율 20%가 기재되어 있다.
- [0077] 블록체인 네트워크(200)는 복호화된 보증서와 스마트컨트랙트 블록에 저장된 보증서를 비교하여, 지분비율 및 공유자의 개인정보 등 보증서의 내용이 동일한지 및 해당 지분 비율에 공유자의 개인키의 서명이 있는지 여부를 검증한다.
- [0078] 복호화된 보증서와 원본 보증서가 동일한 경우, 블록체인 네트워크(200)는 트랜잭션이 유효한 것으로 판단한다. 따라서, 블록체인 네트워크(200)는 토큰의 거래를 위한 트랜잭션을 실행하여 공유자의 전자지갑에 존재하는 토큰을 구매자의 지갑주소로 전송한다.

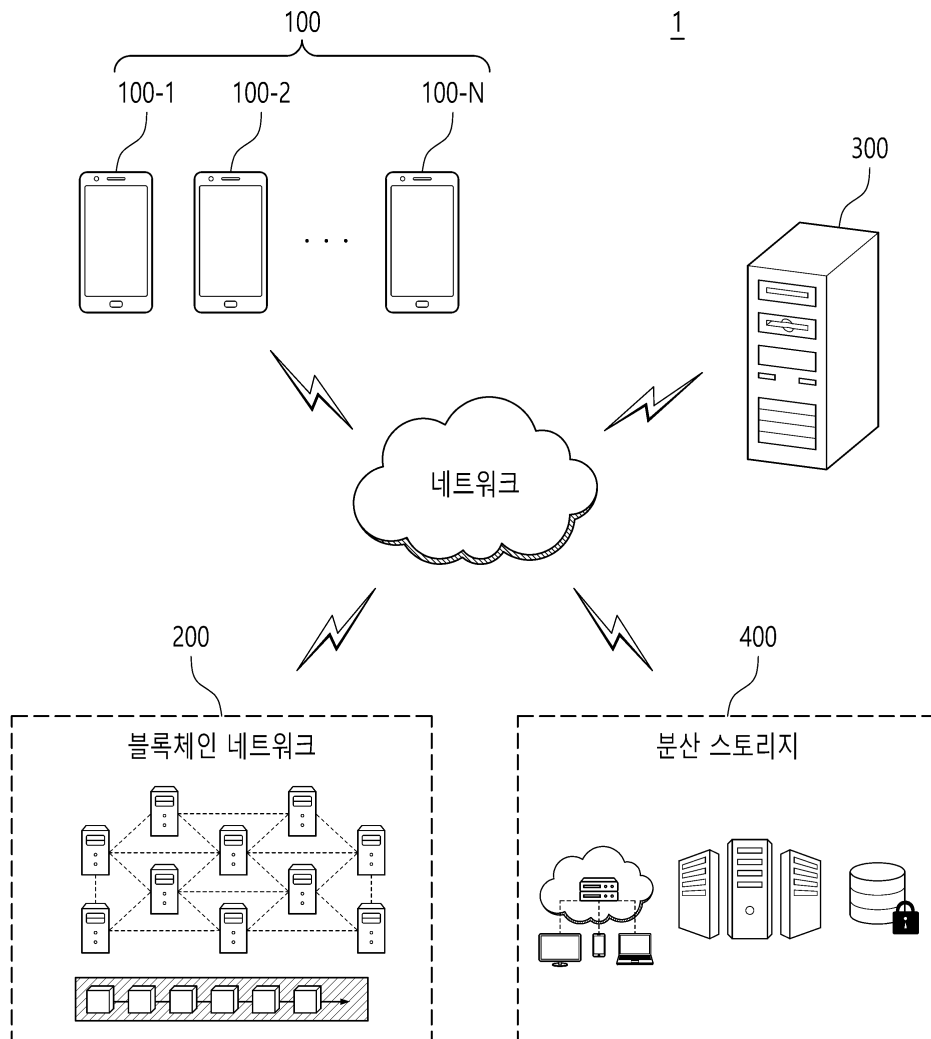
- [0080] 이와 같은, 블록체인 기반 공유자산 거래 시스템의 제어방법은 애플리케이션으로 구현되거나 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다.
- [0081] 컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다.
- [0082] 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.
- [0083] 이상에서는 실시예들을 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

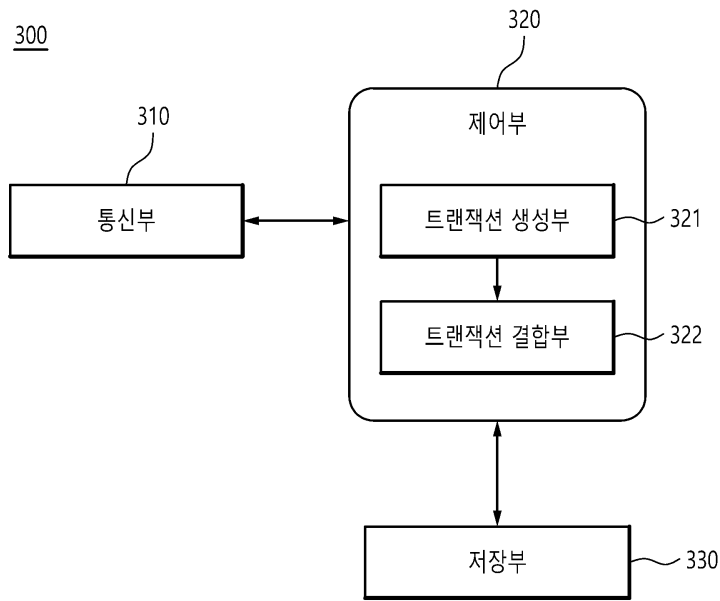
- [0084] 1: 블록체인 기반 공유자산 거래 시스템
- 100: 공유자 단말기
- 200: 블록체인 네트워크
- 300: 전자지갑 관리 서버
- 310: 통신부
- 320: 제어부
- 321: 트랜잭션 생성부
- 322: 트랜잭션 결합부
- 33: 저장부
- 400: 분산 스토리지

도면

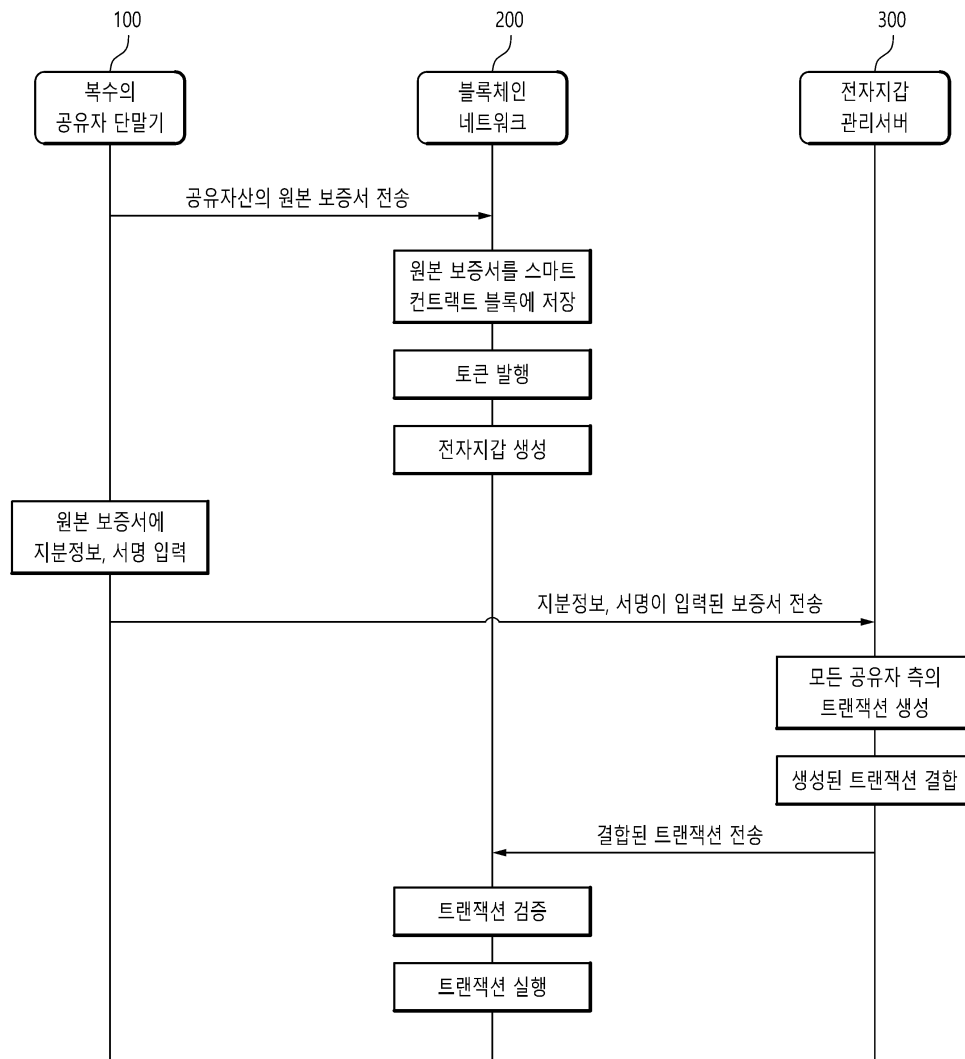
도면1



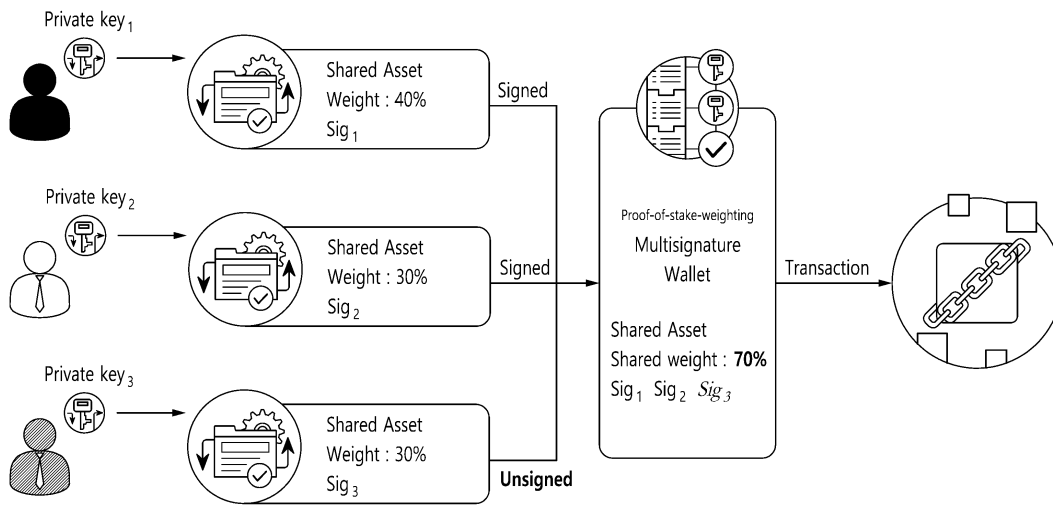
도면2



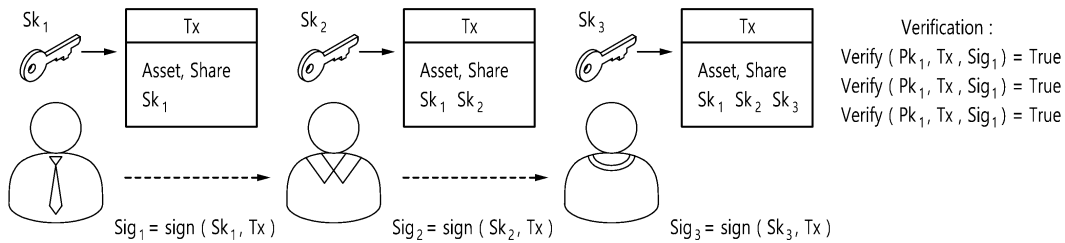
도면3



도면4



도면5



Sk : Secret key , Pk : Public key , Sig : Signature , Tx : Transaction

Share = { Pk_1 : 50% , Pk_2 : 30% , Pk_3 : 20% }

Tx = { Asset , Share }