(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년08월11일
(11) 등록번호 10-2431835
(24) 등록일자 2022년08월08일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) *G06F 16/23* (2019.01)
G06F 21/64 (2013.01) *G06F 9/46* (2006.01)
H04L 65/40 (2022.01)
(52) CPC특허분류
H04L 63/123 (2013.01)
G06F 16/2365 (2019.01)
(21) 출원번호 10-2020-0153158
(22) 출원일자 2020년11월16일
심사청구일자 2020년11월16일
(65) 공개번호 10-2022-0066769
(43) 공개일자 2022년05월24일
(56) 선행기술조사문헌
KR1020200018967 A*
KR1020200061827 A*
KR102172903 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
포항공과대학교 산학협력단
경상북도 포항시 남구 청암로 77 (지곡동)
(72) 발명자
박찬익
경상북도 포항시 남구 지곡로 155, 6동 1105호
황제영
경상북도 포항시 남구 효자로77번길 5, 202호
(뒷면에 계속)
(74) 대리인
특허법인이상

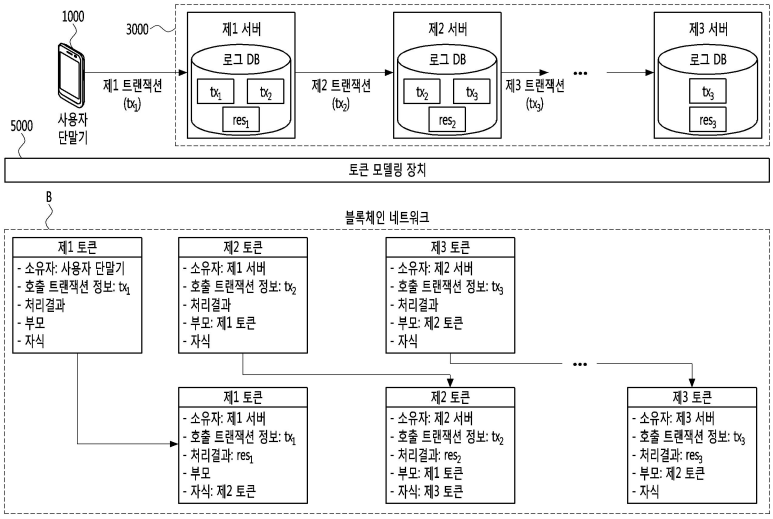
전체 청구항 수 : 총 15 항 심사관 : 장우진

(54) 발명의 명칭 **토큰 모델링 장치 및 이를 포함하는 데이터 무결성 검증 시스템 및 방법**

(57) 요 약

토큰 모델링 장치 및 이를 포함하는 데이터 무결성 검증 시스템 및 방법이 개시된다. 상기 토큰 모델링 장치 및 이를 포함하는 데이터 무결성 검증 시스템 및 방법은 트랜잭션을 수신하도록 하는 명령, 상기 트랜잭션에 기반한 토큰을 발행하도록 하는 명령, 상기 토큰을 상기 복수의 서버들 중 어느 하나의 서버로 송신하도록 하는 명령 및 상기 서버로부터 상기 토큰의 호출 트랜잭션 속성 정보 및 상기 서버 내 트랜잭션의 속성 정보를 비교한 처리 결과값을 수신하도록 하는 명령을 포함함으로써, 사용자 또는 서버들 간 API 호출 트랜잭션 정보를 블록체인에 기록하여 사용자 또는 서버들의 트랜잭션 무결성 및 부인 방지를 보장할 수 있다.

대 표 도



(52) CPC특허분류
G06F 21/64 (2013.01)
G06F 9/466 (2013.01)
H04L 67/1089 (2022.05)

(72) 발명자
노용두
대전광역시 유성구 봉산로 39, 203동 907호

홍상원
서울특별시 노원구 석계로 49, 111동 405호

이 발명을 지원한 국가연구개발사업

과제고유번호	1711125876
과제번호	2020-0-00936-002
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	블록체인융합기술개발(R&D)
연구과제명	5G 초저지연 서비스를 위한 무선 단말용 블록체인 기술 개발
기 여 율	1/2
과제수행기관명	포항공과대학교 산학협력단
연구기간	2021.01.01 ~ 2021.12.31

이 발명을 지원한 국가연구개발사업

과제고유번호	1711152571
과제번호	2021-0-00484-002
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	데이터경제를위한블록체인기술개발(R&D)
연구과제명	노드 간 메시지 전달과 합의를 위한 최적 경로 네트워크 프로토콜 기술개발
기 여 율	1/2
과제수행기관명	포항공과대학교 산학협력단
연구기간	2022.01.01 ~ 2022.12.31

명 세 서

청구범위

청구항 1

사용자 단말 및 다중 계층 구조로 제공되는 복수의 서버들과 연동하여, 상기 사용자 단말 및 복수의 서버들 간의 함수 호출에 의한 트랜잭션 전송 시 상기 트랜잭션의 무결성을 검증하는 토큰 모델링 장치에 있어서,

메모리(memory); 및

상기 메모리에 저장된 적어도 하나의 명령을 실행하는 프로세서(processor)를 포함하되,

상기 적어도 하나의 명령은,

상기 사용자 단말 또는 상기 복수의 서버들 중 어느 하나의 상위 서버인 호출 단말로부터 상기 트랜잭션의 검증 요청을 수신하도록 하는 명령,

상기 트랜잭션에 기반한 토큰을 블록체인 네트워크 상에 발행하도록 요청하는 명령,

상기 토큰을 상기 호출 단말의 하위 서버로 송신하도록 하는 명령,

상기 하위 서버로부터, 상기 토큰 내 트랜잭션 정보를 기초로 함수 호출에 의해 상기 호출 단말로부터 수신된 상기 트랜잭션의 무결성을 검증한 검증 결과값을 수신하도록 하는 명령, 및

상기 검증 결과값을 상기 토큰 내 처리 결과 속성 값으로 입력시키도록 하는 명령을 포함하고,

상기 토큰은 대체 불가능한, 무결성이 보장된 토큰인, 토큰 모델링 장치.

청구항 2

제1 항에 있어서,

상기 호출 단말로부터 상기 트랜잭션의 검증 요청을 수신하도록 하는 명령은,

상기 호출 단말로부터 상기 트랜잭션의 검증을 위한 요청 트랜잭션을 수신하도록 하는 명령을 포함하는, 토큰 모델링 장치.

청구항 3

제2 항에 있어서,

상기 요청 트랜잭션은,

상기 호출 단말로부터 상기 트랜잭션의 정보 및 상기 호출 단말의 서명 정보를 포함하는, 토큰 모델링 장치.

청구항 4

제1 항에 있어서,

상기 트랜잭션에 기반한 토큰을 블록체인 네트워크 상에 발행하도록 요청하는 명령은,

요청 트랜잭션을 바탕으로 상기 트랜잭션에 기반한 토큰 발행을 요청하기 위한 블록체인 트랜잭션을 송신하도록 하는 명령,

상기 블록체인 네트워크로부터 상기 토큰의 발행 완료 정보를 수신하여 상기 호출 단말에 송신하도록 하는 명령,

상기 토큰의 소유자를 상기 호출 단말로 설정하도록 하는 명령; 및

상기 토큰의 소유자 속성 정보를 상기 사용자 단말로 설정하고, 설정 완료 정보를 상기 호출 단말로 송신하도록 하는 명령을 포함하는, 토큰 모델링 장치.

청구항 5

삭제

청구항 6

제1 항에 있어서,

상기 토큰을 상기 호출 단말의 하위 서버로 송신하도록 하는 명령에서는,

상기 토큰의 소유자가 상기 하위 서버로 변경되는, 토큰 모델링 장치.

청구항 7

제1 항에 있어서,

상기 검증 결과값은,

상기 토큰 내 트랜잭션 정보와 상기 호출 단말로부터 수신된 상기 트랜잭션 정보가 일치할 경우, 상기 하위 서버가 상기 트랜잭션을 처리하고 발행한 처리 결과 값인, 토큰 모델링 장치.

청구항 8

삭제

청구항 9

사용자 단말 및 다중 계층 구조로 제공되는 복수의 서버들과 연동하여 상기 사용자 단말 및 복수의 서버들 간의 함수 호출에 의한 트랜잭션 전송 시 상기 트랜잭션의 무결성을 검증하는 토큰 모델링 장치를 이용해, 데이터의 무결성을 검증하는 방법에 있어서,

상기 사용자 단말 또는 상기 복수의 서버들 중 어느 하나의 상위 서버인 호출 단말로부터 상기 트랜잭션의 검증 요청을 수신하는 단계;

상기 트랜잭션에 기반한 토큰을 블록체인 네트워크 상에 발행하도록 요청하는 단계;

상기 토큰을 상기 호출 단말의 하위 서버로 송신하는 단계;

상기 하위 서버로부터, 상기 토큰 내 트랜잭션 정보를 기초로 함수 호출에 의해 상기 호출 단말로부터 수신된 상기 트랜잭션의 무결성을 검증한 검증 결과값을 수신하는 단계; 및

상기 검증 결과값을 상기 토큰 내 처리 결과 속성 값으로 입력시키는 단계를 포함하고,

상기 토큰은 대체 불가능한, 무결성이 보장된 토큰인, 데이터 무결성 검증 방법.

청구항 10

제9 항에 있어서,

상기 호출 단말로부터 상기 트랜잭션의 검증 요청을 수신하는 단계는,

상기 호출 단말로부터 상기 트랜잭션의 검증을 위한 요청 트랜잭션을 수신하는 단계를 포함하는, 데이터 무결성 검증 방법.

청구항 11

제10 항에 있어서,

상기 요청 트랜잭션은,

상기 호출 단말로부터 상기 트랜잭션의 정보 및 상기 호출 단말의 서명 정보를 포함하는, 데이터 무결성 검증 방법.

청구항 12

제9 항에 있어서,

상기 트랜잭션에 기반한 토큰을 블록체인 네트워크 상에 발행하도록 요청하는 단계는,

요청 트랜잭션을 바탕으로 상기 트랜잭션에 기반한 토큰 발행을 요청하기 위한 블록체인 트랜잭션을 송신하는 단계;

상기 블록체인 네트워크로부터 상기 토큰의 발행 완료 정보를 수신하여 상기 호출 단말에 송신하는 단계;

상기 토큰의 소유자를 상기 호출 단말로 설정하는 단계; 및

상기 토큰의 소유자 속성 정보를 상기 사용자 단말로 설정하고, 설정 완료 정보를 상기 호출 단말로 송신하는 단계를 포함하는, 데이터 무결성 검증 방법.

청구항 13

삭제

청구항 14

제9 항에 있어서,

상기 토큰을 상기 호출 단말의 하위 서버로 송신하는 단계에서는,

상기 토큰의 소유자가 상기 하위 서버로 변경되는, 데이터 무결성 검증 방법.

청구항 15

제9 항에 있어서,

상기 검증 결과값은,

상기 토큰 내 트랜잭션 정보와 상기 호출 단말로부터 수신된 상기 트랜잭션 정보가 일치할 경우, 상기 하위 서버가 상기 트랜잭션을 처리하고 발행한 처리 결과 값인, 데이터 무결성 검증 방법.

청구항 16

삭제

청구항 17

사용자 단말;

다중 계층 구조로 제공되는 복수의 서버들; 및

상기 사용자 단말 및 상기 복수의 서버들과 연동하여, 상기 사용자 단말 및 복수의 서버들 간의 함수 호출에 의한 트랜잭션 전송 시 상기 트랜잭션의 무결성을 검증하는 토큰 모델링 장치를 포함하되,

상기 토큰 모델링 장치는,

메모리(memory); 및

상기 메모리에 저장된 적어도 하나의 명령을 실행하는 프로세서(processor)를 포함하되,

상기 적어도 하나의 명령은,

상기 사용자 단말 또는 상기 복수의 서버들 중 어느 하나의 상위 서버인 호출 단말로부터 상기 트랜잭션의 검증 요청을 수신하도록 하는 명령,

상기 트랜잭션에 기반한 토큰을 블록체인 네트워크 상에 발행하도록 요청하는 명령,

상기 토큰을 상기 호출 단말의 하위 서버로 송신하도록 하는 명령,

상기 하위 서버로부터, 상기 토큰 내 트랜잭션 정보를 기초로 함수 호출에 의해 상기 호출 단말로부터 수신된 상기 트랜잭션의 무결성을 검증한 검증 결과값을 수신하도록 하는 명령, 및

상기 검증 결과값을 상기 토큰 내 처리 결과 속성 값으로 입력시키도록 하는 명령을 포함하고,

상기 토큰은 대체 불가능한, 무결성이 보장된 토큰인, 데이터 무결성 검증 시스템.

청구항 18

제17 항에 있어서,

상기 호출 단말로부터 상기 트랜잭션의 검증 요청을 수신하도록 하는 명령은,

상기 호출 단말로부터 상기 트랜잭션의 검증을 위한 요청 트랜잭션을 수신하도록 하는 명령을 포함하되,

상기 요청 트랜잭션은,

상기 호출 단말로부터 상기 트랜잭션의 정보 및 상기 호출 단말의 서명 정보를 포함하는, 데이터 무결성 검증 시스템.

청구항 19

삭제

청구항 20

제17 항에 있어서,

상기 검증 결과값은,

상기 토큰 내 트랜잭션 정보와 상기 호출 단말로부터 수신된 상기 트랜잭션 정보가 일치할 경우, 상기 하위 서버가 상기 트랜잭션을 처리하고 발행한 처리 결과 값인, 데이터 무결성 검증 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 토큰 모델링 장치 및 이를 포함하는 데이터 무결성 검증 시스템 및 방법에 관한 것으로서, 보다 상세하게는, 블록체인 네트워크 기술을 활용하여, 복수의 서버들이 개별적으로 트랜잭션의 정합성을 검증하도록 하는 토큰 모델링 장치 및 이를 포함하는 데이터 무결성 검증 시스템 및 방법을 제공하는 것에 그 목적이 있다.

배 경 기 술

[0002] 대부분의 온라인 웹 서비스들은 사용자가 API(Application Programming Interface)를 통해 서버 함수를 호출하면, 호출된 서버가 관련 로직을 실행함으로써 내부 상태를 변경하는 방식으로 제공된다.

[0003] 이때, 서버는 일반적으로, API 호출로 상호 연계된 다중 계층 서버들로 구성된다.

[0004] 다중 계층 서버로 구성된 온라인 웹 서비스의 경우에는 사용자 요청을 처리하는데 여러 서버들을 거쳐야 하므로, 개별 서버들이 독자적으로 유지하고 있는 시스템 로그 데이터 정보 간에 연관성을 가진다.

[0005] 여기서, 내부 서버 동작과 관련한 로그 데이터는 사후 검증을 위해 호출된 함수 처리 명령을 포함하여 함수 실행 중 서버에서 발생하는 주요 시스템 이벤트를 모두 저장한 데이터로, 매우 민감한 정보가 포함되어 있어 서버 외부로 공개하지 않는다. 따라서 서버들 간 로그 데이터에 대한 상호 정합성 검증은 매우 복잡한 과정을 거쳐야 한다.

[0006] 고도의 보안을 요구하는 금융이나 의료 서비스의 경우, 종래에는, 사용자가 생성하는 모든 트랜잭션에 대해 사용자 서명을 함께 기록해서 추후 트랜잭션 무결성(integrity) 및 부인방지(non-repudiation) 등을 확인하고 있다.

[0007] 이 경우, 사용자에게 직접적인 API를 제공하는 최상위 서버는 사용자 서명 정보를 로그 데이터에 저장할 수 있으나, 하위 서버들 간 API 호출 시에는 사용자 서명 정보를 로그 데이터로 기록할 수 없다는 문제가 있다.

[0008] 다시 말해, 하위 서버의 경우 자신의 로그 정보에서는 사용자 서명을 확인할 수 없으므로, 자신의 로그 정보에 대한 정합성, 즉, 사용자 요청 트랜잭션과 연관하여 무결성 및 부인 방지 등을 확인하기 위해, 상위 계층의 서

버들의 모든 로그 정보를 통합하여 분석해야 하는 복잡한 과정이 필요하다.

[0009] 예를 들어, 종래의 금융이나 의료 서비스의 경우에는, 다중 계층 서버들 간의 API 통신에서 API 호출을 통한 트랜잭션 송수신 시, 사용자 요청 트랜잭션에 대한 무결성 및 부인 방지를 위해 매 트랜잭션마다 사용자 서명 정보를 함께 전송하고 있다.

[0010] 이에, 사용자와 직접적으로 연결된 최상위 계층 서버에서는 사용자 서명 정보를 확인하고 해당 트랜잭션을 처리하고 있으나, 하위 서버에서는 사용자 서명 정보를 확인하지 못하고 상위 서버로부터 수신한 트랜잭션을 실행할 수밖에 없으며, 하위 서버에서 사용자와 관련한 상태 정보를 업데이트 해야할 경우, 큰 보안 문제가 발생될 문제가 있다.

발명의 내용

해결하려는 과제

[0011] 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은 고효율, 고신뢰성, 저비용 및 고안전성의 토큰 모델링 장치를 제공하는 데 있다.

[0012] 또한, 상기와 같은 문제점을 해결하기 위한 본 발명의 다른 목적은 고효율, 고신뢰성, 저비용 및 고안전성의 데이터 무결성 검증 방법을 제공하는 데 있다.

[0013] 또한, 상기와 같은 문제점을 해결하기 위한 본 발명의 또 다른 목적은 고효율, 고신뢰성, 저비용 및 고안전성의 데이터 무결성 검증 시스템을 제공하는 데 있다.

과제의 해결 수단

[0014] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따라 사용자 단말 및 다중 계층 구조로 제공되는 복수의 서버들과 연동하여, 상기 사용자 단말 및 복수의 서버들 간의 함수 호출에 의한 트랜잭션 전송 시 상기 트랜잭션의 무결성을 검증하는 토큰 모델링 장치는, 메모리(memory) 및 상기 메모리에 저장된 적어도 하나의 명령을 실행하는 프로세서(processor)를 포함하고, 상기 적어도 하나의 명령은, 상기 사용자 단말 또는 상기 복수의 서버들 중 어느 하나의 상위 서버인 호출 단말로부터 상기 트랜잭션의 검증 요청을 수신하도록 하는 명령, 상기 트랜잭션에 기반한 토큰을 블록체인 네트워크 상에 발행하도록 요청하는 명령, 상기 토큰을 상기 호출 단말의 하위 서버로 송신하도록 하는 명령 및 상기 하위 서버로부터, 상기 토큰 내 트랜잭션 정보를 기초로 함수 호출에 의해 상기 호출 단말로부터 수신된 상기 트랜잭션의 무결성을 검증한 검증 결과값을 수신하도록 하는 명령을 포함한다.

[0015] 여기서, 상기 호출 단말로부터 상기 트랜잭션의 검증 요청을 수신하도록 하는 명령은, 상기 호출 단말로부터 상기 트랜잭션의 검증을 위한 요청 트랜잭션을 수신하도록 하는 명령을 포함할 수 있다.

[0016] 이때, 상기 요청 트랜잭션은, 상기 호출 단말로부터 상기 트랜잭션의 정보 및 상기 호출 단말의 서명 정보를 포함할 수 있다.

[0017] 또한, 상기 트랜잭션에 기반한 토큰을 블록체인 네트워크 상에 발행하도록 요청하는 명령은, 상기 요청 트랜잭션을 바탕으로 상기 트랜잭션에 기반한 토큰 발행을 요청하기 위한 블록체인 트랜잭션을 송신하도록 하는 명령, 상기 블록체인 네트워크로부터 상기 토큰의 발행 완료 정보를 수신하여 상기 호출 단말에 송신하도록 하는 명령, 상기 토큰의 소유자를 상기 호출 단말로 설정하도록 하는 명령 및 상기 토큰의 소유자 속성 정보를 상기 사용자 단말로 설정하고, 설정 완료 정보를 상기 호출 단말로 송신하도록 하는 명령을 포함할 수 있다.

[0018] 이때, 상기 토큰은 대체 불가능한, 무결성이 보장된 토큰일 수 있다.

[0019] 상기 토큰을 상기 호출 단말의 하위 서버로 송신하도록 하는 명령에서는, 상기 토큰의 소유자가 상기 하위 서버로 변경할 수 있다.

[0020] 또한, 상기 검증 결과값은, 상기 토큰 내 트랜잭션 정보와 상기 호출 단말로부터 수신된 상기 트랜잭션 정보가 일치할 경우, 상기 하위 서버가 상기 트랜잭션을 처리하고 발행한 처리 결과 값일 수 있다.

[0021] 상기 토큰 모델링 장치는 상기 트랜잭션의 무결성을 검증한 검증 결과값을 수신하도록 하는 명령 이후에, 상기 검증 결과값을 상기 토큰 내 처리 결과 속성 값으로 입력시키도록 하는 명령을 더 포함할 수 있다.

[0022] 상기 목적을 달성하기 위한 본 발명의 다른 실시예에 따라 사용자 단말 및 다중 계층 구조로 제공되는 복수의

서버들과 연동하여 상기 사용자 단말 및 복수의 서버들 간의 함수 호출에 의한 트랜잭션 전송 시 상기 트랜잭션의 무결성을 검증하는 토큰 모델링 장치를 이용해, 데이터의 무결성을 검증하는 방법은, 상기 사용자 단말 또는 상기 복수의 서버들 중 어느 하나의 상위 서버인 호출 단말로부터 상기 트랜잭션의 검증 요청을 수신하는 단계, 상기 트랜잭션에 기반한 토큰을 블록체인 네트워크 상에 발행하도록 요청하는 단계, 상기 토큰을 상기 호출 단말의 하위 서버로 송신하는 단계 및 상기 하위 서버로부터, 상기 토큰 내 트랜잭션 정보를 기초로 함수 호출에 의해 상기 호출 단말로부터 수신된 상기 트랜잭션의 무결성을 검증한 검증 결과값을 수신하는 단계를 포함한다.

[0023] 여기서, 상기 호출 단말로부터 상기 트랜잭션의 검증 요청을 수신하는 단계는, 상기 호출 단말로부터 상기 트랜잭션의 검증을 위한 요청 트랜잭션을 수신하는 단계를 포함할 수 있다.

[0024] 이때, 상기 요청 트랜잭션은, 상기 호출 단말로부터 상기 트랜잭션의 정보 및 상기 호출 단말의 서명 정보를 포함할 수 있다.

[0025] 상기 트랜잭션에 기반한 토큰을 블록체인 네트워크 상에 발행하도록 요청하는 단계는, 상기 요청 트랜잭션을 바탕으로 상기 트랜잭션에 기반한 토큰 발행을 요청하기 위한 블록체인 트랜잭션을 송신하는 단계, 상기 블록체인 네트워크로부터 상기 토큰의 발행 완료 정보를 수신하여 상기 호출 단말에 송신하는 단계, 상기 토큰의 소유자를 상기 호출 단말로 설정하는 단계 및 상기 토큰의 소유자 속성 정보를 상기 사용자 단말로 설정하고, 설정 완료 정보를 상기 호출 단말로 송신하는 단계를 포함할 수 있다.

[0026] 또한, 상기 토큰은 대체 불가능한, 무결성이 보장된 토큰일 수 있다.

[0027] 상기 토큰을 상기 호출 단말의 하위 서버로 송신하는 단계에서는, 상기 토큰의 소유자가 상기 하위 서버로 변경될 수 있다.

[0028] 또한, 상기 검증 결과값은, 상기 토큰 내 트랜잭션 정보와 상기 호출 단말로부터 수신된 상기 트랜잭션 정보가 일치할 경우, 상기 하위 서버가 상기 트랜잭션을 처리하고 발행한 처리 결과 값일 수 있다.

[0029] 상기 데이터 무결성 검증 방법은 상기 트랜잭션의 무결성을 검증한 검증 결과값을 수신하는 단계 이후에, 상기 검증 결과값을 상기 토큰 내 처리 결과 속성 값으로 입력시키는 단계를 더 포함할 수 있다.

[0030] 상기 목적을 달성하기 위한 본 발명의 또 다른 실시예에 따른 데이터 무결성 검증 시스템은 사용자 단말, 다중 계층 구조로 제공되는 복수의 서버들 및 상기 사용자 단말 및 상기 복수의 서버들과 연동하여, 상기 사용자 단말 및 복수의 서버들 간의 함수 호출에 의한 트랜잭션 전송 시 상기 트랜잭션의 무결성을 검증하는 토큰 모델링 장치를 포함하되, 상기 토큰 모델링 장치는, 메모리(memory) 및 상기 메모리에 저장된 적어도 하나의 명령을 실행하는 프로세서(processor)를 포함하되, 상기 적어도 하나의 명령은, 상기 사용자 단말 또는 상기 복수의 서버들 중 어느 하나의 상위 서버인 호출 단말로부터 상기 트랜잭션의 검증 요청을 수신하도록 하는 명령, 상기 트랜잭션에 기반한 토큰을 블록체인 네트워크 상에 발행하도록 요청하는 명령, 상기 토큰을 상기 호출 단말의 하위 서버로 송신하도록 하는 명령 및 상기 하위 서버로부터, 상기 토큰 내 트랜잭션 정보를 기초로 함수 호출에 의해 상기 호출 단말로부터 수신된 상기 트랜잭션의 무결성을 검증한 검증 결과값을 수신하도록 하는 명령을 포함한다.

[0031] 이때, 상기 호출 단말로부터 상기 트랜잭션의 검증 요청을 수신하도록 하는 명령은, 상기 호출 단말로부터 상기 트랜잭션의 검증을 위한 요청 트랜잭션을 수신하도록 하는 명령을 포함하되, 상기 요청 트랜잭션은, 상기 호출 단말로부터 상기 트랜잭션의 정보 및 상기 호출 단말의 서명 정보를 포함할 수 있다.

[0032] 또한, 상기 토큰은, 대체 불가능한, 무결성이 보장된 토큰일 수 있다.

[0033] 또한, 상기 검증 결과값은, 상기 토큰 내 트랜잭션 정보와 상기 호출 단말로부터 수신된 상기 트랜잭션 정보가 일치할 경우, 상기 하위 서버가 상기 트랜잭션을 처리하고 발행한 처리 결과 값일 수 있다.

발명의 효과

[0034] 본 발명의 실시예에 따른 토큰 모델링 장치 및 이를 포함하는 데이터 무결성 검증 시스템 및 방법은 상기 사용자 단말 또는 상기 복수의 서버들 중 어느 하나의 상위 서버인 호출 단말로부터 상기 트랜잭션의 검증 요청을 수신하도록 하는 명령, 상기 트랜잭션에 기반한 토큰을 블록체인 네트워크 상에 발행하도록 요청하는 명령, 상기 토큰을 상기 호출 단말의 하위 서버로 송신하도록 하는 명령 및 상기 하위 서버로부터, 상기 토큰 내 트랜잭션 정보를 기초로 함수 호출에 의해 상기 호출 단말로부터 수신된 상기 트랜잭션의 무결성을 검증한 검증 결과값을 수신하도록 하는 명령을 포함함으로써, 사용자 단말 또는 복수의 서버들 간 API 호출에 따른 트랜잭션의

정보를 블록체인에 기록하여 상기 트랜잭션의 무결성 및 부인 방지를 보장할 수 있다.

[0035] 또한, 블록체인 네트워크를 통해, 하위 서버들이, 사용자 단말의 요청에 부합하는 트랜잭션이 최하위 서버까지 제대로 전달되었지 개별적으로 검증 가능함으로써, 개별 서버가 보유한 트랜잭션 정보에 대한 상호 정합성을 스스로 검증할 수 있으며, 다양한 계층적 서버 환경에서 내부 로그 데이터를 전부 공개하지 않아도, 정합성 검증이 가능한, 고효율, 고신뢰성, 저비용 및 고안전성의 토큰 모델링 장치 및 이를 포함하는 데이터 무결성 검증 시스템 및 방법을 제공할 수 있다.

도면의 간단한 설명

[0036] 도 1은 본 발명의 실시예에 따른 데이터 무결성 검증 시스템의 동작 구성도이다.

도 2는 본 발명의 실시예에 따른 데이터 무결성 검증 시스템의 블록 구성도이다.

도 3은 본 발명의 실시예에 따른 토큰 모델링 장치의 소프트웨어 구성들을 설명하기 위한 블록 구성도이다.

도 4는 본 발명의 실시예에 따른 대체 불가능한 토큰의 데이터 구조를 설명하기 위한 표이다.

도 5는 본 발명의 실시예에 따른 토큰 모델링 장치의 하드웨어 구성들을 설명하기 위한 블록 구성도이다.

도 6은 본 발명의 실시예에 따른 토큰 모델링 장치를 이용한 데이터 무결성 검증 방법을 설명하기 위한 순서도이다.

도 7은 본 발명의 실시예에 따른 데이터 무결성 검증 시스템을 이용한 오픈 뱅킹 서비스 구조를 설명하기 위한 이미지이다.

발명을 실시하기 위한 구체적인 내용

[0037] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하여 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0038] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는 데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. "및/또는"이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0039] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0040] 본 출원에서 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 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0041] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0042] 본 발명에서 개시되는 블록체인(blockchain)은 트랜잭션(transaction)들의 집합으로 구성된 블록이 이전 블록의 해시(hash)값을 담아 모든 블록을 체인 형식으로 연결하는 데이터 구조로서, 블록체인 네트워크에 참여하는 모든 노드(node)가 상기 데이터 구조를 동일하게 유지하고, 합의 알고리즘(consensus algorithm)을 기반으로 새로

운 블록을 생성하여 연결하는 분산 원장 기술(distributed ledger technology)이다. 특정 노드의 블록체인 데이터가 임의로 조작되더라도 블록 간에 이전 블록의 해시값을 가지고 있으므로 데이터 조작을 바로 탐지할 수 있으며, 조작된 데이터는 노드 간에 합의된 것이 아니기 때문에 블록체인에 반영되지 않는다. 이처럼 블록체인은 데이터를 임의로 위변조하는 것이 불가능하여 데이터의 무결성 및 투명성을 보장해준다.

[0043] 블록체인은 무허가형 블록체인(permissionless blockchain)과 허가형 블록체인(permissioned blockchain)으로 구분된다. 무허가형 블록체인은 사용자 및 노드가 아무런 제약 없이 블록체인 네트워크에 참여할 수 있는 블록체인이다. 대표적인 무허가형 블록체인으로는 비트코인(Bitcoin) 및 이더리움(Ethereum)이 있다. 허가형 블록체인은 허가된 사용자 및 노드들만 블록체인 네트워크에 참여할 수 있는, 비즈니스 환경에서 활용하기에 적합한 블록체인이다. 대표적인 허가형 블록체인으로는 하이퍼레저 패브릭(Hyperledger Fabric)이 있다.

[0044] 블록체인 상에서 실행되는 프로그램인 스마트 컨트랙트(smart contract)에 비즈니스 로직을 구성하여 분산 애플리케이션(distributed application: dApp)을 개발 및 운영할 수 있다.

[0045] 스마트 컨트랙트는 제3자의 개입 없이 요청을 비즈니스 로직에 따라 자동으로 실행한다는 장점을 갖고 있다. 대표적인 dApp으로 토큰(token)이 있다.

[0046] 토큰은 디지털 자산(digital asset)을 블록체인 상에 표현한 것이다. 블록체인에 디지털 자산을 토큰화하면 디지털 자산의 소유권 증명, 투명성 및 유동성 보장 등의 장점을 확보할 수 있다. 토큰은 대체가능 토큰(fungible token)과 대체불가능 토큰(non-fungible token)으로 구분된다. 대체가능 토큰은 쪼개질 수 있는 디지털 자산을 표현한 토큰이고, 대체불가능 토큰은 쪼개질 수 없는 디지털 자산을 표현한 토큰이다.

[0047] API 기반 서비스는 기업 및 조직 내부의 데이터나 업무 프로세스를 표준 기술에 기반한 네트워크 통신을 통해 시스템 간의 연계, 소프트웨어 컴포넌트 간의 통합, 혹은 다양한 디바이스 간의 연결을 손쉽게 구현할 수 있도록 하는 기술이다. API 기반 서비스를 사용하면 서비스 간의 조합이나 확대가 매우 용이하므로, 많은 서비스들에서는 한 서버에서 특정 서비스를 구축하기 위해 타 서버에서 제공하는 API를 호출하여 구성하는 경우가 일반적이다. API를 제공해준 서버 또한 타 서버에서 제공하는 API를 호출하여 특정 서비스를 구축할 수 있다. 이처럼 여러 서버들이 API 호출로 상호 연결된 계층적 구조를 다중 계층 서버 간 API 통신이라고 한다.

[0048] API 기반 서비스를 제공하는 서버들은 내부적으로 실행되는 트랜잭션 처리 내용을 모두 기록(로깅)하여 로그 데이터로 관리한다. 로그 데이터는 사후 분석을 통해 서버 동작에 대한 악의적 공격 유무를 판단하는데 활용되는 매우 중요한 정보이다.

[0049] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 본 발명을 설명함에 있어 전체적인 이해를 용이하게 하기 위하여 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다.

[0051] 도 1은 본 발명의 실시예에 따른 데이터 무결성 검증 시스템의 동작 구성도이다.

[0052] 도 1을 참조하면, 데이터 무결성 검증 시스템(S)은 사용자 단말(1000), 복수의 서버(3000)들 및 토큰 모델링 장치(5000)를 포함할 수 있다.

[0053] 보다 구체적으로 설명하면, 사용자 단말(1000) 및 복수의 서버(3000)들은 토큰 모델링 장치(5000)와 연동될 수 있다. 이에 따라, 토큰 모델링 장치(5000)는 사용자 단말(1000) 및 복수의 서버(3000)들로부터 수신된 트랜잭션 정보에 기반한 토큰을 블록체인 네트워크(B) 상에 발행할 수 있다. 여기서, 트랜잭션은 데이터베이스의 상태를 변환시키기 위해 논리적 기능을 수행하는 기본 작업 단위로, 트랜잭션 정보로는 로그 데이터의 일부 정보가 포함될 수 있다.

[0054] 이후, 복수의 서버(3000)들 중 어느 하나는 함수 호출에 의해 동적 수신된 트랜잭션을 블록체인 네트워크(B) 상에 발행된 토큰 내 트랜잭션 정보와 비교함으로써, 상기 트랜잭션이 사용자 단말(1000) 또는 해당 서버(3000)의 상위 서버로부터 수신된 트랜잭션 정보가 맞는지의 여부를 확인할 수 있다.

[0055] 다시 말하면, 복수의 서버(3000)들은 블록체인 네트워크(B) 상의 노드(node)로 참여하여, 외부로부터 함수 호출에 의해 수신된 트랜잭션을 토큰 내 트랜잭션 정보와 비교함으로써 상기 트랜잭션의 무결성 및 정합성을 검증할 수 있다. 따라서, 복수의 서버(3000)들은 무결성 및 정합성이 검증된 트랜잭션을 처리할 수 있다.

[0056] 하기 도 2에서는 데이터 무결성 검증 시스템(S)에 대해 구성별로 보다 구체적으로 설명하겠다.

[0058] 도 2는 본 발명의 실시예에 따른 데이터 무결성 검증 시스템의 블록 구성도이다.

[0059] 도 2를 참조하면, 사용자 단말(1000)은 적어도 하나의 온라인 웹 서비스를 실행하기 위한 하드웨어(Hardware) 단말로 제공될 수 있다.

[0060] 실시예에 따르면, 사용자 단말(1000)은 사용자 요청에 따른 온라인 웹 서비스를 제공하기 위해, API(Application Programming Interface)를 이용하여 어느 하나의 서버(3000)를 호출할 수 있다.

[0061] 다시 말하면, 사용자 단말(1000)은 API에 의해 특정 서버를 호출하여 트랜잭션을 송신할 수 있다. 여기서, 특정 서버는 후술될 복수의 서버(3000)들 중 최상위 계층에 존재하는 제1 서버일 수 있다.

[0062] 또한, 사용자 단말(1000)은 후술될 토큰 모델링 장치(5000)를 호출하기 위해, 상기 트랜잭션의 정보 및 사용자 단말(1000)의 서명 정보를 포함하는 요청 트랜잭션을 송신할 수 있다. 이에 따라, 토큰 모델링 장치(5000)는 블록체인 네트워크(B) 상에 상기 트랜잭션의 정보 및 사용자 단말(1000)의 서명 정보를 포함하는 토큰을 발행할 수 있다.

[0063] 이후, 사용자 단말(1000)은 토큰 모델링 장치(5000)를 호출하여, 상기 토큰을 제1 서버로 송신시킬 수 있다. 다시 말하면, 토큰 모델링 장치(5000)는 사용자 단말(1000)의 요청에 의해 블록체인 네트워크(B) 상에 발행된 토큰을 최상위 서버로 전송할 수 있다.

[0064] 이에 따라, 제1 서버는 사용자 단말(1000)로부터 수신된 트랜잭션의 무결성 및 정합성을 검증할 수 있다.

[0065] 일 실시예에 따르면, 제1 서버는 사용자 단말(1000)로부터 수신된 트랜잭션 내 사용자 단말(1000)의 서명 정보를 이용하여, 트랜잭션의 무결성 및 정합성을 검증할 수 있다.

[0066] 다른 실시예에 따르면, 제1 서버는 사용자 단말(1000)로부터 수신된 트랜잭션을 토큰 모델링 장치(5000)로부터 전송된 토큰 내 트랜잭션 정보와 비교하여, 상기 트랜잭션의 무결성 및 정합성을 검증할 수 있다.

[0067] 복수의 서버(3000)들은 특정 온라인 웹 서비스를 실행하기 위한 적어도 하나의 정보를 포함할 수 있다.

[0068] 또한, 복수의 서버(3000)들은 API 호출로 상호 연결된 다중 계층 서버 구조(제1 서버 내지 제n 서버)로 제공될 수 있다. 이에 따라, 사용자가 특정 온라인 웹 서비스를 실행하고자 할 경우, 사용자 단말(1000)은 API를 호출하여 복수의 서버(3000)들 중 제1 서버를 실행하고, 제1 서버는 API 호출에 의해 이하 하위 서버를 순차적으로 실행함으로써 특정 온라인 웹 서비스의 실행을 위한 적어도 하나의 정보를 제공하는 최하위 서버인 제n 서버까지 트랜잭션을 전송할 수 있다.

[0069] 이때, 제1 서버는 앞서 설명한 바와 같이, 사용자 단말(1000)로부터 수신된 트랜잭션의 무결성 및 정합성이 검증될 경우, 상기 트랜잭션을 처리하고, 토큰 모델링 장치(5000)를 호출하여 상기 트랜잭션의 처리 결과값을 상기 토큰에 기록시킬 수 있다.

[0070] 이후, 제1 서버는 API 호출에 의해 신규 트랜잭션을 하위 서버인 제2 서버로 전송할 수 있다.

[0071] 또한, 제1 서버는 앞서 설명한 사용자 단말(1000)에서와 같이, 토큰 모델링 장치(5000)로 하여금, 상기 신규 트랜잭션의 정보 및 제1 서버의 서명 정보를 포함하는 토큰을 블록체인 네트워크(B) 상에 발행하도록 하고, 신규 발행된 토큰을 제2 서버로 전송하도록 호출할 수 있다.

[0072] 이에 따라, 신규 트랜잭션을 수신한 제2 서버는 앞서 설명한 제1 서버와 같이, 상기 신규 트랜잭션과 토큰 모델링 장치(5000)로부터 전송된 신규 토큰 내 신규 트랜잭션 정보를 비교하여, 상기 신규 트랜잭션의 무결성 및 정합성을 검증하고, 상기 신규 토큰에 처리 결과값을 기록할 수 있다.

[0073] 이후, 제2 서버는 API 호출에 의해, 하위 서버인 제3 서버를 호출할 수 있다.

[0074] 이하, 제3 서버 내지 최하위 서버인 제N 서버들은, 앞서 설명된 제1 서버 및 제2 서버의 일련의 동작들을 반복 수행하여, 각각 상위 서버로부터 수신된 해당 트랜잭션의 무결성 및 정합성을 검증할 수 있다.

[0075] 토큰 모델링 장치(5000)로부터 발행된 토큰을 이용하여 사용자 단말(1000) 또는 복수의 서버(3000)들 중 상위 서버로부터 수신된 트랜잭션의 무결성 및 정합성을 검증하는 방법은 토큰 모델링 장치(5000)를 이용한 후술될 데이터 무결성 검증 방법의 설명 시 보다 자세히 설명하겠다.

[0076] 토큰 모델링 장치(5000)는 사용자 단말(1000) 및 복수의 서버(3000)들과 블록체인 네트워크(B) 사이의 통신 환경을 제공할 수 있다.

[0077] 다시 말하면, 토큰 모델링 장치(5000)는 사용자 단말(1000) 또는 복수의 서버(3000)들로부터 수신되는 요청 트

랜잭션을 바탕으로, 상기 요청 트랜잭션에 기반한 토큰을 블록체인 네트워크(B) 상에 발행할 수 있다. 다시 말하면, 토큰 모델링 장치(5000)는 상기 요청 트랜잭션에 기반한 토큰을 모델링 할 수 있다.

[0078] 토큰 모델링 장치에 대해서는 하기 도 3 및 도 4를 참조하여 구성별로 보다 자세히 설명하겠다.

[0080] 도 3은 본 발명의 실시예에 따른 토큰 모델링 장치의 소프트웨어 구성들을 설명하기 위한 블록 구성도이다.

[0081] 도 3을 참조하면, 토큰 모델링 장치(5000)는 발행부(5100), 전송부(5300), 수정부(5500) 및 알림부(5700)를 포함할 수 있다.

[0082] 보다 구체적으로 설명하면, 발행부(5100)는 사용자 단말(1000) 또는 복수의 서버(3000)들 중 어느 하나의 상위 서버에 의해 호출되어 실행될 수 있다.

[0083] 실시예에 따르면, 발행부(5100)는 사용자 단말(1000) 또는 복수의 서버(3000)들 중 어느 하나의 상위 서버로부터 호출되어, 해당 구성으로부터 수신된 요청 트랜잭션에 기반하여 토큰을 발행을 위한 블록체인 트랜잭션을 생성할 수 있다. 이에 따라, 발행부(5100)는 생성된 블록체인 트랜잭션을 블록체인 네트워크(B)로 전송함으로써, 블록체인 네트워크(B) 상에 토큰이 발행될 수 있다.

[0084] 실시예에 따르면, 상기 블록체인은 허가형 블록체인(permissioned blockchain)으로 제공될 수 있다. 여기서, 허가형 블록체인은 허가된 노드인 복수의 서버(3000)들만이 블록체인 네트워크(B) 상에 참여하도록 제한한 것일 수 있다. 이에 따라 허가형 블록체인은 비즈니스 환경에 적용되기 적합할 수 있다. 예를 들어, 허가형 블록체인은 하이퍼레저 패브릭(hyperledger fabric) 구조로 제공될 수 있다.

[0085] 발행부(5100)는 토큰의 발행 시, 요청 트랜잭션을 전송한 해당 구성을 토큰의 소유자로 지정할 수 있다. 실시예에 따르면, 발행부(5100)는 사용자 단말(1000)로부터 요청 트랜잭션을 수신할 경우, 사용자 단말(1000)을 해당 토큰의 소유자로 지정할 수 있다.

[0086] 하기 도 4에서는 발행부(5100)에 의해 발행되는 대체 불가능한 토큰의 데이터 구조를 보다 자세히 설명하겠다.

[0088] 도 4는 본 발명의 실시예에 따른 대체 불가능한 토큰의 데이터 구조를 설명하기 위한 표이다.

[0089] 도 4를 참조하면, 대체 불가능한 토큰은 표준 속성 및 확장 속성으로 분류될 수 있다.

[0090] 실시예에 따르면, 대체 불가능한 토큰의 표준 속성으로는 토큰 ID, 토큰 타입, 소유자 및 피승인자의 속성 정보 중 적어도 하나가 포함될 수 있다.

[0091] 또한, 대체 불가능한 토큰의 확장 속성으로는 온체인(on-chain) 확장 속성 및 오프체인(off-chain) 확장 속성 중 적어도 하나가 포함될 수 있다.

[0092] 이때, 온체인 확장 속성은 하위 속성으로 API 호출에 따른 트랜잭션의 정보, 처리 결과, 부모 및 자식 중 적어도 하나의 속성 정보를 포함할 수 있으며, 오픈체인 확장 속성은 하위 속성으로 경로 및 해시 중 적어도 하나의 속성 정보를 포함할 수 있다. 예를 들면, 대체 불가능한 토큰은 토큰 ID, 토큰 타입, 소유자, API 호출에 따른 트랜잭션 정보, 부모, 자식 속성 및 처리 결과 속성 정보 중 적어도 하나를 포함한 데이터 구조로 제공될 수 있다.

[0093] 실시예에 따라 보다 구체적으로 설명하면, API 호출에 따른 트랜잭션의 정보는, 앞서 설명한 바와 같이, 사용자 단말(1000) 또는 복수의 서버(3000)들 중 어느 하나의 API 호출에 의해 전송되는 해당 트랜잭션의 속성 정보일 수 있으며, 토큰의 처리 결과 속성 정보는 해당 트랜잭션 및 토큰 내 해당 트랜잭션의 비교를 통해 검증된 검증 결과값일 수 있다.

[0094] 또한, 토큰의 타입 속성으로는 로그 데이터가 적용될 수 있다.

[0095] 또한, 부모 속성은 복수의 서버(3000)들 중 상위 서버의 트랜잭션 정보에 기반한 대체 불가능한 토큰의 토큰 ID 정보일 수 있으며, 자식 속성은 하위 서버의 트랜잭션 정보를 기록한 대체 불가능한 토큰의 토큰 ID 정보일 수 있다.

[0096] 예를 들어, 사용자 단말(1000)이 대체 불가능한 제1 토큰을 발행하여 최상위 서버인 제1 서버로 전송하고, 상기 제1 토큰을 이용하여 API 호출에 따른 트랜잭션의 검증을 완료한 상기 제1 서버가 대체 불가능한 제2 토큰을 발행하여 하위 서버인 제2 서버로 전송할 경우, 제2 토큰의 부모 속성은 제1 토큰일 수 있다. 다시 말해, 제1 토큰의 자식 속성은 제2 토큰일 수 있다.

[0097]

[0098] 다시 도 3을 참조하면, 전송부(5300)는 발행부(5100)에 의해 블록체인 네트워크(B) 상에 발행된 대체 불가능한 토큰을 전송할 수 있다.

[0099] 실시예에 따라 보다 구체적으로 설명하면, 전송부(5300)는 발행부(5100)에 의해 블록체인 네트워크(B) 상에 발행된 대체 불가능한 토큰을 하위 서버(3000)로 전송하기 위한 블록체인 트랜잭션을 생성할 수 있다. 이에 따라, 전송부(5300)는 해당 토큰을 특정 하위 서버(3000)로 전송할 수 있다.

[0100] 또한, 특정 하위서버로의 토큰 전송으로 인해, 상기 토큰의 소유권은 해당 하위 서버로 변경될 수 있다.

[0101] 수정부(5500)는 토큰 내 확장 속성의 하위 속성값 수정을 요청하기 위한 블록체인 트랜잭션을 생성하여, 블록체인 네트워크(B) 상의 토큰으로 전송할 수 있다. 이에 따라, 블록체인 네트워크(B) 상에 발행된 토큰 내 하위 속성값이 수정될 수 있다.

[0102] 실시예에 따라 보다 구체적으로 설명하면, 특정 서버가, 상위 서버(특정 서버가 제1 서버일 경우, 사용자 단말)로부터 API 호출에 의해 전달받은 해당 트랜잭션의 무결성 및 정합성을 검증한 후, 검증 결과값을 포함하는 요청 트랜잭션을 수정부(5500)로 전송할 경우, 수정부(5500)는 블록체인 네트워크 상에 블록체인 트랜잭션을 전송하여 토큰 내 확장 속성의 하위 속성값을 상기 검증 결과값으로 수정할 수 있다. 이때, 특정 서버는 토큰 소유자로, 수정부(5500)는 토큰의 소유자에 의해 호출될 수 있다.

[0103] 알림부(5700)는 토큰 모델링 장치(5000)가 블록체인 네트워크(B)로부터 이벤트를 수신할 경우, 상기 이벤트와 관련된 사용자 단말(1000) 또는 복수의 서버(3000)들 중 어느 하나에 알림을 송신할 수 있다.

[0104] 실시예에 따르면, 알림부(5700)는 발행부(5100), 전송부(5300) 및 수정부(5500)의 호출에 따른 상기 토큰의 처리 결과를 상기 토큰의 소유자에게 송신할 수 있다.

[0105] 예를 들어, 알림부(5700)는 사용자 단말(1000) 또는 복수의 서버(3000)들 중 어느 하나가 발행부(5100)를 호출하여, 블록체인 네트워크(B) 상에 대체 불가능한 토큰을 발행할 경우, 발행부(5100)를 호출한 상기 토큰의 소유자에게 토큰 발행 완료 이벤트를 송신할 수 있다.

[0106] 또한, 알림부(5700)는 사용자 단말(1000) 또는 복수의 서버(3000)들 중 어느 하나가 전송부(5300)를 호출하여, 발행된 토큰을 하위 서버로 전송할 경우, 상기 토큰을 전송 받은 새로운 소유자에게 상기 토큰의 전송 완료 이벤트를 송신할 수 있다.

[0107] 그리고, 알림부(5700)는 복수의 서버(3000)들 중 어느 하나가 수정부(5500)를 호출하여 토큰의 소유자 속성 정보를 변경할 경우, 다시 말해, 토큰의 확장 속성의 하위 속성값을 기록할 경우, 수정부(5500)를 호출한 호출자에게 토큰의 수정 완료 이벤트를 호출자에게 송신할 수 있다.

[0109] 도 5는 본 발명의 실시예에 따른 토큰 모델링 장치의 하드웨어 구성들을 설명하기 위한 블록 구성도이다.

[0110] 도 5를 참조하면, 토큰 모델링 장치(5000)는 적어도 하나의 명령을 저장하는 메모리(100) 및 상기 메모리(100)의 적어도 하나의 명령을 실행하는 프로세서(200)를 포함할 수 있다.

[0111] 또한, 토큰 모델링 장치(5000)는 상기 프로세서(200)를 통해 실행되는 네트워크와 연결되어 통신을 수행하는 송수신 장치(300), 입력 인터페이스 장치(400), 출력 인터페이스 장치(500) 및 저장 장치(600) 등을 더 포함할 수 있다.

[0112] 토큰 모델링 장치(5000)에 포함된 각각의 구성 요소들은 버스(bus, 700)에 의해 연결되어 서로 통신을 수행할 수 있다.

[0113] 토큰 모델링 장치(5000) 내 메모리(100) 및 저장 장치(600)는 각각 휘발성 저장 매체 및 비휘발성 저장 매체 중에서 적어도 하나로 구성될 수 있다. 예를 들어, 메모리(100)는 읽기 전용 메모리(read only memory, ROM) 및 랜덤 액세스 메모리(random access memory, RAM) 중에서 적어도 하나로 구성될 수 있다.

[0114] 메모리(100)는 후술될 프로세서(200)에 의해 실행될 적어도 하나의 명령을 포함할 수 있다. 실시예에 따르면, 적어도 하나의 명령은, 상기 사용자 단말 또는 상기 복수의 서버들 중 어느 하나의 상위 서버인 호출 단말로부터 상기 트랜잭션의 검증 요청을 수신하도록 하는 명령, 상기 트랜잭션에 기반한 토큰을 블록체인 네트워크 상에 발행하도록 요청하는 명령, 상기 토큰을 상기 호출 단말의 하위 서버로 송신하도록 하는 명령 및 상기 하위 서버로부터, 상기 토큰 내 트랜잭션 정보를 기초로 함수 호출에 의해 상기 호출 단말로부터 수신된 상기 트랜잭

션의 무결성을 검증한 검증 결과값을 수신하도록 하는 명령을 포함할 수 있다.

[0115] 프로세서(200)는 중앙 처리 장치(central processing unit, CPU), 그래픽 처리 장치(graphics processing unit, GPU), 또는 본 발명의 실시예들에 따른 방법들이 수행되는 전용의 프로세서를 의미할 수 있다.

[0116] 프로세서(200)는 앞서 설명한 바와 같이, 메모리(100)에 저장된 적어도 하나의 프로그램 명령(program command)을 실행할 수 있다. 실시예에 따르면, 프로세서(200)는 메모리(100)에 저장된 적어도 하나의 명령에 따라 적어도 하나의 앞서 설명된 적어도 하나의 소프트웨어 구성들을 실행할 수 있다.

[0117] 상기 적어도 하나의 명령을 수행하는 프로세서(200)의 동작은 후술될 본 발명의 실시예에 따른 토큰 모델링 장치를 이용한 데이터 무결성 검증 방법의 설명 시 보다 자세히 설명하겠다.

[0119] 이상, 본 발명의 실시예에 따른 토큰 모델링 장치를 포함하는 데이터 무결성 검증 시스템에 대해 설명하겠다. 이하에서는, 상기 토큰 모델링 장치의 프로세서(200)에 따라 구현되는 데이터 무결성 검증 방법에 대해 설명하겠다.

[0121] 도 6은 본 발명의 실시예에 따른 토큰 모델링 장치를 이용한 데이터 무결성 검증 방법을 설명하기 위한 순서도이다.

[0122] 도 6을 참조하면, 토큰 모델링 장치 내 프로세서(200)는 사용자 단말(1000)의 호출에 의해 실행되어, 사용자 단말(1000)로부터 요청 트랜잭션을 수신할 수 있다(S1000). 이때, 요청 트랜잭션은 사용자 단말(1000)의 서명 정보 및 API 호출에 의해 사용자 단말(1000)로부터 최상위 서버인 제1 서버로 전송된 제1 트랜잭션의 정보를 포함할 수 있다.

[0123] 이후, 프로세서(200)는 사용자 단말(1000)의 호출에 의해 발행부(5100)를 실행하여, 요청 트랜잭션에 기반한 제1 토큰의 생성을 요청하는 블록체인 트랜잭션을 블록체인 네트워크(B)로 송신할 수 있다(S2000). 이에 따라, 블록체인 네트워크(B)에 제1 토큰이 발행될 수 있다. 이때, 제1 토큰의 소유자는 프로세서(200)를 호출한 사용자 단말(1000)일 수 있으며, 트랜잭션 속성 정보는 제1 트랜잭션 정보로 설정될 수 있다.

[0124] 블록체인 네트워크(B) 상에 제1 토큰이 발행된 경우, 프로세서(200)는 알림부(5700)를 실행하여, 제1 토큰의 발행 완료 정보를 사용자 단말(1000)에 전송할 수 있다(S3000). 이후, 프로세서(200)는 사용자 단말(1000)의 호출에 의해 전송부(5300)를 실행하여, 상기 사용자 단말(1000)의 하위 서버인 제1 서버로 제1 토큰을 전송할 수 있다(S4000). 다시 말해, 제1 토큰의 소유자는 제1 서버로 변경될 수 있다.

[0125] 제1 토큰의 소유자가 변경되면, 프로세서(200)는 알림부(5700)를 실행하여, 제1 토큰의 전송 완료 정보를 제1 서버로 송신할 수 있다(S5000). 이에 따라, 제1 서버는 사용자 단말(1000)로부터 API 호출에 의해 수신된 제1 트랜잭션을, 프로세서(200)로부터 수신된 제1 토큰 내 제1 트랜잭션 정보와 비교하여, 제1 트랜잭션의 무결성 및 정합성을 검증할 수 있다. 실시예에 따르면, API 호출에 의해 수신된 제1 트랜잭션 및 프로세서(200)로부터 수신된 제1 토큰 내 제1 트랜잭션 정보가 일치할 경우, 제1 서버는 API 호출에 의해 수신된 제1 트랜잭션을 처리할 수 있다.

[0126] 이후, 프로세서(200)는 제1 서버의 호출에 의해 수정부(5500)를 실행하여, 블록체인 네트워크(B) 상에 발행된 제1 토큰의 트랜잭션 처리 결과 값의 기록을 요청하는 블록체인 트랜잭션을 발행할 수 있다(S6000).

[0127] 이후, 프로세서(200)는 알림부(5700)를 실행하여, 제1 서버로 트랜잭션 처리 결과 값의 수정 완료 정보를 전송할 수 있다(S7000). 따라서, 제1 서버로 수신된 API 호출에 의한 제1 트랜잭션의 무결성 검증이 완료될 수 있다.

[0128] 이후, 제1 서버는 하위 서버인 제2 서버로 API 호출에 의한 제2 트랜잭션을 전송할 수 있다. 이에 따라 프로세서(200)는 제1 서버의 호출에 의해 S1000 내지 S7000 단계를 반복 수행함으로써, 제2 트랜잭션의 데이터 무결성을 검증할 수 있다. 다시 말해, 이는 제N 서버가 최하위 서버일 때까지 N을 N+1 만큼 증가(S8000)시켜, 제N 서버가 최하위 서버(S9000)일 때까지 S1000 내지 S7000 단계를 반복 수행할 수 있다.

[0129] 이때, 이후의 S4000 단계를 수행하는 프로세서(200)는 제N 토큰의 소유자 변경 시, 제N 토큰의 부모 속성을 제N-1 토큰으로 설정할 수 있으며, 제N 서버의 호출에 의해 수정부(5500)를 실행하여, 제N-1 토큰의 자식 속성을 제N 토큰으로 변경할 수 있다. 이에 따라, 하위 서버인 복수의 서버(3000)들 중 어느 하나는 블록체인 네트워크(B) 상에 발행된 토큰을 통해, API 호출에 의한 트랜잭션 간 상관관계의 추적이 가능함으로써, 트랜잭션의 발행을 최초로 요청한 사용자 단말(1000)에 대한 검증이 가능할 수 있다.

[0131] 이상, 본 발명의 실시예에 따라 토큰 모델링 장치를 포함하는 데이터 무결성 검증 시스템 및 방법을 설명하였다.

[0132] 이하에서는, 본 발명의 실시예에 따른 데이터 무결성 검증 시스템을 이용한 서비스 구조 모델을 설명하겠다.

[0134] 도 7은 본 발명의 실시예에 따른 데이터 무결성 검증 시스템을 이용한 오픈 뱅킹 서비스 구조를 설명하기 위한 이미지이다.

[0135] 도 7을 참조하면, 오픈 뱅킹 서비스는 사용자 단말(D), 이용 기관(A), 오픈 뱅킹 센터(C), 참가 은행(P)들로 구성될 수 있다.

[0136] 실시예에 따르면, 오픈 뱅킹 서비스는 사용자 단말(D), 이용 기관(A), 오픈 뱅킹 센터(C), 참가 은행(P)들이 API 호출로 상호 연계된 다중 계층 서버 구조로 제공될 수 있다.

[0137] 보다 구체적으로 설명하면, 이용 기관(A)은 카카오페이, 토스 등의 핀테크 서비스 및 핀테크 업체일 수 있으며, 트랜잭션 발생시 마다 사용자 서명 정보를 확인할 수 있는 최상위 계층의 서버일 수 있다.

[0138] 또한, 오픈 뱅킹 센터(C)는 오픈 뱅킹 API를 제공하는 금융 결제원을 나타내는 중간 계층 서버일 수 있다.

[0139] 그리고, 참가 은행(P)들은 사용자의 은행 계좌를 관리하는 금융 기관을 나타내는 최하위 계층 서버이다.

[0140] 최상위 계층 서버인 이용 기관(A)은 사용자 요청 트랜잭션을 처리하기 위해 중간 계층 서버인 오픈 뱅킹 센터(C)를 거쳐 최하위 계층 서버인 참가 은행(P)들에게 명령 트랜잭션을 전송함으로써 사용자 계좌를 조회하기도 하고, 사용자 계좌 상태 정보를 수정할 수 있다.

[0141] 일반적으로, 오픈 뱅킹 서비스 중 출금 이체 기능은 최하위 계층 서버인 참가 은행(P)에서 사용자 계좌 상태를 업데이트 해야하는 과정이 필수적으로 요구된다.

[0142] 이에, 종래의 오픈 뱅킹 서비스는 사용자 서명 정보가 매 트랜잭션마다 전송되어, 트랜잭션 실행을 담당하는 해당 서버에서 트랜잭션 무결성 및 부인 방지를 검증하였다.

[0143] 보다 자세히 설명하면, 종래의 오픈 뱅킹 서비스는 사용자 단말과 API 호출로 직접 연계된 최상위 서버의 경우 트랜잭션을 사용자 단말의 서명 정보와 함께 수신하여 로그 데이터로 저장하고, 이에 따라 최상위 서버로부터 수신된 사용자 단말의 서명 정보를 이용하여 상기 트랜잭션의 무결성 및 부인 방지를 검증하였다.

[0144] 그러나, 사용자 단말과 직접 연결되지 않은 하위 서버의 경우, 상위 서버로부터 전송된 트랜잭션에 사용자 단말의 서명 정보가 포함되어 있지 않기 때문에 해당 트랜잭션이 사용자 요청에 기반한 것인지를 검증하기 어려운 단점이 발생하였다.

[0145] 이를 해결하고자, 종래에는 하위 서버의 트랜잭션 검증을 위해 상위 서버의 로그 정보 및 하위 서버 API 호출 트랜잭션 정보, 그리고 하위 서버의 로그 데이터 정보를 모두 통합하여 정합성을 확인하는 오픈 뱅킹 서비스를 제공하고 있다.

[0146] 그러나, 로그 데이터는 고객 개인정보 또는 기업이나 조직 내부의 매우 민감한 금융 정보를 담고 있기 때문에, 외부에서의 접근이 매우 엄격하게 통제되므로, 해당 오픈 뱅킹 서비스 또한, 해당 트랜잭션의 정합성 검증을 위해 기관별 별도의 승인 절차를 거쳐야하는 단점이 있다.

[0147] 한편, 본 발명의 실시예에 따라 토큰 모델링 장치를 포함하는 데이터 무결성 검증 시스템 및 방법을 오픈 뱅킹 서비스에 적용할 경우, 종래의 오픈 뱅킹 서비스와 같이 상위 서버로부터 수신된 통합 로그 데이터 정보를 모두 확인하여 정합성을 검증하지 않아도, 하위 서버들인 오픈 뱅킹 센터 및 참가 은행들이 블록체인 네트워크 상에 기록된 상위 서버의 토큰 정보를 이용하여 각각 개별적으로 사용자 단말 또는 상위 서버로부터 수신된 트랜잭션의 무결성 및 정합성 검증이 가능함으로써, 고효율, 고신뢰성, 저비용 및 고안전성의 데이터 무결성 검증 시스템 및 방법을 제공할 수 있다.

[0148]

[0149] 이상, 본 발명의 실시예에 따라 토큰 모델링 장치 및 이를 포함하는 데이터 무결성 검증 시스템 및 방법을 설명하였다.

[0150] 본 발명의 실시예에 따른 토큰 모델링 장치 및 이를 포함하는 데이터 무결성 검증 시스템 및 방법은 상기 사용자 단말 또는 상기 복수의 서버들 중 어느 하나의 상위 서버인 호출 단말로부터 상기 트랜잭션의 검증 요청을

수신하도록 하는 명령, 상기 트랜잭션에 기반한 토큰을 블록체인 네트워크 상에 발행하도록 요청하는 명령, 상기 토큰을 상기 호출 단말의 하위 서버로 송신하도록 하는 명령 및 상기 하위 서버로부터, 상기 토큰 내 트랜잭션 정보를 기초로 함수 호출에 의해 상기 호출 단말로부터 수신된 상기 트랜잭션의 무결성을 검증한 검증 결과값을 수신하도록 하는 명령을 포함함으로써, 사용자 단말 또는 복수의 서버들 간 API 호출에 따른 트랜잭션의 정보를 블록체인에 기록하여 상기 트랜잭션의 무결성 및 부인 방지를 보장할 수 있다.

[0151] 또한, 블록체인 네트워크를 통해 하위 서버들이, 사용자 단말의 요청에 부합하는 트랜잭션이 최하위 서버까지 제대로 전달되었지 개별적으로 검증 가능함으로써, 개별 서버가 보유한 트랜잭션 정보에 대한 상호 정합성을 스스로 검증할 수 있으며, 다양한 계층적 서버 환경에서 내부 로그 데이터를 전부 공개하지 않아도, 정합성 검증이 가능한, 고효율, 고신뢰성, 저비용 및 고안전성의 토큰 모델링 장치 및 이를 포함하는 데이터 무결성 검증 시스템 및 방법을 제공할 수 있다.

[0153] 본 발명의 실시예에 따른 방법의 동작은 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 프로그램 또는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의해 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산 방식으로 컴퓨터로 읽을 수 있는 프로그램 또는 코드가 저장되고 실행될 수 있다.

[0154] 또한, 컴퓨터가 읽을 수 있는 기록매체는 롬(rom), 램(ram), 플래시 메모리(flash memory) 등과 같이 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치를 포함할 수 있다. 프로그램 명령은 컴파일러(compiler)에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터(interpreter) 등을 사용해서 컴퓨터에 의해 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

[0155] 본 발명의 일부 측면들은 장치의 문맥에서 설명되었으나, 그것은 상응하는 방법에 따른 설명 또한 나타낼 수 있고, 여기서 블록 또는 장치는 방법 단계 또는 방법 단계의 특징에 상응한다. 유사하게, 방법의 문맥에서 설명된 측면들은 또한 상응하는 블록 또는 아이템 또는 상응하는 장치의 특징으로 나타낼 수 있다. 방법 단계들의 몇몇 또는 전부는 예를 들어, 마이크로프로세서, 프로그램 가능한 컴퓨터 또는 전자 회로와 같은 하드웨어 장치에 의해(또는 이용하여) 수행될 수 있다. 몇몇의 실시예에서, 가장 중요한 방법 단계들의 하나 이상은 이와 같은 장치에 의해 수행될 수 있다.

[0156] 실시예들에서, 프로그램 가능한 로직 장치(예를 들어, 필드 프로그머블 게이트 어레이)가 여기서 설명된 방법들의 기능의 일부 또는 전부를 수행하기 위해 사용될 수 있다. 실시예들에서, 필드 프로그머블 게이트 어레이는 여기서 설명된 방법들 중 하나를 수행하기 위한 마이크로프로세서와 함께 작동할 수 있다. 일반적으로, 방법들은 어떤 하드웨어 장치에 의해 수행되는 것이 바람직하다.

[0157] 이상 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

[0158] 1000: 사용자 단말 3000: 서버

5000: 토큰 모델링 장치 5100: 발행부

5300: 전송부 5500: 수정부

5700: 알림부 100: 메모리

200: 프로세서 300: 송수신 장치

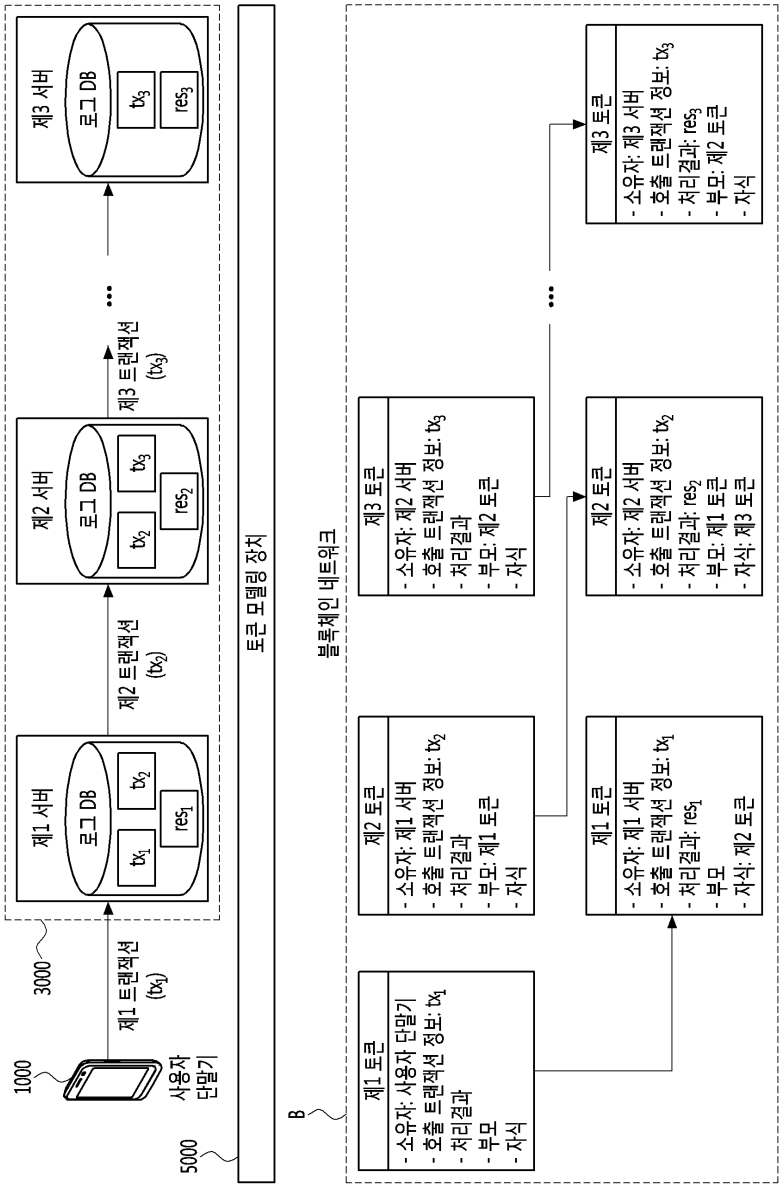
400: 입력 인터페이스 장치 500: 출력 인터페이스 장치

600: 저장 장치 700: 버스(bus)

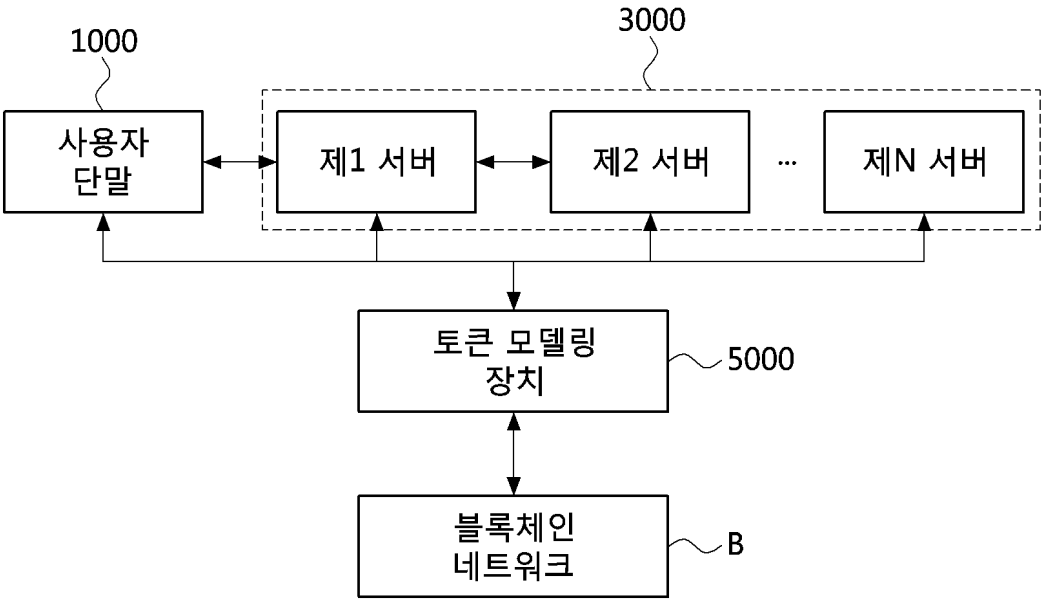
B: 블록체인 네트워크

도면

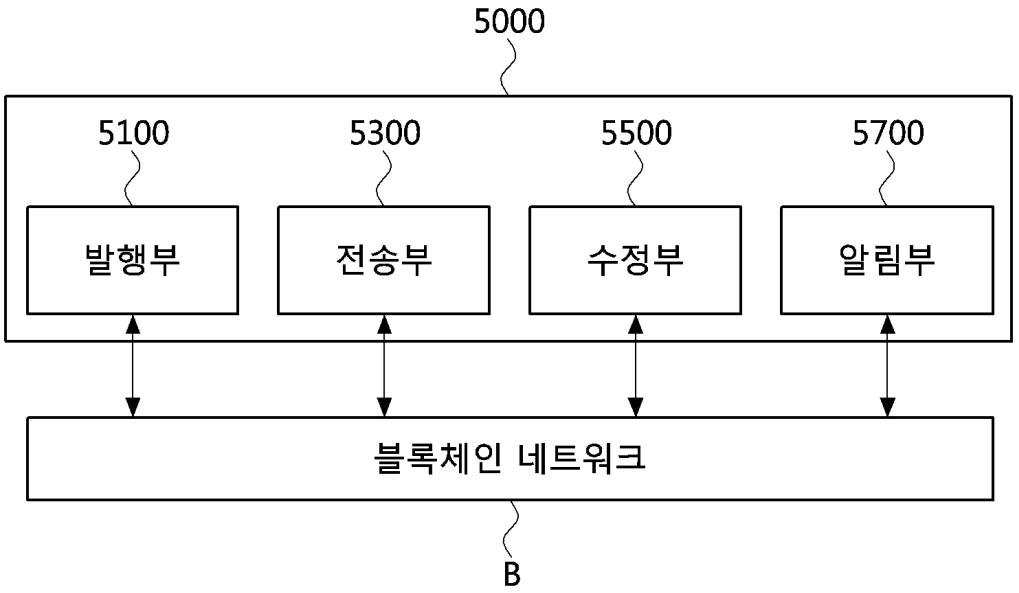
도면1


제1 서버
로그 DB
tx_1
tx_2
res_1
제2 서버
로그 DB
tx_2
tx_3
res_2
제3 서버
로그 DB
tx_3
res_3
제1 트랜잭션 (tx_1)
제2 트랜잭션 (tx_2)
제3 트랜잭션 (tx_3)
3000
1000
사용자 단말기
5000
토큰 모델링 장치
B
블록체인 네트워크
제1 토큰
- 소유자: 사용자 단말기
- 호출 트랜잭션 정보: tx_1
- 처리결과
- 부모
- 자식
제2 토큰
- 소유자: 제1 서버
- 호출 트랜잭션 정보: tx_2
- 처리결과
- 부모: 제1 토큰
- 자식
제3 토큰
- 소유자: 제2 서버
- 호출 트랜잭션 정보: tx_3
- 처리결과
- 부모: 제2 토큰
- 자식
제1 토큰
- 소유자: 제1 서버
- 호출 트랜잭션 정보: tx_1
- 처리결과: res_1
- 부모
- 자식: 제2 토큰
제2 토큰
- 소유자: 제2 서버
- 호출 트랜잭션 정보: tx_2
- 처리결과: res_2
- 부모: 제1 토큰
- 자식: 제3 토큰
제3 토큰
- 소유자: 제3 서버
- 호출 트랜잭션 정보: tx_3
- 처리결과: res_3
- 부모: 제2 토큰
- 자식

도면2


1000
3000
사용자 단말
제1 서버
제2 서버
...
제N 서버
토큰 모델링 장치
5000
블록체인 네트워크
B

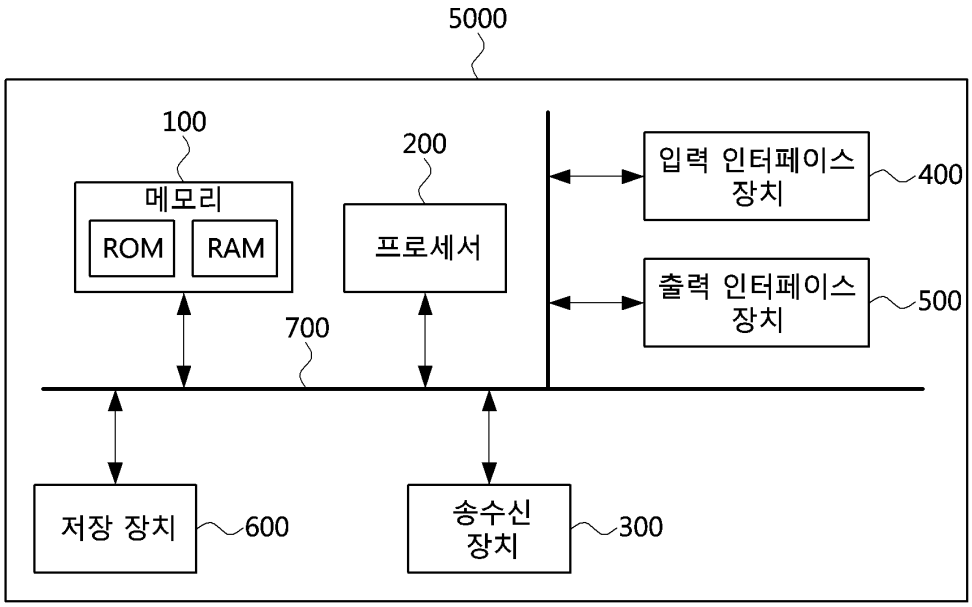
도면3


5000
5100
5300
5500
5700
발행부
전송부
수정부
알림부
블록체인 네트워크
B

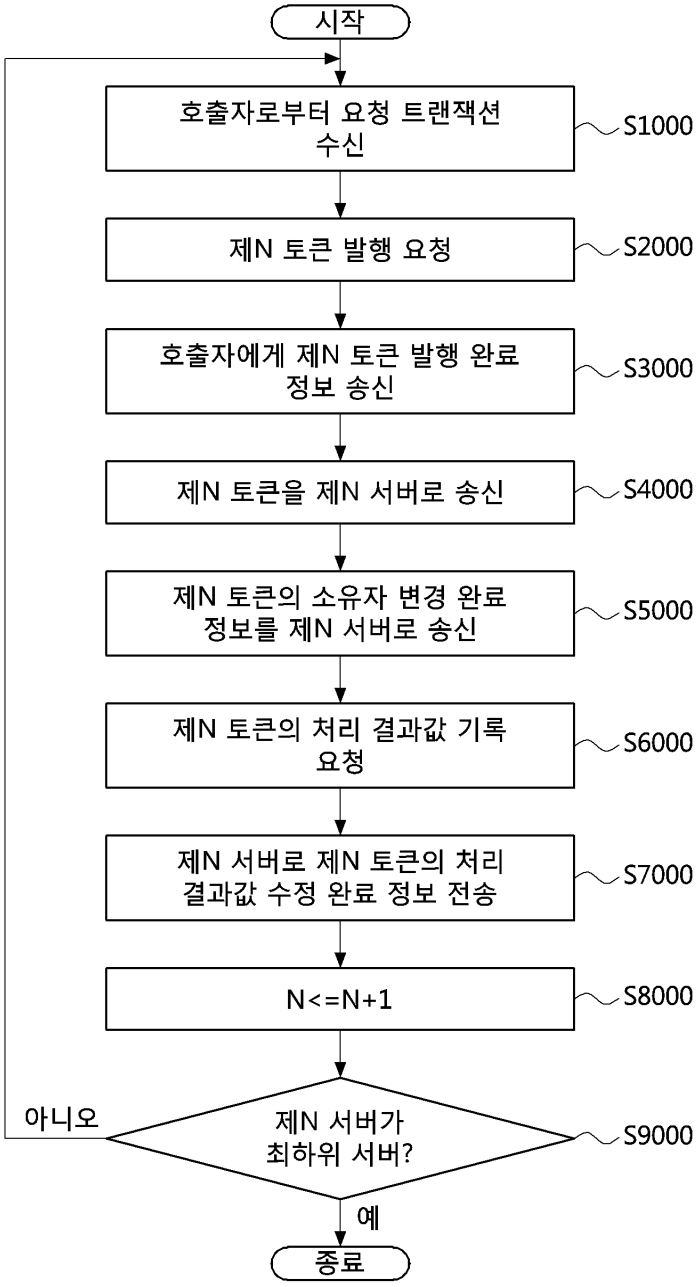
도면4

대체 불가능 토큰	
표준 속성	확장 속성
토큰 ID 토큰 타입 소유자 피승인자	온체인 확장 속성 - 호출 트랜잭션 정보 - 처리 결과 - 부모 - 자식 오프체인 확장 속성 - 경로 - 해시

도면5



도면6


시작
호출자로부터 요청 트랜잭션 수신
S1000
제N 토큰 발행 요청
S2000
호출자에게 제N 토큰 발행 완료 정보 송신
S3000
제N 토큰을 제N 서버로 송신
S4000
제N 토큰의 소유자 변경 완료 정보를 제N 서버로 송신
S5000
제N 토큰의 처리 결과값 기록 요청
S6000
제N 서버로 제N 토큰의 처리 결과값 수정 완료 정보 전송
S7000
N<=N+1
S8000
제N 서버가 최하위 서버?
S9000
아니오
예
종료

도면7