



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0063055
(43) 공개일자 2021년06월01일

(51) 국제특허분류(Int. Cl.)
G06F 21/53 (2013.01) G06F 21/60 (2013.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
G06F 21/53 (2013.01)
G06F 21/60 (2013.01)
(21) 출원번호 10-2019-0151504
(22) 출원일자 2019년11월22일
심사청구일자 없음

(71) 출원인
서강대학교산학협력단
서울특별시 마포구 백범로 35 (신수동, 서강대학교)
(72) 발명자
박성용
서울특별시 서대문구 가재울미래로 2 DMC파크뷰자
이 107동 1001호
송제호
서울특별시 마포구 백범로 17 20
(74) 대리인
이지연

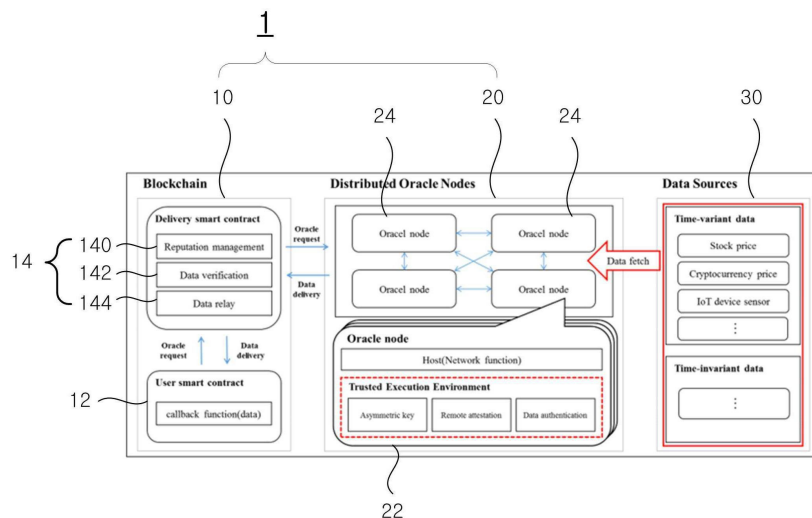
전체 청구항 수 : 총 11 항

(54) 발명의 명칭 신뢰 실행 환경을 이용한 분산 블록체인 오라클 시스템 및 상기 시스템에서의 외부 데이터 전달 방법

(57) 요약

본 발명은 TEE를 이용한 분산 블록체인 오라클 시스템에 관한 것이다. 상기 분산 블록체인 오라클 시스템은, 사용자 스마트 컨트랙트 및 전달 스마트 컨트랙트가 기록된 블록체인; 및 TEE를 기반으로 동작되는 복수 개의 오라클 노드들로 구성되며, 상기 블록체인 네트워크로부터 외부 데이터 요청이 발생하면, 외부 데이터 소스로부터 데이터를 수집하여 상기 블록체인 네트워크로 제공하는 분산 오라클;을 구비한다. 상기 전달 스마트 컨트랙트는 평판을 기준으로 하여 분산 오라클 중 오라클 리더를 설정하고, 오라클 리더에게 외부 데이터를 요청하며, 상기 오라클 리더는 외부 데이터를 수집하여 TEE 기반의 비밀키로 암호화하여 상기 전달 스마트 컨트랙트에게 전달한다. 따라서, 본 발명은 TEE 기반으로 운영되는 분산 오라클을 통해, 데이터 출처로부터 데이터의 무결성을 보장하고, 편향을 최소화하는 방법으로 외부 데이터를 수집하여 블록체인 네트워크에 제공할 수 있게 된다.

대표도



(52) CPC특허분류

H04L 63/123 (2013.01)
H04L 67/1057 (2013.01)
H04L 9/0825 (2013.01)
H04L 9/085 (2013.01)
G06F 2221/2149 (2013.01)
H04L 2209/38 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711093140
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보통신기술인력양성(R&D)
연구과제명	적응형 블록체인 플랫폼 기술 개발 및 전문 인력 양성
기 여 율	1/1
과제수행기관명	서강대학교산학협력단
연구기간	2019.01.01 ~ 2019.12.31

명세서

청구범위

청구항 1

사용자 스마트 컨트랙트 및 전달 스마트 컨트랙트가 기록된 블록체인을 구비하는 노드들을 포함하는 블록체인 네트워크;

신뢰 실행 환경(Trusted Execution Environment; TEE)을 기반으로 동작되는 복수 개의 오라클 노드들로 구성되며, 상기 블록체인 네트워크로부터 외부 데이터 요청이 발생하면, 외부 데이터 소스로부터 데이터를 수집하여 상기 블록체인 네트워크로 제공하는 분산 오라클;

을 구비하고, 상기 사용자 스마트 컨트랙트는 상기 전달 스마트 컨트랙트에게 외부 데이터를 요청하고, 상기 전달 스마트 컨트랙트로부터 무결성을 갖는 외부 데이터를 전달받는 것을 특징으로 하며,

상기 전달 스마트 컨트랙트는 상기 사용자 스마트 컨트랙트로부터 외부 데이터의 요청이 입력되면, 상기 분산 오라클에게 외부 데이터를 요청하고, 상기 분산 오라클로부터 상기 외부 데이터가 제공되면 외부 데이터를 검증하여 상기 사용자 스마트 컨트랙트에게 전달하는 것을 특징으로 하는 TEE를 이용한 분산 블록체인 오라클 시스템.

청구항 2

제1항에 있어서, 상기 전달 스마트 컨트랙트는,

분산 오라클을 구성하는 오라클 노드들에 대한 평판을 관리하고, 사용자 스마트 컨트랙트로부터 외부 데이터 요청이 발생하면 평판을 기준으로 하여 분산 오라클 중 오라클 리더를 선출하는 리더 선출 모듈;

분산 오라클로부터 외부 데이터가 수신되면, 외부 데이터를 검증하는 데이터 검증 모듈;

분산 오라클로부터 수신된 외부 데이터가 상기 데이터 검증 모듈에 의해 데이터 검증되면, 상기 검증된 외부 데이터를 상기 사용자 스마트 컨트랙트에게 전달하는 데이터 전달 모듈;

을 구비하는 것을 특징으로 하는 TEE를 이용한 분산 블록체인 오라클 시스템.

청구항 3

제2항에 있어서, 상기 오라클 노드에 대한 평판은 응답 시간이 빠르고 취합한 다른 오라클 노드의 비율이 높을수록 높은 값을 갖도록 설계된 것을 특징으로 하는 TEE를 이용한 분산 블록체인 오라클 시스템.

청구항 4

제2항에 있어서, 상기 리더 선출 모듈은 아래의 수학식에 따라 각 오라클에 대한 평판을 측정하고,

$$Reputation\ of\ node_i = \frac{C}{Longest\ response\ time} \times \frac{Number\ of\ gathered\ response}{Number\ of\ total\ nodes}$$

여기서, *Longest response time* 는 가장 느린 응답 시간이며, *Number of gathered response* 는 수집된 응답 개수이며, *Number of total nodes* 는 분산 오라클을 구성하는 오라클 노드들의 개수이며, *C* 는 상수값인 것을 특징으로 하는 TEE를 이용한 분산 블록체인 오라클 시스템.

청구항 5

제2항에 있어서, 상기 TEE의 공개키는 상기 전달 스마트 컨트랙트와 분산 오라클의 오라클 노드들이 공유하고, 상기 전달 스마트 컨트랙트의 데이터 검증 모듈은,

상기 분산 오라클로부터 암호화된 메시지를 제공받고, 상기 공개키를 이용하여 암호화된 메시지를 복호화하고, 복호화된 메시지가 원본 데이터와 일치하면, 해당 데이터를 사용자 스마트 컨트랙트에게 전달하는 것을 특징으로 하는 TEE를 이용한 분산 블록체인 오라클 시스템.

청구항 6

제1항에 있어서, 상기 분산 오라클 중 오라클 리더는,

다른 오라클 노드에게 외부 데이터 요청을 보내고, 다른 오라클 노드로부터 전달받은 외부 데이터와 해당 오라클 노드의 응답 시간을 기록하며,

사전 설정된 개수 이상의 응답을 받거나 응답 시간을 초과하면,

상기 오라클 리더는

기록된 외부 데이터와 응답 시간의 원본, 상기 원본에 대하여 TEE 내부에서 만들어진 비밀키로 암호화된 내용을 포함한 메시지를 생성하여 상기 전달 스마트 컨트랙트로 전송하는 것을 특징으로 하는 TEE를 이용한 분산 블록체인 오라클 시스템.

청구항 7

제6항에 있어서, 상기 TEE의 공개키는 상기 전달 스마트 컨트랙트와 분산 오라클의 오라클 노드들이 공유하고,

상기 전달 스마트 컨트랙트는,

상기 분산 오라클로부터 메시지를 제공받고, 상기 공개키를 이용하여 상기 메시지 중 암호화된 내용을 복호화하고, 복호화된 내용과 원본 데이터가 일치하면, 해당 데이터를 사용자 스마트 컨트랙트에게 전달하는 것을 특징으로 하는 TEE를 이용한 분산 블록체인 오라클 시스템.

청구항 8

제1항에 있어서, 상기 분산 오라클의 오라클 노드들은,

TEE 내부의 비대칭키 모듈을 구비하고,

상기 비대칭키 모듈은 TEE 내부에서 생성된 비밀키와 공개키의 쌍을 구비하고, 상기 공개키는 전달 스마트 컨트랙트와 다른 오라클 노드들과 공유하고, 상기 비밀키는 TEE 내부에서만 암호화하는 용도로 사용되는 것을 특징으로 하는 TEE를 이용한 분산 블록체인 오라클 시스템.

청구항 9

사용자 스마트 컨트랙트와 전달 스마트 컨트랙트가 기록된 블록체인을 구비하는 블록체인 네트워크와 신뢰 실행 환경(TEE)을 기반으로 한 복수 개의 오라클 노드들로 이루어진 분산 오라클을 구비하는 분산 블록체인 오라클 시스템에서의 오라클 노드에 의해 수행되는 외부 데이터 전달 방법에 있어서,

(a) 상기 전달 스마트 컨트랙트에 의해 분산 오라클의 복수 개의 오라클 노드들 중 오라클 리더가 선출되는 단계;

(b) 상기 오라클 리더는 다른 오라클 노드에게 외부 데이터를 요청하고, 상기 요청에 따라 외부 데이터를 전달 받으면, 전달받은 외부 데이터와 응답 시간을 기록하는 단계;

(c) 상기 오라클 리더는 상기 기록된 외부 데이터와 응답 시간을 이용하여 암호화하여 생성된 메시지를 상기 전달 스마트 컨트랙트에게 전달하는 단계;

(d) 상기 전달 스마트 컨트랙트는 상기 오라클 리더로부터 수신한 메시지를 복호화하는 단계;

를 구비하는 것을 특징으로 하는 TEE를 이용한 분산 블록체인 오라클 시스템에서의 외부 데이터 전달 방법.

청구항 10

제9항에 있어서, 상기 외부 데이터 전달 방법은,

상기 오라클 노드들이 TEE 내부에서 비밀키와 공개키 쌍을 생성하고, 상기 공개키는 전달 스마트 컨트랙트와 다

른 오라클 노드들에게 공유하는 단계; 를 더 구비하는 것을 특징으로 하는 TEE를 이용한 분산 블록체인 오라클 시스템에서의 외부 데이터 전달 방법.

청구항 11

제9항에 있어서, 상기 (c) 단계는

상기 오라클 리더는 상기 기록된 외부 데이터와 응답 시간의 원본, 및 TEE 내부의 비밀키를 이용하여 상기 원본을 암호화한 내용을 포함한 메시지를 생성하고, 상기 메시지를 전달 스마트 컨트랙트에게 제공하는 것을 특징으로 하며,

상기 (d) 단계는,

상기 전달 스마트 컨트랙트가 상기 오라클 리더로부터 수신한 메시지 중 암호화한 내용을 공개키로 복호화하고, 복호화된 내용과 원본 데이터를 비교하여 일치하면 상기 외부 데이터를 사용자 스마트 컨트랙트에게 전달하는 것을 특징으로 하는 TEE를 이용한 분산 블록체인 오라클 시스템에서의 외부 데이터 전달 방법.

발명의 설명

기술 분야

[0001] 본 발명은 블록체인 오라클 시스템에 관한 것으로서, 더욱 구체적으로는 각 오라클 노드들을 신뢰 실행 환경을 기반으로 운영하여 외부 데이터를 무결성을 보장하고 편향을 최소화시켜 외부 데이터를 수집하여 블록체인 스마트 컨트랙트에게 제공하도록 구성된 신뢰 실행 환경을 이용한 분산 블록체인 오라클 시스템 및 상기 시스템에서의 외부 데이터 전달 방법에 관한 것이다.

배경 기술

[0002] 블록체인은 비트코인에서 처음으로 등장한 기술로써, 제3자의 개입 없이도 무결성 및 신뢰성을 확보하는 동등 계층간 통신망(Peer-to-Peer Network, P2P) 기반 분산원장 기술이다. 블록체인은 네트워크에서 발생한 입력과 출력, 즉 트랜잭션(Transaction)들을 블록체인 네트워크의 모든 참여자가 저장하고, 저장한 트랜잭션 내용을 바탕으로, 발생한 트랜잭션의 실행(혹은 결과)에 대한 유효성을 검증함으로써 트랜잭션의 무결성(Integrity)을 보장하는 장점을 가진다. 이때 트랜잭션은 다수의 트랜잭션 묶음인 블록(Block)이라는 단위로 합의(Consensus) 과정을 거친다. 합의는 모든 참여자가 동일한 트랜잭션의 실행 결과를 공유하기 위해 어떤 블록(혹은 결과)으로 통일할지 채택하는 과정이다.

[0003] 스마트 컨트랙트(Smart contract)는 블록체인 네트워크에서 실행되는 응용 프로그램의 실행 코드다. 트랜잭션을 통해 실행을 요청할 수 있으며, 마찬가지로 네트워크의 모든 참여자 입력과 출력을 저장하고, 실행하는 특징을 갖고 있다. 또한, 코드의 내용이 블록에 저장되어 모든 블록체인 참여자에게 공유되어 있고, 모든 구성원의 실행과 검증을 통해 실행 결과가 블록에 저장되므로 응용 프로그램의 투명하고 무결한 실행이 가능하다.

[0004] 한편, 블록체인의 스마트 컨트랙트는 일반 응용 프로그램과 달리 특수한 한계점이 존재한다. 모든 참여자가 트랜잭션의 실행과 검증에 참여하는 블록체인의 특징상, 어떤 참여자의 환경에서 실행해도 같은 입력에 같은 결과가 나오는 결정성(Deterministic)이 보장되어야 하나의 실행 결과로 합의가 가능하다. 실행 결과의 결정성을 위해 스마트 컨트랙트는 네트워크를 통해 외부 데이터에 접근이 불가능하고, 오직 원장(혹은 블록)에 저장된 데이터만 접근이 가능하다. 블록체인 외부 데이터(이하 외부 데이터)에 접근이 불가능한 한계점을 오라클 문제(Oracle problem)라고 하고, 이런 한계점을 극복하기 위해 외부 데이터를 블록체인에 제공하는 데이터 중개자를 오라클(Oracle)이라고 한다. 오라클은 데이터 중개자로서, 외부 출처로부터 받은 외부 데이터에 변조가 없다는 무결성(Integrity)을 증명해야 한다.

[0005] 신뢰 실행 환경(Trusted Execution Environment; 이하 'TEE' 라 한다)는 안전성을 높이기 위하여 프로세서, 주변 장치 및 저장 장치를 대상으로 보안 서비스를 제공하는 소프트웨어 플랫폼을 말한다. TEE는 일반적으로 보안 영역과 비보안 영역의 분리를 지원하는 하드웨어 기능과 이를 이용하여 보안 서비스를 제공하는 소프트웨어로 구성된다. 따라서, TEE는 특정 프로세서만 접근이 가능한 영역으로, 운영체제와 하이퍼바이저를 비롯한 소프트웨어의 비인가된 접근을 하드웨어 단계에서 막는다. 즉, TEE는 악성 소프트웨어 감염 위험이 있는 소프트웨어의 접근을 차단함으로써 프로세스 실행의 기밀성(Confidentiality)과 무결성을 보장한다. 또한, 특정 프로세스를 TEE에서 실행했음을 증명하는 기능을 제공하여, 원격의 사용자 간에 지정된 프로세스를 조작없이 실행할 수 있

는 환경을 제공한다. 위의 특징을 활용하여 보안성과 무결성을 요구하는 여러 응용들이 TEE를 활용하여 개발되고 있다.

선행기술문헌

특허문헌

- [0006] (특허문헌 0001) 한국등록특허공보 제 10-2023101호
(특허문헌 0002) 한국공개특허공보 제 10-2018-0069856호
(특허문헌 0003) 미국공개특허공보 US 2019/0095879

발명의 내용

해결하려는 과제

- [0007] 전술한 문제점을 해결하기 위한 본 발명의 목적은, 단일 장애점 (Single-point-of-failure) 문제를 보완하면서 데이터 무결성을 보장하며 블록체인 네트워크에 외부 데이터를 제공하기 위하여 신뢰 실행 환경(TEE)을 이용하여 데이터의 무결성을 증명하고 데이터를 출처로부터 블록체인 네트워크까지 전달할 수 있도록 하는 분산 블록체인 오라클 시스템을 제공하는 것이다.
- [0008] 본 발명의 다른 목적은 TEE를 기반으로 한 분산 블록체인 오라클 시스템에서 데이터의 무결성을 보장하면서 데이터를 출처로부터 블록체인 네트워크까지 전달할 수 있도록 하는 데이터 전달 방법을 제공하는 것이다.

과제의 해결 수단

- [0009] 전술한 기술적 과제를 달성하기 위한 본 발명의 제1 특징에 따른 TEE를 이용한 분산 블록체인 오라클 시스템은, 사용자 스마트 컨트랙트 및 전달 스마트 컨트랙트가 기록된 블록체인을 구비하는 노드들을 포함하는 블록체인 네트워크; 신뢰 실행 환경(Trusted Execution Environment; TEE)을 기반으로 동작되는 복수 개의 오라클 노드들로 구성되며, 상기 블록체인 네트워크로부터 외부 데이터 요청이 발생하면, 외부 데이터 소스로부터 데이터를 수집하여 상기 블록체인 네트워크로 제공하는 분산 오라클;을 구비하고,
- [0010] 상기 사용자 스마트 컨트랙트는 상기 전달 스마트 컨트랙트에게 외부 데이터를 요청하고, 상기 전달 스마트 컨트랙트로부터 무결성을 갖는 외부 데이터를 전달받는 것을 특징으로 하며,
- [0011] 상기 전달 스마트 컨트랙트는 상기 사용자 스마트 컨트랙트로부터 외부 데이터의 요청이 입력되면, 상기 분산 오라클에게 외부 데이터를 요청하고, 상기 분산 오라클로부터 상기 외부 데이터가 제공되면 외부 데이터를 검증하여 상기 사용자 스마트 컨트랙트에게 전달하는 것을 특징으로 한다.
- [0012] 전술한 제1 특징에 따른 TEE를 이용한 분산 블록체인 오라클 시스템에 있어서, 상기 전달 스마트 컨트랙트는, 분산 오라클을 구성하는 오라클 노드들에 대한 평판을 관리하고, 사용자 스마트 컨트랙트로부터 외부 데이터 요청이 발생하면 평판을 기준으로 하여 분산 오라클 중 오라클 리더를 선출하는 리더 선출 모듈; 분산 오라클로부터 외부 데이터가 수신되면, 외부 데이터를 검증하는 데이터 검증 모듈; 분산 오라클로부터 수신된 외부 데이터가 상기 데이터 검증 모듈에 의해 데이터 검증되면, 상기 검증된 외부 데이터를 상기 사용자 스마트 컨트랙트에게 전달하는 데이터 전달 모듈;을 구비한다.
- [0013] 전술한 제1 특징에 따른 TEE를 이용한 분산 블록체인 오라클 시스템에 있어서, 상기 오라클 노드에 대한 평판은 응답 시간이 빠르고 취약한 다른 오라클 노드의 비율이 높을수록 높은 값을 갖도록 설계된 것이 바람직하다.
- [0014] 전술한 제1 특징에 따른 TEE를 이용한 분산 블록체인 오라클 시스템에 있어서, 상기 TEE 의 공개키는 상기 전달 스마트 컨트랙트와 분산 오라클의 오라클 노드들이 공유하고, 상기 전달 스마트 컨트랙트의 데이터 검증 모듈은, 상기 분산 오라클로부터 원본 데이터와 암호화된 내용을 포함하는 메시지를 제공받고, 상기 공개키를 이용하여 암호화된 내용을 복호화하고, 복호화된 메시지가 원본 데이터와 일치하면, 해당 데이터를 사용자 스마트 컨트랙트에게 전달하는 것이 바람직하다.
- [0015] 전술한 제1 특징에 따른 TEE를 이용한 분산 블록체인 오라클 시스템에 있어서, 상기 분산 오라클 중 오라클 리

더는, 다른 오라클 노드에게 외부 데이터를 요청하고, 다른 오라클 노드로부터 전달받은 외부 데이터와 해당 오라클 노드의 응답 시간을 기록하며, 사전 설정된 개수 이상의 응답을 받거나 응답 시간을 초과하면, 기록된 외부 데이터와 응답 시간의 원본, 상기 원본에 대하여 TEE 내부에서 만들어진 비밀키로 암호화된 내용을 포함한 메시지를 생성하여 상기 전달 스마트 컨트랙트로 전송하는 것이 바람직하다.

[0016] 전술한 제1 특징에 따른 TEE를 이용한 분산 블록체인 오라클 시스템에 있어서, 상기 TEE의 공개키는 상기 전달 스마트 컨트랙트와 분산 오라클의 오라클 노드들이 공유하고, 상기 전달 스마트 컨트랙트는, 상기 분산 오라클로부터 메시지를 제공받고, 상기 공개키를 이용하여 상기 메시지 중 암호화된 내용을 복호화하고, 복호화된 내용과 원본 데이터가 일치하면, 해당 데이터를 사용자 스마트 컨트랙트에게 전달하는 것이 바람직하다.

[0017] 본 발명의 제2 특징에 따른 외부 데이터 전달 방법은, 사용자 스마트 컨트랙트와 전달 스마트 컨트랙트가 기록된 블록체인을 구비하는 블록체인 네트워크와 신뢰 실행 환경(TEE)을 기반으로 한 복수 개의 오라클 노드들로 이루어진 분산 오라클을 구비하는 분산 블록체인 오라클 시스템에서의 오라클 노드에 의해 수행되는 외부 데이터 전달 방법에 있어서, (a) 상기 오라클 노드들이 TEE 내부에서 비밀키와 공개키 쌍을 생성하고, 상기 공개키는 전달 스마트 컨트랙트와 다른 오라클 노드들에게 공유하는 단계; (b) 상기 전달 스마트 컨트랙트에 의해 분산 오라클의 복수 개의 오라클 노드들 중 오라클 리더가 선출되는 단계; (c) 상기 오라클 리더는 다른 오라클 노드에게 외부 데이터를 요청하고, 상기 요청에 따라 외부 데이터를 전달받으면, 전달받은 외부 데이터와 응답 시간을 기록하는 단계; (d) 상기 오라클 리더는 상기 기록된 외부 데이터와 응답 시간의 원본 데이터 및 이를 암호화한 내용을 포함하여 생성된 메시지를 상기 전달 스마트 컨트랙트에게 전달하는 단계; (e) 상기 전달 스마트 컨트랙트는 상기 오라클 리더로부터 수신한 메시지 중 암호화된 내용을 복호화하고 원본 데이터를 검증하는 단계;를 구비한다.

[0018] 전술한 제2 특징에 따른 외부 데이터 전달 방법에 있어서, 상기 (d) 단계는 상기 오라클 리더는 상기 기록된 외부 데이터와 응답 시간의 원본, 및 TEE 내부의 비밀키를 이용하여 상기 원본을 암호화한 내용을 포함한 메시지를 생성하고, 상기 메시지를 전달 스마트 컨트랙트에게 제공하는 것을 특징으로 하며,

[0019] 상기 (e) 단계는, 상기 전달 스마트 컨트랙트가 상기 오라클 리더로부터 수신한 메시지 중 암호화한 내용을 공개키로 복호화하고, 복호화된 내용과 원본 데이터를 비교하여 일치하면 상기 외부 데이터를 사용자 스마트 컨트랙트에게 전달하는 것이 바람직하다.

발명의 효과

[0020] 본 발명에 따른 분산 블록체인 오라클 시스템은, 신뢰 실행 환경(TEE)을 이용함으로써, 조작하지 않은 원본의 외부 데이터를 수집하여 블록체인 네트워크에 제공할 수 있게 된다. 따라서, 본 발명에 따른 시스템은, 외부 데이터에 대한 무결성을 증명하고 외부 데이터를 소스로부터 블록체인 네트워크까지 전달할 수 있게 된다.

[0021] 또한, 본 발명에 따른 분산 블록체인 오라클 시스템은, 분산 오라클 네트워크를 구성하여 단일 장애점 문제와 편향된 데이터 제공의 문제를 해결할 수 있다. 편향된 데이터 제공은 오라클이 데이터 출처로부터 조작없이 데이터를 제공하되, 오라클이 원하는 데이터만 선택적으로 제공하는 악의적인 행위를 말한다. 본 발명은 각 오라클 노드에 대한 평판을 기준으로 하여 오라클 노드들을 평가하고 이에 따라 오라클 리더 노드를 선택함으로써, 선택적으로 데이터를 제공하는 노드를 배제하고, 빠르고 편향없이 데이터를 제공하는 노드를 장려하여 데이터에 편향이 반영되는 것을 막을 수 있다.

[0022] 또한, 본 발명에 따른 시스템은 복수의 오라클 노드들이 존재하는 분산 오라클을 구성함으로써, 단일 장애점(Single-point-of-failure)문제와 같은 단일 노드 오라클의 문제점을 해결할 수 있게 된다.

도면의 간단한 설명

[0023] 도 1은 본 발명의 바람직한 실시예에 따른 분산 블록체인 오라클 시스템을 전체적으로 도시한 구성도이다.

도 2는 본 발명의 바람직한 실시예에 따른 분산 블록체인 오라클 시스템에 있어서, 분산 오라클을 도시한 구성도이다.

도 3은 본 발명의 바람직한 실시예에 따른 분산 블록체인 오라클 시스템에 있어서, 외부 데이터 전달 방법을 순차적으로 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0024] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다. 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.
- [0025] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예에 따른 TEE를 이용한 분산 블록체인 오라클 시스템 및 상기 분산 블록체인 오라클 시스템에서의 데이터 전달 방법을 구체적으로 설명한다.
- [0026] 먼저, 외부 소프트웨어로부터 고립된 환경에서 안전한 실행이 가능한 TEE는 여러 형태로 구현되어 각각 용어가 상이하다. 본 발명에서는 Intel Software Guard Extensions(SGX)를 기준으로 용어를 기술한다. 또한, 스마트 컨트랙트의 설명은 스마트 컨트랙트를 지원하는 블록체인 플랫폼 중 하나인 이더리움(Ethereum)의 스마트 컨트랙트를 기준으로 기술한다.
- [0027] Enclave는 악의적인 개체로부터 응용 프로그램을 보호할 수 있는 독립적이고 안정성이 보장된 메모리 영역을 의미한다. Remote attestation은 Intel SGX의 고급 기능으로, Enclave가 안전한 환경에서 설정되었음을 원격 사용자에게 증명하는 프로세스다. Remote attestation을 통해 프로세스가 Enclave 내부에서 실행되었음과, 프로세스의 신원(Identity), 그리고 데이터와 코드의 무결성을 증명할 수 있다.
- [0028] 이더리움의 스마트 컨트랙트는 고유의 주소를 갖는 응용 프로그램이며, 실행하고자 하는 스마트 컨트랙트의 주소, 함수, 그리고 인자(Argument)를 지정한 트랜잭션을 생성함으로써 실행시킬 수 있다. 소스코드와 응용 프로그램의 데이터는 원장(혹은 블록)에 저장되어 있으며, 데이터들은 오로지 트랜잭션을 통해 값을 변화시킬 수 있다.
- [0029] 도 1은 본 발명의 바람직한 실시예에 따른 분산 블록체인 오라클 시스템을 전체적으로 도시한 구성도이다. 도 1을 참조하면, 본 발명에 따른 분산 블록체인 오라클 시스템(1)은 블록체인(10)을 기록한 노드들을 구비한 블록체인 네트워크 및 신뢰 실행 환경(Trusted Execution Environment; 'TEE')을 기반으로 한 복수 개의 오라클 노드들(24)로 이루어진 분산 오라클(20)을 구비하여, 상기 분산 오라클은 외부 데이터 소스(30)들로부터 외부 데이터를 수집하여 무결성의 외부 데이터를 블록체인 네트워크로 전달하는 것을 특징으로 한다.
- [0030] 상기 블록체인(10)은 사용자 스마트 컨트랙트(12; User smart contract)와 전달 스마트 컨트랙트(14; Delivery smart contract)를 구비한다.
- [0031] 상기 사용자 스마트 컨트랙트(12)는 블록체인 네트워크의 노드들로부터 외부 데이터의 요청을 받고, 이러한 요청에 응답하여 상기 전달 스마트 컨트랙트에게 외부 데이터를 요청하고, 상기 전달 스마트 컨트랙트로부터 무결성의 외부 데이터를 최종적으로 전달받는 스마트 컨트랙트로서, 외부 데이터의 중착지를 의미한다.
- [0032] 상기 전달 스마트 컨트랙트(14)는 오라클로부터 받은 데이터의 검증, 평판(Reputation) 관리 및 리더 선출, 그리고 데이터 전달의 역할을 하는 중개자 스마트 컨트랙트이다. 상기 전달 스마트 컨트랙트(14)는 리더 선출 모듈(140), 데이터 검증 모듈(142) 및 데이터 전달 모듈(144)을 구비한다.
- [0033] 상기 리더 선출 모듈(140)은 분산 오라클을 구성하는 오라클 노드들에 대한 평판을 관리하고, 사용자 스마트 컨트랙트로부터 외부 데이터 요청이 발생하면 평판을 기준으로 하여 분산 오라클 중 오라클 리더를 선출한다.
- [0034] 상기 오라클 노드에 대한 평판(Reputation)은 응답 시간이 빠르고 취합한 다른 오라클 노드의 비율이 높을수록 높은 값을 갖도록 설계된 것으로서, 수학식 1에 따라 계산될 수 있다.

수학식 1

$$Reputation\ of\ node_i = \frac{C}{Longest\ response\ time} \times \frac{Number\ of\ gathered\ response}{Number\ of\ total\ nodes}$$

[0035]

[0036] 여기서, *Longest response time* 는 가장 느린 응답 시간이며, *Number of gathered response* 는 수집된

응답 개수이며, *Number of total nodes* 는 분산 오라클을 구성하는 오라클 노드들의 개수이며, C 는 상수값이다.

- [0037] 상기 리더 선출 모듈은 사용자 스마트 컨트랙트로부터 외부 데이터의 요청이 발생하면 상기 측정된 평판들을 기준으로 하여 임의로 오라클 리더를 선출하고, 상기 리더로 선출된 노드는 해당 외부 데이터 요청에 대한 응답의 책임을 갖게 된다. 상기 평판은 해당 노드의 과거 응답을 기준으로 수학적 식에 따라 계산되며, 응답하는데 사전 설정된 일정 시간을 초과한 노드는 오프라인 상태로 간주하고 리더 후보에서 제외한다.
- [0038] 상기 데이터 검증 모듈(142)은 분산 오라클로부터 외부 데이터가 수신되면, 외부 데이터를 검증한다. 상기 데이터 검증 모듈은 분산 오라클의 오라클 노드들로부터 TEE 내부의 공개키를 제공받게 되며, 상기 오라클 노드로부터 외부 데이터를 암호화된 메시지의 형태로 전달받으면, 상기 공개키를 이용하여 상기 암호화된 메시지를 복호화하고 이로부터 무결성의 외부 데이터를 얻을 수 있게 된다.
- [0039] 상기 데이터 전달 모듈(144)은 분산 오라클로부터 수신된 외부 데이터가 상기 데이터 검증 모듈에 의해 데이터 검증되면, 상기 검증된 무결성의 외부 데이터를 상기 사용자 스마트 컨트랙트에게 전달한다.
- [0040] 상기 분산 오라클(20)은 신뢰 실행 환경(Trusted Execution Environment; TEE)(22)을 기반으로 동작되는 복수 개의 오라클 노드들(24)로 구성되며, 상기 블록체인 네트워크로부터 외부 데이터 요청이 발생하면, 외부 데이터 소스들(30)로부터 데이터를 수집하고 무결성을 갖는 데이터를 상기 블록체인 네트워크로 제공한다.
- [0041] 도 2는 본 발명의 바람직한 실시예에 따른 분산 블록체인 오라클 시스템에 있어서, 분산 오라클을 도시한 구성도이다. 도 2를 참조하면, 분산 오라클은 복수 개의 오라클 노드들이 존재하며, 서로 데이터를 주고받는다. 오라클 노드는 기밀성과 무결성이 보장되는 TEE 내부에서 수행되는 기능과 TEE 외부의 네트워크 기능으로 나뉜다. TEE 내부의 비대칭키(Asymmetric key)는 TEE 내부에서 생성한 비밀키와 공개키 쌍과 그에 관련된 모듈을 의미한다. 공개키는 전달 스마트 컨트랙트와 다른 오라클 노드에게 공유하고, 비밀키는 TEE 내부에서만 암호화하는 용도로 사용한다. TEE 내부의 데이터는 외부에서 읽거나 사용할 수 없기 때문에, TEE 내부에서 만든 비밀키로 암호화한 메시지는 TEE 환경에서 수행하였고, 지정된 프로세스를 수행하여 만든 메시지임을 증명할 수 있다. 본 발명에서는 위의 방법을 통해 오라클 간에 나누는 각종 메시지와 스마트 컨트랙트에 전달하는 데이터가 TEE의 검증을 거친 메시지 혹은 데이터임을 증명한다.
- [0042] 각 오라클 노드는 외부의 데이터 소스들(30)로부터 외부 데이터를 얻는다. 이 과정에서 가져오는 데이터의 무결성을 증명하기 위해, 오라클 노드는 데이터 소스와 SSL 연결을 위한 각종 암호키 교환과 X.509 인증서를 TEE 내부에서 생성하여 데이터 소스로부터 받은 데이터를 임의로 조작하지 못하는 SSL 채널을 구축하여 데이터를 수신한다.
- [0043] 이하, 도 3을 참조하여, 본 발명에 따른 분산 블록체인 오라클 시스템에서의 데이터 전달 방법을 구체적으로 설명한다.
- [0044] 도 3은 본 발명의 바람직한 실시예에 따른 분산 블록체인 오라클 시스템에 있어서, 데이터 전달 방법을 순차적으로 도시한 흐름도이다. 도 3을 참조하면, 먼저 상기 분산 블록체인 오라클 시스템의 오라클 노드들은 TEE 내부에서 비밀키와 공개키 쌍을 생성하고 상기 공개키는 전달 스마트 컨트랙트와 다른 오라클 노드들과 공유한다(단계 300). 다음, 사용자 스마트 컨트랙트로부터 외부 데이터 요청이 발생되면(단계 310), 전달 스마트 컨트랙트는 각 오라클 노드들에 대한 평판을 측정하고 이를 기반으로 하여 오라클 리더를 선출하고, 선출된 오라클 리더에게 외부 데이터를 요청한다(단계 320).
- [0045] 상기 오라클 리더는 다른 오라클 노드들에게 외부 데이터를 요청하고(단계 330), 이러한 요청에 따라 다른 오라클 노드들로부터 데이터를 전달받으면, 전달받은 데이터와 해당 노드의 응답 시간을 기록한다(단계 340). 사전 설정된 개수 이상의 응답을 받거나 사전 설정된 응답 시간을 초과하면, 상기 오라클 리더는 기록된 데이터와 응답시간의 원본, 및 TEE 내부에서 생성된 비밀키를 이용하여 상기 원본을 암호화한 내용을 포함하는 메시지를 생성하고(단계 360), 상기 생성된 메시지를 트랜잭션의 형태로 상기 전달 스마트 컨트랙트에 전달한다(단계 370).
- [0046] 상기 전달 스마트 컨트랙트는 상기 오라클 리더로부터 전달받은 메시지 등 암호화된 내용을 공개키로 복호화하고(단계 380), 복호화된 내용과 원본 데이터를 비교하여 서로 일치하면(단계 382) 사용자 스마트 컨트랙트에 전달하고(단계 390), 수학적 식을 기반으로 하여 오라클 리더에 대한 평판을 업데이트시킨다(단계 392).
- [0047] 이상에서 본 발명에 대하여 그 바람직한 실시예를 중심으로 설명하였으나, 이는 단지 예시일 뿐 본 발명을 한정

하는 것이 아니며, 본 발명이 속하는 분야의 통상의 지식을 가진 자라면 본 발명의 본질적인 특성을 벗어나지 않는 범위에서 이상에 예시되지 않은 여러 가지의 변형과 응용이 가능함을 알 수 있을 것이다. 그리고, 이러한 변형과 응용에 관계된 차이점들은 첨부된 청구 범위에서 규정하는 본 발명의 범위에 포함되는 것으로 해석되어야 할 것이다.

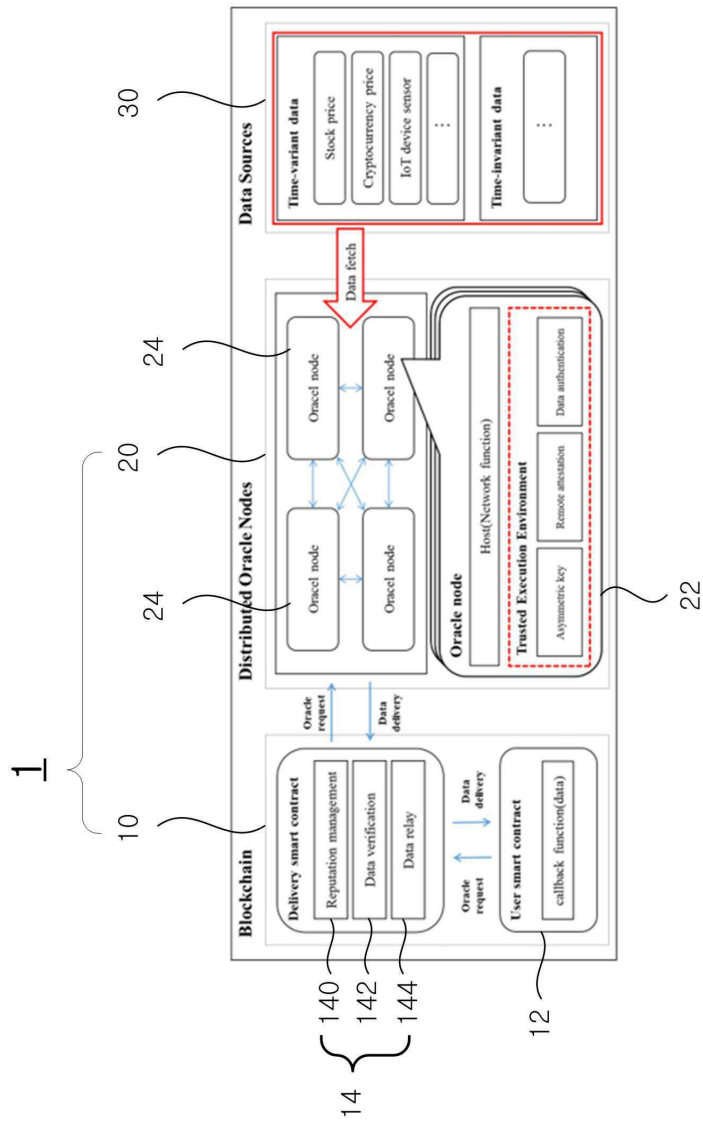
부호의 설명

- 1 : 분산 블록체인 오라클 시스템
- 10 : 블록체인
- 12 : 사용자 스마트 컨트랙트
- 14 : 전달 스마트 컨트랙트
- 20 : 분산 오라클
- 22 : 신뢰 실행 환경(TEE)
- 24 : 오라클 노드들
- 140 : 리더 선출 모듈
- 142 : 데이터 검증 모듈
- 144 : 데이터 전달 모듈

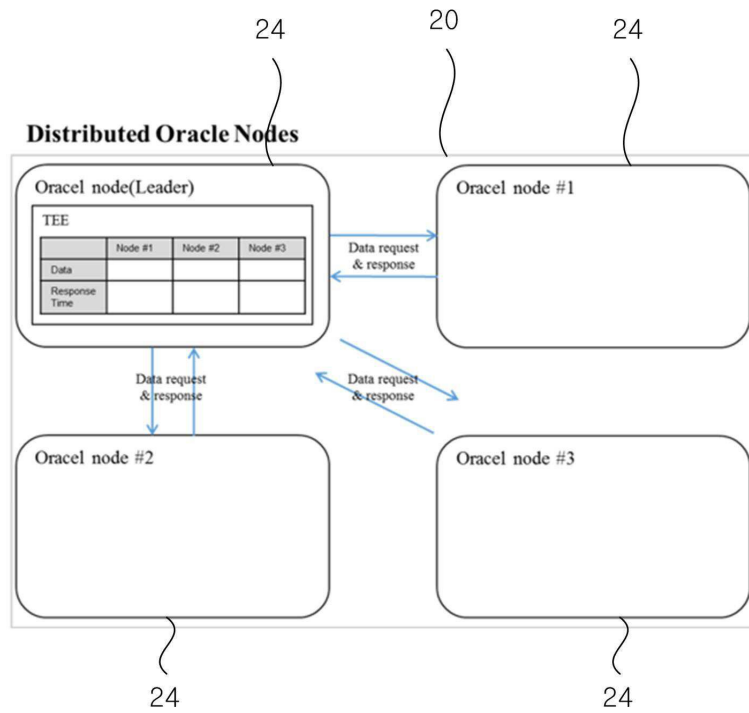
[0048]

도면

도면1



도면2



도면3

