



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0060356
(43) 공개일자 2021년05월26일

- | | |
|---|---|
| <p>(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01)</p> <p>(52) CPC특허분류
H04L 9/321 (2013.01)
H04L 9/3247 (2013.01)</p> <p>(21) 출원번호 10-2020-0154224</p> <p>(22) 출원일자 2020년11월18일
심사청구일자 2020년11월18일</p> <p>(30) 우선권주장
1020190147721 2019년11월18일 대한민국(KR)</p> | <p>(71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)</p> <p>(72) 발명자
류재철
대전광역시 유성구 어은로 57 한빛아파트 132-801</p> <p>박준후
대전광역시 유성구 유성대로720번길 6 아인스빌 411호
(뒷면에 계속)</p> <p>(74) 대리인
이은철, 김재문</p> |
|---|---|

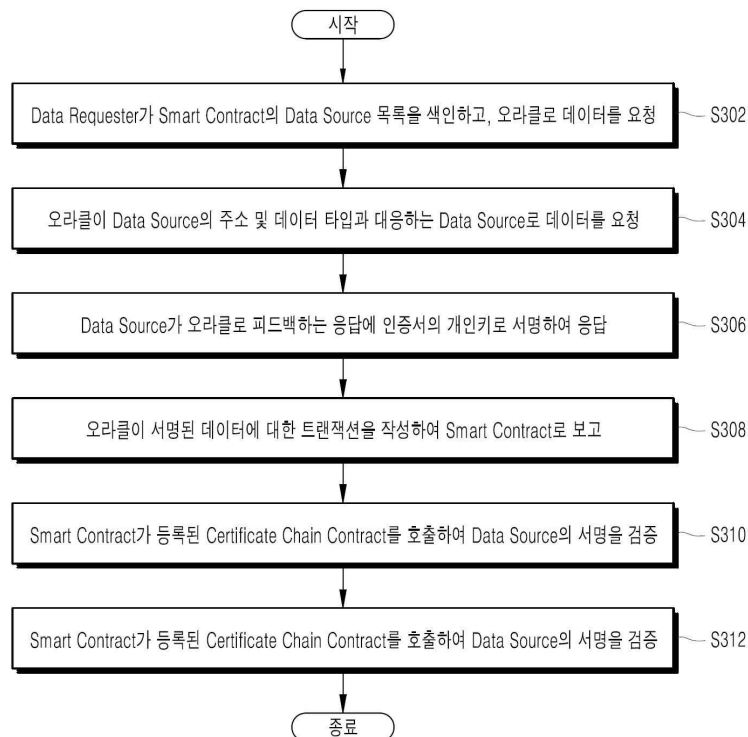
전체 청구항 수 : 총 4 항

(54) 발명의 명칭 공개키 인프라 구조를 이용한 스마트 컨트랙트의 인증된 데이터 피드 방법

(57) 요약

본 발명은 공개키 인프라 구조를 이용한 스마트 컨트랙트의 인증된 데이터 피드 방법에 관한 것으로서, 데이터 요청자(Data Requester)가 스마트 컨트랙트(Smart Contract)의 데이터 소스(Data Source) 목록을 색인하고, 오라클로 데이터를 요청하는 (a) 단계; 오라클이 스마트 컨트랙트(Smart Contract)를 색인하여 데이터 소스(Data Source)를 식별하고, 데이터 소스(Data Source)가 오라클로 피드백하는 응답에 인증서의 개인키로 서명하여 응답하는 (b) 단계; 오라클이 서명된 데이터에 대한 트랜잭션을 작성하여 스마트 컨트랙트로 보고하는 (c) 단계; 스마트 컨트랙트가 등록된 Certificate Chain Contract를 호출하여 데이터 소스의 서명을 검증하는 (d) 단계; 스마트 컨트랙트가 등록된 Certificate Chain Contract를 호출하여 데이터 소스의 서명을 검증하는 (e) 단계;를 포함한다.

대표도 - 도3



Source)의 주소 및 데이터 타입과 대응하는 데이터 소스(Data Source)로 데이터를 요청하는 (b) 단계; 데이터 소스(Data Source)가 오라클로 피드백하는 응답에 인증서를 서명하여 응답하는 (c) 단계; 오라클이 서명된 데이터에 대한 트랜잭션을 작성하여 스마트 컨트랙트로 보고하는 (d) 단계; 스마트 컨트랙트가 등록된 인증서 체인 컨트랙트(Certificate Chain Contract)를 호출하여 데이터 소스(Data Source)의 서명을 검증하는 (e) 단계; 및 스마트 컨트랙트가 서명이 검증된 경우, 검증 결과를 데이터 요청자(Data Requester)로 반환하는 (f) 단계를 포함한다.

(52) CPC특허분류

H04L 9/3265 (2013.01)

H04L 2209/38 (2013.01)

H04L 2209/56 (2013.01)

(72) 발명자

김근영

대전광역시 유성구 장대로 87 퍼스트캐슬 202호

김혁진

대전광역시 서구 대덕대로168번길 82 웰리움

이 발명을 지원한 국가연구개발사업

과제고유번호	1711102895
과제번호	2019-0-00108-002
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	블록체인융합기술개발(R&D)
연구과제명	블록체인 외부 정보 접근을 위한 스마트 컨트랙트 오라클 기술 개발
기 여 율	1/1
과제수행기관명	(주)아이오투러스트
연구기간	2019.04.01 ~ 2020.12.31

명세서

청구범위

청구항 1

- (a) 데이터 요청자(Data Requester)가 스마트 컨트랙트(Smart Contract)의 데이터 소스(Data Source) 목록을 색인하고, 오라클로 데이터를 요청하는 단계;
- (b) 오라클이 스마트 컨트랙트(Smart Contract)를 색인하여 데이터 소스(Data Source)의 주소 및 데이터 타입과 대응하는 데이터 소스(Data Source)로 데이터를 요청하는 단계;
- (c) 데이터 소스(Data Source)가 오라클로 피드백하는 응답에 인증서를 서명하여 응답하는 단계;
- (d) 오라클이 서명된 데이터에 대한 트랜잭션을 작성하여 스마트 컨트랙트로 보고하는 단계;
- (e) 스마트 컨트랙트가 등록된 인증서 체인 컨트랙트(Certificate Chain Contract)를 호출하여 데이터 소스(Data Source)의 서명을 검증하는 단계; 및
- (f) 스마트 컨트랙트가 서명이 검증된 경우, 검증 결과를 데이터 요청자(Data Requester)로 반환하는 단계를 포함하는 것을 특징으로 하는 공개키 인프라 구조를 이용한 스마트 컨트랙트의 인증된 데이터 피드 방법.

청구항 2

제1항에 있어서,

상기 (a) 단계 이전에,

- (g) 데이터 소스(Data Source)가 데이터 제공자로의 기능을 수행하기 위한 인증서 발급을 요청하는 단계;
- (h) PKI 서버가 기존의 Root CA로부터 하위 계층의 CA로 구성된 인증서 체인(Certificate Chain)에 데이터 소스(Data Source)의 인증서를 추가하여 서명된 인증서를 발급하는 단계;
- (i) 인증서 체인(Certificate Chain)이 업데이트를 위해 추가된 데이터 소스(Data Source)의 인증서를 등록하는 단계;
- (j) 데이터 소스(Data Source)가 발급된 인증서의 Chain과 블록체인에 기 저장된 인증서 체인 컨트랙트(Certificate Chain Contract)와 비교하여 발급 사실을 확인하는 단계; 및
- (k) 스마트 컨트랙트가 인증된 데이터 소스(Data Source) 목록에 발급된 인증서를 추가하여 관리하는 단계를 포함하는 것을 특징으로 하는 공개키 인프라 구조를 이용한 스마트 컨트랙트의 인증된 데이터 피드 방법.

청구항 3

제1항에 있어서,

상기 (c) 단계는,

데이터 소스(Data Source)가 개인키로 인증서를 서명하는 것을 특징으로 하는 것을 특징으로 하는 공개키 인프라 구조를 이용한 스마트 컨트랙트의 인증된 데이터 피드 방법.

청구항 4

제1항에 있어서,

상기 (e) 단계는,

스마트 컨트랙트가 공개키를 통해 데이터 소스(Data Source)의 서명을 검증하는 것을 특징으로 하는 공개키 인프라 구조를 이용한 스마트 컨트랙트의 인증된 데이터 피드 방법.

발명의 설명

기술 분야

- [0001] 본 발명은 공개키 인프라 구조를 이용한 스마트 컨트랙트의 인증된 데이터 피드 방법에 관한 것으로 더욱 상세하게는, TLS(Transport Layer Security) 프로토콜을 수정하지 않으면서 제3자에게 출처 인증을 검증시킴으로써, 오라클이 전달한 데이터가 위변조 되지 않았음을 증명하는 기술에 관한 것이다.

배경 기술

- [0002] 스마트 컨트랙트는 블록체인에서 동작하는 프로그램으로 다양한 분야에서 활용될 수 있다. 블록체인에서 구현되는 합의는 내부 시스템에서 검증되어야 하는 요소(예를 들어 계정의 잔액)에 대해서만 검증이 이루어지기 때문에 외부 세계(Off-chain)의 데이터에 대한 연결은 신뢰할 수 없다.
- [0003] 블록체인 외부에서 발생한 일련의 데이터를 내부로 전달해주는 역할을 오라클이라고 하며, 이 오라클은 외부 데이터에 대한 신뢰성이 확보되어야 한다. 신뢰성을 이루는 여러 가지 요소 중에 외부 데이터의 출처에 대한 인증이 포함된다.
- [0004] 오라클은 URL로 관리되는 외부 웹사이트와 HTTPS 통신으로 접근하여, JSON 또는 XML 타입으로 정의된 데이터를 파싱하여 요청된 부분만을 스마트 컨트랙트로 전달하는 역할을 수행한다. 하지만, 현재 인터넷을 구성하는 웹 프로토콜인 HTTPS를 지원하는 TLS 프로토콜은 제3자(스마트 컨트랙트)에 대한 증명을 위한 인증 기법을 제공하지 않는다.
- [0005] TLS는 handshake 과정에서 개인키를 통신 주체가 보유하고 있지만, HTTPS는 쌍방의 통신과정에서 기밀성을 유지하기 위한 목적으로 활용되고 있다. 따라서, 이를 해결하기 위한 방법으로 제안된 'TLS-N' 프로토콜은, 제3자에게 인증을 위해서는 TLS 프로토콜의 수정이 필요하다.
- [0006] 이에 본 출원인은 TLS 프로토콜을 수정하지 않으면서 제3자에게 출처 인증을 검증시킴으로써, 오라클이 전달한 데이터가 위변조 되지 않았음을 증명하는 방법을 제안한다. 또 이를 위해서 네트워크 스택에서 TLS 계층이 아닌 어플리케이션 계층의 공개키 인프라구조를 활용하였다.

선행기술문헌

특허문헌

- [0007] (특허문헌 0001) 한국공개특허 제10-2017-0041729호(2017.04.17)

발명의 내용

해결하려는 과제

- [0008] 본 발명의 목적은, 네트워크 스택에서 어플리케이션 계층의 공개키 인프라 구조를 활용하여 제3자에게 출처 인증을 검증시킴으로써, 별도의 하드웨어를 구성하지 않고, TLS 프로토콜을 수정하지 않으면서 오라클이 전달한 데이터가 위변조 되지 않았음을 증명하는데 있다.
- [0009] 본 발명의 목적들은 이상에서 언급한 목적으로 제한되지 않으며, 언급되지 않은 본 발명의 다른 목적 및 장점들은 하기의 설명에 의해서 이해될 수 있고 아래의 기재로부터 당업자에게 명확하게 이해되어질 수 있을 것이다. 또한, 본 발명의 목적 및 장점들은 특허 청구 범위에 나타낸 수단 및 그 조합에 의해 실현될 수 있음을 쉽게 알 수 있을 것이다.

과제의 해결 수단

[0010] 이러한 기술적 과제를 달성하기 위한 본 발명의 공개키 인프라 구조를 이용한 스마트 컨트랙트의 인증된 데이터 피드 방법은, 데이터 요청자(Data Requester)가 스마트 컨트랙트(Smart Contract)의 데이터 소스(Data Source) 목록을 색인하고, 오라클로 데이터를 요청하는 (a) 단계; 오라클이 스마트 컨트랙트를 색인하여 데이터 소스(Data Source)의 주소 및 데이터 타입과 대응하는 데이터 소스(Data Source)로 데이터를 요청하는 (b) 단계; 데이터 소스(Data Source)가 오라클로 피드백하는 응답에 인증서를 서명하여 응답하는 (c) 단계; 오라클이 서명된 데이터에 대한 트랜잭션을 작성하여 스마트 컨트랙트로 보고하는 (d) 단계; 스마트 컨트랙트가 등록된 인증서 체인 컨트랙트(Certificate Chain Contract)를 호출하여 데이터 소스(Data Source)의 서명을 검증하는 (e) 단계; 및 스마트 컨트랙트가 서명이 검증된 경우, 검증 결과를 데이터 요청자(Data Requester)로 반환하는 (f) 단계를 포함하는 것을 특징으로 한다.

[0011] 바람직하게는, (a) 단계 이전에 데이터 소스(Data Source)가 데이터 제공자로의 기능을 수행하기 위한 인증서 발급을 요청하는 (g) 단계; PKI 서버가 기존의 Root CA로부터 하위 계층의 CA로 구성된 인증서 체인(Certificate Chain)에 데이터 소스(Data Source)의 인증서를 추가하여 서명된 인증서를 발급하는 (h) 단계; 인증서 체인(Certificate Chain)이 업데이트를 위해 추가된 데이터 소스(Data Source)의 인증서를 등록하는 (i) 단계; 데이터 소스(Data Source)가 발급된 인증서의 체인(Chain)과 블록체인에 기 저장된 인증서 체인 컨트랙트(Certificate Chain Contract)와 비교하여 발급 사실을 확인하는 (j) 단계; 및 스마트 컨트랙트가 인증된 데이터 소스(Data Source) 목록에 발급된 인증서를 추가하여 관리하는 (k) 단계를 포함하는 것을 특징으로 한다.

[0012] (c) 단계는 데이터 소스(Data Source)가 개인키로 인증서를 서명하는 것을 특징으로 하는 것을 특징으로 한다.

[0013] (e) 단계는 스마트 컨트랙트가 공개키를 통해 데이터 소스(Data Source)의 서명을 검증하는 것을 특징으로 한다.

발명의 효과

[0014] 상기와 같은 본 발명에 따르면, 네트워크 스택에서 어플리케이션 계층의 공개키 인프라 구조를 활용하여 제3자에게 출처 인증을 검증시킴으로써, 별도의 하드웨어를 구성하지 않고, TLS 프로토콜을 수정하지 않으면서 오라클이 전달한 데이터가 위변조 되지 않았음을 증명하는 효과가 있다.

[0015] 이에 따라 블록체인에서 생성되지 않는 암호 화폐 시장 가격, 환율, 주식 시장과 같은 외부 정보에 대해서, 오라클이 검증된 사이트로부터 인증된 데이터 보고가 가능한 효과가 있다.

[0016] 또한, 블록체인 외부의 기기(IoT 등), 이체 내역, 경기 결과 등과 같은 외부 발생 이벤트에 대한 데이터 피드에 대해 신뢰성을 제공하는 효과가 있다.

[0017] 그리고, 이름, 주민번호, 주거 지역, 자격 현황, 직업 현황, 자산 현황 등의 내용을 발급하는 데이터 소스(Data Source)로부터 인증된 데이터를 블록체인 내부로 유입하는 효과가 있다.

도면의 간단한 설명

[0018] 도 1은 본 발명의 일 실시예에 따른 공개키 인프라 구조를 이용한 스마트 컨트랙트의 인증된 데이터 피드 방법에 대한 PKI 기반 인증과 데이터 피드 절차를 도시한 블록도.

도 2는 본 발명의 일 실시예에 따른 공개키 인프라 구조를 이용한 스마트 컨트랙트의 인증된 데이터 피드 방법에 대한 인증서 발급 및 등록 절차를 도시한 순서도.

도 3은 본 발명의 일 실시예에 따른 공개키 인프라 구조를 이용한 스마트 컨트랙트의 인증된 데이터 피드 방법을 도시한 순서도.

발명을 실시하기 위한 구체적인 내용

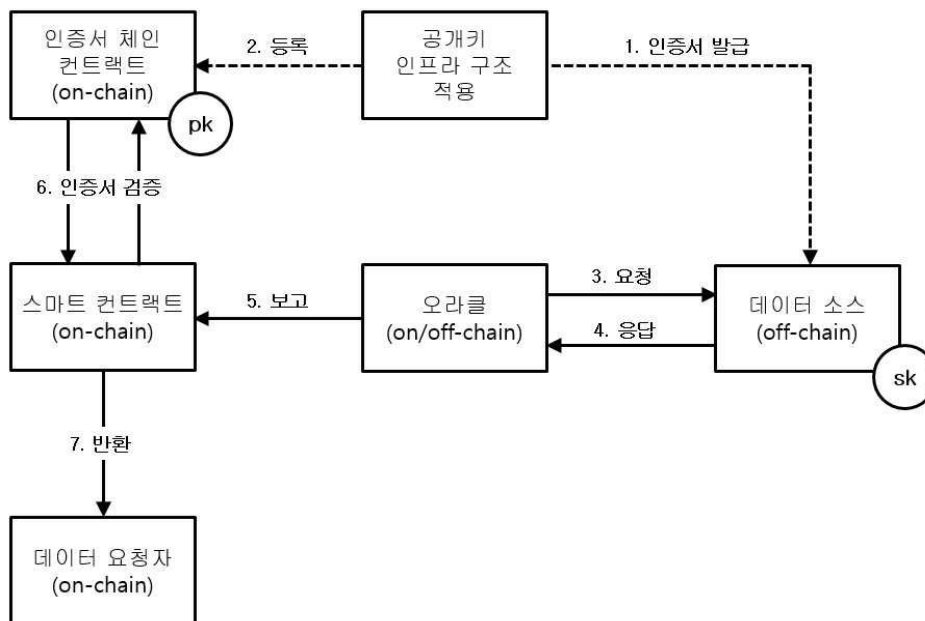
[0019] 본 발명의 구체적인 특징 및 이점들은 첨부도면에 의거한 다음의 상세한 설명으로 더욱 명백해질 것이다. 이에 앞서, 본 명세서 및 청구범위에 사용된 용어나 단어는 발명자가 그 자신의 발명을 가장 최선의 방법으로 설명하기 위해 용어의 개념을 적절하게 정의할 수 있다는 원칙에 입각하여 본 발명의 기술적 사상에 부합하는 의미와 개념으로 해석되어야 할 것이다. 또한, 본 발명에 관련된 공지 기능 및 그 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는, 그 구체적인 설명을 생략하였음에 유의해야 할 것이다.

- [0020] 도 1은 본 발명의 일 실시예에 따른 오라클 환경의 구성을 도시한 도면으로, 데이터 요청자(Data Requester)는 DAPP(Decentralized Application)과 같은 서비스의 일부로, 오라클을 구동시키는 출발점이자 데이터의 최종 목적지이다.
- [0021] 스마트 컨트랙트(Smart Contract, SC)는 오라클의 모니터링 대상으로 데이터 요청자(Data Requester)에게 요청을 받고, 오라클로부터 수신한 데이터를 반환하기 위해 존재한다.
- [0022] 오라클은 블록체인에서 생성할 수 없는 데이터를 데이터 소스(Data Source)로 요청하여 스마트 컨트랙트로 전송하는 기능을 수행하고, 데이터 소스(Data Source)는 실제 데이터를 보유하고 있는 웹서버와 동일한 형태로 구성된다.
- [0023] 본 발명의 일 실시예는 일반적인 오라클 환경에서 공개키 인프라 구조 적용(Application Public Key Infrastructure)를 추가하여 도 1에 도시된 바와 같이 구성하였다. 데이터 요청자가 스마트 컨트랙트(Smart Contract)로 데이터를 요청한 것에 대해 오라클이 데이터 소스(Data Source)로 요청을 보내는 프로세스는 종래와 동일하다.
- [0024] 하지만, 사전 작업으로 데이터 소스가 PKI 서버로부터 인증서를 발급 받아야 한다. 추가로 인증서로 서명한 응답(response)에 대해서 제3자에 해당하는 스마트 컨트랙트(Smart Contract)에서 자동으로 공개키에 대해 서명할 수 있도록 블록체인 상에 인증서 체인(Certificate Chain)에 등록이 되어야 한다.
- [0025] 이하, 도 1 및 도 2를 참조하여 본 발명의 일 실시예에 따른 공개키 인프라 구조를 이용한 스마트 컨트랙트의 인증된 데이터 피드 방법의 인증서 발급 및 등록 절차에 대해 살펴보면 아래와 같다.
- [0026] 먼저, 데이터 소스(Data Source)가 데이터 제공자로의 기능을 수행하기 위한 인증서 발급을 요청한다(S202).
- [0027] 이어서, PKI 서버가 기존의 Root CA로부터 하위 계층의 CA로 구성된 인증서 체인(Certificate Chain)에 데이터 소스(Data Source)의 인증서를 추가하여 서명된 인증서를 발급한다(S204). (도 1의 1. 인증서 발급(Issue Certificate))
- [0028] 뒤이어, 인증서 체인(Certificate Chain)이 업데이트를 위해 추가된 데이터 소스(Data Source)의 인증서를 등록한다(S206). (도 1의 2. 등록(Register))
- [0029] 이어서, 데이터 소스(Data Source)가 발급된 인증서의 Chain과 블록체인에 기 저장된 인증서 체인 컨트랙트(Certificate Chain Contract)와 비교하여 발급 사실을 확인한다(S208).
- [0030] 그리고, 스마트 컨트랙트(Smart Contract)가 인증된 데이터 소스(Data Source) 목록에 발급된 인증서를 추가하여 관리한다(S210). 이후, 데이터 요청자가 데이터 소스(Data Source)를 대상으로 오라클에게 데이터를 요청할 수 있다.
- [0031] 이하, 도 1 및 도 3을 참조하여 본 발명의 일 실시예에 따른 공개키 인프라 구조를 이용한 스마트 컨트랙트의 인증된 데이터 피드 방법의 오라클 인증된 데이터 피드 절차에 대해 살펴보면 아래와 같다.
- [0032] 먼저, 데이터 요청자(Data Requester)가 스마트 컨트랙트(Smart Contract)의 데이터 소스(Data Source) 목록을 색인하고, 오라클로 데이터를 요청한다(S302).
- [0033] 이어서, 오라클이 스마트 컨트랙트(Smart Contract)를 색인하여 데이터 소스(Data Source)의 주소(URL 등) 및 데이터 타입과 대응하는 데이터 소스(Data Source)로 데이터를 요청한다(S304). (도 1의 3. 요청(Request))
- [0034] 뒤이어, 데이터 소스(Data Source)가 오라클로 피드백하는 응답에 인증서의 개인키(sk)로 서명하여 응답한다(S306). (도 1의 4. 응답(Response))
- [0035] 이어서, 오라클이 서명된 데이터에 대한 트랜잭션을 작성하여 스마트 컨트랙트(Smart Contract)로 보고한다(S308). (도 1의 5. 보고(Report))
- [0036] 뒤이어, 스마트 컨트랙트가 등록된 인증서 체인 컨트랙트(Certificate Chain Contract)를 호출하여 데이터 소스(Data Source)의 서명을 검증한다(S310). 이때 검증은 공개키(pk)와 인증서 체인(Certificate Chain)을 확인하여 이루어진다. (도 1의 6. 인증서 검증(Verify Certificate))
- [0037] 그리고, 스마트 컨트랙트(Smart Contract)가 서명이 검증된 경우, 검증 결과를 데이터 요청자(Data Requester)로 반환한다(S312). (도 1의 7. 반환(Return))

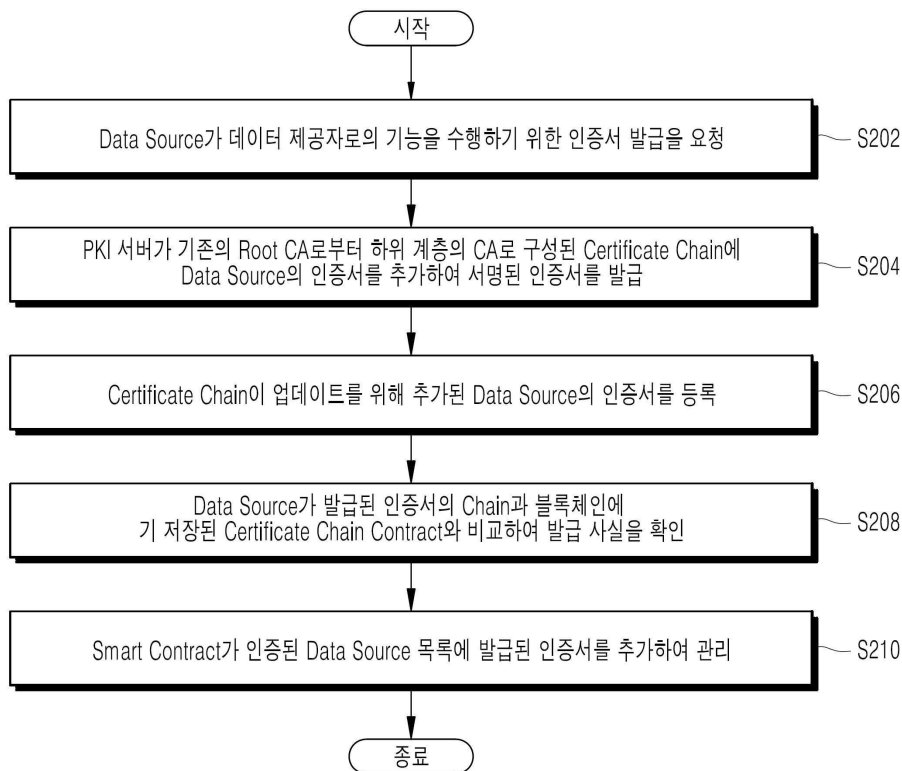
- [0038] 이처럼 전술한 바와 같은 본 발명의 일 실시예에 의하면, 네트워크 스택에서 어플리케이션 계층의 공개키 인프라 구조를 활용하여 제3자에게 출처 인증을 검증시킴으로써, 별도의 하드웨어를 구성하지 않고, TLS 프로토콜을 수정하지 않으면서 오라클이 전달한 데이터가 위변조 되지 않았음을 증명하는 효과가 있다.
- [0039] 아울러, 종래의 경우 TEE를 활용한 오라클 솔루션으로 외부 정보에 대한 인증 대신에, 오라클이 위변조 하지 않았다는 사실을 TEE 내에서 증명함에 따라, Intel SGX와 같은 별도의 하드웨어를 필수적으로 보유해야만 했으나, 본 발명의 일 실시예에 의하면 하드웨어에 의존적이지 않다는 장점이 있다.
- [0040] 그리고, 하드웨어를 사용하지 않고 오라클과 데이터 소스(Data Source)간의 TLS 통신 기록 단위(record)에 대해 순서대로 서명한 후, 오라클은 서명된 데이터를 스마트 컨트랙스로 제출하는 종래의 TLS-N 기법의 경우, TLS 프로토콜의 수정이 불가피하나, 본 발명의 일 실시예에 의하면 인증서 발급 및 등록과 오라클의 인증된 데이터 피드에 대한 일련의 절차를 TLS 계층이 아닌 Application 계층에서 수행함으로써, TLS 프로토콜을 수정하지 않아도 되는 장점이 있다.
- [0041] 이상으로 본 발명의 기술적 사상을 예시하기 위한 바람직한 실시예와 관련하여 설명하고 도시하였지만, 본 발명은 이와 같이 도시되고 설명된 그대로의 구성 및 작용에만 국한되는 것이 아니며, 기술적 사상의 범주를 일탈함이 없이 본 발명에 대해 다수의 변경 및 수정이 가능함을 당업자들은 잘 이해할 수 있을 것이다. 따라서 그러한 모든 적절한 변경 및 수정과 균등 물들도 본 발명의 범위에 속하는 것으로 간주되어야 할 것이다.

도면

도면1



도면2



도면3

