



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년04월22일
(11) 등록번호 10-2103179
(24) 등록일자 2020년04월16일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) H04L 29/06 (2006.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 9/3218 (2013.01)
H04L 63/166 (2013.01)
(21) 출원번호 10-2019-0152094
(22) 출원일자 2019년11월25일
심사청구일자 2019년11월25일
(56) 선행기술조사문헌
W02019092552 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
충남대학교 산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
류재철
대전광역시 유성구 어은로 57 한빛아파트 132-801
박준후
대전광역시 유성구 유성대로720번길 6 아인스빌 411호
(뒷면에 계속)
(74) 대리인
이은철, 김재문

전체 청구항 수 : 총 3 항

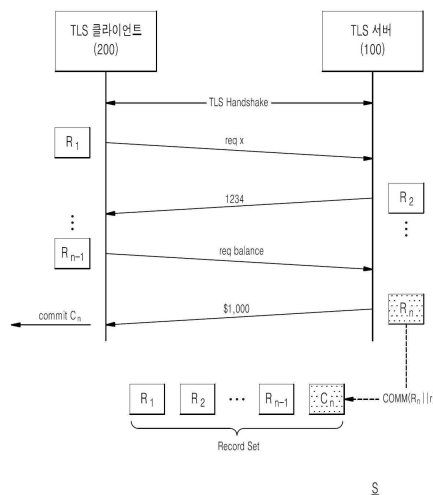
심사관 : 한지혜

(54) 발명의 명칭 **블록체인 오라클에서의 프라이버시 보호를 위한 영지식 증명 시스템 및 그 방법**

(57) 요약

본 발명은 블록체인 오라클에서의 프라이버시 보호를 위한 영지식 증명 시스템 및 그 방법에 관한 것으로서, 데이터를 제공하는 TLS 서버; 블록체인에 외부 데이터를 요청하여 전달하는 기능을 수행하는 오라클 TLS 클라이언트; 제시한 증거 proof를 검증하는 기능을 수행하는 Verification Contract; 및 TLS 서버를 포함한 웹 사이트의 인증서 기능을 수행하는 TLS Certchain을 포함하되, TLS 서버 및 TLS 클라이언트는, 각각이 handshake 과정을 거쳐 세션을 맺고, TLS 통신 과정에서 Record 단위로 각자 기록하고, TLS 세션 종료시 Record Set을 서로 비교하되, 비교 결과 Record Set이 동일할 경우, 개인정보에 해당하는 Record에 대해서 random 'r'을 포함한 C_n 을 생성한다.

대표도 - 도2



(52) CPC특허분류

H04L 9/0869 (2013.01)

H04L 9/3263 (2013.01)

H04L 2209/38 (2013.01)

(72) 발명자

김근영

대전광역시 유성구 장대로 87 퍼스트캐슬 202호

김혁진

대전광역시 서구 대덕대로168번길 82 웰리움

이 발명을 지원한 국가연구개발사업

과제고유번호 2018-0-00251

부처명 과학기술정보통신부

연구관리전문기관 정보통신기획평가원

연구사업명 정보보호핵심원천기술개발

연구과제명 스마트 컨트랙트 프라이버시 보호 및 취약점 분석 기술개발

기 여 율 1/1

주관기관 충남대학교 산학협력단

연구기간 2018.04.01 ~ 2020.12.31

명세서

청구범위

청구항 1

데이터를 제공하는 TLS 서버;

블록체인에 외부 데이터를 요청하여 전달하는 기능을 수행하는 오라클 TLS 클라이언트;

제시한 증거 proof를 검증하는 기능을 수행하는 Verification Contract; 및

상기 TLS 서버를 포함한 웹 사이트의 인증서 기능을 수행하는 TLS Certchain을 포함하되,

상기 TLS 서버 및 TLS 클라이언트는,

각각이 handshake 과정을 거쳐 세션을 맺고, TLS 통신 과정에서 Record 단위로 각자 기록하고, TLS 세션 종료시 Record Set을 서로 비교하되, 비교 결과 Record Set이 동일할 경우, TLS클라이언트가 개인정보에 해당하는 Record R에 대해서 random 'r'을 포함한 C_n 을 생성하고,

상기 TLS 클라이언트는,

상기 TLS 서버로부터 수신한 Record Set에 sk로 서명한 값, Record R 및 C_n 을 이용한 proof를 생성하며,

상기 Verification Contract는,

사전에 공유된 Circuit Verify()와 vk를 이용하여 proof가 참인지 거짓인지 여부를 검증하되,

검증결과 proof가 참일 경우, 상기 TLS 클라이언트가 Record R을 증명하기 위한 조건 Condition을 만족하면서 상기 TLS 서버로부터 수신한 서명이 확인된 것으로 판단

하는 것을 특징으로 하는 블록체인 오라클에서의 프라이버시 보호를 위한 영지식 증명 시스템.

청구항 2

제1항에 있어서,

상기 TLS 클라이언트는 C_n 을 블록체인에 commit하고,

상기 TLS 서버는 블록체인에 상기 TLS 클라이언트(200)가 제시한 C_n 이 확인되면 상기 Record Set에 sk로 서명

하는 것을 특징으로 하는 블록체인 오라클에서의 프라이버시 보호를 위한 영지식 증명 시스템.

청구항 3

삭제

청구항 4

삭제

청구항 5

(a) TLS 서버 및 TLS 클라이언트 각각이 handshake 과정을 거쳐 세션을 맺는 단계;

(b) TLS 서버 및 TLS 클라이언트가 TLS 세션 종료시 서로의 Record Set을 비교하는 단계;

(c) 상기 (b) 단계의 비교결과 Record Set이 동일할 경우, TLS 클라이언트가 개인정보에 해당하는 Record R에 대해서 random r을 포함하는 C_n 을 생성하는 단계;

(d) TLS 클라이언트가 C_n 을 블록체인에 commit하는 단계;

- (e) TLS 서버가 블록체인에 commit된 C_n 이 확인되면, Record Set에 sk로 서명한 값을 TLS 클라이언트로 전송하는 단계;
- (f) TLS 클라이언트가 TLS 서버로부터 수신한 Record Set에 sk로 서명한 값, Record R 및 C_n 을 이용한 proof를 생성하는 단계;
- (g) Verification Contract가 사전에 공유된 Circuit Verify()와 vk를 이용하여 proof가 참인지 거짓인지 여부를 검증하는 단계; 및
- (h) 상기 (g) 단계의 검증결과, proof가 참일 경우 TLS 클라이언트가 Record R을 증명하기 위한 조건 Condition을 만족하면서 TLS 서버로부터 수신한 서명이 확인된 것으로 판단하는 단계를 포함하는 것을 특징으로 하는 블록체인 오라클에서의 프라이버시 보호를 위한 영지식 증명 방법.

청구항 6

삭제

발명의 설명

기술 분야

- [0001] 본 발명은 블록체인 오라클에서의 프라이버시 보호를 위한 영지식 증명 시스템 및 그 방법에 관한 것으로 더욱 상세하게는, 오라클을 통해 블록체인 외부에서 발생한 이벤트나 데이터 수신을 제공하는 Transport Layer Security(TLS) 환경에서, 사용자의 프라이버시 보호를 위한 영지식 증명(Zero-knowledge proof)을 적용하는 기술에 관한 것이다.

배경 기술

- [0002] 블록체인에서 외부(off-chain)에서 발생한 이벤트나 데이터를 가져올 때 신뢰성을 판단하는 것은 매우 어렵다. 예를 들어, 스포츠 경기 결과에 따라 돈을 배당하는 계약을 블록체인에 저장할 경우 계약의 이행 자체는 스마트 컨트랙트로 보장되지만, 실제 경기 결과는 블록체인 외부에서 발생한 사건이기 때문에, 결과를 잘못 입력할 경우, 계약이 올바르게 실행되지 않을 수 있다.
- [0003] 이 같은 문제를 해결하기 위해 신뢰할 수 있는 데이터를 전달하는 역할 또는 방법으로 오라클(oracle)있으나, 이러한 오라클을 이용하여 인터넷에 존재하는 수많은 데이터를 활용하기 위해서는 HTTPS를 지원하는 TLS를 블록체인과 연결해야 한다. 이를 위해 신뢰 실행 환경 Trusted Execution Environments(TEE) 내부에 TLS를 설치하여 신뢰성을 제공하는 Town Crier, Chainlink, 또는 TLS 프로토콜을 수정하여 인증을 제공하는 TLS-N과 같은 방법이 제시되었다.
- [0004] 그러나, 종래에 제안된 방법들은 외부 데이터를 가져오기 위한 인증은 제공하지만, 외부 데이터가 개인의 민감한 데이터일 경우 프라이버시 보호 문제가 발생할 수 있다.
- [0005] 이에 본 출원인은 이러한 문제점을 해소하기 위해, TLS를 지원하는 환경에서 프라이버시 보호를 위해 영지식 증명을 적용하는 시스템과 그 방법을 제안하고자 한다.

선행기술문헌

특허문헌

- [0006] (특허문헌 0001) 한국공개특허 제10-2019-0076535호(2019.07.02)

발명의 내용

해결하려는 과제

- [0007] 본 발명의 목적은, 오라클을 통해 블록체인 외부에서 발생한 이벤트나 데이터 수신을 제공하는 TLS 환경에 영지

식 증명을 적용하여 데이터의 출처에 대한 인증과 조건 condition에 대한 정확성을 제공함으로써, 사용자의 프라이버시를 보호하는데 있다.

과제의 해결 수단

- [0008] 이러한 기술적 과제를 달성하기 위한 본 발명의 블록체인 오라클에서의 프라이버시 보호를 위한 영지식 증명 시스템은, 데이터를 제공하는 TLS 서버; 블록체인에 외부 데이터를 요청하여 전달하는 기능을 수행하는 오라클 TLS 클라이언트; 제시한 증거 proof를 검증하는 기능을 수행하는 Verification Contract; 및 TLS 서버를 포함한 웹 사이트의 인증서 기능을 수행하는 TLS Certchain을 포함하되, TLS 서버 및 TLS 클라이언트는, 각각이 handshake 과정을 거쳐 세션을 맺고, TLS 통신 과정에서 Record 단위로 각자 기록하고, TLS 세션 종료시 Record Set을 서로 비교하되, 비교 결과 Record Set이 동일할 경우, 개인정보에 해당하는 Record에 대해서 random 'r' 을 포함한 C_n 을 생성하는 것을 특징으로 한다.
- [0009] 바람직하게는, TLS 클라이언트는 C_n 을 블록체인에 commit하고, TLS 서버는 블록체인에 상기 TLS 클라이언트 (200)가 제시한 C_n 이 확인되면 상기 Record Set에 sk로 서명하는 것을 특징으로 한다.
- [0010] TLS 클라이언트는, TLS 서버로부터 Record Set에 sk로 서명한 값을 수신하여 색인한 Record R 및 Commitment C를 결합한 proof를 생성하는 것을 특징으로 한다.
- [0011] Verification Contract는, 사전에 공유된 Circuit Verify()와 vk를 이용하여 proof가 참인지 거짓인지 여부를 TLS Certchain을 통해 검증하되, 검증결과 proof가 참일 경우, TLS 클라이언트가 조건 condition을 만족하면서 상기 TLS 서버로부터 수신한 서명이 확인된 것으로 판단하는 것을 특징으로 한다.
- [0012] 전술한 시스템을 기반으로 하는 블록체인 오라클에서의 프라이버시 보호를 위한 영지식 증명 방법은, TLS 클라이언트가 TLS 서버로부터 Record Set에 sk로 서명한 값을 수신하는 (a) 단계; TLS 클라이언트가 기 생성된 Record R 및 Commitment C를 색인하는 (b) 단계; TLS 클라이언트가 Auth_D, 와 Record R, Commitment C를 결합한 proof를 생성하는 (c) 단계; TLS 클라이언트가 생성된 proof와 Public input x를 Verification Contract로 전송하는 (d) 단계; Verification Contract가 사전에 공유된 Circuit Verify()와 vk를 이용하여 proof가 참인지 거짓인지 여부를 검증하는 (e) 단계; 및 (e) 단계의 검증결과, proof가 참일 경우 TLS 클라이언트가 조건 condition을 만족하면서 TLS 서버로부터 수신한 서명이 확인된 것으로 판단하는 (f) 단계를 포함하는 것을 특징으로 한다.
- [0013] 바람직하게는, (a) 단계 이전에 TLS 서버 및 TLS 클라이언트 각각이 handshake 과정을 거쳐 세션을 맺는 (g) 단계; TLS 서버 및 TLS 클라이언트가 TLS 세션 종료시 서로의 Record Set을 비교하는 (h) 단계; (h) 단계의 비교결과 Record Set이 동일할 경우, TLS 클라이언트가 개인정보에 해당하는 Record에 대해서 random r을 포함하는 C_n 을 생성하는 (i) 단계; TLS 클라이언트가 C_n 을 블록체인에 commit하는 (j) 단계; 및 TLS 서버가 블록체인에 commit된 C_n 이 확인되면, Record Set에 sk로 서명한 값을 TLS 클라이언트로 전송하는 (k) 단계를 포함하는 것을 특징으로 한다.

발명의 효과

- [0014] 상기와 같은 본 발명에 따르면, 오라클을 통해 블록체인 외부에서 발생한 이벤트나 데이터 수신을 제공하는 TLS 환경에 영지식 증명을 적용하여 데이터의 출처에 대한 인증과 조건 condition에 대한 정확성을 제공함으로써, 사용자의 프라이버시를 보호하는 효과가 있다.

도면의 간단한 설명

- [0015] 도 1은 본 발명의 일 실시예에 따른 블록체인 오라클에서의 프라이버시 보호를 위한 영지식 증명 시스템의 오라클 환경을 도시한 블록도.
- 도 2는 본 발명의 일 실시예에 따른 블록체인 오라클에서의 프라이버시 보호를 위한 영지식 증명 시스템의 세부 절차를 도시한 도면.
- 도 3은 본 발명의 일 실시예에 따른 블록체인 오라클에서의 프라이버시 보호를 위한 영지식 증명 방법의 인증된 데이터 요청 절차를 도시한 순서도.

도 4는 본 발명의 일 실시예에 따른 블록체인 오라클에서의 프라이버시 보호를 위한 영지식 증명 방법의 proof 생성 절차를 도시한 순서도.

도 5는 본 발명의 일 실시예에 따른 블록체인 오라클에서의 프라이버시 보호를 위한 영지식 증명 방법의 proof 검증 절차를 도시한 순서도.

발명을 실시하기 위한 구체적인 내용

- [0016] 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.
- [0017] 본 발명의 일 실시예에 따른 블록체인 오라클에서의 프라이버시 보호를 위한 영지식 증명 시스템(S)은 도 1에 도시된 바와 같이, 데이터를 제공하는 TLS 서버(100), 블록체인에 외부 데이터를 요청하여 전달하는 기능을 수행하는 오라클 TLS 클라이언트(200), 제시한 증거 proof를 검증하는 기능을 수행하는 Verification Contract(300), 및 TLS 서버(100)를 포함한 웹 사이트의 인증서 기능을 수행하는 TLS Certchain(400)을 포함하여 구성됨에 따라 종래와 달리 누구나 오라클 기능 수행이 가능한 환경으로 구성된다.
- [0018] 또한, 본 발명의 일 실시예에 따른 영지식 증명은 크게 증거(proof)를 생성하는 Prove 과정과 이를 검증하는 Verify 과정으로 구성된다.
- [0019] 여기서, Prove는 proving key(pk)와 비밀값이 포함된 w, 및 public input x를 입력받아 계산된 proof를 생성하고 이를 Proof(pk, w, x)로 표현하며, Verify는 Verifying key(vk), proof 및 x를 입력으로 proof가 참인지 거짓인지 여부를 판별하며 이를 Verify(vk, proof, x)로 표현한다.
- [0020] 이때, Prove를 실행하는 기능은 Prover가 수행하고, Verify를 실행하는 기능은 Verifier가 수행하며, 도 1에서는 TLS 클라이언트(200)가 Prover이고, Verification Contract(300)가 Verifier인 것으로 이해함이 바람직하다.
- [0021] 본 발명의 일 실시예에서는 오라클 환경에서 영지식 증명을 위해 아래의 두 가지 조건을 상정하여 영지식 증명을 통해 처리하였다.
- [0022] 이러한 영지식 증명을 구성하기 위한 사전 작업으로 아래의 조건 1의 Auth_D 생성을 위한 절차와, 2.를 위한 proof 생성 절차를 제안하며 proof를 검증함으로써, 1, 2가 만족됨을 보장한다.
- [0023] 1. 데이터의 출처에 대한 인증 : TLS 서버(100)의 개인키 sk로 서명한 Auth_D로 증명
- [0024] 2. 조건 condition에 대한 정확성 : (예를 들어 balance \$1,000 > conditionPrice \$500)
- [0025] 이하, 도 2를 참조하여 본 발명의 일 실시예에 따른 블록체인 오라클에서의 프라이버시 보호를 위한 영지식 증명 시스템(S)의 세부 절차에 대해 살펴보면 아래와 같다.
- [0026] 먼저, 인증된 데이터(Auth D) 요청 및 응답 절차를 수행하는 절차는, TLS 서버(100) 및 TLS 클라이언트(200) 각각이 handshake 과정을 거쳐 세션을 맺고, TLS 통신 과정에서 Record 단위로 각자 기록한다.
- [0027] 또한, TLS 서버(100) 및 TLS 클라이언트(200)는 TLS 세션 종료시 Record Set을 서로 비교하되, 비교 결과 Record Set이 동일할 경우, TLS 클라이언트(200)가 개인정보에 해당하는 $R_n(\$1,000)$ 과 같은 Record R에 대해서 random 'r'을 포함한 $C_n = \text{COMM}(R_n || r)$ 을 생성한다.
- [0028] 이때, COMM() 함수는 SHA-256과 같은 해시를 사용할 수 있고, r 값은 TLS 클라이언트(200)가 생성하여 TLS 서버(100)와 공유한다.
- [0029] 또한, TLS 클라이언트(200)는 C_n 을 블록체인에 commit하고, TLS 서버(100)는 블록체인에 TLS 클라이언트(200)가 제시한 C_n 이 확인되면 Record Set에 sk로 서명한 Auth_D = Sign(sk, Record Set)을 TLS 클라이언트(200)로 전송한다.

- [0030] 한편, proof를 생성하는 Prover(pk, w, x) 절차는 다음과 같다.
- [0031] TLS 클라이언트(200)는 TLS 서버(100)로부터 수신한 Auth_D와 Record R, Commitment C을 바탕으로 proof를 생성한다. 이때, TLS 클라이언트(200)는 는 비밀값이 포함된 w, 및 public input x를 입력받아 계산된 Proof(pk, w, x)를 생성하는데, pk와 vk의 Key Generation과 Proof() 및 Verify()를 수행하는 Circuit은 사전에 Setup 단계로 구성된 것으로 상정한다.
- [0032] 또한, witness w는 [개인정보에 해당하는 Record R, random r]로 구성되고, Public input x는 [서버의 개인키 sk로 서명한 데이터인 Auth_D, TLS 통신 과정을 기록한 데이터인 Record Set, condition, Certchain]으로 구성된다. 여기서, condition은 secret Record R에 대해 증명하기 위한 조건을 의미한다.
- [0033] 또한, Prove() 함수는 비대화형 영지식 증명(Non Interactive Zero Knowledge Proof)의 어떤 알고리즘도 사용할 수 있다.
- [0034] 최종적으로 Prover(pk, w, x)의 결과로 proof가 생성되고, TLS 클라이언트(200)가 생성된 proof와 Public input x를 Verification Contract(300)로 전송한다.
- [0035] 그리고, proof를 검증하는 Verify(vk, proof, x) 절차는 아래와 같다.
- [0036] Verification Contract(300)은 TLS 클라이언트(200)로부터 전달받은 proof와 Public input x에 대한 검증을 수행하는데, 사전에 공유된 Circuit Verify()와 vk를 이용하여 proof가 참인지 거짓인지 여부를 검증한다. 이때, Certchain의 조작을 방지하기 위해 Public input x의 Certchain은 블록체인에 저장된 TLS Certchain(400)을 이용한다.
- [0037] Verification Contract(300)의 proof 검증결과 참인 경우, TLS 클라이언트(200)가 제시한 조건 condition을 만족하면서 TLS 서버(100)로부터 수신한 서명이 확인된 것으로 판단하고, proof가 거짓일 경우 폐기한다.
- [0038] 한편, 본 발명의 일 실시예에 따른 블록체인 오라클에서의 프라이버시 보호를 위한 영지식 증명 방법은, 인증된 데이터(Auth_D) 요청, proof 생성, 및 proof 검증 절차로 이루어지는데, 도 3 내지 도 5를 참조하여 살펴보면 아래와 같다.
- [0039] **1. 인증된 데이터(Auth D) 요청 (도 3)**
- [0040] 먼저, TLS 서버(100) 및 TLS 클라이언트(200) 각각이 handshake 과정을 거쳐 세션을 맺는다(S302).
- [0041] 이어서, TLS 서버(100) 및 TLS 클라이언트(200)가 TLS 세션 종료시 서로의 Record Set을 비교한다(S304).
- [0042] 제S304 단계의 비교결과 Record Set이 동일할 경우, TLS 클라이언트(200)가 개인정보에 해당하는 Record R에 대해서 random r을 포함하는 값(C_n)을 생성한다(S306).
- [0043] 뒤이어, TLS 클라이언트(200)가 random r을 포함하는 값(C_n)을 블록체인에 commit한다(S308).
- [0044] 그리고, TLS 서버(100)가 블록체인에 commit된 C_n 이 확인되면, Record Set에 sk로 서명한 Auth_D를 TLS 클라이언트(200)로 전송한다(S310).
- [0045] **2. proof 생성 (도 4)**
- [0046] 먼저, TLS 클라이언트(200)가 TLS 서버(100)로부터 Record Set에 sk로 서명한 값(Auth_D)을 수신한다(S402).
- [0047] 이어서, TLS 클라이언트(200)가 기 생성된 Record R 및 Commitment C을 색인한다(S404).
- [0048] 뒤이어, TLS 클라이언트(200)가 Auth_D와 Record R, Commitment C를 결합한 proof를 생성한다(S406).
- [0049] 그리고, TLS 클라이언트(200)가 생성된 proof와 Public input x를 Verification Contract(300)로 전송한다(S408).
- [0050] **2. proof 검증 (도 5)**
- [0051] 먼저, Verification Contract(300)가 TLS 클라이언트(200)로부터 proof를 수신한다(S502).
- [0052] 이어서, Verification Contract(300)가 사전에 공유된 Circuit Verify()와 vk를 이용하여 proof가 참인지 거짓인지 여부를 검증한다(S504). 이때, proof 검증은 블록체인에 저장된 TLS Certchain(400)을 통해 수행된다.

- [0053] 제S504단계의 판단결과, proof가 참일 경우, Verification Contract(300)는 TLS 클라이언트(200)가 조건 condition을 만족하면서 TLS 서버(100)로부터 수신한 서명이 확인된 것으로 판단한다(S506).
- [0054] 반면에, 제S504단계의 검증결과 proof가 거짓일 경우, Verification Contract(300)가 proof를 폐기한다(S508).
- [0055] 이처럼, 전술한 바와 같은 본 발명의 일 실시예에 따른 블록체인 오라클에서의 프라이버시 보호를 위한 영지식 증명 방법에 의하면, 오라클을 통해 블록체인 외부에서 발생한 이벤트나 데이터 수신을 제공하는 TLS 환경에 영지식 증명을 적용하여 데이터의 출처에 대한 인증과 조건 condition에 대한 정확성을 제공함으로써, 사용자의 프라이버시를 보호할 수 있다.
- [0056] 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 균등물들도 본 발명의 범위에 속하는 것으로 간주되어야 할 것이다.

부호의 설명

- [0057] S: 블록체인 오라클에서의 프라이버시 보호를 위한 영지식 증명 시스템

100: TLS 서버

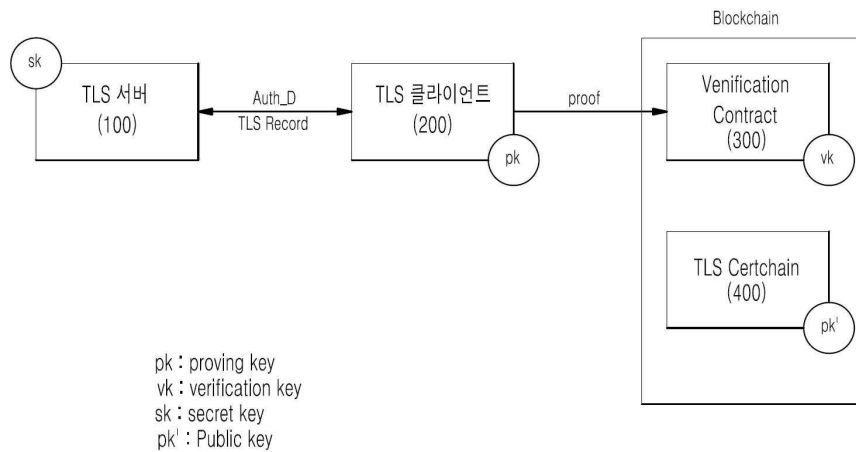
200: TLS 클라이언트

300: Verification Contract

400: TLS Certchain

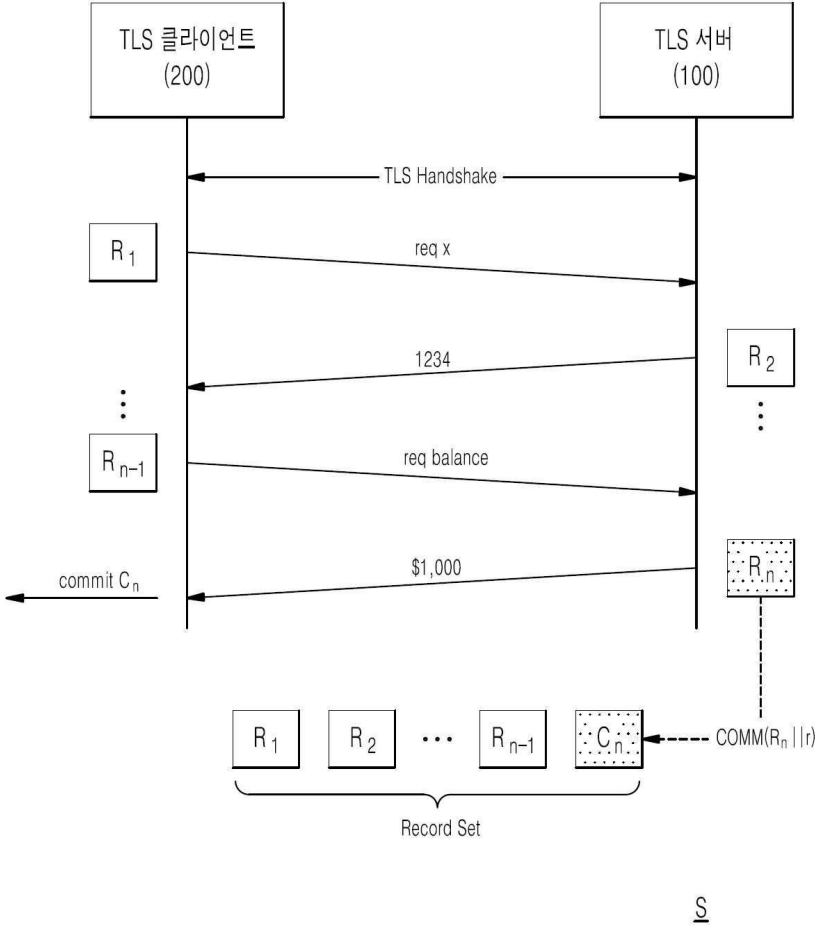
도면

도면1

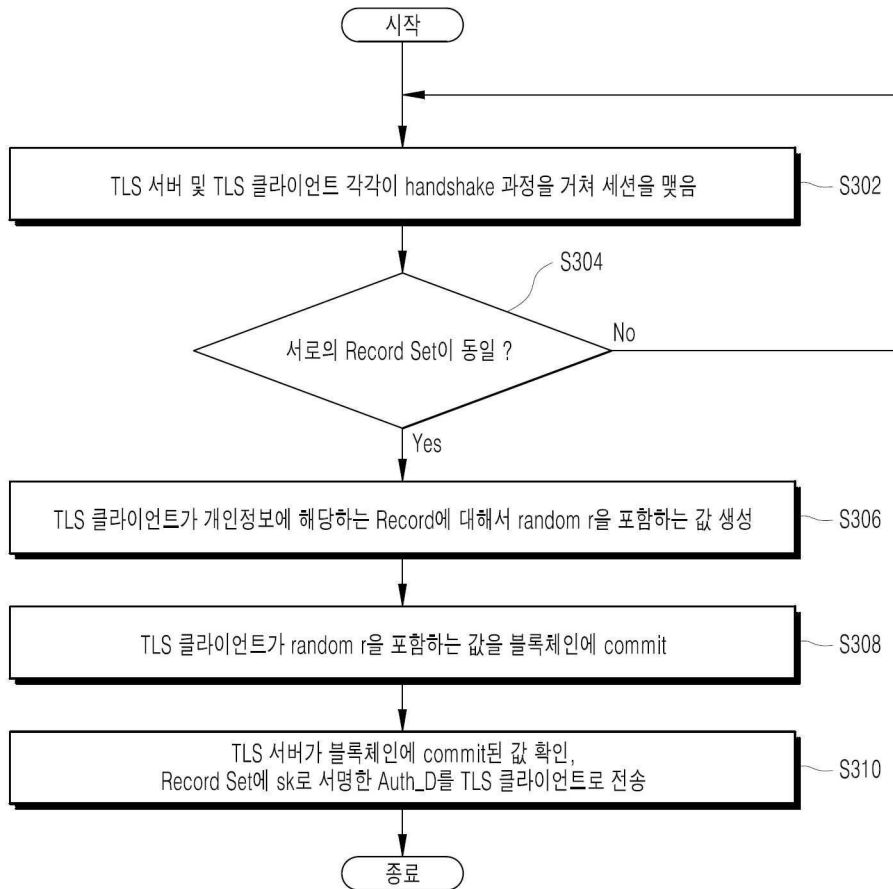


S

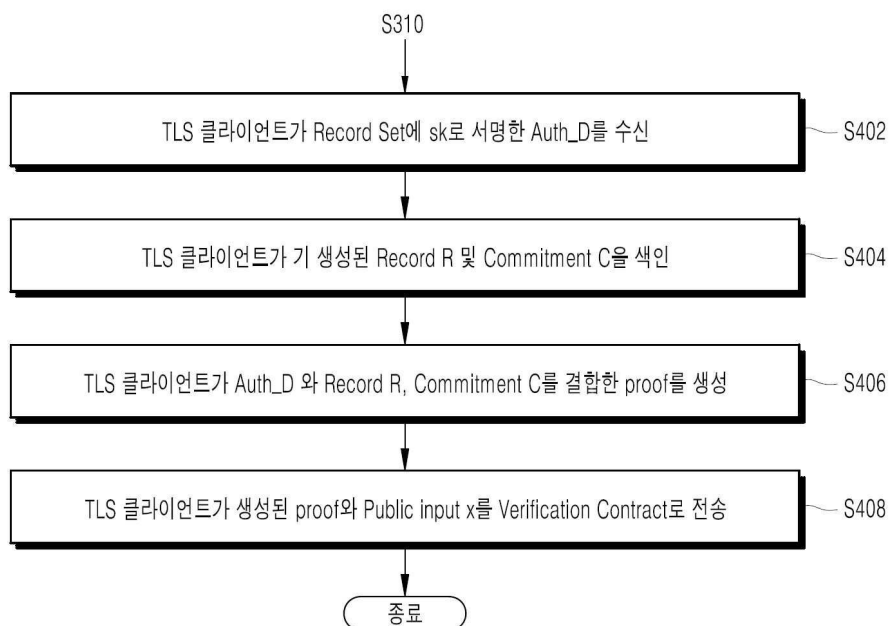
도면2



도면3



도면4



도면5

