

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)(11) 공개번호 10-2022-0096092
(43) 공개일자 2022년07월07일

(51) 국제특허분류(Int. Cl.)

H04L 9/32 (2006.01) H04L 65/40 (2022.01)

H04L 9/00 (2022.01) H04L 9/06 (2006.01)

H04L 9/08 (2006.01)

(52) CPC특허분류

H04L 9/3242 (2013.01)

H04L 67/1097 (2022.05)

(21) 출원번호 10-2020-0188231

(22) 출원일자 2020년12월30일

심사청구일자 2020년12월30일

(71) 출원인

조선대학교산학협력단

광주광역시 동구 필문대로 309 (서석동)

(72) 발명자

김영식

광주광역시 서구 풍암2로 66 금호2차아파트 201동 1005호

(74) 대리인

김효성

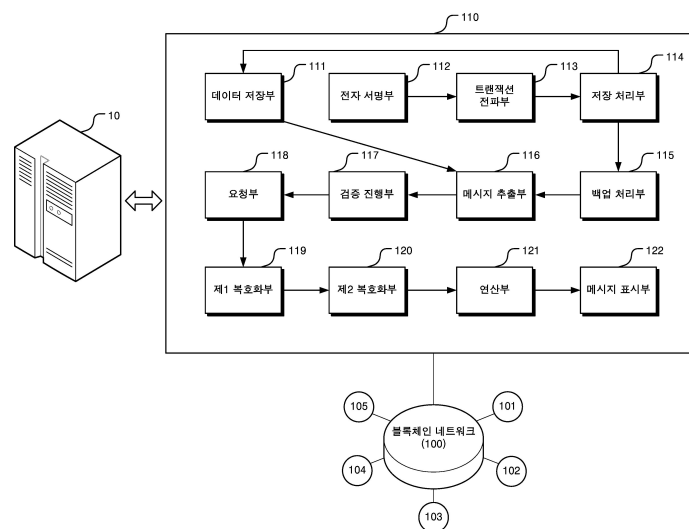
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 블록체인 기반의 차량용 메시지 관리 장치 및 그 동작 방법

(57) 요약

블록체인 기반의 차량용 메시지 관리 장치 및 그 동작 방법이 개시된다. 본 발명에 따른 차량용 메시지 관리 장치 및 그 동작 방법은 커넥티드 카에서 소정의 통신 메시지가 전송되는 경우, 상기 통신 메시지를 암호화한 후 상기 통신 메시지에 대한 해시 값과 암호화된 통신 메시지를 블록체인 네트워크를 구성하고 있는 노드 장치들과 연동하여 블록체인 상에 등록함으로써, 상기 통신 메시지에 대한 무결성이 보장될 수 있도록 지원할 수 있다.

대표도 - 도1



(52) CPC특허분류

H04L 9/008 (2013.01)
H04L 9/0618 (2013.01)
H04L 9/0643 (2013.01)
H04L 9/0825 (2013.01)
H04L 9/3247 (2013.01)
H04L 9/50 (2022.05)
H04L 2209/84 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711102950
과제번호	2016-0-00142-005
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보보호핵심원천기술개발(R&D, 정보화)
연구과제명	(창조씨앗 2단계) IoT 및 클라우드 컴퓨팅을 위한 경량 포스트 양자 암호 시스템 연

구

기 여 율	1/1
과제수행기관명	서울대학교 산학협력단
연구기간	2020.01.01 ~ 2020.12.31

명세서

청구범위

청구항 1

블록체인 네트워크를 구성하는 복수의 노드 장치들 중 하나로서, 커넥티드 카(Connected Car)에 탑재되어 상기 커넥티드 카에서 전송되는 통신 메시지를 상기 블록체인 네트워크에 저장하기 위한 블록체인 기반의 차량용 메시지 관리 장치에 있어서,

복수의 블록들이 체인으로 연결된 블록체인 데이터 - 상기 블록체인 데이터는 상기 복수의 노드 장치들 중 상기 차량용 메시지 관리 장치를 제외한 나머지 노드 장치들에도 저장되어 있음 - 를 저장하고 있는 데이터 저장부;

상기 커넥티드 카에서 제1 통신 메시지가 생성되어 외부의 데이터 수신 장치로 전송된 경우, 사전 설정된 해시 함수에 상기 제1 통신 메시지를 입력으로 인가하여 제1 해시 값을 생성하고, 상기 제1 해시 값을 사전 발급된 개인키로 전자 서명하여 제1 전자 서명 값을 생성하는 전자 서명부;

상기 제1 통신 메시지를 암호화한 후 상기 암호화된 제1 통신 메시지와 상기 제1 해시 값 및 상기 제1 전자 서명 값을 포함하는 제1 트랜잭션을 생성하고, 상기 복수의 노드 장치들 중 상기 차량용 메시지 관리 장치를 제외한 나머지 노드 장치들로 상기 제1 트랜잭션을 전파함으로써, 상기 제1 트랜잭션의 상기 블록체인 네트워크에의 등록을 시도하는 트랜잭션 전파부; 및

상기 제1 트랜잭션이 상기 나머지 노드 장치들로 전파된 후 상기 복수의 노드 장치들 중 어느 하나인 제1 노드 장치에서 상기 제1 트랜잭션을 포함하는 $N(N$ 은 2이상의 자연수임)개의 트랜잭션들이 포함된 블록이 생성됨에 따라, 상기 블록체인 네트워크를 통해 상기 블록이 수신되면, 상기 데이터 저장부에 저장되어 있는 상기 블록체인 데이터에 상기 블록을 체인으로 연결함으로써, 상기 블록에 대한 저장을 완료하는 저장 처리부

를 포함하는 차량용 메시지 관리 장치.

청구항 2

제1항에 있어서,

상기 트랜잭션 전파부는

동형 암호화(Homomorphic Encryption)를 위한 사전 설정된 암호화키를 이용하여 상기 제1 통신 메시지에 대한 동형 암호화를 수행함으로써, 상기 제1 통신 메시지를 암호화하는 차량용 메시지 관리 장치.

청구항 3

제2항에 있어서,

상기 블록에 대한 저장이 완료되면, 사전 설정된 백업 서버 - 상기 백업 서버에는 상기 암호화키를 기초로 동형 암호화가 수행된 복수의 통신 메시지들이 사전 저장되어 있음 - 로 상기 암호화된 제1 통신 메시지를 전송하면서, 상기 암호화된 제1 통신 메시지에 대한 저장 요청 명령을 전송하는 백업 처리부

를 더 포함하는 차량용 메시지 관리 장치.

청구항 4

제3항에 있어서,

상기 블록에 대한 저장이 완료된 이후, 사용자에 의해 상기 블록에 포함되어 있는 상기 암호화된 제1 통신 메시지에 대한 복호화 요청이 수신되면, 상기 블록에 포함된 상기 제1 트랜잭션으로부터 상기 암호화된 제1 통신 메시지와 상기 제1 해시 값 및 상기 제1 전자 서명 값을 추출하는 메시지 추출부;

상기 개인키에 대응하는 공개키를 기초로 상기 제1 전자 서명 값을 복원하였을 때 생성되는 복원 값이 상기 제1 해시 값과 일치하는지 비교함으로써, 상기 제1 전자 서명 값에 대한 검증을 진행하는 검증 진행부;

상기 제1 전자 서명 값에 대한 검증이 완료되면, 상기 백업 서버로, 상기 암호화된 제1 통신 메시지의 복호화를

위한 검증 데이터를 피드백할 것을 요청하는 요청부;

상기 백업 서버로부터 상기 검증 데이터로서, 상기 백업 서버에서 생성된 제1 연산 데이터 - 상기 제1 연산 데이터는 상기 백업 서버에 저장되어 있는 상기 암호화된 제1 통신 메시지와 상기 백업 서버에 저장되어 있는 암호화된 제2 통신 메시지가 사전 설정된 제1 동형 연산식에 따라 서로 연산되어 생성된 데이터임 - 와 상기 백업 서버에 저장되어 있는 상기 암호화된 제2 통신 메시지가 피드백되면, 상기 암호화키에 대응되는 사전 설정된 복호화키를 이용하여 상기 제1 연산 데이터를 복호화함으로써, 제1 복호화 값을 생성하는 제1 복호화부;

상기 제1 트랜잭션으로부터 추출된 상기 암호화된 제1 통신 메시지와 상기 백업 서버로부터 수신된 상기 암호화된 제2 통신 메시지를 각각 상기 복호화키를 이용하여 복호화함으로써, 상기 암호화된 제1 통신 메시지에 대한 제1 복호화 메시지와 상기 암호화된 제2 통신 메시지에 대한 제2 복호화 메시지를 생성하는 제2 복호화부;

상기 제1 동형 연산식에 대응되는 평문 도메인에서의 제1 연산식에 기초하여 상기 제1 복호화 메시지와 상기 제2 복호화 메시지 간의 연산을 수행함으로써, 평문 연산 데이터를 생성하는 연산부; 및

상기 평문 연산 데이터가 상기 제1 복호화 값과 서로 일치하는지 비교하여 상기 평문 연산 데이터가 상기 제1 복호화 값과 일치하는 것으로 확인되면, 상기 제1 복호화 메시지를 상기 암호화된 제1 통신 메시지에 대한 복호화 메시지로서 화면 상에 표시하는 메시지 표시부

를 더 포함하는 차량용 메시지 관리 장치.

청구항 5

제4항에 있어서,

상기 백업 서버는

상기 차량용 메시지 관리 장치로부터 상기 검증 데이터의 피드백 요청이 수신되면, 상기 백업 서버에 저장되어 있는 암호화가 수행된 상기 복수의 통신 메시지들 중 어느 하나의 통신 메시지를 상기 암호화된 제2 통신 메시지로서 랜덤하게 선택한 후, 상기 백업 서버에 저장되어 있는 상기 암호화된 제1 통신 메시지와 상기 백업 서버에 저장되어 있는 상기 암호화된 제2 통신 메시지를 상기 제1 동형 연산식에 따라 서로 연산함으로써, 상기 제1 연산 데이터를 생성하고, 상기 제1 연산 데이터가 생성되면, 상기 제1 연산 데이터와 상기 백업 서버에 저장되어 있는 상기 암호화된 제2 통신 메시지를 상기 차량용 메시지 관리 장치로 피드백하는 것을 특징으로 하는 차량용 메시지 관리 장치.

청구항 6

블록체인 네트워크를 구성하는 복수의 노드 장치들 중 하나로서, 커넥티드 카(Connected Car)에 탑재되어 상기 커넥티드 카에서 전송되는 통신 메시지를 상기 블록체인 네트워크에 저장하기 위한 블록체인 기반의 차량용 메시지 관리 장치의 동작 방법에 있어서,

복수의 블록들이 체인으로 연결된 블록체인 데이터 - 상기 블록체인 데이터는 상기 복수의 노드 장치들 중 상기 차량용 메시지 관리 장치를 제외한 나머지 노드 장치들에도 저장되어 있음 - 을 저장하고 있는 데이터 저장부를 유지하는 단계;

상기 커넥티드 카에서 제1 통신 메시지가 생성되어 외부의 데이터 수신 장치로 전송된 경우, 사전 설정된 해시 함수에 상기 제1 통신 메시지를 입력으로 인가하여 제1 해시 값을 생성하고, 상기 제1 해시 값을 사전 발급된 개인키로 전자 서명하여 제1 전자 서명 값을 생성하는 단계;

상기 제1 통신 메시지를 암호화한 후 상기 암호화된 제1 통신 메시지와 상기 제1 해시 값 및 상기 제1 전자 서명 값을 포함하는 제1 트랜잭션을 생성하고, 상기 복수의 노드 장치들 중 상기 차량용 메시지 관리 장치를 제외한 나머지 노드 장치들로 상기 제1 트랜잭션을 전파함으로써, 상기 제1 트랜잭션의 상기 블록체인 네트워크에의 등록을 시도하는 단계; 및

상기 제1 트랜잭션이 상기 나머지 노드 장치들로 전파된 후 상기 복수의 노드 장치들 중 어느 하나인 제1 노드 장치에서 상기 제1 트랜잭션을 포함하는 N(N은 2이상의 자연수임)개의 트랜잭션들이 포함된 블록이 생성됨에 따라, 상기 블록체인 네트워크를 통해 상기 블록이 수신되면, 상기 데이터 저장부에 저장되어 있는 상기 블록체인 데이터에 상기 블록을 체인으로 연결함으로써, 상기 블록에 대한 저장을 완료하는 단계

를 포함하는 차량용 메시지 관리 장치의 동작 방법.

청구항 7

제6항에 있어서,

상기 등록을 시도하는 단계는

동형 암호화(Homomorphic Encryption)를 위한 사전 설정된 암호화키를 이용하여 상기 제1 통신 메시지에 대한 동형 암호화를 수행함으로써, 상기 제1 통신 메시지를 암호화하는 차량용 메시지 관리 장치의 동작 방법.

청구항 8

제7항에 있어서,

상기 블록에 대한 저장이 완료되면, 사전 설정된 백업 서버 - 상기 백업 서버에는 상기 암호화키를 기초로 동형 암호화가 수행된 복수의 통신 메시지들이 사전 저장되어 있음 - 로 상기 암호화된 제1 통신 메시지를 전송하면서, 상기 암호화된 제1 통신 메시지에 대한 저장 요청 명령을 전송하는 단계

를 더 포함하는 차량용 메시지 관리 장치의 동작 방법.

청구항 9

제8항에 있어서,

상기 블록에 대한 저장이 완료된 이후, 사용자에게 의해 상기 블록에 포함되어 있는 상기 암호화된 제1 통신 메시지에 대한 복호화 요청이 수신되면, 상기 블록에 포함된 상기 제1 트랜잭션으로부터 상기 암호화된 제1 통신 메시지와 상기 제1 해시 값 및 상기 제1 전자 서명 값을 추출하는 단계;

상기 개인키에 대응하는 공개키를 기초로 상기 제1 전자 서명 값을 복원하였을 때 생성되는 복원 값이 상기 제1 해시 값과 일치하는지 비교함으로써, 상기 제1 전자 서명 값에 대한 검증을 진행하는 단계;

상기 제1 전자 서명 값에 대한 검증이 완료되면, 상기 백업 서버로, 상기 암호화된 제1 통신 메시지의 복호화를 위한 검증 데이터를 피드백할 것을 요청하는 단계;

상기 백업 서버로부터 상기 검증 데이터로서, 상기 백업 서버에서 생성된 제1 연산 데이터 - 상기 제1 연산 데이터는 상기 백업 서버에 저장되어 있는 상기 암호화된 제1 통신 메시지와 상기 백업 서버에 저장되어 있는 암호화된 제2 통신 메시지가 사전 설정된 제1 동형 연산식에 따라 서로 연산되어 생성된 데이터임 - 와 상기 백업 서버에 저장되어 있는 상기 암호화된 제2 통신 메시지가 피드백되면, 상기 암호화키에 대응되는 사전 설정된 복호화키를 이용하여 상기 제1 연산 데이터를 복호화함으로써, 제1 복호화 값을 생성하는 단계;

상기 제1 트랜잭션으로부터 추출된 상기 암호화된 제1 통신 메시지와 상기 백업 서버로부터 수신된 상기 암호화된 제2 통신 메시지를 각각 상기 복호화키를 이용하여 복호화함으로써, 상기 암호화된 제1 통신 메시지에 대한 제1 복호화 메시지와 상기 암호화된 제2 통신 메시지에 대한 제2 복호화 메시지를 생성하는 단계;

상기 제1 동형 연산식에 대응되는 평문 도메인에서의 제1 연산식에 기초하여 상기 제1 복호화 메시지와 상기 제2 복호화 메시지 간의 연산을 수행함으로써, 평문 연산 데이터를 생성하는 단계; 및

상기 평문 연산 데이터가 상기 제1 복호화 값과 서로 일치하는지 비교하여 상기 평문 연산 데이터가 상기 제1 복호화 값과 일치하는 것으로 확인되면, 상기 제1 복호화 메시지를 상기 암호화된 제1 통신 메시지에 대한 복호화 메시지로서 화면 상에 표시하는 단계

를 더 포함하는 차량용 메시지 관리 장치의 동작 방법.

청구항 10

제9항에 있어서,

상기 백업 서버는

상기 차량용 메시지 관리 장치로부터 상기 검증 데이터의 피드백 요청이 수신되면, 상기 백업 서버에 저장되어 있는 암호화가 수행된 상기 복수의 통신 메시지들 중 어느 하나의 통신 메시지를 상기 암호화된 제2 통신 메시

지로서 랜덤하게 선택한 후, 상기 백업 서버에 저장되어 있는 상기 암호화된 제1 통신 메시지와 상기 백업 서버에 저장되어 있는 상기 암호화된 제2 통신 메시지를 상기 제1 동형 연산식에 따라 서로 연산함으로써, 상기 제1 연산 데이터를 생성하고, 상기 제1 연산 데이터가 생성되면, 상기 제1 연산 데이터와 상기 백업 서버에 저장되어 있는 상기 암호화된 제2 통신 메시지를 상기 차량용 메시지 관리 장치로 피드백하는 것을 특징으로 하는 차량용 메시지 관리 장치의 동작 방법.

청구항 11

제6항 내지 제10항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 컴퓨터 프로그램을 기록한 컴퓨터 판독 가능 기록 매체.

청구항 12

제6항 내지 제10항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램.

발명의 설명

기술 분야

[0001] 본 발명은 블록체인 기반의 차량용 메시지 관리 장치 및 그 동작 방법에 대한 것이다.

배경 기술

[0002] 최근, 차량에 통신 모듈이 탑재되어, 네트워크를 통해 다른 차량들 또는 외부의 교통 시설들과 데이터를 송수신할 수 있는 커넥티드 카에 대한 연구가 지속되고 있다.

[0003] 아울러, 자율 주행 차량에 대한 관심이 증가됨에 따라, 자율 주행 차량에 적용되는 다양한 최신 기술들이 등장하고 있다.

[0004] 이렇게 첨단 기술이 탑재된 차량은 해당 차량이 스스로 주행 환경을 판단하여 차량 주행을 할 것인지 아니면, 멈출 것인지 등을 결정하는 기능을 제공하고 있다는 점에서 차량 주변 환경을 감지하기 위한 다양한 센서들이 탑재되고 있다.

[0005] 이러한 센서들로는 차량 주변에 장애물이 존재하는지 여부를 감지하기 위한 감지 센서, 차량의 현재 위치를 판단하기 위한 GPS 센서 등이 존재하며, 만약 감지 센서가 차량 주변에 장애물이 존재하는 것으로 감지하게 되면, 차량의 감속을 유도하기 위한 센싱 결과 값을 출력하고, 차량 주변에 장애물이 존재하지 않는 것으로 감지하면, 차량의 속도를 유지시키거나 가속을 유도하기 위한 센싱 결과 값을 출력하는 형태로 동작한다.

[0006] 참고로, 이러한 감지 센서들로는 초음파를 이용하여 장애물을 감지하는 초음파 센서, 카메라를 통해 촬영한 영상으로부터 오브젝트 추적을 수행하여 장애물을 감지하는 영상 감지 센서, 레이더(RADAR)를 이용하여 장애물을 감지하는 레이더 센서, 레이저 광을 이용하여 장애물을 감지하는 라이더(LiDAR) 센서 등이 활용되고 있다.

[0007] 네트워크 기능이 탑재된 커넥티드 카는 외부의 데이터 수신 장치와 데이터를 송수신하기 때문에 네트워크를 통한 보안 공격의 위험에 노출될 수 있다. 이로 인해, 커넥티드 카에서의 데이터 보안을 강화하기 위한 보안 기술이 적용될 필요가 있다.

[0008] 아울러, 커넥티드 카에서 외부의 데이터 수신 장치로 전송되는 통신 메시지들은 추후 교통사고가 발생하거나 차량에 문제가 발생하였을 때, 로그 기록으로서 활용될 수 있기 때문에, 데이터의 무결성이 보장될 필요가 있다.

[0009] 이와 관련해서, 최근에는 소정의 데이터를 체인화된 블록으로 구성하여 중앙 서버가 아닌 노드 장치들에 분산 저장함으로써, 해당 데이터에 대한 무결성을 보장할 수 있는 블록체인 기술이 널리 활용되고 있다.

[0010] 블록체인 기술은 데이터를 중앙 서버가 아닌 다수의 노드 장치들에 분산 보관하기 때문에 특정 노드 장치에서 데이터의 변형이 발생하는 경우, 다른 노드 장치들에 저장되어 있는 데이터를 기초로 데이터의 변형이 발생하였는지 여부를 쉽게 검증할 수 있어서, 데이터의 무결성을 보장하는데 최적화된 기술이다.

[0011] 따라서, 커넥티드 카에서 외부의 데이터 수신 장치로 소정의 통신 메시지가 전송될 때마다, 해당 통신 메시지를 블록체인 네트워크 상에 등록해 둬으로써, 통신 메시지에 대한 무결성을 보장하는 기술에 대한 연구가

필요하다.

[0012] 또한, 앞서 언급한 바와 같이, 커넥티드 카에서는 안전 등의 이유로 인해 강력한 보안 체계가 갖추어져야 하기 때문에, 커넥티드 카에서 외부 장치로 전송되는 통신 메시지를 강력한 암호화 방식으로 암호화하여 보관할 필요도 있다.

[0013] 이와 관련해서, 최근에는 차세대 암호화 방식 중 하나로 동형 암호화(Homomorphic Encryption)와 관련된 기술의 관심이 증가하고 있다. 동형 암호화란 암호화된 데이터를 복호화 없이도 암호화된 상태에서 데이터 간의 연산을 수행할 수 있도록 지원하는 암호 기술을 의미한다. 다시 말해서, 동형 암호화란 암호화된 상태에서 연산한 결과 값을 복호화하게 되면, 평문 상태의 데이터를 연산한 결과와 동일한 값을 얻을 수 있도록 하는 암호화 기술을 의미한다.

[0014] 예컨대, A와 B라고 하는 평문 데이터가 존재한다고 하고, A를 동형 암호화하여 생성한 암호화 데이터를 E_A , B를 동형 암호화하여 생성한 암호화 데이터를 E_B 라고 가정하자. 이때, E_A 와 E_B 에 대해 소정의 연산을 수행하여 E_S 라고 하는 연산 값을 산출하였다고 하는 경우, E_S 를 복호화하게 되면 그 복호화 값이 A와 B를 합산하거나 곱셈한 값과 동일하게 되도록 하는 것이 동형 암호화의 기본 개념이다. 즉, 암호화 도메인에서 두 암호화 데이터에 대해 소정의 연산을 수행하여 산출된 값을 복호화하게 되면, 그 복호화 값이 평문 도메인에서 두 평문 데이터를 합산하거나 곱한 값과 일치하게 되도록 하는 암호화를 동형 암호화라고 한다.

[0015] 따라서, 커넥티드 카에서도 통신 메시지를 동형 암호화를 기반으로 암호화하여 보관함으로써, 통신 메시지가 외부로 노출되는 문제를 차단할 수 있는 기술에 대한 연구가 필요하다.

발명의 내용

해결하려는 과제

[0016] 본 발명에 따른 차량용 메시지 관리 장치 및 그 동작 방법은 커넥티드 카에서 소정의 통신 메시지가 전송되는 경우, 상기 통신 메시지를 암호화한 후 상기 통신 메시지에 대한 해시 값과 암호화된 통신 메시지를 블록체인 네트워크를 구성하고 있는 노드 장치들과 연동하여 블록체인 상에 등록함으로써, 상기 통신 메시지에 대한 무결성이 보장될 수 있도록 지원하고자 한다.

과제의 해결 수단

[0017] 본 발명의 일실시예에 따른 블록체인 네트워크를 구성하는 복수의 노드 장치들 중 하나로서, 커넥티드 카(Connected Car)에 탑재되어 상기 커넥티드 카에서 전송되는 통신 메시지를 상기 블록체인 네트워크에 저장하기 위한 블록체인 기반의 차량용 메시지 관리 장치는 복수의 블록들이 체인으로 연결된 블록체인 데이터 - 상기 블록체인 데이터는 상기 복수의 노드 장치들 중 상기 차량용 메시지 관리 장치를 제외한 나머지 노드 장치들에도 저장되어 있음 - 를 저장하고 있는 데이터 저장부, 상기 커넥티드 카에서 제1 통신 메시지가 생성되어 외부의 데이터 수신 장치로 전송된 경우, 사전 설정된 해시 함수에 상기 제1 통신 메시지를 입력으로 인가하여 제1 해시 값을 생성하고, 상기 제1 해시 값을 사전 발급된 개인키로 전자 서명하여 제1 전자 서명 값을 생성하는 전자 서명부, 상기 제1 통신 메시지를 암호화한 후 상기 암호화된 제1 통신 메시지와 상기 제1 해시 값 및 상기 제1 전자 서명 값을 포함하는 제1 트랜잭션을 생성하고, 상기 복수의 노드 장치들 중 상기 차량용 메시지 관리 장치를 제외한 나머지 노드 장치들로 상기 제1 트랜잭션을 전파함으로써, 상기 제1 트랜잭션의 상기 블록체인 네트워크에의 등록을 시도하는 트랜잭션 전파부 및 상기 제1 트랜잭션이 상기 나머지 노드 장치들로 전파된 후 상기 복수의 노드 장치들 중 어느 하나인 제1 노드 장치에서 상기 제1 트랜잭션을 포함하는 $N(N \geq 2)$ 개의 트랜잭션들이 포함된 블록이 생성됨에 따라, 상기 블록체인 네트워크를 통해 상기 블록이 수신되면, 상기 데이터 저장부에 저장되어 있는 상기 블록체인 데이터에 상기 블록을 체인으로 연결함으로써, 상기 블록에 대한 저장을 완료하는 저장 처리부를 포함한다.

[0018] 또한, 본 발명의 일실시예에 따른 블록체인 네트워크를 구성하는 복수의 노드 장치들 중 하나로서, 커넥티드 카에 탑재되어 상기 커넥티드 카에서 전송되는 통신 메시지를 상기 블록체인 네트워크에 저장하기 위한 블록체인 기반의 차량용 메시지 관리 장치의 동작 방법은 복수의 블록들이 체인으로 연결된 블록체인 데이터 - 상기 블록체인 데이터는 상기 복수의 노드 장치들 중 상기 차량용 메시지 관리 장치를 제외한 나머지 노드 장치들에도 저장되어 있음 - 를 저장하고 있는 데이터 저장부를 유지하는 단계, 상기 커넥티드 카에서 제1 통신 메시지가 생성되어 외부의 데이터 수신 장치로 전송된 경우, 사전 설정된 해시 함수에 상기 제1 통신 메시지를 입력으로 인

가하여 제1 해시 값을 생성하고, 상기 제1 해시 값을 사전 발급된 개인키로 전자 서명하여 제1 전자 서명 값을 생성하는 단계, 상기 제1 통신 메시지를 암호화한 후 상기 암호화된 제1 통신 메시지와 상기 제1 해시 값 및 상기 제1 전자 서명 값을 포함하는 제1 트랜잭션을 생성하고, 상기 복수의 노드 장치들 중 상기 차량용 메시지 관리 장치를 제외한 나머지 노드 장치들로 상기 제1 트랜잭션을 전파함으로써, 상기 제1 트랜잭션의 상기 블록체인 네트워크에 등록을 시도하는 단계 및 상기 제1 트랜잭션이 상기 나머지 노드 장치들로 전파된 후 상기 복수의 노드 장치들 중 어느 하나인 제1 노드 장치에서 상기 제1 트랜잭션을 포함하는 N(N은 2이상의 자연수임)개의 트랜잭션들이 포함된 블록이 생성됨에 따라, 상기 블록체인 네트워크를 통해 상기 블록이 수신되면, 상기 데이터 저장부에 저장되어 있는 상기 블록체인 데이터에 상기 블록을 체인으로 연결함으로써, 상기 블록에 대한 저장을 완료하는 단계를 포함한다.

발명의 효과

[0019] 본 발명에 따른 차량용 메시지 관리 장치 및 그 동작 방법은 커넥티드 카에서 소정의 통신 메시지가 전송되는 경우, 상기 통신 메시지를 암호화한 후 상기 통신 메시지에 대한 해시 값과 암호화된 통신 메시지를 블록체인 네트워크를 구성하고 있는 노드 장치들과 연동하여 블록체인 상에 등록함으로써, 상기 통신 메시지에 대한 무결성이 보장될 수 있도록 지원할 수 있다.

도면의 간단한 설명

[0020] 도 1은 본 발명의 일실시예에 따른 차량용 메시지 관리 장치의 구조를 도시한 도면이다.
도 2는 본 발명의 일실시예에 따른 차량용 메시지 관리 장치의 동작 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0021] 이하에서는 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명하기로 한다. 이러한 설명은 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 사용하였으며, 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 본 명세서 상에서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 사람에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다.

[0022] 본 문서에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있다는 것을 의미한다. 또한, 본 발명의 다양한 실시예들에 있어서, 각 구성요소들, 기능 블록들 또는 수단들은 하나 또는 그 이상의 하부 구성요소로 구성될 수 있고, 각 구성요소들이 수행하는 전기, 전자, 기계적 기능들은 전자회로, 집적회로, ASIC(Application Specific Integrated Circuit) 등 공지된 다양한 소자들 또는 기계적 요소들로 구현될 수 있으며, 각각 별개로 구현되거나 2 이상이 하나로 통합되어 구현될 수도 있다.

[0023] 한편, 첨부된 블록도의 블록들이나 흐름도의 단계들은 범용 컴퓨터, 특수용 컴퓨터, 휴대용 노트북 컴퓨터, 네트워크 컴퓨터 등 데이터 프로세싱이 가능한 장비의 프로세서나 메모리에 탑재되어 지정된 기능들을 수행하는 컴퓨터 프로그램 명령들(instructions)을 의미하는 것으로 해석될 수 있다. 이들 컴퓨터 프로그램 명령들은 컴퓨터 장치에 구비된 메모리 또는 컴퓨터에서 판독 가능한 메모리에 저장될 수 있기 때문에, 블록도의 블록들 또는 흐름도의 단계들에서 설명된 기능들은 이를 수행하는 명령 수단을 내포하는 제조물로 생산될 수도 있다. 아울러, 각 블록 또는 각 단계는 특정된 논리적 기능(들)을 실행하기 위한 하나 이상의 실행 가능한 명령들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다. 또, 몇 가지 대체 가능한 실시예들에서는 블록들 또는 단계들에서 언급된 기능들이 정해진 순서와 달리 실행되는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들 또는 단계들은 실질적으로 동시에 수행되거나, 역순으로 수행될 수 있으며, 경우에 따라 일부 블록들 또는 단계들이 생략된 채로 수행될 수도 있다.

[0024] 도 1은 본 발명의 일실시예에 따른 차량용 메시지 관리 장치의 구조를 도시한 도면이다.

[0025] 도 1을 참조하면, 본 발명에 따른 차량용 메시지 관리 장치(110)는 데이터 저장부(111), 전자 서명부(112), 트랜잭션 전파부(113) 및 저장 처리부(114)를 포함한다.

[0026] 먼저, 본 발명에 따른 차량용 메시지 관리 장치(110)는 블록체인 네트워크(100)를 구성하는 복수의 노드 장치들(110, 101, 102, 103, 104) 중 하나로서, 커넥티드 카(Connected Car)에 탑재되어 상기 커넥티드 카에서 전송

되는 통신 메시지를 상기 블록체인 네트워크(100)에 저장하기 위한 동작을 수행한다.

- [0027] 여기서, 차량용 메시지 관리 장치(110)뿐 아니라, 나머지 노드 장치들(101, 102, 103, 104, 105)도 소정의 커넥티드 카에 탑재되어, 커넥티드 카에서 전송되는 통신 메시지를 상기 블록체인 네트워크(100)에 저장하기 위한 동작을 수행하게 된다.
- [0028] 이러한 상황에서, 차량용 메시지 관리 장치(110)의 데이터 저장부(111)에는 복수의 블록들이 체인으로 연결된 블록체인 데이터를 저장하고 있다. 여기서, 상기 블록체인 데이터는 복수의 노드 장치들(110, 101, 102, 103, 104, 105) 중 차량용 메시지 관리 장치(110)를 제외한 나머지 노드 장치들(101, 102, 103, 104, 105)에도 저장되어 있다. 이러한 상기 블록체인 데이터는 복수의 노드 장치들(110, 101, 102, 103, 104, 105)이 각 노드 장치가 탑재된 커넥티드 카로부터 수집한 통신 메시지들을 포함하는 블록들로 구성된다.
- [0029] 전자 서명부(112)는 차량용 메시지 관리 장치(110)가 탑재되어 있는 상기 커넥티드 카에서 제1 통신 메시지가 생성되어 외부의 데이터 수신 장치로 전송된 경우, 사전 설정된 해시 함수에 상기 제1 통신 메시지를 입력으로 인가하여 제1 해시 값을 생성하고, 상기 제1 해시 값을 사전 발급된 개인키로 전자 서명하여 제1 전자 서명 값을 생성한다.
- [0030] 트랜잭션 전파부(113)는 상기 제1 통신 메시지를 암호화한 후 상기 암호화된 제1 통신 메시지와 상기 제1 해시 값 및 상기 제1 전자 서명 값을 포함하는 제1 트랜잭션을 생성하고, 복수의 노드 장치들(110, 101, 102, 103, 104, 105) 중 차량용 메시지 관리 장치(110)를 제외한 나머지 노드 장치들(101, 102, 103, 104, 105)로 상기 제1 트랜잭션을 전파함으로써, 상기 제1 트랜잭션의 상기 블록체인 네트워크에의 등록을 시도한다.
- [0031] 이때, 본 발명의 일실시예에 따르면, 트랜잭션 전파부(113)는 동형 암호화(Homomorphic Encryption)를 위한 사전 설정된 암호화기를 이용하여 상기 제1 통신 메시지에 대한 동형 암호화를 수행함으로써, 상기 제1 통신 메시지를 암호화할 수 있다.
- [0032] 이렇게, 상기 제1 트랜잭션이 나머지 노드 장치들(101, 102, 103, 104, 105)로 전파되면, 블록체인 네트워크(100)를 구성하는 복수의 노드 장치들(110, 101, 102, 103, 104, 105)은 블록체인 네트워크(100)에서 또 다른 트랜잭션이 발생함에 따라 총 N (N 은 2이상의 자연수임)개의 트랜잭션들이 발생할 때, 상기 N 개의 트랜잭션들을 포함하는 블록의 생성을 시도할 수 있다.
- [0033] 만약, 복수의 노드 장치들(110, 101, 102, 103, 104, 105) 중 어느 하나인 제1 노드 장치(101)에서 상기 제1 트랜잭션을 포함하는 상기 N 개 트랜잭션들이 포함된 블록이 생성되었다고 하는 경우, 제1 노드 장치(101)는 상기 블록을 자신의 블록체인 데이터에 체인으로 연결하여 저장한 후 블록체인 네트워크(100)를 통해 상기 블록을 제1 노드 장치(101)를 제외한 나머지 노드 장치들(110, 102, 103, 104, 105)로 전파할 수 있다.
- [0034] 이렇게, 제1 노드 장치(101)에서 상기 제1 트랜잭션을 포함하는 N 개의 트랜잭션들이 포함된 블록이 생성됨에 따라, 상기 블록체인 네트워크(100)를 통해 상기 블록이 차량용 메시지 관리 장치(110)에 수신되면, 저장 처리부(114)는 데이터 저장부(111)에 저장되어 있는 상기 블록체인 데이터에 상기 블록을 체인으로 연결함으로써, 상기 블록에 대한 저장을 완료한다.
- [0035] 이때, 제1 노드 장치(101)로부터 상기 블록을 전파받은 나머지 노드 장치들(102, 103, 104, 105)도 동일하게 상기 블록을 자신의 블록체인 데이터에 체인으로 연결함으로써, 상기 블록에 대한 저장을 완료할 수 있다.
- [0036] 결국, 본 발명에 따른 차량용 메시지 관리 장치(110)는 커넥티드 카에서 소정의 통신 메시지가 전송되는 경우, 상기 통신 메시지를 암호화한 후 상기 통신 메시지에 대한 해시 값과 암호화된 통신 메시지를 블록체인 네트워크(100)를 구성하고 있는 노드 장치들과 연동하여 블록체인 상에 등록함으로써, 상기 통신 메시지에 대한 무결성이 보장될 수 있도록 지원할 수 있다.
- [0037] 본 발명의 일실시예에 따르면, 차량용 메시지 관리 장치(110)는 백업 처리부(115)를 더 포함할 수 있다.
- [0038] 백업 처리부(115)는 저장 처리부(114)를 통해 상기 블록에 대한 저장이 완료되면, 사전 설정된 백업 서버(10)로 상기 암호화된 제1 통신 메시지를 전송하면서, 상기 암호화된 제1 통신 메시지에 대한 저장 요청 명령을 전송한다.
- [0039] 이때, 백업 서버(10)는 차량용 메시지 관리 장치(110)로부터 상기 암호화된 제1 통신 메시지와 상기 저장 요청 명령이 수신되면, 상기 암호화된 제1 통신 메시지를 백업 서버(10)의 저장소 상에 저장해 둘 수 있다.
- [0040] 이때, 백업 서버(10)는 차량용 메시지 관리 장치(110)뿐 아니라, 나머지 노드 장치들(101, 102, 103, 104,

105)에서 통신 메시지의 저장을 위한 트랜잭션이 생성됨에 따라, 통신 메시지의 블록체인 네트워크에의 등록 이벤트가 발생하게 되면, 각 노드 장치로부터도 동형 암호화를 위한 상기 사전 설정된 암호화키를 기초로 동형 암호화가 수행된 통신 메시지들을 수신하여 저장소 상에 저장해 둘 수 있다.

[0041] 이로 인해, 백업 서버(10)에는 상기 암호화키를 기초로 동형 암호화가 수행된 복수의 통신 메시지들이 저장되어 있을 수 있다.

[0042] 이때, 본 발명의 일실시예에 따르면, 차량용 메시지 관리 장치(110)는 메시지 추출부(116), 검증 진행부(117), 요청부(118), 제1 복호화부(119), 제2 복호화부(120), 연산부(121) 및 메시지 표시부(122)를 더 포함할 수 있다.

[0043] 메시지 추출부(116)는 저장 처리부(114)를 통해 상기 블록에 대한 저장이 완료되고, 백업 서버(10)에 상기 암호화된 제1 통신 메시지의 저장이 완료된 이후에, 사용자로부터 상기 블록에 포함되어 있는 상기 암호화된 제1 통신 메시지에 대한 복호화 요청이 수신되면, 데이터 저장부(111)에 저장되어 있는 상기 블록체인 데이터로부터 상기 블록을 검색한 후 상기 블록에 포함된 상기 제1 트랜잭션으로부터 상기 암호화된 제1 통신 메시지와 상기 제1 해시 값 및 상기 제1 전자 서명 값을 추출한다.

[0044] 이렇게, 상기 암호화된 제1 통신 메시지와 상기 제1 해시 값 및 상기 제1 전자 서명 값이 추출되면, 검증 진행부(117)는 상기 개인키에 대응하는 공개키를 기초로 상기 제1 전자 서명 값을 복원하였을 때 생성되는 복원 값이 상기 제1 해시 값과 일치하는지 비교함으로써, 상기 제1 전자 서명 값에 대한 검증을 진행한다.

[0045] 관련해서, 검증 진행부(117)는 상기 공개키를 기초로 상기 제1 전자 서명 값을 복호화하여 상기 복원 값을 생성한 후 상기 복원 값과 상기 제1 해시 값을 비교하여, 상기 복원 값이 상기 제1 해시 값과 일치하는 것으로 확인되면, 상기 제1 전자 서명 값에 대한 검증을 성공으로 판정할 수 있다.

[0046] 이렇게, 상기 제1 전자 서명 값에 대한 검증이 완료되면, 요청부(118)는 백업 서버(10)로, 상기 암호화된 제1 통신 메시지의 복호화를 위한 검증 데이터를 피드백할 것을 요청한다.

[0047] 이때, 본 발명의 일실시예에 따르면, 백업 서버(10)는 차량용 메시지 관리 장치(110)로부터 상기 검증 데이터의 피드백 요청이 수신되면, 백업 서버(10)에 저장되어 있는 암호화가 수행된 상기 복수의 통신 메시지들 중 어느 하나의 통신 메시지인 암호화된 제2 통신 메시지를 랜덤하게 선택할 수 있다.

[0048] 그리고 나서, 백업 서버(10)는 백업 서버(10)에 저장되어 있는 상기 암호화된 제1 통신 메시지와 백업 서버(10)에 저장되어 있는 상기 암호화된 제2 통신 메시지를 사전 설정된 제1 동형 연산식에 따라 서로 연산함으로써, 제1 연산 데이터를 생성할 수 있다.

[0049] 여기서, 상기 제1 동형 연산식은 동형 암호화가 수행된 두 데이터 간에 연산을 수행하기 위한 연산식으로, 개발자에 의해 사전 설정될 수 있다. 이러한 제1 동형 연산식은 평문 도메인에서 두 평문 데이터 간에 수행되는 소정의 연산식에 대응되는 결과를 암호화 도메인에서 생성하기 위해서 지정된 연산식을 의미한다. 예컨대, 평문 데이터를 서로 곱하는 곱셈이라는 연산식이 있을 때, 해당 곱셈에 대응되는 동형 곱셈이 존재할 수 있다. 관련해서, 평문 데이터 A, B가 존재하고, A, B가 각각 동형 암호화가 되어, E(A), E(B)라고 하는 암호화 데이터가 생성되었다고 하며, 상기 제1 동형 연산식이 평문 도메인에서의 곱셈에 대응되는 동형 곱셈이라고 하는 경우, 암호화 도메인에서 E(A)와 E(B)를 동형 곱셈하게 되면, ' $E(A) \otimes E(B)$ '라는 연산 결과가 생성될 수 있고, 평문 도메인에서 A와 B를 곱셈하게 되면, ' $A \times B$ '라는 연산 결과가 생성될 수 있다. 이때, ' $E(A) \otimes E(B)$ '를 복호화한 결과는 ' $A \times B$ '와 같아지게 된다. 이러한 관계가 성립할 때, 상기 제1 동형 연산식인 동형 곱셈은 평문 도메인에서의 곱셈에 대응되는 관계가 있다고 말할 수 있다. 여기서, 동형 곱셈은 평문 도메인에서의 곱셈과 같이, 단순히 암호화된 두 데이터를 곱하는 형태의 연산이 수행되는 것은 아니다. 동형 곱셈은 평문 도메인에서의 곱셈과 대응되는 결과를 만들기 위한 동형 연산식이기 때문에, 단순히 암호화된 두 데이터를 곱하는 형태의 연산 과정이 이루어지는 것이 아니라, 동형 암호화의 특성에 따라 곱하기, 더하기, 나누기, 모듈로 연산 등이 복합적으로 수행되는 소정의 연산 알고리즘으로 정의될 수 있다.

[0050] 이렇게, 상기 암호화된 제1 통신 메시지와 상기 암호화된 제2 통신 메시지를 상기 제1 동형 연산식에 따라 서로 연산함으로써, 상기 제1 연산 데이터가 생성되면, 백업 서버(10)는 상기 제1 연산 데이터와 백업 서버(10)에 저장되어 있는 상기 암호화된 제2 통신 메시지를 차량용 메시지 관리 장치(110)로 피드백할 수 있다.

- [0051] 이때, 제1 복호화부(119)는 백업 서버(10)로부터 상기 검증 데이터로서, 백업 서버(10)에서 생성된 상기 제1 연산 데이터와 백업 서버(10)에 저장되어 있는 상기 암호화된 제2 통신 메시지가 피드백되면, 상기 암호화키에 대응되는 사전 설정된 복호화키를 이용하여 상기 제1 연산 데이터를 복호화함으로써, 제1 복호화 값을 생성한다.
- [0052] 제2 복호화부(120)는 상기 제1 트랜잭션으로부터 추출된 상기 암호화된 제1 통신 메시지와 백업 서버(10)로부터 수신된 상기 암호화된 제2 통신 메시지를 각각 상기 복호화키를 이용하여 복호화함으로써, 상기 암호화된 제1 통신 메시지에 대한 제1 복호화 메시지와 상기 암호화된 제2 통신 메시지에 대한 제2 복호화 메시지를 생성한다.
- [0053] 그리고, 연산부(121)는 상기 제1 동형 연산식에 대응되는 평문 도메인에서의 제1 연산식에 기초하여 상기 제1 복호화 메시지와 상기 제2 복호화 메시지 간의 연산을 수행함으로써, 평문 연산 데이터를 생성한다.
- [0054] 그 이후, 메시지 표시부(122)는 상기 평문 연산 데이터가 상기 제1 복호화 값과 서로 일치하는지 비교하여 상기 평문 연산 데이터가 상기 제1 복호화 값과 일치하는 것으로 확인되면, 상기 제1 복호화 메시지를 상기 암호화된 제1 통신 메시지에 대한 복호화 메시지로서 화면 상에 표시한다.
- [0055] 예컨대, 상기 제1 동형 연산식이 $\otimes$ 로 표현되는 동형 곱셈이라고 하고, 상기 제1 동형 연산식에 대응되는 평문 도메인에서의 상기 제1 연산식이 곱셈이라고 하며, 상기 제1 통신 메시지를 'A', 상기 제2 통신 메시지를 'B', 상기 암호화된 제1 통신 메시지를 'E(A)', 암호화된 제2 통신 메시지를 'E(B)'라고 가정하자.
- [0056] 이때, 백업 서버(10)로부터 수신된, 상기 암호화된 제1 통신 메시지인 'E(A)'와 상기 암호화된 제2 통신 메시지인 'E(B)' 간의 상기 제1 동형 연산식에 따라 연산된 상기 제1 연산 데이터는 ' $E(A) \otimes E(B)$ '가 될 수 있고, 상기 제1 통신 메시지(상기 제1 복호화 메시지)인 'A'와 상기 제2 통신 메시지(상기 제2 복호화 메시지)인 'B' 간의 상기 제1 연산식에 따라 연산된 평문 연산 데이터는 ' $A \times B$ '가 될 수 있으므로, 메시지 표시부(122)는 상기 제1 연산 데이터인 ' $E(A) \otimes E(B)$ '의 복호화 결과인 상기 제1 복호화 값이 상기 평문 연산 데이터인 ' $A \times B$ '와 일치하는지 여부를 비교할 수 있다.
- [0057] 만약, 상기 제1 연산 데이터인 ' $E(A) \otimes E(B)$ '의 복호화 결과인 상기 제1 복호화 값이 상기 평문 연산 데이터인 ' $A \times B$ '와 일치하는 것으로 확인된다면, 백업 서버(10)에 저장되어 있는 상기 암호화된 제1 통신 데이터와 데이터 저장부(111)에 저장되어 있는 블록체인 데이터로부터 추출된 상기 암호화된 제1 통신 데이터는 서로 동일한 암호화키를 이용하여 정상적으로 동형 암호화가 수행된 데이터가 맞다는 것을 의미하기 때문에, 메시지 표시부(122)는 상기 제1 복호화 메시지를 상기 암호화된 제1 통신 메시지에 대한 복호화 메시지로서 화면 상에 표시할 수 있다.
- [0058] 도 2는 본 발명의 일실시예에 따른 블록체인 네트워크를 구성하는 복수의 노드 장치들 중 하나로서, 커넥티드 카에 탑재되어 상기 커넥티드 카에서 전송되는 통신 메시지를 상기 블록체인 네트워크에 저장하기 위한 블록체인 기반의 차량용 메시지 관리 장치의 동작 방법을 도시한 순서도이다.
- [0059] 단계(S210)에서는 복수의 블록들이 체인으로 연결된 블록체인 데이터(상기 블록체인 데이터는 상기 복수의 노드 장치들 중 상기 차량용 메시지 관리 장치를 제외한 나머지 노드 장치들에도 저장되어 있음)를 저장하고 있는 데이터 저장부를 유지한다.
- [0060] 단계(S220)에서는 상기 커넥티드 카에서 제1 통신 메시지가 생성되어 외부의 데이터 수신 장치로 전송된 경우, 사전 설정된 해시 함수에 상기 제1 통신 메시지를 입력으로 인가하여 제1 해시 값을 생성하고, 상기 제1 해시 값을 사전 발급된 개인키로 전자 서명하여 제1 전자 서명 값을 생성한다.
- [0061] 단계(S230)에서는 상기 제1 통신 메시지를 암호화한 후 상기 암호화된 제1 통신 메시지와 상기 제1 해시 값 및 상기 제1 전자 서명 값을 포함하는 제1 트랜잭션을 생성하고, 상기 복수의 노드 장치들 중 상기 차량용 메시지 관리 장치를 제외한 나머지 노드 장치들로 상기 제1 트랜잭션을 전파함으로써, 상기 제1 트랜잭션의 상기 블록체인 네트워크에의 등록을 시도한다.
- [0062] 단계(S240)에서는 상기 제1 트랜잭션이 상기 나머지 노드 장치들로 전파된 후 상기 복수의 노드 장치들 중 어느 하나인 제1 노드 장치에서 상기 제1 트랜잭션을 포함하는 N(N은 2이상의 자연수임)개의 트랜잭션들이 포함된 블

록이 생성됨에 따라, 상기 블록체인 네트워크를 통해 상기 블록이 수신되면, 상기 데이터 저장부에 저장되어 있는 상기 블록체인 데이터에 상기 블록을 체인으로 연결함으로써, 상기 블록에 대한 저장을 완료한다.

[0063] 이때, 본 발명의 일실시예에 따르면, 단계(S230)에서는 동형 암호화를 위한 사전 설정된 암호화키를 이용하여 상기 제1 통신 메시지에 대한 동형 암호화를 수행함으로써, 상기 제1 통신 메시지를 암호화할 수 있다.

[0064] 이때, 본 발명의 일실시예에 따르면, 상기 차량용 메시지 관리 장치의 동작 방법은 상기 블록에 대한 저장이 완료되면, 사전 설정된 백업 서버(상기 백업 서버에는 상기 암호화키를 기초로 동형 암호화가 수행된 복수의 통신 메시지들이 사전 저장되어 있음)로 상기 암호화된 제1 통신 메시지를 전송하면서, 상기 암호화된 제1 통신 메시지에 대한 저장 요청 명령을 전송하는 단계를 더 포함할 수 있다.

[0065] 또한, 본 발명의 일실시예에 따르면, 상기 차량용 메시지 관리 장치의 동작 방법은 상기 블록에 대한 저장이 완료된 이후, 사용자에게 의해 상기 블록에 포함되어 있는 상기 암호화된 제1 통신 메시지에 대한 복호화 요청이 수신되면, 상기 블록에 포함된 상기 제1 트랜잭션으로부터 상기 암호화된 제1 통신 메시지와 상기 제1 해시 값 및 상기 제1 전자 서명 값을 추출하는 단계, 상기 개인키에 대응하는 공개키를 기초로 상기 제1 전자 서명 값을 복원하였을 때 생성되는 복원 값이 상기 제1 해시 값과 일치하는지 비교함으로써, 상기 제1 전자 서명 값에 대한 검증은 진행되는 단계, 상기 제1 전자 서명 값에 대한 검증이 완료되면, 상기 백업 서버로, 상기 암호화된 제1 통신 메시지의 복호화를 위한 검증 데이터를 피드백할 것을 요청하는 단계, 상기 백업 서버로부터 상기 검증 데이터로서, 상기 백업 서버에서 생성된 제1 연산 데이터(상기 제1 연산 데이터는 상기 백업 서버에 저장되어 있는 상기 암호화된 제1 통신 메시지와 상기 백업 서버에 저장되어 있는 암호화된 제2 통신 메시지가 사전 설정된 제1 동형 연산식에 따라 서로 연산되어 생성된 데이터임)와 상기 백업 서버에 저장되어 있는 상기 암호화된 제2 통신 메시지가 피드백되면, 상기 암호화키에 대응되는 사전 설정된 복호화키를 이용하여 상기 제1 연산 데이터를 복호화함으로써, 제1 복호화 값을 생성하는 단계, 상기 제1 트랜잭션으로부터 추출된 상기 암호화된 제1 통신 메시지와 상기 백업 서버로부터 수신된 상기 암호화된 제2 통신 메시지를 각각 상기 복호화키를 이용하여 복호화함으로써, 상기 암호화된 제1 통신 메시지에 대한 제1 복호화 메시지와 상기 암호화된 제2 통신 메시지에 대한 제2 복호화 메시지를 생성하는 단계, 상기 제1 동형 연산식에 대응되는 평문 도메인에서의 제1 연산식에 기초하여 상기 제1 복호화 메시지와 상기 제2 복호화 메시지 간의 연산을 수행함으로써, 평문 연산 데이터를 생성하는 단계 및 상기 평문 연산 데이터가 상기 제1 복호화 값과 서로 일치하는지 비교하여 상기 평문 연산 데이터가 상기 제1 복호화 값과 일치하는 것으로 확인되면, 상기 제1 복호화 메시지를 상기 암호화된 제1 통신 메시지에 대한 복호화 메시지로서 화면 상에 표시하는 단계를 더 포함할 수 있다.

[0066] 이때, 본 발명의 일실시예에 따르면, 상기 백업 서버는 상기 차량용 메시지 관리 장치로부터 상기 검증 데이터의 피드백 요청이 수신되면, 상기 백업 서버에 저장되어 있는 암호화가 수행된 상기 복수의 통신 메시지들 중 어느 하나의 통신 메시지를 상기 암호화된 제2 통신 메시지로서 랜덤하게 선택한 후, 상기 백업 서버에 저장되어 있는 상기 암호화된 제1 통신 메시지와 상기 백업 서버에 저장되어 있는 상기 암호화된 제2 통신 메시지를 상기 제1 동형 연산식에 따라 서로 연산함으로써, 상기 제1 연산 데이터를 생성하고, 상기 제1 연산 데이터가 생성되면, 상기 제1 연산 데이터와 상기 백업 서버에 저장되어 있는 상기 암호화된 제2 통신 메시지를 상기 차량용 메시지 관리 장치로 피드백할 수 있다.

[0067] 이상, 도 2를 참조하여 본 발명의 일실시예에 따른 차량용 메시지 관리 장치의 동작 방법에 대해 설명하였다. 여기서, 본 발명의 일실시예에 따른 차량용 메시지 관리 장치의 동작 방법은 도 1을 이용하여 설명한 차량용 메시지 관리 장치(110)의 동작에 대한 구성과 대응될 수 있으므로, 이에 대한 보다 상세한 설명은 생략하기로 한다.

[0068] 본 발명의 일실시예에 따른 차량용 메시지 관리 장치의 동작 방법은 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다.

[0069] 또한, 본 발명의 일실시예에 따른 차량용 메시지 관리 장치의 동작 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의

예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0070] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0071] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0072]

110: 차량용 메시지 관리 장치

111: 데이터 저장부 112: 전자 서명부

113: 트랜잭션 전파부 114: 저장 처리부

115: 백업 처리부 116: 메시지 추출부

117: 검증 진행부 118: 요청부

119: 제1 복호화부 120: 제2 복호화부

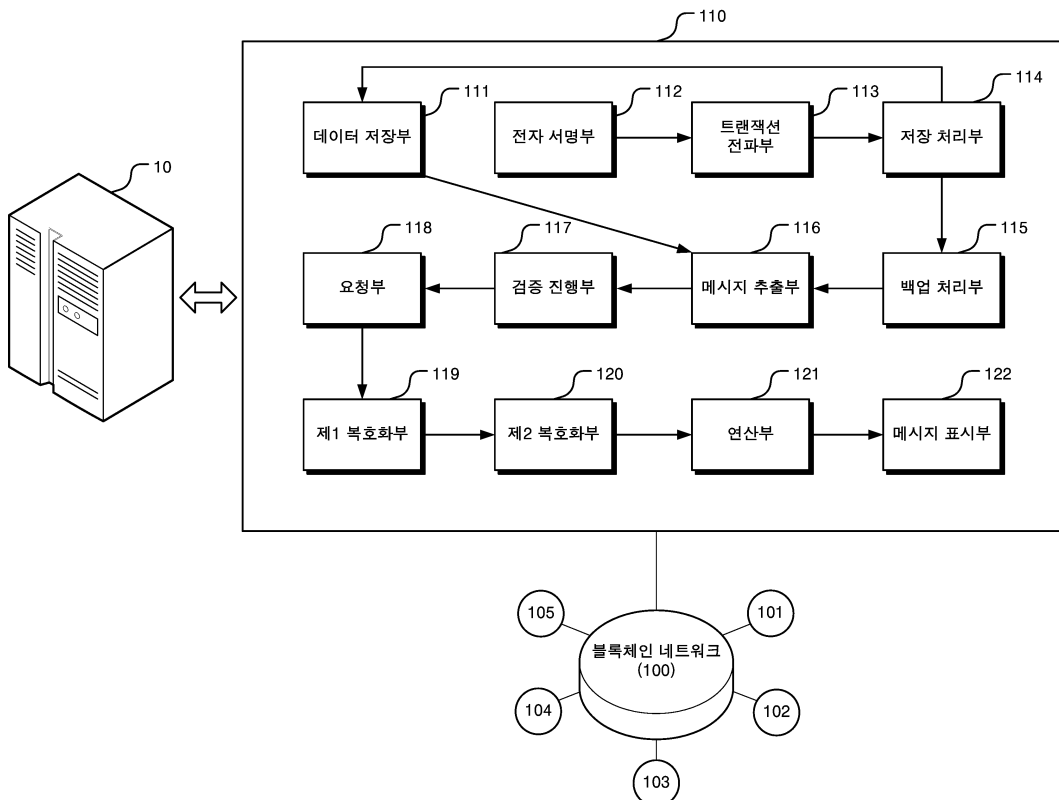
121: 연산부 122: 메시지 표시부

101, 102, 103, 104, 105: 나머지 노드 장치들

10: 백업 서버

도면

도면1



도면2

