(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0128712
(43) 공개일자 2023년09월05일

(51) 국제특허분류(Int. Cl.)
H04L 9/06 (2006.01) *H04L 67/1097* (2022.01)
H04L 9/30 (2006.01) *H04L 9/32* (2006.01)
H04W 4/40 (2018.01)
(52) CPC특허분류
H04L 9/0643 (2013.01)
H04L 67/1097 (2022.05)
(21) 출원번호 10-2022-0025923
(22) 출원일자 2022년02월28일
심사청구일자 2022년02월28일

(71) 출원인
조선대학교산학협력단
광주광역시 동구 필문대로 309 (서석동)
(72) 발명자
김영식
광주광역시 서구 풍암2로 66 금호2차아파트 201동 1005호
(74) 대리인
김효성

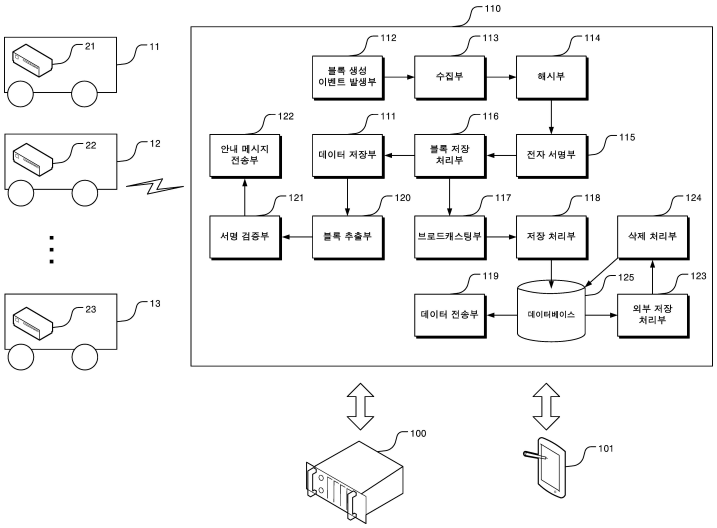
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 **차량에서 생성되는 운행 데이터의 무결성 보장을 위한 블록체인 기반의 데이터 저장 장치 및 그 동작 방법**

(57) 요 약

차량에서 생성되는 운행 데이터의 무결성 보장을 위한 블록체인 기반의 데이터 저장 장치 및 그 동작 방법이 개시된다. 본 발명은 차량에서 생성되는 운행 데이터에 대한 서명 정보를 소정의 블록체인 데이터의 형식으로 구성하여 저장해 둠으로써, 운행 데이터의 무결성을 보장할 수 있는 기술에 대한 것이다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/30 (2023.01)
H04L 9/3247 (2013.01)
H04L 9/50 (2022.05)
H04W 4/40 (2020.05)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711128149
과제번호	2021R1A2C2011082
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	개인기초연구(과기정통부)(R&D)
연구과제명	양자 내성 동형암호기반 스마트카 침입 탐지 시스템 연구
기 여 율	1/1
과제수행기관명	조선대학교
연구기간	2021.03.01 ~ 2022.02.28

명 세 서

청구범위

청구항 1

차량에 탑재되어, 상기 차량에서 생성되는 운행 데이터의 무결성 보장을 위한 블록체인 기반의 데이터 저장 장치에 있어서,

복수의 블록들이 체인으로 연결된 제1 블록체인 데이터를 저장하고 있는 데이터 저장부;

사전 설정된 제1 주기 간격으로, 상기 제1 블록체인 데이터에 연결될 신규 블록을 생성하기 위한 블록 생성 이벤트를 발생시키는 블록 생성 이벤트 발생부;

상기 블록 생성 이벤트가 발생되면, 상기 제1 주기에 해당되는 시간 동안 상기 차량 내부에서 생성되는 운행 데이터를 확보하고, 상기 제1 주기에 해당되는 시간 동안 상기 차량의 주변에 위치하고 있는 다른 차량들 각각에 탑재된 데이터 저장 장치에서 생성되어 브로드캐스팅되는 블록들을 확보하는 수집부;

상기 수집부를 통해, 제1 운행 데이터와 제1 블록들이 확보된 경우, 상기 제1 운행 데이터와 상기 제1 블록들로 구성되는 데이터셋을 사전 설정된 해시 함수에 입력으로 인가하여 제1 해시 값을 생성하는 해시부;

전자 서명을 위한 제1 개인키와 제1 공개키를 생성한 후, 상기 제1 해시 값을 상기 제1 개인키로 전자 서명하여 제1 전자 서명 값을 생성하는 전자 서명부;

상기 제1 해시 값, 상기 제1 전자 서명 값 및 상기 제1 공개키를 포함하는 제1 신규 블록을 생성한 후, 상기 제1 신규 블록을 상기 제1 블록체인 데이터에 체인으로 연결하는 블록 저장 처리부; 및

상기 제1 신규 블록이 상기 제1 블록체인 데이터에 체인으로 연결되면, 상기 제1 신규 블록을, 상기 차량의 주변에 위치하고 있는 다른 차량들에 탑재된 데이터 저장 장치가 수신할 수 있도록 브로드캐스팅하는 브로드캐스팅부

를 포함하는 데이터 저장 장치.

청구항 2

제1항에 있어서,

상기 제1 신규 블록이 브로드캐스팅되면, 운행 데이터들을 저장하기 위해 마련된 데이터베이스 상에, 상기 제1 운행 데이터와 상기 제1 해시 값을 서로 대응시켜 저장하는 저장 처리부; 및

상기 데이터베이스 상에 상기 제1 운행 데이터의 저장이 완료된 이후, 관리자 단말로부터 상기 제1 운행 데이터의 전송 요청이 수신되면, 상기 데이터베이스로부터 상기 제1 운행 데이터를 추출하여 상기 관리자 단말로 전송하는 데이터 전송부

를 더 포함하는 데이터 저장 장치.

청구항 3

제2항에 있어서,

상기 저장 처리부는

상기 제1 신규 블록이 브로드캐스팅되면, 동형 암호화(Homomorphic Encryption)를 위한 사전 설정된 암호화키 - 상기 암호화키에 대응되는 복호화키는 상기 관리자 단말에 사전 저장되어 있음 - 를 이용하여 상기 제1 운행 데이터를 암호화한 후, 상기 데이터베이스 상에, 암호화된 상기 제1 운행 데이터와 상기 제1 해시 값을 서로 대응시켜 저장하고,

상기 데이터 전송부는

상기 관리자 단말로부터 상기 제1 운행 데이터의 전송 요청이 수신되면, 상기 데이터베이스로부터 암호화된 상

기 제1 운행 데이터를 추출한 후, 더미(dummy) 데이터를 랜덤하게 생성하여, 상기 더미 데이터를 상기 암호화키로 암호화하고, 암호화된 상기 제1 운행 데이터와 암호화된 상기 더미 데이터를 사전 설정된 제1 동형 연산식에 따라 동형 연산을 수행함으로써, 제1 동형 연산 데이터를 생성한 후, 상기 제1 동형 연산 데이터와 상기 더미 데이터를 상기 관리자 단말로 전송하며,

상기 관리자 단말은

상기 제1 동형 연산 데이터와 상기 더미 데이터가 수신되면, 상기 복호화키를 이용하여 상기 제1 동형 연산 데이터에 대한 복호화를 수행함으로써, 제1 복호화 데이터를 생성한 후, 상기 제1 동형 연산식에 대응되는 평문 도메인에서의 제1 연산식에 따라 상기 더미 데이터와 서로 연산이 수행되었을 경우에 산출되는 연산 결과가, 상기 제1 복호화 데이터가 되도록 하는 해(solution)를 연산함으로써, 상기 제1 운행 데이터를 복원하는 것을 특징으로 하는 데이터 저장 장치.

청구항 4

제2항에 있어서,

상기 제1 운행 데이터가 상기 관리자 단말로 전송된 이후, 상기 관리자 단말로부터 상기 제1 운행 데이터에 대한 무결성 검증 요청이 수신되면, 상기 데이터베이스로부터 상기 제1 해시 값을 확인한 후, 상기 데이터 저장부에 저장되어 있는 상기 제1 블록체인 데이터로부터, 블록 내에 상기 제1 해시 값을 포함하고 있는 상기 제1 신규 블록을 추출하는 블록 추출부;

상기 제1 신규 블록이 추출되면, 상기 제1 신규 블록에 포함되어 있는 상기 제1 공개키를 기초로 상기 제1 전자 서명 값을 복호화하였을 때 생성되는 결과가 상기 제1 신규 블록에 포함되어 있는 상기 제1 해시 값과 일치하는지 여부 확인함으로써, 상기 제1 전자 서명 값에 대한 검증을 수행하는 서명 검증부; 및

상기 제1 전자 서명 값에 대한 검증이 완료되면, 상기 관리자 단말로, 상기 제1 운행 데이터의 무결성이 보장됨을 알리는 안내 메시지를 전송하는 안내 메시지 전송부

를 더 포함하는 데이터 저장 장치.

청구항 5

제2항에 있어서,

상기 데이터베이스에 저장되어 있는 운행 데이터들의 개수가 사전 설정된 기준 개수를 초과하는지 여부를 확인하여, 상기 기준 개수를 초과하는 것으로 확인되는 경우, 상기 데이터베이스에 저장되어 있는 운행 데이터들을, 사전 설정된 외부 스토리지 서버로 전송함으로써, 상기 데이터베이스에 저장되어 있는 운행 데이터들을 상기 외부 스토리지 서버에 저장하는 외부 저장 처리부; 및

상기 데이터베이스에 저장되어 있는 운행 데이터들이 상기 외부 스토리지 서버에 저장 완료되면, 상기 데이터베이스에 저장되어 있는 운행 데이터들을 삭제하는 삭제 처리부

를 더 포함하는 데이터 저장 장치.

청구항 6

차량에 탑재되어, 상기 차량에서 생성되는 운행 데이터의 무결성 보장을 위한 블록체인 기반의 데이터 저장 장치의 동작 방법에 있어서,

복수의 블록들이 체인으로 연결된 제1 블록체인 데이터를 저장하고 있는 데이터 저장부를 유지하는 단계;

사전 설정된 제1 주기 간격으로, 상기 제1 블록체인 데이터에 연결될 신규 블록을 생성하기 위한 블록 생성 이벤트를 발생시키는 단계;

상기 블록 생성 이벤트가 발생되면, 상기 제1 주기에 해당되는 시간 동안 상기 차량 내부에서 생성되는 운행 데이터를 확보하고, 상기 제1 주기에 해당되는 시간 동안 상기 차량의 주변에 위치하고 있는 다른 차량들 각각에 탑재된 데이터 저장 장치에서 생성되어 브로드캐스팅되는 블록들을 확보하는 단계;

상기 확보하는 단계를 통해, 제1 운행 데이터와 제1 블록들이 확보된 경우, 상기 제1 운행 데이터와 상기 제1 블록들로 구성되는 데이터셋을 사전 설정된 해시 함수에 입력으로 인가하여 제1 해시 값을 생성하는 단계;

전자 서명을 위한 제1 개인키와 제1 공개키를 생성한 후, 상기 제1 해시 값을 상기 제1 개인키로 전자 서명하여 제1 전자 서명 값을 생성하는 단계;

상기 제1 해시 값, 상기 제1 전자 서명 값 및 상기 제1 공개키를 포함하는 제1 신규 블록을 생성한 후, 상기 제1 신규 블록을 상기 제1 블록체인 데이터에 체인으로 연결하는 단계; 및

상기 제1 신규 블록이 상기 제1 블록체인 데이터에 체인으로 연결되면, 상기 제1 신규 블록을, 상기 차량의 주변에 위치하고 있는 다른 차량들에 탑재된 데이터 저장 장치가 수신할 수 있도록 브로드캐스팅하는 단계

를 포함하는 데이터 저장 장치의 동작 방법.

청구항 7

제6항에 있어서,

상기 제1 신규 블록이 브로드캐스팅되면, 운행 데이터들을 저장하기 위해 마련된 데이터베이스 상에, 상기 제1 운행 데이터와 상기 제1 해시 값을 서로 대응시켜 저장하는 단계; 및

상기 데이터베이스 상에 상기 제1 운행 데이터의 저장이 완료된 이후, 관리자 단말로부터 상기 제1 운행 데이터의 전송 요청이 수신되면, 상기 데이터베이스로부터 상기 제1 운행 데이터를 추출하여 상기 관리자 단말로 전송하는 단계

를 더 포함하는 데이터 저장 장치의 동작 방법.

청구항 8

제7항에 있어서,

상기 저장하는 단계는

상기 제1 신규 블록이 브로드캐스팅되면, 동형 암호화(Homomorphic Encryption)를 위한 사전 설정된 암호화키 - 상기 암호화키에 대응되는 복호화키는 상기 관리자 단말에 사전 저장되어 있음 - 를 이용하여 상기 제1 운행 데이터를 암호화한 후, 상기 데이터베이스 상에, 암호화된 상기 제1 운행 데이터와 상기 제1 해시 값을 서로 대응시켜 저장하고,

상기 전송하는 단계는

상기 관리자 단말로부터 상기 제1 운행 데이터의 전송 요청이 수신되면, 상기 데이터베이스로부터 암호화된 상기 제1 운행 데이터를 추출한 후, 더미(dummy) 데이터를 랜덤하게 생성하여, 상기 더미 데이터를 상기 암호화키로 암호화하고, 암호화된 상기 제1 운행 데이터와 암호화된 상기 더미 데이터를 사전 설정된 제1 동형 연산식에 따라 동형 연산을 수행함으로써, 제1 동형 연산 데이터를 생성한 후, 상기 제1 동형 연산 데이터와 상기 더미 데이터를 상기 관리자 단말로 전송하며,

상기 관리자 단말은

상기 제1 동형 연산 데이터와 상기 더미 데이터가 수신되면, 상기 복호화키를 이용하여 상기 제1 동형 연산 데이터에 대한 복호화를 수행함으로써, 제1 복호화 데이터를 생성한 후, 상기 제1 동형 연산식에 대응되는 평문 도메인에서의 제1 연산식에 따라 상기 더미 데이터와 서로 연산이 수행되었을 경우에 산출되는 연산 결과가, 상기 제1 복호화 데이터가 되도록 하는 해(solution)를 연산함으로써, 상기 제1 운행 데이터를 복원하는 것을 특징으로 하는 데이터 저장 장치의 동작 방법.

청구항 9

제7항에 있어서,

상기 제1 운행 데이터가 상기 관리자 단말로 전송된 이후, 상기 관리자 단말로부터 상기 제1 운행 데이터에 대한 무결성 검증 요청이 수신되면, 상기 데이터베이스로부터 상기 제1 해시 값을 확인한 후, 상기 데이터 저장부에 저장되어 있는 상기 제1 블록체인 데이터로부터, 블록 내에 상기 제1 해시 값을 포함하고 있는 상기 제1 신규 블록을 추출하는 단계;

상기 제1 신규 블록이 추출되면, 상기 제1 신규 블록에 포함되어 있는 상기 제1 공개키를 기초로 상기 제1 전자

서명 값을 복호화하였을 때 생성되는 결과가 상기 제1 신규 블록에 포함되어 있는 상기 제1 해시 값과 일치하는지 여부 확인함으로써, 상기 제1 전자 서명 값에 대한 검증을 수행하는 단계; 및

상기 제1 전자 서명 값에 대한 검증이 완료되면, 상기 관리자 단말로, 상기 제1 운행 데이터의 무결성이 보장됨을 알리는 안내 메시지를 전송하는 단계

를 더 포함하는 데이터 저장 장치의 동작 방법.

청구항 10

제7항에 있어서,

상기 데이터베이스에 저장되어 있는 운행 데이터들의 개수가 사전 설정된 기준 개수를 초과하는지 여부를 확인하여, 상기 기준 개수를 초과하는 것으로 확인되는 경우, 상기 데이터베이스에 저장되어 있는 운행 데이터들을, 사전 설정된 외부 스토리지 서버로 전송함으로써, 상기 데이터베이스에 저장되어 있는 운행 데이터들을 상기 외부 스토리지 서버에 저장하는 단계; 및

상기 데이터베이스에 저장되어 있는 운행 데이터들이 상기 외부 스토리지 서버에 저장 완료되면, 상기 데이터베이스에 저장되어 있는 운행 데이터들을 삭제하는 단계

를 더 포함하는 데이터 저장 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

기 술 분 야

[0001] 본 발명은 차량에 탑재되어, 상기 차량에서 생성되는 운행 데이터의 무결성 보장을 위한 블록체인 기반의 데이터 저장 장치 및 그 동작 방법에 대한 것이다.

배 경 기 술

[0002] 차량에 있어서, 주행 기록이나 운행 중 발생한 다양한 이벤트와 관련된 운행 데이터는 사고 발생시의 책임소재 확인이나 중고 차량의 판매에 있어서, 매우 중요한 데이터라는 점에서, 데이터에 조작이 발생하면 안되는 무결성이 보장되어야 하는 데이터이다.

[0003] 따라서, 차량에서 생성되는 운행 데이터의 무결성을 보장할 수 있는 기술에 대한 연구가 필요하다.

[0004] 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.

[0005] 이러한 블록체인 기술에서, 블록체인 데이터는, 블록체인 데이터를 구성하는 각 블록의 해시 값을 기초로 블록들을 서로 체인으로 연결한 데이터라는 점에서, 블록의 위조나 변조가 불가능하다는 장점을 가지고 있다. 즉, 현재 블록의 블록 헤더에는 이전 블록의 블록 해시 값이 포함되어 있고, 각 블록은 이전 블록의 블록 해시 값을 참조로 하여, 서로 연결되어 있다는 점에서, 블록체인 데이터에서 특정 블록만을 수정하는 것은 불가능하다고 볼 수 있다.

[0006] 따라서, 차량에서 생성되는 운행 데이터에 대한 서명 정보를 소정의 블록체인 데이터의 형식으로 구성하여 저장해 둠으로써, 운행 데이터의 무결성을 보장할 수 있는 기술의 도입을 고려할 수 있다.

발명의 내용

해결하려는 과제

[0007] 본 발명은 차량에서 생성되는 운행 데이터에 대한 서명 정보를 소정의 블록체인 데이터의 형식으로 구성하여 저장해 둠으로써, 운행 데이터의 무결성을 보장할 수 있는 기술을 제시하고자 한다.

과제의 해결 수단

[0008] 본 발명의 일실시예에 따른, 차량에 탑재되어, 상기 차량에서 생성되는 운행 데이터의 무결성 보장을 위한 블록체인 기반의 데이터 저장 장치는 복수의 블록들이 체인으로 연결된 제1 블록체인 데이터를 저장하고 있는 데이터 저장부, 사전 설정된 제1 주기 간격으로, 상기 제1 블록체인 데이터에 연결될 신규 블록을 생성하기 위한 블록 생성 이벤트를 발생시키는 블록 생성 이벤트 발생부, 상기 블록 생성 이벤트가 발생되면, 상기 제1 주기에 해당되는 시간 동안 상기 차량 내부에서 생성되는 운행 데이터를 확보하고, 상기 제1 주기에 해당되는 시간 동안 상기 차량의 주변에 위치하고 있는 다른 차량들 각각에 탑재된 데이터 저장 장치에서 생성되어 브로드캐스팅되는 블록들을 확보하는 수집부, 상기 수집부를 통해, 제1 운행 데이터와 제1 블록들이 확보된 경우, 상기 제1 운행 데이터와 상기 제1 블록들로 구성되는 데이터셋을 사전 설정된 해시 함수에 입력으로 인가하여 제1 해시 값을 생성하는 해시부, 전자 서명을 위한 제1 개인키와 제1 공개키를 생성한 후, 상기 제1 해시 값을 상기 제1 개인키로 전자 서명하여 제1 전자 서명 값을 생성하는 전자 서명부, 상기 제1 해시 값, 상기 제1 전자 서명 값 및 상기 제1 공개키를 포함하는 제1 신규 블록을 생성한 후, 상기 제1 신규 블록을 상기 제1 블록체인 데이터에 체인으로 연결하는 블록 저장 처리부 및 상기 제1 신규 블록이 상기 제1 블록체인 데이터에 체인으로 연결되면, 상기 제1 신규 블록을, 상기 차량의 주변에 위치하고 있는 다른 차량들에 탑재된 데이터 저장 장치가 수신할 수 있도록 브로드캐스팅하는 브로드캐스팅부를 포함한다.

[0009] 또한, 본 발명의 일실시예에 따른, 차량에 탑재되어, 상기 차량에서 생성되는 운행 데이터의 무결성 보장을 위한 블록체인 기반의 데이터 저장 장치의 동작 방법은 복수의 블록들이 체인으로 연결된 제1 블록체인 데이터를 저장하고 있는 데이터 저장부를 유지하는 단계, 사전 설정된 제1 주기 간격으로, 상기 제1 블록체인 데이터에 연결될 신규 블록을 생성하기 위한 블록 생성 이벤트를 발생시키는 단계, 상기 블록 생성 이벤트가 발생되면, 상기 제1 주기에 해당되는 시간 동안 상기 차량 내부에서 생성되는 운행 데이터를 확보하고, 상기 제1 주기에 해당되는 시간 동안 상기 차량의 주변에 위치하고 있는 다른 차량들 각각에 탑재된 데이터 저장 장치에서 생성되어 브로드캐스팅되는 블록들을 확보하는 단계, 상기 확보하는 단계를 통해, 제1 운행 데이터와 제1 블록들이 확보된 경우, 상기 제1 운행 데이터와 상기 제1 블록들로 구성되는 데이터셋을 사전 설정된 해시 함수에 입력으로 인가하여 제1 해시 값을 생성하는 단계, 전자 서명을 위한 제1 개인키와 제1 공개키를 생성한 후, 상기 제1 해시 값을 상기 제1 개인키로 전자 서명하여 제1 전자 서명 값을 생성하는 단계, 상기 제1 해시 값, 상기 제1 전자 서명 값 및 상기 제1 공개키를 포함하는 제1 신규 블록을 생성한 후, 상기 제1 신규 블록을 상기 제1 블록체인 데이터에 체인으로 연결하는 단계 및 상기 제1 신규 블록이 상기 제1 블록체인 데이터에 체인으로 연결되면, 상기 제1 신규 블록을, 상기 차량의 주변에 위치하고 있는 다른 차량들에 탑재된 데이터 저장 장치가 수신할 수 있도록 브로드캐스팅하는 단계를 포함한다.

발명의 효과

[0010] 본 발명은 차량에서 생성되는 운행 데이터에 대한 서명 정보를 소정의 블록체인 데이터의 형식으로 구성하여 저장해 두는 기술을 제시함으로써, 운행 데이터의 무결성을 보장할 수 있다.

도면의 간단한 설명

[0011] 도 1은 본 발명의 일실시예에 따른 데이터 저장 장치의 구조를 도시한 도면이다.

도 2는 본 발명의 일실시예에 따른 데이터 저장 장치의 동작 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0012] 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 이해

되는 것과 동일한 의미를 가지고 있다.

[0013] 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.

[0014] 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.

[0015] 도 1은 본 발명의 일실시예에 따른 데이터 저장 장치의 구조를 도시한 도면이다.

[0016] 도 1을 참조하면, 본 발명에 따른 데이터 저장 장치(110)는 차량에 탑재되어, 상기 차량에서 생성되는 운행 데이터의 무결성 보장을 위한 블록체인 기반의 데이터 저장 장치로서, 데이터 저장부(111), 블록 생성 이벤트 발생부(112), 수집부(113), 해시부(114), 전자 서명부(115) 및 블록 저장 처리부(116)를 포함한다.

[0017] 먼저, 본 발명에서는, 상기 차량 이외의 사전 지정된 다른 차량들(11, 12, 13)에도 본 발명의 데이터 저장 장치(110)와 동일한 구성의 데이터 저장 장치들(21, 22, 23)이 각각 탑재되어 있음을 가정한다.

[0018] 이로 인해, 상기 차량 주변에 존재하는 다른 차량들(11, 12, 13)에 탑재된 데이터 저장 장치들(21, 22, 23)은 본 발명의 데이터 저장 장치(110)와 동일한 동작을 수행하기 때문에, 후술할 내용인 본 발명의 블록 생성 방식에 따라 소정의 블록을 생성하여 브로드캐스팅할 수 있다.

[0019] 데이터 저장부(111)는 복수의 블록들이 체인으로 연결된 제1 블록체인 데이터를 저장하고 있다. 여기서, 상기 복수의 블록들은, 후술할 내용인 본 발명의 블록 생성 방식에 따라 이미 생성이 완료된 블록들을 의미한다.

[0020] 블록 생성 이벤트 발생부(112)는 사전 설정된 제1 주기 간격으로, 상기 제1 블록체인 데이터에 연결될 신규 블록을 생성하기 위한 블록 생성 이벤트를 발생시킨다.

[0021] 수집부(113)는 상기 블록 생성 이벤트가 발생되면, 상기 제1 주기에 해당되는 시간 동안 상기 차량 내부에서 생성되는 운행 데이터를 확보하고, 상기 제1 주기에 해당되는 시간 동안 상기 차량의 주변에 위치하고 있는 다른 차량들(11, 12, 13) 각각에 탑재된 데이터 저장 장치(21, 22, 23)에서 생성되어 브로드캐스팅되는 블록들을 확보한다.

[0022] 여기서, 운행 데이터란, 상기 블록 생성 이벤트가 발생된 시점으로부터 상기 제1 주기에 해당되는 시간 동안의 주행 거리 값, 블랙박스 녹화 영상 데이터, 주행 중 브레이크를 밟았는지, 가속 페달을 밟았는지 등을 지시하는 이벤트 데이터 등을 의미한다.

[0023] 예컨대, 상기 제1 주기가 '5분'이라고 하는 경우, 블록 생성 이벤트 발생부(112)는 '5분' 간격으로, 상기 제1 블록체인 데이터에 연결될 신규 블록을 생성하기 위한 블록 생성 이벤트를 발생시킬 수 있고, 수집부(113)는 상기 블록 생성 이벤트가 발생되면, '5분'에 해당되는 시간 동안 상기 차량 내부에서 생성되는 운행 데이터를 확보하고, '5분'에 해당되는 시간 동안 상기 차량의 주변에 위치하고 있는 다른 차량들(11, 12, 13) 각각에 탑재된 데이터 저장 장치(21, 22, 23)에서 생성되어 브로드캐스팅되는 블록들을 확보할 수 있다.

[0024] 이렇게 수집부(113)를 통해, 상기 제1 주기에 해당되는 시간 동안 상기 차량 내부에서 생성되는 운행 데이터와 다른 차량들(11, 12, 13) 각각에 탑재된 데이터 저장 장치(21, 22, 23)에서 생성되어 브로드캐스팅되는 블록들이 확보된 결과, 제1 운행 데이터와 제1 블록들이 확보된 경우, 해시부(114)는 상기 제1 운행 데이터와 상기 제

1 블록들로 구성되는 데이터셋을 사전 설정된 해시 함수에 입력으로 인가하여 제1 해시 값을 생성한다.

[0025] 전자 서명부(115)는 전자 서명을 위한 제1 개인키와 제1 공개키를 생성한 후, 상기 제1 해시 값을 상기 제1 개인키로 전자 서명하여 제1 전자 서명 값을 생성한다.

[0026] 블록 저장 처리부(116)는 상기 제1 해시 값, 상기 제1 전자 서명 값 및 상기 제1 공개키를 포함하는 제1 신규 블록을 생성한 후, 상기 제1 신규 블록을 상기 제1 블록체인 데이터에 체인으로 연결한다.

[0027] 브로드캐스팅부(117)는 상기 제1 신규 블록이 상기 제1 블록체인 데이터에 체인으로 연결되면, 상기 제1 신규 블록을, 상기 차량의 주변에 위치하고 있는 다른 차량들(11, 12, 13)에 탑재된 데이터 저장 장치(21, 22, 23)가 수신할 수 있도록 브로드캐스팅한다.

[0028] 이때, 다른 차량들(11, 12, 13)에 탑재된 데이터 저장 장치(21, 22, 23)는 본 발명의 데이터 저장 장치(110)로부터 브로드캐스팅되는 상기 제1 신규 블록이 수신되면, 각 데이터 저장 장치(21, 22, 23) 내에서 블록 생성 이벤트가 발생하였다고 하였을 때, 소정의 시간 동안, 각 차량(11, 12, 13) 내부의 운행 데이터와 주변 다른 차량들의 데이터 저장 장치로부터 브로드캐스팅되는 블록들 및 본 발명의 데이터 저장 장치(110)로부터 브로드캐스팅되는 상기 제1 신규 블록을 확보한 후, 이 확보된 데이터셋에 대한 해시 값을 만들고, 그 해시 값에 대한 전자 서명을 수행함으로써, 각 데이터 저장 장치(21, 22, 23)에서의 신규 블록을 생성하여, 각 데이터 저장 장치(21, 22, 23)에 저장되어 있는 블록체인 데이터에 체인으로 연결한 후 다시 이 신규 블록을 브로드캐스팅할 수 있다.

[0029] 이러한 방식으로, 본 발명의 데이터 저장 장치(110)와 다른 차량들(11, 12, 13)의 데이터 저장 장치(21, 22, 23)는 소정 주기 간격으로 자신의 운행 데이터와 주변 차량의 데이터 저장 장치로부터 수신되는 블록들을 확보하고, 확보된 데이터셋에 대한 해시 값을 만든 후 이 해시 값에 대해 전자 서명을 수행함으로써, 신규 블록을 생성하여 각 데이터 저장 장치(110)의 블록체인 데이터에 연결한 후, 이 신규 블록을 주변으로 브로드캐스팅하는 과정을 반복 수행할 수 있다.

[0030] 이를 통해, 본 발명의 데이터 저장 장치(110)와 다른 차량들(11, 12, 13)의 데이터 저장 장치(21, 22, 23)에 저장되어 있는 블록체인 데이터에는 자신의 운행 데이터와 다른 차량들의 블록이 혼재된 데이터에 대한 전자 서명 값이 포함된 블록들이 쌓이게 되기 때문에, 사용자가 임의로 블록을 수정할 수 없게 되고, 이로 인해, 각 블록에 포함된 전자 서명 값을 통해서 운행 데이터에 대한 무결성 보장이 가능해질 수 있다.

[0031] 본 발명의 일실시예에 따르면, 데이터 저장 장치(110)는 저장 처리부(118) 및 데이터 전송부(119)를 더 포함할 수 있다.

[0032] 저장 처리부(118)는 브로드캐스팅부(117)를 통해, 상기 제1 신규 블록이 브로드캐스팅되면, 운행 데이터들을 저장하기 위해 마련된 데이터베이스(125) 상에, 상기 제1 운행 데이터와 상기 제1 해시 값을 서로 대응시켜 저장한다.

[0033] 데이터 전송부(119)는 데이터베이스(125) 상에 상기 제1 운행 데이터의 저장이 완료된 이후, 관리자 단말(101)로부터 상기 제1 운행 데이터의 전송 요청이 수신되면, 데이터베이스(125)로부터 상기 제1 운행 데이터를 추출하여 관리자 단말(101)로 전송한다.

[0034] 이때, 본 발명의 일실시예에 따르면, 저장 처리부(118)는 브로드캐스팅부(117)를 통해, 상기 제1 신규 블록이 브로드캐스팅되면, 동형 암호화(Homomorphic Encryption)를 위한 사전 설정된 암호화키(상기 암호화키에 대응되는 복호화키는 관리자 단말(101)에 사전 저장되어 있음)를 이용하여 상기 제1 운행 데이터를 암호화한 후, 데이터베이스(125) 상에, 암호화된 상기 제1 운행 데이터와 상기 제1 해시 값을 서로 대응시켜 저장할 수 있다.

[0035] 이때, 데이터 전송부(119)는 관리자 단말(101)로부터 상기 제1 운행 데이터의 전송 요청이 수신되면, 데이터베이스(125)로부터 암호화된 상기 제1 운행 데이터를 추출한 후, 더미 데이터를 랜덤하게 생성하여, 상기 더미 데이터를 상기 암호화키로 암호화하고, 암호화된 상기 제1 운행 데이터와 암호화된 상기 더미 데이터를 사전 설정된 제1 동형 연산식에 따라 동형 연산을 수행함으로써, 제1 동형 연산 데이터를 생성한 후, 상기 제1 동형 연산 데이터와 상기 더미 데이터를 관리자 단말(101)로 전송할 수 있다.

[0036] 그러면, 관리자 단말(101)은 데이터 저장 장치(110)로부터 상기 제1 동형 연산 데이터와 상기 더미 데이터가 수신되면, 상기 복호화키를 이용하여 상기 제1 동형 연산 데이터에 대한 복호화를 수행함으로써, 제1 복호화 데이터를 생성한 후, 상기 제1 동형 연산식에 대응되는 평문 도메인에서의 제1 연산식에 따라 상기 더미 데이터와 서로 연산이 수행되었을 경우에 산출되는 연산 결과가, 상기 제1 복호화 데이터가 되도록 하는 해(solution)를

연산함으로써, 상기 제1 운행 데이터를 복원할 수 있다.

[0037] 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.

[0038] 예컨대, A와 B라고 하는 평문 데이터가 존재한다고 하고, A를 동형 암호화하여 생성한 암호화 데이터를 E_A, B를 동형 암호화하여 생성한 암호화 데이터를 E_B라고 가정하자. 이때, E_A와 E_B에 대해 소정의 연산을 수행하여 E_S라고 하는 연산 값을 산출하였다고 하는 경우, E_S를 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.

[0039] 이와 관련해서, 저장 처리부(118)는 브로드캐스팅부(117)를 통해, 상기 제1 신규 블록이 브로드캐스팅되면, 동형 암호화를 위한 사전 설정된 암호화키를 이용하여 상기 제1 운행 데이터를 암호화한 후, 데이터베이스(125) 상에, 암호화된 상기 제1 운행 데이터와 상기 제1 해시 값을 서로 대응시켜 저장해 둘 수 있고, 그 이후, 관리자 단말(101)로부터 데이터 저장 장치(110)에 상기 제1 운행 데이터의 전송 요청이 수신되면, 데이터 전송부(119)는 데이터베이스(125)로부터 암호화된 상기 제1 운행 데이터를 추출한 후, 더미 데이터를 랜덤하게 생성하여, 상기 더미 데이터를 상기 암호화키로 암호화하고, 암호화된 상기 제1 운행 데이터와 암호화된 상기 더미 데이터를 사전 설정된 제1 동형 연산식에 따라 동형 연산을 수행함으로써, 제1 동형 연산 데이터를 생성한 후, 상기 제1 동형 연산 데이터와 상기 더미 데이터를 관리자 단말(101)로 전송할 수 있다.

[0040] 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.

[0041] 관련해서, 상기 제1 동형 연산식이 $\otimes$로 표현되는 동형 곱셈이라고 하고, 상기 제1 동형 연산식에 대응되는 평문 도메인에서의 상기 제1 연산식이 곱셈이라고 하며, 상기 제1 운행 데이터를 'A', 상기 더미 데이터를 'B', 상기 암호화된 제1 운행 데이터를 'E(A)'라고 하면, 데이터 전송부(119)는 데이터베이스(125)로부터 암호화된 상기 제1 운행 데이터인 'E(A)'를 추출하고, 상기 더미 데이터인 'B'를 랜덤하게 생성한 후 상기 더미 데이터를 상기 암호화키로 암호화함으로써, 암호화된 더미 데이터인 'E(B)'를 생성할 수 있다. 그러고 나서, 데이터 전송부(119)는 암호화된 상기 제1 운행 데이터인 'E(A)'와 암호화된 상기 더미 데이터인 'E(B)'를 상기 제1 동형 연산식에 따라 연산함으로써, '$E(A)\otimes E(B)$'라고 하는 제1 동형 연산 데이터를 생성한 후, 상기 제1 동형 연산 데이터인 '$E(A)\otimes E(B)$'와 상기 더미 데이터인 'B'를 관리자 단말(101)로 전송할 수 있다.

[0042] 이렇게, 데이터 전송부(119)를 통해, 관리자 단말(101)에 상기 제1 동형 연산 데이터인 '$E(A)\otimes E(B)$'와 상기 더미 데이터인 'B'가 전송됨에 따라, 관리자 단말(101)에 상기 제1 동형 연산 데이터인 '$E(A)\otimes E(B)$'와 상기 더미 데이터인 'B'가 수신되면, 관리자 단말(101)은 상기 제1 운행 데이터를 복호

화하기 위해서, 우선, 관리자 단말(101)에 저장되어 있는 복호화키를 이용하여 상기 제1 동형 연산 데이터인 '$E(A)\otimes E(B)$'에 대한 복호화를 수행함으로써, 제1 복호화 데이터를 생성할 수 있다. 이때, '$E(A)\otimes E(B)$'는 동형 암호화가 수행된 'E(A)'와 'E(B)'가 서로 동형 곱셈되어 생성된 결과이기 때문에, '$E(A)\otimes E(B)$'에 대한 복호화 값인 상기 제1 복호화 데이터는 평문 도메인에서의 곱셈의 결과인 '$A\times B$'가 될 수 있다.

[0043] 여기서, 'A'는 상기 제1 운행 데이터를 의미하고, 'B'는 상기 더미 데이터를 의미하기 때문에, 관리자 단말(101)은 '$E(A)\otimes E(B)$'로부터 상기 제1 복호화 데이터인 '$A\times B$'가 생성되면, 데이터 저장 장치(110)로부터 수신된 상기 더미 데이터인 'B'를 기초로 '$A\times B$'로부터 상기 제1 운행 데이터인 'A'를 찾아낼 수 있다.

[0044] 구체적으로, 관리자 단말(101)은 상기 제1 연산식인 곱셈에 따라 상기 더미 데이터인 'B'와 서로 연산이 수행되었을 때 산출되는 연산 결과가, 상기 제1 복호화 데이터인 '$A\times B$'가 되도록 하는 해를 연산함으로써, 상기 제1 운행 데이터인 'A'를 복원할 수 있다. 즉, 관리자 단말(101)은 상기 제1 연산식이 곱셈이기 때문에, 상기 더미 데이터인 'B'에 어떤 값을 곱하였을 때 산출되는 결과가 '$A\times B$'가 되도록 하는 해를 연산함으로써, 상기 제1 운행 데이터인 'A'를 복원할 수 있게 된다.

[0045] 본 발명의 일실시예에 따르면, 데이터 저장 장치(110)는 블록 추출부(120), 서명 검증부(121) 및 안내 메시지 전송부(122)를 더 포함할 수 있다.

[0046] 블록 추출부(120)는 상기 제1 운행 데이터가 관리자 단말(101)로 전송된 이후, 관리자 단말(101)로부터 상기 제1 운행 데이터에 대한 무결성 검증 요청이 수신되면, 데이터베이스(125)로부터 상기 제1 해시 값을 확인한 후, 데이터 저장부(111)에 저장되어 있는 상기 제1 블록체인 데이터로부터, 블록 내에 상기 제1 해시 값을 포함하고 있는 상기 제1 신규 블록을 추출한다.

[0047] 관련해서, 전술한 바와 같이, 상기 제1 신규 블록은 블록 내에 상기 제1 해시 값, 상기 제1 전자 서명 값 및 상기 제1 공개키를 포함하고 있기 때문에, 블록 추출부(120)는 상기 제1 해시 값을 기초로 검색을 수행함으로써, 데이터 저장부(111)에 저장되어 있는 상기 제1 블록체인 데이터로부터, 블록 내에 상기 제1 해시 값을 포함하고 있는 상기 제1 신규 블록을 추출할 수 있다.

[0048] 서명 검증부(121)는 상기 제1 신규 블록이 추출되면, 상기 제1 신규 블록에 포함되어 있는 상기 제1 공개키를 기초로 상기 제1 전자 서명 값을 복호화하였을 때 생성되는 결과가 상기 제1 신규 블록에 포함되어 있는 상기 제1 해시 값과 일치하는지 여부 확인함으로써, 상기 제1 전자 서명 값에 대한 검증을 수행한다.

[0049] 관련해서, 전술한 바와 같이, 상기 제1 신규 블록 내에 포함되어 있는 상기 제1 전자 서명 값은 상기 제1 해시 값이 상기 제1 공개키에 대응되는 제1 개인키로 서명되어 생성된 값이기 때문에, 서명 검증부(121)가 상기 제1 신규 블록에 포함되어 있는 상기 제1 공개키를 기초로 상기 제1 전자 서명 값을 복호화하게 되면, 상기 제1 신규 블록에 포함되어 있는 상기 제1 해시 값과 일치하는 값이 산출되게 된다. 이로 인해, 서명 검증부(121)는 상기 제1 신규 블록에 포함되어 있는 상기 제1 전자 서명 값에 대한 검증을 완료할 수 있게 된다.

[0050] 안내 메시지 전송부(122)는 서명 검증부(121)에 의해, 상기 제1 전자 서명 값에 대한 검증이 완료되면, 관리자 단말(101)로, 상기 제1 운행 데이터의 무결성이 보장됨을 알리는 안내 메시지를 전송한다.

[0051] 이를 통해, 관리자는 관리자 단말(101)에 수신된 상기 제1 운행 데이터가 위조되거나 변조되지 않은 무결성이 보장되는 데이터임을 확인할 수 있게 된다.

[0052] 본 발명의 일실시예에 따르면, 데이터 저장 장치(110)는 외부 저장 처리부(123) 및 삭제 처리부(124)를 더 포함할 수 있다.

[0053] 외부 저장 처리부(123)는 데이터베이스(125)에 저장되어 있는 운행 데이터들의 개수가 사전 설정된 기준 개수를 초과하는지 여부를 확인하여, 상기 기준 개수를 초과하는 것으로 확인되는 경우, 데이터베이스(125)에 저장되어 있는 운행 데이터들을, 사전 설정된 외부 스토리지 서버(100)로 전송함으로써, 데이터베이스(125)에 저장되어

있는 운행 데이터들을 외부 스토리지 서버(100)에 저장한다.

[0054] 삭제 처리부(124)는 데이터베이스(125)에 저장되어 있는 운행 데이터들이 외부 스토리지 서버(100)에 저장 완료되면, 데이터베이스(125)에 저장되어 있는 운행 데이터들을 삭제한다.

[0055] 관련해서, 데이터 저장 장치(110)는 차량에 탑재되는 장치로서, 내부의 데이터베이스(125)에 데이터를 저장할 수 있는 용량에 한계가 존재할 수 있기 때문에, 데이터베이스(125)에 저장되는 운행 데이터들의 개수가 소정의 기준 개수를 초과하는 경우, 이 운행 데이터들을 외부 스토리지 서버(100)로 이동시킴으로써, 내부 데이터베이스(125)에 대한 저장 용량 한계 문제를 해소할 수 있다.

[0056] 도 2는 본 발명의 일실시예에 따른, 차량에 탑재되어, 상기 차량에서 생성되는 운행 데이터의 무결성 보장을 위한 블록체인 기반의 데이터 저장 장치의 동작 방법을 도시한 순서도이다.

[0057] 단계(S210)에서는 복수의 블록들이 체인으로 연결된 제1 블록체인 데이터를 저장하고 있는 데이터 저장부를 유지한다.

[0058] 단계(S220)에서는 사전 설정된 제1 주기 간격으로, 상기 제1 블록체인 데이터에 연결될 신규 블록을 생성하기 위한 블록 생성 이벤트를 발생시킨다.

[0059] 단계(S230)에서는 상기 블록 생성 이벤트가 발생되면, 상기 제1 주기에 해당되는 시간 동안 상기 차량 내부에서 생성되는 운행 데이터를 확보하고, 상기 제1 주기에 해당되는 시간 동안 상기 차량의 주변에 위치하고 있는 다른 차량들 각각에 탑재된 데이터 저장 장치에서 생성되어 브로드캐스팅되는 블록들을 확보한다.

[0060] 단계(S240)에서는 단계(S230)을 통해, 제1 운행 데이터와 제1 블록들이 확보된 경우, 상기 제1 운행 데이터와 상기 제1 블록들로 구성되는 데이터셋을 사전 설정된 해시 함수에 입력으로 인가하여 제1 해시 값을 생성한다.

[0061] 단계(S250)에서는 전자 서명을 위한 제1 개인키와 제1 공개키를 생성한 후, 상기 제1 해시 값을 상기 제1 개인키로 전자 서명하여 제1 전자 서명 값을 생성한다.

[0062] 단계(S260)에서는 상기 제1 해시 값, 상기 제1 전자 서명 값 및 상기 제1 공개키를 포함하는 제1 신규 블록을 생성한 후, 상기 제1 신규 블록을 상기 제1 블록체인 데이터에 체인으로 연결한다.

[0063] 단계(S270)에서는 상기 제1 신규 블록이 상기 제1 블록체인 데이터에 체인으로 연결되면, 상기 제1 신규 블록을, 상기 차량의 주변에 위치하고 있는 다른 차량들에 탑재된 데이터 저장 장치가 수신할 수 있도록 브로드캐스팅한다.

[0064] 이때, 본 발명의 일실시예에 따르면, 상기 데이터 저장 장치의 동작 방법은 상기 제1 신규 블록이 브로드캐스팅되면, 운행 데이터들을 저장하기 위해 마련된 데이터베이스 상에, 상기 제1 운행 데이터와 상기 제1 해시 값을 서로 대응시켜 저장하는 단계 및 상기 데이터베이스 상에 상기 제1 운행 데이터의 저장이 완료된 이후, 관리자 단말로부터 상기 제1 운행 데이터의 전송 요청이 수신되면, 상기 데이터베이스로부터 상기 제1 운행 데이터를 추출하여 상기 관리자 단말로 전송하는 단계를 더 포함할 수 있다.

[0065] 이때, 본 발명의 일실시예에 따르면, 상기 저장하는 단계는 상기 제1 신규 블록이 브로드캐스팅되면, 동형 암호화를 위한 사전 설정된 암호화키(상기 암호화키에 대응되는 복호화키는 상기 관리자 단말에 사전 저장되어 있음)를 이용하여 상기 제1 운행 데이터를 암호화한 후, 상기 데이터베이스 상에, 암호화된 상기 제1 운행 데이터와 상기 제1 해시 값을 서로 대응시켜 저장할 수 있고, 상기 전송하는 단계는 상기 관리자 단말로부터 상기 제1 운행 데이터의 전송 요청이 수신되면, 상기 데이터베이스로부터 암호화된 상기 제1 운행 데이터를 추출한 후, 더미 데이터를 랜덤하게 생성하여, 상기 더미 데이터를 상기 암호화키로 암호화하고, 암호화된 상기 제1 운행 데이터와 암호화된 상기 더미 데이터를 사전 설정된 제1 동형 연산식에 따라 동형 연산을 수행함으로써, 제1 동형 연산 데이터를 생성한 후, 상기 제1 동형 연산 데이터와 상기 더미 데이터를 상기 관리자 단말로 전송할 수 있다.

[0066] 이때, 상기 관리자 단말은 상기 제1 동형 연산 데이터와 상기 더미 데이터가 수신되면, 상기 복호화키를 이용하여 상기 제1 동형 연산 데이터에 대한 복호화를 수행함으로써, 제1 복호화 데이터를 생성한 후, 상기 제1 동형 연산식에 대응되는 평문 도메인에서의 제1 연산식에 따라 상기 더미 데이터와 서로 연산이 수행되었을 경우에 산출되는 연산 결과가, 상기 제1 복호화 데이터가 되도록 하는 해를 연산함으로써, 상기 제1 운행 데이터를 복원할 수 있다.

[0067] 또한, 본 발명의 일실시예에 따르면, 상기 데이터 저장 장치의 동작 방법은 상기 제1 운행 데이터가 상기 관리

자 단말로 전송된 이후, 상기 관리자 단말로부터 상기 제1 운행 데이터에 대한 무결성 검증 요청이 수신되면, 상기 데이터베이스로부터 상기 제1 해시 값을 확인한 후, 상기 데이터 저장부에 저장되어 있는 상기 제1 블록체인 데이터로부터, 블록 내에 상기 제1 해시 값을 포함하고 있는 상기 제1 신규 블록을 추출하는 단계, 상기 제1 신규 블록이 추출되면, 상기 제1 신규 블록에 포함되어 있는 상기 제1 공개키를 기초로 상기 제1 전자 서명 값을 복호화하였을 때 생성되는 결과가 상기 제1 신규 블록에 포함되어 있는 상기 제1 해시 값과 일치하는지 여부 확인함으로써, 상기 제1 전자 서명 값에 대한 검증을 수행하는 단계 및 상기 제1 전자 서명 값에 대한 검증이 완료되면, 상기 관리자 단말로, 상기 제1 운행 데이터의 무결성이 보장됨을 알리는 안내 메시지를 전송하는 단계를 더 포함할 수 있다.

[0068] 또한, 본 발명의 일실시예에 따르면, 상기 데이터 저장 장치의 동작 방법은 상기 데이터베이스에 저장되어 있는 운행 데이터들의 개수가 사전 설정된 기준 개수를 초과하는지 여부를 확인하여, 상기 기준 개수를 초과하는 것으로 확인되는 경우, 상기 데이터베이스에 저장되어 있는 운행 데이터들을, 사전 설정된 외부 스토리지 서버로 전송함으로써, 상기 데이터베이스에 저장되어 있는 운행 데이터들을 상기 외부 스토리지 서버에 저장하는 단계 및 상기 데이터베이스에 저장되어 있는 운행 데이터들이 상기 외부 스토리지 서버에 저장 완료되면, 상기 데이터베이스에 저장되어 있는 운행 데이터들을 삭제하는 단계를 더 포함할 수 있다.

[0069] 이상, 도 2를 참조하여 본 발명의 일실시예에 따른 데이터 저장 장치의 동작 방법에 대해 설명하였다. 여기서, 본 발명의 일실시예에 따른 데이터 저장 장치의 동작 방법은 도 1을 이용하여 설명한 데이터 저장 장치(110)의 동작에 대한 구성과 대응될 수 있으므로, 이에 대한 보다 상세한 설명은 생략하기로 한다.

[0070] 본 발명의 일실시예에 따른 데이터 저장 장치의 동작 방법은 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다.

[0071] 또한, 본 발명의 일실시예에 따른 데이터 저장 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.

[0072] 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.

[0073] 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

[0074] 110: 데이터 저장 장치

111: 데이터 저장부 112: 블록 생성 이벤트 발생부

113: 수집부 114: 해시부

115: 전자 서명부 116: 블록 저장 처리부

117: 브로드캐스팅부 118: 저장 처리부

119: 데이터 전송부 120: 블록 추출부

121: 서명 검증부 122: 안내 메시지 전송부

123: 외부 저장 처리부 124: 삭제 처리부

125: 데이터베이스

11, 12, 13: 다른 차량들

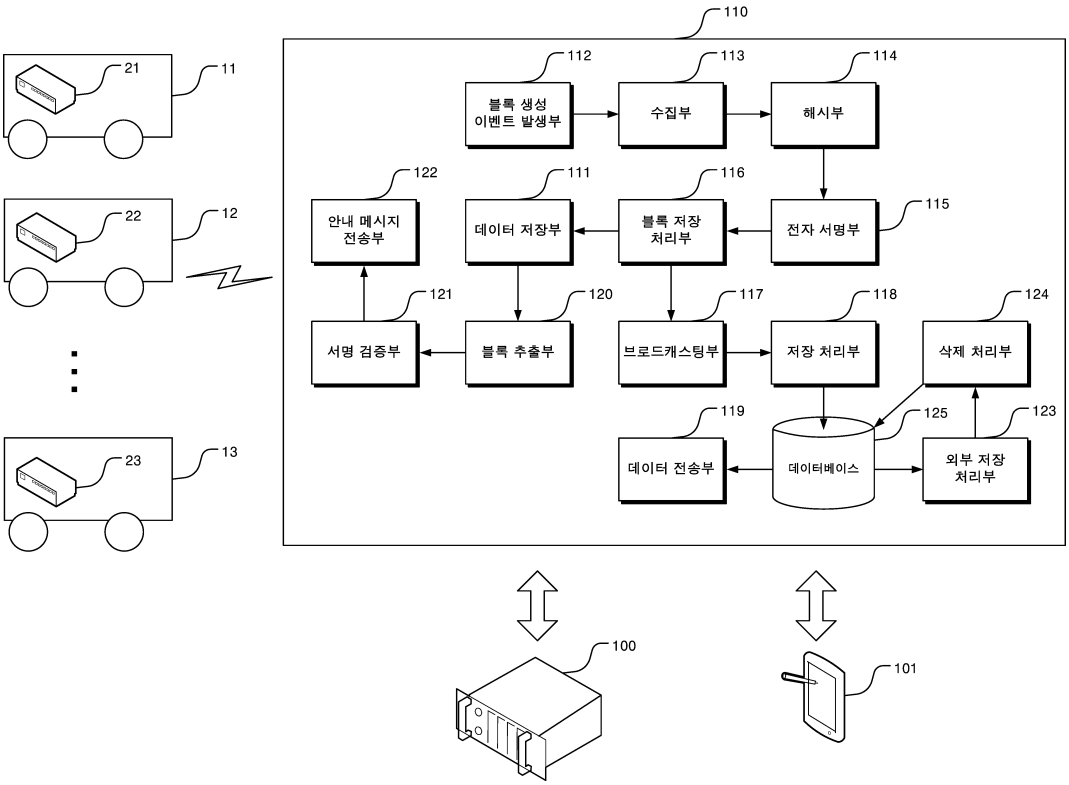
21, 22, 23: 다른 차량들에 탑재된 데이터 저장 장치

101: 관리자 단말

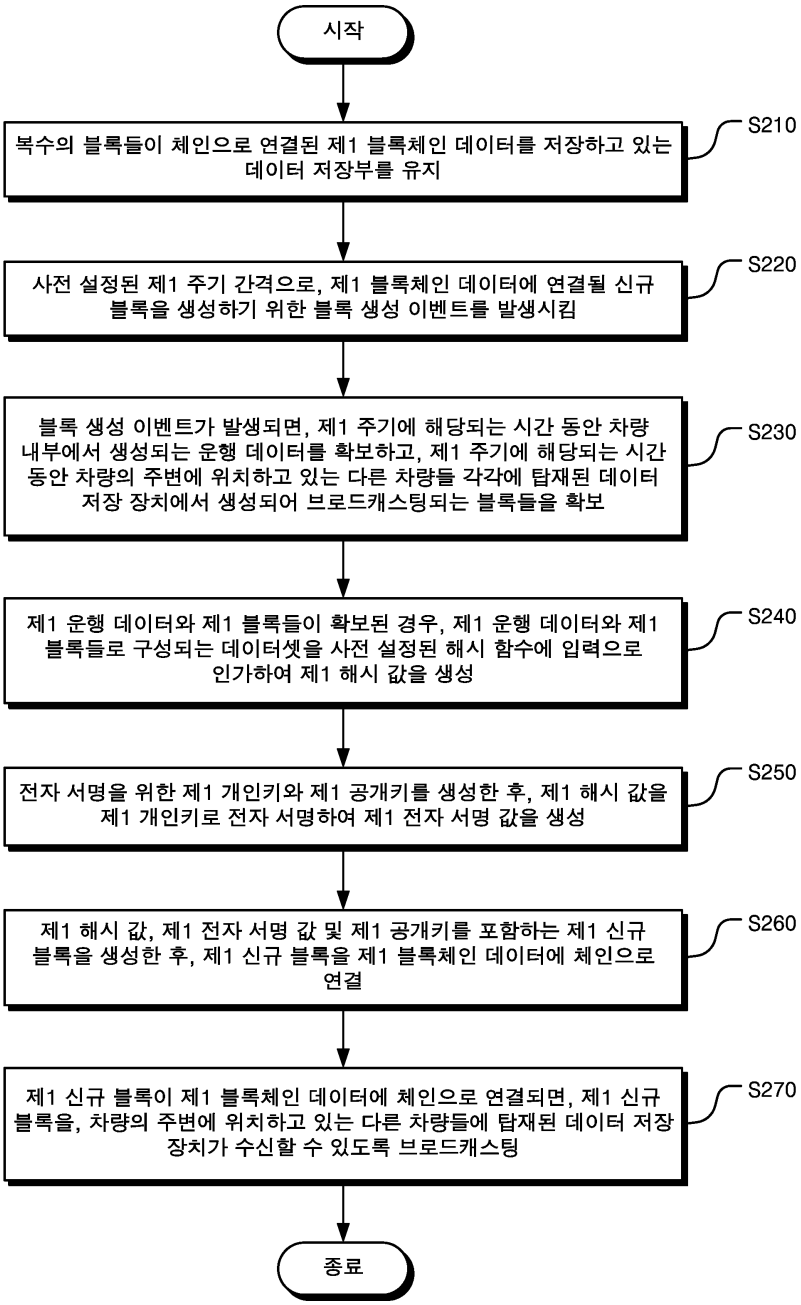
100: 외부 스토리지 서버

도면

도면1



도면2


시작
복수의 블록들이 체인으로 연결된 제1 블록체인 데이터를 저장하고 있는 데이터 저장부를 유지
S210
사전 설정된 제1 주기 간격으로, 제1 블록체인 데이터에 연결될 신규 블록을 생성하기 위한 블록 생성 이벤트를 발생시킴
S220
블록 생성 이벤트가 발생되면, 제1 주기에 해당되는 시간 동안 차량 내부에서 생성되는 운행 데이터를 확보하고, 제1 주기에 해당되는 시간 동안 차량의 주변에 위치하고 있는 다른 차량들 각각에 탑재된 데이터 저장 장치에서 생성되어 브로드캐스팅되는 블록들을 확보
S230
제1 운행 데이터와 제1 블록들이 확보된 경우, 제1 운행 데이터와 제1 블록들로 구성되는 데이터셋을 사전 설정된 해시 함수에 입력으로 인가하여 제1 해시 값을 생성
S240
전자 서명을 위한 제1 개인키와 제1 공개키를 생성한 후, 제1 해시 값을 제1 개인키로 전자 서명하여 제1 전자 서명 값을 생성
S250
제1 해시 값, 제1 전자 서명 값 및 제1 공개키를 포함하는 제1 신규 블록을 생성한 후, 제1 신규 블록을 제1 블록체인 데이터에 체인으로 연결
S260
제1 신규 블록이 제1 블록체인 데이터에 체인으로 연결되면, 제1 신규 블록을, 차량의 주변에 위치하고 있는 다른 차량들에 탑재된 데이터 저장 장치가 수신할 수 있도록 브로드캐스팅
S270
종료