(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0034091
(43) 공개일자 2020년03월31일

(51) 국제특허분류(Int. Cl.)
G06Q 50/30 (2012.01) *G06Q 10/10* (2012.01)
(52) CPC특허분류
G06Q 50/30 (2013.01)
G06Q 10/10 (2013.01)
(21) 출원번호 10-2018-0113342
(22) 출원일자 2018년09월21일
심사청구일자 2018년09월21일

(71) 출원인
비벡 소니
대한민국 16670 경기도 수원시 권선구 동수원로146번길 300-10, 501호
(72) 발명자
비벡 소니
대한민국 16670 경기도 수원시 권선구 동수원로146번길 300-10, 501호
(74) 대리인
이대호, 박건홍

전체 청구항 수 : 총 12 항

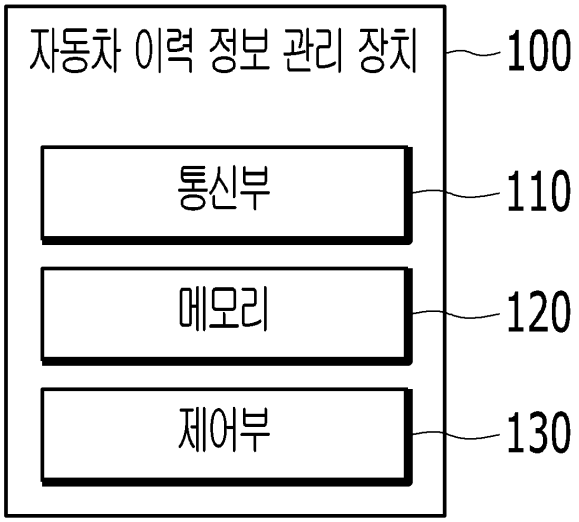
(54) 발명의 명칭 **자동차 이력 정보 관리 컴퓨터 프로그램 및 장치**

(57) 요 약

본 개시의 일 실시예에 따른, 컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램이 개시된다. 상기 컴퓨터 프로그램은 프로세서에 의해 실행되는 경우, 프로세서로 하여금 이하의 동작들을 수행하도록 하기 위한 명령들을 포함하며, 상기 동작들은: 자동차 시스템으로부터 자동차 식별 정보를 수신하는 동작; 상기 자동차 식별 정보 및

(뒷면에 계속)

대 표 도 - 도4



메모리에 저장된 이력 정보 수신 권한 키를 이용하여 자동차 이력 정보 전송 요청 신호를 생성하는 동작; 블록체인 네트워크에 상기 자동차 이력 정보 전송 요청 신호를 전송하는 동작; 상기 자동차 식별 정보에 대응되는 자동차 이력 정보를 블록체인 네트워크에서 수신하는 동작; 상기 블록체인 네트워크에서 수신한 상기 자동차 이력 정보를 상기 메모리에 저장하는 동작; 기 설정된 조건을 만족한 경우, 자동차 활동 정보를 상기 자동차 시스템으로부터 수신하는 동작; 상기 자동차 활동 정보를 수신함에 따라, 상기 블록체인 네트워크에 저장된 상기 자동차 이력 정보를 상기 자동차 활동 정보에 기초하여 업데이트하는 명령 코드 및 상기 명령 코드를 제 1 개인키로 암호화한 서명 데이터를 포함하는 제 1 트랜잭션을 생성하는 동작; 및 상기 제 1 트랜잭션 및 상기 제 1 개인키에 대응되는 제 1 공개키를 블록체인 네트워크에 전송하는 동작을 포함할 수 있다.

명 세 서

청구범위

청구항 1

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램으로서,

상기 컴퓨터 프로그램은 프로세서에 의해 실행되는 경우, 프로세서로 하여금 이하의 동작들을 수행하도록 하기 위한 명령들을 포함하며, 상기 동작들은:

자동차 시스템으로부터 자동차 식별 정보를 수신하는 동작;

상기 자동차 식별 정보 및 메모리에 저장된 이력 정보 수신 권한 키를 이용하여 자동차 이력 정보 전송 요청 신호를 생성하는 동작;

블록체인 네트워크에 상기 자동차 이력 정보 전송 요청 신호를 전송하는 동작;

상기 자동차 식별 정보에 대응되는 자동차 이력 정보를 블록체인 네트워크에서 수신하는 동작;

상기 블록체인 네트워크에서 수신한 상기 자동차 이력 정보를 상기 메모리에 저장하는 동작;

기 설정된 조건을 만족한 경우, 자동차 활동 정보를 상기 자동차 시스템으로부터 수신하는 동작;

상기 자동차 활동 정보를 수신함에 따라, 상기 블록체인 네트워크에 저장된 상기 자동차 이력 정보를 상기 자동차 활동 정보에 기초하여 업데이트하는 명령 코드 및 상기 명령 코드를 제 1 개인키로 암호화한 서명 데이터를 포함하는 제 1 트랜잭션을 생성하는 동작; 및

상기 제 1 트랜잭션 및 상기 제 1 개인키에 대응되는 제 1 공개키를 블록체인 네트워크에 전송하는 동작;

을 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 2

제 1 항에 있어서,

상기 자동차 활동 정보는,

주행 거리, 주행 회수, 주유 내역, 주행 중 발생한 문제 내역 및 주차 중 발생한 문제 내역 중 적어도 하나를 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 3

제 1항에 있어서,

관리자 단말로부터 자동차 관리 정보를 수신한 경우, 상기 자동차 관리 정보가 유효한지 여부를 결정하는 동작;

상기 자동차 관리 정보가 유효한 경우, 상기 블록체인 네트워크에 저장된 상기 자동차 이력 정보를 상기 자동차 관리 정보에 기초하여 업데이트하는 명령 코드 및 상기 명령 코드를 제 2 개인키로 암호화한 서명 데이터를 포함하는 제 2 트랜잭션을 생성하는 동작; 및

상기 제 2 트랜잭션 및 상기 제 2 개인키에 대응되는 제 2 공개키를 블록체인 네트워크에 전송하는 동작;

을 더 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 4

제 3 항에 있어서,

상기 자동차 관리 정보는,

유통업체 정보, 수입업체 정보, 정부 인증 정보, 자동차를 수리한 엔지니어 정보, 변경된 부품 내역 정보, 추가된 부품 내역 정보 및 수리한 부품 내역 정보 중 적어도 하나를 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 5

제 1 항에 있어서,

소유자 단말로부터 소유권 관련 정보를 수신한 경우, 상기 소유권 관련 정보가 유효한지 결정하는 동작;

상기 소유권 관련 정보가 유효한 경우, 상기 블록체인 네트워크에 저장된 상기 자동차 이력 정보를 상기 소유권 관련 정보에 기초하여 업데이트하는 명령 코드 및 상기 명령 코드를 제 3 개인키로 암호화한 서명 데이터를 포함하는 제 3 트랜잭션을 생성하는 동작; 및

상기 제 3 트랜잭션 및 상기 제 3 개인키에 대응되는 제 3 공개키를 블록체인 네트워크에 전송하는 동작;

을 더 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 6

제 5 항에 있어서,

상기 소유권 관련 정보는,

개인 인증 정보 변경 정보, 소유권 이전 정보, 자동차 대여 정보, 자동차 관리 접수 정보, 자동차 이력 조회 허용 정보 및 도난 신고 정보 중 적어도 하나를 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 7

제 1 항에 있어서,

조회자 단말로부터 자동차 이력 정보 조회 요청 신호를 수신한 경우, 상기 자동차 이력 정보 조회 요청 신호가 유효한지 결정하는 동작; 및

상기 자동차 이력 정보 조회 요청 신호가 유효한 경우, 상기 조회자 단말에 상기 자동차 이력 정보를 전송하는 동작;

을 더 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 8

제 1 항에 있어서,

상기 메모리에 저장된 자동차 이력 정보에 기초하여, 자동차 정기 검진 조건이 만족되는지 여부를 결정하는 동작; 및

상기 자동차 정기 검진 조건을 만족하는 경우, 소유자 단말에 자동차 정기 검진 권유 정보를 전송하는 동작;

을 더 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 9

제 1 항에 있어서,

상기 메모리에 저장된 자동차 이력 정보에 운행 금지 관련 정보가 포함되어 있는 경우, 상기 운행 금지 관련 정보가 유효한지 결정하는 동작;

상기 운행 금지 관련 정보가 유효한 경우, 상기 자동차 시스템에 운행 금지 요청 정보를 전송하는 동작;

을 더 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 10

제 1 항에 있어서,

상기 기 설정된 조건은,

기 설정된 시간이 경과한 경우 만족되는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 11

제 1 항에 있어서,

상기 기 설정된 조건은,

기 설정된 이벤트가 발생한 경우 만족되는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 12

자동차 이력 정보 관리 장치에 있어서,

자동차 시스템으로부터 자동차 식별 정보를 수신하고, 상기 자동차 식별 정보 및 메모리에 저장된 이력 정보 수신 권한 키를 이용하여 자동차 이력 정보 전송 요청 신호를 생성하고, 블록체인 네트워크에 상기 자동차 이력 정보 전송 요청 신호를 전송하고, 상기 자동차 식별 정보에 대응되는 자동차 이력 정보를 블록체인 네트워크에서 수신하고 기 설정된 조건을 만족한 경우, 자동차 활동 정보를 상기 자동차 시스템으로부터 수신하고, 제 1 트랜잭션 및 제 1 개인키에 대응되는 제 1 공개키를 블록체인 네트워크에 전송하는 통신부;

상기 블록체인 네트워크에서 수신한 상기 자동차 이력 정보를 저장하는 메모리; 및

상기 자동차 활동 정보를 수신함에 따라, 상기 블록체인 네트워크에 저장된 상기 자동차 이력 정보를 상기 자동차 활동 정보에 기초하여 업데이트하는 명령 코드 및 상기 명령 코드를 상기 제 1 개인키로 암호화한 서명 데이터를 포함하는 상기 제 1 트랜잭션을 생성하는 제어부;

를 포함하는,

자동차 이력 정보 관리 장치.

발명의 설명

기 술 분 야

[0001] 본 개시는 자동차 이력 정보 관리 컴퓨터 프로그램 및 장치에 관한 것으로서, 구체적으로 블록체인 네트워크를 이용하여 자동차 이력 정보를 관리하는 자동차 이력 정보 관리 컴퓨터 프로그램 및 장치에 관한 것이다.

배 경 기 술

[0002] 현대 사회에 있어서, 자동차는 단순히 이동수단에 그치는 것이 아니라, 자신의 사회, 경제적 위치를 나타내는 것으로도 활용되고 있다. 이에 따라 자동차는 높은 재산적 가치는 가지고 있다.

[0003] 이러한 높은 재산적 가치를 가지는 자동차들은 매년 범죄로 인해 도난당하고 있으며, 중고차 거래 시장에서는 사고 이력을 숨긴 상태 자동차를 정상적인 자동차인 것처럼 속여서 거래하거나, 실제로 팔지 않는 자동차를 마치 파는 것처럼 속이는 허위매물이 존재하고 있다.

[0004] 종래 기술은 도난방지를 구현하기 위해 차량 식별 번호(Vehicle Identification Number)를 활용하기도 하고, 사고 이력을 숨기지 않도록 하기 위해 성능 기록 점검부를 활용하기도 했다. 그러나, 차량 식별 번호의 경우 자동차 소유자들이 숨겨진 자동차 식별 번호를 확인하기 쉽지 않아 자신의 차량 식별 번호를 잘 모르고 있다. 또한, 자동차를 훔친 자들은 차량 식별 번호의 위치를 잘 알고 있어 쉽게 변경할 수 있기 때문에, 차량 식별 번호는 도난방지에 큰 도움이 되지 못하다. 그리고, 성능 기록 점검부는 자동차에 관한 모든 사항을 다 나타내는 것 아니기 때문에 성능 기록 점검부상 문제가 없는 자동차이더라도 침수 이력이 있는 자동차일 수 있는 등 사고이력을 숨기는 것에 대해 방지하지 못하는 문제점이 존재하고 있다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 대한민국 등록특허공보 10-1878869

발명의 내용

해결하려는 과제

[0006] 본 개시는 전술한 배경기술에 대응하여 안출된 것으로, 자동차 이력 정보 관리 컴퓨터 프로그램 및 장치를 제공하고자 한다.

[0007] 본 개시의 기술적 과제들은 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0008] 전술한 바와 같은 과제를 해결하기 위한 본 개시의 일 실시예에 따라, 컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램을 제공할 수 있다. 상기 컴퓨터 프로그램은 프로세서에 의해 실행되는 경우, 프로세서로 하여금 이하의 동작들을 수행하도록 하기 위한 명령들을 포함하며, 상기 동작들은: 자동차 시스템으로부터 자동차 식별 정보를 수신하는 동작; 상기 자동차 식별 정보 및 메모리에 저장된 이력 정보 수신 권한 키를 이용하여 자동차 이력 정보 전송 요청 신호를 생성하는 동작; 블록체인 네트워크에 상기 자동차 이력 정보 전송 요청 신호를 전송하는 동작; 상기 자동차 식별 정보에 대응되는 자동차 이력 정보를 블록체인 네트워크에서 수신하는 동작; 상기 블록체인 네트워크에서 수신한 상기 자동차 이력 정보를 상기 메모리에 저장하는 동작; 기 설정된 조건을 만족한 경우, 자동차 활동 정보를 상기 자동차 시스템으로부터 수신하는 동작; 상기 자동차 활동 정보를 수신함에 따라, 상기 블록체인 네트워크에 저장된 상기 자동차 이력 정보를 상기 자동차 활동 정보에 기초하여 업데이트하는 명령 코드 및 상기 명령 코드를 제 1 개인키로 암호화한 서명 데이터를 포함하는 제 1 트랜잭션을 생성하는 동작; 및 상기 제 1 트랜잭션 및 상기 제 1 개인키에 대응되는 제 1 공개키를 블록체인 네트워크에 전송하는 동작을 포함할 수 있다.

[0009] 본 개시의 다른 몇몇 실시예에 따르면, 상기 자동차 활동 정보는, 주행 거리, 주행 회수, 주유 내역, 주행 중 발생한 문제 내역 및 주차 중 발생한 문제 내역 중 적어도 하나를 포함할 수 있다.

[0010] 본 개시의 또 다른 몇몇 실시예에 따르면, 관리자 단말로부터 자동차 관리 정보를 수신한 경우, 상기 자동차 관리 정보가 유효한지 여부를 결정하는 동작; 상기 자동차 관리 정보가 유효한 경우, 상기 블록체인 네트워크에 저장된 상기 자동차 이력 정보를 상기 자동차 관리 정보에 기초하여 업데이트하는 명령 코드 및 상기 명령 코드를 제 2 개인키로 암호화한 서명 데이터를 포함하는 제 2 트랜잭션을 생성하는 동작; 및 상기 제 2 트랜잭션 및 상기 제 2 개인키에 대응되는 제 2 공개키를 블록체인 네트워크에 전송하는 동작을 더 포함할 수 있다.

[0011] 본 개시의 또 다른 몇몇 실시예에 따르면, 상기 자동차 관리 정보는, 유통업체 정보, 수입업체 정보, 정부 인증 정보, 자동차를 수리한 엔지니어 정보, 변경된 부품 내역 정보, 추가된 부품 내역 정보 및 수리한 부품 내역 정보 중 적어도 하나를 포함할 수 있다.

[0012] 본 개시의 또 다른 몇몇 실시예에 따르면, 소유자 단말로부터 소유권 관련 정보를 수신한 경우, 상기 소유권 관련 정보가 유효한지 결정하는 동작; 상기 소유권 관련 정보가 유효한 경우, 상기 블록체인 네트워크에 저장된 상기 자동차 이력 정보를 상기 소유권 관련 정보에 기초하여 업데이트하는 명령 코드 및 상기 명령 코드를 제 3 개인키로 암호화한 서명 데이터를 포함하는 제 3 트랜잭션을 생성하는 동작; 및 상기 제 3 트랜잭션 및 상기 제 3 개인키에 대응되는 제 3 공개키를 블록체인 네트워크에 전송하는 동작을 더 포함할 수 있다.

[0013] 본 개시의 또 다른 몇몇 실시예에 따르면, 상기 소유권 관련 정보는, 개인 인증 정보 변경 정보, 소유권 이전 정보, 자동차 대여 정보, 자동차 관리 접수 정보, 자동차 이력 조회 허용 정보 및 도난 신고 정보 중 적어도 하나를 포함할 수 있다.

[0014] 본 개시의 또 다른 몇몇 실시예에 따르면, 조회자 단말로부터 자동차 이력 정보 조회 요청 신호를 수신한 경우, 상기 자동차 이력 정보 조회 요청 신호가 유효한지 결정하는 동작; 및 상기 자동차 이력 정보 조회 요청 신호가 유효한 경우, 상기 조회자 단말에 상기 자동차 이력 정보를 전송하는 동작을 더 포함할 수 있다.

[0015] 본 개시의 또 다른 몇몇 실시예에 따르면, 상기 메모리에 저장된 자동차 이력 정보에 기초하여, 자동차 정기 검진 조건이 만족되는지 여부를 결정하는 동작; 및

[0016] 상기 자동차 정기 검진 조건을 만족하는 경우, 소유자 단말에 자동차 정기 검진 권유 정보를 전송하는 동작을 더 포함할 수 있다.

[0017] 본 개시의 또 다른 몇몇 실시예에 따르면, 상기 메모리에 저장된 자동차 이력 정보에 운행 금지 관련 정보가 포함되어 있는 경우, 상기 운행 금지 관련 정보가 유효한지 결정하는 동작; 상기 운행 금지 관련 정보가 유효한 경우, 상기 자동차 시스템에 운행 금지 요청 정보를 전송하는 동작을 더 포함할 수 있다.

[0018] 본 개시의 또 다른 몇몇 실시예에 따르면, 상기 기 설정된 조건은, 기 설정된 시간이 경과한 경우 만족될 수 있다.

[0019] 본 개시의 또 다른 몇몇 실시예에 따르면, 상기 기 설정된 조건은, 기 설정된 이벤트가 발생한 경우 만족될 수 있다.

[0020] 본 개시의 또 다른 몇몇 실시예에 따르면, 자동차 이력 정보 관리 장치를 제공할 수 있다. 상기 자동차 이력 정보 관리 장치는 자동차 시스템으로부터 자동차 식별 정보를 수신하고, 상기 자동차 식별 정보 및 메모리에 저장된 이력 정보 수신 권한 키를 이용하여 자동차 이력 정보 전송 요청 신호를 생성하고, 블록체인 네트워크에 상기 자동차 이력 정보 전송 요청 신호를 전송하고, 상기 자동차 식별 정보에 대응되는 자동차 이력 정보를 블록체인 네트워크에서 수신하고 기 설정된 조건을 만족한 경우, 자동차 활동 정보를 상기 자동차 시스템으로부터 수신하고, 제 1 트랜잭션 및 제 1 개인키에 대응되는 제 1 공개키를 블록체인 네트워크에 전송하는 통신부; 상기 블록체인 네트워크에서 수신한 상기 자동차 이력 정보를 저장하는 메모리; 및 상기 자동차 활동 정보를 수신함에 따라, 상기 블록체인 네트워크에 저장된 상기 자동차 이력 정보를 상기 자동차 활동 정보에 기초하여 업데이트하는 명령 코드 및 상기 명령 코드를 상기 제 1 개인키로 암호화한 서명 데이터를 포함하는 상기 제 1 트랜잭션을 생성하는 제어부를 포함할 수 있다.

[0021] 본 개시에서 얻을 수 있는 기술적 해결 수단은 이상에서 언급한 해결 수단들로 제한되지 않으며, 언급하지 않은 또 다른 해결 수단들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

발명의 효과

[0022] 본 개시는 자동차 이력 정보 관리 컴퓨터 프로그램 및 장치를 제공할 수 있다.

[0023] 본 개시에서 얻을 수 있는 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0024] 다양한 양상들이 이제 도면들을 참조로 기재되며, 여기서 유사한 참조 번호들은 총괄적으로 유사한 구성요소들을 지칭하는데 이용된다. 이하의 실시예에서, 설명 목적을 위해, 다수의 특정 세부사항들이 하나 이상의 양상들의 총체적 이해를 제공하기 위해 제시된다. 그러나, 그러한 양상(들)이 이러한 구체적인 세부사항들 없이 실시

될 수 있음은 명백할 것이다.

도 1은 본 발명의 몇몇 실시예에 따른 자동차 이력 정보 관리 시스템에 관한 도면이다.

도 2는 본 발명의 몇몇 실시예에 따른 블록체인 네트워크의 일례를 나타낸 도면이다.

도 3은 본 발명의 몇몇 실시예에 따른 블록체인 네트워크에 포함된 블록의 일례를 나타낸 도면이다.

도 4는 본 발명의 몇몇 실시예에 따른 자동차 이력 정보 관리 장치의 블록구성도를 나타낸 도면이다.

도 5는 본 발명의 몇몇 실시예에 따른 자동차 이력 정보를 블록체인 네트워크에서 수신하여 저장하는 방법의 일례를 나타낸 순서도이다.

도 6은 본 발명의 몇몇 실시예에 따른 제 1 트랜잭션을 이용하여 자동차 이력 정보를 업데이트하는 방법의 일례를 나타낸 순서도이다.

도 7은 본 발명의 몇몇 실시예에 따른 제 2 트랜잭션을 이용하여 자동차 이력 정보를 업데이트하는 방법의 일례를 나타낸 순서도이다.

도 8은 본 발명의 몇몇 실시예에 따른 제 3 트랜잭션을 이용하여 자동차 이력 정보를 업데이트하는 방법의 일례를 나타낸 순서도이다.

도 9는 본 발명의 몇몇 실시예에 따른 조회자 단말에 자동차 이력 정보를 전송하는 방법의 일례를 나타낸 순서도이다.

도 10는 본 발명의 몇몇 실시예에 따른 소유자 단말에 자동차 정기 검진 권유 정보를 전송하는 방법의 일례를 나타낸 순서도이다.

도 11은 본 발명의 몇몇 실시예에 따른 자동차 시스템에 운행 금지 요청 정보를 전송하는 방법의 일례를 나타낸 순서도이다.

도 12는 본 발명의 다른 몇몇 실시예에 따른 애플리케이션을 통해 단말에 표시되는 화면의 일례를 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

[0025] 다양한 실시예들 및/또는 양상들이 이제 도면들을 참조하여 개시된다. 하기 설명에서는 설명을 목적으로, 하나 이상의 양상들의 전반적 이해를 돕기 위해 다수의 구체적인 세부사항들이 개시된다. 그러나, 이러한 양상(들)은 이러한 구체적인 세부사항들 없이도 실행될 수 있다는 점 또한 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 감지될 수 있을 것이다. 이후의 기재 및 첨부된 도면들은 하나 이상의 양상들의 특정한 예시적인 양상들을 상세하게 기술한다. 하지만, 이러한 양상들은 예시적인 것이고 다양한 양상들의 원리들에서의 다양한 방법들 중 일부가 이용될 수 있으며, 기술되는 설명들은 그러한 양상들 및 그들의 균등물들을 모두 포함하고자 하는 의도이다. 구체적으로, 본 명세서에서 사용되는 "실시예", "예", "양상", "예시" 등은 기술되는 임의의 양상 또는 설계가 다른 양상 또는 설계들보다 양호하다거나, 이점이 있는 것으로 해석되지 않을 수도 있다.

[0026] 이하, 도면 부호에 관계없이 동일하거나 유사한 구성 요소는 동일한 참조 번호를 부여하고 이에 대한 중복되는 설명은 생략한다. 또한, 본 명세서에 개시된 실시예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 명세서에 개시된 실시예의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 첨부된 도면은 본 명세서에 개시된 실시예를 쉽게 이해할 수 있도록 하기 위한 것일 뿐, 첨부된 도면에 의해 본 명세서에 개시된 기술적 사상이 제한되지 않는다.

[0027] 비록 제1, 제2 등이 다양한 소자나 구성요소들을 서술하기 위해서 사용되나, 이들 소자나 구성요소들은 이들 용어에 의해 제한되지 않음은 물론이다. 이들 용어들은 단지 하나의 소자나 구성요소를 다른 소자나 구성요소와 구별하기 위하여 사용하는 것이다. 따라서, 이하에서 언급되는 제1 소자나 구성요소는 본 발명의 기술적 사상 내에서 제2 소자나 구성요소 일 수도 있음은 물론이다.

[0028] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.

[0029] 더불어, 용어 "또는"은 배타적 "또는"이 아니라 내포적 "또는"을 의미하는 것으로 의도된다. 즉, 달리 특정되지 않거나 문맥상 명확하지 않은 경우에, "X는 A 또는 B를 이용한다"는 자연적인 내포적 치환 중 하나를 의미하는 것으로 의도된다. 즉, X가 A를 이용하거나; X가 B를 이용하거나; 또는 X가 A 및 B 모두를 이용하는 경우, "X는 A 또는 B를 이용한다"가 이들 경우들 어느 것으로도 적용될 수 있다. 또한, 본 명세서에 사용된 "및/또는"이라는 용어는 열거된 관련 아이템들 중 하나 이상의 아이템의 가능한 모든 조합을 지칭하고 포함하는 것으로 이해되어야 한다.

[0030] 또한, "포함한다" 및/또는 "포함하는"이라는 용어는, 해당 특징 및/또는 구성요소가 존재함을 의미하지만, 하나 이상의 다른 특징, 구성요소 및/또는 이들의 그룹의 존재 또는 추가를 배제하지 않는 것으로 이해되어야 한다. 또한, 달리 특정되지 않거나 단수 형태를 지시하는 것으로 문맥상 명확하지 않은 경우에, 본 명세서와 청구범위에서 단수는 일반적으로 "하나 또는 그 이상"을 의미하는 것으로 해석되어야 한다.

[0031] 더불어, 본 명세서에서 사용되는 용어 "정보" 및 "데이터"는 종종 서로 상호교환 가능하도록 사용될 수 있다.

[0032] 이하, 도면 부호에 관계없이 동일하거나 유사한 구성 요소는 동일한 참조 번호를 부여하고 이에 대한 중복되는 설명은 생략한다. 또한, 본 명세서에 개시된 실시예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 명세서에 개시된 실시예의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 첨부된 도면은 본 명세서에 개시된 실시예를 쉽게 이해할 수 있도록 하기 위한 것일 뿐, 첨부된 도면에 의해 본 명세서에 개시된 기술적 사상이 제한되지 않는다.

[0033] 비록 제1, 제2 등이 다양한 소자나 구성요소들을 서술하기 위해서 사용되나, 이들 소자나 구성요소들은 이들 용어에 의해 제한되지 않음은 물론이다. 이들 용어들은 단지 하나의 소자나 구성요소를 다른 소자나 구성요소와 구별하기 위하여 사용하는 것이다. 따라서, 이하에서 언급되는 제1 소자나 구성요소는 본 개시의 기술적 사상 내에서 제2 소자나 구성요소 일 수도 있음은 물론이다.

[0034] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.

[0035] 이하의 설명에서 사용되는 구성 요소에 대한 접미사 "모듈" 및 "부"는 명세서 작성의 용이함만이 고려되어 부여되거나 혼용되는 것으로서 그 자체로 서로 구별되는 의미 또는 역할을 갖는 것은 아니다.

[0036] 본 개시의 목적 및 효과, 그리고 그것들을 달성하기 위한 기술적 구성들은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 본 개시를 설명하는데 있어서 공지 기능 또는 구성에 대한 구체적인 설명이 본 개시의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 개시에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다.

[0037] 그러나 본 개시는 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있다. 단지 본 실시예들은 본 개시가 완전하도록 하고, 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 개시의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 개시는 청구항의 범주에 의해 정의될 뿐이다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0039] 도 1은 본 발명의 몇몇 실시예에 따른 자동차 이력 정보 관리 시스템에 관한 도면이다.

[0040] 도 1을 참조하면, 자동차 이력 정보 관리 시스템은, 블록체인 네트워크(1), 자동차 시스템(10), 제조사 단말(20), 자동차 이력 정보 관리 장치(100), 관리자 단말(200), 소유자 단말(300) 및 조회자 단말(400)을 포함할 수 있다. 다만, 상술한 구성 요소들은 자동차 이력 정보 관리 시스템을 구현하는데 있어서 필수적인 것은 아니어서, 자동차 이력 정보 관리 시스템은 위에서 열거된 구성요소들 보다 많거나, 또는 적은 구성 요소들을 가질 수 있다.

[0041] 블록체인 네트워크(1)는 복수의 노드(2)들로 이루어지고 각 노드(2)들 간에 합의 알고리즘을 통해 블록을 생성 및 저장하고 있는 네트워크일 수 있다. 블록체인 네트워크(1)에 관한 구체적인 내용은 도 2에서 후술한다.

[0042] 자동차 시스템(10)은 자동차의 내부에서 자동차의 전반적인 동작을 제어하는 시스템을 의미할 수 있다. 일례로, 자동차 시스템(10)은 엔진 제어 유닛(Engine Control Unit)을 포함할 수 있다. 다만 이는 예시일 뿐이며, 본 개

시는 이에 제한되지 않는다.

[0043] 자동차 시스템(10)은 내부에 자동차 이력 정보 관리에 필요한 자동차 식별 정보 를 저장하고 있을 수 있다.

[0044] 여기서 자동차 식별 정보는 자동차 간의 식별을 위해 포함하는 정보 일 수 있다. 일례로, 자동차 식별 정보는 다른 자동차와 중복되지 않는 사전 결정된 자리수의 문자 및 숫자의 조합을 포함할 수 있다. 다만 이는 일 예시일 뿐이며, 본 개시의 자동차 식별 정보는 이에 제한되지 않는다.

[0045] 자동차 시스템(10)은 보안을 위해 자동차 식별 정보를 암호화하여 저장하고 있을 수 있다. 또한, 자동차 식별 정보의 위조를 방지하기 위하여 물리적 복제 방지 기술(Physical Unclonable Function)을 사용할 수도 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0046] 몇몇 실시예에 따르면, 자동차 시스템(10)과 제조사 단말(20)은 유무선 통신을 통해 연결되고, 자동차 시스템(10)은 제조사 단말(20)로부터 자동차 식별 정보를 수신하여, 수신한 자동차 식별 정보를 자동차 시스템(10) 내부에 저장할 수 있다. 여기서, 유무선 통신은 컴퓨팅 장치와 관련하여 상술한 유선 네트워크 기술 및 유선 네트워크 기술을 활용하는 통신일 수 있다.

[0047] 몇몇 실시예에 따르면 자동차 시스템(10)은 자동차 이력 정보 관리 장치(100)와 유무선 통신을 통해 연결되어 자동차 식별 정보를 전송할 수 있다. 자동차 시스템(10)과 자동차 이력 정보 관리 장치(100)간의 구체적인 동작에 관해서는 도 4 이하에서 후술한다.

[0048] 제조사 단말(20), 관리자 단말(200), 소유자 단말(300) 및 조회자 단말(400)은 컴퓨팅 장치 일 수 있다.

[0049] 여기서 컴퓨팅 장치는, PC(personal computer), 데스크 탑 컴퓨터, 랩-탑(lap-top) 컴퓨터, 컴퓨터 워크스테이션(computer workstation), 태블릿(tablet) PC, 비디오 게임 플랫폼(또는 비디오 게임 콘솔), TV, DTV(Digital TV), IPTV(internet protocol TV), 서버 및 모바일 컴퓨팅 장치 중의 하나로 구현될 수 있다. 여기서, 모바일 컴퓨팅 장치는 이동 전화기, 스마트 폰(smart phone), EDA(enterprise digital assistant), 디지털 스틸 카메라(digital still camera), 디지털 비디오 카메라(digital video camera), PMP(portable multimedia player), PND(personal navigation device 또는 portable navigation device), 모바일 인터넷 장치(mobile internet device(MID)), 웨어러블 컴퓨터, 사물 인터넷(Internet of Things; IOT) 장치, 만물 인터넷(Internet of Everything; IOE) 장치 또는 e-book으로 구현될 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0050] 컴퓨팅 장치는 다른 장치와 상호작용하기 위하여, 유무선 네트워크 모듈을 포함할 수 있다. 여기서 유무선 네트워크 모듈은 유선 네트워크 기술 및 무선 네트워크 기술에 따른 통신망에서 유무선 신호를 송수신하는 모듈일 수 있다. 유선 네트워크 기술로는 XDSL(Digital Subscriber Line), FTTH(Fibers to the home), PLC(Power Line Communication), USB(Universal Serial Bus) 등을 포함할 수 있다. 무선 네트워크 기술로는 블루투스(Bluetooth), Wi-Fi(Wireless-Fidelity), Wi-Fi(Wireless Fidelity) Direct, 적외선 통신, WLAN(Wireless LAN), DLNA(Digital Living Network Alliance), WiBro(Wireless Broadband), WiMAX(World Interoperability for Microwave Access), HSDPA(High Speed Downlink Packet Access), HSUPA(High Speed Uplink Packet Access), LTE(Long Term Evolution), LTE-A(Long Term Evolution-Advanced) 등을 포함할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0051] 컴퓨팅 장치는, 개인키 및 공개키를 포함하고 있을 수 있다. 컴퓨팅 장치는 정보를 전달할 때 위/변조 방지 및 무결성을 증명하기 위해 개인키 및 공개키를 사용할 수 있다.

[0052] 제조사 단말(20), 관리자 단말(200), 소유자 단말(300) 및 조회자 단말(400)은 단말(미도시)을 사용하는 주체 및 단말이 사용하는 기능에 따라 구별되는 것일 수 있다. 예를 들어, 단말은 단말을 사용하는 주체에 따라 제조사 단말(20), 관리자 단말(200), 소유자 단말(300) 및 조회자 단말(400) 중 하나로 기능할 수 있다. 즉 각각의 단말들은 사용하는 주체에 따라 구별되는 것일 뿐, 별도의 장치를 의미하는 것은 아닐 수 있다. 일례로, A단말을 제조사가 사용할 때는 A는 제조사 단말(20)이 될 수 있고, A단말을 관리자가 사용할 때는 관리자 단말(200)이 될 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다. 제조사 단말(20), 관리자 단말(200), 소유자 단말(300) 및 조회자 단말(400)의 구체적인 내용에 대해서는 도 2이하에서 후술한다.

[0053] 자동차 이력 정보 관리 장치(100)는 단말과 연결되어 자동차 이력 정보 관리에 필요한 동작을 수행할 수 있는 장치일 수 있다.

[0054] 자동차 이력 정보 관리 장치(100)의 구체적인 내용에 대해서는 도 2이하에서 후술한다.

[0056] 도 2는 본 발명의 몇몇 실시예에 따른 블록체인 네트워크의 일례를 나타낸 도면이다.

[0057] 블록체인 네트워크(1)는 복수의 노드(node)(2)로 이루어 질 수 있다. 여기서 각각의 노드(2)는 트랜잭션의 공유, 트랜잭션의 검증, 다음 블록 후보 생성 및 블록의 저장을 수행할 수 있다.

[0058] 각각의 노드(2)는 블록체인 네트워크(1) 상에 트랜잭션을 공유할 수 있다. 여기서, 각각의 노드(2)는 직접 트랜잭션을 생성하여 블록체인 네트워크(1) 상에 트랜잭션을 공유하는 것도 가능하지만, 클라이언트(미도시)와 연결되어 클라이언트 로부터 트랜잭션을 수신하고, 수신한 트랜잭션을 블록체인 네트워크(1) 상에 공유할 수도 있다. 여기서 클라이언트는 상술한 제조사 단말(20), 관리자 단말(200), 소유자 단말(300), 조회자 단말(400) 및 자동차 이력 정보 관리 장치(100) 중 하나일 수 있다.

[0059] 트랜잭션은 원본 데이터, 해쉬 함수 및 개인키를 통해 생성될 수 있다. 여기서 원본 데이터는 트랜잭션의 구체적인 요청 동작에 관한 것일 수 있다. 구체적으로, 트랜잭션은 원본 데이터와 원본 데이터를 해쉬 함수로 변환하고, 개인키를 통해 암호화한 서명 데이터를 통합하여 생성할 수 있다.

[0060] 각각의 노드(2)는 트랜잭션을 공유할 때 개인키에 대응되는 공개키를 같이 공유할 수 있다.

[0061] 각각의 노드(2)는 블록체인 네트워크(1) 상에 공유된 트랜잭션 검증할 수 있다.

[0062] 구체적으로, 각각의 노드(2)는 트랜잭션에 포함된 원본 데이터 및 서명 데이터를 확인하여 트랜잭션을 검증할 수 있다. 노드(2)는 트랜잭션에 포함된 서명 데이터를 공개키로 복호화하여 제 1 값을 산출할 수 있다. 그리고, 노드(2)는 트랜잭션에 포함된 원본 데이터를 해쉬 함수로 변환하여 제 2 값을 산출할 수 있다. 제 1 값과 제 2 값은 둘다 원본 데이터를 해쉬 함수로 변환한 값에 대한 데이터이므로 트랜잭션의 값이 변조되지 않았다면, 두 값은 동일할 것이다.

[0063] 따라서 노드(2)는 트랜잭션에 포함된 서명 데이터를 공개키로 복호화한 값과 트랜잭션에 포함된 원본 데이터를 해쉬함수로 변환한 값이 동일하다면 트랜잭션이 유효하다고 검증할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0064] 각각의 노드(2)는 트랜잭션 검증 결과 해당 트랜잭션이 유효하지 않은 트랜잭션인 것으로 인식할 경우, 이에 대응되는 동작을 수행할 수 있다. 일례로, 해당 트랜잭션이 노드(2)에서 직접 생성한 트랜잭션일 경우 유효하지 않은 트랜잭션이라는 피드백을 출력할 수 있다. 다른 일례로, 노드(2)의 해당 트랜잭션이 클라이언트로부터 수신받은 트랜잭션일 경우, 노드(2)는 유효하지 않은 트랜잭션이라는 피드백을 클라이언트에 전송할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0065] 각각의 노드(2)는 트랜잭션 검증 결과 해당 트랜잭션이 유효한 트랜잭션인 것으로 인식할 경우, 해당 트랜잭션을 새로운 블록에 기록될 수 있는 유효한 트랜잭션으로 결정할 수 있다.

[0066] 각각의 노드(2)들은 각각의 다른 노드(2)들에게 블록체인(500)을 서로 배포 및 공유함으로써 블록체인 네트워크(1)를 구성할 수 있다.

[0067] 각각의 노드(2)들 중 일부는 라이트 노드(Lightweight Node)일 수 있다. 여기서, 라이트 노드(Lightweight Node)는 모든 블록 정보의 원본을 가지고 있지 않고, 헤더(Header) 정보만을 포함하는 노드일 수 있다. 라이트 노드(Lightweight Node)가 트랜잭션을 확인하기 위해서는 모든 블록 정보의 원본을 가지는 노드(Full Block Chain Node)에게 블록 정보를 요청하고, 전송받은 블록 정보에 기초하여 트랜잭션의 인증 내용을 확인할 수 있다. 다만, 설명의 편의를 위해 복수의 노드(2)는, 모든 블록 정보의 원본을 가지는 노드(Full Block Chain Node)임을 가정하고 설명할 수 있다.

[0068] 한편, 노드(2)는 일부 트랜잭션을 처리하기 위해 스마트 컨트랙트(Smart Contract)를 이용할 수 있다. 여기서, 스마트 컨트랙트란 특정 계약을 스스로 수립, 검증 및 이행하기 위한 컴퓨터 프로토콜을 의미할 수 있다. 그리고, 스마트 컨트랙트는 계약의 조건 및 실행에 따라 새로운 스마트 컨트랙트를 생성하거나, 특정 스마트 컨트랙트 상의 함수를 실행하거나, 또는 데이터를 전송하도록 구성될 수 있다.

[0069] 스마트 컨트랙트를 이용하면 입력받은 트랜잭션 값과 블록에 저장된 스마트 컨트랙트 코드의 내용에 따라 다른 동작을 수행하는 것이 가능할 수 있다.

[0070] 스마트 컨트랙트와 상호작용하여 특정 동작을 수할 수 있는 애플리케이션(Application)은 DApp(Decentralized

application)일 수 있다. 몇몇 실시예에 따르면, 도 12에서 표현되는 화면은 DApp을 통해 구현되는 것일 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0071] 한편 블록체인 네트워크(1)는 블록체인 네트워크(1) 상에서 만든 인증방식을 통해서 검증된 노드(2)만이 참여할 수 있는 프라이빗 블록체인 네트워크(Private Blockchain Network)일 수 있다. 블록체인 네트워크(1)가 프라이빗 블록체인 네트워크로 구성될 경우, 보안성을 향상할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0073] 이하에서는 블록체인 네트워크(1)에 포함된 노드(2)가 클라이언트와 상호작용하는 구체적인 예시를 설명하도록 한다.

[0074] 몇몇 실시예에 따르면, 클라이언트는 사용자로부터 인증을 위한 데이터를 수신할 수 있다. 여기서 인증을 위한 데이터는, 자신이 특정 단말(예를 들어 소유자 단말)임을 증명할 수 있는 해제키와 관련된 데이터일 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다. 그리고, 클라이언트는 인증을 위한 데이터에 기초하여 인증을 위한 트랜잭션을 생성할 수 있다.

[0075] 다른 몇몇 실시예에 따르면, 클라이언트는 클라이언트 내부에 인증을 위한 데이터를 메모리에 미리 저장해둘 수 있다. 그리고, 클라이언트는 인증이 필요할 때 마다 저장된 인증을 위한 데이터에 기초하여 인증을 위한 트랜잭션을 생성할 수 있다.

[0076] 클라이언트는 생성한 인증을 위한 트랜잭션을 블록체인 네트워크(1)에 전송할 수 있다.

[0077] 블록체인 네트워크(1)는 상기 트랜잭션을 수신하고, 유효한 트랜잭션으로 인식할 경우, 클라이언트에 인증 결과 데이터를 전송할 수 있다.

[0078] 클라이언트는 수신한 인증 결과 데이터에 기초하여 제조사 단말(20), 관리자 단말(200), 소유자 단말(300), 조회자 단말(400) 및 자동차 이력 정보 관리 장치(100) 중 하나로 기능할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0079] 몇몇 실시예에 따르면, 클라이언트는 제조사 단말(20)일 수 있다. 여기서, 제조사 단말(20)은 자동차를 제조한 업체에서 생산한 자동차에 관한 정보를 블록체인 네트워크(1)에 등록하기 위한 단말일 수 있다.

[0080] 제조사 단말(20)은 제조사 단말을 사용하는 사용자로부터 자동차 식별 정보 및 자동차 제조 관련 정보를 수신할 수 있다.

[0081] 여기서 자동차 식별 정보는 자동차 시스템(10)과 관련하여 상술한 자동차 식별 정보와 동일할 수 있다.

[0082] 그리고, 자동차 제조 관련 정보는, 자동차를 제조할 때와 관련된 정보 일 수 있다. 예를 들어, 자동차 제조 관련 정보는, 자동차의 제조년도, 제조일, 자동차의 차종, 사용된 부품의 정보, 자동차를 생산한 엔지니어의 정보 중 적어도 하나를 포함할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0083] 제조사 단말(20)은 자동차 식별 정보 및 자동차 제조 관련 정보를 수신함에 따라, 블록체인 네트워크(1)에 자동차 제조 관련 정보에 기초하여 자동차 이력 정보를 생성하는 명령 코드 및 상기 명령 코드를 개인키로 암호화한 서명 데이터를 포함하는 트랜잭션을 생성할 수 있다.

[0084] 그리고, 제조사 단말(20)은 상기 트랜잭션 및 개인키에 대응되는 공개키를 블록체인 네트워크(1)에 전송할 수 있다.

[0085] 블록체인 네트워크(1)는 상기 트랜잭션을 수신하고, 유효한 트랜잭션으로 인식하여 트랜잭션을 블록에 저장할 경우, 자동차 식별 정보에 대응되는 자동차 이력 정보를 자동차 제조 관련 정보에 기초하여 생성하여 자동차를 블록체인 네트워크(1)에 등록할 수 있다. 즉 블록체인 네트워크(1)는 자동차 이력 정보를 최초로 생성할 수 있다.

[0086] 여기서 자동차 이력 정보는, 자동차와 관련된 모든 정보를 나타내는 것일 수 있다. 예를 들어, 자동차 이력 정보는, 자동차 제조 관련 정보, 자동차 관리 정보, 자동차 활동 정보, 소유권 관련 정보, 개인 인증 정보, 자동차 식별 정보 및 자동차 이력 정보 조회 허용 여부 등을 포함할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0087] 블록체인 네트워크(1)는 상기 트랜잭션을 수신하고, 유효하지 않은 트랜잭션으로 인식하여 트랜잭션을 블록에 저장하지 않을 경우, 제조사 단말(20)에 유효하지 않은 트랜잭션이라는 피드백을 전송할 수 있다.

[0088] 블록체인 네트워크(1)는, 서명 데이터가 유효하지 않는 경우, 자동차 이력 정보 생성을 위한 잠금 해제키가 유효하지 않는 경우, 자동차 식별 정보에 대응되는 자동차 이력 정보가 이미 생성되어 있는 경우 또는 자동차 제조 관련 정보에 유효하지 않은 데이터가 포함되어 있는 경우에 수신한 트랜잭션을 유효하지 않은 트랜잭션으로 인식할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0089] 몇몇 실시예에 따르면, 클라이언트는 관리자 단말(200)일 수 있다. 여기서 관리자 단말은 자동차를 관리할 수 있는 관리자가 이용하는 단말일 수 있다.

[0090] 좀더 구체적으로, 관리자는 자동차와 간접적인 관계를 맺는 사람일 수 있다. 예를 들어 관리자는, 자동차 유통업체, 자동차 정비점검 업체, 자동차 수입 업체, 정부 기관 등을 포함할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0091] 관리자 단말(200)은 자동차 식별 정보 및 자동차 관리 정보를 수신할 수 있다.

[0092] 여기서 자동차 관리 정보는, 간접적인 원인으로 인해 자동차의 상태가 변화되는 정보일 수 있다. 예를 들어, 자동차 관리 정보는 관리 유통업체 정보, 수입업체 정보, 정부 인증 정보, 자동차를 수리한 엔지니어 정보, 변경된 부품 내역 정보, 추가된 부품 내역 정보 및 수리한 부품 내역 정보 중 적어도 하나를 포함할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0093] 관리자 단말(200)은 자동차 식별 정보 및 자동차 관리 정보를 수신함에 따라, 블록체인 네트워크(1)에 저장된 자동차 식별 정보에 대응되는 자동차 이력 정보를 자동차 관리 정보에 기초하여 업데이트하는 명령 코드 및 상기 명령 코드를 개인키로 암호화한 서명 데이터를 포함하는 트랜잭션을 생성할 수 있다.

[0094] 그리고, 관리자 단말(200)은 상기 트랜잭션 및 개인키에 대응되는 공개키를 블록체인 네트워크(1)에 전송할 수 있다.

[0095] 블록체인 네트워크(1)는 상기 트랜잭션을 수신하고, 유효한 트랜잭션으로 인식하여 트랜잭션을 블록에 저장할 경우, 자동차 식별 정보에 대응되는 자동차 이력 정보를 자동차 관리 정보에 기초하여 업데이트할 수 있다.

[0096] 블록체인 네트워크(1)는 상기 트랜잭션을 수신하고, 유효하지 않은 트랜잭션으로 인식하여 트랜잭션을 블록에 저장하지 않을 경우, 관리자 단말(200)에 유효하지 않은 트랜잭션이라는 피드백을 전송할 수 있다.

[0097] 블록체인 네트워크(1)는, 서명 데이터가 유효하지 않는 경우, 자동차 이력 정보 변경을 위한 잠금 해제키가 유효하지 않은 경우, 자동차 식별 정보에 대응되는 자동차 이력 정보가 존재하지 않는 경우 또는 자동차 관리 정보에 유효하지 않은 데이터가 포함되어 있는 경우에 수신한 트랜잭션을 유효하지 않은 트랜잭션으로 인식할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0098] 몇몇 실시예에 따르면, 클라이언트는 소유자 단말(300)일 수 있다. 여기서 소유자 단말(300)은 자동차를 현재 소유하고 있는 소유자가 이용하는 단말일 수 있다.

[0099] 소유자 단말(300)은 자동차 식별 정보 및 소유권 관련 정보를 수신할 수 있다.

[0100] 여기서, 소유권 관련 정보는, 소유자가 자신의 자동차와 관련해서 사용할 수 있는 특정한 기능과 관련된 정보일 수 있다. 예를 들어, 개인 인증 정보 변경 정보, 소유권 이전 정보, 자동차 대여 정보, 자동차 관리 접수 정보, 자동차 이력 조회 허용 정보 및 도난신고 정보 중 적어도 하나를 포함할 수 있다.

[0101] 몇몇 실시예에 따르면, 소유자 단말(300)은 자동차 식별 정보를 최초 한번만 수신하고, 그 뒤에는 소유자 단말(300)의 내부에 저장해둘 수 있다. 이 경우, 소유자는 자동차 식별 정보를 한번만 입력해 두면, 그 뒤에 관련 동작을 수행할 때마다 계속, 자동차 식별 정보를 입력할 필요가 없을 수 있다.

[0102] 소유자 단말(300)은 자동차 식별 정보 및 소유권 관련 정보를 수신함에 따라, 블록체인 네트워크(1)에 저장된 자동차 식별 정보에 대응되는 자동차 이력 정보를 상기 소유권 관련 정보에 기초하여 업데이트하는 명령 코드 및 상기 명령 코드를 개인키로 암호화한 서명 데이터를 포함하는 트랜잭션을 생성할 수 있다.

[0103] 그리고, 소유자 단말(300)은 상기 트랜잭션 및 개인키에 대응되는 공개키를 블록체인 네트워크(1)에 전송할 수 있다.

[0104] 블록체인 네트워크(1)는 상기 트랜잭션을 수신하고, 유효한 트랜잭션으로 인식하여 트랜잭션을 블록에 저장할 경우, 자동차 식별 정보에 대응되는 자동차 이력 정보를 소유권 관련 정보에 기초하여 업데이트할 수 있다.

[0105] 블록체인 네트워크(1)는 상기 트랜잭션을 수신하고, 유효하지 않은 트랜잭션으로 인식하여 트랜잭션을 블록에 저장하지 않을 경우, 소유자 단말(300)에 유효하지 않은 트랜잭션이라는 피드백을 전송할 수 있다.

[0106] 블록체인 네트워크(1)는, 서명 데이터가 유효하지 않는 경우, 자동차 이력 정보 변경을 위한 잠금 해제키가 유효하지 않은 경우, 자동차 식별 정보에 대응되는 자동차 이력 정보가 존재하지 않는 경우 또는 소유권 관련 정보에 유효하지 않은 데이터가 포함되어 있는 경우에 트랜잭션을 유효하지 않은 트랜잭션으로 인식할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0107] 몇몇 실시예에 따르면, 클라이언트는 조회자 단말(400)일 수 있다. 여기서 조회자 단말(400)은 자동차를 구매를 원하는 등의 이유로 자동차 이력 정보를 조회하고자 하는 조회자가 이용하는 단말일 수 있다.

[0108] 조회자 단말(400)은 자동차 식별 정보 및 자동차 이력 요청 정보를 수신할 수 있다. 여기서 자동차 이력 요청 정보는 자동차 이력 정보를 조회하기 위해 필요한 정보일 수 있다.

[0109] 그리고, 조회자 단말(400)은 자동차 식별 정보 및 자동차 이력 정보 조회 요청 정보를 이용하여 자동차 이력 정보 조회 요청 신호를 생성할 수 있다.

[0110] 그리고, 조회자 단말(400)은 상기 자동차 이력 정보 조회 요청 신호를 블록체인 네트워크(1)에 전송할 수 있다.

[0111] 블록체인 네트워크(1)는 자동차 이력 정보 조회 요청 신호를 수신하여, 수신한 자동차 이력 정보 조회 요청 신호가 유효한 것으로 인식할 경우, 블록체인 네트워크(1)는 자동차 이력 정보를 조회자 단말(400)에 전송할 수 있다.

[0112] 한편, 블록체인 네트워크(1)는 수신한 자동차 이력 정보 조회 요청 신호가 유효하지 않은 것으로 인식할 경우, 조회자 단말(400)에 자동차 이력 정보를 전송할 수 없다는 피드백을 전송할 수 있다.

[0113] 예를 들어, 블록체인 네트워크(1)는 자동차 식별 정보에 해당하는 자동차 이력 정보를 조회할 권한이 없는 경우 또는 자동차 식별 정보에 해당하는 자동차 이력 정보가 생성되어 있지 않은 경우 자동차 식별 정보 조회 요청 신호가 유효하지 않다고 인식할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0114] 몇몇 실시예에 따르면, 클라이언트는 자동차 이력 정보 관리 장치(100)일 수 있다.

[0115] 여기서, 자동차 이력 정보 관리 장치(100)는 상술한 바와 같이 단말과 연결되어 자동차 이력 정보 관리에 필요한 동작을 수행할 수 있는 장치일 수 있다. 자동차 이력 정보 관리 장치의 구체적인 구성 및 동작에 대해서는 도 4이하에서 후술한다.

[0116] 도 2 전체에 걸쳐 전술한 블록체인 네트워크(1)에 대한 자세한 기재는 일 예시일 뿐, 본 개시는 이에 제한되지 않는다.

[0118] 도 3은 본 발명의 몇몇 실시예에 따른 블록체인 네트워크에 포함된 블록의 일례를 나타낸 도면이다.

[0119] 이하의 설명에서, 블록을 기준으로 설명한다. 도 3에 기재된 용어 “최초”, “제 1” 및 “제 2”은 복수의 블록을 용이하게 구분하기 위해 기재되었다. 또한, 블록에 포함된 구성에서, “블록이 생성된 시간”, “블록의 해쉬값”, “트랜잭션의 해쉬값” 등과 같이 동일하게 사용된 용어는 동일한 역할을 수행한다. 다만, 상술한 복수의 블록 각각에 저장되어 있는 정보는 다를 수 있다.

[0120] 몇몇 실시예에 따르면, 블록체인(500)은 최초 블록(510), 제 1 블록(520), 제 2 블록(530)을 포함할 수 있다. 다만, 상술한 구성 요소들은 블록체인(500)을 구현하는데 있어서 필수적인 것은 아니어서, 블록체인(500)은 위에서 열거된 구성요소들 보다 많거나, 또는 적은 구성요소들을 가질 수 있다.

[0121] 블록(510, 520, 530)은 블록 생성 시간(511, 521, 531), 이전 블록의 해쉬값(512, 522, 532), 현재 블록의 해쉬값(513, 523, 533), 현재 블록의 트랜잭션의 해쉬값(514, 524, 534), 현재 블록의 트랜잭션(515, 525, 535)을 포함할 수 있다. 다만 블록은 위에서 열거된 구성요소들 보다 많거나, 또는 적은 구성요소들을 가질 수 있다.

[0122] 몇몇 실시예에 따르면, 현재 블록의 트랜잭션의 해쉬값(514, 524, 534)은 머클루트를 이용하여 생성될 수 있다. 머클루트는 트랜잭션 각각을 해쉬 함수에 입력하여 해쉬값을 구하고, 구해진 각각의 해쉬값을 다시 해쉬 함수에 입력하여 새로운 해쉬값을 구하여 하나의 해쉬값으로 통합하는 것일 수 있다.

[0123] 예를 들어, 최초 트랜잭션(515)에 대한 머클루트를 통해 최초 트랜잭션의 해쉬값(514)을 생성하는 과정은, 제조

사에서 A 자동차를 등록이라는 트랜잭션을 해쉬 함수에 입력하여 제 1 머클 해쉬값을 생성하고, 제조사가 A 자동차를 유통사에게 전달이라는 트랜잭션을 해쉬 함수에 입력하여 제 2 머클 해쉬값을 생성하고, 유통사가 a에게 A자동차를 판매라는 트랜잭션을 해쉬 함수에 입력하여 제 3 머클 해쉬값을 생성할 수 있다. 그리고, 제 1 머클 해쉬값과 제 2 머클 해쉬값을 해쉬 함수에 입력하여 제 4 머클 해쉬값을 생성할 수 있다. 그리고 제 3 머클 해쉬값과 제 4 머클 해쉬값을 해쉬 함수에 입력하여 최초 트랜잭션의 해쉬값(514)을 생성할 수 있다.

[0124] 머클루트를 통해 트랜잭션의 해쉬값을 생성할 경우, 트랜잭션의 어느 하나의 정보가 위조 또는 변조된 때 전혀 다른 해쉬값이 생성되므로 트랜잭션의 무결성을 검증할 수 있게 된다.

[0125] 몇몇 실시예에 따르면 블록(510, 520, 530)은 블록체인 기술에서 활용되는 블록으로 자동차 이력 정보 및 이와 관련된 다양한 정보(예를 들어, 스마트 컨트랙트 코드 등)들을 저장하고 있을 수 있다.

[0126] 몇몇 실시예에 따르면, 블록(510, 520, 530)은 특정 시간 간격(예컨대, 10분)으로 생성될 수 있다. 여기서, 특정 시간은 블록 생성의 난이도 등에 기초하여 변경될 수 있다. 또한, 블록(510, 520, 530)은 특정 시간 간격 동안 변경된 자동차 이력 정보를 저장할 수 있다.

[0127] 도면에 도시되지는 않았지만, 블록(510, 520, 530)은 블록의 버전에 대한 정보, 논스(nonce)에 대한 정보 및 난이도 목표에 대한 정보를 더 포함할 수도 있다.

[0128] 블록의 버전에 대한 정보, 논스(nonce), 블록 생성 시간(511, 521, 531), 이전 블록의 해쉬값(512, 522, 532), 합의 메타데이터(미도시), 블록 메타데이터(미도시), 현재 블록의 해쉬값(513, 523, 533) 및 난이도 목표는 블록(510, 520, 530)의 헤더(Header)에 포함될 수 있다. 그리고, 현재 블록의 트랜잭션(515, 525, 535)은 블록(510, 520, 530)의 바디(Body)에 포함될 수 있다.

[0129] 블록의 버전에 대한 정보는, 현재 이 블록(510, 520, 530)을 만든 블록체인 프로그램의 버전 정보가 될 수 있다.

[0130] 논스(nonce)에 대한 정보는 블록(510, 520, 530)을 만드는 과정에서 해쉬값을 구할 때, 사용된 값으로 일반적인 블록체인 기술의 논스가 이에 해당한다. 몇몇 실시예에 따르면 논스에 대한 정보는 합의 알고리즘을 만족하는 블록을 생성하기위해 변경될 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0131] 난이도 목표에 대한 정보는 영어로 Bits라고 표현할 수 있다. Bits는 난이도 해쉬 목표 값을 의미할 수 있다.

[0132] 블록 생성 시간(511, 521, 531)은 블록(510, 520, 530)이 생성된 시간(예를 들어, 2018년 04월 02일 15시)에 대한 정보일 수 있다.

[0133] 이전 블록의 해쉬값(512, 522, 532)은 이전 블록(예를 들어, 현재 블록이 제 1 블록(520)일 경우, 이전 블록은 최초 블록(510))의 헤더에 포함된 정보들을 해쉬값으로 변환하여 생성된 정보일 수 있다. 이전 블록의 해쉬값(512, 522, 532)은 알고리즘의 종류에 따라, 문자의 길이와 값(예를 들어, 256bits, 512bits)이 달라질 수 있다.

[0134] 따라서, 현재 블록과 이전 블록은 체인으로 연결된 것과 같다고 볼 수 있다. 다시 말해서, 현재 블록과 이전 블록은 블록체인을 형성할 수 있다. 상술한 내용에 따라, 블록체인 구조의 데이터는 위변조가 불가능하다는 효과를 가질 수 있다.

[0135] 현재 블록에 이전 블록의 해쉬값이 포함되는 경우, 트랜잭션의 위/변조를 방지할 수 있고, 트랜잭션의 무결성을 검증할 수 있다.

[0136] 상술한 해쉬값은 해쉬 알고리즘을 통해 도출된 해쉬값을 의미한다. 상술한 해쉬 알고리즘(hash algorithm)은 문장의 길이에 관계없이 일정한 길이의 값으로 변경하는 알고리즘을 지칭한다. 해쉬 알고리즘은 문장의 내용이 완전히 같은 경우, 완전히 같은 해쉬값을 가진다. 반면, 해쉬 알고리즘은 문장의 내용이 일부라도 다른 경우, 완전히 다른 해쉬값을 가진다. 따라서, 해쉬 알고리즘을 이용하는 경우, 트랜잭션의 위/변조가 사실상 불가능할 수 있다.

[0138] 도 4는 본 발명의 몇몇 실시예에 따른 자동차 이력 정보 관리 장치의 블록구성도를 나타낸 도면이다.

[0139] 도 4를 참조하면, 자동차 이력 정보 관리 장치(100)는 통신부(110), 메모리(120) 및 제어부(130)를 포함할 수 있다. 다만, 상술한 구성 요소들은 자동차 이력 정보 관리 장치(100)를 구현하는데 있어서 필수적인 것은 아니어서, 자동차 이력 정보 관리 장치(100)는 위에서 열거된 구성요소들 보다 많거나, 또는 적은 구성 요소들을 가

질 수 있다. 여기서, 각각의 구성 요소들은 별개의 칩이나 모듈이나 장치로 구성될 수 있고, 하나의 장치 내에 포함될 수도 있다.

[0140] 통신부(110)는 컴퓨팅 장치에 관련하여 상술한 유선 네트워크 접속 또는 무선 네트워크 접속을 위한 모듈과 동일한 모듈일 수 있다.

[0141] 몇몇 실시예에 따르면, 자동차 이력 정보 관리 장치(100)는 USB, Wi-Fi 또는 블루투스를 통해 자동차 시스템(10)과 연결될 수 있다. 그리고, 자동차 이력 정보 관리 장치(100)는 Wi-Fi 또는 블루투스를 통해 블록체인 네트워크(1), 제조사 단말(20), 관리자 단말(200), 소유자 단말(300) 및 조회자 단말(400)과 연결될 수 있다. 다만 상술한 연결의 예시는 일 예시일 뿐이며, 자동차 이력 정보 관리 장치(100)와 다른 장치들 간의 연결 방법 및 수단은 제한되지 않는다.

[0142] 메모리(120)는 플래시 메모리 타입(flash memory type), 하드디스크 타입(hard disk type), 멀티미디어 카드 마이크로 타입(multimedia card micro type), 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램(Random Access Memory, RAM), SRAM(Static Random Access Memory), 롬(Read-Only Memory, ROM), EEPROM(Electrically Erasable Programmable Read-Only Memory), PROM(Programmable Read-Only Memory), 자기 메모리, 자기 디스크, 광디스크 중 적어도 하나의 타입의 저장매체를 포함할 수 있다.

[0143] 메모리(120)는 자동차 이력 정보 관리 장치(100)에서 구동되는 다수의 응용 프로그램(application program 또는 애플리케이션(application)), 자동차 이력 정보 관리 장치(100)의 동작을 위한 데이터들, 명령어들을 저장할 수 있다. 이러한 응용 프로그램 중 적어도 일부는, 유무선 통신을 통해 외부 서버로부터 다운로드 될 수 있다.

[0144] 한편, 응용 프로그램은, 메모리(120)에 저장되고, 자동차 이력 정보 관리 장치 (100) 상에 설치되어, 제어부(130)에 의하여 자동차 이력 정보 관리 장치(100)의 동작(또는 기능)을 수행하도록 구동될 수 있다.

[0145] 제어부(130)는 통상적으로 자동차 이력 정보 관리 장치(100)의 전반적인 동작을 제어할 수 있다. 제어부(130)는 위에서 살펴본 구성요소들을 통해 입력 또는 출력되는 신호, 데이터, 정보 등을 처리하거나 메모리(120)에 저장된 응용 프로그램을 구동함으로써, 사용자에게 적절한 정보 또는 기능을 제공 또는 처리할 수 있다.

[0146] 또한, 제어부(130)는 메모리(120)에 저장된 응용 프로그램을 구동하기 위하여, 자동차 이력 정보 관리 장치(100)의 구성요소들 중 적어도 일부를 제어할 수 있다. 나아가, 제어부(130)는 상기 응용 프로그램의 구동을 위하여, 자동차 이력 정보 관리 장치(100)에 포함된 구성요소들 중 적어도 둘 이상을 서로 조합하여 동작 시킬 수 있다.

[0147] 본 개시의 몇몇 실시예에 따라 제어부(130)가 제어할 수 있는 자동차 이력 정보 관리 장치(100)의 구체적인 동작에 대해서는 도 5 이하에서 후술한다.

[0148] 몇몇 실시예에 따르면, 자동차 이력 정보 관리 장치(100)는 자동차와 탈 부착 가능할 수 있다.

[0149] 다른 몇몇 실시예에 따르면, 자동차 이력 정보 관리 장치(100)는 자동차 내부에 일체로 고정되는 장치일 수 있다.

[0151] 도 5는 본 발명의 몇몇 실시예에 따른 자동차 이력 정보를 블록체인 네트워크에서 수신하여 저장하는 방법의 일례를 나타낸 순서도이다.

[0152] 도 5를 참조하면, 자동차 이력 정보 관리 장치(100)의 통신부(110)는 자동차 시스템(10)으로부터 자동차 식별 정보를 수신할 수 있다(S110).

[0153] 자동차 이력 정보 관리 장치(100)의 제어부(130)는 단계(S110)에서 수신한 자동차 식별 정보 및 메모리에 저장된 이력 정보 수신 권한 키를 이용하여 자동차 이력 정보 전송 요청 신호를 생성할 수 있다(S120). 여기서 이력 정보 수신 권한 키는 자동차 이력 정보 관리 장치가 블록체인 네트워크(1)로부터 자동차 이력 정보를 수신하기 위해 필요한 인증용 키 정보일 수 있다.

[0154] 그리고, 통신부(110)는 상기 자동차 이력 정보 전송 요청 신호를 블록체인 네트워크(1)에 전송할 수 있다(S130).

[0155] 블록체인 네트워크(1)는 자동차 이력 정보 전송 요청 신호를 수신하여, 수신한 자동차 이력 정보 전송 요청 신호가 유효한 것으로 인식할 경우, 블록체인 네트워크(1)는 자동차 식별 정보에 대응되는 자동차 이력 정보를 자동차 이력 정보 관리 장치(100)에 전송할 수 있다.

[0156] 블록체인 네트워크(1)는 자동차 이력 정보 전송 요청 신호를 수신하여, 수신한 자동차 이력 정보 전송 요청 신호가 유효하지 않은 것으로 인식한 경우, 자동차 이력 정보 관리 장치(100)에 유효하지 않은 자동차 이력 정보 전송 요청 신호라는 피드백을 전송할 수 있다.

[0157] 자동차 이력 정보 전송 요청 신호가 유효하지 않은 것으로 인식하는 경우는, 자동차 식별 정보에 대응되는 자동차 이력 정보가 존재하지 않는 경우일 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다. 이하에서는 설명의 편의를 위해 블록체인 네트워크(1)는 자동차 이력 정보 전송 요청 신호를 유효한 것으로 인식한 것으로 가정한다.

[0158] 그리고, 상술한 과정을 통해 통신부(110)는 블록체인 네트워크(1)로부터 자동차 식별 정보에 대응되는 자동차 이력 정보를 수신할 수 있다(S140).

[0159] 자동차 이력 정보 관리 장치(100)의 제어부(130)는 단계(S140)에서 수신한 자동차 이력 정보를 메모리(120)에 저장할 수 있다(S150).

[0160] 상술한 도 5와 관련된 동작들은 자동차 이력 정보 관리 장치(100)의 전원이 최초로 켜졌을 때, 자동차 이력 정보 관리 장치(100)가 블록체인 네트워크(1) 또는 사용자로부터 데이터 동기화 요청을 받았을 때, 자동차 이력 정보 관리 장치(100)가 일정한 시간 간격이 지났다고 인식했을 때 수행될 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0161] 상술한 과정을 통해, 자동차 이력 정보 관리 장치(100)는 자동차 식별 정보에 대응되는 관련된 자동차 이력 정보를 수신하여 저장함으로써, 블록체인 네트워크(1) 상의 자동차 식별 정보에 대응되는 자동차 이력 정보와 일정한 시간 간격으로 동일한 정보를 저장할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0162] 자동차 이력 정보 관리 장치(100)의 메모리(120)에 자동차 이력 정보를 저장해 둘 경우 후술한 자동차 이력 정보를 이용하는 것과 관련된 동작 중 일부를 수행할 때마다 블록체인 네트워크(1)에 자동차 이력 정보를 요청하지 않아도 되어 처리 속도가 상승하고 네트워크 데이터를 절약할 수 있다.

[0164] 도 6은 본 발명의 몇몇 실시예에 따른 제 1 트랜잭션을 이용하여 자동차 이력 정보를 업데이트하는 방법의 일례를 나타낸 순서도이다.

[0165] 도 6을 참조하면, 자동차 이력 정보 관리 장치(100)의 제어부(130)는 기설정된 조건이 만족되었다고 인식한 경우(S210, Yes), 자동차 활동 정보를 자동차 시스템(10)으로부터 수신할 수 있다(S220).

[0166] 여기서 자동차 활동 정보는 자동차가 시간이 흐름에 따라 변화되는 정보에 관한 것일 수 있다. 예를 들어, 자동차 활동 정보는 주행 거리, 주행 회수, 주유 내역, 주행 중 발생한 문제 내역, 주차 중 발생한 문제 내역 중 적어도 하나를 포함할 수 있다.

[0167] 몇몇 실시예에 따르면, 기 설정된 조건은 기 설정된 시간이 경과한 경우 만족될 수 있다. 예를 들어, 기 설정된 시간은 1시간일 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0168] 다른 몇몇 실시예에 따르면, 기 설정된 조건은 기 설정된 이벤트가 발생한 경우 만족될 수 있다. 제어부(130)는 자동차가 충돌한 것으로 인식되거나 자동차가 침수된 것으로 인식되거나 자동차의 시동이 비정상적으로 꺼진 것으로 인식되거나, 자동차에 화재가 발생한 것으로 인식되는 경우 기 설정된 이벤트가 발생한 것으로 인식할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0169] 자동차 이력 정보 관리 장치(100)의 제어부(130)는 단계(S220)에서 자동차 활동 정보를 수신함에 따라, 블록체인 네트워크에 저장된 자동차 식별 정보에 대응되는 자동차 이력 정보를 자동차 활동 정보에 기초하여 업데이트하는 명령 코드 및 상기 명령 코드를 제 1 개인키로 암호화한 서명 데이터를 포함하는 제 1 트랜잭션을 생성할 수 있다(S230).

[0170] 그리고 제어부(130)는 단계(S230)에서 생성한 제 1 트랜잭션 및 제 1 개인키에 대응되는 제 1 공개키를 블록체인 네트워크에 전송할 수 있다(S240).

[0171] 블록체인 네트워크(1)는 제 1 트랜잭션을 수신하고, 유효한 트랜잭션으로 인식하여 제 1 트랜잭션을 블록에 저장할 경우, 자동차 식별 정보에 대응되는 자동차 이력 정보를 자동차 활동 정보에 기초하여 업데이트할 수 있다.

[0172] 자동차 이력 정보 관리 장치(100)가 자동차의 활동 정보에 기초하여 블록체인 네트워크(1)에 저장된 자동차 식별 정보에 대응되는 자동차의 이력정보를 업데이트할 경우, 해당 자동차가 어느정도 운행되었는지, 주행 중 사고가 났는지 여부를 기록할 수 있다.

[0173] 자동차 이력 정보 관리 장치(100)가 기 설정된 조건에 따라(예를 들어 자동차가 충돌한 것으로 인식한 경우) 자동차 식별 정보에 대응되는 자동차 활동 정보를 자동차 시스템(10)으로부터 수신하고, 수신한 자동차 활동 정보에 기초하여 자동차 이력 정보를 블록체인 네트워크(1)에 업데이트하는 트랜잭션을 자동으로 생성하도록 할 경우, 소유자가 자신에게 불리한 자동차 활동 정보를 숨기는 것을 방지할 수 있다.

[0175] 도 7은 본 발명의 몇몇 실시예에 따른 제 2 트랜잭션을 이용하여 자동차 이력 정보를 업데이트하는 방법의 일례를 나타낸 순서도이다.

[0176] 도 7을 참조하면, 자동차 이력 정보 관리 장치(100)의 제어부(130)는 관리자 단말(200)로부터 자동차 관리 정보를 수신한 경우(S310, Yes) 자동차 관리 정보가 유효한지 결정할 수 있다(S320). 여기서 자동차 관리 정보는, 상술한 바와 같이 간접적인 원인으로 인해 자동차의 상태가 변화되는 정보일 수 있다.

[0177] 제어부(130)는, 자동차 관리 정보에 포함된 데이터가 사전 결정된 조건을 만족할 때 자동차 관리 정보가 유효하다고 결정할 수 있다. 예를 들어, 제어부(130)는 자동차 관리 정보에 자동차 타이어 교체라는 데이터가 포함되어 있을 경우, 상기 자동차 관리 정보에 교환한 타이어의 위치 및 교환한 타이어 모델명이 포함되어 있다고 인식한 때 사전 결정된 조건이 만족되었다고 인식할 수 있다. 즉, 제어부(130)는 자동차 타이어 교체 데이터에 교환한 타이어 위치 및 교환한 타이어 모델명이 포함되어 있으면 자동차 관리 정보가 유효한 것으로 결정할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0178] 자동차 이력 정보 관리 장치(100)의 제어부(130)는 단계(S310)에서 수신한 자동차 관리 정보가 유효하다고 인식한 경우(S320, Yes), 블록체인 네트워크에 저장된 자동차 식별 정보에 대응되는 자동차 이력 정보를 자동차 관리 정보에 기초하여 업데이트하는 명령 코드 및 상기 명령 코드를 제 2 개인키로 암호화한 서명 데이터를 포함하는 제 2 트랜잭션을 생성할 수 있다(S330).

[0179] 그리고, 자동차 이력 정보 관리 장치(100)의 제어부(130)는 단계(S330)에서 생성한 제 2 트랜잭션 및 제 2 개인키에 대응되는 제 2 공개키를 상기 블록체인 네트워크에 전송할 수 있다(S340).

[0180] 블록체인 네트워크(1)는 제 2 트랜잭션을 수신하고, 유효한 트랜잭션으로 인식하여 제 2 트랜잭션을 블록에 저장할 경우, 자동차 식별 정보에 대응되는 자동차 이력 정보를 자동차 관리 정보에 기초하여 업데이트할 수 있다.

[0181] 블록체인 네트워크(1)는 제 2 트랜잭션을 수신하고, 유효하지 않은 트랜잭션으로 인식하여 제 2 트랜잭션을 블록에 저장하지 않을 경우, 자동차 이력 정보 관리 장치(100)에 유효하지 않은 트랜잭션이라는 피드백을 전송할 수 있다.

[0182] 블록체인 네트워크(1)는, 서명 데이터가 유효하지 않는 경우, 자동차 이력 정보 변경을 위한 잠금 해제키가 유효하지 않은 경우, 자동차 식별 정보에 대응되는 자동차 이력 정보가 존재하지 않는 경우 또는 자동차 관리 정보에 유효하지 않은 데이터가 포함되어 있는 경우에 수신한 트랜잭션을 유효하지 않은 트랜잭션으로 인식할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0183] 자동차 이력 정보 관리 장치(100)는 유효하지 않은 트랜잭션이라는 피드백을 수신할 경우, 이를 관리자 단말(200)에 전송할 수 있다.

[0184] 즉 자동차 이력 정보 관리 장치(100)는 관리자 단말(200)을 대신하여 블록체인 네트워크(1)에 자동차 이력 정보를 자동차 관리 정보에 기초하여 업데이트하는 트랜잭션을 전송할 수 있다.

[0185] 관리자 단말(200)이 직접 블록체인 네트워크(1)에 트랜잭션을 전송하는 것 대신에 자동차 이력 정보 관리 장치(100)가 관리자 단말(200)로부터 자동차 관리 정보를 수신하고, 자동차 이력 정보 관리 장치(100)가 자동차 이력 정보를 자동차 관리 정보에 기초하여 업데이트하는 트랜잭션을 블록체인 네트워크(1)에 전송할 경우, 관리자 단말(200)이 관리자로부터 자동차 식별 정보를 수신하는 과정을 생략할 수 있다. 이를 통해, 관리자 단말(200)이 관리자로부터 잘못된 자동차 식별 정보를 수신하는 것을 방지할 수 있다.

[0186] 그리고, 자동차 이력 정보 관리 장치(100)가 관리자 단말(200)을 대신하여 블록체인 네트워크(1)에 자동차 이력 정보를 자동차 관리 정보에 기초하여 업데이트하는 트랜잭션을 전송하고, 관리자 단말(200)이 자동차 이력 정보

변경을 위한 해제키를 저장하지 않고 자동차 이력 정보 관리 장치(100)가 저장해둘 경우, 자동차 식별 정보에 대응되는 자동차 이력 정보 변경을 위한 해제키가 외부 단말로 유출되지 않아, 악의적인 공격자로부터 자동차 이력 정보를 업데이트하는 것을 방지할 수 있다.

[0188] 도 8은 본 발명의 몇몇 실시예에 따른 제 3 트랜잭션을 이용하여 자동차 이력 정보를 업데이트하는 방법의 일례를 나타낸 순서도이다.

[0189] 도 8을 참조하면, 자동차 이력 정보 관리 장치(100)의 제어부(130)는 소유자 단말(300)로부터 소유권 관련 정보를 수신한 경우(S410, Yes), 소유권 관련 정보가 유효한지 결정할 수 있다(S420).

[0190] 여기서, 소유권 관련 정보는, 상술한 바와 같이 소유자가 자신의 자동차와 관련해서 사용할 수 있는 특정한 기능과 관련된 정보일 수 있다.

[0191] 제어부(130)는 소유권 관련 정보에 포함된 정보가 사전 결정된 조건을 만족할 경우, 소유권 관련 정보가 유효하다고 결정할 수 있다. 예를 들어, 소유권 관련 정보에 관리 접수 데이터가 포함되어 있을 경우, 관리 접수 데이터는 관리 접수 활성화를 위한 스마트 컨트랙트 주소 및 잠금 해제 키를 반드시 포함해야만 하는 것이 사전 결정된 조건일 수 있다. 제어부(130)는 소유권 관련 정보에 포함된 관리 접수 데이터가 관리 접수 활성화를 위한 스마트 컨트랙트 주소 및 잠금 해제 키를 포함하고 있을 경우, 소유권 관련 정보가 유효한 것으로 결정할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0192] 한편, 소유권 관련 정보와 관련된 잠금 해제키를 자동차 이력 정보 관리 장치(100)에 저장해둘 경우 자동차와 자동차 이력 정보 관리 장치(100)가 도난될 때 소유권 관련 정보와 관련된 잠금 해제키가 같이 유출될 수 있으므로, 소유권 관련 정보와 관련된 잠금 해제키는 소유자 단말(300)에 저장해두는 것이 바람직할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0193] 자동차 이력 정보 관리 장치(100)의 제어부(130)는 단계(S410)에서 수신한 소유권 관련 정보가 유효하다고 인식한 경우(S420, Yes), 블록체인 네트워크에 저장된 자동차 식별 정보에 대응되는 자동차 이력 정보를 소유권 관련 정보에 기초하여 업데이트하는 명령 코드 및 상기 명령 코드를 제 3 개인키로 암호화한 서명 데이터를 포함하는 제 3 트랜잭션을 생성할 수 있다(S430).

[0194] 그리고, 자동차 이력 정보 관리 장치(100)의 제어부(130)는 단계(S430)에서 생성한 제 3 트랜잭션 및 제 3 개인키에 대응되는 제 3 공개키를 블록체인 네트워크에 전송할 수 있다.

[0195] 블록체인 네트워크(1)는 제 3 트랜잭션을 수신하고, 유효한 트랜잭션으로 인식하여 제 3 트랜잭션을 블록에 저장할 경우, 자동차 식별 정보에 대응되는 자동차 이력 정보를 소유권 관련 정보에 기초하여 업데이트할 수 있다.

[0196] 블록체인 네트워크(1)는 제 3 트랜잭션을 수신하고, 유효하지 않은 트랜잭션으로 인식하여 트랜잭션을 블록에 저장하지 않을 경우, 자동차 이력 정보 관리 장치(100)에 유효하지 않은 트랜잭션이라는 피드백을 전송할 수 있다.

[0197] 블록체인 네트워크(1)는 서명 데이터가 유효하지 않는 경우, 자동차 이력 정보 변경을 위한 잠금 해제키가 유효하지 않은 경우, 자동차 식별 정보에 대응되는 자동차 이력 정보가 존재하지 않는 경우에 수신한 트랜잭션을 유효하지 않은 트랜잭션으로 인식할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0198] 자동차 이력 정보 관리 장치(100)는 유효하지 않은 트랜잭션이라는 피드백을 수신할 경우, 이를 소유자 단말(300)에 전송할 수 있다.

[0199] 즉 자동차 이력 정보 관리 장치(100)는 소유자 단말(300)을 대신하여 블록체인 네트워크(1)에 자동차 이력 정보를 업데이트하는 트랜잭션을 전송할 수 있다.

[0200] 소유자 단말(300)이 직접 블록체인 네트워크(1)에 트랜잭션을 전송하는 것 대신에 자동차 이력 정보 관리 장치(100)가 소유자 단말(300)로부터 자동차 관리 정보를 수신하고, 자동차 이력 정보 관리 장치(100)가 자동차 이력 정보를 업데이트하는 트랜잭션을 블록체인 네트워크(1)에 전송할 경우, 소유자 단말(300)이 소유자로부터 자동차 식별 정보를 수신하는 과정을 생략할 수 있다. 이를 통해, 소유자 단말(300)은 소유자로부터 잘못된 자동차 식별 정보를 수신하는 것을 방지할 수 있다.

[0201] 몇몇 실시예에 따르면 블록체인 네트워크(1)는 소유권 관련 정보 중 일부에 대해서는 소유자 단말(300)을 통해서만 자동차의 이력 정보를 업데이트 가능하게 허용하고, 다른 일부 기능에 대해서는 자동차 이력 정보 관리 장

치(100)를 통해서만 자동차의 이력 정보를 업데이트 가능하게 허용할 수 있다.

[0202] 예를 들어, 소유권 관련 정보 중 도난 신고의 경우 도난된 상태일 경우 자동차 이력 정보 관리 장치(100)에 접속하기 힘들 것이고, 자동차 이력 정보 관리 장치(100)와 접속할 수 있는 상태이면 자동차가 도난되지 않은 상태일 것이다. 따라서, 블록체인 네트워크(1)는 자동차 이력 정보 관리 장치(100)로부터는 도난 신고를 받지 않도록 설정해 둬 특정 장치가 보내기에 부적합한 트랜잭션에 대해 잘못된 트랜잭션으로 설정할 수 있다. 이로 인해 블록체인 네트워크(1)는 자동차 이력 정보 관리 장치(100)가 사용자로부터 잘못된 트랜잭션을 입력하여 실수로 도난신고를 하는 것을 방지할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0203] 따라서, 블록체인 네트워크(1)는 소유권 관련 정보 중 일부에 대해서는 소유자 단말(300)을 통해서만 자동차의 이력 정보를 업데이트 가능하게 허용하고, 다른 일부 기능에 대해서는 자동차 이력 정보 관리 장치(100)를 통해서만 자동차의 이력 정보를 업데이트 가능하게 허용하고, 또 다른 일부에 대해서는 소유자 단말(300) 및 자동차 이력 정보 관리 장치(100)에 관계없이 업데이트 가능하게 허용할 수 있다. 이를 통해 블록체인 네트워크(1)는 자동차 이력 정보 관리 장치(100)가 전송하기 부적합한 트랜잭션은 유효한 트랜잭션으로 인식하지 않고, 자동차 이력 정보 관리 장치(100)가 전송하기 적합한 트랜잭션은 유효한 트랜잭션으로 인식할 수 있다. 다만 상술한 예들은 일 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0205] 도 9는 본 발명의 몇몇 실시예에 따른 조회자 단말에 자동차 이력 정보를 전송하는 방법의 일례를 나타낸 순서도이다.

[0206] 도 9를 참조하면, 자동차 이력 정보 관리 장치(100)의 제어부(130)는 조회자 단말(400)로부터 자동차 이력 정보 조회 요청 신호를 수신한 경우(S510, Yes), 자동차 이력 정보 조회 요청 신호가 유효한지 결정할 수 있다(S520).

[0207] 여기서 자동차 이력 정보 조회 요청 신호는, 상술한 바와 같이 자동차 이력 정보를 조회하기 위해 필요한 정보일 수 있다.

[0208] 일례로, 제어부(130)가 자동차 이력 정보 조회 요청 신호가 유효한지 결정하는 방법은 자동차 이력 정보 관리 장치(100)가 자동차 이력 정보에 포함된 정보 중 자동차 이력 정보 조회 허용 여부가 허용인 것으로 인식한 경우, 자동차 이력 정보 조회 요청 신호가 유효한 것으로 결정하는 방법일 수 있다.

[0209] 다른 일례로, 제어부(130)가 자동차 이력 정보 조회 요청 신호가 유효한지 결정하는 방법은, 통신부(110)가 소유자 단말(300)에 자동차 이력 정보 조회 요청 신호를 전송하고, 소유자 단말(300)로부터 자동차 이력 정보 조회 허용 신호를 수신할 경우, 자동차 이력 정보 조회 요청 신호가 유효한 것으로 결정하는 방법일 수 있다.

[0210] 다만 상술한 자동차 이력 정보 조회 요청 신호가 유효한지 결정하는 방법은 일 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0211] 자동차 이력 정보 관리 장치(100)의 제어부(130)는 단계(S510)에서 수신한 자동차 이력 정보 조회 요청 신호가 유효하다고 인식한 경우(S520, Yes), 조회자 단말(400)에 자동차 이력 정보를 전송할 수 있다(S530).

[0212] 조회자 단말(400)이 자동차 이력 정보 관리 장치(100)를 통해 자동차 이력 정보를 조회 경우, 조회자 단말(400)은 조회할 자동차 식별 정보를 수신하는 과정을 생략할 수 있다. 이를 통해 조회자 단말(400)은 사용자로부터 잘못된 자동차의 식별 정보를 수신하여 잘못된 자동차 이력 정보를 조회하는 것을 방지할 수 있다.

[0213]

[0214] 도 10는 본 발명의 몇몇 실시예에 따른 소유자 단말에 자동차 정기 검진 권유 정보를 전송하는 방법의 일례를 나타낸 순서도이다.

[0215] 도 10을 참조하면, 자동차 이력 정보 관리 장치(100)의 제어부(130)는 메모리에 저장된 자동차 이력 정보에 기초하여, 자동차 정기 검진 조건이 만족한 경우(S610, Yes), 소유자 단말(300)에 자동차 정기 검진 권유 정보를 전송할 수 있다(S620).

[0216] 여기서 자동차 정기 검진 조건은 자동차 이력 정보에 기초하여, 자동차 이력 정보에 포함된 일부 데이터가 기설정된 조건을 만족하는 것일 수 있다.

[0217] 예를 들어, 제어부(130)는 자동차 이력 정보에 포함된 차종 정보 및 마지막 엔진 오일을 교환했던 날로부터 기설정된 km(예를 들어, 10000km)가 더 운행된 경우 기 설정된 조건을 만족되었다고 인식할 수 있다. 그리고 제어

부(130)는 기 설정된 조건이 만족된 경우, 소유자 단말(300)에 엔진오일 교환 권유 정보를 전송하도록 통신부(110)를 제어할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0218] 자동차 이력 정보 관리 장치(100)는 소유자 단말(300)에 자동차 정기 검진 권유 정보를 전송하여, 소유자에게 자동차 검진에 관한 정보를 알려줄 수 있다. 이로 인해 소유자는 언제 정기 검진을 받는 것이 좋은 지, 어떤 부품을 언제 교환하는 것이 좋은 지 등을 쉽게 확인할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0220] 도 11은 본 발명의 몇몇 실시예에 따른 자동차 시스템에 운행 금지 요청 정보를 전송하는 방법의 일례를 나타낸 순서도이다.

[0221] 자동차 이력 정보 관리 장치(100)의 통신부(110)는 운행 금지 관련 정보가 포함된 자동차 이력 정보를 수신할 수 있다.

[0222] 한편, 도 11을 참조하면, 자동차 이력 정보 관리 장치(100)의 제어부(130)는 상기 수신된 자동차 이력 정보에 운행 금지 관련 정보가 포함되어 있다고 인식한 경우(S710, Yes), 운행 금지 관련 정보가 유효한지 결정할 수 있다(S720).

[0223] 여기서, 운행 금지 관련 정보는 소유자 단말(300)이 소유권 관련 정보에 기초하여(예를 들어 도난 신고 정보에 기초하여) 자동차 이력 정보를 업데이트하는 트랜잭션을 블록체인 네트워크(1)에 전송하고, 트랜잭션이 블록에 포함되어 자동차 이력 정보에 포함된 것일 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0224] 자동차 이력 정보 관리 장치(100)의 제어부(130)는 단계(S710)의 운행 금지 관련 정보가 유효하다고 인식한 경우(S720, Yes), 자동차 시스템(10)에 운행 금지 요청 정보를 전송할 수 있다(S730).

[0225] 제어부(130)는 운행 금지 관련 정보에 잘못된 데이터가 포함되어 있지 않은 경우 또는 운행 금지 관련 정보에 포함된 서명 정보가 유효한 경우, 운행 금지 관련 정보가 유효하다고 인식할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0226] 또한, 자동차 시스템(10)은 자동차 이력 정보 관리 장치(100)가 단계(S730)에서 전송한 운행 금지 요청 정보를 수신할 수 있다.

[0227] 그리고 자동차 시스템(10)은 운행 금지 요청 정보를 수신한 경우, 운행 금지 요청 정보가 유효한지 결정할 수 있다.

[0228] 여기서 자동차 시스템(10)은 운행 금지 요청 정보에 잘못된 데이터가 포함되어 있지 않은 경우 또는 운행 금지 관련 정보에 포함된 서명 정보가 유효한 경우, 운행 금지 요청 정보가 유효하다고 결정할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0229] 자동차 시스템(10)이 운행 금지 요청 정보가 유효하다고 결정한 경우, 자동차 시스템(10)은 운행 금지 모드로 전환할 수 있다.

[0230] 예를 들어, 자동차 시스템(10)은 운행 금지 모드로 전환할 경우, 현재 운행에 대해서는 자동차의 조작에 대해 제한하지 않고, 현재 운행이 종료되어 시동이 완전히 꺼진 후 다음 시동이 걸렸을 때 자동차의 조작에 대해 제한하고, 운행 금지 상태이므로 해제가 필요하다는 메시지를 출력할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0231] 위와 같은 과정을 통해 자동차 이력 정보 관리 장치(100)는 자동차 시스템(10)에게 자동차의 운행을 제한하도록 요청할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0233] 도 12는 본 발명의 다른 몇몇 실시예에 따른 애플리케이션을 통해 단말에 표시되는 화면의 일례를 나타낸 도면이다.

[0234] 도 12를 참조하면, 화면(600)은 자동차 ID 정보(601), 계정 정보(602), 간단정보 메뉴(603), 관리정보 메뉴(604), 상세정보 메뉴(605), 정보 표시 객체(606) 및 특수기능 관련 정보 메뉴(610)를 포함할 수 있다. 다만, 상술한 구성 요소들은 화면(600)을 구현하는데 있어서 필수적인 것은 아니어서, 화면(600)은 위에서 열거된 구성요소들 보다 많거나, 또는 적은 구성 요소들을 가질 수 있다.

[0235] 화면(600)은 단말이 블록체인 네트워크(1)와 직접 연결되거나, 자동차 이력 정보 관리 장치(100)를 통해 연결되

었을 경우 디스플레이되는 자동차 이력 정보와 관련된 화면일 수 있다.

[0236] 자동차 ID 정보(601)는 자동차 식별 정보와 관련된 정보일 수 있다.

[0237] 몇몇 실시예에 따르면, 자동차 ID 정보(601)는 사용자 단말에서만 디스플레이될 수 있고, 관리자 단말, 조회자 단말 및 제조사 단말 등에서는 디스플레이되지 않을 수 있다. 다만, 관리자 단말 또는 조회자 단말이 자동차 이력 정보 관리 장치(100)와 연결되는 경우, 자동차 ID 정보(601)가 관리자 단말 또는 조회자 단말에서 디스플레이될 수도 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0238] 계정 정보(602)는 현재 연결된 단말의 계정 ID를 나타낸 정보일 수 있다. 몇몇 실시예에 따르면, 계정 정보(602)는 인증 결과 데이터에 기초하여 표시될 수 있다. 예를 들어 소유자 단말(300)일 경우, 자동차 소유자라는 정보를 더 표시할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0239] 간단정보 메뉴(603)는 정보 표시 객체(606)에 자동차와 관련된 간단정보를 표시하도록 제어하기 위해 구비된 메뉴일 수 있다.

[0240] 관리정보 메뉴(604)는 정보 표시 객체(606)에 자동차와 관련된 관리정보를 표시하도록 제어하기 위해 구비된 메뉴일 수 있다.

[0241] 상세정보 메뉴(605)는 정보 표시 객체(606)에 상세정보를 표시하도록 제어하기 위해 구비된 메뉴일 수 있다.

[0242] 정보 표시 객체(606)는 간단정보 메뉴(603), 관리정보 메뉴(604) 및 상세정보 메뉴(605) 중 사용자로부터 선택된 메뉴에 따라 다르게 표시될 수 있다.

[0243] 일례로, 간단정보 메뉴(603)가 선택된 경우, 자동차와 관련된 간단정보가 정보 표시 객체(606)에 표시될 수 있다. 여기서, 정보 표시 객체(606)는 "차종, 생산년도, 제조일, 주행거리, 현재 소유자, 차량등록여부, 대여 여부, 수리 접수 여부, 이력 조회 허용 및 도난 신고 여부"가 표시될 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0244] 다른 일례로 관리정보 메뉴(604)가 선택된 경우, 자동차와 관련된 관리정보가 정보 표시 객체(606)에 표시할 수 있다. 여기서, 정보 표시 객체(606)는 "2016.08.10 자동차 제조, 2016.10.20 A자동차 유통점에서 자동차 인수, 2017.10.20 한국 정부에 자동차 등록완료, 2017.12.20 B정비소에서 엔진오일 교체, 2018.01.20 C정비소에서 타이어 교체"가 표시될 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0245] 또 다른 일례로 상세정보 메뉴(605)가 선택된 경우, 자동차와 관련된 상세정보 가 정보 표시 객체(606)에 표시될 수 있다. 여기서, 정보 표시 객체(606)는 "2017.12.19 엔진 정지, 2018.01.18 자동차에 강한 충돌감지, 급격한 감속감지"가 표시될 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0246] 몇몇 실시예에 따르면, 자동차 이력 정보의 조회가 허용되지 않은 단말이 자동차 이력 정보를 조회하는 경우, 자동차 이력 정보의 조회가 필요하다는 텍스트가 정보 표시 객체(606)에 표시될 수 있다.

[0247] 예를 들어, 자동차 이력 정보의 조회가 허용되지 않은 단말이 자동차 이력 정보를 조회하는 경우, 정보 표시 객체(606)에는 "자동차 식별 정보에 해당하는 자동차 이력 정보를 조회할 수 없습니다."라는 텍스트가 표시될 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0248] 특수기능 관련 정보 메뉴(610)는 접속한 단말의 종류에 따라 사용할 수 있는 특수한 기능들에 관한 트랜잭션을 생성하기 위한 메뉴들을 제공하기 위해 구비된 메뉴일 수 있다.

[0249] 몇몇 실시예에 따르면, 특수기능 관련 정보 메뉴(610)는 단말의 종류에 따라 다르게 표시될 수 있다. 여기서 블록체인 네트워크(1)에서 전송받은 인증 결과 데이터에 따라 다르게 표시될 수 있다.

[0250] 일례로, 블록체인 네트워크(1)에서 전송받은 인증 결과 데이터가 소유자일 경우, 도 12와 같이 개인인증변경 메뉴(611), 소유권이전 메뉴(612), 대여 메뉴(613), 관리접수 메뉴(614), 이력조회허용 메뉴(615) 및 도난신고 메뉴(616)가 특수기능 관련 정보 메뉴(610)에 표시될 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0251] 개인인증변경 메뉴(611)는 자동차 이력 정보에 포함된 개인 인증 정보를 변경하고자 할 때 사용될 수 있다. 단말은, 개인인증변경 메뉴(611)가 선택된 경우, 자동차 이력 정보를 소유권 관련 정보 중 개인 인증 정보 변경 정보에 기초하여 업데이트하는 트랜잭션을 생성하기 위한 절차를 수행할 수 있다.

[0252] 여기서 개인 인증 정보 변경 정보는, 블록체인 네트워크(1)에서 저장된 자동차 이력 정보에 포함된 정보 중 개

인 인증 정보(예를 들어 잠금 해제키)를 변경하기위한 정보를 포함할 수 있다. 일례로, 개인 인증 정보 변경 정보는, 기존의 개인 인증 정보 및 변경할 개인 인증 정보를 포함할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0253] 소유권이전 메뉴(612)는 소유자가 소유하고 있는 자동차를 다른 사람에게 판매하고자 할 때 사용될 수 있다. 단말은, 소유권이전 메뉴(612)가 선택된 경우, 자동차 이력 정보를 소유권 관련 정보 중 소유권 이전 정보에 기초하여 업데이트하는 트랜잭션을 생성하기 위한 절차를 수행할 수 있다.

[0254] 여기서 소유권 이전 정보는, 블록체인 네트워크(1)에 저장된 자동차 이력 정보에 포함된 정보 중 소유권 정보를 업데이트하기 위한 정보를 포함할 수 있다. 일례로, 소유권 이전 정보는, 개인 인증 정보, 새로운 소유자에 관한 정보 및 소유권을 넘기기 위한 조건 정보를 포함할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0255] 대여 메뉴(613)는 소유자가 소유하고 있는 자동차를 다른 사람에게 대여하고자 할 때 사용될 수 있다. 단말은, 대여 메뉴(613)가 선택된 경우, 자동차 이력 정보를 소유권 관련 정보 중 자동차 대여 정보에 기초하여 업데이트하는 트랜잭션을 생성하기 위한 절차를 수행할 수 있다.

[0256] 여기서 자동차 대여 정보는, 블록체인 네트워크(1)에 저장된 자동차 이력 정보에 대여 정보를 포함시키기 위한 정보를 포함할 수 있다. 일례로, 자동차 대여 정보는, 개인 인증 정보, 대여자에 관한 정보 및 대여가 중지되는 조건에 관한 정보를 포함할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0257] 관리접수 메뉴(614)는 소유자가 소유하고 있는 자동차를 관리자에게 접수하여 자동차 관리 정보를 추가하는 것을 허용하고자 할 때 사용될 수 있다. 단말은, 관리접수 메뉴(614)가 선택된 경우, 자동차 이력 정보를 소유권 관련 정보 중 자동차 관리 접수 정보에 기초하여 업데이트하는 트랜잭션을 생성하기 위한 절차를 수행할 수 있다.

[0258] 여기서 자동차 관리 접수 정보는, 블록체인 네트워크(1)에 저장된 자동차 이력 정보를 업데이트할 수 있는 권한을 특정 관리자에게 부여하기 위한 정보를 포함할 수 있다. 일례로, 자동차 관리 접수 정보는, 개인 인증 정보, 관리자에 관한 정보 및 관리접수가 중지되는 조건에 관한 정보를 포함할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0259] 이력조회허용 메뉴(615)는 소유자가 소유하고 있는 자동차에 관하여 조회자에게 자동차 이력 정보를 조회하는 것을 허용하고자 할 때 사용될 수 있다. 단말은 이력조회허용 메뉴(615)가 선택된 경우, 자동차 이력 정보를 소유권 관련 정보 중 자동차 이력 조회 허용 정보에 기초하여 업데이트하는 트랜잭션을 생성하기 위한 절차를 수행할 수 있다.

[0260] 여기서 자동차 이력 조회 허용 정보는, 블록체인 네트워크(1)에 저장된 자동차 이력 정보를 열람할 수 있는 권한을 특정인에게 부여하기 위한 정보를 포함할 수 있다.

[0261] 일례로, 자동차 이력 조회 허용 정보는, 개인 인증 정보, 조회자에 관한 정보 및 조회가 중지되는 조건에 관한 정보를 포함할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0262] 도난신고 메뉴(616)는 소유자가 소유하고 있는 자동차에 관하여 도난을 당했을 때 신고하기 위하여 사용될 수 있다. 단말은 도난신고 메뉴(616)가 선택된 경우, 자동차 이력 정보를 소유권 관련 정보 중 도난 신고 정보에 기초하여 업데이트하는 트랜잭션을 생성하기 위한 절차를 수행할 수 있다.

[0263] 여기서 도난 신고 정보는 블록체인 네트워크(1)에 저장된 자동차 이력 정보에 운행 금지 관련 정보를 포함시키기 위한 정보를 포함할 수 있다. 일례로, 도난 신고 정보는 개인 인증 정보 및 도난 신고가 중지되는 조건에 관한 정보를 포함할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0264] 다른 일례로, 블록체인 네트워크(1)에서 전송받은 인증 결과 데이터가 관리 정보 추가 메뉴 등이 특수기능 관련 정보 메뉴(610)에 표시될 수 있다.

[0265] 관리 정보 추가 메뉴는 관리자가 접수받은 자동차에 관하여 자동차 관리 정보를 자동차 이력 정보에 추가하기 위하여 사용될 수 있다. 단말은 관리 정보 추가 메뉴가 선택된 경우, 블록체인 네트워크에 저장된 자동차 식별 정보에 대응되는 자동차 이력 정보를 자동차 관리 정보에 기초하여 업데이트하기 위한 절차를 수행할 수 있다.

[0266] 또, 다른 일례로, 블록체인 네트워크(1)에서 전송받은 인증 결과 데이터가 조회자일 경우, 이력 정보 조회 요청 메뉴 등이 특수기능 관련 정보 메뉴(610)에 표시될 수 있다.

[0267] 이력 정보 조회 요청 메뉴는 블록체인 네트워크(1) 또는 자동차 이력 정보 관리 장치(100)에 저장된 자동차 이력 정보의 전송을 요청하기 위해 사용될 수 있다. 단말은, 이력 정보 조회 요청 메뉴가 선택된 경우, 블록체인 네트워크(1) 또는 자동차 이력 정보 관리 장치(100)에 자동차 이력 정보 조회 요청 신호를 전송하기 위한 절차를 수행할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0268] 여기서 자동차 이력 정보 조회 요청 신호는, 조회하고자 하는 자동차에 대응되는 자동차 식별 정보 및 조회하는 조회자에 관한 정보를 포함할 수 있다. 다만 이는 예시일 뿐이며, 본 개시는 이에 제한되지 않는다.

[0269] 또 다른 일례로, 블록체인 네트워크(1)에서 전송받은 인증 결과 데이터가 제조사일 경우, 자동차 등록 메뉴 등이 특수기능 관련 정보 메뉴(610)에 표시될 수 있다.

[0270] 자동차 등록 메뉴는 블록체인 네트워크(1)에 자동차의 이력 정보를 최초로 등록하기 위해 사용될 수 있다. 단말은, 자동차 등록 메뉴가 선택된 경우, 블록체인 네트워크(1)에 자동차 이력 정보를 최초로 등록하기 위한 절차를 수행할 수 있다. 다만 이는 예시일 뿐이며 본 개시는 이에 제한되지 않는다.

[0271] 특수기능 관련 정보 메뉴(610)와 관련하여 상술한 예들은 일 예시일 뿐이며, 특수기능 관련 정보 메뉴(610)는 상술한 예들로 제한되지 않는다.

[0273] 전술한 본 발명은, 프로그램이 기록된 매체에 컴퓨터가 판독 가능한 코드로서 구현하는 것이 가능하다.

[0274] 몇몇 실시예에 따르면, 컴퓨터로 판독 가능한 매체는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM 및 DVD와 같은 광매체 및 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical medium)일 수도 있고 캐리어 웨이브(예를 들어, 인터넷을 통한 정송)의 형태로 구현될 수도 있다.

[0275] 다른 몇몇 실시예에 따르면, 컴퓨터로 판독 가능한 매체는, 프로그램 명령어를 저장하고 실행하도록 특별히 구성된 하드웨어 장치일 수 있다. 여기서, 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0276] 일례로, 매체는 RAM(random access memory), SRAM(static RAM), DRAM (dynamic RAM), SDRAM(synchronous DRAM), T-RAM(thyristor RAM), Z-RAM(zero capacitor RAM), TTRAM(Twin Transistor RAM) 또는 SRAM(Static Random Access Memory)과 같은 휘발성 메모리일 수 있다.

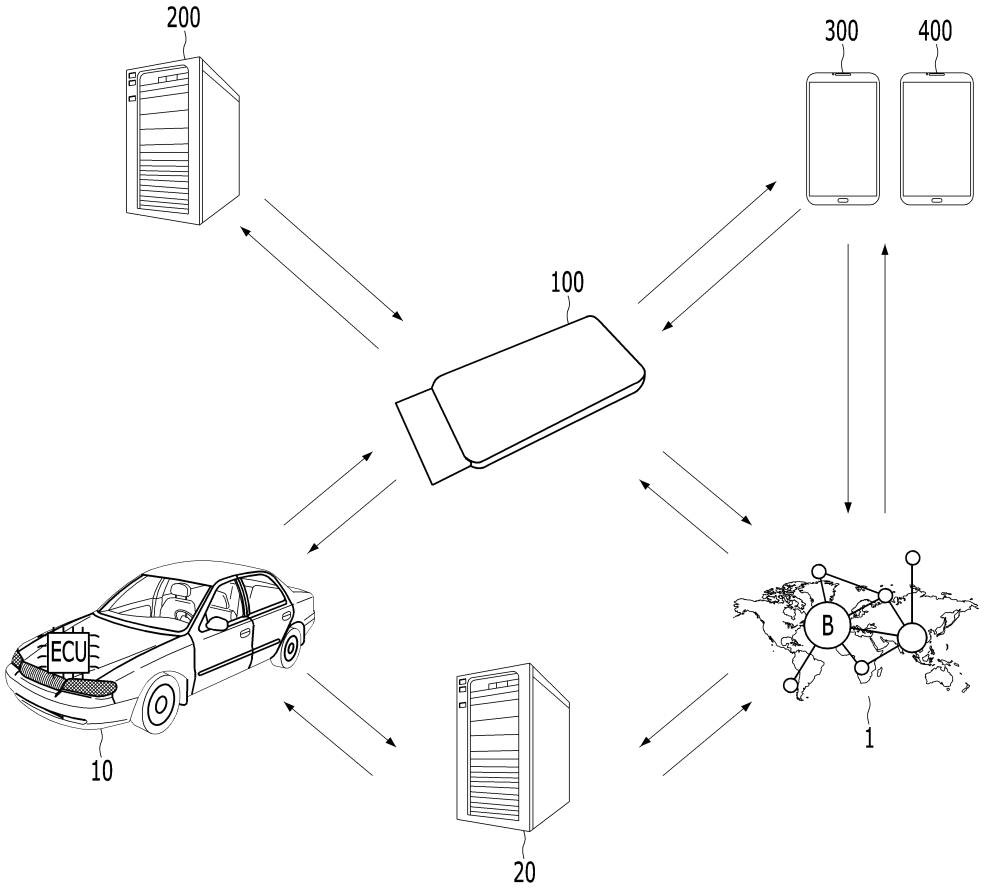
[0277] 다른 일례로, 매체는 낸드 플래시 메모리(NAND Flash Memory), 수직형 낸드 플래시 메모리(Vertical NAND; VNAND), 노아 플래시 메모리(NOR Flash Memory), 저항성 램(Resistive Random Access Memory: RRAM), 상변화 메모리(Phase-Change Memory: PRAM), 자기저항 메모리(Magneto resistive Random Access Memory: MRAM), 강유전체 메모리(Ferroelectric Random Access Memory:FRAM), 스핀주입 자화반전 메모리(Spin Transfer Torque Random Access Memory:STT-RAM) 등과 같은 비휘발성 메모리일 수 있다.

[0278] 한편, 상기 컴퓨터 프로그램은 본 발명을 위하여 특별히 설계되고 구성된 것이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수 있다. 컴퓨터 프로그램의 예에는, 컴파일러에 의하여 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용하여 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함될 수 있다

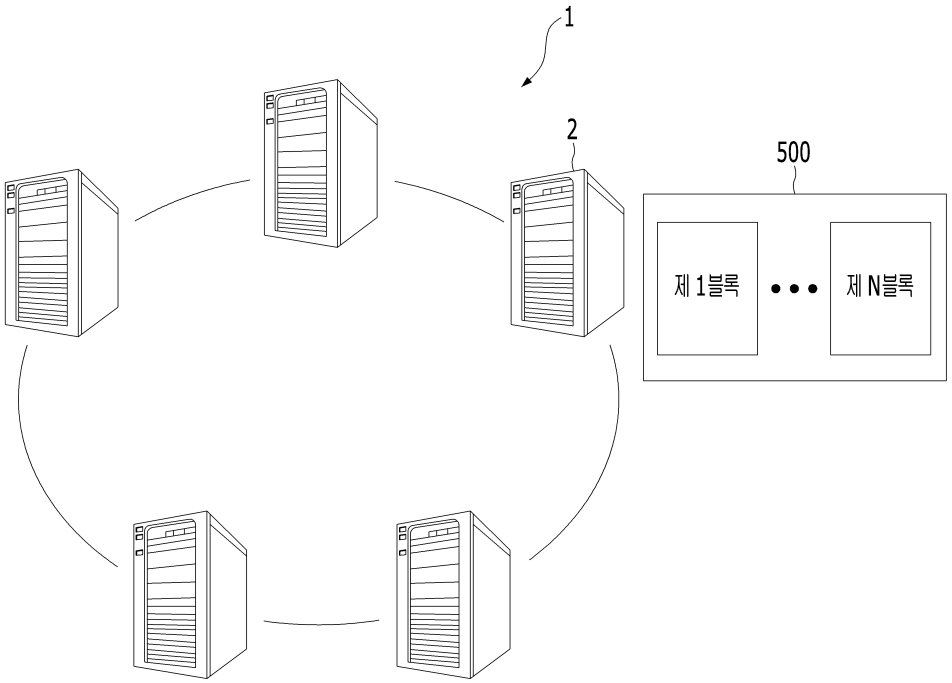
[0279] 제시된 실시예들에 대한 설명은 임의의 본 개시의 기술 분야에서 통상의 지식을 가진 자가 본 개시를 이용하거나 또는 실시할 수 있도록 제공된다. 이러한 실시예들에 대한 다양한 변형들은 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 명백할 것이며, 여기에 정의된 일반적인 원리들은 본 개시의 범위를 벗어남이 없이 다른 실시예들에 적용될 수 있다. 그리하여, 본 개시는 여기에 제시된 실시예들로 한정되는 것이 아니라, 여기에 제시된 원리들 및 신규한 특징들과 일관되는 최광의의 범위에서 해석되어야 할 것이다.

도면

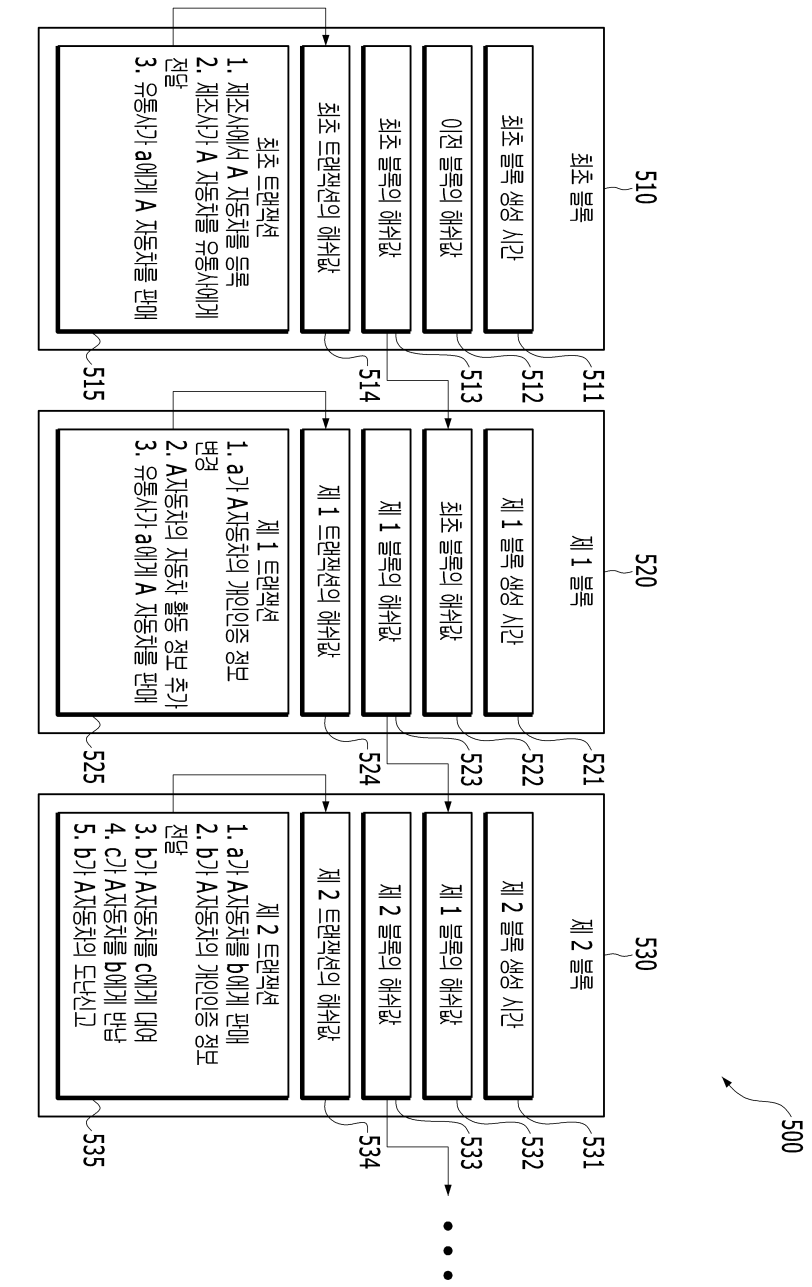
도면1



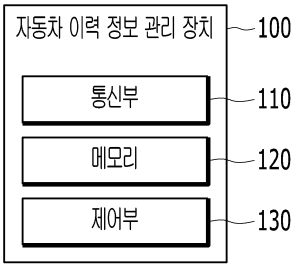
도면2



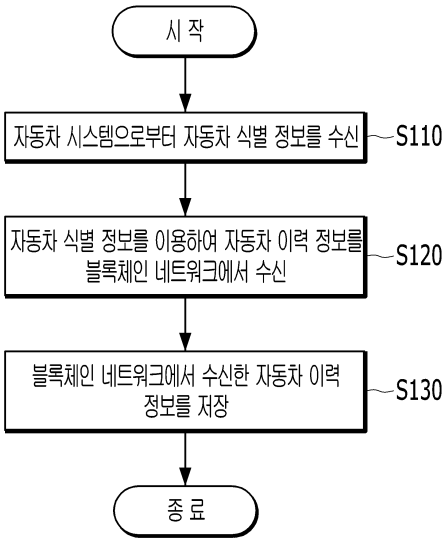
도면3


최초 블록
최초 블록 생성 시간
이전 블록의 해쉬값
최초 블록의 해쉬값
최초 트랜잭션의 해쉬값
최초 트랜잭션
1. 제조사에서 A 자동차를 등록
2. 제조사가 A 자동차를 유통사에게 전달
3. 유통사가 a에게 A 자동차를 판매
510
511
512
513
514
515
제 1 블록
제 1 블록 생성 시간
최초 블록의 해쉬값
제 1 블록의 해쉬값
제 1 트랜잭션의 해쉬값
제 1 트랜잭션
1. a가 A자동차의 개인인증 정보 변경
2. A자동차의 자동차 활동 정보 추가
3. 유통사가 a에게 A 자동차를 판매
520
521
522
523
524
525
제 2 블록
제 2 블록 생성 시간
제 1 블록의 해쉬값
제 2 블록의 해쉬값
제 2 트랜잭션의 해쉬값
제 2 트랜잭션
1. a가 A자동차를 b에게 판매
2. b가 A자동차의 개인인증 정보 전달
3. b가 A자동차를 c에게 대여
4. c가 A자동차를 b에게 반납
5. b가 A자동차의 도난신고
530
531
532
533
534
535
500

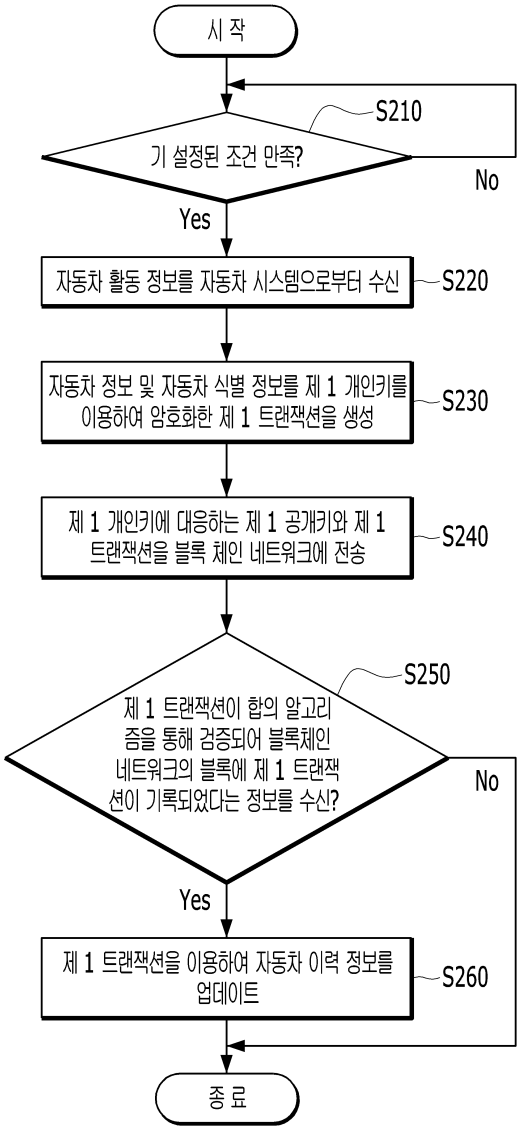
도면4


자동차 이력 정보 관리 장치
100
통신부
110
메모리
120
제어부
130

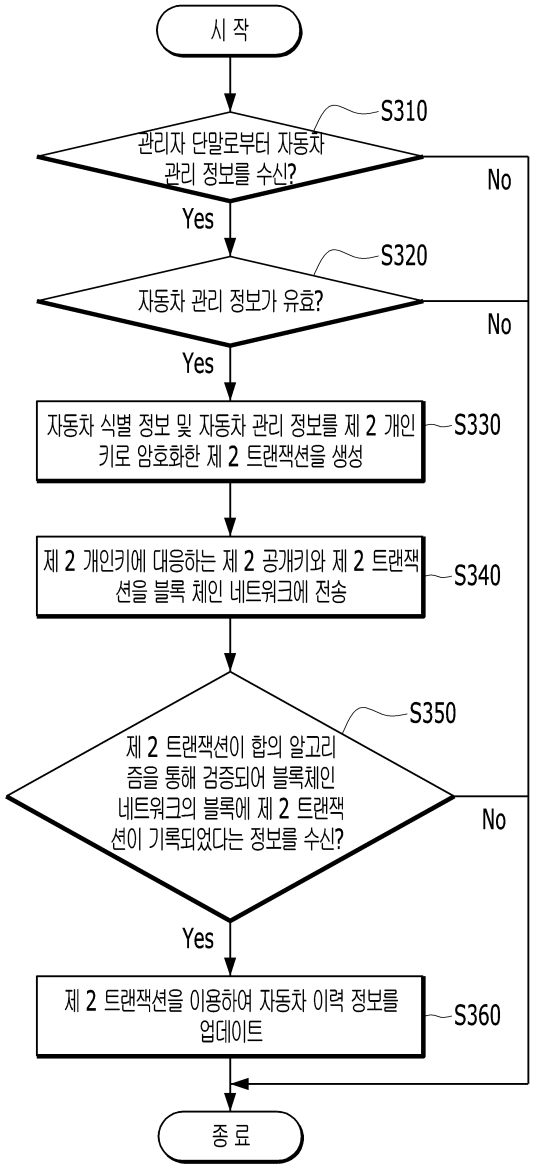
도면5


시 작
자동차 시스템으로부터 자동차 식별 정보를 수신
S110
자동차 식별 정보를 이용하여 자동차 이력 정보를 블록체인 네트워크에서 수신
S120
블록체인 네트워크에서 수신한 자동차 이력 정보를 저장
S130
종 료

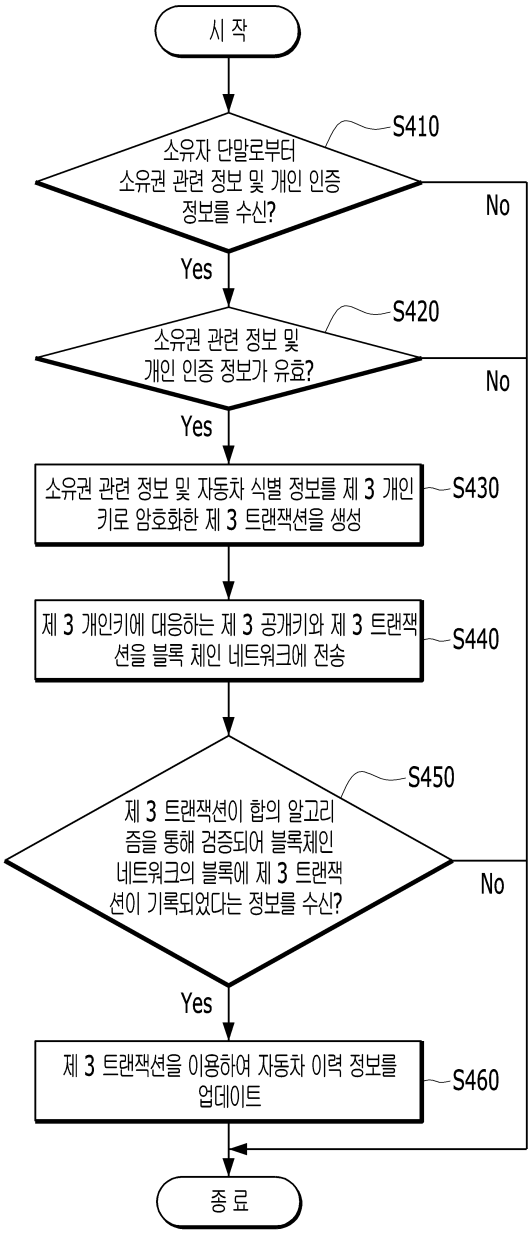
도면6


시 작
S210
기 설정된 조건 만족?
No
Yes
자동차 활동 정보를 자동차 시스템으로부터 수신
S220
자동차 정보 및 자동차 식별 정보를 제 1 개인키를 이용하여 암호화한 제 1 트랜잭션을 생성
S230
제 1 개인키에 대응하는 제 1 공개키와 제 1 트랜잭션을 블록 체인 네트워크에 전송
S240
S250
제 1 트랜잭션이 합의 알고리즘을 통해 검증되어 블록체인 네트워크의 블록에 제 1 트랜잭션이 기록되었다는 정보를 수신?
No
Yes
제 1 트랜잭션을 이용하여 자동차 이력 정보를 업데이트
S260
종 료

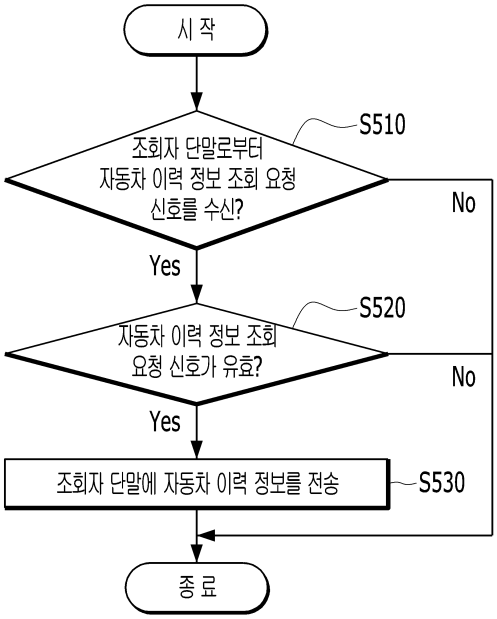
도면7


시 작
S310
관리자 단말로부터 자동차 관리 정보를 수신?
No
Yes
S320
자동차 관리 정보가 유효?
No
Yes
자동차 식별 정보 및 자동차 관리 정보를 제 2 개인키로 암호화한 제 2 트랜잭션을 생성
S330
제 2 개인키에 대응하는 제 2 공개키와 제 2 트랜잭션을 블록 체인 네트워크에 전송
S340
S350
제 2 트랜잭션이 합의 알고리즘을 통해 검증되어 블록체인 네트워크의 블록에 제 2 트랜잭션이 기록되었다는 정보를 수신?
No
Yes
제 2 트랜잭션을 이용하여 자동차 이력 정보를 업데이트
S360
종 료

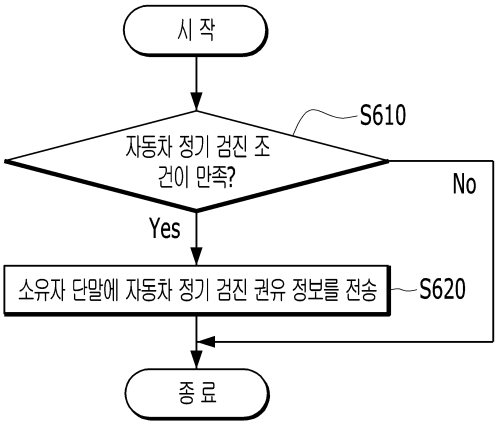
도면8


시작
S410
소유자 단말로부터 소유권 관련 정보 및 개인 인증 정보를 수신?
No
Yes
S420
소유권 관련 정보 및 개인 인증 정보가 유효?
No
Yes
소유권 관련 정보 및 자동차 식별 정보를 제 3 개인키로 암호화한 제 3 트랜잭션을 생성
S430
제 3 개인키에 대응하는 제 3 공개키와 제 3 트랜잭션을 블록 체인 네트워크에 전송
S440
S450
제 3 트랜잭션이 합의 알고리즘을 통해 검증되어 블록체인 네트워크의 블록에 제 3 트랜잭션이 기록되었다는 정보를 수신?
No
Yes
제 3 트랜잭션을 이용하여 자동차 이력 정보를 업데이트
S460
종료

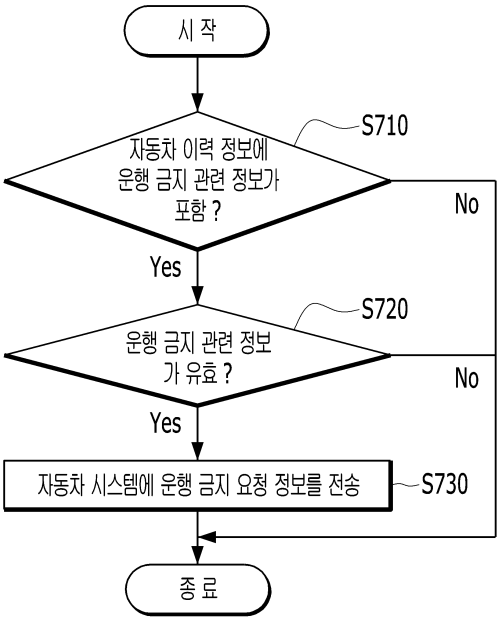
도면9


시 작
조회자 단말로부터 자동차 이력 정보 조회 요청 신호를 수신?
S510
No
Yes
자동차 이력 정보 조회 요청 신호가 유효?
S520
No
Yes
조회자 단말에 자동차 이력 정보를 전송
S530
종 료

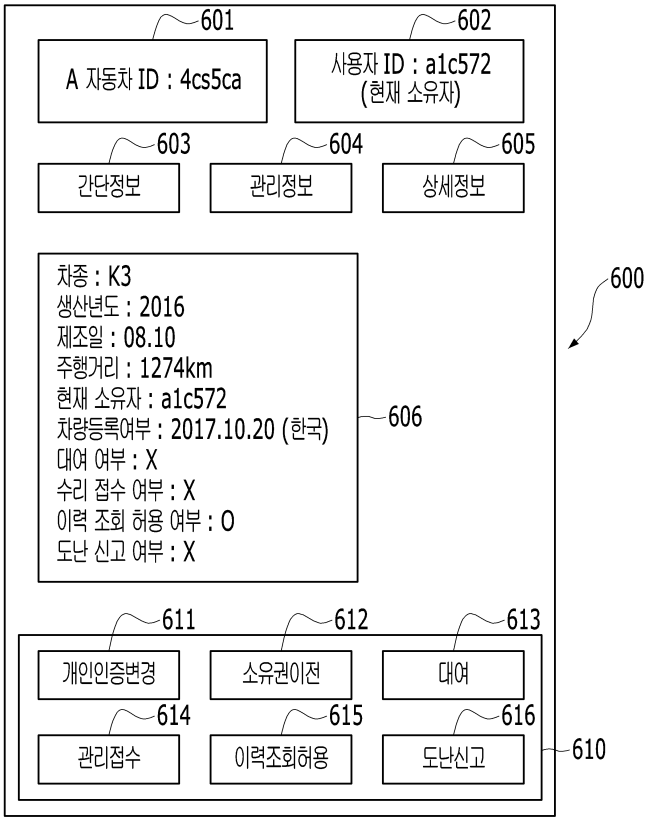
도면10


시 작
자동차 정기 검진 조건이 만족?
S610
No
Yes
소유자 단말에 자동차 정기 검진 권유 정보를 전송
S620
종 료

도면11


시 작
S710
자동차 이력 정보에
운행 금지 관련 정보가
포함 ?
No
Yes
S720
운행 금지 관련 정보
가 유효 ?
No
Yes
자동차 시스템에 운행 금지 요청 정보를 전송
S730
종 료

도면12


601
A 자동차 ID : 4cs5ca
602
사용자 ID : a1c572
(현재 소유자)
603
간단정보
604
관리정보
605
상세정보
차종 : K3
생산년도 : 2016
제조일 : 08.10
주행거리 : 1274km
현재 소유자 : a1c572
차량등록여부 : 2017.10.20 (한국)
대여 여부 : X
수리 접수 여부 : X
이력 조회 허용 여부 : O
도난 신고 여부 : X
606
600
611
개인인증변경
612
소유권이전
613
대여
614
관리접수
615
이력조회허용
616
도난신고
610