(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년02월08일
(11) 등록번호 10-2359782
(24) 등록일자 2022년02월03일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *B60W 60/00* (2020.01)
G06F 21/64 (2013.01) *H04L 9/40* (2022.01)
(52) CPC특허분류
H04L 9/3247 (2013.01)
B60W 60/001 (2020.02)
(21) 출원번호 10-2021-0098651
(22) 출원일자 2021년07월27일
심사청구일자 2021년07월27일
(56) 선행기술조사문헌
KR102256730 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
건양대학교산학협력단
충청남도 논산시 대학로 121 (내동)
(72) 발명자
정승욱
대전광역시 서구 청사로 281 샘머리아파트2단지, 218동 204호
(74) 대리인
강정빈, 심찬, 송두현

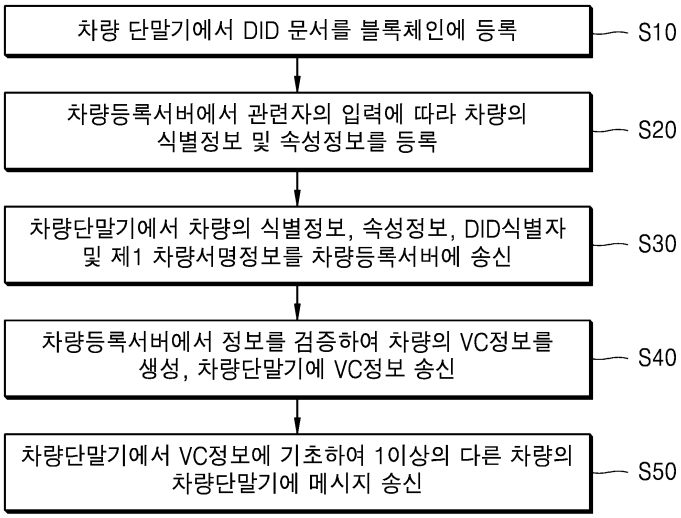
전체 청구항 수 : 총 4 항 심사관 : 나용수

(54) 발명의 명칭 **자율주행 환경에서 블록체인 기반의 차량간 메시지 전송방법**

(57) 요 약

본 발명은 자율주행 환경에서 블록체인 기반의 차량간 메시지 전송방법에 관한 것으로서, 더욱 상세하게는 차량에 구비된 차량단말기에서 DID문서를 생성하여 블록체인에 등록하고, 차량등록서버는 해당 차량의 관련자가 입력한 정보에 기초하여 상기 차량단말기에서 생성한 제1차량서명정보를 수신하고, 상기 블록체인에 등록된 차량단말기의 DID문서를 통해 상기 제1차량서명정보를 검증하여, 해당 차량에 대한 Verifiable Credential(VC)정보를 생성하여 해당 차량의 차량단말기로 송신하고, 해당 차량의 차량단말기는 상기 VC정보에 기초하여 메시지를 생성하고, 상기 메시지를 1 이상의 타 차량의 차량단말기에 송신하는 것으로 차량의 신원증명에 따라 메시지를 송,수신할 수 있도록 하는, 자율주행 환경에서 블록체인 기반의 차량간 메시지 전송방법에 관한 것이다.

대 표 도 - 도3



(52) CPC특허분류
G06F 21/64 (2013.01)
H04L 63/123 (2013.01)
H04L 9/3263 (2013.01)
B60W 2554/4045 (2020.02)
B60W 2556/65 (2020.02)
H04L 2209/38 (2013.01)
H04L 2209/84 (2013.01)

명 세 서

청구범위

청구항 1

블록체인 기반 DID(Decentralized Identifier)를 이용한 차량간 메시지 전송방법으로서,

차량에 구비된 차량단말기에서, 차량개인키, 차량공개키 및 DID식별자를 생성하고, 상기 DID식별자 및 상기 차량공개키를 포함하는 DID문서를 직접적 혹은 간접적으로 블록체인에 등록하는 차량DID문서등록단계;

차량등록서버에서, 해당 차량에 대한 관련자의 입력에 따라 해당 차량의 식별정보, 및 해당 차량의 속성정보를 등록하는 제1차량정보등록단계;

상기 차량단말기에서, 상기 생성된 해당 차량의 식별정보, 속성정보, DID식별자, 및 상기 생성된 해당 차량의 식별정보와 속성정보와 DID식별자 중 1 이상을 포함하는 제1검증정보를 해당 차량의 차량개인키로 서명한 제1차량서명정보를 상기 차량등록서버에 송신하는 제2차량정보등록단계;

상기 차량등록서버에서, 상기 제1차량정보등록단계에서 등록된 정보와 상기 제2차량정보등록단계에서 수신한 정보를 검증하여, 해당 차량에 대한 VC(Verifiable Credential)정보를 생성하고, 상기 VC정보를 상기 차량단말기에 송신하는 VC정보전송단계; 및

상기 차량단말기에서, 상기 VC정보에 기초하여 1 이상의 다른 차량의 차량단말기에 메시지를 송신하는 차량메시지송신단계;를 포함하고,

상기 VC정보전송단계는,

상기 제2차량정보등록단계를 통해 상기 차량단말기로부터 수신한 상기 DID식별자에 기초하여 상기 블록체인에 등록된 해당 DID식별자를 포함하는 DID문서를 획득하는 DID문서획득단계;

획득한 상기 DID문서에 포함된 차량공개키를 사용하여 상기 제2차량정보등록단계를 통해 상기 차량단말기로부터 수신한 제1차량서명정보를 검증하는 차량서명정보검증단계; 및

상기 차량서명정보검증단계를 통해 상기 제1차량서명정보가 정상적으로 검증된 경우에 상기 VC정보를 생성하고, 생성된 상기 VC정보를 상기 차량등록서버의 서버개인키로 서명하여, 서명된 상기 VC정보를 상기 차량에 전송하는 VC정보서명단계;를 포함하는, 블록체인 기반 DID를 이용한 차량간 메시지 전송방법.

청구항 2

삭제

청구항 3

블록체인 기반 DID(Decentralized Identifier)를 이용한 차량간 메시지 전송방법으로서,

차량에 구비된 차량단말기에서, 차량개인키, 차량공개키 및 DID식별자를 생성하고, 상기 DID식별자 및 상기 차량공개키를 포함하는 DID문서를 직접적 혹은 간접적으로 블록체인에 등록하는 차량DID문서등록단계;

차량등록서버에서, 해당 차량에 대한 관련자의 입력에 따라 해당 차량의 식별정보, 및 해당 차량의 속성정보를 등록하는 제1차량정보등록단계;

상기 차량단말기에서, 상기 생성된 해당 차량의 식별정보, 속성정보, DID식별자, 및 상기 생성된 해당 차량의 식별정보와 속성정보와 DID식별자 중 1 이상을 포함하는 제1검증정보를 해당 차량의 차량개인키로 서명한 제1차량서명정보를 상기 차량등록서버에 송신하는 제2차량정보등록단계;

상기 차량등록서버에서, 상기 제1차량정보등록단계에서 등록된 정보와 상기 제2차량정보등록단계에서 수신한 정보를 검증하여, 해당 차량에 대한 VC(Verifiable Credential)정보를 생성하고, 상기 VC정보를 상기 차량단말기에 송신하는 VC정보전송단계; 및

상기 차량단말기에서, 상기 VC정보에 기초하여 1 이상의 다른 차량의 차량단말기에 메시지를 송신하는 차량메시지송신단계;를 포함하고,

상기 차량메시지송신단계는,

상기 VC정보, 메시지정보, 시점정보 및 상기 VC정보와 상기 메시지정보와 상기 시점정보 가운데 1 이상을 포함하는 제2검증정보를 해당 차량의 차량개인키로 서명한 제2차량서명정보를 포함하는 VP(Verifiable Presentation)정보를 생성하고, 상기 VP정보를 직접적 혹은 간접적으로 1 이상의 다른 차량의 차량단말기에 송신하고,

상기 VP정보를 수신한 1 이상의 다른 차량의 차량단말기는,

상기 VP정보를 생성한 차량에 상응하는 DID문서 및 상기 VC정보를 생성한 차량등록서버에 상응하는 DID문서를 상기 블록체인으로부터 직접적 혹은 간접적으로 획득하고, 획득한 DID문서 각각에 포함된 해당 차량의 차량공개키 및 해당 차량등록서버의 서버공개키를 사용하여 상기 VP정보에 포함된 제2차량서명정보 및 상기 VC정보를 검증하는, 블록체인 기반 DID를 이용한 차량간 메시지 전송방법.

청구항 4

청구항 1에 있어서,

상기 속성정보는, 필요에 따라 긴급하게 주행해야 하는 차량에 대한 정보에 해당하고,

상기 메시지는, 긴급상황의 발생에 따라 해당 차량이 긴급하게 주행할 수 있도록 상기 1 이상의 다른 차량의 주행 차선의 변경을 요청하는 정보에 해당하는, 블록체인 기반 DID를 이용한 차량간 메시지 전송방법.

청구항 5

블록체인 기반 DID(Decentralized Identifier)를 이용한 차량간 메시지 전송방법으로서,

차량에 구비된 차량단말기에서, 차량개인키, 차량공개키 및 DID식별자를 생성하고, 상기 DID식별자 및 상기 차량공개키를 포함하는 DID문서를 직접적 혹은 간접적으로 블록체인에 등록하는 차량DID문서등록단계;

차량등록서버에서, 해당 차량에 대한 관련자의 입력에 따라 해당 차량의 식별정보, 및 해당 차량의 속성정보를 등록하는 제1차량정보등록단계;

상기 차량단말기에서, 상기 생성된 해당 차량의 식별정보, 속성정보, DID식별자, 및 상기 생성된 해당 차량의 식별정보와 속성정보와 DID식별자 중 1 이상을 포함하는 제1검증정보를 해당 차량의 차량개인키로 서명한 제1차량서명정보를 상기 차량등록서버에 송신하는 제2차량정보등록단계;

상기 차량등록서버에서, 상기 제1차량정보등록단계에서 등록된 정보와 상기 제2차량정보등록단계에서 수신한 정보를 검증하여, 해당 차량에 대한 VC(Verifiable Credential)정보를 생성하고, 상기 VC정보를 상기 차량단말기에 송신하는 VC정보전송단계; 및

상기 차량단말기에서, 상기 VC정보에 기초하여 1 이상의 다른 차량의 차량단말기에 메시지를 송신하는 차량메시지송신단계;를 포함하고,

상기 블록체인 기반 DID를 이용한 차량간 메시지 전송방법은,

상기 차량등록서버에서, 상기 차량등록서버에 대한 서버개인키, 서버공개키 및 DID식별자를 생성하고, 상기 DID식별자 및 상기 서버공개키를 포함하는 DID문서를 상기 블록체인에 등록하는 서버DID문서등록단계;를 더 포함하고,

상기 VC정보전송단계는,

생성된 상기 VC정보를 상기 서버개인키로 서명하고, 상기 서명된 VC정보를 상기 차량에 전송하는, 블록체인 기반 DID를 이용한 차량간 메시지 전송방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 자율주행 환경에서 블록체인 기반의 차량간 메시지 전송방법에 관한 것으로서, 더욱 상세하게는 차량에 구비된 차량단말기에서 DID문서를 생성하여 블록체인에 등록하고, 차량등록서버는 해당 차량의 관련자가 입력한 정보에 기초하여 상기 차량단말기에서 생성한 제1차량서명정보를 수신하고, 상기 블록체인에 등록된 차량단말기의 DID문서를 통해 상기 제1차량서명정보를 검증하여, 해당 차량에 대한 Verifiable Credential(VC)정보를 생성하여 해당 차량의 차량단말기로 송신하고, 해당 차량의 차량단말기는 상기 VC정보에 기초하여 메시지를 생성하고, 상기 메시지를 1 이상의 타 차량의 차량단말기에 송신하는 것으로 차량의 신원증명에 따라 메시지를 송,수신할 수 있도록 하는, 자율주행 환경에서 블록체인 기반의 차량간 메시지 전송방법에 관한 것이다.

배 경 기 술

[0003] 최근 인공지능 기술의 발달로 인해, 차량을 포함하는 모빌리티 수단의 자율주행 기술 개발이 활발하게 이루어지고 있다. 종래의 개발된 자율주행 기술은 차량에 구비된 카메라, 레이더 센서, 라이다 센서 등을 통해 차량의 주변의 타 차량 또는 장애물 등을 식별하고, 식별한 정보들을 바탕으로 차량 스스로 주행하도록 제어하는 것을 중심으로 개발되고 있는 상황이다.

[0004] 한편, 종래에 알려진 자율주행 기술 개발단계에서 5단계에 해당하는 완전 자동화(Full Automation) 단계와 같이, 높은 수준의 자율주행 기술을 달성하기 위해서는 단순히 주변 사물을 식별하여 제어하는 것뿐만 아니라, 주변 사물과 커뮤니케이션 할 수 있는 기술의 개발이 보조되어야 한다. 예를 들어, 교통사고와 같이 돌발 상황이 발생하는 경우에 차량이 해당 상황을 인지하기 위해서는 사고 현장 주변에 위치한 사물(노변기지국)이나, 다른 차량과의 커뮤니케이션을 통해 해당 상황을 인지해야 한다.

[0005] 이와 같이, 자율주행 기술을 완성도 있게 구현하기 위하여 다른 사물 또는 다른 차량과 통신하기 위한 기술의 개발이 필요하며, 특히 타 차량에서 송신한 메시지를 무분별하게 수신하는 것이 아니라, 메시지를 송신한 차량의 신원을 검증하고, 신원이 인증된 경우에 해당 메시지에 대한 응답을 수행할 수 있도록 하는 통신 기술의 개발이 중요하다.

[0006] 한편, 객체의 신원을 증명하기 위한 방법으로 최근 블록체인을 기반으로 하는 탈중앙화 신원증명 또는 분산 신원증명인 Decentralized Identity(DID) 기술이 개발되고 있다. DID 기술은 블록체인에 신원을 증명하기 위한 정보들을 등록하고 인증이 필요한 경우에 자신의 개인키로 서명하고, 개인키로 서명된 신원 증명 정보를 검증하는 것으로 해당 객체의 신원을 인증하는 기술이다.

[0007] 다만, 종래의 DID 기술은 사람의 신원을 증명하기 위한 것으로 개발되고 있으며, 차량과 같이 모빌리티 수단에 대한 신원 증명에 대해서는 개념적으로만 논의되고 있을 뿐, DID 기술을 기반으로 차량의 신원을 증명하여 메시지를 송수신할 수 있는 실질적인 기술은 아직 개발되지 않은 상황이다.

발명의 내용

해결하려는 과제

[0009] 본 발명은 자율주행 환경에서 블록체인 기반의 차량간 메시지 전송방법에 관한 것으로서, 더욱 상세하게는 차량에 구비된 차량단말기에서 DID문서를 생성하여 블록체인에 등록하고, 차량등록서버는 해당 차량의 관련자가 입력한 정보에 기초하여 상기 차량단말기에서 생성한 제1차량서명정보를 수신하고, 상기 블록체인에 등록된 차량단말기의 DID문서를 통해 상기 제1차량서명정보를 검증하여, 해당 차량에 대한 Verifiable Credential(VC)정보를 생성하여 해당 차량의 차량단말기로 송신하고, 해당 차량의 차량단말기는 상기 VC정보에 기초하여 메시지를 생성하고, 상기 메시지를 1 이상의 타 차량의 차량단말기에 송신하는 것으로 차량의 신원증명에 따라 메시지를 송,수신할 수 있도록 하는, 자율주행 환경에서 블록체인 기반의 차량간 메시지 전송방법을 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0011] 상기와 같은 과제를 해결하기 위하여, 블록체인 기반 DID(Decentralized Identifier)를 이용한 차량간 메시지 전송방법으로서, 차량에 구비된 차량단말기에서, 차량개인키, 차량공개키 및 DID식별자를 생성하고, 상기 DID식

별자 및 상기 차량공개키를 포함하는 DID문서를 직접적 혹은 간접적으로 블록체인에 등록하는 차량DID문서등록단계; 차량등록서버에서, 해당 차량에 대한 관련자의 입력에 따라 해당 차량의 식별정보, 및 해당 차량의 속성정보를 등록하는 제1차량정보등록단계; 상기 차량단말기에서, 상기 생성된 해당 차량의 식별정보, 속성정보, DID식별자, 및 상기 생성된 해당 차량의 식별정보와 속성정보와 DID식별자 중 1 이상을 포함하는 제1검증정보를 해당 차량의 차량개인키로 서명한 제1차량서명정보를 상기 차량등록서버에 송신하는 제2차량정보등록단계; 상기 차량등록서버에서, 상기 제1차량정보등록단계에서 등록된 정보와 상기 제2차량정보등록단계에서 수신한 정보를 검증하여, 해당 차량에 대한 VC(Verifiable Credential)정보를 생성하고, 상기 VC정보를 상기 차량단말기에 송신하는 VC정보전송단계; 및 상기 차량단말기에서, 상기 VC정보에 기초하여 1 이상의 다른 차량의 차량단말기에 메시지를 송신하는 차량메시지송신단계;를 포함하는, 블록체인 기반 DID를 이용한 차량간 메시지 전송방법을 제공한다.

[0012] 본 발명의 일 실시예에서는, 상기 VC정보전송단계는, 상기 제2차량정보등록단계를 통해 상기 차량단말기로부터 수신한 상기 DID식별자에 기초하여 상기 블록체인에 등록된 해당 DID식별자를 포함하는 DID문서를 획득하는 DID문서획득단계; 획득한 상기 DID문서에 포함된 차량공개키를 사용하여 상기 제2차량정보등록단계를 통해 상기 차량단말기로부터 수신한 제1차량서명정보를 검증하는 차량서명정보검증단계; 및 상기 차량서명정보검증단계를 통해 상기 제1차량서명정보가 정상적으로 검증된 경우에 상기 VC정보를 생성하고, 생성된 상기 VC정보를 상기 차량등록서버의 서버개인키로 서명하여, 서명된 상기 VC정보를 상기 차량에 전송하는 VC정보서명단계;를 포함할 수 있다.

[0013] 본 발명의 일 실시예에서는, 상기 차량메시지송신단계는, 상기 VC정보, 메시지정보, 시점정보 및 상기 VC정보와 상기 메시지정보와 상기 시점정보 가운데 1 이상을 포함하는 제2검증정보를 해당 차량의 차량개인키로 서명한 제2차량서명정보를 포함하는 VP(Verifiable Presentation)정보를 생성하고, 상기 VP정보를 직접적 혹은 간접적으로 1 이상의 다른 차량의 차량단말기에 송신하고, 상기 VP정보를 수신한 1 이상의 다른 차량의 차량단말기는, 상기 VP정보를 생성한 차량에 상응하는 DID문서 및 상기 VC정보를 생성한 차량등록서버에 상응하는 DID문서를 상기 블록체인으로부터 직접적 혹은 간접적으로 획득하고, 획득한 DID문서 각각에 포함된 해당 차량의 차량공개키 및 해당 차량등록서버의 서버공개키를 사용하여 상기 VP정보에 포함된 제2차량서명정보 및 상기 VC정보를 검증할 수 있다.

[0014] 본 발명의 일 실시예에서는, 상기 속성정보는, 필요에 따라 긴급하게 주행해야 하는 차량에 대한 정보에 해당하고, 상기 메시지는, 긴급상황의 발생에 따라 해당 차량이 긴급하게 주행할 수 있도록 상기 1 이상의 다른 차량의 주행 차선의 변경을 요청하는 정보에 해당할 수 있다.

[0015] 본 발명의 일 실시예에서는, 상기 블록체인 기반 DID를 이용한 차량간 메시지 전송방법은, 상기 차량등록서버에서, 상기 차량등록서버에 대한 서버개인키, 서버공개키 및 DID식별자를 생성하고, 상기 DID식별자 및 상기 서버공개키를 포함하는 DID문서를 상기 블록체인에 등록하는 서버DID문서등록단계;를 더 포함하고, 상기 VC정보전송단계는, 생성된 상기 VC정보를 상기 서버개인키로 서명하고, 상기 서명된 VC정보를 상기 차량에 전송할 수 있다.

발명의 효과

[0017] 본 발명의 일 실시예에 따르면, 블록체인에 차량에 대한 DID문서를 등록하고, 상기 DID문서에 포함된 해당 차량의 공개키를 통해 해당 차량의 신원을 검증하므로, 중앙화 된 시스템이 없이도 차량의 신원을 검증하여 메시지를 송수신할 수 있는 시스템을 구현할 수 있는 효과를 발휘할 수 있다.

[0018] 본 발명의 일 실시예에 따르면, 블록체인에 차량에 대한 DID문서를 등록하여 DID문서의 위,변조 가능성을 낮출 수 있는 효과를 발휘할 수 있다.

[0019] 본 발명의 일 실시예에 따르면, 구급차, 경찰차 등과 같이 긴급하게 주행해야 하는 차량을 대상으로 하여 차량등록서버에서 VC정보를 생성하여 해당 차량에 제공하고, 해당 차량은 VC정보에 기초하여 메시지를 생성하여 타 차량에 전송할 수 있으므로, 긴급차량이 주행 경로에 있는 타 차량에게 차선의 변경을 요청하는 메시지를 용이하게 송신할 수 있는 효과를 발휘할 수 있다.

도면의 간단한 설명

[0021] 도 1은 본 발명의 일 실시예에 따른 블록체인 기반 DID를 이용한 차량간 메시지 전송방법을 수행하기 위한 구성요소들을 개략적으로 도시한다.

도 2는 본 발명의 일 실시예에 따른 차량단말기 및 차량등록서버 각각의 내부 구성요소들을 개략적으로 도시한다.

도 3은 본 발명의 일 실시예에 따른 블록체인 기반 DID를 이용한 차량간 메시지 전송방법의 세부단계들을 개략적으로 도시한다.

도 4는 본 발명의 일 실시예에 따른 차량단말기에 VC정보를 제공하는 과정을 개략적으로 도시한다.

도 5는 본 발명의 일 실시예에 따른 서버DID문서등록단계를 개략적으로 도시한다.

도 6은 본 발명의 일 실시예에 따른 VP정보의 구성요소들을 개략적으로 도시한다.

도 7은 본 발명의 일 실시예에 따른 VC정보를 수신한 차량단말기에서 타 차량의 차량단말기로 메시지를 송신하는 과정을 개략적으로 도시한다.

도 8은 본 발명의 일 실시예에 따른 컴퓨팅장치의 내부 구성을 개략적으로 도시한다.

발명을 실시하기 위한 구체적인 내용

[0022] 이하에서는, 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 발명의 기술 분야에서 통상의 지식을 가진 자에게 인식될 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.

[0024] 또한, 다양한 양상들 및 특징들이 다수의 디바이스들, 컴포넌트들 및/또는 모듈들 등을 포함할 수 있는 시스템에 의하여 제시될 것이다. 다양한 시스템들이, 추가적인 장치들, 컴포넌트들 및/또는 모듈들 등을 포함할 수 있다는 점 그리고/또는 도면들과 관련하여 논의된 장치들, 컴포넌트들, 모듈들 등 전부를 포함하지 않을 수도 있다는 점 또한 이해되고 인식되어야 한다.

[0025] 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. 아래에서 사용되는 용어들 '~부', '컴포넌트', '모듈', '시스템', '인터페이스' 등은 일반적으로 컴퓨터 관련 엔티티(computer-related entity)를 의미하며, 예를 들어, 하드웨어, 하드웨어와 소프트웨어의 조합, 소프트웨어를 의미할 수 있다.

[0026] 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.

[0027] 또한, 제1, 제2 등과 같이 서수를 포함하는 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되지는 않는다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0028] 또한, 본 발명의 실시예들에서, 별도로 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 발명의 실시예에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0030] 도 1은 본 발명의 일 실시예에 따른 블록체인(3000) 기반 DID를 이용한 차량간 메시지 전송방법을 수행하기 위한 구성요소들을 개략적으로 도시한다.

[0031] 도 1에 도시된 바와 같이, 복수의 구성요소에 의하여 본 발명의 블록체인(3000) 기반의 DID를 이용한 차량간 메시지 전송방법을 수행할 수 있고, 상기 복수의 구성요소는, 메시지를 송신하는 차량(1000), 차량등록서버(2000), 블록체인(3000), 차량관련자단말기(4000), 상기 메시지를 수신하는 1 이상의 타 차량(5000) 및 노변기지국(6000)을 포함할 수 있다.

[0033] 상기 메시지를 송신하는 차량(1000)에는 차량단말기(1100)가 구비되어 있고, 상기 차량단말기(1100)에서 본 발명의 블록체인(3000) 기반의 DID를 이용한 차량간 메시지 전송방법이 수행될 수 있다. 본 발명에서 상기 메시지를 송신하는 차량(1000)은 통상적으로 도로를 주행할 수 있는 다양한 유형의 모빌리티 수단을 의미할 수 있다. 또한, 상기 메시지를 송신하는 차량(1000)은 차량의 용도 또는 목적(상업용, 운수용, 승용, 공무 등의 긴급을 요하는 상황 대처 목적 등)과 무관하게 다양한 목적을 갖는 차량에 해당할 수 있으나, 바람직하게는 상기 메시지를 송신하는 차량(1000)은 구급차, 경찰차, 소방차 등과 같이 긴급한 상황에서 주행해야 하는 차량(긴급차량)에 해당할 수 있다.

[0035] 상기 차량등록서버(2000)는 상기 차량(1000)에서 메시지를 송신하기 위하여 필요한 정보, 바람직하게는 Verifiable Credential(VC)정보를 생성하여 상기 차량의 차량단말기(1100)에 제공한다. 상기 VC정보는 해당 차량(1000)의 신원을 식별할 수 있는 1 이상의 정보(Claim)들을 포함할 수 있다. 예를 들어, 차량에 대한 속성정보, 차량번호정보, 차대번호, 차량의 소유자 정보 등이 상기 VC정보에 포함될 수 있다.

[0036] 한편, 상기 차량등록서버(2000)는 상기 차량(1000)에 대한 VC정보를 생성하기 위하여, 해당 차량(1000)의 DID식별자 및 해당 차량(1000)의 차량공개키가 포함되어 있는 DID문서가 등록되어 있는 상기 블록체인(3000)에서 상기 DID문서를 획득하여 해당 차량(1000)을 검증할 수 있다. 또한 상기 차량등록서버(2000)는 해당 차량(1000)의 관련자가 사용 주체가 되는 차량관련자단말기(4000)와 통신을 수행하여 해당 차량(1000)에 대한 정보, 예를 들어, 해당 차량(1000)의 식별정보 및 속성정보를 수신할 수 있다.

[0037] 본 발명에서 상기 차량의 관련자는, 해당 차량의 소유자만을 의미하는 것이 아니라 해당 차량과 관련된 다양한 주체 가운데 어느 하나의 주체에 해당할 수 있다. 예를 들어, 상기 차량의 관련자는 해당 차량의 소유자, 해당 차량의 운전자, 해당 차량의 생산자, 해당 차량의 판매자, 해당 차량의 관리자 등 가운데 어느 하나의 주체에 해당할 수 있고, 상기 차량관련자단말기(4000)는 상기 어느 하나의 주체가 사용하는 단말기에 해당할 수 있다.

[0039] 상기 블록체인(3000)은 복수의 노드(3100)를 포함하고, 각각의 노드(3100)는 1 이상의 트랜잭션을 포함하는 블록을 생성하며, 특정 노드에서 생성된 블록은 나머지 타 노드로 전파될 수 있다. 한편, 노드(3100)에서 생성된 블록에 포함되는 트랜잭션은 차량단말기(1100)에서 생성되는 해당 차량(1000)에 대한 DID문서에 대한 정보에 해당할 수 있다.

[0040] 한편, 도 1에서는 블록체인(3000)에 포함되는 노드(3100) 및 상기 차량단말기(1100)가 개별적으로 도시되어, 상기 차량단말기(1100)에서 생성한 DID문서를 블록체인(3000)에 참여하는 특정 노드로 전송하는 것으로 도시되어 있으나, 본 발명의 다른 실시예에서는 상기 차량단말기(1100)가 상기 블록체인(3000)의 노드(3100)로 직접 참여하여 생성한 DID문서를 트랜잭션으로 하는 블록을 직접 생성하고, 이를 타 노드로 전파할 수도 있다.

[0041] 본 발명의 다른 실시예에서 상기 차량등록서버(2000) 또한 상술한 바와 같이 블록체인(3000)에 참여하는 노드(3100)에 해당할 수도 있다.

[0043] 상기 1 이상의 타 차량(5000)은 상기 차량등록서버(2000)로부터 VC정보를 제공받은 차량(1000)으로부터 메시지를 수신하며, 상기 1 이상의 타 차량(5000) 각각에도 별도의 차량단말기가 구비될 수 있다. 상기 1 이상의 타 차량(5000)의 차량단말기는 수신한 메시지를 검증하기 위하여 블록체인(3000)에 등록된 해당 차량의 DID문서를 획득하고, 상기 획득한 DID문서를 사용하여 상기 메시지를 검증하여, 상기 메시지가 유효한 것으로 검증된 경우에 메시지에 따른 응답을 수행할 수 있다.

[0044] 한편, 상기 타 차량(5000)의 차량단말기에서 수행하는 메시지에 따른 응답은 메시지를 송신한 차량(1000)의 차량단말기(1100)에 별도의 메시지를 송신하거나, 상기 메시지에 따라 속도를 줄이거나, 주행 차선을 변경하는 등의 행위를 의미할 수 있다.

[0046] 상기 노변기지국(6000)은 각 차량에 구비된 차량단말기(1100)의 통신을 중계할 수 있다. 예를 들어, 상기 노변기지국(6000)은 차량단말기(1100)와 블록체인(3000), 차량등록서버(2000) 또는 타 차량(5000)의 차량단말기와의 통신을 중계할 수 있다.

[0047] 본 발명의 다른 실시예에서, 차량단말기(1100)에서 생성된 메시지의 목적지가 상기 노변기지국(6000)에 해당할 수도 있다. 예를 들어, 차량단말기(1100)에서 특정 지역에 대한 정보를 요청하고자 하는 메시지를 생성하는 경우에 상기 메시지는 상기 특정 지역에 위치한 노변기지국(6000)을 목적지로 할 수 있으며, 상기 노변기지국(6000)은 상기 메시지를 수신하여 검증하고, 상기 특정 지역에 대한 정보를 상기 차량단말기(1100)에 제공할 수도 있다.

[0048] 본 발명의 또 다른 실시예에서 상기 메시지를 생성하는 차량(1000)의 차량단말기(1100) 및 상기 메시지를 수신하는 1 이상의 타 차량(5000)의 차량단말기는 노변기지국(6000)의 중계없이 직접적으로 통신을 수행할 수도 있다.

[0050] 이하에서는, 상술한 복수의 구성요소들에 의해 수행되는 본 발명의 블록체인(3000) 기반 DID를 이용한 차량간 메시지 전송방법에 대해 자세하게 설명하도록 한다.

[0052] 도 2는 본 발명의 일 실시예에 따른 차량단말기(1100) 및 차량등록서버(2000) 각각의 내부 구성요소들을 개략적으로 도시한다.

[0053] 상기 차량단말기(1100)는 1 이상의 프로세서 및 1 이상의 메모리를 포함하며, 차량의 내부에 구비될 수 있으며, 종래의 On-Board Unit(OBU)에 해당할 수 있다. 구체적으로 도 2의 (A)에 도시된 바와 같이, 상기 차량단말기(1100)는 차량DID문서등록부(1110), 제2차량정보등록부(1120), 차량메시지송신부(1130) 및 DID지갑(1140)을 포함한다.

[0055] 상기 차량DID문서등록부(1110)는 차량DID문서등록단계(S10)를 수행하여 해당 차량에 대한 차량개인키, 차량공개키 및 DID식별자를 생성하고, 상기 차량공개키 및 상기 DID식별자를 포함하는 해당 차량에 대한 DID문서를 도출하여 상기 블록체인(3000)에 등록한다. 상기 DID식별자는 해당 차량의 신원을 식별할 수 있는 정보가 아니라 해당 차량에 대해 부여되는 고유한 값에 해당할 수 있고, 상기 블록체인(3000)에 등록되는 DID문서는 해당 차량에서 생성된 정보를 검증하기 위한 요소로 사용될 수 있다.

[0056] 상기 제2차량정보등록부(1120)는 제2차량정보등록단계(S30)를 수행하여 후술하는 차량등록서버(2000)의 제1차량정보등록부(2100)로부터 수신하는 정보들을 포함하는 제1검증정보를 상기 차량DID문서등록부(1110)에서 생성된 차량개인키로 서명하여 제1차량서명정보를 생성하고, 상기 제1차량서명정보를 포함하는 정보를 상기 차량등록서버(2000)로 송신한다. 한편, 상기 차량등록서버(2000)로 송신된 상기 제1차량서명정보를 포함하는 정보는 상기 차량등록서버(2000)에 저장될 수 있다. 이와 같이, 생성된 제1차량서명정보를 포함하는 정보 는 후술하는 상기 차량등록서버(2000)의 VC정보전송부(2200)에서 해당 차량에 대한 VC정보를 도출하기 위하여 사용될 수 있다.

[0057] 상기 차량메시지송신부(1130)는 차량메시지송신단계(S50)를 수행하여 상기 차량등록서버(2000)로부터 수신한 VC정보에 기초하여 메시지를 생성하고, 상기 메시지를 1 이상의 다른 차량의 차량단말기(1100)에 송신한다. 상기 차량메시지송신부(1130)는 해당 차량이 긴급하게 주행해야 하는 경우와 같이, 기설정된 특정 상황이 발생하는 경우에 해당 특정 상황에 따라 메시지를 생성할 수 있으며, 해당 차량의 운전자 등의 메시지생성요청입력을 수신함에 따라 메시지를 생성할 수 있다.

[0058] 한편, 상기 차량메시지송신부(1130)에서 생성된 메시지에는 해당 차량의 차량개인키로 서명된 정보를 포함하여, 상기 메시지를 수신한 1 이상의 다른 차량의 차량단말기(1100)에서 상기 차량개인키로 서명된 정보를 검증하는 것으로 수신한 상기 메시지가 유효한지를 판단할 수 있다.

[0059] 상기 DID지갑(1140)에는 상기 차량DID문서등록부(1110)에서 생성된 해당 차량의 차량개인키, 차량공개키 및 차량의 DID식별자가 저장될 수 있고, 상기 차량등록서버(2000)로부터 수신한 VC정보가 추가적으로 저장될 수 있다. 따라서, 상기 차량단말기(1100)에서 차량개인키를 통해 서명하거나, 다른 차량에 송신하기 위한 메시지를 생성하고자 하는 경우에 상기 DID지갑(1140)에 저장된 정보들을 사용할 수 있다.

[0060] 본 발명의 다른 실시예에서, 상기 DID지갑(1140)은 소프트웨어적으로 1 이상의 정보들이 저장되는 가상의 공간에 해당할 수 있고, 물리적으로는 상기 1 이상의 정보들은 차량단말기(1100)에 포함된 1 이상의 메모리에 저장될 수 있다.

[0062] 한편, 상기 차량등록서버(2000)는 1 이상의 프로세서 및 1 이상의 메모리를 포함하며, 구체적으로 도 2의 (B)에 도시된 바와 같이, 상기 차량등록서버(2000)는 제1차량정보등록부(2100), VC정보전송부(2200), 서버DID문서등록부(2300), DID지갑(2400) 및 DB(2500)를 포함한다.

[0064] 상기 제1차량정보등록부(2100)는 제1차량정보등록단계(S20)를 수행하여 차량관련자단말기(4000)로부터 해당 차량에 대한 1 이상의 정보들을 수신하여 등록한다. 구체적으로, 해당 차량에 대한 1 이상의 정보는 해당 차량의 식별정보 및 해당 차량의 속성정보를 포함할 수 있다. 한편, 상기 제1차량정보등록단계(S20)에서는 상기 차량관련자단말기(4000)로부터 해당 차량에 대한 1 이상의 정보들을 수신하여 등록하는 경우에, 해당 차량의 차량단말기(1100)에서 상기 제2차량정보등록단계(S30)의 수행을 요청하는 정보를 해당 차량의 차량단말기(1100)로 송신할 수도 있다.

[0065] 상기 VC정보전송부(2200)는 VC정보전송단계(S40)를 수행하여 해당 차량의 차량단말기(1100)의 제2차량정보등록부(1120)로부터 수신한 제1차량서명정보를 포함하는 정보 및 해당 차량에 대한 차량관련자단말기(4000)로부터 수신하여 등록한 1 이상의 정보에 기초하여 해당 차량에 대한 Verifiable Credential(VC)정보를 생성하여, 해당 차량의 차량단말기(1100)로 송신한다.

[0066] 본 발명에서 상기 VC정보는 해당 차량의 신원을 식별할 수 있는 1 이상의 정보를 포함할 수 있다. 예를 들어, 상기 1 이상의 정보는 해당 차량의 차량번호, 차대번호, 소유자정보, 차량용도정보, 차량의 유형에 대한 정보와 같이 차량의 속성정보 등을 포함할 수 있다.

[0067] 상기 서버DID문서등록부(2300)는 서버DID문서등록단계를 수행하여 상술한 차량DID문서등록부(1110)와 유사하게 상기 차량등록서버에 대한 서버개인키, 서버공개키 및 DID식별자를 생성하고, 상기 서버공개키 및 상기 DID식별자를 포함하는 상기 차량등록서버(2000)에 대한 DID문서를 도출하여 상기 블록체인(3000)에 등록한다. 마찬가지로 상기 서버DID문서등록부(2300)에서 생성된 DID식별자는 상기 차량등록서버(2000)에 대해 부여되는 고유한 값에 해당할 수 있고, 상기 블록체인(3000)에 등록되는 상기 차량등록서버(2000)에 대한 DID문서는 VC정보를 수신한 차량단말기(1100)에서 상기 VC정보를 검증하기 위한 요소로 사용되거나, 상기 메시지를 수신한 차량단말기(1100)에서 상기 메시지에 포함된 VC정보를 검증하기 위한 요소로 사용될 수 있다.

[0068] 상기 차량등록서버(2000)의 DID지갑(2400)에는 상기 서버DID문서등록부(2300)에서 생성된 상기 서버개인키, 서버공개키 및 차량등록서버(2000)의 DID식별자가 저장될 수 있다. 이와 같이, 상기 차량등록서버(2000)의 DID지갑(2400)에는 상기 차량등록서버(2000)에서 생성된 모든 정보들이 저장되는 것이 아니라 상기 차량등록서버(2000)에 대한 고유한 정보들이 저장될 수 있다.

[0069] 본 발명의 다른 실시예에서, 상기 DID지갑(2400)은 소프트웨어적으로 1 이상의 정보들이 저장되는 가상의 공간에 해당할 수 있고, 물리적으로는 상기 1 이상의 정보들은 차량단말기(1100)에 포함된 1 이상의 메모리에 저장될 수 있다.

[0070] 상기 차량등록서버(2000)의 DB(2500)에는 각 차량에 대한 정보들이 저장될 수 있다. 예를 들어, 차량의 차량관련자단말기(4000)로부터 수신한 해당 차량의 식별정보 및 속성정보가 저장될 수 있고, 차량단말기(1100)로부터 수신한 제1차량서명정보를 포함하는 정보에 포함된 해당 차량의 DID식별자 및 상기 VC정보전송부(2200)에서 생성된 차량에 대한 VC정보가 추가적으로 저장될 수 있다.

[0071] 한편, 도 2의 (B)에 도시된 바와 같이 정보의 종류별로 상기 DB(2500)에 저장될 수 있으나, 본 발명의 다른 실시예에서는 차량에 대한 식별정보, 속성정보, DID식별자 및 VC정보가 각각의 차량별로 상기 DB(2500)에 저장될 수도 있다.

[0073] 도 3은 본 발명의 일 실시예에 따른 블록체인(3000) 기반 DID를 이용한 차량간 메시지 전송방법의 세부단계들을 개략적으로 도시한다.

[0075] 도 3에 도시된 바와 같이, 블록체인(3000) 기반 DID(Decentralized Identifier)를 이용한 차량간 메시지 전송방법으로서, 차량에 구비된 차량단말기(1100)에서, 차량개인키, 차량공개키 및 DID식별자를 생성하고, 상기 DID식별자 및 상기 차량공개키를 포함하는 DID문서를 직접적 혹은 간접적으로 블록체인(3000)에 등록하는 차량DID문서등록단계(S10); 차량등록서버(2000)에서, 해당 차량에 대한 관련자의 입력에 따라 해당 차량의 식별정보, 및 해당 차량의 속성정보를 등록하는 제1차량정보등록단계(S20); 상기 차량단말기(1100)에서, 상기 생성된 해당 차량의 식별정보, 속성정보, DID식별자, 및 상기 생성된 해당 차량의 식별정보와 속성정보와 DID식별자 중 1 이상을 포함하는 제1검증정보를 해당 차량의 차량개인키로 서명한 제1차량서명정보를 상기 차량등록서버(2000)에 송신하는 제2차량정보등록단계(S30); 상기 차량등록서버(2000)에서, 상기 제1차량정보등록단계(S20)에서 등록된 정보와 상기 제2차량정보등록단계(S30)에서 수신한 정보를 검증하여, 해당 차량에 대한 VC(Verifiable Credential)정보를 생성하고, 상기 VC정보를 상기 차량단말기(1100)에 송신하는 VC정보전송단계(S40); 및 상기 차량단말기(1100)에서, 상기 VC정보에 기초하여 1 이상의 다른 차량의 차량단말기(1100)에 메시지를 송신하는 차량메시지송신단계(S50);를 포함할 수 있다.

[0077] 구체적으로, 상기 차량단말기(1100)의 차량DID문서등록부(1110)에서 수행하는 차량DID문서등록단계(S10)는 상기 차량단말기(1100)가 구비된 차량에 대한 DID문서를 생성하고, 상기 생성된 DID문서를 블록체인(3000)에 등록시킬 수 있다. 이를 위해 상기 차량DID문서등록단계(S10)는 상기 차량에 대한 차량개인키, 차량공개키 및 DID식별자를 우선 생성한다.

[0078] 상기 차량개인키는 상기 차량단말기(1100)에서 생성되는 정보에 대해 서명을 수행하기 위한 요소로 사용될 수 있고, 상기 차량공개키는 상기 차량단말기(1100)에서 서명한 정보를 수신한 타 구성요소, 예를 들어, 상기 차량등록서버(2000), 타 차량(5000)의 차량단말기, 또는 상기 노변기지국(6000)에서 서명을 검증하기 위한 요소로 사용될 수 있으며, 상기 DID식별자는 해당 차량(1000) 또는 차량단말기(1100)에 고유하게 부여되는 값으로써, 블록체인(3000)에 등록된 복수의 DID문서 가운데 특정 차량의 DID문서를 획득하기 위한 요소로 사용될 수 있다. 상기 차량개인키 및 상기 차량공개키는 통상적으로 정보의 서명 및 검증에 사용되는 개인키/공개키 쌍의 형태와 동일한 형태로 생성될 수 있으며, 상기 DID식별자는 종래의 사용되는 DID식별자의 형태와 동일하게 생성되거나, 혹은 기설정된 크기를 갖는 난수값에 해당할 수도 있다.

[0079] 한편, 상기 차량DID문서등록단계(S10)에서는 생성된 상기 차량공개키 및 상기 DID식별자를 포함하는 해당 차량에 대한 DID문서를 도출하여 이를 직접적, 혹은 간접적으로 블록체인(3000)에 등록하게 된다. 상기 차량단말기(1100)가 블록체인(3000)에 참여하는 특정 노드에 해당하거나, 혹은 상기 차량단말기(1100)가 블록체인(3000)에 참여하는 특정 노드와 직접적으로 통신을 수행하는 경우에 상기 차량단말기(1100)는 DID문서에 대한 정보가 포함된 블록을 직접 생성하여 전파하거나, 혹은 직접 통신을 수행하는 특정 노드로 하여금 DID문서에 대한 정보가 포함된 블록을 생성하도록 요청할 수 있다.

[0080] 반면에, 상기 차량단말기(1100)가 노변기지국(6000) 등을 통해 간접적으로 블록체인(3000)에 참여하는 특정 노드와 통신을 수행하는 경우에 상기 노변기지국(6000)과 같은 중계 요소를 통해 간접적으로 DID문서가 상기 블록체인(3000)에 등록되도록 요청할 수도 있다.

[0082] 한편, 상기 차량등록서버(2000)의 제1차량정보등록부(2100)에서 수행하는 제1차량정보등록단계(S20)는 상기 차량등록서버(2000)와 통신을 수행하는 차량관련자단말기(4000)로부터 해당 차량의 식별정보 및 해당 차량의 속성정보를 수신하여 등록한다. 상기 식별정보는 해당 차량을 식별할 수 있는 고유한 정보로써, 예를 들어 해당 차량의 차대번호, 차량번호, vehicle identification number(VIN) 등이 상기 식별정보에 포함될 수 있다.

[0084] 상기 속성정보는 필요에 따라 긴급하게 주행해야 하는 차량에 대한 정보에 해당할 수 있다.

[0086] 구체적으로, 상기 속성정보는 해당 차량의 용도, 목적 등과 같이 해당 차량의 속성에 대한 정보에 해당할 수 있다. 예를 들어, 구급차, 경찰차, 소방차 등에 대한 정보, 운수용, 영업용, 대여용 등에 대한 정보들이 상기 속성정보에 포함될 수 있다.

[0087] 본 발명의 다른 실시예에서 상기 제1차량정보등록단계(S20)는 상기 차량관련자단말기(4000)로부터 해당 차량의 식별정보 및 속성정보를 수신하여 저장하고, 저장된 상기 식별정보 및 상기 속성정보를 포함하는 제1차량서명정보에 대한 생성 요청을 해당 차량의 차량단말기(1100)로 송신하고, 상기 요청을 수신한 상기 차량단말기(1100)는 후술하는 제2차량정보등록단계(S30)를 수행할 수도 있다.

[0089] 상기 차량단말기(1100)의 제2차량정보등록부(1120)에서 수행하는 제2차량정보등록단계(S30)에서는 상기 차량등록서버(2000)에 등록된 해당 차량의 식별정보 및 속성정보와 상기 차량DID문서등록단계(S10)에서 생성된 해당 차량의 DID식별자 및 상기 식별정보 가운데 1 이상을 포함하는 제1검증정보를 상기 차량DID문서등록단계(S10)에서 생성된 차량개인키로 서명하여 제1차량서명정보를 생성하고, 상기 제1차량서명정보, 상기 식별정보, 상기 속성정보, 상기 DID식별자를 포함하는 정보를 상기 차량등록서버(2000)에 송신한다.

[0090] 바람직하게는 상기 제1검증정보는 상기 식별정보, 상기 속성정보 및 상기 DID식별자를 모두 포함하며, 상기 제1검증정보에 포함되는 상기 식별정보, 상기 속성정보 및 상기 DID식별자는 서로 연결(Concatenation)될 수 있다.

[0092] 상기 제2차량정보등록단계(S30)를 통해 상기 차량단말기(1100)로부터 상기 제1차량서명정보, 상기 식별정보, 상기 속성정보, 상기 DID식별자를 포함하는 정보를 수신한 상기 차량등록서버(2000)는 상기 정보를 저장하고, VC정보전송부(2200)를 통해 VC정보전송단계(S40)를 수행한다.

[0093] 상기 VC정보전송단계(S40)는 상기 제1차량정보등록단계(S20)에서 등록된 정보 및 상기 제2차량정보등록단계(S30)에서 수신한 정보를 검증하고, 정상적으로 검증된 경우에 해당 차량에 대한 VC정보를 생성하여 해당 차량단말기(1100)에 송신한다.

[0094] 구체적으로, 상기 VC정보전송단계(S40)는 상기 제2차량정보등록단계(S30)를 통해 수신한 DID식별자 및 상기 블록체인(3000)에 등록되어 있는 DID문서에 포함된 DID식별자에 기초하여 상기 제2차량정보등록단계(S30)를 통해 수신한 DID식별자에 상응하는 DID문서를 블록체인(3000)을 통해 획득하고, 상기 DID문서에 포함된 차량공개키를 사용하여 상기 제2차량정보등록단계(S30)를 통해 수신한 제1차량서명정보를 검증한다. 만약 차량공개키를 통해

정상적으로 검증이 완료된 경우에 상기 VC정보전송단계(S40)는 해당 차량에 대한 VC정보를 생성하고, 상기 VC정보를 해당 차량의 차량단말기(1100)로 송신한다.

[0095] 바람직하게는 생성된 VC정보는 상기 차량등록서버(2000)의 서버개인키로 서명될 수 있고, 서명된 VC정보를 수신하는 차량단말기(1100)는 상기 차량등록서버(2000)의 서버공개키로 상기 서명된 VC정보를 검증할 수 있으며, 이에 대해서는 후술하는 도 5에서 상세하게 설명하도록 한다.

[0096] 한편, 본 발명의 다른 실시예에서 상기 VC정보전송단계(S40)에서 상기 제1차량서명정보가 정상적으로 검증되지 않은 경우에 VC정보를 생성하지 않고, VC정보가 생성되지 않았음을 해당 차량의 차량단말기(1100)로 송신할 수도 있다.

[0097] 상기 VC정보를 수신한 차량단말기(1100)는 기설정된 특정 상황 혹은 해당 차량에 탑승한 탑승자(운전자 또는 동승자)의 입력에 따라 차량메시지송신단계(S50)가 수행될 수 있다. 상기 차량메시지송신단계(S50)에서는 1 이상의 다른 차량에 송신하기 위한 메시지를 생성하고, 상기 메시지를 1 이상의 다른 차량 각각의 차량단말기(1100)로 송신하며, 이에 대해서는 후술하는 도 6 및 도 7에서 상세하게 설명하도록 한다.

[0099] 도 4는 본 발명의 일 실시예에 따른 차량단말기(1100)에 VC정보를 제공하는 과정을 개략적으로 도시한다.

[0100] 도 4는 본 발명의 일 실시예에 따른 상기 차량DID문서등록단계(S10), 상기 제1차량정보등록단계(S20), 상기 제2차량정보등록단계(S30) 및 상기 VC정보전송단계(S40)를 블록체인(3000) 기반 DID를 이용한 차량간 메시지 전송 방법을 수행하기 위한 구성요소를 중심으로 도시한 도면에 해당한다.

[0101] 도 4에 기재된 번호의 순서에 따라 설명하면, 상기 차량단말기(1100)는 차량DID문서등록단계(S10)를 수행하여, 해당 차량에 대한 차량개인키 및 차량공개키를 생성하고(도 4의 1번), 해당 차량에 대한 DID식별자를 생성한다(도 4의 2번). 이어서 상기 차량DID문서등록단계(S10)는 생성된 차량공개키 및 DID식별자를 포함하는 DID문서를 생성하고(도 4의 3번), 상기 블록체인(3000)에 DID문서의 등록을 요청(도 4의 4번)하는 것으로 상기 블록체인(3000)에는 상기 DID문서가 등록(도 4의 5번)될 수 있다. 한편, 상기 차량DID문서등록단계(S10)를 통해 생성된 정보들은 상기 차량단말기(1100)의 DID지갑(1140)에 저장될 수 있다.

[0102] 한편, 해당 차량에 대한 차량관련자단말기(4000)로부터 상기 차량등록서버(2000)는 차량정보등록에 대한 정보를 수신한다(도 4의 6번). 구체적으로 상기 차량정보등록에 대한 정보에는 해당 차량의 식별정보 및 속성정보를 포함할 수 있다. 상기 차량등록서버(2000)는 수신한 차량의 식별정보 및 속성정보를 저장한다.

[0103] 이어서, 상기 차량등록서버(2000)는 상기 차량단말기(1100)에 수신한 차량의 식별정보 및 속성정보에 따른 제1차량서명정보의 생성을 요청하고, 상기 차량단말기(1100)는 상기 차량등록서버(2000)로부터 수신한 식별정보, 속성정보 및 상기 차량단말기(1100)에서 생성한 DID식별자에 기초하여 제1차량서명정보를 생성하고, 상기 제1차량서명정보, 상기 식별정보, 상기 속성정보 및 상기 DID식별자를 포함하는 정보를 상기 차량등록서버(2000)로 송신한다(도 4의 7번).

[0104] 이어서, 상기 차량단말기(1100)로부터 상기 제1차량서명정보, 상기 식별정보, 상기 속성정보 및 상기 DID식별자를 포함하는 정보를 수신한 차량등록서버(2000)는 상기 VC정보전송단계(S40)를 수행한다.

[0106] 상기 VC정보전송단계(S40)는, 상기 제2차량정보등록단계(S30)를 통해 상기 차량단말기(1100)로부터 수신한 상기 DID식별자에 기초하여 상기 블록체인(3000)에 등록된 해당 DID식별자를 포함하는 DID문서를 획득하는 DID문서획득단계; 획득한 상기 DID문서에 포함된 차량공개키를 사용하여 상기 제2차량정보등록단계(S30)를 통해 상기 차량단말기(1100)로부터 수신한 제1차량서명정보를 검증하는 차량서명정보검증단계; 및 상기 차량서명정보검증단계를 통해 상기 제1차량서명정보가 정상적으로 검증된 경우에 상기 VC정보를 생성하고, 생성된 상기 VC정보를 상기 차량등록서버(2000)의 서버개인키로 서명하여, 서명된 상기 VC정보를 상기 차량에 전송하는 VC정보서명단계;를 포함할 수 있다.

[0108] 구체적으로, 상기 DID문서획득단계는 상기 차량단말기(1100)로부터 수신한 제1차량서명정보를 검증하기 위한 차량공개키를 획득하기 위하여 상기 차량공개키가 포함된 DID문서를 상기 블록체인(3000)을 통해 획득한다. 더 구체적으로 상기 DID문서획득단계는 상기 차량단말기(1100)로부터 수신한 DID식별자를 사용하여 해당 DID식별자를 포함하는 DID문서를 상기 블록체인(3000)을 통해 획득할 수 있다(도 4의 8번).

[0109] 상기 차량서명정보검증단계는 상기 DID문서획득단계를 통해 획득한 DID문서에 포함된 차량공개키를 사용하여 상기 차량단말기(1100)로부터 수신한 제1차량서명정보를 검증한다. 상기 제1차량서명정보는 상술한 바와 같이 상기 차량단말기(1100)에서 차량개인키를 사용하여 서명한 정보에 해당하므로, 상기 DID문서에 포함된 차량공개키

를 통해 상기 제1차량서명정보를 검증할 수 있다.

[0110] 한편, 상기 차량서명정보검증단계를 통해 상기 제1차량서명정보의 검증이 정상적으로 이루어진 경우에 상기 VC정보서명단계는 해당 차량의 식별정보, 속성정보 및 DID식별자에 기초하여 VC정보를 생성하고(도 4의 9번), 상기 VC정보를 상기 차량등록서버(2000)의 서버개인키로 서명하여 상기 서명된 VC정보를 해당 차량의 차량단말기(1100)로 송신한다(도 4의 10번). 상기 차량단말기(1100)는 수신한 상기 서명된 VC정보를 저장하고, 기설정된 특정 상황 또는 해당 차량의 탑승자의 입력에 따라 상기 VC정보에 기초하여 메시지를 생성할 수 있다.

[0111] 본 발명의 다른 실시예에서 상기 차량등록서버(2000) 또한 차량단말기(1100)와 유사하게 상기 차량등록서버(2000)에 대한 서버개인키, 서버공개키 및 DID식별자를 생성하고, 상기 서버공개키 및 상기 DID식별자를 포함하는 DID문서를 생성하여 블록체인(3000)에 등록할 수 있으며, 이에 대해서는 후술하는 도 5에서 상세하게 설명하도록 한다.

[0113] 도 5는 본 발명의 일 실시예에 따른 서버DID문서등록단계를 개략적으로 도시한다.

[0115] 도 5에 도시된 바와 같이, 상기 블록체인(3000) 기반 DID를 이용한 차량간 메시지 전송방법은, 상기 차량등록서버(2000)에서, 상기 차량등록서버(2000)에 대한 서버개인키, 서버공개키 및 DID식별자를 생성하고, 상기 DID식별자 및 상기 서버공개키를 포함하는 DID문서를 상기 블록체인(3000)에 등록하는 서버DID문서등록단계;를 더 포함하고, 상기 VC정보전송단계(S40)는, 생성된 상기 VC정보를 상기 서버개인키로 서명하고, 상기 서명된 VC정보를 상기 차량에 전송할 수 있다.

[0117] 구체적으로, 상기 차량등록서버(2000)에 포함된 서버DID문서등록부(2300)에서 수행하는 서버DID문서등록단계는 상술한 차량DID문서등록단계(S10)와 유사하게 상기 차량등록서버(2000)에 대한 서버개인키, 서버공개키 및 DID식별자를 생성할 수 있다. 마찬가지로 상기 서버개인키는 상기 차량등록서버(2000)에서 생성되는 정보에 대해 서명을 수행하기 위한 요소로 사용될 수 있고, 상기 서버공개키는 상기 차량등록서버(2000)에서 서명한 정보를 수신한 타 구성요소, 예를 들어, 상기 차량단말기(1100)에서 서명을 검증하기 위한 요소로 사용될 수 있으며, 상기 DID식별자는 상기 차량등록서버(2000)에 고유하게 부여되는 값으로써, 블록체인(3000)에 등록된 복수의 DID문서 가운데 상기 차량등록서버(2000)의 DID문서를 획득하기 위한 요소로 사용될 수 있다. 상기 서버개인키 및 상기 서버공개키는 통상적으로 정보의 서명 및 검증에 사용되는 개인키/공개키 쌍의 형태와 동일한 형태로 생성될 수 있으며, 상기 DID식별자는 종래의 사용되는 DID식별자의 형태와 동일하게 생성되거나, 혹은 기설정된 크기를 갖는 난수값에 해당할 수도 있다.

[0118] 한편, 상기 서버DID문서등록단계에서는 생성된 상기 서버공개키 및 상기 DID식별자를 포함하는 상기 차량등록서버(2000)에 대한 DID문서를 도출하여 블록체인(3000)에 등록하게 된다. 상기 차량등록서버(2000)가 블록체인(3000)에 참여하는 특정 노드에 해당하는 경우에 상기 차량등록서버(2000)는 DID문서에 대한 정보가 포함되는 블록을 생성하여 1 이상의 타 노드에 전파하는 것으로 블록체인(3000)에 상기 DID문서를 등록할 수 있다.

[0119] 이와 같이, 상기 서버DID문서등록단계를 통해 블록체인(3000)에 등록된 상기 차량등록서버(2000)의 DID문서는 서버개인키로 서명된 VC정보를 상기 차량단말기(1100)에서 검증하거나, 혹은 상기 차량단말기(1100)에서 생성된 메시지를 수신하는 1 이상의 타 차량(5000)의 차량단말기에서 상기 메시지에 포함된 VC정보를 검증하기 위한 용도로 사용될 수 있다.

[0121] 도 6은 본 발명의 일 실시예에 따른 VP정보의 구성요소들을 개략적으로 도시한다.

[0123] 도 6에 도시된 바와 같이, 상기 차량메시지송신단계(S50)는, 상기 VC정보, 메시지정보, 시점정보 및 상기 VC정보와 상기 메시지정보와 상기 시점정보 가운데 1 이상을 포함하는 제2검증정보를 해당 차량의 차량개인키로 서명한 제2차량서명정보를 포함하는 VP(Verifiable Presentation)정보를 생성하고, 상기 VP정보를 직접적 혹은 간접적으로 1 이상의 다른 차량의 차량단말기(1100)에 송신할 수 있다.

[0125] 구체적으로, 상기 차량메시지송신부(1130)에서 수행하는 차량메시지송신단계(S50)는 Verifiable Presentation(VP)정보를 생성하고, 상기 VP정보가 상술한 메시지에 해당할 수 있다. 상기 VP정보는 해당 차량(1000)의 신원을 식별할 수 있는 검증가능한 1 이상의 정보들을 포함할 수 있다. 이를 위해 상기 차량메시지송신단계(S50)에서 생성되는 VP정보는 상기 VC정보 혹은 상기 VC정보에 포함된 복수의 세부정보 가운데 1 이상의 세부정보, 1 이상의 다른 차량단말기(1100)로 전송하고자 하는 메시지정보, 시점정보 및 상기 VC정보 혹은 상기 VC정보에 포함되는 복수의 세부정보 가운데 1 이상의 세부정보, 상기 메시지정보, 상기 시점정보 가운데 1 이상을 포함하는 제2검증정보를 해당 차량의 차량개인키로 서명한 제2차량서명정보를 포함할 수 있다.

[0126] 상기 시점정보는 재전송 공격(Replay Attack)을 방지하기 위한 정보로써, 특정 시점에 대한 정보, 또는 시퀀스 숫자 정보, 또는 Challenge-Response 방식에서 Response 정보에 해당할 수 있다. 한편, 상기 시점정보가 상기 Response 정보에 해당하는 경우에 상기 시점정보는 무작위 숫자에 해당하거나 무작위 숫자에 1을 더한 값에 해당할 수 있다. 또한 도 6에서는 상기 시점정보와 상기 메시지정보를 구분하여 도시하였으나, 본 발명의 다른 실시예에서 상기 시점정보는 상기 메시지정보 내에 포함될 수도 있다.

[0127] 한편, 상기 차량개인키에 의해 서명되는 제2검증정보에 포함되는 정보가 복수인 경우에, 즉 상기 VC정보, 상기 메시지정보 및 상기 시점정보 가운데 2 이상의 정보가 포함되는 경우에 각 정보들은 서로 연결(Concatenation)될 수 있다. 상기 제2검증정보가 차량개인키로 서명되어 도출된 제2차량서명정보는 상기 메시지에 해당하는 VP정보를 수신하는 1 이상의 타 차량(5000)의 차량단말기에서 상기 VP정보를 검증하기 위한 요소로 사용될 수 있다.

[0129] 도 7은 본 발명의 일 실시예에 따른 VC정보를 수신한 차량단말기(1100)에서 타 차량(5000)의 차량단말기로 메시지를 송신하는 과정을 개략적으로 도시한다.

[0130] 도 7은 본 발명의 일 실시예에 따른 상기 차량메시지송신단계(S50)를 블록체인(3000) 기반 DID를 이용한 차량간 메시지 전송방법을 수행하기 위한 구성요소를 중심으로 도시한 도면에 해당한다.

[0132] 도 7에 도시된 바와 같이, 상기 VP정보를 수신한 1 이상의 다른 차량의 차량단말기(1100)는, 상기 VP정보를 생성한 차량에 상응하는 DID문서 및 상기 VC정보를 생성한 차량등록서버(2000)에 상응하는 DID문서를 상기 블록체인(3000)으로부터 직접적 혹은 간접적으로 획득하고, 획득한 DID문서 각각에 포함된 해당 차량의 차량공개키 및 해당 차량등록서버(2000)의 서버공개키를 사용하여 상기 VP정보에 포함된 제2차량서명정보 및 상기 VC정보를 검증할 수 있다.

[0134] 구체적으로, 도 7에 기재된 번호의 순서에 따라 설명하면, 상기 차량(1000)의 차량단말기(1100)는 상기 차량메시지송신단계(S50)를 수행하여 메시지에 해당하는 VP정보를 생성한다. 상술한 바와 같이 상기 VP정보는 해당 차량(1000)에 대하여 상기 차량등록서버(2000)에서 생성된 VC정보, 상기 차량단말기(1000)에서 생성된 메시지정보, 시점정보 및 제2차량서명정보를 포함할 수 있다(도 7의 1번). 이후에 상기 차량메시지송신단계(S50)는 생성한 상기 VP정보를 상기 노변기지국(6000)을 통해 1 이상의 타 차량(5000)의 차량단말기로 송신한다(도 7의 2번). 도 7에서는 상기 노변기지국(6000)을 통해 상기 VP정보를 1 이상의 타 차량(5000)의 차량단말기로 송신하는 것으로 도시되어 있으나, 본 발명의 다른 실시예에서는 상기 차량(1000) 및 1 이상의 타 차량(5000)는 직접적으로 통신할 수 있고, 따라서 상기 VP정보를 상기 노변기지국(6000)을 경유하지 않고 직접적으로 송신할 수도 있다.

[0135] 한편, 상기 VP정보를 수신한 상기 타 차량(5000)의 차량단말기에서는 상기 VP정보를 생성한 차량단말기(1100)에 상응하는 DID문서를 상기 블록체인(3000)에 요청하고(도 7의 3번), 상기 블록체인(3000)으로부터 해당 DID문서를 제공받는다(도 7의 4번). 더 구체적으로 상기 VP정보를 송신하는 차량단말기(1100)는 상기 1 이상의 타 차량(5000)의 차량단말기에 상기 VP정보 외에도 자신의 DID식별자를 추가적으로 송신하고, 상기 1 이상의 타 차량(5000)의 차량단말기는 추가적으로 수신한 DID식별자와 동일한 DID식별자를 포함하고 있는 DID문서를 블록체인(3000)으로부터 획득하게 된다.

[0136] 본 발명의 다른 실시예에서 상기 VP정보에 포함되는 VC정보는 상기 서버개인키에 의해 서명되어 있고, 상기 서명된 VC정보를 포함하는 VP정보를 수신하는 1 이상의 타 차량(5000)의 차량단말기는 상기 서버개인키에 의해 서명된 VC정보를 추가적으로 검증하기 위하여 상기 차량등록서버(2000)에 대한 DID문서를 블록체인(3000)으로부터 추가적으로 획득할 수도 있다.

[0137] 구체적으로, 상기 VP정보를 송신하는 차량단말기(1100)는 상기 1 이상의 타 차량(5000)의 차량단말기에 상기 VP정보 및 자신의 DID식별자 외에도 상기 차량등록서버(2000)의 DID식별자를 추가적으로 송신하고, 상기 1 이상의 타 차량(5000)의 차량단말기는 추가적으로 수신한 차량등록서버(2000)의 DID식별자와 동일한 DID식별자를 포함하고 있는 DID문서를 블록체인(3000)으로부터 획득하게 된다.

[0138] 이를 통해 1 이상의 타 차량(5000)의 차량단말기는 블록체인(3000)으로부터 획득한 상기 VP정보를 송신한 차량단말기(1100)의 상응하는 DID문서에 포함된 차량공개키를 통해 VP정보, 바람직하게는 상기 VP정보에 포함된 제2차량서명정보를 검증하고, 상술한 바와 같이, 서버공개키를 통해 서명된 VC정보를 검증하고자 하는 경우에도 상기 블록체인(3000)으로부터 획득한 상기 차량등록서버(2000)에 상응하는 DID문서에 포함된 서버공개키를 사용하여 상기 서명된 VC정보를 검증할 수 있다. 이에 따라 상기 VP정보의 검증이 정상적으로 완료된 경우에 상기 VP

정보에 포함된 메시지정보에 따라 상기 1 이상의 타 차량(5000)은 메시지에 해당하는 VP정보에 따른 응답을 수행할 수 있다(도 7의 5번).

[0140] 구체적으로, 상기 메시지는, 긴급상황의 발생에 따라 해당 차량이 긴급하게 주행할 수 있도록 상기 1 이상의 다른 차량의 주행 차선의 변경을 요청하는 정보에 해당할 수 있다.

[0142] 본 발명에서의 메시지는 상기 차량단말기(1100)에서 생성하는 VP정보에 해당할 수 있고, 상기 VP정보는 메시지를 수신하는 1 이상의 타 차량(5000)에게 특정 행동 등과 같이 특정 응답을 요청하는 메시지정보를 포함한다. 상기 메시지정보는 VP정보를 도출하는 차량이 필요에 따라 긴급하게 주행해야 하는 차량인 경우에, 긴급상황의 발생에 따라 해당 차량이 긴급하게 주행할 수 있도록 타 차량(5000)으로 하여금 차선의 변경을 요청하는 정보에 해당할 수 있다.

[0143] 따라서, 상기 VP정보를 수신한 1 이상의 타 차량(5000)의 차량단말기에서는 상기 VP정보를 검증하고, 검증이 정상적으로 이루어진 경우에 상기 메시지정보에 포함된 정보에 따라 해당 차량이 차선을 변경하도록 하는 제어를 수행할 수 있다.

[0144] 본 발명의 다른 실시예에서 상기 VP정보에 포함된 VC정보에는 해당 차량에 대한 속성정보를 포함할 수 있고, 상기 속성정보에는 필요에 따라 긴급하게 주행해야 하는 차량임을 식별할 수 있는 정보를 포함하므로, 상기 VP정보를 수신한 1 이상의 타 차량(5000)의 차량단말기에서 상기 속성정보를 통해 VP정보를 송신한 차량이 긴급하게 주행해야 하는 차량임을 판단할 수도 있다.

[0146] 도 8은 본 발명의 일 실시예에 따른 컴퓨팅장치의 내부 구성을 개략적으로 도시한다.

[0147] 상술한 도 2에 도시된 차량단말기(1100) 및 차량등록서버(2000)는 상기 도 8에 도시된 컴퓨팅장치(11000)의 구성요소들을 포함할 수 있다.

[0148] 도 8에 도시된 바와 같이, 컴퓨팅장치(11000)는 적어도 하나의 프로세서(processor)(11100), 메모리(memory)(11200), 주변장치 인터페이스(peripheral interface)(11300), 입/출력 서브시스템(I/O subsystem)(11400), 전력 회로(11500) 및 통신 회로(11600)를 적어도 포함할 수 있다. 이때, 컴퓨팅장치(11000)는 도 2에 도시된 차량단말기(1100) 및 차량등록서버(2000)에 해당될 수 있다.

[0149] 메모리(11200)는 일례로 고속 랜덤 액세스 메모리(high-speed random access memory), 자기 디스크, 에스램(SRAM), 디램(DRAM), 롬(ROM), 플래시 메모리 또는 비휘발성 메모리를 포함할 수 있다. 메모리(11200)는 컴퓨팅장치(11000)의 동작에 필요한 소프트웨어 모듈, 명령어 집합 또는 그 밖에 다양한 데이터를 포함할 수 있다.

[0150] 이때, 프로세서(11100)나 주변장치 인터페이스(11300) 등의 다른 컴포넌트에서 메모리(11200)에 액세스하는 것은 프로세서(11100)에 의해 제어될 수 있다.

[0151] 주변장치 인터페이스(11300)는 컴퓨팅장치(11000)의 입력 및/또는 출력 주변장치를 프로세서(11100) 및 메모리(11200)에 결합시킬 수 있다. 프로세서(11100)는 메모리(11200)에 저장된 소프트웨어 모듈 또는 명령어 집합을 실행하여 컴퓨팅장치(11000)을 위한 다양한 기능을 수행하고 데이터를 처리할 수 있다.

[0152] 입/출력 서브시스템은 다양한 입/출력 주변장치들을 주변장치 인터페이스(11300)에 결합시킬 수 있다. 예를 들어, 입/출력 서브시스템은 모니터나 키보드, 마우스, 프린터 또는 필요에 따라 터치스크린이나 센서 등의 주변장치를 주변장치 인터페이스(11300)에 결합시키기 위한 컨트롤러를 포함할 수 있다. 다른 측면에 따르면, 입/출력 주변장치들은 입/출력 서브시스템을 거치지 않고 주변장치 인터페이스(11300)에 결합될 수도 있다.

[0153] 전력 회로(11500)는 단말기의 컴포넌트의 전부 또는 일부로 전력을 공급할 수 있다. 예를 들어 전력 회로(11500)는 전력 관리 시스템, 배터리나 교류(AC) 등과 같은 하나 이상의 전원, 충전 시스템, 전력 실패 감지 회로(power failure detection circuit), 전력 변환기나 인버터, 전력 상태 표시자 또는 전력 생성, 관리, 분배를 위한 임의의 다른 컴포넌트들을 포함할 수 있다.

[0154] 통신 회로(11600)는 적어도 하나의 외부 포트를 이용하여 다른 컴퓨팅장치와 통신을 가능하게 할 수 있다.

[0155] 또는 상술한 바와 같이 필요에 따라 통신 회로(11600)는 RF 회로를 포함하여 전자기 신호(electromagnetic signal)라고도 알려진 RF 신호를 송수신함으로써, 다른 컴퓨팅장치와 통신을 가능하게 할 수도 있다.

[0156] 이러한 도 8의 실시예는, 컴퓨팅장치(11000)의 일례일 뿐이고, 컴퓨팅장치(11000)는 도 8에 도시된 일부 컴포넌트가 생략되거나, 도 8에 도시되지 않은 추가의 컴포넌트를 더 구비하거나, 2개 이상의 컴포넌트를 결합시키는

구성 또는 배치를 가질 수 있다. 예를 들어, 모바일 환경의 통신 단말을 위한 컴퓨팅장치는 도 8에 도시된 컴포넌트들 외에도, 터치스크린이나 센서 등을 더 포함할 수도 있으며, 통신 회로(11600)에 다양한 통신방식(WiFi, 3G, LTE, Bluetooth, NFC, Zigbee 등)의 RF 통신을 위한 회로가 포함될 수도 있다. 컴퓨팅장치(11000)에 포함 가능한 컴포넌트들은 하나 이상의 신호 처리 또는 어플리케이션에 특화된 집적 회로를 포함하는 하드웨어, 소프트웨어, 또는 하드웨어 및 소프트웨어 양자의 조합으로 구현될 수 있다.

[0157] 본 발명의 실시예에 따른 방법들은 다양한 컴퓨팅장치를 통하여 수행될 수 있는 프로그램 명령(instruction) 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 특히, 본 실시예에 따른 프로그램은 PC 기반의 프로그램 또는 모바일 단말 전용의 어플리케이션으로 구성될 수 있다. 본 발명이 적용되는 어플리케이션은 파일 배포 시스템이 제공하는 파일을 통해 컴퓨팅장치(11000)에 설치될 수 있다. 일 예로, 파일 배포 시스템은 컴퓨팅장치(11000)의 요청에 따라 상기 파일을 전송하는 파일 전송부(미도시)를 포함할 수 있다.

[0159] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 어플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0160] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨팅장치 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0161] 실시예에 따른 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 실시예를 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. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0163] 본 발명의 일 실시예에 따르면, 블록체인에 차량에 대한 DID문서를 등록하고, 상기 DID문서에 포함된 해당 차량의 공개키를 통해 해당 차량의 신원을 검증하므로, 중앙화 된 시스템이 없이도 차량의 신원을 검증하여 메시지를 송수신할 수 있는 시스템을 구현할 수 있는 효과를 발휘할 수 있다.

[0164] 본 발명의 일 실시예에 따르면, 블록체인에 차량에 대한 DID문서를 등록하여 DID문서의 위,변조 가능성을 낮출 수 있는 효과를 발휘할 수 있다.

[0165] 본 발명의 일 실시예에 따르면, 구급차, 경찰차 등과 같이 긴급하게 주행해야 하는 차량을 대상으로 하여 차량 등록서버에서 VC정보를 생성하여 해당 차량에 제공하고, 해당 차량은 VC정보에 기초하여 메시지를 생성하여 타

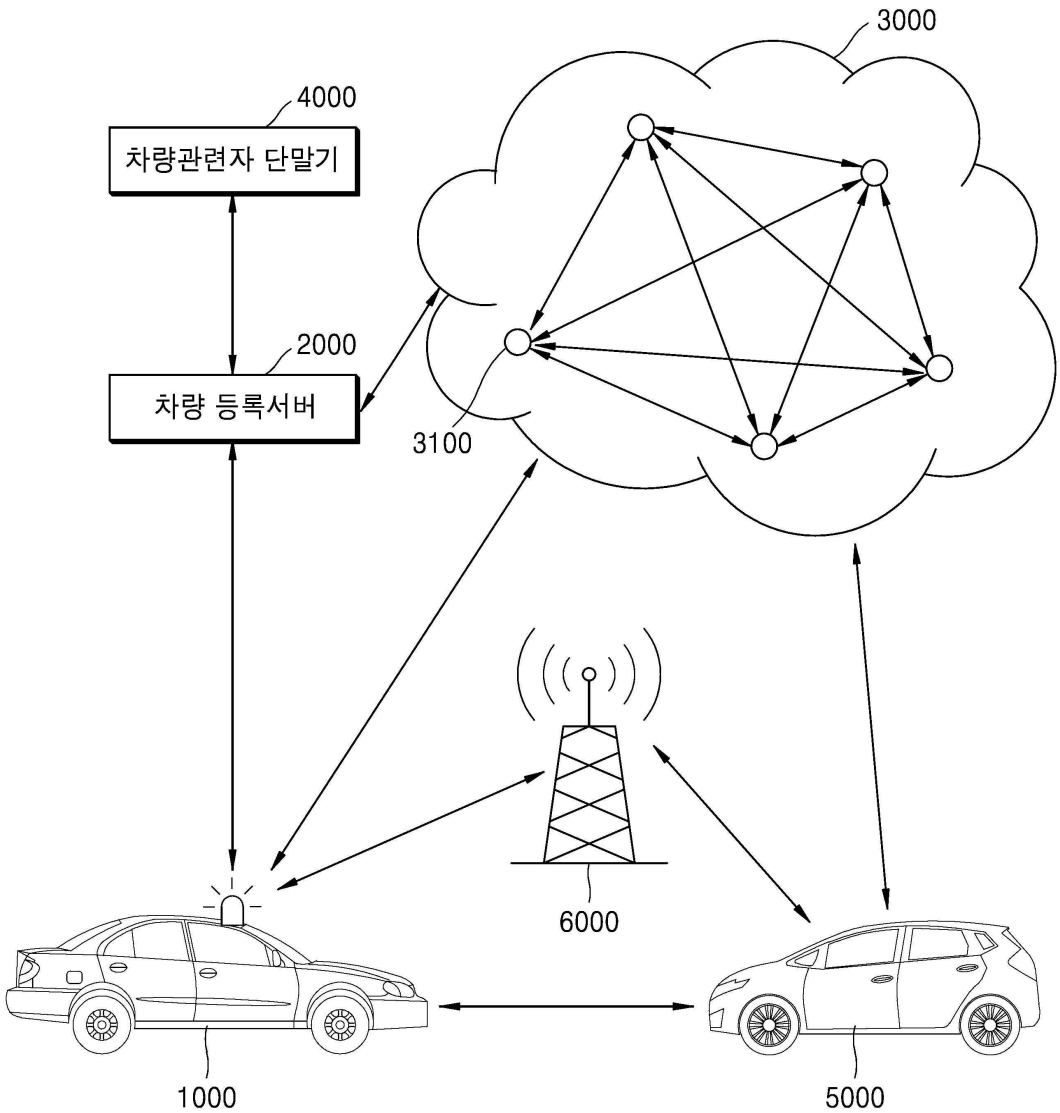
차량에 전송할 수 있으므로, 긴급차량이 주행 경로에 있는 타 차량에게 차선의 변경을 요청하는 메시지를 용이하게 송신할 수 있는 효과를 발휘할 수 있다.

[0167] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

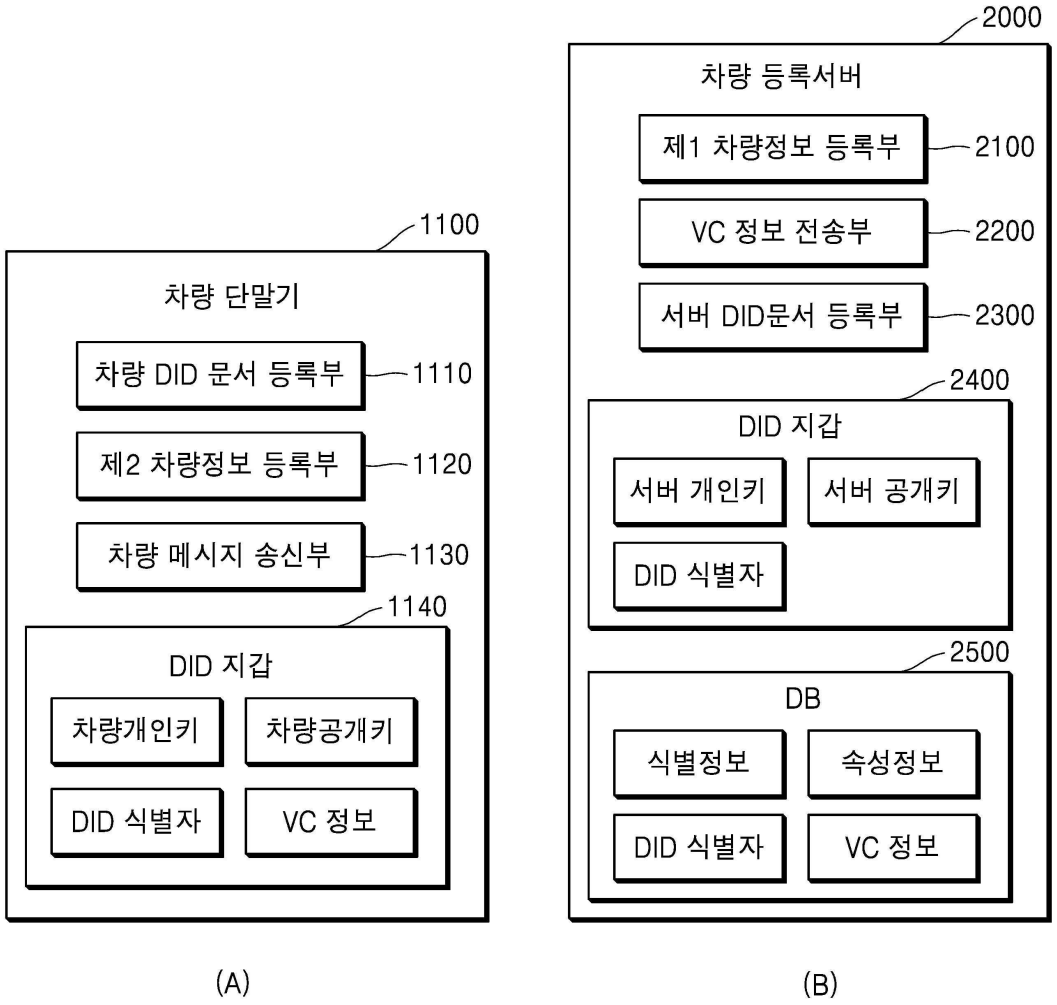
[0168] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

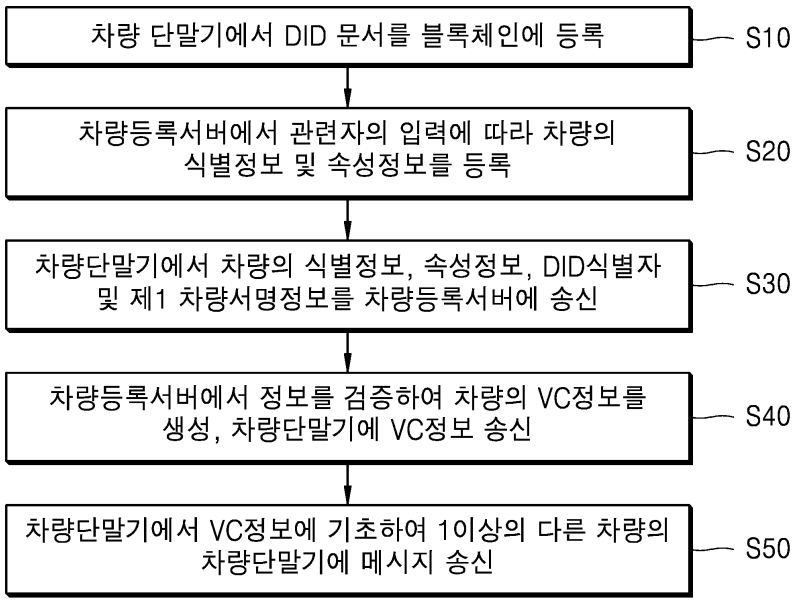
도면1



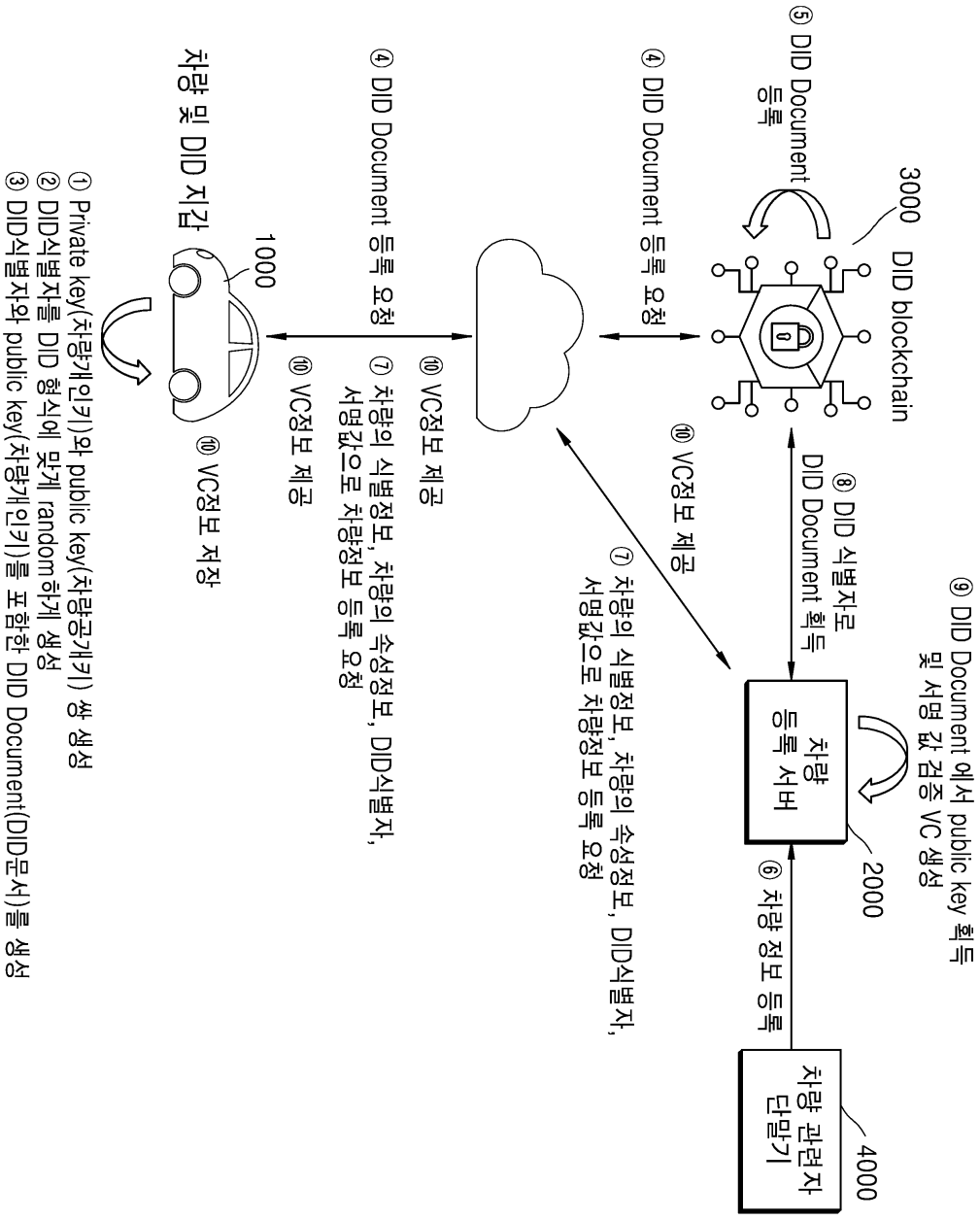
도면2


2000
차량 등록서버
제1 차량정보 등록부
2100
VC 정보 전송부
2200
서버 DID문서 등록부
2300
2400
DID 지갑
서버 개인키
서버 공개키
DID 식별자
2500
DB
식별정보
속성정보
DID 식별자
VC 정보
1100
차량 단말기
차량 DID 문서 등록부
1110
제2 차량정보 등록부
1120
차량 메시지 송신부
1130
1140
DID 지갑
차량개인키
차량공개키
DID 식별자
VC 정보
(A)
(B)

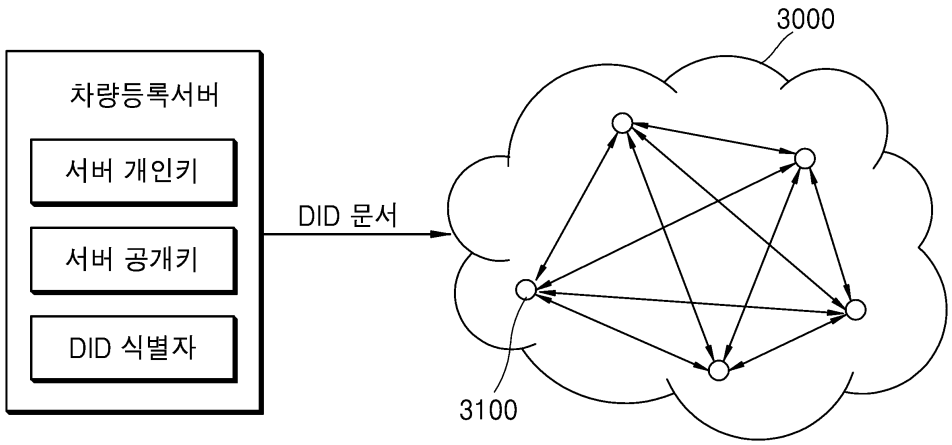
도면3


차량 단말기에서 DID 문서를 블록체인에 등록
S10
차량등록서버에서 관련자의 입력에 따라 차량의 식별정보 및 속성정보를 등록
S20
차량단말기에서 차량의 식별정보, 속성정보, DID식별자 및 제1 차량서명정보를 차량등록서버에 송신
S30
차량등록서버에서 정보를 검증하여 차량의 VC정보를 생성, 차량단말기에 VC정보 송신
S40
차량단말기에서 VC정보에 기초하여 1이상의 다른 차량의 차량단말기에 메시지 송신
S50

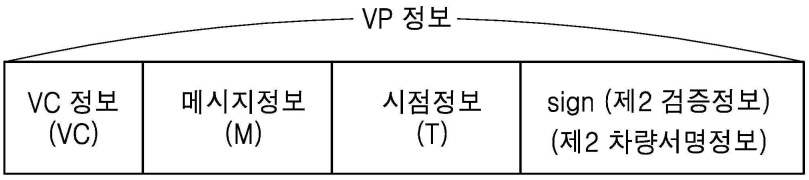
도면4


① Private key(차량개인키)와 public key(차량공개키) 쌍 생성
② DID식별자를 DID 형식에 맞게 random하게 생성
③ DID식별자와 public key(차량개인키)를 포함한 DID Document(DID문서)를 생성
차량 및 DID 지갑
1000
④ DID Document 등록 요청
⑦ 차량의 식별정보, 차량의 속성정보, DID식별자, 서명값으로 차량정보 등록 요청
⑩ VC정보 제공
⑩ VC정보 저장
⑤ DID Document 등록
④ DID Document 등록 요청
3000
DID blockchain
⑩ VC정보 제공
⑦ 차량의 식별정보, 차량의 속성정보, DID식별자, 서명값으로 차량정보 등록 요청
⑧ DID 식별자로 DID Document 획득
⑨ DID Document 에서 public key 획득 및 서명 값 검증 VC 생성
차량 등록 서버
2000
⑥ 차량 정보 등록
차량 관련자 단말기
4000

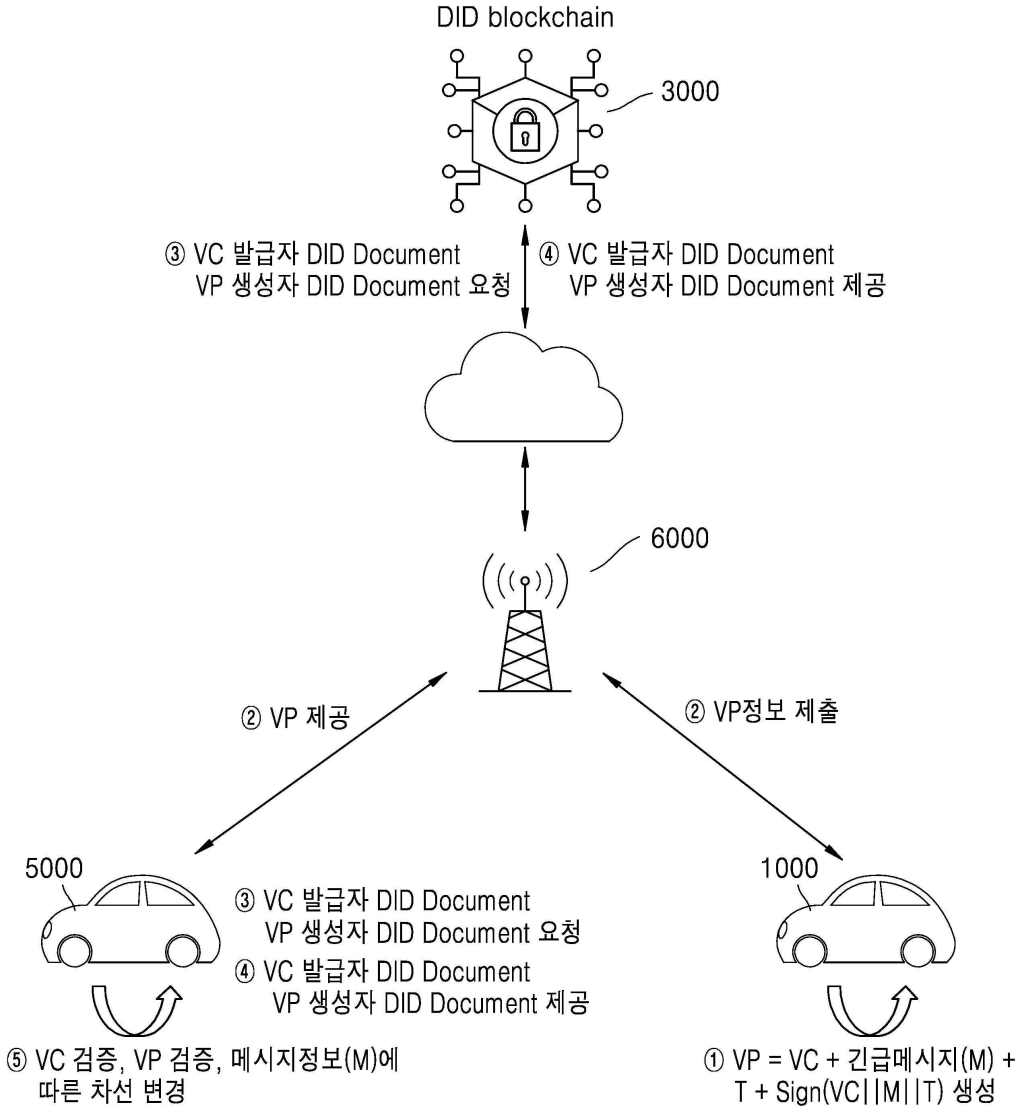
도면5


차량등록서버
서버 개인키
서버 공개키
DID 식별자
DID 문서
3000
3100

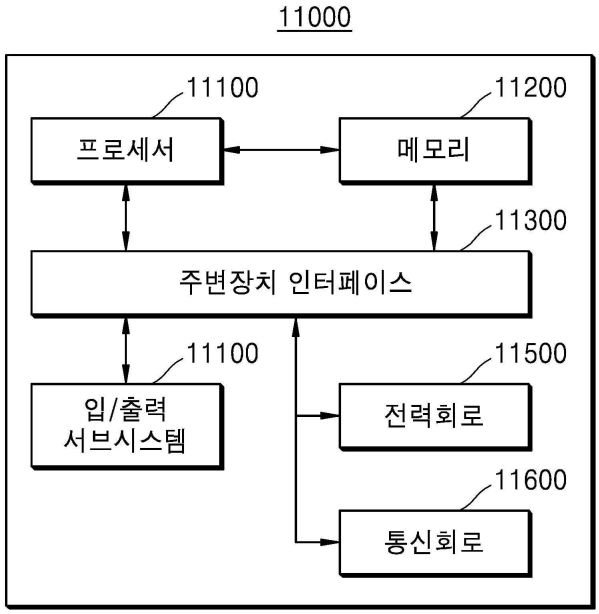
도면6


VP 정보
VC 정보
(VC)
메시지정보
(M)
시점정보
(T)
sign (제2 검증정보)
(제2 차량서명정보)

도면7


DID blockchain
3000
③ VC 발급자 DID Document
VP 생성자 DID Document 요청
④ VC 발급자 DID Document
VP 생성자 DID Document 제공
6000
② VP 제공
② VP정보 제출
5000
1000
③ VC 발급자 DID Document
VP 생성자 DID Document 요청
④ VC 발급자 DID Document
VP 생성자 DID Document 제공
⑤ VC 검증, VP 검증, 메시지정보(M)에
따른 차선 변경
① VP = VC + 긴급메시지(M) +
T + Sign(VC||M||T) 생성

도면8


11000
11100
프로세서
11200
메모리
11300
주변장치 인터페이스
11100
입/출력
서브시스템
11500
전력회로
11600
통신회로