(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0066801
(43) 공개일자 2022년05월24일

(51) 국제특허분류(Int. Cl.)
H04L 51/00 (2022.01) *G06Q 50/30* (2012.01)
H04L 9/40 (2022.01)
(52) CPC특허분류
H04L 51/043 (2022.05)
G06Q 50/30 (2015.01)
(21) 출원번호 10-2021-0004233
(22) 출원일자 2021년01월12일
심사청구일자 2022년01월14일
(30) 우선권주장
1020200152547 2020년11월16일 대한민국(KR)

(71) 출원인
포항공과대학교 산학협력단
경상북도 포항시 남구 청암로 77 (지곡동)
(72) 발명자
박찬익
경상북도 포항시 남구 지곡로 155, 6동 1105호
홍상원
서울특별시 노원구 석계로 49, 111동 405호
(뒷면에 계속)
(74) 대리인
특허법인이상

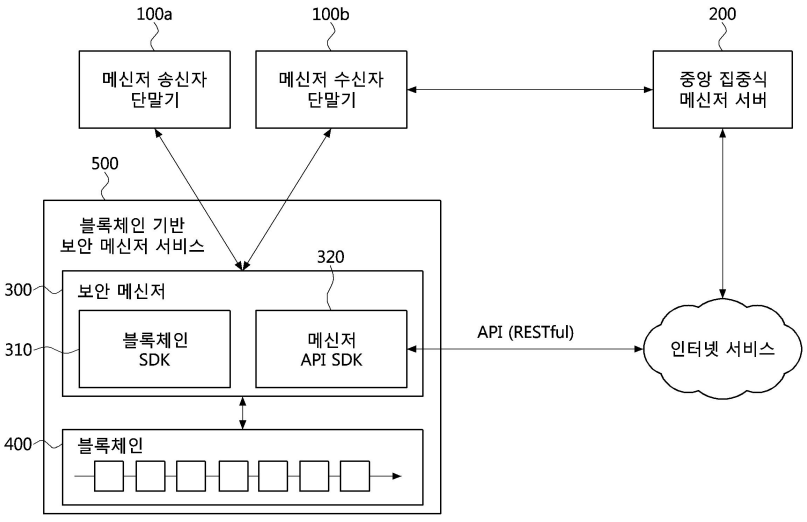
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **블록체인 기반 보안 메신저 서비스 방법 및 장치**

(57) 요 약

블록체인 기반의 보안 메신저 서비스를 제공하는 방법 및 장치가 개시된다. 블록체인 기반 보안 메신저 서비스 방법은, 송신자의 제1 사용자 단말에 의해 실행되는 블록체인 기반 보안 메신저 서비스 방법으로서, 수신자의 제2 사용자 단말에게 전송할 메시지를 암호화하는 단계, 암호화된 메시지를 중앙 집중식 메신저 서버로 전달하는 단계, 중앙 집중식 메신저 서버로 전달한 입력 메시지 데이터를 획득하는 단계, 입력 메시지 데이터에 대한 블록체인 기반 대체불가능 토큰을 발행하는 단계 및 대체불가능 토큰을 제2 사용자 단말에게 전송하는 단계를 포함한다.

대 표 도



(52) CPC특허분류
H04L 51/23 (2022.05)
H04L 63/0435 (2013.01)
H04L 63/108 (2013.01)
H04L 9/50 (2022.05)
(72) 발명자
황제영
경상북도 포항시 남구 효자로77번길 5, 202호

노용두
대전광역시 유성구 봉산로 39 , 203동 907호

이 발명을 지원한 국가연구개발사업
과제고유번호 1711116142
과제번호 2018-0-01441-003
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 정보통신방송혁신인재양성
연구과제명 크로스 도메인 호환성을 위한 블록체인 플랫폼 및 비즈모델 개발
기 여 율 25/100
과제수행기관명 포항공과대학교 산학협력단
연구기간 2020.01.01 ~ 2020.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711116985
과제번호 2020-0-00936-001
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 블록체인융합기술개발
연구과제명 5G 초저지연 서비스를 위한 무선 단말용 블록체인 기술 개발
기 여 율 75/100
과제수행기관명 포항공과대학교 산학협력단
연구기간 2020.04.01 ~ 2020.12.31

명 세 서

청구범위

청구항 1

송신자의 제1 사용자 단말에 의해 실행되는 블록체인 기반 보안 메신저 서비스 방법으로서,

수신자의 제2 사용자 단말에게 전송할 메시지나 첨부파일을 암호화하는 단계;

상기 암호화하는 단계에서 암호화된 메시지를 중앙 집중식 메신저 서버를 통한 상기 제2 사용자 단말에게 전송하는 단계;

상기 암호화된 메시지에 대응하는 블록체인 기반 대체불가능 토큰을 발행하는 단계; 및

상기 대체불가능 토큰을 상기 제2 사용자 단말에게 전송하는 단계;

를 포함하는 블록체인 기반 보안 메신저 서비스 방법.

청구항 2

청구항 1에 있어서,

상기 암호화하는 단계는 상기 수신자의 공개키를 이용하여 상기 메시지 또는 상기 첨부파일을 암호화하는, 블록체인 기반 보안 메신저 서비스 방법.

청구항 3

청구항 1에 있어서,

상기 발행하는 단계 후에 상기 대체불가능 토큰의 소유자를 상기 수신자로 변경하는 단계를 더 포함하는, 블록체인 기반 보안 메신저 서비스 방법.

청구항 4

청구항 1에 있어서,

상기 제1 사용자 단말 및 상기 제2 사용자 단말은 인증기관(Certificate Authority)에서 인증하는 공개키 기반(Public Key Infrastructure) 키 쌍을 보유하는, 블록체인 기반 보안 메신저 서비스 방법.

청구항 5

청구항 1에 있어서,

상기 대체불가능 토큰의 속성은 토큰 식별자(ID), 토큰 타입, 소유자 정보, 송신자 메신저 ID, 수신자 메신저 ID, 메시지 내용 암호화 대칭키 정보, 유효기간 및 토큰 조회 상태 정보를 포함하는, 블록체인 기반 보안 메신저 서비스 방법.

청구항 6

청구항 1에 있어서,

상기 대체불가능 토큰은 토큰 생성 및 전송 트랜잭션 처리 정보에 대한 토큰 속성을 포함하고, 여기에서 상기 송신자 또는 상기 수신자는 상기 토큰 생성 및 전송 트랜잭션 처리 정보를 통해 상기 메시지의 송신 여부 또는 수신 여부에 대한 부인 방지 증명을 획득하는, 블록체인 기반 보안 메신저 서비스 방법.

청구항 7

청구항 1에 있어서,

상기 대체불가능 토큰은 유효기간에 대한 토큰 속성을 포함하고, 여기에서 상기 송신자 또는 상기 수신자는 상기 유효기간을 통해 메시지 유효성을 자체 판단하는, 블록체인 기반 보안 메신저 서비스 방법.

청구항 8

청구항 1에 있어서,

상기 제1 사용자 단말과 상기 제2 사용자 단말은 상기 중앙 집중식 메신저 서버를 통해 신호 및 데이터의 송수신하는 메신저 클라이언트들이며, XMPP(Extensible Messaging and Presence Protocol) 또는 메신저 자체 프로토콜을 사용하는, 블록체인 기반 보안 메신저 서비스 방법.

청구항 9

청구항 1에 있어서,

상기 송신자는 상기 대체불가능 토큰의 토큰 조회 상태 속성을 통해 상기 수신자의 수신 부인 방지를 검증하거나,

상기 수신자는 상기 대체불가능 토큰을 조회하여 상기 대체불가능 토큰에 기록되어 있는 송신자 서명과 메신저 ID를 확인하여 상기 송신자의 신원을 검증하거나, 상기 수신자의 공개키에 대응하는 메시지 암호화 대칭키를 통해 암호화된 메시지를 복호화하는, 블록체인 기반 보안 메신저 서비스 방법.

청구항 10

청구항 1에 있어서,

상기 제1 사용자 단말이나 상기 제2 사용자 단말에서 비보안 메시지 전송과 보안 메시지 전송을 선택하는 사용자 인터페이스에서 사용자 입력이나 명령을 획득하는 단계를 더 포함하며, 상기 사용자 입력이나 명령에 따라 상기 메시지를 암호화하는 단계, 상기 암호화된 메시지를 전송하는 단계, 상기 메시지 토큰을 발행하는 단계 및 상기 메시지 토큰을 전송하는 단계를 포함한 일련의 과정이 수행되는, 블록체인 기반 보안 메신저 서비스 방법.

청구항 11

청구항 1에 있어서,

상기 메시지에 포함되는 사진, 동영상, 문서 데이터 또는 이들 조합의 첨부 파일은 네트워크를 통해 접근가능한 오프체인 공간에 저장되며, 상기 대체불가능 토큰은 상기 첨부파일에 대한 상기 오프체인 공간의 저장 경로를 기록하는, 블록체인 기반 보안 메신저 서비스 방법.

청구항 12

청구항 11에 있어서,

상기 제1 사용자 단말의 메신저 화면에 상기 첨부파일의 암호화된 첨부파일 데이터를 획득하고, 상기 암호화된 첨부파일 데이터에 대한 블록체인 기반 대체불가능 추가 토큰을 발행하고, 상기 대체불가능 추가 토큰을 상기 제2 사용자 단말에 전송하기 위한 사용자 인터페이스를 제공하는 단계를 더 포함하는, 블록체인 기반 보안 메신저 서비스 방법.

청구항 13

송신자의 제1 사용자 단말에 탑재되는 블록체인 기반 보안 메신저 서비스 장치로서,

수신자의 제2 사용자 단말에게 전송할 메시지나 첨부파일의 암호화된 메시지를 중앙 집중식 메신저 서버를 통해 상기 제2 사용자 단말에게 전송하는 메시지 처리부; 및

상기 암호화된 메시지에 대한 입력 메시지 데이터를 획득하고 상기 입력 메시지 데이터에 대한 블록체인 기반 대체불가능 토큰을 발행하며, 상기 대체불가능 토큰을 상기 제2 사용자 단말에게 전송하는 토큰 처리부;

를 포함하는 블록체인 기반 보안 메신저 서비스 장치.

청구항 14

청구항 13에 있어서, 상기 토큰 처리부는,

상기 암호화된 메시지에 대한 입력 메시지 데이터를 획득하고 상기 입력 메시지 데이터에 대한 블록체인 기반

대체불가능 토큰을 발행하는 토큰 발행 모듈;

상기 대체불가능 토큰을 상기 제2 사용자 단말에게 전송하는 토큰 전송 모듈; 및

상기 대체불가능 토큰의 소유자를 상기 수신자로 변경하는 토큰 수정 모듈;

을 구비하는 블록체인 기반 보안 메신저 서비스 장치.

청구항 15

청구항 13에 있어서,

상기 메시지 토큰의 속성을 조회하는 트랜잭션을 생성하고 생성한 트랜잭션을 블록체인으로 전송하여 상기 메시지 토큰의 암호화 대칭키를 조회하는 토큰 조회 모듈을 더 포함하는, 블록체인 기반 보안 메신저 서비스 장치.

청구항 16

청구항 13에 있어서,

상기 토큰 발행 모듈, 상기 토큰 전송 모듈 및 상기 토큰 수정 모듈에 의한 메시지 토큰에 대한 동작 결과가 블록체인에 최종적으로 저장될 때, 상기 블록체인으로부터 이벤트를 받는 이벤트 관리 모듈을 더 포함하는 블록체인 기반 보안 메신저 서비스 장치.

청구항 17

청구항 13에 있어서,

상기 토큰 처리부는, 토큰 검증 모듈을 호출하여 상기 메시지 토큰에 기록된 상대방 메신저 ID를 확인하고, 상대방 메신저 ID에 대응하는 사용자 정보 및 공개키와 상대방의 사용자 정보 및 공개키와의 일치 여부를 비교함으로써, 상대방의 사용자 신원을 인증하는, 블록체인 기반 보안 메신저 서비스 장치.

청구항 18

청구항 13에 있어서,

상기 제1 사용자 단말 또는 상기 제2 사용자 단말은 인증기관(Certificate Authority)에서 인증하는 공개키 기반(Public Key Infrastructure) 키 쌍을 보유하는, 블록체인 기반 보안 메신저 서비스 장치.

청구항 19

청구항 13에 있어서,

상기 대체불가능 토큰의 속성은 토큰 식별자(ID), 토큰 타입, 소유자 정보, 송신자 메신저 ID, 수신자 메신저 ID, 메시지 내용 암호화 대칭키 정보, 유효기간 및 토큰 조회 상태 정보를 포함하는, 블록체인 기반 보안 메신저 서비스 장치.

청구항 20

청구항 13에 있어서,

상기 메신저 처리부와 상기 토큰 처리부를 포함하는 보안 메신저는 사용자 단말의 메신저 서비스 화면에 제공되는 사용자 인터페이스에서의 특정 입력 혹은 명령에 따라 비보안 메시지 전송과 보안 메시지 전송을 선택하는, 블록체인 기반 보안 메신저 서비스 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 보안 메신저 서비스에 관한 것으로, 보다 상세하게는, 블록체인 기반의 보안 메신저 서비스를 제공하는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 메신저 서비스는 스마트폰 도입 이후 가장 활발히 사용되고 있는 의사소통 수단이다. 대표적인 상용 메신저 서비스에는 카카오톡, 라인, 텔레그램 등이 있다. 이러한 상용 메신저 서비스 환경에서 사용자는 메시지를 송신하거나 수신할 때 모든 것을 중앙 집중식 메신저 서비스 제공자에게 의존해야 한다.

[0003] 사용자가 메신저 서비스를 통해 법적인 의미를 가지는 매우 중요한 메시지를 송·수신할 때, 다음과 같은 4가지 추가 기능을 필요로 한다. 즉, 메시지 상대방 신원 인증, 송·수신 메시지 내용 기밀성 보장, 송·수신 메시지 내용 무결성 증명, 메시지 송·수신 행위 부인 방지 증명이 필요하다.

[0004] 그러나, 사용자가 모든 기능을 전적으로 의존해야 하는 중앙 집중식 메신저 서비스는 내부 관리자에 의한 위변조 혹은 외부 해킹 공격에 취약하므로 법적 메시지 송·수신에 필수적으로 요구되는 4가지 기능을 지원할 수 없는 문제가 있다.

발명의 내용

해결하려는 과제

[0005] 본 발명은 전술한 종래 기술의 문제점을 해결하기 위해 도출된 것으로, 본 발명의 목적은 사용자가 법적인 의미를 가지는 중요한 메시지를 전송할 때 상용 메신저 서비스를 활용하면서도, 필수적으로 지원이 필요한 메시지 상대방 신원 인증, 송·수신 메시지 내용 기밀성 보장, 송·수신 메시지 내용 무결성 증명, 메시지 송·수신 행위 부인 방지 증명의 4가지 기능을 지원할 수 있는, 블록체인 기반의 보안 메시지 서비스 방법을 제공하는데 있다.

[0006] 본 발명의 다른 목적은 전술한 블록체인 기반의 보안 메시지 서비스 방법을 위한 블록체인 기반의 보안 메시지 서비스 장치를 제공하는 데 있다.

과제의 해결 수단

[0007] 상기 기술적 과제를 해결하기 위한 본 발명의 일 측면에 따른 블록체인 기반 보안 메신저 서비스 방법은, 송신자의 제1 사용자 단말에 의해 실행되는 블록체인 기반 보안 메신저 서비스 방법으로서, 수신자의 제2 사용자 단말에게 전송할 메시지나 첨부파일을 암호화하는 단계; 상기 암호화하는 단계에서 암호화된 메시지를 중앙 집중식 메신저 서버를 통한 제2 사용자 단말에게 전송하는 단계; 암호화된 메시지에 대응하는 블록체인 기반 대체불가능 토큰을 발행하는 단계; 및 대체불가능 토큰을 제2 사용자 단말에게 전송하는 단계를 포함한다.

[0008] 일실시예에서, 상기 암호화하는 단계는 수신자의 공개키를 이용하여 메시지 또는 첨부파일을 암호화한다.

[0009] 일실시예에서, 블록체인 기반 보안 메신저 서비스 방법은, 상기 발행하는 단계 후에 상기 대체불가능 토큰의 소유자를 상기 수신자로 변경하는 단계를 더 포함할 수 있다.

[0010] 일실시예에서, 상기 제1 사용자 단말 및 상기 제2 사용자 단말은 인증기관(Certificate Authority)에서 인증하는 공개키 기반(Public Key Infrastructure) 키 쌍을 보유할 수 있다.

[0011] 일실시예에서, 상기 대체불가능 토큰의 속성은 토큰 식별자(ID), 토큰 타입, 소유자 정보, 송신자 메신저 ID, 수신자 메신저 ID, 메시지 내용 암호화 대칭키 정보, 유효기간 및 토큰 조회 상태 정보를 포함할 수 있다.

[0012] 일실시예에서, 상기 대체불가능 토큰은 토큰 생성 및 전송 트랜잭션 처리 정보에 대한 토큰 속성을 포함하고, 여기서 송신자 또는 수신자는 토큰 생성 및 전송 트랜잭션 처리 정보를 통해 메시지의 송신 여부 또는 수신 여부에 대한 부인 방지 증명을 획득할 수 있다.

[0013] 일실시예에서, 상기 대체불가능 토큰은 유효기간에 대한 토큰 속성을 포함하고, 여기서 송신자 또는 수신자는 유효기간을 통해 메시지 유효성을 자체 판단할 수 있다.

[0014] 일실시예에서, 상기 제1 사용자 단말과 상기 제2 사용자 단말은 중앙 집중식 메신저 서버를 통해 신호 및 데이터의 송수신하는 메신저 클라이언트들이며, XMPP(Extensible Messaging and Presence Protocol) 또는 메신저 자체 프로토콜을 사용할 수 있다.

[0015] 일실시예에서, 상기 송신자는 대체불가능 토큰의 토큰 조회 상태 속성을 통해 수신자의 수신 부인 방지를 검증할 수 있다. 혹은, 상기 수신자는 대체불가능 토큰을 조회하여 대체불가능 토큰에 기록되어 있는 송신자 서명과 메신저 ID를 확인하여 송신자의 신원을 검증하거나, 수신자의 공개키에 대응하는 메시지 암호화 대칭키를 통해 암호화된 메시지를 복호화할 수 있다.

[0016] 일실시예에서, 상기 제1 사용자 단말이나 상기 제2 사용자 단말에서 비보안 메시지 전송과 보안 메시지 전송을 선택하는 사용자 인터페이스에서 사용자 입력이나 명령을 획득하는 단계를 더 포함하며, 상기 사용자 입력이나 명령에 따라 상기 메시지를 암호화하는 단계, 상기 암호화된 메시지를 전송하는 단계, 상기 메시지 토큰을 발행하는 단계 및 상기 메시지 토큰을 전송하는 단계를 포함한 일련의 과정이 수행될 수 있다.

[0017] 일실시예에서, 상기 메시지에 포함되는 사진, 동영상, 문서 데이터 또는 이들 조합의 첨부파일은 네트워크를 통해 접근가능한 오프체인 공간에 저장되며, 상기 대체불가능 토큰은 첨부파일에 대한 오프체인 공간의 저장 경로를 기록할 수 있다.

[0018] 일실시예에서, 상기 블록체인 기반 보안 메신저 서비스 방법은, 상기 제1 사용자 단말의 메신저 화면에 첨부파일의 암호화된 첨부파일 데이터를 획득하고, 암호화된 첨부파일 데이터에 대한 블록체인 기반 대체불가능 추가 토큰을 발행하고, 대체불가능 추가 토큰을 제2 사용자 단말에 전송하기 위한 사용자 인터페이스를 제공하는 단계를 더 포함할 수 있다.

[0019] 상기 기술적 과제를 해결하기 위한 본 발명의 일 측면에 따른 블록체인 기반 보안 메신저 서비스 장치는, 송신자의 제1 사용자 단말에 탑재되는 블록체인 기반 보안 메신저 서비스 장치로서, 수신자의 제2 사용자 단말에게 전송할 메시지나 첨부파일의 암호화된 메시지를 중앙 집중식 메신저 서버를 통해 상기 제2 사용자 단말에게 전송하는 메시지 처리부; 및 상기 암호화된 메시지에 대한 입력 메시지 데이터를 획득하고 상기 입력 메시지 데이터에 대한 블록체인 기반 대체불가능 토큰을 발행하며, 상기 대체불가능 토큰을 상기 제2 사용자 단말에게 전송하는 토큰 처리부를 포함한다.

[0020] 일실시예에서, 상기 토큰 처리부는, 암호화된 메시지에 대한 입력 메시지 데이터를 획득하고 입력 메시지 데이터에 대한 블록체인 기반 대체불가능 토큰을 발행하는 토큰 발행 모듈; 대체불가능 토큰을 제2 사용자 단말에게 전송하는 토큰 전송 모듈; 및 대체불가능 토큰의 소유자를 수신자로 변경하는 토큰 수정 모듈을 구비한다.

[0021] 일실시예에서, 상기 토큰 처리부는, 메시지 토큰의 속성을 조회하는 트랜잭션을 생성하고 생성한 트랜잭션을 블록체인으로 전송하여 메시지 토큰의 암호화 대칭키를 조회하는 토큰 조회 모듈을 더 구비한다.

[0022] 일실시예에서, 상기 토큰 처리부는, 토큰 발행 모듈, 토큰 전송 모듈 및 토큰 수정 모듈에 의한 메시지 토큰에 대한 동작 결과가 블록체인에 최종적으로 저장될 때, 블록체인으로부터 이벤트를 받는 이벤트 관리 모듈을 더 구비한다.

[0023] 일실시예에서, 상기 토큰 처리부는, 토큰 검증 모듈을 호출하여 메시지 토큰에 기록된 상대방 메신저 ID를 확인하고, 상대방 메신저 ID에 대응하는 사용자 정보 및 공개키와 상대방의 사용자 정보 및 공개키와의 일치 여부를 비교함으로써, 상대방의 사용자 신원을 인증한다.

[0024] 일실시예에서, 메신저 처리부와 토큰 처리부를 포함하는 보안 메신저는 사용자 단말의 메신저 서비스 화면에 제공되는 사용자 인터페이스에서의 특정 입력 혹은 명령에 따라 비보안 메시지 전송과 보안 메시지 전송을 선택할 수 있다.

발명의 효과

[0025] 전술한 본 발명에 의하면, 사용자가 송신하는 메시지는 암호화하여 전송되고, 해당 메시지의 암호화 키 정보, 송신 정보, 수신자 ID 등 관련 메타 데이터를 블록체인 상에 대체불가능 토큰으로 저장하고 수신자에게 전송함으로써, 메시지 내용에 대한 무결성과 기밀성을 블록체인의 보안 수준으로 보장할 수 있다.

[0026] 또한, 본 발명에 의하면, 사용자는 전송하는 메시지의 중요도에 따라서 블록체인을 활용하지 않는 일반적인 평문 메시지를 전송하거나, 블록체인 기반 보안 메신저 서비스를 활용하여 보안 메시지를 전송할 수 있으므로, 기존의 중앙 집중식 메신저 서비스와 블록체인 기반 보안 메신저 서비스를 함께 사용할 수 있고, 특히 기존의 상용 메신저 서비스의 부가 기능으로 구현할 수 있으므로, 그 활용성을 높은 장점이 있다.

[0027] 또한, 본 발명에 의하면, 블록체인 상의 대체불가능 토큰 생성 및 전송과 토큰 소유자의 변경을 통해 블록체인 상의 토큰 소유자 정보를 활용하여 메시지 송·수신자에 대한 신원 인증을 획득할 수 있고, 또한 토큰 생성 및 전송 트랜잭션 처리 정보를 통해 메시지 송·수신 여부에 대해 부인 방지 증명을 블록체인의 보안 수준으로 제공할 수 있다.

[0028] 또한, 본 발명에 의하면, 대체불가능 토큰의 유효기간을 토큰 속성으로 설정함으로써, 중앙 집중식 상용 메신저 서비스에서 독자적으로 메시지 보관 정책을 실시하더라도, 토큰 유효기간을 통해 해당 메시지 유효성을 사용자

가 직접 최종 판단하도록 할 수 있다.

[0029] 또한, 본 발명에 의하면, 사용자는 기본적으로 상용 메신저 서비스를 활용하여 메시지를 전송하기 때문에, 메시지에 다양한 데이터 예컨대, 사진, 동영상, 문서 등을 첨부할 수 있으며, 해당 첨부파일 데이터에 대한 암호화 처리도 메시지 내용과 유사한 형태로 처리할 수 있으므로, 메시지 데이터뿐 아니라 첨부 데이터에 대한 보안성도 함께 지원할 수 있다.

[0030] 아울러, 본 발명에 의하면, 블록체인 특성을 이용하여 메시지 송·수신자 신원 인증, 메시지 내용 기밀성 및 무결성 보장, 그리고 메시지 송·수신 행위 부인 방지 증명 등을 블록체인의 보안 수준으로 지원하므로 높은 보안성을 요구하는 군용 또는 금융 분야 등의 분야에 적극 활용할 수 있는 장점이 있다.

도면의 간단한 설명

[0031] 도 1 은 본 발명의 일실시예에 따른 블록체인 기반 보안 메신저 서비스 시스템의 전체적인 구성도이다.

도 2는 도 1의 블록체인 기반 보안 메신저 서비스 시스템의 메신저 클라이언트에 대응하는 보안 메신저의 기능을 설명하기 위한 예시도이다.

도 3은 도 2의 보안 메신저에서 발생되는 대체불가능 토큰에 채용할 수 있는 데이터 구조에 대한 예시도이다.

도 4는 도 1의 블록체인 기반 보안 메신저 서비스 시스템에 의한 보안 메신저 서비스의 작동 원리를 설명하기 위한 예시도이다.

도 5는 본 발명의 일실시예에 따른 블록체인 기반 보안 메신저 서비스 방법에 대한 흐름도이다.

도 6 및 도 7은 도 5의 보안 메신저 서비스 방법의 사용자 단말에서 채용할 수 있는 인터페이스를 나타낸 예시도들이다.

발명을 실시하기 위한 구체적인 내용

[0032] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0033] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는 데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 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.

[0034] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0035] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0036] 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 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0037] 본 발명의 바람직한 실시예를 설명하기에 앞서 주요 용어를 살펴보면 다음과 같다.

[0038] 블록체인(blockchain)은 분산화된 거래장부를 네트워크에 참여하는 노드들이 유지하는 시스템을 의미한다. 즉, 블록체인은 트랜잭션(transaction)들의 집합으로 구성된 블록이 이전 블록의 해시(hash)값을 담아 모든 블록을 체인 형식으로 연결하는 데이터 구조로서, 블록체인 네트워크에 참여하는 모든 노드(node)가 상기 데이터 구조를 동일하게 유지하고, 합의 알고리즘(consensus algorithm)을 기반으로 새로운 블록을 생성하여 연결하는 분산 원장 기술(distributed ledger technology)이다. 특정 노드의 블록체인 데이터가 임의로 조작되더라도 블록 간에 이전 블록의 해시값을 가지고 있으므로 데이터 조작을 바로 탐지할 수 있으며, 조작된 데이터는 노드 간에 합의된 것이 아니기 때문에 블록체인에 반영되지 않는다. 이처럼 블록체인은 데이터를 임의로 위변조하는 것이 불가능하여 데이터의 무결성 및 투명성을 보장해준다.

[0039] 블록체인은 비허가형 블록체인(permissionless blockchain)과 허가형 블록체인(permissioned blockchain)으로 구분된다. 비허가형 블록체인은 사용자 및 노드가 아무런 제약 없이 블록체인 네트워크에 참여할 수 있는 블록체인이다. 대표적인 비허가형 블록체인으로는 비트코인(Bitcoin) 및 이더리움(Ethereum)이 있다. 허가형 블록체인은 허가된 사용자 및 노드들만 블록체인 네트워크에 참여할 수 있는, 비즈니스 환경에서 활용하기에 적합한 블록체인이다. 대표적인 허가형 블록체인으로는 하이퍼레저 패브릭(Hyperledger Fabric)이 있다.

[0040] 스마트 컨트랙트(smart contract)란 블록체인을 기반으로 공증, 부동산 계약 등 다양한 형태의 계약을 체결하고 이행하는 계약을 말한다. 스마트 컨트랙트를 통해 비즈니스 로직을 구성하여 탈중앙화 애플리케이션(distributed application, dApp)을 개발 및 운영할 수 있다. 스마트 컨트랙트는 제 3자의 개입 없이 요청을 비즈니스 로직에 따라 자동으로 실행한다는 장점을 갖고 있다. 대표적인 dApp으로 토큰(token)이 있다.

[0041] 토큰은 디지털 자산(digital asset)을 블록체인 상에 표현한 것이다. 블록체인에 디지털 자산을 토큰화하면 디지털 자산의 소유권 증명, 투명성 및 유동성 보장 등의 장점을 확보할 수 있다. 토큰은 대체가능 토큰(fungible token)과 대체불가능 토큰(non-fungible token)으로 구분된다. 대체가능 토큰은 쪼개질 수 있는 디지털 자산을 표현한 토큰이고, 대체불가능 토큰은 쪼개질 수 없는 디지털 자산을 표현한 토큰이다.

[0042] 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0043] 도 1 은 본 발명의 일실시예에 따른 블록체인 기반 보안 메신저 서비스 시스템의 전체적인 구성도이다.

[0044] 도 1을 참조하면, 블록체인 기반 보안 메신저 서비스 시스템은, 메신저 송신자 단말기(100a), 메신저 수신자 단말기(100b), 중앙 집중식 메신저 서버(200) 및 블록체인 기반 보안 메신저 서비스 장치(500)로 구성된다. 여기서, 중앙 집중식 메신저 서버(200)는 외부 메신저 서비스를 통해 메신저 송신기 단말기(100a)와 메신저 수신기 단말기(100b) 간의 메시지 송·수신 기능을 지원한다.

[0045] 메신저 송신자 단말기(100a)와 메신저 수신자 단말기(100b)는 스마트 폰, 퍼스널 컴퓨터(personal computer, PC), 개인휴대통신 단말 등을 포함하며, 송·수신을 위한 메시지 및 다양한 형태의 첨부 데이터 입력을 담당한다. 메시지 및 첨부 데이터 암호화는 단말기 상에서 암호화키를 생성하고 처리될 수 있다.

[0046] 또한 메신저 송신자 단말기(100a)와 메신저 수신자 단말기(100b)는 중앙 집중식 메신저 서버(200)와 연동하는 메신저 클라이언트를 탑재할 수 있고, 이 경우 메신저 클라이언트는 블록체인 기반 보안 메신저 서비스 장치를 구현한 소프트웨어 모듈을 포함하거나, 블록체인 기반 보안 메신저 서비스 장치 혹은 이를 구현한 소프트웨어 모듈과 연동할 수 있다.

[0047] 또한, 메신저 송신자 단말기(100a)는 일반 메시지와 보안 메시지 중 어느 하나를 선택하여 메시지를 전송할 수 있다. 이때, 보안 메신저(300)는 메신저 송신자 단말기(100a)에서 선택한 메시지 형태에 따라서, 일반 메시지 송신을 원하는 경우 종래의 메신저 서비스와 동일하게 메신저 API SDK(320)을 통해 중앙 집중식 메신저 서버(200)로 일반적인 메시지를 전송하고, 보안 메시지를 전송하고자 할 경우에는 보안 메신저(300) 내 블록체인 SDK(310)에서 블록체인 트랜잭션을 블록체인(400)에 전송하여 메시지와 연계된 블록체인 대체불가능 토큰을 생성하고, 동시에 메신저 API SDK(320)를 통해 중앙 집중식 메신저 서버(200)로 해당 메시지를 전송할 수 있다.

[0048] 중앙 집중식 메신저 서버(200)는 인터넷 환경에서 메시지 송·수신 서비스를 지원한다. 현재 상용화 서비스를 제공하고 있는 카카오톡, 라인, 텔레그램 등 메시지 송·수신 서비스 API를 제공하는 메신저 서비스들을 포함할 수 있다. 이 경우, 상용화 메신저 서비스는 본 실시예의 보안 메신저 서비스의 내용과는 독립적인 서비스로 간주할 수 있다.

[0049] 블록체인 기반 보안 메신저 서비스 장치(500)는 보안 메신저(300)와 블록체인(400)으로 구성된다. 보안 메신저(300)는 블록체인과의 연계를 담당하는 블록체인 SDK(software development kit, 310)와 중앙 집중식 메신저

서버(200)와의 연계를 담당하는 메신저 API SDK(320)로 구성된다. 블록체인 기반 보안 메신저 서비스 장치(500)는 본 실시예에 따른 블록체인을 활용한 보안 메신저 서비스를 제공한다.

[0050] 블록체인 기반 보안 메신저 서비스 장치(500)가 중앙 집중식 메신저 서버(200)와 연계하는 일례로서 도 1에서는 REST(Representational State Transfer) 기반으로 API(application programming interface)를 제공하는 웹 서비스를 총칭하는 RESTful 형태의 API로 연계됨을 표현하고 있다.

[0051] 보안 메신저(300)의 메신저 API SDK(320)는 메신저 송신자 단말기(100a)에 의한 메시지 송신을 외부 중앙 집중식 메신저 서버(200)를 통해 처리한다. 그리고, 블록체인 SDK(310)는 블록체인 기반 대체불가능 토큰을 생성하거나 관리한다. 보안 메신저(300)는 메신저 수신자 단말기(100b)에서 메시지 확인을 위해 대체불가능 토큰의 조회를 블록체인 SDK(310)를 통해 지원한다.

[0052] 블록체인(400)은 허가형 혹은 비허가형 블록체인 등 어떤 형태의 블록체인이든 가능하며, 블록체인 기반 보안 메신저 서비스 장치의 블록체인 기반 보안 메신저 서비스와는 독립적으로 구성 가능하다.

[0053] 블록체인(400)은 메시지 내용을 관장하는 기관의 노드가 참여 노드로 구성될 수 있으며, 생성된 메시지 토큰을 블록에 담아 관리하는 역할을 한다. 이때, 메신저 서버(200)가 비즈니스 목적을 위해 활용되는 경우 블록체인 네트워크의 참여자를 제한하기 위해 허가형 블록체인으로 구성 가능하며, 기타 다른 경우에서는 비허가형인 퍼블릭 블록체인으로도 구성 가능하다.

[0054] 도 2는 도 1의 블록체인 기반 보안 메신저 서비스 시스템의 메신저 클라이언트에 대응하는 보안 메신저의 기능을 설명하기 위한 예시도이다.

[0055] 도 2를 참조하면, 본 실시예에 따른 블록체인 기반 보안 메신저 서비스 장치의 보안 메신저(300)는, 블록체인 SDK(310)와 메신저 API SDK(320)를 구비하며, 메시지 당 블록체인 토큰 생성, 전송, 검색 등의 기능을 지원함으로써 메시지를 관리한다.

[0056] 이를 위해 블록체인 SDK(310)는 토큰 발행 모듈(311), 토큰 전송 모듈(312), 토큰 수정 모듈(313), 토큰 조회 모듈(314), 블록체인 상에서 발생하는 이벤트를 전달받는 이벤트 모듈 (315), 토큰 검증 모듈(316)을 정의한다. 그리고 메신저 API SDK(320)는 중앙 집중식 메신저 서버(200)와 통신하는 API 모듈(321)을 정의한다.

[0057] 토큰 발행 모듈(311)은 메시지 토큰을 발행하는 트랜잭션을 생성하고 생성한 트랜잭션을 블록체인(400)으로 전송한다. 보다 구체적으로는, 메신저 송신자 단말기(100a)가 보안 메시지 전송을 요청하면, 보안 메신저(300)는 토큰 발행 모듈(311)을 호출하여 블록체인 트랜잭션을 생성하고, 블록체인(400) 상에 메시지 토큰을 발행한다. 최초 메시지 토큰을 발행하면 이를 발행한 주체가 토큰의 소유자가 된다. 블록체인 토큰의 데이터 구조는 도 3을 참조하는 아래의 상세 설명에서 설명하기로 한다.

[0058] 토큰 전송 모듈(312)은 메시지 토큰을 특정 대상에게 전송하는 트랜잭션을 블록체인(400)으로 전송한다. 보다 구체적으로는, 최초 메시지 토큰의 소유자인 메신저 송신자 단말기(100a)가 메신저 수신자 단말기(100b) 정보를 담아 토큰 전송 모듈(312)을 호출하여 트랜잭션을 생성하고, 메신저 수신자 단말기(100b)에게 메시지 토큰의 소유권을 양도한다. 즉, 토큰 전송 모듈(312) 호출이 완료되면 토큰의 소유자가 상기 메신저 수신자 단말기(100b)로 변경된다.

[0059] 이때, 메시지 토큰에서 토큰 전송 모듈(312)의 호출 권한이 소유자, 피승인자, 운영자에게 존재하지만, 본 실시예에서는 피승인자, 운영자 역할은 사용하지 않기 때문에 토큰 전송 모듈(312) 호출 권한은 소유자에게만 있다. 하지만. 본 발명의 다른 실시예에서는 피승인자 혹은 운영자에게도 호출 권한을 부여할 수 있다.

[0060] 토큰 수정 모듈(313)은 메시지 토큰의 확장 속성의 하위 속성값을 기록하는 트랜잭션을 생성하고 블록체인(400)으로 전송한다. 보다 구체적으로는, 토큰 수정 모듈(313)에 대한 호출 권한은 소유자에게만 있으나, 본 실시예에서는 보안 메신저(500)에 의해 메신저 송신자 단말기(100a)와 메신저 수신자 단말기(100b)가 토큰 수정 모듈(313)을 호출할 수 있도록 구성된다.

[0061] 메신저 송신자 단말기(100a)가 토큰 전송 모듈(313)을 호출하여 보안 메시지를 메신저 수신자 단말기(100b)에게 전송하면, 메신저 수신자 단말기(100b)는 보안 메시지를 수신했다는 것을 토큰 수정 모듈(313)을 호출하여 토큰 조회 상태 속성에 기록할 수 있다. 이를 통해 메신저 송·수신자 단말기(100a, 100b)는 각각 보안 메시지를 송·수신했다는 사실을 추후 증명할 수 있다.

[0062] 토큰 조회 모듈(314)은 메시지 토큰의 속성을 조회하는 트랜잭션을 생성하고 블록체인(400)으로 전송한다. 보안

메시지가 수신되면, 메신저 수신자 단말기(100b)는 토큰 조회 모듈(314)을 호출하여 메신저 송신자 단말기(100a)가 전송한 메시지 토큰의 암호화 대칭키 속성을 조회하고, 조회한 암호화 대칭키로 보안 메시지를 복호화하여 메시지 내용을 열람할 수 있다.

[0063] 보안 메신저(300)가 블록체인(400)으로부터 이벤트를 받으면, 이벤트 관리 모듈(315)은 호출한 주체에게 알림을 보내는 기능을 한다. 토큰 발행 모듈(311), 토큰 전송 모듈(312), 그리고 토큰 수정 모듈(313)이 호출된 후 메시지 토큰에 대한 동작 결과가 블록체인(400)에 최종적으로 저장되면 보안 메신저(300)는 블록체인(400)으로부터 이벤트를 받을 수 있다.

[0064] 일례로, 메신저 송신자 단말기(100a)가 토큰 발행 모듈(311)을 통해 블록체인(400) 상에 메시지 토큰을 발행하면, 이벤트 관리 모듈(315)은 성공적인 메시지 토큰 발행을 메신저 송신자 단말기(100a)에게 알린다.

[0065] 또한, 메신저 송신자 단말기(100a)가 토큰 전송 모듈(312)을 통해 블록체인(400) 상에 존재하는 메시지 토큰의 소유권을 양도하면, 이벤트 관리 모듈(315)은 토큰 전송 모듈(312)을 호출한 주체에게 성공적인 소유권 양도를 알린다.

[0066] 또한, 메신저 송신자 단말기(100a)와 메신저 수신자 단말기(100b)가 토큰 수정 모듈(313)을 통해 메시지 토큰의 확장 속성의 하위 속성값을 수정하게 되면, 이벤트 관리 모듈(315)은 성공적인 수정 내용을 메신저 송·수신자 단말기(100a, 100b)에게 성공적인 수정을 알릴 수 있다.

[0067] 토큰 검증 모듈(316)은 대체불가능 토큰을 발행한 사용자의 신원을 인증하는 기능을 담당한다. 즉, 대체불가능 토큰을 발행한 사용자가 실제 자신에게 메시지를 전송한 사용자인지 판단 기준을 제공하는 기능을 한다.

[0068] 모든 사용자는 사용자 신원을 검증받은 후 블록체인에 등록되므로, 자신의 서명 정보를 기반으로 트랜잭션을 생성할 수 있다. 따라서, 메시지 토큰 수신자는 토큰 검증 모듈(316)을 호출하여 송신자가 발행한 메시지 토큰에 기록된 송신자 메신저 ID를 확인하고, 송신자 메신저 ID와 대응되는 사용자 정보 및 공개키가 송신자의 사용자 정보 및 공개키와의 일치 여부를 비교함으로써, 송신자의 사용자 신원 인증을 수행한다.

[0069] 메신저 API SDK(320)의 API 모듈(321)은 중앙 집중식 메신서 서버(200)와 통신하는 기능을 한다. 보안 메신저(300)를 통해 송신자가 메시지 토큰을 성공적으로 발행하면 암호화된 메시지 내용을 API 모듈(321)을 통해 중앙 집중식 메신저 서버(200)로 전송한다. 최종적으로, 보안 메시지를 전송받은 중앙 집중식 메신저 서버(200)는 이를 수신자에게 전송할 수 있다.

[0070] 본 실시예에 따른 블록체인 기반 보안 메신저 서비스 장치의 보안 메신저는 암호화된 송신 메시지 즉, 입력 메시지 데이터에 대해 블록체인 상에 생성하는 대체불가능 토큰을 생성하며, 이때 생성되는 대체불가능 토큰의 데이터 구조를 예시하면 도 3과 같다.

[0071] 도 3은 도 2의 보안 메신저에서 발생되는 대체불가능 토큰에 채용할 수 있는 데이터 구조에 대한 예시도이다.

[0072] 도 3을 참조하면, 입력 메시지 데이터의 메시지 토큰(30)인 대체불가능 토큰의 데이터 구조는 표준 속성(32)과 확장 속성(34)을 포함한다. 표준 속성(32)은 토큰 식별자(id), 토큰 타입(type), 소유자(owner) 및 피승인자(approvee)를 포함하며, 확장 속성(34)은 온체인 확장 속성(xattr)과 오프체인 확장 속성을 포함하고, 온체인 확장 속성(xattr)의 하위 속성으로 송·수신자 메신저 ID, 암호화 대칭키, 유효기간 및 토큰 조회 상태를 정의하고, 오프체인 확장 하위 속성으로 경로, 해쉬를 정의한다.

[0073] 또한, 메시지 토큰은 전송 메시지 당 새롭게 생성될 수도 있고, 송·수신자 메시지 통신 세션 당 새롭게 생성될 수도 있다. 송신 메시지 하나 하나가 중요한 내용을 담고 있는 경우에는 전송 메시지 당 하나의 메시지 토큰을 생성하며, 메시지 하나하나보다 송·수신자 간에 주고 받은 전체 메시지들의 내용이 중요하다면 송·수신자 메시지 통신 세션 당 하나의 메시지 토큰을 생성함으로써 오버헤드를 줄일 수 있다. 본 실시예에서는 전송 메시지 당 하나의 메시지 토큰을 생성하는 것으로 일례를 서술하고 있으나, 송·수신자 메시지 통신 세션 당 메시지 토큰을 생성하는 방법도 본 실시예의 범위에 포함된다.

[0074] 송·수신자 메신저 ID 속성에는 각각 송신자와 수신자의 중앙 집중식 메신저의 ID 정보를 입력할 수 있다. 암호화 대칭키 속성에는 송신자가 전송하는 메시지 내용을 암호화할 때 사용하는 대칭키를 수신자의 공개키로 암호화한 대칭키를 입력할 수 있다. 유효기간 속성에는 토큰의 유효기간을 입력함으로써 해당 메시지 유효성을 메신저 서버와 관계없이 송신자 또는 수신자가 최종 판단할 수 있다. 마지막으로, 수신자가 토큰을 전송받은 후, 토큰 조회 시 자신의 서명 정보를 토큰 조회 상태 속성에 입력할 수 있다.

[0075] 본 실시예의 메시지 토큰에 의하면, 토큰 타입 메시지(Message)인 메시지 토큰의 표준 속성으로서 토큰 식별자(id), 토큰 타입(type), 소유자(owner) 및 피승인자(approvee)를 설정하고, 온체인 확장 속성(xattr)의 하위 속성으로 중앙 집중식 메신저 서버(200)에 가입한 송·수신자 메신저 ID, 암호화 대칭키, 유효기간, 토큰 조회 상태 속성을 설정하고, 오픈체인 확장 하위 속성으로 경로, 해쉬 속성을 설정함으로써, 메시지 송·수신에 따른 사용자 인증, 메시지 무결성 검증, 송·수신 부인방지 기능을 효과적으로 제공할 수 있다.

[0076] 도 4는 도 1의 블록체인 기반 보안 메신저 서비스 시스템에 의한 보안 메신저 서비스의 작동 원리를 설명하기 위한 예시도이다.

[0077] 본 실시예에 따른 블록체인 기반 보안 메신저 서비스 시스템의 전체적인 작동 원리는 도 4에 도시한 바와 같다.

[0078] 도 4를 참조하면, 메신저 송·수신자 단말기(100a, 100b)와 중앙 집중식 메신저 서버(200)는 모두 블록체인(400)에 등록된 사용자이며, 등록 시 사용자 신원을 인증한다. 또한, 인증된 사용자는 PKI 기반 공개키와 비밀키를 발급받는다.

[0079] 메신저 송·수신자 단말기(100a, 100b)와 중앙 집중식 메신저 서버(200)는 네트워크를 통해 보안 메신저 서비스 장치(500)와 연결될 수 있다. 본 실시예에서 보안 메신저 서비스 장치(500)는 거시 측면에서 보안 메신저(300)와 블록체인(400)을 포함할 수 있고, 미시 측면에서 보안 메신저(300)을 구비하고 블록체인(400)과 연결되거나 연동할 수 있다.

[0080] 보안 메신저(300)는 블록체인에 접근할 수 있는 사용자를 제어하기 위해 사용자들의 정보와 공개키를 저장한다. 이에, 허가된 사용자는 보안 메신저(300)에서 관리하는 자신의 공개키를 이용하여 블록체인 기반 대체불가능 토큰을 통한 사용자 인증을 수행할 수 있다.

[0081] 메신저 송신자 단말기(100a)에서 보안 메시지를 전송하고자 하면, 메시지 내용을 입력한 후 메시지 내용을 암호화하기 위해 대칭키를 생성하고 보안 메신저(300)를 통해 수신자의 공개키를 획득한다.

[0082] 또한, 보안 메시지를 전송하고자 하면, 송신자가 생성한 대칭키로 메시지 내용을 암호화하고, 메시지 내용을 암호화한 대칭키는 보안 메신저(300)의 블록체인 SDK(310)를 통해 수신자의 공개키로 암호화되어 블록체인(400)의 메시지 토큰 속성에 기록된다. 따라서, 블록체인(400)의 메시지 토큰은 제 3자가 접근할 수 있으나, 암호화된 메시지 내용을 복호화하기 위해서는 수신자의 개인키가 필요하다.

[0083] 구체적으로, 메신저 송신자 단말기(100a)에서 보안 메시지를 전송하면 블록체인 기반 보안 메신저 서비스(500)의 동작 과정은 다음과 같다.

[0084] 먼저, 메신저 송신자 단말기(100a)는 토큰 발행 모듈을 호출하여 블록체인(400) 상에 보안 메신저 메시지 기반의 메시지 토큰(토큰 id는 T_0)을 발행한다(S110). 메시지 토큰은 확장 속성의 하위 속성으로 메신저 송신자 단말기(100a)의 ID, 메신저 수신자 단말기(100b)의 ID, 수신자의 공개키로 암호화한 대칭키 정보, 보안 메시지의 유효기간 그리고 토큰 조회 상태 속성을 포함한다.

[0085] 다음, 보안 메신저(300)의 이벤트 관리 모듈은 메신저 송신자 단말기(100a)에 메시지 토큰(T_0)의 발행이 완료되었음을 알리며, 메신저 송신자 단말기(100a)는 토큰 전송 모듈을 통해 메신저 수신자 단말기(100b)에게 메시지 토큰(T_0)를 전송한다(S120).

[0086] 다음, 보안 메신저(300)의 이벤트 관리 모듈로부터 토큰 전송에 대한 성공 알림을 받은 메신저 송신자 단말기(100a)는 메시지 토큰(T_0)과 전송 메시지 내용을 포함한 보안 메시지를 네트워크를 통해 중앙 집중식 메신저 서버(200)로 전송한다(S210).

[0087] 다음, 중앙 집중식 메신저 서버(200)는 수신한 보안 메시지를 메신저 수신자 단말기(100b)에게 전송한다(S220).

[0088] 다음, 메신저 수신자 단말기(100b)는 전송받은 보안 메시지를 검증하기 위해 검증 모듈(316)을 호출한다(S310). 메신저 수신자 단말기(100b)는 송신자의 서명을 기반으로 발행된 메시지 토큰을 검증하여 송신자의 신원을 확인한다. 즉, 제 3자가 송신자로 신원을 위장하여 메시지를 전송하기 위해서는 송신자의 서명을 기반으로 메시지 토큰을 발행해야 하므로 메시지 전송이 불가능하다. 따라서, 수신자는 송신자가 발행한 메시지 토큰에 기록된 송신자 메신저 ID를 확인하고, 송신자 메신저 ID와 관련된 사용자 정보 및 공개키가 수신자가 알고 있는 송신자의 사용자 정보 및 공개키와 일치하는지 여부를 비교함으로써, 송신자 신원 인증을 수행한다.

[0089] 또한, 메시지 내용의 무결성을 보장하기 위해 메시지 송신자는 메시지 내용을 기반으로 대체불가능 토큰을 발행

하여 블록체인 상에 등록한다. 따라서 암호화된 메시지 내용은 메시지 토큰 내 저장된 대칭키를 통해 복호화할 수 있고, 그에 따라 메신저 수신자 단말기(100b)에서 메시지 내용을 확인할 수 있다(S320).

[0090] 또한, 메시지 송·수신 행위 부인 방지 증명에 대해서는, 메신저 송신자 단말기(100a)의 서명 정보를 기반으로 토큰을 발행하므로 송신 행위에 대한 부인 방지 증빙이 가능하다. 추가적으로 발행된 메시지 토큰을 메신저 수신자 단말기(100b)가 수신하고, 메시지 내용을 확인하기 위해 토큰에 기록되어 있는 대칭키 조회시 보안 메신저(300)의 토큰 수정 모듈을 호출하여 수신자가 메시지 토큰을 조회했다는 사실을 메시지 토큰의 토큰 조회 상태 속성에 수신자의 서명 정보를 기록함으로써 수신 행위 부인 방지 증빙을 제공한다.

[0091] 본 실시예에 따르면 블록체인 기반 보안 메신저 서비스 방법 및 장치는 사용자 신원 인증, 메시지 내용 무결성 및 기밀성 보장, 그리고 송신/수신 행위 부인 방지 증명을 블록체인을 통해 해결할 수 있으며, 특히 대체불가능 토큰을 모델링하여 메신저에서 보안이 강화된 메시지를 전송하거나 수신하도록 할 수 있다.

[0092] 한편, 본 실시예에 따른 블록체인 기반 보안 메신저 서비스 장치(500)가 네트워크를 통해 메신저 송·수신자 단말기(100a, 100b) 및 중앙 집중식 메신저 서버(200)와 연결되는 별도의 장치 형태인 것으로 설명하였으나, 본 발명은 그러한 구성으로 한정되지 않고, 응용 어플리케이션 형태로 메신저 송신자 단말기(100a)와 메신저 수신자 단말기(100b)에 각각 설치되는 설치 구조를 가질 수 있다.

[0093] 도 5는 본 발명의 일실시예에 따른 블록체인 기반 보안 메신저 서비스 방법에 대한 흐름도이다.

[0094] 본 실시예에서 특정 메시지의 송신자에 대응하는 제1 사용자 단말(100A)은 제1 보안 메신저(300a)를 구비하고, 상기의 특정 메시지의 수신자에 대응하는 제2 사용자 단말(100B)은 제2 보안 메신저(300b)를 구비한다. 보안 메신저는 중앙 집중식 메신저 서버와 연동하는 메신저 클라이언트에 대응될 수 있다.

[0095] 제1 보안 메신저(300a)와 제2 보안 메신저(300b)는 도 2를 참조하여 앞서 설명한 블록체인 SDK 및 메신저 API SDK를 각각 구비할 수 있다. 블록체인 SDK는 토큰 발행 모듈, 토큰 전송 모듈, 토큰 수정 모듈, 토큰 조회 모듈, 이벤트 관리 모듈 및 토큰 검증 모듈을 구비하고, 메신저 API SDK는 API 모듈을 구비할 수 있다.

[0096] 도 5를 참조하면, 네트워크 상에서 메신저 서비스의 메시지를 통해 대화하는 제1 사용자와 제2 사용자가 있을 때, 제1 사용자 단말(100A)은 제1 보안 메신저(300a)를 통해 수신자 공개키를 이용해 메시지를 암호화하고(S51), 암호화된 메시지를 중앙 집중식 메신저 서버(200)를 통해 제2 사용자 단말(100B)에게 전달한다(S52, S53). 이때 메신저 서버(200)는 복호화를 위한 대칭키가 없으므로 암호화된 메시지의 내용을 볼 수 없다.

[0097] 다음, 제1 사용자 단말(100A)에서 제2 사용자 단말(100B)로 암호화된 메시지 즉, 보안 메시지가 전송됨에 따라, 제1 보안 메신저(300a)는 입력 메시지 데이터를 획득한다(S54). 입력 메시지 데이터는 앞서 제1 사용자 단말(100A)이 제2 사용자 단말(100B)에게 보낸 암호화된 메시지 혹은 이와 관련된 고유 식별자를 포함할 수 있다.

[0098] 다음, 제1 보안 메신저(300a)는 입력 메시지 데이터 기반의 메시지 토큰을 블록체인 상에 발행한다. 예컨대, 제1 보안 메신저(300a)는 입력 메시지 데이터 기반의 메시지 토큰을 발행하기 위한 메시지 토큰 발행 요청 신호를 블록체인(400)에 전달하고(S55) 메시지 토큰 발행 요청 신호에 응하여 메시지 토큰을 발행한 블록체인(400)으로부터 메시지 토큰을 전달받을 수 있다(S56, S57).

[0099] 다음, 제1 보안 메신저(300a)는 메시지 토큰의 소유자를 제2 사용자 단말(100B)로 변경한다(S58). 그리고, 소유자가 변경된 메시지 토큰을 제2 사용자 단말(100B)에게 전송한다(S59).

[0100] 한편, 앞서 암호화된 메시지를 수신한 제2 사용자 단말(100B)의 제2 보안 메신저(300b)는 메시지 토큰의 수신에 응하여 메시지 토큰을 디코딩하고(S61), 디코딩을 통해 얻은 토큰 아이디로 블록체인(400)에 토큰을 조회하고(S620) 송신자의 신원을 검증받을 수 있다(S63).

[0101] 또 한편으로, 메시지 토큰의 수신 이전이나 이후에 상관없이 제2 사용자 단말(100B)은 암호화된 메시지의 수신시, 자신이 소유한 대칭키로 메시지를 복호화하여 메시지 내용을 확인할 수 있다. 이때, 대칭키는 암호화된 메시지의 암호화에 사용된 공개키와 쌍을 이루는 키를 지칭한다.

[0102] 이와 같이, 본 실시예의 구성에 의하면, 사용자 단말의 프로세서에 탑재되는 응용 어플리케이션의 형태인 보안 메신저를 통해 상용 메신저 서비스에서 사용자들의 메시지를 효과적으로 보안하여 비밀 혹은 비공개 대화가 가능하도록 할 수 있다.

[0103] 한편, 전술한 실시예의 보안 메신저 서비스 방법이나 장치에 채용할 수 있는 블록체인(400)은 대체불가능 토큰을 지원하는 체인코드(chaincode) 또는 허가형 블록체인 시스템을 포함할 수 있고, 또한 블록체인(400)은 스마

트 컨트랙트(smart contract)를 이용하여 블록체인 상에 유일성을 갖는 객체에 대한 대체불가능 토큰(non-fungible token)을 생성하는 피어 서버를 포함할 수 있다. 이 경우, 탈중앙화 애플리케이션(decentralized application, dApp)를 통해 특정 객체에 대한 대체불가능 토큰의 발행이 요청되면, 피어 서버는 토큰관리부를 통해 토큰 발행함수를 호출하여 토큰 식별자, 토큰타입, 및 소유자를 포함하는 기본속성과 토큰타입 별로 설정되는 확장속성으로 구성된 데이터 구조를 갖는 대체불가능 토큰을 발행하고, 발행된 대체불가능 토큰의 현재 상태(state)를 데이터베이스에 기록할 수 있다.

[0104] 여기서 대체불가능 토큰은 메시지 토큰에 대응될 수 있다. 대체불가능 토큰이 이더리움(Ethereum) 등의 공개형 블록체인인 경우, 대체불가능 토큰은 표준(standard) 데이터 구조와 확장(extensible) 데이터 구조를 구비하고, ERC-721, 디폴트(default) 등의 표준 인터페이스와 확장 인터페이스를 구비할 수 있다. 그리고 대체불가능 토큰을 위한 보안 메신저 서비스 장치의 프레임워크에서는 dApp과의 통신을 위해 표준 프로토콜과 확장 프로토콜을 구비할 수 있다. 여기서 표준 프로토콜은 ERC-721 프로토콜과 디폴트 프로토콜로 구성될 수 있다. ERC-721 프로토콜은 패브릭 환경(fabric environment)에서 이더리움 ERC-721 토큰 표준 인터페이스를 제공하기 위해 정의되고, 디폴트 프로토콜은 표준 데이터 구조에 정의된 속성들을 위한 함수들을 정의한다. 그리고 확장 프로토콜은 확장 데이터 구조를 관리하는 xattr과 uri를 위한 getter와 setter 함수들을 정의한다.

[0105] 이때, 프로토콜에 정의된 함수는 데이터 구조에서 속성에 직접 접근하지 못하고 속성 관리 함수를 통해 접근하도록 구현될 수 있다. 예를 들어, 온체인 확장 데이터 구조를 IType 인터페이스와 Adapter 디자인 패턴으로 구현할 수 있다. IType 인터페이스에는 xattr 하위 속성을 위한 속성 관리 함수들이 정의되어 있다.타입1을 추가하는 경우, 타입1 클래스에 xattr 하위 속성을 정의하고, IType 인터페이스를 상속하여 속성 관리 함수들을 구현할 수 있다. 그리고 Adapter 디자인 패턴을 통해 토큰 타입에 따라 다른 xattr 하위 속성을 지정할 수 있도록 XAttrAdapter 클래스에 타입1을 등록할 수 있다.

[0106] 또한, 전술한 보안 메신저 서비스 방법에 채용할 수 있는 제1 보안 메신저(300a) 혹은 제2 보안 메신저(300b)는 카카오톡, 라인, 텔레그램 등의 기존의 상용 메신저 서비스에 보안 기능이 추가된 형태로 구현될 수 있으나, 이에 한정되지 않고, 별도의 메신저 기능 확장 응용 애플리케이션으로서 기존의 상용 메신저 서비스에 결합되는 형태를 구비하거나, 별도로 본 실시예의 보안 기능을 갖춘 메신저 응용 애플리케이션의 형태로 구현될 수 있다.

[0107] 도 6 및 도 7은 도 5의 보안 메신저 서비스 방법을 구현하는 사용자 단말에서 채용할 수 있는 인터페이스를 나타낸 예시도들이다.

[0108] 도 6을 참조하면, 보안 메신저가 탑재된 사용자 단말(100A)은 메신저 화면(110)에 선택된 단일 메시지나 그룹 메시지의 암호화, 암호화된 메시지의 전송, 메시지 토큰의 발행, 메시지 토큰 전송 등의 일련의 보안 메신저 동작 실행을 명령하는 사용자 인터페이스를 구비할 수 있다. 이러한 사용자 인터페이스는 비보안 메시지 전송과 보안 메시지 전송을 선택하는 메시지 전송 사용자 인터페이스를 포함한다. 본 실시예에서 메시지 전송 사용자 인터페이스는 메신저 화면(110)의 하단에 '보안'으로 표시된 버튼(120) 형태를 구비하나, 이에 한정되지는 않고 이미지, 음성, 진동 등 다양한 사용자 입력 형태가 단일 혹은 조합으로 사용될 수 있다.

[0109] 아울러, 도 7에 도시한 바와 같이, 본 실시예에 따른 보안 메신저 서비스 방법이나 장치에 채용할 수 있는 사용자 단말(100A)은 메신저 서비스 중에 전송되는 텍스트 파일, 문서 파일, 이미지 파일, 영상 파일, 음성 파일 등을 포함하는 첨부파일에 대하여도 도 5 등을 참조하여 설명한 방법과 유사하게 첨부파일을 암호화하여 수신자측의 사용자 단말에 전송하고, 암호화된 첨부파일에 대한 입력 첨부파일 데이터를 획득하고, 입력 첨부파일 데이터에 대한 블록체인 기반 대체불가능 추가 토큰을 발행하고, 대체불가능 추가 토큰을 수신자측의 사용자 단말에 전송하는 것 등의 일련의 보안 메신저 동작의 실행을 명령하는 사용자 인터페이스를 구비할 수 있다. 이러한 사용자 인터페이스는 도 7의 메신저 화면(110)의 상단에 '첨부보안'으로 표시된 버튼(130) 형태를 구비하나, 이에 한정되지는 않는다.

[0110] 또한, 도면에 도시하지는 않았지만, 보안 메신저를 탑재한 사용자 단말이 암호화된 메시지를 수신하거나 메시지 토큰을 수신하는 경우에, 메신저 화면에는 '보안해제', '디코딩' 등의 버튼으로 표시되는 암호화 메시지의 복호화용 사용자 인터페이스나 메시지 토큰의 디코딩용 사용자 인터페이스를 구비할 수 있다.

[0111] 한편, 전술한 실시예에 따른 보안 메신저 서비스 방법의 동작은 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 프로그램 또는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의해 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산 방식으로 컴퓨터로 읽을 수 있는 프로그램 또는 코

드가 저장되고 실행될 수 있는 저장소나 데이터베이스를 포함할 수 있다.

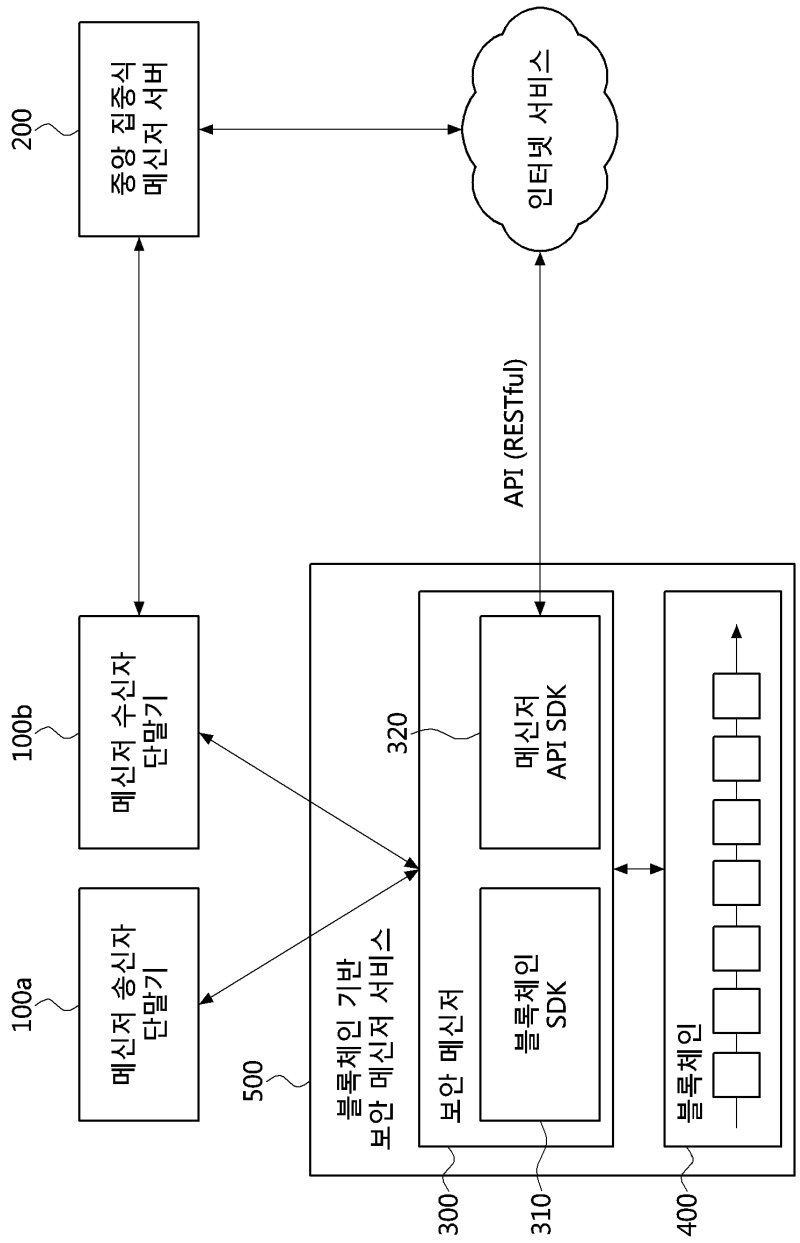
[0112] 또한, 컴퓨터가 읽을 수 있는 기록매체는 롬(rom), 램(ram), 플래시 메모리(flash memory) 등과 같이 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치를 포함할 수 있다. 프로그램 명령은 컴파일러(compiler)에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터(interpreter) 등을 사용해서 컴퓨터에 의해 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

[0113] 또한, 본 실시예에 따른 보안 메신저 서비스 방법의 일련의 절차 중 적어도일부는 예를 들어, 마이크로프로세서, 프로그램 가능한 컴퓨터 또는 전자 회로와 같은 하드웨어 장치에 의해 혹은 하드웨어 장치를 이용하여 구현될 수 있다. 또한, 필드 프로그머블 게이트 어레이 등의 프로그램 가능한 로직 장치가 여기서 설명된 방법들의 기능 일부 또는 전부를 수행하기 위해 사용될 수 있다. 실시예들에서, 필드 프로그머블 게이트 어레이는 여기서 설명된 방법들 중 하나를 수행하기 위한 마이크로프로세서와 함께 작동할 수 있다. 일반적으로, 방법들은 어떤 하드웨어 장치에 의해 수행되는 것이 바람직하다.

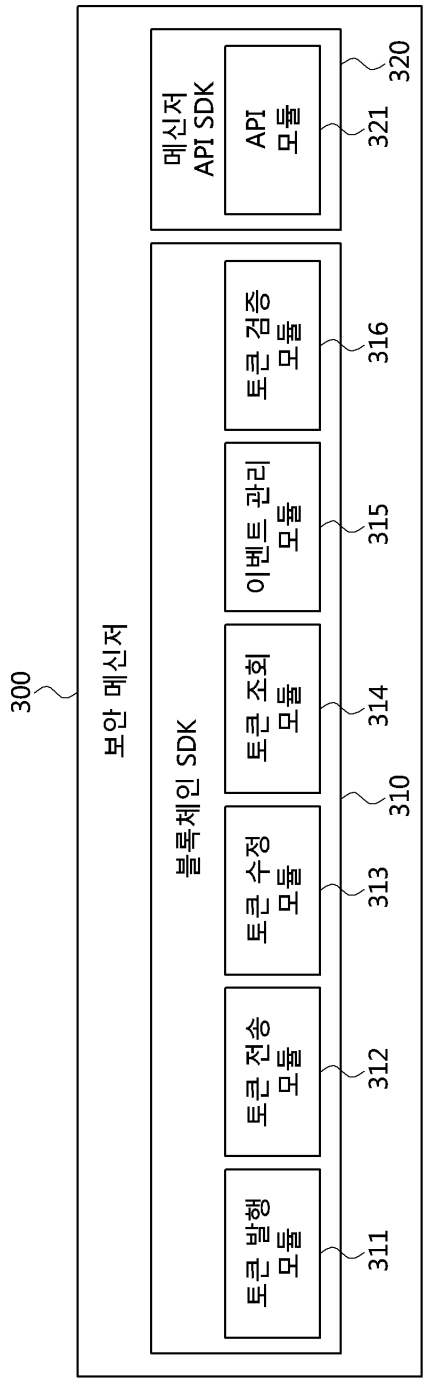
[0114] 이상 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

도면

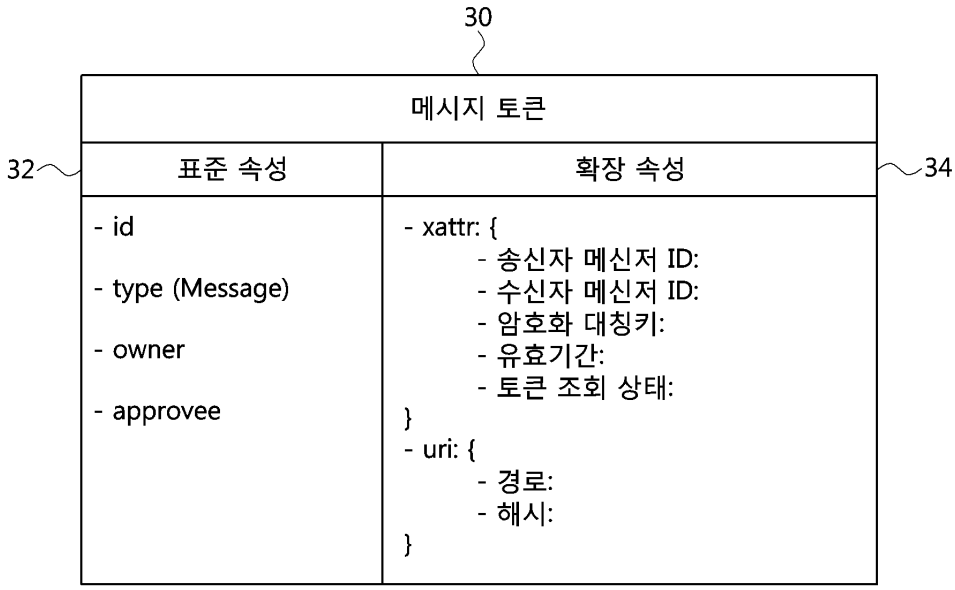
도면1


200
중앙 집중식
메신저 서버
인터넷 서비스
API (RESTful)
100b
메신저 수신자
단말기
100a
메신저 송신자
단말기
500
블록체인 기반
보안 메신저 서비스
보안 메신저
320
메신저
API SDK
블록체인
SDK
블록체인
300
310
400

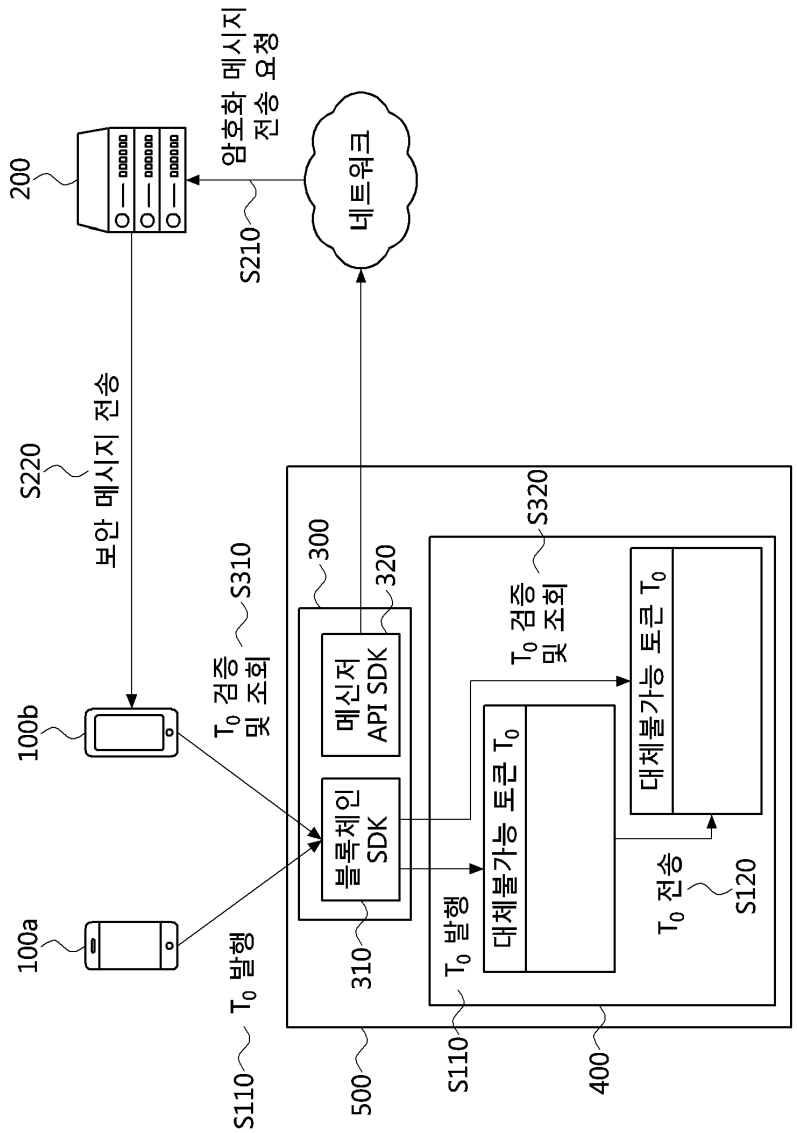
도면2


300
보안 메신저
블록체인 SDK
토큰 발행 모듈
311
토큰 전송 모듈
312
토큰 수정 모듈
313
토큰 조회 모듈
314
이벤트 관리 모듈
315
토큰 검증 모듈
316
310
메신저 API SDK
API 모듈
321
320

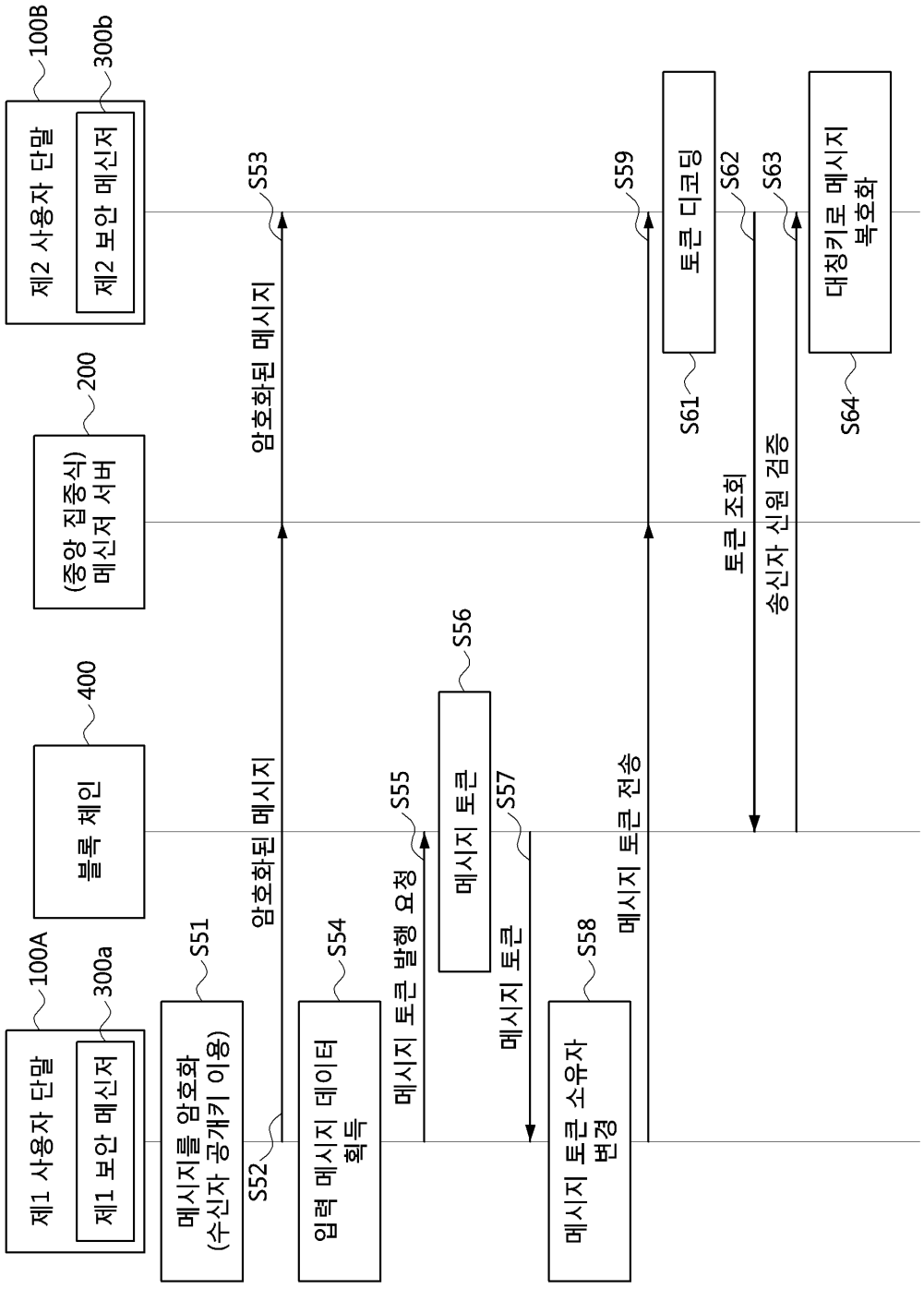
도면3


30
메시지 토큰
32
표준 속성
확장 속성
34
- id
- type (Message)
- owner
- approvee
- xattr: {
- 송신자 메신저 ID:
- 수신자 메신저 ID:
- 암호화 대칭키:
- 유효기간:
- 토큰 조회 상태:
}
- uri: {
- 경로:
- 해시:
}

도면4


200
암호화 메시지
전송 요청
S210
네트워크
S220
보안 메시지 전송
100b
100a
T_0 검증
및 조회
S310
T_0 발행
S110
300
320
메신저
API SDK
블록체인
SDK
310
500
S110
T_0 발행
대체불가능 토큰 T_0
S320
T_0 검증
및 조회
대체불가능 토큰 T_0
T_0 전송
S120
400

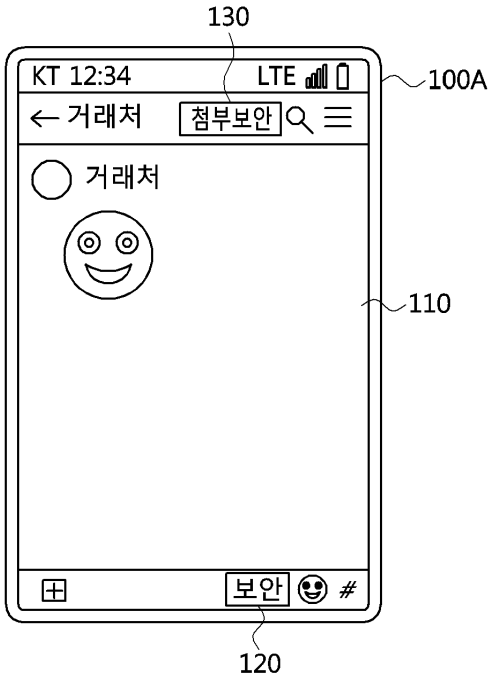
도면5


제1 사용자 단말
100A
제1 보안 메신저
300a
블록 체인
400
(중앙 집중식)
메신저 서버
200
제2 사용자 단말
100B
제2 보안 메신저
300b
메시지를 암호화
(수신자 공개키 이용)
S51
암호화된 메시지
S52
암호화된 메시지
S53
입력 메시지 데이터
획득
S54
메시지 토큰 발행 요청
S55
메시지 토큰
S56
메시지 토큰
S57
메시지 토큰 소유자
변경
S58
메시지 토큰 전송
S59
토큰 디코딩
S61
토큰 조회
S62
송신자 신원 검증
S63
대칭키로 메시지
복호화
S64

도면6


KT 12:34
LTE
100A
← 거래처
거래처
110
보안
120

도면7


130
KT 12:34
LTE
100A
← 거래처
첨부보안
거래처
110
보안
120