(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2024년01월03일
(11) 등록번호 10-2620268
(24) 등록일자 2023년12월27일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) *H04L 51/00* (2022.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 63/1483 (2013.01)
H04L 51/23 (2022.05)
(21) 출원번호 10-2021-0123372
(22) 출원일자 2021년09월15일
심사청구일자 2021년09월15일
(65) 공개번호 10-2022-0066823
(43) 공개일자 2022년05월24일
(30) 우선권주장
1020200153171 2020년11월16일 대한민국(KR)
(56) 선행기술조사문헌
KR102003272 B1*
KR1020180000220 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
포항공과대학교 산학협력단
경상북도 포항시 남구 청암로 77 (지곡동)
(72) 발명자
박찬익
경상북도 포항시 남구 지곡로 155, 6동 1105호
노용두
대전광역시 유성구 봉산로 39, 203동 907호
(뒷면에 계속)
(74) 대리인
특허법인이상

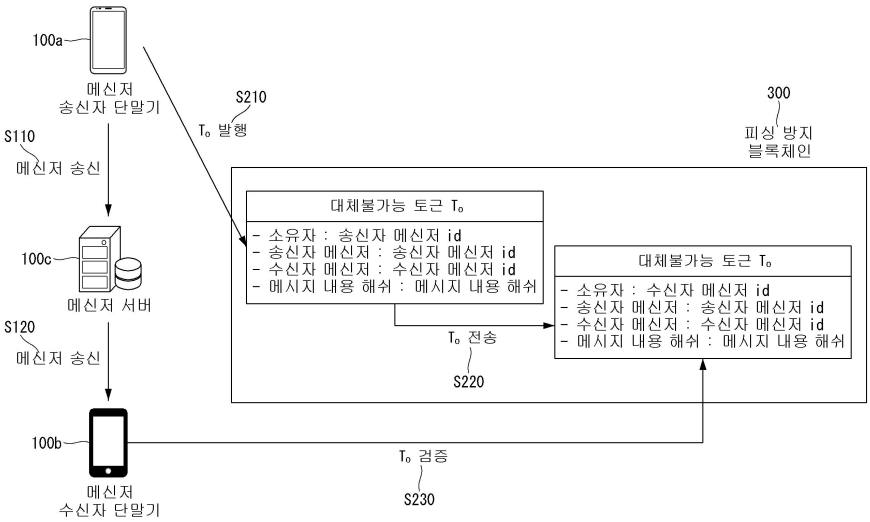
전체 청구항 수 : 총 26 항 심사관 : 문형섭

(54) 발명의 명칭 **블록체인 기반 피싱 방지 시스템, 장치 및 방법**

(57) 요 약

본 발명의 블록체인 기반 피싱 방지 시스템은 메시지 관련 정보를 트랜잭션으로 생성하는 메시지 송신자와, 메시지 송신자가 송부한 송신 메시지를 수신하는 메시지 수신자와, 송신 메시지 및 수신 메시지를 중계하는 메시지 서버, 및 이메일, 문자 메시지 및 메신저 서비스 사용자의 신원 정보를 블록체인을 통해 관리하고, 메시지를 송신하여 송신 메시지 관련 정보를 블록체인에 기록하고, 블록체인에 기록된 송신 메시지 관련 정보를 이용하여 송신자 신원 정보를 검증하여 지인 사칭에 의한 피싱을 방지하는 블록체인 기반 피싱 방지 장치를 포함한다.

대 표 도



(52) CPC특허분류
H04L 63/12 (2013.01)
H04L 9/3236 (2013.01)
H04L 9/50 (2022.05)

(72) 발명자
홍상원
서울특별시 노원구 석계로 49, 111동 405호

황제영
경상북도 포항시 남구 효자로77번길 5, 202호

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
공지예외적용 : 있음

명 세 서

청구범위

청구항 1

메시지 관련 정보를 트랜잭션으로 생성하는 메시지 송신자;

메시지 송신자가 송부한 송신 메시지를 수신하는 메시지 수신자;

송신 메시지 및 수신 메시지를 중계하는 메시지 서버; 및

이메일, 문자 메시지 및 메신저 서비스 사용자의 신원 정보를 블록체인을 통해 관리하고, 메시지를 송신하여 송신 메시지 관련 정보를 블록체인에 기록하고, 블록체인에 기록된 송신 메시지 관련 정보를 이용하여 송신자 신원 정보를 검증하여 지인 사칭에 의한 피싱을 방지하는 블록체인 기반 피싱 방지 장치;를 포함하고,

상기 메시지 수신자가 대체불가능 토큰에 기록된 메시지 송신자 아이디(id) 속성을 이용하여 상기 메시지 송신자의 신원을 검증하고, 메시지 내용 해쉬 정보를 이용하여 송신 메시지 내용의 무결성을 검증하는,

블록체인 기반 피싱 방지 시스템.

청구항 2

청구항 1에 있어서, 상기 시스템은,

메시지를 송신한 상대방의 신원을 블록체인을 통해 인증하여 지인 사칭에 의한 피싱을 방지하기 위하여 상대방의 메시지 정보와 대응하는 블록체인 상의 대체불가능 토큰(Non-fungible token, NFT) 검증 여부를 통해 사용자 인증을 수행하는,

블록체인 기반 피싱 방지 시스템.

청구항 3

청구항 2에 있어서, 상기 대체불가능 토큰(Non-fungible token)은,

대체불가능 토큰의 데이터 구조를 기반으로 표준 속성과 온체인(on-chain) 및 오프체인(off-chain) 확장 속성으로 구성되는,

블록체인 기반 피싱 방지 시스템.

청구항 4

청구항 2에 있어서,

상기 대체불가능 토큰(Non-fungible token)의 표준 속성은 토큰 아이디(ID) 속성, 토큰 타입 속성, 소유자 속성, 피승인자 속성을 포함하여 구성되는, 블록체인 기반 피싱 방지 시스템.

청구항 5

청구항 2에 있어서,

상기 대체불가능 토큰(Non-fungible token)의 온체인 확장 속성은 표준 속성의 토큰 타입에 따라 하위 속성이 다르게 정의되고, 피싱 방지 토큰 타입으로 송신자 아이디(id), 수신자 아이디(id), 및 메시지 내용 해쉬 속성으로 구성되는, 블록체인 기반 피싱 방지 시스템.

청구항 6

청구항 2에 있어서,

상기 대체불가능 토큰(Non-fungible token)의 오프체인 확장 속성은 대체불가능 토큰을 표현할 때 오프체인 데이터가 필요한 경우, 오프체인 저장소를 연결하기 위해 오프체인 저장소 경로를 저장하는 경로 속성과 오프체인 저장소의 데이터들로 구성된 머클 트리(merkle tree)의 머클 루트(merkle root)를 저장하는 해시 속성이 하위

속성으로 구성되는, 블록체인 기반 피싱 방지 시스템.

청구항 7

청구항 2에 있어서,

상기 대체불가능 토큰(Non-fungible token)의 온체인 확장 속성은 메시지를 송신하는 메시지 송신자 아이디(id) 정보와 해당 메시지를 수신하는 수신자 아이디(id) 정보를 각각 저장하는 송신자 아이디(id) 속성 및 수신자 아이디(id) 속성을 온체인 확장 속성의 하위 속성으로 정의하는, 블록체인 기반 피싱 방지 시스템.

청구항 8

청구항 2에 있어서, 상기 대체불가능 토큰(Non-fungible token)은,

송신 메시지 내용의 무결성을 증명하기 위한 메시지 내용 해쉬 속성을 온체인 확장 속성의 하위 속성으로 정의되는,

블록체인 기반 피싱 방지 시스템.

청구항 9

청구항 2에 있어서, 상기 대체불가능 토큰의 데이터 구조는,

탈중앙화 애플리케이션(dApp)을 통해 특정 객체에 대한 대체불가능 토큰의 발행이 요청되면, 토큰 발행 함수를 호출하여 토큰 식별자, 토큰타입, 및 소유자를 포함하는 표준 속성과 토큰타입 별로 설정되는 확장 속성으로 구성된 데이터 구조인,

블록체인 기반 피싱 방지 시스템.

청구항 10

블록체인 기반 피싱 방지 장치에 있어서,

허가형 블록체인으로 구성되는 피싱 방지 블록체인; 및

메시지 송신자 및 메시지 수신자의 트랜잭션 전송을 중계하는 피싱 방지 소프트웨어 개발 키트(Software Development Kit, SDK); 를 포함하고,

메시지 관련 정보를 트랜잭션으로 생성하는 메시지 송신자와, 메시지 송신자가 송부한 송신 메시지를 수신하는 메시지 수신자 및 송신 메시지 및 수신 메시지를 중계하는 메시지 서버와 연동되어, 사용자의 신원 정보를 블록체인을 통해 관리하고, 메시지를 송신하여 송신 메시지 관련 정보를 블록체인에 기록하고, 블록체인에 기록된 송신 메시지 관련 정보를 이용하여 송신자 신원 정보를 검증하여 지인 사칭에 의한 피싱을 방지하며,

상기 메시지 수신자가 대체불가능 토큰에 기록된 메시지 송신자 아이디(id) 속성을 이용하여 상기 메시지 송신자의 신원을 검증하고, 메시지 내용 해쉬 정보를 이용하여 송신 메시지 내용의 무결성을 검증하는, 블록체인 기반 피싱 방지 장치.

청구항 11

청구항 10에 있어서, 피싱 방지 SDK는,

피싱 방지 블록체인 상에 메시지 내용을 기반으로 하는 피싱 방지 토큰을 발행하는 트랜잭션을 생성하는 발행부;

피싱 방지 블록체인 상에서 피싱 방지 토큰을 다른 사용자에게 전송하는 기능을 담당하는 전송부;

대체불가능 토큰을 발행한 사용자의 신원을 인증하는 기능을 담당하는 토큰 속성 검증부; 및

피싱 방지 SDK가 피싱 방지 블록체인으로부터 이벤트를 받으면, 호출한 주체에게 알림을 보내는 기능을 하는 이벤트부; 를 포함하는,

블록체인 기반 피싱 방지 장치.

청구항 12

청구항 11에 있어서, 발행부는,

메신저 송신자 단말기가 발행부를 통해 블록체인 트랜잭션을 생성하여 피싱 방지 블록체인 상에 피싱 방지 토큰을 발행하는,

블록체인 기반 피싱 방지 장치.

청구항 13

청구항 11에 있어서, 전송부는,

피싱 방지 토큰의 소유자가 전송부를 통해 피싱 방지 토큰의 소유권을 다른 사용자에게 양도하는 블록체인 트랜잭션을 생성하는,

블록체인 기반 피싱 방지 장치.

청구항 14

청구항 11에 있어서, 토큰 속성 검증부는,

대체불가능 토큰을 발행한 사용자가 실제 자신이 알고 있는 지인과 동일한 사용자인지 혹은 지인을 사칭한 피싱 공격자인지에 대한 판단 기준을 제공하는 기능을 하는,

블록체인 기반 피싱 방지 장치.

청구항 15

청구항 11에 있어서, 이벤트부는,

발행부, 전송부가 호출된 후 피싱 방지 토큰에 대한 동작 결과가 피싱 방지 블록체인에 최종적으로 커밋(commit)되면 피싱 방지 블록체인 이벤트를 수신하여 전달하는,

블록체인 기반 피싱 방지 장치.

청구항 16

청구항 11에 있어서, 이벤트부는,

메신저 송신자 단말기가 발행부를 통해 피싱 방지 토큰 발행을 요청한 후, 피싱 방지 블록체인 상에 토큰 생성이 완료되는 경우, 토큰 발행 완료 사실을 메신저 송신자 단말기에게 이벤트로 알리고,

메신저 송신자 단말기가 전송부를 통해 피싱 방지 토큰을 다른 사용자에게 전송을 요청한 후, 피싱 방지 블록체인 상에서 전송이 완료되는 경우, 성공적인 소유권 양도 완료 사실을 메신저 송신자 단말기에게 이벤트로 알리는,

블록체인 기반 피싱 방지 장치.

청구항 17

메시지 송신자가 송신하려는 메시지와 관련된 메시지 송신자 아이디(id) 및 수신자 아이디(id)와 메시지 내용 해쉬 정보를 포함하여 대체불가능 토큰을 발행하는 단계;

메시지 송신자가 발행된 대체불가능 토큰을 메시지 수신자에게 전송하는 단계;

메시지 송신자가 발행한 대체불가능 토큰 관련 정보와 송신 메시지 내용을 메시지 서버에게 전송하는 단계;

메시지 서버가 메시지 수신자에게 대체불가능 토큰 관련 정보와 송신 메시지 내용을 송신하는 단계;

메시지 수신자가 대체불가능 토큰에 기록된 메시지 송신자 아이디(id) 속성을 이용하여 메시지 송신자의 신원을 검증하고, 메시지 내용 해쉬 정보를 이용하여 송신 메시지 내용의 무결성을 검증하는 단계; 를 포함하는,

블록체인 기반 피싱 방지 방법.

청구항 18

청구항 17에 있어서, 상기 방법은,

메신저 메시지를 송신한 상대방의 신원 인증을 수행하기 위하여 블록체인을 활용하고,

사용자의 신원 인증을 제공하기 위한 정보 등을 블록체인 네트워크상에 유지 관리하기 위하여 송신자의 메시지 내용과 대응되는 대체불가능 토큰을 블록체인에서 유지 관리하는,

블록체인 기반 피싱 방지 방법.

청구항 19

청구항 17에 있어서, 상기 방법은,

송신자는 자신의 서명 정보를 기반으로 대체불가능 토큰을 발행하며,

대체불가능 토큰은 송·수신 대상자 및 메시지 내용 무결성 검증을 위한 메시지 내용 해쉬 정보를 포함하여 송신자 신원 및 메시지 내용 무결성 검증을 구현하는,

블록체인 기반 피싱 방지 방법.

청구항 20

청구항 17에 있어서, 상기 방법은,

송신자는 대체불가능 토큰을 발행 및 수신자에게 전송하여 자신이 피싱 공격자가 아니라는 증빙을 제공하는,

블록체인 기반 피싱 방지 방법.

청구항 21

청구항 17에 있어서, 상기 방법은,

메시지 송신자가 송신하려는 메시지 내용을 기반으로 대체불가능 토큰을 블록체인 상에 발행한 후, 토큰을 메시지 수신자에게 전달하는,

블록체인 기반 피싱 방지 방법.

청구항 22

청구항 17에 있어서, 상기 방법은,

대체불가능 토큰 속성으로는 토큰 고유 식별 아이디(id) 속성, 토큰을 발행한 소유자 속성, 메시지 송신자 및 수신자 아이디(id) 속성, 메시지 내용 무결성 검증을 위한 메시지 내용 해쉬 속성으로 정의하는,

블록체인 기반 피싱 방지 방법.

청구항 23

청구항 17에 있어서, 상기 방법은,

사용자가 메신저 메시지를 송신할 때 과정은,

사용자가 PKI(Public Key Infrastructure) 기반한 공개키, 비밀키 쌍을 가지고 있으며 블록체인 트랜잭션을 생성할 수 있는,

블록체인 기반 피싱 방지 방법.

청구항 24

청구항 17에 있어서, 상기 방법은,

메신저 서비스, 이메일, 문자 메시지 기능이 포함된 사용자 인증을 거치지 않는 서비스에 적용 가능한,

블록체인 기반 피싱 방지 방법.

청구항 25

청구항 17 내지 청구항 24 중 어느 한 항의 블록체인 기반 피싱 방지 방법을 구현하기 위한 컴퓨터 판독 가능한 기록매체에 저장된 컴퓨터 프로그램.

청구항 26

청구항 17 내지 청구항 24 중 어느 한 항의 블록체인 기반 피싱 방지 방법의 프로그램을 구현하기 위한 컴퓨터 판독 가능한 기록매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 메시지를 송신한 상대방의 신원을 블록체인을 통해 인증함으로써, 지인 사칭에 의한 피싱 문제를 해결하기 위한 것으로, 상대방의 메시지 정보와 대응하는 블록체인 상의 대체불가능 토큰(Non-fungible token, NFT) 검증 여부를 통해 사용자 인증을 수행하는 블록체인 기반 피싱 방지 시스템, 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 피싱(Phishing)이란 개인정보(Private data)와 낚는다(Fishing)의 합성어로, 전화, 메신저 및 문자 메시지 등을 토대로 이용자의 개인정보를 불법적으로 획득하여 금전적 피해를 입히는 사기수법이다. 피싱의 대표적인 유형은 보이스 피싱, 문자 피싱, 메신저 피싱 등이 있다. 피싱은 오래전부터 대중에게 잘 알려진 사기 수법이지만, 사용자의 심리를 교묘하게 이용하는 범죄 행위로써 현재 시점에도 끊임없이 발생하고 있다. 본 발명에서는 피싱 공격에 대한 대응 방법을 서술한다.

[0003] 최근에는 인터넷 상에 노출된 개인 신원 정보를 이용하는 지인 사칭에 의한 피싱 공격이 증가하고 있다. 보편적으로 사용자는 온라인 상 이메일, 문자 메시지, 혹은 메신저 서비스 등을 이용하거나, 페이스북, 인스타그램 등 다양한 SNS 서비스들을 활용하여, 친구, 가족 및 여러 지인들과 비형식적인 대화를 한다.

[0004] 그러나 이처럼 온라인 상 정보 전달을 위한 이메일, 문자 메시지 및 메신저 서비스들은 사용자 간 비대면으로 정보 교환이 이루어지며, 또한 메시지 송·수신 시 사용자 인증 절차를 전혀 수행하지 않으므로 사용자 신원을 사칭하는 범죄 사고에 취약하다는 문제점을 내포하고 있다. 특히, 실시간 대화형 특징을 갖는 문자 메시지 혹은 메신저 서비스는 공식적인 업무 처리 용도보다 가까운 친구, 가족 및 지인과 함께 일상적인 대화를 나누는 방식으로 주로 사용되므로, 지인 사칭에 의한 피싱 공격에 항상 노출되어 있다. 피싱 공격자는 이러한 문제점을 교묘하게 이용하여 피싱 대상자의 가까운 친구, 가족 및 지인을 사칭하여 대상자에게 개인정보, 금전 등 민감한 정보를 요구한다. 특히, 메신저 서비스의 경우 피싱 공격자는 대상자의 지인과 완전히 동일한 프로필, 배경 사진 및 상태 메시지 등을 표시함으로써 대상자의 경계심을 낮추어 피싱 가능성을 최대한 높이는 등 광범위한 공격을 시도한다.

[0005] 이처럼 온라인 상 정보 교환을 위해 주로 사용하는 수단들은 상대방 신원에 대한 인증 부재 및 사용자의 심리를 이용한 광범위한 사기 수법 때문에, 지인 사칭에 의한 피싱에 항상 노출되어 있다. 또한, 그에 따른 범죄 사고가 지속적으로 발생하고 있음에도 불구하고, 현재로서는 해당 범죄 행위를 근절하기 위한 물리적인 장치 및 방법이 미흡한 실정이다.

[0006] 이메일, 문자 메시지 및 메신저 등은 현재 대부분의 사용자들에게 온라인 상 정보 전달을 위한 필수적인 서비스이다. 그러나 상기 서비스들은 사용자 신원 인증을 수행하지 않기 때문에, 개인정보 및 금전 요구를 하는 상대방이 자신이 실제 알고 있는 지인과 동일 인물인지 혹은 피싱 공격자인지에 대한 사실 여부 파악이 어렵다는 문제점을 가지고 있다.

[0007] 지인 사칭 피싱 공격자는 상술한 문제점을 기반으로 피싱 대상자의 심리를 이용하여, 즉 대상자에게 접근 시 주로 긴급한 상황을 가정할 뿐만 아니라 프로필, 배경 사진 및 상태 메시지 등을 대상자의 지인과 동일하게 설정하는 등 꼼꼼하고 치밀하게 사기 행각을 벌인다. 이와 같은 피싱 행위를 차단할 수 있는 적절한 물리적인 장치는 현재 미비한 상황이며, 따라서 피싱 행위를 차단하기 위해 사용자의 주관적인 피싱 의식 수준에 전적으로 의존해야만 하는 현재의 실정은 지인 사칭 피싱을 완벽히 근절할 수 없는 상황이다.

발명의 내용

해결하려는 과제

[0008] 본 발명은 상술한 문제점을 해결하기 위한 것으로서, 이메일, 문자 메시지 및 메신저 서비스에서 메시지를 송신한 상대방의 신원 인증을 블록체인 기술을 활용하여 제공받는, 블록체인 기반 피싱 방지 방법 및 장치에 관한 것이다.

과제의 해결 수단

[0009] 상기 목적을 달성하기 위한 본 발명의 일실시예의 블록체인 기반 피싱 방지 시스템은, 메시지 관련 정보를 트랜잭션으로 생성하는 메시지 송신자; 메시지 송신자가 송부한 송신 메시지를 수신하는 메시지 수신자; 송신 메시지 및 수신 메시지를 중계하는 메시지 서버; 및 이메일, 문자 메시지 및 메신저 서비스 사용자의 신원 정보를 블록체인을 통해 관리하고, 메시지를 송신하여 송신 메시지 관련 정보를 블록체인에 기록하고, 블록체인에 기록된 송신 메시지 관련 정보를 이용하여 송신자 신원 정보를 검증하여 지인 사칭에 의한 피싱을 방지하는 블록체인 기반 피싱 방지 장치; 를 포함할 수 있다.

[0010] 상기 시스템은, 메시지를 송신한 상대방의 신원을 블록체인을 통해 인증하여 지인 사칭에 의한 피싱을 방지하기 위하여 상대방의 메시지 정보와 대응하는 블록체인 상의 대체불가능 토큰(Non-fungible token, NFT) 검증 여부를 통해 사용자 인증을 수행할 수 있다.

[0011] 상기 대체불가능 토큰(Non-fungible token)은, 대체불가능 토큰의 데이터 구조를 기반으로 표준 속성과 온체인(on-chain) 및 오프체인(off-chain) 확장 속성으로 구성될 수 있다.

[0012] 상기 대체불가능 토큰(Non-fungible token)은, 표준 속성은 토큰 아이디(ID) 속성, 토큰 타입 속성, 소유자 속성, 피승인자 속성을 포함하여 구성될 수 있다.

[0013] 상기 대체불가능 토큰(Non-fungible token)은, 온체인 확장 속성은 표준 속성의 토큰 타입에 따라 하위 속성이 다르게 정의되고, 피싱 방지 토큰 타입으로 송신자 아이디(id), 수신자 아이디(id), 및 메시지 내용 해쉬 속성으로 구성될 수 있다.

[0014] 상기 대체불가능 토큰(Non-fungible token)은, 오프체인 확장 속성은 대체불가능 토큰을 표현할 때 오프체인 데이터가 필요한 경우, 오프체인 저장소를 연결하기 위해 오프체인 저장소 경로를 저장하는 경로 속성과 오프체인 저장소의 데이터들로 구성된 머클 트리(merkle tree)의 머클 루트(merkle root)를 저장하는 해시 속성이 하위 속성으로 구성될 수 있다.

[0015] 상기 대체불가능 토큰(Non-fungible token)은, 온체인 확장 속성은 메시지를 송신하는 메시지 송신자 아이디(id) 정보와 해당 메시지를 수신하는 수신자 아이디(id) 정보를 각각 저장하는 송신자 아이디(id) 속성 및 수신자 아이디(id) 속성을 온체인 확장 속성의 하위 속성으로 정의할 수 있다.

[0016] 상기 대체불가능 토큰(Non-fungible token)은, 송신 메시지 내용의 무결성을 증명하기 위한 메시지 내용 해쉬 속성을 온체인 확장 속성의 하위 속성으로 정의될 수 있다.

[0017] 상기 대체불가능 토큰의 데이터 구조는, 탈중앙화 애플리케이션(dApp)을 통해 특정 객체에 대한 대체불가능 토큰의 발행이 요청되면, 토큰 발행 함수를 호출하여 토큰 식별자, 토큰타입, 및 소유자를 포함하는 표준 속성과 토큰타입 별로 설정되는 확장 속성으로 구성된 데이터 구조일 수 있다.

[0018] 본 발명의 다른 목적을 달성하기 위한 블록체인 기반 피싱 방지 장치는, 허가형 블록체인으로 구성되는 피싱 방지 블록체인; 및 메시지 송신자 및 메시지 수신자의 트랜잭션 전송을 중계하는 피싱 방지 소프트웨어 개발 키트(Software Development Kit, SDK); 를 포함하고, 메시지 관련 정보를 트랜잭션으로 생성하는 메시지 송신자와, 메시지 송신자가 송부한 송신 메시지를 수신하는 메시지 수신자 및 송신 메시지 및 수신 메시지를 중계하는 메시지 서버와 연동되어, 사용자의 신원 정보를 블록체인을 통해 관리하고, 메시지를 송신하여 송신 메시지 관련 정보를 블록체인에 기록하고, 블록체인에 기록된 송신 메시지 관련 정보를 이용하여 송신자 신원 정보를 검증하여 지인 사칭에 의한 피싱을 방지할 수 있다.

[0019] 피싱 방지 SDK는, 피싱 방지 블록체인 상에 메시지 내용을 기반으로 하는 피싱 방지 토큰을 발행하는 트랜잭션을 생성하는 발행부; 피싱 방지 블록체인 상에서 피싱 방지 토큰을 다른 사용자에게 전송하는 기능을 담당하는 전송부; 대체불가능 토큰을 발행한 사용자의 신원을 인증하는 기능을 담당하는 토큰 속성 검증부; 및 피싱 방지

SDK가 피싱 방지 블록체인으로부터 이벤트를 받으면, 호출한 주체에게 알림을 보내는 기능을 하는 이벤트부; 를 포함할 수 있다.

[0020] 발행부는, 메신저 송신자 단말기가 발행부를 통해 블록체인 트랜잭션을 생성하여 피싱 방지 블록체인 상에 피싱 방지 토큰을 발행할 수 있다.

[0021] 전송부는, 피싱 방지 토큰의 소유자가 전송부를 통해 피싱 방지 토큰의 소유권을 다른 사용자에게 양도하는 블록체인 트랜잭션을 생성할 수 있다.

[0022] 토큰 속성 검증부는, 대체불가능 토큰을 발행한 사용자가 실제 자신이 알고 있는 지인과 동일한 사용자인지 혹은 지인을 사칭한 피싱 공격자인지에 대한 판단 기준을 제공하는 기능을 할 수 있다.

[0023] 이벤트부는, 발행부, 전송부가 호출된 후 피싱 방지 토큰에 대한 동작 결과가 피싱 방지 블록체인에 최종적으로 커밋(commit)되면 피싱 방지 블록체인 이벤트를 수신하여 전달할 수 있다.

[0024] 이벤트부는, 메신저 송신자 단말기가 발행부를 통해 피싱 방지 토큰 발행을 요청한 후, 피싱 방지 블록체인 상에 토큰 생성이 완료되는 경우, 토큰 발행 완료 사실을 메신저 송신자 단말기에게 이벤트로 알리고, 메신저 송신자 단말기가 전송부를 통해 피싱 방지 토큰을 다른 사용자에게 전송을 요청한 후, 피싱 방지 블록체인 상에서 전송이 완료되는 경우, 성공적인 소유권 양도 완료 사실을 메신저 송신자 단말기에게 이벤트로 알릴 수 있다.

[0025] 본 발명의 또 다른 목적을 달성하기 위한 블록체인 기반 피싱 방지 방법은, 메시지 송신자가 송신하려는 메시지와 관련된 메시지 송신자 아이디(id) 및 수신자 아이디(id)와 메시지 내용 해쉬 정보를 포함하여 대체불가능 토큰을 발행하는 단계; 메시지 송신자가 발행된 대체불가능 토큰을 메시지 수신자에게 전송하는 단계; 메시지 송신자가 발행한 대체불가능 토큰 관련 정보와 송신 메시지 내용을 메시지 서버에게 전송하는 단계; 메시지 서버가 메시지 수신자에게 대체불가능 토큰 관련 정보와 송신 메시지 내용을 송신하는 단계; 메시지 수신자가 대체불가능 토큰에 기록된 메시지 송신자 아이디(id) 속성을 이용하여 메시지 송신자의 신원을 검증하고, 메시지 내용 해쉬 정보를 이용하여 송신 메시지 내용의 무결성을 검증하는 단계; 를 포함할 수 있다.

[0026] 상기 방법은, 메신저 메시지를 송신한 상대방의 신원 인증을 수행하기 위하여 블록체인을 활용하고, 사용자의 신원 인증을 제공하기 위한 정보 등을 블록체인 네트워크상에 유지 관리하기 위하여 송신자의 메시지 내용과 대응되는 대체불가능 토큰을 블록체인에서 유지 관리할 수 있다.

[0027] 상기 방법은, 송신자는 자신의 서명 정보를 기반으로 대체불가능 토큰을 발행하며, 대체불가능 토큰은 송·수신 대상자 및 메시지 내용 무결성 검증을 위한 메시지 내용 해쉬 정보를 포함하여 송신자 신원 및 메시지 내용 무결성 검증을 구현할 수 있다.

[0028] 상기 방법은, 송신자는 대체불가능 토큰을 발행 및 수신자에게 전송하여 자신이 피싱 공격자가 아니라는 증빙을 제공할 수 있다.

[0029] 상기 방법은, 메시지 송신자가 송신하려는 메시지 내용을 기반으로 대체불가능 토큰을 블록체인 상에 발행한 후, 토큰을 메시지 수신자에게 전달할 수 있다.

[0030] 상기 방법은, 대체불가능 토큰 속성으로는 토큰 고유 식별 아이디(id) 속성, 토큰을 발행한 소유자 속성, 메시지 송신자 및 수신자 아이디(id) 속성, 메시지 내용 무결성 검증을 위한 메시지 내용 해쉬 속성으로 정의할 수 있다.

[0031] 상기 방법은, 사용자가 메신저 메시지를 송신할 때 과정은, 사용자가 PKI(Public Key Infrastructure) 기반한 공개키, 비밀키 쌍을 가지고 있으며 블록체인 트랜잭션을 생성할 수 있다.

[0032] 상기 방법은, 메신저 서비스, 이메일, 문자 메시지 기능이 포함된 사용자 인증을 거치지 않는 서비스에 적용가능할 수 있다.

[0033] 본 발명의 또 다른 목적을 달성하기 위한 전술한 항 중 어느 한 항의 블록체인 기반 피싱 방지 방법을 구현하기 위한 컴퓨터 판독 가능한 기록매체에 저장된 컴퓨터 프로그램일 수 있다.

[0034] 본 발명의 또 다른 목적을 달성하기 위한 전술한 항 중 어느 한 항의 블록체인 기반 피싱 방지 방법의 프로그램을 구현하기 위한 컴퓨터 판독 가능한 기록매체일 수 있다.

발명의 효과

[0035] 본 발명은 온라인 상 정보 전달을 위한 목적으로 이메일, 문자 메시지 및 메신저 서비스 등에 사용자 인증 절차를 제공하기 위한 블록체인 기술을 적용함으로써, 사용자 신원 사칭 여부를 판별하여 지인 사칭 피싱을 방지하는 효과가 있다.

[0036] 자신과 메시지를 주고받는 상대방이 실제 피싱 공격자가 아니며(실제 지인에 해당하는 경우) 개인정보 혹은 금전을 요청하고자 한다면, 메시지 송신자는 먼저 블록체인 상 대체불가능 토큰을 발행하고 메시지 수신자에게 대체불가능 토큰 정보를 제공함으로써 사용자 인증에 대한 증빙을 제공할 수 있다. 메시지 수신자는 대체불가능 토큰을 통해 송신자의 사용자 인증이 확인되면, 본래 알고 있던 실제 지인과 메시지 송신자가 일치하다고 판단할 수 있으며, 반대로 송신자의 사용자 인증이 실패하는 경우, 송신자를 피싱 공격자로 판단하는 것이 가능해진다.

[0037] 따라서, 지인 사칭 피싱 행위를 판별하기 위해, 기존 방안과 달리, 블록체인을 통해 송신자 신원 인증을 수행함으로써 상대방이 자신이 실제 알고 있는 지인과 동일 인물인지 혹은 피싱 공격자인지에 대한 사실 여부를 객관적으로 판단할 수 있다. 본 발명에서 블록체인을 통해 송신자 신원과 메시지 무결성을 블록체인 토큰을 통해 검증하고 있으며, 본 발명의 결과는 향후 블록체인 기반 탈중앙화 신원 DID (Decentralized Identification) 서비스와 쉽게 연계할 수 있는 장점을 아울러 가진다.

도면의 간단한 설명

[0038] 도 1은 본 발명의 일 실시예의 블록체인 기반 피싱 방지 장치를 포함한 시스템 구성을 보여주는 도면이다.

도 2는 본 발명의 일 실시예의 블록체인 기반 피싱 방지 장치의 피싱 방지 SDK(Software Development Kit)의 구성을 보여주는 도면이다.

도 3은 본 발명의 일 실시예의 블록체인 활용의 한 가지 예로서, 송·수신하는 메시지에 대해 사용자 인증, 무결성 검증 특성을 제공하기 위해 메시지 관련 정보를 대체불가능 토큰으로 표현한 데이터 구조를 보여주는 도면이다.

도 4는 본 발명의 일 실시예의 블록체인을 활용하는 한 가지 예로서, 메시지 관련 정보를 대체불가능 토큰으로 표현할 경우, 블록체인 기반 피싱 방지 방법 및 장치를 활용한 메신저 시스템 구성의 전체적인 진행 과정을 보여주는 도면이다.

도 5는 본 발명의 일 실시예의 블록체인 기반 피싱 방지 장치의 구성도이다.

발명을 실시하기 위한 구체적인 내용

[0039] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하여 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.

[0040] 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.

[0041] 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.

[0042] 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.

[0043] 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.

[0044] 본 발명에서 개시되는 블록체인(blockchain)은 트랜잭션(transaction)들의 집합으로 구성된 블록이 이전 블록의 해시(hash)값을 담아 모든 블록을 체인 형식으로 연결하는 데이터 구조이다. 블록체인 네트워크에 참여하는 모든 노드(node)는 상기 데이터 구조를 동일하게 유지하고, 새로운 블록 생성 시 합의 알고리즘(consensus algorithm)을 기반으로 생성하기 때문에, 데이터의 무결성 및 투명성을 보장받을 수 있다.

[0045] 블록체인은 무허가형 블록체인(permissionless blockchain)과 허가형 블록체인(permissioned blockchain)으로 구분된다. 무허가형 블록체인에서 사용자 및 노드는 아무런 제약 없이 블록체인 네트워크에 참여하는 것이 가능하며, 허가형 블록체인에서는 허가된 사용자 및 노드들만 블록체인 네트워크에 참여할 수 있다. 따라서, 허가형 블록체인은 비즈니스 환경에서 활용하기에 적합한 블록체인이다.

[0046] 블록체인 상에서 실행되는 프로그램인 스마트 컨트랙트(smart contract)에 비즈니스 로직을 구성하여 분산 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.

[0047] 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 토큰의 성질에 따라 대체가능 토큰(fungible token)과 대체불가능 토큰(non-fungible token)으로 구분된다. 대체가능 토큰은 쪼개질 수 있는 성질을 가진 디지털 자산을 표현한 토큰이고, 대체불가능 토큰은 쪼개질 수 없는 성질을 내포하는 디지털 자산을 표현한 토큰이다.

[0048] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 본 발명을 설명함에 있어 전체적인 이해를 용이하게 하기 위하여 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다.

[0050] 도 1은 본 발명의 일 실시예의 블록체인 기반 피싱 탐지 장치(400)를 포함한 블록체인 기반 피싱 탐지 시스템(1000) 구성을 보여주는 도면이다.

[0051] 도 1을 참조하면, 본 발명의 일 실시 예에 따른 블록체인 기반 피싱 탐지 시스템(1000)은 사용자의 메시지를 송신하는 메신저 송신자 단말기(100a)와, 메신저 송신자 단말기(100a)가 송신한 메시지를 중계하는 메신저 서버(100c)와, 메신저 송신자 단말기(100a)가 송신한 메시지를 최종 수신하는 메신저 수신자 단말기(100b), 및 블록체인 기반 피싱 탐지 장치(400)를 포함하여 구성된다.

[0052] 메신저 송신자 단말기(100a)는 일반적인 메시지와 피싱 방지 메시지 중 선택하여 송신할 수 있다. 일반적인 메시지 송신을 선택하는 경우 기존 메신저 서비스와 동일하게 메신저 서버(100c)를 통해 전송하며, 피싱 방지 메시지 송신을 선택할 경우에는 메신저 서버(100c)를 통해 메시지를 전송하고 추가적으로 피싱 방지 SDK(200)와 연동되어 피싱 방지 블록체인(300)에 피싱 방지를 위한 블록체인 트랜잭션을 생성하도록 동작한다.

[0053] 메신저 서버(100c)는 비즈니스 영역에서 활용될 수 있으므로 기존 서비스를 그대로 활용할 수 있도록 구성하며, 사용자 신원을 미리 확인하고 서비스를 제공하기 위해서 피싱 방지 블록체인(300)을 허가형 블록체인으로 구성한다.

[0054] 블록체인 기반 피싱 탐지 장치(400)는 허가형 블록체인으로 구성되는 피싱 방지 블록체인(300) 및 메신저 송·수신자 단말기(100a~100b)의 트랜잭션 전송을 중계하는 피싱 방지 SDK(200)를 포함하여 구성된다.

[0056] 도 2는 본 발명의 일 실시예의 피싱 방지 SDK(200)의 구성을 보여주는 도면이다.

[0057] 도 2를 참조하면, 본 발명의 일 실시 예에 따른 블록체인 기반 피싱 탐지 시스템(1000)의 피싱 방지 SDK(Software Development Kit)(200)의 구성이 도시된다.

[0058] 피싱 방지 SDK(200)는 발행부(510), 전송부(520), 토큰 속성 검증부(530) 및 이벤트 부(540)를 포함하여 구성될 수도 있고, 발행부(510), 전송부(520), 토큰 속성 검증부(530) 및 이벤트 부(540)가 포함되는 별도의 장치와 연동될 수도 있다.

[0059] 발행부(510)는 피싱 방지 블록체인(300) 상에 메시지 내용을 기반으로 하는 피싱 방지 토큰을 발행하는 트랜잭션을 생성한다. 보다 구체적으로는, 메신저 송신자 단말기(100a)가 발행부(510)를 통해 블록체인 트랜잭션을 생성하여 피싱 방지 블록체인(300) 상에 피싱 방지 토큰을 발행한다. 피싱 방지 토큰 속성은 도 3에서 서술한다. 참고로, 토큰 소유자는 토큰을 발행한 주체가 된다.

[0060] 전송부(520)는 피싱 방지 블록체인(300) 상에서 피싱 방지 토큰을 다른 사용자에게 전송하는 기능을 담당한다. 보다 구체적으로는, 피싱 방지 토큰의 소유자가 전송부(520)를 통해 피싱 방지 토큰의 소유권을 다른 사용자에게 양도하는 블록체인 트랜잭션을 생성한다. 즉, 전송부(520) 호출이 완료되면 토큰의 소유자가 변경된다. 전송부(520) 호출 권한은 토큰 소유자만 가능하다.

[0061] 토큰 속성 검증부(530)는 대체불가능 토큰을 발행한 사용자의 신원을 인증하는 기능을 담당한다. 즉, 대체불가능 토큰을 발행한 사용자가 실제 자신이 알고 있는 지인과 동일한 사용자인지 혹은 지인을 사칭한 피싱 공격자인지에 대한 판단 기준을 제공하는 기능을 한다. 모든 사용자는 사용자 신원을 검증받은 후 피싱 방지 블록체인에 등록되므로, 자신의 사용자 정보와 관련된 서명 정보를 기반으로 하는 트랜잭션만 생성할 수 있다. 따라서, 대체불가능 토큰 수신자는 토큰 속성 검증부(530)를 호출하여 송신자가 발행한 대체불가능 토큰에 기록된 송·수신자 메신저 아이디(id)를 확인하며, 송신자 메신저 아이디(id)와 대응되는 사용자 정보 및 공개키가 수신자가 본래 알고 있던 지인의 사용자 정보 및 공개키와의 일치 여부를 비교함으로써, 송신자 당사자 인증을 수행할 수 있다. 추가적으로, 토큰 속성에는 메시지 내용에 대한 해쉬 정보를 저장하고 있으므로, 이를 통해 수신된 메시지의 무결성을 검증하는 과정도 진행할 수 있다.

[0062] 이벤트부(540)는 피싱 방지 SDK(200)가 피싱 방지 블록체인(300)으로부터 이벤트를 받으면, 호출한 주체에게 알림을 보내는 기능을 한다. 발행부(510), 전송부(520)가 호출된 후 피싱 방지 토큰에 대한 동작 결과가 피싱 방지 블록체인(300)에 최종적으로 커밋(commit)되면 피싱 방지 SDK(200)는 이벤트부 (540)를 통해 피싱 방지 블록체인(300) 이벤트를 받게 된다. 본 발명에서 이벤트부(540)가 전달하는 이벤트들은 다음과 같다. 메신저 송신자 단말기(100a)가 발행부(510)를 통해 피싱 방지 토큰 발행을 요청한 후, 피싱 방지 블록체인(300) 상에 토큰 생성이 완료되는 경우, 이벤트부(540)는 토큰 발행 완료 사실을 메신저 송신자 단말기(100a)에게 이벤트로 알린다. 또한, 메신저 송신자 단말기(100a)가 전송부(520)를 통해 피싱 방지 토큰을 다른 사용자에게 전송을 요청한 후, 피싱 방지 블록체인(300) 상에서 전송이 완료되는 경우, 이벤트부(540)는 성공적인 소유권 양도 완료 사실을 메신저 송신자 단말기(100a)에게 이벤트로 알린다.

[0064] 도 3은 본 발명의 일 실시예의 블록체인을 활용하는 예시 중 하나로서, 피싱 방지 토큰 속성 구조를 대체불가능 토큰으로 표현한 데이터 구조를 보여주는 도면이다.

[0065] 도 3을 참조하면, 피싱 방지 토큰은 표준 속성으로서 토큰 식별자(id), 토큰 타입(type), 소유자(owner), 운영자(operator), 및 피승인자(approvee) 속성을 가지며, 온체인 확장 속성(xattr)의 하위 속성으로 송·수신자의 메신저 아이디(id) 속성을 포함한다. 또한 송신자가 송신하는 피싱 방지 메시지 내용의 무결성을 검증하기 위한 메시지 내용 해쉬 속성을 가진다.

[0066] 블록체인 기반 피싱 방지 시스템, 장치 및 방법에서는 피싱 방지 토큰으로 대체불가능 토큰(Non-fungible token)이 사용되게 되는데, 대체불가능 토큰의 데이터 구조를 기반으로 표준 속성과 온체인(on-chain) 및 오프체인(off-chain) 확장 속성으로 구성되며, 표준 속성은 토큰 아이디(id) 속성, 토큰 타입 속성, 소유자 속성, 피승인자 속성을 포함한다.

[0067] 대체불가능 토큰(Non-fungible token)은, 온체인 확장 속성은 표준 속성의 토큰 타입에 따라 하위 속성이 다르게 정의되고, 피싱 방지 토큰 타입으로 송신자 아이디(id), 수신자 아이디(id), 및 메시지 내용 해쉬 속성으로 구성된다.

[0068] 이때, 오프체인 확장 속성은 대체불가능 토큰을 표현할 때 오프체인 데이터가 필요한 경우, 오프체인 저장소를 연결하기 위해 오프체인 저장소 경로를 저장하는 경로 속성과 오프체인 저장소의 데이터들로 구성된 머클 트리(merkle tree)의 머클 루트(merkle root)를 저장하는 해시 속성이 하위 속성으로 구성된다.

[0069] 그리고, 온체인 확장 속성은 메시지를 송신하는 메시지 송신자 아이디(id) 정보와 해당 메시지를 수신하는 수신자 아이디(id) 정보를 각각 저장하는 송신자 아이디(id) 속성 및 수신자 아이디(id) 속성을 온체인 확장 속성의 하위 속성으로 정의한다. 그리고, 송신 메시지 내용의 무결성을 증명하기 위한 메시지 내용 해쉬 속성을 온체인 확장 속성의 하위 속성으로 정의된다.

[0070] 그리고, 대체불가능 토큰의 데이터 구조는, 탈중앙화 애플리케이션(dApp)을 통해 특정 객체에 대한 대체불가능 토큰의 발행이 요청되면, 토큰 발행 함수를 호출하여 토큰 식별자, 토큰타입, 및 소유자를 포함하는 표준 속성과 토큰타입 별로 설정되는 확장 속성으로 구성된 데이터 구조이다.

[0071]

[0072] 도 4는 본 발명의 일 실시예의 블록체인을 활용하는 예시 중 하나로서, 블록체인 기반 피싱 방지 장치(400)를 포함한 시스템(1000)의 전체적인 진행 과정을 통한 블록체인 기반 피싱 방지 방법을 보여주는 도면이다.

[0073] 도 4를 참조하면, 본 발명의 일 실시예의 블록체인 기반 피싱 방지 방법은, 메시지 송신자가 송신하려는 메시지와 관련된 메시지 송신자 아이디(id) 및 수신자 아이디(id)와 메시지 내용 해쉬 정보를 포함하여 대체불가능 토큰을 발행하는 단계(S210), 메시지 송신자가 발행된 대체불가능 토큰을 메시지 수신자에게 전송하는 단계(S220), 메시지 송신자가 발행한 대체불가능 토큰 관련 정보와 송신 메시지 내용을 메시지 서버에게 전송하는 단계(S110), 메시지 서버가 메시지 수신자에게 대체불가능 토큰 관련 정보와 송신 메시지 내용을 송신하는 단계(S120), 메시지 수신자가 대체불가능 토큰에 기록된 메시지 송신자 아이디(id) 속성을 이용하여 메시지 송신자의 신원을 검증하고, 메시지 내용 해쉬 정보를 이용하여 송신 메시지 내용의 무결성을 검증하는 단계(S230)를 포함한다.

[0075] 본 발명의 일 실시예의 블록체인 기반 피싱 방지 방법은 도 4에 개시된 블록체인 기반 피싱 방지 장치(400)를 포함한 시스템(1000)의 전체적인 진행 과정을 통하여 실행된다.

[0076] 본 발명의 일 실시예의 블록체인 기반 피싱 방지 방법은, 메신저 송·수신자 단말기(100a~100b) 모두 피싱 방지 블록체인(300)에 등록된 사용자이며, 등록 시 사용자 신원을 인증받는다. 인증 받은 각 사용자는 사용자 정보와 대응되는 PKI 기반 공개키와 비밀키를 발급받는다. 피싱 방지 SDK(200)는 허가된 사용자들만 피싱 방지 블록체인(300)을 접근할 수 있도록 제어하기 위해 사용자들의 정보 및 해당 정보와 대응되는 공개키를 저장한다. 따라서, 각 사용자는 피싱 방지 SDK(200)가 관리하는 사용자 별 공개키를 이용하여, 블록체인 상 대체불가능 토큰을 통한 사용자 인증을 수행할 수 있다.

[0077] 메신저 송신자 단말기(100a)가 피싱 방지 메시지를 송신하고자 한다면, 메신저 서비스 상 메시지 내용을 기입한 뒤 피싱 방지 메시지를 송신한다. 메신저 송신자 단말기(100a)의 메시지 송신 과정은 우선 발행부(510)를 호출한다. 메신저 송신자 단말기(100a)가 호출한 발행부(510)는 피싱 방지 블록체인(300) 상에 피싱 방지 메시지 기반의 피싱 방지 토큰(토큰의 id는 T_0)을 발행한다(S210).

[0078] 발행된 토큰 T_0는 확장 속성의 하위 속성으로 메신저 송·수신자 아이디(id) 및 메시지 내용 해쉬 정보를 포함한다. 이벤트부(540)는 메신저 송신자 단말기(100a)에게 토큰 T_0의 성공적인 발행 완료 사실을 알리며, 메신저 송신자 단말기(100a)는 전송부(520)를 호출하여 메신저 수신자 단말기(100b)에게 토큰 T_0를 전송한다(S220).

[0079] 토큰 T_0의 소유권이 메신저 수신자 단말기(100b)에게 성공적으로 양도되면, 이벤트부(540)는 메신저 송신자 단말기(100a)에게 성공적인 양도 완료 사실을 알린다. 이벤트부(540)로부터 성공적인 알림을 받은 메신저 송신자 단말기(100a)는 메신저 수신자 단말기(100b)에게 피싱 방지 메시지(T_0 및 송신 메시지 내용)를 메신저 서버(100c)로 송신한다(S110).

[0080] 메시지를 수신한 메신저 서버(100c)는 메신저 수신자 단말기(100b)에게 메시지를 송신한다(S120).

[0081] 마지막으로, 메신저 수신자 단말기(100b)는 메신저 송신자 단말기(100a)가 송신한 메시지를 확인하기 위해 토큰 속성 검증부(530)를 호출한다. 메신저 수신자 단말기(100b)는 송신자의 서명 정보를 기반으로 발행한 대체불가능 토큰을 통해 송신자의 사용자 신원을 검증한다. 피싱 공격자는 수신자가 본래 알고 있는 지인을 사칭하기 위해 지인의 실제 서명 정보를 기반으로 대체불가능 토큰을 발행해야 한다. 그러나, 피싱 공격자는 지인의 서명 정보를 알 수 없으므로 사칭하기 위한 대체불가능 토큰을 발행할 수 없다. 따라서, 수신자는 송신자가 발행한 대체불가능 토큰에 기록된 송·수신자 메신저 아이디(id)를 확인하며, 송신자 메신저 아이디(id)와 관련된 사용자 정보 및 공개키가 수신자가 본래 알고 있던 지인의 사용자 정보 및 공개키와의 일치 여부를 비교함으로써, 송신자 당사자 인증을 수행할 수 있다. 사용자 신원이 확인되면, 메시지 내용의 무결성을 검증 해야한다. 메시지 내용 무결성은 메시지 내용을 해싱한 값과 대체불가능 토큰에 기록된 메시지 내용 해쉬 값을 비교함으로써 검증할 수 있다. 검증이 모두 완료되면, 메신저 수신자 단말기(100b)는 메시지 내용을 확인한다(S230).

[0083] 본 발명의 일 실시예에 따른 블록체인 기반 피싱 방지 방법은, 메신저 메시지를 송신한 상대방의 신원 인증을 수행하기 위하여 블록체인을 활용한다. 본 발명은 사용자의 신원 인증을 제공하기 위한 정보 등을 블록체인 네트워크상에 유지 관리하는 다양한 방법을 포함하고 있으며, 하나의 구체적인 일례로 송신자의 메시지 내용과 대응되는 대체불가능 토큰을 블록체인에서 유지 관리하는 방법을 서술한다. 송신자는 자신의 서명 정보를 기반으로 대체불가능 토큰을 발행하며, 해당 대체불가능 토큰은 송·수신 대상자 및 메시지 내용 무결성 검증을 위한 메시지 내용 해쉬 정보를 포함하기 때문에, 송신자 신원 및 메시지 내용 무결성 검증 방법을 용이하게 제공할 수 있다. 따라서, 송신자는 대체불가능 토큰을 발행 및 수신자에게 전송함으로써, 자신이 피싱 공격자가 아니라는 확실한 증빙을 제공하는 것이 가능해진다. 메시지 송신자가 송신하려는 메시지 내용을 기반으로 대체불가능 토큰을 블록체인 상에 발행한 후, 토큰을 메시지 수신자에게 전달한다. 대체불가능 토큰 속성으로는 토큰 고유 식별 아이디(id) 속성, 토큰을 발행한 소유자 속성, 메시지 송신자 및 수신자 아이디(id) 속성, 메시지 내용 무결성 검증을 위한 메시지 내용 해쉬 속성 등으로 정의하며, 토큰 속성은 필요시 다양하게 추가 및 정의할 수 있다.

[0084] 사용자가 메신저 메시지를 송신할 때 과정은 다음과 같다. 모든 사용자는 PKI(Public Key Infrastructure) 기반한 공개키, 비밀키 쌍을 가지고 있으며, 따라서 모든 사용자는 블록체인 트랜잭션을 생성할 수 있다고 가정한다.

[0085] 첫째. 송신자는 메신저 서비스 상에서 메시지 내용을 작성 및 송신한다.

[0086] 둘째. 송신자는 방금 전송한 메시지 내용을 기반으로 블록체인 상에 대체불가능 토큰을 발행하며, 토큰 속성으로는 토큰 아이디(id), 소유자, 송·수신자 메신저 아이디(id) 및 메시지 내용 해쉬 정보 등을 포함한다. 이때, 토큰을 발행하기 위한 트랜잭션 정보에 메시지 송신자의 서명 정보가 포함되며, 따라서 발행된 토큰의 소유자는 메시지 송신자가 된다.

[0087] 셋째. 송신자는 블록체인 상 초기화한 대체불가능 토큰을 수신자에게 전송하여 토큰의 소유자를 메시지 수신자로 변경한다.

[0088] 넷째. 송신자는 메신저 서비스를 통해 대체불가능 토큰 관련 정보와 메시지 내용을 송신한다.

[0089] 다섯째. 수신자는 수신한 대체불가능 토큰 정보를 기반으로 블록체인 상 대체불가능 토큰을 조회하며, 이를 통해 송신자의 신원을 검증한다. 피싱 공격자는 수신자가 본래 알고 있는 지인으로 사칭하기 위해 지인의 실제 서명 정보를 기반으로 대체불가능 토큰을 발행해야 한다. 그러나, 피싱 공격자는 지인의 서명 정보를 알 수 없으므로 사칭하기 위한 대체불가능 토큰을 발행할 수 없다. 따라서, 수신자는 송신자가 발행한 대체불가능 토큰에 기록된 송신자 메신저 아이디(id)를 확인하여 송신자 당사자 인증을 수행할 수 있다. 송신자 신원이 검증되면, 메시지 내용의 무결성을 검증한다. 수신자가 수신한 메시지 내용을 해싱한 값이 대체불가능 토큰에 기록된 메시지 내용 해쉬 값과 일치하는지를 비교함으로써, 메시지 내용이 무결한지 검증할 수 있다.

[0090] 여섯째. 송신자의 신원 및 메시지 내용의 무결성이 블록체인 상 대체불가능 토큰을 통해 검증 완료되면, 수신자는 최종적으로 메시지 내용을 확인한다.

[0091] 본 발명에서 상술하는 지인 사칭 피싱 방지 방법은 메신저 서비스뿐만 아니라 이메일과 문자 메시지처럼 사용자 인증을 거치지 않는 다양한 서비스들에 동일하게 적용할 수 있다.

[0093] 도 5는 본 발명의 일 실시예의 블록체인 기반 피싱 방지 장치(400)의 구성도이다.

[0094] 도 5를 참조하면, 본 발명의 일 실시예의 블록체인 기반 피싱 방지 장치(400)는, 프로세서(410), 메모리(420), 송수신 장치(transceiver, 430), 입력 인터페이스 장치(440), 출력 인터페이스 장치(450), 저장 장치(460) 및 버스(bus)(470)를 포함하여 구성될 수 있다.

[0095] 본 발명의 블록체인 기반 피싱 방지 장치(400)는, 프로세서(processor)(410) 및 프로세서(410)를 통해 실행되는 적어도 하나의 명령이 저장된 메모리(memory)(420)를 포함하되, 적어도 하나의 명령은 상기 프로세서(410)가, 메시지 송신자가 송신하려는 메시지와 관련된 메시지 송·수신자 아이디(id)와 메시지 내용 해쉬 정보를 포함하여 대체불가능 토큰을 발행하는 단계; 메시지 송신자가 발행된 대체불가능 토큰을 메시지 수신자에게 전송하는 단계; 메시지 송신자가 발행한 대체불가능 토큰 관련 정보와 송신 메시지 내용을 메시지 서버에게 전송하는 단계; 메시지 서버가 메시지 수신자에게 대체불가능 토큰 관련 정보와 송신 메시지 내용을 송신하는 단계; 메시지 수신자가 대체불가능 토큰에 기록된 메시지 송신자 아이디(id) 속성을 이용하여 메시지 송신자의 신원을 검증하고, 메시지 내용 해쉬 정보를 이용하여 송신 메시지 내용의 무결성을 검증하는 단계; 를 수행하도록 구성된다.

[0096] 프로세서(410)는 중앙 처리 장치(central processing unit, CPU), 그래픽 처리 장치(graphics processing unit, GPU), 또는 본 발명의 실시예들에 따른 방법들이 수행되는 전용의 프로세서를 의미할 수 있다.

[0097] 메모리(420) 및 저장 장치(460) 각각은 휘발성 저장 매체 및 비휘발성 저장 매체 중에서 적어도 하나로 구성될 수 있다. 예를 들어, 메모리(420)는 읽기 전용 메모리(read only memory, ROM) 및 랜덤 액세스 메모리(random access memory, RAM) 중에서 적어도 하나로 구성될 수 있다.

[0098] 또한, 블록체인 기반 피싱 방지 장치(400)는 무선 네트워크를 통해 통신을 수행하는 송수신 장치(transceiver)(430)를 포함할 수 있다.

[0099] 또한, 블록체인 기반 피싱 방지 장치(400)는 입력 인터페이스 장치(440), 출력 인터페이스 장치(450), 저장 장치(460) 등을 더 포함할 수 있다.

[0100] 또한, 블록체인 기반 피싱 방지 장치(400)에 포함된 각각의 구성 요소들은 버스(bus)(470)에 의해 연결되어 서로 통신을 수행할 수 있다.

[0101] 본 발명의 블록체인 기반 피싱 방지 장치(400)의 예를 들면, 통신 가능한 데스크탑 컴퓨터(desktop computer), 랩탑 컴퓨터(laptop computer), 노트북(notebook), 스마트폰(smart phone), 태블릿 PC(tablet PC), 모바일폰(mobile phone), 스마트 워치(smart watch), 스마트 글래스(smart glass), e-book 리더기, PMP(portable multimedia player), 휴대용 게임기, 네비게이션(navigation) 장치, 디지털 카메라(digital camera), DMB(digital multimedia broadcasting) 재생기, 디지털 음성 녹음기(digital audio recorder), 디지털 음성 재생기(digital audio player), 디지털 동영상 녹화기(digital video recorder), 디지털 동영상 재생기(digital video player), PDA(Personal Digital Assistant) 등일 수 있다.

[0103] 이와 같이, 본 발명에 따르면 일반적인 메신저 서비스의 사용자 인증 부재에 따른 지인 사칭 피싱 공격을 블록체인 기술을 적용하여 해결할 수 있으며, 구체적인 실시 예로 대체불가능 토큰을 모델링하여 사용자 인증을 수행함으로써 지인 사칭 피싱 공격을 차단할 수 있음을 확인하였다. 또한, 메신저 서비스뿐만 아니라 사용자 인증을 거치지 않는 보편적인 이메일 혹은 문자 메시지 서비스 등에서도 동일하게 적용하여 지인 사칭 피싱 공격을 차단할 수 있다.

[0104] 메시지 수신자는 대체불가능 토큰을 통해 송신자의 사용자 인증 및 메시지 내용 무결성이 검증되면 송신자를 실제 지인이라고 판단할 수 있으며, 반대로 송신자의 사용자 인증 및 메시지 내용 무결성 검증이 실패하는 경우, 송신자를 피싱 공격자로 판단하는 것이 가능해진다.

[0105] 따라서, 지인 사칭 피싱 공격을 판별하기 위해 사용자의 주관적인 피싱 의식 수준에만 전적으로 의존하던 방법에서 벗어나, 상대방이 자신이 실제 알고 있는 지인과 동일 인물인지 혹은 피싱 공격자인지에 대한 사용자 인증을 블록체인을 통해 객관적인 방법으로 수행할 수 있으므로 지인 사칭 피싱 공격을 차단할 수 있다.

[0107] 본 발명의 실시예에 따른 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 코드가 저장되고 실행될 수 있다.

[0108] 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.

[0109] 본 발명의 일부 측면들은 장치의 문맥에서 설명되었으나, 그것은 상응하는 방법에 따른 설명 또한 나타낼 수 있고, 여기서 블록 또는 장치는 방법 단계 또는 방법 단계의 특징에 상응한다. 유사하게, 방법의 문맥에서 설명된 측면들은 또한 상응하는 블록 또는 아이템 또는 상응하는 장치의 특징으로 나타낼 수 있다. 방법 단계들의 몇몇 또는 전부는 예를 들어, 마이크로프로세서, 프로그램 가능한 컴퓨터 또는 전자 회로와 같은 하드웨어 장치에 의해(또는 이용하여) 수행될 수 있다. 몇몇의 실시예에서, 가장 중요한 방법 단계들의 하나 이상은 이와 같은 장치에 의해 수행될 수 있다.

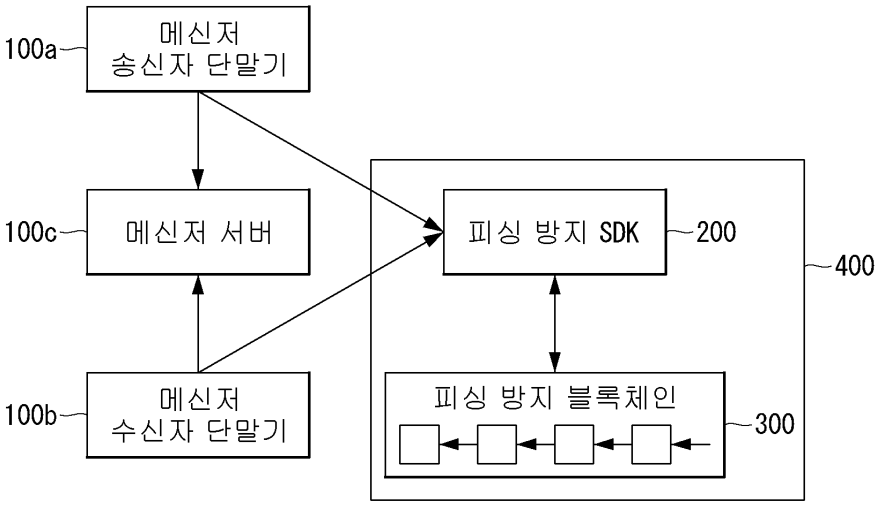
[0110] 실시예들에서, 프로그램 가능한 로직 장치(예를 들어, 필드 프로그머블 게이트 어레이)가 여기서 설명된 방법들의 기능의 일부 또는 전부를 수행하기 위해 사용될 수 있다. 실시예들에서, 필드 프로그머블 게이트 어레이는

여기서 설명된 방법들 중 하나를 수행하기 위한 마이크로프로세서와 함께 작동할 수 있다. 일반적으로, 방법들은 어떤 하드웨어 장치에 의해 수행되는 것이 바람직하다.

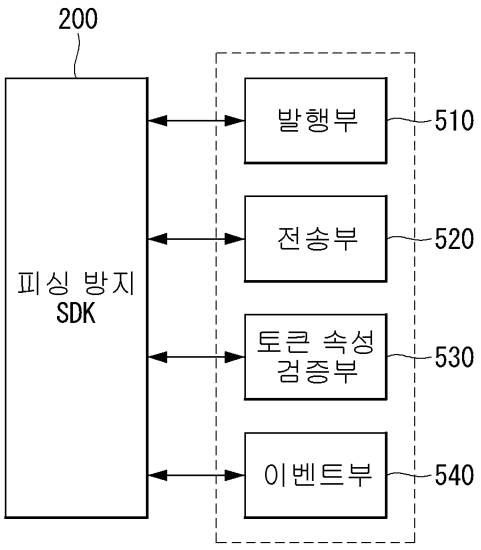
[0111] 이상 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

도면

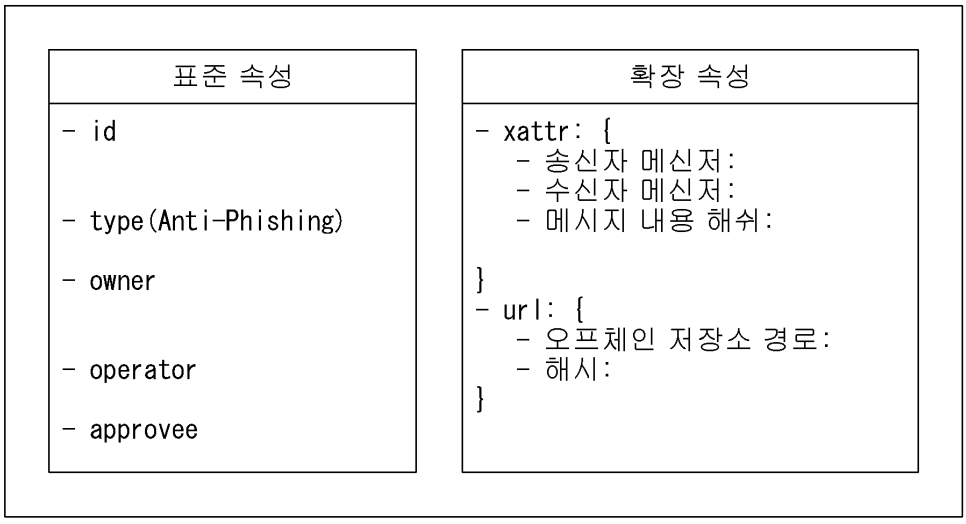
도면1



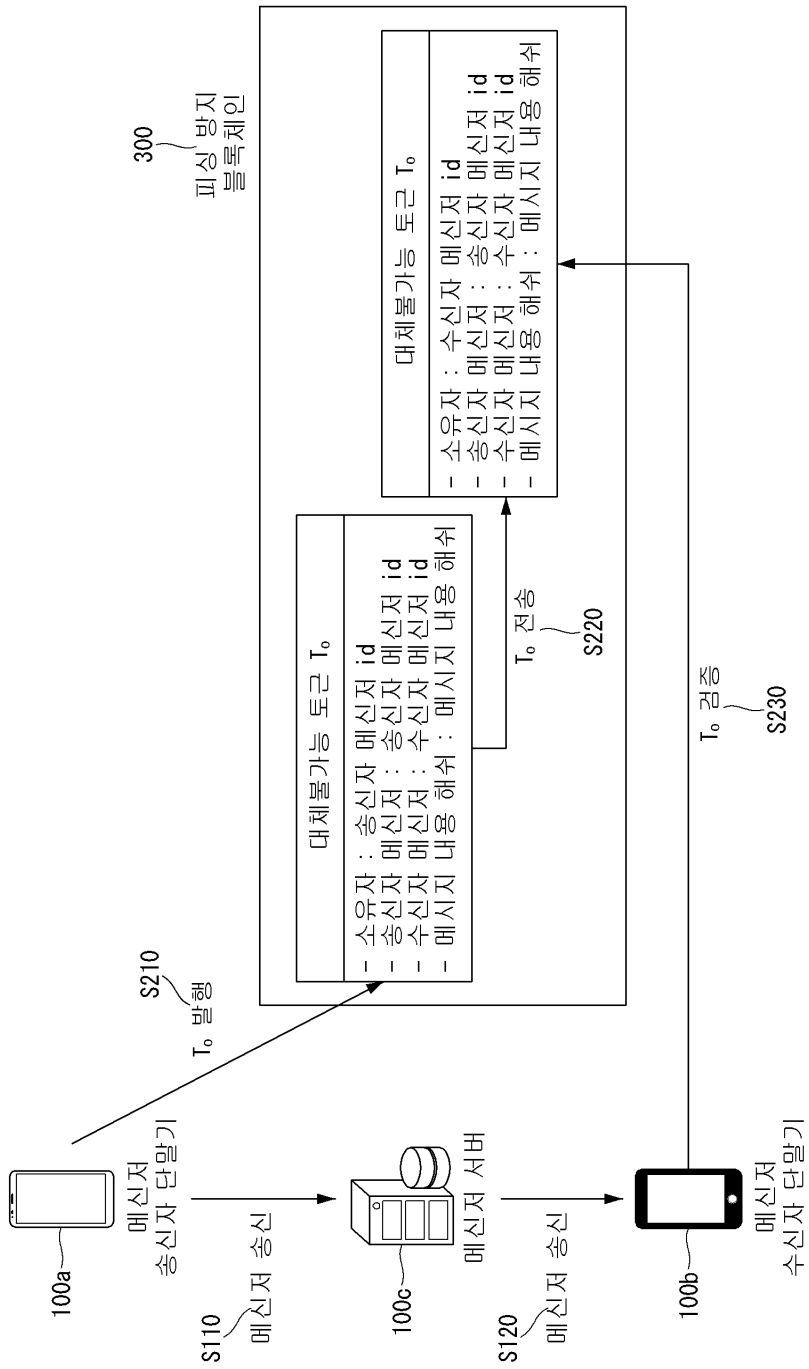
도면2



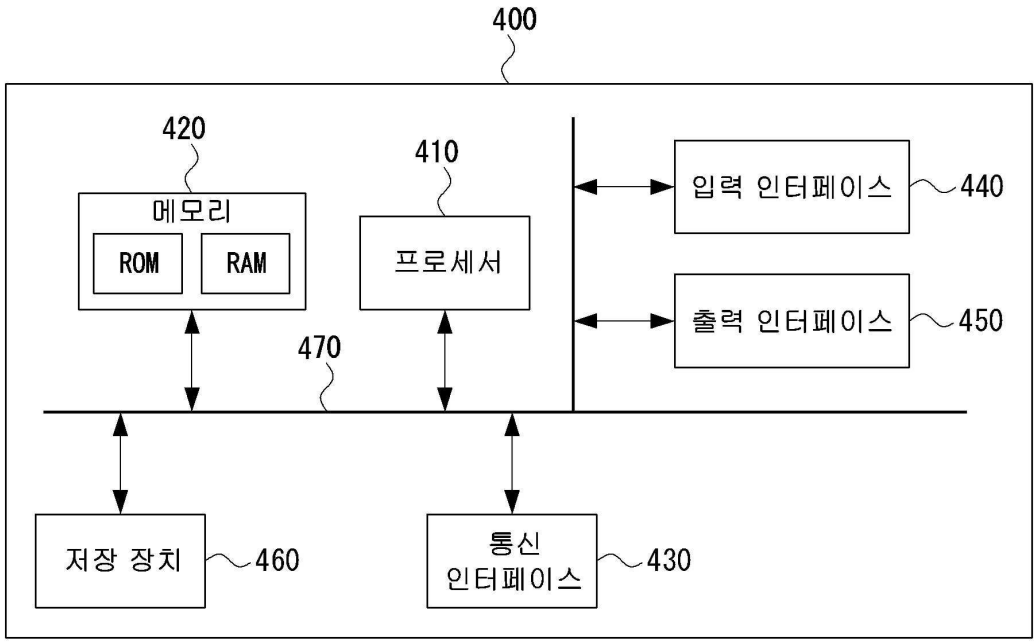
도면3


표준 속성
- id
- type(Anti-Phishing)
- owner
- operator
- approvee
확장 속성
- xattr: {
- 송신자 메신저:
- 수신자 메신저:
- 메시지 내용 해쉬:
}
- url: {
- 오프체인 저장소 경로:
- 해시:
}

도면4


300
피싱 방지
블록체인
대체불가능 토근 T_o
- 소유자 : 송신자 메신저 id
- 송신자 메신저 : 송신자 메신저 id
- 수신자 메신저 : 수신자 메신저 id
- 메시지 내용 해쉬 : 메시지 내용 해쉬
대체불가능 토근 T_o
- 소유자 : 수신자 메신저 id
- 송신자 메신저 : 송신자 메신저 id
- 수신자 메신저 : 수신자 메신저 id
- 메시지 내용 해쉬 : 메시지 내용 해쉬
S210
T_o 발행
T_o 전송
S220
T_o 검증
S230
100a
메신저
송신자 단말기
S110
메신저 송신
100c
메신저 서버
S120
메신저 송신
100b
메신저
수신자 단말기

도면5


400
420
메모리
ROM
RAM
410
프로세서
입력 인터페이스
440
출력 인터페이스
450
470
저장 장치
460
통신
인터페이스
430