(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년12월15일
(11) 등록번호 10-2191111
(24) 등록일자 2020년12월09일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 12/58* (2006.01)
H04L 9/06 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 63/0421 (2013.01)
H04L 51/30 (2013.01)
(21) 출원번호 10-2018-0116799
(22) 출원일자 2018년10월01일
심사청구일자 2018년10월01일
(65) 공개번호 10-2020-0037508
(43) 공개일자 2020년04월09일
(56) 선행기술조사문헌
KR1020180018234 A*
KR1020180029695 A
KR1020180025771 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
명지대학교 산학협력단
경기도 용인시 처인구 명지로 116 (남동, 명지대학교)
(72) 발명자
한승철
경기도 과천시 광창1로 7 (과천동)
김정운
경기도 수원시 영통구 봉영로1517번길 76, 623동 105호(영통동, 동보.신명 아파트)
(뒷면에 계속)
(74) 대리인
송인호, 최관락

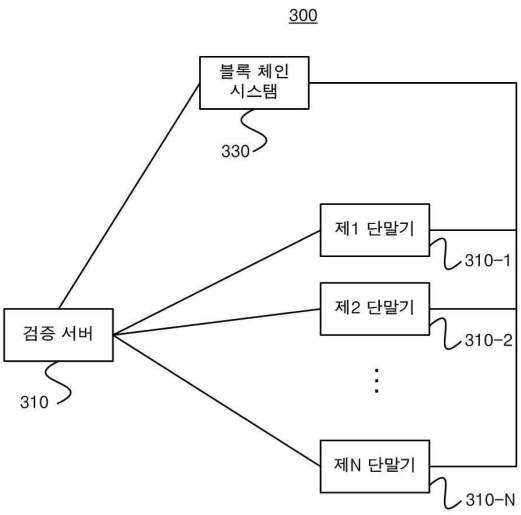
전체 청구항 수 : 총 9 항 심사관 : 홍기완

(54) 발명의 명칭 **블록 체인을 이용하여 익명 메시지 서비스를 제공하기 시스템 및 방법**

(57) 요 약

블록 체인을 이용하여 익명 메시지 서비스를 제공하기 시스템 및 방법이 개시된다. 개시된 방법은 익명 메시지를 작성한 작성자 단말기, 수신자 단말기 또는 블록 체인 시스템과 상기 검증 서버를 연결하는 단계; 및 익명 메시지 ID 요청을 위한 데이터, 블록 체인에 의한 블록 업데이트와 익명 메시지 수신과 관련된 데이터, 및 익명 메시지의 실명 공개 요청에 의한 데이터 중 적어도 하나를 상기 작성자 단말기, 상기 수신자 단말기 및 상기 블록 체인 시스템과 송수신하는 단계;를 포함하되, 상기 블록 체인에 따른 블록 전파를 통해 상기 익명 메시지가 상기 수신자 단말기로 배포되며, 상기 익명 메시지를 작성한 작성자의 실명이 상기 작성자의 실명 공개 요청에 따라 상기 블록 체인을 통해 공개된다.

대 표 도 - 도3



(52) CPC특허분류
H04L 51/32 (2013.01)
H04L 9/0618 (2013.01)
H04L 9/0643 (2013.01)
H04L 9/0833 (2013.01)
H04L 2209/38 (2013.01)

(72) 발명자
권유진
인천광역시 남동구 아암대로1503번길 98, 606동 2703호(논현동, 에코메트로6단지한화꿈에그린아파트)
남기원
서울특별시 서초구 신반포로15길 33, 401호(반포동, 반포파크빌)
한동호
경기도 과천시 광창1로 7(과천동)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711068909
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	개인기초연구(과기정통부)(R&D)
연구과제명	봇넷탐지를 위한 빅데이터 3D 시각화 시스템
기 여 율	1/1
과제수행기관명	명지대학교
연구기간	2018.03.01 ~ 2019.02.28

명 세 서

청구범위

청구항 1

검증 서버에서의 익명 메시지 서비스 제공 방법에 있어서,

익명 메시지를 작성한 작성자 단말기, 수신자 단말기 또는 블록 체인 시스템과 상기 검증 서버를 연결하는 단계; 및

익명 메시지 ID 요청을 위한 데이터, 블록 체인에 의한 블록 업데이트와 익명 메시지 수신과 관련된 데이터, 및 익명 메시지의 실명 공개 요청에 의한 데이터 중 적어도 하나를 상기 작성자 단말기, 상기 수신자 단말기 및 상기 블록 체인 시스템과 송수신하는 단계;를 포함하되,

상기 익명 메시지 ID 요청을 위한 데이터에 대한 송수신 단계 (a)는,

상기 작성자의 ID(UID), 상기 작성자 및 상기 수신자를 멤버로 하는 그룹의 그룹키(GK)로 상기 작성자가 작성한 메시지의 내용(TEXT)을 암호화한 값(GK(TEXT)), 상기 TEXT의 해시값(H(TEXT)), 및 상기 TEXT가 작성된 시간(TS(TEXT))를 상기 작성자 단말기로부터 수신하는 단계 (a1);

상기 메시지의 ID(MID), 상기 MID의 생성 시간(TS(MID)) 및 상기 메시지의 번호(Msg_No)를 생성하는 단계 (a2);

익명성 검증을 위해, 상기 H(TEXT), 상기 MID 및 상기 TS(MID)를 해시한 해시값(H(H(TEXT), MID, TS(MID)))을 생성하는 단계 (a3); 및

상기 생성된 H(TEXT), MID, TS(MID) 및 Msg_No를 상기 작성자와 상기 검증 서버가 공유하는 대칭키(KVS-A)로 암호화하여 상기 작성자 단말기로 전송하는 단계 (a4)를 포함하되,

상기 단계 (a1) 이전에, 상기 작성자 단말기는 상기 TEXT 및 상기 H(TEXT)를 상기 작성자 단말기의 DB 테이블(TABLE_A)에 저장하고,

상기 단계 (a4) 이후에, 상기 작성자 단말기는 상기 대칭키(KVS-A)를 이용하여 상기 검증 서버에서 전송받은 H(TEXT), MID, TS(MID) 및 Msg_No의 암호화된 값을 복호화하고, 상기 TABLE_A에 저장된 H(TEXT)와 상기 복호화된 H(TEXT)를 비교하여 일치하는 경우, 상기 복호화된 MID, TS(MID), Msg_No를 상기 TABLE_A에 저장하며,

상기 블록 체인에 따른 블록 전파를 통해 상기 익명 메시지가 상기 수신자 단말기로 배포되며, 상기 익명 메시지를 작성한 작성자의 실명이 상기 작성자의 실명 공개 요청에 따라 상기 블록 체인을 통해 공개되는 것을 특징으로 하는 검증 서버에서 익명 메시지 서비스 제공 방법.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 작성자 단말기로부터 수신된 UID, GK(TEXT), H(TEXT) 및 TS(TEXT)는 상기 대칭키(KVS-A)로 암호화된 값인 것을 특징으로 하는 검증 서버에서 익명 메시지 서비스 제공 방법.

청구항 4

삭제

청구항 5

제1항에 있어서,

상기 블록 체인에 의한 블록 업데이트와 익명 메시지 수신과 관련된 데이터에 대한 송수신 단계 (b)는,

상기 단계 (a1)에서 수신된 GK(TEXT), H(TEXT), TS(TEXT)와, 상기 단계 (a2)에서 생성된 Msg_No와, 상기 단계 (a3)에서 생성된 H(H(TEXT), MID, TS(MID))를 포함하는 제1 트랜잭션을 생성하는 단계 (b1); 및

상기 생성된 제1 트랜잭션을 상기 블록 체인 시스템에 전송하는 단계 (b2);를 포함하되,

상기 블록 체인 시스템은 상기 전송된 제1 트랜잭션에 기초하여 제1 블록을 생성하고, 상기 생성된 제1 블록은 상기 블록 체인에 등록되어 전파되는 것을 특징으로 하는 검증 서버에서 익명 메시지 서비스 제공 방법.

청구항 6

제5항에 있어서,

상기 수신자 단말기 각각은,

상기 제1 블록의 상기 제1 트랜잭션에서 GK(TEXT) 및 H(TEXT)를 추출하고, 상기 GK를 이용해 상기 추출된 GK(TEXT)를 복호화하여 TEXT를 추출하고, 상기 추출된 TEXT에 대해 H(TEXT)를 생성하며, 상기 생성된 H(TEXT)와 상기 추출된 H(TEXT)를 비교하여 TEXT의 무결성을 검증하며 TEXT를 수신하는 것을 특징으로 하는 검증 서버에서 익명 메시지 서비스 제공 방법.

청구항 7

제5항에 있어서,

상기 익명 메시지의 실명 공개 요청에 의한 데이터에 대한 송수신 단계 (c)는,

상기 작성자 단말기에서 전송된 UID, Msg_No, 및 GK(MID, H(TEXT), TS(MID))를 수신하는 단계 (c1);

상기 수신된 UID, Msg_No, GK(MID, H(TEXT), TS(MID))을 포함하는 제2 트랜잭션을 생성하는 단계 (c2);

상기 생성된 제2 트랜잭션을 상기 블록 체인 시스템에 전송하는 단계 (c3);를 포함하되,

상기 블록 체인 시스템은 상기 전송된 제2 트랜잭션에 기초하여 제2 블록을 생성하고, 상기 생성된 제2 블록은 상기 블록 체인에 등록되어 전파되는 것을 특징으로 하는 검증 서버에서 익명 메시지 서비스 제공 방법.

청구항 8

제7항에 있어서,

상기 수신자 단말기 각각은, 상기 제2 블록의 제2 트랜잭션의 Msg_No에 기초하여 상기 제1 블록을 검색하고, 상기 제1 블록 내의 제1 트랜잭션에서 H(TEXT) 및 H(H(TEXT), MID, TS(MID))를 추출하고, 상기 제2 블록의 상기 제2 트랜잭션에서 추출된 MID, TS(MID)와 상기 제1 블록 내의 제1 트랜잭션에서 추출된 H(TEXT)의 해시값 H(H(TEXT), MID, TS(MID)를 생성하고 상기 추출된 H(H(TEXT), MID, TS(MID)와 상기 생성된 H(H(TEXT), MID, TS(MID)을 비교하여 일치하면 상기 작성자가 공개되는 것을 특징으로 하는 검증 서버에서 익명 메시지 서비스 제공 방법.

청구항 9

제7항에 있어서,

상기 작성자 단말기로부터 수신된 UID, Msg_No, 및 GK(MID, H(TEXT), TS(MID)는 상기 대칭키(KVS-A)로 암호화된 값인 것을 특징으로 하는 검증 서버에서 익명 메시지 서비스 제공 방법.

청구항 10

제1항, 제3항, 제5항 내지 제9항 중 어느 한 항의 방법을 수행하는 프로그램을 기록한 컴퓨터 판독 가능 기록매체.

청구항 11

익명 메시지 서비스 제공을 위한 검증 서버에 있어서,

익명 메시지를 작성한 작성자 단말기, 수신자 단말기 또는 블록 체인 시스템과 상기 검증 서버를 연결하는 통신부; 및

익명 메시지 ID 요청을 위한 데이터, 블록 체인에 의한 블록 업데이트와 익명 메시지 수신과 관련된 데이터, 및 익명 메시지의 실명 공개 요청에 의한 데이터 중 적어도 하나를 상기 작성자 단말기, 상기 수신자 단말기 및 상기 블록 체인 시스템과 송수신하는 메시지부;를 포함하되,

상기 메시지부는,

상기 작성자의 ID(UID), 상기 작성자 및 상기 수신자를 멤버로 하는 그룹의 그룹키(GK)로 상기 작성자가 작성한 메시지의 내용(TEXT)을 암호화한 값(GK(TEXT)), 상기 TEXT의 해시값(H(TEXT)), 및 상기 TEXT가 작성된 시간(TS(TEXT))를 상기 작성자 단말기로부터 수신하고(a1), 상기 메시지의 ID(MID), 상기 MID의 생성 시간(TS(MID)) 및 상기 메시지의 번호(Msg_No)를 생성하며(a2), 익명성 검증을 위해, 상기 H(TEXT), 상기 MID 및 상기 TS(MID)를 해시한 해시값(H(H(TEXT), MID, TS(MID)))을 생성하고(a3), 상기 생성된 H(TEXT), MID, TS(MID) 및 Msg_No를 상기 작성자와 상기 검증 서버가 공유하는 대칭키(KVS-A)로 암호화하여 상기 작성자 단말기로 전송(a4)하되,

상기 작성자 단말기는,

상기 단계 (a1) 이전에, 상기 작성자 단말기는 상기 (a1) 이전에 상기 TEXT 및 상기 H(TEXT)를 상기 작성자 단말기의 DB 테이블(TABLE_A)에 저장하고, 상기 (a4) 이후에 상기 대칭키(KVS-A)를 이용하여 상기 검증 서버에서 전송받은 H(TEXT), MID, TS(MID) 및 Msg_No의 암호화된 값을 복호화하고, 상기 TABLE_A에 저장된 H(TEXT)와 상기 복호화된 H(TEXT)를 비교하여 일치하는 경우, 상기 복호화된 MID, TS(MID), Msg_No를 상기 TABLE_A에 저장하며,

상기 블록 체인에 따른 블록 전파를 통해 상기 익명 메시지가 상기 수신자 단말기로 배포되며, 상기 익명 메시지를 작성한 작성자의 실명이 상기 작성자의 실명 공개 요청에 따라 상기 블록 체인을 통해 공개되는 것을 특징으로 하는 검증 서버.

청구항 12

삭제

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예들은 블록 체인을 이용하여 익명 메시지 서비스를 제공하기 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 블록 체인은 분산되고 독립적이며 개방된 공통 장부 관리 기술이다. 블록 체인에 참여한 모든 사용자는 공통 장부의 내용을 소유하고 있고, 정해진 룰에 의해 검증된 블록만이 블록 체인에 연결된다. 블록 체인은 어떤 가치를 다루는 복잡한 시스템을 저가로 교체하거나 신규 개발하는데 이용되거나, 복수의 조직에서 공유하여 조직간에 맞물려 있던 특정한 중앙 처리 시스템을 경유하지 않고 효율적으로 사용하는 것에 이용되거나, 업무를 자동화하여 업무 비용을 삭감하는 것에 이용되거나, 직접 참가하는 형태의 새로운 서비스를 구축하는 것에 이용된다.

[0003] 한편, 최근, SNS 등 그룹 사용자들 사이에 대화를 할 수 있는 많은 대화 서비스가 존재한다. 이러한 대화 서비스에서 대화 시 누가 메시지를 보냈는지가 실명으로 공개된다.

[0004] 이러한 실명 공개는 범죄 예방 등 많은 부분에서 유리한 점이 있으나, 범죄와 전혀 관계없는 실명으로 보내는 것이 망설여지는 메시지를 대화창에 입력하여야 할 때는 사용자에게 불편을 야기시켰다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) KR 10-2016-0081448 A

발명의 내용

해결하려는 과제

[0006] 상기한 바와 같은 종래기술의 문제점을 해결하기 위해, 본 발명에서는 블록 체인을 이용하여, 그룹 대화에서 메시지들 중 적어도 일부를 익명 메시지로 입력하고, 추후 작성자가 원할 경우 작성자의 실명을 공개할 수 있는 익명 메시지 서비스를 제공하기 시스템 및 방법을 제공하는 것이다.

[0007] 본 발명의 다른 목적들은 하기의 실시예를 통해 당업자에 의해 도출될 수 있을 것이다.

과제의 해결 수단

[0008] 상기한 목적을 달성하기 위해 본 발명의 바람직한 일 실시예에 따르면, 검증 서버에서의 익명 메시지 서비스 제공 방법에 있어서, 익명 메시지를 작성한 작성자 단말기, 수신자 단말기 또는 블록 체인 시스템과 상기 검증 서버를 연결하는 단계; 및 익명 메시지 ID 요청을 위한 데이터, 블록 체인에 의한 블록 업데이트와 익명 메시지 수신과 관련된 데이터, 및 익명 메시지의 실명 공개 요청에 의한 데이터 중 적어도 하나를 상기 작성자 단말기, 상기 수신자 단말기 및 상기 블록 체인 시스템과 송수신하는 단계를 포함하되, 상기 블록 체인에 따른 블록 전파를 통해 상기 익명 메시지가 상기 수신자 단말기로 배포되며, 상기 익명 메시지를 작성한 작성자의 실명이 상기 작성자의 실명 공개 요청에 따라 상기 블록 체인을 통해 공개되는 것을 특징으로 하는 검증 서버에서 익명 메시지 서비스 제공 방법이 제공된다.

[0009] 상기 익명 메시지 ID 요청을 위한 데이터에 대한 송수신 단계 (a)는, 상기 작성자의 ID(UID), 상기 작성자 및 상기 수신자를 멤버로 하는 그룹의 그룹키(GK)로 상기 작성자가 작성한 메시지의 내용(TEXT)을 암호화한 값(GK(TEXT)), 상기 TEXT의 해시값(H(TEXT)), 및 상기 TEXT가 작성된 시간(TS(TEXT))를 상기 작성자 단말기로부터 수신하는 단계 (a1); 상기 메시지의 ID(MID), 상기 MID의 생성 시간(TS(MID)) 및 상기 메시지의 번호(Msg_No)를 생성하는 단계 (a2); 익명성 검증을 위해, 상기 H(TEXT), 상기 MID 및 상기 TS(MID)를 해시한 해시값(H(H(TEXT), MID, TS(MID)))을 생성하는 단계 (a3); 및 상기 생성된 H(TEXT), MID, TS(MID) 및 Msg_No를 상기 작성자와 상기 검증 서버가 공유하는 대칭키(KVS-A)로 암호화하여 상기 작성자 단말기로 전송하는 단계 (a4);를 포함할 수 있다.

[0010] 상기 작성자 단말기로부터 수신된 UID, GK(TEXT), H(TEXT) 및 TS(TEXT)는 상기 대칭키(KVS-A)로 암호화된 값일 수 있다.

[0011] 상기 단계 (a1) 이전에, 상기 작성자 단말기는 상기 TEXT 및 상기 H(TEXT)를 상기 작성자 단말기의 DB 테이블(TABLE_A)에 저장하고, 상기 단계 (a4) 이후에, 상기 작성자 단말기는 상기 대칭키(KVS-A)를 이용하여 상기 검증 서버에서 전송받은 H(TEXT), MID, TS(MID) 및 Msg_No의 암호화된 값을 복호화하고, 상기 TABLE_A에 저장된 H(TEXT)와 상기 복호화된 H(TEXT)를 비교하여 일치하는 경우, 상기 복호화된 MID, TS(MID), Msg_No를 상기 TABLE_A에 저장할 수 있다.

[0012] 상기 블록 체인에 의한 블록 업데이트와 익명 메시지 수신과 관련된 데이터에 대한 송수신 단계 (b)는, 상기 단계 (a1)에서 수신된 GK(TEXT), H(TEXT), TS(TEXT)와, 상기 단계 (a2)에서 생성된 Msg_No와, 상기 단계 (a3)에서 생성된 H(H(TEXT), MID, TS(MID))를 포함하는 제1 트랜잭션을 생성하는 단계 (b1); 및 상기 생성된 제1 트랜잭션을 상기 블록 체인 시스템에 전송하는 단계 (b2);를 포함하되, 상기 블록 체인 시스템은 상기 전송된 제1 트랜잭션에 기초하여 제1 블록을 생성하고, 상기 생성된 제1 블록은 상기 블록 체인에 등록되어 전파될 수 있다.

[0013] 상기 수신자 단말기 각각은, 상기 제1 블록의 상기 제1 트랜잭션에서 GK(TEXT) 및 H(TEXT)를 추출하고, 상기 GK를 이용해 상기 추출된 GK(TEXT)를 복호화하여 TEXT를 추출하고, 상기 추출된 TEXT에 대해 H(TEXT)를 생성하며, 상기 생성된 H(TEXT)와 상기 추출된 H(TEXT)를 비교하여 TEXT의 무결성을 검증하며 TEXT를 수신할 수 있다.

[0014] 상기 익명 메시지의 실명 공개 요청에 의한 데이터에 대한 송수신 단계 (c)는, 상기 작성자 단말기에서 전송된 UID, Msg_No, 및 GK(MID, H(TEXT), TS(MID))를 수신하는 단계 (c1); 상기 수신된 UID, Msg_No, GK(MID, H(TEXT), TS(MID))을 포함하는 제2 트랜잭션을 생성하는 단계 (c2); 상기 생성된 제2 트랜잭션을 상기 블록 체인 시스템에 전송하는 단계 (c3);를 포함하되, 상기 블록 체인 시스템은 상기 전송된 제2 트랜잭션에 기초하여 제2 블록을 생성하고, 상기 생성된 제2 블록은 상기 블록 체인에 등록되어 전파될 수 있다.

[0015] 상기 수신자 단말기 각각은, 상기 제2 블록의 제2 트랜잭션의 Msg_No에 기초하여 상기 제1 블록을 검색하고, 상기 제1 블록 내의 제1 트랜잭션에서 H(TEXT) 및 H(H(TEXT), MID, TS(MID))를 추출하고, 상기 제2 블록의 상기 제2 트랜잭션에서 추출된 MID, TS(MID)와 상기 제1 블록 내의 제1 트랜잭션에서 추출된 H(TEXT)의 해시값 H(H(TEXT), MID, TS(MID)를 생성하고 상기 추출된 H(H(TEXT), MID, TS(MID)와 상기 생성된 H(H(TEXT), MID, TS(MID)을 비교하여 일치하면 상기 작성자가 공개될 수 있다.

[0016] 상기 작성자 단말기로부터 수신된 UID, Msg_No, 및 GK(MID, H(TEXT), TS(MID)는 상기 대칭키(KVS-A)로 암호화된 값일 수 있다.

[0017] 또한, 본 발명의 다른 실시예에 따르면, 익명 메시지 서비스 제공을 위한 검증 서버에 있어서, 익명 메시지를 작성한 작성자 단말기, 수신자 단말기 또는 블록 체인 시스템과 상기 검증 서버를 연결하는 통신부; 및 익명 메시지 ID 요청을 위한 데이터, 블록 체인에 의한 블록 업데이트와 익명 메시지 수신과 관련된 데이터, 및 익명 메시지의 실명 공개 요청에 의한 데이터 중 적어도 하나를 상기 작성자 단말기, 상기 수신자 단말기 및 상기 블록 체인 시스템과 송수신하는 메시지부;를 포함하되, 상기 블록 체인에 따른 블록 전파를 통해 상기 익명 메시지가 상기 수신자 단말기로 배포되며, 상기 익명 메시지를 작성한 작성자의 실명이 상기 작성자의 실명 공개 요청에 따라 상기 블록 체인을 통해 공개되는 것을 특징으로 하는 검증 서버가 제공된다.

[0018] 또한, 본 발명의 다른 실시예에 따르면, 익명 메시지 서비스를 제공하는 컴퓨팅 장치에 있어서, 그룹의 사용자 단말기들로 대화창과 관련된 정보를 제공하는 제 1 수단; 상기 사용자 단말기들 중 적어도 하나에서 상기 대화창에 익명 메시지가 입력 가능하고 실명 공개가 가능하도록 익명 메시지 ID 요청 동작 및 블록 체인에 의한 블록 업데이트와 익명 메시지 수신 동작을 수행하는 제 2 수단; 및 상기 익명 메시지 작성자의 실명이 상기 대화창에 공개 가능하도록 익명 메시지 실명 공개 동작을 수행하는 제 3 수단을 포함하되, 상기 블록 체인에 따른 블록 전파를 통해 상기 익명 메시지가 상기 수신자 단말기로 배포되며, 상기 익명 메시지를 작성한 작성자의 실명이 상기 작성자의 실명 공개 요청에 따라 상기 블록 체인을 통해 공개되는 것을 특징으로 하는 컴퓨팅 장치가 제공된다.

발명의 효과

[0019] 본 발명에 따르면, 익명 메시지를 대화창으로 입력할 수 있으므로, 자신을 노출시키길 원하지 않을 때 유용하게 활용할 수 있고, 대화 서비스에 새로운 흥미를 부여할 수 있다. 서비스 사업자 관점에서는, 익명 서비스를 제공하는 시스템은 새로운 흥미의 창출로 가입자의 증가를 유도할 수 있다.

[0020] 또한, 시스템이 모든 익명 메시지를 암호화하여 전송하고 메시지에 대한 익명성을 보장하기 위해 메시지 서버와 검증 서버를 분리하여 구성하므로, 기밀성(confidentiality), 무결성(integrity), 익명성(anoymity), 재전송 공격(replay attack) 방지 및 중간자 공격(man-in-the-middle attack) 방지를 제공할 수 있다.

[0021] 또한, 본 발명의 효과는 상기한 효과로 한정되는 것은 아니며, 본 발명의 상세한 설명 또는 특허청구범위에 기재된 발명의 구성으로부터 추론 가능한 모든 효과를 포함하는 것으로 이해되어야 한다.

도면의 간단한 설명

[0022] 도 1 및 도 2는 본 발명의 일 실시예에 따른 익명 메시지 서비스를 제공하는 과정을 도시한 도면들이다.

도 3은 본 발명의 일 실시예에 따른 익명 메시지 서비스를 제공하는 시스템을 개략적으로 도시한 도면이다.

도 4는 본 발명의 일 실시예에 따른 작성자가 보유한 키들을 도시한 도면이다.

도 5는 본 발명의 일 실시예에 따른 블록 체인의 개념을 도시한 도면이다.

도 6은 본 발명의 일 실시예에 따른 익명 메시지 작성 및 익명 메시지 아이디 요청 과정을 도시한 도면이다.

도 7은 본 발명의 일 실시예에 따른 블록체인에 의한 블록 업데이트와 익명 메시지 수신 과정을 도시한 도면이

다.

도 8은 본 발명의 일 실시예에 따른 익명 메시지의 실명 공개 요청 과정을 도시한 도면이다

도 9는 본 발명의 일 실시예에 따른 검증 서버를 도시한 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0023] 본 명세서에서 사용되는 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "구성된다" 또는 "포함한다" 등의 용어는 명세서상에 기재된 여러 구성 요소들, 또는 여러 단계들을 반드시 모두 포함하는 것으로 해석되지 않아야 하며, 그 중 일부 구성 요소들 또는 일부 단계들은 포함되지 않을 수도 있고, 또는 추가적인 구성 요소 또는 단계들을 더 포함할 수 있는 것으로 해석되어야 한다. 또한, 명세서에 기재된 "...부", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어 또는 소프트웨어로 구현되거나 하드웨어와 소프트웨어의 결합으로 구현될 수 있다.

[0024] 이하, 본 발명의 다양한 실시예들을 첨부된 도면을 참조하여 상술한다.

[0026] 본 발명은 SNS, 채팅 어플리케이션, 메신저, 게시판 등과 같이 사용자들이 대화를 주고받을 수 있는 대화 서비스에서 메시지 보안과 익명 서비스를 제공하는 시스템 및 방법을 제공한다.

[0027] 특히, 본 발명의 시스템 및 방법은 블록 체인을 활용하여 그룹 내 익명 메시지 작성, 전달과 검증 방법을 제시한다. 그룹 내 발생하는 메시지들은 트랜잭션으로 간주되어 블록 체인을 활용하여 그룹 내 사용자들에게 전달 및 기록될 수 있다. 작성자는 익명 메시지를 작성하며, 이후에 자신이 작성했음을 그룹 내 다른 사용자(수신자)에게 검증시켜 줄 수 있다. 또한, 보안 관점에서, 본 발명의 시스템은 기밀성(confidentiality), 무결성(integrity), 익명성(anoymity) 및 인증성 등을 제공할 수 있다.

[0028] 한편, 종래의 대화 서비스 중 일부 서비스는 비밀 대화 서비스를 제공하였다. 비밀 대화 서비스는 대화창에 입력된 모든 메시지가 저장되지 않고 사라지는 서비스로서, 비밀 대화 서비스의 대화창에 메시지 입력시 모든 메시지가 실명으로 입력된다. 즉, 종래의 대화 서비스는 대화창에서 익명으로 메시지를 입력할 수 있는 본 발명과 다르다.

[0030] 이하, 본 발명의 다양한 실시예들을 첨부된 도면을 참조하여 상술하기로 한다.

[0031] 도 1 및 도 2는 본 발명의 일 실시예에 따른 익명 메시지 서비스를 제공하는 과정을 도시한 도면들이다. 도 1 및 도 2는 예를 들어 SNS에서의 대화창을 도시한다.

[0032] 도 1을 참조하면, 대화창(100)에서 그룹 멤버들(A, B, D 등, 이하 "사용자들"이라 함)이 대화 영역(110)에 메시지를 입력하여 대화를 주고받고 있다. 메시지의 입력은 메시지 입력 영역(112)에 메시지를 입력하고 전송 버튼(114)을 선택함에 의해 실행된다.

[0033] 대화 영역(110)을 살펴보면, 사용자들 중 특정인이 익명 메시지(120a), "C양 나와?" 메시지를 입력하였음을 확인할 수 있다. 메시지가 입력되었음에도 어느 사용자가 입력하였는지를 대화 영역(110)에서 전혀 확인할 수가 없다.

[0034] 일 실시예에 따르면, 익명 메시지(120a)는 메시지 입력 영역(112)에 메시지를 입력하고, 익명 버튼(116) 및 전송 버튼(114)을 선택함에 의해 대화 영역(110)으로 입력될 수 있다.

[0035] 다른 실시예에 따르면, 익명 메시지(120a)는 메시지 입력 영역(112)에 메시지를 입력하고, 메시지 위에 마우스를 위치시킨 후 오른쪽 버튼을 누름에 의해 활성화되는 메뉴 중 익명 메시지 메뉴를 선택하고 전송 버튼(114)을 선택함에 의해 대화 영역(110)으로 입력될 수도 있다.

[0036] 또 다른 실시예에 따르면, 익명 메시지(120a)는 메시지 입력 영역(112)에 입력하여 전송 버튼(114)을 누르면 "익명 메시지로 메시지를 입력할까요?"라는 문의가 활성화되고 "YES"를 선택함에 의해 대화 영역(110)으로 입력될 수도 있다.

[0037] 또 다른 실시예에 따르면, 익명 메시지로 메시지를 보내도록 환경 설정에서 설정된 후, 사용자가 메시지 입력 영역(112)에 메시지를 입력하고 전송 버튼(114)을 선택함에 의해 대화 영역(110)으로 입력될 수 있다.

[0038] 즉, 익명 메시지(120a)의 입력 방법은 다양하게 변형될 수 있으며, 익명으로 메시지를 대화 영역(110)으로 입력할 수 있는 한 익명 메시지(120a) 입력 방법은 다양하게 변형될 수 있다. 특히, 익명 메시지(120a)의 입력을

위한 사용자 인터페이스(User Interface, UI)의 표시 형태, 배열, 설정 등은 서비스 제공자 또는 사용자의 편의성을 고려하여 다양하게 변형될 수 있다.

[0039] 다음으로, 작성자는 스스로 실명 공개를 요청할 수 있으며, 이 경우 익명 메시지(120a)가 실명 메시지(120b)로 변경될 수 있다. 여기서, 실명(도 2에서는 "D")은 사용자의 이름, 이미지 또는 캐릭터 등 사용자를 표시하는 모든 개체를 포함한다.

[0040] 실명 공개는 대화 영역(110)에 이미 입력한 익명 메시지들 전부를 실명 메시지로 전환하는 기술, 익명 메시지들 중 작성자의 요청에 의해 요청된 익명 메시지만 실명 메시지로 전환하는 기술 등을 포함할 수 있다.

[0041] 한편, 공개 버튼(118)을 선택하는 방법 외에도 마우스를 이용하는 방법, 환경 설정을 활용하는 방법 등 다양한 방법이 실명 공개 요청을 위해 사용될 수 있다.

[0042] 또한, 실명 메시지(120b)의 제공을 위한 UI의 표시 형태, 배열, 설정 등도 서비스 제공자 또는 사용자의 편의성을 고려하여 다양하게 변형될 수 있다.

[0043] 도 3은 본 발명의 일 실시예에 따른 익명 메시지 서비스를 제공하는 시스템을 개략적으로 도시한 도면이다.

[0044] 도 3을 참조하면, 본 실시예의 시스템(300)은 검증 서버(VS: Verification Server, 310), 복수의 단말기들(320-1, ... ,320-N) 및 블록 체인 시스템(330)를 포함한다. 여기서, 검증 서버(310) 및 복수의 단말기들(320-1, ... ,320-N)은 내부 프로세서를 통하여 메시지 등을 처리한다는 점에서, 컴퓨팅 장치로 통칭될 수 있다. 또한, 검증 서버(310), 복수의 단말기들(320-1, ... ,320-N), 및 블록 체인 시스템(330) 각각은 서로 무선 또는 유선으로 연결될 수 있다.

[0045] 검증 서버(310)는 검증 서버(Verification Server, 'VS'로 지칭)

[0046] 검증 서버는 메시지의 아이디(MID) 및 타임 스탬프(TS: Time Stamp)에 대한 생성 및 관리, 사용자 계정 관리, 암복호화를 위한 키 관리, 익명 메시지 작성자가 요청하는 실명 공개에 대한 검증 등의 역할을 수행한다.

[0047] 복수의 단말기들(320-1, ... ,320-N)은 그룹의 멤버들, 즉 사용자들이 사용하는 단말기들로서, 스마트폰, 태블릿 PC, 노트북, 개인용 PC, TV 등 메시지로 대화를 주고받을 수 있는 모든 단말기를 포함한다.

[0048] 이러한 사용자들은 동일한 그룹에 포함하되, 일반 메시지 또는 익명 메시지를 작성하는 작성자 및 작성자가 작성한 메시지를 수신하는 수신자로 분류될 수 있다. 즉, 그룹 대화 시 각 사용자들은 작성자 또는 수신자가 될 수 있다.

[0049] 블록 체인 시스템(330)는 복수의 블록 체인 서버(331)를 포함하며, 블록 체인에 기록될 수 있는 블록을 생성하는 역할을 수행한다. 이 때, 복수의 블록 체인 서버(331) 역시 컴퓨팅 장치로 통칭될 수 있다. 또한, 복수의 블록 체인 서버(331) 각각은 익명 메시지와 관련된 트랜잭션을 포함하는 블록 및 익명 메시지의 공개와 관련된 트랜잭션을 포함하는 블록을 생성할 수 있다. 이 때, 복수의 블록 체인 서버(331) 중 어느 하나의 블록 체인 서버(331)가 블록을 생성한다. 블록을 생성한 블록 체인 서버(331)는 생성 블록을 다른 블록 체인 서버(331)로 전송하며, 생성 블록은 복수의 블록 체인 서버(331)에 저장된 블록 체인에 기록된다.

[0050] 즉, 블록 체인 시스템(330)는 검증 서버(310)가 생성한 메시지인 트랜잭션을 그룹 내에 전파하고, 일정량의 트랜잭션이 모이면 블록을 생성하고 기록하는 역할을 수행하며, 블록들에 대한 관리를 수행한다. 작성자에 의해 작성된 메시지는 블록 체인에 의해 트랜잭션이 발생되고, 트랜잭션은 블록에 기록된다. 트랜잭션에는 아래에서 설명하는 바와 같이 GK(TEXT), H(TEXT), TS(send), H(H(TEXT), MID, TS(MID), UID, MID, TS(MID) 에 대한 정보가 기록된다. 이 때, GK(TEXT), H(TEXT), TS(send), H(H(TEXT), MID, TS(MID)에 대한 정보는 익명 메시지의 작성 시 사용되고, UID, MID, TS(MID)는 검증 시 사용된다.

[0051] 본 발명의 익명 메시지 서비스 제공 과정을 설명하기 전, 전제 및 각 엘리먼트들의 특성을 먼저 살펴보면 다음과 같다. 이 때, 설명의 편의를 위해, 검증 서버(310)를 "VS", 복수의 단말기들(320-1, ... ,320-N)을 "사용자들", 작성자가 소지한 단말기를 "작성자", 수신자가 소지한 단말기를 "수신자"로 각각 호칭하기로 한다.

[0053] 1. 전제

[0055] (1) VS, 작성자, 수신자는 모두 각각의 공개키와 개인키를 보유하고 있다.

[0056] (2) 작성자, 수신자는 동일한 그룹키(GK)를 공유하며, 그룹키(GK)는 그룹 내 전달되는 메시지의 암복호화에 사용한다.

[0057] (3) 작성자, 수신자는 VS와 상호간의 대칭키(KVS-USER)를 나누어 가지고 있다.

[0058] (4) 블록 생성 및 트랜잭션 전파는 블록 체인 시스템(330)이 담당한다.

[0059] (5) 사용자들은 그룹 내 고유한 사용자 ID(UID)를 갖고 있다.

[0061] 결과적으로 하나의 그룹 내의 컴포넌트들이 가지고 있는 키는 도 4에 도시된 바와 같다. 그리고, 블록 체인은 도 5와 같은 구조를 가진다.

[0062] 또한, 본 발명의 일 실시예에 따르면, 작성자는 자신이 작성한 메시지들에 대한 정보를 표 1와 같은 자신의 DB 테이블(TABLE_A)에 저장한다. 여기서, MID는 메시지의 ID, Msg_no는 메시지의 번호, TEXT는 메시지 내용, H( )는 해시 함수, TS는 타임 스탬프를 각각 의미한다.

표 1

TABLE_A
MID
Msg_No
TEXT
H(TEXT)
TS(MID)

[0064]

[0066] 2 프로토콜

[0068] 본 발명에 따른 프로토콜은 블록 체인을 이용한 메시지 교환에 있어서, 익명 메시지에 대한 익명성 보장 및 실명 검증을 보장한다. 즉, 익명의 메시지를 작성할 때 작성자의 익명성을 보장하고, 추후 익명 메시지를 작성한 작성자가 원할 때 메시지 작성자임을 증명할 수 있도록 동작된다. 또한 그룹 내의 사용자만이 메시지 읽기 및 쓰기가 가능하다

[0069] SNS 등에서 블록 체인을 활용하면, 블록 체인의 장점 즉, 중앙 서버의 통제나 관리 없이 투명하게 관리가 가능하다.

[0070] 본 발명에서 제안하는 프로토콜은 크게 3단계의 과정으로 구분된다. 이 때, 프로토콜 기술에 사용되는 기호는 표 2과 같다.

표 2

[0072]

기호	설명
VS	검증 서버
USER_A	익명 메시지를 작성하는 작성자
USER_X	익명 메시지를 수신하는 동일 그룹에 속한 유저(즉, 수신자)
KVS-A	검증 서버(VS)와 작성자(USER_A) 간의 대칭키
UID	작성자의 ID
MID	익명 메시지의 ID
TEXT	메시지의 내용
TABLE_A	작성자의 DB 테이블
TS	작성자의 MID 발급 요청 시간
TS(MID)	검증 서버(VS)의 MID 발급 시간
TS(TEXT)	TEXT가 작성된 시간
GK	그룹에 속해있는 사용자들이 공유하는 그룹키
H( )	해시 함수
Msg_No	익명 메시지 식별을 위한 메시지의 번호

[0074] 이하, 위의 기호들을 참조하여 프로토콜의 3단계 과정들을 첨부된 도면들을 참조하여 살펴보겠다.

[0075] 도 6은 본 발명의 일 실시예에 따른 익명 메시지 작성 및 익명 메시지 아이디 요청 과정을 도시한 도면이며, 도 7은 본 발명의 일 실시예에 따른 블록체인에 의한 블록 업데이트와 익명 메시지 수신 과정을 도시한 도면이고, 도 8은 본 발명의 일 실시예에 따른 익명 메시지의 실명 공개 요청 과정을 도시한 도면이다. 이하, 상기한 도면을 참조하여 각 과정을 설명하면 다음과 같다. 이 때, 설명의 편의를 위해 도면 부호는 생각하기로 한다.

[0077] 2.1. 익명 메시지 작성 및 익명 메시지 아이디 요청 과정

[0079] 본 과정은 작성자가 익명 메시지의 작성을 위해, 메시지 내용 작성 후 검증 서버에 메시지 ID 발급을 요청하는 과정이다. 검증 서버는 추후 실명 공개를 위한 필요한 추가 정보를 생성하고 작성자에게 전달한다. 모든 과정은 작성자와 검증 서버가 공유하는 대칭키(K_{VS-A})로 암복호화된다.

[0080] 이하, 도 6을 참조하여 구체적으로 살펴보면 다음과 같다.

[0081] 단계 1)에서, 작성자는 익명 메시지의 내용(TEXT)를 작성한다.

[0082] 단계 2)에서, 작성자는 작성한 메시지 내용(TEXT)와, TEXT의 해시값(H(TEXT))를 작성자의 DB 테이블(TABLE_A)에 저장한다.

[0083] 단계 3)에서, 작성자는 검증 서버에 익명 메시지 아이디(MID)의 발급을 요청한다. 이를 위해, 작성자는 그룹의 그룹키(GK)로 작성자가 작성한 메시지의 내용(TEXT)을 암호화한 값(GK(TEXT)), TEXT의 해시값(H(TEXT)), 및 TEXT가 작성된 시간(TS(TEXT))를 작성자와 검증 서버가 공유하는 대칭키(KVS-A)로 암호화하여 검증 서버로 전송한다.

[0084] 단계 4)에서, 검증 서버는 TS로 유효성을 체크하고(재전송 공격 여부 등), 유효한 경우 메시지의 ID(MID), 메시지 ID의 생성시간(TS(MID)) 및 메시지 번호(Msg_No)를 생성한다.

[0085] 단계 5)에서, 검증서버는 익명성 검증을 위해, H(TEXT), MID 및 TS(MID)를 해시한 해시값(H(H(TEXT), MID, TS(MID)))을 생성한다.

[0086] 단계 6)에서, 검증 서버는 H(TEXT), MID, TS(MID) 및 Msg_No를 작성자와 검증 서버가 공유하는 대칭키(KVS-A)로 암호화하여 작성자에게 전송한다.

[0087] 단계 7)에서, 작성자는 검증 서버로부터 전송받은 H(TEXT), MID, TS(MID) 및 Msg_No의 암호화된 값을 대칭키(KVS-A)를 이용하여 복호화하고, TABLE_A에 저장된 H(TEXT)와 복호화된 H(TEXT)를 비교하여 일치하는 경우, 복호화된 MID, TS(MID), Msg_No를 TABLE_A에 저장한다.

[0089] 2.2. 블록체인에 의한 블록 업데이트와 익명 메시지 수신 과정

[0091] 작성자가 작성한 익명 메시지를 그룹 내 배포를 위해 검증 서버는 블록 체인을 사용한다. 본 과정은 검증 서버가 익명 메시지에 대해 트랜잭션을 생성하면, 블록 체인 시스템은 트랜잭션을 블록에 기록하고, 블록 전파를 통해 그룹 내 사용자들에게 배포하는 과정이다.

[0092] 이하, 도 7를 참조하여 구체적으로 살펴보면 다음과 같다.

[0093] 단계 8)에서, 검증 서버는 작성자로부터 수신된 GK(TEXT), H(TEXT), TS(TEXT)와, 검증 서버에서 생성된 Msg_No 및 H(H(TEXT), MID, TS(MID))를 포함하는 제1 트랜잭션을 생성한다.

[0094] 단계 9)에서, 검증 서버는 생성된 제1 트랜잭션을 블록 체인 시스템에 전송한다. 즉, 단계 9)에서 트랜잭션이 전파된다.

[0095] 단계 10)에서, 블록 체인 시스템은 일장한 트랜잭션이 모이면 제1 블록을 생성하고 업로드한다.

[0096] 즉, 단계 9) 및 10)을 참조하면, 블록 체인 시스템은 전송된 제1 트랜잭션에 기초하여 제1 블록을 생성하고, 생성된 제1 블록은 블록 체인에 등록되어 전파된다.

[0097] 단계 11)에서, 작성자 및 수신자를 포함한 그룹의 사용자들은 제1 블록에서 해당 트랜잭션의 GK(TEXT)값에 대하여 그룹키(GK)로 복호화 후, TEXT에 대하여 H(TEXT)를 생성한다.

[0098] 즉, 사용자들은 제1 블록의 제1 트랜잭션에서 GK(TEXT) 및 H(TEXT)를 추출하고, 추출된 GK(TEXT)를 그룹키(GK)를 이용해 복호화하여 TEXT를 추출하고, 추출된 TEXT에 대해 H(TEXT)를 생성한다.

[0099] 단계 12)에서, 사용자들은 생성한 H(TEXT)와 제1 트랜잭션의 H(TEXT)값을 비교하여 메시지(TEXT)에 대한 무결성을 검증한다.

[0100] 단계 13)에서, 모든 수신자는 이러한 과정을 거쳐 익명의 작성자가 작성한 TEXT를 수신한다.

[0102] 2.3. 익명 메시지의 실명 공개 요청

[0104] 본 과정은 익명 메시지를 작성한 작성자가 추후 자신이 메시지를 작성했음을 공개하고자 할 때 수행되는 과정이다.

[0105] 이하, 도 8을 참조하여 구체적으로 살펴보면 다음과 같다.

[0106] 단계 14)에서, 작성자는 실명 공개 요청을 위해, UID, Msg_No, GK(MID, H(TEXT), TS(MID))를 작성자와 검증 서버가 공유하는 대칭키(KVS-A)로 암호화하여 검증 서버로 전송한다. 여기서, GK(MID, H(TEXT), TS(MID))는 MID와 H(TEXT)와 TS(MID)를 그룹키(GK)로 암호화한 값이다.

[0107] 단계 15)에서, 검증 서버는 UID, Msg_No, GK(MID, H(TEXT), TS(MID))을 포함하는 제2 트랜잭션을 생성한다.

[0108] 단계 16)에서, 제2 트랜잭션은 블록 체인에 따른 제2 블록을 통해 전파한다. 즉, 제2 트랜잭션은 블록 체인 시스템에 전송되며, 블록 체인 시스템은 제2 트랜잭션에 기초하여 제2 블록을 생성하고, 생성된 제2 블록은 블록 체인에 등록되어 전파된다.

[0109] 단계 17)에서, 수신자를 포함하는 그룹원은 Msg_No로 익명 메시지가 기록된 제1 블록에서 해당 익명 메시지에 대한 정보를 읽어 온다. 여기서 읽어온 정보는 GK(TEXT), H(TEXT), TS(send), H(H(TEXT), MID, TS(MID)), Msg_No를 의미한다.

[0110] 단계 18)에서, 수신자를 포함하는 그룹원은 Msg_No에 해당하는 MID, TS(MID)값과 제1 블록에 기록된 H(TEXT)을 이용하여 H(H(TEXT), MID, TS(MID))를 생성한다. 여기서의 Hash값은 무결성 검증을 위해 사용된다.

[0111] 단계 19)에서, 단계 18)에서 생성한 H(H(TEXT), MID, TS(MID))와, 제1 블록에 저장된 H(H(TEXT), MID, TS(MID))값을 비교하여 일치하면 단계 14)를 진행한 사용자가 익명 메시지에 대한 작성자임을 확인할 수 있다.

[0112] 즉, 단계 17) 내지 단계 19)에서, 수신자를 포함한 그룹원 각각은 제2 블록의 제2 트랜잭션의 Msg_No에 기초하여 제1 블록을 검색하고, 제1 블록 내의 제1 트랜잭션에서 H(TEXT) 및 H(H(TEXT), MID, TS(MID))를 추출하고, 제2 블록의 제2 트랜잭션에서 추출된 MID, TS(MID)와 제1 블록 내의 제1 트랜잭션에서 추출된 H(TEXT)의 해시값 H(H(TEXT), MID, TS(MID)를 생성하고, 추출된 H(H(TEXT), MID, TS(MID)와 생성된 H(H(TEXT), MID, TS(MID)을 비교하여 일치하면 작성자가 공개될 수 있다.

[0114] 한편, 위의 과정들은 위에 기술된 단계들로 제한되지는 않으며, 익명 메시지를 배포하고 익명 메시지의 작성자의 실명을 공개할 수 있는 한 다양하게 변형될 수 있다.

[0116] 도 9는 본 발명의 일 실시예에 따른 검증 서버를 도시한 블록도이다.

[0117] 도 9를 참조하면, 본 실시예의 검증 서버(310)는 제어부(311), 통신부(312), 메시지부(313), 암호화부(314), 검증부(315)를 포함할 수 있다.

[0118] 제어부(311)는 검증 서버(310)의 엘리먼트들의 전반적인 동작을 제어하며, 트랜잭션 기타 메시지의 송수신과 관련된 값들을 생성한다.

[0119] 통신부(312)는 복수의 단말기들(320) 및 블록 체인 시스템(330)와의 연결 통로이다.

[0120] 메시지부(313)는 메시지의 송수신과 관련된 전반적인 동작을 관리한다.

[0121] 암복호화부(314)는 데이터 송수신하는 모든 과정에서 데이터를 암복호화시킨다.

[0122] 검증부(315)는 유효성 여부를 확인한다.

[0123] (1) 익명 메시지 작성 및 익명 메시지 아이디 요청 과정에서, 메시지부(313)는 작성자의 ID(UID), 작성자 및 수신자를 멤버로 하는 그룹의 그룹키(GK)로 작성자가 작성한 메시지의 내용(TEXT)을 암호화한 값(GK(TEXT)), TEXT의 해시값(H(TEXT)), 및 TEXT가 작성된 시간(TS(TEXT))를 작성자로부터 수신한다. 이 때, 작성자로부터 수신된

UID, GK(TEXT), H(TEXT) 및 TS(TEXT)는 대칭키(KVS-A)로 암호화된 값이다.

[0124] 또한, 제어부(311)는 메시지의 ID(MID), MID의 생성 시간(TS(MID)) 및 메시지의 번호(Msg_No)를 생성하고, 익명성 검증을 위해, H(TEXT), MID 및 TS(MID)를 해시한 해시값(H(H(TEXT), MID, TS(MID)))을 생성한다.

[0125] 게다가, 메시지부(313)는 생성된 H(TEXT), MID, TS(MID) 및 Msg_No를 작성자와 검증 서버가 공유하는 대칭키(KVS-A)로 암호화하여 작성자에게 전송한다.

[0126] (2) 블록체인에 의한 블록 업데이트와 익명 메시지 수신 과정에서, 제어부(311)는 작성자로부터 수신된 GK(TEXT), H(TEXT), TS(TEXT)와, 생성된 Msg_No, H(H(TEXT), MID, TS(MID))를 포함하는 제1 트랜잭션을 생성한다.

[0127] 그 후, 메시지부(313)는 생성된 제1 트랜잭션을 블록 체인 시스템에 전송한다.

[0128] (3) 익명 메시지의 실명 공개 요청에서, 메시지부(313)는 작성자로부터 전송된 UID, Msg_No, 및 GK(MID, H(TEXT), TS(MID))를 수신한다.

[0129] 또한, 제어부(311)는 수신된 UID, Msg_No, GK(MID, H(TEXT), TS(MID))을 포함하는 제2 트랜잭션을 생성한다.

[0130] 그 후, 메시지부(313)는 생성된 제2 트랜잭션을 블록 체인 시스템에 전송한다.

[0131] 한편, 상기한 과정들의 상세한 설명은 위에서 상술하였으므로, 설명은 생략한다.

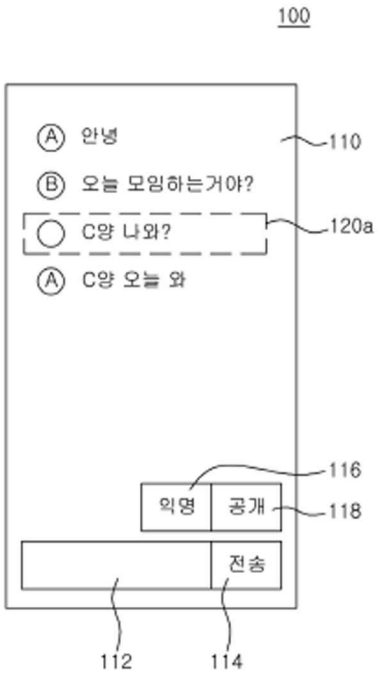
[0133] 또한, SNS 등의 프로그램 관점에서 살펴보면, 익명 메시지 서비스를 제공하는 컴퓨팅 장치(검증 서버)는 그룹의 사용자 단말기들로 대화창과 관련된 정보를 제공하는 제 1 수단, 사용자 단말기들 중 적어도 하나에서 대화창에 익명 메시지가 입력 가능하고 실명 공개가 가능하도록 익명 메시지 ID 요청 동작 및 블록 체인에 의한 블록 업데이트와 익명 메시지 수신 동작을 수행하는 제 2 수단, 및 익명 메시지 작성자의 실명이 대화창에 공개 가능하도록 익명 메시지 실명 공개 동작을 수행하는 제 3 수단을 포함한다. 상기한 과정들의 상세한 설명은 위에서 상술하였으므로, 설명은 생략한다.

[0135] 본 발명의 실시예들은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 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 본 발명의 일 실시예들의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

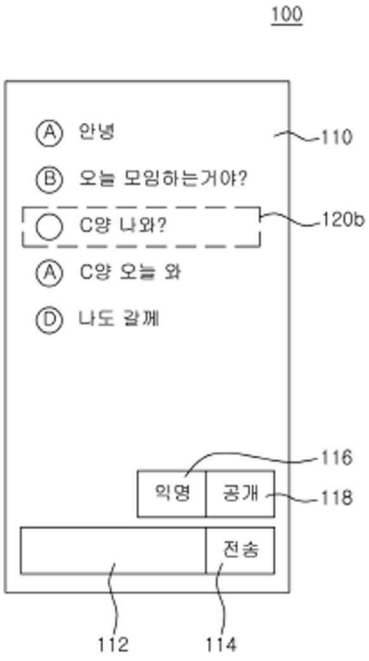
[0136] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

도면

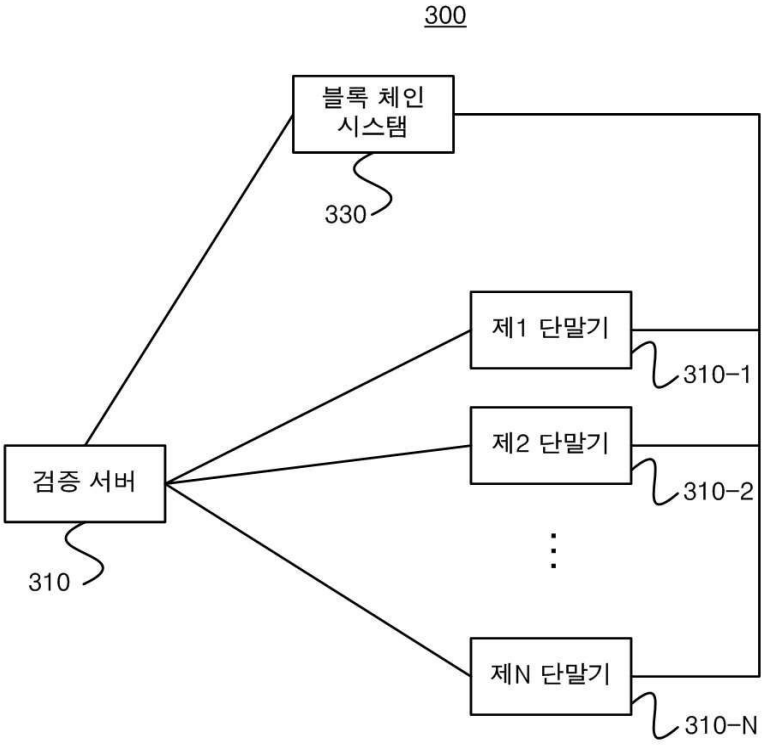
도면1


100
Ⓐ 안녕
110
Ⓑ 오늘 모임하는거야?
C양 나와?
120a
Ⓐ C양 오늘 와
116
익명
공개
118
전송
112
114

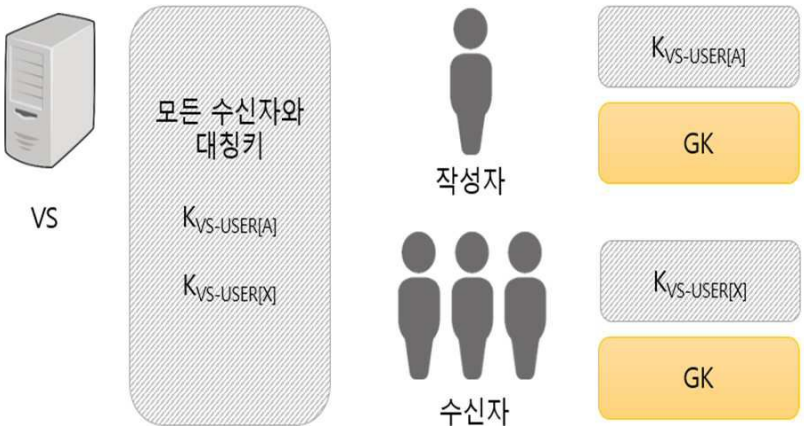
도면2


100
Ⓐ 안녕
110
Ⓑ 오늘 모임하는거야?
C양 나와?
120b
Ⓐ C양 오늘 와
Ⓓ 나도 갈께
116
익명
공개
118
전송
112
114

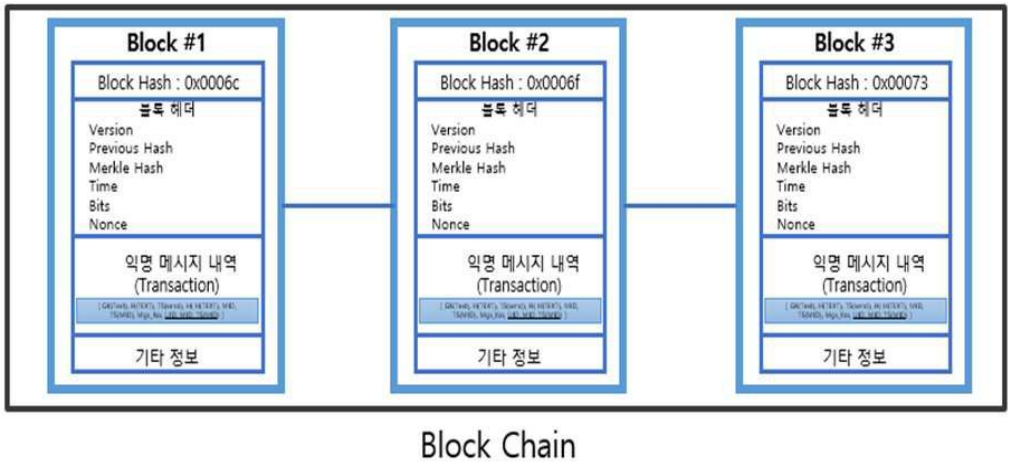
도면3


300
블록 체인 시스템
330
제1 단말기
310-1
제2 단말기
310-2
검증 서버
310
제N 단말기
310-N

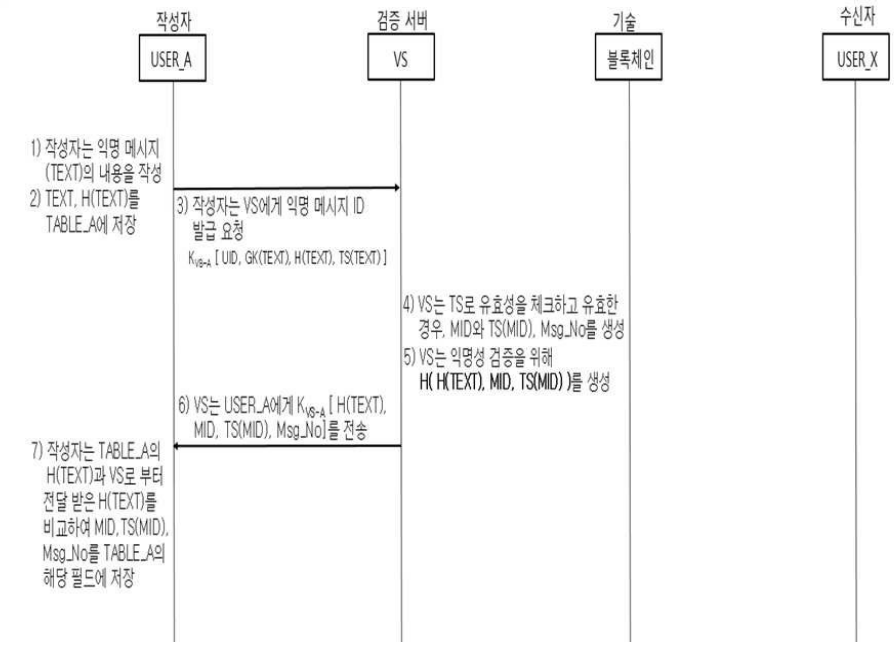
도면4


VS
모든 수신자와 대칭키
$K_{VS-USER[A]}$
$K_{VS-USER[X]}$
작성자
수신자
$K_{VS-USER[A]}$
GK
$K_{VS-USER[X]}$
GK

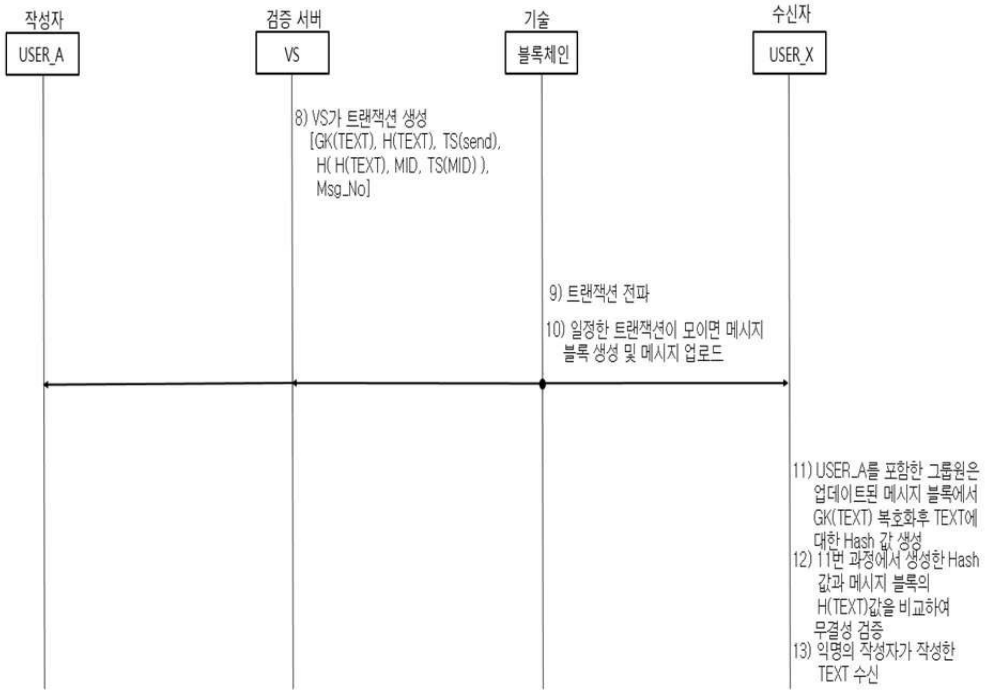
도면5


Block #1
Block Hash : 0x0006c
블록 헤더
Version
Previous Hash
Merkle Hash
Time
Bits
Nonce
익명 메시지 내역
(Transaction)
기타 정보
Block #2
Block Hash : 0x0006f
블록 헤더
Version
Previous Hash
Merkle Hash
Time
Bits
Nonce
익명 메시지 내역
(Transaction)
기타 정보
Block #3
Block Hash : 0x00073
블록 헤더
Version
Previous Hash
Merkle Hash
Time
Bits
Nonce
익명 메시지 내역
(Transaction)
기타 정보
Block Chain

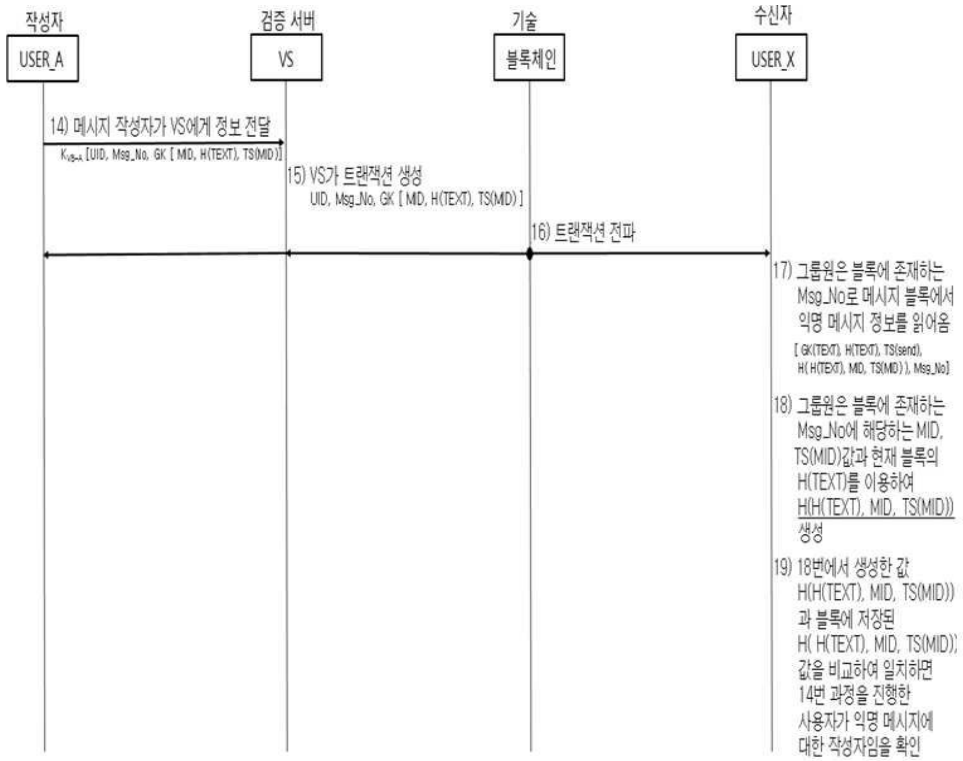
도면6


작성자
USER_A
검증 서버
VS
기술
블록체인
수신자
USER_X
1) 작성자는 익명 메시지 (TEXT)의 내용을 작성
2) TEXT, H(TEXT)를 TABLE_A에 저장
3) 작성자는 VS에게 익명 메시지 ID 발급 요청
K_{VS-A} [UID, GK(TEXT), H(TEXT), TS(TEXT)]
4) VS는 TS로 유효성을 체크하고 유효한 경우, MID와 TS(MID), Msg_No를 생성
5) VS는 익명성 검증을 위해 H(H(TEXT), MID, TS(MID))를 생성
6) VS는 USER_A에게 K_{VS-A} [H(TEXT), MID, TS(MID), Msg_No]를 전송
7) 작성자는 TABLE_A의 H(TEXT)과 VS로 부터 전달 받은 H(TEXT)를 비교하여 MID, TS(MID), Msg_No를 TABLE_A의 해당 필드에 저장

도면7


작성자
USER_A
검증 서버
VS
기술
블록체인
수신자
USER_X
8) VS가 트랜잭션 생성
[GK(TEXT), H(TEXT), TS(send),
H(H(TEXT), MID, TS(MID)),
Msg_No]
9) 트랜잭션 전파
10) 일정한 트랜잭션이 모이면 메시지
블록 생성 및 메시지 업로드
11) USER_A를 포함한 그룹원은
업데이트된 메시지 블록에서
GK(TEXT) 복호화후 TEXT에
대한 Hash 값 생성
12) 11번 과정에서 생성한 Hash
값과 메시지 블록의
H(TEXT)값을 비교하여
무결성 검증
13) 익명의 작성자가 작성한
TEXT 수신

도면8


작성자
USER_A
검증 서버
VS
기술
블록체인
수신자
USER_X
14) 메시지 작성자가 VS에게 정보 전달
[UID, Msg_No, GK [MID, H(TEXT), TS(MID)]
15) VS가 트랜잭션 생성
UID, Msg_No, GK [MID, H(TEXT), TS(MID)]
16) 트랜잭션 전파
17) 그룹원은 블록에 존재하는
Msg_No로 메시지 블록에서
익명 메시지 정보를 읽어옴
[GK(TEXT), H(TEXT), TS(send),
H(H(TEXT), MID, TS(MID)), Msg_No]
18) 그룹원은 블록에 존재하는
Msg_No에 해당하는 MID,
TS(MID)값과 현재 블록의
H(TEXT)를 이용하여
H(H(TEXT), MID, TS(MID))
생성
19) 18번에서 생성한 값
H(H(TEXT), MID, TS(MID))
과 블록에 저장된
H(H(TEXT), MID, TS(MID))
값을 비교하여 일치하면
14번 과정을 진행한
사용자가 익명 메시지에
대한 작성자임을 확인

도면9