(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0083178
(43) 공개일자 2020년07월08일

(51) 국제특허분류(Int. Cl.)
G06Q 20/38 (2012.01) *G06Q 20/16* (2012.01)
H04L 9/06 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
G06Q 20/382 (2013.01)
G06Q 20/16 (2013.01)
(21) 출원번호 10-2019-0114269(분할)
(22) 출원일자 2019년09월17일
심사청구일자 없음
(62) 원출원 특허 10-2018-0174278
원출원일자 2018년12월31일
심사청구일자 2018년12월31일

(71) 출원인
주식회사 코인플러그
경기도 성남시 분당구 판교역로146번길 20, 오피스에이치 11층 (백현동)
(72) 발명자
어준선
경기도 성남시 분당구 느티로 22 ,B동1710호(정자동,백궁동양파라곤)
송주한
경기도 성남시 분당구 느티로 22, A동 2114호(정자동, 백궁동양파라곤)
(74) 대리인
특허법인 수

전체 청구항 수 : 총 20 항

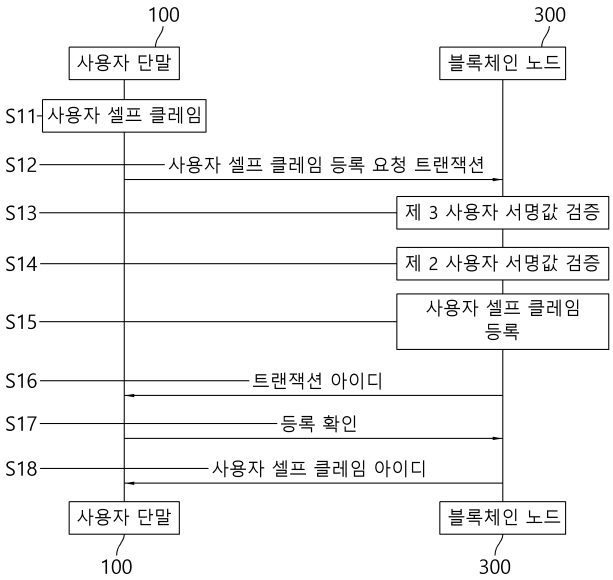
(54) 발명의 명칭 **블록체인 네트워크를 이용하여 사용자의 아이덴티티를 관리하는 방법 및 서버, 그리고, 블록체인 네트워크 기반의 사용자 아이덴티티를 이용하여 사용자를 인증하는 방법 및 단말**

(57) 요 약

본 발명은 블록체인 네트워크를 이용하여 사용자의 아이덴티티를 관리하는 방법에 있어서, (a) 사용자 단말로부터의 사용자 어드레스를 이용한 사용자 아이디 생성 데이터와 상기 사용자 아이디 생성 데이터를 사용자 마스터 프라이빗 키로 서명한 제1 사용자 서명값을 포함하는 사용자 아이디 생성 트랜잭션이 획득되면, 블록체인 네트워

(뒷면에 계속)

대 표 도 - 도3a



크를 구성하는 다수의 블록체인 노드들 중 적어도 하나의 블록체인 노드가, 상기 제1 사용자 서명값을 검증하여 상기 제1 사용자 서명값이 유효한 것으로 확인되면, 상기 블록체인 네트워크의 분산원장에 등록된 아이디 관리 컨트랙트를 실행하여 사용자 아이덴티티들에 대한 클레임을 생성하도록 하는 사용자 클레임 스마트 컨트랙트를 상기 분산원장에 등록하도록 하고, 상기 사용자 클레임 스마트 컨트랙트를 상기 분산원장에 등록하도록 하는 사용자 클레임 스마트 컨트랙트 등록 트랜잭션에 대응되는 사용자 클레임 스마트 컨트랙트 등록 트랜잭션 아이디를 상기 사용자 단말로 전송함으로써, 상기 사용자 단말로 하여금 상기 사용자 클레임 스마트 컨트랙트 등록 트랜잭션 아이디를 이용하여 상기 분산원장에 등록된 상기 사용자 클레임 스마트 컨트랙트의 어드레스를 사용자 아이디로 획득하도록 하는 단계; 및 (b) 상기 사용자 단말로부터의 사용자 셀프 클레임 등록 요청 트랜잭션 - 상기 사용자 셀프 클레임 등록 요청 트랜잭션은 상기 사용자 아이디, 상기 사용자 아이덴티티들을 가공한 사용자 특정값, 및 상기 사용자 아이디와 상기 사용자 특정값을 사용자 프라이빗 키로 서명한 제2 사용자 서명값을 포함하는 사용자 셀프 클레임 데이터와, 상기 사용자 셀프 클레임 데이터를 상기 사용자 마스터 프라이빗 키로 서명한 제3 사용자 서명값을 포함함 - 이 획득되면, 상기 적어도 하나의 블록체인 노드가, 상기 제3 사용자 서명값을 검증하여 상기 제3 사용자 서명값이 유효한 것으로 확인되면, 상기 사용자 아이디에 대응되는 상기 사용자 클레임 스마트 컨트랙트를 실행하여 상기 사용자 셀프 클레임 데이터에 대응하는 사용자 셀프 클레임이 상기 분산원장에 등록되도록 하며, 상기 분산원장에 등록된 상기 사용자 셀프 클레임에 대응되는 사용자 셀프 클레임 트랜잭션 아이디가 상기 사용자 단말로 전송되도록 하는 단계; 를 포함하는 방법에 관한 것이다.

(52) CPC특허분류
H04L 9/0643 (2013.01)
H04L 9/3263 (2013.01)
H04L 2209/38 (2013.01)

명 세 서

청구범위

청구항 1

블록체인 네트워크를 이용하여 사용자의 아이덴티티를 관리하는 방법에 있어서,

(a) 사용자 단말로부터의 사용자 어드레스를 이용한 사용자 아이디 생성 데이터와 상기 사용자 아이디 생성 데이터를 사용자 마스터 프라이빗 키로 서명한 제1 사용자 서명값을 포함하는 사용자 아이디 생성 트랜잭션이 획득되면, 블록체인 네트워크를 구성하는 다수의 블록체인 노드들 중 적어도 하나의 블록체인 노드가, 상기 제1 사용자 서명값을 검증하여 상기 제1 사용자 서명값이 유효한 것으로 확인되면, 상기 블록체인 네트워크의 분산원장에 등록된 아이디 관리 컨트랙트를 실행하여 사용자 아이덴티티들에 대한 클레임을 생성하도록 하는 사용자 클레임 스마트 컨트랙트를 상기 분산원장에 등록하도록 하고, 상기 사용자 클레임 스마트 컨트랙트를 상기 분산원장에 등록하도록 하는 사용자 클레임 스마트 컨트랙트 등록 트랜잭션에 대응되는 사용자 클레임 스마트 컨트랙트 등록 트랜잭션 아이디를 상기 사용자 단말로 전송함으로써, 상기 사용자 단말로 하여금 상기 사용자 클레임 스마트 컨트랙트 등록 트랜잭션 아이디를 이용하여 상기 분산원장에 등록된 상기 사용자 클레임 스마트 컨트랙트의 어드레스를 사용자 아이디로 획득하도록 하는 단계; 및

(b) 상기 사용자 단말로부터의 사용자 셀프 클레임 등록 요청 트랜잭션 - 상기 사용자 셀프 클레임 등록 요청 트랜잭션은 상기 사용자 아이디, 상기 사용자 아이덴티티들을 가공한 사용자 특정값, 및 상기 사용자 아이디와 상기 사용자 특정값을 사용자 프라이빗 키로 서명한 제2 사용자 서명값을 포함하는 사용자 셀프 클레임 데이터와, 상기 사용자 셀프 클레임 데이터를 상기 사용자 마스터 프라이빗 키로 서명한 제3 사용자 서명값을 포함함 - 이 획득되면, 상기 적어도 하나의 블록체인 노드가, 상기 제3 사용자 서명값을 검증하여 상기 제3 사용자 서명값이 유효한 것으로 확인되면, 상기 사용자 아이디에 대응되는 상기 사용자 클레임 스마트 컨트랙트를 실행하여 상기 사용자 셀프 클레임 데이터에 대응하는 사용자 셀프 클레임이 상기 분산원장에 등록되도록 하며, 상기 분산원장에 등록된 상기 사용자 셀프 클레임에 대응되는 사용자 셀프 클레임 트랜잭션 아이디가 상기 사용자 단말로 전송되도록 하는 단계;

를 포함하는 방법.

청구항 2

제1항에 있어서,

상기 사용자 특정값은, 상기 사용자 아이덴티티들 각각에 대한 해시값들이 각각의 리프 노드들 중 적어도 일부에 할당된 머클트리의 루트 해시값인 것을 특징으로 하는 방법.

청구항 3

제1항에 있어서,

상기 (a) 단계에서,

상기 적어도 하나의 블록체인 노드는, 상기 분산원장에 등록된 디지털 서명 검증 모듈을 실행하여 상기 제1 사용자 서명값과 상기 사용자 아이디 생성 데이터를 참조하여 상기 사용자 마스터 프라이빗 키에 대응되는 사용자 마스터 퍼블릭 키를 획득하도록 하며, 상기 사용자 마스터 퍼블릭 키를 이용하여 상기 제1 사용자 서명값으로부터 확인되는 제1 비교 대상 데이터와 상기 사용자 아이디 생성 데이터가 일치하는 지를 확인함으로써 상기 제1 사용자 서명값이 유효한지를 검증하는 것을 특징으로 하는 방법.

청구항 4

제1항에 있어서,

상기 (a) 단계에서,

상기 사용자 아이디 생성 트랜잭션은 상기 사용자 마스터 프라이빗 키에 대응되는 사용자 마스터 퍼블릭 키를

더 포함하며,

상기 적어도 하나의 블록체인 노드가, 상기 사용자 마스터 퍼블릭 키를 이용하여 상기 제1 사용자 서명값으로부터 확인되는 제1 비교 대상 데이터와 상기 사용자 아이디 생성 데이터가 일치하는 지를 확인함으로써 상기 제1 사용자 서명값이 유효한지를 검증하는 것을 특징으로 하는 방법.

청구항 5

제1항에 있어서,

상기 (b) 단계에서,

상기 적어도 하나의 블록체인 노드는,

상기 제3 사용자 서명값 검증 이후, 상기 분산원장에 상기 사용자 셀프 클레임에 대응되는 이전 등록된 이전 사용자 셀프 클레임이 있는지를 확인하며, 이전 사용자 셀프 클레임이 등록된 상태일 경우, 상기 사용자 셀프 클레임을 상기 분산원장에 등록하되, 상기 사용자 셀프 클레임이 상기 사용자 아이디에 대응되도록 상기 분산원장의 상태 데이터베이스를 업데이트하는 것을 특징으로 하는 방법.

청구항 6

제1항에 있어서,

상기 사용자 아이덴티티들은 사용자를 식별하기 위한 특징 정보들을 포함하며, 상기 특징 정보들은 상기 사용자 단말에 저장된 것을 특징으로 하는 방법.

청구항 7

제1항에 있어서,

상기 (b) 단계에서,

상기 적어도 하나의 블록체인 노드는, 상기 분산원장에 등록된 디지털 서명 검증 모듈을 실행하여 상기 제3 사용자 서명값과 상기 사용자 셀프 클레임 데이터를 참조하여 상기 사용자 마스터 프라이빗 키에 대응되는 사용자 마스터 퍼블릭 키를 획득하도록 하며, 상기 사용자 마스터 퍼블릭 키를 이용하여 상기 제3 사용자 서명값으로부터 확인되는 제3 비교 대상 데이터와 상기 사용자 셀프 클레임 데이터가 일치하는지를 확인함으로써 상기 제3 사용자 서명값이 유효한지를 검증하는 것을 특징으로 하는 방법.

청구항 8

제1항에 있어서,

상기 (b) 단계에서,

상기 사용자 셀프 클레임 등록 요청 트랜잭션은, 상기 사용자 마스터 프라이빗 키에 대응되는 사용자 마스터 퍼블릭 키를 더 포함하며,

상기 적어도 하나의 블록체인 노드는, 상기 사용자 마스터 퍼블릭 키를 이용하여 상기 제3 사용자 서명값으로부터 확인되는 제3 비교 대상 데이터와 상기 사용자 셀프 클레임 데이터가 일치하는지를 확인함으로써 상기 제3 사용자 서명값이 유효한지를 검증하는 것을 특징으로 하는 방법.

청구항 9

제1항에 있어서,

상기 (b) 단계에서,

상기 적어도 하나의 블록체인 노드는, 상기 제3 사용자 서명값의 검증 이후, 상기 제2 사용자 서명값을 검증하여 상기 제2 사용자 서명값이 유효한 것으로 확인되면, 상기 사용자 클레임 스마트 컨트랙트를 실행하는 것을 특징으로 하는 방법.

청구항 10

제1항에 있어서,

상기 (a) 단계에서,

상기 적어도 하나의 블록체인 노드는, (i) 상기 사용자 아이디 생성 트랜잭션을 프록시 서버로부터 획득하되, 상기 프록시 서버로부터 상기 사용자 아이디 생성 트랜잭션과 상기 사용자 아이디 생성 트랜잭션을 상기 프록시 서버의 프록시 서버 마스터 프라이빗 키로 서명한 제1 프록시 서버 서명값을 획득하며, 상기 제1 프록시 서버 서명값을 검증하여 상기 제1 프록시 서버 서명값이 유효한 경우 상기 제1 사용자 서명값을 검증하며, (ii) 상기 사용자 클레임 스마트 컨트랙트 등록 트랜잭션 아이디를 상기 프록시 서버로 전송함으로써 상기 프록시 서버가 상기 사용자 클레임 스마트 컨트랙트 등록 트랜잭션 아이디를 상기 사용자 단말로 전송하도록 하고,

상기 (b) 단계에서,

상기 적어도 하나의 블록체인 노드는, (i) 상기 사용자 셀프 클레임 등록 요청 트랜잭션을 상기 프록시 서버로부터 획득하되, 상기 프록시 서버로부터 상기 사용자 셀프 클레임 등록 요청 트랜잭션과 상기 사용자 셀프 클레임 등록 요청 트랜잭션을 상기 프록시 서버의 상기 프록시 서버 마스터 프라이빗 키로 서명한 제2 프록시 서버 서명값을 획득하며, 상기 제2 프록시 서버 서명값을 검증하여 상기 제2 프록시 서버 서명값이 유효한 경우 상기 제3 사용자 서명값을 검증하며, (ii) 상기 사용자 셀프 클레임 트랜잭션 아이디를 상기 프록시 서버로 전송함으로써 상기 프록시 서버가 상기 사용자 셀프 클레임 트랜잭션 아이디를 상기 사용자 단말로 전송하도록 하는 것을 특징으로 하는 방법.

청구항 11

블록체인 네트워크를 이용하여 사용자의 아이덴티티를 관리하는 블록체인 네트워크의 블록체인 노드에 있어서,

사용자 아이덴티티를 관리하기 위한 인스트럭션들이 저장된 메모리; 및

상기 메모리에 저장된 상기 인스트럭션들에 따라 상기 사용자 아이덴티티를 관리하는 동작을 수행하는 프로세서;

를 포함하되,

상기 프로세서는,

(i) 사용자 단말로부터의 사용자 어드레스를 이용한 사용자 아이디 생성 데이터와 상기 사용자 아이디 생성 데이터를 사용자 마스터 프라이빗 키로 서명한 제1 사용자 서명값을 포함하는 사용자 아이디 생성 트랜잭션이 획득되면, 상기 제1 사용자 서명값을 검증하여 상기 제1 사용자 서명값이 유효한 것으로 확인되면, 상기 블록체인 네트워크의 분산원장에 등록된 아이디 관리 컨트랙트를 실행하여 사용자 아이덴티티들에 대한 클레임을 생성하도록 하는 사용자 클레임 스마트 컨트랙트를 상기 분산원장에 등록하도록 하고, 상기 사용자 클레임 스마트 컨트랙트를 상기 분산원장에 등록하도록 하는 사용자 클레임 스마트 컨트랙트 등록 트랜잭션에 대응되는 사용자 클레임 스마트 컨트랙트 등록 트랜잭션 아이디를 상기 사용자 단말로 전송함으로써, 상기 사용자 단말로 하여금 상기 사용자 클레임 스마트 컨트랙트 등록 트랜잭션 아이디를 이용하여 상기 분산원장에 등록된 상기 사용자 클레임 스마트 컨트랙트의 어드레스를 사용자 아이디로 획득하도록 하는 프로세스, 및 (ii) 상기 사용자 단말로부터의 사용자 셀프 클레임 등록 요청 트랜잭션 - 상기 사용자 셀프 클레임 등록 요청 트랜잭션은 상기 사용자 아이디, 상기 사용자 아이덴티티들을 가공한 사용자 특정값, 및 상기 사용자 아이디와 상기 사용자 특정값을 사용자 프라이빗 키로 서명한 제2 사용자 서명값을 포함하는 사용자 셀프 클레임 데이터와, 상기 사용자 셀프 클레임 데이터를 상기 사용자 마스터 프라이빗 키로 서명한 제3 사용자 서명값을 포함함 - 이 획득되면, 상기 제3 사용자 서명값을 검증하여 상기 제3 사용자 서명값이 유효한 것으로 확인되면, 상기 사용자 아이디에 대응되는 상기 사용자 클레임 스마트 컨트랙트를 실행하여 상기 사용자 셀프 클레임 데이터에 대응하는 사용자 셀프 클레임이 상기 분산원장에 등록되도록 하며, 상기 분산원장에 등록된 상기 사용자 셀프 클레임에 대응되는 사용자 셀프 클레임 트랜잭션 아이디가 상기 사용자 단말로 전송되도록 하는 프로세스를 수행하는 것을 특징으로 하는 블록체인 노드.

청구항 12

제11항에 있어서,

상기 사용자 특정값은, 상기 사용자 아이덴티티들 각각에 대한 해시값들이 각각의 리프 노드들 중 적어도 일부

에 할당된 머클트리의 루트 해시값인 것을 특징으로 하는 블록체인 노드.

청구항 13

제11항에 있어서,

상기 프로세서는,

상기 (i) 프로세스에서, 상기 분산원장에 등록된 디지털 서명 검증 모듈을 실행하여 상기 제1 사용자 서명값과 상기 사용자 아이디 생성 데이터를 참조하여 상기 사용자 마스터 프라이빗 키에 대응되는 사용자 마스터 퍼블릭 키를 획득하도록 하며, 상기 사용자 마스터 퍼블릭 키를 이용하여 상기 제1 사용자 서명값으로부터 확인되는 제1 비교 대상 데이터와 상기 사용자 아이디 생성 데이터가 일치하는 지를 확인함으로써 상기 제1 사용자 서명값이 유효한지를 검증하는 것을 특징으로 하는 블록체인 노드.

청구항 14

제11항에 있어서,

상기 사용자 아이디 생성 트랜잭션은 상기 사용자 마스터 프라이빗 키에 대응되는 사용자 마스터 퍼블릭 키를 더 포함하며,

상기 프로세서는,

상기 (i) 프로세스에서, 상기 사용자 마스터 퍼블릭 키를 이용하여 상기 제1 사용자 서명값으로부터 확인되는 제1 비교 대상 데이터와 상기 사용자 아이디 생성 데이터가 일치하는 지를 확인함으로써 상기 제1 사용자 서명값이 유효한지를 검증하는 것을 특징으로 하는 블록체인 노드.

청구항 15

제11항에 있어서,

상기 프로세서는,

상기 (ii) 프로세스에서, 상기 제3 사용자 서명값 검증 이후, 상기 분산원장에 상기 사용자 셀프 클레임에 대응되는 이전 등록된 이전 사용자 셀프 클레임이 있는지를 확인하며, 이전 사용자 셀프 클레임이 등록된 상태일 경우, 상기 사용자 셀프 클레임을 상기 분산원장에 등록하되, 상기 사용자 셀프 클레임이 상기 사용자 아이디에 대응되도록 상기 분산원장의 상태 데이터베이스를 업데이트하는 것을 특징으로 하는 블록체인 노드.

청구항 16

제11항에 있어서,

상기 사용자 아이덴티티들은 사용자를 식별하기 위한 특징 정보들을 포함하며, 상기 특징 정보들은 상기 사용자 단말에 저장된 것을 특징으로 하는 블록체인 노드.

청구항 17

제11항에 있어서,

상기 프로세서는,

상기 (ii) 프로세스에서, 상기 분산원장에 등록된 디지털 서명 검증 모듈을 실행하여 상기 제3 사용자 서명값과 상기 사용자 셀프 클레임 데이터를 참조하여 상기 사용자 마스터 프라이빗 키에 대응되는 사용자 마스터 퍼블릭 키를 획득하도록 하며, 상기 사용자 마스터 퍼블릭 키를 이용하여 상기 제3 사용자 서명값으로부터 확인되는 제3 비교 대상 데이터와 상기 사용자 셀프 클레임 데이터가 일치하는지를 확인함으로써 상기 제3 사용자 서명값이 유효한지를 검증하는 것을 특징으로 하는 블록체인 노드.

청구항 18

제11항에 있어서,

상기 사용자 셀프 클레임 등록 요청 트랜잭션은, 상기 사용자 마스터 프라이빗 키에 대응되는 사용자 마스터 퍼

블릭 키를 더 포함하며,

상기 프로세서는,

상기 (ii) 프로세스에서, 상기 사용자 마스터 퍼블릭 키를 이용하여 상기 제3 사용자 서명값으로부터 확인되는 제3 비교 대상 데이터와 상기 사용자 셀프 클레임 데이터가 일치하는지를 확인함으로써 상기 제3 사용자 서명값이 유효한지를 검증하는 것을 특징으로 하는 블록체인 노드.

청구항 19

제11항에 있어서,

상기 블록체인 노드는,

상기 (ii) 프로세스에서, 상기 제3 사용자 서명값의 검증 이후, 상기 제2 사용자 서명값을 검증하여 상기 제2 사용자 서명값이 유효한 것으로 확인되면, 상기 사용자 클레임 스마트 컨트랙트를 실행하는 것을 특징으로 하는 블록체인 노드.

청구항 20

제11항에 있어서,

상기 프로세서는,

상기 (i) 프로세스에서, (i-1) 상기 사용자 아이디 생성 트랜잭션을 프록시 서버로부터 획득하되, 상기 프록시 서버로부터 상기 사용자 아이디 생성 트랜잭션과 상기 사용자 아이디 생성 트랜잭션을 상기 프록시 서버의 프록시 서버 마스터 프라이빗 키로 서명한 제1 프록시 서버 서명값을 획득하며, 상기 제1 프록시 서버 서명값을 검증하여 상기 제1 프록시 서버 서명값이 유효한 경우 상기 제1 사용자 서명값을 검증하며, (i-2) 상기 사용자 클레임 스마트 컨트랙트 등록 트랜잭션 아이디를 상기 프록시 서버로 전송함으로써 상기 프록시 서버가 상기 사용자 클레임 스마트 컨트랙트 등록 트랜잭션 아이디를 상기 사용자 단말로 전송하도록 하고,

상기 (ii) 프로세스에서, (ii-1) 상기 사용자 셀프 클레임 등록 요청 트랜잭션을 상기 프록시 서버로부터 획득하되, 상기 프록시 서버로부터 상기 사용자 셀프 클레임 등록 요청 트랜잭션과 상기 사용자 셀프 클레임 등록 요청 트랜잭션을 상기 프록시 서버의 상기 프록시 서버 마스터 프라이빗 키로 서명한 제2 프록시 서버 서명값을 획득하며, 상기 제2 프록시 서버 서명값을 검증하여 상기 제2 프록시 서버 서명값이 유효한 경우 상기 제3 사용자 서명값을 검증하며, (ii-2) 상기 사용자 셀프 클레임 트랜잭션 아이디를 상기 프록시 서버로 전송함으로써 상기 프록시 서버가 상기 사용자 셀프 클레임 트랜잭션 아이디를 상기 사용자 단말로 전송하도록 하는 것을 특징으로 하는 블록체인 노드.

발명의 설명

기 술 분 야

[0001] 본 발명은 블록체인 네트워크를 이용하여 사용자의 아이덴티티를 관리하는 방법 및 서버, 그리고, 블록체인 네트워크 기반의 사용자 아이덴티티를 이용하여 사용자를 인증하는 방법 및 단말에 관한 것으로, 보다 상세하게는, 사용자 단말로부터의 사용자 어드레스를 이용한 사용자 아이디 생성 데이터와 사용자 아이디 생성 데이터를 사용자 마스터 프라이빗 키로 서명한 제1 사용자 서명값을 포함하는 사용자 아이디 생성 트랜잭션이 획득되면, 제1 사용자 서명값을 검증하여 제1 사용자 서명값이 유효한 것으로 확인되면, 블록체인 네트워크의 분산원장에 등록된 아이디 관리 컨트랙트를 실행하여 사용자 아이덴티티들에 대한 클레임을 생성하도록 하는 사용자 클레임 스마트 컨트랙트를 분산원장에 등록하도록 하고, 사용자 클레임 스마트 컨트랙트를 분산원장에 등록하도록 하는 사용자 클레임 스마트 컨트랙트 등록 트랜잭션에 대응되는 사용자 클레임 스마트 컨트랙트 등록 트랜잭션 아이디를 사용자 단말로 전송함으로써, 사용자 단말로 하여금 사용자 클레임 스마트 컨트랙트 등록 트랜잭션 아이디를 이용하여 분산원장에 등록된 사용자 클레임 스마트 컨트랙트의 어드레스를 사용자 아이디로 획득하도록 하며, 사용자 아이디, 사용자 아이덴티티들을 가공한 사용자 특정값, 및 사용자 아이디와 사용자 특정값을 사용자 프라이빗 키로 서명한 제2 사용자 서명값을 포함하는 사용자 셀프 클레임 데이터와, 사용자 셀프 클레임 데이터를 사용자 마스터 프라이빗 키로 서명한 제3 사용자 서명값을 포함하는 사용자 셀프 클레임 등록 요청 트랜잭션이 획득되면, 제3 사용자 서명값을 검증하여 제3 사용자 서명값이 유효한 것으로 확인되면, 사용자 아이디에 대응되는 사용자 클레임 스마트 컨트랙트를 실행하여 사용자 셀프 클레임 데이터에 대응하는 사용

자 셀프 클레임이 분산원장에 등록되도록 하며, 분산원장에 등록된 사용자 셀프 클레임에 대응되는 사용자 셀프 클레임 트랜잭션 아이디가 사용자 단말로 전송되도록 하는 블록체인 네트워크를 이용하여 사용자의 아이덴티티를 관리하는 방법 및 서버, 그리고, 블록체인 네트워크 기반의 사용자 아이덴티티를 이용하여 사용자를 인증하는 방법 및 단말에 관한 것이다.

배 경 기 술

[0002] 일반적인 거래 구조에서 생산기술, 교통 수단 등의 발전으로 거래의 대상이 늘어나고 거래의 범위가 넓어짐에 따라 거래의 구조는 점차 복잡해지고, 거래비용은 증가해 왔다. 또한, 직접 거래 대신 대부분의 거래가 간접적으로 이뤄짐에 따라, 거래의 당사자와 대상을 신뢰하기 위해 많은 비용이 필요해졌다.

[0003] 예를 들어, 거래 당사자를 신뢰하기 위해 신용 평가기관을 활용해 평가하고, 상품의 품질이나 가치를 보증하기 위해 인증서나 보증서, 제3자에 의한 담보 등이 필요하게 됐다. 또한 대금의 지급/결제의 안정성과 신뢰를 위한 금융 기관이나 계약을 보증하기 위한 공증이나 신뢰기관 등 무수히 많은 중간자가 등장하고, 신뢰의 비용이 발생하고 있다.

[0004] 특히, 사용자 인증을 위한 개인 인증서에 대한 정보는 인증 기관 등이 보유하고 있으므로, 본인 인증을 위한 인증서 정보를 확인하는 동안 해킹에 노출될 위험이 있을 수 있으므로, 이를 방지하기 위한 보안 강화를 위하여 여러 보안 프로그램을 이용하여야 하는 불편함이 있다.

[0005] 또한, 사용자 개인 인증서에 대한 정보를 보관하고 있는 인증 기관 등이 해킹 당하면 대량의 개인 정보가 해킹 당하는 피해도 발생하고 있다.

[0006] 한편, 종래 사용자 인증을 위한 개인 인증서 등의 인증 정보는 인증을 받은 각각의 인증 기관 등에 보관되게 되며, 사용자는 다수의 인증 기관 등에 보관된 각각의 인증 정보에 접근하기 위한 해당 인증 정보가 보관된 인증 기관을 매번 확인하여야 하는 불편함이 있으며, 각각의 인증 기관 등에 보관에 인증 정보에 대한 권한은 각각의 인증 기관이 소유하고 있어서 사용자가 자신의 인증 정보들을 용이하게 관리하는 데 어려움이 있다.

발명의 내용

해결하려는 과제

[0007] 본 발명은 상술한 문제점들을 모두 해결하는 것을 그 목적으로 한다.

[0008] 또한, 본 발명은 사용자 인증을 위한 각각의 사용자 아이덴티티들에 대한 권한을 사용자 자신이 소유할 수 있도록 하는 것을 다른 목적으로 한다.

[0009] 또한, 본 발명은 사용자 인증을 위한 각각의 사용자 아이덴티티들에 대한 관리를 용이하게 할 수 있도록 하는 것을 또 다른 목적으로 한다.

[0010] 또한, 본 발명은 사용자 아이덴티티들에 대한 접근 권한을 사용자 자신이 직접 관리할 수 있도록 하는 것을 또 다른 목적으로 한다.

과제의 해결 수단

[0011] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따르면, 블록체인 네트워크를 이용하여 사용자의 아이덴티티를 관리하는 방법에 있어서, (a) 사용자 단말로부터의 사용자 어드레스를 이용한 사용자 아이디 생성 데이터와 상기 사용자 아이디 생성 데이터를 사용자 마스터 프라이빗 키로 서명한 제1 사용자 서명값을 포함하는 사용자 아이디 생성 트랜잭션이 획득되면, 블록체인 네트워크를 구성하는 다수의 블록체인 노드들 중 적어도 하나의 블록체인 노드가, 상기 제1 사용자 서명값을 검증하여 상기 제1 사용자 서명값이 유효한 것으로 확인되면, 상기 블록체인 네트워크의 분산원장에 등록된 아이디 관리 컨트랙트를 실행하여 사용자 아이덴티티들에 대한 클레임을 생성하도록 하는 사용자 클레임 스마트 컨트랙트를 상기 분산원장에 등록하도록 하고, 상기 사용자 클레임 스마트 컨트랙트를 상기 분산원장에 등록하도록 하는 사용자 클레임 스마트 컨트랙트 등록 트랜잭션에 대응되는 사용자 클레임 스마트 컨트랙트 등록 트랜잭션 아이디를 상기 사용자 단말로 전송함으로써, 상기 사용자 단말로 하여금 상기 사용자 클레임 스마트 컨트랙트 등록 트랜잭션 아이디를 이용하여 상기 분산원장에 등록된 상기 사용자 클레임 스마트 컨트랙트의 어드레스를 사용자 아이디로 획득하도록 하는 단계; 및 (b) 상기 사용자 단말로부터의 사용자 셀프 클레임 등록 요청 트랜잭션 - 상기 사용자 셀프 클레임 등록 요청 트랜잭션은 상기 사용자

아이디, 상기 사용자 아이덴티티들을 가공한 사용자 특정값, 및 상기 사용자 아이디와 상기 사용자 특정값을 사용자 프라이빗 키로 서명한 제2 사용자 서명값을 포함하는 사용자 셀프 클레임 데이터와, 상기 사용자 셀프 클레임 데이터를 상기 사용자 마스터 프라이빗 키로 서명한 제3 사용자 서명값을 포함함 - 이 획득되면, 상기 적어도 하나의 블록체인 노드가, 상기 제3 사용자 서명값을 검증하여 상기 제3 사용자 서명값이 유효한 것으로 확인되면, 상기 사용자 아이디에 대응되는 상기 사용자 클레임 스마트 컨트랙트를 실행하여 상기 사용자 셀프 클레임 데이터에 대응하는 사용자 셀프 클레임이 상기 분산원장에 등록되도록 하며, 상기 분산원장에 등록된 상기 사용자 셀프 클레임에 대응되는 사용자 셀프 클레임 트랜잭션 아이디가 상기 사용자 단말로 전송되도록 하는 단계; 를 포함하는 방법이 제공된다.

[0012] 본 발명의 일 실시예에 따르면, 블록체인 네트워크를 이용하여 사용자의 아이덴티티를 관리하는 블록체인 네트워크의 블록체인 노드에 있어서, 사용자 아이덴티티를 관리하기 위한 인스트럭션들이 저장된 메모리; 및 상기 메모리에 저장된 상기 인스트럭션들에 따라 상기 사용자 아이덴티티를 관리하는 동작을 수행하는 프로세서; 를 포함하되, 상기 프로세서는, (i) 사용자 단말로부터의 사용자 어드레스를 이용한 사용자 아이디 생성 데이터와 상기 사용자 아이디 생성 데이터를 사용자 마스터 프라이빗 키로 서명한 제1 사용자 서명값을 포함하는 사용자 아이디 생성 트랜잭션이 획득되면, 상기 제1 사용자 서명값을 검증하여 상기 제1 사용자 서명값이 유효한 것으로 확인되면, 상기 블록체인 네트워크의 분산원장에 등록된 아이디 관리 컨트랙트를 실행하여 사용자 아이덴티티들에 대한 클레임을 생성하도록 하는 사용자 클레임 스마트 컨트랙트를 상기 분산원장에 등록하도록 하고, 상기 사용자 클레임 스마트 컨트랙트를 상기 분산원장에 등록하도록 하는 사용자 클레임 스마트 컨트랙트 등록 트랜잭션에 대응되는 사용자 클레임 스마트 컨트랙트 등록 트랜잭션 아이디를 상기 사용자 단말로 전송함으로써, 상기 사용자 단말로 하여금 상기 사용자 클레임 스마트 컨트랙트 등록 트랜잭션 아이디를 이용하여 상기 분산원장에 등록된 상기 사용자 클레임 스마트 컨트랙트의 어드레스를 사용자 아이디로 획득하도록 하는 프로세스, 및 (ii) 상기 사용자 단말로부터의 사용자 셀프 클레임 등록 요청 트랜잭션 - 상기 사용자 셀프 클레임 등록 요청 트랜잭션은 상기 사용자 아이디, 상기 사용자 아이덴티티들을 가공한 사용자 특정값, 및 상기 사용자 아이디와 상기 사용자 특정값을 사용자 프라이빗 키로 서명한 제2 사용자 서명값을 포함하는 사용자 셀프 클레임 데이터와, 상기 사용자 셀프 클레임 데이터를 상기 사용자 마스터 프라이빗 키로 서명한 제3 사용자 서명값을 포함함 - 이 획득되면, 상기 제3 사용자 서명값을 검증하여 상기 제3 사용자 서명값이 유효한 것으로 확인되면, 상기 사용자 아이디에 대응되는 상기 사용자 클레임 스마트 컨트랙트를 실행하여 상기 사용자 셀프 클레임 데이터에 대응하는 사용자 셀프 클레임이 상기 분산원장에 등록되도록 하며, 상기 분산원장에 등록된 상기 사용자 셀프 클레임에 대응되는 사용자 셀프 클레임 트랜잭션 아이디가 상기 사용자 단말로 전송되도록 하는 프로세스를 수행하는 것을 특징으로 하는 블록체인 노드가 제공된다.

[0013] 본 발명의 일 실시예에 따르면, 블록체인 네트워크를 이용하여 사용자의 아이덴티티를 관리하는 방법에 있어서, (a) 사용자들 및 인증기관들의 아이덴티티들에 대한 클레임을 생성하도록 하는 클레임 스마트 컨트렉트가 사용자들 및 인증기관들에 대응하여 각각 사용자 클레임 스마트 컨트랙트들과 인증기관 클레임 스마트 컨트랙트들로 다수의 블록체인 노드들에 의해 구성되는 블록체인 네트워크의 분산원장에 등록되며, 상기 사용자 클레임 스마트 컨트랙트들 및 상기 인증기관 스마트 컨트랙트들에 대한 상기 분산원장 상의 어드레스들이 상기 사용자들 및 상기 인증기관들의 아이디들로 관리되고, 상기 사용자들에 각각 대응되는 사용자 아이덴티티들을 가공한 사용자 특정값들을 포함하는 각각의 사용자 셀프 클레임들이 상기 분산원장에 등록된 상태에서, 특정 사용자 단말로부터의 특정 사용자 아이디, 특정 사용자 아이덴티티들 중 인증을 위한 특정 사용자 특정 아이덴티티, 및 적어도 상기 특정 사용자 아이덴티티들을 가공한 제1 특정 사용자 특정값을 포함하는 특정 사용자 특정 아이덴티티에 대한 특정 사용자 특정 아이덴티티 클레임 등록 요청에 대응하여 특정 인증기관 서버로부터 특정 사용자 셀프 클레임에 대응하는 특정 사용자 셀프 클레임 아이디에 대한 확인 요청이 획득되면, 상기 다수의 블록체인 노드들 중 적어도 하나의 블록체인 노드가, 특정 사용자 클레임 스마트 컨트랙트를 실행하여 상기 분산원장에 등록된 상기 특정 사용자 셀프 클레임에 대응하는 상기 특정 사용자 셀프 클레임 아이디를 상기 특정 인증기관 서버로 전송함으로써 상기 특정 인증기관 서버로 하여금 상기 특정 사용자 셀프 클레임 아이디를 이용하여 상기 분산원장에 등록된 상기 특정 사용자 셀프 클레임을 확인하여 상기 특정 사용자 셀프 클레임에 포함된 제2 특정 사용자 특정값을 획득하도록 하는 단계; 및 (b) 상기 특정 인증기관 서버로부터 특정 사용자 특정 아이덴티티 클레임 - 상기 특정 사용자 특정 아이덴티티 클레임은 상기 특정 인증기관 서버에서 생성된 것으로, 상기 특정 사용자 단말로부터의 상기 특정 사용자 특정 아이덴티티 클레임 등록 요청에 포함된 상기 제1 특정 사용자 특정값과 상기 분산원장의 상기 특정 사용자 셀프 클레임에 포함된 상기 제2 특정 사용자 특정값이 일치하는 상태에서, 상기 특정 인증기관 서버가 상기 특정 사용자 특정 아이덴티티를 검증한 다음, 상기 특정 인증기관 서버에 대응되는 특정 인증기관 아이디, 적어도 상기 특정 사용자 특정 아이덴티티를 가공한 특정 아이덴티티 가공값,

및 상기 특정 사용자 아이디와 상기 특정 아이덴티티 가공값을 상기 특정 인증기관 서버의 프라이빗 키로 서명한 제1 특정 인증기관 서명값을 포함하여 생성한 것임 - 과 상기 특정 사용자 특정 아이덴티티 클레임을 상기 특정 인증기관의 마스터 프라이빗 키로 서명한 제2 특정 인증기관 서명값을 포함하는 특정 사용자 특정 아이덴티티 클레임 등록 요청 트랜잭션이 획득되면, 상기 적어도 하나의 블록체인 노드가, 상기 제2 특정 인증기관 서명값을 검증하여 상기 제2 특정 인증기관 서명값이 유효한 경우, 상기 특정 사용자 스마트 컨트랙트를 실행하여 상기 특정 사용자 특정 아이덴티티 클레임이 상기 분산원장에 등록되도록 하고, 상기 특정 사용자 특정 아이덴티티 클레임을 상기 분산원장에 등록하도록 하는 특정 사용자 특정 아이덴티티 클레임 등록 트랜잭션에 대응되는 특정 사용자 특정 아이덴티티 클레임 등록 트랜잭션 아이디를 상기 특정 인증기관 서버로 전송함으로써, 상기 특정 인증기관 서버로 하여금 상기 특정 사용자 특정 아이덴티티 클레임 등록 트랜잭션 아이디를 이용하여 상기 분산원장에 등록된 상기 특정 사용자 특정 아이덴티티 클레임에 대응하는 특정 사용자 특정 아이덴티티 클레임 아이디를 획득하고, 상기 특정 사용자 특정 아이덴티티 클레임 아이디를 상기 특정 사용자 단말로 전송하도록 하는 단계; 를 포함하는 방법이 제공된다.

[0014] 본 발명의 일 실시예에 따르면, 블록체인 네트워크를 이용하여 사용자의 아이덴티티를 관리하는 블록체인 네트워크의 블록체인 노드에 있어서, 사용자 아이덴티티를 관리하기 위한 인스트럭션들이 저장된 메모리; 및 상기 메모리에 저장된 상기 인스트럭션들에 따라 상기 사용자 아이덴티티를 관리하는 동작을 수행하는 프로세서; 를 포함하되, 상기 프로세서는, (i) 사용자들 및 인증기관들의 아이덴티티들에 대한 클레임을 생성하도록 하는 클레임 스마트 컨트렉트가 사용자들 및 인증기관들에 대응하여 각각 사용자 클레임 스마트 컨트랙트들과 인증기관 클레임 스마트 컨트랙트들로 다수의 블록체인 노드들에 의해 구성되는 블록체인 네트워크의 분산원장에 등록되며, 상기 사용자 클레임 스마트 컨트랙트들 및 상기 인증기관 스마트 컨트랙트들에 대한 상기 분산원장 상의 어드레스들이 상기 사용자들 및 상기 인증기관들의 아이디들로 관리되고, 상기 사용자들에 각각 대응되는 사용자 아이덴티티들을 가공한 사용자 특정값들을 포함하는 각각의 사용자 셀프 클레임들이 상기 분산원장에 등록된 상태에서, 특정 사용자 단말로부터의 특정 사용자 아이디, 특정 사용자 아이덴티티들 중 인증을 위한 특정 사용자 특정 아이덴티티, 및 적어도 상기 특정 사용자 아이덴티티들을 가공한 제1 특정 사용자 특정값을 포함하는 특정 사용자 특정 아이덴티티에 대한 특정 사용자 특정 아이덴티티 클레임 등록 요청에 대응하여 특정 인증기관 서버로부터 특정 사용자 셀프 클레임에 대응하는 특정 사용자 셀프 클레임 아이디에 대한 확인 요청이 획득되면, 특정 사용자 클레임 스마트 컨트랙트를 실행하여 상기 분산원장에 등록된 상기 특정 사용자 셀프 클레임에 대응하는 상기 특정 사용자 셀프 클레임 아이디를 상기 특정 인증기관 서버로 전송함으로써 상기 특정 인증기관 서버로 하여금 상기 특정 사용자 셀프 클레임 아이디를 이용하여 상기 분산원장에 등록된 상기 특정 사용자 셀프 클레임을 확인하여 상기 특정 사용자 셀프 클레임에 포함된 제2 특정 사용자 특정값을 획득하도록 하는 프로세스, 및 (ii) 상기 특정 인증기관 서버로부터 특정 사용자 특정 아이덴티티 클레임 - 상기 특정 사용자 특정 아이덴티티 클레임은 상기 특정 인증기관 서버에서 생성된 것으로, 상기 특정 사용자 단말로부터의 상기 특정 사용자 특정 아이덴티티 클레임 등록 요청에 포함된 상기 제1 특정 사용자 특정값과 상기 분산원장의 상기 특정 사용자 셀프 클레임에 포함된 상기 제2 특정 사용자 특정값이 일치하는 상태에서, 상기 특정 인증기관 서버가 상기 특정 사용자 특정 아이덴티티를 검증한 다음, 상기 특정 인증기관 서버에 대응되는 특정 인증기관 아이디, 적어도 상기 특정 사용자 특정 아이덴티티를 가공한 특정 아이덴티티 가공값, 및 상기 특정 사용자 아이디와 상기 특정 아이덴티티 가공값을 상기 특정 인증기관 서버의 프라이빗 키로 서명한 제1 특정 인증기관 서명값을 포함하여 생성한 것임 - 과 상기 특정 사용자 특정 아이덴티티 클레임을 상기 특정 인증기관의 마스터 프라이빗 키로 서명한 제2 특정 인증기관 서명값을 포함하는 특정 사용자 특정 아이덴티티 클레임 등록 요청 트랜잭션이 획득되면, 상기 제2 특정 인증기관 서명값을 검증하여 상기 제2 특정 인증기관 서명값이 유효한 경우, 상기 특정 사용자 스마트 컨트랙트를 실행하여 상기 특정 사용자 특정 아이덴티티 클레임이 상기 분산원장에 등록되도록 하고, 상기 특정 사용자 특정 아이덴티티 클레임을 상기 분산원장에 등록하도록 하는 특정 사용자 특정 아이덴티티 클레임 등록 트랜잭션에 대응되는 특정 사용자 특정 아이덴티티 클레임 등록 트랜잭션 아이디를 상기 특정 인증기관 서버로 전송함으로써, 상기 특정 인증기관 서버로 하여금 상기 특정 사용자 특정 아이덴티티 클레임 등록 트랜잭션 아이디를 이용하여 상기 분산원장에 등록된 상기 특정 사용자 특정 아이덴티티 클레임에 대응하는 특정 사용자 특정 아이덴티티 클레임 아이디를 획득하고, 상기 특정 사용자 특정 아이덴티티 클레임 아이디를 상기 특정 사용자 단말로 전송하도록 하는 프로세스를 수행하는 것을 특징으로 하는 블록체인 노드가 제공된다.

[0015] 본 발명의 일 실시예에 따르면, 블록체인 네트워크 기반의 사용자 아이덴티티를 이용하여 사용자를 인증하는 방법에 있어서, (a) 사용자들의 아이덴티티들에 대한 클레임을 생성하도록 하는 클레임 스마트 컨트렉트가 사용자들에 각각 대응하여 사용자 클레임 스마트 컨트랙트들로 다수의 블록체인 노드들에 의해 구성되는 블록체인 네트워크의 분산원장에 등록되며, 상기 사용자 클레임 스마트 컨트랙트들에 대한 상기 분산원장 상의 어드레스들

이 상기 사용자들의 아이디들로 관리되고, 상기 사용자들에 각각 대응되는 사용자 아이덴티티들을 가공한 사용자 특정값들을 포함하는 각각의 사용자 셀프 클레임들, 사용자 아이덴티티들 각각에 대하여 적어도 하나의 인증기관이 인증하여 등록한 사용자 아이덴티티 클레임들, 및 사용자 키에 대응하는 사용자 어드레스들이 상기 분산원장 상에 등록되어 관리되는 상태에서, 서비스 이용 단말의 특정 사용자에 대한 사인 업 요청에 대응한 서비스 제공 서버로부터의 특정 사용자 특정 정보에 대한 요청이 획득되면, 사용자 단말이, 상기 특정 사용자 특정 정보에 대응되는 각각의 특정 사용자 특정 아이덴티티 클레임이 상기 분산원장에 등록되어 있는지를 확인하는 단계; 및 (b) 상기 특정 사용자 특정 아이덴티티 클레임이 상기 분산원장에 등록되어 있는지를 확인한 결과 상기 특정 사용자 특정 아이덴티티 클레임이 상기 분산원장에 등록되어 있는 경우, 상기 사용자 단말이, 상기 특정 사용자 아이디, 상기 특정 사용자 특정 정보에 대응되는 특정 사용자 특정 아이덴티티, 상기 특정 사용자 특정 아이덴티티 클레임 아이디, 특정 사용자 셀프 클레임 아이디, 특정 사용자 특정값, 특정 사용자 특정 아이덴티티를 이용한 상기 특정 사용자 특정값의 생성 정보, 및 상기 특정 사용자 특정값을 특정 사용자 프라이빗 키로 서명한 특정 사용자 서명값을 포함하는 특정 사용자 클레임 정보를 상기 서비스 제공 서버로 제공함으로써 상기 서비스 제공 서버로 하여금 상기 특정 사용자 셀프 클레임 아이디 및 상기 특정 사용자 특정 아이덴티티 클레임 아이디를 참조하여 상기 분산원장에 등록된 특정 사용자 셀프 클레임 및 특정 사용자 특정 아이덴티티 클레임을 확인하도록 하고, 확인된 상기 특정 사용자 셀프 클레임 및 상기 특정 사용자 특정 아이덴티티 클레임을 참조하여 상기 특정 사용자 클레임 정보를 인증하도록 하며, 상기 특정 사용자 클레임 정보가 인증되면 상기 특정 사용자의 사인 업을 허용하게 하도록 하는 단계; 를 포함하는 방법이 제공된다,

[0016] 본 발명의 일 실시예에 따르면, 블록체인 네트워크 기반의 사용자 아이덴티티를 이용하여 사용자를 인증하는 사용자 단말에 있어서, 사용자 아이덴티티를 이용하여 사용자를 인증하기 위한 인스트럭션들이 저장된 메모리; 및 상기 메모리에 저장된 상기 인스트럭션들에 따라 상기 사용자 아이덴티티를 이용하여 상기 사용자를 인증하는 동작을 수행하는 프로세서; 를 포함하되, 상기 프로세서는, (i) 사용자들의 아이덴티티들에 대한 클레임을 생성하도록 하는 클레임 스마트 컨트렉트가 사용자들에 각각 대응하여 사용자 클레임 스마트 컨트랙트들로 다수의 블록체인 노드들에 의해 구성되는 블록체인 네트워크의 분산원장에 등록되며, 상기 사용자 클레임 스마트 컨트랙트들에 대한 상기 분산원장 상의 어드레스들이 상기 사용자들의 아이디들로 관리되고, 상기 사용자들에 각각 대응되는 사용자 아이덴티티들을 가공한 사용자 특정값들을 포함하는 각각의 사용자 셀프 클레임들, 사용자 아이덴티티들 각각에 대하여 적어도 하나의 인증기관이 인증하여 등록한 사용자 아이덴티티 클레임들, 및 사용자 키에 대응하는 사용자 어드레스들이 상기 분산원장 상에 등록되어 관리되는 상태에서, 서비스 이용 단말의 특정 사용자에 대한 사인 업 요청에 대응한 서비스 제공 서버로부터의 특정 사용자 특정 정보에 대한 요청이 획득되면, 상기 특정 사용자 특정 정보에 대응되는 각각의 특정 사용자 특정 아이덴티티 클레임이 상기 분산원장에 등록되어 있는지를 확인하는 프로세스, 및 (ii) 상기 특정 사용자 특정 아이덴티티 클레임이 상기 분산원장에 등록되어 있는지를 확인한 결과 상기 특정 사용자 특정 아이덴티티 클레임이 상기 분산원장에 등록되어 있는 경우, 상기 특정 사용자 아이디, 상기 특정 사용자 특정 정보에 대응되는 특정 사용자 특정 아이덴티티, 상기 특정 사용자 특정 아이덴티티 클레임 아이디, 특정 사용자 셀프 클레임 아이디, 특정 사용자 특정값, 특정 사용자 특정 아이덴티티를 이용한 상기 특정 사용자 특정값의 생성 정보, 및 상기 특정 사용자 특정값을 특정 사용자 프라이빗 키로 서명한 특정 사용자 서명값을 포함하는 특정 사용자 클레임 정보를 상기 서비스 제공 서버로 제공함으로써 상기 서비스 제공 서버로 하여금 상기 특정 사용자 셀프 클레임 아이디 및 상기 특정 사용자 특정 아이덴티티 클레임 아이디를 참조하여 상기 분산원장에 등록된 특정 사용자 셀프 클레임 및 특정 사용자 특정 아이덴티티 클레임을 확인하도록 하고, 확인된 상기 특정 사용자 셀프 클레임 및 상기 특정 사용자 특정 아이덴티티 클레임을 참조하여 상기 특정 사용자 클레임 정보를 인증하도록 하며, 상기 특정 사용자 클레임 정보가 인증되면 상기 특정 사용자의 사인 업을 허용하게 하도록 하는 프로세스를 수행하는 것을 특징으로 하는 사용자 단말이 제공된다.

[0017] 본 발명의 일 실시예에 따르면, 블록체인 네트워크 기반의 사용자 아이덴티티를 이용하여 사용자를 인증하는 방법에 있어서, (a) 사용자들의 아이덴티티들에 대한 클레임을 생성하도록 하는 클레임 스마트 컨트렉트가 사용자들에 각각 대응하여 사용자 클레임 스마트 컨트랙트들로 다수의 블록체인 노드들에 의해 구성되는 블록체인 네트워크의 분산원장에 등록되며, 상기 사용자 클레임 스마트 컨트랙트들에 대한 상기 분산원장 상의 어드레스들이 상기 사용자들의 아이디들로 관리되고, 상기 사용자들에 각각 대응되는 사용자 아이덴티티들을 가공한 사용자 특정값들을 포함하는 각각의 사용자 셀프 클레임들, 사용자 아이덴티티들 각각에 대하여 적어도 하나의 인증기관이 인증하여 등록한 사용자 아이덴티티 클레임들, 및 사용자 키에 대응하는 사용자 어드레스들이 상기 분산원장 상에 등록되어 관리되는 상태에서, 서비스 이용 단말의 서비스 요청에 대응한 서비스 제공 서버로부터의 특정 사용자 서명값 요청 정보가 획득되면, 사용자 단말이, 상기 특정 사용자 서명값 요청 정보에 대응되는 데

이터를 확인하며, 상기 데이터를 특정 사용자 프라이빗 키로 서명한 특정 사용자 서명값을 생성하는 단계; 및 (b) 상기 사용자 단말이, 특정 사용자 아이디, 특정 사용자 어드레스, 상기 데이터, 및 상기 특정 사용자 서명값을 상기 서비스 제공 서버로 전송함으로써 상기 서비스 제공 서버로 하여금 상기 특정 사용자 서명값이 유효한지를 확인하도록 하며, 상기 특정 사용자 서명값이 유효한 경우 상기 특정 사용자 아이디를 참조하여 상기 블록체인 네트워크의 분산원장에 등록된 비교 대상 사용자 어드레스를 확인하고, 상기 비교 대상 사용자 어드레스를 참조하여 상기 특정 사용자 어드레스가 유효한지를 확인한 다음 상기 서비스 요청 단말로 요청된 서비스를 제공하여 주도록 하는 단계; 를 포함하는 것을 특징으로 하는 방법이 제공된다.

[0018] 본 발명의 일 실시예에 따르면, 블록체인 네트워크 기반의 사용자 아이덴티티를 이용하여 사용자를 인증하는 사용자 단말에 있어서, 사용자 아이덴티티를 이용하여 사용자를 인증하기 위한 인스트럭션들이 저장된 메모리; 및 상기 메모리에 저장된 상기 인스트럭션들에 따라 상기 사용자 아이덴티티를 이용하여 상기 사용자를 인증하는 동작을 수행하는 프로세서; 를 포함하되, 상기 프로세서는, (i) 사용자들의 아이덴티티들에 대한 클레임을 생성하도록 하는 클레임 스마트 컨트렉트가 사용자들에 각각 대응하여 사용자 클레임 스마트 컨트랙트들로 다수의 블록체인 노드들에 의해 구성되는 블록체인 네트워크의 분산원장에 등록되며, 상기 사용자 클레임 스마트 컨트랙트들에 대한 상기 분산원장 상의 어드레스들이 상기 사용자들의 아이디들로 관리되고, 상기 사용자들에 각각 대응되는 사용자 아이덴티티들을 가공한 사용자 특정값들을 포함하는 각각의 사용자 셀프 클레임들, 사용자 아이덴티티들 각각에 대하여 적어도 하나의 인증기관이 인증하여 등록한 사용자 아이덴티티 클레임들, 및 사용자 키에 대응하는 사용자 어드레스들이 상기 분산원장 상에 등록되어 관리되는 상태에서, 서비스 이용 단말의 서비스 요청에 대응한 서비스 제공 서버로부터의 특정 사용자 서명값 요청 정보가 획득되면, 상기 특정 사용자 서명값 요청 정보에 대응되는 데이터를 확인하며, 상기 데이터를 특정 사용자 프라이빗 키로 서명한 특정 사용자 서명값을 생성하는 프로세스, 및 (ii) 특정 사용자 아이디, 특정 사용자 어드레스, 상기 데이터, 및 상기 특정 사용자 서명값을 상기 서비스 제공 서버로 전송함으로써 상기 서비스 제공 서버로 하여금 상기 특정 사용자 서명값이 유효한지를 확인하도록 하며, 상기 특정 사용자 서명값이 유효한 경우 상기 특정 사용자 아이디를 참조하여 상기 블록체인 네트워크의 분산원장에 등록된 비교 대상 사용자 어드레스를 확인하고, 상기 비교 대상 사용자 어드레스를 참조하여 상기 특정 사용자 어드레스가 유효한지를 확인한 다음 상기 서비스 요청 단말로 요청된 서비스를 제공하여 주도록 하는 프로세스를 수행하는 것을 특징으로 하는 사용자 단말이 제공된다.

[0019] 이 외에도, 본 발명의 방법을 실행하기 위한 컴퓨터 프로그램을 기록하기 위한 컴퓨터 판독 가능한 기록 매체가 더 제공된다.

발명의 효과

[0020] 본 발명에 의하면, 다음과 같은 효과가 있다.

[0021] 본 발명은 보안성이 우수한 블록체인 기술을 이용하여 사용자 인증을 위한 각각의 사용자 아이덴티티들에 대한 권한을 사용자 자신이 소유할 수 있게 되므로, 사용자 의지와는 관계없이 사용자 정보가 거래되는 것을 방지할 수 있게 된다.

[0022] 본 발명은 사용자 아이덴티티들을 사용자가 보관하므로 각각의 사용자 아이덴티티들에 대한 관리를 용이하게 할 수 있게 된다.

[0023] 본 발명은 사용자 아이덴티티들에 대한 접근 권한을 사용자 자신이 직접 관리할 수 있도록 함으로써 사용자의 의지와는 관계없이 사용자 정보가 노출되는 것을 방지할 수 있게 된다.

도면의 간단한 설명

[0024] 도 1은 본 발명의 일 실시예에 따른 블록체인 네트워크를 이용하여 사용자의 아이덴티티를 관리하는 시스템을 개략적으로 도시한 것이고,

도 2a와 도 2b는 본 발명의 일 실시예에 따른 블록체인 네트워크를 이용하여 사용자 아이덴티티를 관리하는 방법에서 사용자 아이디 등을 생성하는 방법을 개략적으로 도시한 것이고,

도 3a와 도 3b는 본 발명의 일 실시예에 따른 블록체인 네트워크를 이용하여 사용자 아이덴티티를 관리하는 방법에서 사용자 셀프 클레임을 등록하는 방법을 개략적으로 도시한 것이고,

도 4a와 도 4b는 본 발명의 일 실시예에 따른 블록체인 네트워크를 이용하여 사용자 아이덴티티를 관리하는 방법에서 사용자 키를 추가 및 삭제하는 방법을 개략적으로 도시한 것이고,

도 5a와 도 5b는 본 발명의 일 실시예에 따른 블록체인 네트워크를 이용하여 사용자 아이덴티티를 관리하는 방법에서 사용자 데이터를 백업하는 방법을 개략적으로 도시한 것이고,

도 6은 본 발명의 일 실시예에 따른 블록체인 네트워크를 이용하여 사용자 아이덴티티를 관리하는 방법에서 사용자 데이터를 복구하는 방법을 개략적으로 도시한 것이고,

도 7a와 도 7b는 본 발명의 일 실시예에 따른 블록체인 네트워크를 이용하여 사용자 아이덴티티를 관리 방법에서 특정 아이덴티티 클레임을 등록하는 방법을 개략적으로 도시한 것이고,

도 8a와 도 8b는 본 발명의 일 실시예에 따른 블록체인 네트워크를 이용하여 사용자 아이덴티티를 관리하는 방법에서 특정 아이덴티티 클레임을 삭제하는 방법을 개략적으로 도시한 것이고,

도 9a와 도 9b는 본 발명의 일 실시예에 따른 블록체인 네트워크를 이용하여 사용자 아이덴티티를 관리하는 방법에서 특정 아이덴티티 클레임을 삭제하는 다른 방법을 개략적으로 도시한 것이고,

도 10a와 도 10b는 본 발명의 일 실시예에 다른 블록체인 네트워크 기반의 사용자 아이덴티티를 이용하여 사용자를 인증하는 방법을 개략적으로 도시한 것이다.

발명을 실시하기 위한 구체적인 내용

[0025] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 당업자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의 다양한 실시예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시예에 관련하여 본 발명의 정신 및 범위를 벗어나지 않으면서 다른 실시예로 구현될 수 있다. 또한, 각각의 개시된 실시예 내의 개별 구성요소의 위치 또는 배치는 본 발명의 정신 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 본 발명의 범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다.

[0026] 이하, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있도록 하기 위하여, 본 발명의 바람직한 실시예들에 관하여 첨부된 도면을 참조하여 상세히 설명하기로 한다.

[0027] 도 1은 본 발명의 일 실시예에 따른 블록체인 네트워크를 이용하여 사용자의 아이덴티티를 관리하는 시스템에 관한 것으로, 시스템은 사용자 단말(100), 인증기관 서버(200), 및 블록체인 노드(300)를 포함할 수 있다.

[0028] 먼저, 사용자 단말(100)은 사용자 아이덴티티를 관리하는 주체로, PC(Personal Computer), 모바일 컴퓨터, PDA/EDA, 휴대 전화, 스마트폰, 태블릿, IoT 기기 등을 포함할 수 있다. 그리고, 사용자 단말(100)은 이에 한정되지 않으며, 유무선 통신 기능을 가진 휴대용 게임기, 디지털 카메라, 개인 내비게이션 등의 모든 디바이스를 포함할 수 있다. 또한, 사용자 단말(100)은 사용자 아이덴티티의 관리를 위한 인스트럭션들을 저장하는 메모리(110)와 메모리(110)에 저장된 인스트럭션들에 대응하여 사용자 아이덴티티의 관리를 위한 동작을 수행하는 프로세서(120)를 포함할 수 있다. 이때, 도1에서는 하나의 사용자 단말(100)만을 도시하였으나, 이는 설명의 편의를 위한 것으로, 사용자 단말(100)은 각각의 사용자에 대응되는 다수 개로 이루어질 수 있다.

[0029] 구체적으로, 사용자 단말(100)은 전형적으로 컴퓨팅 장치(예컨대, 컴퓨터 프로세서, 메모리, 스토리지, 입력 장치 및 출력 장치, 기타 기존의 컴퓨팅 장치의 구성요소들을 포함할 수 있는 장치; 라우터, 스위치 등과 같은 전자 통신 장치; 네트워크 부착 스토리지(NAS) 및 스토리지 영역 네트워크(SAN)와 같은 전자 정보 스토리지 시스템)와 컴퓨터 소프트웨어(즉, 컴퓨팅 장치로 하여금 특정의 방식으로 기능하게 하는 인스트럭션들)의 조합을 이용하여 원하는 시스템 성능을 달성하는 것일 수 있다.

[0030] 또한, 컴퓨팅 장치의 프로세서는 MPU(Micro Processing Unit) 또는 CPU(Central Processing Unit), 캐쉬 메모리(Cache Memory), 데이터 버스(Data Bus) 등의 하드웨어 구성을 포함할 수 있다. 또한, 컴퓨팅 장치는 운영체제, 특정 목적을 수행하는 애플리케이션의 소프트웨어 구성을 더 포함할 수도 있다.

[0031] 다음으로, 인증기관 서버(200)는 사용자 아이덴티티들에 대한 인증을 수행하는 것으로, 사용자 아이덴티티 인증을 위한 인스트럭션들을 저장하는 메모리(210)와 메모리(210)에 저장된 인스트럭션들에 대응하여 사용자 아이덴티티의 인증을 위한 동작을 수행하는 프로세서(220)를 포함할 수 있다. 이때, 도1에서는 하나의 인증기관 서버(200)만을 도시하였으나, 이는 설명의 편의를 위한 것으로, 인증기관 서버(200)는 사용자 아이덴티티에 대한 인

증을 수행하는 각각의 인증기관에 대응되는 다수 개로 이루어질 수 있다.

[0032] 구체적으로, 인증기관 서버(200)는 전형적으로 컴퓨팅 장치(예컨대, 컴퓨터 프로세서, 메모리, 스토리지, 입력 장치 및 출력 장치, 기타 기존의 컴퓨팅 장치의 구성요소들을 포함할 수 있는 장치; 라우터, 스위치 등과 같은 전자 통신 장치; 네트워크 부착 스토리지(NAS) 및 스토리지 영역 네트워크(SAN)와 같은 전자 정보 스토리지 시스템)와 컴퓨터 소프트웨어(즉, 컴퓨팅 장치로 하여금 특정의 방식으로 기능하게 하는 인스트럭션들)의 조합을 이용하여 원하는 시스템 성능을 달성하는 것일 수 있다.

[0033] 다음으로, 블록체인 노드(300)들은 사용자 아이덴티들에 대응되는 클레임들 또는 클레임들과 관련한 정보를 저장 및 관리하는 것으로, 블록체인 네트워크를 구성하는 서버일 수 있으며, 사용자 아이덴티티 관리를 위한 인스트럭션들을 저장하는 메모리(310)와 메모리(310)의 인스트럭션들에 대응하여 사용자 아이덴티티 관리를 위한 동작을 수행하는 프로세서(320)를 포함할 수 있다. 이때, 도 1에서는 블록체인 노드(300)를 6개로 도시하였으나, 이는 설명의 편의를 위한 것으로, 블록체인 노드(300)의 개수는 이에 한정되지 않는다.

[0034] 구체적으로, 블록체인 노드(300)는 구체적으로, 정보 관리 서버(200)는 전형적으로 컴퓨팅 장치(예컨대, 컴퓨터 프로세서, 메모리, 스토리지, 입력 장치 및 출력 장치, 기타 기존의 컴퓨팅 장치의 구성요소들을 포함할 수 있는 장치; 라우터, 스위치 등과 같은 전자 통신 장치; 네트워크 부착 스토리지(NAS) 및 스토리지 영역 네트워크(SAN)와 같은 전자 정보 스토리지 시스템)와 컴퓨터 소프트웨어(즉, 컴퓨팅 장치로 하여금 특정의 방식으로 기능하게 하는 인스트럭션들)의 조합을 이용하여 원하는 시스템 성능을 달성하는 것일 수 있다.

[0035] 이에 더하여, 본 발명의 일 실시예에 따른 블록체인 네트워크를 이용하여 사용자의 아이덴티티를 관리하는 시스템은 서비스 제공 서버(미도시)를 더 포함할 수 있으며, 서비스 제공 서버는 사용자 아이덴티티를 이용한 사용자 인증 등을 통해 사용자 단말(100)을 통해 사용자가 원하는 서비스를 제공하여 줄 수 있다. 이때, 서비스 제공 서버는 전형적으로 컴퓨팅 장치와 컴퓨터 소프트웨어의 조합을 이용하여 원하는 시스템 성능을 달성하는 것일 수 있다.

[0036] 이와 같이 구성된 본 발명의 일 실시예에 따른 블록체인 네트워크를 이용하여 사용자 아이덴티티를 관리하는 시스템을 이용하여 사용자 아이덴티티를 관리하는 방법을 설명하면 다음과 같다.

[0037] 도 2a를 참조하여 본 발명의 일 실시예에 따른 블록체인 네트워크를 이용하여 사용자 아이덴티티를 관리하는 방법에서 사용자 아이디 등을 생성하는 방법을 설명한다.

[0038] 사용자가 사용자 단말(100)에 설치된 아이덴티티 관리 앱을 실행하여 사용자 프라이빗 키와 사용자 퍼블릭 키를 생성하고, 사용자 퍼블릭 키를 이용하여 사용자 어드레스를 생성한 상태에서, 사용자가 사용자 아이디를 생성하기 위하여 사용자 단말(100), 일 예로, 사용자 단말(100)에 설치된 아이덴티티 관리 앱을 실행하여 사용자 아이디 생성 트랜잭션이 블록체인 네트워크로 전송(S1)되도록 한다. 이때, 사용자 아이디 생성 트랜잭션은 사용자 어드레스를 이용한 사용자 아이디 생성 데이터와 사용자 아이디 생성 데이터를 사용자 마스터 프라이빗 키로 서명한 제1 사용자 서명값을 포함할 수 있다. 그리고, 사용자 마스터 프라이빗 키는 사용자 프라이빗 키일 수 있다.

[0039] 그러면, 블록체인 네트워크를 구성하는 다수의 블록체인 노드들 중 적어도 하나의 블록체인 노드(300)가, 사용자 아이디 생성 트랜잭션에 포함된 제1 사용자 서명값을 검증(S2)한다.

[0040] 일 예로, 적어도 하나의 블록체인 노드(300)는 블록체인 네트워크 상의 분산원장에 등록된 디지털 서명 검증 모듈을 실행하여 제1 사용자 서명값과 사용자 아이디 생성 데이터를 참조하여 사용자 마스터 프라이빗 키에 대응되는 사용자 마스터 퍼블릭 키를 획득하도록 할 수 있다. 즉, 적어도 하나의 블록체인 노드(300)는 제1 사용자 서명값과 사용자 아이디 생성 데이터를 블록체인 네트워크 상의 분산원장에 등록된 디지털 서명 검증 모듈로 전송하게 되며, 디지털 서명 검증 모듈은 입력되는 제1 사용자 서명값과 사용자 아이디 생성 데이터를 이용하여 제1 사용자 서명값의 서명에 이용된 사용자 마스터 프라이빗 키에 대응되는 사용자 마스터 프라이빗 키를 획득하게 된다. 그리고, 적어도 하나의 블록체인 노드(300)는 획득된 사용자 마스터 퍼블릭 키를 이용하여 제1 사용자 서명값으로부터 확인되는 제1 비교 대상 데이터와 사용자 아이디 생성 데이터가 일치하는 지를 확인함으로써 제1 사용자 서명값이 유효한지를 검증하게 된다.

[0041] 다른 예로, 사용자 단말(100)이 사용자 아이디 생성 트랜잭션에 사용자 마스터 프라이빗 키에 대응되는 사용자 마스터 퍼블릭 키를 더 포함하여 전송함으로써, 적어도 하나의 블록체인 노드(100)가, 사용자 마스터 퍼블릭 키를 이용하여 제1 사용자 서명값으로부터 확인되는 제1 비교 대상 데이터와 사용자 아이디 생성 데이터가 일치하

는 지를 확인함으로써 제1 사용자 서명값이 유효한지를 검증하게 된다.

[0042] 이후, 제1 사용자 서명값이 유효한 것으로 확인되면, 적어도 하나의 블록체인 노드(300)는 블록체인 네트워크의 분산원장에 등록된 아이디 관리 컨트랙트를 실행하여 사용자 아이덴티티들에 대한 클레임을 생성하도록 하는 사용자 클레임 스마트 컨트랙트를 분산원장에 등록(S3)하도록 한다.

[0043] 그리고, 적어도 하나의 블록체인 노드(300)는 사용자 클레임 스마트 컨트랙트를 분산원장에 등록하도록 하는 사용자 클레임 스마트 컨트랙트 등록 트랜잭션에 대응되는 사용자 클레임 스마트 컨트랙트 등록 트랜잭션 아이디를 사용자 단말(100)로 전송(S4)한다.

[0044] 그러면, 사용자 단말(100)은 사용자 클레임 스마트 컨트랙트 등록 트랜잭션 아이디를 이용하여 사용자 클레임 스마트 컨트랙트가 분산원장에 등록되었는지를 확인(S5)하며, 블록체인 네트워크를 구성하는 블록체인 노드(300)들의 합의에 의해 사용자 클레임 스마트 컨트랙트가 분산원장에 등록된 경우, 분산원장에서 사용자 클레임 스마트 컨트랙트가 등록된 위치 정보인 사용자 클레임 스마트 컨트랙트 어드레스를 획득(S6)하게 되며, 획득된 사용자 클레임 스마트 컨트랙트 어드레스를 사용자 아이디로 사용자 단말(100)에 등록하게 된다.

[0045] 도 2a에서는 사용자 단말(100)이 블록체인 네트워크로 직접 사용자 아이디 생성 트랜잭션을 전송함으로써 블록체인 네트워크 상에서의 트랜잭션 피(fee)를 사용자 단말(100)이 지급하여야 한다. 하지만, 이와는 사용자 단말(100)이 직접적으로 트랜잭션 피를 지급하지 않고 타 장치를 통해 트랜잭션 피를 지급하도록 할 수도 있다.

[0046] 즉, 도 2b를 참조하면, 사용자 아이디 생성 트랜잭션에 대한 트랜잭션 피를 사용자 단말(100)이 지급하는 것이 아니라, 프록시 서버(150)로 하여금 트랜잭션 피를 지급하도록 할 수 있다.

[0047] 이때, 사용자 단말(100)은 사용자 아이디 생성 트랜잭션을 프록시 서버(150)로 전송(S1-1)한다.

[0048] 그러면, 프록시 서버(150)는 사용자 아이디 생성 트랜잭션과 사용자 아이디 생성 트랜잭션을 프록시 서버(150)의 프록시 서버 마스터 프라이빗 키로 서명한 제1 프록시 서버 서명값을 블록체인 네트워크로 전송(S1-2)하게 되며, 그에 따라, 블록체인 네트워크를 구성하는 적어도 하나의 블록체인 노드(300)는 제1 프록시 서버 서명값을 검증(S1-3)하게 되며, 제1 프록시 서버 서명값이 유효한 경우 제1 사용자 서명값을 검증(S2)하게 된다. 이때, 적어도 하나의 블록체인 노드(300)가 제1 사용자 검증값을 검증하였으나, 이와는 달리 프록시 서버(150)가 제1 사용자 검증값을 검증할 수도 있다.

[0049] 또한, 적어도 하나의 블록체인 서버(300)는 사용자 클레임 스마트 컨트랙트 등록 트랜잭션 아이디를 프록시 서버(150)로 전송(S4-1)함으로써 프록시 서버(150)가 사용자 클레임 스마트 컨트랙트 등록 트랜잭션 아이디를 사용자 단말(100)로 전송(S4-2)하게 된다.

[0050] 상기에서는 사용자 단말(100)을 통해 사용자 아이디를 생성하는 과정을 설명하였으나, 인증기관 서버, 서비스 제공 서버 등도 동일한 방법에 의해 각각의 아이디를 생성할 수 있다.

[0051] 도 3a를 참조하여 본 발명의 일 실시예에 따른 블록체인 네트워크를 이용하여 사용자 아이덴티티를 관리하는 방법에서 사용자 셀프 클레임을 등록하는 방법을 설명한다.

[0052] 사용자가 사용자 단말(100)의 사용자 아이덴티티 관리 앱을 이용하여 등록하고자 하는 사용자 셀프 클레임을 생성(S11)한다.

[0053] 이때, 사용자 셀프 클레임은 사용자 아이디, 사용자 아이덴티티들을 가공한 사용자 특정값, 및 사용자 아이디와 사용자 특정값을 사용자 프라이빗 키로 서명한 제2 사용자 서명값을 포함할 수 있다.

[0054] 일 예로, 사용자 셀프 클레임은 1. 토픽, 2. scheme, 3. 소유자, 4, 서명값, 5. 데이터의 포멧으로 생성될 수 있다. 이때, 토픽은 사용자 아이덴티티들과 관련한 클레임의 타입, scheme은 사용되는 암호화 알고리즘, 소유자는 클레임을 생성하는 주체, 서명값은 주체의 서명값, 데이터는 클레임 내용일 수 있다.

[0055] 한편, 사용자 아이덴티티들은 사용자를 식별하기 위한 특징 정보들을 포함하며, 특징 정보들은 사용자 단말에 저장된 상태일 수 있다. 그리고, 사용자 아이덴티티들은 사용자 성명, 생년월일, 성별, 별명, 전화번호, 이메일 주소, 생체 정보, 행동 특성, 취미, 신체 특징, 생활 패턴 등 사용자와 관련한 모든 특징 정보들을 포함할 수 있고, 토픽을 통해 각각의 특징 정보들을 타입별로 분류할 수 있으며, 필요에 따라 토픽을 추가 및 삭제할 수 있다. 그리고, 소유자는 도 2a 또는 도 2b의 방법에 의해 생성된 사용자 아이디일 수 있다. 또한, 데이터는 클레임을 위한 아이덴티티 정보일 수 있으며, 사용자 셀프 클레임에서는 사용자의 모든 아이덴티티들을 가공한 사용자 특정값이고, 아이덴티티 클레임에서는 적어도 하나의 특정 아이덴티티의 가공값일 수 있다. 그리고, 데이

터에는 사용자 아이디 등을 추가하여 보안성을 향상시킬 수 있다.

[0056] 또한, 사용자 특정값은 사용자 아이덴티티들 각각에 대한 해시값들이 각각의 리프 노드들 중 적어도 일부에 할당된 머클트리의 루트 해시값일 수 있다.

[0057] 이후, 사용자 단말(100)은 생성된 사용자 셀프 클레임을 등록하기 위한 사용자 셀프 클레임 등록 요청 트랜잭션을 블록체인 네트워크로 전송(S12)한다. 이때, 사용자 셀프 클레임 등록 요청 트랜잭션은 사용자 셀프 클레임 데이터, 즉, 사용자 아이디, 사용자 아이덴티티들을 가공한 사용자 특정값, 및 사용자 아이디와 사용자 특정값을 사용자 프라이빗 키로 서명한 제2 사용자 서명값을 포함하는 사용자 셀프 클레임과, 사용자 셀프 클레임 데이터를 사용자 마스터 프라이빗 키로 서명한 제3 사용자 서명값을 포함할 수 있다.

[0058] 그러면, 블록체인 네트워크를 구성하는 다수의 블록체인 노드들 중 적어도 하나의 블록체인 노드(300)가 제3 사용자 서명값을 검증(S13)한다. 이때, 제3 사용자 서명값의 검증은 도 2a를 참조하여 설명한 것과 동일한 방법으로 수행할 수 있으며, 이하의 설명에서는 서명값의 검증에 대한 구체적인 방법은 생략하기로 한다.

[0059] 이후, 제3 사용자 서명값이 유효한 것으로 확인되면, 적어도 하나의 블록체인 노드(300)는 사용자 셀프 클레임에 포함된 제2 사용자 서명값을 검증(S14)한다.

[0060] 그리고, 제2 사용자 서명값이 유효한 것으로 확인되면, 적어도 하나의 블록체인 노드(300)는 블록체인 네크워크의 분산원장에 등록된 사용자 아이디에 대응되는 사용자 클레임 스마트 컨트랙트를 실행하여 사용자 셀프 클레임 데이터에 대응하는 사용자 셀프 클레임이 분산원장에 등록(S15)되도록 하며, 분산원장에 사용자 셀프 클레임을 등록하기 위한 트랜잭션에 대응되는 사용자 셀프 클레임 트랜잭션 아이디를 사용자 단말(100)로 전송하여 준다(S18).

[0061] 그러면, 사용자 단말(100)은 사용자 셀프 클레임 트랜잭션 아이디를 이용하여 사용자 셀프 클레임이 분산원장에 등록되었는지를 확인하며, 블록체인 네트워크를 구성하는 블록체인 노드(300)들의 합의에 의해 사용자 셀프 클레임이 분산원장에 등록된 경우, 분산원장에서 사용자 셀프 클레임이 등록된 위치 정보인 사용자 셀프 클레임 어드레스, 즉, 사용자 셀프 클레임 아이디를 획득하게 된다.

[0062] 한편, 도 3b를 참조하면, 사용자 단말(100)이 사용자 셀프 클레임 등록 요청 트랜잭션을 프록시 서버(150)로 전송(S12-1)하며, 프록시 서버(150)가 사용자 셀프 클레임 등록 요청 트랜잭션과, 사용자 셀프 클레임 등록 요청 트랜잭션을 프록시 서버 마스터 프라이빗 키로 서명한 제2 프록시 서버 서명값을 블록체인 네트워크로 전송(S12-2)하게 된다. 그러면, 블록체인 네트워크를 구성하는 다수의 블록체인 노드들 중 적어도 하나의 블록체인 노드(300)는 제2 프록시 서버 서명값을 검증(S13-1)하고, 제2 프록시 서버 서명값이 유효하면 제2 사용자 서명값을 검증(S14)하게 된다. 이때, 적어도 하나의 블록체인 노드(300)가 제2 사용자 서명값을 검증하였으나, 이와는 달리, 프록시 서버(150)가 제2 사용자 서명값을 검증할 수도 있다.

[0063] 또한, 적어도 하나의 블록체인 노드(300)는 사용자 셀프 클레임 트랜잭션 아이디를 프록시 서버(150)로 전송(S16-1)하여 주며, 프록시 서버(150)는 사용자 셀프 클레임 트랜잭션 아이디를 사용자 단말(100)로 전송(S16-2)하여, 사용자 단말(100)이 사용자 셀프 클레임 아이디를 획득하도록 할 수 있다.

[0064] 이를 통해, 도 3a에서는 사용자 단말(100)이 트랜잭션 피를 지급하였으나, 도 3b에서는 프록시 서버(150)가 사용자 단말(100)을 대신하여 트랜잭션 피를 지급하도록 할 수 있다.

[0065] 도 4a를 참조하여 본 발명의 일 실시예에 따른 블록체인 네트워크를 이용하여 사용자 아이덴티티를 관리하는 방법에서 사용자 키를 추가 및 삭제하는 방법을 설명한다.

[0066] 본 발명의 일 실시예에 따른 블록체인 네트워크를 이용하여 사용자 아이덴티티를 관리하는 방법에서는 사용자 어드레스를 이용하여 사용자 프라이빗 키를 생성하게 되며, 키의 사용 목적에 따라 각각의 사용자 키를 추가하거나 삭제할 수 있다. 그리고, 각각의 목적에 대응되는 사용자 키에 대해서만 해당하는 목적의 동작을 수행하도록 할 수 있다.

[0067] 사용자가 사용자 단말(100)의 사용자 아이덴티티 관리 앱을 통해 사용자 어드레스 및 키 목적을 포함하는 사용자 키 추가 또는 삭제 요청 데이터와 이를 사용자 마스터 프라이빗 키로 서명한 사용자 서명값을 포함하는 사용자 키 추가 또는 삭제 요청 트랜잭션을 전송(S21)을 전송하면, 적어도 하나의 블록체인 노드(300)가 사용자 서명값을 검증(S22)한다.

[0068] 이때, 사용자 서명값이 유효한 것으로 확인되면, 적어도 하나의 블록체인 노드(300)는 분산원장 상의 사용자 키

리스트에서 키 목적에 따른 사용자 키를 추가하거나 키 리스트에 등록된 사용자 키를 삭제하도록 한다(S23).

[0069] 그리고, 적어도 하나의 블록체인 노드(300)는 사용자 키 추가 또는 삭제 요청 트랜잭션을 분산원장에 등록하기 위한 트랜잭션 아이디를 사용자 단말(100)로 전송(S24)하여 준다.

[0070] 그러면, 사용자 단말(100)은 트랜잭션 아이디를 이용하여 요청한 사용자 키가 분산원장에서 추가 또는 삭제되었는지를 확인(S25)하고, 블록체인 네트워크의 분산원장으로부터의 결과 정보를 전송받음(S26)으로써 분산원장에서 요청한 사용자 키가 추가 또는 삭제되었는지에 대한 결과를 확인할 수 있게 된다. 이때, 사용자 어드레스는 최초에는 디폴트로 모든 목적의 키 리스트에 등록될 수 있으며, 사용자 키 추가에 따라 해당하는 목적의 각각 다른 사용자 어드레스가 각각의 목적의 키 리스트에 등록될 수 있다.

[0071] 또한, 도 4b를 참조하면, 사용자 단말(100)이 사용자 키 추가 또는 삭제 요청 트랜잭션을 프록시 서버(150)로 전송(S21-1)하면, 프록시 서버가 사용자 키 추가 또는 삭제 요청 트랜잭션과, 이를 프록시 서버 마스터 프라이빗 키로 서명한 프록시 서버 서명값을 블록체인 네트워크로 전송(S21-2)하게 되며, 블록체인 네트워크를 구성하는 다수의 블록체인 노드들 중 적어도 하나의 블록체인 노드(300)가 프록시 서버 서명값을 검증(S21-3)하여 유효한 것으로 판단되면 사용자 키를 추가하거나 삭제하게 된다(S23). 이때, 사용자 키 추가 또는 삭제 요청 트랜잭션에 포함된 사용자 서명값은 프록시 서버(150)가 검증하거나, 적어도 하나의 블록체인 노드(300)가 검증할 수 있다.

[0072] 또한, 적어도 하나의 블록체인 노드(300)는 트랜잭션 아이디를 프록시 서버(150)로 전송(S24-1)하여 주며, 프록시 서버(150)가 트랜잭션 아이디를 사용자 단말(100)로 전송(S24-2)하여 줌으로써 사용자 단말(100)이 트랜잭션 아이디를 이용하여 사용자 키의 추가 또는 삭제된 결과를 확인할 수 있도록 한다.

[0073] 이를 통해, 도 4a에서는 사용자 단말(100)이 트랜잭션 피를 지급하였으나, 도 4b에서는 프록시 서버(150)가 사용자 단말(100)을 대신하여 트랜잭션 피를 지급하도록 할 수 있다.

[0074] 도 5a를 참조하여 본 발명의 일 실시예에 따른 블록체인 네트워크를 이용하여 사용자 아이덴티티를 관리하는 방법에서 사용자 데이터를 백업하는 방법을 설명한다.

[0075] 사용자 데이터 백업은 사용자 단말(100)에 설치된 사용자 아이덴티티 관리 앱이 삭제되거나 관리할 수 없을 경우, 사용자가 검증받은 데이터를 복구할 수 있도록 하기 위하여 사용자 아이덴티티들 및 사용자 키들을 IPFS(InterPlanetary File System) 등과 같은 분산저장 시스템에 저장하는 것일 수 있다.

[0076] 사용자는 사용자 단말(100)의 사용자 아이덴티티 앱을 통해 백업 하고자 하는 사용자 데이터, 일 예로, 사용자 아이덴티티들과 사용자 키들을 사용자 퍼블릭 키로 암호화하여 암호화된 사용자 데이터를 생성(S31)한다.

[0077] 그리고, 사용자 단말(100)은 생성된 암호화된 사용자 데이터를 분산저장 시스템으로 전송하여 암호화된 사용자 데이터 등록 요청(S32)을 하며, 이에 따라 분산저장 시스템을 구성하는 다수의 분산저장 서버 중 적어도 하나의 분산저장 서버(400)는 암호화된 사용자 데이터를 분산저장 시스템에 등록(S33)하게 된다.

[0078] 이후, 분산저장 서버(400)는 분산저장 시스템에 등록된 암호화된 사용자 데이터의 위치 정보인 파일 아이디를 사용자 단말(100)로 전송(S34)하여 준다.

[0079] 그러면, 사용자 단말(100)은 사용자 아이디와 파일 아이디를 포함하는 사용자 셀프 클레임을 생성(S35)한다.

[0080] 그리고, 도 3a에서와 같은 방법에 의해, 사용자 단말(100)은 블록체인 네트워크로 사용자 셀프 클레임 등록 요청(S36)을 하며, 블록체인 네트워크를 구성하는 적어도 하나의 블록체인 노드(300)는 파일 아이디에 대한 사용자 셀프 클레임을 분산원장에 등록(S37)하게 된다. 이후, 사용자 단말(100)은 사용자 셀프 클레임 아이디를 확인(S38)함으로써 등록 결과를 확인할 수 있게 된다.

[0081] 또한, 도 5b를 참조하면, 사용자 단말(100)은 프록시 서버(150)로 암호화된 사용자 데이터 등록 요청(S32-1)을 하고, 프록시 서버(15)가 분산저장 시스템으로 암호화된 사용자 데이터 등록 요청(S32-2)을 하며, 이에 따라 분산저장 시스템을 구성하는 다수의 분산저장 서버 중 적어도 하나의 분산저장 서버(400)가 암호화된 사용자 데이터를 분산저장 시스템에 등록(S33)하게 된다.

[0082] 그리고, 분산저장 서버(400)는 분산저장 시스템에 등록된 암호화된 사용자 데이터의 위치 정보인 파일 아이디를 프록시 서버(150)로 전송(S34-1)하고, 프록시 서버(150)가 파일 아이디를 사용자 단말(100)로 전송(S34-2)하여 준다.

[0083] 또한, 도 3b에서와 같은 방법에 의해, 사용자 단말(100)은 프록시 서버(150)로 사용자 셀프 클레임 등록 요청(S36-1)하고, 프록시 서버(150)가 블록체인 네트워크로 사용자 셀프 클레임 등록 요청(S36-2)을 한다.

[0084] 이를 통해, 도 5a에서는 사용자 단말(100)이 트랜잭션 피를 지급하였으나, 도 5b에서는 프록시 서버(150)가 사용자 단말(100)을 대신하여 트랜잭션 피를 지급하도록 할 수 있다.

[0085] 도 6을 참조하여 본 발명의 일 실시예에 따른 블록체인 네트워크를 이용하여 사용자 아이덴티티를 관리하는 방법에서 사용자 데이터를 복구하는 방법을 설명한다.

[0086] 사용자가 사용자 아이덴티티들에 대한 사용자 데이터의 복구를 위하여, 사용자 단말(100)의 사용자 아이덴티티 관리 앱을 통해 블록체인 네트워크로 사용자 셀프 클레임 아이디 확인 요청(S41)을 한다. 이때, 확인하고자 하는 사용자 셀프 클레임은 도 5a에서와 같은 방법에 의해 등록한 파일 아이디에 대응되는 사용자 셀프 클레임일 수 있다.

[0087] 그러면, 블록체인 네트워크를 구성하는 적어도 하나의 블록체인 서버(300)는 사용자 클레임 스마트 컨트랙트를 실행하여 분산원장에 등록된 사용자 클레임들 중 파일 아이디와 관련하여 등록된 사용자 셀프 클레임 아이디를 확인하고, 사용자 단말(100)로 사용자 셀프 클레임 아이디를 전송(S42)하여 준다.

[0088] 그리고, 사용자 단말(100)은 확인된 사용자 셀프 클레임 아이디를 이용하여 블록체인 네트워크로 사용자 셀프 클레임에 대한 확인 요청(S43)을 하며, 그에 따라 블록체인 네트워크를 구성하는 적어도 하나의 블록체인 노드(300)는 사용자 클레임 스마트 컨트랙트를 실행하여 사용자 셀프 클레임에 포함된 파일 아이디를 사용자 단말(100)로 전송(S44)하여 준다.

[0089] 그러면, 사용자 단말(100)은 획득된 파일 아이디를 이용하여 분산저장 시스템으로 파일 아이디에 대응되는 암호화된 사용자 데이터를 요청(S45)하며, 분산저장 시스템의 적어도 하나의 분산저장 서버(400)는 파일 아이디에 대응되는 암호화된 사용자 데이터를 확인하고, 확인된 암호화된 사용자 데이터를 사용자 단말(100)로 전송(S46)하여 준다.

[0090] 그리고, 사용자 단말(100)은 획득된 암호화된 사용자 데이터를 사용자 프라이빗 키로 복호화하여 사용자 데이터를 획득하게 하며, 이를 통해 사용자 데이터를 복구(S47)하게 된다.

[0091] 상기에서는 사용자 단말(100)이 직접적으로 분산저장 시스템 및 블록체인 네트워크와 통신을 하였으나, 이와는 달리, 상기에서와 같은 방법에 의해 프록시 서버를 통해 통신을 중개할 수도 있다.

[0092] 도 7a를 참조하여 본 발명의 일 실시예에 따른 블록체인 네트워크를 이용하여 사용자 아이덴티티를 관리 방법에서 특정 아이덴티티 클레임을 등록하는 방법을 설명한다.

[0093] 도 2a와 도 3a에서와 같은 방법에 의해 사용자들 및 인증기관들의 아이덴티티들에 대한 클레임을 생성하도록 하는 클레임 스마트 컨트렉트가 사용자들 및 인증기관들에 대응하여 각각 사용자 클레임 스마트 컨트랙트들과 인증기관 클레임 스마트 컨트랙트들로 다수의 블록체인 노드들에 의해 구성되는 블록체인 네트워크의 분산원장에 등록되며, 사용자 클레임 스마트 컨트랙트들 및 인증기관 스마트 컨트랙트들에 대한 분산원장 상의 어드레스들이 사용자들 및 인증기관들의 아이디들로 관리되고, 사용자들에 각각 대응되는 사용자 아이덴티티들을 가공한 사용자 특정값들을 포함하는 각각의 사용자 셀프 클레임들이 분산원장에 등록된 상태에서, 특정 사용자 단말(100)로부터 인증기관들의 리스트 요청(S51)이 획득되면, 적어도 하나의 블록체인 노드(300)는 분산원장에 등록된 인증기관들의 리스트를 특정 사용자 단말(100)로 전송(S52)하여 준다. 그러면, 특정 사용자 단말(100)은 인증기관 리스트에서 사용자가 특정 사용자 아이덴티티에 대한 인증을 수행할 특정 인증기관을 선택할 수 있도록 하며, 사용자에 의해 특정 인증기관이 선택되면, 선택된 특정 인증기관 서버(200)로 특정 인증기관에 대한 정보를 요청(S53)한다.

[0094] 그리고, 특정 인증기관 서버(200)는 사용자 단말(100)로부터의 정보 요청에 대응하여 자신의 정보, 즉, 특정 인증기관 정보를 사용자 단말(100)로 전송(S54)하여 준다, 이때, 특정 인증기관 서버(200)는 서버에 저장하고 있는 인증기관 정보를 전송하여 주거나, 블록체인 네트워크 또는 분산저장 시스템에 등록된 특정 인증기관 정보에 대한 접근 키를 전송하여 줌으로써 사용자 단말(100)이 접근 키를 통해 블록체인 네트워크 또는 분산저장 시스템에서 특정 인증기관 정보를 획득할 수 있도록 할 수 있다. 그리고, 특정 인증기관 정보는 인증기관에 대한 정보 및 인증 가능한 사용자 아이덴티티들에 대한 정보를 포함할 수 있으나, 이에 한정되는 것은 아니다.

[0095] 그러면, 특정 사용자 단말(100)은 특정 사용자에 의해 선택된 특정 아이덴티티에 대한 인증을 위하여 특정 인증기관 서버(200)로 특정 사용자 특정 아이덴티티 클레임 등록 요청을 전송(S55)한다. 이때, 특정 사용자 특정 아

이덴티티 클레임 등록 요청에는 특정 사용자 아이디, 특정 사용자 아이덴티티들 중 인증을 위한 특정 사용자 특정 아이덴티티, 및 특정 사용자 아이덴티티들을 가공한 제1 특정 사용자 특정값이 포함될 수 있다. 그리고, 제1 특정 사용자 특정값은 특정 사용자 아이덴티티들 각각에 대한 해시값들이 각각의 리프 노드들 중 적어도 일부에 할당된 머클트리의 루트 해시값일 수 있으며, 특정 사용자 특정 아이덴티티 클레임 등록 요청에는 머클트리 정보가 포함될 수 있다.

[0096] 그리고, 특정 인증기관 서버(200)는 특정 사용자 단말(100)로부터의 특정 사용자 특정 아이덴티티 클레임 등록 요청에 대응하여, 블록체인 네트워크로 특정 사용자 아이디에 대응되는 특정 사용자 셀프 클레임에 대한 특정 사용자 셀프 클레임 아이디에 대한 확인을 요청(S56)한다.

[0097] 그러면, 블록체인 네트워크를 구성하는 다수의 블록체엔 노드들 중 적어도 하나의 블록체인 노드(300)가, 특정 사용자 클레임 스마트 컨트랙트를 실행하여 분산원장에 등록된 특정 사용자 셀프 클레임에 대응되는 특정 사용자 셀프 클레임 아이디를 확인하여 특정 인증기관 서버(200)로 전송(S57)하여 준다. 이때, 적어도 하나의 블록체인 노드(300)는 특정 사용자에 대응되는 클레임들에서 셀프 클레임에 해당하는 클레임을 확인함으로써 특정 사용자 셀프 클레임 아이디를 확인할 수 있게 된다.

[0098] 이후, 특정 인증기관 서버(200)는 특정 사용자 셀프 클레임 아이디를 이용하여 분산원장에 등록된 특정 사용자 셀프 클레임을 확인(S58)하여 특정 사용자 셀프 클레임에 포함된 제2 특정 사용자 특정값을 획득(S59)할 수 있다.

[0099] 그리고, 특정 인증기관 서버(200)는 특정 사용자 단말(100)로부터의 특정 사용자 특정 아이덴티티 클레임 등록 요청에 포함된 제1 특정 사용자 특정값과 분산원장의 특정 사용자 셀프 클레임에 포함된 제2 특정 사용자 특정값이 일치하는지를 확인하고, 제1 특정 사용자 특정값과 제2 특정 사용자 특정값이 일치하면 특정 사용자 특정 아이덴티티를 검증(S60)한다.

[0100] 일 예로, 제1 특정 사용자 특정값이 특정 사용자 아이덴티티들 각각에 대한 해시값들을 리프 노드로 하는 머클트리의 루트 해시값일 경우, 특정 사용자 특정 아이덴티티 클레임 등록 요청에 포함된 제1 루트 해시값과 분산원장의 특정 사용자 셀프 클레임에 포함된 제2 루트 해시값이 동일한지 확인하며, 제1 루트 해시값과 제2 루트 해시값이 동일한 경우, 머클트리 정보와 특정 사용자 특정 아이덴티티의 해시값을 이용하여 비교 대상 루트 해시값을 생성하고, 생성된 비교 대상 해시값이 제1 루트 해시값과 동일한지 확인하여 특정 사용자 특정 아이덴티티가 특정 사용자의 정보인지를 확인한다. 그리고, 특정 아이덴티티가 정확하지를 검증한다. 이때, 특정 아이덴티티의 검증은 특정 인증기관 서버(200)가 수행하는 것으로, 특정 사용자 특정 아이덴티티가 특정 사용자의 특징 정보와 일치하는 지를 확인하여 인증하여 줄 수 있다. 예를 들어, 특정 아이덴티티가 전화번호일 경우 일반적인 전화번호 인증을 수행하여 해당 전화번호가 특정 사용자의 전화번호와 일치하는 지 확인한다.

[0101] 그리고, 특정 사용자 특정 아이덴티티가 검증되면, 특정 인증기관 서버(200)는 특정 사용자 특정 아이덴티티 클레임을 생성(S61)한다.

[0102] 이때, 특정 사용자 특정 아이덴티티 클레임은 특정 인증기관 서버(200)에 대응되는 특정 인증기관 아이디, 적어도 특정 사용자 특정 아이덴티티를 가공한 특정 아이덴티티 가공값, 및 특정 사용자 아이디와 특정 아이덴티티 가공값을 특정 인증기관 서버의 프라이빗 키로 서명한 제1 특정 인증기관 서명값을 포함할 수 있다. 이때, 특정 아이덴티티 가공값은 특정 사용자 특정 아이덴티티에 특정 사용자 아이디를 추가하여 생성할 수 있으며, 특정 사용자 특정 아이덴티티와 사용자 아이디에 해시함수를 적용하여 생성한 해시값일 수 있으나, 이에 한정되는 것을 아니다.

[0103] 일 예로, 특정 사용자 특정 아이덴티티 클레임은 도 3a를 참조한 설명에서와 같이, 1. 토픽, 2. scheme, 3. 소유자, 4, 서명값, 5. 데이터의 포멧으로 생성될 수 있다. 이때, 토픽은 사용자 아이덴티티들과 관련한 클레임의 타입, scheme은 사용되는 암호화 알고리즘, 소유자는 클레임을 생성하는 주체, 서명값은 주체의 서명값, 데이터는 클레임 내용일 수 있다.

[0104] 이후, 특정 인증기관 서버(200)는 생성된 특정 사용자 특정 아이덴티티 클레임을 등록하기 위한 특정 사용자 특정 아이덴티티 클레임 등록 요청 트랜잭션을 블록체인 네트워크로 전송(S62)한다. 이때, 특정 사용자 특정 아이덴티티 클레임 등록 요청 트랜잭션은 특정 사용자 특정 아이덴티티 클레임과 특정 사용자 특정 아이덴티티 클레임을 특정 인증기관의 마스터 프라이빗 키로 서명한 제2 특정 인증기관 서명값을 포함할 수 있다.

[0105] 그러면, 블록체인 네트워크의 적어도 하나의 블록체인 노드(300)는 제2 특정 인증기관 서명값을 검증한다. 이에 더하여 적어도 하나의 블록체인 노드(300)는 제2 특정 인증기관 서명값이 유효한 경우, 특정 사용자 특정 아이

덴티티 클레임에 포함된 제2 특정 인증기관 서명값을 검증할 수 있다.

[0106] 그리고, 적어도 하나의 블록체인 노드(300)는 분산원장에 등록된 특정 사용자 클레임 스마트 컨트랙트를 실행하여 특정 사용자 특정 아이덴티티 클레임이 분산원장에 등록(S63)되도록 하며, 특정 사용자 특정 아이덴티티 클레임을 분산원장에 등록하도록 하는 특정 사용자 특정 아이덴티티 클레임 등록 트랜잭션에 대응되는 특정 사용자 특정 아이덴티티 클레임 등록 트랜잭션 아이디를 특정 인증기관 서버(200)로 전송(S64)하여 준다.

[0107] 그러면, 특정 인증기관 서버(200)는 특정 사용자 특정 아이덴티티 클레임 등록 트랜잭션 아아디를 이용하여 특정 사용자 특정 아이덴티티 클레임이 분산원장에 등록되었는지를 확인(S65)하며, 블록체인 네트워크를 구성하는 블록체인 노드(300)들의 합의에 의해 특정 사용자 특정 아이덴티티 클레임이 분산원장에 등록된 경우, 분산원장에서 특정 사용자 특정 아이덴티티 클레임이 등록된 위치 정보인 특정 사용자 특정 아이덴티티 클레임 아이디를 획득(S66)하고, 획득된 특정 사용자 특정 아이덴티티 클레임 아이디를 사용자 단말(100)로 전송(S67)하여 준다.

[0108] 이에 더하여, 특정 인증기관 서버(200)에 의해 등록된 특정 사용자 특정 아이덴티티 클레임에 대하여 사용자가 승인을 하기 위하여, 특정 사용자 단말(100)을 통해 블록체인 네트워크로 특정 사용자 특정 아이덴티티 클레임 승인 트랜잭션을 전송(S68)한다.

[0109] 이때, 특정 사용자 특정 아이덴티티 클레임 승인 트랜잭션은 특정 사용자 특정 아이덴티티 승인 데이터와 특정 사용자 특정 아이덴티티 승인 데이터를 특정 사용자 마스터 프라이빗 키로 서명한 제3 특정 사용자 서명값을 포함할 수 있으며, 특정 사용자 특정 아이덴티티 승인 데이터는 특정 사용자 특정 아이덴티티 클레임 아이디와 특정 사용자 특정 아이덴티티 클레임에 대한 승인 정보를 포함할 수 있다.

[0110] 그러면, 블록체인 네트워크의 적어도 하나의 블록체인 노드(300)는 제3 특정 사용자 서명값을 검증하여 제3 특정 사용자 서명값이 유효한 경우, 특정 사용자 클레임 스마트 컨트랙트를 실행하여 특정 사용자 특정 아이덴티티 클레임 승인 트랜잭션이 분산원장에 등록(S69)되도록 한다.

[0111] 그리고, 적어도 하나의 블록체인 노드(300)는 분산원장에 특정 사용자 특정 아이덴티티 클레임 승인 트랜잭션을 등록하기 위한 특정 사용자 특정 아이덴티티 클레임 승인 트랜잭션 아이디를 특정 사용자 단말(100)로 전송하여 주며, 특정 사용자 단말(100)은 특정 사용자 특정 아이덴티티 클레임 승인 트랜잭션 아이디를 이용하여 특정 사용자 특정 아이덴티티 클레임 승인 트랜잭션이 분산원장에 등록되었는지를 확인(S71)(S72)한다.

[0112] 한편, 도 7b를 참조하면, 특정 인증기관 서버(200)는 생성된 특정 사용자 특정 아이덴티티 클레임을 등록하기 위한 특정 사용자 특정 아이덴티티 클레임 등록 요청 트랜잭션을 프록시 서버(150)로 전송(S62-1)하며, 프록시 서버(150)가 특정 사용자 특정 아이덴티티 클레임 등록 요청 트랜잭션과, 이를 프록시 서버 마스터 프라이빗 키로 서명한 제2 프록시 서버 서명값을 블록체인 네트워크로 전송(S62-2)하게 된다. 그러면, 블록체인 네트워크의 적어도 하나의 블록체인 노드(300)는 제2 프록시 서버 서명값을 검증하고, 제2 프록시 서버 서명값이 유효하면 특정 사용자 특정 아이덴티티 클레임을 분산원장에 등록(S63)하게 된다. 그리고, 블록체인 네트워크의 적어도 하나의 블록체인 노드(300)는 특정 사용자 특정 아이덴티티 클레임 등록 트랜잭션 아이디를 프록시 서버(150)로 전송(S64-1)하게 되며, 프록시 서버(150)가 특정 사용자 특정 아이덴티티 클레임 등록 트랜잭션 아이디를 특정 인증기관 서버(200)로 전송(S64-2)하여 준다.

[0113] 또한, 특정 사용자 단말(100)을 통해 특정 사용자 특정 아이덴티티 클레임 승인 트랜잭션을 프록시 서버(150)로 전송(S68-1)하여 주며, 프록시 서버(150)가 특정 사용자 특정 아이덴티티 클레임 승인 트랜잭션과 이를 프록시 서버 마스터 프라이빗 키로 서명한 제1 프록시 서버 서명값을 전송(S68-2)한다. 그러면, 블록체인 네트워크의 적어도 하나의 블록체인 노드(300)는 제1 프록시 서버 서명값을 검증하여 제1 프록시 서버 서명값이 유효한 경우 특정 사용자 클레임 스마트 컨트랙트를 실행하여 특정 사용자 특정 아이덴티티 클레임 승인 트랜잭션이 분산원장에 등록(S69)되도록 한다. 그리고, 블록체인 네트워크의 적어도 하나의 블록체인 노드(300)는 특정 사용자 특정 아이덴티티 클레임 승인 트랜잭션 아이디를 프록시 서버(150)로 전송(S78-1)하게 되며, 프록시 서버(150)가 특정 사용자 특정 아이덴티티 클레임 승인 트랜잭션 아이디를 특정 사용자 단말(100)로 전송(S70-2)하게 된다.

[0114] 이를 통해, 도 7a에서는 특정 사용자 단말(100) 및 특정 인증기관 서버(200)가 트랜잭션 피를 지급하였으나, 도 7b에서는 프록시 서버(150)가 사용자 단말(100) 및 특정 인증기관 서버(200)를 대신하여 트랜잭션 피를 지급하도록 할 수 있다.

[0115] 상기에서는 새로운 특정 사용자 특정 아이덴티티 클레임을 등록하는 동작을 설명하였으나, 같은 방법에 의해 기등록되어 있는 특정 사용자 특정 아이덴티티 클레임을 업데이트할 수 있다. 즉, 등록하고자 하는 특정 아이덴티

티에 대응하는 이전의 아이덴티티 클레임이 있을 경우, 동일한 특정 아이덴티티 클레임에 대한 등록 요청이 있을 경우, 이를 분산원장에 등록하고, 새롭게 등록된 특정 아이덴티티 클레임을 특정 사용자의 특정 아이덴티티에 대응하는 클레임으로 업데이트한다. 이때, 특정 아이덴티티에 대응하는 클레임의 확인은 기설정된 토픽을 이용할 수 있으며, 동일한 토픽에 대해서 새로운 클레임이 등록될 경우, 사용자 아이덴티티 클레임에 대한 업데이트인 것을 인지할 수 있다. 하지만, 이에 한정되지 않으며, 클레임을 등록 클레임, 업데이트 클레임, 삭제 클레임 등과 같이 각각의 클레임의 기능을 정의하여 수행할 수도 있다.

[0116] 도 8a를 참조하여 본 발명의 일 실시예에 따른 블록체인 네트워크를 이용하여 사용자 아이덴티티를 관리하는 방법에서 특정 아이덴티티 클레임을 삭제하는 방법을 설명한다.

[0117] 도 7a에서와 같은 방법에 의해 특정 사용자 특정 아이덴티티 클레임이 등록된 상태에서, 특정 사용자 단말(100)이 사용자의 선택에 따라 특정 사용자 특정 아이덴티티 클레임을 삭제하기 위하여 블록체인 네트워크로 특정 사용자 특정 아이덴티티 클레임 삭제 요청 트랜잭션을 전송(S81)한다. 이때, 특정 사용자 특정 아이덴티티 클레임 삭제 요청 트랜잭션은 특정 사용자 특정 아이덴티티 클레임 아이디를 이용한 특정 사용자 특정 아이덴티티 삭제 클레임 데이터와, 특정 사용자 특정 아이덴티티 삭제 클레임 데이터를 특정 사용자 마스터 프라이빗 키로 서명한 제1 특정 사용자 서명값을 포함할 수 있다.

[0118] 그러면, 블록체인 네트워크의 적어도 하나의 블록체인 노드(300)는 제1 특정 사용자 서명값을 검증하여 제1 특정 사용자 서명값이 유효한 경우, 특정 사용자 스마트 컨트랙트를 실행하여 특정 사용자 특정 아이덴티티 클레임 아이디에 대응되는 특정 사용자 특정 아이덴티티 클레임을 삭제하기 위한 특정 사용자 특정 아이덴티티 클레임 삭제 트랜잭션이 분산원장에 등록(S82)되도록 한다.

[0119] 그리고, 블록체인 네트워크의 적어도 하나의 블록체인 노드(300)는 특정 사용자 특정 아이덴티티 클레임 삭제 트랜잭션 아이디를 특정 사용자 단말(100)로 전송(S83)하여 주며, 특정 사용자 단말(100)은 특정 사용자 특정 아이덴티티 클레임 삭제 트랜잭션 아이디를 이용하여 삭제하고자 하는 특정 사용자 특정 아이덴티티 클레임이 분산원장에서 삭제되었는지를 확인(S84)(S85)한다.

[0120] 또한, 도 8b를 참조하면, 특정 사용자 단말(100)은 프록시 서버(150)로 특정 사용자 특정 아이덴티티 클레임 삭제 요청 트랜잭션을 전송(S81-1)하며, 프록시 서버(150)가 특정 사용자 특정 아이덴티티 클레임 삭제 요청 트랜잭션과 이를 프록시 서버 마스터 프라이빗 키로 서명한 프록시 서버 서명값을 블록체인 네트워크로 전송(S81-2)한다.

[0121] 그러면, 블록체인 네트워크의 적어도 하나의 블록체인 노드(300)는 프록시 서버 서명값을 검증(S81-3)하고, 프록시 서버 서명값이 유효하면 특정 사용자 특정 아이덴티티 클레임 삭제 요청 트랜잭션에 포함된 제1 특정 사용자 서명값을 검증한 다음 특정 사용자 특정 아이덴티티 클레임을 삭제하기 위한 특정 사용자 특정 아이덴티티 클레임 삭제 트랜잭션이 분산원장에 등록(S82)되도록 한다.

[0122] 그리고, 블록체인 네트워크의 적어도 하나의 블록체인 노드(300)는 특정 사용자 특정 아이덴티티 클레임 삭제 트랜잭션 아이디를 프록시 서버(150)로 전송(S83-1)하며, 프록시 서버(150)가 특정 사용자 특정 아이덴티티 클레임 삭제 트랜잭션 아이디를 특정 사용자 단말(100)로 전송(S83-2)하여 준다.

[0123] 이를 통해, 도 8a에서는 사용자 단말(100)이 트랜잭션 피를 지급하였으나, 도 8b에서는 프록시 서버(150)가 사용자 단말(100)을 대신하여 트랜잭션 피를 지급하도록 할 수 있다.

[0124] 도 9a를 참조하여 본 발명의 일 실시예에 따른 블록체인 네트워크를 이용하여 사용자 아이덴티티를 관리하는 방법에서 특정 아이덴티티 클레임을 삭제하는 다른 방법을 설명한다.

[0125] 도 7a에서와 같은 방법에 의해 특정 사용자 특정 아이덴티티 클레임이 등록된 상태에서, 특정 인증기관 서버(200)가 특정 사용자 특정 아이덴티티 클레임을 삭제하기 위하여 블록체인 네트워크로 특정 사용자 특정 아이덴티티 클레임 삭제 요청 트랜잭션을 전송(S91)한다. 이때, 특정 사용자 특정 아이덴티티 클레임 삭제 요청 트랜잭션은 특정 사용자 특정 아이덴티티 클레임 아이디를 이용한 특정 사용자 특정 아이덴티티 삭제 클레임 데이터와, 특정 사용자 특정 아이덴티티 삭제 클레임 데이터를 특정 인증기관 마스터 프라이빗 키로 서명한 제3 특정 인증기관 서명값을 포함할 수 있다.

[0126] 그러면, 블록체인 네트워크의 적어도 하나의 블록체인 노드(300)는 제3 특정 인증기관 서명값을 검증하여 제3 특정 인증기관 서명값이 유효한 경우, 특정 사용자 스마트 컨트랙트를 실행하여 특정 사용자 특정 아이덴티티 클레임 아이디에 대응되는 특정 사용자 특정 아이덴티티 클레임을 삭제하기 위한 특정 사용자 특정 아이덴티티

클레임 삭제 트랜잭션이 분산원장에 등록되도록 한다.

[0127] 그리고, 블록체인 네트워크의 적어도 하나의 블록체인 노드(300)는 특정 사용자 특정 아이덴티티 클레임 삭제 트랜잭션 아이디를 특정 인증기관 서버(200)로 전송(S92)하여 주며, 특정 인증기관 서버(200)는 특정 사용자 특정 아이덴티티 클레임 삭제 트랜잭션 아이디를 이용하여 분산원장에 등록된 상기 특정 사용자 특정 아이덴티티 삭제 클레임의 아이디인 특정 사용자 특정 아이덴티티 삭제 클레임 아이디를 확인(S93)(S94)한다.

[0128] 이후, 특정 인증기관 서버(200)는 특정 사용자 특정 아이덴티티 삭제 클레임 아이디를 특정 사용자 단말(100)로 전송(S95)하여 준다.

[0129] 그러면, 특정 사용자 단말(100)은 특정 사용자 특정 아이덴티티 클레임 삭제 승인 트랜잭션을 블록체인 네트워크로 전송(S96)하여 준다. 이때, 특정 사용자 특정 아이덴티티 클레임 삭제 승인 트랜잭션은 특정 사용자 특정 아이덴티티 클레임 삭제 승인 데이터와 이를 특정 사용자 마스터 프라이빗 키로 서명한 제2 특정 사용자 서명값을 포함할 수 있으며, 특정 사용자 특정 아이덴티티 클레임 삭제 승인 데이터는 특정 사용자 특정 아이덴티티 삭제 클레임 아이디와 특정 사용자 특정 아이덴티티 삭제 클레임에 대한 승인 정보를 포함할 수 있다.

[0130] 그리고, 블록체인 네트워크의 적어도 하나의 블록체인 노드(300)는 제2 특정 사용자 서명값을 검증하여 제2 특정 사용자 서명값이 유효한 경우, 특정 사용자 클레임 스마트 컨트랙트를 실행하여 삭제하고자 하는 특정 사용자 특정 아이덴티티 클레임이 분산원장에서 삭제(S97)되도록 한다.

[0131] 이후, 블록체인 네트워크의 적어도 하나의 블록체인 노드(300)는 특정 사용자 특정 아이덴티티 클레임 삭제 승인 트랜잭션 아이디를 특정 사용자 단말(100)로 전송(S98)하여 주며, 특정 사용자 단말(100)은 특정 사용자 특정 아이덴티티 클레임 삭제 승인 트랜잭션 아이디를 이용하여 삭제하고자 하는 특정 사용자 특정 아이덴티티 클레임이 분산원장에서 삭제되었는지를 확인(S99)(S100)한다.

[0132] 또한, 도 9b를 참조하면, 특정 인증기관 서버(200)가 프록시 서버(150)로 특정 사용자 특정 아이덴티티 클레임 삭제 요청 트랜잭션을 전송(S91-1)하며, 프록시 서버(150)가 특정 사용자 특정 아이덴티티 삭제 요청 트랜잭션과 이를 프록시 서버 마스터 프라이빗 키로 서명한 프록시 서버 서명값을 블록체인 네트워크로 전송(S91-2)한다.

[0133] 그러면, 블록체인 네트워크의 적어도 하나의 블록체인 노드(300)는 프록시 서버 서명값을 검증하여 프록시 서버 서명값이 유효한 경우, 특정 사용자 스마트 컨트랙트를 실행하여 특정 사용자 특정 아이덴티티 클레임 아이디에 대응되는 특정 사용자 특정 아이덴티티 클레임을 삭제하기 위한 특정 사용자 특정 아이덴티티 클레임 삭제 트랜잭션이 분산원장에 등록되도록 한다.

[0134] 그리고, 블록체인 네트워크의 적어도 하나의 블록체인 노드(300)는 특정 사용자 특정 아이덴티티 클레임 삭제 트랜잭션 아이디를 프록시 서버(150)로 전송(S92-1)하고, 프록시 서버(150)가 특정 사용자 특정 아이덴티티 클레임 삭제 트랜잭션 아이디를 특정 인증기관 서버(200)로 전송(S92-2)하여 준다.

[0135] 또한, 특정 사용자 단말(100)은 프록시 서버(150)로 특정 사용자 특정 아이덴티티 삭제 승인 트랜잭션을 전송(S96-1)하여 주며, 프록시 서버(150)는 특정 사용자 특정 아이덴티티 클레임 삭제 승인 트랜잭션을 블록체인 네트워크로 전송(S96-2)하여 준다.

[0136] 그리고, 블록체인 네트워크의 적어도 하나의 블록체인 노드(300)는 특정 사용자 특정 아이덴티티 클레임 삭제 승인 트랜잭션 아이디를 프록시 서버(150)로 전송(S98-1)하여 주며, 프록시 서버(150)는 특정 사용자 특정 아이덴티티 클레임 삭제 승인 트랜잭션 아이디를 특정 사용자 단말(100)로 전송(S98-2)하여 준다.

[0137] 이를 통해, 도 9a에서는 특정 사용자 단말(100) 및 특정 인증기관 서버(200)가 트랜잭션 피를 지급하였으나, 도 9b에서는 프록시 서버(150)가 사용자 단말(100) 및 특정 인증기관 서버(200)를 대신하여 트랜잭션 피를 지급하도록 할 수 있다.

[0138] 상기에서와 같은 방법에 의해 셀프 클레임, 아이덴티티 클레임들을 생성할 경우, 클레임을 생성하는 주체, 클레임의 소유주, 클레임을 이용하는 주체 등에 각각의 클레임에 대응하는 성취도를 제공할 수 있으며, 성취도에 대응하는 보상을 제공할 수 있다. 이때, 성취도 현황 및 보상 지급 현황 등은 상기에서의 설명한 것과 유사한 방법에 의해 블록체인 네트워크를 통해 관리할 수 있다. 즉, 주체가 획득한 각각의 성취도들을 셀프 클레임과 유사한 방법으로 블록체인 네트워크에 등록하며, 성취도들 중 보상을 원하는 특정 보상들을 아이덴티티 클레임과 유사한 방법으로 블록체인 네트워크에 등록하여 관리할 수 있다.

[0139] 도 10a와 도 10b를 참조하여 본 발명의 일 실시예에 다른 블록체인 네트워크 기반의 사용자 아이덴티티를 이용하여 사용자를 인증하는 방법을 설명한다.

[0140] 먼저, 도 10a를 참조하여 블록체인 네트워크 기반의 사용자 아이덴티티를 이용하여 사인 업(sign up)을 수행하는 방법을 설명한다.

[0141] 사용자들의 아이덴티티들에 대한 클레임을 생성하도록 하는 클레임 스마트 컨트렉트가 사용자들에 각각 대응하여 사용자 클레임 스마트 컨트랙트들로 다수의 블록체인 노드들에 의해 구성되는 블록체인 네트워크의 분산원장에 등록되며, 사용자 클레임 스마트 컨트랙트들에 대한 분산원장 상의 어드레스들이 사용자들의 아이디들로 관리되고, 사용자들에 각각 대응되는 사용자 아이덴티티들을 가공한 사용자 특정값들을 포함하는 각각의 사용자 셀프 클레임들, 사용자 아이덴티티들 각각에 대하여 적어도 하나의 인증기관이 인증하여 등록한 사용자 아이덴티티 클레임들, 및 사용자 키에 대응하는 사용자 어드레스들이 분산원장 상에 등록되어 관리되는 상태에서, 사용자가 서비스 이용 단말(110)을 통해 서비스 제공 서버(500)로 사인 업을 요청(S111)하면, 서비스 제공 서버(500)는 서비스 이용 단말(110)로 사인 업에 필요한 사용자 특정 정보를 요청(S112)한다. 이때, 서비스 이용 단말(110)에서 앱(application) 또는 웹(web)을 통해 서비스 제공 서버(500)로 접속할 수 있으며, 서비스 제공 서버(500)는 사용자 특정 정보 요청에 콜백(callback) URL 또는 URL scheme을 추가하여 서비스 제공 서버(500)로의 접속 정보를 제공하여 줄 수 있다.

[0142] 그리고, 서비스 이용 단말(110)은 서비스 제공 서버(500)로부터의 사용자 특정 정보 요청을 사용자 단말(100)로 전송(S113)하여 준다. 이때, 서비스 이용 단말(110)은 사용자 단말(100)과 동일한 단말이거나 서로 다른 단말일 수 있다.

[0143] 그러면, 사용자 단말(100)은 사용자 아이덴티티 관리 앱을 통해 서비스 제공 서버(500)로부터 요청된 사용자 특정 정보를 확인(S114)한다. 이때, 사용자 단말(100)은 요청된 사용자 특정 정보에 대응하는 사용자 특정 아이덴티티들의 사용자 특정 아이덴티티 클레임들이 블록체인 네트워크의 분산원장 상에 등록된 상태인지를 확인한다.

[0144] 그리고, 사용자 단말(100)은 요청된 사용자 특정 정보를 서비스 제공 단말(500)로 제공(S115)하여 준다.

[0145] 이때, 사용자 단말(100)은 요청된 사용자 특정 정보에 대응하는 사용자 특정 아이덴티티 클레임들이 분산원장에 등록된 상태일 경우에는, 특정 사용자 아이디, 특정 사용자 특정 정보에 대응되는 사용자 특정 아이덴티티, 특정 사용자 특정 아이덴티티 클레임 아이디, 사용자 셀프 클레임 아이디, 특정 사용자 특정값, 특정 사용자 특정 아이덴티티를 이용한 특정 사용자 특정값의 생성 정보, 및 특정 사용자 특정값을 특정 사용자 프라이빗 키로 서명한 특정 사용자 서명값을 포함하는 특정 사용자 클레임 정보를 서비스 제공 서버(500)로 제공하여 줄 수 있다.

[0146] 그러면, 서비스 제공 서버(500)는 특정 사용자 특정값 및 특정 사용자 특정 아이덴티티를 이용한 특정 사용자 특정값의 생성 정보를 참조하여 특정 사용자 특정값의 생성 정보가 유효한지를 확인하고, 특정 사용자 특정값의 생성 정보가 유효하면 특정 사용자 서명값이 유효한지를 확인(S116)한다.

[0147] 이때, 특정 사용자 특정값은 특정 사용자 아이덴티티들 각각에 대한 해시값들이 각각의 리프 노드들 중 적어도 일부에 할당된 머클트리의 루트 해시값이며, 특정 사용자 특정 아이덴티티를 이용한 특정 사용자 특정값의 생성 정보는 특정 사용자 특정 아이덴티티에 대한 머클트리정보일 수 있으며, 이 경우, 서비스 제공 서버(500)는 머클트리 정보와 특정 사용자 특정 아이덴티티를 이용하여 비교 대상 루트 해시값을 생성하며, 비교 대상 루트 해시값과 루트 해시값이 일치하는지를 확인하여 특정 사용자 특정값의 생성 정보가 유효한지를 확인할 수 있다.

[0148] 또한, 서비스 제공 서버(500)는 분산원장에 등록된 디지털 서명 검증 모듈을 실행하여 특정 사용자 서명값과 특정 사용자 특정값을 참조하여 특정 사용자 프라이빗 키에 대응되는 특정 사용자 퍼블릭 키를 획득하거나, 사용자 단말(100)이 특정 사용자 클레임 정보에 특정 사용자 프라이빗 키에 대응되는 특정 사용자 퍼블릭 키를 포함하여 전송함으로써 특정 사용자 클레임 정보로부터 특정 사용자 퍼블릭 키를 획득할 수 있으며, 특정 사용자 퍼블릭 키를 이용하여 특정 사용자 서명값으로부터 확인되는 비교 대상 데이터와 특정 사용자 특정값이 일치하는지를 확인함으로써 특정 사용자 서명값이 유효한지를 확인할 수 있다.

[0149] 그리고, 서비스 제공 서버(500)는 특정 사용자 서명값이 유효한 경우, 특정 사용자 셀프 클레임 아이디 및 특정 사용자 특정 아이덴티티 클레임 아이디를 참조하여 분산원장에 등록된 특정 사용자 셀프 클레임 및 특정 사용자 특정 아이덴티티 클레임을 확인(S117)(S118)하고, 확인된 특정 사용자 셀프 클레임 및 특정 사용자 특정 아이덴티티 클레임을 참조하여 특정 사용자 클레임 정보를 인증(S119)한다.

[0150] 이때, 서비스 제공 서버(500)는 특정 사용자 셀프 클레임을 이용하여 특정 사용자 특정값을 검증하고, 특정 사용자 특정 아이덴티티 클레임을 이용하여 특정 사용자 특정 아이덴티티를 검증할 수 있다.

[0151] 또한, 서비스 제공 서버(500)는 특정 사용자 특정값 및 특정 사용자 특정 아이덴티티를 검증한 다음 특정 사용자 특정 아이덴티티 클레임을 생성한 인증기관을 확인하며, 인증기관이 신뢰성이 있는 것으로 판단될 경우 특정 사용자 특정 아이덴티티가 유효한 것으로 인증할 수 있다.

[0152] 이후, 서비스 제공 서버(500)는 특정 사용자 클레임 정보가 인증되면 특정 사용자의 사인 업을 허용(S120)한다. 일 예로, 서비스 제공 서버(500)는 특정 사용자 아이디를 서비스 제공 서버(500)의 유저 아이디로 등록할 수 있다.

[0153] 그리고, 리플레이 어택을 방지하기 위하여, 사용자 단말(100)은 특정 사용자 클레임 정보에 타임스탬프를 포함시키고, 특정 사용자 특정값과 타임스탬프를 특정 사용자 프라이빗 키로 서명하여 특정 사용자 서명값을 생성하여 전송할 수 있으며, 서비스 제공 서버(500)는 특정 사용자 서명값이 유효한지 확인한 다음, 타임스탬프의 유효성을 확인할 수 있다.

[0154] 한편, 사용자 단말(100)은 요청된 사용자 특정 정보에 대응하는 사용자 특정 아이덴티티 클레임들이 분산원장에 등록되어 있지 않은 상태일 경우에는, 특정 사용자 아이디, 특정 사용자 특정 아이덴티티, 특정 사용자 셀프 클레임 아이디, 특정 사용자 특정값, 특정 사용자 특정 아이덴티티를 이용한 특정 사용자 특정값의 생성 정보, 및 특정 사용자 특정값을 특정 사용자 프라이빗 키로 서명한 특정 사용자 서명값을 포함하는 특정 사용자 클레임 정보를 서비스 제공 서버(500)로 제공하여 줄 수 있다.

[0155] 그러면, 서비스 제공 서버(500)는 사용자 서명값을 확인(S116)한 다음, 특정 사용자 셀프 클레임 아이디를 참조하여 분산원장에 등록된 특정 사용자 셀프 클레임을 확인(S117)(S118)하고, 확인된 특정 사용자 셀프 클레임을 참조하여 상기 특정 사용자 클레임 정보를 인증하고, 특정 사용자 특정 아이덴티티가 특정 사용자의 특징 정보와 일치하는 지를 확인하여 인증(S119)한 다음 특정 사용자의 사인 업을 허용(S120)할 수 있다. 이때, 특정 사용자 특정 아이덴티티가 특정 사용자의 특징 정보와 일치하는지를 확인하여 인증하는 것은, 서비스 제공 서버(500) 자체에서 특정 사용자 특정 아이덴티티를 인증하는 것일 수 있다. 예를 들어, 특정 아이덴티티가 전화번호일 경우 일반적인 전화번호 인증을 수행하여 해당 전화번호가 특정 사용자의 전화번호와 일치하는 지 확인할 수 있다.

[0156] 이에 더하여, 서비스 제공 서버(500)는 도 7a에서와 같은 방법에 의해 인증한 특정 아이덴티티에 대한 특정 사용자 특정 아이덴티티 클레임을 블록체인 네트워크의 분산원장에 등록(S121)할 수 있다.

[0157] 즉, 서비스 제공 서버(500)는 인증된 상기 특정 사용자 특정 아이덴티티를 참조하여, 서비스 제공 서버에 대응되는 서비스 제공 서버 아이디, 적어도 특정 사용자 특정 아이덴티티를 가공한 특정 아이덴티티 가공값, 및 특정 사용자 아이디와 특정 아이덴티티 가공값을 서비스 제공 서버(500)의 프라이빗 키로 서명한 제1 서비스 제공 서버 서명값을 포함하는 특정 사용자 특정 아이덴티티 클레임을 생성하며, 특정 사용자 특정 아이덴티티 클레임과 특정 사용자 특정 아이덴티티 클레임을 서비스 제공 서버의 프라이빗 키로 서명한 제2 서비스 제공 서버 서명값을 포함하는 특정 사용자 특정 아이덴티티 클레임 등록 요청 트랜잭션을 블록체인 네트워크로 전송한다. 그러면, 블록체인 네트워크의 적어도 하나의 블록체인 노드(300)가 제2 서비스 제공 서버 서명값을 검증하여 제2 서비스 제공 서버 서명값이 유효한 경우, 특정 사용자 스마트 컨트랙트를 실행하여 특정 사용자 특정 아이덴티티 클레임을 분산원장에 등록하게 된다.

[0158] 다음으로, 도 10b를 참조하여 블록체인 네트워크를 기반의 사용자 아이덴티티를 이용하여 서비스를 이용하는 방법을 설명한다.

[0159] 사용자들의 아이덴티티들에 대한 클레임을 생성하도록 하는 클레임 스마트 컨트렉트가 사용자들에 각각 대응하여 사용자 클레임 스마트 컨트랙트들로 다수의 블록체인 노드들에 의해 구성되는 블록체인 네트워크의 분산원장에 등록되며, 사용자 클레임 스마트 컨트랙트들에 대한 분산원장 상의 어드레스들이 사용자들의 아이디들로 관리되고, 사용자들에 각각 대응되는 사용자 아이덴티티들을 가공한 사용자 특정값들을 포함하는 각각의 사용자 셀프 클레임들, 사용자 아이덴티티들 각각에 대하여 적어도 하나의 인증기관이 인증하여 등록한 사용자 아이덴티티 클레임들, 및 사용자 키에 대응하는 사용자 어드레스들이 분산원장 상에 등록되어 관리되는 상태에서, 사용자가 서비스 이용 단말(110)을 통해 서비스 제공 서버(500)로 서비스 요청(S131)하면, 서비스 제공 서버(500)는 서비스 이용 단말(110)로 서비스 제공을 위한 특정 사용자 서명값을 요청(S132)한다. 이때, 서비스 이용 단말(110)에서 앱(application) 또는 웹(web)을 통해 서비스 제공 서버(500)로 접속할 수 있으며, 서비스 제공

서버(500)는 특정 사용자 서명값 요청에 콜백(callback) URL 또는 URL scheme을 추가하여 서비스 제공 서버(500)로의 접속 정보를 제공하여 줄 수 있다.

[0160] 그리고, 서비스 이용 단말(110)은 서비스 제공 서버(500)로부터의 사용자 서명값 요청을 사용자 단말(100)로 전송(S133)하여 준다. 이때, 서비스 이용 단말(110)은 사용자 단말(100)과 동일한 단말이거나 서로 다른 단말일 수 있다.

[0161] 그러면, 사용자 단말(100)은 사용자 아이덴티티 관리 앱을 통해 특정 사용자 서명값을 생성(S134)한다.

[0162] 이때, 사용자 단말(100)은 특정 사용자 서명값 요청에 대응되는 데이터를 확인하며, 데이터를 특정 사용자 프라이빗 키로 서명한 특정 사용자 서명값을 생성할 수 있다.

[0163] 또한, 데이터는 서비스 제공 서버(500)에서 생성되고, 특정 사용자 서명값 요청 정보에 포함된 것일 수 있으며, 거래 정보에 대한 데이터, 서비스 제공을 위하여 사용자가 확인을 하여야 하는 정보에 대한 데이터, 서명값 확인을 위한 논스에 대한 데이터 등을 포함할 수 있으나, 이에 한정되지 않으며, 서비스 제공과 관련하여 서비스 제공 서버(500)가 생성하는 모든 데이터를 포함할 수 있다.

[0164] 이에 더하여, 데이터는 서비스 제공 서버(500)에서 요청된 정보에 대응하여 사용자 단말(100)이 생성한 것일 수 있으며, 서비스 이용에 필요한 거래 정보에 대한 데이터, 로그인을 위한 특정 사용자 아이덴티티, 비밀 번호 등의 데이터, 서명값 확인에 이용하기 위한 논스에 대한 데이터 등을 포함할 수 있으나, 이에 한정되지 않으며, 서비스 이용과 관련하여 사용자 단말(100)이 생성하는 모든 데이터를 포함할 수 있다.

[0165] 이후, 사용자 단말(100)은 특정 사용자 아이디, 특정 사용자 어드레스, 데이터, 및 특정 사용자 서명값을 서비스 제공 서버(500)로 전송(S135)하여 준다.

[0166] 그러면, 서비스 제공 서버(500)는 특정 사용자 서명값이 유효한지를 확인(S136)하며, 특정 사용자 서명값이 유효한 경우 특정 사용자 아이디를 참조하여 블록체인 네트워크의 분산원장에 등록된 비교 대상 사용자 어드레스를 확인(S137)(S138)하고, 비교 대상 사용자 어드레스를 참조하여 특정 사용자 어드레스가 유효한지를 확인(S139)한 다음, 서비스 요청 단말(100)로 요청된 서비스를 제공(S140)하여 줄 수 있다.

[0167] 이때, 사용자 단말(100)에서 전송되는 데이터가 특정 사용자 특정 아이덴티티 및 특정 사용자 특정 아이덴티티 클레임 아이디를 포함할 경우, 서비스 제공 서버(500)는 특정 사용자 특정 아이덴티티 클레임 아이디를 참조하여 블록체인 네트워크의 분산원장에서 특정 사용자 특정 아이덴티티 클레임을 획득하도록 하며, 특정 사용자 특정 아이덴티티 클레임을 참조하여 특정 사용자 특정 아이덴티티를 검증할 수 있다.

[0168] 또한, 서비스 제공 서버(500)는 분산원장에 등록된 디지털 서명 검증 모듈을 실행하여 특정 사용자 서명값과 데이터를 참조하여 특정 사용자 프라이빗 키에 대응되는 특정 사용자 퍼블릭 키를 획득하거나, 사용자 단말(100)이 특정 사용자 프라이빗 키에 대응되는 특정 사용자 퍼블릭 키를 추가하여 전송함으로써 특정 사용자 퍼블릭 키를 획득할 수 있으며, 특정 사용자 퍼블릭 키를 이용하여 특정 사용자 서명값으로부터 확인되는 비교 대상 데이터와 데이터가 일치하는지를 확인함으로써 특정 사용자 서명값이 유효한지를 확인할 수 있다.

[0169] 또한, 이상 설명된 본 발명에 따른 실시예들은 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 상기 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0170] 이상에서 본 발명이 구체적인 구성요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나, 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명이 상기 실시예들에 한정되는 것은 아니며, 본 발명이 속하는 기술분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형을 꾀할 수 있다.

[0171] 따라서, 본 발명의 사상은 상기 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등하게 또는 등가적으로 변형된 모든 것들은 본 발명의 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0172] 100: 사용자 단말,

150: 프록시 서버

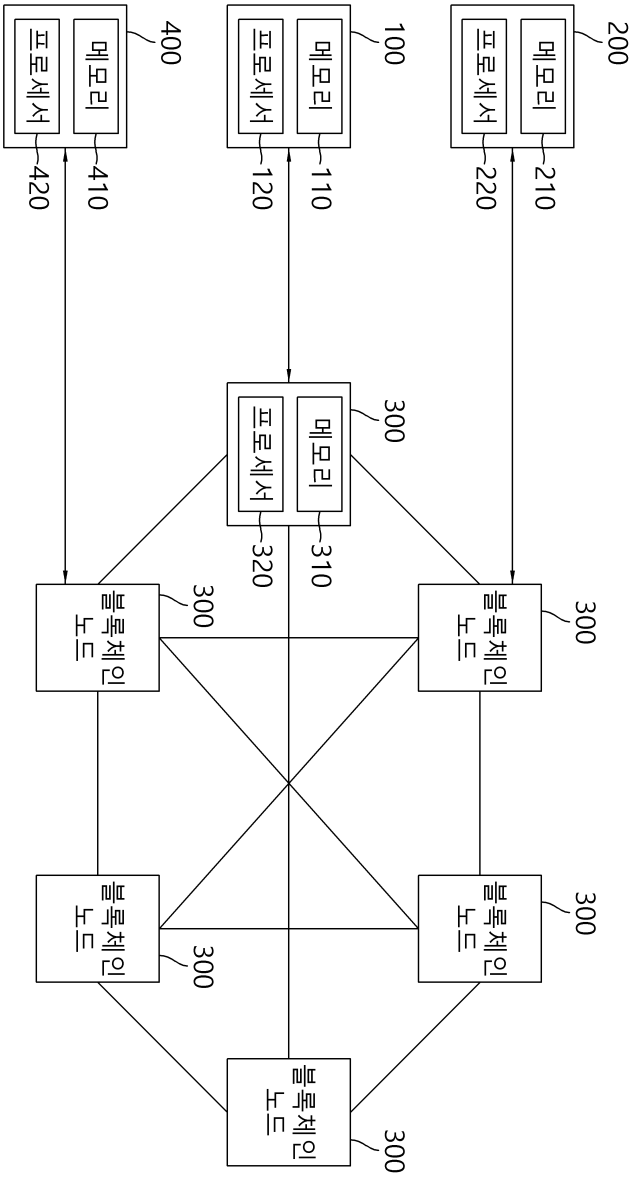
200: 인증기관 서버,

300: 블록체인 노드,

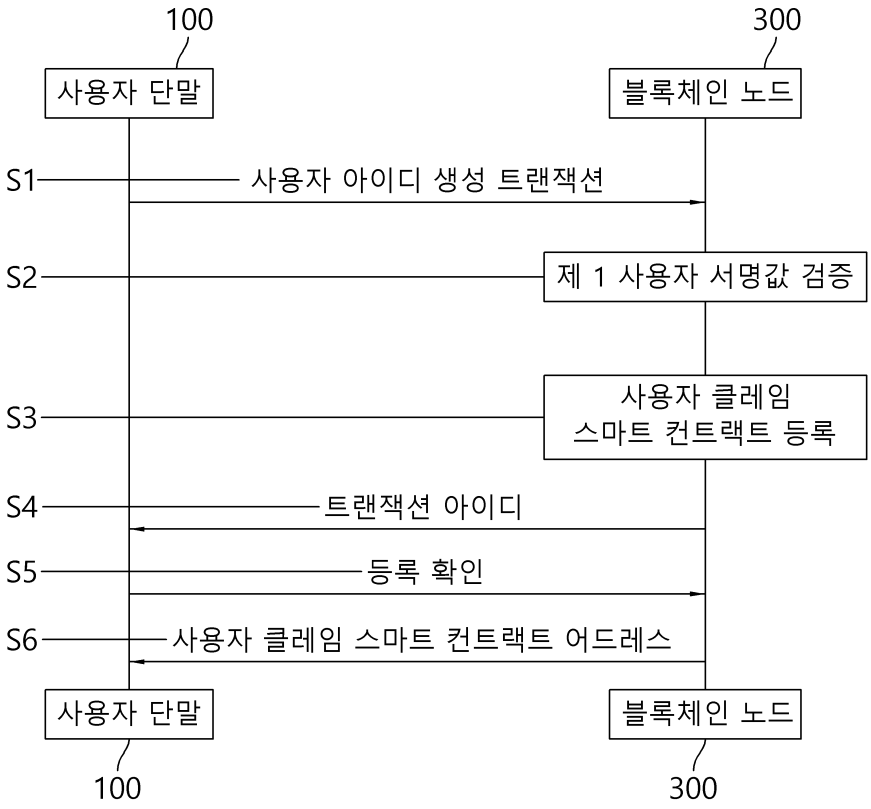
500: 서비스 제공 서버

도면

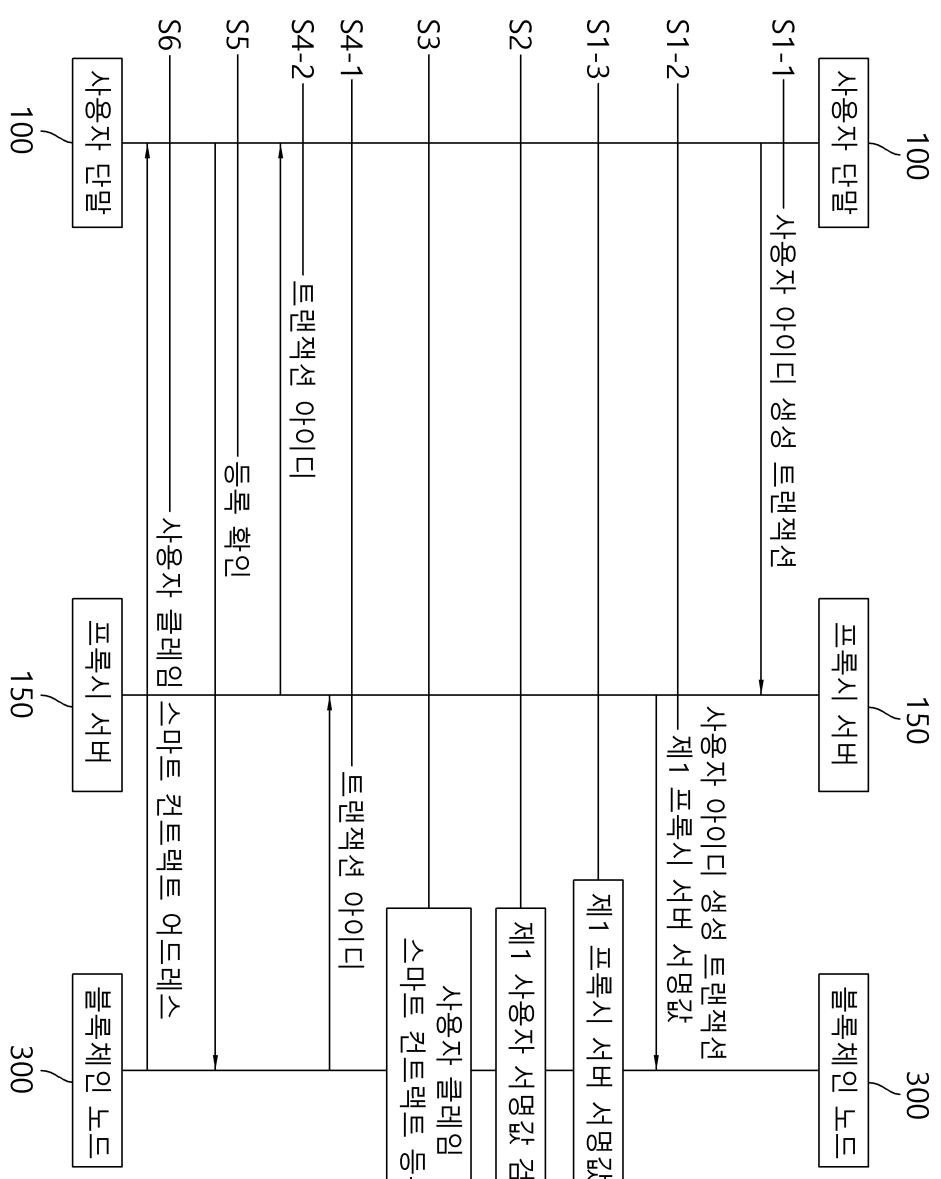
도면1



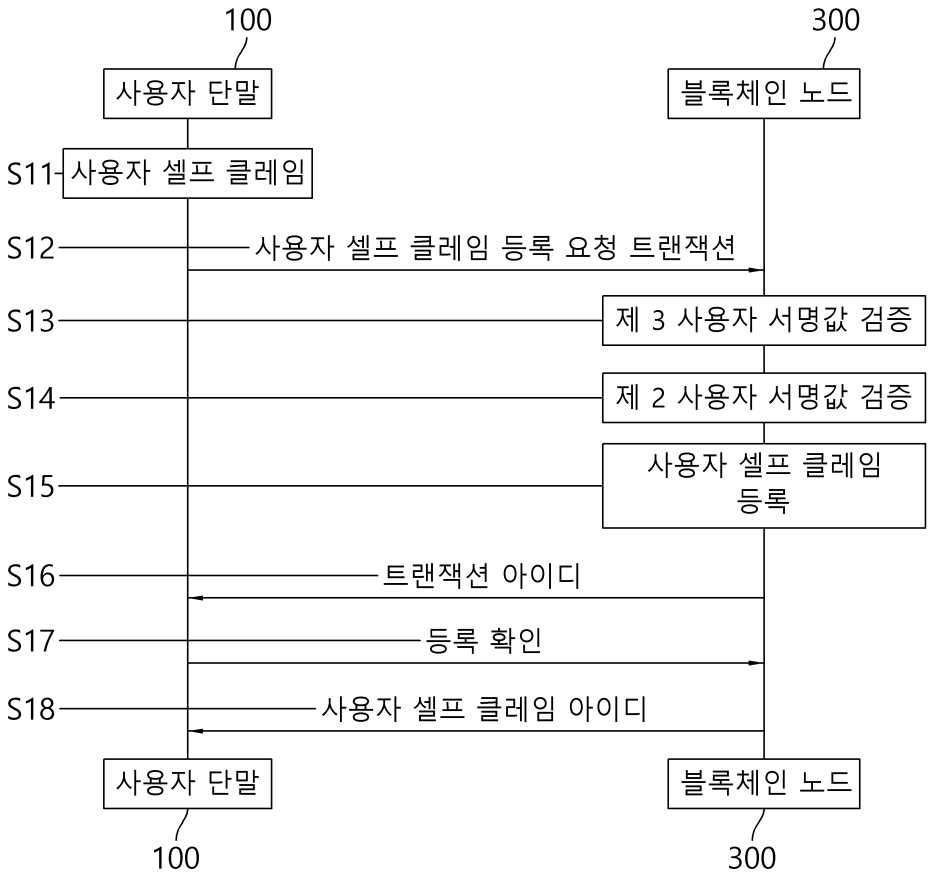
도면2a


100
300
사용자 단말
블록체인 노드
S1
사용자 아이디 생성 트랜잭션
S2
제 1 사용자 서명값 검증
S3
사용자 클레임
스마트 컨트랙트 등록
S4
트랜잭션 아이디
S5
등록 확인
S6
사용자 클레임 스마트 컨트랙트 어드레스
사용자 단말
블록체인 노드
100
300

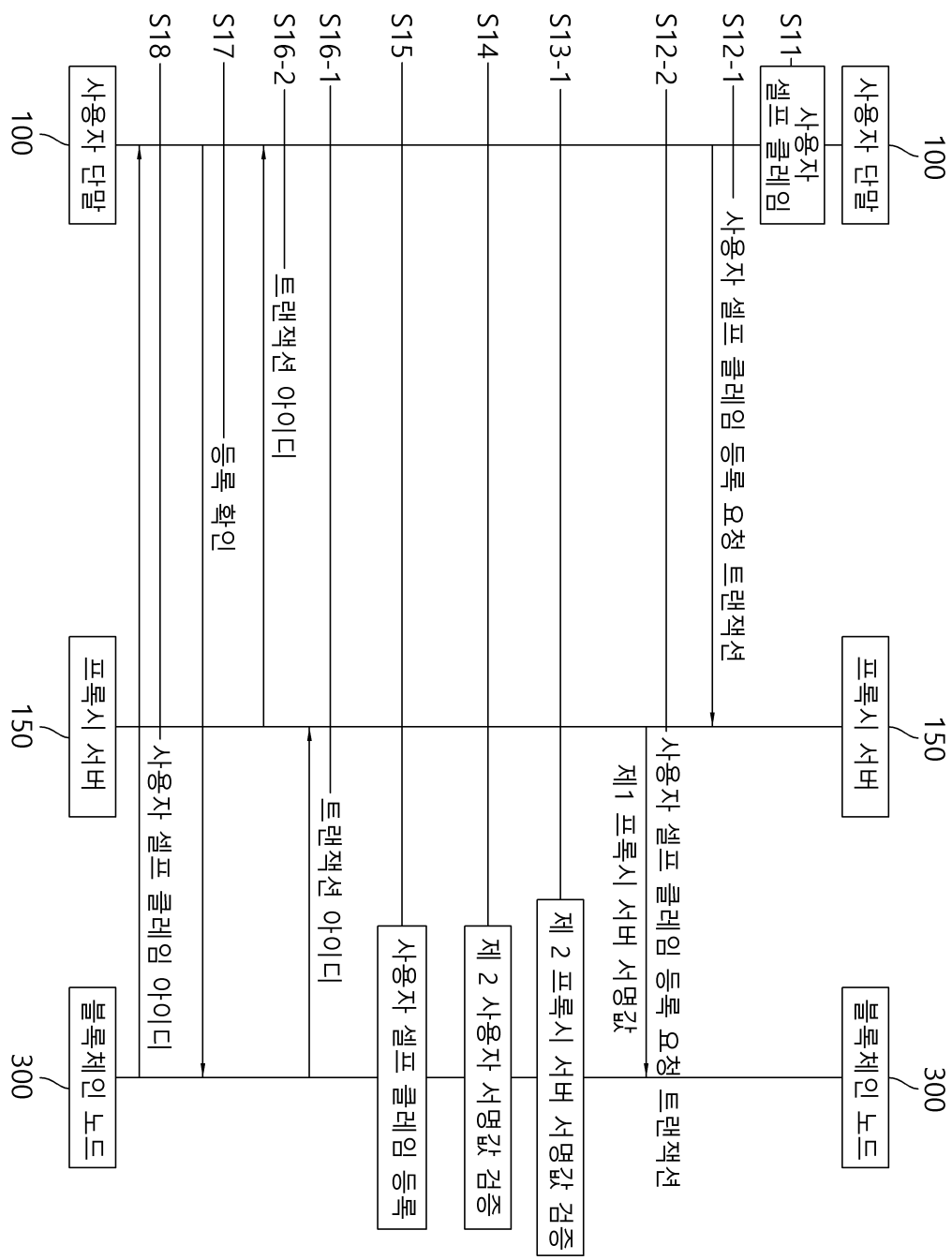
도면2b


사용자 단말
100
프록시 서버
150
블록체인 노드
300
S1-1
사용자 아이디 생성 트랜잭션
S1-2
사용자 아이디 생성 트랜잭션
제1 프록시 서버 서명값
S1-3
제1 프록시 서버 서명값 검증
S2
제1 사용자 서명값 검증
S3
사용자 클레임
스마트 컨트랙트 등록
S4-1
트랜잭션 아이디
S4-2
트랜잭션 아이디
S5
등록 확인
S6
사용자 클레임 스마트 컨트랙트 어드레스
사용자 단말
100
프록시 서버
150
블록체인 노드
300

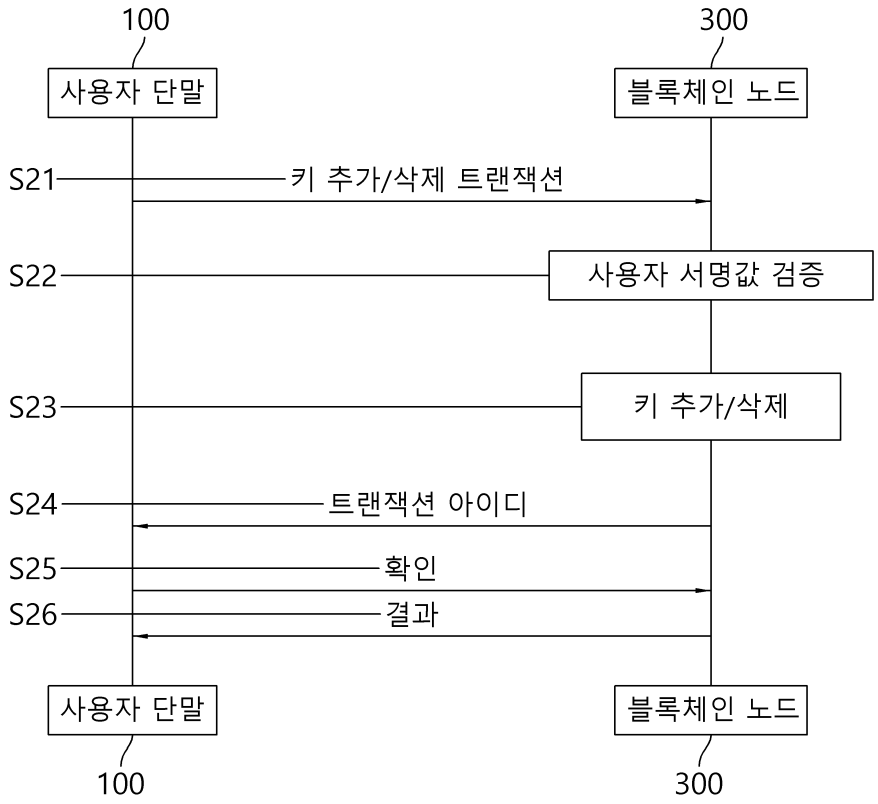
도면3a


100
사용자 단말
300
블록체인 노드
S11
사용자 셀프 클레임
S12
사용자 셀프 클레임 등록 요청 트랜잭션
S13
제 3 사용자 서명값 검증
S14
제 2 사용자 서명값 검증
S15
사용자 셀프 클레임 등록
S16
트랜잭션 아이디
S17
등록 확인
S18
사용자 셀프 클레임 아이디
사용자 단말
100
블록체인 노드
300

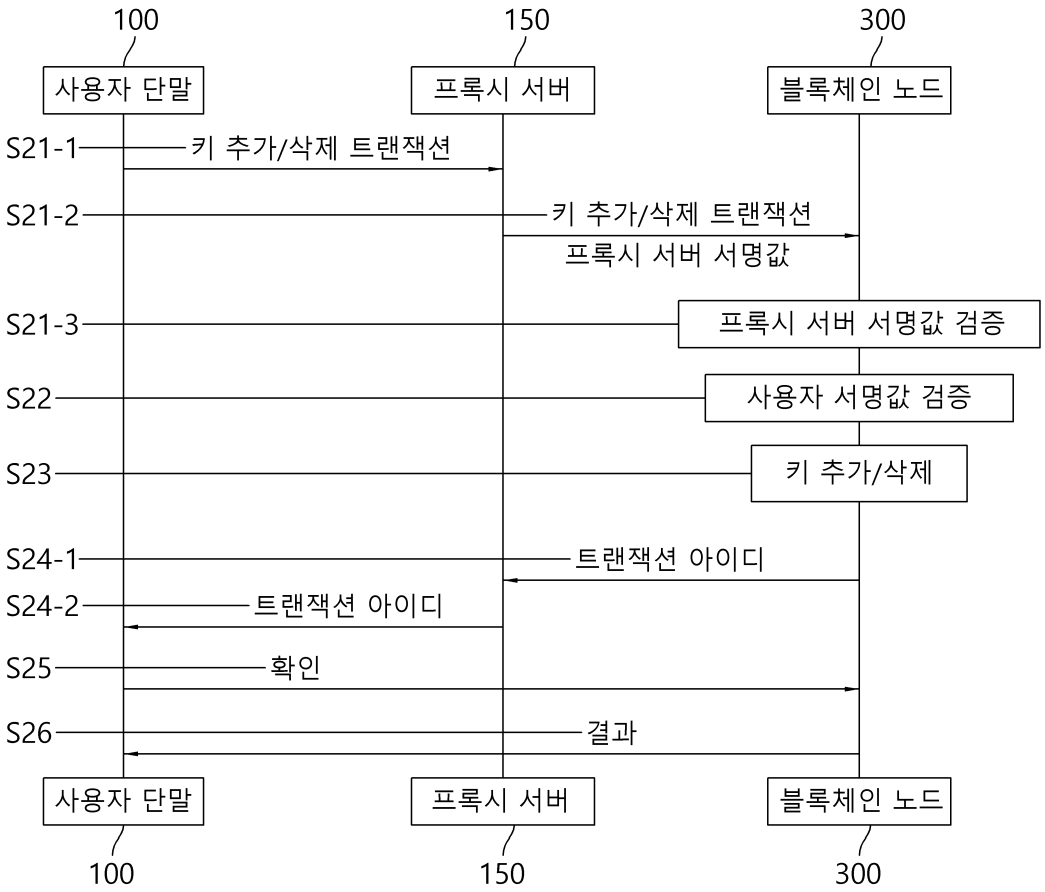
도면3b


100
사용자 단말
150
프록시 서버
300
블록체인 노드
S11
사용자 셀프 클레임
S12-1
사용자 셀프 클레임 등록 요청 트랜잭션
S12-2
사용자 셀프 클레임 등록 요청 트랜잭션
제1 프록시 서버 서명값
S13-1
제 2 프록시 서버 서명값 검증
S14
제 2 사용자 서명값 검증
S15
사용자 셀프 클레임 등록
S16-1
트랜잭션 아이디
S16-2
트랜잭션 아이디
S17
등록 확인
S18
사용자 셀프 클레임 아이디
100
사용자 단말
150
프록시 서버
300
블록체인 노드

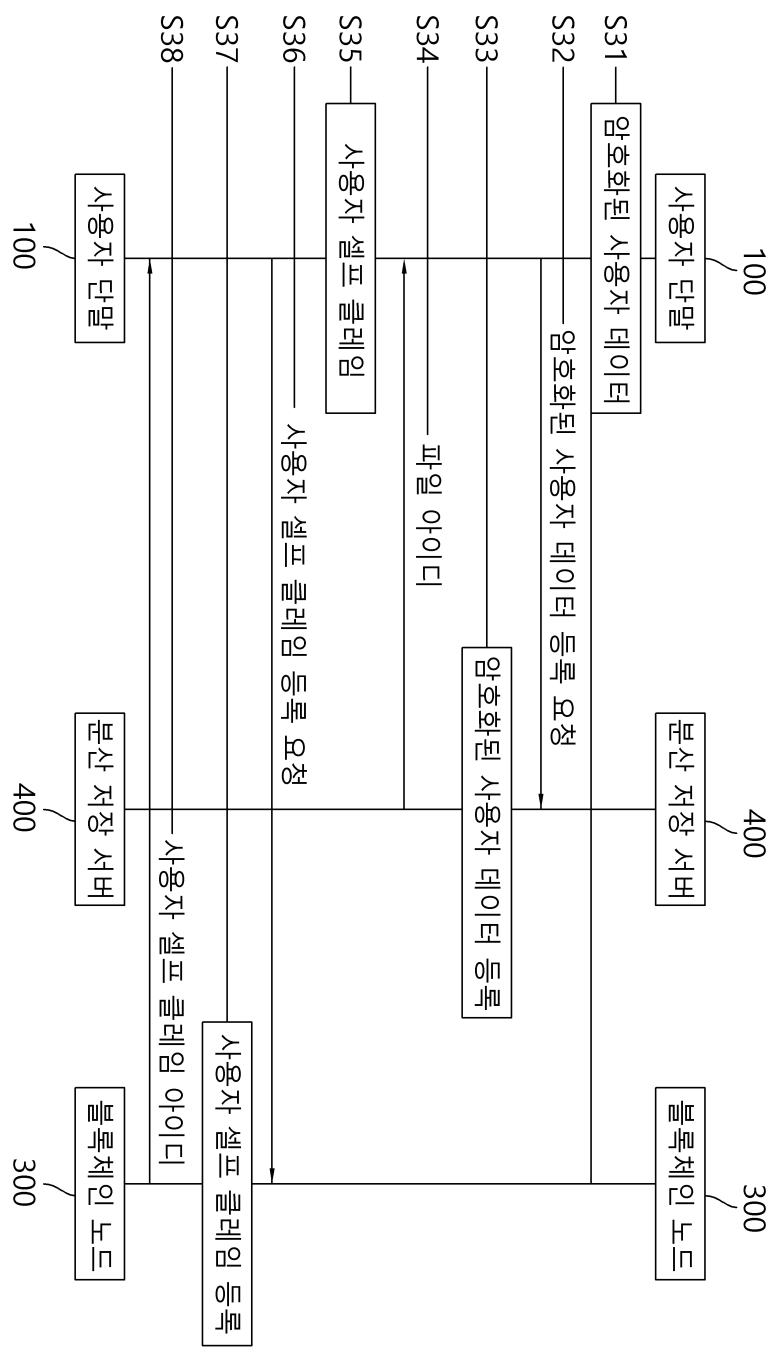
도면4a


100
300
사용자 단말
블록체인 노드
S21
키 추가/삭제 트랜잭션
S22
사용자 서명값 검증
S23
키 추가/삭제
S24
트랜잭션 아이디
S25
확인
S26
결과
사용자 단말
블록체인 노드
100
300

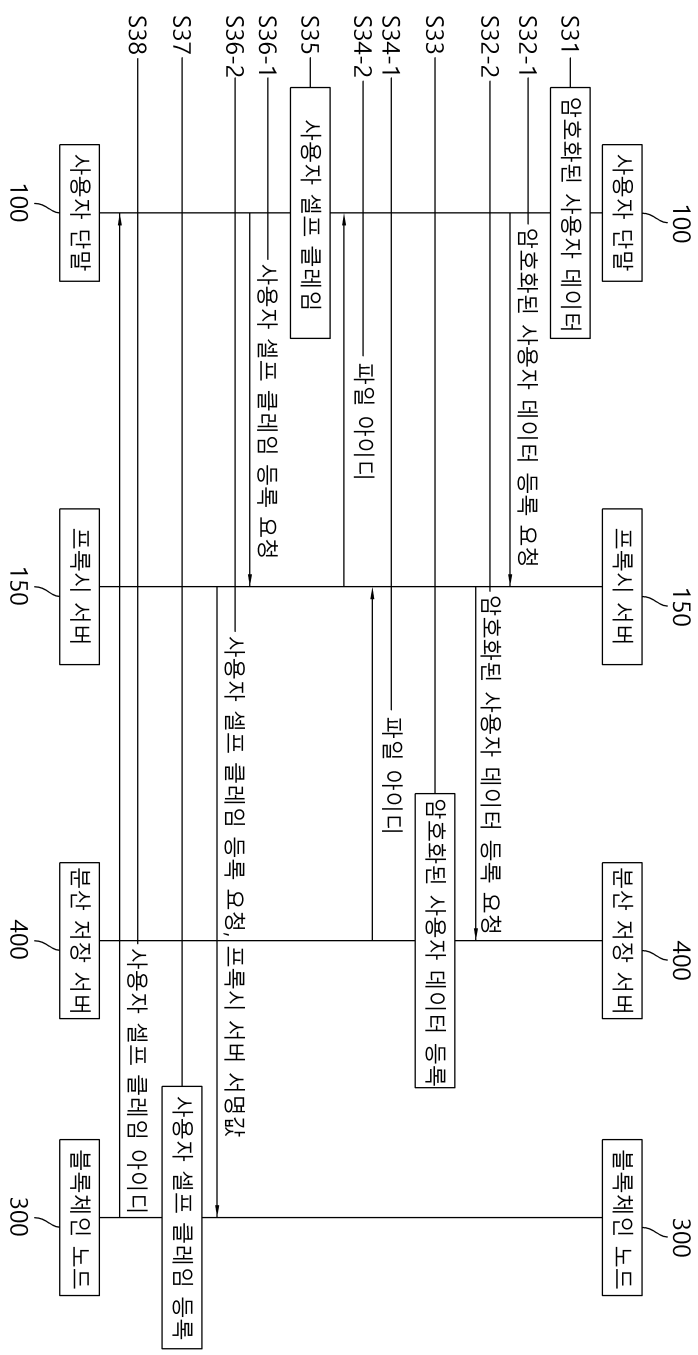
도면4b


100
150
300
사용자 단말
프록시 서버
블록체인 노드
S21-1
키 추가/삭제 트랜잭션
S21-2
키 추가/삭제 트랜잭션
프록시 서버 서명값
S21-3
프록시 서버 서명값 검증
S22
사용자 서명값 검증
S23
키 추가/삭제
S24-1
트랜잭션 아이디
S24-2
트랜잭션 아이디
S25
확인
S26
결과
사용자 단말
프록시 서버
블록체인 노드
100
150
300

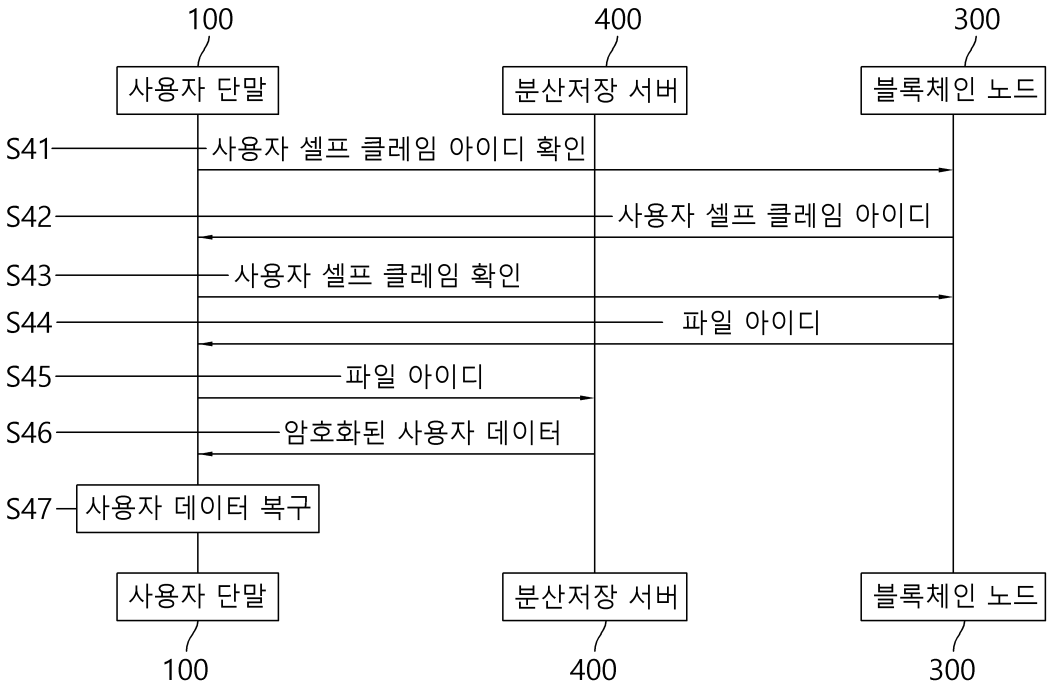
도면5a


사용자 단말
100
분산 저장 서버
400
블록체인 노드
300
S31
암호화된 사용자 데이터
S32
암호화된 사용자 데이터 등록 요청
S33
암호화된 사용자 데이터 등록
S34
파일 아이디
S35
사용자 셀프 클레임
S36
사용자 셀프 클레임 등록 요청
S37
사용자 셀프 클레임 등록
S38
사용자 셀프 클레임 아이디

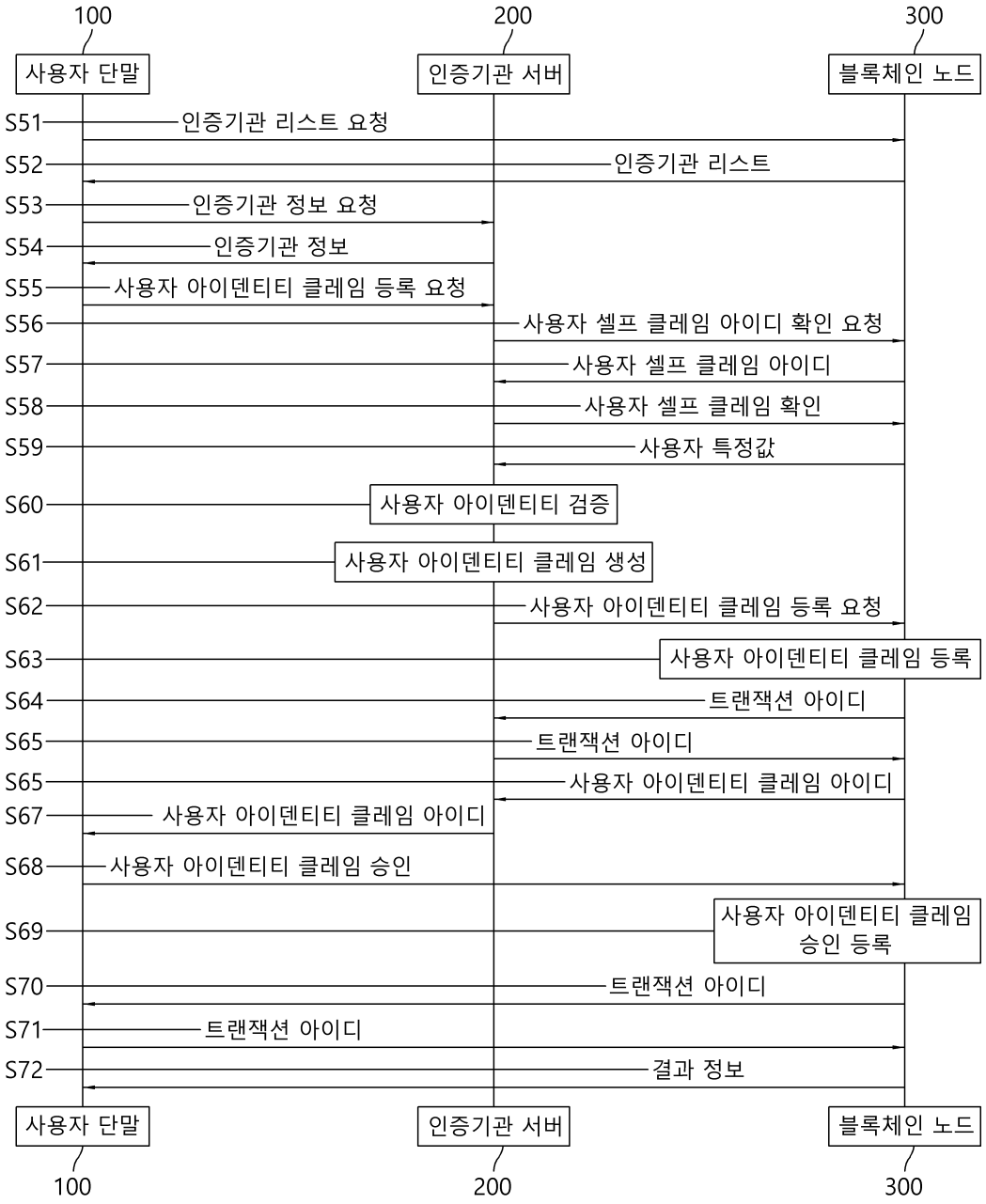
도면5b


사용자 단말
100
암호화된 사용자 데이터
암호화된 사용자 데이터 등록 요청
파일 아이디
사용자 셀프 클레임
사용자 셀프 클레임 등록 요청
파일 아이디
암호화된 사용자 데이터 등록
암호화된 사용자 데이터 등록 요청
사용자 셀프 클레임 등록 요청, 프록시 서버 서명값
사용자 셀프 클레임 아이디
사용자 셀프 클레임 등록
S31
S32-1
S32-2
S33
S34-1
S34-2
S35
S36-1
S36-2
S37
S38
사용자 단말
100
프록시 서버
150
분산 저장 서버
400
블록체인 노드
300

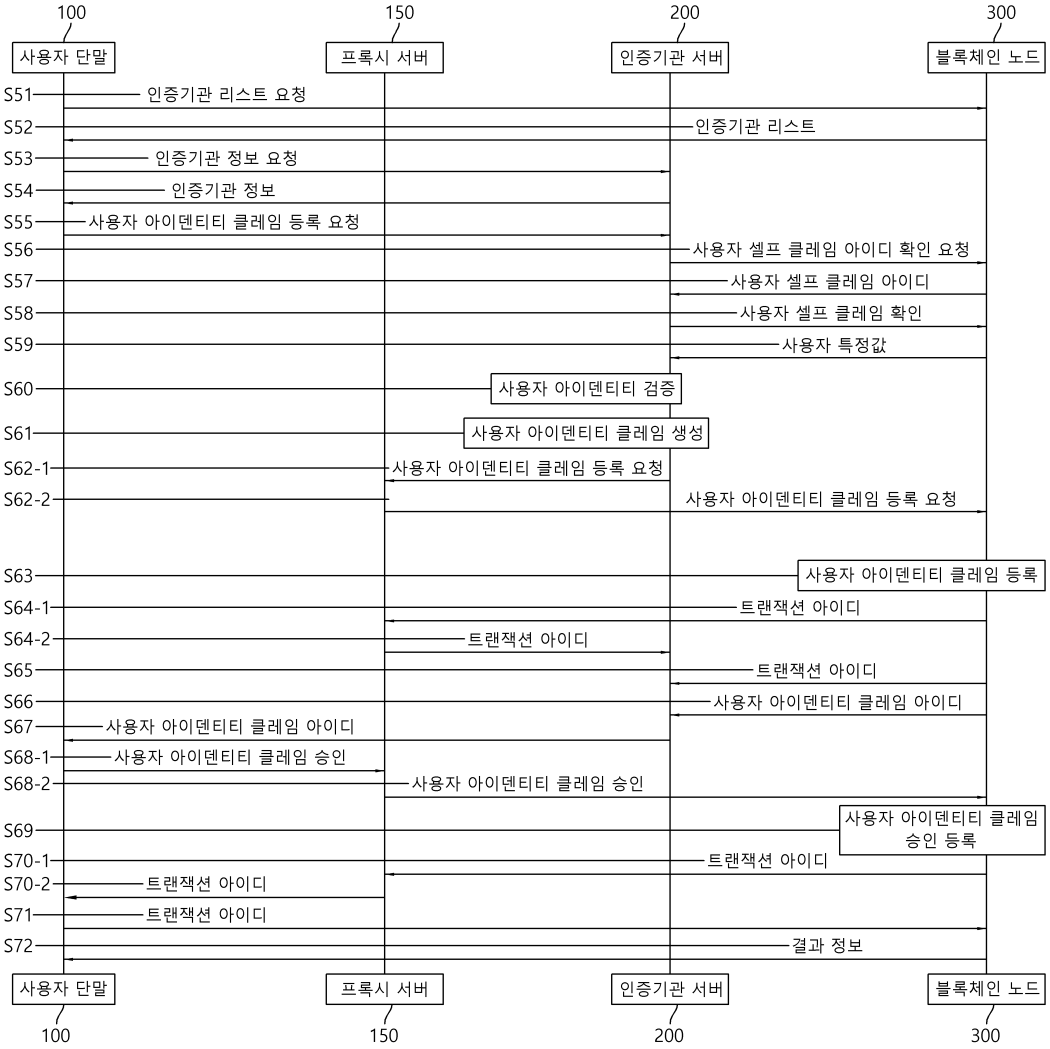
도면6


100
400
300
사용자 단말
분산저장 서버
블록체인 노드
S41
사용자 셀프 클레임 아이디 확인
S42
사용자 셀프 클레임 아이디
S43
사용자 셀프 클레임 확인
S44
파일 아이디
S45
파일 아이디
S46
암호화된 사용자 데이터
S47
사용자 데이터 복구
사용자 단말
분산저장 서버
블록체인 노드
100
400
300

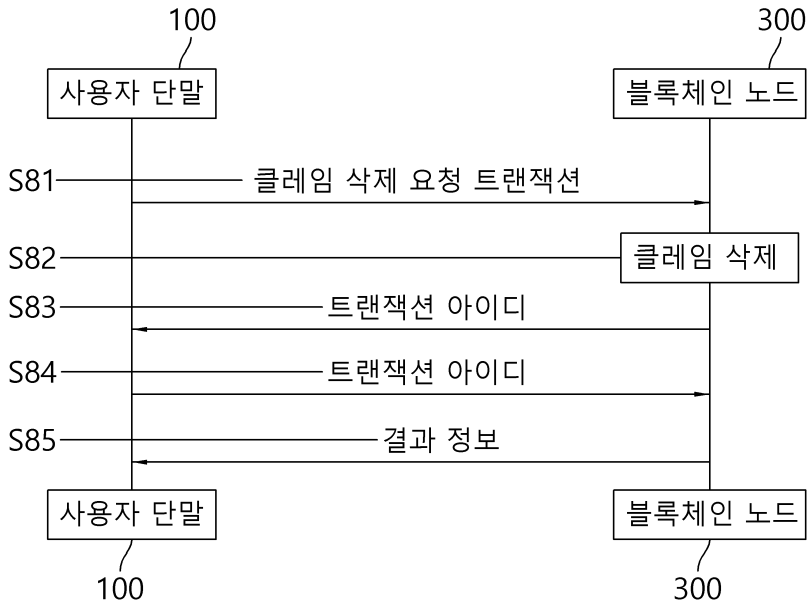
도면7a


100
200
300
사용자 단말
인증기관 서버
블록체인 노드
S51
인증기관 리스트 요청
S52
인증기관 리스트
S53
인증기관 정보 요청
S54
인증기관 정보
S55
사용자 아이덴티티 클레임 등록 요청
S56
사용자 셀프 클레임 아이디 확인 요청
S57
사용자 셀프 클레임 아이디
S58
사용자 셀프 클레임 확인
S59
사용자 특정값
S60
사용자 아이덴티티 검증
S61
사용자 아이덴티티 클레임 생성
S62
사용자 아이덴티티 클레임 등록 요청
S63
사용자 아이덴티티 클레임 등록
S64
트랜잭션 아이디
S65
트랜잭션 아이디
S65
사용자 아이덴티티 클레임 아이디
S67
사용자 아이덴티티 클레임 아이디
S68
사용자 아이덴티티 클레임 승인
S69
사용자 아이덴티티 클레임 승인 등록
S70
트랜잭션 아이디
S71
트랜잭션 아이디
S72
결과 정보
사용자 단말
인증기관 서버
블록체인 노드
100
200
300

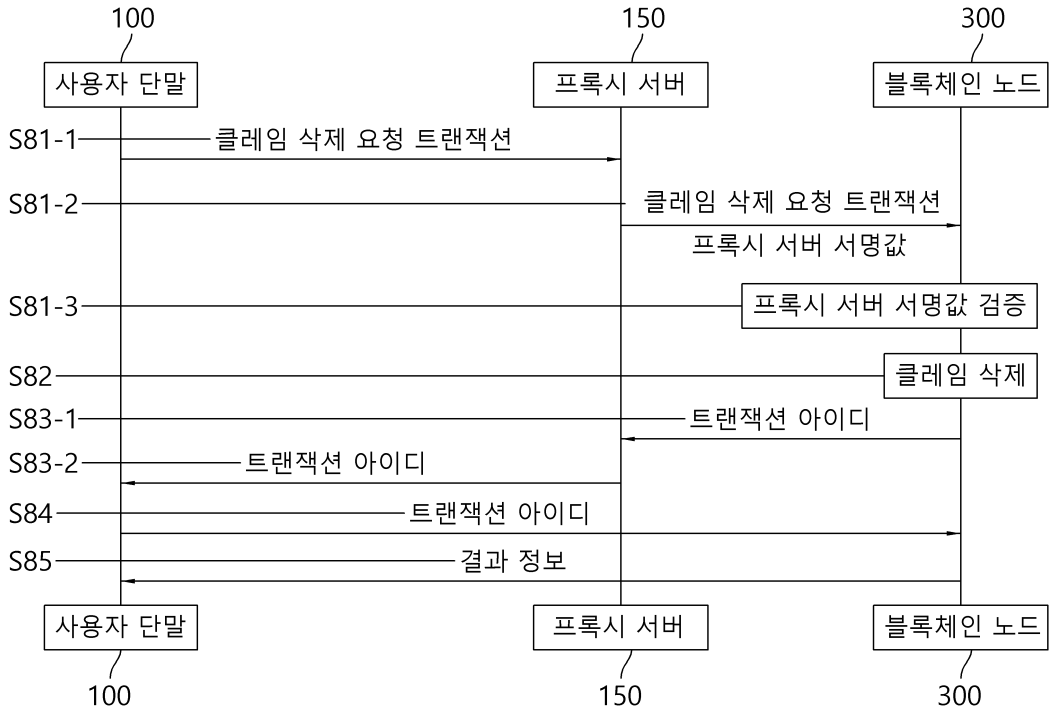
도면7b


100
150
200
300
사용자 단말
프록시 서버
인증기관 서버
블록체인 노드
S51
인증기관 리스트 요청
S52
인증기관 리스트
S53
인증기관 정보 요청
S54
인증기관 정보
S55
사용자 아이덴티티 클레임 등록 요청
S56
사용자 셀프 클레임 아이디 확인 요청
S57
사용자 셀프 클레임 아이디
S58
사용자 셀프 클레임 확인
S59
사용자 특정값
S60
사용자 아이덴티티 검증
S61
사용자 아이덴티티 클레임 생성
S62-1
사용자 아이덴티티 클레임 등록 요청
S62-2
사용자 아이덴티티 클레임 등록 요청
S63
사용자 아이덴티티 클레임 등록
S64-1
트랜잭션 아이디
S64-2
트랜잭션 아이디
S65
트랜잭션 아이디
S66
사용자 아이덴티티 클레임 아이디
S67
사용자 아이덴티티 클레임 아이디
S68-1
사용자 아이덴티티 클레임 승인
S68-2
사용자 아이덴티티 클레임 승인
S69
사용자 아이덴티티 클레임 승인 등록
S70-1
트랜잭션 아이디
S70-2
트랜잭션 아이디
S71
트랜잭션 아이디
S72
결과 정보
사용자 단말
프록시 서버
인증기관 서버
블록체인 노드
100
150
200
300

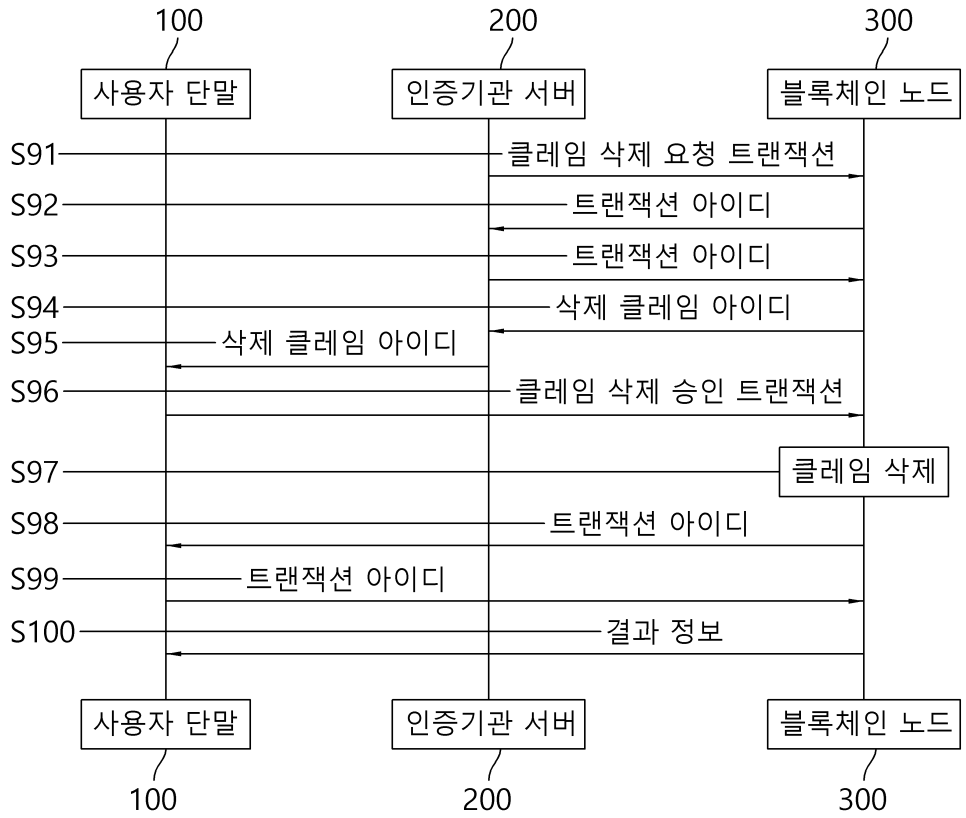
도면8a


100
300
사용자 단말
블록체인 노드
S81
클레임 삭제 요청 트랜잭션
S82
클레임 삭제
S83
트랜잭션 아이디
S84
트랜잭션 아이디
S85
결과 정보
사용자 단말
블록체인 노드
100
300

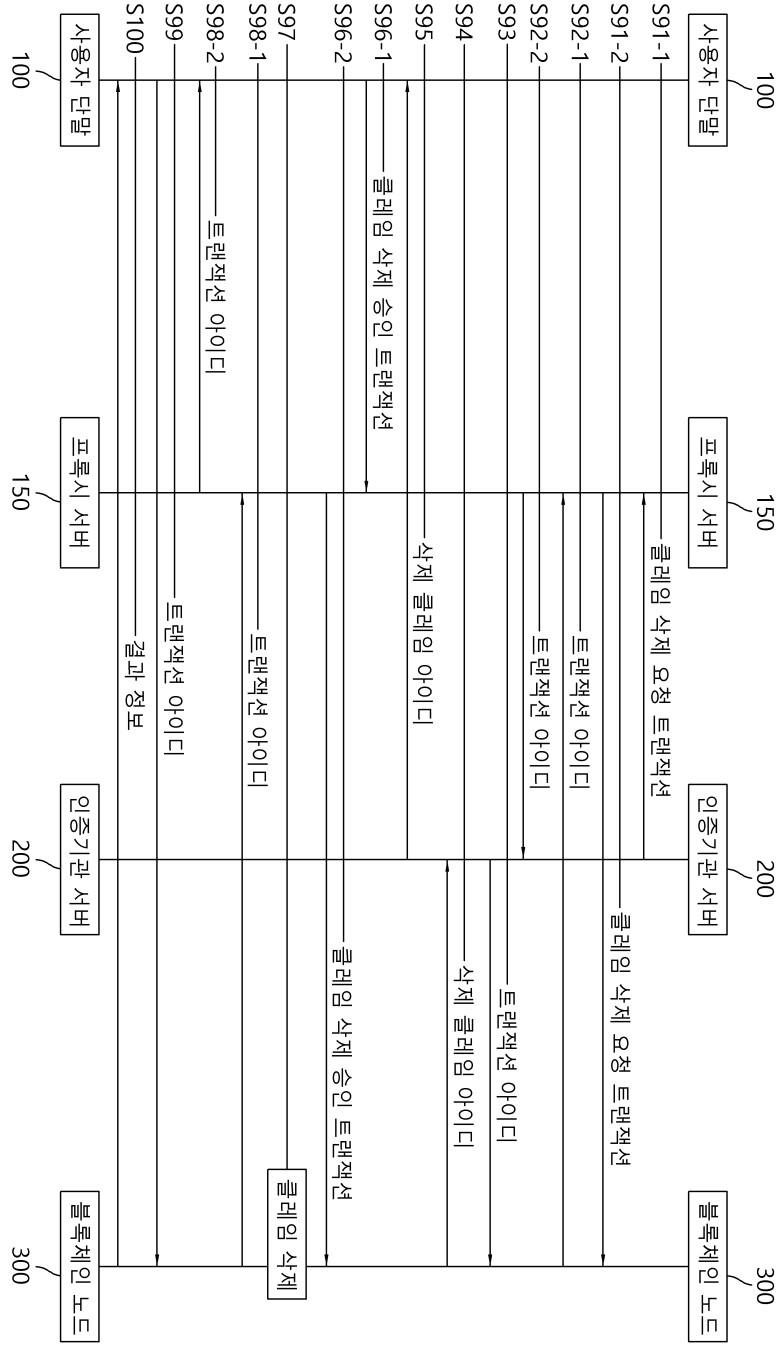
도면8b


100
150
300
사용자 단말
프록시 서버
블록체인 노드
S81-1
클레임 삭제 요청 트랜잭션
S81-2
클레임 삭제 요청 트랜잭션
프록시 서버 서명값
S81-3
프록시 서버 서명값 검증
S82
클레임 삭제
S83-1
트랜잭션 아이디
S83-2
트랜잭션 아이디
S84
트랜잭션 아이디
S85
결과 정보
사용자 단말
프록시 서버
블록체인 노드
100
150
300

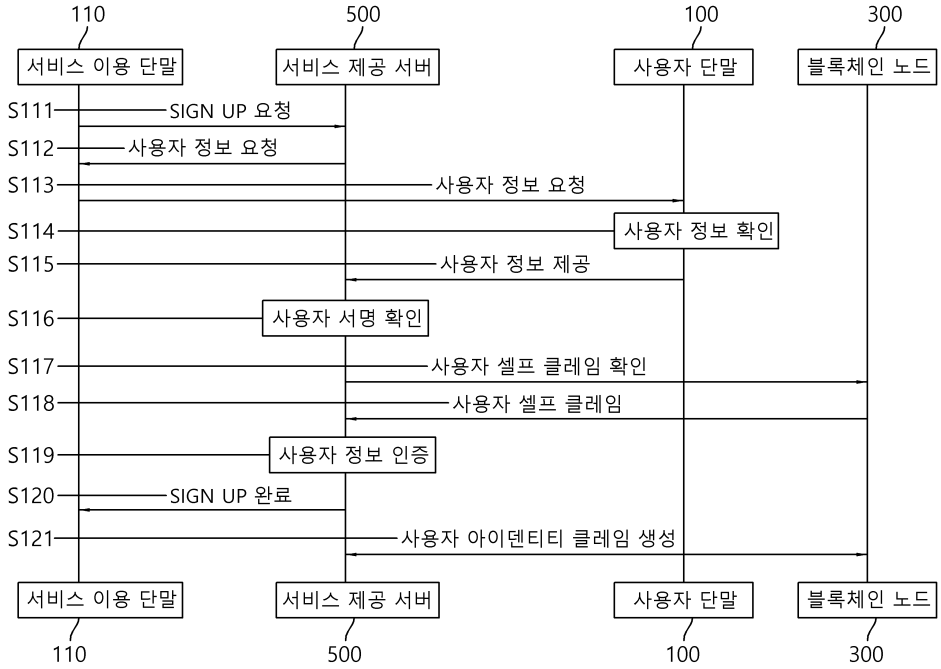
도면9a


100
200
300
사용자 단말
인증기관 서버
블록체인 노드
S91
클레임 삭제 요청 트랜잭션
S92
트랜잭션 아이디
S93
트랜잭션 아이디
S94
삭제 클레임 아이디
S95
삭제 클레임 아이디
S96
클레임 삭제 승인 트랜잭션
S97
클레임 삭제
S98
트랜잭션 아이디
S99
트랜잭션 아이디
S100
결과 정보
사용자 단말
인증기관 서버
블록체인 노드
100
200
300

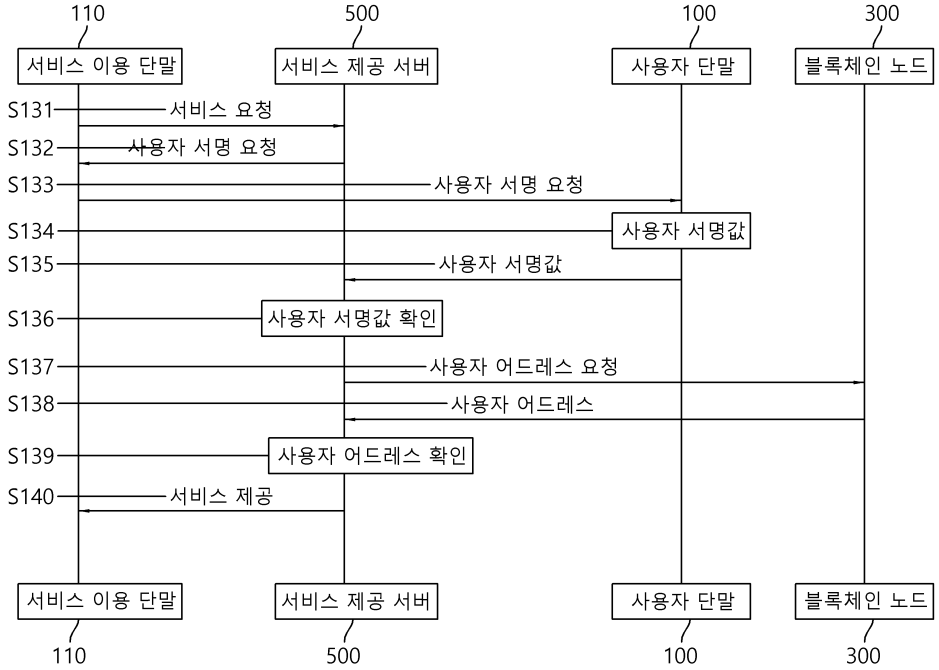
도면9b


사용자 단말
100
프록시 서버
150
인증기관 서버
200
블록체인 노드
300
S91-1
S91-2
S92-1
S92-2
S93
S94
S95
S96-1
S96-2
S97
S98-1
S98-2
S99
S100
클레임 삭제 요청 트랜잭션
트랜잭션 아이디
트랜잭션 아이디
클레임 삭제 요청 트랜잭션
삭제 클레임 아이디
클레임 삭제 승인 트랜잭션
클레임 삭제 승인 트랜잭션
삭제 클레임 아이디
트랜잭션 아이디
클레임 삭제
트랜잭션 아이디
트랜잭션 아이디
결과 정보

도면10a


110
500
100
300
서비스 이용 단말
서비스 제공 서버
사용자 단말
블록체인 노드
S111
SIGN UP 요청
S112
사용자 정보 요청
S113
사용자 정보 요청
S114
사용자 정보 확인
S115
사용자 정보 제공
S116
사용자 서명 확인
S117
사용자 셀프 클레임 확인
S118
사용자 셀프 클레임
S119
사용자 정보 인증
S120
SIGN UP 완료
S121
사용자 아이덴티티 클레임 생성
서비스 이용 단말
서비스 제공 서버
사용자 단말
블록체인 노드
110
500
100
300

도면10b


110
500
100
300
서비스 이용 단말
서비스 제공 서버
사용자 단말
블록체인 노드
S131
서비스 요청
S132
사용자 서명 요청
S133
사용자 서명 요청
S134
사용자 서명값
S135
사용자 서명값
S136
사용자 서명값 확인
S137
사용자 어드레스 요청
S138
사용자 어드레스
S139
사용자 어드레스 확인
S140
서비스 제공
서비스 이용 단말
서비스 제공 서버
사용자 단말
블록체인 노드
110
500
100
300