(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0114432
(43) 공개일자 2019년10월10일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 29/06* (2006.01)
(52) CPC특허분류
H04L 9/3236 (2013.01)
H04L 63/0807 (2013.01)
(21) 출원번호 10-2018-0037129
(22) 출원일자 2018년03월30일
심사청구일자 2018년03월30일

(71) 출원인
주식회사 코인플러그
경기도 성남시 분당구 판교역로146번길 20, 오피스에이치 11층 (백현동)
(72) 발명자
어준선
경기도 성남시 분당구 느티로 22 ,B동1710호(정자동,백궁동양파라곤)
홍재우
서울특별시 은평구 연서로 149, 베르빌 1203호 (갈현동)
서문규
서울특별시 서초구 명달로 33 ,102동602호(방배동,삼환나띠르빌)
(74) 대리인
특허법인 수

전체 청구항 수 : 총 24 항

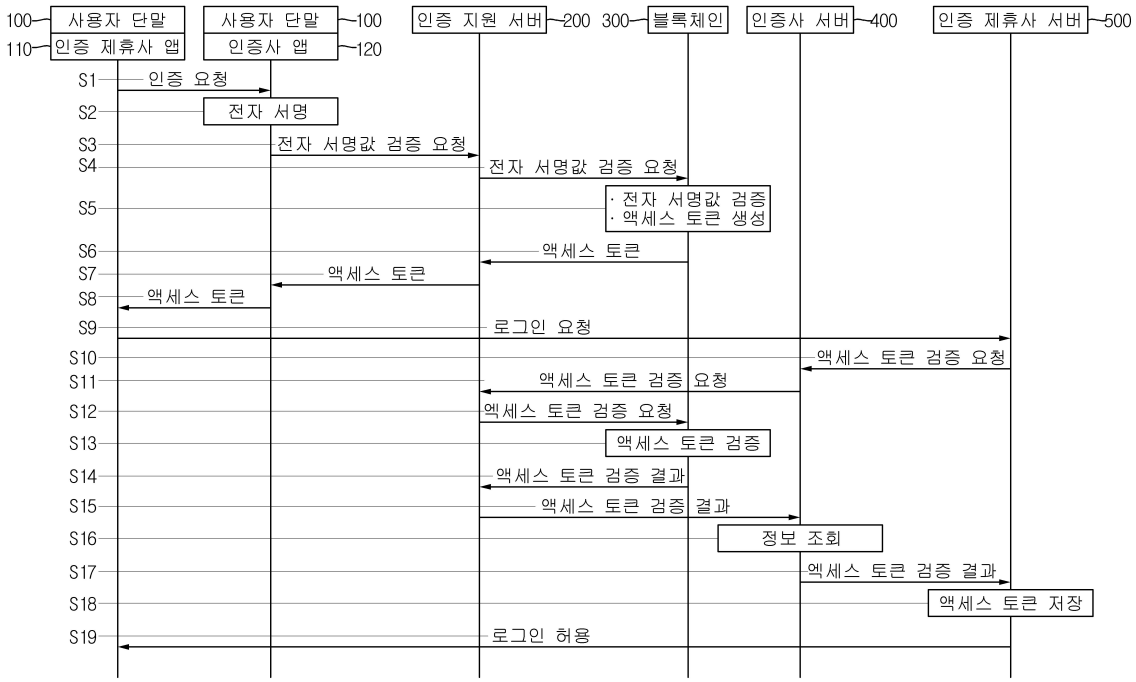
(54) 발명의 명칭 **블록체인 기반의 권한 인증 방법, 단말 및 이를 이용한 서버**

(57) 요 약

본 발명은 사용자 단말의 인증 제휴사 앱으로부터의 검증 확인값을 포함하는 인증 요청 정보에 대응한 인증사 앱으로부터 전자 서명값에 대한 전자 서명값 검증 요청 정보를 획득하고, 전자 서명값을 검증하여 유효한 것으로 확인되면 액세스 토큰을 생성하여 사용자 단말로 전송되도록 함으로써 인증 제휴사 앱으로 하여금 액세스 토큰을

(뒷면에 계속)

대 표 도



이용하여 인증 제휴사 서버로 로그인을 요청하도록 지원하고, 액세스 토큰을 블록체인에 등록하며, 액세스 토큰을 포함하는 액세스 토큰 검증 요청 정보가 인증 제휴사 서버로부터 획득되면, 액세스 토큰을 검증하여 유효한 것일 경우 액세스 토큰 검증 결과 정보를 인증 제휴사 서버로 전송함으로써 상기 인증 제휴사 서버로 하여금 액세스 토큰을 인증 제휴사 서버에 연동되는 저장 장치에 저장하도록 하고, 액세스 토큰 검증 결과에 대응하여 사용자 단말의 인증 제휴사 앱을 통한 인증 제휴사 서버로의 로그인을 허용하도록 지원하는 블록체인 기반의 권한 인증 방법, 단말 및 이를 이용한 서버에 관한 것이다.

(52) CPC특허분류

H04L 9/3213 (2013.01)

H04L 9/3247 (2013.01)

H04L 2209/38 (2013.01)

명 세 서

청구범위

청구항 1

블록체인 기반의 권한 인증 방법에 있어서,

(a) 사용자 단말의 인증 제휴사 앱으로부터의 검증 확인값을 포함하는 인증 요청 정보에 대응한 상기 사용자 단말의 인증사 앱으로부터 전자 서명값에 대한 전자 서명값 검증 요청 정보 - 상기 전자 서명값 검증 요청 정보는 적어도 상기 검증 확인값과 상기 검증 확인값을 상기 인증사 앱의 프라이빗키를 사용하여 전자 서명한 상기 전자 서명값을 포함한 - 가 획득되면, 인증 지원 서버가, (i) 상기 전자 서명값을 검증하거나 상기 인증 지원 서버에 연동되는 타 장치로 하여금 상기 전자 서명값을 검증하도록 지원하며, 상기 전자 서명값이 유효한 것으로 확인되면 액세스 토큰을 생성하여 상기 사용자 단말로 전송하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 사용자 단말로 전송되도록 함으로써 상기 사용자 단말로 하여금 상기 인증사 앱을 통해 상기 액세스 토큰을 수신하며 상기 인증 제휴사 앱을 통해 상기 액세스 토큰을 이용하여 인증 제휴사 서버로 로그인을 요청하도록 지원하고, 상기 액세스 토큰을 블록체인에 등록하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 블록체인에 상기 액세스 토큰을 등록하도록 지원하거나, (ii) 상기 블록체인으로 상기 전자 서명값에 대한 검증을 요청하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 블록체인으로 상기 전자 서명값에 대한 검증을 요청하도록 함으로써 상기 블록체인으로 하여금 상기 전자 서명값이 유효한 것으로 확인되면 액세스 토큰을 생성하여 상기 인증 지원 서버로 전송하도록 하며, 상기 액세스 토큰을 상기 블록체인에 등록하도록 하고, 상기 블록체인으로부터 상기 액세스 토큰이 획득되면 상기 액세스 토큰을 상기 사용자 단말로 전송하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 사용자 단말로 전송되도록 함으로써 상기 사용자 단말로 하여금 상기 인증사 앱을 통해 상기 액세스 토큰을 수신하며 상기 인증 제휴사 앱을 통해 상기 액세스 토큰을 이용하여 인증 제휴사 서버로 로그인을 요청하도록 지원하는 단계; 및

(b) 적어도 상기 액세스 토큰을 포함하는 액세스 토큰 검증 요청 정보가 상기 인증 제휴사 서버로부터 획득되거나 상기 인증 제휴사 서버로부터의 상기 액세스 토큰 검증 요청 정보가 인증사 서버를 통해 획득되면, 상기 인증 지원 서버가, (i) 상기 액세스 토큰을 검증하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 액세스 토큰을 검증하도록 하거나, (ii) 상기 블록체인으로 상기 액세스 토큰에 대한 검증을 요청하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 블록체인으로 상기 액세스 토큰에 대한 검증을 요청하도록 함으로써 상기 블록체인으로 하여금 상기 액세스 토큰을 검증하도록 지원하며, 상기 액세스 토큰이 유효한 것으로 확인되면, 액세스 토큰 검증 결과 정보를 상기 인증 제휴사 서버로 전송하거나 상기 인증 지원 서버에 연동되는 타 장치 또는 상기 인증사 서버를 통해 상기 액세스 토큰 검증 결과 정보가 상기 인증 제휴사 서버로 전송되도록 함으로써 상기 인증 제휴사 서버로 하여금 상기 액세스 토큰을 상기 인증 제휴사 서버에 연동되는 저장 장치에 저장하도록 하며, 상기 액세스 토큰 검증 결과에 대응하여 상기 사용자 단말의 상기 인증 제휴사 앱을 통한 상기 인증 제휴사 서버로의 로그인을 허용하도록 지원하는 단계;

를 포함하는 것을 특징으로 하는 방법.

청구항 2

제1항에 있어서,

상기 (a) 단계에서,

상기 인증 지원 서버는, 상기 인증사 앱에 대응되는 퍼블릭키를 이용하여 상기 전자 서명값의 서명에 사용된 검증 확인값인 전자 서명 검증 확인값을 확인하며, 상기 확인된 전자 서명 검증 확인값이 상기 전자 서명값 검증 요청 정보에 포함된 상기 검증 확인값과 일치하는지 여부를 확인함으로써 상기 전자 서명값을 검증하거나, 상기 블록체인으로 하여금 상기 인증사 앱에 대응되는 퍼블릭키를 이용하여 상기 전자 서명값의 서명에 사용된 상기 전자 서명 검증 확인값을 확인하며, 상기 확인된 전자 서명 검증 확인값이 상기 전자 서명값 검증 요청 정보에 포함된 상기 검증 확인값과 일치하는지 여부를 확인하여 상기 전자 서명값을 검증하도록 하는 것을 특징으로 하는 방법.

청구항 3

제1항에 있어서,

상기 액세스 토큰은 사용자 단말 식별 정보, 및 사용자 식별 정보 중 적어도 하나 이상을 포함하거나, 상기 사용자 단말의 식별 정보와 상기 사용자 식별 정보의 해쉬값들 중 적어도 하나 이상을 포함하는 것을 특징으로 하는 방법.

청구항 4

제1항에 있어서,

상기 (a) 단계에서,

상기 사용자 단말의 상기 인증 제휴사 앱으로부터 상기 인증 제휴사 서버로의 로그인 요청에는 상기 액세스 토큰, 사용자 단말 식별 정보, 및 사용자 식별 정보 중 적어도 하나 이상이 포함되는 것을 특징으로 하는 방법.

청구항 5

제1항에 있어서,

상기 (b) 단계에서,

상기 액세스 토큰 검증 결과 정보에 사용자 단말 식별 정보, 및 사용자 식별 정보 중 적어도 하나 이상을 더 포함하는 것을 특징으로 하는 방법.

청구항 6

제1항에 있어서,

상기 (b) 단계에서,

상기 인증 지원 서버는, 상기 액세스 토큰 검증 결과 정보에 사용자 정보를 더하여 상기 인증 제휴사 서버로 전송하거나, 상기 인증 지원 서버에 연동되는 타 장치 또는 상기 인증사 서버로 하여금 상기 액세스 토큰 검증 결과 정보에 상기 사용자 정보를 더하여 상기 인증 제휴사 서버로 전송하도록 하는 것을 특징으로 하는 방법.

청구항 7

블록체인 기반의 권한 인증 방법에 있어서,

(a) 사용자 단말의 인증 제휴사 앱으로부터의 검증 확인값을 포함하는 인증 요청 정보에 대응한 상기 사용자 단말의 인증사 앱으로부터 전자 서명값에 대한 전자 서명값 검증 요청 정보가 획득되면 상기 전자 서명값을 검증하거나 블록체인으로 하여금 상기 전자 서명값을 검증하도록 하며, 상기 전자 서명값의 유효한 결과에 대응되어 액세스 토큰이 생성되면 상기 액세스 토큰을 상기 블록체인에 등록되도록 하며 상기 액세스 토큰을 상기 사용자 단말로 전송되도록 함으로써 상기 사용자 단말로 하여금 상기 인증사 앱을 통해 상기 액세스 토큰을 수신하며 상기 인증 제휴사 앱을 통해 상기 액세스 토큰을 이용하여 인증 제휴사 서버로 상기 액세스 토큰의 등록을 요청하도록 지원하고, 적어도 상기 액세스 토큰을 포함하는 액세스 토큰 검증 요청 정보가 상기 인증 제휴사 서버로부터 획득되거나 상기 인증 제휴사 서버로부터의 상기 액세스 토큰 검증 요청 정보가 인증사 서버를 통해 획득되면, 상기 액세스 토큰을 검증하거나 상기 블록체인으로 하여금 상기 액세스 토큰을 검증하도록 지원하며, 상기 액세스 토큰이 유효한 것으로 확인되면, 액세스 토큰 검증 결과 정보를 상기 인증 제휴사 서버로 전송하거나 상기 인증 지원 서버에 연동되는 타 장치 또는 상기 인증사 서버를 통해 상기 액세스 토큰 검증 결과 정보가 상기 인증 제휴사 서버로 전송되도록 함으로써 상기 인증 제휴사 서버로 하여금 상기 액세스 토큰을 상기 인증 제휴사 서버에 연동되는 저장 장치에 저장하도록 한 상태에서, 상기 사용자 단말의 상기 인증 제휴사 앱을 통한 로그인 요청에 대응하여 확인된 상기 액세스 토큰을 포함하는 액세스 토큰 검증 요청 정보가 상기 인증 제휴사 서버로부터 획득되거나 상기 인증 제휴사 서버로부터의 상기 액세스 토큰 검증 요청 정보가 인증사 서버를 통해 획득되면, 상기 인증 지원 서버가, (i) 상기 액세스 토큰을 검증하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 액세스 토큰을 검증하도록 하거나, (ii) 상기 블록체인으로 상기 액세스 토큰에 대한 검증을 요청하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 블록체인으로 상기 액세스 토큰에 대한 검증을 요청하도록 함으로써 상기 블록체인으로 하여금 상기 액세스 토큰을 검증하도록 지원하는 단계; 및

(b) 상기 액세스 토큰이 유효한 것으로 확인되면, 상기 인증 지원 서버가, 액세스 토큰 검증 결과 정보를 상기 인증 제휴사 서버로 전송하거나 상기 인증 지원 서버에 연동되는 타 장치 또는 상기 인증사 서버를 통해 상기 액세스 토큰 검증 결과 정보가 상기 인증 제휴사 서버로 전송되도록 함으로써 상기 인증 제휴사 서버로 하여금 상기 액세스 토큰 검증 결과에 대응하여 상기 사용자 단말의 상기 인증 제휴사 앱을 통한 상기 인증 제휴사 서버로의 로그인을 허용하도록 지원하는 단계;

를 포함하는 것을 특징으로 하는 방법.

청구항 8

제7항에 있어서,

상기 액세스 토큰은 사용자 단말 식별 정보, 및 사용자 식별 정보 중 적어도 하나 이상을 포함하거나, 상기 사용자 단말의 식별 정보와 상기 사용자 식별 정보의 해쉬값들 중 적어도 하나 이상을 포함하는 것을 특징으로 하는 방법.

청구항 9

제7항에 있어서,

상기 (a) 단계에서,

상기 사용자 단말의 상기 인증 제휴사 앱을 통한 로그인 요청은 사용자 단말 식별 정보, 및 사용자 식별 정보 중 적어도 하나 이상을 더 포함하는 것을 특징으로 하는 방법.

청구항 10

블록체인 기반의 권한 인증 방법에 있어서,

(a) 사용자 단말이, 인증 제휴사 앱으로부터의 검증 확인값을 포함하는 인증 요청 정보에 대응하여 인증사 앱을 통해 전자 서명값에 대한 전자 서명값 검증 요청 정보 - 상기 전자 서명값 검증 요청 정보는 적어도 상기 검증 확인값과 상기 검증 확인값을 상기 인증사 앱의 프라이빗키를 사용하여 전자 서명한 상기 전자 서명값을 포함한 - 를 인증 지원 서버로 전송하거나 상기 사용자 단말에 연동되는 타 장치를 통해 상기 전자 서명값 요청 정보를 인증 지원 서버로 전송하도록 함으로써 상기 인증 지원 서버로 하여금 (i) 상기 전자 서명값을 검증하거나 상기 인증 지원 서버에 연동되는 타 장치로 하여금 상기 전자 서명값을 검증하도록 지원하며, 상기 전자 서명값이 유효한 것으로 확인되면 액세스 토큰을 생성하고, 상기 액세스 토큰을 블록체인에 등록하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 블록체인에 상기 액세스 토큰을 등록하도록 지원하며, 상기 액세스 토큰을 상기 사용자 단말로 전송하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 액세스 토큰이 상기 사용자 단말로 전송되도록 지원하게 하거나, (ii) 상기 블록체인으로 상기 전자 서명값에 대한 검증을 요청하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 블록체인으로 상기 전자 서명값에 대한 검증을 요청하도록 하고, 상기 블록체인을 통해 상기 전자 서명값이 유효한 것으로 확인되면 상기 액세스 토큰을 생성하여 상기 블록체인에 등록하도록 하며, 상기 액세스 토큰을 상기 인증 지원 서버로 전송하도록 하며, 상기 블록체인으로부터 상기 액세스 토큰이 획득되면 상기 액세스 토큰을 상기 사용자 단말로 전송하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 사용자 단말로 전송되도록 지원하게 하는 단계; 및

(b) 상기 인증사 앱을 통해 상기 액세스 토큰이 획득되면, 상기 사용자 단말이, 상기 인증 제휴사 앱을 통해 상기 액세스 토큰을 이용하여 인증 제휴사 서버로 로그인을 요청하거나 상기 사용자 단말에 연동되는 타 장치를 통해 상기 인증 제휴사 서버로 로그인을 요청하도록 함으로써 상기 인증 제휴사 서버로 하여금, (i) 적어도 상기 액세스 토큰을 포함하는 액세스 토큰 검증 요청 정보를 상기 인증 지원 서버로 전송하도록 지원하거나 인증사 서버를 통해 상기 액세스 토큰 검증 요청 정보가 상기 인증 지원 서버로 전송되도록 지원하여 상기 인증 지원 서버를 통해 (i-1) 상기 액세스 토큰을 검증하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 액세스 토큰을 검증하도록 하거나, (i-2) 상기 블록체인으로 상기 액세스 토큰에 대한 검증을 요청하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 블록체인으로 상기 액세스 토큰에 대한 검증을 요청하도록 지원하며, (ii) 상기 액세스 토큰이 유효한 것으로 확인되어 액세스 토큰 검증 결과 정보가 상기 인증 지원 서버 또는 상기 인증사 서버를 통해 획득되면 상기 액세스 토큰을 상기 인증 제휴사 서버에 연동되는 저장 장치에 저장하도록 지원하며, 상기 액세스 토큰 검증 결과에 대응하여 상기 사용자 단말의 상기 인증 제휴사 앱을 통한 상

기 인증 제휴사 서버로의 로그인을 허용하도록 지원하는 단계;

를 포함하는 것을 특징으로 하는 방법.

청구항 11

제10항에 있어서,

상기 액세스 토큰은 사용자 단말 식별 정보, 및 사용자 식별 정보 중 적어도 하나 이상을 포함하거나, 상기 사용자 단말의 식별 정보와 상기 사용자 식별 정보의 해쉬값들 중 적어도 하나 이상을 포함하는 것을 특징으로 하는 방법.

청구항 12

제10항에 있어서,

상기 (a) 단계에서,

상기 사용자 단말의 상기 인증 제휴사 앱으로부터 상기 인증 제휴사 서버로의 로그인 요청에는 상기 액세스 토큰, 사용자 단말 식별 정보, 및 사용자 식별 정보 중 적어도 하나 이상이 포함되는 것을 특징으로 하는 방법.

청구항 13

블록체인 기반의 권한 인증을 수행하는 인증 지원 서버에 있어서,

사용자 단말의 인증 제휴사 앱으로부터의 검증 확인값을 포함하는 인증 요청 정보에 대응한 상기 사용자 단말의 인증사 앱으로부터 전자 서명값에 대한 전자 서명값 검증 요청 정보 - 상기 전자 서명값 검증 요청 정보는 적어도 상기 검증 확인값과 상기 검증 확인값을 상기 인증사 앱의 프라이빗키를 사용하여 전자 서명한 상기 전자 서명값을 포함한 - 를 획득하는 통신부; 및

상기 통신부를 통해 상기 전자 서명값 검증 요청 정보가 획득되면, (i) 상기 전자 서명값을 검증하거나 상기 인증 지원 서버에 연동되는 타 장치로 하여금 상기 전자 서명값을 검증하도록 지원하며, 상기 전자 서명값이 유효한 것으로 확인되면 액세스 토큰을 생성하여 상기 사용자 단말로 전송하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 사용자 단말로 전송되도록 함으로써 상기 사용자 단말로 하여금 상기 인증사 앱을 통해 상기 액세스 토큰을 수신하며 상기 인증 제휴사 앱을 통해 상기 액세스 토큰을 이용하여 인증 제휴사 서버로 로그인을 요청하도록 지원하고, 상기 액세스 토큰을 블록체인에 등록하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 블록체인에 상기 액세스 토큰을 등록하도록 지원하거나, (ii) 상기 블록체인으로 상기 전자 서명값에 대한 검증을 요청하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 블록체인으로 상기 전자 서명값에 대한 검증을 요청하도록 함으로써 상기 블록체인으로 하여금 상기 전자 서명값이 유효한 것으로 확인되면 액세스 토큰을 생성하여 상기 인증 지원 서버로 전송하도록 하며, 상기 액세스 토큰을 상기 블록체인에 등록하도록 하고, 상기 블록체인으로부터 상기 액세스 토큰이 획득되면 상기 액세스 토큰을 상기 사용자 단말로 전송하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 사용자 단말로 전송되도록 함으로써 상기 사용자 단말로 하여금 상기 인증사 앱을 통해 상기 액세스 토큰을 수신하며 상기 인증 제휴사 앱을 통해 상기 액세스 토큰을 이용하여 인증 제휴사 서버로 로그인을 요청하도록 지원하는 제1 프로세스와, 적어도 상기 액세스 토큰을 포함하는 액세스 토큰 검증 요청 정보가 상기 인증 제휴사 서버로부터 획득되거나 상기 인증 제휴사 서버로부터의 상기 액세스 토큰 검증 요청 정보가 인증사 서버를 통해 획득되면, (i) 상기 액세스 토큰을 검증하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 액세스 토큰을 검증하도록 하거나, (ii) 상기 블록체인으로 상기 액세스 토큰에 대한 검증을 요청하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 블록체인으로 상기 액세스 토큰에 대한 검증을 요청하도록 함으로써 상기 블록체인으로 하여금 상기 액세스 토큰을 검증하도록 지원하며, 상기 액세스 토큰이 유효한 것으로 확인되면, 액세스 토큰 검증 결과 정보를 상기 인증 제휴사 서버로 전송하거나 상기 인증 지원 서버에 연동되는 타 장치 또는 상기 인증사 서버를 통해 상기 액세스 토큰 검증 결과 정보가 상기 인증 제휴사 서버로 전송되도록 함으로써 상기 인증 제휴사 서버로 하여금 상기 액세스 토큰을 상기 인증 제휴사 서버에 연동되는 저장 장치에 저장하도록 하며, 상기 액세스 토큰 검증 결과에 대응하여 상기 사용자 단말의 상기 인증 제휴사 앱을 통한 상기 인증 제휴사 서버로의 로그인을 허용하도록 지원하는 제2 프로세스를 수행하는 프로세서;

를 포함하는 것을 특징으로 하는 인증 지원 서버.

청구항 14

제13항에 있어서,

상기 프로세서는,

상기 제1 프로세스에서,

상기 인증사 앱에 대응되는 퍼블릭키를 이용하여 상기 전자 서명값의 서명에 사용된 검증 확인값인 전자 서명 검증 확인값을 확인하며, 상기 확인된 전자 서명 검증 확인값이 상기 전자 서명값 검증 요청 정보에 포함된 상기 검증 확인값과 일치하는지 여부를 확인함으로써 상기 전자 서명값을 검증하거나, 상기 블록체인으로 하여금 상기 인증사 앱에 대응되는 퍼블릭키를 이용하여 상기 전자 서명값의 서명에 사용된 상기 전자 서명 검증 확인값을 확인하며, 상기 확인된 전자 서명 검증 확인값이 상기 전자 서명값 검증 요청 정보에 포함된 상기 검증 확인값과 일치하는지 여부를 확인하여 상기 전자 서명값을 검증하도록 하는 것을 특징으로 하는 인증 지원 서버.

청구항 15

제13항에 있어서,

상기 액세스 토큰은 사용자 단말 식별 정보, 및 사용자 식별 정보 중 적어도 하나 이상을 포함하거나, 상기 사용자 단말의 식별 정보와 상기 사용자 식별 정보의 해쉬값들 중 적어도 하나 이상을 포함하는 것을 특징으로 하는 인증 지원 서버.

청구항 16

제13항에 있어서,

상기 사용자 단말의 상기 인증 제휴사 앱으로부터 상기 인증 제휴사 서버로의 로그인 요청에는 상기 액세스 토큰, 사용자 단말 식별 정보, 및 사용자 식별 정보 중 적어도 하나 이상이 포함되는 것을 특징으로 하는 인증 지원 서버.

청구항 17

제13항에 있어서,

상기 액세스 토큰 검증 결과 정보에 사용자 단말 식별 정보, 및 사용자 식별 정보 중 적어도 하나 이상을 더 포함하는 것을 특징으로 하는 인증 지원 서버.

청구항 18

제13항에 있어서,

상기 프로세서는,

상기 제2 프로세스에서,

상기 액세스 토큰 검증 결과 정보에 사용자 정보를 더하여 상기 인증 제휴사 서버로 전송하거나, 상기 인증 지원 서버에 연동되는 타 장치 또는 상기 인증사 서버로 하여금 상기 액세스 토큰 검증 결과 정보에 상기 사용자 정보를 더하여 상기 인증 제휴사 서버로 전송하도록 하는 것을 특징으로 하는 인증 지원 서버.

청구항 19

블록체인 기반의 권한 인증을 수행하는 인증 지원 서버에 있어서,

사용자 단말의 인증 제휴사 앱으로부터의 검증 확인값을 포함하는 인증 요청 정보에 대응한 상기 사용자 단말의 인증사 앱으로부터 전자 서명값에 대한 전자 서명값 검증 요청 정보가 획득되면 상기 전자 서명값을 검증하거나 블록체인으로 하여금 상기 전자 서명값을 검증하도록 하며, 상기 전자 서명값의 유효한 결과에 대응되어 액세스 토큰이 생성되면 상기 액세스 토큰을 상기 블록체인에 등록되도록 하며 상기 액세스 토큰을 상기 사용자 단말로 전송되도록 함으로써 상기 사용자 단말로 하여금 상기 인증사 앱을 통해 상기 액세스 토큰을 수신하며 상기 인증 제휴사 앱을 통해 상기 액세스 토큰을 이용하여 인증 제휴사 서버로 상기 액세스 토큰의 등록을 요청하도록 지원하고, 적어도 상기 액세스 토큰을 포함하는 액세스 토큰 검증 요청 정보가 상기 인증 제휴사 서버로부터 획

득되거나 상기 인증 제휴사 서버로부터의 상기 액세스 토큰 검증 요청 정보가 인증사 서버를 통해 획득되면, 상기 액세스 토큰을 검증하거나 상기 블록체인으로 하여금 상기 액세스 토큰을 검증하도록 지원하며, 상기 액세스 토큰이 유효한 것으로 확인되면, 액세스 토큰 검증 결과 정보를 상기 인증 제휴사 서버로 전송하거나 상기 인증 지원 서버에 연동되는 타 장치 또는 상기 인증사 서버를 통해 상기 액세스 토큰 검증 결과 정보가 상기 인증 제휴사 서버로 전송되도록 함으로써 상기 인증 제휴사 서버로 하여금 상기 액세스 토큰을 상기 인증 제휴사 서버에 연동되는 저장 장치에 저장하도록 한 상태에서, 상기 사용자 단말의 상기 인증 제휴사 앱을 통한 로그인 요청에 대응하여 확인된 상기 액세스 토큰을 포함하는 액세스 토큰 검증 요청 정보가 상기 인증 제휴사 서버로부터 획득되거나 상기 인증 제휴사 서버로부터의 상기 액세스 토큰 검증 요청 정보가 인증사 서버를 통해 획득하는 통신부; 및

상기 통신부를 통해 획득된 상기 액세스 토큰 검증 요청 정보에 대응하여, (i) 상기 액세스 토큰을 검증하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 액세스 토큰을 검증하도록 하거나, (ii) 상기 블록체인으로 상기 액세스 토큰에 대한 검증을 요청하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 블록체인으로 상기 액세스 토큰에 대한 검증을 요청하도록 함으로써 상기 블록체인으로 하여금 상기 액세스 토큰을 검증하도록 지원하는 제1 프로세스와, 상기 액세스 토큰이 유효한 것으로 확인되면, 액세스 토큰 검증 결과 정보를 상기 인증 제휴사 서버로 전송하거나 상기 인증 지원 서버에 연동되는 타 장치 또는 상기 인증사 서버를 통해 상기 액세스 토큰 검증 결과 정보가 상기 인증 제휴사 서버로 전송되도록 함으로써 상기 인증 제휴사 서버로 하여금 상기 액세스 토큰 검증 결과에 대응하여 상기 사용자 단말의 상기 인증 제휴사 앱을 통한 상기 인증 제휴사 서버로의 로그인을 허용하도록 지원하는 제2 프로세스를 수행하는 프로세서;

를 포함하는 것을 특징으로 하는 인증 지원 서버.

청구항 20

제19항에 있어서,

상기 액세스 토큰은 사용자 단말 식별 정보, 및 사용자 식별 정보 중 적어도 하나 이상을 포함하거나, 상기 사용자 단말의 식별 정보와 상기 사용자 식별 정보의 해쉬값들 중 적어도 하나 이상을 포함하는 것을 특징으로 하는 인증 지원 서버.

청구항 21

제19항에 있어서,

상기 사용자 단말의 상기 인증 제휴사 앱을 통한 로그인 요청은 사용자 단말 식별 정보, 및 사용자 식별 정보 중 적어도 하나 이상을 더 포함하는 것을 특징으로 하는 인증 지원 서버.

청구항 22

블록체인 기반의 권한 인증을 수행하는 사용자 단말에 있어서,

통신부; 및

인증 제휴사 앱으로부터의 검증 확인값을 포함하는 인증 요청 정보에 대응하여 인증사 앱을 통해 전자 서명값에 대한 전자 서명값 검증 요청 정보 - 상기 전자 서명값 검증 요청 정보는 적어도 상기 검증 확인값과 상기 검증 확인값을 상기 인증사 앱의 프라이빗키를 사용하여 전자 서명한 상기 전자 서명값을 포함한 - 를 상기 통신부를 이용하여 인증 지원 서버로 전송하거나 상기 사용자 단말에 연동되는 타 장치를 통해 상기 전자 서명값 요청 정보를 인증 지원 서버로 전송하도록 함으로써 상기 인증 지원 서버로 하여금 (i) 상기 전자 서명값을 검증하거나 상기 인증 지원 서버에 연동되는 타 장치로 하여금 상기 전자 서명값을 검증하도록 지원하며, 상기 전자 서명값이 유효한 것으로 확인되면 액세스 토큰을 생성하고, 상기 액세스 토큰을 블록체인에 등록하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 블록체인에 상기 액세스 토큰을 등록하도록 지원하며, 상기 액세스 토큰을 상기 사용자 단말로 전송하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 액세스 토큰이 상기 사용자 단말로 전송되도록 지원하게 하거나, (ii) 상기 블록체인으로 상기 전자 서명값에 대한 검증을 요청하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 블록체인으로 상기 전자 서명값에 대한 검증을 요청하도록 하고, 상기 블록체인을 통해 상기 전자 서명값이 유효한 것으로 확인되면 상기 액세스 토큰을 생성하여 상기 블록체인에 등록하도록 하며, 상기 액세스 토큰을 상기 인증 지원 서버로 전송하도록 하며, 상기 블록체인으로부터 상기 액세스 토큰이 획득되면 상기 액세스 토큰을 상기 사용자 단말로 전송하거나 상기 인증 지원 서버

에 연동되는 타 장치를 통해 상기 사용자 단말로 전송되도록 지원하게 하는 제1 프로세스와, 상기 통신부를 통해 상기 인증사 앱을 통해 상기 액세스 토큰이 획득되면, 상기 인증 제휴사 앱을 통해 상기 액세스 토큰을 이용하여 인증 제휴사 서버로 로그인을 요청하거나 상기 사용자 단말에 연동되는 타 장치를 통해 상기 인증 제휴사 서버로 로그인을 요청하도록 함으로써 상기 인증 제휴사 서버로 하여금, (i) 적어도 상기 액세스 토큰을 포함하는 액세스 토큰 검증 요청 정보를 상기 인증 지원 서버로 전송하도록 지원하거나 인증사 서버를 통해 상기 액세스 토큰 검증 요청 정보가 상기 인증 지원 서버로 전송되도록 지원하여 상기 인증 지원 서버를 통해 (i-1) 상기 액세스 토큰을 검증하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 액세스 토큰을 검증하도록 하거나, (i-2) 상기 블록체인으로 상기 액세스 토큰에 대한 검증을 요청하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 블록체인으로 상기 액세스 토큰에 대한 검증을 요청하도록 지원하며, (ii) 상기 액세스 토큰이 유효한 것으로 확인되어 액세스 토큰 검증 결과 정보가 상기 인증 지원 서버 또는 상기 인증사 서버를 통해 획득되면 상기 액세스 토큰을 상기 인증 제휴사 서버에 연동되는 저장 장치에 저장하도록 지원하며, 상기 액세스 토큰 검증 결과에 대응하여 상기 사용자 단말의 상기 인증 제휴사 앱을 통한 상기 인증 제휴사 서버로의 로그인을 허용하도록 지원하는 제2 프로세스를 수행하는 프로세서;

를 포함하는 것을 특징으로 하는 사용자 단말.

청구항 23

제22항에 있어서,

상기 액세스 토큰은 사용자 단말 식별 정보, 및 사용자 식별 정보 중 적어도 하나 이상을 포함하거나, 상기 사용자 단말의 식별 정보와 상기 사용자 식별 정보의 해쉬값들 중 적어도 하나 이상을 포함하는 것을 특징으로 하는 사용자 단말.

청구항 24

제22항에 있어서,

상기 사용자 단말의 상기 인증 제휴사 앱으로부터 상기 인증 제휴사 서버로의 로그인 요청에는 상기 액세스 토큰, 사용자 단말 식별 정보, 및 사용자 식별 정보 중 적어도 하나 이상이 포함되는 것을 특징으로 하는 사용자 단말.

발명의 설명

기 술 분 야

[0001] 본 발명은 블록체인 기반의 권한 인증 방법, 단말 및 이를 이용한 서버에 관한 것으로, 보다 상세하게는, 사용자 단말의 인증 제휴사 앱으로부터의 검증 확인값을 포함하는 인증 요청 정보에 대응한 인증사 앱으로부터 전자 서명값에 대한 전자 서명값 검증 요청 정보를 획득하고, 전자 서명값을 검증하여 유효한 것으로 확인되면 액세스 토큰을 생성하여 사용자 단말로 전송되도록 함으로써 인증 제휴사 앱으로 하여금 액세스 토큰을 이용하여 인증 제휴사 서버로 로그인을 요청하도록 지원하고, 액세스 토큰을 블록체인에 등록하며, 액세스 토큰을 포함하는 액세스 토큰 검증 요청 정보가 인증 제휴사 서버로부터 획득되면, 액세스 토큰을 검증하여 유효한 것일 경우 액세스 토큰 검증 결과 정보를 인증 제휴사 서버로 전송함으로써 상기 인증 제휴사 서버로 하여금 액세스 토큰을 인증 제휴사 서버에 연동되는 저장 장치에 저장하도록 하고, 액세스 토큰 검증 결과에 대응하여 사용자 단말의 인증 제휴사 앱을 통한 인증 제휴사 서버로의 로그인을 허용하도록 지원하는 블록체인 기반의 권한 인증 방법, 단말 및 이를 이용한 서버에 관한 것이다.

배 경 기 술

[0002] OAuth는 하나의 OpenID에 기초하여, 복수의 웹 사이트 또는 응용 프로그램(application)에 인증을 수행할 수 있도록 개발된 표준 인증 방식이며, OAuth 프로토콜은 별도의 인증 절차 없이 응용 프로그램끼리 인증을 공유할 수 있다. 즉, OAuth 프로토콜은 클라이언트의 식별자나 증명서를 공개하지 않고 웹 사이트나 응용 프로그램에서 자원에 대한 액세스 권한을 부여 받기 위한 프로토콜이다.

[0003] 그리고, OAuth는 2007년 12월 OAuth core 1.0에서부터 최근 OAuth 2.0까지 클라이언트별로 접근 권한을 설정하고, 클라이언트의 정보를 서드 파티에 노출하지 않을 수 있는 방법 등을 개정해왔으며, OAuth 프로토콜은 인증

서버로부터 발급된 토큰을 이용하여 자원 서버에 있는 자원에 대한 접근 권한을 획득할 수 있다.

[0004] 그러나, 현재 제정된 OAuth 프로토콜 표준에서는 클라이언트가 사용할 수 있는 토큰의 횟수에 대한 제한이 명확하지 않다.

[0005] 그러므로, OAuth 프로토콜에서는 정상적으로 토큰을 획득한 악의적인 클라이언트가 자원 서버에 여러 번 접근하여 악의적인 행동을 시도할 수 있다.

[0006] 특히, 종래 OAuth에서는 사용자의 인증 정보가 공격자에 의하여 탈취되는 경우 OpenID와 관련한 모든 제휴 서비스에 공격자가 접근할 수 있도록 한다는 문제점이 있다.

[0007] 따라서, OAuth와 같이 별도의 인증 절차 없이 응용 프로그램끼리 인증을 공유할 수 있도록 하면서도 개인정보와 같은 사용자 인증 정보를 외부 공격으로부터 효과적으로 보호할 수 있는 새로운 보안 알고리즘(algorithm)의 필요성이 대두되고 있다.

발명의 내용

해결하려는 과제

[0008] 본 발명은 상술한 문제점들을 모두 해결하는 것을 그 목적으로 한다.

[0009] 또한, 본 발명은 가상 화폐의 블록체인 기술을 이용하여 사용자의 인증 정보를 외부 공격으로부터 효과적으로 보호할 수 있도록 하는 권한 인증을 제공하는 것을 다른 목적으로 한다.

[0010] 또한, 본 발명은 액세스 토큰을 해쉬함수와 암호화 기술을 이용하여 블록체인에 등록하여 보안이 보장되고 위/변조가 불가능한 권한 인증을 제공하는 것을 또 다른 목적으로 한다.

[0011] 또한, 본 발명은 위/변조가 불가능한 블록체인을 통해 권한 인증을 위한 액세스 토큰을 검증하므로 사용자 정보 도용에 따른 문제점을 미연에 방지할 수 있도록 하는 권한 인증을 제공하는 것을 또 다른 목적으로 한다.

과제의 해결 수단

[0012] 상기 목적을 달성하기 위한 본 발명의 대표적인 구성은 다음과 같다.

[0013] 본 발명의 일 실시예에 따르면, 블록체인 기반의 권한 인증 방법에 있어서, (a) 사용자 단말의 인증 제휴사 앱으로부터의 검증 확인값을 포함하는 인증 요청 정보에 대응한 상기 사용자 단말의 인증사 앱으로부터 전자 서명값에 대한 전자 서명값 검증 요청 정보 - 상기 전자 서명값 검증 요청 정보는 적어도 상기 검증 확인값과 상기 검증 확인값을 상기 인증사 앱의 프라이빗키를 사용하여 전자 서명한 상기 전자 서명값을 포함한 - 가 획득되면, 인증 지원 서버가, (i) 상기 전자 서명값을 검증하거나 상기 인증 지원 서버에 연동되는 타 장치로 하여금 상기 전자 서명값을 검증하도록 지원하며, 상기 전자 서명값이 유효한 것으로 확인되면 액세스 토큰을 생성하여 상기 사용자 단말로 전송하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 사용자 단말로 전송되도록 함으로써 상기 사용자 단말로 하여금 상기 인증사 앱을 통해 상기 액세스 토큰을 수신하며 상기 인증 제휴사 앱을 통해 상기 액세스 토큰을 이용하여 인증 제휴사 서버로 로그인을 요청하도록 지원하고, 상기 액세스 토큰을 블록체인에 등록하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 블록체인에 상기 액세스 토큰을 등록하도록 지원하거나, (ii) 상기 블록체인으로 상기 전자 서명값에 대한 검증을 요청하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 블록체인으로 상기 전자 서명값에 대한 검증을 요청하도록 함으로써 상기 블록체인으로 하여금 상기 전자 서명값이 유효한 것으로 확인되면 액세스 토큰을 생성하여 상기 인증 지원 서버로 전송하도록 하며, 상기 액세스 토큰을 상기 블록체인에 등록하도록 하고, 상기 블록체인으로부터 상기 액세스 토큰이 획득되면 상기 액세스 토큰을 상기 사용자 단말로 전송하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 사용자 단말로 전송되도록 함으로써 상기 사용자 단말로 하여금 상기 인증사 앱을 통해 상기 액세스 토큰을 수신하며 상기 인증 제휴사 앱을 통해 상기 액세스 토큰을 이용하여 인증 제휴사 서버로 로그인을 요청하도록 지원하는 단계; 및 (b) 적어도 상기 액세스 토큰을 포함하는 액세스 토큰 검증 요청 정보가 상기 인증 제휴사 서버로부터 획득되거나 상기 인증 제휴사 서버로부터의 상기 액세스 토큰 검증 요청 정보가 인증사 서버를 통해 획득되면, 상기 인증 지원 서버가, (i) 상기 액세스 토큰을 검증하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 액세스 토큰을 검증하도록 하거나, (ii) 상기 블록체인으로 상기 액세스 토큰에 대한 검증을 요청하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 블록체인으로 상기 액세스 토큰에 대한 검증을 요청하도록 함으로써 상기 블록체인으로 하여금 상기 액세스 토큰을 검증하도록 지원

하며, 상기 액세스 토큰이 유효한 것으로 확인되면, 액세스 토큰 검증 결과 정보를 상기 인증 제휴사 서버로 전송하거나 상기 인증 지원 서버에 연동되는 타 장치 또는 상기 인증사 서버를 통해 상기 액세스 토큰 검증 결과 정보가 상기 인증 제휴사 서버로 전송되도록 함으로써 상기 인증 제휴사 서버로 하여금 상기 액세스 토큰을 상기 인증 제휴사 서버에 연동되는 저장 장치에 저장하도록 하며, 상기 액세스 토큰 검증 결과에 대응하여 상기 사용자 단말의 상기 인증 제휴사 앱을 통한 상기 인증 제휴사 서버로의 로그인을 허용하도록 지원하는 단계; 를 포함하는 방법이 제공된다.

[0014] 또한, 본 발명의 일 실시예에 따르면, 블록체인 기반의 권한 인증 방법에 있어서, (a) 사용자 단말의 인증 제휴사 앱으로부터의 검증 확인값을 포함하는 인증 요청 정보에 대응한 상기 사용자 단말의 인증사 앱으로부터 전자 서명값에 대한 전자 서명값 검증 요청 정보가 획득되면 상기 전자 서명값을 검증하거나 블록체인으로 하여금 상기 전자 서명값을 검증하도록 하며, 상기 전자 서명값의 유효한 결과에 대응되어 액세스 토큰이 생성되면 상기 액세스 토큰을 상기 블록체인에 등록되도록 하며 상기 액세스 토큰을 상기 사용자 단말로 전송되도록 함으로써 상기 사용자 단말로 하여금 상기 인증사 앱을 통해 상기 액세스 토큰을 수신하며 상기 인증 제휴사 앱을 통해 상기 액세스 토큰을 이용하여 인증 제휴사 서버로 상기 액세스 토큰의 등록을 요청하도록 지원하고, 적어도 상기 액세스 토큰을 포함하는 액세스 토큰 검증 요청 정보가 상기 인증 제휴사 서버로부터 획득되거나 상기 인증 제휴사 서버로부터의 상기 액세스 토큰 검증 요청 정보가 인증사 서버를 통해 획득되면, 상기 액세스 토큰을 검증하거나 상기 블록체인으로 하여금 상기 액세스 토큰을 검증하도록 지원하며, 상기 액세스 토큰이 유효한 것으로 확인되면, 액세스 토큰 검증 결과 정보를 상기 인증 제휴사 서버로 전송하거나 상기 인증 지원 서버에 연동되는 타 장치 또는 상기 인증사 서버를 통해 상기 액세스 토큰 검증 결과 정보가 상기 인증 제휴사 서버로 전송되도록 함으로써 상기 인증 제휴사 서버로 하여금 상기 액세스 토큰을 상기 인증 제휴사 서버에 연동되는 저장 장치에 저장하도록 한 상태에서, 상기 사용자 단말의 상기 인증 제휴사 앱을 통한 로그인 요청에 대응하여 확인된 상기 액세스 토큰을 포함하는 액세스 토큰 검증 요청 정보가 상기 인증 제휴사 서버로부터 획득되거나 상기 인증 제휴사 서버로부터의 상기 액세스 토큰 검증 요청 정보가 인증사 서버를 통해 획득되면, 상기 인증 지원 서버가, (i) 상기 액세스 토큰을 검증하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 액세스 토큰을 검증하도록 하거나, (ii) 상기 블록체인으로 상기 액세스 토큰에 대한 검증을 요청하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 블록체인으로 상기 액세스 토큰에 대한 검증을 요청하도록 함으로써 상기 블록체인으로 하여금 상기 액세스 토큰을 검증하도록 지원하는 단계; 및 (b) 상기 액세스 토큰이 유효한 것으로 확인되면, 상기 인증 지원 서버가, 액세스 토큰 검증 결과 정보를 상기 인증 제휴사 서버로 전송하거나 상기 인증 지원 서버에 연동되는 타 장치 또는 상기 인증사 서버를 통해 상기 액세스 토큰 검증 결과 정보가 상기 인증 제휴사 서버로 전송되도록 함으로써 상기 인증 제휴사 서버로 하여금 상기 액세스 토큰 검증 결과에 대응하여 상기 사용자 단말의 상기 인증 제휴사 앱을 통한 상기 인증 제휴사 서버로의 로그인을 허용하도록 지원하는 단계; 를 포함하는 방법이 제공된다.

[0015] 또한, 본 발명의 일 실시예에 따르면, 블록체인 기반의 권한 인증 방법에 있어서, (a) 사용자 단말이, 인증 제휴사 앱으로부터의 검증 확인값을 포함하는 인증 요청 정보에 대응하여 인증사 앱을 통해 전자 서명값에 대한 전자 서명값 검증 요청 정보 - 상기 전자 서명값 검증 요청 정보는 적어도 상기 검증 확인값과 상기 검증 확인값을 상기 인증사 앱의 프라이빗키를 사용하여 전자 서명한 상기 전자 서명값을 포함한 - 를 인증 지원 서버로 전송하거나 상기 사용자 단말에 연동되는 타 장치를 통해 상기 전자 서명값 요청 정보를 인증 지원 서버로 전송하도록 함으로써 상기 인증 지원 서버로 하여금 (i) 상기 전자 서명값을 검증하거나 상기 인증 지원 서버에 연동되는 타 장치로 하여금 상기 전자 서명값을 검증하도록 지원하며, 상기 전자 서명값이 유효한 것으로 확인되면 액세스 토큰을 생성하고, 상기 액세스 토큰을 블록체인에 등록하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 블록체인에 상기 액세스 토큰을 등록하도록 지원하며, 상기 액세스 토큰을 상기 사용자 단말로 전송하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 액세스 토큰이 상기 사용자 단말로 전송되도록 지원하게 하거나, (ii) 상기 블록체인으로 상기 전자 서명값에 대한 검증을 요청하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 블록체인으로 상기 전자 서명값에 대한 검증을 요청하도록 하고, 상기 블록체인을 통해 상기 전자 서명값이 유효한 것으로 확인되면 상기 액세스 토큰을 생성하여 상기 블록체인에 등록하도록 하며, 상기 액세스 토큰을 상기 인증 지원 서버로 전송하도록 하며, 상기 블록체인으로부터 상기 액세스 토큰이 획득되면 상기 액세스 토큰을 상기 사용자 단말로 전송하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 사용자 단말로 전송되도록 지원하게 하는 단계; 및 (b) 상기 인증사 앱을 통해 상기 액세스 토큰이 획득되면, 상기 사용자 단말이, 상기 인증 제휴사 앱을 통해 상기 액세스 토큰을 이용하여 인증 제휴사 서버로 로그인을 요청하거나 상기 사용자 단말에 연동되는 타 장치를 통해 상기 인증 제휴사 서버로 로그인을 요청하도록 함으로써 상기 인증 제휴사 서버로 하여금, (i) 적어도 상기 액세스 토큰을 포함하는 액세스 토큰 검증 요청

정보를 상기 인증 지원 서버로 전송하도록 지원하거나 인증사 서버를 통해 상기 액세스 토큰 검증 요청 정보가 상기 인증 지원 서버로 전송되도록 지원하여 상기 인증 지원 서버를 통해 (i-1) 상기 액세스 토큰을 검증하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 액세스 토큰을 검증하도록 하거나, (i-2) 상기 블록체인으로 상기 액세스 토큰에 대한 검증을 요청하거나 상기 인증 지원 서버에 연동되는 타 장치를 통해 상기 블록체인으로 상기 액세스 토큰에 대한 검증을 요청하도록 지원하며, (ii) 상기 액세스 토큰이 유효한 것으로 확인되어 액세스 토큰 검증 결과 정보가 상기 인증 지원 서버 또는 상기 인증사 서버를 통해 획득되면 상기 액세스 토큰을 상기 인증 제휴사 서버에 연동되는 저장 장치에 저장하도록 지원하며, 상기 액세스 토큰 검증 결과에 대응하여 상기 사용자 단말의 상기 인증 제휴사 앱을 통한 상기 인증 제휴사 서버로의 로그인을 허용하도록 지원하는 단계; 를 포함하는 방법이 제공된다.

[0016] 또한, 본 발명의 일 실시예에 따르면, 상기의 방법을 수행하기 위한 사용자 단말 및 인증 지원 서버가 제공된다.

[0017] 이 외에도, 본 발명의 방법을 실행하기 위한 컴퓨터 프로그램을 기록하기 위한 컴퓨터 판독 가능한 기록 매체가 더 제공된다.

발명의 효과

[0018] 본 발명에 의하면, 다음과 같은 효과가 있다.

[0019] 본 발명은 가상 화폐의 블록체인 기술을 이용하여 권한 인증을 구현함으로써 사용자의 인증 정보를 외부 공격으로부터 효과적으로 보호할 수 있게 된다.

[0020] 또한, 본 발명은 액세스 토큰을 해쉬함수와 암호화 기술을 이용하여 보호함으로써 보안이 보장되고 위/변조가 불가능한 권한 인증을 제공할 수 있게 된다.

[0021] 또한, 본 발명은 위/변조가 불가능한 블록체인을 통해 권한 인증을 위한 액세스 토큰을 검증하므로 사용자 정보 도용에 따른 문제점을 미연에 방지할 수 있도록 하는 권한 인증을 제공할 수 있게 된다.

도면의 간단한 설명

[0022] 도 1은 본 발명의 일 실시예에 따른 블록체인 기반의 권한 인증 시스템을 개략적으로 도시한 것이고,

도 2는 본 발명의 일 실시예에 따른 블록체인 기반의 권한 인증을 수행하는 방법을 개략적으로 도시한 것이고,

도 3과 도 4는 본 발명의 일 실시예에 따른 블록체인 기반의 권한 인증 방법에서 권한 인증과 관련한 트랜잭션을 블록체인에 등록하는 다른 실시예를 개략적으로 도시한 것이고,

도 5는 본 발명의 일 실시예에 따른 블록체인 기반의 권한 인증을 수행하는 또 다른 방법을 개략적으로 도시한 것이다.

발명을 실시하기 위한 구체적인 내용

[0023] 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.

[0024] 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.

[0025] 도 1은 본 발명의 일 실시예에 따른 블록체인 기반의 권한 인증을 수행하는 시스템을 개략적으로 도시한 것으로, 시스템은 사용자 단말(100), 인증 지원 서버(200), 블록체인(300), 인증사 서버(400), 및 인증 제휴사 서버(500)를 포함할 수 있다.

[0026] 먼저, 사용자 단말(100)은 인증사 앱(120) 및 인증 제휴사 앱(110)들에 의해 사용자에게 서비스되는 정보를 표시하여 주며 권한 인증을 수행하는 디바이스로, PC, 모바일 컴퓨터, PDA/EDA, 휴대 전화, 스마트폰, 태블릿 등을 포함할 수 있다. 그리고, 사용자 단말(100)은 이에 한정되지 않으며, 유무선 통신 기능을 가진 휴대용 게임기, 디지털 카메라 개인 내비게이션 등의 모든 통신 디바이스를 포함할 수 있다. 또한, 사용자 단말(100)은 정보의 송수신을 지원하는 통신부와 정보를 처리하는 프로세서를 포함할 수 있다.

[0027] 다음으로, 인증 지원 서버(200)는 블록체인 기반의 권한 인증을 수행하는 것으로, 통신부와 프로세서를 포함할 수 있다. 동일한 참조 부호를 이용하여 나타낸 것은 설명의 편의를 위한 것일 뿐, 이들 개별 장치들이 동일하다는 의미로 의도된 것은 아니다. 그리고, 본 발명의 다른 실시예에서의 방법은 서버를 상이하게 구성하여 해당 방법을 수행하거나 동일한 인증 지원 서버(200)를 통해 해당 방법을 수행할 수도 있다. 또한, 인증 지원 서버(200)는 블록체인의 각각의 노드에 대응하는 서버이거나, 블록체인의 노드를 관리하는 서버 또는 트랜잭션 서버일 수 있다.

[0028] 구체적으로, 인증 지원 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.

[0029] 이와 같은 컴퓨팅 장치의 통신부는 연동되는 타 컴퓨팅 장치와 요청과 응답을 송수신할 수 있는 바, 일 예시로서 그러한 요청과 응답은 동일한 TCP 세션에 의하여 이루어질 수 있지만, 이에 한정되지는 않는바, 예컨대 UDP 데이터그램으로서 송수신될 수도 있을 것이다.

[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, 운영체제, 특정 목적을 수행하는 애플리케이션의 소프트웨어 구성을 더 포함할 수도 있다.

[0031] 다음으로, 블록체인(300)은 데이터들에 대한 블록을 체인으로 연결하여 분산원장에 기록하는 데이터 분산 처리를 수행하는 주체일 수 있다. 이때, 블록체인(300)은 다수의 블록체인으로 구성될 수 있으며, 각각의 블록체인은 프라이빗 블록체인 또는 퍼블릭 블록체인일 수 있다.

[0032] 다음으로, 인증사 서버(400)는 사용자 단말의 인증사 앱(120)을 통해 사용자가 사용할 수 있는 다양한 서비스를 제공하여 주며, 타 서버와의 통신을 위한 인터페이스를 제공하는 것으로, 정보의 송수신을 지원하는 통신부와 정보를 처리하는 프로세서를 포함할 수 있다.

[0033] 다음으로, 인증 제휴사 서버(500)는 사용자 단말의 인증 제휴사 앱(121)을 통해 사용자가 사용할 수 있는 다양한 서비스를 제공하여 주는 것으로, 인증사 서버(400)와의 제휴를 통해 인증사 서버(400)에서의 사용자 식별 정보 등을 이용하여 사용자 단말(100)의 인증 제휴사 앱(120)으로 권한 인증을 제공하여 줄 수 있으며, 정보의 송수신을 지원하는 통신부와 정보를 처리하는 프로세서를 포함할 수 있다.

[0035] 이와 같이 구성된 시스템을 통해 본 발명의 일 실시예에 따른 블록체인 기반의 권한 인증 방법을 설명하면 다음과 같다.

[0036] 먼저, 도 2를 참조하여 본 발명의 일 실시예에 따른 블록체인 기반의 권한 인증 방법을 설명한다.

[0037] 사용자가 사용자 단말(100)을 통해 인증 제휴사 서버(500)에서 제공되는 서비스를 이용하기 위하여, 사용자 단말(100)의 인증 제휴사 앱(110)을 통해 인증 요청을 생성하도록 한다(S1). 이때, 인증 제휴사 앱(110)은 URL scheme에 의해 인증사 앱(120)을 호출하여 인증사 앱(120)을 통해 검증 확인값을 서명하고 전송하도록 할 수 있으며, 인증 요청 정보는 전자 서명을 위한 검증 확인값을 포함할 수 있으며, 검증 확인값은 논스(nonce), OTP(one time password), 또는 타임스탬프 등을 포함할 수 있다.

[0038] 그리고, 사용자 단말(100)의 인증사 앱(120)은 인증 요청 정보에 포함된 검증 확인값을 인증사 앱(120)의 프라이빗키를 이용하여 전자 서명하여 전자 서명값을 생성한다(S2). 이때, 인증사 앱(120)의 프라이빗키는 인증사 앱(120)의 사용자 인증을 위하여 생성된 PKI 인증서에서의 프라이빗키이며, 프라이빗키에 대응되는 퍼블릭키는 블록체인(300)에 등록된 상태일 수 있다. 또한, 인증사 앱(120)의 프라이빗키를 이용한 전자 서명에서 사용자 단말(100)은 사용자에게 비밀번호, PIN 코드, 사용자의 지문 정보, 및 사용자의 생체 정보 중 적어도 하나를 포

함할 수 있는 패스 정보의 입력을 요청할 수 있으며, 사용자에 의해 입력되는 패스 정보가 기설정된 패스 정보와 일치할 경우에만 전자 서명이 가능하도록 할 수 있다.

[0039] 이후, 사용자 단말(100)의 인증사 앱(120)은 인증 지원 서버(200)로 전자 서명값에 대한 검증을 요청한다(S3). 이때, 전자 서명값에 대한 검증 요청을 위한 전자 서명값 검증 요청 정보에는 인증 요청 정보로부터 획득된 검증 확인값과 전자 서명값을 포함할 수 있다. 또한, 전자 서명값 검증 요청 정보에는 UUID(universally unique identifier) 등의 사용자 단말 식별 정보, 및 전화 번호 등의 사용자 식별 정보 중 적어도 하나 이상을 포함될 수 있다.

[0040] 그러면, 인증 지원 서버(200)는 통신부를 통해 획득되는 전자 서명값 검증 요청 정보에 대응하여 전자 서명값을 검증하거나 전자 서명값을 검증하도록 지원할 수 있다.

[0041] 일 예로, 인증 지원 서버(200)는 인증 지원 서버(200)에 연동된 타 장치에 저장된 인증사 앱(120)에 대응되는 퍼블릭키, 즉, 사용자 식별 정보 또는 사용자 단말 식별 정보에 대응하여 저장된 퍼블릭키를 획득하거나 블록체인(300)으로부터 인증사 앱(120)에 대응되는 퍼블릭키를 획득하며, 인증사 앱에 대응되는 퍼블릭키를 이용하여 전자 서명값의 서명에 사용된 검증 확인값인 전자 서명 검증 확인값을 확인하고, 확인된 전자 서명 검증 확인값이 전자 서명값 검증 요청 정보에 포함된 검증 확인값과 일치하는지 여부를 확인함으로써 전자 서명값을 검증할 수 있다. 그리고, 전자 서명값이 유효한 것으로 확인되면 인증 지원 서버(200)는 액세스 토큰을 생성하여 사용자 단말(100)로 전송하거나 인증 지원 서버(200)에 연동되는 타 장치를 통해 사용자 단말(100)로 전송되도록 한다(S7). 또한, 인증 지원 서버(200)는 생성된 액세스 토큰을 블록체인(300)에 등록하거나 인증 지원 서버(200)에 연동되는 타 장치를 통해 블록체인(300)에 액세스 토큰을 등록하도록 지원한다. 이때, 액세스 토큰은 사용자 단말 식별 정보, 사용자 식별 정보, 및 전자 서명값 중 적어도 하나 이상을 포함하거나, 이들의 해쉬값 중 적어도 하나 이상을 포함할 수 있다.

[0042] 다른 예로, 인증 지원 서버(200)는 블록체인(300)으로 전자 서명값에 대한 검증을 요청하거나 인증 지원 서버(200)에 연동되는 타 장치를 통해 블록체인(300)으로 전자 서명값에 대한 검증을 요청하도록 한다(S4). 그러면, 블록체인(300)은 인증사 앱(120)에 대응되는 퍼블릭키를 이용하여 전자 서명값의 서명에 사용된 전자 서명 검증 확인값을 확인하며, 확인된 전자 서명 검증 확인값이 전자 서명값 검증 요청 정보에 포함된 검증 확인값과 일치하는지 여부를 확인하여 전자 서명값을 검증할 수 있다(S5). 그리고, 전자 서명값이 유효한 것으로 확인되면, 블록체인(300)은 액세스 토큰을 생성하여 블록체인에 등록하고, 생성된 액세스 토큰을 인증 지원 서버(300)로 전송하여 주며(S6), 인증 지원 서버(200)는 블록체인(300)으로부터 획득되는 액세스 토큰을 사용자 단말(100)로 전송하거나 인증 지원 서버(200)에 연동되는 타 장치를 통해 사용자 단말(100)로 전송되도록 한다(S7).

[0043] 상기에서는 액세스 토큰을 블록체인(300)에 등록하였으나, 블록체인(300)이 다수로 이루어질 수 있으며, 일 예로, 블록체인(300)이 제1 블록체인과 제2 블록체인으로 구성될 경우, 인증 지원 서버(200)가 액세스 토큰을 제1 블록체인과 제2 블록체인에 등록하는 과정을 상세히 설명하면 다음과 같다.

[0044] 인증 지원 서버(200)는 액세스 토큰을 제1 블록체인에 등록하거나 인증 지원 서버(200)에 연동되는 타 장치로 하여금 제1 블록체인에 등록하도록 한다.

[0045] 그리고, 제2 블록체인에 소정의 해쉬값을 등록하기 위한 트리거링 조건이 만족되면, 인증 지원 서버(200)는 액세스 토큰에 해쉬함수를 적용하여 생성한 특정 해쉬값과 특정 해쉬값에 매칭되는 적어도 하나의 이웃 해쉬값을 연산함으로써 머클 루트인 대표 해쉬값 또는 대표 해쉬값을 가공한 값을 생성한다.

[0046] 또한, 인증 지원 서버(200)는 생성된 대표 해쉬값 또는 대표 해쉬값을 가공한 값을 제1 블록체인에 등록하거나 인증 지원 서버(200)에 연동되는 타 장치 또는 제1 블록체인으로 하여금 대표 해쉬값 또는 대표 해쉬값을 가공한 값을 제2 블록체인에 등록하도록 할 수 있다.

[0047] 한편, 인증 지원 서버(200)는 제1 특정 해쉬값과 적어도 하나의 이웃 해쉬값을 소정의 데이터 구조로 저장하여 관리할 수 있다. 여기서, 데이터 구조는 다양할 수 있는 데, 일 예로 머클 트리(merkle tree) 구조가 될 수도 있다.

[0048] 즉, 인증 지원 서버(300)는 특정 해쉬값이 특정 리프 노드에 할당된 머클 트리(merkle tree)를 생성하거나 생성하도록 지원할 수 있고, 트리거링 조건이 만족되면, 특정 해쉬값과 매칭되는 적어도 하나의 다른 리프 노드에 할당된 해쉬값을 연산하여 생성되는 머클 루트인 대표 해쉬값 또는 대표 해쉬값을 가공한 값을 제2 블록체인에 등록하거나 인증 지원 서버(200)에 연동되는 타 장치 또는 제1 블록체인으로 하여금 제2 블록체인에 등록하도록

지원할 수 있다.

[0049] 좀더 구체적으로 설명하면, (x1) 인증 지원 서버(200)는, (i) 특정 해쉬값과 (ii) 특정 해쉬값이 할당된 노드의 형제 노드에 할당된 해쉬값을 연산하거나 인증 지원 서버(200)에 연동된 타 장치로 하여금 연산하도록 지원하고, 연산값에 대한 해쉬값을 노드의 부모 노드에 할당하거나 인증 지원 서버(200)에 연동된 타 장치로 하여금 부모 노드에 할당하도록 지원할 수 있다. (x2) 만일, 부모 노드가 머클 트리의 루트 노드이면, 부모 노드에 할당된 해쉬값이 대표 해쉬값 또는 대표 해쉬값을 가공한 값이 된다. (x3) 반면, 부모 노드가 머클 트리의 루트 노드가 아니면, 인증 지원 서버(200)는, 부모 노드에 할당된 해쉬값을 특정 해쉬값으로 하여 (x1) 내지 (x3)를 반복하여 수행한다.

[0050] 그리고, 인증 지원 서버(200)는 최종적으로 머클 트리의 루트 노드에 할당된 해쉬값을 대표 해쉬값 또는 대표 해쉬값을 가공한 값으로서 제2 블록체인에 등록하거나 인증 지원 서버(200)에 연동된 타 장치 또는 제1 블록체인으로 하여금 제2 블록체인에 등록하도록 지원한다. 이때, 대표 해쉬값을 가공한 값은, 예를 들어, 대표 해쉬값에 hex 연산이 수행된 결과값일 수 있다.

[0051] 한편, 인증 지원 서버(200)가 특정 해쉬값과 적어도 하나의 이웃 해쉬값을 소정의 제1-1 데이터 구조로 저장하고, 이후 제1-1 데이터 구조와 동일한 형태의 제1-2 데이터 구조를 저장하여 관리하는 경우, 제1-1 데이터 구조와 제1-2 데이터 구조는 체인 형태로 연결될 수 있다.

[0052] 특히, 상술한 예에서와 같이 제1-1 데이터 구조 및 제1-2 데이터 구조가 머클 트리인 경우, 제1-1 데이터 구조의 루트값 또는 루트값의 해쉬값이 제1-2 데이터 구조의 첫번째 리프 노드에 할당될 수 있다.

[0053] 또한, 제1-2 데이터 구조를 생성할 때는 제1-1 데이터 구조에 대한 검증이 이루어짐으로써 데이터 integrity가 좀더 보장될 수 있다. 제1-2 데이터 구조의 검증에 대해서는 후술하기로 한다.

[0054] 또한, 체인 형태로 연결된 적어도 하나의 머클 트리 중 첫번째 머클 트리의 경우, 첫번째 머클 트리의 첫번째 리프 노드에는 텍스트, 숫자, 또는 기호로 이루어진 소정의 메시지 데이터의 해쉬값 또는 이를 가공한 값이 할당될 수 있다. 예를 들어, 머클 트리 생성시 인증 지원 서버(200)에 의해 최초로 부여된 입력 메시지의 해쉬값이 할당될 수 있다.

[0055] 도 3 및 도 4는 본 발명의 일 실시예에 따라 생성된 머클 트리의 예를 도시한 것이다.

[0056] 도 3에서는 리프 노드의 개수가 4개인 머클 트리가 도시된다. 도시된 머클 트리는 첫번째 머클 트리이기 때문에 (tree_id=0), 첫번째 리프 노드인 h0 노드에는 소정의 메시지 데이터의 해쉬값(sha256(coinplug_unique_message))이 할당되었음을 알 수 있다. 기록 데이터에 대한 등록 요청이 있는 경우, 인증 지원 서버(200)는 현재 구성 중인 머클 트리의 가장 마지막 리프 노드의 다음 리프 노드를 생성하여 특정 해쉬값 또는 특정 해쉬값을 가공한 값을 할당하거나 할당하도록 지원한다. 예를 들어, 도 3의 머클 트리에서 두번째 리프 노드인 h1 노드까지 값 할당이 완료된 상태에서 새로운 리프 노드를 생성하여야 하는 경우, 다음 리프 노드인 h2 노드를 생성하여 특정 해쉬값 또는 특정 해쉬값을 가공한 값(sha256(input2))을 할당할 수 있다. 또한, 인증 지원 서버(200)는 (i) h2 노드에 할당된 특정 해쉬값과 (ii) h2 노드의 형제 노드인 h3 노드에 할당된 해쉬값을 연산하거나 연산하도록 지원할 수 있다. 연산값에 대한 해쉬값은 h2 노드와 h3 노드의 부모 노드(h23 노드)에 할당된다. 부모 노드(h23 노드)가 머클 트리의 루트 노드가 아니므로 인증 지원 서버(200)는 h23 노드에 할당된 해쉬값을 특정 해쉬값으로 하여 상기 과정을 반복하여 수행할 수 있다. 즉, h23 노드에 할당된 해쉬값을 특정 해쉬값으로 하고, h23 노드에 할당된 해쉬값과 h01 노드에 할당된 해쉬값을 연산하여 h23 노드와 h01 노드의 부모 노드(h0123 노드)에 할당할 수 있다. 이때, h0123 노드가 머클 트리의 루트 노드이므로 인증 지원 서버(200)는, h0123 노드에 할당된 해쉬값을 가공한 값(hex(h{node_index}))을 제2 블록체인에 등록하거나 인증 지원 서버(200)에 연동된 타 장치 또는 제1 블록체인으로 하여금 제2 블록체인에 등록하도록 지원할 수 있다

[0057] 한편, 전술한 트리거링 조건이란, (i) 소정의 개수만큼 액세스 토큰과 트랜잭션이 생성되는 조건, (ii) 소정 시간이 경과하는 조건, (iii) 제1 블록체인에서 블록이 생성되는 조건, (iv) 서비스 특성에 대한 조건 중 적어도 하나를 포함할 수 있다.

[0058] 한편, 예를 들어, 액세스 토큰과 관련한 트랜잭션이 머클 트리의 리프 노드 수만큼 획득되면 머클 트리를 생성하고, 머클 트리의 루트값을 제2 블록체인에 등록하거나 타 장치로 하여금 등록하도록 지원할 수 있다.

[0059] 또한, 인증 지원 서버(200)는 소정 시간 단위로 전술한 머클 트리의 루트값을 생성할 수 있다(상기 (ii) 조건).

이 경우 인증 지원 서버(200)는 소정의 시간이 경과되면 그때까지의 입력값을 이용하여 머클 트리를 생성하고 머클 트리의 루트값을 제2 블록체인에 등록하거나 인증 지원 서버(200)에 연동된 타 장치 또는 제1 블록체인으로 하여금 제2 블록체인에 등록하도록 지원할 수 있다.

[0060] 그런데, 이 경우에는 소정 시간이 경과하였음에도 머클 트리의 특정 해쉬값이 할당된 노드의 형제 노드에 값이 할당되지 않을 수 있다. 이처럼 트리거링 조건이 만족되었음에도 특정 해쉬값이 할당된 노드의 형제 노드에 해쉬값이 할당되어 있지 않은 경우, 인증 지원 서버(200)는, 형제 노드에 소정의 해쉬값을 할당하거나 할당하도록 지원하여 전술한 방식으로 머클 트리의 루트값이 산출되도록 할 수 있다. 예를 들어, 인증 지원 서버(200)는 특정 해쉬값을 복제하여 형제 노드에 할당하거나 할당하도록 지원할 수 있다.

[0061] 그리고, 서비스 특성이란, 액세스 토큰과 관련한 트랜잭션을 발행한 발행자가 제공한 비용 정보, 액세스 토큰 관련 트랜잭션 등록이 이루어지는 시간대 정보, 액세스 토큰 관련 트랜잭션 등록 서비스가 이루어지는 지역 정보, 액세스 토큰 관련 트랜잭션 등록 요청을 한 회사 타입 정보 중 적어도 일부가 될 수 있다. 다만, 여기서 기재한 것에 한정할 것은 아니고, 통상적으로 인정되는 차등적 서비스가 제공될 수 있는 다양한 조건 정보를 포함한다.

[0062] 한편, 새로운 머클 트리 생성이 시작되고, 액세스 토큰 관련 트랜잭션이 없는 상태에서 트리거링 조건이 만족되면, 인증 지원 서버(200)는, 소정의 메시지 데이터가 첫번째 리프 노드와 두번째 리프 노드에 할당된 머클 트리를 생성하거나 생성하도록 지원하고, 머클 트리의 루트값 또는 이를 가공한 값을 제2 블록체인에 등록하거나 인증 지원 서버(200)에 연동된 타 장치 또는 제1 블록체인으로 하여금 제2 블록체인에 등록하도록 지원할 수 있다. 이 경우에는 리프 노드 2개짜리 머클 트리가 생성될 수도 있는 것이다.

[0063] 또한, 전술한 것처럼 인증 지원 서버(200)가 특정 해쉬값과 적어도 하나의 이웃 해쉬값을 소정의 제1-1 데이터 구조로 저장하고, 이후 제1-1 데이터 구조와 동일한 형태의 제1-2 데이터 구조를 저장하여 관리하는 경우, 제1-1 데이터 구조와 제1-2 데이터 구조는 체인 형태로 연결될 수 있다. 특히, 제1-1 데이터 구조 및 제1-2 데이터 구조가 머클 트리인 경우, 제1-1 데이터 구조의 루트값 또는 루트값의 해쉬값이 제1-2 데이터 구조의 첫번째 리프 노드에 할당될 수 있다.

[0064] 도 4는 본 발명의 일 실시예에 따라 제1-2 데이터 구조로서 생성된 머클 트리를 도시한 도면이다.

[0065] 도 4를 참조하면, 도 3의 머클 트리(tree_id=0)의 루트값(hex(h0123))이 새로운 머클 트리의 첫번째 리프 노드(h4 노드)에 할당되었음을 알 수 있다(sha256(input4)). 본 발명은 이와 같이 트랜잭션 발생시 생성되는 복수의 데이터 구조를 연결함으로써 중간에 데이터가 변조가 발생되는 경우라도 쉽게 트래킹이 가능하여 데이터 integrity를 향상시키는 장점을 가진다.

[0067] 다시 도 2를 참조하면, 인증 지원 서버(200)로부터 액세스 토큰이 전송되면, 사용자 단말(100)은 인증사 앱(120)을 통해 액세스 토큰을 수신하여 인증 제휴사 앱(110)으로 전달하며(S8), 인증 제휴사 앱(110)을 통해 액세스 토큰을 이용하여 인증 제휴사 서버(500)로 로그인을 요청하도록 한다(S9). 이때, 로그인 요청 정보에는 액세스 토큰, 사용자 단말 식별 정보, 및 사용자 식별 정보 중 적어도 하나 이상이 포함될 수 있으나, 이에 한정되지 않으며 이들의 해쉬값 중 적어도 하나 이상이 포함될 수도 있다.

[0068] 그리고, 인증 제휴사 서버(500)는 사용자 단말(100)의 인증 제휴사 앱(110)으로부터의 로그인 요청에 대응하여 로그인 요청 정보로부터 획득된 액세스 토큰에 대한 검증을 인증 지원 서버(200)로 요청하거나 인증사 서버(400)를 통해 인증 지원 서버(200)로 액세스 토큰 검증 요청이 이루어지도록 할 수 있다(S10)(S11). 이때, 액세스 토큰 검증 요청 정보에는 액세스 토큰, 사용자 단말 식별 정보, 및 사용자 식별 정보 중 적어도 하나 이상을 포함하거나, 이들의 해쉬값 중 적어도 하나 이상을 포함할 수 있다.

[0069] 그러면, 인증 지원 서버(200)는 액세스 토큰 검증 요청 정보가 인증 제휴사 서버(500)로부터 획득되거나 인증 제휴사 서버(500)로부터의 액세스 토큰 검증 요청 정보가 인증사 서버(400)를 통해 획득됨에 따라, 액세스 토큰을 검증하거나 인증 지원 서버(200)에 연동되는 타 장치를 통해 액세스 토큰을 검증하도록 할 수 있다. 또한, 인증 지원 서버(200)는 블록체인(300)으로 액세스 토큰에 대한 검증을 요청하거나 인증 지원 서버(200)에 연동되는 타 장치를 통해 블록체인(300)으로 액세스 토큰에 대한 검증을 요청(S12)하도록 함으로써 블록체인(300)으로 하여금 액세스 토큰을 검증(S13)하도록 지원할 수 있다.

[0070] 이때, 액세스 토큰의 검증은, 검증 요청된 액세스 토큰이 사용자 단말 식별 정보 또는 사용자 식별 정보에 대응

하여 블록체인(300)에 등록된 액세스 토큰과 일치하는지를 확인함으로써 이루어질 수 있다.

[0071] 한편, 블록체인(300)이 제1 블록체인과 제2 블록체인으로 구성된 경우에는, 사용자 식별 정보 또는 사용자 단말 식별 정보에 대응하여 제2 블록체인에 등록된 대표 해쉬값 또는 대표 해쉬값을 가공한 값을 확인하고, 제2 블록체인에서 확인된 대표 해쉬값 또는 대표 해쉬값을 가공한 값과 대응하여 제1 블록체인에 등록된 머클 트리 정보 및 리프 노드 정보를 확인하며, 머클 트리 정보 및 리프 노드 정보를 참조하여 제1 블록체인에 등록된 액세스 토큰을 확인하거나 타 장치로 하여금 확인하도록 지원할 수 있다.

[0072] 이후, 액세스 토큰이 유효한 것으로 확인되면(S14), 인증 지원 서버(200)는 액세스 토큰 검증 결과 정보를 인증 제휴사 서버(500)로 전송하거나 인증 지원 서버(200)에 연동되는 타 장치 또는 인증사 서버(400)를 통해 액세스 토큰 검증 결과 정보가 인증 제휴사 서버(500)로 전송되도록 한다(S15)(S17). 이때, 인증 지원 서버(200)는 사용자 단말 식별 정보 또는 사용자 식별 정보에 대응하는 사용자 정보를 확인하고(S16) 확인된 사용자 정보를 액세스 토큰 검증 결과 정보에 더하여 인증 제휴사 서버(500)로 전송하거나, 인증 지원 서버(200)에 연동되는 타 장치 또는 인증사 서버(400)로 하여금 사용자 단말 식별 정보 또는 사용자 식별 정보에 대응하는 사용자 정보를 확인하고(S16) 확인된 사용자 정보를 액세스 토큰 검증 결과 정보에 더하여 인증 제휴사 서버(500)로 전송하도록 할 수 있다.

[0073] 그러면, 인증 제휴사 서버(500)는 액세스 토큰 검증 결과 정보에 대응하여 액세스 토큰을 인증 제휴사 서버(500)에 연동되는 저장 장치에 저장하며(S18), 액세스 토큰 검증 결과에 대응하여 사용자 단말(100)의 인증 제휴사 앱(110)을 통한 인증 제휴사 서버(500)로의 로그인을 허용하도록 지원할 수 있다(S19). 이때, 인증 제휴사 서버(500)는 액세스 토큰의 저장시, 사용자 단말 식별 정보 또는 사용자 식별 정보에 대응하여 액세스 토큰이 저장되도록 할 수 있으며, 액세스 토큰에 더하여 획득된 사용자 정보를 추가적으로 저장할 수도 있다.

[0075] 다음으로, 도 5를 참조하여 본 발명의 다른 실시예에 따른 블록체인 기반의 권한 인증 방법을 설명한다.

[0076] 먼저, 도 2에서와 같은 방법에 의해 인증 제휴사 서버(500)에 액세스 토큰이 저장될 수 있다.

[0077] 즉, 사용자 단말(100)의 인증 제휴사 앱(110)으로부터의 검증 확인값을 포함하는 인증 요청 정보에 대응한 사용자 단말(100)의 인증사 앱(120)으로부터 전자 서명값에 대한 전자 서명값 검증 요청 정보가 획득되면, 인증 지원 서버(200)가 전자 서명값을 검증하거나 블록체인(300)으로 하여금 전자 서명값을 검증하도록 하며, 전자 서명값의 유효한 결과에 대응되어 액세스 토큰이 생성되면 액세스 토큰을 블록체인(300)에 등록되도록 하며, 액세스 토큰을 사용자 단말(100)로 전송되도록 한다. 그러면, 사용자 단말(100)은 인증사 앱(120)을 통해 액세스 토큰을 수신하며 인증 제휴사 앱(110)을 통해 액세스 토큰을 이용하여 인증 제휴사 서버(500)로 액세스 토큰의 등록을 요청하도록 지원한다. 이후, 적어도 액세스 토큰을 포함하는 액세스 토큰 검증 요청 정보가 인증 제휴사 서버(500)로부터 획득되거나 인증 제휴사 서버(500)로부터의 액세스 토큰 검증 요청 정보가 인증사 서버(400)를 통해 획득되면, 인증 지원 서버(200)가 액세스 토큰을 검증하거나 블록체인(300)으로 하여금 액세스 토큰을 검증하도록 지원하며, 액세스 토큰이 유효한 것으로 확인되면, 액세스 토큰 검증 결과 정보를 인증 제휴사 서버(500)로 전송하거나 인증 지원 서버(200)에 연동되는 타 장치 또는 인증사 서버(400)를 통해 액세스 토큰 검증 결과 정보가 인증 제휴사 서버(500)로 전송되도록 한다. 이에 따라, 인증 제휴사 서버(500)는 액세스 토큰을 인증 제휴사 서버(500)에 연동되는 저장 장치에 저장한다. 이때, 액세스 토큰에 더하여, 사용자 단말 식별 정보, 사용자 식별 정보, 및 사용자 정보 등이 추가적으로 저장될 수도 있다.

[0078] 이때, 블록체인(300)은 도 2에서의 설명에서와 같이 제1 블록체인과 제2 블록체인으로 구성될 수 있으며, 제1 블록체인에는 액세스 토큰이 등록되고, 제2 블록체인에는 액세스 토큰에 대응되는 머클 루트가 등록될 수 있다.

[0079] 상기에서와 같이, 인증 제휴사 서버(500)에 액세스 토큰이 저장된 상태에서, 사용자가 사용자 단말(100)을 통해 인증 제휴사 서버(500)에서 제공되는 서비스를 이용하기 위하여, 사용자 단말(100)의 인증 제휴사 앱(110)을 통해 인증 제휴사 서버(500)로 로그인을 요청한다(S51). 이때, 로그인 요청 정보에는 사용자 단말 식별 정보, 및 사용자 식별 정보 중 적어도 하나 이상이 포함될 수 있으나, 이에 한정되지 않으며 이들의 해쉬값 중 적어도 하나 이상이 포함될 수도 있다.

[0080] 그러면, 인증 제휴사 서버(500)는 로그인 정보에 대응하여 저장된 액세스 토큰을 확인하며(S52), 확인된 액세스 토큰에 대한 검증을 인증 지원 서버(200)로 요청하거나 인증사 서버(400)를 통해 인증 지원 서버(200)로 액세스 토큰 검증 요청이 이루어지도록 할 수 있다(S53)(S54). 이때, 액세스 토큰 검증 요청 정보에는 액세스 토큰, 사용자 단말 식별 정보, 및 사용자 식별 정보 중 적어도 하나 이상을 포함하거나, 이들의 해쉬값 중 적어도 하나

이상을 포함할 수 있다.

[0081] 그러면, 인증 지원 서버(200)는 액세스 토큰 검증 요청 정보가 인증 제휴사 서버(500)로부터 획득되거나 인증 제휴사 서버(500)로부터의 액세스 토큰 검증 요청 정보가 인증사 서버(400)를 통해 획득됨에 따라, 액세스 토큰을 검증하거나 인증 지원 서버(200)에 연동되는 타 장치를 통해 액세스 토큰을 검증하도록 할 수 있다. 또한, 인증 지원 서버(200)는 블록체인(300)으로 액세스 토큰에 대한 검증을 요청하거나 인증 지원 서버(200)에 연동되는 타 장치를 통해 블록체인(300)으로 액세스 토큰에 대한 검증을 요청(S55)하도록 함으로써 블록체인(300)으로 하여금 액세스 토큰을 검증(S56)하도록 지원할 수 있다.

[0082] 이때, 액세스 토큰의 검증은, 검증 요청된 액세스 토큰이 사용자 단말 식별 정보 또는 사용자 식별 정보에 대응하여 블록체인(300)에 등록된 액세스 토큰과 일치하는지를 확인함으로써 이루어질 수 있다.

[0083] 한편, 블록체인(300)이 제1 블록체인과 제2 블록체인으로 구성된 경우에는, 사용자 식별 정보 또는 사용자 단말 식별 정보에 대응하여 제2 블록체인에 등록된 대표 해쉬값 또는 대표 해쉬값을 가공한 값을 확인하고, 제2 블록체인에서 확인된 대표 해쉬값 또는 대표 해쉬값을 가공한 값과 대응하여 제1 블록체인에 등록된 머클 트리 정보 및 리프 노드 정보를 확인하며, 머클 트리 정보 및 리프 노드 정보를 참조하여 제1 블록체인에 등록된 액세스 토큰을 확인하거나 타 장치로 하여금 확인하도록 지원할 수 있다.

[0084] 이후, 액세스 토큰이 유효한 것으로 확인되면(S57), 인증 지원 서버(200)는 액세스 토큰 검증 결과 정보를 인증 제휴사 서버(500)로 전송하거나 인증 지원 서버(200)에 연동되는 타 장치 또는 인증사 서버(400)를 통해 액세스 토큰 검증 결과 정보가 인증 제휴사 서버(500)로 전송되도록 한다(S58)(S59).

[0085] 그러면, 인증 제휴사 서버(500)는 액세스 토큰 검증 결과 정보에 대응하여 사용자 단말(100)의 인증 제휴사 앱(110)을 통한 인증 제휴사 서버(500)로의 로그인을 허용하도록 지원할 수 있다(S60).

[0087] 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.

[0088] 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.

[0089] 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

[0090] 100: 사용자 단말,

110: 인증 제휴사 앱,

120: 인증사 앱,

200: 인증 지원 서버,

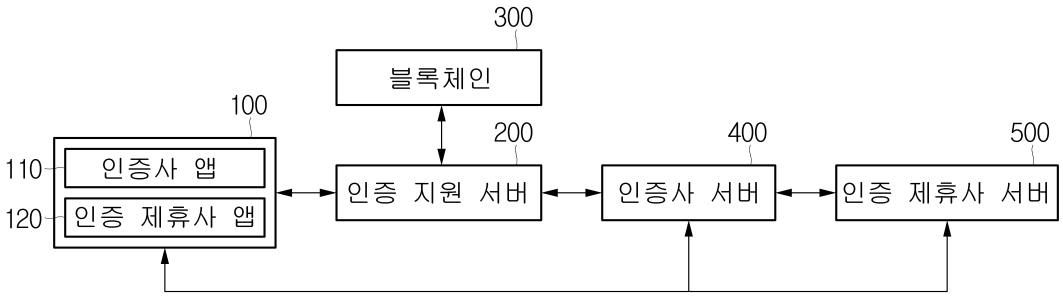
300: 블록체인,

400: 인증사 서버,

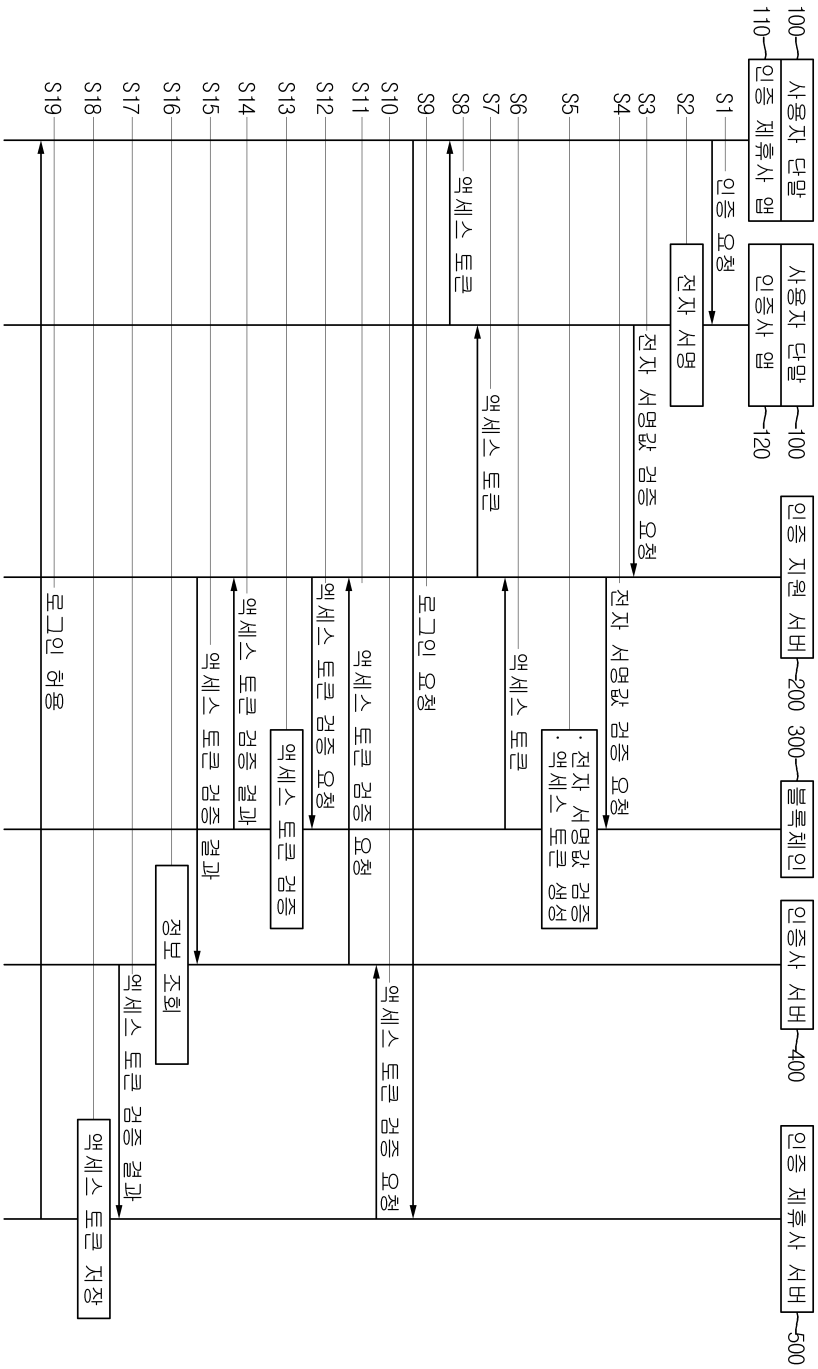
500: 인증 제휴사 서버

도면

도면1



도면2


사용자 단말
인증 제휴사 앱
100
110
사용자 단말
인증사 앱
100
120
인증 지원 서버
200
블록체인
300
인증사 서버
400
인증 제휴사 서버
500
S1
인증 요청
S2
전자 서명
S3
S4
전자 서명값 검증 요청
S5
· 전자 서명값 검증
· 액세스 토큰 생성
S6
액세스 토큰
S7
액세스 토큰
S8
S9
로그인 요청
S10
S11
액세스 토큰 검증 요청
S12
액세스 토큰 검증 요청
S13
액세스 토큰 검증
S14
액세스 토큰 검증 결과
S15
액세스 토큰 검증 결과
S16
정보 조회
S17
액세스 토큰 검증 결과
S18
액세스 토큰 저장
S19
로그인 허용

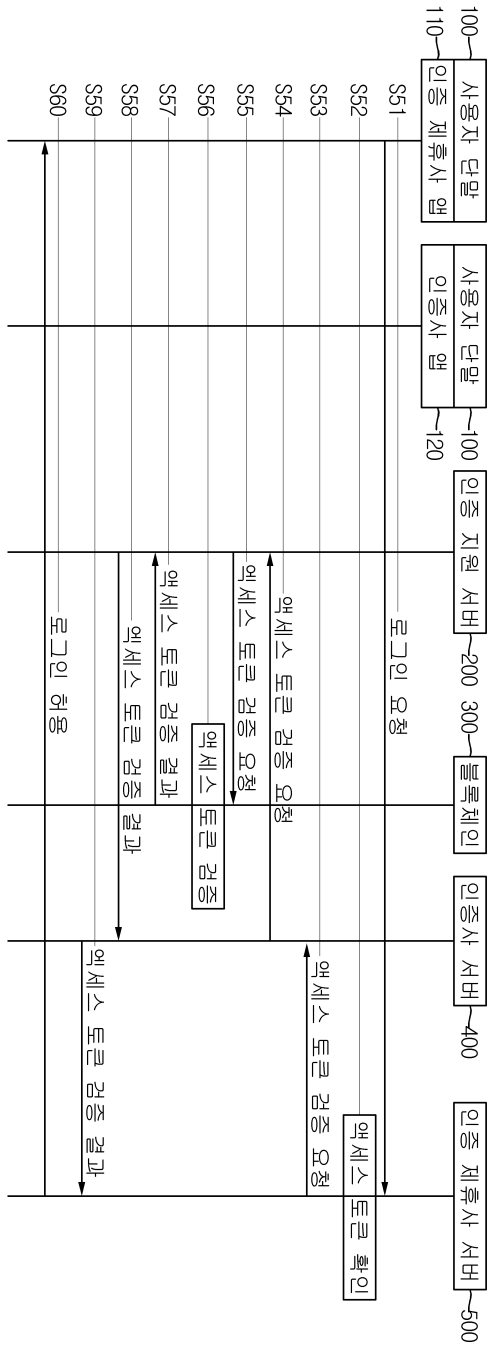
도면3

tree_id = 0 hex(h{node_index}) = node_hash
h0123
hex(h0123) = root_hash
sha256 digest
(ROOT)
sha256 digest
h01
h23
sha256 digest
(LEAVES)
INPUT MESSAGE
h0
UNIQUE ID = (0, 0)
Coinplug_unique_message
node_index = 0
h1
UNIQUE ID = (0, 1)
input1
node_index = 1
h2
UNIQUE ID = (0, 2)
input2
node_index = 2
h3
UNIQUE ID = (0, 3)
input3
node_index = 3
input0 = PrivBCM_unique_message
input1 = RN+SigPrivA(RN)+PubA (= User A registration)
input2 = TrxA
input3 = delta_0
h0 = sha256(input0)
h1 = sha256(input1)
h2 = sha256(input2)
h3 = sha256(input3)
h01 = sha256(h0 + h1)
h23 = sha256(h2 + h3)
h0123 = sha256(h01 + h23)

도면4

tree_id = 1 hex(h{node_index}) = node_hash
h4567
hex(h4567) = root_hash
sha256 digest
(ROOT)
sha256 digest
h45
h67
sha256 digest
(LEAVES)
INPUT MESSAGE
h4
UNIQUE ID = (1, 0)
previous_root_hash
node_index = 0
h5
UNIQUE ID = (1, 1)
input5
node_index = 1
h6
UNIQUE ID = (1, 2)
input6
node_index = 2
h7
UNIQUE ID = (1, 3)
input7
node_index = 3
input4 = previous_root_hash
input5 = TrxD
input6 = RN+SigPrivB(RN)+PubB (= User B registration)
input7 = delta_1
h4 = sha256(input4)
h5 = sha256(input5)
h6 = sha256(input6)
h7 = sha256(input7)
h45 = sha256(h4 + h5)
h67 = sha256(h6 + h7)
h4567 = sha256(h45 + h67)

도면5


사용자 단말
인증 제휴사 앱
100
110
사용자 단말
인증사 앱
100
120
인증 지원 서버
200
블록체인
300
인증사 서버
400
인증 제휴사 서버
500
S51
S52
S53
S54
S55
S56
S57
S58
S59
S60
로그인 요청
액세스 토큰 검증 요청
액세스 토큰 검증 요청
액세스 토큰 검증 결과
액세스 토큰 검증
액세스 토큰 검증 결과
액세스 토큰 검증 결과
액세스 토큰 확인
로그인 허용