(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년01월29일
(11) 등록번호 10-2209481
(24) 등록일자 2021년01월25일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01)
(52) CPC특허분류
H04L 63/06 (2013.01)
H04L 63/0823 (2013.01)
(21) 출원번호 10-2019-0146935
(22) 출원일자 2019년11월15일
심사청구일자 2019년11월15일
(65) 공개번호 10-2020-0057660
(43) 공개일자 2020년05월26일
(30) 우선권주장
1020180141326 2018년11월16일 대한민국(KR)
(56) 선행기술조사문헌
KR101066063 B1*
KR1020100068046 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
에듀해시글로벌파트너스 주식회사
서울특별시 영등포구 영등포로 414 (신길동) 5층
(72) 발명자
전중훤
경기도 부천시 길주로 91, 1303호
김재규
서울특별시 관악구 성현로 80, 140동 1402호
(74) 대리인
김남식, 김한, 이인행

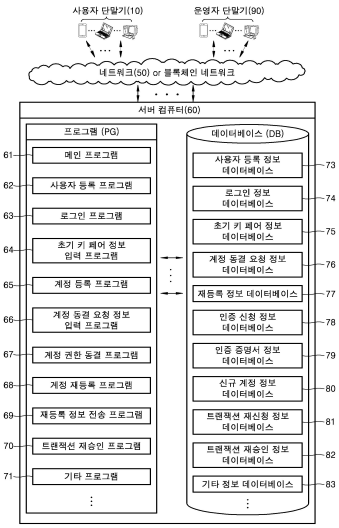
전체 청구항 수 : 총 10 항 심사관 : 이준석

(54) 발명의 명칭 **계정 키 페어 기반 계정 인증 서비스를 운영하는 방법과 시스템 및 이 방법을 기록한 컴퓨터로 읽을 수 있는 기록 매체**

(57) 요 약

본 발명은 적어도 하나의 사용자 단말기와 운영자 단말기 및 네트워크를 통하여 연결된 서버 컴퓨터를 구비한 컴퓨터 시스템을 이용하여 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법에 있어서, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 단계; 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 단계; 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 단계; 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 단계; 및 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 단계;를 포함할 수 있다.

대 표 도 - 도1



(52) CPC특허분류
H04L 63/0876 (2013.01)

명 세 서

청구범위

청구항 1

적어도 하나의 사용자 단말기와 운영자 단말기 및 네트워크를 통하여 연결된 서버 컴퓨터를 구비한 컴퓨터 시스템을 이용하여 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법에 있어서,

상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 단계;

상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 단계;

상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 단계;

상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 단계; 및

상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 단계;

를 포함하고,

상기 초기 키 페어 정보를 입력받는 단계는,

상기 사용자 단말기로부터 사용자 인증 신청 정보를 입력받는 단계;

상기 사용자 인증 신청 정보를 이용하여 사용자를 인증하고, 인증 증명서 정보를 발급하는 단계;

상기 사용자 단말기로 상기 인증 증명서 정보를 전송하는 단계;

상기 사용자 단말기로부터 블록체인 네트워크를 통해 상기 인증 증명서 정보 및 신규 계정 신청 정보를 입력받는 단계;

상기 블록체인 네트워크를 통해 인증서의 정당성을 조회하여 신규 계정 정보를 생성하고, 상기 사용자 단말기로 상기 신규 계정 정보를 전송하는 단계; 및

상기 사용자 단말기로부터 신규 계정 정보 및 이와 매칭된 상기 초기 키 페어 정보를 입력받는 단계;

를 포함하는, 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법.

청구항 2

적어도 하나의 사용자 단말기와 운영자 단말기 및 네트워크를 통하여 연결된 서버 컴퓨터를 구비한 컴퓨터 시스템을 이용하여 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법에 있어서,

상기 서버 컴퓨터는, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 초기 키 페어 정보 입력 프로그램, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 계정 등록 프로그램, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 계정 동결 요청 정보 입력 프로그램, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 계정 권한 동결 프로그램, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 계정 재등록 프로그램, 상기 초기 키 페어 정보가 저장되는 초기 키 페어 정보 데이터베이스, 상기 계정 동결 요청 정보가 저장되는 계정 동결 요청 정보 데이터베이스, 상기 재등록 정보가 저장되는 재등록 정보 데이터베이스를 포함하고,

(a) 상기 초기 키 페어 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 단계;

(b) 상기 계정 등록 프로그램에 의해서, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 단계;

(c) 상기 계정 동결 요청 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 단계;

(d) 상기 계정 권한 동결 프로그램에 의해서, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 단계; 및

(e) 상기 계정 재등록 프로그램에 의해서, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 단계;

를 포함하고,

상기 초기 키 페어 정보 입력 프로그램은, 상기 사용자 단말기로부터 사용자 인증 신청 정보를 입력받는 인증 신청 정보 입력 프로그램, 상기 사용자 인증 신청 정보를 이용하여 사용자를 인증하고, 인증 증명서 정보를 발급하는 인증 증명서 발급 프로그램, 상기 사용자 단말기로 상기 인증 증명서 정보를 전송하는 인증 증명서 정보 전송 프로그램, 상기 사용자 단말기로부터 블록체인 네트워크를 통해 상기 인증 증명서 정보 및 신규 계정 신청 정보를 입력받는 신규 계정 신청 정보 입력 프로그램, 상기 블록체인 네트워크를 통해 인증서의 정당성을 조회하여 신규 계정 정보를 생성하고, 상기 사용자 단말기로 상기 신규 계정 정보를 전송하는 신규 계정 정보 전송 프로그램, 상기 사용자 단말기로부터 신규 계정 정보 및 이와 매칭된 상기 초기 키 페어 정보를 입력받는 계정 매칭 정보 입력 프로그램, 상기 인증 신청 정보가 저장되는 인증 신청 정보 데이터베이스, 상기 인증 증명서 정보가 저장되는 인증 증명서 정보 데이터베이스, 상기 신규 계정 정보가 저장되는 신규 계정 정보 데이터베이스를 포함하고,

상기 (a) 단계는,

(a-1) 상기 인증 신청 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 사용자 인증 신청 정보를 입력받는 단계;

(a-2) 상기 인증 증명서 발급 프로그램에 의해서, 상기 사용자 인증 신청 정보를 이용하여 사용자를 인증하고, 인증 증명서 정보를 발급하는 단계;

(a-3) 상기 인증 증명서 정보 전송 프로그램에 의해서, 상기 사용자 단말기로 상기 인증 증명서 정보를 전송하는 단계;

(a-4) 상기 신규 계정 신청 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 블록체인 네트워크를 통해 상기 인증 증명서 정보 및 신규 계정 신청 정보를 입력받는 단계;

(a-5) 상기 신규 계정 정보 전송 프로그램에 의해서, 상기 블록체인 네트워크를 통해 인증서의 정당성을 조회하여 신규 계정 정보를 생성하고, 상기 사용자 단말기로 상기 신규 계정 정보를 전송하는 단계; 및

(a-6) 상기 계정 매칭 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 신규 계정 정보 및 이와 매칭된 상기 초기 키 페어 정보를 입력받는 단계;

를 포함하는, 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법.

청구항 3

삭제

청구항 4

적어도 하나의 사용자 단말기와 운영자 단말기 및 네트워크를 통하여 연결된 서버 컴퓨터를 구비한 컴퓨터 시스템을 이용하여 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법에 있어서,

상기 서버 컴퓨터는, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 초기 키 페어 정보 입력 프로그램, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 계정 등록 프로그램, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 계정 동결 요청 정보 입력 프로그램, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 계정 권한 동결 프로그램, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 계정 재등록 프로그램, 상기 초기 키 페어 정보가 저장되는 초기 키 페어 정보 데이터베이스, 상기 계정 동결 요청 정보가 저장되는 계정 동결 요청 정보 데이터베이스, 상기 재등록 정보가 저장되는 재등록 정보 데이터베이스를 포함하고,

(a) 상기 초기 키 페어 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 단계;

(b) 상기 계정 등록 프로그램에 의해서, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 단계;

(c) 상기 계정 동결 요청 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 단계;

(d) 상기 계정 권한 동결 프로그램에 의해서, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 단계; 및

(e) 상기 계정 재등록 프로그램에 의해서, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 단계;

를 포함하고,

상기 계정 권한 동결 프로그램은, 상기 계정 동결 요청 정보의 적절성을 심사하는 계정 동결 적절성 심사 프로그램, 상기 계정 동결 요청 정보가 계정 동결 조건을 충족하면, 상기 제 1 키를 이용한 상기 계정을 동결 조치하는 계정 동결 프로그램, 상기 제 1 키를 이용한 상기 계정의 모든 트랜잭션의 승인을 거부하는 트랜잭션 거부 프로그램을 포함하고,

상기 (c) 단계는,

(c-1) 상기 계정 동결 적절성 심사 프로그램에 의해서, 상기 계정 동결 요청 정보의 적절성을 심사하는 단계;

(c-2) 상기 계정 동결 프로그램에 의해서, 상기 계정 동결 요청 정보가 계정 동결 조건을 충족하면, 상기 제 1 키를 이용한 상기 계정을 동결 조치하는 단계; 및

(c-3) 상기 트랜잭션 거부 프로그램에 의해서, 상기 제 1 키를 이용한 상기 계정의 모든 트랜잭션의 승인을 거부하는 단계;

를 포함하는, 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법.

청구항 5

적어도 하나의 사용자 단말기와 운영자 단말기 및 네트워크를 통하여 연결된 서버 컴퓨터를 구비한 컴퓨터 시스템을 이용하여 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법에 있어서,

상기 서버 컴퓨터는, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 초기 키 페어 정보 입력 프로그램, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 계정 등록 프로그램, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 계정 동결 요청 정보 입력 프로그램, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 계정 권한 동결 프로그램, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 계정 재등록 프로그램, 상기 초기 키 페어 정보가 저장되는 초기 키 페어 정보 데이터베이스, 상기 계정 동결 요청 정보가 저장되는 계정 동결 요청 정보 데이터베이스, 상기 재등록 정보가 저장되는 재등록 정보 데이터베이스를 포함하고,

(a) 상기 초기 키 페어 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 단계;

(b) 상기 계정 등록 프로그램에 의해서, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 단계;

(c) 상기 계정 동결 요청 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 단계;

(d) 상기 계정 권한 동결 프로그램에 의해서, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 단계; 및

(e) 상기 계정 재등록 프로그램에 의해서, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 단계;

를 포함하고,

상기 계정 재등록 프로그램은, 상기 사용자 단말기로부터 사용자 인증 재신청 정보를 입력받는 인증 재신청 정보 입력 프로그램, 상기 사용자 인증 재신청 정보를 이용하여 사용자를 재인증하고, 재인증 증명서 정보를 발급하는 인증 증명서 재발급 프로그램, 상기 사용자 단말기로 상기 재인증 증명서 정보를 전송하는 인증 증명서 정보 재전송 프로그램, 상기 사용자 단말기로부터 블록체인 네트워크를 통해 상기 재인증 증명서 정보를 입력받는 재신청 정보 입력 프로그램, 상기 블록체인 네트워크를 통해 인증서의 정당성을 조회하는 인증서 재조회 프로그램, 사용자의 재등록 정보를 바탕으로 재등록이 인정되는 계정 재등록 인정 프로그램을 포함하고,

상기 (e) 단계는,

(e-1) 상기 인증 재신청 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 사용자 인증 재신청 정보를 입력받는 단계;

(e-2) 상기 인증 증명서 재발급 프로그램에 의해서, 상기 사용자 인증 재신청 정보를 이용하여 사용자를 재인증하고, 재인증 증명서 정보를 발급하는 단계;

(e-3) 상기 인증 증명서 정보 재전송 프로그램에 의해서, 상기 사용자 단말기로 상기 재인증 증명서 정보를 전송하는 단계;

(e-4) 상기 재신청 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 블록체인 네트워크를 통해 상기 재인증 증명서 정보를 입력받는 단계;

(e-5) 상기 인증서 재조회 프로그램에 의해서, 상기 블록체인 네트워크를 통해 인증서의 정당성을 조회하는 단계; 및

(e-6) 상기 계정 재등록 인정 프로그램에 의해서, 사용자의 재등록 정보를 바탕으로 재등록이 인정되는 단계;

를 포함하는, 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법.

청구항 6

적어도 하나의 사용자 단말기와 운영자 단말기 및 네트워크를 통하여 연결된 서버 컴퓨터를 구비한 컴퓨터 시스템을 이용하여 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법에 있어서,

상기 서버 컴퓨터는, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 초기 키 페어 정보 입력 프로그램, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 계정 등록 프로그램, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 계정 동결 요청 정보 입력 프로그램, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 계정 권한 동결 프로그램, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 계정 재등록 프로그램, 상기 초기 키 페어 정보가 저장되는 초기 키 페어 정보 데이터베이스, 상기 계정 동결 요청 정보가 저장되는 계정 동결 요청 정보 데이터베이스, 상기 재등록 정보가 저장되는 재등록 정보 데이터베이스를 포함하고,

(a) 상기 초기 키 페어 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 단계;

(b) 상기 계정 등록 프로그램에 의해서, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 단계;

(c) 상기 계정 동결 요청 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 단계;

(d) 상기 계정 권한 동결 프로그램에 의해서, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 단계; 및

(e) 상기 계정 재등록 프로그램에 의해서, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 단계;

를 포함하고,

상기 초기 키 페어 정보는, 하나의 계정에 1차 내지 N차 키 정보들이 순차적으로 나열되는, 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법.

청구항 7

적어도 하나의 사용자 단말기와 운영자 단말기 및 네트워크를 통하여 연결된 서버 컴퓨터를 구비한 컴퓨터 시스템을 이용하여 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법에 있어서,

상기 서버 컴퓨터는, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 초기 키 페어 정보 입력 프로그램, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 계정 등록 프로그램, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 계정 동결 요청 정보 입력 프로그램, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 계정 권한 동결 프로그램, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 계정 재등록 프로그램, 상기 초기 키 페어 정보가 저장되는 초기 키 페어 정보 데이터베이스, 상기 계정 동결 요청 정보가 저장되는 계정 동결 요청 정보 데이터베이스, 상기 재등록 정보가 저장되는 재등록 정보 데이터베이스를 포함하고,

(a) 상기 초기 키 페어 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 단계;

(b) 상기 계정 등록 프로그램에 의해서, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 단계;

(c) 상기 계정 동결 요청 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 단계;

(d) 상기 계정 권한 동결 프로그램에 의해서, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 단계; 및

(e) 상기 계정 재등록 프로그램에 의해서, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 단계;

를 포함하고,

상기 초기 키 페어 정보는, 하나의 계정에 N개의 키 정보들이 랜덤하게 나열되는, 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법.

청구항 8

적어도 하나의 사용자 단말기와 운영자 단말기 및 네트워크를 통하여 연결된 서버 컴퓨터를 구비한 컴퓨터 시스템을 이용하여 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법에 있어서,

상기 서버 컴퓨터는, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 초기 키 페어 정보 입력 프로그램, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 계정 등록 프로그램, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 계정 동결 요청 정보 입력 프로그램, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 계정 권한 동결 프로그램, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 계정 재등록 프로그램, 상기 초기 키 페어 정보가 저장되는 초기 키 페어 정보 데이터베이스, 상기 계정 동결 요청 정보가 저장되는 계정 동결 요청 정보 데이터베이스, 상기 재등록 정보가 저장되는 재등록 정보 데이터베이스를 포함하고,

(a) 상기 초기 키 페어 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 단계;

(b) 상기 계정 등록 프로그램에 의해서, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 단계;

(c) 상기 계정 동결 요청 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 단계;

(d) 상기 계정 권한 동결 프로그램에 의해서, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 단계; 및

(e) 상기 계정 재등록 프로그램에 의해서, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 단계;

를 포함하고,

상기 서버 컴퓨터는, 상기 재등록 정보를 상기 사용자 단말기로 전송하는 재등록 정보 전송 프로그램을 더 포함하고,

상기 (e) 단계 이후에,

(f) 상기 재등록 정보 전송 프로그램에 의해서, 상기 재등록 정보를 상기 사용자 단말기로 전송하는 단계;

를 더 포함하는, 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법.

청구항 9

제 8 항에 있어서,

상기 서버 컴퓨터는, 상기 사용자 단말기로부터 상기 재등록 정보에 의한 트랜잭션 재신청 정보를 입력받고, 상기 사용자 단말기로 트랜잭션 재승인 정보를 전송하는 트랜잭션 재승인 프로그램, 상기 트랜잭션 재신청 정보가 저장되는 트랜잭션 재신청 정보 데이터베이스, 상기 트랜잭션 재승인 정보가 저장되는 트랜잭션 재승인 정보 데이터베이스를 포함하고,

상기 (f) 단계 이후에,

(g) 상기 트랜잭션 재승인 프로그램에 의해서, 상기 사용자 단말기로부터 상기 재등록 정보에 의한 트랜잭션 재신청 정보를 입력받고, 상기 사용자 단말기로 트랜잭션 재승인 정보를 전송하는 단계;

를 더 포함하는, 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법.

청구항 10

적어도 하나의 사용자 단말기와 운영자 단말기 및 네트워크를 통하여 연결된 서버 컴퓨터를 구비한 컴퓨터 시스템을 이용하여 계정 키 페어 기반 계정 인증 서비스를 운영하는 시스템에 있어서,

상기 서버 컴퓨터는, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 초기 키 페어 정보 입력 프로그램, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 계정 등록 프로그램, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 계정 동결 요청 정보 입력 프로그램, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 계정 권한 동결 프로그램, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 계정 재등록 프로그램, 상기 초기 키 페어 정보가 저장되는 초기 키 페어 정보 데이터베이스, 상기 계정 동결 요청 정보가 저장되는 계정 동결 요청 정보 데이터베이스를 포함하고,

상기 초기 키 페어 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받고, 상기 계정 등록 프로그램에 의해서, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키고, 상기 계정 동결 요청 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받고, 상기 계정 권한 동결 프로그램에 의해서, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하고, 상기 계정 재등록 프로그램에 의해서, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키도록 재등록 정보를 생성하도록 프로그램된 제어부를 포함하고,

상기 초기 키 페어 정보 입력 프로그램은, 상기 사용자 단말기로부터 사용자 인증 신청 정보를 입력받는 인증 신청 정보 입력 프로그램, 상기 사용자 인증 신청 정보를 이용하여 사용자를 인증하고, 인증 증명서 정보를 발급하는 인증 증명서 발급 프로그램, 상기 사용자 단말기로 상기 인증 증명서 정보를 전송하는 인증 증명서 정보 전송 프로그램, 상기 사용자 단말기로부터 블록체인 네트워크를 통해 상기 인증 증명서 정보 및 신규 계정 신청 정보를 입력받는 신규 계정 신청 정보 입력 프로그램, 상기 블록체인 네트워크를 통해 인증서의 정당성을 조회하여 신규 계정 정보를 생성하고, 상기 사용자 단말기로 상기 신규 계정 정보를 전송하는 신규 계정 정보 전송 프로그램, 상기 사용자 단말기로부터 신규 계정 정보 및 이와 매칭된 상기 초기 키 페어 정보를 입력받는 계정 매칭 정보 입력 프로그램, 상기 인증 신청 정보가 저장되는 인증 신청 정보 데이터베이스, 상기 인증 증명서 정보가 저장되는 인증 증명서 정보 데이터베이스, 상기 신규 계정 정보가 저장되는 신규 계정 정보 데이터베이스를 포함하는, 계정 키 페어 기반 계정 인증 서비스를 운영하는 시스템.

청구항 11

적어도 하나의 사용자 단말기와 운영자 단말기 및 네트워크를 통하여 연결된 서버 컴퓨터를 구비한 컴퓨터 시스템을 이용하여 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법을 기록한 컴퓨터로 읽을 수 있는 기록 매체에 있어서,

상기 서버 컴퓨터는, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 초기 키 페어 정보 입력 프로그램, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 계정 등록 프로그램, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 계정 동결 요청 정보 입력 프로그램, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 계정 권한 동결 프로그램, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 계정 재등록 프로그램, 상기 초기 키 페어 정보가 저장되는 초기 키 페어 정보 데이터베이스, 상기 계정 동결 요청 정보가 저장되는 계정 동결 요청 정보 데이터베이스를 포함하고,

(a) 상기 초기 키 페어 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 단계;

(b) 상기 계정 등록 프로그램에 의해서, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 단계;

(c) 상기 계정 동결 요청 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 단계;

(d) 상기 계정 권한 동결 프로그램에 의해서, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 단계; 및

(e) 상기 계정 재등록 프로그램에 의해서, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 단계;

를 포함하고,

상기 초기 키 페어 정보 입력 프로그램은, 상기 사용자 단말기로부터 사용자 인증 신청 정보를 입력받는 인증 신청 정보 입력 프로그램, 상기 사용자 인증 신청 정보를 이용하여 사용자를 인증하고, 인증 증명서 정보를 발급하는 인증 증명서 발급 프로그램, 상기 사용자 단말기로 상기 인증 증명서 정보를 전송하는 인증 증명서 정보 전송 프로그램, 상기 사용자 단말기로부터 블록체인 네트워크를 통해 상기 인증 증명서 정보 및 신규 계정 신청 정보를 입력받는 신규 계정 신청 정보 입력 프로그램, 상기 블록체인 네트워크를 통해 인증서의 정당성을 조회하여 신규 계정 정보를 생성하고, 상기 사용자 단말기로 상기 신규 계정 정보를 전송하는 신규 계정 정보 전송 프로그램, 상기 사용자 단말기로부터 신규 계정 정보 및 이와 매칭된 상기 초기 키 페어 정보를 입력받는 계정 매칭 정보 입력 프로그램, 상기 인증 신청 정보가 저장되는 인증 신청 정보 데이터베이스, 상기 인증 증명서 정보가 저장되는 인증 증명서 정보 데이터베이스, 상기 신규 계정 정보가 저장되는 신규 계정 정보 데이터베이스를 포함하고,

상기 (a) 단계는,

(a-1) 상기 인증 신청 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 사용자 인증 신청 정보를 입력받는 단계;

(a-2) 상기 인증 증명서 발급 프로그램에 의해서, 상기 사용자 인증 신청 정보를 이용하여 사용자를 인증하고, 인증 증명서 정보를 발급하는 단계;

(a-3) 상기 인증 증명서 정보 전송 프로그램에 의해서, 상기 사용자 단말기로 상기 인증 증명서 정보를 전송하는 단계;

(a-4) 상기 신규 계정 신청 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 블록체인 네트워크를 통해 상기 인증 증명서 정보 및 신규 계정 신청 정보를 입력받는 단계;

(a-5) 상기 신규 계정 정보 전송 프로그램에 의해서, 상기 블록체인 네트워크를 통해 인증서의 정당성을 조회하여 신규 계정 정보를 생성하고, 상기 사용자 단말기로 상기 신규 계정 정보를 전송하는 단계; 및

(a-6) 상기 계정 매칭 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 신규 계정 정보 및 이와 매칭된

상기 초기 키 페어 정보를 입력받는 단계;

를 포함하는, 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법을 기록한 컴퓨터로 읽을 수 있는 기록 매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법과 시스템 및 이 방법을 기록한 컴퓨터로 읽을 수 있는 기록 매체에 관한 것으로서, 보다 상세하게는, 계정 데이터가 분리되어 존재하고 또한 하나의 계정이 여러 키(Key Pair/키 페어)들에 의해 종속되어 관리되어 무결성 검증을 가능하게 할 수 있게 하는 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법과 시스템 및 이 방법을 기록한 컴퓨터로 읽을 수 있는 기록 매체에 관한 것이다.

배 경 기 술

[0002] 일반적으로, 통상적인 사용자 인증 시스템들 및 절차들은 사용자의 아이덴티티를 인증하기 위해 패스워드를 사용한다.

[0003] 대다수의 웹 사이트들은 SSL(보안 소켓 레이어) 또는 다른 프로토콜들을 사용하여 인증된다. 상기 SSL은 인터넷을 통해 정보를 안전하게 송신하기 위한 프로토콜이며, 상기 SSL을 사용할 경우, 웹 사이트는 그의 인증서(Certificate)를 통해 인증된다. 그 후, 웹 사이트에 대한 액세스를 추구하는 사용자는 사용자명 및 패스워드에 의해 인증된다.

[0004] 이러한 패스워드들이 사용자들을 인증하기 위해 일반적으로 사용되지만, 패스워드들은 피싱(phishing) 공격, 소셜 엔지니어링 공격, 사전(dictionary) 공격 등과 같은 다양한 공격들에 취약하다.

[0005] 통상적으로, 문자들과 숫자들의 결합을 갖는 더 긴 패스워드들이 더 높은 레벨의 보안을 제공한다. 그러나, 이들 더 긴 패스워드들은 사용자가 기억해내기 더 어렵다. 또한, 패스워드들은, 사용자가 아는 임의의 것을 제공하도록 그 사용자에게 요구함으로써 인증의 단일 팩터를 제공한다. 이러한 팩터는 사용자의 아이덴티티의 임의의 물리적인 인증을 제공하지는 않는다.

[0006] 따라서, 임의의 사람이 사용자의 패스워드 및 사용자명의 정보를 획득하면, 그 사람은 웹기반 계정 및 정보에 액세스할 수 있다. 또한, 사용자의 패스워드의 정보를 갖는 임의의 사람은 사용자의 허가없이 트랜잭션(예를 들어, 구매 트랜잭션 및 금전 이체)를 개시할 수 있다.

[0007] 이러한 패스워드를 사용할 경우 발생하는 또 다른 잠재적인 위협은, "맨 인 더 브라우저(Man in the Browser)" 공격으로서 일반적으로 지칭된다.

[0008] 이들 타입의 공격들은, 사용자가 웹 사이트에 로그인 상태이거나 금융 트랜잭션을 수행하는 동안, 인터넷 브라우저에서 구동하는 악성(malicious) 소프트웨어 애플리케이션들(몰웨어)에 관련된다.

[0009] 이러한 공격의 구현들 중 하나는, 사용자가 그들의 패스워드를 인터넷 브라우저에 제공할 경우 사용자의 패스워드에 액세스하는 것이다. 이러한 포인트 이후, 몰웨어는 사용자의 계정으로 임의의 타입의 악의적인 액션을 수행할 수 있다.

[0010] 따라서, 중요한 금융 동작들을 수행할 경우나 또는 웹 계정에 로그인할 경우 브라우저 사용자 인터페이스를 신뢰할 수 없다는 문제점이 있다.

발명의 내용

해결하려는 과제

[0011] 본 발명은 상기와 같은 문제점을 포함한 여러 문제점들을 해결하기 위한 것으로서, 계정 데이터가 분리되어 존재하며, 하나의 계정이 여러 키들에 의해 종속되어 관리될 수 있게 하는 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법과 시스템 및 이 방법을 기록한 컴퓨터로 읽을 수 있는 기록 매체를 제공하는 것을 목적으로 한다. 그러나 이러한 과제는 예시적인 것으로, 이에 의해 본 발명의 범위가 한정되는 것은 아니다.

과제의 해결 수단

[0012] 상기 과제를 해결하기 위한 본 발명의 사상에 따른 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법은, 적어도 하나의 사용자 단말기와 운영자 단말기 및 네트워크를 통하여 연결된 서버 컴퓨터를 구비한 컴퓨터 시스템을 이용하여 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법에 있어서, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 단계; 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 단계; 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 단계; 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 단계; 및 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 단계;를 포함할 수 있다.

[0013] 한편, 상기 과제를 해결하기 위한 본 발명의 사상에 따른 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법은, 적어도 하나의 사용자 단말기와 운영자 단말기 및 네트워크를 통하여 연결된 서버 컴퓨터를 구비한 컴퓨터 시스템을 이용하여 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법에 있어서, 상기 서버 컴퓨터는, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 초기 키 페어 정보 입력 프로그램, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 계정 등록 프로그램, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 계정 동결 요청 정보 입력 프로그램, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 계정 권한 동결 프로그램, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 계정 재등록 프로그램, 상기 초기 키 페어 정보가 저장되는 초기 키 페어 정보 데이터베이스, 상기 계정 동결 요청 정보가 저장되는 계정 동결 요청 정보 데이터베이스, 상기 재등록 정보가 저장되는 재등록 정보 데이터베이스를 포함하고, (a) 상기 초기 키 페어 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 단계; (b) 상기 계정 등록 프로그램에 의해서, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 단계; (c) 상기 계정 동결 요청 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 단계; (d) 상기 계정 권한 동결 프로그램에 의해서, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 단계; 및 (e) 상기 계정 재등록 프로그램에 의해서, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 단계;를 포함할 수 있다.

[0014] 또한, 본 발명에 따르면, 상기 초기 키 페어 정보 입력 프로그램은, 상기 사용자 단말기로부터 사용자 인증 신청 정보를 입력받는 인증 신청 정보 입력 프로그램, 상기 사용자 인증 신청 정보를 이용하여 사용자를 인증하고, 인증 증명서 정보를 발급하는 인증 증명서 발급 프로그램, 상기 사용자 단말기로 상기 인증 증명서 정보를 전송하는 인증 증명서 정보 전송 프로그램, 상기 사용자 단말기로부터 블록체인 네트워크를 통해 상기 인증 증명서 정보 및 신규 계정 신청 정보를 입력받는 신규 계정 신청 정보 입력 프로그램, 상기 블록체인 네트워크를 통해 인증서의 정당성을 조회하여 신규 계정 정보를 생성하고, 상기 사용자 단말기로 상기 신규 계정 정보를 전송하는 신규 계정 정보 전송 프로그램, 상기 사용자 단말기로부터 신규 계정 정보 및 이와 매칭된 상기 초기 키 페어 정보를 입력받는 계정 매칭 정보 입력 프로그램, 상기 인증 신청 정보가 저장되는 인증 신청 정보 데이터베이스, 상기 인증 증명서 정보가 저장되는 인증 증명서 정보 데이터베이스, 상기 신규 계정 정보가 저장되는 신규 계정 정보 데이터베이스를 포함하고, 상기 (a) 단계는, (a-1) 상기 인증 신청 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 사용자 인증 신청 정보를 입력받는 단계; (a-2) 상기 인증 증명서 발급 프로그램에 의해서, 상기 사용자 인증 신청 정보를 이용하여 사용자를 인증하고, 인증 증명서 정보를 발급하는 단계; (a-3) 상기 인증 증명서 정보 전송 프로그램에 의해서, 상기 사용자 단말기로 상기 인증 증명서 정보를 전송하는 단계; (a-4) 상기 신규 계정 신청 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 블록체인 네트워크를 통해 상기 인증 증명서 정보 및 신규 계정 신청 정보를 입력받는 단계; (a-5) 상기 신규 계정 정보 전송 프로그램에 의해서, 상기 블록체인 네트워크를 통해 인증서의 정당성을 조회하여 신규 계정 정보를 생성하고, 상기 사용자 단말기로 상기 신규 계정 정보를 전송하는 단계; 및 (a-6) 상기 계정 매칭 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 신규 계정 정보 및 이와 매칭된 상기 초기 키 페어 정보를 입력받는 단계;를 포함할 수 있다.

[0015] 또한, 본 발명에 따르면, 상기 계정 권한 동결 프로그램은, 상기 계정 동결 요청 정보의 적절성을 심사하는 계정 동결 적절성 심사 프로그램, 상기 계정 동결 요청 정보가 계정 동결 조건을 충족하면, 상기 제 1 키를 이용한 상기 계정을 동결 조치하는 계정 동결 프로그램, 상기 제 1 키를 이용한 상기 계정의 모든 트랜잭션의 승인

을 거부하는 트랜잭션 거부 프로그램을 포함하고, 상기 (c) 단계는, (c-1) 상기 계정 동결 적절성 심사 프로그램에 의해서, 상기 계정 동결 요청 정보의 적절성을 심사하는 단계; (c-2) 상기 계정 동결 프로그램에 의해서, 상기 계정 동결 요청 정보가 계정 동결 조건을 충족하면, 상기 제 1 키를 이용한 상기 계정을 동결 조치하는 단계; 및 (c-3) 상기 트랜잭션 거부 프로그램에 의해서, 상기 제 1 키를 이용한 상기 계정의 모든 트랜잭션의 승인을 거부하는 단계;를 포함할 수 있다.

[0016] 또한, 본 발명에 따르면, 상기 계정 재등록 프로그램은, 상기 사용자 단말기로부터 사용자 인증 재신청 정보를 입력받는 인증 재신청 정보 입력 프로그램, 상기 사용자 인증 재신청 정보를 이용하여 사용자를 재인증하고, 재인증 증명서 정보를 발급하는 인증 증명서 재발급 프로그램, 상기 사용자 단말기로 상기 재인증 증명서 정보를 전송하는 인증 증명서 정보 재전송 프로그램, 상기 사용자 단말기로부터 블록체인 네트워크를 통해 상기 재인증 증명서 정보를 입력받는 재신청 정보 입력 프로그램, 상기 블록체인 네트워크를 통해 인증서의 정당성을 조회하는 인증서 재조회 프로그램, 사용자의 재등록 정보를 바탕으로 재등록이 인정되는 계정 재등록 인정 프로그램을 포함하고, 상기 (e) 단계는, (e-1) 상기 인증 재신청 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 사용자 인증 재신청 정보를 입력받는 단계; (e-2) 상기 인증 증명서 재발급 프로그램에 의해서, 상기 사용자 인증 재신청 정보를 이용하여 사용자를 재인증하고, 재인증 증명서 정보를 발급하는 단계; (e-3) 상기 인증 증명서 정보 재전송 프로그램에 의해서, 상기 사용자 단말기로 상기 재인증 증명서 정보를 전송하는 단계; (e-4) 상기 재신청 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 블록체인 네트워크를 통해 상기 재인증 증명서 정보를 입력받는 단계; (e-5) 상기 인증서 재조회 프로그램에 의해서, 상기 블록체인 네트워크를 통해 인증서의 정당성을 조회하는 단계; 및 (e-6) 상기 계정 재등록 인정 프로그램에 의해서, 사용자의 재등록 정보를 바탕으로 재등록이 인정되는 단계;를 포함할 수 있다.

[0017] 또한, 본 발명에 따르면, 상기 초기 키 페어 정보는, 하나의 계정에 1차 내지 N차 키 정보들이 순차적으로 나열될 수 있다.

[0018] 또한, 본 발명에 따르면, 상기 초기 키 페어 정보는, 하나의 계정에 N개의 키 정보들이 랜덤하게 나열될 수 있다.

[0019] 또한, 본 발명에 따르면, 상기 서버 컴퓨터는, 상기 재등록 정보를 상기 사용자 단말기로 전송하는 재등록 정보 전송 프로그램을 더 포함하고, 상기 (e) 단계 이후에, (f) 상기 재등록 정보 전송 프로그램에 의해서, 상기 재등록 정보를 상기 사용자 단말기로 전송하는 단계;를 더 포함할 수 있다.

[0020] 또한, 본 발명에 따르면, 상기 서버 컴퓨터는, 상기 사용자 단말기로부터 상기 재등록 정보에 의한 트랜잭션 재신청 정보를 입력받고, 상기 사용자 단말기로 트랜잭션 재승인 정보를 전송하는 트랜잭션 재승인 프로그램, 상기 트랜잭션 재신청 정보가 저장되는 트랜잭션 재신청 정보 데이터베이스, 상기 트랜잭션 재승인 정보가 저장되는 트랜잭션 재승인 정보 데이터베이스를 포함하고, 상기 (f) 단계 이후에, (g) 상기 트랜잭션 재승인 프로그램에 의해서, 상기 사용자 단말기로부터 상기 재등록 정보에 의한 트랜잭션 재신청 정보를 입력받고, 상기 사용자 단말기로 트랜잭션 재승인 정보를 전송하는 단계;를 더 포함할 수 있다.

[0021] 한편, 상기 과제를 해결하기 위한 본 발명의 사상에 따른 계정 키 페어 기반 계정 인증 서비스를 운영하는 시스템은, 적어도 하나의 사용자 단말기와 운영자 단말기 및 네트워크를 통하여 연결된 서버 컴퓨터를 구비한 컴퓨터 시스템을 이용하여 계정 키 페어 기반 계정 인증 서비스를 운영하는 시스템에 있어서, 상기 서버 컴퓨터는, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 초기 키 페어 정보 입력 프로그램, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 계정 등록 프로그램, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 계정 동결 요청 정보 입력 프로그램, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 계정 권한 동결 프로그램, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 계정 재등록 프로그램, 상기 초기 키 페어 정보가 저장되는 초기 키 페어 정보 데이터베이스, 상기 계정 동결 요청 정보가 저장되는 계정 동결 요청 정보 데이터베이스를 포함하고, 상기 초기 키 페어 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받고, 상기 계정 등록 프로그램에 의해서, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키고, 상기 계정 동결 요청 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받고, 상기 계정 권한 동결 프로그램에 의해서, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하고, 상기 계정 재등록 프로그램에 의해서, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키도록 재등록 정보를 생성하도록 프

로그램된 제어부를 포함할 수 있다.

[0022] 한편, 상기 과제를 해결하기 위한 본 발명의 사상에 따른 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법을 기록한 컴퓨터로 읽을 수 있는 기록 매체는, 적어도 하나의 사용자 단말기와 운영자 단말기 및 네트워크를 통하여 연결된 서버 컴퓨터를 구비한 컴퓨터 시스템을 이용하여 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법을 기록한 컴퓨터로 읽을 수 있는 기록 매체에 있어서, 상기 서버 컴퓨터는, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 초기 키 페어 정보 입력 프로그램, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 계정 등록 프로그램, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 계정 동결 요청 정보 입력 프로그램, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 계정 권한 동결 프로그램, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 계정 재등록 프로그램, 상기 초기 키 페어 정보가 저장되는 초기 키 페어 정보 데이터베이스, 상기 계정 동결 요청 정보가 저장되는 계정 동결 요청 정보 데이터베이스를 포함하고, (a) 상기 초기 키 페어 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 단계; (b) 상기 계정 등록 프로그램에 의해서, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 단계; (c) 상기 계정 동결 요청 정보 입력 프로그램에 의해서, 상기 사용자 단말기로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 단계; (d) 상기 계정 권한 동결 프로그램에 의해서, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 단계; 및 (e) 상기 계정 재등록 프로그램에 의해서, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 단계;를 포함할 수 있다.

발명의 효과

[0023] 상기한 바와 같이 이루어진 본 발명의 여러 실시예들에 따르면, 계정 데이터가 분리되어 존재하며, 하나의 계정이 여러 키들에 의해 종속되어 관리됨으로써, 블록체인에서 필수적인 무결성 검증을 가능하게 하고, 이를 통해서, 운영자는 사용자에게 단일 계정만 제공할 수 있어서 계정 사용의 편의성과, 거래의 무결성을 입증할 수 있고, 금융 사고를 사전에 방지할 수 있으며, 사용자는 운영자에게 이에 대한 대가로 각종 등록비, 수수료, 거래대금, 신용 정보 등을 제공할 수 있어서 모두에 이익이 될 수 있는 비즈니스 모델을 제공할 수 있는 효과를 갖는 것이다. 물론 이러한 효과에 의해 본 발명의 범위가 한정되는 것은 아니다.

도면의 간단한 설명

[0024] 도 1은 본 발명의 일부 실시예들에 따른 계정 키 페어 기반 계정 인증 서비스를 운영하는 시스템을 나타내는 개념도이다.

도 2는 도 1의 계정 키 페어 기반 계정 인증 서비스를 운영하는 시스템의 초기 키 페어 정보 입력 프로그램을 보다 상세하게 나타내는 블록도이다.

도 3은 도 1의 계정 키 페어 기반 계정 인증 서비스를 운영하는 시스템의 계정 권한 동결 프로그램을 보다 상세하게 나타내는 블록도이다.

도 4는 도 1의 계정 키 페어 기반 계정 인증 서비스를 운영하는 시스템의 계정 재등록 프로그램을 보다 상세하게 나타내는 블록도이다.

도 5는 본 발명의 계정 키 페어 기반 계정 인증 서비스를 운영하는 시스템을 운영하는 운영자와 사용자 간의 관계를 나타내는 개념도이다.

도 6은 본 발명의 일부 실시예들에 따른 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법을 나타내는 순서도이다.

도 7a, 도 7b는 본 발명의 일부 다른 실시예들에 따른 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법을 나타내는 순서도이다.

도 8은 본 발명의 계정 키 페어 기반 계정 인증 서비스를 운영하는 시스템의 연속적 데이터 무결성 입증 과정을 나타내는 참고도이다.

도 9는 도 8의 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법에 따른 신규 계정을 생성하는 과정을 나타

내는 참고도이다.

도 10은 도 8의 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법에 따른 도난 신고 및 긴급 권한 동결 과정을 나타내는 참고도이다.

도 11은 도 8의 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법에 따른 키 페어 재등록 과정을 나타내는 참고도이다.

발명을 실시하기 위한 구체적인 내용

[0025] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 여러 실시예들을 상세히 설명하기로 한다.

[0026] 본 발명의 실시예들은 당해 기술 분야에서 통상의 지식을 가진 자에게 본 발명을 더욱 완전하게 설명하기 위하여 제공되는 것이며, 하기 실시예는 여러 가지 다른 형태로 변형될 수 있으며, 본 발명의 범위가 하기 실시예에 한정되는 것은 아니다. 오히려 이들 실시예들은 본 개시를 더욱 충실하고 완전하게 하고, 당업자에게 본 발명의 사상을 완전하게 전달하기 위하여 제공되는 것이다. 또한, 도면에서 각 층의 두께나 크기는 설명의 편의 및 명확성을 위하여 과장된 것이다.

[0027] 본 명세서에서 사용된 용어는 특정 실시예를 설명하기 위하여 사용되며, 본 발명을 제한하기 위한 것이 아니다. 본 명세서에서 사용된 바와 같이, 단수 형태는 문맥상 다른 경우를 분명히 지적하는 것이 아니라면, 복수의 형태를 포함할 수 있다. 또한, 본 명세서에서 사용되는 경우 "포함한다(comprise)" 및/또는 "포함하는(comprising)"은 언급한 형상들, 숫자, 단계, 동작, 부재, 요소 및/또는 이들 그룹의 존재를 특정하는 것이며, 하나 이상의 다른 형상, 숫자, 동작, 부재, 요소 및/또는 그룹들의 존재 또는 부가를 배제하는 것이 아니다.

[0028] 이하, 본 발명의 실시예들은 본 발명의 이상적인 실시예들을 개략적으로 도시하는 도면들을 참조하여 설명한다. 도면들에 있어서, 예를 들면, 제조 기술 및/또는 공차(tolerance)에 따라, 도시된 형상의 변형들이 예상될 수 있다. 따라서, 본 발명 사상의 실시예는 본 명세서에 도시된 영역의 특정 형상에 제한된 것으로 해석되어서는 아니 되며, 예를 들면 제조상 초래되는 형상의 변화를 포함하여야 한다.

[0029] 이하, 본 발명의 일부 실시예들에 따른 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법과 시스템 및 이 방법을 기록한 컴퓨터로 읽을 수 있는 기록 매체를 도면을 참조하여 상세히 설명한다.

[0030] 도 1은 본 발명의 일부 실시예들에 따른 계정 키 페어 기반 계정 인증 서비스를 운영하는 시스템을 나타내는 개념도이다.

[0031] 먼저, 도 1에 도시된 바와 같이, 본 발명의 일부 실시예들에 따른 계정 키 페어 기반 계정 인증 서비스를 운영하는 시스템은, 크게 사용자 단말기(10)와, 운영자 단말기(90) 및 네트워크(50)를 통하여 연결된 서버 컴퓨터(60)를 포함하여 이루어질 수 있다.

[0032] 여기서, 상기 서버 컴퓨터(60)는, 상기 사용자 단말기(10)로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받고, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키고, 상기 사용자 단말기(10)로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받고, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하고, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하도록 프로그램된 것으로서, 상기 네트워크(50) 또는 블록체인 네트워크를 통해 계정 키 페어 기반 계정 인증 서비스를 운영할 수 있는 데이터 센서나, 기업이나, 단체나, 공장이나, 사업체나, 본사나, 지사나, 영업소나, 대리점 등에 구비된 컴퓨터일 수 있다.

[0033] 또한, 예컨대, 상기 사용자 단말기(10)는, 블록체인 기술을 이용하여 각종 거래나, 채굴이나, 정보 전송이나, 금융 서비스 등 각종 서비스를 수행할 수 있는 각종 컴퓨터 또는 서버 컴퓨터 등을 포함할 수 있다.

[0034] 여기서, 이러한 상기 사용자 단말기(10)는 반드시 컴퓨터에만 국한되지 않고, 각종 정보를 처리할 수 있는 모든 정보 단말 장치들이 적용될 수 있다. 예컨대, 각종 스마트 폰은 물론이고, 각종 웨어러블 디바이스나, 스마트 센서나, 스마트 패드나, 스마트 워치나, 모바일 단말기, PDA, 노트북, 랩탑 컴퓨터, 스마트 카메라, 스마트 캠코더, 전자책, 스마트 스캐너 등이 모두 적용될 수 있다.

[0035] 또한, 예컨대, 상기 운영자 단말기(90)는, 상기 서버 컴퓨터(60)를 관리하고 운영하는 데이터 센터나, 개인이나, 단체나, 기업이나, 공장이나, 사업체나, 중앙 관재소나, 본사나, 지사나, 영업소나 전산 담당자의 단말기나 컴퓨터로서, 반드시 컴퓨터나 스마트 폰에 국한되지 않는 것으로 각종 문자 정보나, 숫자 정보나 이미지 정보를 제공받을 수 있고, 다양한 명령을 선택할 수 있는 각종 정보 단말기, PDA, 스마트 워치, 스마트 패드,

카메라, 캠코더, 노트북, 랩탑 컴퓨터, 전자책, 개인용 컴퓨터, 다른 서버 컴퓨터 등이 모두 적용될 수 있다.

[0036] 한편, 도 1에 도시된 바와 같이, 상기 사용자 단말기(10)와 상기 운영자 단말기(90)는 반드시 독립적으로 구비되지 않는 것으로서, 예컨대, 상기 사용자 단말기(10)와 상기 운영자 단말기(90)가 동일한 경우도 있을 수 있다.

[0037] 또한, 예컨대, 도 1의 상기 사용자 단말기(10)와, 상기 운영자 단말기(90) 및 서버 컴퓨터(60)는 각종 어플리케이션, 앱, 하이브리드 앱, 프로그램 등이 설치되어, 상기 네트워크(50)를 통해 서로 연결되고, 이러한 상기 네트워크(50)에 의해 연결된 단말기들은, 기존의 2G, 3G, 4G, 5G, LTE 등 이동 통신망, WIFI 통신망, 블루투스 통신망, 셀룰러 통신망, CDMA 통신망, LTE 통신망, 이더넷 통신망, 와이맥스 통신망, 근거리 통신망(LAN), 광역 통신망(WAN), RF 통신망, 적외선 통신망, 광 통신망 등의 통신망을 이용할 수 있는 것은 물론이고, HTML, XML, HTML5 등의 형태로 웹 내용을 디스플레이할 수 있는 인터넷 브라우저(Netscape, Internet Explorer 등)나 사내 또는 사외 또는 근거리/원거리 유무선 네트워크 접속용 프로토콜 장치 등을 가질 수 있다.

[0038] 한편, 상기 서버 컴퓨터(60)는, 도 1에 도시된 바와 같이, 프로그램을 제어하는 프로그램 제어부(PG)와 각종 정보들을 저장하는 데이터베이스(DB)를 포함할 수 있다.

[0039] 특히, 상기 프로그램 제어부(PG)는, 도 1에 도시된 바와 같이, 전체 프로그램을 운영하는 메인 프로그램(61), 상기 사용자 단말기(10)나 상기 운영자 단말기(90)로부터 등록 신청 정보를 입력받아 사용자로 등록하는 사용자 등록 프로그램(62), 상기 사용자 단말기(10)나 상기 운영자 단말기(90)로부터 로그인 정보를 입력받는 로그인 프로그램(63), 상기 사용자 단말기(10)로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 초기 키 페어 정보 입력 프로그램(64), 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 계정 등록 프로그램(65), 상기 사용자 단말기(10)로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 계정 동결 요청 정보 입력 프로그램(66), 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 계정 권한 동결 프로그램(67), 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 계정 재등록 프로그램(68), 상기 재등록 정보를 상기 사용자 단말기(10)로 전송하는 재등록 정보 전송 프로그램(69), 상기 사용자 단말기(10)로부터 상기 재등록 정보에 의한 트랜잭션 재신청 정보를 입력받고, 상기 사용자 단말기(10)로 트랜잭션 재승인 정보를 전송하는 트랜잭션 재승인 프로그램(70), 기타 각종 그래픽이나 결재나 게시판 등의 기능을 수행하는 기타 프로그램(71) 등을 포함할 수 있다.

[0040] 여기서, 예컨대, 상기 메인 프로그램(61)은 전체 프로그램을 운영하는 것으로서, 온라인 상에서 데이터 관리 홈페이지나 어플리케이션이나 프로그램의 메인 화면 형태로 표현되는 것이 가능하고, 상기 사용자 단말기(10)나 상기 운영자 단말기(90)로부터 각종 정보와 명령 신호를 전송받아 상기 모든 프로그램들을 제어할 수 있는 프로그램일 수 있다.

[0041] 또한, 예컨대, 상기 사용자 등록 프로그램(62)은, 상기 사용자 단말기(10) 또는 상기 운영자 단말기(90)로부터 등록 신청 정보를 입력받아 회원으로 등록하는 프로그램으로서, 사용자 등록 정보를 저장할 수 있도록 상기 사용자 단말기(10)를 인증할 수 있는 프로그램일 수 있다.

[0042] 이외에도, 상기 사용자 등록 프로그램(62)은, 상기 사용자 단말기(10)나 상기 운영자 단말기(90)로부터 고유 정보를 입력받아 표준 약관이나 정보 수집 및 이용에 대한 약관 등에 동의하게 할 수 있고, 실명 확인이나 공공 아이핀이나 아이디나 패스워드나 이메일이나 휴대전화나 주소나 개인 정보, 환자 정보, 주민 번호 정보, 고유 번호, 유심 카드에 저장된 전화 번호 등으로 등록할 수 있는 프로그램일 수 있다.

[0043] 또한, 예컨대, 상기 로그인 프로그램(63)은, 상기 사용자 단말기(10)로부터 로그인 정보를 입력받아서 로그인 과정을 수행 할 수 있는 프로그램으로서, 사용자는 상기 서버 컴퓨터(60)에 접속한 후, 아이디나 패스워드나 전화 번호를 자동 또는 수동으로 입력하여 로그인할 수 있도록 상기 사용자 단말기(10)로부터 로그인 정보를 입력받을 수 있는 프로그램일 수 있다.

[0044] 또한, 예컨대, 도 1에 도시된 바와 같이, 상기 초기 키 페어 정보 입력 프로그램(64)은, 상기 사용자 단말기(10)로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 프로그램으로서, 여기서, 상기 초기 키 페어 정보는, 하나의 계정에 1차 내지 N차 키 정보들이 순차적으로 나열될 수 있다.

[0045] 이러한, 상기 초기 키 페어가 순차적으로 나열되는 경우에는, 재등록시 상기 계정 정보와 상기 키 정보가 순차적으로 매칭될 수 있는 것으로서, 사용자의 재등록시 반드시 순서에 맞추어서 재등록이 이루어져야 한다. 여기

서, 이러한 순서는 나열된 차례에 따라서도 가능하고 별도의 암호화된 순서 기준이 설정되는 것도 가능하다.

[0046] 따라서, 하나의 계정에 순서에 따라 N개의 키 정보들이 예정되어 있으므로, 상기 계정은 각종 해킹이나 도난 등의 사고에서도 신속하게 재등록이 가능하여 연속성과 무결성을 유지할 수 있다.

[0047] 이외에도, 상기 초기 키 페어 정보는, 하나의 계정에 N개의 키 정보들이 랜덤하게 나열되는 것도 가능하다.

[0048] 이 경우에는, 순서에 상관없이 사용자의 재등록시 키 정보가 초기 키 페어 중에 포함되어 있기만 한다면 재등록이 가능하게 할 수도 있다.

[0049] 또한, 예컨대, 도 1에 도시된 바와 같이, 상기 계정 등록 프로그램(65)은, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 프로그램으로서, 상기 제 1 키는 상기 키 페어 정보들 중에서 첫 번째인 것이 가능하다. 그러나, 이에 반드시 국한되지 않고, 랜덤하게 상기 키 페어 정보들 중에 포함되어 있기만 한다면 등록될 수도 있다.

[0050] 또한, 예컨대, 도 1에 도시된 바와 같이, 상기 계정 동결 요청 정보 입력 프로그램(66)은, 상기 사용자 단말기(10)로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 프로그램으로서, 상기 사용자의 신고에 의해서 이루어지거나, 또는 상기 계정으로 잘못된 키 정보가 수 차례 이상 입력되면 자동으로 계정 동결 요청 정보를 입력받을 수도 있다.

[0051] 또한, 예컨대, 도 1에 도시된 바와 같이, 상기 계정 권한 동결 프로그램(67)은, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 프로그램으로서, 상기 제 1 키를 이용하여 어떠한 트랜젝션 요청도 모두 거절될 수 있게 하는 프로그램일 수 있다.

[0052] 또한, 예컨대, 상기 계정 재등록 프로그램(68)은, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 프로그램으로서, 예컨대, 상기 제 2 키는 상기 키 페어 정보들 중에서 두 번째인 것이 가능하다. 그러나, 이에 반드시 국한되지 않고, 랜덤하게 상기 키 페어 정보들 중에 포함되어 있기만 한다면 등록될 수도 있다.

[0053] 또한, 예컨대, 도 1에 도시된 바와 같이, 상기 재등록 정보 전송 프로그램(69)은, 상기 재등록 정보를 상기 사용자 단말기(10)로 전송하는 프로그램으로서, 이를 통해서 사용자는 기존의 계정을 새로운 키 정보로 그대로 사용할 수 있음을 알 수 있다.

[0054] 또한, 예컨대, 상기 트랜잭션 재승인 프로그램(70)은, 상기 사용자 단말기(10)로부터 상기 재등록 정보에 의한 트랜잭션 재신청 정보를 입력받고, 상기 사용자 단말기(10)로 트랜잭션 재승인 정보를 전송하는 프로그램으로서, 사용자는 하나의 계정으로 이후 새로운 키 정보를 이용하여 트랜잭션을 재신청할 수 있다.

[0055] 여기서, 상술된 프로그램들은 상기 사용자 단말기(10)나, 상기 운영자 단말기(90)에 다운로드되거나 인스톨된 실행 프로그램이나, 화면 제어 프로그램이나 사용자 어플리케이션과 연동되는 형태로 운영될 수 있다.

[0056] 그러나, 상술된 프로그램들은 반드시 실행 프로그램이나 스마트 폰 어플리케이션과 연동되는 것에 국한되지 않고, 모든 다양한 형태의 단말기와 연동될 수 있다.

[0057] 한편, 도 1에 도시된 바와 같이, 상기 데이터베이스(DB)는, 상기 사용자 등록 정보가 저장되는 사용자 등록 정보 데이터베이스(73), 상기 로그인 정보가 저장되는 로그인 정보 데이터베이스(74), 상기 초기 키 페어 정보가 저장되는 초기 키 페어 정보 데이터베이스(75), 상기 계정 동결 요청 정보가 저장되는 계정 동결 요청 정보 데이터베이스(76), 상기 재등록 정보가 저장되는 재등록 정보 데이터베이스(77), 상기 인증 신청 정보가 저장되는 인증 신청 정보 데이터베이스(78), 상기 인증 증명서 정보가 저장되는 인증 증명서 정보 데이터베이스(79), 상기 신규 계정 정보가 저장되는 신규 계정 정보 데이터베이스(80), 상기 트랜잭션 재신청 정보가 저장되는 트랜잭션 재신청 정보 데이터베이스(81), 상기 트랜잭션 재승인 정보가 저장되는 트랜잭션 재승인 정보 데이터베이스(82), 기타 데이터 관리 홈페이지나 각종 광고나 홍보나 결재나 게시판 등의 정보가 저장되는 기타 정보 데이터베이스(83) 등을 포함할 수 있다.

[0058] 따라서, 상기 서버 컴퓨터(60)는, 상기 초기 키 페어 정보 입력 프로그램(64)에 의해서, 상기 사용자 단말기(10)로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받고, 상기 계정 등록 프로그램(65)에 의해서, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키고, 상기 계정 동결 요청 정보 입력 프로그램(66)에 의해서, 상기 사용자 단말기(10)로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받고, 상기 계정 권한 동결 프로그램(67)에 의해서, 상기 제 1 키를 이용한

상기 계정의 권한을 동결하고, 상기 계정 재등록 프로그램(68)에 의해서, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 계정 키 페어 기반 계정 인증 서비스를 수행할 수 있다.

[0059] 도 2는 도 1의 계정 키 페어 기반 계정 인증 서비스를 운영하는 시스템의 초기 키 페어 정보 입력 프로그램(64)을 보다 상세하게 나타내는 블록도이다.

[0060] 더욱 구체적으로 예를 들면, 도 2에 도시된 바와 같이, 상기 초기 키 페어 정보 입력 프로그램(64)은, 상기 사용자 단말기(10)로부터 사용자 인증 신청 정보를 입력받는 인증 신청 정보 입력 프로그램(64-1), 상기 사용자 인증 신청 정보를 이용하여 사용자를 인증하고, 인증 증명서 정보를 발급하는 인증 증명서 발급 프로그램(64-2), 상기 사용자 단말기(10)로 상기 인증 증명서 정보를 전송하는 인증 증명서 정보 전송 프로그램(64-3), 상기 사용자 단말기(10)로부터 블록체인 네트워크를 통해 상기 인증 증명서 정보 및 신규 계정 신청 정보를 입력받는 신규 계정 신청 정보 입력 프로그램(64-4), 상기 블록체인 네트워크를 통해 인증서의 정당성을 조회하여 신규 계정 정보를 생성하고, 상기 사용자 단말기(10)로 상기 신규 계정 정보를 전송하는 신규 계정 정보 전송 프로그램(64-5), 상기 사용자 단말기(10)로부터 신규 계정 정보 및 이와 매칭된 상기 초기 키 페어 정보를 입력받는 계정 매칭 정보 입력 프로그램(64-6)를 포함할 수 있다.

[0061] 따라서, 상기 초기 키 페어 정보 입력 프로그램(64)을 이용하여, 상기 사용자 단말기(10)로부터 사용자 인증 신청 정보를 입력받고, 상기 사용자 인증 신청 정보를 이용하여 사용자를 인증하고, 인증 증명서 정보를 발급하고, 상기 사용자 단말기(10)로 상기 인증 증명서 정보를 전송하고, 상기 사용자 단말기(10)로부터 블록체인 네트워크를 통해 상기 인증 증명서 정보 및 신규 계정 신청 정보를 입력받고, 상기 블록체인 네트워크를 통해 인증서의 정당성을 조회하여 신규 계정 정보를 생성하고, 상기 사용자 단말기(10)로 상기 신규 계정 정보를 전송하고, 상기 사용자 단말기(10)로부터 신규 계정 정보 및 이와 매칭된 상기 초기 키 페어 정보를 입력받을 수 있다.

[0062] 도 3은 도 1의 계정 키 페어 기반 계정 인증 서비스를 운영하는 시스템의 계정 권한 동결 프로그램(67)을 보다 상세하게 나타내는 블록도이다.

[0063] 더욱 구체적으로 예를 들면, 상기 계정 권한 동결 프로그램(67)은, 상기 계정 동결 요청 정보의 적절성을 심사하는 계정 동결 적절성 심사 프로그램(67-1), 상기 계정 동결 요청 정보가 계정 동결 조건을 충족하면, 상기 제 1 키를 이용한 상기 계정을 동결 조치하는 계정 동결 프로그램(67-2), 상기 제 1 키를 이용한 상기 계정의 모든 트랜잭션의 승인을 거부하는 트랜잭션 거부 프로그램(67-3)을 포함할 수 있다.

[0064] 따라서, 상기 계정 권한 동결 프로그램(67)을 이용하여 상기 계정 동결 요청 정보의 적절성을 심사하고, 상기 계정 동결 요청 정보가 계정 동결 조건을 충족하면, 상기 제 1 키를 이용한 상기 계정을 동결 조치하고, 상기 제 1 키를 이용한 상기 계정의 모든 트랜잭션의 승인을 거부할 수 있다.

[0065] 도 4는 도 1의 계정 키 페어 기반 계정 인증 서비스를 운영하는 시스템의 계정 재등록 프로그램(68)을 보다 상세하게 나타내는 블록도이다.

[0066] 더욱 구체적으로 예를 들면, 상기 계정 재등록 프로그램(68)은, 상기 사용자 단말기(10)로부터 사용자 인증 재신청 정보를 입력받는 인증 재신청 정보 입력 프로그램(68-1), 상기 사용자 인증 재신청 정보를 이용하여 사용자를 재인증하고, 재인증 증명서 정보를 발급하는 인증 증명서 재발급 프로그램(68-2), 상기 사용자 단말기(10)로 상기 재인증 증명서 정보를 전송하는 인증 증명서 정보 재전송 프로그램(68-3), 상기 사용자 단말기(10)로부터 블록체인 네트워크를 통해 상기 재인증 증명서 정보를 입력받는 재신청 정보 입력 프로그램(68-4), 상기 블록체인 네트워크를 통해 인증서의 정당성을 조회하는 인증서 재조회 프로그램(68-5), 사용자의 재등록 정보를 바탕으로 재등록이 인정되는 계정 재등록 인정 프로그램(68-6)을 포함할 수 있다.

[0067] 따라서, 상기 계정 재등록 프로그램(68)을 이용하여, 상기 사용자 단말기(10)로부터 사용자 인증 재신청 정보를 입력받고, 상기 사용자 인증 재신청 정보를 이용하여 사용자를 재인증하고, 재인증 증명서 정보를 발급하고, 상기 사용자 단말기(10)로 상기 재인증 증명서 정보를 전송하고, 상기 사용자 단말기(10)로부터 블록체인 네트워크를 통해 상기 재인증 증명서 정보를 입력받고, 상기 블록체인 네트워크를 통해 인증서의 정당성을 조회하고, 사용자의 재등록 정보를 바탕으로 재등록이 인정될 수 있다.

[0068] 도 5는 본 발명의 계정 키 페어 기반 계정 인증 서비스를 운영하는 시스템을 운영하는 운영자와 사용자 간의 관계를 나타내는 개념도이다.

[0069] 그러므로, 도 5에 도시된 바와 같이, 본 발명에 따르면, 계정 데이터가 분리되어 존재하며, 하나의 계정이 여러 키들에 의해 종속되어 관리됨으로써, 블록체인에서 필수적인 무결성 검증을 가능하게 하고, 이를 통해서, 운영자는 사용자에게 단일 계정만 제공할 수 있어서 계정 사용의 편의성과, 거래의 무결성을 입증할 수 있고, 금융 사고를 사전에 방지할 수 있으며, 사용자는 운영자에게 이에 대한 대가로 각종 등록비, 수수료, 거래 대금, 신용 정보 등을 제공할 수 있어서 모두에 이익이 될 수 있는 비즈니스 모델을 제공할 수 있다.

[0070] 도 6은 본 발명의 일부 실시예들에 따른 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법을 나타내는 순서도이다.

[0071] 한편, 도 1 내지 도 6에 도시된 바와 같이, 본 발명의 일부 실시예들에 따른 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법을 순서적으로 나타내면, 본 발명의 일부 실시예들에 따른 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법은, 먼저, 계정 키 페어 기반 계정 인증 서비스를 제공할 수 있는 서버 컴퓨터(60)를 구성하고, (a) 상기 초기 키 페어 정보 입력 프로그램(64)에 의해서, 상기 사용자 단말기(10)로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 단계; (b) 상기 계정 등록 프로그램(65)에 의해서, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 단계; (c) 상기 계정 동결 요청 정보 입력 프로그램(66)에 의해서, 상기 사용자 단말기(10)로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 단계; (d) 상기 계정 권한 동결 프로그램(67)에 의해서, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 단계; 및 (e) 상기 계정 재등록 프로그램(68)에 의해서, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 단계;를 포함할 수 있다.

[0072] 그러나, 이러한 본 발명은 반드시 도면에만 국한되지 않고, 이외에도 다양한 단계들이 추가로 포함될 수 있다.

[0073] 도 7a, 7b는 본 발명의 일부 다른 실시예들에 따른 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법을 나타내는 순서도이다.

[0074] 한편, 도 1 내지 도 7에 도시된 바와 같이, 본 발명의 일부 다른 실시예들에 따른 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법을 순서적으로 나타내면, 본 발명의 일부 다른 실시예들에 따른 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법은, 먼저, 계정 키 페어 기반 계정 인증 서비스를 제공할 수 있는 서버 컴퓨터(60)를 구성하고, (a) 상기 초기 키 페어 정보 입력 프로그램(64)에 의해서, 상기 사용자 단말기(10)로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받는 단계; (b) 상기 계정 등록 프로그램(65)에 의해서, 상기 계정에 상기 키 페어 정보들 중 제 1 키를 매칭시켜서 등록시키는 단계; (c) 상기 계정 동결 요청 정보 입력 프로그램(66)에 의해서, 상기 사용자 단말기(10)로부터 상기 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받는 단계; (d) 상기 계정 권한 동결 프로그램(67)에 의해서, 상기 제 1 키를 이용한 상기 계정의 권한을 동결하는 단계; (e) 상기 계정 재등록 프로그램(68)에 의해서, 상기 계정에 상기 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성하는 단계; (f) 상기 재등록 정보 전송 프로그램(69)에 의해서, 상기 재등록 정보를 상기 사용자 단말기(10)로 전송하는 단계; 및 (g) 상기 트랜잭션 재승인 프로그램(70)에 의해서, 상기 사용자 단말기(10)로부터 상기 재등록 정보에 의한 트랜잭션 재신청 정보를 입력받고, 상기 사용자 단말기(10)로 트랜잭션 재승인 정보를 전송하는 단계;를 포함할 수 있다.

[0075] 여기서, 상기 (a) 단계는, (a-1) 상기 인증 신청 정보 입력 프로그램(64-1)에 의해서, 상기 사용자 단말기(10)로부터 사용자 인증 신청 정보를 입력받는 단계; (a-2) 상기 인증 증명서 발급 프로그램(64-2)에 의해서, 상기 사용자 인증 신청 정보를 이용하여 사용자를 인증하고, 인증 증명서 정보를 발급하는 단계; (a-3) 상기 인증 증명서 정보 전송 프로그램(64-3)에 의해서, 상기 사용자 단말기(10)로 상기 인증 증명서 정보를 전송하는 단계; (a-4) 상기 신규 계정 신청 정보 입력 프로그램(64-4)에 의해서, 상기 사용자 단말기(10)로부터 블록체인 네트워크를 통해 상기 인증 증명서 정보 및 신규 계정 신청 정보를 입력받는 단계; (a-5) 상기 신규 계정 정보 전송 프로그램(64-5)에 의해서, 상기 블록체인 네트워크를 통해 인증서의 정당성을 조회하여 신규 계정 정보를 생성하고, 상기 사용자 단말기(10)로 상기 신규 계정 정보를 전송하는 단계; 및 (a-6) 상기 계정 매칭 정보 입력 프로그램(64-6)에 의해서, 상기 사용자 단말기(10)로부터 신규 계정 정보 및 이와 매칭된 상기 초기 키 페어 정보를 입력받는 단계;를 포함할 수 있다.

[0076] 또한, 상기 (c) 단계는, (c-1) 상기 계정 동결 적절성 심사 프로그램(66-1)에 의해서, 상기 계정 동결 요청 정보의 적절성을 심사하는 단계; (c-2) 상기 계정 동결 프로그램(66-2)에 의해서, 상기 계정 동결 요청 정보가 계정 동결 조건을 충족하면, 상기 제 1 키를 이용한 상기 계정을 동결 조치하는 단계; 및 (c-3) 상기 트랜잭션 거

부 프로그램(66-3)에 의해서, 상기 제 1 키를 이용한 상기 계정의 모든 트랜잭션의 승인을 거부하는 단계;를 포함할 수 있다.

[0077] 또한, 상기 (e) 단계는, (e-1) 상기 인증 재신청 정보 입력 프로그램(68-1)에 의해서, 상기 사용자 단말기(10)로부터 사용자 인증 재신청 정보를 입력받는 단계; (e-2) 상기 인증 증명서 재발급 프로그램(68-2)에 의해서, 상기 사용자 인증 재신청 정보를 이용하여 사용자를 재인증하고, 재인증 증명서 정보를 발급하는 단계; (e-3) 상기 인증 증명서 정보 재전송 프로그램(68-3)에 의해서, 상기 사용자 단말기로 상기 재인증 증명서 정보를 전송하는 단계; (e-4) 상기 재신청 정보 입력 프로그램(68-4)에 의해서, 상기 사용자 단말기(10)로부터 블록체인 네트워크를 통해 상기 재인증 증명서 정보를 입력받는 단계; (e-5) 상기 인증서 재조회 프로그램(68-5)에 의해서, 상기 블록체인 네트워크를 통해 인증서의 정당성을 조회하는 단계; 및 (e-6) 상기 계정 재등록 인정 프로그램(68-6)에 의해서, 사용자의 재등록 정보를 바탕으로 재등록이 인정되는 단계;를 포함할 수 있다.

[0078] 도 8은 본 발명의 계정 키 페어 기반 계정 인증 서비스를 운영하는 시스템의 연속적 데이터 무결성 입증 과정을 나타내는 참고도이고, 도 9는 도 8의 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법에 따른 신규 계정을 생성하는 과정을 나타내는 참고도이고, 도 10은 도 8의 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법에 따른 도난 신고 및 긴급 권한 동결 과정을 나타내는 참고도이고, 도 11은 도 8의 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법에 따른 키 페어 재등록 과정을 나타내는 참고도이다.

[0079] 도 8 내지 도 11에 도시된 바와 같이, 통상적으로, 블록체인 및 타 탈중앙화적 체계들은 공개 키 암호학(Public Key Cryptography)을 사용하므로 모든 전자서명은서명인의 ID(Public Key, 공개키)와 암호학적으로 서명할 때 쓰이는 프라이빗키(Privatekey)가 존재한다.

[0080] 초기 블록체인들은 이러한 공개 키 그 자체를 계정ID로 쓰고 있고 그로 인해, 프라이빗 키가 분실되거나 도난당할 시 계정에 종속되어있는 모든 데이터 및 계좌 권리를 잃게 된다.

[0081] 이러한 것은 정부 및 기업형 전산체계에서는 있을 수 없는 일이며, 블록체인이 내제하고 있는 탈중항화적 가치가 있다고 하더라도 용인될 수 없는 일이다.

[0082] 그러므로, 탈중앙화를 유지하면서 키를 재등록할 수 있는 기전을 동반하는 블록체인이 있다면 키페어 관리(Key Pair Management) 및 보안에 관한 많은 문제점들을 해결할 수 있다.

[0083] 이하, 도 8 내지 도 11을 참조하여, 본 발명에 따른 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법을 살펴보고자 한다.

[0084] 본 발명에 따른 탈중앙화 네트워크의 계정 키 페어 재등록 및 연속적 데이터 무결성 입증 방법은 계정 데이터를 분리시켜 존재하고, 하나의 계정이 여러 키들에 의해 종속되어 관리될 수 있게 하여, 블록체인에서 필수적인 무결성 검증을 가능하게 한 것으로, 상기 무결성 검증 방식은 다음과 같다.

[0085] 도 8에 도시된 바와 같이, 계정 데이터의 계정이 생성된 시점을 계정 생성 시점(t0)이라 하며, 이후, 프라이빗 키가 분실되거나 도난당했을 시에, 상기 계정에 종속되어있는 모든 데이터 및 계좌 권리를 유지하기 위한 계정 재등록이 행해지는데, 상기 계정 재등록이 행해지는 시점을 계정 재등록 시점(t1)이라한다.

[0086] 이와 마찬가지로, 프라이빗 키가 재차 분실되거나 도난당했을 시에, 상기 계

[0087] 정에 종속되어있는 모든 데이터 및 계좌 권리를 유지하기 위한 계정 2차 재등록이 행해지는데, 상기 계정 2차 재등록이 행해지는 시점을 계정 2차 재등록 시점(t2)이라 하며, 이후 계정 재등록이 행해질 때 마다 새로운 계정 재등록 시점이 발행하는데, 예를 들어, 계정 3차 재등록이 행해지는 시점은 계정 3차 재등록 시점(t3), 계정 4차 재등록이 행해지는 시점은 계정 4차 재등록 시점(t4), 계정 5차 재등록이 행해지는 시점은 계정 5차 재등록 시점(t5), 계정 n차 재등록이 행해지는 시점은 계정 n차 재등록 시점(tn)이라 한다.

[0088] 여기서, 상기 계정 등록 시점(t0)부터 상기 계정 재등록 시점(t1)까지는 예를 들어, a 키 페어가 유효 키로 등록되며, 상기 a 키 페어가 유효 키로 간주되는 기간을 a 키 페어 유효 기간(t0~t1)이라 한다. 상기 a 키 페어 유효 기간(t0~t1)에는 a키 페어 유효 기간(t0~t1)에는 a 키 페어가 사용되어 서명되어야 한다.

[0089] 또한, 상기 계정 재등록 시점(t1)부터 계정 2차 재등록이 재차 행해지는 시점인 계정 2차 재등록 시점(t2)까지는 예를 들어, b 키 페어가 유효 키로 등록된다.

[0090] 이때, 상기 b 키 페어가 유효 키로 간주되는 기간을 b 키 페어 유효 기간(t1~t2)이라 한다. 상기 b 키 페어 유효 기간(t1~t2)에는 상기 b 키 페어가 사용되어 서명되어야 한다.

[0091] 이와 마찬가지로, 상기 계정 2차 재등록 시점(t2)부터 계정 3차 재등록이 행해지는 계정 2차 재등록 시점(t3)까지는 예를 들어, c 키 페어가 유효 키로 등록된다. 이때, 상기 c 키 페어가 유효 키로 간주되는 기간을 c 키 페어 유효 기간(t2~t3)이라 한다. 상기 c 키 페어 유효 기간(t2~t3)에는 상기 c 키 페어가 사용되어 서명되어야 한다.

[0092] 또한, 계정 n차 재등록 시점(tn)부터 현재까지는 예를 들어, n 키 페어가 유효 키로 등록된다. 이때, 상기 n 키 페어가 유효 키로 간주되는 기간을 n 키 페어 유효 기간(tn~현재)이라 한다. 상기 n 키 페어 유효 기간(tn~현재)에는 상기 n 키페어가 사용되어 서명되어야 한다.

[0093] 이러한 방식으로 키 페어 유효 기간 마다 상이한 유효 키 페어가 사용되어 서명되어야 하기에, 무결점 검증 절차가 이루어 진다.

[0094] 본 발명에 따른 계정 키 페어 기반 계정 인증 서비스를 운영하는 방법에서, 계정 생성 및 초기 키 페어 등록을 위한 계정 생성 및 초기 키 페어 등록 방법은 다음과 같다.

[0095] 먼저, 사용자가 개인이 신뢰하는 기기(예를 들어, 단말)을 통해 초기 키 페어가 생성된다.

[0096] 이후, 사용자의 단말을 통해 인증 네트워크에 접속하여, 인증 네트워크에서 사용자를 인증 받는다.

[0097] 그 후, 인증 네트워크에 의해 사용자가 인증된 후, 인증 네트워크를 통해 사용자 단말로 인증 증명서가 발급된다.

[0098] 이후, 사용자 단말을 통해 블록체인 네트워크에 접속하여, 인증 증명서와 함께, 신규 계정 등록이 요청된다. 이때, 초기 키페어로 사용될 공개 키가 필수적으로 첨부된다.

[0099] 그 후, 블록체인 네트워크가 인증 네트워크를 통해 인증 증명서가 정당한 지가 조회된다.

[0100] 이후, 상기 인증 증명서가 조회된 후, 사용자의 등록 정보를 바탕으로 블록체인 네트워크에 의해 신규 계정이 생성된다.

[0101] 이러한 방식으로 생성된 계정 및 등록된 초기 키 페어가 사용되어 진다.

[0102] 한편, 프라이빗 키가 분실되거나 도난당했을 시에, 계정에 종속되어있는 모든 데이터 및 계좌 권리를 유지하기 위한 계정 재등록이 행해지는데, 상기 계정 재등록 방법은 다음과 같다.

[0103] 먼저, 사용자 단말에 의해 블록체인 네트워크로 도난 신고 및 긴급 계정 동결이 요청된다.

[0104] 이후, 블록체인 네트워크를 통해, 긴급 계정 동결 요청이 적당한지가 심사된다. 상기 단계에서, 긴급 계정 동결 요청이 계정 동결 조건을 충족한다면, 현재의 유효 키 페어가 동결된다. 이때, 상기 유효 키 페어가 동결된 후에 진행되어진 상기 동결된 유효 키 페어로 서명된 모든 트랜잭션은 거부된다.

[0105] 상기 동결된 유효 키 페어로 서명된 모든 트랜잭션은 거부된다. 또 한편, 키 페어 등록을 위한 키 페어 등록 방법은 다음과 같다.

[0106] 먼저, 사용자가 단말을 통해 새로운 키 페어가 생성된다. 이후, 사용자의 단말을 통해 인증 네트워크에 접속하여, 인증 네트워크에서 사용자를 인증 받는다.

[0107] 그 후, 인증 네트워크에 의해 사용자가 인증된 후, 인증 네트워크를 통해 사용자 단말로 인증 증명서가 발급된다.

[0108] 이후, 사용자 단말을 통해 블록체인 네트워크에 접속하여, 인증 증명서와 함께, 키 페어 재등록이 요청된다. 이때, 키페어로 사용될 새로운 공개 키가 필수적으로 첨부된다.

[0109] 그 후, 블록체인 네트워크가 인증 네트워크를 통해 인증 증명서가 정당한 지가 조회된다.

[0110] 이후, 상기 인증 증명서가 조회된 후, 사용자의 재등록 정보를 바탕으로 블록체인 네트워크에 의해 재등록이 인정된다. 이러한 방식으로 재등록된 초기 키 페어가 사용되어 진다.

[0111] 전술한 바와 같이, 본 발명에 따른 탈중앙화 네트워크의 계정 키 페어 재등록 및 연속적 데이터 무결성 입증 방법은 계정 데이터가 분리되어 존재하며, 하나의 계정이 여러 키들에 의해 종속되어 관리됨으로써, 블록체인에서 필수적인 무결성 검증을 가능하게 할 수 있다.

[0112] 한편, 본 발명은 또한 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로서 구현되는 것이 가능

하다.

[0113] 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함할 수 있다.

[0114] 컴퓨터가 읽을 수 있는 기록 매체의 예로는 상술된 서버 컴퓨터(60)는 물론이고, ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광자기 디스크, 광데이터 저장장치, 플래시 메모리, USB 메모리 등이 있으며, 또한 캐리어 웨이브(예를 들면 인터넷을 통한 전송)의 형태로 구현되는 것도 포함할 수 있다.

[0115] 또한, 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

[0116] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 당해 기술분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 다른 실시예가 가능하다는 점을 이해할 것이다. 따라서 본 발명의 진정한 기술적 보호 범위는 첨부된 특허청구범위의 기술적 사상에 의하여 정해져야 할 것이다.

부호의 설명

[0117] 10: 사용자 단말기

90: 운영자 단말기

50: 네트워크

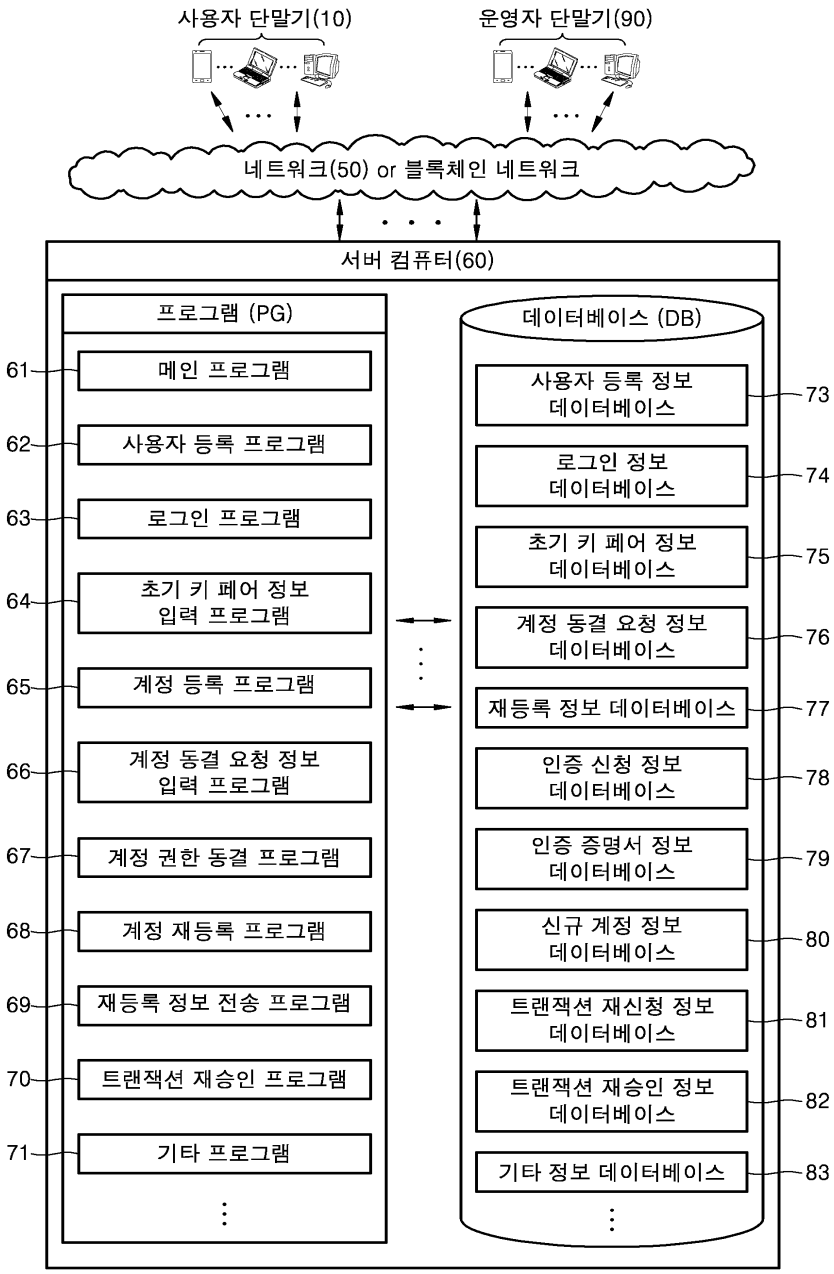
60: 서버 컴퓨터

PG: 프로그램 제어부

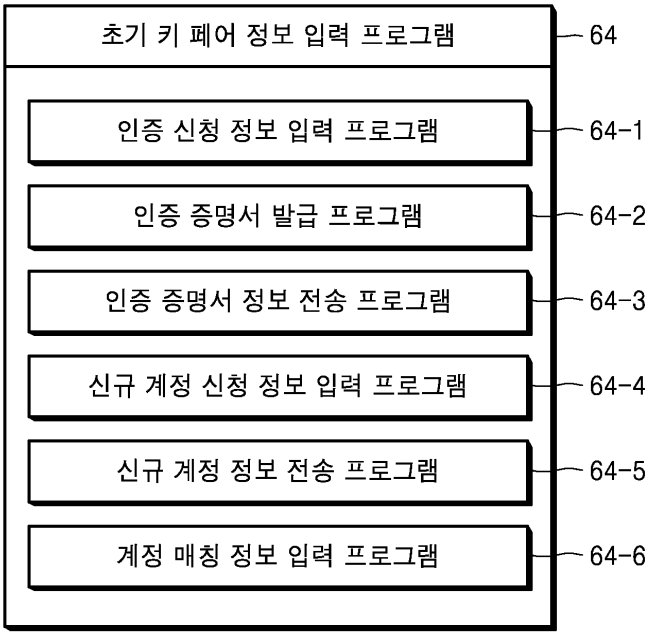
DB: 데이터베이스

도면

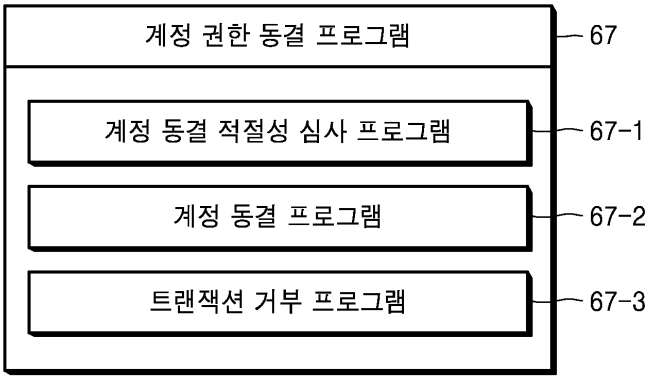
도면1


사용자 단말기(10)
운영자 단말기(90)
네트워크(50) or 블록체인 네트워크
서버 컴퓨터(60)
프로그램 (PG)
61 메인 프로그램
62 사용자 등록 프로그램
63 로그인 프로그램
64 초기 키 페어 정보 입력 프로그램
65 계정 등록 프로그램
66 계정 동결 요청 정보 입력 프로그램
67 계정 권한 동결 프로그램
68 계정 재등록 프로그램
69 재등록 정보 전송 프로그램
70 트랜잭션 재승인 프로그램
71 기타 프로그램
데이터베이스 (DB)
사용자 등록 정보 데이터베이스 73
로그인 정보 데이터베이스 74
초기 키 페어 정보 데이터베이스 75
계정 동결 요청 정보 데이터베이스 76
재등록 정보 데이터베이스 77
인증 신청 정보 데이터베이스 78
인증 증명서 정보 데이터베이스 79
신규 계정 정보 데이터베이스 80
트랜잭션 재신청 정보 데이터베이스 81
트랜잭션 재승인 정보 데이터베이스 82
기타 정보 데이터베이스 83

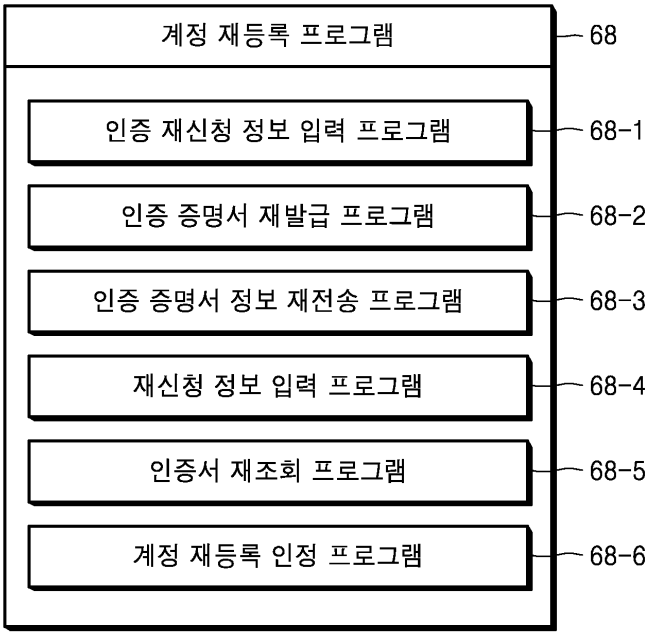
도면2


초기 키 페어 정보 입력 프로그램
64
인증 신청 정보 입력 프로그램
64-1
인증 증명서 발급 프로그램
64-2
인증 증명서 정보 전송 프로그램
64-3
신규 계정 신청 정보 입력 프로그램
64-4
신규 계정 정보 전송 프로그램
64-5
계정 매칭 정보 입력 프로그램
64-6

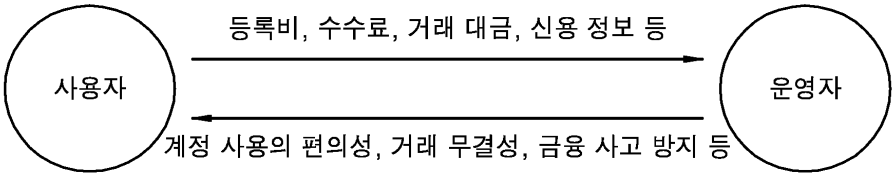
도면3


계정 권한 동결 프로그램
67
계정 동결 적절성 심사 프로그램
67-1
계정 동결 프로그램
67-2
트랜잭션 거부 프로그램
67-3

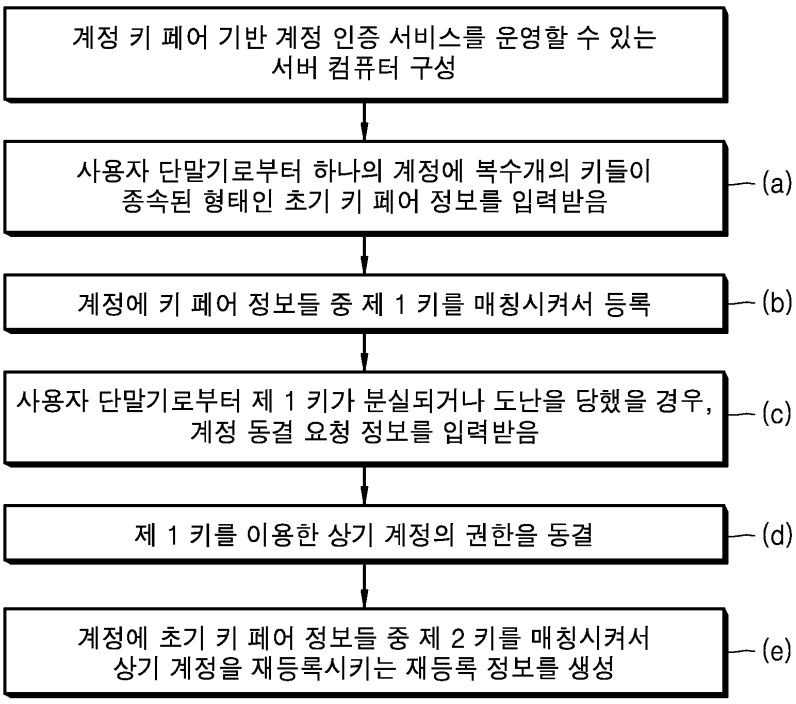
도면4


계정 재등록 프로그램
68
인증 재신청 정보 입력 프로그램
68-1
인증 증명서 재발급 프로그램
68-2
인증 증명서 정보 재전송 프로그램
68-3
재신청 정보 입력 프로그램
68-4
인증서 재조회 프로그램
68-5
계정 재등록 인정 프로그램
68-6

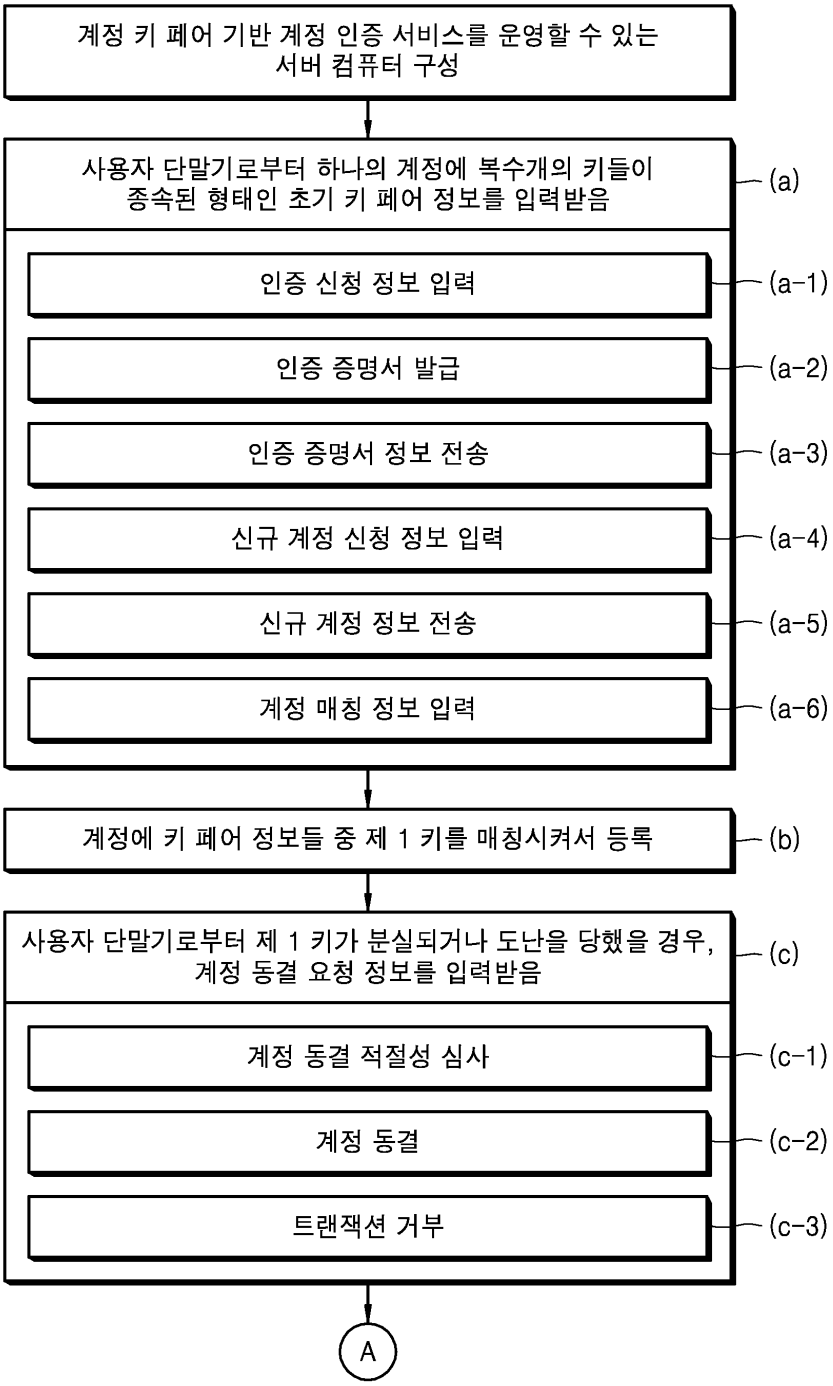
도면5


사용자
등록비, 수수료, 거래 대금, 신용 정보 등
운영자
계정 사용의 편의성, 거래 무결성, 금융 사고 방지 등

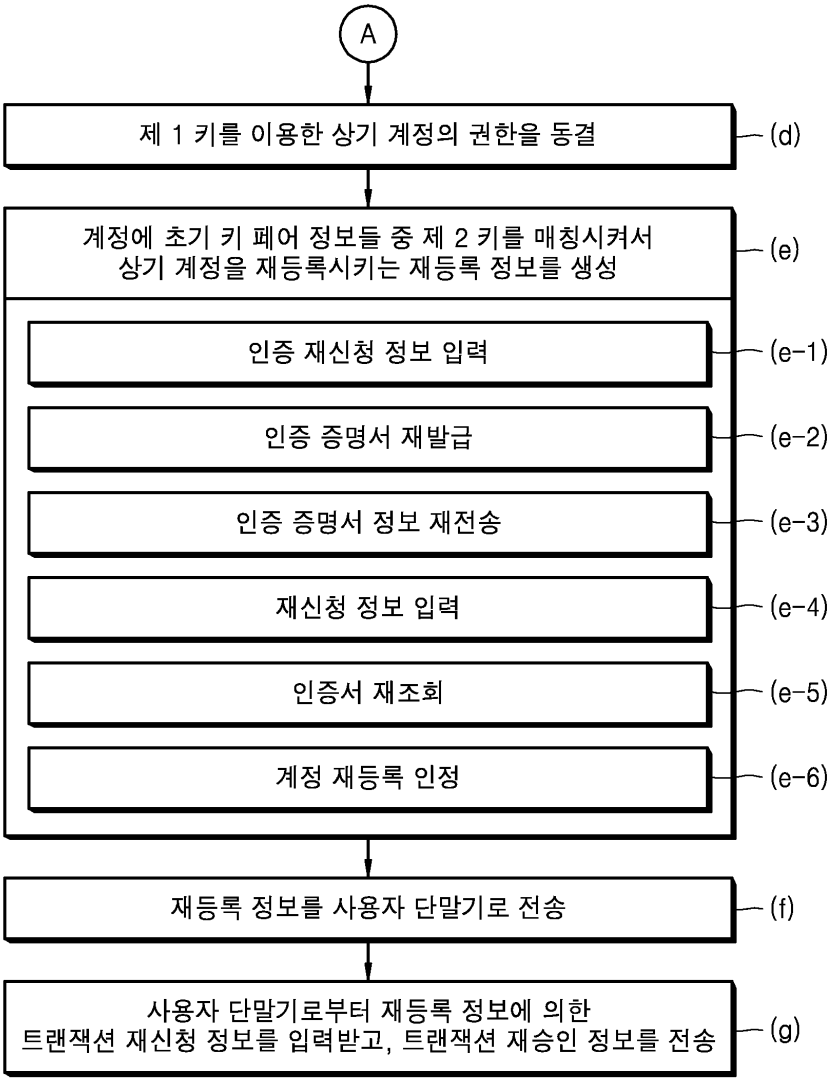
도면6


계정 키 페어 기반 계정 인증 서비스를 운영할 수 있는 서버 컴퓨터 구성
사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받음
(a)
계정에 키 페어 정보들 중 제 1 키를 매칭시켜서 등록
(b)
사용자 단말기로부터 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받음
(c)
제 1 키를 이용한 상기 계정의 권한을 동결
(d)
계정에 초기 키 페어 정보들 중 제 2 키를 매칭시켜서 상기 계정을 재등록시키는 재등록 정보를 생성
(e)

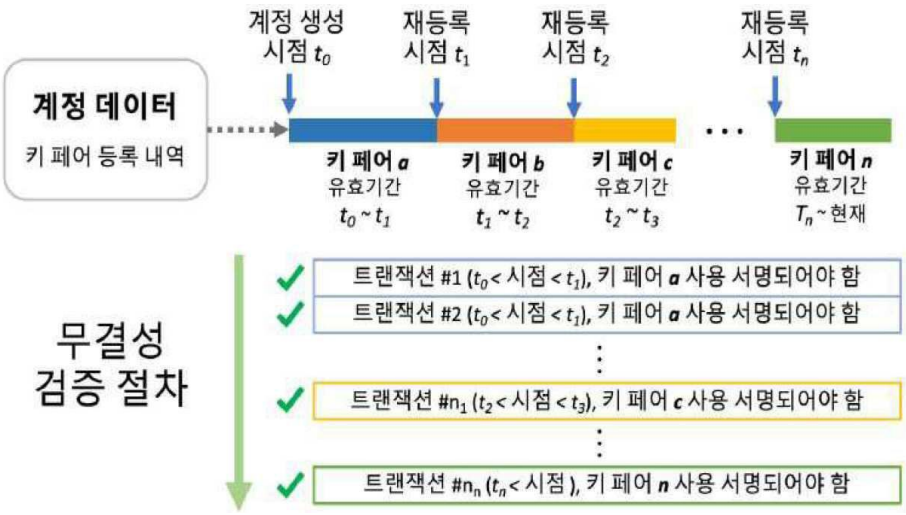
도면7a


계정 키 페어 기반 계정 인증 서비스를 운영할 수 있는 서버 컴퓨터 구성
사용자 단말기로부터 하나의 계정에 복수개의 키들이 종속된 형태인 초기 키 페어 정보를 입력받음
(a)
인증 신청 정보 입력
(a-1)
인증 증명서 발급
(a-2)
인증 증명서 정보 전송
(a-3)
신규 계정 신청 정보 입력
(a-4)
신규 계정 정보 전송
(a-5)
계정 매칭 정보 입력
(a-6)
계정에 키 페어 정보들 중 제 1 키를 매칭시켜서 등록
(b)
사용자 단말기로부터 제 1 키가 분실되거나 도난을 당했을 경우, 계정 동결 요청 정보를 입력받음
(c)
계정 동결 적절성 심사
(c-1)
계정 동결
(c-2)
트랜잭션 거부
(c-3)
A

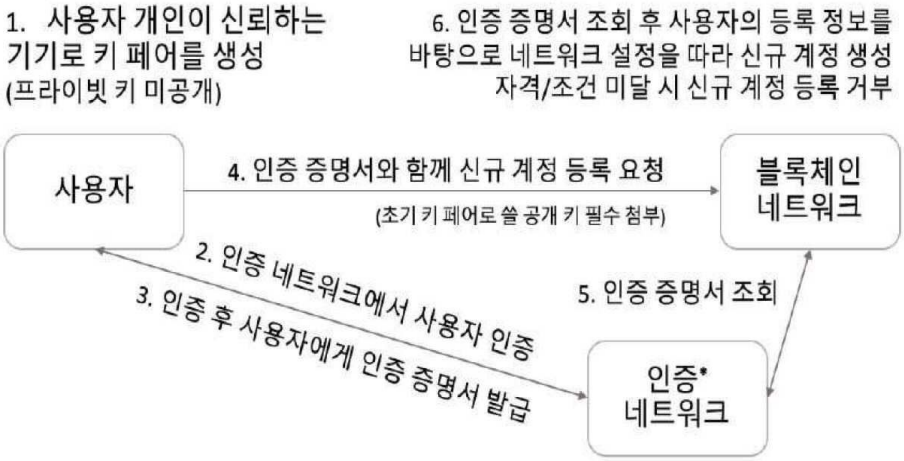
도면7b


A
제 1 키를 이용한 상기 계정의 권한을 동결
(d)
계정에 초기 키 페어 정보들 중 제 2 키를 매칭시켜서
상기 계정을 재등록시키는 재등록 정보를 생성
(e)
인증 재신청 정보 입력
(e-1)
인증 증명서 재발급
(e-2)
인증 증명서 정보 재전송
(e-3)
재신청 정보 입력
(e-4)
인증서 재조회
(e-5)
계정 재등록 인정
(e-6)
재등록 정보를 사용자 단말기로 전송
(f)
사용자 단말기로부터 재등록 정보에 의한
트랜잭션 재신청 정보를 입력받고, 트랜잭션 재승인 정보를 전송
(g)

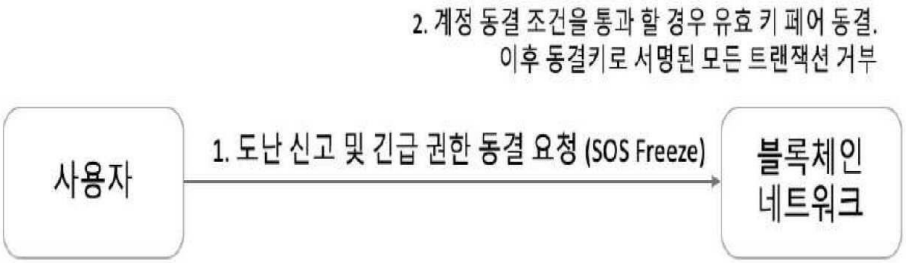
도면8


계정 생성 시점 t_0
재등록 시점 t_1
재등록 시점 t_2
재등록 시점 t_n
계정 데이터
키 페어 등록 내역
키 페어 a 유효기간 $t_0 \sim t_1$
키 페어 b 유효기간 $t_1 \sim t_2$
키 페어 c 유효기간 $t_2 \sim t_3$
키 페어 n 유효기간 $T_n \sim$ 현재
무결성 검증 절차
트랜잭션 #1 (t_0 < 시점 < t_1), 키 페어 a 사용 서명되어야 함
트랜잭션 #2 (t_0 < 시점 < t_1), 키 페어 a 사용 서명되어야 함
트랜잭션 #n_1 (t_2 < 시점 < t_3), 키 페어 c 사용 서명되어야 함
트랜잭션 #n_n (t_n < 시점), 키 페어 n 사용 서명되어야 함

도면9



도면10



도면11