



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년06월18일
(11) 등록번호 10-1990761
(24) 등록일자 2019년06월12일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) G06Q 20/38 (2012.01)
G06Q 20/40 (2012.01)
(52) CPC특허분류
H04L 63/0861 (2013.01)
G06Q 20/3827 (2013.01)
(21) 출원번호 10-2018-7030963
(22) 출원일자(국제) 2016년03월29일
심사청구일자 2018년10월25일
(85) 번역문제출일자 2018년10월25일
(65) 공개번호 10-2018-0122025
(43) 공개일자 2018년11월09일
(86) 국제출원번호 PCT/US2016/024776
(87) 국제공개번호 WO 2017/171733
국제공개일자 2017년10월05일
(30) 우선권주장
15/083,241 2016년03월28일 미국(US)
(56) 선행기술조사문헌
US20150356523 A1
US20150324789 A1

(73) 특허권자
블랙 골드 코인 인코포레이티드
미국 네바다주 89130 라스베가스 스위트 100 애저
드라이브 7495
(72) 발명자
안드라데 마르쿠스
미국 네바다주 89130 라스베가스 스위트 100 애저
드라이브 7495
(74) 대리인
특허법인태평양

전체 청구항 수 : 총 20 항

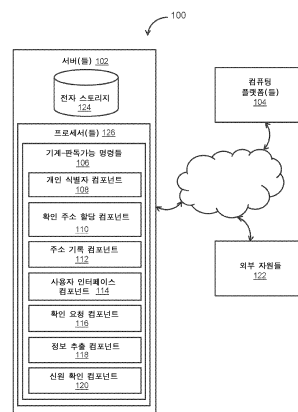
심사관 : 문형섭

(54) 발명의 명칭 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 시스템들 및 방법들

(57) 요약

블록 체인-기반 멀티팩터 개인 신원 확인이 제공될 수 있다. 식별자들을 이전에 확인된 개인 신원들을 가진 개인들과 연관시키며, 블록 체인에 대한 확인 주소들을 개인들에게 할당하며 그리고 개인들과 연관된 식별자들 및 생체인증 데이터를 대응하는 확인 주소들에 기록함으로써, 블록 체인 상에 확인 주소들이 설정될 수 있다. 확인 주소들을 사용하는 블록 체인-기반 멀티팩터 개인 신원 확인은 하나 이상의 개인들의 신원을 확인하기 위한 하나 이상의 요청들과 관련한 하나 이상의 식별자들을 수신하며, 하나 이상의 개인들과 연관된 생체인증 데이터를 대응하는 확인 주소들로부터 추출하며 그리고 서로 매칭하는 생체인증 데이터 및 개인 키들을 수신할 때 하나 이상의 개인들의 신원을 확인함으로써 수행될 수 있다.

대표도 - 도1



(52) CPC특허분류

G06Q 20/3829 (2013.01)

G06Q 20/40145 (2013.01)

H04L 2463/082 (2013.01)

명세서

청구범위

청구항 1

블록 체인-기반 멀티팩터 개인 신원 확인(verification)을 제공하는 시스템으로서,

블록 체인을 저장하도록 구성되는 하나 이상의 컴퓨터-판독 가능 저장 매체; 및

컴퓨터 프로그램 명령들을 실행하도록 프로그램된 하나 이상의 프로세서를 포함하는 서버-측 컴퓨터 시스템을 포함하고,

상기 컴퓨터 프로그램 명령들이 실행될 때 상기 서버-측 컴퓨터 시스템으로 하여금:

이전의 확인된 개인 신원을 가지는 개인에게 상기 블록 체인에 연관된 확인 주소를 할당하고,

상기 하나 이상의 컴퓨터-판독 가능 저장 매체에 상기 블록 체인과 연관된 상기 확인 주소와 관련하여 상기 개인의 생체 해시 및 상기 개인의 식별자를 저장하고 - 상기 생체 해시는 상기 개인의 생체 데이터의 해시이고, 상기 식별자, 상기 생체 해시 및 상기 확인 주소 각각은 서로 상이하고, 상기 확인 주소가 추출되는 개인 키 및 공개 키와 상이함-,

클라이언트-측 디바이스로부터, 상기 개인의 신원을 확인하기 위한 요청과 관련하여 상기 식별자 및 상기 생체 데이터를 획득하고-상기 요청은 상기 블록 체인과 연관된 상기 확인 주소를 나타냄-,

상기 요청에 의해 나타난 상기 확인 주소를 이용하여 상기 저장된 식별자 및 상기 저장된 생체 해시를 획득하고,

상기 요청의 상기 식별자 및 상기 요청의 상기 생체 데이터가 상기 저장된 식별자 및 상기 저장된 생체 해시에 매칭한다는 결정에 따라 상기 개인의 신원의 확인을 서명하도록 하는 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 시스템.

청구항 2

청구항 1에 있어서,

상기 서버-측 컴퓨터 시스템으로 하여금:

상기 요청의 상기 식별자 및 상기 요청의 상기 생체 데이터가 상기 저장된 식별자 및 상기 저장된 생체 해시에 매칭한다는 결정에 따라, 상기 확인 주소가 추출되는 상기 개인 키를 이용하여, 상기 개인의 신원의 확인을 서명하도록 하는 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 시스템.

청구항 3

청구항 2에 있어서,

상기 서버-측 컴퓨터 시스템으로 하여금:

상기 하나 이상의 컴퓨터-판독 가능 저장 매체에, 상기 블록 체인에 연관된 상기 확인 주소와 관련하여 상기 개인 키를 저장하고,

상기 클라이언트-측 디바이스로부터 상기 개인의 신원을 확인하기 위한 상기 요청에 관련하여 상기 개인 키를 획득하고,

상기 요청에 의해 나타난 상기 확인 주소를 이용하여 상기 저장된 개인 키를 획득하고, 그리고,

상기 요청의 상기 식별자, 상기 요청의 상기 생체 데이터, 및 상기 요청의 상기 개인 키가 상기 저장된 식별자, 상기 저장된 생체 해시, 및 상기 저장된 개인 키에 매칭한다는 결정에 따라, 상기 개인 키를 이용하여, 상기 개인의 신원의 확인을 서명하도록 하는 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 시스템.

청구항 4

청구항 3에 있어서,

상기 개인 키는 또한 상기 클라이언트-측 디바이스에 저장되고, 상기 클라이언트-측 디바이스는 상기 개인의 사용자 디바이스인 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 시스템.

청구항 5

청구항 1에 있어서,

상기 서버-측 컴퓨터 시스템으로 하여금:

상기 블록 체인에 연관된 다른 확인 주소를 상기 개인에게 할당하고;

상기 하나 이상의 컴퓨터-판독 가능 저장 매체에 상기 블록 체인과 연관된 상기 다른 확인 주소와 관련하여 상기 개인의 다른 생체 해시를 저장하고-상기 다른 생체 해시는 상기 개인의 다른 생체 데이터의 해시임-;

상기 클라이언트-측 디바이스로부터, 상기 개인의 신원을 확인하기 위한 상기 요청에 관련하여 상기 다른 생체 데이터를 획득하고-상기 요청은 상기 블록 체인에 연관된 상기 다른 확인 주소를 더 나타냄-;

상기 요청에 의해 나타난 상기 다른 확인 주소를 이용하여 상기 저장된 다른 생체 해시를 획득하고; 그리고

상기 요청의 상기 식별자, 상기 요청의 상기 생체 데이터 및 상기 요청의 상기 다른 생체 데이터가 상기 저장된 식별자, 상기 저장된 생체 해시 및 상기 저장된 다른 생체 해시에 매칭한다는 결정에 따라 상기 개인의 신원의 확인을 서명하도록 하는 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 시스템.

청구항 6

청구항 5에 있어서,

상기 서버-측 컴퓨터 시스템으로 하여금:

상기 개인에 대한 상기 블록 체인의 주소로서의 상기 다른 확인 주소를 추가하기 위한 사용자-개시 명령을 사용자 인터페이스를 통하여 획득하고;

상기 사용자-개시 명령에 기반하여 상기 블록 체인과 연관된 상기 다른 확인 주소를 상기 개인에게 할당하도록 하는 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 시스템.

청구항 7

청구항 5에 있어서,

상기 서버-측 컴퓨터 시스템으로 하여금:

상기 개인에 대한 상기 블록 체인의 주소로서의 상기 다른 확인 주소를 제거하기 위한 사용자-개시(user-initiated) 명령을 사용자 인터페이스를 통하여 획득하고;

상기 사용자-개시 명령에 기반하여 상기 개인으로부터 상기 블록 체인과 연관된 상기 다른 확인 주소를 할당 해지하도록 하는 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 시스템.

청구항 8

청구항 1에 있어서,

상기 서버-측 컴퓨터 시스템으로 하여금:

상기 개인과는 다른 제1 사용자에게 상기 블록 체인과 연관된 상기 확인 주소와 관련하여 상기 하나 이상의 컴퓨터-판독 가능 저장 매체에 저장된 데이터로의 액세스를 제공하고-상기 제1 사용자가 제1 개인 키를 가진다는 확인에 기반하여 상기 제1 사용자에게 상기 저장된 데이터로의 액세스가 제공되고, 상기 제1 개인키는 상기 확인 주소가 추출된 상기 개인 키와는 다름-; 그리고

상기 개인과는 다른 제2 사용자에게, 상기 제2 사용자가 제2 개인 키를 가진다는 확인에 기반하여 상기 저장된

데이터로의 액세스를 거부하는 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 시스템.

청구항 9

청구항 1에 있어서,

상기 생체 데이터는 이미지, 기록(recording) 또는 템플릿을 포함하는 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 시스템.

청구항 10

청구항 1에 있어서,

상기 생체 데이터는 지문, 손바닥 정맥, 얼굴 인식, DNA, 장문, 손 모양, 홍채 인식, 망막, 냄새, 걸음 걸이 또는 음성과 관련되는 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 시스템.

청구항 11

블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 방법으로서,

상기 방법은, 실행될 때 상기 방법을 수행하는 컴퓨터 프로그램 명령들을 실행하는 하나 이상의 프로세서를 포함하는 서버-측 컴퓨터 시스템에 의하여 구현되고,

상기 방법은:

상기 서버-측 컴퓨터 시스템에 의하여, 상기 서버-측 컴퓨터 시스템의 하나 이상의 컴퓨터-판독 가능 저장 매체에 블록 체인을 저장하는 단계;

상기 서버-측 컴퓨터 시스템에 의하여, 상기 블록 체인에 연관된 확인 주소를 개인에게 할당하는 단계-상기 개인은 이전에 확인된 개인 신원을 가짐-;

상기 서버-측 컴퓨터 시스템에 의하여, 상기 하나 이상의 컴퓨터-판독 가능 저장 매체에 상기 블록 체인에 연관된 상기 확인 주소와 관련하여 상기 개인의 생체 해시 및 상기 개인의 식별자를 저장하는 단계-상기 생체 해시는 상기 개인의 생체 데이터의 해시이고, 상기 식별자, 상기 생체 해시 및 상기 확인 주소 각각은 서로 상이하고, 상기 확인 주소가 추출되는 개인 키 및 공개 키와 상이함-;

상기 서버-측 컴퓨터 시스템에 의하여, 클라이언트-측 디바이스로부터 상기 개인의 신원을 확인하기 위한 요청과 관련하여 상기 식별자 및 상기 생체 데이터를 획득하는 단계-상기 요청은 상기 블록 체인에 연관된 상기 확인 주소를 나타냄-;

상기 서버-측 컴퓨터 시스템에 의하여, 상기 요청에 의해 나타난 상기 확인 주소를 이용하여 상기 저장된 식별자 및 상기 저장된 생체 해시를 획득하는 단계; 및

상기 서버-측 컴퓨터 시스템에 의하여, 상기 요청의 상기 식별자 및 상기 요청의 상기 생체 데이터가 상기 저장된 식별자 및 상기 저장된 생체 해시에 매칭한다는 결정에 따라 상기 개인의 신원의 확인을 서명하는 단계를 포함하는 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 방법.

청구항 12

청구항 11에 있어서,

상기 서버-측 컴퓨터 시스템에 의하여, 상기 요청의 상기 식별자 및 상기 요청의 상기 생체 데이터가 상기 저장된 식별자 및 상기 저장된 생체 해시에 매칭한다는 결정에 따라, 상기 확인 주소가 추출된 상기 개인 키를 이용하여, 상기 개인의 신원의 확인을 서명하는 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 방법.

청구항 13

청구항 12에 있어서,

상기 서버-측 컴퓨터 시스템에 의하여, 상기 하나 이상의 컴퓨터-판독 가능 저장 매체에 상기 블록 체인에 연관된 상기 확인 주소와 관련하여 상기 개인 키를 저장하는 단계;

상기 서버-측 컴퓨터 시스템에 의하여, 상기 클라이언트-측 디바이스로부터 상기 개인의 신원을 확인하기 위한

상기 요청과 관련하여 상기 개인 키를 획득하는 단계;

상기 요청에 의해 나타난 상기 확인 주소를 이용하여 상기 저장된 개인 키를 획득하는 단계; 및

상기 서버-측 컴퓨터 시스템에 의하여, 상기 요청의 상기 식별자, 상기 요청의 상기 생체 데이터, 및 상기 요청의 상기 개인 키가 상기 저장된 식별자, 상기 저장된 생체 해시, 및 상기 저장된 개인 키에 매칭한다는 결정에 따라, 상기 개인 키를 이용하여, 상기 개인의 신원의 확인을 서명하는 단계를 더 포함하는 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 방법.

청구항 14

청구항 11에 있어서,

상기 서버-측 컴퓨터 시스템에 의하여, 상기 블록 체인에 연관된 다른 확인 주소를 상기 개인에게 할당하는 단계;

상기 서버-측 컴퓨터 시스템에 의하여, 상기 하나 이상의 컴퓨터-관독 가능 저장 매체에 상기 블록 체인과 연관된 상기 다른 확인 주소와 관련하여 상기 개인의 다른 생체 해시를 저장하는 단계-상기 다른 생체 해시는 상기 개인의 다른 생체 데이터의 해시임-;

상기 서버-측 컴퓨터 시스템에 의하여, 상기 클라이언트-측 디바이스로부터 상기 개인의 신원을 확인하기 위한 상기 요청에 관련하여 상기 다른 생체 데이터를 획득하는 단계-상기 요청은 상기 블록 체인에 연관된 상기 다른 확인 주소를 더 나타냄-;

상기 서버-측 컴퓨터 시스템에 의하여, 상기 요청에 의해 나타난 상기 다른 확인 주소를 이용하여 상기 저장된 다른 생체 해시를 획득하는 단계; 및

상기 서버-측 컴퓨터 시스템에 의하여, 상기 요청의 상기 식별자, 상기 요청의 상기 생체 데이터 및 상기 요청의 상기 다른 생체 데이터가 상기 저장된 식별자, 상기 저장된 생체 해시 및 상기 저장된 다른 생체 해시에 매칭한다는 결정에 따라 상기 개인의 신원의 확인을 서명하는 단계를 포함하는 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 방법.

청구항 15

청구항 14에 있어서,

상기 서버-측 컴퓨터 시스템에 의하여, 상기 개인에 대한 상기 블록 체인의 주소로서의 상기 다른 확인 주소를 추가하기 위한 사용자-개시 명령을 사용자 인터페이스를 통하여 획득하는 단계; 및

상기 서버-측 컴퓨터 시스템에 의하여, 상기 사용자-개시 명령에 기반하여 상기 블록 체인에 연관된 상기 다른 확인 주소를 상기 개인에게 할당하는 단계를 포함하는 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 방법.

청구항 16

청구항 14에 있어서,

상기 서버-측 컴퓨터 시스템에 의하여, 상기 개인에 대한 상기 블록 체인의 주소로서의 상기 다른 확인 주소를 제거하기 위한 사용자-개시 명령을 사용자 인터페이스를 통하여 획득하는 단계; 및

상기 서버-측 컴퓨터 시스템에 의하여, 상기 사용자-개시 명령에 기반하여 상기 개인으로부터 상기 블록 체인에 연관된 상기 다른 확인 주소의 할당을 해지하는 단계를 포함하는 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 방법.

청구항 17

청구항 11에 있어서,

상기 서버-측 컴퓨터 시스템에 의하여, 상기 개인과는 다른 제1 사용자에게 상기 블록 체인에 연관된 상기 확인 주소와 관련하여 상기 하나 이상의 컴퓨터-관독 가능 저장 매체에 저장된 데이터로의 액세스를 제공하는 단계-상기 제1 사용자가 제1 개인 키를 가진다는 확인에 기반하여 상기 제1 사용자에게 상기 저장된 데이터로의 액세스

스가 제공되고, 상기 제1 개인키는 상기 확인 주소가 추출된 상기 개인 키와는 다름; 및

상기 서버-측 컴퓨터 시스템에 의하여, 상기 개인과는 다른 제2 사용자에게, 상기 제2 사용자가 제2 개인 키를 가진다는 확인에 기반하여 상기 저장된 데이터로의 액세스를 거부하는 단계를 포함하는 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 방법.

청구항 18

청구항 11에 있어서,

상기 생체 데이터는 이미지, 기록 또는 템플릿을 포함하는 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 방법.

청구항 19

청구항 11에 있어서,

상기 생체 데이터는 지문, 손바닥 정맥, 얼굴 인식, DNA, 장문, 손 모양, 홍채 인식, 망막, 냄새, 걸음 걸이 또는 음성과 관련되는 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 방법.

청구항 20

블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 시스템으로서

블록 체인을 저장하도록 구성되는 하나 이상의 컴퓨터-판독 가능 저장 매체; 및

컴퓨터 프로그램 명령들을 실행하도록 프로그램된 하나 이상의 프로세서를 포함하는 서버-측 컴퓨터 시스템;을 포함하고,

상기 컴퓨터 프로그램 명령들이 실행될 때, 상기 서버-측 컴퓨터 시스템으로 하여금:

상기 블록 체인의 복수의 확인 주소들을 개인에게 할당하고-상기 개인은 이전에 확인된 개인 신원을 가지고, 상기 복수의 확인 주소들은 상기 블록 체인에 연관된 제1 확인 주소와 상기 블록 체인에 연관된 제2 확인 주소를 포함함;

상기 하나 이상의 컴퓨터-판독 가능 저장 매체에, (i) 상기 블록 체인과 연관된 상기 제1 확인 주소와 관련하여 상기 개인의 제1 생체 해시 및 상기 개인의 식별자, (ii) 상기 블록 체인에 연관된 상기 제2 확인 주소와 관련하여 상기 개인의 제2 생체 해시를 저장하고

-상기 제1 생체 해시는 상기 개인의 제1 생체 데이터의 해시이고, 상기 제2 생체 해시는 상기 개인의 제2 생체 데이터의 해시이고,

상기 식별자, 상기 제1 생체 해시, 상기 제2 생체 해시, 상기 제1 확인 주소, 및 상기 제2 확인 주소 각각은 서로 상이하고, 상기 제1 확인 주소가 추출된 제1 개인 키 및 제1 공개 키와는 상이하고, 상기 제2 확인 주소가 추출된 제2 개인 키 및 제2 공개 키와는 상이함;

클라이언트-측 디바이스로부터, 상기 개인의 신원을 확인하기 위한 요청과 관련된 상기 식별자, 상기 제1 생체 데이터 및 상기 제2 생체 데이터를 획득하고-상기 요청은 상기 블록 체인에 연관된 상기 제1 확인 주소 및 상기 블록 체인에 연관된 상기 제2 확인 주소를 나타냄;

- (1) 상기 요청에 나타난 상기 제1 확인 주소를 이용하여 상기 저장된 식별자 및 상기 저장된 제1 생체 해시 및,
- (2) 상기 요청에 나타난 제2 확인 주소를 이용하여 상기 저장된 제2 생체 해시를 획득하고,

상기 요청의 상기 식별자, 상기 요청의 상기 제1 생체 데이터, 및 상기 요청의 상기 제2 생체 데이터가 상기 저장된 식별자, 상기 저장된 제1 생체 해시, 및 상기 저장된 제2 생체 해시와 매칭한다는 결정에 따라, 상기 제1 확인 주소가 추출된 상기 개인 키를 이용하여, 상기 개인의 신원의 확인을 서명하고,

상기 개인과는 다른 제1 사용자에게 상기 블록 체인과 연관된 상기 제1 확인 주소와 관련하여 상기 하나 이상의 컴퓨터-판독 가능 저장 매체에 저장된 데이터로의 액세스를 제공하고- 상기 제1 사용자가 제1 개인 키를 가진다는 확인에 기반하여 상기 제1 사용자에게 상기 저장된 데이터로의 액세스가 제공되고, 상기 제1 개인 키는 상기 제1 확인 주소가 추출된 상기 개인 키와는 다르고, 상기 제2 확인 주소가 추출된 상기 개인 키와는 다름;

상기 개인과는 다른 제2 사용자에게, 상기 제2 사용자가 제2 개인 키를 가진다는 확인에 기반하여 상기 저장된 데이터로의 액세스를 거부하도록 하는 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하는 시스템.

발명의 설명

기술 분야

[0001] 본 개시내용은 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하기 위한 시스템들 및 방법들에 관한 것이다.

발명의 내용

[0002] 본 개시내용의 일 태양은 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하기 위한 시스템에 관한 것이다. 시스템은 블록 체인 상에 확인 주소들을 설정하고 그리고/또는 확인 주소들을 사용하여 블록 체인-기반 멀티팩터 개인 신원 확인을 수행하는 기계-판독가능 명령들로 구성된 하나 이상의 하드웨어 프로세서들을 포함할 수 있다. 블록 체인 상에 확인 주소들을 설정하는 것은 식별자들을 이전에 확인된 개인 신원들을 갖는 개인들과 연관시키는 것 - 제1 식별자는 제1 개인과 연관되며, 제1 개인은 이전에 확인된 개인 신원을 가짐 -; 블록 체인에 대한 확인 주소들을 개인들에게 할당하는 것 - 특정 확인 주소는 공개 키 및 개인 키를 포함하며, 제1 확인 주소는 제1 개인에게 할당되며, 제1 확인 주소는 제1 공개 키 및 제1 개인 키를 포함함 -; 및 개인들과 연관된 식별자들 및 생체인증 데이터를 대응하는 확인 주소들에 기록하는 것-, 제1 개인과 연관된 제1 식별자 및 제1 생체인증 데이터는 제1 확인 주소에 기록됨-을 포함할 수 있다. 확인 주소들을 사용하여 블록 체인-기반 멀티팩터 개인 신원 확인을 수행하는 것은 하나 이상의 개인들의 신원을 확인하기 위한 하나 이상의 요청들과 관련한 하나 이상의 식별자들을 수신하는 것 - 제1 식별자는 제1 개인의 신원을 확인하기 위한 요청과 관련하여 수신됨 -; 하나 이상의 개인들과 연관된 생체인증 데이터를 대응하는 확인 주소들로부터 추출하는 것 - 제1 개인과 연관된 제1 생체인증 데이터는 제1 확인 주소로부터 추출됨 -; 및 매칭하는 생체인증 데이터 및 개인 키들을 수신할 때 하나 이상의 개인들의 신원을 확인하는 것-, 제1 개인의 개인 신원은 (1) 제1 생체인증 데이터와 매칭하는 생체인증 데이터 및 (2) 제1 개인 키와 매칭하는 개인 키의 수신시 확인됨-을 포함할 수 있다.

[0003] 본 개시내용의 다른 태양은 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하기 위해 블록 체인 상에 확인 주소들을 설정하기 위한 방법에 관한 것이다. 본 방법은 기계-판독가능 명령들로 구성된 하나 이상의 하드웨어 프로세서들에 의해 수행될 수 있다. 본 방법은 식별자들을 이전에 확인된 개인 신원들을 갖는 개인들과 연관시키는 단계 - 제1 식별자는 제1 개인과 연관되며, 제1 개인은 이전에 확인된 개인 신원을 가짐 -; 블록 체인 상에 확인 주소들을 개인들에게 할당하는 단계 - 특정 확인 주소는 공개 키 및 개인 키를 포함하며, 제1 확인 주소는 제1 개인에게 할당되며 제1 확인 주소는 제1 공개 키 및 제1 개인 키를 포함함 -; 및 개인들과 연관된 식별자들 및 생체인증 데이터를 대응하는 확인 주소들에 기록하는 단계 - , 제1 개인과 연관된 제1 식별자 및 제1 생체인증 데이터는 제1 확인 주소에 기록됨-를 포함할 수 있다. 하나 이상의 개인들의 신원은, 제1 개인의 개인 신원이 (1) 제1 생체인증 데이터와 매칭하는 생체인증 데이터 및 (2) 제1 개인 키와 매칭하는 개인 키의 수신시에 확인 가능하도록, 서로 매칭하는 생체인증 데이터 및 개인 키들을 수신할 때 확인가능할 수 있다.

[0004] 본 개시내용의 또 다른 태양은 확인 주소들을 사용하여 블록 체인-기반 멀티팩터 개인 신원 확인을 수행하기 위한 방법에 관한 것이다. 본 방법은 기계-판독가능 명령들로 구성된 하나 이상의 하드웨어 프로세서들에 의해 수행될 수 있다. 본 방법은 하나 이상의 개인들의 신원을 확인하기 위한 하나 이상의 요청들과 관련한 하나 이상의 식별자들을 수신하는 단계 - 제1 식별자는 제1 개인의 신원을 확인하기 위한 요청과 관련하여 수신됨 -; 하나 이상의 개인들과 연관된 생체인증 데이터를 블록 체인 상에 대응하는 확인 주소들로부터 추출하는 단계 - 특정 확인 주소는 공개 키 및 개인 키를 포함하며, 제1 개인과 연관된 제1 생체인증 데이터는 제1 개인에게 할당된 제1 확인 주소로부터 추출되며, 제1 확인 주소는 제1 공개 키 및 제1 개인 키를 포함함 -; 및 서로 매칭하는 생체인증 데이터 및 개인 키들을 수신할 때 하나 이상의 개인들의 신원을 확인하는 단계 -, 제1 개인의 개인 신원은 (1) 제1 생체인증 데이터와 매칭하는 생체인증 데이터 및 (2) 제1 개인 키와 매칭하는 개인 키의 수신시 확인됨 - 를 포함할 수 있다.

[0005] 본 기술의 이들 및 다른 특징들과 특성들뿐만 아니라 구성의 관련 엘리먼트들의 기능들 및 동작 방법들 및 제조 부품들의 조합과 제조 경제성들은 첨부 도면들을 참조로 하여 이하의 상세한 설명 및 첨부한 청구항들을 고려할 때 더 명백하게 될 것이며, 첨부 도면들 전부는 본 명세서의 일부분을 형성하며, 다양한 도면들에서 유사한 참

조부호들은 대응 부분들을 표시한다. 그러나, 도면들은 단지 예시 및 설명을 위한 것이며, 본 발명의 범위를 한정하는 것으로 의도되지 않는다는 것이 명백하게 이해될 것이다. 명세서 및 청구항들에서 사용되는 바와 같이, 단수 형태는 문맥이 달리 명확하게 표시하지 않는 한 복수의 지시대상들을 포함한다.

도면의 간단한 설명

- [0006] 도 1은 하나 이상의 실시예들에 따라, 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하기 위한 시스템을 도시한다.
- 도 2는 하나 이상의 실시예들에 따라, 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하기 위해 블록 체인 상에 확인 주소들을 설정하기 위한 방법을 도시한다.
- 도 3은 하나 이상의 실시예들에 따라, 확인 주소들을 사용하여 블록 체인-기반 멀티팩터 개인 신원 확인을 수행하기 위한 방법을 도시한다.

발명을 실시하기 위한 구체적인 내용

- [0007] 도 1은 하나 이상의 실시예들에 따라, 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하기 위한 시스템(100)을 도시한다. 일부 실시예들에서, 시스템(100)은 하나 이상의 서버들(102)을 포함할 수 있다. 서버(들)(102)는 클라이언트/서버 아키텍처, 피어-투-피어 아키텍처, 및/또는 다른 아키텍처들에 따라 하나 이상의 컴퓨팅 플랫폼들(104)과 통신하도록 구성될 수 있다. 사용자들은 컴퓨팅 플랫폼(들)(104)을 통해 시스템(100)에 액세스할 수 있다.
- [0008] 서버(들)(102)는 기계-판독가능 명령들(106)을 실행하도록 구성될 수 있다. 기계-판독가능 명령들(106)은 개인 식별자 컴포넌트(108), 확인 주소 할당 컴포넌트(110), 주소 기록 컴포넌트(112), 사용자 인터페이스 컴포넌트(114), 확인 요청 컴포넌트(116), 정보 추출 컴포넌트(118), 신원 확인 컴포넌트(120) 및/또는 다른 기계-판독가능 명령 컴포넌트들 중 하나 이상을 포함할 수 있다.
- [0009] 기계-판독가능 명령들(106)은 블록 체인 상에 확인 주소들을 설정하도록 실행 가능할 수 있다. 일반적으로 말하면, 블록 체인은 시스템(100)에 참여하는 일부 또는 모든 노드들에 의해 공유되는 트랜잭션 데이터베이스이다. 이러한 참여는 비트코인 프로토콜, 이더리움 프로토콜, 및/또는 디지털 통화들 및/또는 블록 체인들과 관련된 다른 프로토콜들에 기반될 수 있다. 블록 체인의 전체 사본(copy)은 연관된 디지털 통화에서 지금까지 실행된 모든 트랜잭션을 포함한다. 트랜잭션들 외에도, 본원에서 추가로 설명되는 것과 같은 다른 정보가 블록 체인에 포함될 수 있다.
- [0010] 블록 체인은 여러 블록들에 기반할 수 있다. 블록은 하나 이상의 대기 트랜잭션들을 포함하고 검증하는 레코드를 포함할 수 있다. 주기적으로 (예컨대, 대략 1 분마다), 트랜잭션들 및/또는 다른 정보를 포함하는 새로운 블록이 블록 체인에 첨부(append)될 수 있다. 일부 실시예들에서, 블록 체인 내에 특정 블록은 이전 블록의 해시(hash)를 포함한다. 이는 기원(genesis) 블록(즉, 블록 체인의 첫 번째 블록)으로부터 현재 블록까지 블록들의 체인을 생성하는 효과를 가질 수 있다. 특정 블록은 시간적으로 이전 블록 이후에 나오도록 보장될 수 있는데, 왜냐하면 이전 블록의 해시가 달리 알려지지 않을 것이기 때문이다. 특정 블록은 일단 그 특정 블록이 블록 체인에 포함되면 수정하기가 계산상 비현실적일 수 있는데, 왜냐하면 블록 체인에 포함된 이후 모든 블록이 또한 재생성되어야 하기 때문이다.
- [0011] 특정 확인 주소는 특정 정보가 저장되는 블록 체인의 특정 위치를 포함할 수 있다. 일부 실시예들에서, 개인 확인 주소는 "AtenVerify Address"로 지칭될 수 있다. 확인 주소들은 확인 주소 할당 컴포넌트(110)와 관련하여 이하에서 추가로 설명된다.
- [0012] 개인 식별자 컴포넌트(108)는 식별자들을 이전에 확인된 개인 신원들을 갖는 개인들과 연관시키도록 구성될 수 있다. 예컨대, 제1 식별자는 제1 개인과 연관될 수 있다. 제1 개인은 이전에 확인된 개인 신원을 가질 수 있다. 일반적으로 말하면, 식별자는 숫자, 영숫자 코드, 사용자이름, 및/또는 개인에 링크될 수 있는 다른 정보 중 하나 이상을 포함할 수 있다. 일부 실시예들에서, 개인 식별자는 "Aten ID"로 지칭될 수 있다.
- [0013] 일부 실시예들에 따라, 이전에 확인된 개인 신원을 가진 개인은 다양한 접근법들을 통해 이전에 확인된 개인 신원을 획득했을 수도 있다. 예컨대, 일부 실시예들에서, 개인은 개인의 신원에 대한 증거를 제공하도록 요구받을 수 있다. 그러한 증거는 정부 발급 신분증(예컨대, 여권 및/또는 운전 면허증)의 사본을 제공하는 것, 개인이 수령한 우편물(예컨대, 공공 요금)의 사본을 제공하는 것, 제3 자가 제공한 증거를 제공하는 것, 및/또는 개

인의 신원에 관한 다른 증거를 제공하는 것 중 하나 이상을 포함할 수 있다. 증거는 서버(들)(102)와 연관된 엔터티에 제공될 수 있다.

- [0014] 확인 주소 할당 컴포넌트(110)는 블록 체인 상에 확인 주소들을 개인들에게 할당하도록 구성될 수 있다. 특정 확인 주소는 공개 키 및 개인 키를 포함할 수 있다. 예로서, 제1 확인 주소가 제1 개인에게 할당될 수 있다. 제1 확인 주소는 제1 공개 키 및 제1 개인 키를 포함할 수 있다.
- [0015] 일반적으로 말하면, 공개 및 개인 키 쌍은 하나 이상의 공개 키 알고리즘들에 따라 암호화 및 복호화에 사용될 수 있다. 비-제한적인 예로서, 디지털 서명들을 위해 키 쌍이 사용될 수 있다. 그러한 키 쌍은 서명을 위한 개인 키 및 확인을 위한 공개 키를 포함할 수 있다. 공개 키는 널리 배포될 수 있는 반면에, 개인 키는 비밀로 유지된다(예컨대, 그 개인 키의 소유자에게만 알려짐). 키들은 수학적으로 관련될 수 있지만, 공개 키로부터 개인 키를 계산하는 것은 불가능하다.
- [0016] 일부 실시예들에서, 확인 주소 할당 컴포넌트(110)는 개인 키들이 컴퓨팅 플랫폼(들)(104) 내에 저장될 수 있도록 구성될 수 있다. 예컨대, 제1 개인 키는 컴퓨팅 플랫폼(104) 및/또는 제1 개인과 연관된 다른 위치들 내에 저장될 수 있다. 일부 실시예에 따르면, 개인 키는 "verify.dat" 파일, SIM 카드 및/또는 다른 위치들 중 하나 이상에 저장될 수 있다.
- [0017] 일부 실시예들에서, 확인 주소 할당 컴포넌트(110)는 다수의 확인 주소들이 개별 개인들에게 할당될 수 있도록 구성될 수 있다. 예컨대, 제1 확인 주소 외에도, 제2 확인 주소가 제1 개인에게 할당될 수 있다. 하나 이상의 실시예들에 따라, 하나 이상의 부가적인 확인 주소들이 제1 개인에게 할당될 수 있다.
- [0018] 주소 기록 컴포넌트(112)는 개인들과 연관된 식별자들 및 생체인증 데이터를 대응하는 확인 주소들에 기록하도록 구성될 수 있다. 예컨대, 제1 개인과 연관된 제1 식별자 및 제1 생체인증 데이터는 제1 확인 주소에 기록될 수 있다. 특정 확인 주소에 정보를 기록하는 것은 정보의 해시 또는 다른 암호화된 표현을 기록하는 것을 포함할 수 있다. 일부 실시예들에서, 상이한 생체인증 데이터는 특정 단 한명의 개인에 할당된 다수의 확인 주소들에 기록될 수 있다. 예컨대, 제1 개인과 연관된 제1 식별자 및 제1 생체인증 데이터가 제1 확인 주소에 기록되는 것 외에도, 제1 개인과 연관된 제1 식별자 및 제2 생체인증 데이터는 제2 확인 주소에 기록될 수 있다.
- [0019] 일반적으로 말하면, 생체인증 데이터는 인간의 특성들과 관련된 메트릭들을 포함할 수 있다. 생체인증 식별자들은 개인들을 라벨링(labeling)하고 설명하기 위하여 사용할 수 있는 구별 가능하고 측정 가능한 특성들이다. 생체인증 식별자들은 전형적으로 생리학적 특성들을 포함하지만, 행동 특성들 및/또는 다른 특성들을 또한 포함할 수 있다. 생리학적 특성들은 개인의 신체의 형상과 관련될 수 있다. 생체인증 데이터로서 사용되는 생리학적 특성들의 예들은 지문, 손바닥 정맥들, 얼굴 인식, DNA, 장문(palm print), 손 모양(hand geometry), 홍채 인식, 망막, 냄새(odor) 또는 향기(scent), 및/또는 다른 생리학적 특성들 중 하나 이상을 포함할 수 있다. 행동 특성들은 개인의 행동 패턴과 관련될 수 있다. 생체인증 데이터로서 사용되는 행동 특성들의 예들은 타이핑 리듬(typing rhythm), 걸음걸이, 음성 및/또는 다른 행동 특성들 중 하나 이상을 포함할 수 있다.
- [0020] 생체인증 데이터는 생리학적 특성의 이미지 또는 다른 시각적 표현, 행동 특성의 기록, 생리학적 특성 및/또는 행동 특성의 템플릿(template) 및/또는 다른 생체인증 데이터의 하나 이상을 포함할 수 있다. 템플릿은 소스로부터 추출된 관련 특징들의 합성을 포함할 수 있다. 템플릿은 생리학적 특성 및/또는 행동 특성의 특징들을 설명하는 벡터, 생리학적 특성 및/또는 행동 특성의 수치 표현, 특정 특성들을 갖는 이미지 및/또는 다른 정보 중 하나 이상을 포함할 수 있다.
- [0021] 생체인증 데이터는 개인들과 연관된 컴퓨팅 플랫폼들(104)을 통해 수신될 수 있다. 예컨대, 제1 개인과 연관된 생체인증 데이터는 제1 개인과 연관된 제1 컴퓨팅 플랫폼(104)을 통해 수신될 수 있다. 제1 컴퓨팅 플랫폼(104)은 제1 개인의 생리학적 특성 및/또는 행동 특성을 캡처 및/또는 기록하도록 구성된 입력 디바이스(도시 안됨)를 포함할 수 있다. 이러한 입력 디바이스의 예들은 카메라 및/또는 다른 이미징 디바이스, 지문 스캐너, 마이크로폰, 가속도계, 및/또는 다른 입력 디바이스들 중 하나 이상을 포함할 수 있다.
- [0022] 사용자 인터페이스 컴포넌트(114)는 연관된 컴퓨팅 플랫폼(104)을 통해 개인들에게 프리젠테이션(presentation)을 위한 인터페이스를 제공하도록 구성될 수 있다. 인터페이스는 개인 컴퓨팅 플랫폼들(104)을 통해 제시되는 그래픽 사용자 인터페이스를 포함할 수 있다. 일부 실시예들에 따르면, 인터페이스는 적어도 하나의 확인 주소가 특정 개인에게 할당되기만 하면 그 특정 개인이 그 특정 개인에게 할당된 확인 주소들을 추가하거나 제거할 수 있게 하도록 구성될 수 있다.
- [0023] 일부 실시예들에서, 사용자 인터페이스 컴포넌트(114)는 시스템(100)의 사용자들과 연관된 하나 이상의 사용자

프로필들 및/또는 사용자 정보에 액세스하고 그리고/또는 이를 관리하도록 구성될 수 있다. 하나 이상의 사용자 프로필들 및/또는 사용자 정보는 서버(들)(102), 컴퓨팅 플랫폼(들)(104) 중 하나 이상, 및/또는 다른 저장 위치들에 의해 저장된 정보를 포함할 수 있다. 사용자 프로필들은 예컨대 사용자를 식별하는 정보(예컨대, 사용자 이름 또는 핸들(handle), 번호, 식별자 및/또는 다른 식별 정보), 보안 로그인 정보(예컨대, 로그인 코드 또는 패스워드), 시스템 계정 정보, 가입 정보, (예컨대, 사용자에 대한 크레딧으로 보유되는 통화와 관련된) 디지털 통화 계좌 정보, 관계 정보(예컨대, 시스템(100)의 사용자들간의 관계들에 관련된 정보), 시스템 사용 정보, 사용자들과 연관된 인구통계학적 정보, 시스템(100)의 사용자들간의 상호작용 이력, 사용자들에 의해 서술된 정보, 사용자들의 구매 정보, 사용자들의 브라우징 이력, 사용자와 연관된 컴퓨팅 플랫폼 식별, 사용자와 연관된 전화 번호, 및/또는 사용자들과 관련된 다른 정보를 포함할 수 있다.

[0024] 기계-판독가능 명령들(106)은 확인 주소들을 사용하여 블록 체인-기반 멀티팩터 개인 신원 확인을 수행하도록 실행가능할 수 있다.

[0025] 확인 요청 컴포넌트(116)는 하나 이상의 개인들의 신원을 확인하기 위한 하나 이상의 요청들과 관련한 하나 이상의 식별자들을 수신하도록 구성될 수 있다. 예컨대, 제1 식별자는 제1 개인의 신원을 확인하기 위한 요청과 관련하여 수신될 수 있다. 신원 확인을 위한 요청들은 금융 거래들, 정보 교환들 및/또는 다른 상호작용들과 관련하여 제공될 수 있으며 그리고/또는 이들과 관련될 수 있다. 요청들은 다른 개인들 및/또는 다른 제3 자들로부터 수신될 수 있다.

[0026] 정보 추출 컴포넌트(118)는 하나 이상의 개인들과 연관된 생체인증 데이터를 대응하는 확인 주소들로부터 추출하도록 구성될 수 있다. 예컨대, 제1 개인과 연관된 제1 생체인증 데이터는 제1 확인 주소로부터 추출될 수 있다. 확인 주소로부터 정보(예컨대, 생체인증 데이터)를 추출하는 것은 정보를 복호화하는 것을 포함할 수 있다.

[0027] 일부 실시예들에 따르면, 정보 추출 컴포넌트(118)는, 제1 개인의 신원을 확인하기 위한 요청을 수신한 것에 대응하여, 제1 생체인증 데이터와 매칭하는 생체인증 데이터 및 제1 개인 키와 매칭하는 개인 키에 대한 프롬프트(prompt)가 제1 개인에 제공될 수 있도록 구성될 수 있다. 프롬프트는 제1 개인과 연관된 컴퓨팅 플랫폼(104)을 통해 전달될 수 있다. 프롬프트는 그래픽 사용자 인터페이스 및/또는 제1 개인과 연관된 컴퓨팅 플랫폼(104)에 의해 제공되는 다른 사용자 인터페이스를 통해 전달될 수 있다. 프롬프트는 시각적, 청각적, 촉각적 및/또는 다른 표시(indicating)들 중 하나 이상인 표시를 포함할 수 있다.

[0028] 일부 실시예들에서, 정보 추출 컴포넌트(118)는 제1 개인의 신원을 확인하기 위한 요청을 수신하는 것에 대응하여, 제1 개인과 연관된 컴퓨팅 플랫폼(104)에 프롬프트가 제공될 수 있도록 구성될 수 있다. 프롬프트는 컴퓨팅 플랫폼(104)이 제1 생체인증 데이터와 매칭하는 생체인증 데이터 및/또는 제1 개인 키와 매칭하는 개인 키를 서버(102)에 자동으로 제공하게 할 수 있다.

[0029] 신원 확인 컴포넌트(120)는 서로 매칭하는 생체인증 데이터 및 개인 키들을 수신할 때 또는 이 수신에 대응하여 하나 이상의 개인들의 신원을 확인하도록 구성될 수 있다. 예컨대, 제1 개인의 개인 신원은 (1) 제1 생체인증 데이터와 매칭하는 생체인증 데이터 및 (2) 제1 개인 키와 매칭하는 개인 키의 수신 시 확인될 수 있다. 제1 개인의 개인 신원을 확인하는 것은 저장된 정보를 새로이 수신된 정보와 비교하는 것을 포함할 수 있다.

[0030] 일부 실시예들에 따르면, 신원 확인 컴포넌트(120)는 제1 개인의 개인 신원이 (1) 제1 생체인증 데이터 또는 제2 생체인증 데이터와 매칭하는 생체인증 데이터 및 (2) 제1 개인 키와 매칭하는 개인 키의 수신시에 확인될 수 있도록 구성될 수 있다. 이러한 실시예들은 식별 정보의 더 큰 세트의 일부 서브세트가 요구되는 신원 확인을 위한 소위 "M-오브-N (M-of-N)" 서명들을 제공할 수 있다.

[0031] 일부 실시예들에서, 신원 확인 컴포넌트(120)는 제1 생체인증 데이터와 매칭하는 생체인증 데이터 및 제1 개인 키와 매칭하는 개인 키가 제1 개인의 개인 신원의 확인을 서명하는데 사용될 수 있도록 구성될 수 있다.

[0032] 암호화 서명은 누군가가 소유권을 증명할 수 있게 해주는 수학적 메커니즘이다. 비트코인의 경우, 비트코인 지갑과 이의 개인 키(들)는 일부 수학적 매직(mathematical magic)에 의해 링크된다. 당신의 비트코인 소프트웨어가 적절한 개인 키를 사용하여 트랜잭션을 서명할 때, 전체 네트워크는 서명이 소비되고 있는 비트코인들과 매칭하는 것을 알 수 있다. 그러나, 일반 세상 사람들이 당신의 개인 키를 추측하여 당신이 애써서 얻은 비트코인들을 훔칠 수 있는 방법은 없다.

[0033] 일부 실시예들에서, 적어도 하나의 전용 노드는 제1 개인의 개인 신원의 확인을 위한 서명을 수행한다. 특정 전용 노드는 서버(들)(102) 중 하나 이상을 포함할 수 있다. 특정 전용 노드는 새로운 블록들을 생성하기 위해

그리고/또는 확인을 서명하기 위해 구성된 공개 노드(public node) 또는 개인 노드(private node)일 수 있다.

[0034] 일부 실시예들에서, 서버(들)(102), 컴퓨팅 플랫폼(들)(104) 및/또는 외부 자원들(122)은 하나 이상의 전자 통신 링크들을 통해 동작 가능하게 링크될 수 있다. 예컨대, 그러한 전자 통신 링크들은 적어도 부분적으로 인터넷 및/또는 다른 네트워크들과 같은 네트워크를 통해 확립될 수 있다. 이는 제한하는 것으로 의도되지 않고, 본 개시내용의 범위는 서버(들)(102), 컴퓨팅 플랫폼(들)(104) 및/또는 외부 자원들(122)이 일부 다른 통신 매체를 통해 동작 가능하게 링크될 수 있는 실시예들을 포함한다는 것이 인식될 것이다.

[0035] 특정 컴퓨팅 플랫폼(104)은 기계-판독가능 명령들을 실행하도록 구성된 하나 이상의 프로세서들을 포함할 수 있다. 기계-판독가능 명령들은 특정 컴퓨팅 플랫폼(104)과 연관된 전문가 또는 사용자가 시스템(100) 및/또는 외부 자원들(122)과 인터페이싱하고 그리고/또는 본원에서 컴퓨팅 플랫폼(들)(104)에 기인한 다른 기능을 제공하는 것을 가능하게 하도록 구성될 수 있다. 비-제한적인 예로서, 특정 컴퓨팅 플랫폼(104)은 데스크톱 컴퓨터, 랩톱 컴퓨터, 핸드헬드 컴퓨터, 태블릿 컴퓨팅 플랫폼, 넷북, 스마트폰, 게임 콘솔 및/또는 다른 컴퓨팅 플랫폼들 중 하나 이상을 포함할 수 있다.

[0036] 외부 자원들(122)은 정보 소스들, 시스템(100) 외부의 가상 환경들의 호스트들 및/또는 제공자들, 시스템(100)에 참여하는 외부 엔티티들 및/또는 다른 자원들을 포함할 수 있다. 일부 실시예들에서, 본원에서 외부 자원들(100)에 기인한 기능의 일부 또는 전부가 시스템(100)에 포함된 자원들에 의해 제공될 수 있다.

[0037] 서버(들)(102)는 전자 스토리지(124), 하나 이상의 프로세서들(126) 및/또는 다른 컴포넌트들을 포함할 수 있다. 서버(들)(102)는 네트워크 및/또는 다른 컴퓨팅 플랫폼들과의 정보의 교환을 가능하게 하는 포트들 또는 통신 라인들을 포함할 수 있다. 도 1의 서버(들)(102)의 예시는 제한하는 것으로 의도되지 않는다. 서버(들)(102)는 본원에서 서버(들)(102)에 기인한 기능을 제공하기 위하여 함께 동작하는 복수의 하드웨어, 소프트웨어 및/또는 펌웨어 컴포넌트를 포함할 수 있다. 예컨대, 서버(들)(102)는 서버(들)(102)로서 함께 동작하는 컴퓨팅 플랫폼들의 클라우드에 의해 구현될 수 있다.

[0038] 전자 스토리지(124)는 정보를 전자적으로 저장하는 비-일시적 저장 매체를 포함할 수 있다. 전자 스토리지(124)의 전자 저장 매체는 서버(들)(102)에 일체형으로 (즉, 실질적으로 제거 가능하지 않게) 제공되는 시스템 스토리지 및/또는 예컨대 포트(예컨대, USB 포트, 파이어와이어 포트 등) 또는 드라이브(예컨대, 디스크 드라이브 등)를 통해 서버(들)(102)에 제거 가능하게 연결될 수 있는 제거가능 스토리지 중 하나 또는 둘 모두를 포함할 수 있다. 전자 스토리지(124)는 광학적으로 판독가능한 저장 매체 (예컨대, 광학 디스크들 등), 자기적으로 판독가능한 저장 매체 (예컨대, 자기 테이프, 자기 하드 드라이브, 플로피 드라이브 등), 전하-기반 저장 매체 (예컨대, EEPROM, RAM 등), 고체-상태 저장 매체(예컨대, 플래시 드라이브 등), 및/또는 전자적으로 판독가능한 다른 저장 매체 중 하나 이상을 포함할 수 있다. 전자 스토리지(124)는 하나 이상의 가상 저장 자원들(예컨대, 클라우드 스토리지, 가상 사설망 및/또는 다른 가상 저장 자원들)을 포함할 수 있다. 전자 스토리지(124)는 소프트웨어 알고리즘들, 프로세서(들)(126)에 의해 결정된 정보, 서버(들)(102)로부터 수신된 정보, 컴퓨팅 플랫폼(들)(104)으로부터 수신된 정보, 및/또는 서버(들)(102)가 본원에서 설명된 바와 같은 기능을 하는 것을 가능하게 하는 다른 정보를 저장할 수 있다.

[0039] 프로세서(들)(126)는 서버(들)(102)에 정보 프로세싱 능력들을 제공하도록 구성될 수 있다. 따라서, 프로세서(들)(126)는 디지털 프로세서, 아날로그 프로세서, 정보를 프로세싱하도록 설계된 디지털 회로, 정보를 프로세싱하도록 설계된 아날로그 회로, 상태 기계(state machine) 및/또는 정보를 전자적으로 프로세싱하기 위한 다른 메커니즘들 중 하나 이상을 포함할 수 있다. 비록 프로세서(들)(126)가 단일 엔티티로서 도 1에 도시될지라도, 이는 단지 예시를 위한 것일 뿐이다. 일부 실시예들에서, 프로세서(들)(126)는 복수의 프로세싱 유닛들을 포함할 수 있다. 이러한 프로세싱 유닛들은 동일한 디바이스 내에 물리적으로 위치할 수 있거나, 또는 프로세서(들)(126)는 합동하여 동작하는 복수의 디바이스들의 프로세싱 기능을 나타낼 수 있다. 프로세서(들)(126)는 기계-판독가능 명령 컴포넌트들(108, 110, 112, 114, 116, 118, 120) 및/또는 다른 기계-판독가능 명령 컴포넌트들을 실행하도록 구성될 수 있다. 프로세서(들)(126)는 소프트웨어; 하드웨어; 펌웨어; 소프트웨어, 하드웨어 및/또는 펌웨어의 일부 조합; 및/또는 프로세서(들)(126)상에서의 프로세싱 능력들을 구성하기 위한 다른 메커니즘들에 의해, 기계-판독가능 명령 컴포넌트(108, 110, 112, 114, 116, 118, 120) 및/또는 다른 기계-판독가능 명령 컴포넌트들을 실행하도록 구성될 수 있다. 본원에서 사용되는 바와 같이, "기계-판독가능 명령 컴포넌트"라는 용어는 기계-판독가능 명령 컴포넌트에 기인한 기능을 수행하는 임의의 컴포넌트 또는 컴포넌트들의 세트를 지칭할 수 있다. 이는 프로세서 판독가능 명령들, 프로세서 판독가능 명령들, 회로, 하드웨어, 저장 매체 또는 임의의 다른 컴포넌트들의 실행동안 하나 이상의 물리적 프로세서들을 포함할 수 있

다.

- [0040] 비록 기계-판독가능 명령 컴포넌트들(108, 110, 112, 114, 116, 118 및 120)이 단일 프로세싱 유닛 내에서 구현되는 것으로 도 1에 도시될지라도, 프로세서(들)(126)가 다수의 프로세싱 유닛들을 포함하는 실시예들에서, 기계-판독가능 명령 컴포넌트들(108, 110, 112, 114, 116, 118 및/또는 120) 중 하나 이상은 다른 기계-판독가능 명령 컴포넌트들로부터 원격으로 구현될 수 있다는 것이 인식되어야 한다. 이하에서 설명되는 상이한 기계-판독가능 명령 컴포넌트들(108, 110, 112, 114, 116, 118 및/또는 120)에 의해 제공되는 기능의 설명은 예시를 위한 것이며 제한하는 것으로 의도되지 않는데, 왜냐하면 기계-판독가능 명령 컴포넌트들(108, 110, 112, 114, 116, 118 및/또는 120) 중 임의의 컴포넌트가 설명된 것보다 더 많거나 또는 더 적은 기능을 제공할 수 있기 때문이다. 예컨대, 기계-판독가능 명령 컴포넌트들(108, 110, 112, 114, 116, 118 및/또는 120) 중 하나 이상은 제거될 수 있고, 그 기능의 일부 또는 전부는 기계-판독가능 명령 컴포넌트들(108, 110, 112, 114, 116, 118 및/또는 120) 중 다른 컴포넌트들에 의해 제공될 수 있다. 다른 예로서, 프로세서(들)(126)는 하기의 기계-판독가능 명령 컴포넌트들(108, 110, 112, 114, 116, 118 및/또는 120) 중 하나에 기인한 기능 중 일부 또는 전부를 수행할 수 있는 하나 이상의 부가적인 기계-판독가능 명령 컴포넌트들을 실행하도록 구성될 수 있다.
- [0041] 도 2는 하나 이상의 실시예들에 따라, 블록 체인-기반 멀티팩터 개인 신원 확인을 제공하기 위해 블록 체인 상에 확인 주소들을 설정하기 위한 방법(200)을 도시한다. 이하에서 제시되는 방법(200)의 동작들은 예시적인 것으로 의도된다. 일부 실시예들에서, 방법(200)은 논의된 동작들 중 하나 이상의 동작 없이 그리고/또는 설명되지 않은 하나 이상의 부가적인 동작들을 사용하여 달성될 수 있다. 부가적으로, 도 2에 도시되고 이하에서 설명되는 방법(200)의 동작들의 순서는 제한하는 것으로 의도되지 않는다.
- [0042] 일부 실시예들에서, 방법(200)의 하나 이상의 동작들은 하나 이상의 프로세싱 디바이스들(예컨대, 디지털 프로세서, 아날로그 프로세서, 정보를 프로세싱하도록 설계된 디지털 회로, 정보를 프로세싱하도록 설계된 아날로그 회로, 상태 기계, 및/또는 정보를 전자적으로 프로세싱하기 위한 다른 메커니즘들)로 구현될 수 있다. 하나 이상의 프로세싱 디바이스들은 전자 저장 매체 상에 전자적으로 저장된 명령들에 대응하여 방법(200)의 동작들의 일부 또는 전부를 실행하는 하나 이상의 디바이스들을 포함할 수 있다. 하나 이상의 프로세싱 디바이스들은 방법(200)의 동작들 중 하나 이상의 동작들의 실행을 위해 특별히 설계되도록 하드웨어, 펌웨어 및/또는 소프트웨어를 통해 구성된 하나 이상의 디바이스들을 포함할 수 있다.
- [0043] 동작(202)에서, 식별자들은 이전에 확인된 개인 신원들을 갖는 개인들과 연관될 수 있다. 제1 식별자는 제1 개인과 연관될 수 있다. 제1 개인은 이전에 확인된 개인 신원을 가질 수 있다. 동작(202)은 하나 이상의 실시예들에 따라 (도 1과 관련하여 설명된 바와 같이) 개인 식별자 컴포넌트(108)와 동일하거나 유사한 기계-판독가능 명령 컴포넌트를 실행하도록 구성된 하나 이상의 하드웨어 프로세서들에 의해 수행될 수 있다.
- [0044] 동작(204)에서, 블록 체인 상에 확인 주소들이 개인들에게 할당될 수 있다. 특정 확인 주소는 공개 키 및 개인 키를 포함할 수 있다. 제1 확인 주소는 제1 개인에게 할당될 수 있다. 제1 확인 주소는 제1 공개 키 및 제1 개인 키를 포함할 수 있다. 동작(204)은 하나 이상의 실시예들에 따라 (도 1과 관련하여 설명된 바와 같이) 확인 주소 할당 컴포넌트(110)와 동일하거나 유사한 기계-판독가능 명령 컴포넌트를 실행하도록 구성된 하나 이상의 하드웨어 프로세서에 의해 수행될 수 있다.
- [0045] 동작(206)에서, 개인들과 연관된 식별자들 및 생체인증 데이터는 대응하는 확인 주소들에 기록될 수 있다. 제1 개인과 연관된 제1 식별자 및 제1 생체인증 데이터는 제1 확인 주소에 기록될 수 있다. 하나 이상의 개인들의 신원은 서로 매칭하는 생체인증 데이터 및 개인 키들의 수신시 또는 이에 대응하여 확인 가능할 수 있다. 제1 개인의 개인 신원은 (1) 제1 생체인증 데이터와 매칭하는 생체인증 데이터 및 (2) 제1 개인 키와 매칭하는 개인 키의 수신시 또는 이에 대응하여 확인 가능할 수 있다. 동작(206)은 하나 이상의 실시예들에 따라 (도 1과 관련하여 설명된 바와 같이) 주소 기록 컴포넌트(112)와 동일하거나 유사한 기계-판독가능 명령 컴포넌트를 실행하도록 구성된 하나 이상의 하드웨어 프로세서들에 의해 수행될 수 있다.
- [0046] 도 3은 하나 이상의 실시예들에 따라, 확인 주소들을 사용하여 블록 체인-기반 멀티팩터 개인 신원 확인을 수행하기 위한 방법(300)을 예시한다. 이하 제시되는 방법(300)의 동작들은 예시적인 것으로 의도된다. 일부 실시예들에서, 방법(300)은 논의된 동작들 중 하나 이상의 동작들 없이 그리고/또는 설명되지 않은 하나 이상의 부가적인 동작들을 사용하여 달성될 수 있다. 부가적으로, 도 3에 예시되고 이하에서 설명된 방법(300)의 동작들의 순서는 제한하는 것으로 의도되지 않는다.
- [0047] 일부 실시예들에서, 방법(300)은 하나 이상의 프로세싱 디바이스들(예컨대, 디지털 프로세서, 아날로그 프로세서,

서, 정보를 프로세싱하도록 설계된 디지털 회로, 정보를 프로세싱하도록 설계된 아날로그 회로, 상태 기계 및/또는 정보를 전자적으로 프로세싱하기 위한 메커니즘들)로 구현될 수 있다. 하나 이상의 프로세싱 디바이스들은 전자 저장 매체 상에 전자적으로 저장된 명령들에 대응하여 방법(300)의 동작들 중 일부 또는 전부를 실행하는 하나 이상의 디바이스들을 포함할 수 있다. 하나 이상의 프로세싱 디바이스들은 방법(300)의 동작들 중 하나 이상의 동작의 실행을 위해 특별히 설계되도록 하드웨어, 펌웨어 및/또는 소프트웨어를 통해 구성된 하나 이상의 디바이스들을 포함할 수 있다.

[0048] 동작(302)에서, 하나 이상의 식별자들은 하나 이상의 개인들의 신원을 확인하기 위한 하나 이상의 요청들과 관련하여 수신될 수 있다. 제1 개인의 신원을 확인하기 위한 요청과 관련하여 제1 식별자가 수신될 수 있다. 동작(302)은 하나 이상의 실시예들에 따라, (도 1과 관련하여 설명된 바와 같이) 확인 요청 컴포넌트(116)와 동일하거나 유사한 기계-판독가능 명령 컴포넌트를 실행하도록 구성된 하나 이상의 하드웨어 프로세서들에 의해 수행될 수 있다.

[0049] 동작(304)에서, 하나 이상의 개인들과 연관된 생체인증 데이터는 블록 체인에 대한 대응하는 확인 주소들로부터 추출될 수 있다. 특정 확인 주소는 공개 키 및 개인 키를 포함할 수 있다. 제1 개인과 연관된 제1 생체인증 데이터는 제1 개인에게 할당된 제1 확인 주소로부터 추출될 수 있다. 제1 확인 주소는 제1 공개 키 및 제1 개인 키를 포함할 수 있다. 동작(304)은 하나 이상의 실시예들에 따라, (도 1과 관련하여 설명된 바와 같이) 정보 추출 컴포넌트(118)와 동일하거나 유사한 기계-판독가능 명령 컴포넌트를 실행하도록 구성된 하나 이상의 하드웨어 프로세서들에 의해 수행될 수 있다.

[0050] 동작(306)에서, 하나 이상의 개인들의 신원은 서로 매칭하는 생체인증 데이터 및 개인 키들의 수신시 또는 이에 대응하여 확인될 수 있다. 제1 개인의 개인 신원은 (1) 제1 생체인증 데이터와 매칭하는 생체인증 데이터 및 (2) 제1 개인 키와 매칭하는 개인 키의 수신시 또는 이에 대응하여 확인될 수 있다. 동작(306)은 하나 이상의 실시예들에 따라, (도 1과 관련하여 설명된 바와 같이) 신원 확인 컴포넌트(120)와 동일하거나 유사한 기계-판독가능 명령 컴포넌트를 실행하도록 구성된 하나 이상의 하드웨어 프로세서들에 의해 수행될 수 있다.

[0051] 예시적인 실시예들은 개인 데이터를 블록 체인에 저장하는 것을 용이하게 할 수 있다. 개인 데이터는 암호화된 방식으로 블록 체인에 저장될 수 있다. 사람은 개인 키, 지문, 지문 해시, 눈 망막, 눈 망막 해시 및/또는 다른 고유 정보 중 하나 이상으로 블록 체인 레벨에서 식별될 수 있다. 저장된 데이터는 여권, 신분증, 추출된 여권 정보, 운전 면허증, 추출된 운전 면허증 정보, 지문, 눈 망막 및/또는 다른 정보 중 하나 이상을 포함하거나 또는 이들과 관련될 수 있다. 일부 실시예들에 따르면, 만일 데이터의 일부가 변경되면, 블록 체인에서 그 사람에게 대한 새로운 레코드가 생성될 수 있다. 즉, 모든 변경들이 새로운 레코드들로서 추가된다. 이전 레코드는 항상 블록 체인에 저장될 것이다. 일반적으로 말하면, 블록 체인의 모든 레코드들은 영구히 저장되며 제거될 수 없다. 레코드들이 조작되지 않았다는 것을 보장하기 위하여 블록 체인의 1개 초과 사본이 존재할 것이다.

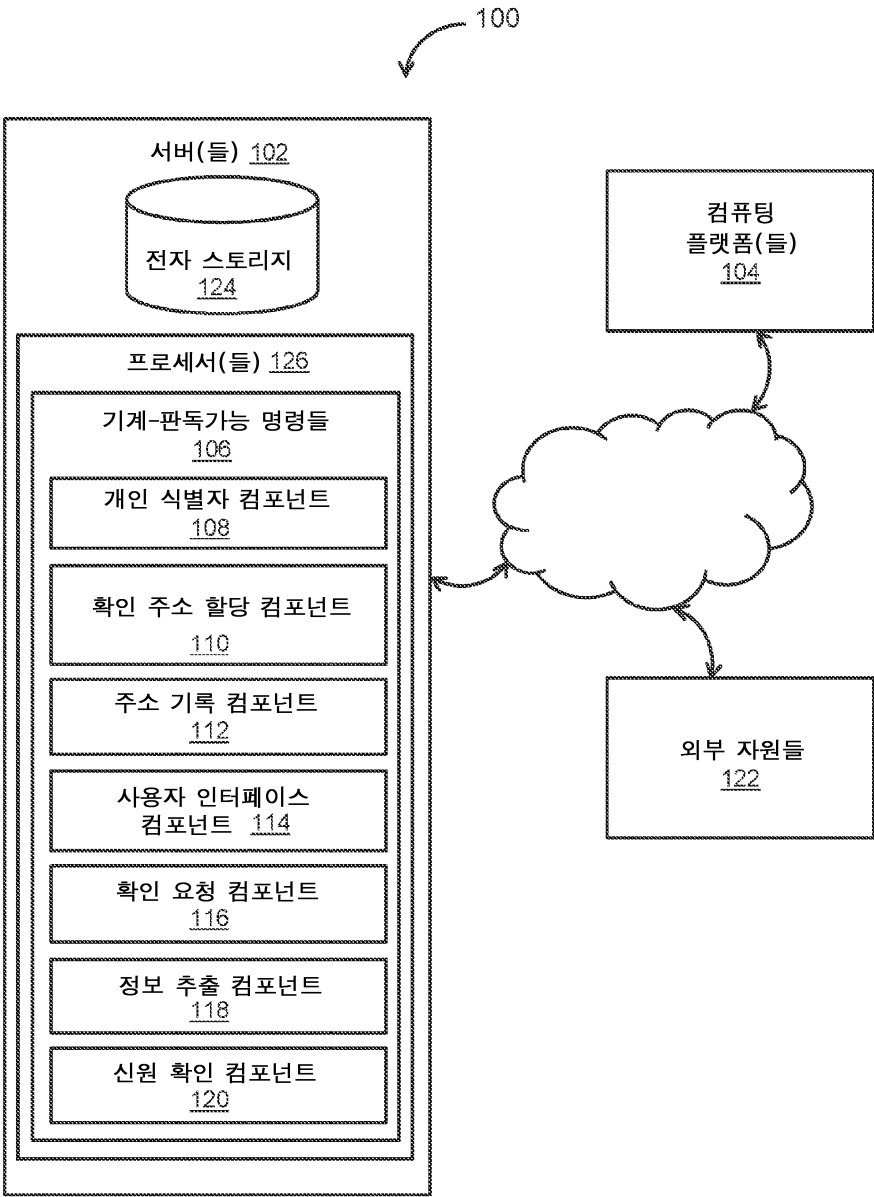
[0052] 예시적인 실시예들은 개인 데이터에 대한 액세스를 용이하게 할 수 있다. 블록 체인의 개인 데이터에 대해 다수의 액세스 레벨들이 존재할 수 있다. 액세스 제어는 공개/개인 키 쌍들의 레벨들에 대해 부여될 수 있다. 액세스 레벨들의 예들은 슈퍼 어드민(Super Admin)(블록 체인에 대한 전체 액세스), 권한-국가 레벨(전체 판독-전용 액세스), 권한-주/로컬 레벨(제한된 판독-전용 액세스), 비상사태를 포함하는 경찰 및 다른 서비스들(특정 개인 데이터에 대한 오직 그 사람의 지문/눈 망막에 의한 액세스), 참여 상인들(제한된 액세스), 및/또는 다른 액세스 레벨들 중 하나 이상을 포함할 수 있다.

[0053] 예시적인 실시예들은 확인 체크(check)를 용이하게 할 수 있다. 확인을 체크하는 것이 가능한 방법에 대해 다수의 레벨들이 존재할 수 있다. 예컨대, 일부 실시예들은 사람이 "회사"의 레코드를 가지나 개인 데이터가 제공되지 않도록 보장할 수 있다. 일부 실시예들은 사람이 회사의 레코드를 가지고 이름(full name), 생일(DOB), 성별, 및/또는 다른 기본 정보와 같은 매우 기본적인 개인 정보를 획득하도록 보장할 수 있다. 일부 실시예들은 사람이 회사의 레코드를 가지며 모든 개인 데이터를 획득하도록 보장할 수 있다.

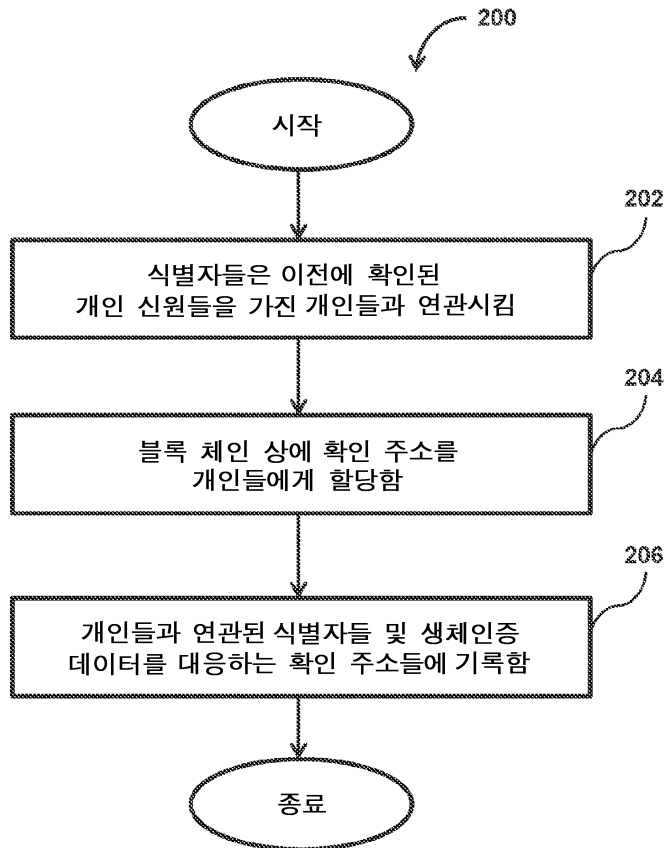
[0054] 비록 본 기술이 가장 실용적이고 바람직한 실시예들인 것으로 현재 고려되는 것에 기반하여 예시적인 목적으로 상세히 설명되었을지라도, 이러한 세부사항이 단지 그 목적을 위한 것이며 본 기술이 개시된 실시예들로 제한되는 것이 아니라 반대로 첨부된 청구항들의 사상 및 범위내에 있는 수정들 및 균등한 어레이지먼트(arrangement)들을 커버하는 것으로 의도된다는 것이 이해되어야 한다. 예컨대, 본 기술은, 가능한 범위까지, 임의의 실시예의 하나 이상의 특징들이 임의의 다른 실시예의 하나 이상의 실시예들과 결합될 수 있다는 것을 고려한다는 것이 이해되어야 한다.

도면

도면1



도면2



도면3

