(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0097773
(43) 공개일자 2020년08월19일

(51) 국제특허분류(Int. Cl.)
G06F 21/62 (2013.01) *G06F 21/64* (2013.01)
H04L 9/32 (2006.01) *H04W 12/02* (2009.01)
(52) CPC특허분류
G06F 21/6254 (2013.01)
G06F 21/64 (2013.01)
(21) 출원번호 10-2020-7020058
(22) 출원일자(국제) 2019년01월15일
심사청구일자 2020년07월10일
(85) 번역문제출일자 2020년07월10일
(86) 국제출원번호 PCT/EP2019/000014
(87) 국제공개번호 WO 2019/141505
국제공개일자 2019년07월25일
(30) 우선권주장
10 2018 000 471.7 2018년01월22일 독일(DE)

(71) 출원인
기제케 + 데브리엔트 모바일 서큐리티 게엠베하
독일 뮌헨 81677, 프린스레겐텐스트라세 159
(72) 발명자
캠, 프랭크 마이클
슈바르츠린스트라세. 3 83607 홀츠키르헨, 독일
(74) 대리인
김창덕

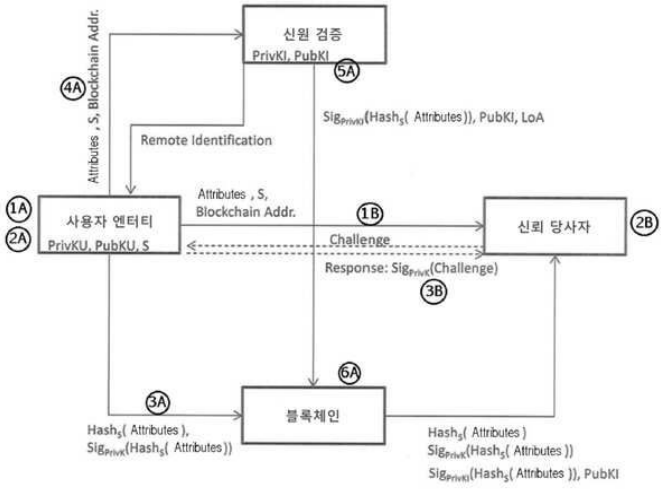
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 **블록체인 기반 신원 시스템**

(57) 요 약

본 발명은 전자 신원 기밀 검증, 소위 블록체인이 사용되는 방법에 관한 것이다. 제안된 방법은 액팅 파티가 블록체인 신원을 인식하는 동시에 각각의 신원 및 신원 속성들의 기밀성이 유지된다. 본 발명은 방법을 수행하거나 제안된 시스템 배열을 운영하는 제어 명령을 갖는 신원 시스템 및 컴퓨터 프로그램 제품을 더 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/3239 (2013.01)
H04L 9/3242 (2013.01)
H04L 9/3263 (2013.01)
H04L 9/3271 (2013.01)
H04W 12/02 (2019.01)
H04L 2209/38 (2013.01)

명 세 서

청구범위

청구항 1

암호화 체인 리스트를 사용하는 동안 신원을 기밀 검증하는 방법에 있어서,

사용자 엔터티에 의하여 대칭키 정보 아이템과 함께 상기 신원의 신원 속성들을 제공하는 단계;

상기 신원 속성이 알려져 있더라도 상기 신원을 추론할 수 없는 방식으로, 각각의 신원 속성에 대한 각각의 해시 값을 계산하는 단계;

적어도 하나의 리스트 엔트리로 상기 계산된 해시 값들을 상기 암호화 체인 리스트에 기록하는 단계;

상기 대칭키 정보 아이템과 함께 상기 적어도 하나의 리스트 엔트리의 어드레스를 상기 사용자 엔터티로부터 검증 엔터티로 전송하는 단계;

상기 신원 속성들을 갖는 신원 문서를 사용하는 동안, 상기 검증 엔터티에 의하여 상기 계산된 해시 값들을 갖는 상기 적어도 하나의 리스트 엔터리를 검증하고, 상기 어드레스에 공급되어 저장된 상기 신원 속성들이 상기 신원 문서의 상기 신원 속성들에 일치하는지 검증하는 단계; 및

상기 검증 엔터티에 의하여 상기 신원 속성들이 긍정적으로 검증되는 경우, 상기 적어도 하나의 리스트 엔트리의 서명을 상기 암호화 체인 리스트에 기록하는 단계를 포함하는 것을 특징으로 하는 신원을 기밀 검증하는 방법.

청구항 2

제 1 항에 있어서,

상기 적어도 하나의 리스트 엔트리의 어드레스, 대칭키 정보 아이템 및 상기 신원 속성들을 상기 사용자 엔트리로부터 상기 신원을 쿼리하는 쿼링 엔터티로 전송하는 단계; 및

상기 쿼링 엔터티는 전송된 데이터에 기초하여 상기 계산된 해시 값들을 갖는 상기 적어도 하나의 리스트 엔트리에서의 기록을 검증하는 단계를 더 포함하는 것을 특징으로 하는 신원을 기밀 검증하는 방법.

청구항 3

제 2 항에 있어서,

상기 적어도 하나의 리스트 엔트리의 검증은 기록된 서명의 검증을 포함하는 것을 특징으로 하는 신원을 기밀 검증하는 방법.

청구항 4

제2항 또는 제3항에 있어서,

시도-응답 인증은 상기 사용자 엔터티 및 상기 쿼링 엔터티 간에 수행되는 것을 특징으로 하는 신원을 기밀 검증하는 방법.

청구항 5

제1항 내지 제4항 중 어느 한 항에 있어서,

상기 해시 값들은 키 해시 값들인 것을 특징으로 하는 신원을 기밀 검증하는 방법.

청구항 6

제1항 내지 제5항 중 어느 한 항에 있어서,

상기 암호화 체인 리스트는 블록체인인 것을 특징으로 하는 신원을 기밀 검증하는 방법.

청구항 7

제1항 내지 제6항 중 어느 한 항에 있어서,

상기 신원 문서를 사용하는 동안 검증은 비디오 식별 방법을 포함하는 것을 특징으로 신원을 기밀 검증하는 방법.

청구항 8

제1항 내지 제7항 중 어느 한 항에 있어서,

상기 서명을 기록하는 단계는 상기 신원의 정확성에서 신뢰가 얼마나 높은지 가리키는 신뢰 레벨을 기록하는 단계를 포함하는 것을 특징으로 하는 신원을 기밀 검증하는 방법.

청구항 9

제 1 항 내지 제 8 항 중 어느 한 항에 있어서,

상기 계산된 해시 값들을 기록하는 단계는 상기 암호화 체인 리스트의 별개 어드레스들에서 각각 발생하는 것을 특징으로 하는 신원을 기밀 검증하는 방법.

청구항 10

제 1 항 내지 제9항 중 어느 한 항에 있어서,

상기 사용자 엔터티, 상기 쿼링 엔터티 및/또는 상기 검증 엔터티 간의 통신에 신뢰할만한 엔터티가 있는 것을 특징으로 하는 신원을 기밀 검증하는 방법.

청구항 11

제 1 항 내지 제10항 중 어느 한 항에 있어서,

상기 사용자 엔터티, 상기 쿼링 엔터티 및 상기 검증 엔터티는 통신 기술 관점에서 연결되어 있는 것을 특징으로 하는 신원을 기밀 검증하는 방법.

청구항 12

제 1 항 내지 제11항 중 어느 한 항에 있어서,

상기 검증 엔터티는 네트워크 기반 서비스에 의하여 공급받는 것을 특징으로 하는 신원을 기밀 검증하는 방법.

청구항 13

제 1 항 내지 제12항 중 어느 한 항에 있어서,

상기 신원을 기밀 검증하는 방법은 데이터 기술 네트워크에서 분산된 방식으로 실행되는 것을 특징으로 하는 신원을 기밀 검증하는 방법.

청구항 14

암호화 체인 리스트를 사용하여 신원을 기밀 검증하는 신원 시스템에 있어서,

대칭키 정보 아이템과 함께 상기 신원의 신원 속성들을 제공하는 사용자 엔터티;

상기 신원 속성이 알려져 있어도 상기 신원을 추론할 수 없는 방식으로 각각의 신원 속성에 대하여 각각의 해시 값을 계산하는 암호화 유닛;

적어도 하나의 리스트 엔트리로서 상기 계산된 해시 값을 상기 암호화 체인 리스트에 기록하는 데이터 인터페이스;

상기 대칭키 정보 아이템과 함께 상기 적어도 하나의 리스트 엔트리의 어드레스를 상기 사용자 엔터티로부터 검증 엔터티로 전송하는 네트워크 구성요소;

상기 신원 속성들을 갖는 신원 문서를 사용하면서 상기 계산된 해시 값을 갖는 상기 적어도 하나의 리스트 엔트리를 검증하고, 상기 어드레스에 공급되어 저장된 상기 신원 속성들이 상기 신원 문서의 상기 신원 속성들과 일치하는지 검증하는 상기 검증 엔터티; 및

상기 검증 엔터티에 의하여 상기 신원 속성들이 긍정적으로 검증되는 경우, 상기 적어도 하나의 리스트 엔트리의 서명을 상기 암호화 체인 리스트에 기록하는 데이터 인터페이스를 포함하는 신원을 기밀 검증하는 신원 시스템.

청구항 15

제 1 항 내지 제13항 중 어느 한 항에 따른 방법을 컴퓨터에서 실행하는 제어 명령을 포함하는 컴퓨터 프로그램 제품.

발명의 설명

기 술 분 야

[0001] 본 발명은 소위 블록체인이 적용된 전자 신원(identity) 기밀 검증 방법에 관한 것이다. 제안된 방법은 액팅 파티(acting party)가 블록체인 신원을 인식할 수 있게 하지만, 신원 속성들과 함께 각각의 신원의 기밀성 수준은 유지된다. 본 발명은 적응적으로 사용되는 신원 시스템 및 방법을 실행하거나 및/또는 제안된 시스템 구성을 작동시키는 제어 명령들로 이루어진 컴퓨터 프로그램 제품에 관한 것이다.

배 경 기 술

[0002] 중국 공개공보 CN 106682530 A1은 기밀성을 유지하는 동안 의료 정보를 쉐어링하는 방법을 개시하고 있다.

[0003] 미국 등록공보 US 9,635,000 B1은 컴퓨터 네트워크에서 신원들을 관리하는 시스템을 개시하고 있다.

[0004] 미국 공개공보 US 2017/0149819 A1는 블록체인 기술에 기반한 보안 매커니즘이 구현된 컴퓨터 네트워크를 개시하고 있다.

[0005] 종래 기술은 블록체인 기술에 대하여 광범위한 활용을 개시하고 있다. 암호화폐 비트코인이 알려져 있고, 그 외 암호화폐들이 수없이 알려져 있다. 더욱이, 은행 또는 보험사들은 블록체인들을 은행간 거래 및 거래 플랫폼들에 대하여 실험을 진행하고 있다. 더 많은 활용들이 공공 등기소(예를 들어, 토지 등기소) 및 신원 플랫폼들에

서 논의되고 있다. 신원 플랫폼은 블록체인에서 전자 신원들을 매핑하고, 블록체인을 신원 관리 시스템에서 데이터 저장소의 하나로 사용하는 것에 관한 것이다.

[0006] 블록체인 접근법 외에, 전통적인 데이터베이스 기반 신원 관리 시스템들 및 모든 범위의 모바일 신원 시스템들은 예를 들어, UICC, 다른 토큰들 또는 eID 카드들을 통한 카드들을 기반으로 한다. 블록체인 접근법의 이점은 신원 플랫폼을 관리하는 중앙 엔터티(entity)가 필요 없다는 점이다.

[0007] 블록체인 기반 신원 어플리케이션들로 만족스럽게 해결되지 않고 있는 문제는 프라이버시 대 신뢰 문제이다. 한편, 블록체인 신원의 소비자(신뢰 당사자; relying party)는 특정 신원(또는 신원 속성들)이 기록되고 확인된 신뢰 레벨을 인식할 수 있어야 한다. 반면에, 특히, 공개 블록체인에서 이들 신원 속성들은 자유롭게 접근할 수 없어야 하고, 서로 또는 실제 사람에게 할당될 수 없어야 한다. 또한, 신뢰 당사자들이 특정 신원과 관련이 되어 있는지 인식할 수 없어야 한다. 사용자는 신뢰 당사자에게 제공할 (개인) 속성들을 결정하거나 안 할 수 있는 옵션을 가지고 있어야 한다. 제공되지 않은 속성들은 제공된 속성들을 기반으로 할당될 수 없어야 한다.

발명의 내용

해결하려는 과제

[0008] 따라서, 본 발명의 목적은 네트워크에서 분산 방식으로 실행될 수 있는 방식으로 전자 신원이 검증될 수 있도록 하는 방법을 제공하고, 또한, 가장 가능성 있는 신원 보유자의 신뢰의 보호가 보장되는 방법을 제공하는 것이다. 이 방법은 기존 인프라를 사용하는 동안 가능해야 하고, 따라서 최소한의 기술 노력만 수반하여야 한다. 또한, 본 발명의 목적은 방법을 실행하고 및/또는 시스템을 동작하는 제어 명령들을 갖는 컴퓨터 프로그램과 대응되도록 적용된 신원 시스템을 제안하는 것이다.

[0009] 본 발명의 목적은 독립 청구항들의 특징에 의하여 달성된다. 또한, 유리한 실시예들이 종속청구항들에 기술되어 있다.

[0010] 따라서, 암호화 체인 리스트를 사용하면서 신원의 기밀 검증에 대한 방법이 제안된다. 이는 바람직하게는 소위 블록체인이다.

과제의 해결 수단

[0011] 방법은 사용자 엔터티에 의하여 대칭키 정보 아이템과 함께 신원의 신원 속성들을 제공하고, 신원 속성이 알려져 있더라도 신원의 해시 값을 추론할 수 없는 방식으로, 대칭키(키 해시)를 사용하는 동안 각각의 신원 속성의 각각의 해시 값을 계산하고, 적어도 하나의 리스트 엔트리로 계산된 해시 값들을 암호화 체인 리스트에 기록하고, 사용자 엔터티로부터 검증 엔터티에 대칭 키 정보 아이템과 함께 적어도 하나의 리스트의 어드레스를 전송하고, 어드레스에 제공되어 저장된 신원 속성들이 신원 문서의 신원 속성들과 일치하는지 검증하고, 신원 속성들을 갖는 신원 문서를 사용하는 동안 계산된 해시 값들을 갖는 적어도 하나의 리스트 엔트리를 검증 엔터티에 의하여 검증하고, 검증 엔터티에 의하여 검증 속성들의 긍정적인 검증이 있는 경우, 적어도 하나의 리스트 엔트리의 서명을 암호화 체인 리스트에 기록하는 단계를 포함한다.

도면의 간단한 설명

[0012] 도 1은 본 발명의 일 실시예에 따라, 신원 시스템 및 대응되는 통신 경로들을 나타낸다.

도 2는 본 발명의 일 실시예에 따른 신원 기밀 검증에 대한 방법을 나타내는 흐름도를 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0013] 당업자는 개별 방법 단계들은 하위 단계들을 가지고 있음을 인식한다. 개별 단계들은 예를 들어, 많은 데이터 및 속성들은 개별적으로 전송되고, 및/또는 계산 단계들은 순차적으로 또는 병행하여 실행될 수 있는 방식으로 반복적으로 실행될 수도 있다.

[0014] 제안된 신원 시스템은 사용자의 프라이버시를 보호하고 동시에 신뢰 당사자는 신원 속성들의 신뢰 레벨을 평가할 수 있다. 제3 엔터티(third entity)에 대해서는, 신뢰 당사자가 특정 신원과 관련되어 있는지 분명하지 않다. 속성들은 개별적으로 공개될 수 있으며, 공개되지 않은 특성들은 할당되지 않는다. 또한, 비록 개별 속성들이 공개적으로 알려져 있어도, 제3 엔터티는 신원들을 할당할 수 없다. 블록체인 외에 실제 속성들이 저장되

어 있는 클라우드 서비스를 운영할 필요가 없다.

[0015] 또한, 평판 기반 신원(reputation-based identity)은 예를 들어, 개별 속성들이 자주 검증되지만 신뢰도가 낮은 반면에 다른 속성들은 덜 빈번하게 검증되어도 더 높은 신뢰 수준을 갖는 방식으로 구축될 수도 있다.

[0016] 기본적인 개념은 "A. 초기 식별"(등록, 검증) 및 "B. 신원 이용" 단계로 나누어진다.

[0017] A. 초기 식별

[0018] 본 발명의 일 실시예에 따라, 신원을 최초로 등록하기 위하여, 다음 단계들이 수행된다:

[0019] 1. 최종 사용자는 그들의 내용(예를 들어, 이름, 생일, 출생지 등등)을 포함하며 검증하고자 하는 속성들을 (예를 들어, 모바일 어플리케이션에서 또는 웹 인터페이스를 통하여) 결정한다;

[0020] 2. 속성들의 키 해시 값(keyed hash value)을 계산하는데 사용되는 대칭키가 생성된다. 각각의 속성에 대하여 별도의 해시 값이 계산된다. 키 해시 방법을 사용함으로써, 키를 알지 못하여도 알려진 속성(예를 들어, 이름)에 기초하여 제3자가 신원을 할당하는 것은 불가능하다;

[0021] 3. 최종 사용자는 블록체인에서 속성들의 키 해시 값들을 발행한다. 지금까지, 최종 사용자는 오로지 속성을 스스로 선언하였지만, 속성은 제3자에 의해서는 검증되지 않는다;

[0022] 4. 다음 단계에서, 사용자는 (예를 들어, VideoIdent 방법으로, 지사에서 등등으로) 신원들을 검증할 수 있는 검증 서비스로 이동한다. 사용자는 상기 서비스를 속성들의 키 해시 값들이 저장되어 있는 블록체인 어드레스에 제공한다. 또한, 사용자는 해시 값들뿐만 아니라 신원 문서의 정확성을 검증할 수 있는 서비스로 해시 계산에 키를 제공한다;

[0023] 5. 본 서비스는 식별을 수행하고, 블록체인으로부터 자체 선언된 속성들을 신원 문서(identity document)의 데이터와 비교한다. 데이터가 일치하는 경우, 서비스는 사용자의 어드레스로 블록체인 트랙잭션(transaction)을 수행하고, (예를 들어, 전자 신원, 승인 및 신뢰 서비스 EIDAS 레벨에 따라) 해시 값들 및 식별의 신뢰 레벨을 전송한다. 비밀은 순차적으로 다시 삭제된다.

[0024] 속성들은 현재 검증되었고, 해시 값들에 대한 서명은 블록체인에 저장되었기 때문에, 검증 서비스의 공개키는 필요한 경우 해당 공개키 인프라 PKI와 함께 인증서로서 저장된다. 이는 제3자들이 인식되고 신뢰할 수 있는 기관에 의하여 속성들이 검증되었음을 평가할 수 있도록 한다.

[0025] B. 본 발명에 따라, 검증된 신원은 다음과 같이 사용될 수 있다.

[0026] 1. 최종 사용자는 블록체인 어드레스, 해시 키 및 획득된 속성들의 내용을 신뢰 당사자에 제공한다.

[0027] 2. 신뢰 당사자(relying party)는 사용자 키로 속성들의 내용으로부터 키 해시 값을 계산하고, 그것을 블록체인에 저장된 데이터와 비교한다. 또한, 신뢰 당사자는 데이터를 통하여 검증 서비스의 서명을 검증한다.

[0028] 3. 필요한 경우, 신뢰 당사자는 블록체인 계정에 대한 비밀키를 가지고 있다는 것을 증명하기 위하여, 사용자로 시도-응답 프로토콜(challenge-response protocol)을 수행한다. 따라서 신뢰 당사자는 실제로 속성들을 전달하는 블록체인 계정의 소유자라는 증거를 가지고 있다.

[0029] 4. 검증이 완료된 후, 신뢰 당사자는 사용자 키를 삭제한다.

[0030] 본 발명의 일 실시예에 있어서, 각각의 속성은 별도의 블록체인 어드레스에 의하여 표현된다. 따라서 개별 속성을 공동 신원에 할당하는 것 외에는 불가능하다. 그 후 활용 단계 B의 3단계는 각각의 속성에 대하여 개별적으로 실행된다.

[0031] 본 발명의 다른 실시예에서, 사용자는 키 해시 값의 계산에 필요한 키를 (잠재적으로 전달될 수 있는 곳으로부터) 신뢰 당사자에게 발행하는 것이 아니라, 선택한 신뢰 서비스(trust service)에 발행하는 것이 제공되고, 그 후, 해시 값들의 분해능(resolution) 및 신뢰 당사자(및 사용자에 의한 승인 후, 예를 들어, OAuth 2.0 프로토콜을 통하여)에 대한 일반 텍스트 값들과의 비교를 가정한다.

[0032] 제안된 방법은 본 발명에 따라 신원 보유자의 정보가 불필요하게 공개되는 것이 금지되기 때문에, 신원의 기밀 검증을 제공한다. 예를 들어, 본 발명에 따라, 이름, 주소 또는 생일과 같은 개별 신원 속성들을 암호화 체인 리스트(cryptographically chained list) 내의 별도의 위치들에 저장 가능하다. 암호화 체인 리스트는 바람직하게는 소위 블록체인이다.

[0033] 블록체인은 서로 및 각각의 경우에서 해시 값들을 나타내는 컨넥터들로 연결된 다수의 데이터 엔트리들로 구성된다. 따라서, 암호화 체인 리스트는 블록들 또는 리스트 엔트리들이라고도 하는 데이터 세트들의 연속적으로 확장 가능한 리스트이다. 각각의 리스트 엔트리는 이전 블록, 타임 스탬프 및 트랜잭션 데이터의 암호 보안 해시(cryptographically secure hash)를 갖는 것이 가능하다. 본 발명에 따라, 개별 신원 속성들은 리스트 엔트리들 또는 블록들로 코딩될 수 있기 때문에 기존의 블록체인의 장점도 함께 발생한다.

[0034] 전자 신원을 모델링하기 위하여, 예를 들어, 신원 보유자의 이름과 같은 신원 속성들이 제공된다. 사용자는 인터페이스를 통하여 신원 속성들의 이름을 지정하고, 이들에 값들을 할당하는 방식으로 수동으로 이루어질 수 있다. 사용자는 단순히 시스템을 운영하기 때문에, 데이터를 입력하기 위하여 사용자에 의하여 사용되는 단말 장치가 사용자 엔터티(user entity)로 현재 지정된다. 따라서 사용자 엔터티는 예를 들어 웹 인터페이스를 갖는 모바일 단말일 수 있다. 이러한 방식으로, 사용자는 신원 속성들을 입력할 수 있는 입력 마스크를 제공받을 수 있다.

[0035] 신원 속성들 각각에 대하여 해시 값이 계산되고, 키 해시 값으로 표시하는 것이 바람직하다. 비록 제3자가 신원 속성들을 가지고 있다고 하더라도 키 해시 값을 통하여 제3자가 신원을 추론하는 것은 가능하지 않다. 키 해시 방법을 사용함으로써, 알려진 속성들의 경우에도 공격자가 키를 알지 못하고 신원을 할당하는 것은 가능하지 않다. 따라서, 사용자의 신원의 기밀성은 항상 유지되고, 데이터는 암호화 체인 리스트에 저장되고, 쿼링 엔터티(querying entity)에 접근 가능해야 하는 이유로 특별한 장점을 갖는다.

[0036] 그 후, 계산된 해시 값들은 블록 또는 리스트 엔트리로서 블록체인에 저장된다. 각각의 해시 값에 대하여 별개의 리스트 엔트리를 생성하는 것이 가능하고, 단일 리스트 엔트리로 복수의 해시 값을 저장하는 것이 가능하다. 알려진 블록체인 기술에 따르면, 해시 값들은 암호화 체인 리스트에 통합되고, 네트워크 기술 측면에서 네트워크 노드들로 분배된다. 블록체인 내의 리스트 엔트리 또는 리스트 엔트리들의 어드레스는 대칭키 정보 아이템(symmetrical key information item)과 함께 사용자로부터 검증 엔터티로 전송된다. 이는 검증 엔터티(validation entity)가 예를 들어 정확성을 위한 엔트리들을 체크하기 위하여 리스트 엔트리들을 검증할 수 있게 한다.

[0037] 사용자는 먼저 스스로 신원 속성들을 생성하였으므로, 이 방법 단계에서는 실제로 이들 사양을 검증할 수 있는 이점이 있다. 이를 위하여, 사용자는 신원 문서, 예를 들어, 여권을 제공할 수 있고, 원격 식별(remote identification)을 수행할 수가 있다. 이는 검증 엔터티가 신원 속성들을 모델링하는 블록체인의 리스트 엔트리들이 실제로 정확하고 신원 문서의 데이터에 일치되는지 체크할 수 있게 한다.

[0038] 소위 VideoIdent 방법은 가능한 검증으로 알려져 있고, 예를 들어, 웹 카메라를 통하여 사용자가 식원 문서를 전송하는 것이 가능하다. 따라서 검증 엔터티는 사용자가 스스로를 식별하고, 큰 노력 없이 신원 문서의 정확한 신원 속성들을 제공할 수 있는 데이터 인터페이스를 제공한다. 여기에서, 신원 속성들이 이용될 수 있는 방식으로 신원 문서를 독출하는 것이 가능한 더 많은 방법들이 알려져 있다. 예를 들어, 이름 및 주소는 여권으로부터 독출될 수 있다.

[0039] 결론적으로, 제공된 신원 속성들은 사용자에 의하여 특정되어 제공되며, 검증 엔터티는 신원 문서로부터 독출되었던 신원 속성들을 가지고 있다. 특히, 두 속성들을 상호 비교하여 정확성을 검증할 수 있다. 본 경우에 있어서, 이는 검증으로 간주되고, 제공된 신원 속성들이 신원 문서로부터 독출된 신원 속성들과 일치된다면 긍정적으로(positive) 진행된다. 만약 속성들이 일치되지 않는다면, 사용자는 부정확한 값을 특정했을 가능성이 있다. 이 경우에는 방법들이 계속 반복될 수 있으며, 사용자는 다시 신원 속성들을 제공하여야 한다. 신원 속성들은 부정확하게 특정되지 않을 가능성도 있지만, 검증 동안 인식되는 공격이 발생할 수도 있다. 따라서, 부정적인 검증의 경우, 방법은 어느 경우이든 종료되거나 다시 실행된다.

[0040] 긍정적인 검증이 발생하는 경우에, 적어도 하나의 리스트 엔트리의 서명을 암호화 체인 리스트에 기록하는 것이 이루어진다. 따라서, 신원 속성들 또는 해시 값들을 갖는 리스트 엔트리가 서명되고, 신원 속성들은 정확하게 블록체인에 저장된다.

[0041] 본 발명의 또 다른 실시예에 따라, 적어도 하나의 리스트 엔트리의 어드레스, 대칭키 정보 아이템 및 신원 속성들은 사용자 엔터티로부터 신원을 쿼리하는 엔터티로 전송되며, 쿼링 엔터티는 전송된 데이터에 기초하여 계산된 해시 값들을 갖는 기록된 적어도 하나의 리스트 엔트리를 검증한다. 신뢰 당사자로 지칭되는 쿼링 엔터티는 신원을 결정하기에 필요한 모든 데이터를 평가할 수 있고, 제3자는 특정 신원이 신뢰 당사자와 관련되어 있는지 알 수는 없다는 이점이 있다. 전송된 데이터로 쿼링 엔터티, 예를 들어, 신뢰 당사자는 블록체인에 저장된 데이

터를 검증할 수 있고, 검증은 비교를 통하여 수행된다. 쿼링 엔터티는 예를 들어, 네트워크를 통하여 사용자 엔터티와 통신하는 계산 유닛일 수 있다. 따라서 쿼링 엔터티는 블록체인 기술에 기초하여 신원을 검증할 수 잇는 기회를 매번 갖는다.

[0042] 본 발명의 또 다른 실시예에 따라, 적어도 하나의 리스트 엔트리의 검증은 기록된 서명의 검증을 포함한다. 검증 엔터티의 트랜잭션이 고려될 수 있고, 검증 엔터티에 의하여 제공된 서명이 검증을 위하여 사용될 수 있다는 이점이 있다. 여기에서, 통상의 기술자는 서명이 어떻게 평가되는지 나타내는 방법을 알고 있다. 서명은 소위 신뢰 당사자에 의하여 블록체인으로부터 독출될 수 있다.

[0043] 본 발명의 또 다른 실시예에 따라, 시도-응답 인증(challenge-response authentication)은 사용자 엔터티와 쿼링 엔터티 사이에 수행된다. 이는 전송된 데이터가 정확한 사용자에 의하여 사용자 엔터티로부터 신뢰 당사자로 실제로 전송되는 이점이 있다. 이는 사용자 엔터티와 신뢰 당사자간의 통신을 보호하고, 그 결과 공격 시나리오가 방해된다. 시도-응답 방법은 전형적으로 신뢰 당사자에 의하여 개시되고, 사용자 엔터티로의 시도 메시지로 시작되며, 다른 것들 중에서도 사용자 엔터티의 개인키로 시도의 서명을 포함하고 있는 응답 메시지로 응답한다.

[0044] 본 발명의 또 다른 실시예에 따라, 해시 값들은 소위 키 해시 값들이다. 이는 이 방법에 의하여 알려진 신원 속성들로부터 신원을 추론할 수 없으며, 따라서 신원 속성들 또는 해시 값들이 블록체인으로부터 독출될 수 있어도 신원은 항상 숨겨져있다.

[0045] 본 발명의 또 다른 실시예에 따라, 암호화 체인 리스트는 블록체인으로 존재한다. 이는 비록 본 발명에 따라 비승인된 접근으로부터 정보를 보호할 수 있더라도 소위 블록체인 기술의 부분으로서 구현된 보안 매커니즘이 채택될 수 있는 이점이 있다. 따라서 블록체인 기술은 사용자의 프라이버시를 보호하는 규칙을 포함하도록 확장된다. 이는 제안된 방법이 기존 인프라에 통합될 수 있도록 한다.

[0046] 본 발명의 또 다른 실시예에 따라, 신원 문서를 사용하는 동안의 검증은 비디오 식별 방법을 포함한다. 이는 사용자가 웹 기반 인터페이스를 통하여 데이터를 공급하고, 사용자의 정확한 데이터 및/도는 신원 속성들이 실제로 존재한다는 것을 보장할 수 있는 이점이 있다. 비디오 식별 방법은, 예를 들어, 사용자가 식별 문서를 카메라에 보유하는 소위 VideoIdent 방법이다. 그 후, 문서는 독출될 수 있고, 사용자 데이터는 특정 신원 속성들과 비교된다. 다른 비디오 식별 방법은 소비자가, 예를 들어, 은행 지점에 그 자신을 제공하고, 스스로를 식별하거나 또는 예를 들어, 전자 개인 식별 카드와 같은 전자 ID 카드의 사용을 식별하는 종래의 방법이다. 또한 이는 현재 방법과 결합될 수 있고, 정확한 신원 속성들이 이 방법으로 획득될 수 있다.

[0047] 본 발명의 또 다른 실시예에 따르면, 서명 기록은 신뢰 레벨(보증(assurance) 레벨)의 기록을 포함한다. 이는 신원의 정확도에 있어서 신뢰가 얼마나 높은지를 나타내는 신뢰 레벨은 블록체인에 있다는 이점이 있다. 전자 식별에 관한 EU 규약 및 전자 트랜잭션에 대한 신뢰 서비스도 이와 관련해서 사용될 수 있다. 특히, 소위 eIDAS 신뢰 레벨도 사용될 수 있다. eIDAS는 전자식별, 인증 및 신뢰 서비스에 대한 유럽 규약을 나타낸다. 따라서 신원 문서로부터 기록된 데이터가 정확하다는 확률을 나타내는 값이 저장될 수 있다.

[0048] 본 발명의 또 다른 실시예에 따르면, 계산된 해시 값들의 기록은 암호화 체인 리스트에서 각각 다른 어드레스들에서 이루어진다. 이는 해시 값들은 다른 블록들 또는 리스트 엔트리들에 저장될 수 있고, 따라서 이들 해시 값들 및/또는 대응되는 신원 속성들이 특정 프로파일 또는 신원에 할당되는 것이 제3자에게는 명백하지 않다는 이점이 있다. 따라서 이들은 서로 독립적으로 저장되며, 처음에는 이들 데이터간 명백한 연결은 없다. 차례로 사용자의 프라이버시를 보호하고, 해시 값들은 서로 연관될 수 없다.

[0049] 본 발명의 또 다른 실시예에 따르면, 사용자 엔터티, 쿼링 엔터티 및/또는 검증 엔터티간의 통신에 신뢰할만한 엔터티(trustworthy entity)가 있을 수 있다. 이는 개별 방법 단계들이 중간 엔터티(intermediate entity) 같은 것에 의하여 실행될 수 있고, 따라서 모든 데이터가 항상 각각의 엔터티들에 전송될 수 있는 것은 아니라는 이점이 있다. 따라서, 센시티브 데이터(sensitive data)는 네트워크를 통해 더 분배되고, 비승인된 접근의 경우 독출될 수 있는 데이터의 수집 지점들은 형성되지 않는다. 예를 들어, 신뢰 당사자에 키 해시 값의 계산을 위한 키를 출력하지 않고 중간 서비스에 전송하는 것이 가능하며, 중간 서비스는 해시 값들의 분해능(resolution)과 신뢰 당사자에 대한 일반 텍스트 값들과의 비교를 가정한다.

[0050] 본 발명의 다른 실시예에 따라, 사용자 엔터티, 쿼링 엔터티 및 검증 엔터티는 통신 기술 관점에서 연결된다. 이는 현재 발명은 컴퓨터에서 수행되고, 관련된 모든 엔터티들이 계산 유닛들로 존재할 수 있다는 이점이 있다. 또한 블록체인은 데이터 기술 관점에서 엔터티들과 연결되고, 이를 위하여 네트워크 구성요소들이 제공되어야

한다. 예를 들어, 개별 엔터티들은 서버 또는 클라이언트일 수 있다.

[0051] 본 발명의 다른 실시예에 따라, 검증 엔터티는 네트워크 기반 서비스에 의하여 제공된다. 이는 식별 방법을 실행하거나 식별 문서를 독출할 수 있는 전통적인 사용자 인터페이스가 제공될 수 있는 이점이 있다. 따라서, 소위 원격 식별이 수행될 수 있다.

[0052] 본 발명의 또 다른 실시예에 따라, 방법은 데이터 기술 네트워크에서 분산적인 방법으로 실행된다. 이는 신원 관리를 수행하는 중앙 엔터티들이 제공되는 것이 아니라, 분산된 데이터 유지 및 데이터 관리를 기초로 하는 블록체인 기술이 적용된다. 따라서, 단순한 네트워크 구성요소, 예를 들어, 네트워크 기술의 관점에서 사용될 수 있는 서버를 의미하는 기반 인프라가 중심이 되고, 그러나 그럼에도 불구하고, 개별 방법 단계들은 분산된 방식으로 실행된다. 특히, 블록체인의 부분들은 네트워크에서 중복성을 유지할 수도 있고 분산될 수도 있다.

[0053] 또한, 목적은 암호화 체인 리스트를 사용하는 동안 신원의 기밀 검증을 위한 신원 시스템으로 달성되며, 이는 대칭키 정보 아이템과 함께 신원의 신원 속성들을 제공하는 사용자 엔터티, 신원 속성이 알려져 있더라도, 신원을 추론할 수 없도록 각각의 신원 속성들에 대한 각각의 해시 값을 계산하는 암호화 유닛, 적어도 하나의 리스트 엔트리로서 계산된 해시 값들을 암호화 체인 리스트에 기록하는 데이터 인터페이스, 사용자 엔터티로부터 검증 엔터티에 대칭키 정보 아이템과 함께 적어도 하나의 리스트 엔트리의 어드레스를 전송하는 네트워크 구성요소, 신원 속성들을 갖는 신원 문서를 사용하면서 적어도 하나의 리스트 엔트리 및 계산된 해시 값들을 검증하고, 어드레스에 공급되어 저장된 신원 속성들이 신원 문서의 신원 속성들과 일치하는지 검증하는 검증 엔터티, 검증 엔터티에 의하여 신원 속성들이 긍정적으로 검증되는 경우, 적어도 하나의 리스트 엔트리의 서명을 암호화 체인 리스트에 기록하는 데이터 인터페이스를 포함한다.

[0054] 당업자는 여기에서 암호화 유닛은 예를 들어 사용자 엔터티에 통합될 수 있다는 것을 인식한다. 데이터 인터페이스는 균일하며, 다른 데이터 인터페이스들로 구현되는 것도 가능하다. 개별 엔트리들은 물리적으로 또는 소프트웨어 기술 관점에서 이용될 수 있다.

[0055] 본 발명의 목적은 제안된 방법을 실행하거나 및/또는 제안된 시스템을 운영하는 제어 명령어들을 갖는 컴퓨터 프로그램 제품에 의하여 더 달성될 수도 있다.

[0056] 본 발명에 따르면, 제안된 방법은 시스템에 의하여 구조적으로 재생될 수 있는 기능을 제공하는 방법 단계들을 가지는 특별한 이점이 있다. 시스템은 방법 단계들로부터 재생될 수 있는 구조적 특징들을 더 포함할 수 있다. 컴퓨터 프로그램 제품은 제안된 방법을 실행하거나 신원 시스템을 운영하는 것을 제공한다. 예를 들어, 컴퓨터 프로그램은 네트워크 프로토콜을 포함할 수도 있다.

[0057] 실시예들의 장점들은 첨부된 도면들과 관련하여 더 자세히 설명된다. 도면들은 아래와 같이 설명된다.

[0058] 도 1은 본 발명의 일 실시예에 따라, 신원 시스템 및 대응되는 통신 경로들을 나타낸다.

[0059] 도 2는 본 발명의 일 실시예에 따른 신원 기밀 검증에 대한 방법을 나타내는 흐름도를 나타낸다.

[0060] 도 1은 신원 시스템의 도식 구조를 나타내고 있으며, 사용자 엔터티가 좌측에 표시되어 있고, 사용자 엔터티는 최종 사용자가 신원 속성들을 특정할 수 있게 하고(1A), 키 해시 값들을 계산하기 위하여 사용되는(2A) 대칭키(S)가 생성된다. A로 지정된 기능들은 초기 식별을 위하여 사용되고, 기능들 1A, 2A, ..., 6A들은 "A. 초기 식별"에 이미 언급된 지점들에 해당한다. 접미사 B를 갖는 기능들은 검증된 신원의 사용을 나타내며, 대응되는 기능들 1B, 2B 및 3B도 마찬가지로 이미 열거된 지점들에 해당한다.

[0061] 3A 기능은 블록체인에서 신원 속성들의 키 해시 값들의 발행을 나타낸다. 도 1에서 기재되어 있는 파라미터들은 다음 의미를 가지고 있다:

[0062] Attributes: 속성들의 일반 텍스트(예를 들어, 이름, 주소 등등)

[0063] S: 키 해시 계산을 위한 대칭키

[0064] PrivKU/PubKU: 블록체인 계정의 "사용자키 페어"

[0065] PrivKI, PubKI: 신원 검증 서비스의 키 페어(증명서 포함)

[0066] LoA: (예를 들어, eIDAS, ISO, NIST, ... 등에 따른) 신원 검증의 보안 레벨

[0067] 도 1에서, "신원 검증"은 검증 엔터티를 나타내고, "신뢰 당사자"는 쿼링 엔터티, 예를 들어, 사용자 신원을 신

뢰하는 유닛을 나타낸다.

[0068] 사용자 엔터티가 블록체인에 속성들의 해시 값들을 저장한 경우(3A), 속성들은 키(S) 및 해시 값들의 블록체인 어드레스(Blockchain Addr.)와 함께 검증 엔터티로 보내진다(4A). 그 후, 검증 엔터티는 예를 들어 VideoIdent 방법을 사용하는 동안 소위 원격 신원(Remote Identification)을 실행한다. 따라서 검증 엔터티는 식별을 실행하는 기능을 제공하고(5A), 사용자에 의하여 선언된 블록체인으로부터의 속성들과 식별 문서로부터의 데이터를 비교한다. 검증이 긍정적인 경우, 서비스 또는 검증 엔터티는 블록체인 트랜잭션을 실행하고(5A), 신원 속성들은 검증되고, 해당 서명은 블록체인에 저장된다(6A).

[0069] 그 후, 저장된 신원이 사용되고, 신뢰 당사자는 사용자의 신원을 쿼리하기를 원한다. 이를 위해, 최종 사용자는 대응되는 블록체인 어드레스, 해시 키 및 요구되는 속성들의 내용을 신뢰 당사자에 제공한다(1B). 신뢰 당사자, 예를 들어, 쿼링 엔터티는 현재 블록체인에 저장된 데이터를 검증하고(2B), 이들과 사용자에 의하여 제공된 데이터를 비교하는데 필요한 모든 데이터를 가지고 있다. 따라서 블록체인에 저장된 신원이 실제 정확한지 아닌지 검증될 수 있다. 예를 들어, 검증 엔터티의 서명은 이 목적을 위하여 검증될 수 있다(2B).

[0070] 비밀키가 사용자의 블록체인 계정에 속하는지 검증하기 위하여, 사용자 엔터티와 신뢰 당사자 간의 데이터 통신을 보호하는 소위 시도-응답(Challenge-Response) 프로토콜이 실행될 수 있다(3B).

[0071] 도 2는 암호화 체인 리스트를 사용하는 동안 신원의 기밀 검증에 대한 방법의 흐름도를 나타내고, 신원의 기밀 검증에 대한 방법은 사용자 엔터티에 의하여 대칭키 정보 아이템과 함께 신원 속성들을 제공하는 단계(100), 신원 속성이 알려져 있어도 신원을 추론할 수 없는 방식으로 각각의 신원 속성에 대한 각각의 해시 값을 계산하는 단계(101), 적어도 하나의 리스트 엔트리로서 해시 값들을 암호화 체인 리스트에 기록하는 단계(102), 사용자 엔터티로부터의 대칭키 정보 아이템과 함께 적어도 하나의 리스트 엔트리의 어드레스를 검증 엔터티로 전송하는 단계(103), 서명 속성들을 갖는 서명 문서를 사용하는 동안 계산된 해시 값들을 갖는 적어도 하나의 리스트 엔트리를 검증 엔터티에 의하여 검증하고, 어드레스에 공급되고 저장된 신원 속성들이 신원 문서의 신원 속성들과 일치하는지 검증하는 단계(104), 및 검증 엔터티에 의하여 신원 속성들의 긍정적인 검증의 경우, 적어도 하나의 리스트 엔트리의 서명을 암호화 체인 리스트에 기록하는 단계(105)를 포함한다.

[0072] 또한, 적어도 하나의 리스트 엔트리의 어드레스, 대칭키 정보 아이템 및 신원 속성들은 사용자 엔터티에서 신원을 쿼리하는 엔터티로 전송되고(106), 이 쿼링 엔터티는 전송된 데이터에 기초하여 계산된 해시 값을 갖는 기록된 적어도 하나의 리스트 엔트리를 검증한다(107).

[0073] 제공된 방법은 무엇보다도 논의된 요구사항을 포함한다:

[0074] 신뢰 당사자와 특정 신원이 관련되는 제3 엔터티는 명백하지 않다: 신뢰 당사자는 실제로 블록체인 트랜잭션을 수행하지 않고, 그 결과 제3자에게 관계가 인식될 수 없다.

[0075] 공개되지 않은 속성들은 할당되지 않은 채 속성들이 개별적으로 공개될 수 있다: 각각의 속성에 대하여 별개의 블록체인 어드레스를 사용함으로써, 속성들을 서로 할당하는 것은 가능하지 않다.

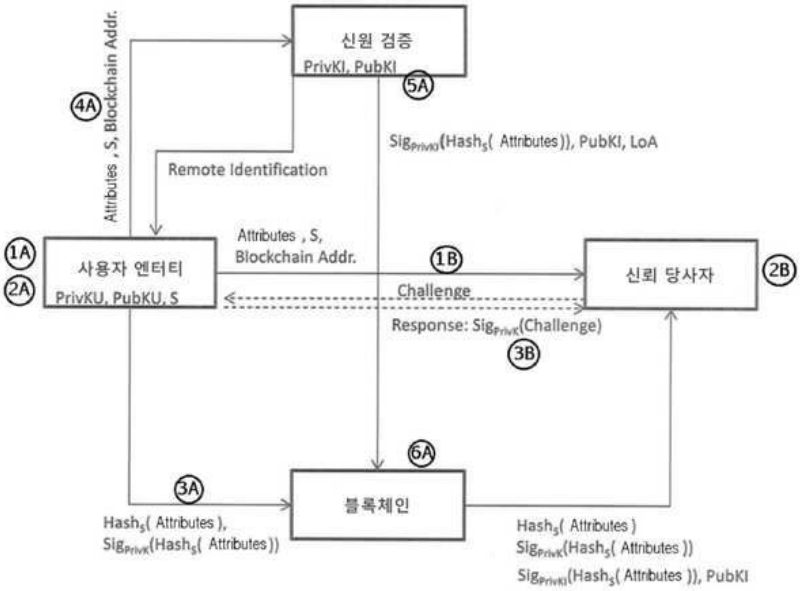
[0076] 또한, 개별 속성들이 공개적으로 알려져 있어도, 제3엔터티는 속성들을 할당하지 않는다: 사용자 키 없이, 비승인된 제3자는 공개적으로 알려진 속성들에 대하여 블록체인 데이터를 할당할 수 없다. 사용자 키를 사용하더라도, 비승인된 제3자는 알고 있는 속성에 대해서만 오직 할당할 수 있다. 그럼에도 불구하고, 비승인된 제3자는 블록체인 계정의 개인키를 가지고 있지 않기 때문에, 사용자를 개인적으로 식별할 수 없다.

[0077] 블록체인에 부가하여 실제 속성들이 저장되는 클라우드 서비스를 운영할 필요는 없다: 오직 키 해시 값들이 블록체인에 저장되기 때문에, 클라우드 서비스에 대한 추가 참조는 요구되지 않는다. 속성들의 내용은 사용자와 신뢰 당사자 사이에 직접 교환된다.

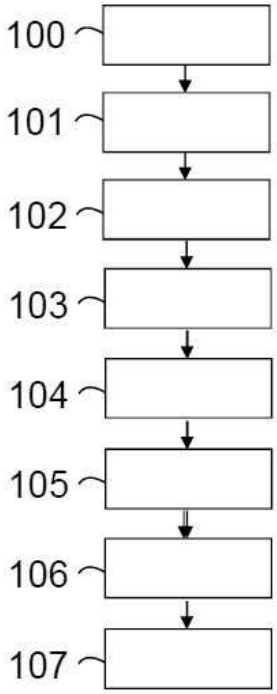
[0078] 또한, 평판 기반 속성은 계획적으로 구출될 수 있다: 속성의 검증들의 횟수는 신뢰 당사자가 신원이 얼마나 검증되었는지를 인식할 수 있게 한다.

도면

도면1


신원 검증
PrivKI, PubKI
5A
4A
Attributes , S, Blockchain Addr.
Remote Identification
$Sig_{PrivKI}(Hash_S(\ Attributes))$, PubKI, LoA
1A
2A
사용자 엔터티
PrivKU, PubKU, S
Attributes , S,
Blockchain Addr.
1B
Challenge
Response: Sig_{PrivK}(Challenge)
3B
신뢰 당사자
2B
6A
3A
블록체인
$Hash_S(\ Attributes\ )$,
$Sig_{PrivK}(Hash_S(\ Attributes))$
$Hash_S(\ Attributes\ )$
$Sig_{PrivK}(Hash_S(\ Attributes\ ))$
$Sig_{PrivKI}(Hash_S(\ Attributes\ ))$, PubKI

도면2


100
101
102
103
104
105
106
107