(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년06월30일
(11) 등록번호 10-2271201
(24) 등록일자 2021년06월24일

(51) 국제특허분류(Int. Cl.)
G06F 21/62 (2013.01) *H04L 29/06* (2006.01)
H04L 29/08 (2006.01) *H04W 12/02* (2021.01)
(52) CPC특허분류
G06F 21/6245 (2013.01)
H04L 63/08 (2013.01)
(21) 출원번호 10-2019-0121715
(22) 출원일자 2019년10월01일
심사청구일자 2019년10월01일
(65) 공개번호 10-2021-0039190
(43) 공개일자 2021년04월09일
(56) 선행기술조사문헌
KR1020160085143 A*
KR1020180129028 A*
KR1020190075771 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
숭실대학교산학협력단
서울특별시 동작구 상도로 369 (상도동)
(72) 발명자
신용태
서울특별시 동작구 사당로 50
이아름
서울특별시 동작구 사당로 50
(뒷면에 계속)
(74) 대리인
심경식, 홍성욱

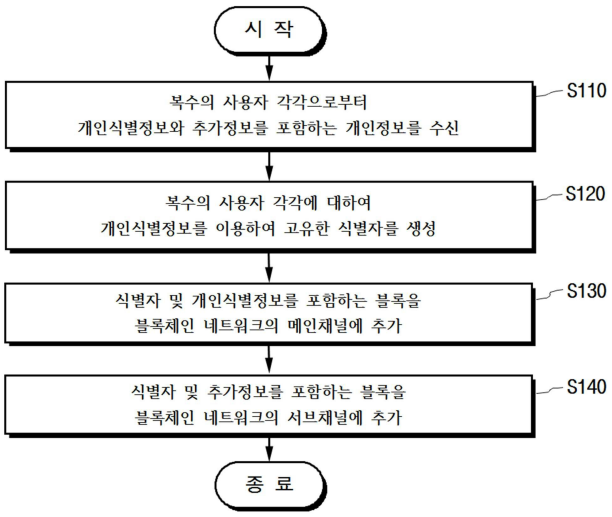
전체 청구항 수 : 총 9 항 심사관 : 구대성

(54) 발명의 명칭 **블록체인을 이용한 개인정보 관리 방법 및 그 방법이 적용된 블록체인 네트워크 관리자**

(57) 요 약

본 발명의 일 실시예에 따른 적어도 하나의 서비스 제공자로부터 서비스를 제공받기 위해 복수의 사용자가 개인정보를 블록체인 네트워크에 저장하여 관리하는 방법은 상기 블록체인 네트워크의 관리자가 상기 복수의 사용자 각각으로부터 개인을 식별하기 위한 정보인 개인식별정보와 개인에 대한 추가적인 정보인 추가정보를 포함하는 개인정보를 수신하는 단계; 상기 관리자가 상기 복수의 사용자 각각에 대하여 상기 개인식별정보를 이용하여 고유한 식별자를 생성하는 단계; 상기 관리자가 상기 식별자 및 상기 개인식별정보를 포함하는 블록을 상기 적어도 하나의 서비스 제공자와 상기 관리자를 포함하는 상기 블록체인 네트워크의 메인채널에 추가하는 단계; 및 상기 관리자가 상기 식별자 및 상기 추가정보를 포함하는 블록을 상기 관리자를 포함하는 상기 블록체인 네트워크의 서브채널에 추가하는 단계를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 67/20 (2013.01)
H04W 12/02 (2021.01)
(72) 발명자
박수용
서울특별시 동작구 사당로 50

배수환
서울특별시 동작구 사당로 50

이 발명을 지원한 국가연구개발사업

과제고유번호	1711078043
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	실험실 특화형 창업선도대학사업
연구과제명	2018년도 실험실 특화형창업선도대학사업
기 여 율	1/1
과제수행기관명	숭실대학교 산학협력단
연구기간	2019.02.01 ~ 2020.01.31

명 세 서

청구범위

청구항 1

적어도 하나의 서비스 제공자로부터 서비스를 제공받기 위해 복수의 사용자가 개인정보를 블록체인 네트워크에 저장하여 관리하는 방법에 있어서,

상기 블록체인 네트워크의 관리장치가 상기 복수의 사용자 각각으로부터 개인을 식별하기 위한 정보인 개인식별정보와 개인에 대한 추가적인 정보인 추가정보를 포함하는 개인정보를 수신하는 단계;

상기 관리장치가 상기 복수의 사용자 각각에 대하여 상기 개인식별정보를 이용하여 고유한 식별자를 생성하는 단계;

상기 관리장치가 상기 식별자 및 상기 개인식별정보를 포함하는 블록을 상기 블록체인 네트워크의 메인채널에 추가하는 단계; 및

상기 관리장치가 상기 식별자 및 상기 추가정보를 포함하는 블록을 상기 블록체인 네트워크의 서브채널에 추가하는 단계

를 포함하고,

상기 메인채널은 블록체인 네트워크의 서비스 제공자와 관리자를 포함하는모든 구성원이 접근 가능한 채널이고, 상기 서브채널은 관리자가 접근 가능한 채널인 것을 특징으로 하는 블록체인을 이용한 개인정보 관리 방법.

청구항 2

제1항에 있어서,

상기 고유한 식별자를 생성하는 단계의 이후에,

상기 관리장치가 상기 복수의 사용자 각각에게 상기 생성된 식별자를 전송하는 단계

를 더 포함하는 것을 특징으로 하는 블록체인을 이용한 개인정보 관리 방법.

청구항 3

제2항에 있어서,

상기 생성된 식별자를 전송하는 단계의 이후에,

상기 관리장치가 상기 복수의 사용자 중 하나인 제1 사용자로부터 상기 식별자 및 조회 대상에 관한 정보인 조회정보를 포함하는 정보조회요청을 수신하는 단계;

상기 관리장치가 상기 제1 사용자에게 소정의 인증 정보를 요청하는 사용자인증요청을 전송하는 단계;

상기 관리장치가가 상기 제1 사용자로부터 상기 인증 정보를 수신하는 단계;

상기 관리장치가가, 상기 인증 정보의 수신에 따라 상기 식별자가 포함된 블록의 조회를 수행하는 체인코드인 조회체인코드가 동작함으로써, 상기 메인채널 또는 상기 서브채널로부터 상기 조회정보에 대응되는 결과정보를 획득하는 단계; 및

상기 관리장치가가 상기 결과정보를 상기 제1 사용자에게 전송하는 단계

를 더 포함하는 것을 특징으로 하는 블록체인을 이용한 개인정보 관리 방법.

청구항 4

제2항에 있어서,

상기 생성된 식별자를 전송하는 단계의 이후에,

상기 관리장치가가 상기 복수의 사용자 중 하나인 제1 사용자로부터 상기 식별자 및 선택적으로 수정 대상에 관한 정보인 수정정보를 포함하는 정보변경요청을 수신하는 단계;

상기 관리장치가가 상기 제1 사용자에게 소정의 인증 정보를 요청하는 사용자인증요청을 전송하는 단계;

상기 관리장치가가 상기 제1 사용자로부터 상기 인증 정보를 수신하는 단계;

상기 관리장치가가, 상기 인증 정보의 수신에 따라 상기 식별자가 포함된 블록의 변경을 수행하는 체인코드인 변경체인코드가 동작함으로써, 상기 수정정보의 포함 여부에 따라 상기 메인채널 또는 상기 서브채널로부터 상기 식별자에 대응되는 개인정보를 수정 또는 삭제하는 단계; 및

상기 관리장치가가 상기 수정 또는 삭제의 결과에 관한 정보인 변경정보를 상기 제1 사용자에게 전송하는 단계

를 더 포함하는 것을 특징으로 하는 블록체인을 이용한 개인정보 관리 방법.

청구항 5

제1항에 있어서,

상기 적어도 하나의 서비스 제공자 중 하나인 대상 서비스 제공자가 상기 복수의 사용자 중 하나인 제2 사용자로부터 서비스 제공을 요청받았을 때,

상기 관리장치가가 상기 대상 서비스 제공자로부터 상기 제2 사용자에 대응되는 식별자 및 조회 대상에 관한 정보인 조회정보를 포함하는 정보조회요청을 수신하는 단계;

상기 관리장치가가 상기 제2 사용자에게 소정의 인증 정보를 요청하는 사용자인증요청을 전송하는 단계;

상기 관리장치가가 상기 제2 사용자로부터 상기 인증 정보를 수신하는 단계;

상기 관리장치가가, 상기 인증 정보의 수신에 따라 상기 식별자가 포함된 블록에 저장된 조회에 대응되는 체인코드인 조회체인코드가 동작함으로써, 상기 메인채널 또는 상기 서브채널로부터 상기 조회정보에 대응되는 결과정보를 획득하는 단계; 및

상기 관리장치가가 상기 결과정보를 상기 대상 서비스 제공자에게 전송하는 단계

를 더 포함하는 것을 특징으로 하는 블록체인을 이용한 개인정보 관리 방법.

청구항 6

제3항 내지 제5항 중 어느 한 항에 있어서,

상기 체인코드의 동작 이후에, 상기 관리장치가 상기 체인코드의 동작에 대응되는 로그를 기록하는 단계

를 더 포함하는 것을 특징으로 하는 블록체인을 이용한 개인정보 관리 방법.

청구항 7

적어도 하나의 서비스 제공자로부터 서비스를 제공받기 위해 복수의 사용자가 개인정보를 저장 및 관리하는 블록체인 네트워크의 관리장치에 있어서,

상기 복수의 사용자 각각으로부터 개인을 식별하기 위한 정보인 개인식별정보와 개인에 대한 추가적인 정보인 추가정보를 포함하는 개인정보를 수신하는 통신부;

상기 복수의 사용자 각각에 대하여 상기 개인식별정보를 이용하여 고유한 식별자를 생성하는 식별자생성부; 및

상기 식별자 및 상기 개인식별정보를 포함하는 블록을 상기 블록체인 네트워크의 메인채널에 추가하고, 상기 식별자 및 상기 추가정보를 포함하는 블록을 상기 블록체인 네트워크의 서브채널에 추가하는 블록체인연결부;

를 포함하고,

상기 메인채널은 블록체인 네트워크의 서비스 제공자와 관리자를 포함하는모든 구성원이 접근 가능한 채널이고, 상기 서브채널은 관리자가 접근 가능한 채널인 것을 특징으로 하는 개인정보를 저장 및 관리하는 블록체인 네트워크 관리장치.

청구항 8

제7항에 있어서,

상기 적어도 하나의 서비스 제공자 중 하나인 대상 서비스 제공자가 상기 복수의 사용자 중 하나인 제2 사용자로부터 서비스 제공을 요청받았을 때,

상기 통신부는 상기 대상 서비스 제공자로부터 상기 제2 사용자에 대응되는 식별자 및 조회 대상에 관한 정보인 조회정보를 포함하는 정보조회요청을 수신하고, 상기 제2 사용자에게 소정의 인증 정보를 요청하는 사용자인증요청을 전송하고, 상기 제2 사용자로부터 상기 인증 정보를 수신하며,

상기 블록체인연결부는 상기 인증 정보의 수신에 따라 상기 식별자가 포함된 블록에 저장된 조회에 대응되는 체인코드인 조회체인코드가 동작함으로써, 상기 메인채널 또는 상기 서브채널로부터 상기 조회정보에 대응되는 결과정보를 획득하고,

상기 통신부는 상기 결과정보를 상기 대상 서비스 제공자에게 전송하는 것을 특징으로 하는 개인정보를 저장 및 관리하는 블록체인 네트워크 관리장치.

청구항 9

제8항에 있어서,

상기 조회체인코드의 동작 이후에, 상기 조회체인코드의 동작에 대응되는 로그를 기록하는 로그기록부

를 더 포함하는 것을 특징으로 하는 개인정보를 저장 및 관리하는 블록체인 네트워크 관리장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 블록체인을 이용하여 개인정보를 관리하는 방법 및 그 방법이 적용된 블록체인 네트워크 관리자에 관한 것이다.

배 경 기 술

[0002] 인터넷을 이용한 서비스를 제공받기 위해서 사용자는 서비스 업체에 회원 가입과 같은 형태로 등록하여야만 해당 서비스를 제공받을 수 있다. 이를 위해 사용자는 자신의 개인정보를 서비스 업체에 제공하게 된다. 이 과정에서 휴대폰 인증, 아이핀, 공인인증서 등을 통해 개인을 인증하고 정보를 제공할 수 있다. 하지만, 각 서비스 업체별로 개인정보가 개별적으로 관리되고 있으며, 통합적으로는 관리되고 있지 않은 상황이다.

[0003] 또한, 개인정보를 각 업체별로 저장 및 관리 하고 있기 때문에 개인정보 보호를 위해 침입탐지 시스템, 방화벽, 접근제어 시스템 등 다양한 보안 장비를 독자적으로 운용해야 한다. 하지만 악의적인 사용자에 의한 공격 기술의 고도화로 인해 모든 공격으로부터 개인정보 유출을 방지하는 것은 현실적으로 어려우며, 개인정보의 내부 유출 또한 지속적으로 발생하고 있다. 나아가 이러한 피해 상황이 발생하는 것을 실시간으로 확인하기 어렵기 때문에 개인정보 유출로 인한 보이스피싱, 명의도용 등의 2차 피해가 발생되고 있다.

[0004] 따라서, 여러 서비스 업체에서 이용되는 사용자의 개인정보를 통합적으로 관리할 뿐만 아니라, 높은 보안성과 신뢰성을 확보할 수 있는 개인정보 관리 방법에 대한 필요성이 대두되고 있다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 한국등록특허공보 제10-1893729호(2018.8.24)

발명의 내용

해결하려는 과제

[0006] 본 발명은 블록체인을 이용하여 사용자의 개인정보를 통합 관리함으로써, 개인정보에 대한 높은 보안성과 신뢰성을 확보하는 개인정보의 유통 및 관리 방법을 제공하고자 한다.

[0007] 본 발명의 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0008] 상기 목적을 달성하기 위해, 본 발명에서 제공하는 블록체인을 이용한 개인정보 관리 방법은 적어도 하나의 서비스 제공자로부터 서비스를 제공받기 위해 복수의 사용자가 개인정보를 블록체인 네트워크에 저장하여 관리하는 방법에 있어서, 상기 블록체인 네트워크의 관리자가 상기 복수의 사용자 각각으로부터 개인을 식별하기 위한 정보인 개인식별정보와 개인에 대한 추가적인 정보인 추가정보를 포함하는 개인정보를 수신하는 단계; 상기 관리자가 상기 복수의 사용자 각각에 대하여 상기 개인식별정보를 이용하여 고유한 식별자를 생성하는 단계; 상기 관리자가 상기 식별자 및 상기 개인식별정보를 포함하는 블록을 상기 적어도 하나의 서비스 제공자와 상기 관리자를 포함하는 상기 블록체인 네트워크의 메인채널에 추가하는 단계; 및 상기 관리자가 상기 식별자 및 상기 추가정보를 포함하는 블록을 상기 관리자를 포함하는 상기 블록체인 네트워크의 서브채널에 추가하는 단계를 포함한다.

[0009] 바람직하게는, 상기 고유한 식별자를 생성하는 단계의 이후에, 상기 관리자가 상기 복수의 사용자 각각에게 상기 생성된 식별자를 전송하는 단계를 더 포함할 수 있다.

[0010] 바람직하게는, 상기 생성된 식별자를 전송하는 단계의 이후에, 상기 관리자가 상기 복수의 사용자 중 하나인 제1 사용자로부터 상기 식별자 및 조회 대상에 관한 정보인 조회정보를 포함하는 정보조회요청을 수신하는 단계; 상기 관리자가 상기 제1 사용자에게 소정의 인증 정보를 요청하는 사용자인증요청을 전송하는 단계; 상기 관리자가 상기 제1 사용자로부터 상기 인증 정보를 수신하는 단계; 상기 관리자가, 상기 인증 정보의 수신에 따라 상기 식별자가 포함된 블록의 조회를 수행하는 체인코드인 조회체인코드가 동작함으로써, 상기 메인채널 또는 상기 서브채널로부터 상기 조회정보에 대응되는 결과정보를 획득하는 단계; 및 상기 관리자가 상기 결과정보를 상기 제1 사용자에게 전송하는 단계를 더 포함할 수 있다.

[0011] 바람직하게는, 상기 생성된 식별자를 전송하는 단계의 이후에, 상기 관리자가 상기 복수의 사용자 중 하나인 제1 사용자로부터 상기 식별자 및 선택적으로 수정 대상에 관한 정보인 수정정보를 포함하는 정보변경요청을 수신하는 단계; 상기 관리자가 상기 제1 사용자에게 소정의 인증 정보를 요청하는 사용자인증요청을 전송하는 단계; 상기 관리자가 상기 제1 사용자로부터 상기 인증 정보를 수신하는 단계; 상기 관리자가, 상기 인증 정보의 수신에 따라 상기 식별자가 포함된 블록의 변경을 수행하는 체인코드인 변경체인코드가 동작함으로써, 상기 수정정보의 포함 여부에 따라 상기 메인채널 또는 상기 서브채널로부터 상기 식별자에 대응되는 개인정보를 수정 또는 삭제하는 단계; 및 상기 관리자가 상기 수정 또는 삭제의 결과에 관한 정보인 변경정보를 상기 제1 사용자에게 전송하는 단계를 더 포함할 수 있다.

[0012] 바람직하게는, 상기 적어도 하나의 서비스 제공자 중 하나인 대상 서비스 제공자가 상기 복수의 사용자 중 하나인 제2 사용자로부터 서비스 제공을 요청받았을 때, 상기 관리자가 상기 대상 서비스 제공자로부터 상기 제2 사용자에 대응되는 식별자 및 조회 대상에 관한 정보인 조회정보를 포함하는 정보조회요청을 수신하는 단계; 상기 관리자가 상기 제2 사용자에게 소정의 인증 정보를 요청하는 사용자인증요청을 전송하는 단계; 상기 관리자가 상기 제2 사용자로부터 상기 인증 정보를 수신하는 단계; 상기 관리자가, 상기 인증 정보의 수신에 따라 상기 식별자가 포함된 블록에 저장된 조회에 대응되는 체인코드인 조회체인코드가 동작함으로써, 상기 메인채널 또는 상기 서브채널로부터 상기 조회정보에 대응되는 결과정보를 획득하는 단계; 및 상기 관리자가 상기 결과정보를 상기 대상 서비스 제공자에게 전송하는 단계를 더 포함할 수 있다.

[0013] 바람직하게는, 상기 체인코드의 동작 이후에, 상기 관리자가 상기 체인코드의 동작에 대응되는 로그를 기록하는 단계를 더 포함할 수 있다.

[0014] 또한, 상기 목적을 달성하기 위해, 본 발명에서 제공하는 개인정보를 저장 및 관리하는 블록체인 네트워크 관리자는 적어도 하나의 서비스 제공자로부터 서비스를 제공받기 위해 복수의 사용자가 개인정보를 저장 및 관리하는 블록체인 네트워크의 관리자에 있어서, 상기 복수의 사용자 각각으로부터 개인을 식별하기 위한 정보인 개인식별정보와 개인에 대한 추가적인 정보인 추가정보를 포함하는 개인정보를 수신하는 통신부; 상기 복수의 사용

자 각각에 대하여 상기 개인식별정보를 이용하여 고유한 식별자를 생성하는 식별자생성부; 및 상기 식별자 및 상기 개인식별정보를 포함하는 블록을 상기 적어도 하나의 서비스 제공자와 상기 관리자를 포함하는 상기 블록체인 네트워크의 메인채널에 추가하고, 상기 식별자 및 상기 추가정보를 포함하는 블록을 상기 관리자를 포함하는 상기 블록체인 네트워크의 서브채널에 추가하는 블록체인연결부;를 포함한다.

[0015] 바람직하게는, 상기 적어도 하나의 서비스 제공자 중 하나인 대상 서비스 제공자가 상기 복수의 사용자 중 하나인 제2 사용자로부터 서비스 제공을 요청받았을 때, 상기 통신부는 상기 대상 서비스 제공자로부터 상기 제2 사용자에 대응되는 식별자 및 조회 대상에 관한 정보인 조회정보를 포함하는 정보조회요청을 수신하고, 상기 제2 사용자에게 소정의 인증 정보를 요청하는 사용자인증요청을 전송하고, 상기 제2 사용자로부터 상기 인증 정보를 수신하며, 상기 블록체인연결부는 상기 인증 정보의 수신에 따라 상기 식별자가 포함된 블록에 저장된 조회에 대응되는 체인코드인 조회체인코드가 동작함으로써, 상기 메인채널 또는 상기 서브채널로부터 상기 조회정보에 대응되는 결과정보를 획득하고, 상기 통신부는 상기 결과정보를 상기 대상 서비스 제공자에게 전송할 수 있다.

[0016] 바람직하게는, 상기 조회체인코드의 동작 이후에, 상기 조회체인코드의 동작에 대응되는 로그를 기록하는 로그기록부를 더 포함할 수 있다.

발명의 효과

[0017] 본 발명은 블록체인을 활용해 사용자의 정보를 관리자가 통합하여 관리함으로써 서비스 제공자의 개별적인 개인정보 저장 및 관리 필요성이 사라진다. 즉, 서비스 제공자는 개인정보를 저장하지 않기 때문에 개인정보 유출을 방지할 수 있다. 또한 사용자의 개인정보 관리를 관리자가 전담하기 때문에 서비스 제공자는 이에 관련된 시스템 운영비용을 절감할 수 있다.

[0018] 또한, 본 발명에서 사용자와 서비스 제공자는 단계별로 저장되는 개인정보에 직접적인 접근이 불가능하며, 서비스 제공자의 경우 사용자의 요청없이는 조회 요청 또한 불가능하기 때문에 기존의 개인 정보 관리 대비 높은 보안성을 확보한다. 또한, 관리자를 통한 개인정보 조회 또는 변경 시, 해당 내역을 네트워크에 저장함으로써 관리자에 대한 신뢰성을 확보할 수 있다.

[0019] 또한, 본 발명에서 저장하는 개인정보는 사용자의 필요에 따라 그 범위를 확장시킬 수 있다. 사용자는 다수의 서비스 제공자가 필요로 하는 개인정보 외의 정보를 블록체인에 저장할 수 있다. 즉, 사용자는 한 번의 정보 저장으로 다수의 서비스 제공자에게 정보를 전달 할 수 있게 되므로 편리성이 증대될 수 있다.

[0020] 본 발명의 효과들은 이상에서 언급한 효과들로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0021] 도 1은 본 발명의 일 실시 예에 따른 블록체인을 이용한 개인정보 관리 방법을 나타내는 흐름도이다.

도 2는 본 발명의 일 실시 예에 따른 사용자의 개인정보 조회 방법을 나타내는 흐름도이다.

도 3은 본 발명의 일 실시 예에 따른 사용자의 개인정보 변경 방법을 나타내는 흐름도이다.

도 4는 본 발명의 일 실시 예에 따른 서비스 제공자의 개인정보 조회 방법을나타내는 흐름도이다.

도 5는 본 발명의 일 실시 예에 따른 개인정보를 저장 및 관리하는 블록체인 네트워크 관리자를 나타내는 블록도이다.

도 7 및 8은 본 발명의 일 실시예에 따른 메인채널 및 서브채널의 블록의 구조를 나타내는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0022] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면을 참조하여 상세하게 설명하도록 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0023] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수

있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재 항목들의 조합 또는 복수의 관련된 기재 항목들 중의 어느 항목을 포함한다.

[0024] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급될 때에는 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0025] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0026] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0027] 명세서 및 청구범위 전체에서, 어떤 부분이 어떤 구성 요소를 포함한다고 할때, 이는 특별히 반대되는 기재가 없는 한 다른 구성 요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있다는 것을 의미한다.

[0028] 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0029] 블록체인은 사토시 나카모토가 투고한 논문인 "Bitcoin : A Peer-to-Peer Electronic Cash System"에서 처음으로 구현되었다. 블록체인은 분산되고 독립적이며 개방된 공통 장부 관리기술이다. 블록체인에 참여한 모든 사용자는 공통 장부의 내용을 소유하고 있고 과반수 이상의 참여자가 인정한 블록만이 블록체인에 연결된다. 초기에 블록체인은 가상화폐의 기반기술로 사용되었지만 최근에는 기존에 존재하던 시스템을 대체하는 비즈니스 모델을 제시하고 있다. 블록체인을 통하여 저가의 비용으로 기존의 서비스나 새로운 서비스를 구축할 수 있기 때문이다. 또한 공유 원장을 통한 무결성 유지로 로그 기반의 서비스에 많이 적용 되고 있다.

[0030] 본 발명에서 사용자, 관리자, 서비스 제공자는 그 사용자, 관리자, 서비스 제공자 각각이 이용하는 스마트폰, 노트북컴퓨터, 데스크탑컴퓨터, 태블릿PC 또는 기타 컴퓨팅 장치를 의미할 수 있다.

[0031] 한편, 도 6을 참조하여, 본 발명의 사용자, 관리자, 서비스 제공자를 설명한다.

[0032] 관리자는 본 발명에서 신뢰할 수 있는 기관의 역할을 수행할 수 있다. 즉, 모든 서비스 제공자들과 사용자들의 기본적인 개인정보와 추가적인 정보를 블록체인에 등록하고 관리하는 역할을 수행할 수 있다. 또한, 서비스 제공자들에게 사용자의 개인정보가 필요한 경우, 이를 제공할 수 있다. 또한, 관리자는 블록체인 네트워크에 속해 있는 노드들의 인증서와 개인키/공개키를 관리할 수 있다. 관리자는 개인정보를 생성, 수정, 열람할 수 있는 서비스 모듈을 제공하고 있으며 사용자는 분산 앱을 통해 개인정보를 관리할 수 있다. 서비스 제공자는 관리자와 같은 블록체인 네트워크에 포함되어 있으며 요청/서비스 모듈을 통해 정보를 교환할 수 있다.

[0033] 서비스 제공자는 일반적으로 인터넷을 이용하여 사용자들에게 다양한 서비스를 제공하는 역할을 수행할 수 있다. 서비스 제공자는 관리자에게 필요한 사용자의 개인정보를 요청하고, 이를 제공받아 사용자에게 서비스를 제공할 수 있다. 서비스 제공자가 사용자의 개인정보를 요청하기 위해서는 사전에 관리자로부터 인증을 받아야 할 수 있다. 서비스 제공자는 단독으로 사용자의 개인정보를 열람할 수 없으며, 사용자의 요청이 있을 경우에만 개인정보를 열람할 수 있다.

[0034] 사용자는 관리자에게 자신의 개인정보를 블록체인에 저장하도록 제공하고, 자신의 개인정보를 보호 받을 수 있다. 사용자는 관리자로부터 부여 받은 식별자를 갖고 있으며, 이 식별자는 개인정보 열람, 수정, 삭제 등의 기능에 사용될 수 있다. 일반적으로 블록체인의 데이터는 삭제가 불가능하나, 예컨대, 사용자의 사망 또는 이민 등으로 인해, 불가피하게 삭제가 필요할 경우, 사용자의 식별자에 해당하는 데이터를 공백으로 변경하여 삭제와 같은 기능을 수행할 수 있다. 서비스 제공자로부터의 개인정보 열람 요청 시, 관리자는 사용자의 동의 여부를 확인하고 원하는 특정 서비스 제공자에 개인정보를 전달할 수 있다.

[0035] 도 1은 본 발명의 일 실시 예에 따른 블록체인을 이용한 개인정보 관리 방법을 나타내는 흐름도이다.

[0036] 단계 S110에서는, 블록체인 네트워크의 관리자가 복수의 사용자 각각으로부터 개인을 식별하기 위한 정보인 개인식별정보와 개인에 대한 추가적인 정보인 추가정보를 포함하는 개인정보를 수신한다.

[0037] 여기서, 복수의 사용자는 적어도 하나의 서비스 제공자가 제공하는 서비스의 사용자일 수 있다. 또한, 서비스 제공자가 제공하는 서비스는 인터넷을 통해 제공되는 다양한 종류의 서비스일 수 있다. 예컨대, 게임, 쇼핑, 음악, 영화, 동영상 스트리밍 등이 해당할 수 있다.

[0038] 개인식별정보는 개인을 식별하기 위해 이용되는 정보일 수 있다. 예컨대, 사용자 ID, 이름, 연락처 등일 수 있다. 또한, 추가정보는 개인식별정보 이외에 다양한 사용자의 개인정보일 수 있다. 예컨대, 주민등록번호, 주소, 암호 등일 수 있다.

[0039] 바람직하게는, 추가정보는 개인식별정보보다 더 보안에 민감한 정보일 수 있다. 이는 아래에서 설명하는 바와 같이, 본 발명에서 보안 상의 이유로 블록체인 네트워크가 메인채널과 서브채널로 구분되어 별도로 관리되기 때문일 수 있다.

[0040] 단계 S120에서는, 관리자가 그 복수의 사용자 각각에 대하여 개인식별정보를 이용하여 고유한 식별자를 생성한다.

[0041] 이때, 식별자는 개인식별정보를 기반으로 하여 생성된 고유한 상수값을 의미할 수 있다. 예컨대, 개인식별정보에 ID, 이름, 연락처가 포함되는 경우를 가정할 때, ID, 이름, 연락처가 모두 같은 사용자는 존재하지 않을 것이므로, 관리자는 복수의 사용자에 대하여 모두 상이한 식별자를 생성할 수 있게 된다.

[0042] 단계 S130에서는, 관리자가 식별자 및 개인식별정보를 포함하는 블록을 적어도 하나의 서비스 제공자와 관리자를 포함하는 블록체인 네트워크의 메인채널에 추가한다.

[0043] 여기서, 도 7을 참조하면, 메인채널의 블록은 블록 헤더, 트랜잭션 정보, 합의 정보, 데이터 부분으로 구성될 수 있으며, 블록의 헤더 부분에는 블록의 번호, 이전 블록의 해시값, 현재 블록의 해시값이 저장될 수 있다. 트랜잭션 정보 부분에는 트랜잭션을 실행할 때 사용하는 체인코드 관련 정보가 저장될 수 있다. 합의 정보 부분에는 트랜잭션 제출 시에 합의한 노드들의 인증서, 공개키, 전자 서명이 저장될 수 있다. 메인채널은 블록체인 네트워크의 모든 노드가 참여하는 채널로서 식별자와 개인식별정보(예, 이름, 연락처, ID 등)를 데이터 부분에 저장할 수 있다. 식별자는 네트워크 내에서 사용자를 식별하기 위해 저장되며, 개인식별정보는 인증된 사용자임을 증명할 때 식별자와 함께 사용될 수 있다.

[0044] 마지막으로 단계 S140에서는, 관리자가 식별자 및 추가정보를 포함하는 블록을 관리자를 포함하는 블록체인 네트워크의 서브채널에 추가한다.

[0045] 여기서, 도 8을 참조하면, 서브채널의 블록의 헤더, 트랜잭션 정보, 합의 정보 부분은 메인채널 블록의 구성과 동일할 수 있다. 서브채널 블록의 데이터 부분에는 어떤 사용자의 정보인지 식별할 수 있는 식별자와 추가정보(예, 주민등록번호, 주소, 인증된 사용자임을 증명하는 Password)와 같은 개인정보를 저장할 수 있다. 추후 추가적인 정보의 저장을 위해 개설되는 또 다른 서브채널의 블록도 같은 구성을 가지고 있으며 저장되는 추가정보의 특성에 따라 블록의 데이터부분만 변경될 수 있다.

[0046] 다른 실시예에서는, 관리자가 복수의 사용자 각각에게 그 생성된 식별자를 전송할 수 있다.

[0047] 이때, 복수의 사용자는 개인정보의 조회, 삭제, 수정 등을 위해 전송된 식별자를 이용할 수 있다. 이에 관한 구체적인 내용은 도 2 내지 도 4에 대한 설명에서 구체적으로 후술한다.

[0048] 또 다른 실시예에서는, 관리자가 하나의 메인채널과 복수의 서브채널을 포함하는 블록체인 네트워크를 이용하여 서비스를 제공할 수 있다.

[0049] 이때, 메인채널은 사용자와 관리자, 서비스 제공자가 참여하고 있으며, 개인정보 유통에 대한 기본적인 거래가 이루어지는 채널일 수 있다. 메인채널에는 사용자를 식별할 수 있는 정보(식별자)가 저장되며, 사용자 및 서비스 제공자는 그 식별자를 이용하여 주요 개인정보를 요청할 수 있다. 또한, 서브채널은 관리자만 포함되어 있는 채널로서 사용자의 요청에 의해 주요 개인정보 외의 추가적인 정보를 저장할 수 있다. 서브채널은 메인채널에 저장된 식별자를 공유하여 식별자에 해당되는 사용자의 추가 정보를 제공할 수 있다. 또한 서브채널은 유통하고자 하는 사용자의 개인정보에 따라 추가로 개설될 수 있다.

[0050] 다시 말하면, 메인채널은 사용자의 식별자를 저장하고 서브채널은 실제 개인정보를 저장함으로써, 개인정보를 단계별로 관리할 수 있다. 즉, 메인채널은 블록체인 네트워크의 모든 구성원이 접근할 수 있으나 서브채널에는 사용자의 직접적인 개인정보가 보관되기 때문에 관리자만 접근이 가능할 수 있다. 이처럼 채널별로 접근 권한을 제한함으로써 외부로부터의 침입 및 해킹을 방지할 수 있다. 따라서 사용자의 민감한 개인정보는 관리자를 통해서만 열람할 수 있다. 추후 관리자는 사용자의 필요에 따라 추가정보를 저장하고자 할 때 새로운 서브채널을 개설하여 저장할 수 있다. 이처럼, 다수의 서브채널을 이용하여 사용자의 개인정보를 분산하여 저장하는 것은 관리를 용이하게 하고 시스템의 전체적인 보안성을 향상시킬 수 있다.

[0051] 도 2는 본 발명의 일 실시 예에 따른 사용자의 개인정보 조회 방법을 나타내는 흐름도이다.

[0052] 한편, 아래의 도 2에 대한 설명은 도 1에 대하여 설명한 과정이 모두 완료된 것을 가정한다.

[0053] 단계 S210에서는, 관리자가 그 복수의 사용자 중 하나인 제1 사용자로부터 식별자 및 조회 대상에 관한 정보인 조회정보를 포함하는 정보조회요청을 수신한다.

[0054] 예컨대, 관리자는 제1 사용자로부터 식별자 및 ID에 관한 조회를 요청하는 조회정보를 포함하는 정보조회요청을 수신할 수 있다.

[0055] 단계 S220에서는, 관리자가 제1 사용자에게 소정의 인증 정보를 요청하는 사용자인증요청을 전송한다.

[0056] 즉, 관리자는 제1 사용자가 정보조회를 할 수 있는 당사자인지 확인하기 위하여 사용자인증요청을 전송할 수 있다.

[0057] 단계 S230에서는, 관리자가 제1 사용자로부터 인증 정보를 수신한다.

[0058] 예컨대, 관리자는 사용자인증요청에 대한 응답으로, 제1 사용자로부터 식별자, ID, 패스워드 등과 같은 인증 정보를 수신할 수 있다.

[0059] 단계 S240에서는, 관리자가, 그 인증 정보의 수신에 따라 식별자가 포함된 블록의 조회를 수행하는 체인코드인 조회체인코드가 동작함으로써, 메인채널 또는 서브채널로부터 조회정보에 대응되는 결과정보를 획득한다.

[0060] 여기서, 체인코드는 조건에 부합하면, 사람의 개입없이 계약이 이행되는 일종의 디지털 자동화 계약으로, 스마트 컨트랙트(smart contract)라고도 부른다. 예컨대, 조회체인코드는 관리자가 그 인증 정보를 수신하는 것을 조건으로 하여, 식별자가 포함된 블록의 조회를 수행하는 계약을 실행하는 코드일 수 있다.

[0061] 즉, 관리자는 조회체인코드의 동작으로 인해, 서브채널로부터 조회정보에 대응되는 결과정보를 획득할 수 있다. 예컨대, 조회정보가 주소에 관한 조회를 요청하는 경우에는, 메인채널 또는 서브채널로부터 그 주소에 관한 정보를 획득할 수 있다.

[0062] 마지막으로 단계 S250에서는, 관리자가 그 결과정보를 제1 사용자에게 전송한다.

[0063] 도 3은 본 발명의 일 실시 예에 따른 사용자의 개인정보 변경 방법을 나타내는 흐름도이다.

[0064] 한편, 아래의 도 3에 대한 설명은 도 1에 대하여 설명한 과정이 모두 완료된 것을 가정한다.

[0065] 단계 S310에서는, 관리자가 복수의 사용자 중 하나인 제1 사용자로부터 식별자 및 선택적으로 수정 대상에 관한 정보인 수정정보를 포함하는 정보변경요청을 수신한다.

[0066] 즉, 관리자는 제1 사용자로부터 식별자를 포함하는 정보변경요청을 수신하거나, 식별자와 수정정보를 포함하는 정보변경요청을 수신할 수 있다.

[0067] 이때, 관리자는 정보변경요청에 수정정보가 포함되지 않은 경우에는, 블록체인에서 그 식별자에 대응되는 정보를 삭제해 줄 것을 요청하는 것으로 판단할 수 있다. 또한, 관리자는 정보변경요청에 수정정보가 포함된 경우에는, 블록체인에서 그 식별자에 대응되는 정보를 수정정보에 기반하여 수정해 줄 것을 요청하는 것으로 판단할 수 있다.

[0068] 단계 S320에서는, 관리자가 제1 사용자에게 소정의 인증 정보를 요청하는 사용자인증요청을 전송한다.

[0069] 단계 S330에서는, 관리자가 제1 사용자로부터 인증 정보를 수신한다.

[0070] 단계 S340에서는, 관리자가, 그 인증 정보의 수신에 따라 식별자가 포함된 블록의 변경을 수행하는 체인코드인 변경체인코드가 동작함으로써, 수정정보의 포함 여부에 따라 메인채널 또는 서브채널로부터 그 식별자에 대응되

는 개인정보를 수정 또는 삭제한다.

[0071] 이때, 변경체인코드는 관리자가 그 인증 정보를 수신하는 것을 조건으로 하여, 식별자가 포함된 블록의 변경를 수행하는 계약을 실행하는 코드일 수 있다.

[0072] 보다 구체적으로, 변경체인코드는 정보변경요청에 수정정보가 포함되어 있으면, 식별자가 포함된 블록을 수정하고, 정보변경요청에 수정정보가 포함되어 있지 않으면, 식별자가 포함된 블록의 데이터(예, 식별자, 연락처, ID, 이름, 주소 등)를 삭제할 수 있다.

[0073] 마지막으로 단계 S340에서는, 관리자가 그 수정 또는 삭제의 결과에 관한 정보인 변경정보를 제1 사용자에게 전송한다.

[0074] 도 4는 본 발명의 일 실시 예에 따른 서비스 제공자의 개인정보 조회 방법을나타내는 흐름도이다.

[0075] 한편, 아래의 도 4에 대한 설명은 도 1에 대하여 설명한 과정이 모두 완료된 것을 가정한다.

[0076] 또한, 적어도 하나의 서비스 제공자 중 하나인 대상 서비스 제공자가 복수의 사용자 중 하나인 제2 사용자로부터 서비스 제공을 요청받은 것을 가정한다.

[0077] 단계 S410에서는, 관리자가 대상 서비스 제공자로부터 제2 사용자에 대응되는 식별자 및 조회 대상에 관한 정보인 조회정보를 포함하는 정보조회요청을 수신한다.

[0078] 즉, 관리자는 대상 서비스 제공자로부터 제2 사용자의 식별자 및 제2 사용자의 조회정보를 포함하는 정보조회요청을 수신할 수 있다. 이때, 대상 서비스 제공자는 제2 사용자로부터 서비스 제공을 요청받으면서 식별자를 직접 제공받거나, 제2 사용자의 서비스 제공 요청에 포함된 ID 등의 개인식별정보를 이용하여, 메인채널에 저장된 제2 사용자의 식별자에 관한 정보를 획득할 수 있다.

[0079] 단계 S420에서는, 관리자가 제2 사용자에게 소정의 인증 정보를 요청하는 사용자인증요청을 전송한다.

[0080] 이때, 사용자 인증은 대상 서비스 제공자의 요청이 제2 사용자의 요청에 의한 것인지를 확인하기 위한 것으로, 개인정보 조회 동의를 구하는 형식으로 진행될 수 있다.

[0081] 단계 S430에서는, 관리자가 제2 사용자로부터 인증 정보를 수신한다.

[0082] 단계 S440에서는, 관리자가, 그 인증 정보의 수신에 따라 식별자가 포함된 블록에 저장된 조회에 대응되는 체인코드인 조회체인코드가 동작함으로써, 메인채널 또는 서브채널로부터 조회정보에 대응되는 결과정보를 획득한다.

[0083] 마지막으로 단계 S450에서는, 관리자가 그 결과정보를 대상 서비스 제공자에게 전송한다.

[0084] 이때, 대상 서비스 제공자는 관리자로부터 그 결과정보를 제공받음으로써, 제2 사용자에게 서비스를 제공할 수 있게 된다.

[0085] 다른 실시예에서는, 관리자가 체인코드의 동작 이후에, 체인코드의 동작에 대응되는 로그를 기록한다.

[0086] 예컨대, 관리자는 매번 체인코드가 동작하여 조회 또는 변경을 수행할 때마다, 해당 동작에 대응되는 로그를 블록체인 네트워크 상에 또는 별도의 데이터베이스에 저장할 수 있다.

[0087] 이처럼, 관리자가 체인코드의 동작에 대응되는 로그를 기록하여 보존함으로써, 관리자에 대한 신뢰성을 확보할 수 있다.

[0088] 도 5는 본 발명의 일 실시 예에 따른 개인정보를 저장 및 관리하는 블록체인 네트워크 관리자를 나타내는 블록도이다.

[0089] 도 5를 참조하면, 본 발명의 일 실시 예에 따른 개인정보를 저장 및 관리하는 블록체인 네트워크 관리자(500)는 통신부(510), 식별자생성부(520) 및 블록체인연결부(530)를 포함한다. 선택적으로, 로그기록부(미도시)를 더 포함할 수 있다.

[0090] 통신부(510)는 복수의 사용자 각각으로부터 개인을 식별하기 위한 정보인 개인식별정보와 개인에 대한 추가적인 정보인 추가정보를 포함하는 개인정보를 수신한다.

[0091] 식별자생성부(520)는 그 복수의 사용자 각각에 대하여 개인식별정보를 이용하여 고유한 식별자를 생성한다.

[0092] 블록체인연결부(530)는 그 식별자 및 개인식별정보를 포함하는 블록을 적어도 하나의 서비스 제공자와 관리자를

포함하는 블록체인 네트워크의 메인채널에 추가하고, 그 식별자 및 추가정보를 포함하는 블록을 관리자를 포함하는 블록체인 네트워크의 서브채널에 추가한다.

[0093] 마지막으로 로그기록부(미도시)는 조회체인코드의 동작 이후에, 조회체인코드의 동작에 대응되는 로그를 기록한다.

[0094] 다른 실시예에서는, 적어도 하나의 서비스 제공자 중 하나인 대상 서비스 제공자가 그 복수의 사용자 중 하나인 제2 사용자로부터 서비스 제공을 요청받았을 때, 통신부(510)는 대상 서비스 제공자로부터 제2 사용자에 대응되는 식별자 및 조회 대상에 관한 정보인 조회정보를 포함하는 정보조회요청을 수신하고, 제2 사용자에게 소정의 인증 정보를 요청하는 사용자인증요청을 전송하고, 제2 사용자로부터 인증 정보를 수신할 수 있다.

[0095] 이때, 블록체인연결부(530)는 그 인증 정보의 수신에 따라 식별자가 포함된 블록에 저장된 조회에 대응되는 체인코드인 조회체인코드가 동작함으로써, 메인채널 또는 서브채널로부터 조회정보에 대응되는 결과정보를 획득할 수 있다.

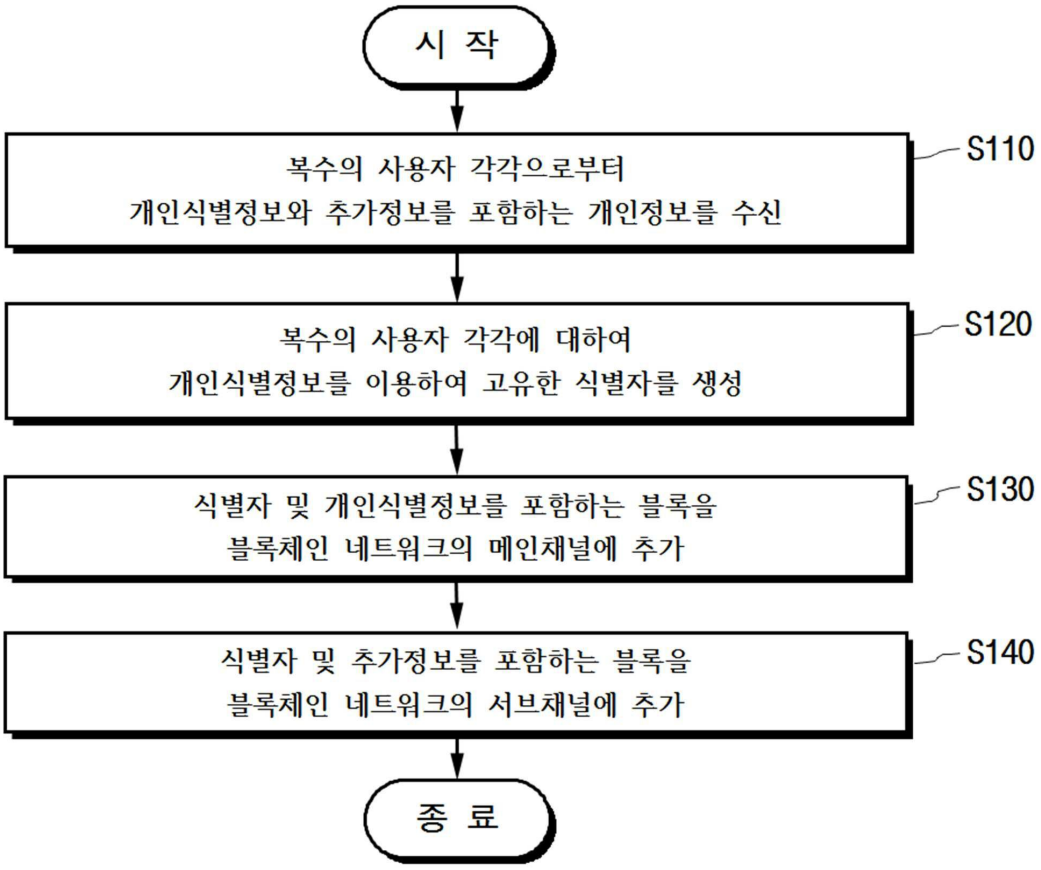
[0096] 또한, 통신부(510)는 그 결과정보를 대상 서비스 제공자에게 전송할 수 있다.

[0097] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 사람이라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

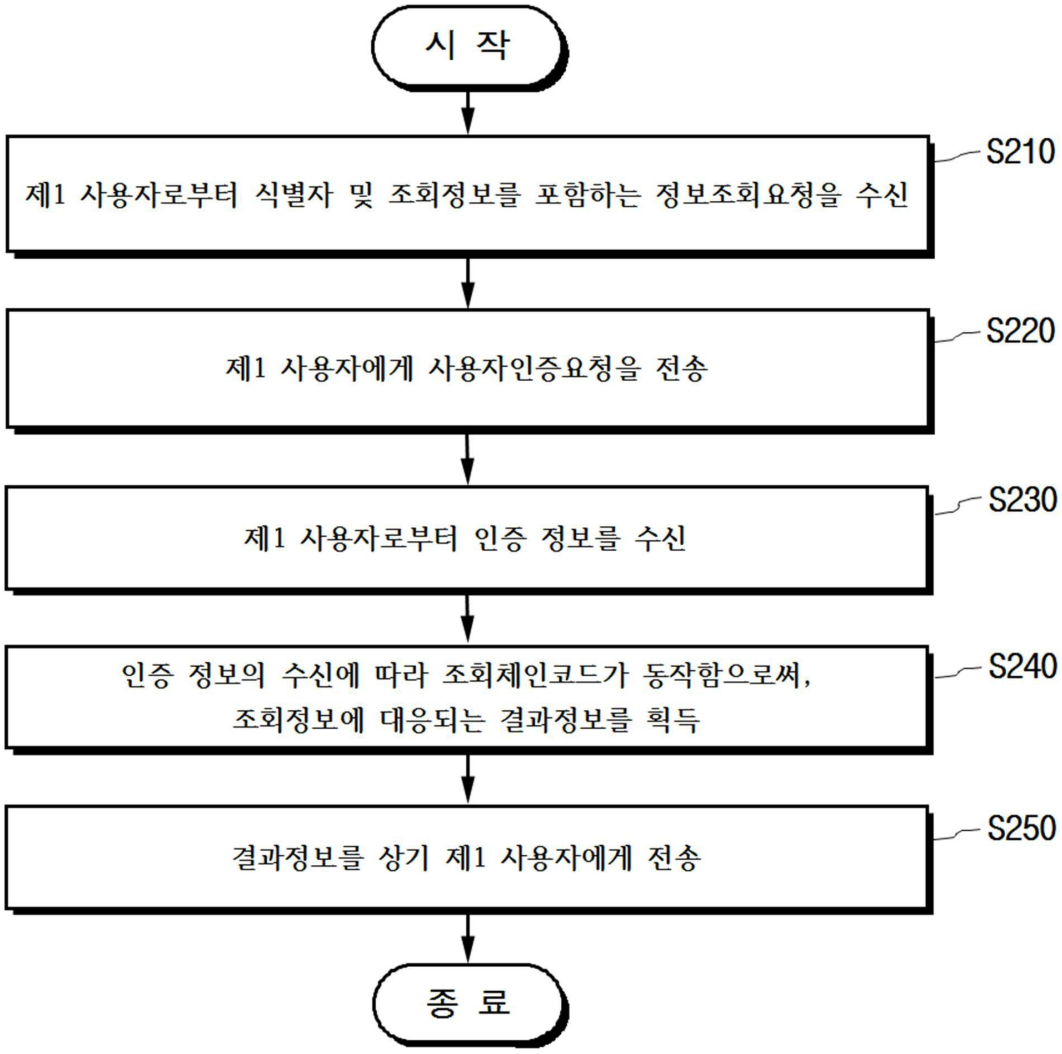
[0098]

도면

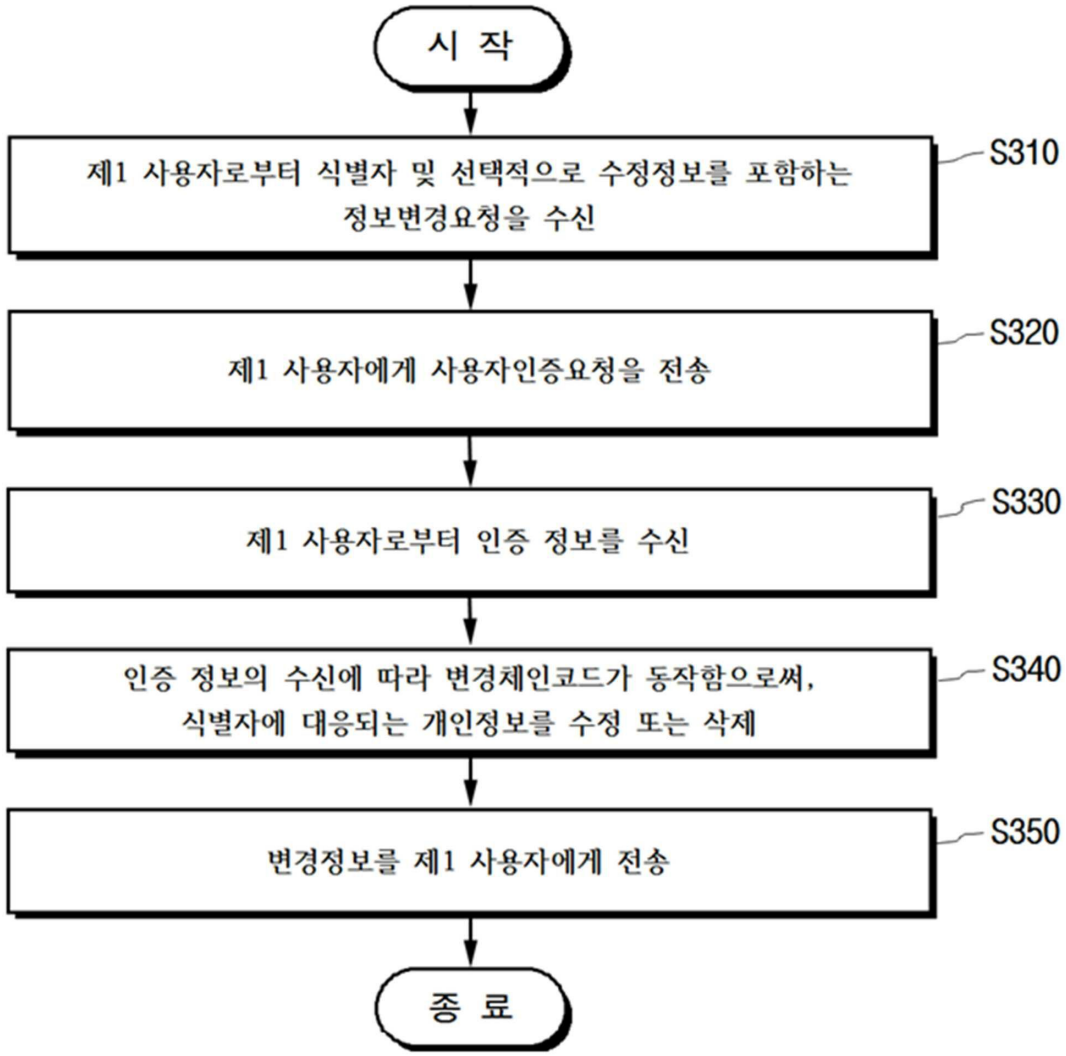
도면1



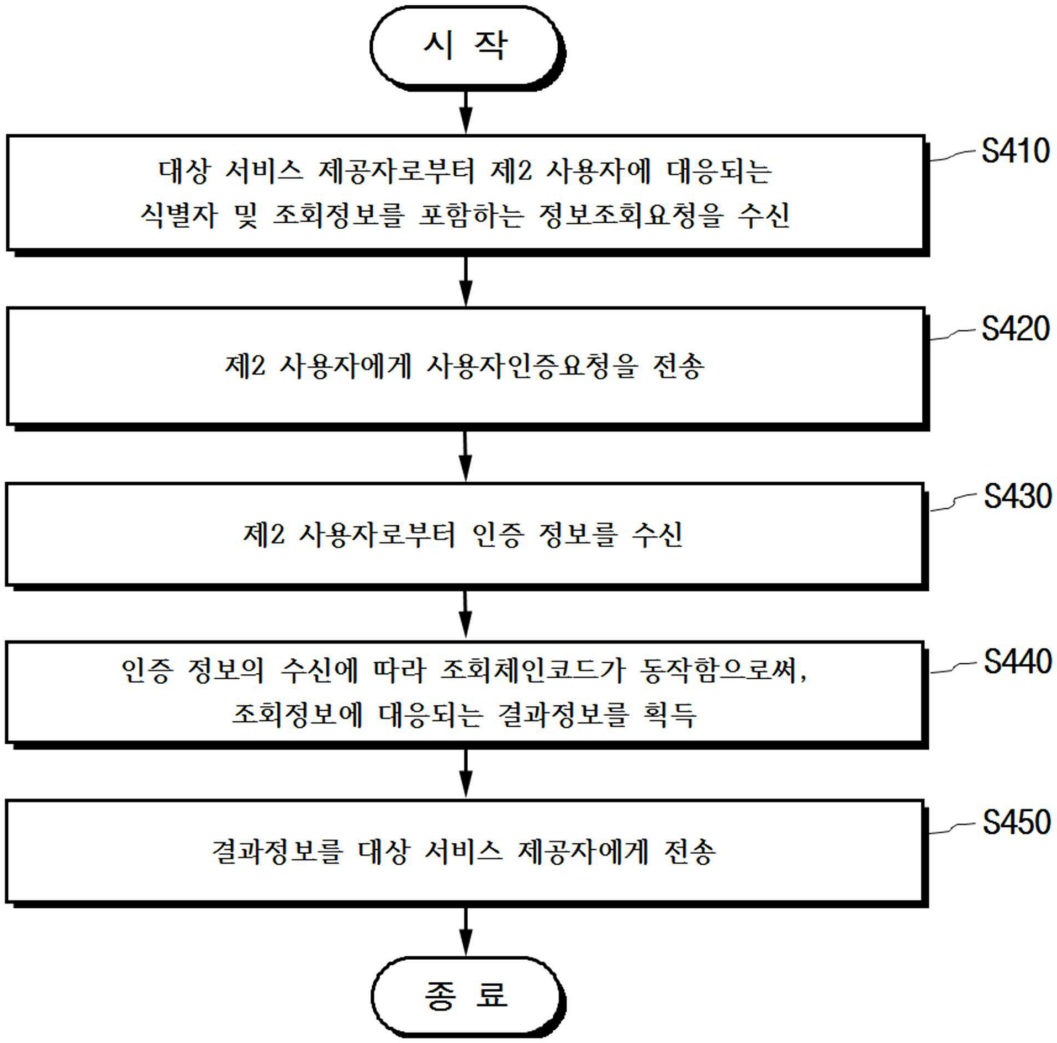
도면2


시 작
제1 사용자로부터 식별자 및 조회정보를 포함하는 정보조회요청을 수신
S210
제1 사용자에게 사용자인증요청을 전송
S220
제1 사용자로부터 인증 정보를 수신
S230
인증 정보의 수신에 따라 조회체인코드가 동작함으로써,
조회정보에 대응되는 결과정보를 획득
S240
결과정보를 상기 제1 사용자에게 전송
S250
종 료

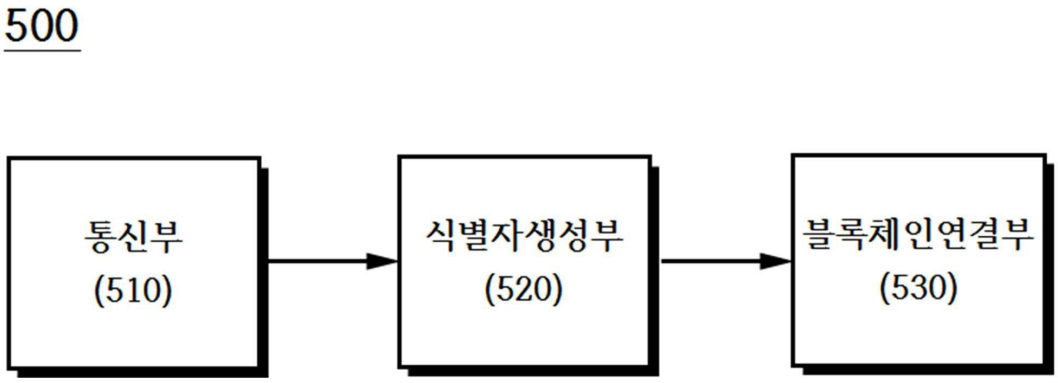
도면3


시 작
제1 사용자로부터 식별자 및 선택적으로 수정정보를 포함하는 정보변경요청을 수신
S310
제1 사용자에게 사용자인증요청을 전송
S320
제1 사용자로부터 인증 정보를 수신
S330
인증 정보의 수신에 따라 변경체인코드가 동작함으로써, 식별자에 대응되는 개인정보를 수정 또는 삭제
S340
변경정보를 제1 사용자에게 전송
S350
종 료

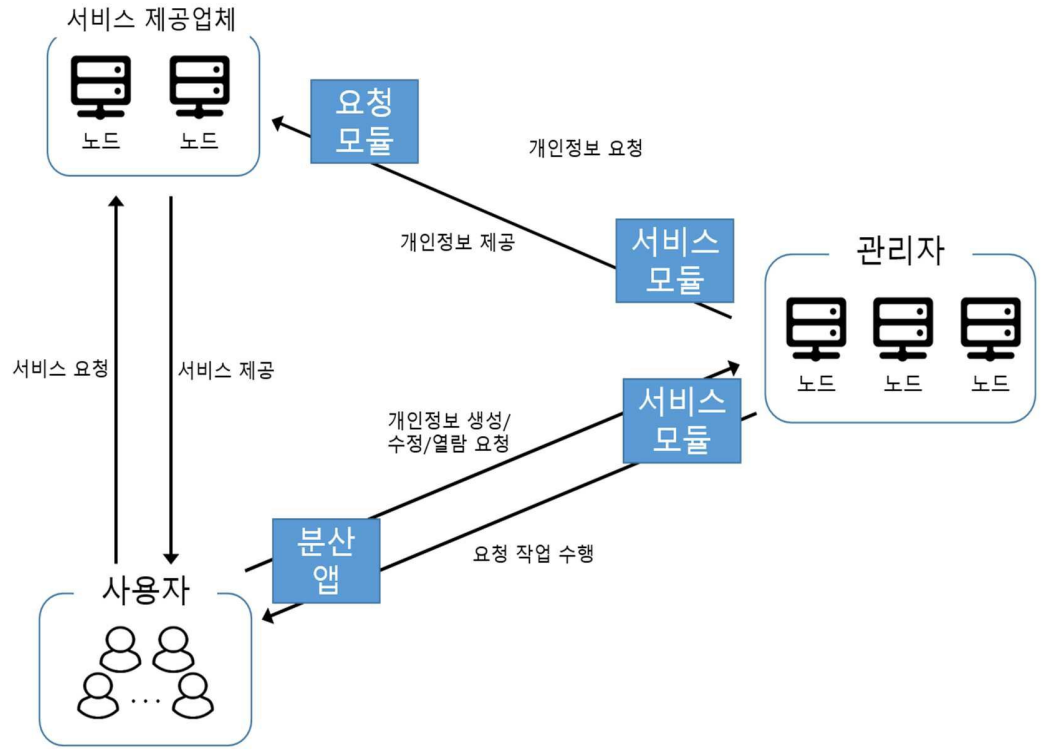
도면4


시 작
대상 서비스 제공자로부터 제2 사용자에 대응되는
식별자 및 조회정보를 포함하는 정보조회요청을 수신
S410
제2 사용자에게 사용자인증요청을 전송
S420
제2 사용자로부터 인증 정보를 수신
S430
인증 정보의 수신에 따라 조회체인코드가 동작함으로써,
조회정보에 대응되는 결과정보를 획득
S440
결과정보를 대상 서비스 제공자에게 전송
S450
종 료

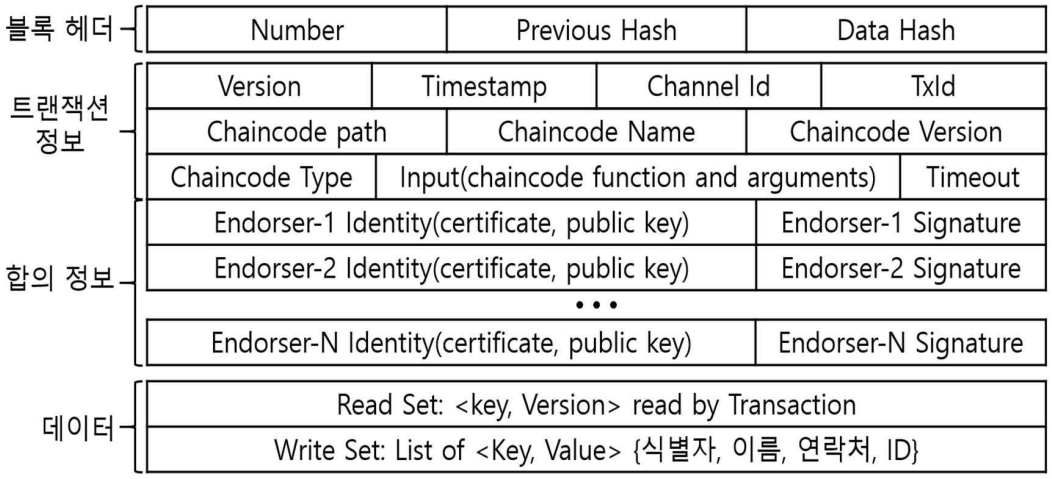
도면5


500
통신부
(510)
식별자생성부
(520)
블록체인연결부
(530)

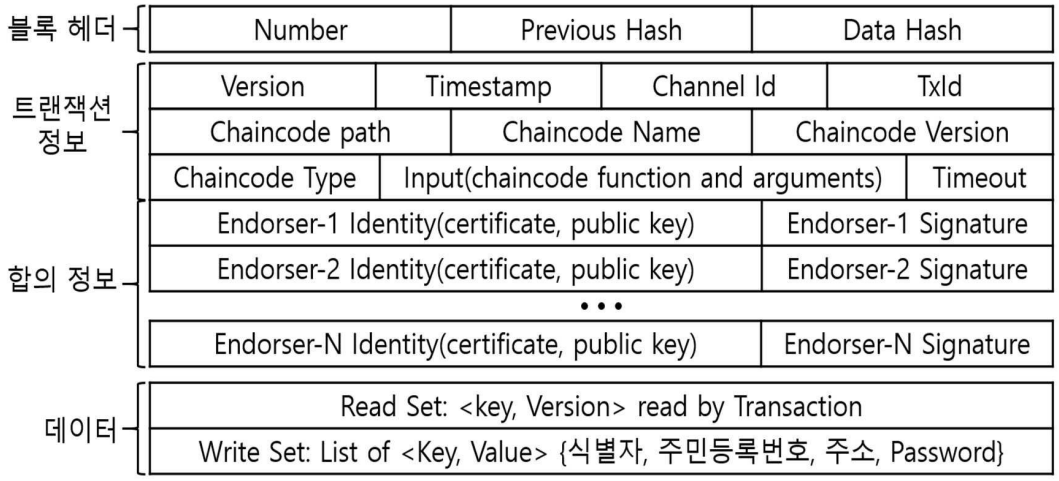
도면6


서비스 제공업체
노드
노드
요청 모듈
개인정보 요청
개인정보 제공
서비스 모듈
관리자
노드
노드
노드
서비스 요청
서비스 제공
개인정보 생성/ 수정/열람 요청
서비스 모듈
분산 앱
요청 작업 수행
사용자

도면7


블록 헤더
Number
Previous Hash
Data Hash
트랜잭션 정보
Version
Timestamp
Channel Id
TxId
Chaincode path
Chaincode Name
Chaincode Version
Chaincode Type
Input(chaincode function and arguments)
Timeout
합의 정보
Endorser-1 Identity(certificate, public key)
Endorser-1 Signature
Endorser-2 Identity(certificate, public key)
Endorser-2 Signature
Endorser-N Identity(certificate, public key)
Endorser-N Signature
데이터
Read Set: <key, Version> read by Transaction
Write Set: List of <Key, Value> {식별자, 이름, 연락처, ID}

도면8


블록 헤더
Number
Previous Hash
Data Hash
트랜잭션 정보
Version
Timestamp
Channel Id
TxId
Chaincode path
Chaincode Name
Chaincode Version
Chaincode Type
Input(chaincode function and arguments)
Timeout
합의 정보
Endorser-1 Identity(certificate, public key)
Endorser-1 Signature
Endorser-2 Identity(certificate, public key)
Endorser-2 Signature
• • •
Endorser-N Identity(certificate, public key)
Endorser-N Signature
데이터
Read Set: <key, Version> read by Transaction
Write Set: List of <Key, Value> {식별자, 주민등록번호, 주소, Password}