



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년04월16일
(11) 등록번호 10-2241246
(24) 등록일자 2021년04월12일

(51) 국제특허분류(Int. Cl.)

G06F 21/64 (2013.01)

(52) CPC특허분류

G06F 21/645 (2013.01)

G06Q 50/26 (2013.01)

(21) 출원번호 10-2020-0078621

(22) 출원일자 2020년06월26일

심사청구일자 2020년06월26일

(56) 선행기술조사문헌

KR101882805 B1*

KR102032780 B1*

WO2020001105 A1*

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

(주)아이앤티

부산광역시 해운대구 센텀중앙로 60, 401호, 402호, 403호(우동, 퍼스트인센텀)

(72) 발명자

박동기

부산광역시 수영구 수영로741번길 46, 206동 1501호 (수영동, 수영협성르네상스타운)

이상민

부산광역시 사하구 하신번영로 400, 106동 2405호 (하단동, 하단동에스케이뷰아파트)

(74) 대리인

특허법인정특

전체 청구항 수 : 총 1 항

심사관 : 구대성

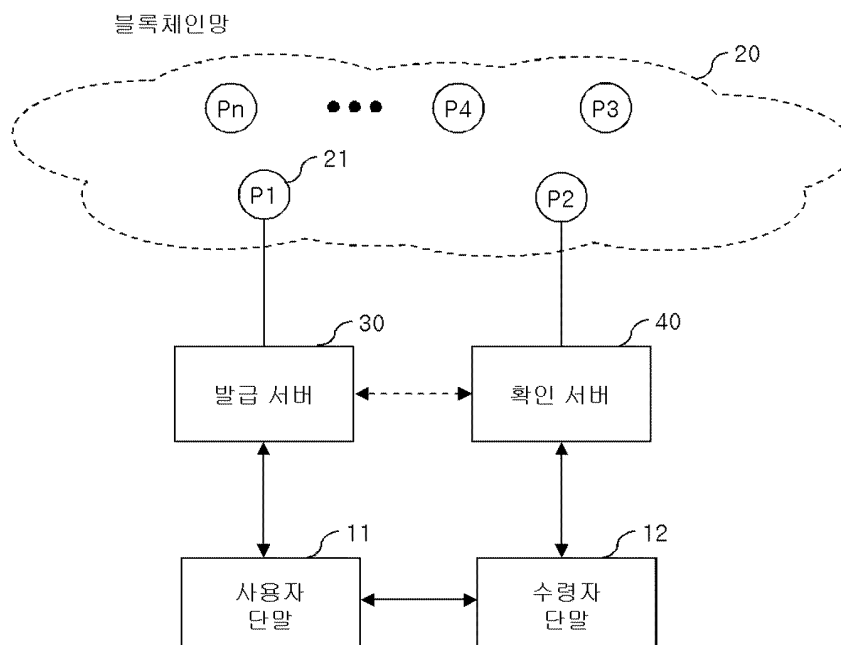
(54) 발명의 명칭 발급문서의 진위 확인을 위한 블록체인 기반 스탬프 인증 시스템

(57) 요약

발급문서가 발급되면 해당 문서의 진위를 확인할 수 있는 스탬프 데이터를 생성하여 블록체인에 저장하고, 전자문서와 함께 진위 확인 요청을 받으면 블록체인에 저장된 스탬프 데이터를 참조하여 진위를 확인해주는, 전자문서의 진위 확인을 위한 블록체인 기반 스탬프 인증 시스템에 관한 것으로서, 다수의 피어로 구성되는 블록체인망

(뒷면에 계속)

대표도 - 도1



으로서, 각 피어는 트랜잭션 메시지를 블록으로 기록하는 블록체인 원장을 보유하고, 모든 피어들의 블록체인 원장들을 동기화 시키는 블록체인망; 전자문서를 발급하고, 상기 전자문서로부터 해당 전자문서의 진위 여부를 확인할 수 있는 제1 인증정보를 추출하여 스탬프 데이터를 구성하고, 상기 스탬프 데이터를 상기 블록체인망에 등록하는 발급 서버; 및, 전자문서를 수신하고, 상기 전자문서로부터 제2 인증정보를 추출하고, 수신한 전자문서에 해당하는 스탬프 데이터를 상기 블록체인망에서 조회하고, 조회된 스탬프 데이터에서 상기 제1 인증정보를 추출하여, 상기 제2 인증정보와 비교하여 해당 전자문서의 진위 여부를 확인하는 확인 서버를 포함하는 구성을 마련한다.

상기와 같은 시스템에 의하여, 진위 확인을 위한 스탬프 데이터를 블록체인 망에 저장함으로써, 진위 확인을 위한 데이터에 대한 위변조가 불가능하여 외부 공격에 노출되지 않을 수 있다.

(52) CPC특허분류

H04L 9/3236 (2013.01)

H04L 9/3263 (2013.01)

G06Q 2220/10 (2013.01)

H04L 2209/38 (2013.01)

명세서

청구범위

청구항 1

전자문서의 진위 확인을 위한 블록체인 기반 스탬프 인증 시스템에 있어서,

다수의 피어로 구성되는 블록체인망으로서, 각 피어는 트랜잭션 메시지를 블록으로 기록하는 블록체인 원장을 보유하고, 모든 피어들의 블록체인 원장들을 동기화 시키는 블록체인망;

전자문서를 발급하고, 상기 전자문서로부터 해당 전자문서의 진위 여부를 확인할 수 있는 제1 인증정보를 추출하여 스탬프 데이터를 구성하고, 상기 스탬프 데이터를 상기 블록체인망에 등록하는 발급 서버; 및,

전자문서를 수신하고, 상기 전자문서로부터 제2 인증정보를 추출하고, 수신한 전자문서에 해당하는 스탬프 데이터를 상기 블록체인망에서 조회하고, 조회된 스탬프 데이터에서 상기 제1 인증정보를 추출하여, 상기 제2 인증정보와 비교하여 해당 전자문서의 진위 여부를 확인하는 확인 서버를 포함하고,

상기 발급 서버는 상기 블록체인망에 속하는 적어도 하나의 피어(이하 제1 피어)와 연동하고, 스탬프 데이터가 구성되면 해당 스탬프 데이터를 상기 제1 피어에 전달하고,

상기 확인 서버는 상기 블록체인망에 속하는 적어도 하나의 피어(이하 제2 피어)와 연동하고, 상기 제2 피어에 요청하여 상기 제2 피어의 블록체인 원장에서 해당 스탬프 데이터를 검색하여 가져오고,

상기 확인 서버는 진위 확인 결과를 화면 상에 표시하되, 전자문서를 표시하고, 표시된 전자문서 상에 확인 결과 마크 형태로 표시하고,

상기 인증정보는 해시함수에 의한 전자문서의 해시값이고,

상기 스탬프 데이터는 인증정보 외에, 발급기관, 발급날짜, 문서종류의 발급 정보와; 발급처, 고유번호의 식별 정보;로 구성되고,

상기 스탬프 데이터는 전자문서의 내용을 포함하지 않는 것을 특징으로 하는 전자문서의 진위 확인을 위한 블록체인 기반 스탬프 인증 시스템.

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

발명의 설명

기술 분야

- [0001] 본 발명은 발급문서가 발급되면 해당 문서의 진위를 확인할 수 있는 스탬프 데이터를 생성하여 블록체인에 저장하고, 전자문서와 함께 진위 확인 요청을 받으면 블록체인에 저장된 스탬프 데이터를 참조하여 진위를 확인해주는, 전자문서의 진위 확인을 위한 블록체인 기반 스탬프 인증 시스템에 관한 것이다.

배경 기술

- [0002] 일반적으로, 입시 또는 취업 자격시험 등을 보기 위해 모든 지원자들은 공공기관 또는 기업 등의 지원기관에 각종 증명서를 제출하고, 지원기관은 다량의 증명서를 수령하여 증명서의 위/변조 및 진위여부를 확인해야 한다. 이를 위해, 지원기관은 해당 증명서를 각각 원본대조 해야 한다.
- [0003] 현재, 증명발급기로 발급되는 대부분의 증명서 또는 증명발급 창구에서 발급되는 증명서의 경우, 증명서를 발급한 발급기관에 유선 또는 공문을 통해 확인하고 있다. 입사지원 등과 같이 대량의 증명서를 수령하는 경우, 발급기관에 증명서를 확인하는 절차가 복잡할 뿐만 아니라, 이를 각각 확인하기 위해 상당한 시간이 소요되고 있다.
- [0004] 상기와 같은 문제점을 해결하고자, 발급문서를 인터넷 등 온라인상에서 확인해주는 기술이 제시되고 있다[특허 문헌 1]. 상기 선행기술은 문서발급을 하는 프린터에 설치된 프린터 모듈이 발급문서를 출력할 때 발급문서의 발급정보와 인증정보를 생성하여 발급확인 서버로 송부하고, 발급확인 서버가 온라인상에서 발급문서의 인증정보를 입력받아 인증하여 발급문서의 발급정보를 보여준다.
- [0005] 또한, 발급문서의 진위확인을 하는 확인서버의 주소를 발급문서에 바코드로 인쇄하여, 이동단말의 카메라로 바코드를 촬상하면 즉시 발급문서의 사본과일을 불러와서 보여주는 기술도 제시되고 있다[특허문헌 2].
- [0006] 그러나 상기 선행기술들은 진위를 확인할 수 있는 확인용 정보를 일반 서버에 등록하므로, 해당 서버가 해킹 등 외부 공격에 노출될 위험이 존재한다. 외부 공격에 의하여 확인용 정보가 손상되거나 변경되면, 진위 여부를 확인할 수 없거나, 실제 발급 문서가 진본이더라도 진본이 아니라는 판단할 수 있다.

선행기술문헌

특허문헌

- [0007] (특허문헌 0001) 한국공개특허 제10-2009-0123555호 (2009.12.02.공개)
(특허문헌 0002) 한국등록특허 제10-1039390호 (2011.06.17.공고)

발명의 내용

해결하려는 과제

- [0008] 본 발명의 목적은 상술한 바와 같은 문제점을 해결하기 위한 것으로, 발급문서가 발급되면 해당 문서의 진위를 확인할 수 있는 스탬프 데이터를 생성하여 블록체인에 저장하고, 전자문서와 함께 진위 확인 요청을 받으면 블록체인에 저장된 스탬프 데이터를 참조하여 진위를 확인해주는, 전자문서의 진위 확인을 위한 블록체인 기반 스탬프 인증 시스템을 제공하는 것이다.

[0009]

과제의 해결 수단

- [0010] 상기 목적을 달성하기 위해 본 발명은 전자문서의 진위 확인을 위한 블록체인 기반 스탬프 인증 시스템에 관한 것으로서, 다수의 피어로 구성되는 블록체인망으로서, 각 피어는 트랜잭션 메시지를 블록으로 기록하는 블록체인 원장을 보유하고, 모든 피어들의 블록체인 원장들을 동기화 시키는 블록체인망; 전자문서를 발급하고, 상기 전자문서로부터 해당 전자문서의 진위 여부를 확인할 수 있는 제1 인증정보를 추출하여 스탬프 데이터를 구성하고, 상기 스탬프 데이터를 상기 블록체인망에 등록하는 발급 서버; 및, 전자문서를 수신하고, 상기 전자문서로

부터 제2 인증정보를 추출하고, 수신한 전자문서에 해당하는 스탬프 데이터를 상기 블록체인망에서 조회하고, 조회된 스탬프 데이터에서 상기 제1 인증정보를 추출하여, 상기 제2 인증정보와 비교하여 해당 전자문서의 진위 여부를 확인하는 확인 서버를 포함하는 것을 특징으로 한다.

[0011] 또한, 본 발명은 전자문서의 진위 확인을 위한 블록체인 기반 스탬프 인증 시스템에 있어서, 상기 발급 서버는 상기 블록체인망에 속하는 적어도 하나의 피어(이하 제1 피어)와 연동하고, 스탬프 데이터가 구성되면 해당 스탬프 데이터를 상기 제1 피어에 전달하고, 상기 확인 서버는 상기 블록체인망에 속하는 적어도 하나의 피어(이하 제2 피어)와 연동하고, 상기 제2 피어에 요청하여 상기 제2 피어의 블록체인 원장에서 해당 스탬프 데이터를 검색하여 가져오는 것을 특징으로 한다.

[0012] 또한, 본 발명은 전자문서의 진위 확인을 위한 블록체인 기반 스탬프 인증 시스템에 있어서, 상기 스탬프 데이터는 상기 발급 서버의 인증서에 의하여 암호화 되어 상기 블록체인망에 등록되고, 상기 확인 서버에 의해 조회되면 상기 발급 서버의 공개키에 의하여 복호화 되는 것을 특징으로 한다.

[0013] 또한, 본 발명은 전자문서의 진위 확인을 위한 블록체인 기반 스탬프 인증 시스템에 있어서, 상기 인증서는 공개키와 개인키로 구성되는 비대칭키로 구성되는 것을 특징으로 한다.

[0014] 또한, 본 발명은 전자문서의 진위 확인을 위한 블록체인 기반 스탬프 인증 시스템에 있어서, 상기 확인 서버는 진위 확인 결과를 화면 상에 표시하되, 전자문서를 표시하고, 표시된 전자문서 상에 확인 결과 마크 형태로 표시하는 것을 특징으로 한다.

[0015] 또한, 본 발명은 전자문서의 진위 확인을 위한 블록체인 기반 스탬프 인증 시스템에 있어서, 상기 인증정보는 해시함수에 의한 전자문서의 해시값인 것을 특징으로 한다.

[0016] 또한, 본 발명은 전자문서의 진위 확인을 위한 블록체인 기반 스탬프 인증 시스템에 있어서, 상기 발급 서버는 상기 확인 서버에 요청하여, 상기 스탬프 데이터를 상기 블록체인망에 등록하도록 하고, 상기 확인 서버는 상기 발급 서버의 요청에 따라 상기 스탬프 데이터를 상기 블록체인망에 등록하는 것을 특징으로 한다.

[0017]

발명의 효과

[0018] 상술한 바와 같이, 본 발명에 따른 전자문서의 진위 확인을 위한 블록체인 기반 스탬프 인증 시스템에 의하면, 진위 확인을 위한 스탬프 데이터를 블록체인 망에 저장함으로써, 진위 확인을 위한 데이터에 대한 위변조가 불가능하여 외부 공격에 노출되지 않는 효과가 얻어진다.

[0019] 또한, 본 발명에 따른 전자문서의 진위 확인을 위한 블록체인 기반 스탬프 인증 시스템에 의하면, 시각적으로 손쉽게 진위 확인이 가능 하여 문서 진위 확인의 복잡한 프로세스를 획기적으로 단축할 수 있는 효과가 얻어진다.

[0020]

도면의 간단한 설명

[0021] 도 1은 본 발명을 실시하기 위한 전체 시스템의 예시 구성도.

도 2는 본 발명의 일실시예에 따른 전자문서의 발급 방법을 설명하는 흐름도.

도 3은 본 발명의 일실시예에 따른 전자문서의 진위 확인 방법을 설명하는 흐름도.

도 4는 본 발명의 일실시예에 따른 진위 확인 결과 마크를 표시한 예시 화면.

발명을 실시하기 위한 구체적인 내용

[0022] 이하, 본 발명의 실시를 위한 구체적인 내용을 도면에 따라서 설명한다.

[0023] 또한, 본 발명을 설명하는데 있어서 동일 부분은 동일 부호를 붙이고, 그 반복 설명은 생략한다.

[0024]

[0025] 먼저, 본 발명을 실시하기 위한 전체 시스템의 구성을 도 1을 참조하여 설명한다.

- [0026] 도 1에서 보는 바와 같이, 본 발명을 실시하기 위한 전체 시스템은 사용자가 사용하는 사용자 단말(11), 수령자 또는 수령 업체가 사용(운영)하는 수령자 단말/서버(12), 다수의 피어(21)로 구성되는 블록체인망(20), 문서를 발급하는 발급서버(30), 및, 문서의 진위 여부를 확인하는 진위서버(40)로 구성된다. 이때, 발급서버(30), 사용자 단말(11), 수령자 단말/서버(12), 확인서버(40) 간에는 서로 네트워크(미도시)를 통해 연결되어 데이터 통신이 수행될 수 있다.
- [0027] 먼저, 사용자 단말(11)은 사용자가 이용하는 컴퓨팅 단말로서, PC, 노트북, 스마트폰, 패블릿, 태블릿PC 등 통상의 컴퓨팅 기능을 구비한 단말이다. 특히, 사용자 단말(11)은 어플리케이션 또는, 모바일용 어플리케이션(또는 앱, 어플) 등이 설치되어 실행될 수 있는 단말이다.
- [0028] 사용자 단말(11)에는 문서발급 어플리케이션 또는 문서발급 앱(미도시) 등이 설치될 수 있다. 사용자는 사용자 단말(11)에 설치된 문서발급 어플리케이션/앱을 이용하여 발급서버(30)의 전자문서 발급 서비스를 이용할 수 있다. 또는, 사용자 단말(11)은 웹브라우저 등이 설치되고, 사용자는 웹브라우저 등을 통해 발급서버(30)에서 제공하는 웹서비스(문서발급 서비스)에 접속하여 서비스를 이용할 수 있다.
- [0029] 특히, 사용자 단말(11)은 발급서버(30)로부터 발급받은 전자문서를 자신의 저장 매체에 저장할 수 있다.
- [0030] 또한, 사용자 단말(11)은 발급받은 전자문서를 수령자 단말 또는 서버(12) 등에 전송하거나 업로드할 수 있다. 이때, 바람직하게는, 사용자 단말(11)은 전자문서의 발급정보 또는 식별정보를 함께 전송할 수 있다.
- [0031] 전자문서 또는 발급문서의 식별정보는 발급처, 문서 고유번호 등을 포함한다. 그외에도 발급날짜, 시간 등을 더 포함할 수 있다. 발급처는 발급 기관명이나 고유 코드, 또는 URL 등 주소 중 어느 하나 이상을 포함하여 구성될 수 있다.
- [0032] 다음으로, 블록체인망(20)은 통상의 블록체인 망으로서, 트랜잭션을 블록으로 기록하되, 각 블록들을 블록 체인으로 연결하여 기록한다.
- [0033] 블록체인망(20)은 네트워크로 연결된 다수의 피어(21)들로 구성된다.
- [0034] 각 피어(21)는 하나의 컴퓨팅 단말 또는 서버로서, 트랜잭션 또는 스탬프 데이터를 블록체인으로 기록한 스탬프 데이터의 원장(이하 블록체인 원장)을 복제하여 저장한다. 따라서 모든 피어(21)는 서로 동기화 하여, 동일한 블록체인 원장을 보유한다.
- [0035] 구체적으로, 스탬프 데이터는 하나의 트랜잭션을 나타내는 데이터로서, 발급된 전자문서로부터 생성된 스탬프 데이터이다. 각 스탬프 데이터의 해시값을 구하여, 해시값들을 블록 체인으로 구성한다. 이때, 블록체인 원장은 각 스탬프 데이터의 해시값들을 블록들의 체인으로 구성한 블록체인과, 스탬프 데이터(또는 스탬프)를 모두 포함한다. 블록체인 원장의 스탬프를 열람함으로써 해당 스탬프의 내용을 열람할 수 있고, 블록체인의 해시값을 인증함으로써 해당 스탬프의 진위 여부를 검증할 수 있다.
- [0036] 특히, 피어(21)는 자신이 어떤 하나의 트랜잭션 작업을 수행하면, 새로운 스탬프 데이터를 자신의 블록체인 원장에 추가하고, 추가된 블록 정보를 다른 피어(21)에 전송한다. 추가되는 정보 또는 블록은 기존의 블록체인 원장에 블록체인으로 추가된다.
- [0037] 또한, 다른 피어(21)들은 앞서 갱신한 피어(21)로부터 추가되는 블록 정보를 수신하여, 자신의 블록체인 원장에 블록 정보를 추가한다. 바람직하게는, 피어(21)는 자신의 주변에 위치하는 피어(21)들에게, 추가되는 블록체인에 대한 갱신 정보(추가 정보)를 전송하고, 주변의 피어(21)들은 블록체인에 대한 갱신 정보를 자신의 블록체인 원장에 기록하고, 또 다시 자신의 주변의 피어들에게 전송한다. 따라서 블록체인망(20) 내에 위치하는 모든 피어(21)들은 블록체인 원장을 동기화 하여 모두 동일한 블록체인 원장을 보유하게 된다.
- [0038] 다음으로, 발급서버(30)는 발급기관에서 전자문서를 발급하기 위한 서버를 의미한다.
- [0039] 발급기관은 관공서, 학교, 일반 기업체 등으로서, 증명서 등 문서를 발급하는 기관을 말한다. 발급되는 문서로 예로 들어보면, 관공서 등에서 발급되는 각종 등본, 초본, 국민연금 가입증명서 등, 학교에서는 재학증명서, 졸업증명서, 학위증명서 등, 일반 기업체에서는 재직증명서, 계약확인서 등 다양한 문서들이 모두 대상이 될 수 있다.
- [0040] 한편, 바람직하게는, 발급문서는 전자문서 형태로 발급된다. 일례로서, PDF 등 일반 문서 형식이나, XML 등 구조화된 문서 형식, 또는 사전에 정해진 데이터 형식 등으로 구성될 수 있다.

- [0041] 특히, 발급서버(30)는 사용자 단말(11)로부터 전자문서의 발급 요청을 수신하면 해당 전자문서를 발급하여 사용자 단말(11)로 전자문서 형태로 회신한다. 즉, 발급서버(30)는 통상의 전자문서의 발급 서비스를 제공한다.
- [0042] 또한, 바람직하게는, 발급서버(30)는 사용자 단말(11)에 전자문서를 전달할 때, 전자문서의 식별정보를 함께 전달할 수 있다.
- [0043] 또한, 발급서버(30)는 발급문서의 진위 여부를 확인할 수 있는 스탬프 데이터를 생성하고, 생성된 스탬프 데이터를 블록체인망(20)에 저장한다. 즉, 발급서버(30)는 스탬프 데이터를 생성하여, 생성된 스탬프 데이터를 블록체인 원장에 추가한다.
- [0044] 특히, 발급서버(30)는 블록체인망(20)에 속하는 적어도 하나의 피어(P1)에 연결된다. 그리고 발급서버(30)는 스탬프 데이터를 생성하여, 제1 피어(P1)에 전달한다. 제1 피어(P1)는 전달 받은 스탬프 데이터를 자신의 블록체인 원장에 등록한다. 제1 피어(P1)는 블록체인망(20)에 소속된 하나의 피어이므로, 블록체인망(20) 내에서 다른 피어들(21)과 블록체인 원장을 동기화 한다. 따라서 블록체인망(20) 내의 모든 피어들(21)은 해당 스탬프 데이터가 추가되도록 블록체인 원장을 갱신한다.
- [0045] 한편, 스탬프 데이터는 전자문서의 해시값 등 인증정보를 포함한다. 해시값은 사전에 정해진 해시함수에 의해 생성된다.
- [0046] 바람직하게는, 인증정보는 암호화될 수 있다. 더욱 바람직하게는, 인증정보는 발급기관 또는 발급처(발급 서버)의 인증서에 의해 암호화된다. 특히, 발급서버의 개인키로 암호화된다. 다른 실시예로서, 암호화되지 않을 수 있다. 즉, 인증서는 공개키와 개인키로 구성되는 비대칭키로 구성된다.
- [0047] 또한, 인증서를 발급하기 위한 인증서 서버(미도시)가 구성되며, 인증서 발급 기능이 발급 서버(30) 내에 구현될 수 있다.
- [0048] 그외, 스탬프 데이터는 발급기관, 발급날짜, 문서종류 등 발급 정보를 더 포함할 수 있다. 또한, 바람직하게는, 스탬프 데이터는 전자문서의 식별정보를 포함할 수 있다. 전자문서의 식별정보는 발급처, 고유번호 등으로 구성된다.
- [0049] 특히, 스탬프 데이터의 식별정보는 해당 스탬프 데이터를 검색하기 위해 사용될 수 있다. 즉, 통상의 블록체인망의 방법에 따라, 스탬프 데이터의 식별정보를 이용하여, 블록체인망 또는 블록체인 원장에서 스탬프 데이터가 조회될 수 있다.
- [0050] 한편, 발급서버(30)는 발급 기능과, 스탬프 데이터의 처리 기능을 분리하여 각자 독립적인 서버로 구분하여 구현될 수 있다. 즉, 발급서버(30)는 발급 기능만 전담하고, 스탬프 처리 서버(미도시)는 스탬프 처리 기능만을 전담하도록 구성할 수 있습니다. 특히, 스탬프 데이터의 처리 기능(또는 스탬프 처리 서버)을 확인 서버(40) 내에 구현될 수도 있다.
- [0051] 다음으로, 수령자 단말/서버(12)은 수령자가 이용하는 컴퓨팅 단말로서, PC, 노트북, 스마트폰, 패블릿, 태블릿 PC 등 통상의 컴퓨팅 기능을 구비한 단말이다. 또 다른 실시예로서, 수령자 단말/서버(12)는 수령자 또는 수령업체가 운영하는 통상의 서버일 수 있다. 이하에서, 설명의 편의를 위하여 수령자 단말(12)로 부르기로 하고, 컴퓨팅 단말 형태를 예시로 설명한다.
- [0052] 특히, 수령자 단말(12)은 어플리케이션 또는, 모바일용 어플리케이션(또는 앱, 어플) 등이 설치되어 실행될 수 있는 단말이다. 특히, 수령자 단말(12)에는 문서의 진위확인 어플리케이션 또는 진위확인 앱(미도시) 등이 설치될 수 있다. 수령자는 수령자 단말(12)에 설치된 진위확인 어플리케이션/앱을 이용하여 확인서버(40)의 전자문서 진위확인 서비스를 이용할 수 있다. 또는, 수령자 단말(12)은 웹브라우저 등이 설치되고, 수령자는 웹브라우저 등을 통해 확인서버(40)에서 제공하는 웹서비스(진위확인 서비스)에 접속하여 서비스를 이용할 수 있다.
- [0053] 수령자 단말(12)은 사용자 단말(11)로부터 전자문서를 수신한다. 이때, 바람직하게는, 수령자 단말(12)은 전자문서의 식별정보를 사용자 단말(11)로부터 함께 수신하거나, 전자문서로부터 식별정보를 추출할 수 있다.
- [0054] 또한, 수령자 단말(12)은 수신된 전자문서를 확인서버(40)에 전송하여 해당 전자문서의 진위 여부의 확인을 요청한다. 바람직하게는, 수신된 전자문서 형태를 그대로 전송한다. 또한, 바람직하게는, 전자문서의 식별정보를 함께 전송할 수 있다.
- [0055] 또한, 수령자 단말(12)은 확인서버(40)로부터 전자문서의 진위 결과를 수신한다. 이때, 수령자 단말(12) 상에서 전자문서의 진위 결과가 표시될 수 있다. 또한, 수령자 단말(12)의 진위확인 앱 상에서 전자문서의 진위 결과가

표시된다.

- [0056] 특히, 바람직하게는, 문서 표시 화면에서 전자문서가 표시되고, 전자문서 상에 진위확인 마크가 생성되어 표시된다.
- [0057] 다음으로, 확인서버(40)는 전자문서를 수신하고 수신된 전자문서의 진위 여부를 확인하여 진위 결과를 회신하는 서버를 의미한다. 특히, 확인서버(40)는 해당 전자문서의 스탬프 데이터를 블록체인망(20)에서 가져와서, 가져온 스탬프 데이터를 이용하여 해당 전자문서의 진위 여부를 확인한다. 즉, 확인서버(40)는 전자문서의 진위확인 서비스를 제공한다.
- [0058] 즉, 확인서버(40)는 수령자 단말(12)로부터 전자문서를 수신한다. 이때, 전자문서의 식별정보를 직접 수신하거나, 수신한 전자문서에서 식별정보를 추출한다.
- [0059] 바람직하게는, 확인서버(40)는 전자문서를 문서 형태로 수신한다. 앞서 예와 같이, PDF 등 일반 문서 형식이나, XML 등 구조화된 문서 형식, 사전에 정해진 데이터 형식 등의 상태인 전자문서를 수신한다.
- [0060] 또한, 확인서버(40)는 블록체인망(20)에서 해당 전자문서의 스탬프 데이터를 가져온다. 즉, 블록체인망(20)의 블록체인 원장에서 스탬프 데이터를 조회한다. 이때, 식별정보를 이용하여 해당 전자문서의 스탬프 데이터를 검색하여 조회한다.
- [0061] 특히, 확인서버(40)는 블록체인망(20)에 속하는 적어도 하나의 피어(P2)에 연결된다. 그리고 확인서버(40)는 해당 전자문서의 식별정보를 제2 피어(P2)에 전달한다. 제2 피어(P2)는 전달 받은 식별정보를 이용하여 해당 전자문서의 스탬프 데이터를 자신의 블록체인 원장에서 검색하여 가져온다. 제2 피어(P2)는 블록체인망(20)에 소속된 하나의 피어이므로, 블록체인망(20) 내에서 다른 피어들(21)과 블록체인 원장을 동기화 한다. 제2 피어(P2)는 앞서 제1 피어(P1)가 등록한 스탬프 데이터를 자신의 블록체인 원장에도 기록하고 있다. 따라서 제2 피어(P2)는 수신한 식별정보를 이용하여 자신의 블록체인 원장에서 해당 전자문서의 스탬프 데이터를 조회할 수 있다.
- [0062] 또한, 확인서버(40)는 조회된 스탬프 데이터에서 전자문서의 해시값 또는 인증정보를 추출한다. 암호화된 경우, 스탬프 데이터를 복호화 하여 인증정보를 추출한다. 특히, 발급서버의 인증서 또는 공개키로 복호화 한다.
- [0063] 또한, 확인서버(40)는 수신한 전자문서의 해시값을 구하고, 구한 해시값(인증정보)과 스탬프 데이터의 해시값(인증정보)을 비교한다. 그리고 동일하면 해당 전자문서는 진본으로 판단하고, 동일하지 않으면 위조 또는 변조된 것으로 판단한다.
- [0064] 또한, 확인서버(40)는 진본/위변조 등으로 판단하면, 판단된 결과를 수령자 단말(12)로 전달한다. 특히, 확인서버(40)는 화면 상에 전자문서를 표시하고, 전자문서 상에서 진위 여부 마크를 표시한다.
- [0065] 한편, 발급서버(30)와, 사용자 단말(11)의 문서발급 어플리케이션(미도시)은 통상의 서버와 클라이언트의 구성 방법에 따라 구현될 수 있다. 즉, 문서발급 기능들을 클라이언트의 성능이나 서버와 통신량 등에 따라 분담될 수 있다.
- [0066] 또한, 확인서버(40)와 수령자 단말(12)의 진위확인 어플리케이션(미도시)도 통상의 서버와 클라이언트의 구성 방법에 따라 구현될 수 있다. 일례로서, 진위확인 어플리케이션(미도시)은 웹브라우저와 같이, 단지 확인서버(40)의 데이터 입력이나 결과 출력 등 인터페이스 기능만을 수행하고, 확인서버(40)가 전자문서의 진위 여부 작업을 모두 수행할 수 있다. 또 다른 예로서, 진위확인 어플리케이션(미도시)이 확인서버(40)로부터 블록체인망의 스탬프 데이터를 수신하고 전자문서에 대한 진위 여부를 직접 판단하고, 확인서버(40)는 블록체인망(20)과 연동하여 스탬프 데이터의 관리만 수행할 수도 있다.
- [0067] 이하에서는 스탬프 인증 시스템으로 설명하나, 서버-클라이언트의 구성 방법에 따라 다양한 분담 형태로 구현될 수 있다.
- [0068]
- [0069] 다음으로, 본 발명의 일실시예에 따른 전자문서의 발급 방법을 도 2를 참조하여 설명한다.
- [0070] 도 2에서 보는 바와 같이, 먼저, 사용자는 사용자 단말(11)을 이용하여 발급 서버(30)에 접속하고, 발급 서버(30)에 전자문서의 발급을 요청한다(S11). 이때, 발급 서버(30)는 사용자를 인증하고 사용자가 발급 권한을 가진 것인지 등을 판단한다.

- [0071] 다음으로, 발급 서버(30)는 사용자의 발급 요청에 따라 전자문서를 생성하고(S21), 생성된 전자문서를 사용자 단말(11)에 전송함으로써 발급한다(S22). 앞서 설명한 바와 같이, 전자문서는 사전에 정해진 특정 문서 포맷으로 작성되며, pdf나 XML 등 문서 파일, 또는 데이터 형식의 파일로 생성된다.
- [0072] 다음으로, 발급 서버(30) 또는 확인 서버(40)는 전자문서로부터 스탬프 데이터를 생성한다(S31). 스탬프 데이터는 전자문서의 해시값 등 인증정보로 구성된다. 또한, 전자문서의 해시값은 암호화 될 수 있다. 특히, 스탬프 데이터는 전자문서의 식별정보를 포함하고, 전자문서의 식별정보에 의해 식별된다.
- [0073] 한편, 실시예에 따라 발급 서버(30)에서 직접 스탬프 데이터를 생성할 수도 있고, 발급 서버(30)가 전자문서를 확인 서버(40)에 전송하면 확인 서버(40)에서 스탬프 데이터를 생성할 수 있다.
- [0074] 다음으로, 발급 서버(30) 또는 확인 서버(40)는 생성된 스탬프 데이터를 블록체인망(20)에 전달하여 기록하게 한다(S32). 이때, 실시예에 따라 발급 서버(30)에서 직접 블록체인망(20)에 저장하거나, 확인 서버(40)에서 스탬프 데이터를 블록체인망(20)에 전달하여 저장할 수 있다.
- [0075] 한편, 이를 위해, 발급 서버(30) 또는 확인 서버(40)는 적어도 하나의 피어(21)와 연결 또는 연동되어, 스탬프 데이터를 해당 피어(21)에 전달한다. 해당 피어(21)는 전달받은 스탬프 데이터를 자신의 블록체인 원장에 등록하고, 원장에 등록된 스탬프 데이터는 블록체인망(20)을 통해 전체로 전파된다.
- [0076] 다음으로, 본 발명의 일실시예에 따른 전자문서의 진위확인 방법을 도 3을 참조하여 설명한다.
- [0077] 도 3에서 보는 바와 같이, 먼저, 수령자는 수령자 단말(12)을 통해 사용자의 전자문서를 수령한다(S51). 즉, 수령자 단말(12)은 전자문서를 사용자 단말(11)로부터 직접 수신한다.
- [0078] 다음으로, 수령자는 수령자 단말(12)에 저장된 전자문서를 확인 서버(40)에 전달하고, 확인 서버(40)에게 해당 전자문서의 진위 확인을 요청한다(S52). 이때, 수령자 단말(12)은 해당 전자문서의 식별정보를 함께 전달할 수 있다. 전자문서의 식별정보는 전자문서를 식별할 수 있는 정보로서, 제출처, 전자문서의 고유번호(발급 번호) 등으로 구성되고, 해당 전자문서에 유일한 식별 데이터이다.
- [0079] 다음으로, 확인 서버(40)는 해당 전자문서의 스탬프 데이터를 블록체인망(20)에서 조회하여(S61), 조회된 스탬프 데이터를 가져온다(S62).
- [0080] 바람직하게는, 확인 서버(40)는 전자문서의 식별정보를 이용하여 스탬프 데이터를 블록체인망(20)에서 검색하고, 해당 식별정보를 가지는 스탬프 데이터를 조회하여 가져온다.
- [0081] 또한, 확인 서버(40)는 스탬프 데이터가 암호화된 경우, 해당 데이터를 복호화 한다.
- [0082] 다음으로, 확인 서버(40)는 전자문서로부터 제1 해시값(또는 제1 인증정보)을 추출하고(S71), 가져온 스탬프 데이터에서 제2 해시값(또는 제2 인증정보)을 추출하고(S72), 이들을 비교하여 동일 여부에 따라 전자문서의 진위 여부를 판단한다(S73). 즉, 동일한 경우에 해당 전자문서는 진본임을 확인한다.
- [0083] 다음으로, 확인 서버(40)는 진위확인 결과를 표시한다(S80). 이때, 바람직하게는, 확인 서버(40)는 해당 전자문서를 표시하고, 전자문서 상에서 진위확인 마크를 표시한다. 진위확인 마크의 예시가 도 4에 도시되고 있다.
- [0084] 이상, 본 발명자에 의해서 이루어진 발명을 실시 예에 따라 구체적으로 설명하였지만, 본 발명은 실시 예에 한정되는 것은 아니고, 그 요지를 이탈하지 않는 범위에서 여러 가지로 변경 가능한 것은 물론이다.

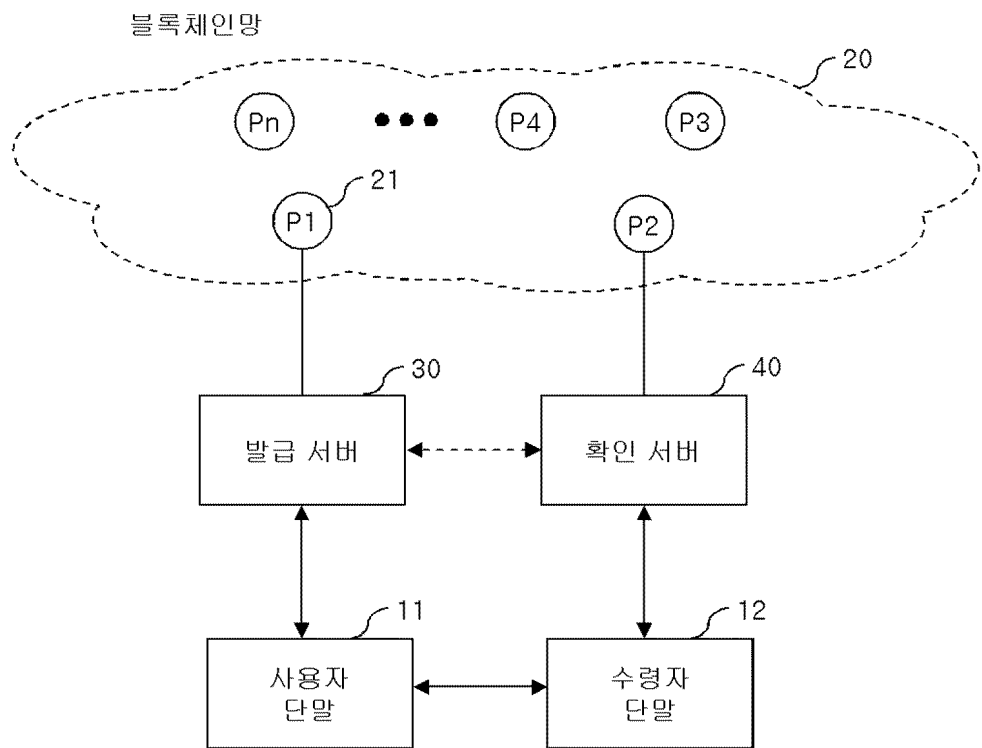
[0085]

부호의 설명

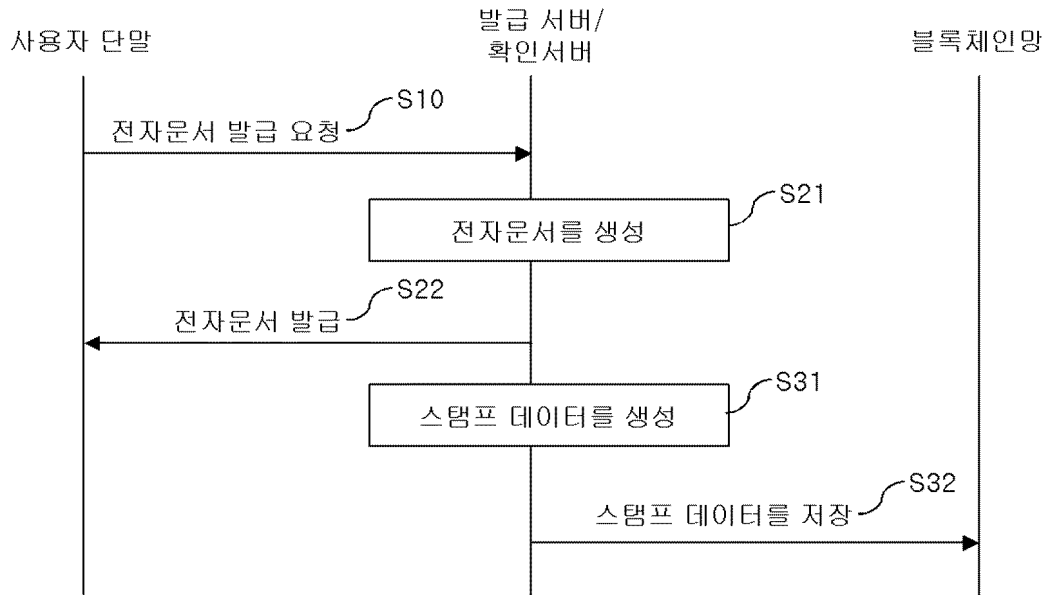
- [0086]
- | | |
|-------------|-------------|
| 11 : 사용자 단말 | 12 : 수령자 단말 |
| 20 : 블록체인망 | 21 : 피어 |
| 30 : 발급 서버 | 40 : 확인 서버 |

도면

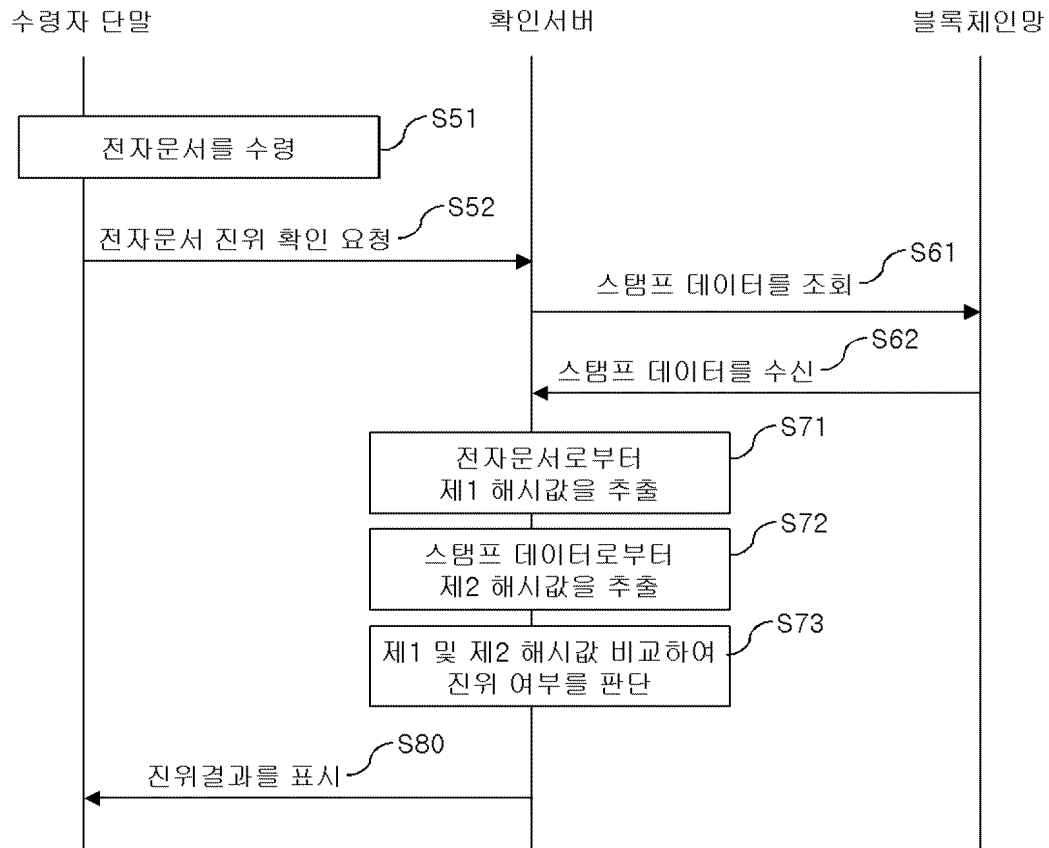
도면1



도면2



도면3



도면4



제 2020-03-06-00215 호

졸업증명서

대 학 (과)

성 명

주민등록번호

졸업 일 자

학위등록번호

학 위 명



위 사실을 증명합니다.

2019년 4월 19일

한국대학교 총장



• 동양대학교장 봉함 학적어근 형

본 증명서는 전자증명서(원본)이므로 진위스펙트 및 공적서명이 없는 증명서는 위조문, 간주, 위변, 무단 인정을 출력할 수 없습니다.