(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2017 년 8 월 31 일 (31.08.2017)

WIPO | PCT

(10) 국제공개번호
WO 2017/146333 A1

(51) 국제특허분류:
G06Q 40/02 (2012.01) *H04L 9/32* (2006.01)
H04L 9/06 (2006.01) *G06Q 20/38* (2012.01)

(21) 국제출원번호: PCT/KR2016/011288

(22) 국제출원일: 2016 년 10 월 10 일 (10.10.2016)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2016-0020437 2016 년 2 월 22 일 (22.02.2016) KR

(71) 출원인: (주)코인플러그 (COINPLUG,INC) [KR/KR]; 13557 경기도 성남시 분당구 정자일로 177 (정자동,에이동 2309 호), Gyeonggi-do (KR).

(72) 발명자: 어준선 (UHR, Joon Sun); 13558 경기도 성남시 분당구 느티로 22, B-1710 (정자동, 백궁동양파라곤), Gyeonggi-do (KR). 홍재우 (HONG, Jay Wu); 03336 서울시 은평구 연서로 149 1203 호, Seoul (KR). 송주한 (SONG, Joo Han); 13557 경기도 성남시 분당구 정자일로 177 인텔리지 2, A 동 2309 호, Gyeonggi-do (KR).

(74) 대리인: 임채국 (LIM, Chae Kook); 06595 서울시 서초구 서초대로 253, 5 층 (승지국제특허법률사무소), Seoul (KR).

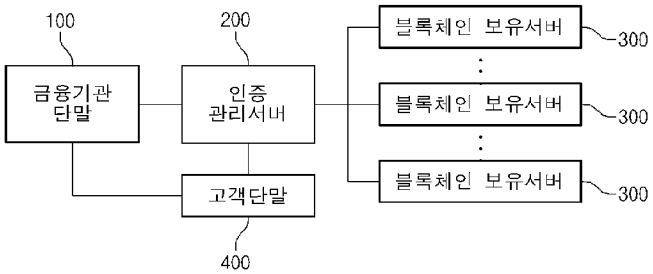
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR),

[다음 쪽 계속]

(54) Title: FORGERY/TAMPERING VERIFICATION SYSTEM AND METHOD FOR FINANCIAL INSTITUTION CERTIFICATES BASED ON BLOCKCHAIN

(54) 발명의 명칭 : 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템 및 방법



100 ... Financial institution's terminal
200 ... Authentication management server
300 ... Blockchain-holding server
400 ... Client's terminal

(57) Abstract: The present invention relates to a forgery/tampering verification system and method for financial institution certificates based on blockchain, where the system and method: can correctly verify forgery/tampering of certificates issued by financial institutions regardless of unverified watermarks using a means for comparing the content of certificates provided by a financial institution to a client when initially generated with the content thereof when issued by a client's request thereafter, so as to verify whether they are forged/tampered with, as well as significantly reduce the cost of registering clients' blockchain-based certificates; can minimise network overload by minimising traffic using a means for bundling and compressing certificate information of a client to a value preset by a system administrator, and registering this compressed information when transaction information including the certificates of the client is registered to a blockchain-holding server during the registration process of the blockchain-based certificates of the client; and verifies whether certificates of the client that are stored and managed by a financial institution are forged/tampered with according to a preset cycle, and can thereby promptly monitor whether certificates of the client are forged/tampered with through malicious actions such as hacking. A system

[다음 쪽 계속]

WO 2017/146333 A1

OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

and a method using the same are provided, the system comprising: a financial institution's terminal (100) for requesting record authentication of generated certificate information for a client when generating the certificate information for a client that is provided to a client by a financial institution, for storing certificate transaction ID information that is transmitted with the record authentication request, and for transmitting the certificate information for a client and the certificate transaction ID information if the certificate information for a client is requested to be downloaded; an authentication management server (200) for hashing the certificates for a client and client identification information identifying a corresponding client due to a record authentication request from the financial institution's terminal (100), and processing the same as node hash information, for accumulatively storing the node hash information in a certificate registration related information DB (211), and if the number of the accumulatively stored certificate node hash information reaches a preset root hash generation section, for operating a hash processing engine (220) so as to extract as many pieces of certificate node hash information as the number corresponding to the root hash generation section that is preset in the certificate registration related information DB (211) and so as to process the same as certificate root hash information for registration in which the extracted certificate node hash information is formed having a Merkle tree structure, for operating a transaction processing engine (230) so as to generate certificate transaction information including the certificate root hash information for registration, and certificate transaction ID information that is used as a key value for retrieving the certificate transaction information, and for transmitting the certificate transaction ID information to the financial institution's terminal (100), wherein the certificate transaction information is transmitted for record authentication; blockchain-holding servers (300) for authenticating bitcoin payments through verification of transmitted transaction information for bitcoin payments when the transaction information for a bitcoin payment is transmitted, wherein an electronic wallet having a blockchain in which the transaction information for bitcoin payments is recorded according to the authentication is placed in the blockchain-holding servers (300), and for recording the certificate transaction information transmitted by the authentication management server (200) in the blockchain; and a client's terminal (400) for requesting a download of the certificate information for a client from the financial institution's terminal (100) and for relay-transmitting the certificate information for a client and the certificate transaction ID information transmitted by the financial institution's terminal (100) due to the download request to the authentication management server (200) so as to request verification of whether the certificate information for a client is forged/tampered with, wherein the authentication management server (200) determines whether the certificate information has been forged/tampered with based on the transmitted certificate information for a client, certificate transaction ID information and client identification information, generates client-requested certificate verification information indicating whether the certificate information for a client has been forged/tampered with according to the determination, and controls the same to be transmitted to the client's terminal (400).

(57) 요약서: 본 발명은 금융기관에서 고객에게 제공되어지는 제증명서를 최초 생성 시 때의 내용과 향후 고객의 요청에 의해 발급되어지는 때의 내용들을 대비하여 위변조 여부를 검증하는 수단을 통해 검증되지 않은 워터마크에 상관없이 정확하게 금융기관에서 발급하는 제증명서류의 위변조 여부를 검증할 수 있을 뿐만 아니라 블록체인을 기반으로 하는 고객의 제증명서를 등록시에도 비용을 획기적으로 감축시켜주고, 블록체인 기반의 고객 제증명서 등록과정 중 고객의 제증명서 정보를 포함하는 트랙잭션정보를 블록체인 보유서버에 등록 시 시스템 관리자가 기설정되는 값만큼 묶어서 압축한 후 그 압축된 고객의 제증명서 정보를 등록하는 수단을 통해 트래픽의 발생을 최소화함으로써 이에 따라, 네트워크 과부하도 최소화시켜주며, 금융기관에서 저장관리되고 있는 고객들의 제증명서를 기설정된 주기마다 위변조 여부를 검증하여 해킹과 같은 악의적인 행위에 의해 고객들의 제증명서가 위변조 되는 것을 신속하게 감시 가능한 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템 및 방법에 관한 것으로, 금융기관에서 고객에게 제공되어지는 제증명서인 고객제공용 제증명서 정보 생성 시 그 생성된 고객제공용 제증명서 정보의 기록 인증을 요청하고, 그 기록 인증 요청에 의해 전송되는 제증명서 트랜잭션 ID 정보를 저장하며, 상기 고객제공용 제증명서 정보의 다운로드가 요청되면 상기 고객제공용 제증명서 정보 및 상기 제증명서 트랜잭션 ID 정보를 전송하는 금융기관단말(100)과; 상기 금융기관단말(100)의 기록 인증 요청에 의해 상기 고객제공용 제증명서 및 해당 고객을 식별하는 고객식별정보를 해싱하여 제증명서 노드해시정보로 가공처리하고, 이를 제증명서 등록관련정보 DB(211)에 누적저장하되, 그 누적저장되는 제증명서 노드해시정보의 개수가 기설정된 루트해시 생성구간에 도달되면, 해시처리엔진(220)을 운영하여 상기 제증명서 등록관련정보 DB(211)에서 기설정된 루트해시 생성구간에 해당하는 개수만큼 추출하고, 그 추출된 제증명서 노드해시정보들이 머클트리 구조로 이루어진 등록용 제증명서 루트해시정보로 가공처리하며, 트랜잭션처리엔진(230)을 운영하여 상기 등록용 제증명서 루트해시정보를 포함하는 제증명서 트랜잭션정보 및 그 제증명서 트랜잭션정보를 검색하는데 키값으로 이용되는 제증명서 트랜잭션 ID 정보를 생성하고, 상기 제증명서 트랜잭션 ID 정보는 상기 금융기관단말(100)로 전송하며, 상기 제증명서 트랜잭션정보는 기록인증을 위해 전송하는 인증관리서버(200)와; 비트코인 결제용 트랜잭션정보가 전송 시 그 전송된 비트코인 결제용 트랜잭션정보를 검증을 통해 비트코인 결제를 인증하고, 그 인증에 따라 비트코인 결제용 트랜잭션정보가 기록되는 블록체인을 갖는 전자지갑이 탑재된 것으로, 상기 인증관리서버(200)로부터 전송되는 제증명서 트랜잭션정보를 상기 블록체인에 기록하는 블록체인 보유서버(300)들과; 상기 금융기관단말(100)로 고객제공용 제증명서 정보의 다운로드를 요청하고, 그 다운로드 요청에 의해

명세서

발명의 명칭: 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템 및 방법

기술분야

[1] 본 발명은 금융기관에서 고객에게 제공되어지는 제증명서를 최초 생성 시 때의 내용과 향후 고객의 요청에 의해 발급되어지는 때의 내용들을 대비하여 위변조 여부를 검증하는 수단을 통해 검증되지 않은 워터마크에 상관 없이 정확하게 금융기관에서 발급하는 제증명서류의 위변조 여부를 검증할 수 있을 뿐만 아니라 블록체인을 기반으로 하는 고객의 제증명서를 등록시에도 비용을 획기적으로 감축시켜주고, 블록체인 기반의 고객 제증명서 등록과정 중 고객의 제증명서 정보를 포함하는 트랙잭션정보를 블록체인 보유서버에 등록 시 시스템 관리자가 기설정되는 값만큼 묶어서 압축한 후 그 압축된 고객의 제증명서 정보를 등록하는 수단을 통해 트래픽의 발생을 최소화함으로써 이에 따라, 네트워크 과부하도 최소화시켜주며, 금융기관에서 저장관리되고 있는 고객들의 제증명서를 기설정된 주기마다 위변조 여부를 검증하여 해킹과 같은 악의적인 행위에 의해 고객들의 제증명서가 위변조 되는 것을 신속하게 감시 가능한 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템 및 방법에 관한 것이다.

배경기술

[2] 금융거래 채널 및 방식이 다면화되고, 상기 금융거래와 관련된 정보들이 각 분야에 적극적으로 활용되면서, 금융기관을 통해 잔액증명서, 부채증명서, 지급보증서, 거래상황확인서, 금융정보제공서, 신용장 등을 포함하는 제증명서 발급이 빈번하게 발생하고 있다.

[3] 이 때문에, 고객은 제증명서 발급을 원할 경우 해당 금융기관 창구에 방문해서 신청해야 하는 등의 번거로움과 불편함이 존재하는 문제점을 포함하고 있었다.

[4] 이를 해소하고자 제안된 것으로, 종래의 증명서 발급 시스템(특허문헌 1 참조)은 단말로부터 소정의 고객정보와 증명서 종류와 용도를 포함하는 발급신청 증명서 정보를 수신하는 정보 수신수단과, 소정의 원장(또는 데이터베이스)으로부터 상기 고객정보와 발급신청 증명서 정보에 대응하는 적어도 하나의 증명서 구성 정보를 추출하는 정보 추출수단과, 상기 증명서 구성 정보를 포함하는 증명서 전자문서를 생성하여 전자문서 보관소에 저장하는 전자문서 생성수단 및 상기 전자문서 보관소에 보관된 상기 증명서 전자문서를 증명서 수신처 단말로 전송하여 발급하는 증명서 발급수단으로 이루어져 있다.

[5] 이를 통해, 고객은 직접 해당 금융기관에 방문 없이 원격지에서도 수신처 단말을 통해 원하는 제증명서를 요청할 경우 실시간으로 제증명서를 발급받을 수 있다.

[6] 그런데 일반적으로, 발급되는 제증명서가 위변조되지 않았다는 것을 증명하고자 금융기관 책임자의 인장이나 철인 또는 스탬프 등을 찍는다.

[7] 이에, 종래의 증명서 발급 시스템은 발급되는 제증명서의 위변조 여부를 확인하는 수단인 인장, 철인 또는 스탬프 등의 책임자 직인을 제공할 수 없는 문제점이 있었다.

[8] 이 또한, 종래의 워터마킹 기술을 이용한 문서 발급 및 인증 시스템(특허문헌 2 참조)을 통해 해소되었다.

[9] 즉, 종래의 워터마킹 기술을 이용한 문서 발급 및 인증 시스템은 온라인 상에서 발급되는 증명서에 워터마크를 삽입하여 발급하도록 하고 이러한 증명서의 제출을 요청한 기관이나 회사 등에서는 워터마크 추출 알고리즘을 이용하여 해당 증명서에 삽입된 워터마크의 추출여부를 통하여 그 증명서의 무결성 및 정당성을 인증하도록 한 워터마킹 기술 기반의 인증 시스템을 제공한다.

[10] 그러나 종래의 워터마킹 기술을 이용한 문서 발급 및 인증 시스템은 제증명서의 위변조가 단지 제증명서에 삽입된 워터마크의 삽입여부를 통해서만 감지되기 때문에 최초 발급된 때의 제증명서를 위변조 한 후 그 위변조된 제증명서에 워터마크를 삽입하면 위변조 되지 않은 정상적인 제증명서로 인식되기 때문에 완전한 위변조 감지 시스템을 운영하지 못하는 문제점이 있었다.

[11] 이러한, 최초 발급된 때의 제증명서 정보를 차후에 위변조한 상태에서 워터마크를 삽입 시 정상적인 제증명서 정보로 인식되는 문제점은 본 출원인에 의해 출원(특허문헌 3 참조)된 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템 및 방법을 통해 해소되었다.

[12] 즉, 종래의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템 및 방법은 금융기관에서 고객에게 제공되어지는 제증명서를 최초 생성 시 때의 내용과 향후 고객의 요청에 의해 발급되어지는 때의 내용 들을 대비하여 위변조 여부를 검증하는 수단을 통해 검증되지 않은 워터마크에 상관 없이 정확하게 금융기관에서 발급하는 제증명서류의 위변조 여부를 검증할 수 있는 특징을 제공한다.

[13] 그런데 이와 같은 이점에도 불구하고, 종래의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템 및 방법은 최초 생성되는 고객의 제증명서 정보를 블록체인 보유서버에서 저장관리하기 위해 초기에 발급비용을 지불해야 한다.

[14] 이때, 발급비용은 0.0001비트코인이 소요되는데, 2014년 1월 시세로 0.0001비트코인은 대한민국 원화로 46원 정도의 저렴한 비용이나 이는, 고객의 제증명서 정보를 블록체인 보유서버에 저장관리를 위해 등록할 때마다 소요되는 비용이기 때문에 고객의 제증명서 정보의 건수가 증가하면 그에 따라 등록비용 또한 비례적으로 증가하는 문제점이 있다.

[15] 더욱이, 종래의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조

검증시스템 및 방법은 해킹 발생 시 블록체인 보유서버에 저장관리되는 고객의 제증명서 정보의 의 위변조가 불가능하도록 십만 개 이상의 블록체인 보유서버에 고객의 제증명서 정보를 등록하여 저장관리한다.

[16] 즉, 고객의 제증명서 정보를 포함하는 트랜잭션정보의 전파는 통신규약(protocol)에 의해 약속된 것으로, 트랜잭션정보의 발생 시 1개의 노드(여기서는 블록체인 보유서버를 칭함)가 지정된 8개의 노드로 전파시키며, 그 비트코인 결제용 트랜잭션정보를 전송받은 8개의 노드마다 각각 지정된 8개의 노드로 반복 전파하는 피라미드식 전파를 통해 비트코인 결제를 수행하기 위해 필요한 블록체인을 갖는 전자지갑이 탑재된 모든 블록체인 보유서버에게 전파됨으로써, 완료된다.

[17] 이 때문에, 종래의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템 및 방법에서 고객의 제증명서 정보의 등록요청이 쇄도할 경우 고객의 제증명서 정보를 포함하는 트랜잭션정보의 과도한 트래픽 발생으로 인해 네트워크 과부하가 유발되는 문제점도 있다.

[18]

[19] [선행기술문헌]

[20] [특허문헌]

[21] 특허문헌 1 : 대한민국특허청 공개특허공보 제10-2009-0000740호(공개일자:2009년01월08일)

[22] 특허문헌 2 : 대한민국특허청 공개특허공보 제10-2003-0020675호(공개일자:2003년03월10일)

[23] 특허문헌 3 : 대한민국특허청 특허출원공보 제10-2015-0086457호(출원일자:2015년06월18일)

발명의 상세한 설명

기술적 과제

[24] 본 발명은 상기 종래기술의 문제점을 해결하기 위한 것으로, 본 발명의 목적은 금융기관에서 고객에게 제공되어지는 제증명서를 최초 생성 시 때의 내용과 향후 고객의 요청에 의해 발급되어지는 때의 내용 들을 대비하여 위변조 여부를 검증하는 수단을 통해 검증되지 않은 워터마크에 상관 없이 정확하게 금융기관에서 발급하는 제증명서류의 위변조 여부를 검증할 수 있을 뿐만 아니라 블록체인을 기반으로 하는 고객의 제증명서를 등록시에도 비용을 획기적으로 감축시켜주는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템 및 방법을 제공하는데 있다.

[25] 본 발명의 다른 목적은 블록체인 기반의 고객 제증명서 등록과정 중 고객의 제증명서 정보를 포함하는 트랙잭션정보를 블록체인 보유서버에 등록 시 시스템 관리자가 기설정되는 값만큼 묶어서 압축한 후 그 압축된 고객의 제증명서 정보를 등록하는 수단을 통해 트래픽의 발생을 최소화함으로써 이에

따라, 네트워크 과부하도 최소화시켜주는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템 및 방법을 제공하는데 있다.

과제 해결 수단

[26] 본 발명을 달성하기 위한 기술적 사상으로 본 발명의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템은, 금융기관에서 고객에게 제공되어지는 제증명서인 고객제공용 제증명서 정보 생성 시 그 생성된 고객제공용 제증명서 정보의 기록 인증을 요청하고, 그 기록 인증 요청에 의해 전송되는 제증명서 트랜잭션 ID정보를 저장하며, 상기 고객제공용 제증명서 정보의 다운로드가 요청되면 상기 고객제공용 제증명서 정보 및 상기 제증명서 트랜잭션 ID정보를 전송하는 금융기관단말과; 상기 금융기관단말의 기록 인증 요청에 의해 상기 고객제공용 제증명서 및 해당 고객을 식별하는 고객식별정보를 해싱하여 제증명서 노드해시정보로 가공처리하고, 이를 제증명서 등록관련정보DB에 누적저장하되, 그 누적저장되는 제증명서 노드해시정보의 개수가 기설정된 루트해시 생성구간에 도달되면, 해시처리엔진을 운영하여 상기 제증명서 등록관련정보DB에서 기설정된 루트해시 생성구간에 해당하는 개수만큼 추출하고, 그 추출된 제증명서 노드해시정보들이 머클트리 구조로 이루어진 등록용 제증명서 루트해시정보로 가공처리하며, 트랜잭션처리엔진을 운영하여 상기 등록용 제증명서 루트해시정보를 포함하는 제증명서 트랜잭션정보 및 그 제증명서 트랜잭션정보를 검색하는데 키값으로 이용되는 제증명서 트랜잭션 ID정보를 생성하고, 상기 제증명서 트랜잭션 ID정보는 상기 금융기관단말로 전송하며, 상기 제증명서 트랜잭션정보는 기록인증을 위해 전송하는 인증관리서버와; 비트코인 결제용 트랜잭션정보가 전송 시 그 전송된 비트코인 결제용 트랜잭션정보를 검증을 통해 비트코인 결제를 인증하고, 그 인증에 따라 비트코인 결제용 트랜잭션정보가 기록되는 블록체인을 갖는 전자지갑이 탑재된 것으로, 상기 인증관리서버로부터 전송되는 제증명서 트랜잭션정보를 상기 블록체인에 기록하는 블록체인 보유서버들과; 상기 금융기관단말로 고객제공용 제증명서 정보의 다운로드를 요청하고, 그 다운로드 요청에 의해 상기 금융기관단말로부터 전송되는 상기 고객제공용 제증명서 정보 및 상기 제증명서 트랜잭션 ID정보를 상기 인증관리서버로 중계전송하여 상기 고객제공용 제증명서 정보의 위변조 여부의 검증을 요청하는 고객단말;로 이루어지고, 상기 인증관리서버는 상기 전송되는 고객제공용 제증명서 정보, 제증명서 트랜잭션 ID정보 및 고객식별정보를 토대로 해당 제증명서 정보가 위변조 되었는지의 여부를 판단하고, 그 판단에 따른 고객제공용 제증명서 정보의 위변조 여부를 안내하는 고객요청 제증명서 검증정보를 생성하고, 이를 상기 고객단말로 전송되도록 제어한다.

[27] 상기 인증관리서버는 상기 제증명서 노드해시정보가 기설정된 루트해시

생성구간에 도달되면 상기 제증명서 위변조 감시관련정보 DB에 누적저장된 제증명서 트랜잭션 ID정보를 모두 추출하고, 그 추출된 각각의 제증명서 트랜잭션 ID정보를 블록체인 보유서버로 전송하며, 상기 블록체인 보유서버는 전송된 각각의 제증명서 트랜잭션 ID정보를 전자지갑에 구비된 블록체인과 매칭하여, 매칭되는 각각의 제증명서 트랜잭션정보에 포함된 등록용 제증명서 루트해시정보를 추출하고, 그 추출된 각각의 등록용 제증명서 루트해시정보를 상기 인증관리서버로 전송하며, 상기 인증관리서버는 전송된 각각의 등록용 제증명서 루트해시정보를 전송받고, 해시처리엔진을 운영하여 제증명서 등록관련정보DB에 누적저장된 제증명서 노드해시정보의 개수를 기설정된 루트해시 생성구간에 해당하는 개수로 구분하고, 그 구분된 기설정된 루트해시 생성구간에 해당하는 개수마다 해싱하여 각각의 대비용 제증명서 루트해시정보로 가공처리하며, 각각의 등록용 제증명서 루트해시정보와 각각의 대비용 제증명서 루트해시정보를 생성순번대로 양자대비하고, 생성순번대로 양자대비되는 각각의 등록용 제증명서 루트해시정보와 각각의 대비용 제증명서 루트해시정보의 해시값을 연산하여 첫 번째 생성순번부터 마지막 생성순번까지 그 연산된 양쪽의 해시값이 동일한지 여부를 확인하여, 상기 인증관리서버에서 저장관리되고 있는 고객제공용 제증명서 정보의 위변조 여부를 검증하는 기능을 수행한다.

[28] 상기 고객요청 제증명서 검증정보의 생성과정은, 상기 인증관리서버에서, 상기 고객제공용 제증명서 정보 및 제증명서 트랜잭션 ID정보가 전송되면, 전송된 정보 중 제증명서 트랜잭션 ID정보를 상기 블록체인 보유서버에게 전송하여, 제증명서 트랜잭션정보의 전송을 요청하고, 상기 블록체인 보유서버의 전자지갑에서, 상기 제증명서 트랜잭션 ID정보를 블록체인에 매칭하여 매칭되는 제증명서 트랜잭션정보를 상기 인증관리서버로 전송하며, 상기 인증관리서버에서, 해시처리엔진을 운영하여 상기 고객단말로부터 전송된 정보 중 고객제공용 제증명서 정보 및 고객식별정보를 해싱하여 대비용 제증명서 노드해시정보로 가공처리하고, 상기 블록체인 보유서버로부터 전송된 제증명서 트랜잭션정보에 포함된 제증명서 검증용 인덱스 해시값과 상기 대비용 제증명서 노드해시정보값을 각각 연산하여, 양쪽의 해시값의 동일여부를 안내하는 고객요청 제증명서 검증정보로 생성된다.

[29] 본 발명의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템을 이용하여 금융기관에서 발급하는 제증명서류의 위변조여부를 검증하는 과정은, 금융기관단말에서, 고객에게 제공되어지는 제증명서인 고객제공용 제증명서 정보 생성 시 그 생성된 고객제공용 제증명서 정보 및 해당 고객을 식별하는 고객식별정보를 인증관리서버로 전송하여 고객제공용 제증명서 정보의 기록 인증을 요청하는 단계와; 상기 인증관리서버에서, 전송된 한 조의 고객제공용 제증명서 정보 및 고객식별정보를 제증명서 등록관련정보 DB에 저장함과 아울러 해시처리엔진을 운영하여 상기 고객제공용 제증명서

정보 및 고객식별정보를 해싱하여 제증명서 노드해시정보로 가공처리하고, 이를 제증명서 등록관련정보DB에 누적저장하는 단계와; 상기 인증관리서버에서, 상기 누적저장되는 제증명서 노드해시정보가 기설정된 루트해시 생성구간에 도달됐는지 확인하는 단계와; 상기 인증관리서버에서, 상기 누적저장되는 제증명서 노드해시정보가 기설정된 루트해시 생성구간에 도달되면, 해시처리엔진을 운영하여 상기 제증명서 등록관련정보DB에서 기설정된 루트해시 생성구간에 해당하는 개수만큼 추출하고, 그 추출된 제증명서 노드해시정보들을 머클트리 구조로 이루어진 등록용 제증명서 루트해시정보로 가공처리하는 단계와; 상기 인증관리서버에서, 트랜잭션처리엔진을 운영하여 상기 등록용 제증명서 루트해시정보를 포함하는 제증명서 트랜잭션정보 및 그 제증명서 트랜잭션정보를 검색하는데 키값으로 이용되는 제증명서 트랜잭션 ID정보를 생성하고, 상기 생성된 정보 중 제증명서 트랜잭션정보를 블록체인 보유서버들로 전송하는 단계와; 상기 블록체인 보유서버들에서, 상기 전송되는 제증명서 트랜잭션정보를 블록체인에 기록하여 기록 인증을 수행하는 단계와; 상기 인증관리서버의 트랜잭션처리엔진에서, 상기 제증명서 트랜잭션 ID정보를 상기 금융기관단말로 전송하는 단계와; 상기 금융기관단말에서, 상기 전송되는 제증명서 트랜잭션 ID정보를 저장관리하는 단계와; 고객단말에서, 상기 금융기관단말로 고객제공용 제증명서 정보의 다운로드를 요청하는 단계와; 상기 금융기관단말에서, 그 다운로드 요청된 고객제공용 제증명서 정보 및 해당 고객제공용 제증명서 정보 에 대응되는 제증명서 트랜잭션 ID정보를 고객단말로 전송하는 단계와; 상기 고객단말에서, 상기 전송되는 고객제공용 제증명서 정보 및 제증명서 트랜잭션 ID정보와 해당 고객임을 식별하는 고객식별정보를 상기 인증관리서버로 중계전송하여 상기 고객제공용 제증명서 정보의 위변조 여부에 따른 검증을 요청하는 단계와; 상기 인증관리서버에서, 상기 전송되는 고객제공용 제증명서 정보, 제증명서 트랜잭션 ID정보 및 고객식별정보를 토대로 해당 제증명서 정보가 위변조 되었는지의 여부를 판단하고, 그 판단에 따른 고객제공용 제증명서 정보의 위변조 여부를 안내하는 고객요청 제증명서 검증정보를 생성하여 상기 고객단말로 전송하는 단계와; 상기 고객단말에서, 상기 전송된 고객요청 제증명서 검증정보를 열람하는 단계;로 이루어진다.

발명의 효과

[30] 본 발명은 금융기관에서 고객에게 제공되어지는 제증명서를 최초 생성 시 때의 내용과 향후 고객의 요청에 의해 발급되어지는 때의 내용들을 대비하여 위변조 여부를 검증하는 수단을 통해 검증되지 않은 워터마크에 상관 없이 정확하게 금융기관에서 발급하는 제증명서류의 위변조 여부를 검증할 수 있을 뿐만 아니라 블록체인을 기반으로 하는 고객의 제증명서를 등록시에도 비용을 획기적으로 감축시켜주는 효과를 발휘한다.

[31] 또한, 본 발명은 블록체인 기반의 고객 제증명서 등록과정 중 고객의 제증명서 정보를 포함하는 트랙잭션정보를 블록체인 보유서버에 등록 시 시스템 관리자가 기설정되는 값만큼 묶어서 압축한 후 그 압축된 고객의 제증명서 정보를 등록하는 수단을 통해 트래픽의 발생을 최소화함으로써 이에 따라, 네트워크 과부하도 최소화시켜주는 효과도 있다.

[32] 또한, 본 발명은 금융기관에서 저장관리되고 있는 고객들의 제증명서를 기설정된 주기마다 위변조 여부를 검증하여 해킹과 같은 악의적인 행위에 의해 고객들의 제증명서가 위변조 되는 것을 신속하게 감시 가능한 효과도 있다.

도면의 간단한 설명

[33] 도 1은 본 발명의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템을 나타낸 전체구성도,

[34] 도 2는 본 발명의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템 중 금융기관단말을 나타낸 블록구성도,

[35] 도 3은 본 발명의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템 중 인증관리서버를 나타낸 블록구성도,

[36] 도 4 내지 도 6은 본 발명의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템을 이용하여 금융기관에서 발급하는 제증명서류의 위변조여부를 검증하는 과정을 나타낸 순서도,

[37] 도 7은 본 발명의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템의 다른 실시예에 따른 금융기관단말을 나타낸 블록구성도,

[38] 도 8 내지 도 10은 본 발명의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템의 다른 실시예에 따른 제증명서류의 위변조여부 검증 과정을 나타낸 순서도이다.

발명의 실시를 위한 최선의 형태

[39] 이하에서는 본 발명의 각 실시예의 구성 및 작용에 대하여 첨부한 도면을 참조하면서 상세히 설명하기로 한다.

[40] 도 1은 본 발명의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템을 나타낸 전체구성도, 도 2는 본 발명의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템 중 금융기관단말을 나타낸 블록구성도, 도 3은 본 발명의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템 중 인증관리서버를 나타낸 블록구성도 및 도 4 내지 도 6은 본 발명의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템을 이용하여 금융기관에서 발급하는 제증명서류의 위변조여부를 검증하는 과정을 나타낸 순서도이다.

[41] 도시된 바와 같이, 본 발명의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템은 크게, 금융기관단말(100), 인증관리서버(200), 블록체인 보유서버(300)들 및 고객단말(400)로 이루어진다.

[42] 먼저, 금융기관단말(100)은 예금에서 자금을 조달하여 기업이나 개인에 대부하거나 증권 투자 등을 수행하는 기관인 은행, 신탁 회사, 보험 회사 및 증권 회사 등에서 운영하는 단말로서, 금융기관이 고객에게 제공하는 제증명서인 고객제공용 제증명서 정보 생성 시 그 생성된 고객제공용 제증명서 정보의 기록 인증을 요청하고, 그 기록 인증 요청에 의해 전송되는 제증명서 트랜잭션 ID정보를 저장하며, 고객제공용제증명서 정보의 다운로드가 요청되면 그 다운로드 요청된 고객제공용 제증명서 정보 및 이에 대응하는 제증명서 트랜잭션 ID정보를 전송하는 기능을 수행한다.

[43] 이를 위해, 금융기관단말(100)에는 DB부(110)가 저장되어진다.

[44] 이처럼, 저장되는 DB부(110)에는 금융기관이 고객에게 제공하는 제증명서인 고객제공용 제증명서 정보, 해당 고객을 식별하는 고객식별정보가 저장되는 고객제공용 제증명서 목록정보 DB(111) 및 제증명서 트랜잭션정보를 검색하는데 키값으로 이용되는 제증명서 트랜잭션 ID정보가 저장되는 트랜잭션 식별자 목록정보 DB(112)로 이루어진다.

[45] 상기 블록체인 보유서버(300)들은 비트코인 결제 시 그 비트코인 결제에 대한 인증 및 기록을 통해 비트코인 결제를 수행하는 비트코인 네트워크를 이루는 장치들이다.

[46] 여기서, 비트코인에 대해 간략하게 설명하기로 한다. 비트코인(Bitcoin)이란 2009년 나카모토 사토시(영문성명 : Satoshi Nakamoto)가 만든 현물에 대한 결제가 가능한 디지털 통화로, 통화를 발행하고 관리하는 중앙 장치가 존재하지 않는 구조로 이루어진다. 대신에, 비트코인의 거래는 동등 계층간 통신망(P2P : peer-to-peer network) 기반 분산 데이터베이스에 의해 이루어지며, 공개 키 암호 방식 기반으로 거래를 수행한다.

[47] 이와 같은, 결제방식을 갖는 비트코인은 신용카드 결제 시에 필요한 카드번호나 유효기간 및 CCV 번호 등의 정보 없이도 이용이 가능할 뿐만 아니라 사용수수료도 저렴한 이점이 있다. 또한, 비트코인은 파일의 형태인 전자지갑에 저장되고, 이 전자지갑에는 각각의 고유 주소(퍼블릭어드레스)가 부여되며, 그 주소를 기반으로 비트코인의 거래가 이루어진다.

[48] 이와 같은, 결제특성을 갖는 비트코인을 이용하기 위해서는 먼저, 비트코인 이용자는 비트코인 거래소(일예 : www.coinplug.com)에 가입하여 전자지갑을 개설한 상태에서 원화에 해당하는 KRW를 충전한다.

[49] 이후, 비트코인 거래소에서 매매되고 있는 비트코인의 현재 시세를 확인한 후 구매를 원하는 비트코인의 수량과 단가를 입력하여 구매주문을 하면, 거래조건에 맞는 판매주문을 통해 거래가 성립됨으로써, 이용자는 물품 구매 시 비트코인을 통해 결제를 수행할 수 있다.

[50] 이러한, 블록체인 보유서버(300)들에는 앞에서 언급한 것처럼, 비트코인 거래소측이 운영하는 서버가 하나의 구성원으로 이루어질 수 있다.

[51] 이를 위해, 개개의 블록체인 보유서버(300)에는 블록체인을 갖는 전자지갑이

탑재되어야 하며, 블록체인 보유서버(300)의 전자지갑에 의해 블록체인에는 일반적인 비트코인 결제에 따라 생성되는 비트코인 결제용 트랜잭션정보가 수신 시 그 수신된 비트코인 결제용 트랜잭션정보를 검증을 통해 비트코인 결제를 인증하고, 그 인증에 따라 비트코인 결제용 트랜잭션정보가 기록됨과 더불어, 지정된 다음 단의 블록체인 보유서버(300)들에게 비트코인 결제용 트랜잭션정보를 전파한다.

[52] 즉, 비트코인 결제용 트랜잭션정보의 전파는 통신규약(protocol)에 의해 약속된 것으로, 비트코인 결제용 트랜잭션정보의 발생 시 1개의 노드(여기서는 블록체인 보유서버를 칭함)가 지정된 8개의 노드로 전파시키며, 그 비트코인 결제용 트랜잭션정보를 전송받은 8개의 노드마다 각각 지정된 8개의 노드로 반복 전파하는 피라미드식 전파를 통해 비트코인 결제를 수행하기 위해 필요한 블록체인을 갖는 전자지갑이 탑재된 모든 블록체인 보유서버(300)에게 전파됨으로써, 완료된다.

[53] 이처럼, 블록체인에 기록되는 비트코인 결제용 트랜잭션정보를 포함하는 모든 정보는 추후 위변조가 불가능하다.

[54] 한편, 블록체인 보유서버(300)들에는 블록체인을 갖는 전자지갑이 탑재된 것으로, 비트코인을 채굴하는 마이너가 운영하는 서버(또는 단말) 또는, 비트코인 결제를 위한 사용자단말(일예로, PC나 스마트폰)도 하나의 구성원으로 이루어질 수 있다.

[55] 이와 더불어, 비트코인 결제의 경우 기본적으로 블록체인이 탑재된 전자지갑을 기반으로 결제가 수행되는데 이처럼, 블록체인이 탑재된 전자지갑을 기반으로 하는 결제에는 라이트코인, 다크코인, 네임코인, 도기코인 및 리플 등이 있으며, 이 또한 본 발명에서 금융기관의 제증명서 서류의 위변조 검증시에 비트코인과 같은 기능을 수행하는 대체제로 사용가능하다.

[56] 그리고 블록체인 보유서버(300)의 블록체인에는 일반적인 비트코인 결제를 위한 비트코인 결제용 트랜잭션정보와 더불어, 개인적인 정보도 기록가능하다. 즉, 금융기관이 고객에게 제공하는 제증명서인 고객제공용 제증명서 정보 및 고객식별정보를 해싱하여 생성된 제증명서 노드해시정보를 포함하는 제증명서 트랜잭션정보도 기록가능하다.

[57] 즉, 비트코인 결제시 발생하는 거래정보인 트랜잭션정보를 이루는 OP리턴(Operation Code RETURN) 영역에 제증명서 노드해시정보를 삽입하여 전송하면, 개개의 블록체인 보유서버(300)의 전자지갑은 일반적인 비트코인 결제가 아닌 사적인 정보로서 취급하고 전파하며, 제증명서 트랜잭션정보가 OP리턴 영역에 기록됨으로써, 디지털 콘텐츠의 위변조 방지를 판단하는 중요 구성으로 활용된다.

[58] 여기서, 블록체인 보유서버(300)의 전자지갑에서 비트코인 결제 인증 시 비트코인 결제용 트랜잭션정보 중 OP리턴 영역에 메세지가 판독되면, 그 OP리턴 영역에 삽입된 메시지가 기록된 정보는 비트코인 거래정보가 아닌

임의의 데이터값이라는 것을 알리기 위한 정보로 활용된다는 것을 인지할 수 있게 안내하는 역할을 수행한다.

[59] 상기 인증관리서버(200)는 금융기관단말(100)의 기록 인증 요청에 의해 고객제공용 제증명서 및 해당 고객을 식별하는 고객식별정보를 해싱하여 제증명서 노드해시정보로 가공처리하고, 이를 제증명서 등록관련정보DB(211)에 누적저장하되, 그 누적저장되는 제증명서 노드해시정보의 개수가 기설정된 루트해시 생성구간에 도달되면, 해시처리엔진(220)을 운영하여 제증명서 등록관련정보DB(211)에서 기설정된 루트해시 생성구간에 해당하는 개수만큼 추출하고, 그 추출된 제증명서 노드해시정보들이 머클트리 구조로 이루어진 등록용 제증명서 루트해시정보로 가공처리하며, 트랜잭션처리엔진(230)을 운영하여 등록용 제증명서 루트해시정보를 포함하는 제증명서 트랜잭션정보 및 그 제증명서 트랜잭션정보를 검색하는데 키값으로 이용되는 제증명서 트랜잭션 ID정보를 생성하고, 제증명서 트랜잭션 ID정보는 금융기관단말(100)로 전송하며, 제증명서 트랜잭션정보는 기록인증을 위해 전송하는 서버부재이다.

[60] 이러한 기능을 수행하기 위해 인증관리서버(200)에는 앞에서 언급한 해시처리엔진(220) 및 트랜잭션처리엔진(230)과 더불어 DB부(210)가 구비되어진다.

[61] 상기 DB부(210)는 고객증명용 제증명서의 인증을 수행하기 위해 필요한 정보가 저장되는 저장매체로서, 제증명서 등록관련정보DB(211) 및 제증명서 위변조 감시관련정보 DB(212)를 포함한다.

[62] 상기 제증명서 등록관련정보DB(211)에는 고객제공용 제증명서 및 해당 고객을 식별하는 고객식별정보, 누적저장되는 제증명서 노드해시정보 및 등록용 제증명서 루트해시정보 등이 저장되어진다.

[63] 상기 제증명서 위변조 감시관련정보 DB(212)에는 제증명서 트랜잭션 정보 및 제증명서 트랜잭션 ID정보가 누적저장된다.

[64] 상기 트랜잭션처리엔진(230)은 인증관리서버(200)에 의해 운영되는 것으로, 제증명서 노드해시정보를 비트코인의 거래 결제가 아닌 사적인 정보로서 취급되도록 안내하는 OP리턴(Operation Code RETURN)영역에 삽입하여 제증명서 트랜잭션정보를 생성하고, 이를 제증명서 위변조 감시관련정보 DB(212)에 저장되도록 제어함과 아울러 제증명서 트랜잭션정보를 검색하는데 키값으로 이용되는 제증명서 트랜잭션 ID정보를 생성하고, 이 또한 제증명서 위변조 감시관련정보 DB(212)에 저장하며, 생성된 정보 중 제증명서 트랜잭션 ID정보는 금융기관단말(100)로 전송하고, 제증명서 트랜잭션정보는 기록인증을 위해 블록체인 보유서버(300)보유서버(300)도록 제어하는 기능을 수행한다.

[65] 이때, 인증관리서버(200)도 비트코인을 거래하는 기능을 수행할 경우 전자지갑이 탑재될 수 있다.

[66] 이 때에는, 인증관리서버(200)에서 기록인증을 위해 블록체인

보유서버(300)들로 먼저 전송하지 않고, 자신이 보유하고 있는 전자지갑에 제증명서 트랜잭션정보를 입력하면, 인증관리서버(200)의 전자지갑은 제증명서 트랜잭션정보를 판독하고, OP리턴 영역에 정보가 삽입된 것을 인지하면 비트코인 결제를 인증하는 과정을 생략하고, 바로 블록체인에 제증명서 노드해시정보를 포함하는 제증명서 트랜잭션정보를 기록하여 기록 인증을 수행한 상태에서 모든 블록체인 보유서버(300)들에게 전파되도록 기지정된 다음의 블록체인 보유서버(300)들에게 전송한다.

[67] 이를 통해, 해시처리엔진(210)은 후술되는 고객단말(400)로부터 고객제공용 제증명서 정보 및 제증명서 트랜잭션 ID정보가 전송되면, 전송된 정보 중 제증명서 트랜잭션 ID정보를 블록체인 보유서버(300)들에게 전송할 필요 없이 인증관리서버(200)에 탑재된 전자지갑의 블록체인에 직접 제증명서 트랜잭션 ID정보를 매칭하여 다른 블록체인 보유서버(300)들에 기록되어 있는 제증명서 트랜잭션정보의 제증명서 노드해시정보값과 동일한 값을 획득할 수 있다.

[68] 상기 루트해시 생성구간은 블록체인 기반의 고객 제증명서 등록과정 중 고객의 제증명서 정보를 포함하는 트랙잭션정보를 블록체인 보유서버에 등록 시 시스템 관리자가 기설정된 개수 만큼 묶어주는 구간으로서, 이를 통해 기설정된 개수만큼 압축된 고객의 제증명서 정보를 트랜잭션 처리함으로써, 트래픽의 발생을 최소화시켜주고, 이에 따라, 네트워크 과부하도 줄일 수 있도록 제공한다.

[69] 이러한 루트해시 생성구간의 개수는 기설정된 제증명서 노드해시정보의 개수이거나 또는 기설정된 시간 동안 누적저장되는 제증명서 노드해시정보의 개수 등 다양한 경우를 산정하여 그 개수를 지정할 수 있다.

[70] 그리고 인증관리서버(200)는 후술되는 고객단말(400)로부터 전송되는 고객제공용 제증명서 정보, 제증명서 트랜잭션 ID정보 및 고객식별정보를 토대로 해당 제증명서 정보가 위변조 되었는지의 여부를 판단하고, 그 판단에 따른 고객제공용 제증명서 정보의 위변조 여부를 안내하는 고객요청 제증명서 검증정보를 생성하는 기능을 수행한다.

[71] 이를 위해, 인증관리서버(200)는 후술되는 고객단말(400)로부터 고객제공용 제증명서 정보 및 제증명서 트랜잭션 ID정보가 전송되면, 전송된 정보 중 제증명서 트랜잭션 ID정보를 상기 블록체인 보유서버(300)에게 전송하여, 제증명서 트랜잭션정보의 전송을 요청한다. 이때, 블록체인 보유서버(300)는 블록체인 보유서버(300)들 중 사전에 특정하여 운영될 수 있다

[72] 블록체인 보유서버(300)의 전자지갑은 제증명서 트랜잭션 ID정보를 블록체인에 매칭하여 매칭되는 제증명서 트랜잭션정보를 상기 인증관리서버(200)로 전송한다.

[73] 인증관리서버(200)는 해시처리엔진(210)을 운영하여 고객단말(400)로부터 전송된 정보 중 고객제공용 제증명서 정보 및 고객식별정보를 해싱하여 대비용 제증명서 노드해시정보로 가공처리하고, 블록체인 보유서버(300)로부터 전송된

제증명서 트랜잭션정보에 포함된 제증명서 검증용 인덱스 해시값과 상기 대비용 제증명서 노드해시정보값을 각각 연산하여, 양쪽의 해시값의 동일여부를 안내하는 고객요청 제증명서 검증정보를 생성한다.

[74] 또한, 인증관리서버(200)는 금융기관에서 저장관리되고 있는 고객들의 제증명서를 기설정된 주기마다 위변조 여부를 검증하여 해킹과 같은 악의적인 행위에 의해 고객들의 제증명서가 위변조 되는 것을 신속하게 감시할 수 있다.

[75] 이를 위해, 인증관리서버(200)는 제증명서 노드해시정보가 기설정된 루트해시 생성구간에 도달되면 제증명서 위변조 감시관련정보 DB(212)에 누적저장된 제증명서 트랜잭션 ID정보를 모두 추출하고, 그 추출된 각각의 제증명서 트랜잭션 ID정보를 블록체인 보유서버(300)로 전송한다.

[76] 블록체인 보유서버(300)는 전송된 각각의 제증명서 트랜잭션 ID정보를 전자지갑에 구비된 블록체인과 매칭하여, 매칭되는 각각의 제증명서 트랜잭션정보에 포함된 등록용 제증명서 루트해시정보를 추출하고, 그 추출된 각각의 등록용 제증명서 루트해시정보를 인증관리서버(200)로 전송한다.

[77] 인증관리서버(200)는 전송된 각각의 등록용 제증명서 루트해시정보를 전송받고, 해시처리엔진(220)을 운영하여 제증명서 등록관련정보DB(211)에 누적저장된 제증명서 노드해시정보의 개수를 기설정된 루트해시 생성구간에 해당하는 개수로 구분하고, 그 구분된 기설정된 루트해시 생성구간에 해당하는 개수마다 해싱하여 각각의 대비용 제증명서 루트해시정보로 가공처리하며, 각각의 등록용 제증명서 루트해시정보와 각각의 대비용 제증명서 루트해시정보를 생성순번대로 양자대비하고, 생성순번대로 양자대비되는 각각의 등록용 제증명서 루트해시정보와 각각의 대비용 제증명서 루트해시정보의 해시값을 연산하여 첫 번째 생성순번부터 마지막 생성순번까지 그 연산된 양쪽의 해시값이 동일한지 여부를 확인하여, 인증관리서버(200)에서 저장관리되고 있는 고객제공용 제증명서 정보의 위변조 여부를 검증한다.

[78] 이를 통해, 인증관리서버(200)는 검증을 통해 위변조가 야기된 경우 그 위변조가 야기된 해당 금융기관으로 고객의 제증명서에 위변조가 발생되었다는 것을 통보하여 신속하게 대처할 수 있게 제공한다.

[79] 상기 고객단말(400)은 금융기관단말(100)로 고객제공용 제증명서 정보의 다운로드를 요청하고, 그 다운로드 요청에 의해 금융기관단말(100)로부터 전송되는 고객제공용 제증명서 정보 및 제증명서 트랜잭션 ID정보를 인증관리서버(200)로 중계전송하여 고객제공용 제증명서 정보의 위변조 여부의 검증을 요청하며, 인증관리서버(200)로부터 전송되는 고객요청 제증명서 검증정보를 고객이 열람가능하도록 디스플레이하여 주는 단말부재이다.

[80] 이와 같은, 구성으로 이루어진 본 발명의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템을 이용하여 금융기관에서 발급하는 제증명서류의 위변조여부를 검증하는 과정을 설명하면 다음과 같다.

[81] 먼저, 금융기관단말(100)을 운영하는 금융기관 관계자는 금융기관단말(100)을

통해 고객에게 제공되어지는 제증명서인 고객제공용 제증명서 정보가 생성될 때마다 고객제공용 제증명서 목록정보 DB(111)에 저장함과 아울러 그 생성된 고객제공용 제증명서 정보 및 해당 고객을 식별하는 고객식별정보를 인증관리서버(200)로 전송하여 고객제공용 제증명서 정보의 기록 인증을 요청(S110)한다.

[82] 인증관리서버(200)는 전송된 한 조의 고객제공용 제증명서 정보 및 고객식별정보를 제증명서 등록관련정보 DB(211)에 저장함과 아울러 해시처리엔진(210)을 운영하여 고객제공용 제증명서 정보 및 고객식별정보를 해싱하여 제증명서 노드해시정보로 가공처리하고, 이를 제증명서 등록관련정보DB(211)에 누적저장(S120)한다.

[83] 인증관리서버(200)는 누적저장되는 제증명서 노드해시정보가 기설정된 루트해시 생성구간에 도달됐는지 확인(S130)하여, 루트해시 생성구간에 도달되지 않은경우 도달될 때까지 계속 확인하며, 루트해시 생성구간에 도달되면, 두 가지의 작업을 수행한다.

[84] 먼저, 인증관리서버(200)는 누적저장되는 제증명서 노드해시정보가 기설정된 루트해시 생성구간에 도달된 경우 금융기관에서 저장관리되고 있는 고객들의 제증명서가 해킹과 같은 악의적인 행위에 의해 고객들의 제증명서가 위변조 되는 것을 감시하기 위해, 제증명서 위변조 감시관련정보 DB(212)에 누적저장된 제증명서 트랜잭션 ID정보를 모두 추출하고, 그 추출된 각각의 제증명서 트랜잭션 ID정보를 블록체인 보유서버(300)로 전송(S131)한다.

[85] 블록체인 보유서버(300)는 전송된 각각의 제증명서 트랜잭션 ID정보를 전자지갑에 구비된 블록체인과 매칭하여, 매칭되는 각각의 제증명서 트랜잭션정보에 포함된 등록용 제증명서 루트해시정보를 추출(S132)한다.

[86] 블록체인 보유서버(300)는 각각의 등록용 제증명서 루트해시정보를 인증관리서버(200)로 전송(S133)한다.

[87] 인증관리서버(200)는 전송된 각각의 등록용 제증명서 루트해시정보를 전송받고, 해시처리엔진(220)을 운영하여 제증명서 등록관련정보DB(211)에 누적저장된 제증명서 노드해시정보의 개수를 기설정된 루트해시 생성구간에 해당하는 개수로 구분하고, 그 구분된 기설정된 루트해시 생성구간에 해당하는 개수마다 해싱하여 각각의 대비용 제증명서 루트해시정보로 가공처리(S134)한다.

[88] 이후, 인증관리서버(200)의 해시처리엔진(220)은 각각의 등록용 제증명서 루트해시정보와 각각의 대비용 제증명서 루트해시정보를 생성순번대로 양자대비하고, 생성순번대로 양자대비되는 각각의 등록용 제증명서 루트해시정보와 각각의 대비용 제증명서 루트해시정보의 해시값을 연산하여 첫 번째 생성순번부터 마지막 생성순번까지 그 연산된 양쪽의 해시값이 동일한지 여부를 확인하여, 인증관리서버(200)에서 저장관리되고 있는 고객제공용 제증명서 정보의 위변조 여부를 검증(S135)한다.

[89] 이와 더불어, 인증관리서버(200)는 누적저장되는 제증명서 노드해시정보가 기설정된 루트해시 생성구간에 도달되면, 추가로 해시처리엔진(220)을 운영하여 제증명서 등록관련정보DB(211)에서 기설정된 루트해시 생성구간에 해당하는 개수만큼 추출하고, 그 추출된 제증명서 노드해시정보들을 머클트리 구조로 이루어진 등록용 제증명서 루트해시정보로 가공처리(S140)한다.

[90] 이후, 인증관리서버(200)는 트랜잭션처리엔진(230)을 운영하여 등록용 제증명서 루트해시정보를 포함하는 제증명서 트랜잭션정보 및 그 제증명서 트랜잭션정보를 검색하는데 키값으로 이용되는 제증명서 트랜잭션 ID정보를 생성하고, 생성된 정보 중 제증명서 트랜잭션정보를 블록체인 보유서버(300)들로 전송(S150)한다.

[91] 블록체인 보유서버(300)들은 전송되는 제증명서 트랜잭션정보를 블록체인에 기록하여 기록 인증을 수행(S160)한다.

[92] 이후, 인증관리서버(200)의 트랜잭션처리엔진(230)은 제증명서 트랜잭션 ID정보를 금융기관단말(100)로 전송(S170)한다.

[93] 금융기관단말(100)은 전송되는 제증명서 트랜잭션 ID정보를 제증명서 위변조 감시관련정보 DB(212)에 저장관리(S180)한다.

[94] 고객단말(400)은 금융기관단말(100)로 고객제공용 제증명서 정보의 다운로드를 요청(S190)한다.

[95] 금융기관단말(100)은 다운로드 요청된 고객제공용 제증명서 정보 및 해당 고객제공용 제증명서 정보에 대응되는 제증명서 트랜잭션 ID정보를 고객단말(400)로 전송(S200)한다.

[96] 고객단말(400)은 전송되는 고객제공용 제증명서 정보 및 제증명서 트랜잭션 ID정보와 해당 고객임을 식별하는 고객식별정보를 인증관리서버(200)로 중계전송하여 고객제공용 제증명서 정보의 위변조 여부에 따른 검증을 요청(S210)한다.

[97] 인증관리서버(200)은 전송되는 고객제공용 제증명서 정보, 제증명서 트랜잭션 ID정보 및 고객식별정보를 토대로 해당 제증명서 정보가 위변조 되었는지의 여부를 판단하고, 그 판단에 따른 고객제공용 제증명서 정보의 위변조 여부를 안내하는 고객요청 제증명서 검증정보를 생성하여 상기 고객단말(400)로 전송(S220)한다.

[98] 이때, 고객요청 제증명서 검증정보 생성과정은 다음과 같다.

[99] 먼저, 인증관리서버(200)는 고객제공용 제증명서 정보 및 제증명서 트랜잭션 ID정보가 전송되면, 전송된 정보 중 제증명서 트랜잭션 ID정보를 블록체인 보유서버(300)에게 전송하여, 제증명서 트랜잭션정보의 전송을 요청(S221)한다.

[100] 블록체인 보유서버(300)의 전자지갑은 전송되는 제증명서 트랜잭션 ID정보를 블록체인에 매칭하여 매칭되는 제증명서 트랜잭션정보를 인증관리서버(200)로 전송(S222)한다.

[101] 인증관리서버(200)는 해시처리엔진(210)을 운영하여 고객단말(400)로부터

전송된 정보 중 고객제공용 제증명서 정보 및 고객식별정보를 해싱하여 대비용 제증명서 노드해시정보로 가공처리하고, 블록체인 보유서버(300)로부터 전송된 제증명서 트랜잭션정보에 포함된 제증명서 검증용 인덱스 해시값과 대비용 제증명서 노드해시정보값을 각각 연산하여, 양쪽의 해시값의 동일여부를 안내하는 고객요청 제증명서 검증정보를 생성(S223)함으로써 완료한다.

[102] 고객단말(400)은 전송된 고객요청 제증명서 검증정보를 열람(S230)하여 위변조 여부를 확인함으로써, 올바르게 금융관련서류를 제공받아 사용할 수 있다.

[103]

[104] 그리고 본 발명의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템은 금융기관에서 발급하는 다양한 고객제공용 제증명서 정보가 위변조 여부의 확인을 위해 인증관리서버(200)로 전송되기 때문에 대외비 서류의 유출 위험성에 노출된다.

[105] 이를 방지하기 위한 본 발명의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템은 다른 실시예를 제공할 수 있다.

[106] 도 7은 본 발명의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템의 다른 실시예에 따른 금융기관단말을 나타낸 블록구성도, 도 8 내지 도 10은 본 발명의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템의 다른 실시예에 따른 제증명서류의 위변조여부 검증 과정을 나타낸 순서도이다.

[107] 이에, 앞에서 언급한 기본실시예에 따른 기술구성인 금융기관단말(100), 인증관리서버(200), 블록체인 보유서버(300)들 및 고객단말(400)은 동일하되, 내부구성 및 작동관계가 일부 차이가 있으며, 앞에서 언급한 기본실시예에 따른 기술구성과 차이가 없고, 동일한 작동관계를 수행하기는 기술구성의 도면부호는 동일한 도면부호를 사용함으로써, 다른 실시예에 따른 본 발명의 설명을 명확하게 언급하기로 한다.

[108] 먼저, 금융기관단말(100)에는 인증관리서버(200)로 고객제공용 제증명서 정보가 전송되지 않으면서도 위변조 여부 과정을 수행할 수 있도록 해시처리엔진(120)이 탑재되어진다.

[109] 이를 통해, 금융기관단말(100)은 금융기관에서, 고객에게 제공되어지는 제증명서인 고객제공용 제증명서 정보가 생성되면, 해시처리엔진(120)을 운영하여 고객제공용 제증명서 정보 및 해당 고객을 식별하는 고객식별정보를 해싱하여 제증명서 노드해시정보로 가공처리하고, 그 가공처리된 제증명서 노드해시정보의 기록 인증을 요청하며, 그 기록 인증 요청에 의해 전송되는 제증명서 트랜잭션 ID정보를 저장하고, 고객제공용 제증명서 정보의 다운로드가 요청되면 고객제공용 제증명서 정보 및 제증명서 트랜잭션 ID정보를 전송하며, 고객단말(400)로부터 고객제공용 제증명서 정보의 다운로드가 요청되면 그 요청된 고객제공용 제증명서 정보 및 제증명서

트랜잭션 ID정보를 고객단말(400)로 전송하는 기능을 수행한다.

[110] 그리고 고객단말(400)에도 해시처리엔진이 탑재되어 있어, 금융기관단말(100)로 고객제공용 제증명서 정보의 다운로드 요청에 의해 금융기관단말(100)로부터 고객제공용 제증명서 정보 및 상기 제증명서 트랜잭션 ID정보가 전송되면, 해시처리엔진을 운영하여 고객제공용 제증명서 정보와 해당 고객을 식별하는 고객식별정보를 해싱하여 대비용 제증명서 노드해시정보로 가공처리하고, 그 가공처리된 대비용 제증명서 노드해시정보와 제증명서 트랜잭션 ID정보를 인증관리서버(200)로 전송하는 기능을 수행한다.

[111] 이에 따라, 인증관리서버(200)는 전송되는 대비용 제증명서 노드해시정보 및 제증명서 트랜잭션 ID정보를 토대로 해당 제증명서 정보가 위변조 되었는지의 여부를 판단하고, 그 판단에 따른 고객제공용 제증명서 정보의 위변조 여부를 안내하는 고객요청 제증명서 검증정보를 생성하여 상기 고객단말(400)로 전송되도록 제어하는 부분이 차이점이다.

[112] 이와 같은, 다른 실시예에 따른 본 발명의 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증과정을 설명하면 다음과 같다.

[113] 먼저, 금융기관단말(100)은 고객에게 제공되어지는 제증명서인 고객제공용 제증명서 정보가 생성되면, 해시처리엔진(120)을 운영하여 고객제공용 제증명서 정보 및 해당 고객을 식별하는 고객식별정보를 해싱하여 제증명서 노드해시정보로 가공처리하고, 그 가공처리된 제증명서 노드해시정보를 인증관리서버(200)로 전송하여 고객제공용 제증명서 정보의 기록 인증을 요청(S310)한다.

[114] 인증관리서버(200)는 전송된 제증명서 노드해시정보를 제증명서 등록관련정보 DB(211)에 누적저장(S320)한다.

[115] 이때, 인증관리서버(200)는 누적저장되는 제증명서 노드해시정보가 기설정된 루트해시 생성구간에 도달됐는지 확인(S330)하여, 루트해시 생성구간에 도달되지 않은경우 도달될 때까지 계속 확인하며, 루트해시 생성구간에 도달되면, 두 가지의 작업을 수행한다.

[116] 먼저, 인증관리서버(200)는 제증명서 노드해시정보가 기설정된 루트해시 생성구간에 도달된 경우 제증명서 위변조 감시관련정보 DB(212)에 누적저장된 제증명서 트랜잭션 ID정보를 모두 추출하고, 그 추출된 각각의 제증명서 트랜잭션 ID정보를 블록체인 보유서버(300)로 전송(S331)한다.

[117] 블록체인 보유서버(300)는 전송된 각각의 제증명서 트랜잭션 ID정보를 전자지갑에 구비된 블록체인과 매칭하여, 매칭되는 각각의 제증명서 트랜잭션정보에 포함된 등록용 제증명서 루트해시정보를 추출(S332)하고, 추출된 각각의 등록용 제증명서 루트해시정보를 인증관리서버(200)로 전송(S333)한다.

[118] 인증관리서버(200)는 전송된 각각의 등록용 제증명서 루트해시정보를 전송받고, 해시처리엔진(220)을 운영하여 제증명서 등록관련정보DB(211)에

누적저장된 제증명서 노드해시정보의 개수를 기설정된 루트해시 생성구간에 해당하는 개수로 구분하고, 그 구분된 기설정된 루트해시 생성구간에 해당하는 개수마다 해싱하여 각각의 대비용 제증명서 루트해시정보로 가공처리(S334)한다.

[119] 이후, 인증관리서버(200)의 해시처리엔진(220)은 각각의 등록용 제증명서 루트해시정보와 각각의 대비용 제증명서 루트해시정보를 생성순번대로 양자대비하고, 생성순번대로 양자대비되는 각각의 등록용 제증명서 루트해시정보와 각각의 대비용 제증명서 루트해시정보의 해시값을 연산하여 첫 번째 생성순번부터 마지막 생성순번까지 그 연산된 양쪽의 해시값이 동일한지 여부를 확인하여, 인증관리서버(200)에서 저장관리되고 있는 고객제공용 제증명서 정보의 위변조 여부를 검증(S335)한다.

[120] 이와 더불어, 인증관리서버(200)는 누적저장되는 제증명서 노드해시정보가 기설정된 루트해시 생성구간에 도달되면, 해시처리엔진(220)을 운영하여 제증명서 등록관련정보DB(211)에서 기설정된 루트해시 생성구간에 해당하는 개수만큼 추출하고, 그 추출된 제증명서 노드해시정보들을 머클트리 구조로 이루어진 등록용 제증명서 루트해시정보로 가공처리(S340)한다.

[121] 이후, 인증관리서버(200)은 트랜잭션처리엔진(230)을 운영하여 등록용 제증명서 루트해시정보를 포함하는 제증명서 트랜잭션정보 및 그 제증명서 트랜잭션정보를 검색하는데 키값으로 이용되는 제증명서 트랜잭션 ID정보를 생성하고, 생성된 정보 중 제증명서 트랜잭션정보를 블록체인 보유서버(300)들로 전송(S350)한다.

[122] 블록체인 보유서버(300)들은 전송되는 제증명서 트랜잭션정보를 블록체인에 기록하여 기록 인증을 수행(S360)한다.

[123] 인증관리서버(200)의 트랜잭션처리엔진(230)은 제증명서 트랜잭션 ID정보를 금융기관단말(100)로 전송(S370)한다.

[124] 금융기관단말(100)은 전송되는 제증명서 트랜잭션 ID정보를 저장관리(S380)한다.

[125] 고객단말(400)은 금융기관단말(100)로 고객제공용 제증명서 정보의 다운로드를 요청(S390)한다.

[126] 금융기관단말(100)은 그 다운로드 요청된 고객제공용 제증명서 정보 및 해당 고객제공용 제증명서 정보 에 대응되는 제증명서 트랜잭션 ID정보를 고객단말(400)로 전송(S400)한다.

[127] 고객단말(400)은 해시처리엔진을 운영하여 전송된 고객제공용 제증명서 정보 및 제증명서 트랜잭션 ID정보 중 고객제공용 제증명서 정보와 해당 고객을 식별하는 고객식별정보를 해싱하여 대비용 제증명서 노드해시정보로 가공처리하고, 그 가공처리된 대비용 제증명서 노드해시정보와 제증명서 트랜잭션 ID정보를 상기 인증관리서버(200)로 전송하여 고객제공용 제증명서 정보의 위변조 여부에 따른 검증을 요청(S410)한다.

[128] 인증관리서버(200)는 전송되는 대비용 제증명서 노드해시정보 및 제증명서 트랜잭션 ID정보를 토대로 해당 제증명서 정보가 위변조 되었는지의 여부를 판단하고, 그 판단에 따른 고객제공용 제증명서 정보의 위변조 여부를 안내하는 고객요청 제증명서 검증정보를 생성하여 상기 고객단말(400)로 전송(S420)한다.

[129] 이때, 고객요청 제증명서 검증정보 생성과정은 다음과 같다.

[130] 인증관리서버(200)는 대비용 제증명서 노드해시정보 및 제증명서 트랜잭션 ID정보가 전송되면, 전송된 정보 중 제증명서 트랜잭션 ID정보를 상기 블록체인 보유서버(300)에게 전송하여, 제증명서 트랜잭션정보의 전송을 요청(S421)한다.

[131] 블록체인 보유서버(300)의 전자지갑은 제증명서 트랜잭션 ID정보를 블록체인에 매칭하여 매칭되는 제증명서 트랜잭션정보를 인증관리서버(200)로 전송(S422)한다.

[132] 인증관리서버(200)는 해시처리엔진(210)을 운영하여 블록체인 보유서버(300)로부터 전송된 제증명서 트랜잭션정보에 포함된 제증명서 검증용 인덱스 해시값과 대비용 제증명서 노드해시정보값을 각각 연산하여, 양쪽의 해시값의 동일여부를 안내하는 고객요청 제증명서 검증정보를 생성(S423)한다.

[133] 고객단말(400)은 전송된 고객요청 제증명서 검증정보를 열람(S430)한다.

[134] [부호의 설명]

[135] 100 : 금융기관단말 110,210 : 해시처리엔진

[136] 110,210 : DB부

[137] 111 : 고객 제공용 제증명서 목록정보 DB

[138] 112 : 트랜잭션 식별자 목록정보 DB

[139] 111 : 제증명서 노드해시정보 목록정보 DB

[140] 112 : 제증명서 검증용 트랜잭션 목록정보 DB

[141] 200 : 인증관리서버

[142] 211 : 제증명서 등록관련정보 DB

[143] 212 : 제증명서 위변조 감시관련정보 DB

[144] 220 : 트랜잭션 전파안내엔진 300 : 블록체인 보유서버

[145] 400 : 고객단말

청구범위

[청구항 1] 금융기관에서 고객에게 제공되어지는 제증명서인 고객제공용 제증명서 정보 생성 시 그 생성된 고객제공용 제증명서 정보의 기록 인증을 요청하고, 그 기록 인증 요청에 의해 전송되는 제증명서 트랜잭션 ID정보를 저장하며, 상기 고객제공용 제증명서 정보의 다운로드가 요청되면 상기 고객제공용 제증명서 정보 및 상기 제증명서 트랜잭션 ID정보를 전송하는 금융기관단말(100)과;
상기 금융기관단말(100)의 기록 인증 요청에 의해 상기 고객제공용 제증명서 및 해당 고객을 식별하는 고객식별정보를 해싱하여 제증명서 노드해시정보로 가공처리하고, 이를 제증명서 등록관련정보DB(211)에 누적저장하되, 그 누적저장되는 제증명서 노드해시정보의 개수가 기설정된 루트해시 생성구간에 도달되면, 해시처리엔진(220)을 운영하여 상기 제증명서 등록관련정보DB(211)에서 기설정된 루트해시 생성구간에 해당하는 개수만큼 추출하고, 그 추출된 제증명서 노드해시정보들이 머클트리 구조로 이루어진 등록용 제증명서 루트해시정보로 가공처리하며, 트랜잭션처리엔진(230)을 운영하여 상기 등록용 제증명서 루트해시정보를 포함하는 제증명서 트랜잭션정보 및 그 제증명서 트랜잭션정보를 검색하는데 키값으로 이용되는 제증명서 트랜잭션 ID정보를 생성하고, 상기 제증명서 트랜잭션 ID정보는 상기 금융기관단말(100)로 전송하며, 상기 제증명서 트랜잭션정보는 기록인증을 위해 전송하는 인증관리서버(200)와;
비트코인 결제용 트랜잭션정보가 전송 시 그 전송된 비트코인 결제용 트랜잭션정보를 검증을 통해 비트코인 결제를 인증하고, 그 인증에 따라 비트코인 결제용 트랜잭션정보가 기록되는 블록체인을 갖는 전자지갑이 탑재된 것으로, 상기 인증관리서버(200)로부터 전송되는 제증명서 트랜잭션정보를 상기 블록체인에 기록하는 블록체인 보유서버(300)들과;
상기 금융기관단말(100)로 고객제공용 제증명서 정보의 다운로드를 요청하고, 그 다운로드 요청에 의해 상기 금융기관단말(100)로부터 전송되는 상기 고객제공용 제증명서 정보 및 상기 제증명서 트랜잭션 ID정보를 상기 인증관리서버(200)로 중계전송하여 상기 고객제공용 제증명서 정보의 위변조 여부의 검증을 요청하는 고객단말(400);로 이루어지고,

상기 인증관리서버(200)는 상기 전송되는 고객제공용 제증명서 정보, 제증명서 트랜잭션 ID정보 및 고객식별정보를 토대로 해당 제증명서 정보가 위변조 되었는지의 여부를 판단하고, 그 판단에 따른 고객제공용 제증명서 정보의 위변조 여부를 안내하는 고객요청 제증명서 검증정보를 생성하고, 이를 상기 고객단말(400)로 전송되도록 제어하는 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템.

[청구항 2] 제1항에 있어서,
상기 루트해시 생성구간은 기설정된 제증명서 노드해시정보의 개수이거나 또는 기설정된 시간동안 누적저장되는 제증명서 노드해시정보의 개수인 것을 특징으로 하는 금융기관 제증명서류 위변조 검증시스템.

[청구항 3] 제1항에 있어서,
상기 인증관리서버(200)는 상기 제증명서 노드해시정보가 기설정된 루트해시 생성구간에 도달되면 상기 제증명서 위변조 감시관련정보 DB(212)에 누적저장된 제증명서 트랜잭션 ID정보를 모두 추출하고, 그 추출된 각각의 제증명서 트랜잭션 ID정보를 블록체인 보유서버(300)로 전송하며,
상기 블록체인 보유서버(300)는 전송된 각각의 제증명서 트랜잭션 ID정보를 전자지갑에 구비된 블록체인과 매칭하여, 매칭되는 각각의 제증명서 트랜잭션정보에 포함된 등록용 제증명서 루트해시정보를 추출하고, 그 추출된 각각의 등록용 제증명서 루트해시정보를 상기 인증관리서버(200)로 전송하며,
상기 인증관리서버(200)는 전송된 각각의 등록용 제증명서 루트해시정보를 전송받고, 해시처리엔진(220)을 운영하여 제증명서 등록관련정보DB(211)에 누적저장된 제증명서 노드해시정보의 개수를 기설정된 루트해시 생성구간에 해당하는 개수로 구분하고, 그 구분된 기설정된 루트해시 생성구간에 해당하는 개수마다 해싱하여 각각의 대비용 제증명서 루트해시정보로 가공처리하며, 각각의 등록용 제증명서 루트해시정보와 각각의 대비용 제증명서 루트해시정보를 생성순번대로 양자대비하고, 생성순번대로 양자대비되는 각각의 등록용 제증명서 루트해시정보와 각각의 대비용 제증명서 루트해시정보의 해시값을 연산하여 첫 번째 생성순번부터 마지막 생성순번까지 그 연산된 양쪽의 해시값이 동일한지 여부를 확인하여, 상기 인증관리서버(200)에서 저장관리되고 있는 고객제공용 제증명서 정보의 위변조 여부를 검증하는 것을

특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템.

[청구항 4] 제1항에 있어서,
상기 인증관리서버(200)의 트랜잭션처리엔진(230)은 상기 등록용 제증명서 루트해시정보를 상기 제증명서 트랜잭션정보 중 비트코인의 거래 결제가 아닌 사적인 정보로서 취급되도록 안내하는 OP리턴(Operation Code RETURN) 영역에 삽입하여 전송되도록 제어하는 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템.

[청구항 5] 제4항에 있어서,
상기 각 블록체인 보유서버(300)에 탑재된 전자지갑은, 상기 전송된 제증명서 트랜잭션정보를 판독하여 OP리턴 영역에 정보가 삽입된 것을 인지하면, 비트코인 결제를 인증하는 과정을 생략하고, 바로 상기 블록체인에 기록되도록 제어하는 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증방법.

[청구항 6] 제1항에 있어서,
상기 고객요청 제증명서 검증정보의 생성과정은,
상기 인증관리서버(200)에서, 상기 고객제공용 제증명서 정보 및 제증명서 트랜잭션 ID정보가 전송되면, 전송된 정보 중 제증명서 트랜잭션 ID정보를 상기 블록체인 보유서버(300)에게 전송하여, 제증명서 트랜잭션정보의 전송을 요청하고,
상기 블록체인 보유서버(300)의 전자지갑에서, 상기 제증명서 트랜잭션 ID정보를 블록체인에 매칭하여 매칭되는 제증명서 트랜잭션정보를 상기 인증관리서버(200)로 전송하며,
상기 인증관리서버(200)에서, 해시처리엔진(210)을 운영하여 상기 고객단말(400)로부터 전송된 정보 중 고객제공용 제증명서 정보 및 고객식별정보를 해싱하여 대비용 제증명서 노드해시정보로 가공처리하고, 상기 블록체인 보유서버(300)로부터 전송된 제증명서 트랜잭션정보에 포함된 제증명서 검증용 인덱스 해시값과 상기 대비용 제증명서 노드해시정보값을 각각 연산하여, 양쪽의 해시값의 동일여부를 안내하는 고객요청 제증명서 검증정보로 생성되는 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템.

[청구항 7] 금융기관단말(100)에서, 고객에게 제공되어지는 제증명서인 고객제공용 제증명서 정보 생성 시 그 생성된 고객제공용 제증명서 정보 및 해당 고객을 식별하는 고객식별정보를 인증관리서버(200)로 전송하여 고객제공용 제증명서 정보의 기록

인증을 요청하는 단계(S110)와;
상기 인증관리서버(200)에서, 전송된 한 조의 고객제공용 제증명서 정보 및 고객식별정보를 제증명서 등록관련정보 DB(211)에 저장함과 아울러 해시처리엔진(210)을 운영하여 상기 고객제공용 제증명서 정보 및 고객식별정보를 해싱하여 제증명서 노드해시정보로 가공처리하고, 이를 제증명서 등록관련정보DB(211)에 누적저장하는 단계(S120)와;
상기 인증관리서버(200)에서, 상기 누적저장되는 제증명서 노드해시정보가 기설정된 루트해시 생성구간에 도달됐는지 확인하는 단계(S130)와;
상기 인증관리서버(200)에서, 상기 누적저장되는 제증명서 노드해시정보가 기설정된 루트해시 생성구간에 도달되면, 해시처리엔진(220)을 운영하여 상기 제증명서 등록관련정보DB(211)에서 기설정된 루트해시 생성구간에 해당하는 개수만큼 추출하고, 그 추출된 제증명서 노드해시정보들을 머클트리 구조로 이루어진 등록용 제증명서 루트해시정보로 가공처리하는 단계(S140)와;
상기 인증관리서버(200)에서, 트랜잭션처리엔진(230)을 운영하여 상기 등록용 제증명서 루트해시정보를 포함하는 제증명서 트랜잭션정보 및 그 제증명서 트랜잭션정보를 검색하는데 키값으로 이용되는 제증명서 트랜잭션 ID정보를 생성하고, 상기 생성된 정보 중 제증명서 트랜잭션정보를 블록체인 보유서버(300)들로 전송하는 단계(S150)와;
상기 블록체인 보유서버(300)들에서, 상기 전송되는 제증명서 트랜잭션정보를 블록체인에 기록하여 기록 인증을 수행하는 단계(S160)와;
상기 인증관리서버(200)의 트랜잭션처리엔진(230)에서, 상기 제증명서 트랜잭션 ID정보를 상기 금융기관단말(100)로 전송하는 단계(S170)와;
상기 금융기관단말(100)에서, 상기 전송되는 제증명서 트랜잭션 ID정보를 저장관리하는 단계(S180)와;
고객단말(400)에서, 상기 금융기관단말(100)로 고객제공용 제증명서 정보의 다운로드를 요청하는 단계(S190)와;
상기 금융기관단말(100)에서, 그 다운로드 요청된 고객제공용 제증명서 정보 및 해당 고객제공용 제증명서 정보 에 대응되는 제증명서 트랜잭션 ID정보를 고객단말(400)로 전송하는 단계(S200)와;
상기 고객단말(400)에서, 상기 전송되는 고객제공용 제증명서

정보 및 제증명서 트랜잭션 ID정보와 해당 고객임을 식별하는 고객식별정보를 상기 인증관리서버(200)로 중계전송하여 상기 고객제공용 제증명서 정보의 위변조 여부에 따른 검증을 요청하는 단계(S210)와;
상기 인증관리서버(200)에서, 상기 전송되는 고객제공용 제증명서 정보, 제증명서 트랜잭션 ID정보 및 고객식별정보를 토대로 해당 제증명서 정보가 위변조 되었는지의 여부를 판단하고, 그 판단에 따른 고객제공용 제증명서 정보의 위변조 여부를 안내하는 고객요청 제증명서 검증정보를 생성하여 상기 고객단말(400)로 전송하는 단계(S220)와;
상기 고객단말(400)에서, 상기 전송된 고객요청 제증명서 검증정보를 열람하는 단계(S230);로 이루어진 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증방법.

[청구항 8] 제7항에 있어서,
상기 루트해시 생성구간은 기설정된 제증명서 노드해시정보의 개수이거나 또는 기설정된 시간동안 누적저장되는 제증명서 노드해시정보의 개수인 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증방법.

[청구항 9] 제7항에 있어서,
상기 인증관리서버(200)에서, 상기 누적저장되는 제증명서 노드해시정보가 기설정된 루트해시 생성구간에 도달됐는지 확인하는 S130단계에 있어서,
상기 인증관리서버(200)에서, 제증명서 노드해시정보가 기설정된 루트해시 생성구간에 도달된 경우 제증명서 위변조 감시관련정보 DB(212)에 누적저장된 제증명서 트랜잭션 ID정보를 모두 추출하고, 그 추출된 각각의 제증명서 트랜잭션 ID정보를 블록체인 보유서버(300)로 전송하는 단계(S131)와;
상기 블록체인 보유서버(300)에서 전송된 각각의 제증명서 트랜잭션 ID정보를 전자지갑에 구비된 블록체인과 매칭하여, 매칭되는 각각의 제증명서 트랜잭션정보에 포함된 등록용 제증명서 루트해시정보를 추출하는 단계(S132)와;
상기 블록체인 보유서버(300)에서 각각의 등록용 제증명서 루트해시정보를 상기 인증관리서버(200)로 전송하는 단계(S133)와;
상기 인증관리서버(200)에서, 전송된 각각의 등록용 제증명서 루트해시정보를 전송받고, 해시처리엔진(220)을 운영하여 제증명서 등록관련정보DB(211)에 누적저장된 제증명서 노드해시정보의 개수를 기설정된 루트해시 생성구간에 해당하는

개수로 구분하고, 그 구분된 기설정된 루트해시 생성구간에 해당하는 개수마다 해싱하여 각각의 대비용 제증명서 루트해시정보로 가공처리하는 단계(S134)와;
상기 인증관리서버(200)의 해시처리엔진(220)에서, 각각의 등록용 제증명서 루트해시정보와 각각의 대비용 제증명서 루트해시정보를 생성순번대로 양자대비하고, 생성순번대로 양자대비되는 각각의 등록용 제증명서 루트해시정보와 각각의 대비용 제증명서 루트해시정보의 해시값을 연산하여 첫 번째 생성순번부터 마지막 생성순번까지 그 연산된 양쪽의 해시값이 동일한지 여부를 확인하여, 상기 인증관리서버(200)에서 저장관리되고 있는 고객제공용 제증명서 정보의 위변조 여부를 검증하는 단계(S135);를 포함하는 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증방법.

[청구항 10] 제7항에 있어서,
상기 인증관리서버(200)에서, 트랜잭션처리엔진(230)을 운영하여 상기 등록용 제증명서 루트해시정보를 포함하는 제증명서 트랜잭션정보 및 그 제증명서 트랜잭션정보를 검색하는데 키값으로 이용되는 제증명서 트랜잭션 ID정보를 생성하고, 상기 생성된 정보 중 제증명서 트랜잭션정보를 블록체인 보유서버(300)들로 전송하는 S150단계에 있어서,
상기 트랜잭션처리엔진(230)은, 상기 등록용 제증명서 루트해시정보를 상기 제증명서 트랜잭션정보 중 비트코인의 거래 결제가 아닌 사적인 정보로서 취급되도록 안내하는 OP리턴(Operation Code RETURN) 영역에 삽입하여 전송되도록 제어하는 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증방법.

[청구항 11] 제10항에 있어서,
상기 블록체인 보유서버(300)들에서, 상기 전송되는 제증명서 트랜잭션정보를 블록체인에 기록하여 기록 인증을 수행하는 S160단계에 있어서,
상기 각 블록체인 보유서버(300)에 탑재된 전자지갑은, 상기 전송된 제증명서 트랜잭션정보를 판독하여 OP리턴 영역에 정보가 삽입된 것을 인지하면, 비트코인 결제를 인증하는 과정을 생략하고, 바로 상기 블록체인에 기록되도록 제어하는 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증방법.

[청구항 12] 제7항에 있어서,
상기 인증관리서버(200)에서, 상기 전송되는 고객제공용 제증명서

정보, 제증명서 트랜잭션 ID정보 및 고객식별정보를 토대로 해당 제증명서 정보가 위변조 되었는지의 여부를 판단하고, 그 판단에 따른 고객제공용 제증명서 정보의 위변조 여부를 안내하는 고객요청 제증명서 검증정보를 생성하여 상기 고객단말(400)로 전송하는 S220단계에 있어서,
상기 고객요청 제증명서 검증정보 생성과정은,
상기 인증관리서버(200)에서, 상기 고객제공용 제증명서 정보 및 제증명서 트랜잭션 ID정보가 전송되면, 전송된 정보 중 제증명서 트랜잭션 ID정보를 상기 블록체인 보유서버(300)에게 전송하여, 제증명서 트랜잭션정보의 전송을 요청하는 단계(S221)와;
상기 블록체인 보유서버(300)의 전자지갑에서 상기 제증명서 트랜잭션 ID정보를 블록체인에 매칭하여 매칭되는 제증명서 트랜잭션정보를 상기 인증관리서버(200)로 전송하는 단계(S222)와;
상기 인증관리서버(200)에서, 해시처리엔진(210)을 운영하여 상기 고객단말(400)로부터 전송된 정보 중 고객제공용 제증명서 정보 및 고객식별정보를 해싱하여 대비용 제증명서 노드해시정보로 가공처리하고, 상기 블록체인 보유서버(300)로부터 전송된 제증명서 트랜잭션정보에 포함된 제증명서 검증용 인덱스 해시값과 상기 대비용 제증명서 노드해시정보값을 각각 연산하여, 양쪽의 해시값의 동일여부를 안내하는 고객요청 제증명서 검증정보를 생성하는 단계(S223);로 이루어진 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증방법.

[청구항 13] 금융기관에서, 고객에게 제공되어지는 제증명서인 고객제공용 제증명서 정보가 생성되면, 해시처리엔진(120)을 운영하여 상기 고객제공용 제증명서 정보 및 해당 고객을 식별하는 고객식별정보를 해싱하여 제증명서 노드해시정보로 가공처리하고, 그 가공처리된 제증명서 노드해시정보의 기록 인증을 요청하며, 그 기록 인증 요청에 의해 전송되는 제증명서 트랜잭션 ID정보를 저장하고, 상기 고객제공용 제증명서 정보의 다운로드가 요청되면 상기 고객제공용 제증명서 정보 및 상기 제증명서 트랜잭션 ID정보를 전송하는 금융기관단말(100)과;
상기 금융기관단말(100)의 기록 인증 요청에 의해 제증명서 노드해시정보를 제증명서 등록관련정보DB(211)에 누적저장하되, 그 누적저장되는 제증명서 노드해시정보의 개수가 기설정된 루트해시 생성구간에 도달되면, 해시처리엔진(220)을 운영하여 상기 제증명서 등록관련정보DB(211)에서 기설정된 루트해시 생성구간에 해당하는 개수만큼 추출하고, 그 추출된 제증명서

노드해시정보들이 머클트리 구조로 이루어진 등록용 제증명서 루트해시정보로 가공처리하며, 트랜잭션처리엔진(230)을 운영하여 상기 등록용 제증명서 루트해시정보를 포함하는 제증명서 트랜잭션정보 및 그 제증명서 트랜잭션정보를 검색하는데 키값으로 이용되는 제증명서 트랜잭션 ID정보를 생성하고, 상기 제증명서 트랜잭션 ID정보는 상기 금융기관단말(100)로 전송하며, 상기 제증명서 트랜잭션정보는 기록인증을 위해 전송하는 인증관리서버(200)와;
비트코인 결제용 트랜잭션정보가 전송 시 그 전송된 비트코인 결제용 트랜잭션정보를 검증을 통해 비트코인 결제를 인증하고, 그 인증에 따라 비트코인 결제용 트랜잭션정보가 기록되는 블록체인을 갖는 전자지갑이 탑재된 것으로, 상기 인증관리서버(200)로부터 전송되는 제증명서 트랜잭션정보를 상기 블록체인에 기록하는 블록체인 보유서버(300)들과;
상기 금융기관단말(100)로 고객제공용 제증명서 정보의 다운로드를 요청하여 상기 고객제공용 제증명서 정보 및 상기 제증명서 트랜잭션 ID정보를 전송받고, 해시처리엔진을 운영하여 상기 고객제공용 제증명서 정보와 해당 고객을 식별하는 고객식별정보를 해싱하여 대비용 제증명서 노드해시정보로 가공처리하고, 그 가공처리된 대비용 제증명서 노드해시정보와 상기 제증명서 트랜잭션 ID정보를 상기 인증관리서버(200)로 전송하여 상기 고객제공용 제증명서 정보의 위변조 여부에 따른 검증을 요청하는 고객단말(400);로 이루어지고,
상기 인증관리서버(200)는 상기 전송되는 대비용 제증명서 노드해시정보 및 제증명서 트랜잭션 ID정보를 토대로 해당 제증명서 정보가 위변조 되었는지의 여부를 판단하고, 그 판단에 따른 고객제공용 제증명서 정보의 위변조 여부를 안내하는 고객요청 제증명서 검증정보를 생성하여 상기 고객단말(400)로 전송되도록 제어하는 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템.

[청구항 14] 제13항에 있어서,
상기 루트해시 생성구간은 기설정된 제증명서 노드해시정보의 개수이거나 또는 기설정된 시간동안 누적저장되는 제증명서 노드해시정보의 개수인 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템.

[청구항 15] 제13항에 있어서,
상기 인증관리서버(200)는 상기 제증명서 노드해시정보가 기설정된 루트해시 생성구간에 도달되면, 제증명서 위변조

감시관련정보 DB(212)에 누적저장된 제증명서 트랜잭션 ID정보를 모두 추출하고, 그 추출된 각각의 제증명서 트랜잭션 ID정보를 블록체인 보유서버(300)로 전송하고,
상기 블록체인 보유서버(300)는 전송된 각각의 제증명서 트랜잭션 ID정보를 전자지갑에 구비된 블록체인과 매칭하여, 매칭되는 각각의 제증명서 트랜잭션정보에 포함된 등록용 제증명서 루트해시정보를 상기 인증관리서버(200)로 전송하며,
상기 인증관리서버(200)는 전송된 각각의 등록용 제증명서 루트해시정보를 전송받고, 해시처리엔진(220)을 운영하여 제증명서 등록관련정보DB(211)에 누적저장된 제증명서 노드해시정보의 개수를 기설정된 루트해시 생성구간에 해당하는 개수로 구분하고, 그 구분된 기설정된 루트해시 생성구간에 해당하는 개수마다 해싱하여 각각의 대비용 제증명서 루트해시정보로 가공처리하며, 각각의 등록용 제증명서 루트해시정보와 각각의 대비용 제증명서 루트해시정보를 생성순번대로 양자대비하고, 생성순번대로 양자대비되는 각각의 등록용 제증명서 루트해시정보와 각각의 대비용 제증명서 루트해시정보의 해시값을 연산하여 첫 번째 생성순번부터 마지막 생성순번까지 그 연산된 양쪽의 해시값이 동일한지 여부를 확인하여, 상기 인증관리서버(200)에서 저장관리되고 있는 고객제공용 제증명서 정보의 위변조 여부를 검증하는 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템.

[청구항 16] 제13항에 있어서,
상기 인증관리서버(200)의 트랜잭션처리엔진(230)은 상기 등록용 제증명서 루트해시정보를 상기 제증명서 트랜잭션정보 중 비트코인의 거래 결제가 아닌 사적인 정보로서 취급되도록 안내하는 OP리턴(Operation Code RETURN) 영역에 삽입하여 전송되도록 제어하는 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템.

[청구항 17] 제16항에 있어서,
상기 각 블록체인 보유서버(300)에 탑재된 전자지갑은, 상기 전송된 제증명서 트랜잭션정보를 판독하여 OP리턴 영역에 정보가 삽입된 것을 인지하면, 비트코인 결제를 인증하는 과정을 생략하고, 바로 상기 블록체인에 기록되도록 제어하는 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템.

[청구항 18] 제13항에 있어서,

상기 고객요청 제증명서 검증정보 생성과정은,
상기 인증관리서버(200)에서, 상기 대비용 제증명서 노드해시정보 및 제증명서 트랜잭션 ID정보가 전송되면, 전송된 정보 중 제증명서 트랜잭션 ID정보를 상기 블록체인 보유서버(300)에게 전송하여, 제증명서 트랜잭션정보의 전송을 요청하고,
상기 블록체인 보유서버(300)의 전자지갑에서 상기 제증명서 트랜잭션 ID정보를 블록체인에 매칭하여 매칭되는 제증명서 트랜잭션정보를 상기 인증관리서버(200)로 전송하며,
상기 인증관리서버(200)에서, 해시처리엔진(210)을 운영하여 상기 블록체인 보유서버(300)로부터 전송된 제증명서 트랜잭션정보에 포함된 제증명서 검증용 인덱스 해시값과 상기 대비용 제증명서 노드해시정보값을 각각 연산하여, 양쪽의 해시값의 동일여부를 안내하는 고객요청 제증명서 검증정보로 생성되는 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증시스템.

[청구항 19] 금융기관단말(100)에서, 고객에게 제공되어지는 제증명서인 고객제공용 제증명서 정보가 생성되면, 해시처리엔진(120)을 운영하여 상기 고객제공용 제증명서 정보 및 해당 고객을 식별하는 고객식별정보를 해싱하여 제증명서 노드해시정보로 가공처리하고, 그 가공처리된 제증명서 노드해시정보를 인증관리서버(200)로 전송하여 고객제공용 제증명서 정보의 기록 인증을 요청하는 단계(S310)와;
상기 인증관리서버(200)에서, 전송된 제증명서 노드해시정보를 제증명서 등록관련정보 DB(211)에 누적저장하는 단계(S320)와;
상기 인증관리서버(200)에서, 상기 누적저장되는 제증명서 노드해시정보가 기설정된 루트해시 생성구간에 도달됐는지 확인하는 단계(S330)와;
상기 인증관리서버(200)에서, 상기 누적저장되는 제증명서 노드해시정보가 기설정된 루트해시 생성구간에 도달되면, 해시처리엔진(220)을 운영하여 상기 제증명서 등록관련정보DB(211)에서 기설정된 루트해시 생성구간에 해당하는 개수만큼 추출하고, 그 추출된 제증명서 노드해시정보들을 머클트리 구조로 이루어진 등록용 제증명서 루트해시정보로 가공처리하는 단계(S340)와;
상기 인증관리서버(200)에서, 트랜잭션처리엔진(230)을 운영하여 상기 등록용 제증명서 루트해시정보를 포함하는 제증명서 트랜잭션정보 및 그 제증명서 트랜잭션정보를 검색하는데 키값으로 이용되는 제증명서 트랜잭션 ID정보를 생성하고, 상기

생성된 정보 중 제증명서 트랜잭션정보를 블록체인 보유서버(300)들로 전송하는 단계(S350)와;
상기 블록체인 보유서버(300)들에서, 상기 전송되는 제증명서 트랜잭션정보를 블록체인에 기록하여 기록 인증을 수행하는 단계(S360)와;
상기 인증관리서버(200)의 트랜잭션처리엔진(230)에서, 상기 제증명서 트랜잭션 ID정보를 상기 금융기관단말(100)로 전송하는 단계(S370)와;
상기 금융기관단말(100)에서, 상기 전송되는 제증명서 트랜잭션 ID정보를 저장관리하는 단계(S380)와;
고객단말(400)에서, 상기 금융기관단말(100)로 고객제공용 제증명서 정보의 다운로드를 요청하는 단계(S390)와;
상기 금융기관단말(100)에서, 그 다운로드 요청된 고객제공용 제증명서 정보 및 해당 고객제공용 제증명서 정보 에 대응되는 제증명서 트랜잭션 ID정보를 고객단말(400)로 전송하는 단계(S400)와;
상기 고객단말(400)에서, 해시처리엔진을 운영하여 전송된 고객제공용 제증명서 정보 및 제증명서 트랜잭션 ID정보 중 고객제공용 제증명서 정보와 해당 고객을 식별하는 고객식별정보를 해싱하여 대비용 제증명서 노드해시정보로 가공처리하고, 그 가공처리된 대비용 제증명서 노드해시정보와 상기 제증명서 트랜잭션 ID정보를 상기 인증관리서버(200)로 전송하여 상기 고객제공용 제증명서 정보의 위변조 여부에 따른 검증을 요청하는 단계(S410)와;
상기 인증관리서버(200)에서, 상기 전송되는 대비용 제증명서 노드해시정보 및 제증명서 트랜잭션 ID정보를 토대로 해당 제증명서 정보가 위변조 되었는지의 여부를 판단하고, 그 판단에 따른 고객제공용 제증명서 정보의 위변조 여부를 안내하는 고객요청 제증명서 검증정보를 생성하여 상기 고객단말(400)로 전송하는 단계(S420)와;
상기 고객단말(400)에서, 상기 전송된 고객요청 제증명서 검증정보를 열람하는 단계(S430);로 이루어진 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증방법.

[청구항 20] 제19항에 있어서,
상기 루트해시 생성구간은 기설정된 제증명서 노드해시정보의 개수이거나 또는 기설정된 시간동안 누적저장되는 제증명서 노드해시정보의 개수인 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증방법.

[청구항 21] 제19항에 있어서,
상기 인증관리서버(200)에서, 상기 누적저장되는 제증명서 노드해시정보가 기설정된 루트해시 생성구간에 도달됐는지 확인하는 S330단계에 있어서,
상기 인증관리서버(200)에서, 제증명서 노드해시정보가 기설정된 루트해시 생성구간에 도달된 경우 제증명서 위변조 감시관련정보 DB(212)에 누적저장된 제증명서 트랜잭션 ID정보를 모두 추출하고, 그 추출된 각각의 제증명서 트랜잭션 ID정보를 블록체인 보유서버(300)로 전송하는 단계(S331)와;
상기 블록체인 보유서버(300)에서 전송된 각각의 제증명서 트랜잭션 ID정보를 전자지갑에 구비된 블록체인과 매칭하여, 매칭되는 각각의 제증명서 트랜잭션정보에 포함된 등록용 제증명서 루트해시정보를 추출하는 단계(S332)와;
상기 블록체인 보유서버(300)에서 각각의 등록용 제증명서 루트해시정보를 상기 인증관리서버(200)로 전송하는 단계(S333)와;
상기 인증관리서버(200)에서, 전송된 각각의 등록용 제증명서 루트해시정보를 전송받고, 해시처리엔진(220)을 운영하여 제증명서 등록관련정보DB(211)에 누적저장된 제증명서 노드해시정보의 개수를 기설정된 루트해시 생성구간에 해당하는 개수로 구분하고, 그 구분된 기설정된 루트해시 생성구간에 해당하는 개수마다 해싱하여 각각의 대비용 제증명서 루트해시정보로 가공처리하는 단계(S334)와;
상기 인증관리서버(200)의 해시처리엔진(220)에서, 각각의 등록용 제증명서 루트해시정보와 각각의 대비용 제증명서 루트해시정보를 생성순번대로 양자대비하고, 생성순번대로 양자대비되는 각각의 등록용 제증명서 루트해시정보와 각각의 대비용 제증명서 루트해시정보의 해시값을 연산하여 첫 번째 생성순번부터 마지막 생성순번까지 그 연산된 양쪽의 해시값이 동일한지 여부를 확인하여, 상기 인증관리서버(200)에서 저장관리되고 있는 고객제공용 제증명서 정보의 위변조 여부를 검증하는 단계(S335);를 포함하는 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증방법.

[청구항 22] 제19항에 있어서,
상기 인증관리서버(200)에서, 트랜잭션처리엔진(230)을 운영하여 상기 등록용 제증명서 루트해시정보를 포함하는 제증명서 트랜잭션정보 및 그 제증명서 트랜잭션정보를 검색하는데 키값으로 이용되는 제증명서 트랜잭션 ID정보를 생성하고, 상기

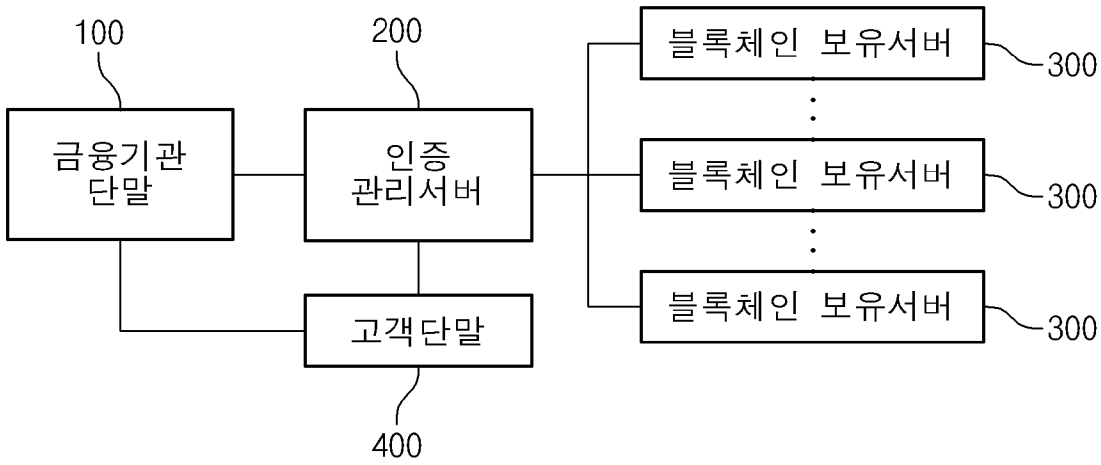
생성된 정보 중 제증명서 트랜잭션정보를 블록체인 보유서버(300)들로 전송하는 S350단계에 있어서,
상기 트랜잭션처리엔진(230)은, 상기 등록용 제증명서 루트해시정보를 상기 제증명서 트랜잭션정보 중 비트코인의 거래 결제가 아닌 사적인 정보로서 취급되도록 안내하는 OP리턴(Operation Code RETURN) 영역에 삽입하여 전송되도록 제어하는 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증방법.

[청구항 23] 제22항에 있어서,
상기 블록체인 보유서버(300)들에서, 상기 전송되는 제증명서 트랜잭션정보를 블록체인에 기록하여 기록 인증을 수행하는 S360단계에 있어서,
상기 각 블록체인 보유서버(300)에 탑재된 전자지갑은, 상기 전송된 제증명서 트랜잭션정보를 판독하여 OP리턴 영역에 정보가 삽입된 것을 인지하면, 비트코인 결제를 인증하는 과정을 생략하고, 바로 상기 블록체인에 기록되도록 제어하는 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증방법.

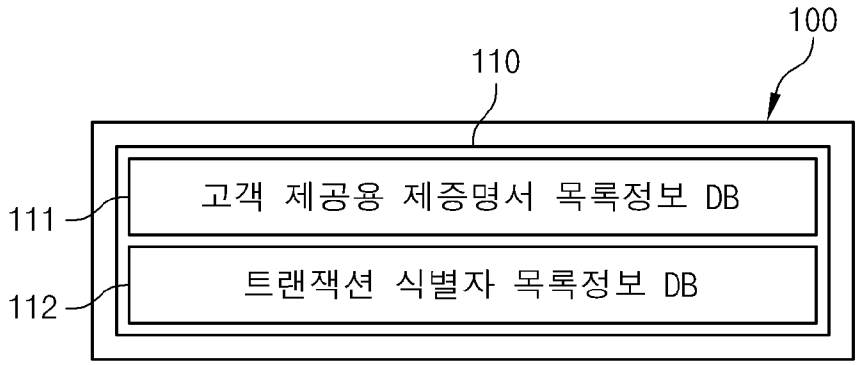
[청구항 24] 제19항에 있어서,
상기 인증관리서버(200)에서, 상기 전송되는 대비용 제증명서 노드해시정보 및 제증명서 트랜잭션 ID정보를 토대로 해당 제증명서 정보가 위변조 되었는지의 여부를 판단하고, 그 판단에 따른 고객제공용 제증명서 정보의 위변조 여부를 안내하는 고객요청 제증명서 검증정보를 생성하여 상기 고객단말(400)로 전송하는 S420단계에 있어서,
상기 고객요청 제증명서 검증정보 생성과정은,
상기 인증관리서버(200)에서, 상기 대비용 제증명서 노드해시정보 및 제증명서 트랜잭션 ID정보가 전송되면, 전송된 정보 중 제증명서 트랜잭션 ID정보를 상기 블록체인 보유서버(300)에게 전송하여, 제증명서 트랜잭션정보의 전송을 요청하는 단계(S421)와;
상기 블록체인 보유서버(300)의 전자지갑에서 상기 제증명서 트랜잭션 ID정보를 블록체인에 매칭하여 매칭되는 제증명서 트랜잭션정보를 상기 인증관리서버(200)로 전송하는 단계(S422)와;
상기 인증관리서버(200)에서, 해시처리엔진(210)을 운영하여 상기 블록체인 보유서버(300)로부터 전송된 제증명서 트랜잭션정보에 포함된 제증명서 검증용 인덱스 해시값과 상기 대비용 제증명서

노드해시정보값을 각각 연산하여, 양쪽의 해시값의 동일여부를 안내하는 고객요청 제증명서 검증정보를 생성하는 단계(S423);로 이루어진 것을 특징으로 하는 블록체인을 기반으로 하는 금융기관 제증명서류 위변조 검증방법.

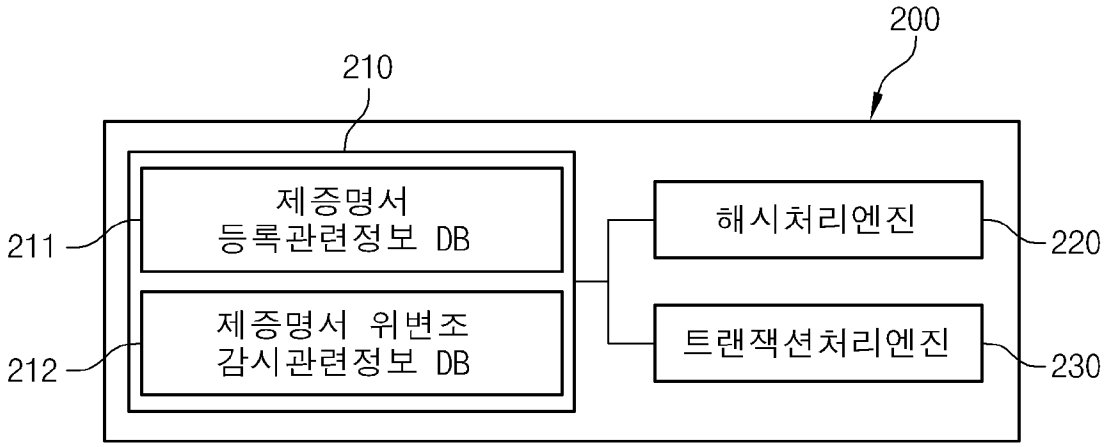
[Fig. 1]



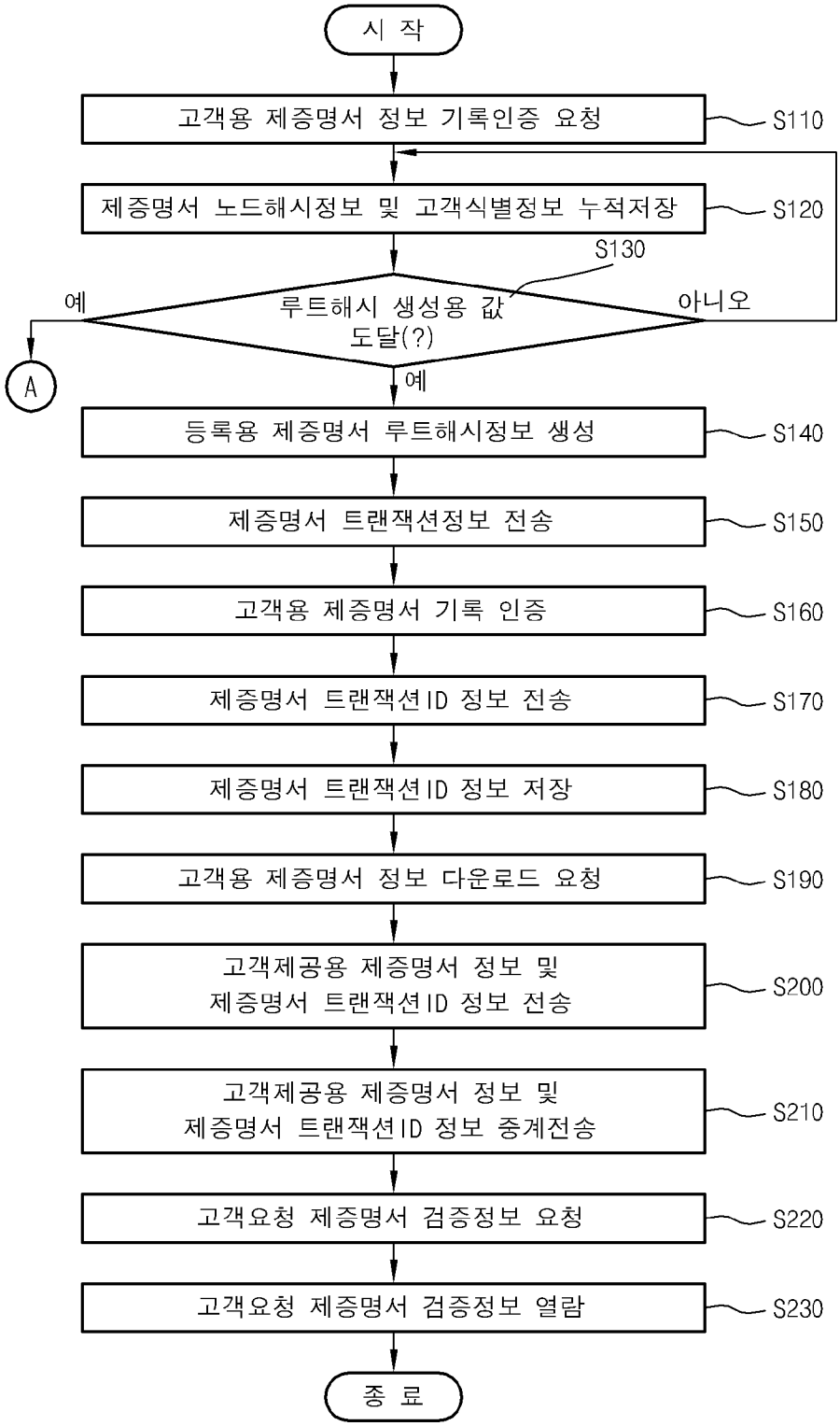
[Fig. 2]



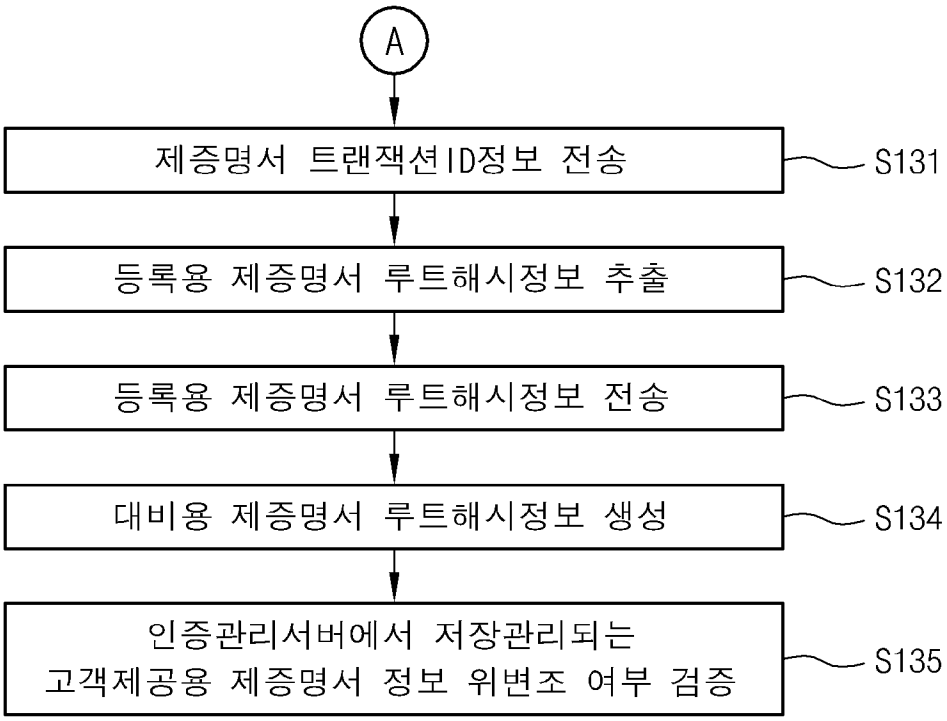
[Fig. 3]



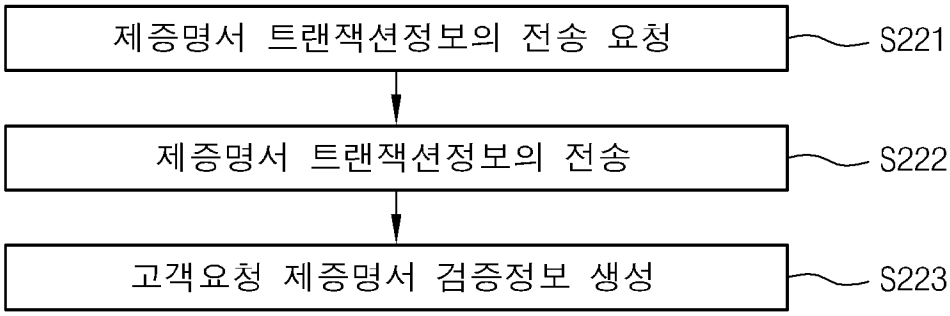
[Fig. 4]


시 작
고객용 제증명서 정보 기록인증 요청
S110
제증명서 노드해시정보 및 고객식별정보 누적저장
S120
S130
루트해시 생성용 값 도달(?)
예
아니오
A
예
등록용 제증명서 루트해시정보 생성
S140
제증명서 트랜잭션정보 전송
S150
고객용 제증명서 기록 인증
S160
제증명서 트랜잭션ID 정보 전송
S170
제증명서 트랜잭션ID 정보 저장
S180
고객용 제증명서 정보 다운로드 요청
S190
고객제공용 제증명서 정보 및
제증명서 트랜잭션ID 정보 전송
S200
고객제공용 제증명서 정보 및
제증명서 트랜잭션ID 정보 중계전송
S210
고객요청 제증명서 검증정보 요청
S220
고객요청 제증명서 검증정보 열람
S230
종 료

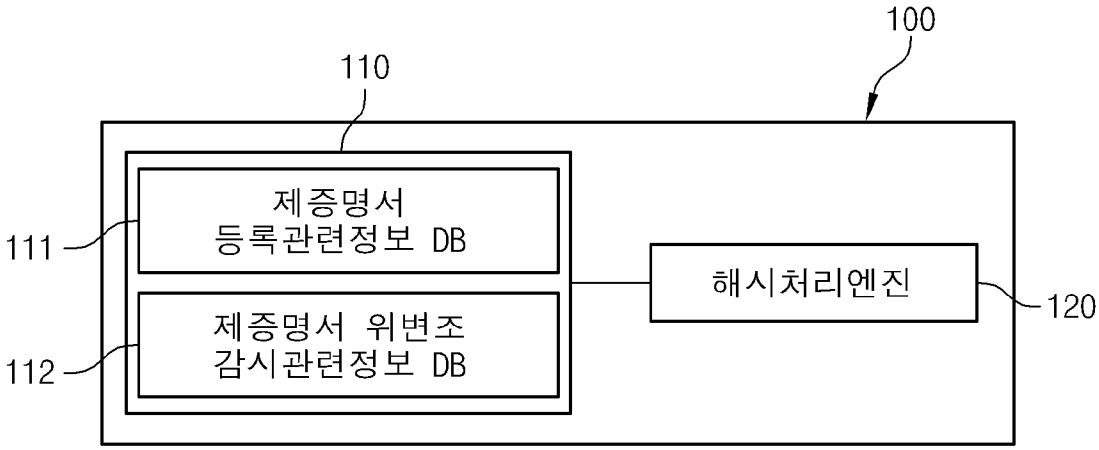
[Fig. 5]



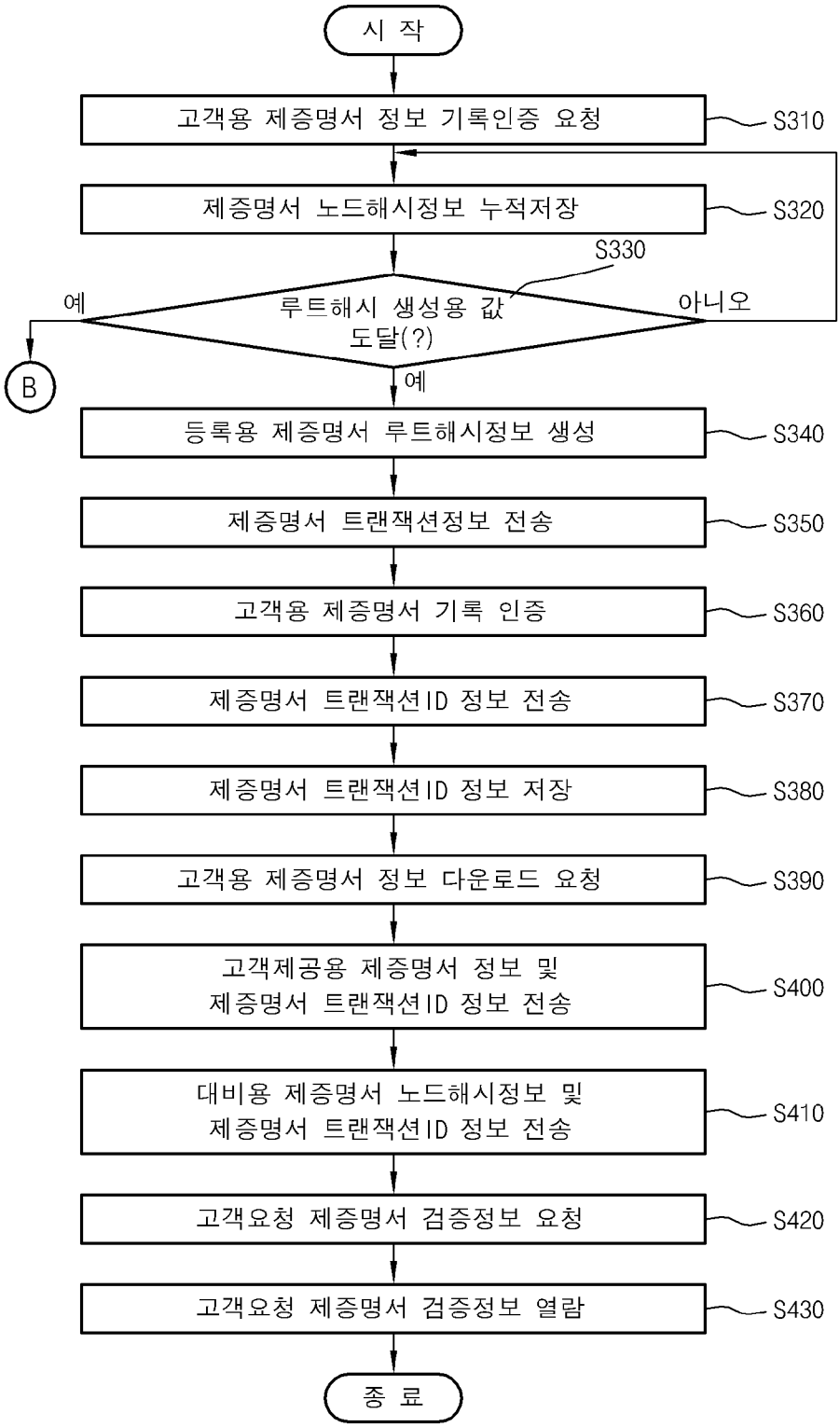
[Fig. 6]



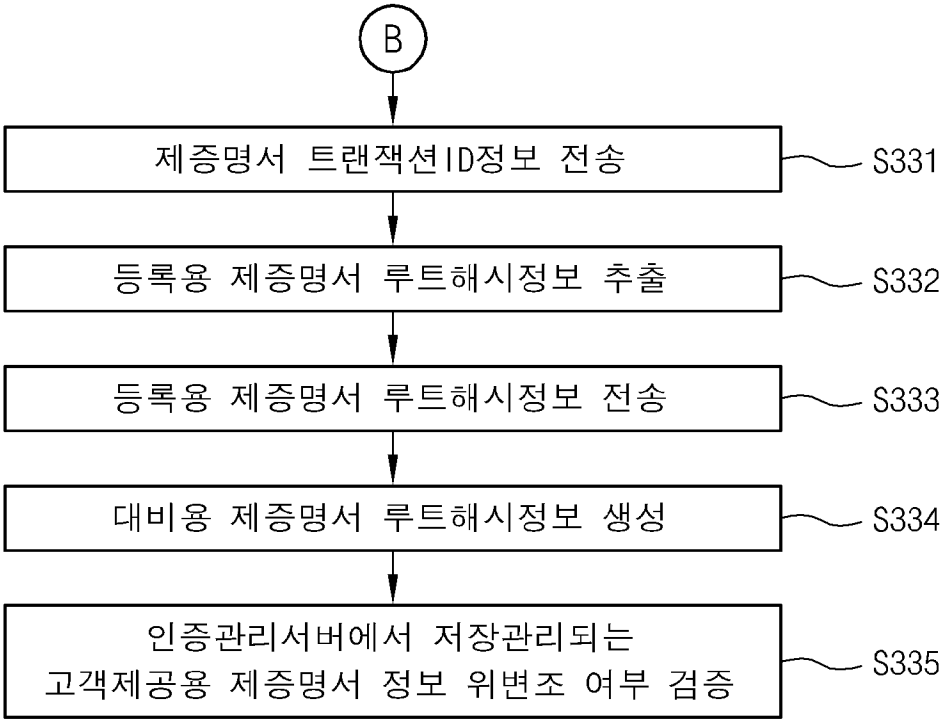
[Fig. 7]



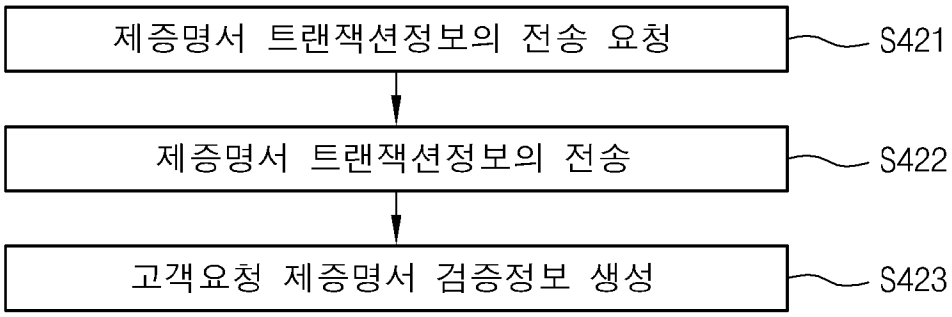
[Fig. 8]


시 작
고객용 제증명서 정보 기록인증 요청
S310
제증명서 노드해시정보 누적저장
S320
S330
루트해시 생성용 값 도달(?)
예
아니오
B
예
등록용 제증명서 루트해시정보 생성
S340
제증명서 트랜잭션정보 전송
S350
고객용 제증명서 기록 인증
S360
제증명서 트랜잭션ID 정보 전송
S370
제증명서 트랜잭션ID 정보 저장
S380
고객용 제증명서 정보 다운로드 요청
S390
고객제공용 제증명서 정보 및
제증명서 트랜잭션ID 정보 전송
S400
대비용 제증명서 노드해시정보 및
제증명서 트랜잭션ID 정보 전송
S410
고객요청 제증명서 검증정보 요청
S420
고객요청 제증명서 검증정보 열람
S430
종 료

[Fig. 9]


B
제증명서 트랜잭션ID정보 전송
S331
등록용 제증명서 루트해시정보 추출
S332
등록용 제증명서 루트해시정보 전송
S333
대비용 제증명서 루트해시정보 생성
S334
인증관리서버에서 저장관리되는
고객제공용 제증명서 정보 위변조 여부 검증
S335

[Fig. 10]


제증명서 트랜잭션정보의 전송 요청
S421
제증명서 트랜잭션정보의 전송
S422
고객요청 제증명서 검증정보 생성
S423

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2016/011288

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 40/02(2012.01)i, H04L 9/06(2006.01)i, H04L 9/32(2006.01)i, G06Q 20/38(2012.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q 40/02; G06F 21/62; G06F 17/40; H04L 9/06; H04L 9/32; G06Q 20/38

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: certificate, root hash, note hash, merkle tree, bitcoin, block chain, forgery, verification

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	AHN, Sang Uk, "[Fintech in Blockchain] 2. P2P Financial Innovation", BLOTER.NET [Online], 17 June 2015 [Searching Date: 15 December 2016]. Internet Search: <URL: http://www.bloter.net/archives/230365> See page 3.	1-24
A	Reporter SON, Kyung Ho, "All documents, Authentication with 'BlockChain'", ZdNetKorea [Online], 17 November 2015, [Searching Date: 15 December 2016], Internet Search: <URL: http://www.zdnet.co.kr/news/news_view.asp?artice_id=20151116185432&type=det&re=> See pages 1-2.	1-24
A	LEE, Seong Bok, "Description of Personal Cryptocurrency System of Bitcoin", SlideShare [Online], 21 May 2015, [Searching Date: 15 December 2016], Internet Search: <URL: http://www.slideshare.net/SeongBokLee/ss-48425470> See page 5.	1-24
A	AHN, Sang Uk, "Bitcoin Technology, Used for Issuing Certificate", BLOTER.NET [Online], 19 September 2014, [Searching Date: 15 December 2016], Internet Search: <URL: http://www.bloter.net/archives/207040> See page 2.	1-24
A	KR 10-1149695 B1 (JACOBS CO., LTD.) 23 May 2012 See abstract, claims 1, 4-6 and figures 1, 3-4.	1-24

☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 JANUARY 2017 (09.01.2017)	**10 JANUARY 2017 (10.01.2017)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. +82-42-481-8578	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2016/011288

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2012-0074817 A (IUCF-HYU (INDUSTRY-UNIVERSITY COOPERATION FOUNDATION HANYANG UNIVERSITY)) 06 July 2012 See abstract, claims 1-4 and figures 1, 5.	1-24

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2016/011288

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-1149695 B1	23/05/2012	NONE	
KR 10-2012-0074817 A	06/07/2012	KR 10-1252375 B1	08/04/2013

국제조사보고서

국제출원번호
PCT/KR2016/011288

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06Q 40/02(2012.01)i, H04L 9/06(2006.01)i, H04L 9/32(2006.01)i, G06Q 20/38(2012.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
G06Q 40/02; G06F 21/62; G06F 17/40; H04L 9/06; H04L 9/32; G06Q 20/38

조사된 기술분야에 속하는 최소문헌 이외의 문헌
한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드: 제증명서, 루트해시, 노트해시, 머클트리, 비트코인, 블록체인, 위변조, 검증

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	안상욱. '[블록체인 속 핀테크] ②P2P 금융혁신'. BLOTER.NET [온라인]. 2015.06.17. [검색일: 2016.12.15]. 인터넷 검색: <URL: http://www.bloter.net/archives/230365> 페이지 3 참조.	1-24
A	손경호 기자. '각종 전자문서, '블록체인'으로 공증한다'. ZdNetKorea [온라인]. 2015.11.17. [검색일: 2016.12.15]. 인터넷 검색: <URL: http://www.zdnet.co.kr/news/news_view.asp?artice_id=20151116185432&type=det&re=> 페이지 1-2 참조.	1-24
A	이성복. '비트코인 개인간 전자화폐시스템 요약 설명'. SlideShare [온라인]. 2015.05.21. [검색일: 2016.12.15]. 인터넷 검색: <URL: http://www.slideshare.net/SeongBokLee/ss-48425470> 페이지 5 참조.	1-24
A	안상욱. '비트코인 기술, 증명서 발급에도 쓰인다'. BLOTER.NET [온라인]. 2014.09.19. [검색일: 2016.12.15]. 인터넷 검색: <URL: http://www.bloter.net/archives/207040> 페이지 2 참조.	1-24
A	KR 10-1149695 B1 (제이콥스 주식회사) 2012.05.23 요약, 청구항 1,4-6 및 도면 1,3-4 참조.	1-24

☒ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2017년 01월 09일 (09.01.2017)	2017년 01월 10일 (10.01.2017)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-481-8578

심사관
이은규
전화번호 +82-42-481-3580

국제조사보고서

국제출원번호
PCT/KR2016/011288

C (계속). 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2012-0074817 A (한양대학교 산학협력단) 2012.07.06 요약, 청구항 1-4 및 도면 1,5 참조.	1-24

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2016/011288

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-1149695 B1	2012/05/23	없음	
KR 10-2012-0074817 A	2012/07/06	KR 10-1252375 B1	2013/04/08