



(19) 대한민국 지식재산청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2025년10월14일
(11) 등록번호 10-2869666
(24) 등록일자 2025년10월01일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) H04L 67/1097 (2022.01)
H04L 9/00 (2022.01) H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 9/3226 (2013.01)
H04L 67/1097 (2022.05)
(21) 출원번호 10-2025-0034578
(22) 출원일자 2025년03월18일
심사청구일자 2025년03월18일
(56) 선행기술조사문헌
KR101284353 B1*
(뒷면에 계속)

(73) 특허권자
김보미
제주특별자치도 서귀포시
(72) 발명자
이상엽
서울특별시 중랑구 신내로 51, 101동 2112호 (신내동, 성원아파트)
(74) 대리인
특허법인테헤란

전체 청구항 수 : 총 6 항

심사관 : 양종필

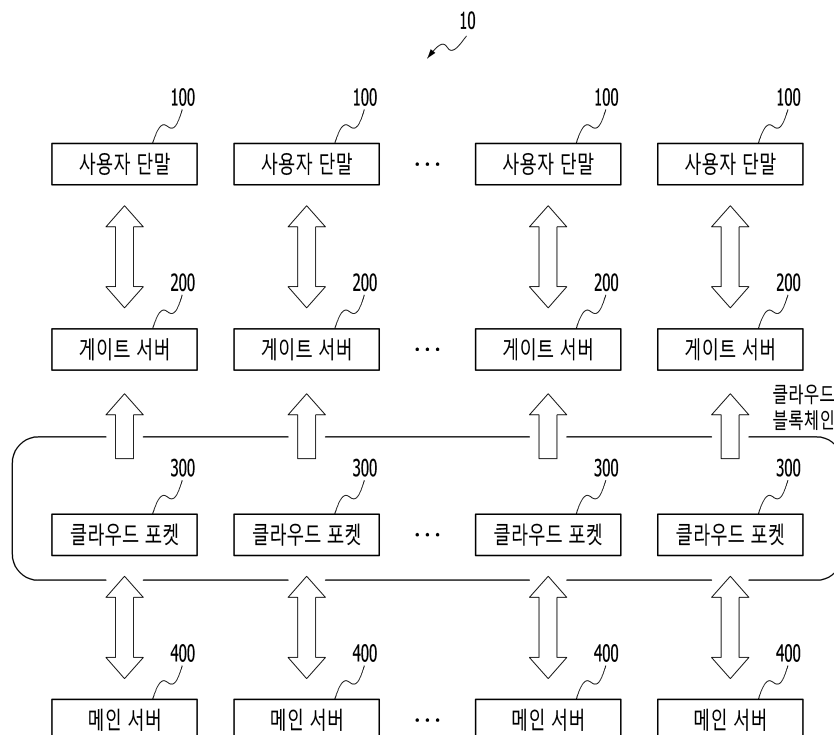
(54) 발명의 명칭 클라우드 블록체인 시스템 및 그의 제어 방법

(57) 요약

본 발명은 클라우드 블록체인 시스템 및 그의 제어 방법을 개시한다. 즉, 본 발명은 사용자 단말에서 원본 데이터를 인증키를 이용해서 암호화하여 암호 블록을 생성하고, 암호 블록과 타임스탬프를 포함하는 요구 정보를 게이트 서버에 등록하고, 클라우드 포켓에서 게이트 서버에 접속하여 요구 정보를 확인한 후, 요구 정보에 포함된

(뒷면에 계속)

대표도 - 도1



암호 블록을 복호하여 원본 데이터를 복원하고, 블록체인에 새로운 블록으로 해당 원본 데이터를 저장하거나, 기존 데이터를 해당 원본 데이터로 수정함으로써, 블록체인을 개인 PC나 디바이스에 구성하는 것이 아니라, 네트워크에 연결되어 있는 클라우드 포켓에 구성함에 따라 개인 디바이스에는 아무 정보도 보관하지 않고, 사용자와 클라우드 포켓 간에 연결하는 암호화 블록 프로토콜만 존재하는 상태에서, 수많은 클라우드 포켓들이 서로 네트워크상에 PtoP로 연결되어 실시간 처리를 통해 화폐의 기능이 가능하며, 실시간 수정, 송신, 생성할 수 있고, 통화량 제어가 가능하고, 가상화폐의 흐름을 추적할 수 있다.

(52) CPC특허분류

H04L 9/0872 (2013.01)

H04L 9/0894 (2013.01)

H04L 9/50 (2022.05)

(56) 선행기술조사문헌

KR1020150107796 A*

KR102062688 B1*

KR102307863 B1*

KR102461050 B1*

*는 심사관에 의하여 인용된 문헌

명세서

청구범위

청구항 1

사용자 단말과 클라우드 포켓을 중계하는 게이트 서버;

클라우드 포켓으로부터 인증키를 발급받기 위해서, 복수의 게이트 서버 중 어느 하나의 특정 게이트 서버에 접속하고, 상기 접속된 특정 게이트 서버 내의 복수의 테이블 중 어느 하나의 테이블에 웹 서버로부터 제공되는 인증용 블록을 등록하고, 상기 등록된 인증용 블록에 대응하는 인증키 블록을 제공받는 상기 사용자 단말; 및

미리 설정된 주기로 상기 특정 게이트 서버에 접속한 후, 상기 특정 게이트 서버 내의 복수의 테이블에 데이터가 등록된 상태인지 여부를 확인하고, 상기 복수의 테이블 중 적어도 하나의 테이블에 데이터가 등록된 상태일 때 상기 테이블에 등록된 데이터를 확인하고, 상기 테이블에 등록된 데이터가 인증용 블록일 때, 상기 특정 게이트 서버와 연동하여, 상기 웹 서버에서 상기 특정 게이트 서버에 등록한 인증용 블록과, 상기 사용자 단말에서 상기 특정 게이트 서버에 등록한 인증용 블록이 일치하는지 여부를 비교하고, 상기 비교 결과 일치할 때, 상기 인증용 블록에 포함된 아이디 및 비밀번호를 확인하고, 상기 확인된 아이디, 비밀번호, 현재 시각과 미리 설정된 유효 기간을 근거로 인증키를 생성하고, 열람 계정키와 수정 계정키와 연산기로 구성된 사용자 계정 암호/복호키를 생성하고, 상기 생성된 인증키와 상기 생성된 사용자 계정 암호/복호키를 포함하는 인증키 블록을 상기 특정 게이트 서버의 테이블에 등록하는 상기 클라우드 포켓을 포함하며,

상기 사용자 단말은,

상기 웹 서버로 아이디 및 비밀번호를 이용해서 로그인하고,

상기 웹 서버는,

상기 사용자 단말의 인증용 블록 생성 요청을 근거로 상기 아이디 및 비밀번호로 구성된 인증용 블록을 생성하고, 상기 생성된 인증용 블록을 상기 사용자 단말에 전송하고, 상기 생성된 인증용 블록을 상기 웹 서버와 연동하는 상기 특정 게이트 서버에 등록하며,

상기 사용자 단말은,

상기 인증용 블록 생성 요청에 응답하여 상기 웹 서버로부터 전송되는 인증용 블록을 수신하며,

상기 클라우드 포켓과 상기 특정 게이트 서버 간의 연결은,

상기 클라우드 포켓에서만 상기 특정 게이트 서버로 접속하는 단방향 통신인 것을 특징으로 하는 클라우드 블록체인 시스템.

청구항 2

삭제

청구항 3

사용자 단말에 의해, 클라우드 포켓으로부터 인증키를 발급받기 위해서, 복수의 게이트 서버 중 어느 하나의 특정 게이트 서버에 접속하는 단계;

상기 사용자 단말에 의해, 상기 접속된 특정 게이트 서버 내의 복수의 테이블 중 어느 하나의 테이블에 웹 서버로부터 제공되는 인증용 블록을 등록하는 단계;

클라우드 포켓에 의해, 미리 설정된 주기로 상기 특정 게이트 서버에 접속한 후, 상기 특정 게이트 서버 내의 복수의 테이블에 데이터가 등록된 상태인지 여부를 확인하는 단계;

상기 확인 결과, 상기 복수의 테이블 중 적어도 하나의 테이블에 데이터가 등록된 상태일 때, 상기 클라우드 포켓에 의해, 상기 테이블에 등록된 데이터를 확인하는 단계;

상기 확인 결과, 상기 테이블에 등록된 데이터가 인증용 블록일 때, 상기 클라우드 포켓에 의해, 상기 특정 게

이트 서버와 연동하여, 상기 웹 서버에서 상기 특정 게이트 서버에 등록된 인증용 블록과, 상기 사용자 단말에서 상기 특정 게이트 서버에 등록된 인증용 블록이 일치하는지 여부를 비교하는 단계;

상기 비교 결과, 상기 웹 서버에서 상기 특정 게이트 서버에 등록된 인증용 블록과, 상기 사용자 단말에서 상기 특정 게이트 서버에 등록된 인증용 블록이 일치할 때, 상기 클라우드 포켓에 의해, 상기 인증용 블록에 포함된 아이디 및 비밀번호를 확인하고, 상기 확인된 아이디, 비밀번호, 현재 시각과 미리 설정된 유효 기간을 근거로 인증키를 생성하는 단계;

상기 클라우드 포켓에 의해, 암호화된 데이터를 해석하고자 할 때 사용하기 위한 미리 설정된 크기의 열람 계정키와, 데이터를 암호화하고자 할 때 사용하기 위한 미리 설정된 크기의 수정 계정키와, 연산부호화 방식을 사용하여 패턴으로 해석이 불가능하게 하기 위한 미리 설정된 크기의 연산키로 구성된 사용자 계정 암호/복호키를 생성하는 단계;

상기 클라우드 포켓에 의해, 상기 생성된 인증키와 상기 생성된 사용자 계정 암호/복호키를 포함하는 인증키 블록을 상기 특정 게이트 서버의 테이블에 등록하는 단계; 및

상기 사용자 단말에 의해, 상기 특정 게이트 서버의 테이블에 등록된 인증키 블록을 확인하는 단계를 포함하며, 상기 사용자 단말은,

상기 웹 서버로 아이디 및 비밀번호를 이용해서 로그인하고,

상기 웹 서버는,

상기 사용자 단말의 인증용 블록 생성 요청을 근거로 상기 아이디 및 비밀번호로 구성된 인증용 블록을 생성하고, 상기 생성된 인증용 블록을 상기 사용자 단말에 전송하고, 상기 생성된 인증용 블록을 상기 웹 서버와 연동하는 상기 특정 게이트 서버에 등록하며,

상기 사용자 단말은,

상기 인증용 블록 생성 요청에 응답하여 상기 웹 서버로부터 전송되는 인증용 블록을 수신하며,

상기 클라우드 포켓과 상기 특정 게이트 서버 간의 연결은,

상기 클라우드 포켓에서만 상기 특정 게이트 서버로 접속하는 단방향 통신인 것을 특징으로 하는 클라우드 블록체인 시스템의 제어 방법.

청구항 4

제 3 항에 있어서,

상기 사용자 단말에 의해, 상기 클라우드 포켓에서 관리하는 클라우드 블록체인에 데이터를 저장하거나 또는 상기 클라우드 블록체인에 등록된 데이터를 조회하기 위해서, 클라우드 블록체인에 등록하고자 하는 원본 데이터를 상기 인증키 블록에 포함된 사용자 계정 암호/복호키를 이용해서 암호화하여, 암호 블록을 생성하는 단계;

상기 사용자 단말에 의해, 상기 생성된 암호 블록 및 상기 인증키 블록에 포함된 인증키를 포함하는 요구문을 생성하는 단계;

상기 사용자 단말에 의해, 상기 특정 게이트 서버에 접속하는 단계;

상기 사용자 단말에 의해, 상기 접속된 특정 게이트 서버 내의 복수의 테이블 중 어느 하나의 테이블에 상기 생성된 요구문을 등록하는 단계;

상기 클라우드 포켓에 의해, 상기 미리 설정된 주기로 상기 특정 게이트 서버에 접속한 후, 상기 특정 게이트 서버 내의 복수의 테이블에 데이터가 등록된 상태인지 여부를 확인하는 단계;

상기 확인 결과, 상기 복수의 테이블 중 적어도 하나의 테이블에 데이터가 등록된 상태일 때, 상기 클라우드 포켓에 의해, 상기 테이블에 등록된 데이터를 확인하는 단계;

상기 확인 결과, 상기 테이블에 등록된 데이터가 요구문일 때, 상기 클라우드 포켓에 의해, 상기 요구문에 대해 검증 기능을 수행하는 단계; 및

상기 클라우드 포켓에 의해, 상기 요구문에 대한 검증이 정상적으로 완료될 때, 상기 요구문으로부터 복호한 원

본 데이터를 근거로 클라우드 블록체인에서 블록 생성 기능, 블록 수정 기능 및 블록 조회 기능 중 어느 하나의 기능을 수행하는 단계를 더 포함하는 것을 특징으로 하는 클라우드 블록체인 시스템의 제어 방법.

청구항 5

제 4 항에 있어서,

상기 요구문에 대해 검증 기능을 수행하는 단계는,

상기 클라우드 포켓에 의해, 상기 데이터의 유효성을 검증하기 위해서, 현재 시각과 상기 요구문에 포함된 타임스탬프 간의 시간 차이가 미리 설정된 기준값을 지난 상태인지 여부를 검증하는 과정;

상기 요구문의 유효성 검증 결과, 상기 요구문이 유효하지 않은 것으로 판단될 때, 상기 클라우드 포켓에 의해, 해당 데이터의 유효성 검증이 실패한 상태를 나타내는 정보를 상기 특정 게이트 서버의 테이블에 등록하고, 상기 특정 게이트 서버와의 연결을 종료하는 과정;

상기 요구문의 유효성 검증 결과, 상기 요구문이 유효한 것으로 판단될 때, 상기 클라우드 포켓에 의해, 상기 요구문에 포함된 헤더값이 미리 설정된 규격을 충족하는지 여부를 확인하는 과정; 및

상기 확인 결과, 상기 요구문에 포함된 헤더값이 상기 규격을 충족할 때, 상기 요구문에 포함된 암호 블록을 상기 인증용 블록을 근거로 생성된 사용자 계정 암호/복호키를 이용해서 복호하여, 원본 데이터를 생성하는 과정을 포함하는 것을 특징으로 하는 클라우드 블록체인 시스템의 제어 방법.

청구항 6

제 4 항에 있어서,

상기 클라우드 포켓에 의해, 상기 미리 설정된 주기로 상기 특정 게이트 서버에 접속한 후, 상기 요구문에 대응하는 기능 수행 결과를 상기 특정 게이트 서버의 테이블에 등록하는 단계; 및

상기 사용자 단말에 의해, 상기 특정 게이트 서버의 테이블에 등록된 기능 수행 결과를 확인하는 단계를 더 포함하는 것을 특징으로 하는 클라우드 블록체인 시스템의 제어 방법.

청구항 7

제 4 항에 있어서,

상기 클라우드 포켓에 의해, 복수의 메인 서버 중에서 어느 하나의 특정 메인 서버와 연결하고, 상기 연결된 특정 메인 서버 내의 데이터베이스 내의 특정 테이블에 상기 요구문에 대응하는 기능 수행 결과를 저장하는 단계;

상기 특정 메인 서버에 의해, 상기 특정 테이블에 대응하는 특정 사서함 번호를 상기 클라우드 포켓에 전송하는 단계;

상기 특정 메인 서버에 의해, 상기 복수의 메인 서버 중에서 상기 특정 메인 서버를 제외한 나머지 메인 서버와 각각 연동하여, 상기 요구문에 대응하는 기능 수행 결과를 상기 나머지 메인 서버의 데이터베이스에 각각 등록하는 단계;

상기 클라우드 포켓에 의해, 상기 특정 메인 서버로부터 전송되는 상기 특정 테이블에 대응하는 특정 사서함 번호를 수신하는 단계;

상기 클라우드 포켓에 의해, 상기 미리 설정된 주기로 상기 특정 게이트 서버에 접속한 후, 상기 특정 사서함 번호를 상기 특정 게이트 서버의 테이블에 등록하는 단계; 및

상기 사용자 단말에 의해, 상기 특정 게이트 서버의 테이블에 등록된 특정 사서함 번호를 확인하는 단계를 더 포함하는 것을 특징으로 하는 클라우드 블록체인 시스템의 제어 방법.

발명의 설명

기술 분야

[0001]

본 발명은 클라우드 블록체인 시스템 및 그의 제어 방법에 관한 것으로서, 특히 사용자 단말에서 원본 데이터를 인증키를 이용해서 암호화하여 암호 블록을 생성하고, 암호 블록과 타임스탬프를 포함하는 요구 정보를 게이트

서버에 등록하고, 클라우드 포켓에서 게이트 서버에 접속하여 요구 정보를 확인한 후, 요구 정보에 포함된 암호 블록을 복호하여 원본 데이터를 복원하고, 블록체인에 새로운 블록으로 해당 원본 데이터를 저장하거나, 기존 데이터를 해당 원본 데이터로 수정하는 클라우드 블록체인 시스템 및 그의 제어 방법에 관한 것이다.

배경 기술

- [0002] 블록체인(blockchain)은 블록에 데이터를 담아 체인 형태로 연결, 수많은 컴퓨터에 동시에 이를 복제해 저장하는 분산형 데이터 저장 기술로 공공 거래 장부라고도 부른다.
- [0003] 이러한 블록체인 기술은 보안에 탁월하며, 데이터의 안정성 및 유실이 불가능하고 허가 없는 수정 등이 불가능하기에 보안에 좋은 장점이 있다.
- [0004] 이런 장점때문에 가상화폐에 블록체인을 사용하고, 이 블록체인이 PtoP로 연결되고 있지만, 코인이 생성되고 코인을 송신할 때 시간의 지연이 발생된다. 또한, 코인이 생성되고 키가 만들어지면 열람키와 데이터를 PtoP로 연결된 모든 디바이스에 전달해야 하며, 이때 시간 지연이 발생하는데 짧게는 30분에서 길게는 2시간 이상이 소요된다. 이러한 시간 지연은 물리적으로 소요되는 시간이기때문에 블록체인 기반의 코인들은 이 지연 시간을 줄일 수 있으나 없애기는 힘들며, 이로 인해 화폐의 기능으로 보면 관리가 어려운 점이 존재하고 있다.

선행기술문헌

특허문헌

- [0005] (특허문헌 0001) 한국등록특허 제10-1727525호 [제목: 블록체인 기반 분산 저장 방법 및 이를 이용한 장치]

발명의 내용

해결하려는 과제

- [0006] 본 발명의 목적은 사용자 단말에서 원본 데이터를 인증키를 이용해서 암호화하여 암호 블록을 생성하고, 암호 블록과 타임스탬프를 포함하는 요구 정보를 게이트 서버에 등록하고, 클라우드 포켓에서 게이트 서버에 접속하여 요구 정보를 확인한 후, 요구 정보에 포함된 암호 블록을 복호하여 원본 데이터를 복원하고, 블록체인에 새로운 블록으로 해당 원본 데이터를 저장하거나, 기존 데이터를 해당 원본 데이터로 수정하는 클라우드 블록체인 시스템 및 그의 제어 방법을 제공하는 데 있다.
- [0007] 본 발명의 다른 목적은 사용자 단말에서 웹 서버로 아이디와 비밀번호를 이용해서 로그인한 후, 요청에 따라 웹 서버에서 제공하는 인증용 블록을 수신하고, 수신된 인증용 블록을 게이트 서버에 등록한 후, 클라우드 포켓에서 사용자 단말이 게이트 서버에 등록한 인증용 블록과 웹 서버가 게이트 서버에 등록한 인증용 블록 간의 일치 여부 확인에 따라 인증 여부를 확인한 후, 인증에 성공한 경우 유효 기간이 설정된 인증키를 생성하여 게이트 서버에 등록하고, 사용자 단말에서 게이트 서버에 등록된 인증키를 이용해서 게이트 서버 및 클라우드 포켓과 연동하여 원본 데이터를 블록 형태로 클라우드 블록체인에 등록하는 클라우드 블록체인 시스템 및 그의 제어 방법을 제공하는 데 있다.

과제의 해결 수단

- [0008] 본 발명의 실시예에 따른 클라우드 블록체인 시스템은 사용자 단말과 클라우드 포켓을 중계하는 게이트 서버; 클라우드 포켓으로부터 인증키를 발급받기 위해서, 복수의 게이트 서버 중 어느 하나의 게이트 서버에 접속하고, 상기 접속된 게이트 서버 내의 복수의 테이블 중 어느 하나의 테이블에 웹 서버로부터 제공되는 인증용 블록을 등록하고, 상기 등록된 인증용 블록에 대응하는 인증키 블록을 제공받는 상기 사용자 단말; 및 미리 설정된 주기로 상기 게이트 서버에 접속한 후, 상기 게이트 서버 내의 복수의 테이블에 데이터가 등록된 상태인지 여부를 확인하고, 상기 복수의 테이블 중 적어도 하나의 테이블에 데이터가 등록된 상태일 때 상기 테이블에 등록된 데이터를 확인하고, 상기 테이블에 등록된 데이터가 인증용 블록일 때, 상기 게이트 서버와 연동하여, 상기 웹 서버에서 상기 게이트 서버에 등록한 인증용 블록과, 상기 사용자 단말에서 상기 게이트 서버에 등록한 인증용 블록이 일치하는지 여부를 비교하고, 상기 비교 결과 일치할 때, 상기 인증용 블록에 포함된 아이디 및 비밀번호를 확인하고, 상기 확인된 아이디, 비밀번호, 현재 시각과 미리 설정된 유효 기간을 근거로 인증키를 생성하고, 열람 계정키와 수정 계정키와 연산기로 구성된 사용자 계정 암호/복호키를 생성하고, 상기 생성된 인

증키와 상기 생성된 사용자 계정 암호/복호키를 포함하는 인증키 블록을 상기 특정 게이트 서버의 테이블에 등록하는 상기 클라우드 포켓을 포함할 수 있다.

[0009] 본 발명과 관련된 일 예로서 상기 사용자 단말은, 상기 웹 서버로 아이디 및 비밀번호를 이용해서 로그인하고, 상기 웹 서버는, 상기 사용자 단말의 인증용 블록 생성 요청을 근거로 상기 아이디 및 비밀번호로 구성된 인증용 블록을 생성하고, 상기 생성된 인증용 블록을 상기 사용자 단말에 전송하고, 상기 생성된 인증용 블록을 상기 웹 서버와 연동하는 게이트 서버에 등록하며, 상기 사용자 단말은, 상기 인증용 블록 생성 요청에 응답하여 상기 웹 서버로부터 전송되는 인증용 블록을 수신할 수 있다.

[0010] 본 발명의 실시예에 따른 클라우드 블록체인 시스템의 제어 방법은 사용자 단말에 의해, 클라우드 포켓으로부터 인증키를 발급받기 위해서, 복수의 게이트 서버 중 어느 하나의 게이트 서버에 접속하는 단계; 상기 사용자 단말에 의해, 상기 접속된 게이트 서버 내의 복수의 테이블 중 어느 하나의 테이블에 웹 서버로부터 제공되는 인증용 블록을 등록하는 단계; 클라우드 포켓에 의해, 미리 설정된 주기로 상기 게이트 서버에 접속한 후, 상기 게이트 서버 내의 복수의 테이블에 데이터가 등록된 상태인지 여부를 확인하는 단계; 상기 확인 결과, 상기 복수의 테이블 중 적어도 하나의 테이블에 데이터가 등록된 상태일 때, 상기 클라우드 포켓에 의해, 상기 테이블에 등록된 데이터를 확인하는 단계; 상기 확인 결과, 상기 테이블에 등록된 데이터가 인증용 블록일 때, 상기 클라우드 포켓에 의해, 상기 게이트 서버와 연동하여, 상기 웹 서버에서 상기 게이트 서버에 등록한 인증용 블록과, 상기 사용자 단말에서 상기 게이트 서버에 등록한 인증용 블록이 일치하는지 여부를 비교하는 단계; 상기 비교 결과, 상기 웹 서버에서 상기 게이트 서버에 등록한 인증용 블록과, 상기 사용자 단말에서 상기 게이트 서버에 등록한 인증용 블록이 일치할 때, 상기 클라우드 포켓에 의해, 상기 인증용 블록에 포함된 아이디 및 비밀번호를 확인하고, 상기 확인된 아이디, 비밀번호, 현재 시각과 미리 설정된 유효 기간을 근거로 인증키를 생성하는 단계; 상기 클라우드 포켓에 의해, 암호화된 데이터를 해석하고자 할 때 사용하기 위한 미리 설정된 크기의 열람 계정키와, 데이터를 암호화하고자 할 때 사용하기 위한 미리 설정된 크기의 수정 계정키와, 연산부호화 방식을 사용하여 패턴으로 해석이 불가능하게 하기 위한 미리 설정된 크기의 연산키로 구성된 사용자 계정 암호/복호키를 생성하는 단계; 상기 클라우드 포켓에 의해, 상기 생성된 인증키와 상기 생성된 사용자 계정 암호/복호키를 포함하는 인증키 블록을 상기 특정 게이트 서버의 테이블에 등록하는 단계; 및 상기 사용자 단말에 의해, 상기 게이트 서버의 테이블에 등록된 인증키 블록을 확인하는 단계를 포함할 수 있다.

[0011] 본 발명과 관련된 일 예로서 상기 사용자 단말에 의해, 상기 클라우드 포켓에서 관리하는 클라우드 블록체인에 데이터를 저장하거나 또는 상기 클라우드 블록체인에 등록된 데이터를 조회하기 위해서, 클라우드 블록체인에 등록하고자 하는 원본 데이터를 상기 인증키 블록에 포함된 사용자 계정 암호/복호키를 이용해서 암호화하여, 암호 블록을 생성하는 단계; 상기 사용자 단말에 의해, 상기 생성된 암호 블록 및 상기 인증키 블록에 포함된 인증키를 포함하는 요구문을 생성하는 단계; 상기 사용자 단말에 의해, 상기 게이트 서버에 접속하는 단계; 상기 사용자 단말에 의해, 상기 접속된 게이트 서버 내의 복수의 테이블 중 어느 하나의 테이블에 상기 생성된 요구문을 등록하는 단계; 상기 클라우드 포켓에 의해, 상기 미리 설정된 주기로 상기 게이트 서버에 접속한 후, 상기 게이트 서버 내의 복수의 테이블에 데이터가 등록된 상태인지 여부를 확인하는 단계; 상기 확인 결과, 상기 복수의 테이블 중 적어도 하나의 테이블에 데이터가 등록된 상태일 때, 상기 클라우드 포켓에 의해, 상기 테이블에 등록된 데이터를 확인하는 단계; 상기 확인 결과, 상기 테이블에 등록된 데이터가 요구문일 때, 상기 클라우드 포켓에 의해, 상기 요구문에 대해 검증 기능을 수행하는 단계; 및 상기 클라우드 포켓에 의해, 상기 요구문에 대한 검증이 정상적으로 완료될 때, 상기 요구문으로부터 복호한 원본 데이터를 근거로 클라우드 블록체인에서 블록 생성 기능, 블록 수정 기능 및 블록 조회 기능 중 어느 하나의 기능을 수행하는 단계를 더 포함할 수 있다.

[0012] 본 발명과 관련된 일 예로서 상기 요구문에 대해 검증 기능을 수행하는 단계는, 상기 클라우드 포켓에 의해, 상기 데이터의 유효성을 검증하기 위해서, 현재 시각과 상기 요구문에 포함된 타임스탬프 간의 시간 차이가 미리 설정된 기준값을 지난 상태인지 여부를 검증하는 과정; 상기 요구문의 유효성 검증 결과, 상기 요구문이 유효하지 않은 것으로 판단될 때, 상기 클라우드 포켓에 의해, 해당 데이터의 유효성 검증이 실패한 상태임을 나타내는 정보를 상기 게이트 서버의 테이블에 등록하고, 상기 게이트 서버와의 연결을 종료하는 과정; 상기 요구문의 유효성 검증 결과, 상기 요구문이 유효한 것으로 판단될 때, 상기 클라우드 포켓에 의해, 상기 요구문에 포함된 헤더값이 미리 설정된 규격을 충족하는지 여부를 확인하는 과정; 및 상기 확인 결과, 상기 요구문에 포함된 헤더값이 상기 규격을 충족할 때, 상기 요구문에 포함된 암호 블록을 상기 인증용 블록을 근거로 생성된 사용자 계정 암호/복호키를 이용해서 복호하여, 원본 데이터를 생성하는 과정을 포함할 수 있다.

[0013] 본 발명과 관련된 일 예로서 상기 클라우드 포켓에 의해, 상기 미리 설정된 주기로 상기 게이트 서버에 접속한

후, 상기 요구문에 대응하는 기능 수행 결과를 상기 게이트 서버의 테이블에 등록하는 단계; 및 상기 사용자 단말에 의해, 상기 게이트 서버의 테이블에 등록된 기능 수행 결과를 확인하는 단계를 더 포함할 수 있다.

[0014] 본 발명과 관련된 일 예로서 상기 클라우드 포켓에 의해, 복수의 메인 서버 중에서 어느 하나의 특정 메인 서버와 연결하고, 상기 연결된 특정 메인 서버 내의 데이터베이스 내의 특정 테이블에 상기 요구문에 대응하는 기능 수행 결과를 저장하는 단계; 상기 특정 메인 서버에 의해, 상기 특정 테이블에 대응하는 특정 사서함 번호를 상기 클라우드 포켓에 전송하는 단계; 상기 특정 메인 서버에 의해, 상기 복수의 메인 서버 중에서 상기 특정 메인 서버를 제외한 나머지 메인 서버와 각각 연동하여, 상기 요구문에 대응하는 기능 수행 결과를 상기 나머지 메인 서버의 데이터베이스에 각각 등록하는 단계; 상기 클라우드 포켓에 의해, 상기 특정 메인 서버로부터 전송되는 상기 특정 테이블에 대응하는 특정 사서함 번호를 수신하는 단계; 상기 클라우드 포켓에 의해, 상기 미리 설정된 주기로 상기 게이트 서버에 접속한 후, 상기 특정 사서함 번호를 상기 게이트 서버의 테이블에 등록하는 단계; 및 상기 사용자 단말에 의해, 상기 게이트 서버의 테이블에 등록된 특정 사서함 번호를 확인하는 단계를 더 포함할 수 있다.

발명의 효과

[0015] 본 발명은 사용자 단말에서 원본 데이터를 인증키를 이용해서 암호화하여 암호 블록을 생성하고, 암호 블록과 타임스탬프를 포함하는 요구 정보를 게이트 서버에 등록하고, 클라우드 포켓에서 게이트 서버에 접속하여 요구 정보를 확인한 후, 요구 정보에 포함된 암호 블록을 복호화하여 원본 데이터를 복원하고, 블록체인에 새로운 블록으로 해당 원본 데이터를 저장하거나, 기존 데이터를 해당 원본 데이터로 수정함으로써, 블록체인을 개인 PC나 디바이스에 구성하는 것이 아니라, 네트워크에 연결되어 있는 클라우드 포켓에 구성함에 따라 개인 디바이스에는 아무 정보도 보관하지 않고, 사용자와 클라우드 포켓 간에 연결하는 암호화 블록 프로토콜만 존재하는 상태에서, 수많은 클라우드 포켓들이 서로 네트워크상에 PtoP로 연결되어 실시간 처리를 통해 화폐의 기능이 가능하며, 실시간 수정, 송신, 생성이 가능하고, 통화량 제어가 가능하고, 가상화폐의 흐름을 추적할 수 있는 효과가 있다.

[0016] 또한, 본 발명은 사용자 단말에서 웹 서버로 아이디와 비밀번호를 이용해서 로그인한 후, 요청에 따라 웹 서버에서 제공하는 인증용 블록을 수신하고, 수신된 인증용 블록을 게이트 서버에 등록한 후, 클라우드 포켓에서 사용자 단말이 게이트 서버에 등록한 인증용 블록과 웹 서버가 게이트 서버에 등록한 인증용 블록 간의 일치 여부 확인에 따라 인증 여부를 확인한 후, 인증에 성공한 경우 유효 기간이 설정된 인증키를 생성하여 게이트 서버에 등록하고, 사용자 단말에서 게이트 서버에 등록된 인증키를 이용해서 게이트 서버 및 클라우드 포켓과 연동하여 원본 데이터를 블록 형태로 클라우드 블록체인에 등록함으로써, 사용자 단말에서는 유효 기간이 설정된 인증키를 이용해서 블록을 생성, 수정 등을 효율적으로 수행할 수 있는 효과가 있다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 실시예에 따른 클라우드 블록체인 시스템의 구성을 나타낸 블록도이다.
 도 2는 본 발명의 실시예에 따른 사용자 계정 암호/복호키의 구조의 예를 나타낸 도이다.
 도 3은 본 발명의 실시예에 따른 메인 서버의 데이터베이스에서 사서함 번호와 테이블 간의 관계의 예를 나타낸 도이다.
 도 4 내지 도 6은 본 발명의 실시예에 따른 클라우드 블록체인 시스템의 제어 방법을 나타낸 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0018] 본 발명에서 사용되는 기술적 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아님을 유의해야 한다. 또한, 본 발명에서 사용되는 기술적 용어는 본 발명에서 특별히 다른 의미로 정의되지 않는 한, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 의미로 해석되어야 하며, 과도하게 포괄적인 의미로 해석되거나, 과도하게 축소된 의미로 해석되지 않아야 한다. 또한, 본 발명에서 사용되는 기술적인 용어가 본 발명의 사상을 정확하게 표현하지 못하는 잘못된 기술적 용어일 때에는 당업자가 올바르게 이해할 수 있는 기술적 용어로 대체되어 이해되어야 할 것이다. 또한, 본 발명에서 사용되는 일반적인 용어는 사전에 정의되어 있는 바에 따라, 또는 전후 문맥상에 따라 해석되어야 하며, 과도하게 축소된 의미로 해석되지 않아야 한다.

[0019] 또한, 본 발명에서 사용되는 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한 복수의 표현을 포함한다.

본 발명에서 "구성된다" 또는 "포함한다" 등의 용어는 발명에 기재된 여러 구성 요소들 또는 여러 단계를 반드시 모두 포함하는 것으로 해석되지 않아야 하며, 그 중 일부 구성 요소들 또는 일부 단계들은 포함되지 않을 수도 있고, 또는 추가적인 구성 요소 또는 단계들을 더 포함할 수 있는 것으로 해석되어야 한다.

[0020] 또한, 본 발명에서 사용되는 제 1, 제 2 등과 같이 서수를 포함하는 용어는 구성 요소들을 설명하는데 사용될 수 있지만, 구성 요소들은 용어들에 의해 한정되어서는 안 된다. 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제 1 구성 요소는 제 2 구성 요소로 명명될 수 있고, 유사하게 제 2 구성 요소도 제 1 구성 요소로 명명될 수 있다.

[0021] 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 실시예를 상세히 설명되되, 도면 부호에 관계없이 동일하거나 유사한 구성 요소는 동일한 참조 번호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다.

[0022] 또한, 본 발명을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 첨부된 도면은 본 발명의 사상을 쉽게 이해할 수 있도록 하기 위한 것일 뿐, 첨부된 도면에 의해 본 발명의 사상이 제한되는 것으로 해석되어서는 아니 됨을 유의해야 한다.

[0023] 도 1은 본 발명의 실시예에 따른 클라우드 블록체인 시스템(10)의 구성을 나타낸 블록도이다.

[0024] 도 1에 도시한 바와 같이, 클라우드 블록체인 시스템(10)은 사용자 단말(100), 복수의 게이트 서버(200), 복수의 클라우드 포켓(300) 및 복수의 메인 서버(400)로 구성된다. 도 1에 도시된 클라우드 블록체인 시스템(10)의 구성 요소 모두가 필수 구성 요소인 것은 아니며, 도 1에 도시된 구성 요소보다 많은 구성 요소에 의해 클라우드 블록체인 시스템(10)이 구현될 수도 있고, 그보다 적은 구성 요소에 의해서도 클라우드 블록체인 시스템(10)이 구현될 수도 있다.

[0025] 상기 사용자 단말(100)은 스마트폰(Smart Phone), 휴대 단말기(Portable Terminal), 이동 단말기(Mobile Terminal), 폴더블 단말기(Foldable Terminal), 개인 정보 단말기(Personal Digital Assistant: PDA), PMP(Portable Multimedia Player) 단말기, 텔레매틱스(Telematics) 단말기, 내비게이션(Navigation) 단말기, 개인용 컴퓨터(Personal Computer), 노트북 컴퓨터, 슬레이트 PC(Slate PC), 태블릿 PC(Tablet PC), 울트라북(ultrabook), 웨어러블 디바이스(Wearable Device, 예를 들어, 워치형 단말기(Smartwatch), 글래스형 단말기(Smart Glass), HMD(Head Mounted Display) 등 포함), 와이브로(Wibro) 단말기, IPTV(Internet Protocol Television) 단말기, 스마트 TV, 디지털방송용 단말기, AVN(Audio Video Navigation) 단말기, A/V(Audio/Video) 시스템, 플렉시블 단말기(Flexible Terminal), 디지털 사이니지 장치, 인공지능 스피커, 공간 컴퓨터(Spatial Computer)(예를 들어 비전프로 등 포함) 등과 같은 다양한 단말기에 적용될 수 있다.

[0026] 상기 게이트 서버(200), 상기 클라우드 포켓(300) 및 상기 메인 서버(400)는 웹 서버, 데이터베이스 서버, 프록시 서버 등의 형태로 구현될 수 있다. 또한, 상기 게이트 서버(200), 상기 클라우드 포켓(300) 및 상기 메인 서버(400)에는 네트워크 부하 분산 메커니즘, 내지 해당 게이트 서버(200), 해당 클라우드 포켓(300) 및 해당 메인 서버(400)가 인터넷 또는 다른 네트워크상에서 동작할 수 있도록 하는 다양한 소프트웨어 중 하나 이상이 설치될 수 있으며, 이를 통해 컴퓨터화된 시스템으로 구현될 수 있다. 또한, 네트워크는 http 네트워크일 수 있으며, 전용 회선(private line), 인트라넷 또는 임의의 다른 네트워크일 수 있다. 나아가, 상기 사용자 단말(100), 상기 게이트 서버(200), 상기 클라우드 포켓(300), 상기 메인 서버(400) 간의 연결은 데이터가 임의의 해커 또는 다른 제3자에 의한 공격을 받지 않도록 보안 네트워크로 연결될 수 있다. 또한, 상기 게이트 서버(200), 상기 클라우드 포켓(300) 및 상기 메인 서버(400)는 복수의 데이터베이스 서버를 포함할 수 있으며, 이러한 데이터베이스 서버가 분산 데이터베이스 서버 아키텍처를 비롯한 임의의 유형의 네트워크 연결을 통해 상기 게이트 서버(200), 상기 클라우드 포켓(300) 및 상기 메인 서버(400)와 별도로 연결되는 방식으로 구현될 수 있다.

[0027] 상기 사용자 단말(100), 상기 게이트 서버(200), 상기 클라우드 포켓(300) 및 상기 메인 서버(400) 각각은 다른 단말들과의 통신 기능을 수행하기 위한 통신부(미도시), 다양한 정보 및 프로그램(또는 애플리케이션)을 저장하기 위한 저장부(미도시), 다양한 정보 및 프로그램 실행 결과를 표시하기 위한 표시부(미도시), 상기 다양한 정보 및 프로그램 실행 결과에 대응하는 음성 정보를 출력하기 위한 음성 출력부(미도시), 각 단말의 다양한 구성 요소 및 기능을 제어하기 위한 제어부(미도시) 등을 포함할 수 있다.

[0028] 상기 사용자 단말(100)은 웹 서버(미도시), 상기 복수의 게이트 서버(200) 등과 통신한다. 이때, 상기 사용자 단말(100)은 해당 웹 서버에서 제공하는 전용 앱 및/또는 웹 사이트를 통해 블록 생성 기능, 블록 수정 기능, 블록 조회 기능, 구독 기능 등을 수행하는 사용자가 소지한 단말일 수 있다.

- [0029] 또한, 상기 사용자 단말(100)은 상기 웹 서버와 연동하여, 상기 웹 서버에서 제공하는 전용 앱 및/또는 웹 사이트를 통해 블록 생성 기능, 블록 수정 기능, 블록 조회 기능, 구독 기능 등을 제공받기 위한 사용자로 회원 가입하며, 개인 정보 등을 상기 웹 서버에 등록한다. 이때, 상기 개인 정보는 아이디, 이메일 주소, 패스워드(또는 비밀번호), 이름, 성별, 생년월일, 연락처, 주소지(또는 주소정보) 등을 포함한다.
- [0030] 또한, 상기 사용자 단말(100)은 상기 웹 서버와의 연동에 의해, 해당 웹 서버에서 제공하는 기능(또는 서비스) 이용을 위해서, 해당 사용자 단말(100)에서 미리 설정한 전자 문서 형태의 개인 정보 이용 동의서 등을 상기 웹 서버에 등록한다.
- [0031] 또한, 상기 사용자 단말(100)은 해당 사용자 단말(100)의 사용자가 가입한 SNS 계정 정보 또는 타사이트 계정 정보를 이용하여 상기 웹 서버에 사용자로 회원 가입할 수도 있다. 여기서, 상기 SNS 계정은 페이스북, 트위터, 인스타그램, 카카오톡, 네이버 블로그 등과 관련한 정보일 수 있다. 또한, 상기 타사이트 계정은 유튜브, 카카오톡, 네이버 등과 관련한 정보일 수 있다. 또한, 상기 모바일 메신저 계정은 카카오톡(KakaoTalk), 라인(line), 바이버(viber), 위챗(wechat), 와츠앱(whatsapp), 텔레그램(Telegram), 스냅챗(snapchat) 등과 관련한 정보일 수 있다.
- [0032] 또한, 회원 가입 절차 수행 시, 상기 사용자 단말(100)은 본인 인증 수단(예를 들어 이동 전화, 신용카드, 아이폰, 디지털 인증서 등 포함)을 통한 인증 기능을 완료해야 상기 웹 서버에 대한 회원 가입 절차를 정상적으로 완료할 수 있다. 여기서, 상기 디지털 인증서는 공동인증서, 금융인증서, 민간인증서 등을 포함한다.
- [0033] 또한, 회원 가입이 완료된 후, 상기 사용자 단말(100)은 상기 웹 서버에서 제공하는 서비스를 이용하기 위해서, 상기 웹 서버로부터 제공되는 전용 앱(또는 애플리케이션/응용 프로그램/특정 앱)을 해당 사용자 단말(100)에 설치한다. 이때, 상기 전용 앱은 네이티브 앱(Native App), 모바일 웹앱(Mobile WebApp), 반응형 웹앱(Mobile WebApp Design: RWD), 적응형 웹앱(Adaptive Web Design: AWD), 하이브리드 앱(Hybrid App) 등을 포함하며, 블록 생성 기능, 블록 수정 기능, 블록 조회 기능, 구독 기능 등을 수행하기 위한 앱일 수 있다.
- [0034] 또한, 회원 가입이 완료된 후, 상기 사용자 단말(100)은 상기 웹 서버에서 제공되는 할인 쿠폰을 해당 전용 앱을 통해 표시할 수 있다. 이때, 상기 할인 쿠폰은 해당 웹 서버에서 제공하는 파일 블록 생성 기능, 블록 수정 기능, 블록 조회 기능, 구독 기능 등을 이용시 일정 비율의 할인 정보를 포함하는 할인 쿠폰일 수 있다.
- [0035] 또한, 상기 사용자 단말(100)은 상기 웹 서버에서 제공하는 기능들을 수행하기 위해서, 상기 웹 서버 및 결제 서버(미도시)와 연동하여, 구독 기능에 따라 결제 기능을 수행한다. 이때, 상기 웹 서버는 카드 결제, 은행의 결제 계좌 연동을 통한 자동 이체, 상기 웹 서버에 회원 가입한 상기 사용자 단말(100)의 계좌에 남아 있는 현금성 포인트나 현금을 이용한 결제, 카카오페이, 네이버페이 등을 포함하는 간편결제 등을 통해 결제 기능을 수행할 수 있다.
- [0036] 결제가 실패한 경우, 상기 사용자 단말(100)은 상기 웹 서버(또는 상기 결제 서버)로부터 전송되는 결제가 실패한 상태임을 나타내는 정보(예를 들어 잔액 부족, 한도 초과 등 포함)를 수신하고, 상기 수신된 결제가 실패한 상태임을 나타내는 정보를 출력(또는 표시)한다.
- [0037] 또한, 상기 사용자 단말(100)은 결제 기능이 정상적으로 수행된 후, 상기 웹 서버로부터 전송되는 결제 기능 수행 결과를 수신하고, 상기 수신된 결제 기능 결과를 출력(또는 표시)한다. 여기서, 상기 결제 기능 수행 결과는 구독 기간, 결제 금액, 결제 일자 및 시각 정보 등을 포함한다.
- [0038] 또한, 상기 사용자 단말(100)은 웹 서버(미도시)로 아이디(또는 해당 사용자 단말(100)의 디바이스 아이디)와 비밀번호(또는 패스워드)를 이용해서 로그인(또는 접속/연결)한다. 이때, 상기 사용자 단말(100)은 해당 웹 서버에서 제공하는 서비스를 이용하기 위한 사용자로 회원 가입한 상태일 수 있다.
- [0039] 또한, 상기 사용자 단말(100)은 해당 사용자 단말(100)의 사용자의 요청에 따른 상기 웹 서버로 인증용 블록 생성을 요청한다.
- [0040] 또한, 상기 웹 서버는 상기 사용자 단말(100)의 인증용 블록 생성 요청(또는 인증용 블록 생성 요청 정보)에 따라, 상기 사용자 단말(100)과 관련한 아이디(또는 해당 사용자 단말(100)의 디바이스 아이디)와 비밀번호로 구성된 인증용 블록을 생성하고, 상기 생성된 인증용 블록을 상기 사용자 단말(100)에 제공(또는 전송)한다.
- [0041] 또한, 상기 웹 서버는 상기 생성된 인증용 블록을 해당 웹 서버와 연동하는 게이트 서버(200)(또는 해당 게이트 서버(200) 내의 복수의 테이블 중 임의의 테이블)에 등록(또는 저장)한다. 이때, 상기 게이트 서버(200)는 해당 웹 서버로부터 제공되는 인증용 블록을 해당 게이트 서버(200) 내의 복수의 테이블(또는 복수의 사서함) 중에서

어느 하나의 테이블에 등록(또는 저장)한다.

- [0042] 또한, 상기 사용자 단말(100)은 앞선 인증용 블록 생성 요청(또는 인증용 블록 생성 요청 정보)에 응답하여 상기 웹 서버로부터 제공되는(또는 전송되는) 인증용 블록을 수신한다. 여기서, 상기 사용자 단말(100)은 해당 인증용 블록을 수신한 후, 해당 웹 서버와의 로그인 상태(또는 접속 상태/연결 상태)를 종료(또는 로그아웃)할 수 있다.
- [0043] 또한, 상기 사용자 단말(100)은 클라우드 포켓(300)으로부터 인증키(또는 인증키 블록)를 발급받기 위해서, 복수의 게이트 서버(200) 중 어느 하나의 특정 게이트 서버(200)에 접속(또는 연결)한다. 이때, 상기 사용자 단말(100)과 상기 게이트 서버(200)는 미리 설정된 HTTP 프로토콜(또는 HTTPS 프로토콜)을 사용하여 통신한다. 여기서, 상기 사용자 단말(100)과 상기 게이트 서버(200) 간에 송/수신되는 데이터(또는 정보)는 https 프로토콜에 내부 암호화를 결합하여 송/수신될 수 있다.
- [0044] 예를 들어, 상기 사용자 단말(100)은 데이터를 암호화하여 암호 블록(일 예로 512 바이트, 1024 바이트 등의 블록)을 생성하고, 상기 생성된 암호 블록(또는 암호화된 데이터 블록)을 HTTP 프로토콜에 바이트 데이터(byte data)로 포함시키면(또는 HTTPS의 argument에 바이트로 설정하면), 자동으로 HTTP 프로토콜이 암호화된다.
- [0045] 또한, 상기 사용자 단말(100)은 상기 수신된 인증용 블록을 상기 접속된 특정 게이트 서버(200)에 등록(또는 저장)한다.
- [0046] 즉, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200) 내의 복수의 테이블(또는 사서함) 중 어느 하나의 특정 테이블(또는 특정 사서함)에 해당 인증용 블록을 등록(또는 저장)한다.
- [0047] 또한, 상기 사용자 단말(100)은 클라우드 포켓(300)에서 관리하는 클라우드 블록체인에 데이터(또는 정보)를 저장(또는 생성/수정)하거나 또는 해당 클라우드 블록체인에 등록된 데이터(또는 정보)를 조회하기 위해서, 클라우드 블록체인에 등록하고자 하는 원본 데이터를 상기 인증키 블록에 포함된 사용자 계정 암호/복호키를 이용해서 암호화하여, 암호 블록(또는 암호화된 데이터)을 생성한다. 여기서, 상기 원본 데이터(또는 목적 블록/목적 데이터/암호화하고자 하는 데이터 블록)는 내용(또는 정보/데이터)(예를 들어 문자, 숫자, 2진 데이터 등 포함)뿐만 아니라, 요구사항(예를 들어 생성 요청 정보, 수정 요청 정보, 조회 요청 정보 등 포함) 등을 포함한다. 또한, 상기 암호 블록에는 원본 데이터뿐만 아니라, 헤더값(또는 암호화와 관련한 헤더값)이 포함된 상태일 수 있고, 해당 원본 데이터의 크기가 큰 경우 미리 설정된 단위(예를 들어 512 바이트, 1024 바이트 등 포함)로 분할되어, 복수의 암호 블록으로 구성할 수도 있다.
- [0048] 이때, 상기 사용자 단말(100)에서 암호 블록을 생성하는 경우, 상기 사용자 단말(100)은 해당 인증키 블록 내의 타임스탬프(time stamp)를 확인하고, 현재 시각을 기준으로 해당 타임스탬프의 유효 기간(또는 유효 시간)이 지난 경우, 해당 인증키(또는 인증키 블록)의 유효 기간이 지난 상태임을 나타내는 정보를 표시하고, 암호 블록을 생성하는 과정을 중단(또는 중지)하며, 상기 웹 서버와의 통신에 의해 인증용 블록을 재발급 받아야 하는 상태임을 나타내는 정보(또는 인증용 블록 재발급 안내 정보)를 표시(또는 출력)할 수도 있다.
- [0049] 또한, 상기 사용자 단말(100)은 상기 생성된 암호 블록, 상기 인증키 블록에 포함된 인증키 등을 포함하는 요구문(또는 명령문/요청문/요구문 블록)을 생성한다.
- [0050] 또한, 상기 사용자 단말(100)은 상기 복수의 게이트 서버(200) 중 어느 하나의 특정 게이트 서버(200)에 접속(또는 통신/연결)한다. 이때, 상기 사용자 단말(100)은 앞선 특정 게이트 서버(200)와의 접속 상태를 유지하고 있는 상태일 수도 있다.
- [0051] 또한, 상기 사용자 단말(100)은 상기 생성된 요구문을 상기 접속된 특정 게이트 서버(200)에 등록(또는 저장)한다.
- [0052] 즉, 상기 사용자 단말(100)은 상기 특정 게이트 서버(200) 내의 복수의 테이블(또는 사서함) 중 어느 하나의 다른 특정 테이블(또는 다른 특정 사서함)에 해당 요구문을 등록(또는 저장)한다. 이때, 상기 사용자 단말(100)은 상기 특정 게이트 서버(200) 내의 복수의 테이블(또는 사서함) 중에서 앞서 사용자 단말(100)에서 데이터(예를 들어 인증용 블록 등 포함)를 등록한 특정 테이블에 해당 요구문을 누적하여 저장하거나 또는, 해당 특정 테이블을 초기화하고 해당 요구문을 저장할 수도 있다.
- [0053] 이와 같이, 상기 사용자 단말(100)은 해당 사용자 단말(100)과 연동하는 특정 게이트 서버(200)에 해당 사용자 단말(100)에서 클라우드 블록체인을 통해 처리(예를 들어 조회, 생성, 수정 등 포함)하고자 하는 데이터를 저장

(또는 등록)할 수 있다.

- [0054] 또한, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록된(또는 저장된) 인증 실패 정보를 확인(또는 표시/출력)한다. 이때, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)와 접속한 상태에서, 해당 특정 게이트 서버(200)의 해당 테이블에 새롭게 정보(예를 들어 인증 실패 정보 등 포함)가 등록됨에 따라, 해당 특정 게이트 서버(200)로부터 전송되는 알림 정보(또는 안내 정보)를 수신하고, 상기 수신된 알림 정보를 근거로 해당 특정 게이트 서버(200) 내의 해당 테이블에 등록된 인증 실패 정보를 확인할 수도 있다. 또한, 상기 사용자 단말(100)은 앞선 단계들을 통해 인증 블록을 새로 발급받아야 함을 포함하는 안내 정보를 추가로 표시할 수도 있다.
- [0055] 또한, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록된(또는 저장된) 인증키 블록을 확인(또는 표시/출력/다운로드)한다. 이때, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)와 접속한 상태에서, 해당 특정 게이트 서버(200)의 해당 테이블에 새롭게 정보(예를 들어 인증키 블록 등 포함)가 등록됨에 따라, 해당 특정 게이트 서버(200)로부터 전송되는 알림 정보(또는 안내 정보)를 수신하고, 상기 수신된 알림 정보를 근거로 해당 특정 게이트 서버(200) 내의 해당 테이블에 등록된 인증키 블록을 확인할 수도 있다.
- [0056] 또한, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록된(또는 저장된) 해당 데이터의 유효성 검증이 실패한 상태임을 나타내는 정보를 확인(또는 표시/출력)한다. 이때, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)와 접속한 상태에서, 해당 특정 게이트 서버(200)의 해당 테이블에 새롭게 정보(예를 들어 해당 데이터의 유효성 검증이 실패한 상태임을 나타내는 정보 등 포함)가 등록됨에 따라, 해당 특정 게이트 서버(200)로부터 전송되는 다른 알림 정보(또는 다른 안내 정보)를 수신하고, 상기 수신된 다른 안내 정보를 근거로 해당 특정 게이트 서버(200) 내의 해당 테이블에 등록된 해당 데이터의 유효성 검증이 실패한 상태임을 나타내는 정보를 확인할 수도 있다. 또한, 상기 사용자 단말(100)은 앞선 단계들을 통해 인증키를 새로 발급받아야 함을 포함하는 안내 정보를 추가로 표시할 수도 있다.
- [0057] 또한, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록된(또는 저장된) 해당 데이터의 규격 검증이 실패한 상태임을 나타내는 정보를 확인(또는 표시/출력)한다. 이때, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)와 접속한 상태에서, 해당 특정 게이트 서버(200)의 해당 테이블에 새롭게 정보(예를 들어 해당 데이터의 규격 검증이 실패한 상태임을 나타내는 정보 등 포함)가 등록됨에 따라, 해당 특정 게이트 서버(200)로부터 전송되는 다른 알림 정보(또는 다른 안내 정보)를 수신하고, 상기 수신된 다른 안내 정보를 근거로 해당 특정 게이트 서버(200) 내의 해당 테이블에 등록된 해당 데이터의 **규격** 검증이 실패한 상태임을 나타내는 정보를 확인할 수도 있다. 또한, 상기 사용자 단말(100)은 앞선 단계들을 통해 인증키를 새로 발급받아야 함을 포함하는 안내 정보를 추가로 표시할 수도 있다.
- [0058] 또한, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록된(또는 저장된) 기능 수행 결과를 확인(또는 표시/출력)한다. 이때, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)와 접속한 상태에서, 해당 특정 게이트 서버(200)의 해당 테이블에 새롭게 정보(예를 들어 기능 수행 결과 등 포함)가 등록됨에 따라, 해당 특정 게이트 서버(200)로부터 전송되는 알림 정보(또는 안내 정보)를 수신하고, 상기 수신된 알림 정보를 근거로 해당 특정 게이트 서버(200) 내의 해당 테이블에 등록된 기능 수행 결과를 확인할 수도 있다.
- [0059] 또한, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록된(또는 저장된) 특정 사서함 번호를 확인(또는 표시/출력)한다.
- [0060] 또한, 상기 사용자 단말(100)은 추후 해당 건과 관련한 정보(또는 데이터)에 대해서 수정 기능, 조회 기능 등을 수행하고자 하는 경우, 해당 특정 사서함 번호를 이용한다.
- [0061] 상기 게이트 서버(Gate Server)(200)는, 상기 웹 서버, 상기 사용자 단말(100), 상기 클라우드 포켓(300) 등과 통신한다. 여기서, 상기 게이트 서버(200)는 상기 사용자 단말(100)로부터 제공되는 데이터(또는 정보)를 임시 저장하고, 상기 클라우드 포켓(300)의 요청에 따라 임시 저장 중인 데이터를 제공하고 해당 데이터에 응답하여 클라우드 포켓(300)으로부터 제공되는 기능 수행 결과를 임시 저장하며, 해당 임시 저장된 기능 수행 결과를 해당 사용자 단말(100)에 제공하는 서버로, 중계자(또는 중계 기능) 역할을 수행하는 서버일 수 있다.
- [0062] 또한, 상기 게이트 서버(200)는 복수로 구성하며, 복수의 게이트 서버(200)는 각 게이트 서버(200)에 각각 저장하는 데이터를 서로 공유하여 저장한다. 이때, 상기 복수의 게이트 서버(200)는 각각의 게이트 서버(200)에 저

장(또는 등록)하는 데이터에 대해서, 서로 공유(또는 데이터 동기화)할 수 있다.

- [0063] 또한, 하나의 게이트 서버(200)에는 복수의 클라우드 포켓(300)이 접속할 수 있다. 여기서, 상기 복수의 게이트 서버(200)는 서로 다른 주소(예를 들어 IP 주소, URL 주소 등 포함)를 가진다.
- [0064] 예를 들어, 제 1 게이트 서버(200)에는 제 1 클라우드 포켓(300) 내지 제 100 클라우드 포켓(300)이 접속하고, 제 2 게이트 서버(200)에는 제 101 클라우드 포켓(300) 내지 제 200 클라우드 포켓(300)이 접속할 수 있다.
- [0065] 또한, 하나의 클라우드 포켓(300)에서도 복수의 게이트 서버(200)에 각각 접속할 수 있다.
- [0066] 이와 같이, 상기 복수의 게이트 서버(200)와 상기 복수의 클라우드 포켓(300) 간의 연결은 미리 설정된 정책(예를 들어 제 1 게이트 서버(200)는 제 1 클라우드 포켓(300) 내지 제 100 클라우드 포켓(300)이 접속한다 등 포함)에 의해 관리될 수 있다.
- [0067] 또한, 상기 게이트 서버(200)는 상기 웹 서버와 연동하여, 해당 웹 서버로부터 제공되는 인증용 블록을 해당 게이트 서버(200)(또는 해당 게이트 서버(200) 내의 복수의 테이블 중 임의의 테이블)에 등록(또는 저장)한다.
- [0068] 또한, 상기 게이트 서버(200)는 전체 복수의 게이트 서버(200) 중에서 해당 게이트 서버(200)를 제외한 나머지 게이트 서버(200)와 각각 연동하여, 상기 인증용 블록을 나머지 게이트 서버(200)에 각각 저장(또는 등록/업데이트)하도록 구성한다.
- [0069] 또한, 상기 게이트 서버(200)는 클라우드 포켓(300)으로부터 인증키(또는 인증키 블록)를 발급받기 위한 사용자 단말(100)과 접속(또는 연결)한다. 이때, 상기 사용자 단말(100)과 상기 게이트 서버(200)는 미리 설정된 HTTP 프로토콜(또는 HTTPS 프로토콜)을 사용하여 통신한다.
- [0070] 또한, 상기 게이트 서버(200)는 상기 사용자 단말(100)과 연동하여, 해당 특정 게이트 서버(200) 내의 복수의 테이블(또는 사서함) 중 어느 하나의 특정 테이블(또는 특정 사서함)에 해당 인증용 블록을 등록(또는 저장)한다. 이때, 상기 특정 게이트 서버(200)는 해당 특정 게이트 서버(200)에서 관리하는 복수의 테이블 중에서 해당 사용자 단말(100)과 관련한 적어도 하나의 테이블을 할당하고, 상기 할당된 적어도 하나의 테이블 중 어느 하나의 테이블에 해당 인증용 블록을 등록할 수도 있다.
- [0071] 또한, 상기 게이트 서버(200)는 상기 복수의 클라우드 포켓(300) 중에서 적어도 하나의 클라우드 포켓(300)과 연결한다. 이때, 상기 게이트 서버(200)와 상기 클라우드 포켓(300) 간의 연결은 해당 클라우드 포켓(300)에서만 해당 특정 게이트 서버(200)로 접속하는 단방향 통신일 수 있다.
- [0072] 또한, 상기 게이트 서버(200) 내의 복수의 테이블 중 적어도 하나의 테이블에 상기 사용자 단말(100)에서 등록한 데이터가 존재하는 경우, 상기 게이트 서버(200)는 상기 클라우드 포켓(300)의 요청에 따라, 해당 데이터를 상기 클라우드 포켓(300)에 전송(또는 제공)한다.
- [0073] 또한, 상기 게이트 서버(200)는 상기 클라우드 포켓(300)과 연동하여, 상기 클라우드 포켓(300)에서 생성된 인증키 블록을 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록(또는 저장)한다. 여기서, 상기 게이트 서버(200)는 해당 특정 게이트 서버(200)의 해당 테이블에서 앞서 저장 중인 데이터(예를 들어 인증용 블록 등 포함)에 추가하여 상기 인증키 블록을 저장하거나 또는, 해당 테이블에 저장 중인 데이터를 삭제하고 상기 인증키 블록을 저장한다. 이때, 상기 게이트 서버(200)는 해당 특정 게이트 서버(200)의 복수의 테이블 중 서로 다른 테이블에 상기 인증키 블록, 상기 인증용 블록 등을 각각 저장할 수도 있다.
- [0074] 또한, 상기 게이트 서버(200)는 상기 사용자 단말(100)과 연동하여, 상기 사용자 단말(100)에서 생성된 요구문을 상기 게이트 서버(200) 내의 복수의 테이블(또는 사서함) 중 어느 하나의 다른 특정 테이블(또는 다른 특정 사서함)에 해당 요구문을 등록(또는 저장)한다.
- [0075] 또한, 상기 게이트 서버(200)는 상기 클라우드 포켓(300)과 연동하여, 상기 클라우드 포켓(300)에서 생성된 기능 수행 결과(예를 들어 블록 생성 기능 수행 결과, 블록 수정 기능 수행 결과, 블록 조회 기능 수행 결과 등 포함)를 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록(또는 저장)한다. 여기서, 상기 게이트 서버(200)는 해당 특정 게이트 서버(200)의 해당 테이블에서 앞서 저장 중인 데이터(예를 들어 인증용 블록, 요구문 등 포함)에 추가하여 상기 기능 수행 결과를 저장하거나 또는, 해당 테이블에 저장 중인 데이터를 삭제하고 상기 기능 수행 결과를 저장한다. 이때, 상기 게이트 서버(200)는 해당 특정 게이트 서버(200)의 복수의 테이블 중 서로 다른 테이블에 상기 인증키 블록, 상기 인증용 블록, 상기 요구문, 상기 기능 수행 결과 등을 각각 분리하여 저장할 수도 있다. 여기서, 상기 인증키 블록, 상기 인증용 블록, 상기 요구문, 상기 기능 수행 결

과 등의 데이터를 각각 분리하여 저장되는 경우에도, 상기 게이트 서버(200)는 해당 데이터에 각각 포함된 헤더(또는 헤더값)에 의해서 각 데이터가 어떤 사용자 단말(100)과 관련한 정보인지를 확인할 수 있다.

- [0076] 상기 클라우드 포켓(Cloud Pocket: CP)(또는 클라우드 서버/클라우드 포켓 서버/블록체인 클라우드 포켓)(300)은 상기 복수의 게이트 서버(200), 상기 복수의 메인 서버(400) 등과 통신한다. 여기서, 상기 클라우드 포켓(300)은 미리 설정된 정책(또는 조건)에 따라, 복수의 게이트 서버(200) 중에서 적어도 하나의 게이트 서버(200)가 할당되며, 할당된 적어도 하나의 게이트 서버(200)와 연결할 수 있다. 이때, 상기 클라우드 포켓(300)은 단방향 통신에 의해 상기 게이트 서버(200)에 접속하며, 미리 설정된 주기로 해당 게이트 서버(200)에 접속한다. 또한, 상기 복수의 클라우드 포켓(300)은 각각의 클라우드 포켓(300)에 저장(또는 등록)하는 데이터에 대해서 서로 공유(또는 데이터 동기화)할 수 있다.
- [0077] 또한, 상기 클라우드 포켓(300)은 블록체인 기술을 활용한 클라우드 서비스를 제공하며, 블록체인 네트워크를 구성하는 인프라(또는 하드웨어)부터 애플리케이션 개발 및 운영 등을 포함한다.
- [0078] 또한, IDC 센터에 있는 서버가 상기 클라우드 포켓(300)이 될 수 있다.
- [0079] 예를 들어, 리눅스 서버이면, 독립으로 실행되는 복수의 스레드를 띄울 수 있다. 이때, 스레드 1개가 해당 클라우드 포켓(300)이 된다.
- [0080] 또 다른 방법으로, 허브를 IDC 센터에 연결하고, 해당 허브에 복수의 디바이스를 붙이면, 개별 디바이스가 상기 클라우드 포켓(300)이 될 수 있다.
- [0081] 이렇게 서버단의 독립 프로세스 CP와 하나의 디바이스 CP가 모두 가능하다.
- [0082] 이 CP들이 모두 블록체인으로 연결된다.
- [0083] 예를 들어 한 개의 서버에 100개의 프로세스가 있고, 허브별로 5개씩 스마트폰 30개가 연결되어 있다면, 클라우드 포켓(300)은 프로세스 100개와 스마트폰 150개 해서, 총 250개의 클라우드 포켓(300)이 있게 된다.
- [0084] 그리고 이 클라우드 포켓(300)은 모두 같은 데이터를 동일하게 가지고 있다.
- [0085] 또한, 상기 클라우드 포켓(300)은 클라우드 블록체인을 관리(또는 구성/운영)한다. 여기서, 상기 클라우드 블록체인(Cloud Blockchain)은 클라우드 컴퓨팅과 블록체인 기술을 결합한 시스템으로, 블록체인 네트워크와 관련된 데이터 저장, 처리, 보안 및 관리를 클라우드 환경에서 제공하는 방식일 수 있다.
- [0086] 이와 같이, 본 발명의 클라우드 블록체인 시스템(10)은 블록체인을 개인 PC나 디바이스에 구성시키는 것이 아니라, 네트워크에 연결되어 있는 클라우드 포켓에 구성시키는 기술이다.
- [0087] 이에 따라, 코인 보유자(또는 해당 사용자 단말(100)의 사용자)와 연결된 네트워크상의 클라우드 포켓(300)에 코인이 블록체인으로 연결되기에, 개인 디바이스에는 아무 정보도 보관되지 않는다. 단, 사용자 단말(100)에는 사용자와 클라우드 포켓(300) 간에 연결하는 암호화 블록 프로토콜만 존재한다.
- [0088] 또한, 수많은 클라우드 포켓(300)들은 서로 네트워크상에 PtoP로 연결되어 있어, 한 개의 클라우드 포켓(300)에 여러 개의 지갑이 저장되기에, PtoP 속도가 매우 빨라 실시간 송신을 처리할 수 있다.
- [0089] 또한, 상기 클라우드 포켓(300)은 다른 클라우드 포켓(300)과 관련한 정보인 포켓 서버 리스트를 관리(또는 저장)한다. 여기서, 상기 포켓 서버 리스트(Pocket Server List)는 사용자 계정에 대응하는 지갑(또는 암호화폐/가상화폐 지갑)이 어느 클라우드 포켓(300)에서 저장(또는 관리) 중인지에 대한 정보를 포함하며, 지갑 정보별 클라우드 포켓 정보(또는 클라우드 포켓(300)의 주소/URL)를 포함한다.
- [0090] 또한, 상기 클라우드 포켓(300)이 독립 단말일 경우, 하나의 주소를 가질 수 있다.
- [0091] 또한, 한 대의 대형 서버의 하나의 프로세스가 상기 클라우드 포켓(300)이 될 수 있다. 이때, 해당 포켓 서버 리스트가 해당 대형 서버에 있을 수 있다.
- [0092] 즉, 상기 클라우드 포켓(300)은 단말(예를 들어 PC 등 포함)일 수도 있고, 한 서버의 쉘 프로세스일 수도 있다.
- [0093] 그래서, 상기 클라우드 포켓(300)은 연결할 때, IP가 있으면 IP로 접속하고, 특정 서버의 프로세스일 경우 해당 특정 서버의 포켓 서버 리스트를 이용해서 연결한다.
- [0094] 또한, 상기 클라우드 포켓(300)은 미리 설정된 주기로 해당 특정 게이트 서버(200)와 연결(또는 통신/접속)한 후, 해당 특정 게이트 서버(200) 내의 복수의 테이블(또는 사서함)에 데이터(예를 들어 인증용 블록 등 포함)가

등록된(또는 저장된) 상태인지 여부를 확인한다. 이때, 상기 클라우드 포켓(300)은 복수의 게이트 서버(200) 중에서 해당 클라우드 포켓(300)에서 관리할 적어도 하나의 게이트 서버(200)가 할당된(또는 설정된) 상태이며, 해당 주기에 따라 적어도 하나의 게이트 서버(200)에 각각 접속하여, 해당 게이트 서버(200) 내의 복수의 테이블에 데이터가 등록된 상태인지 여부를 확인할 수도 있다. 여기서, 상기 클라우드 포켓(300)은 복수의 클라우드 포켓(300) 중 어느 하나이고, 해당 특정 게이트 서버(200)와 통신하도록 미리 설정된 상태이며, 해당 클라우드 포켓(300)과 해당 특정 게이트 서버(200) 간의 연결은 해당 클라우드 포켓(300)에서만 해당 특정 게이트 서버(200)로 접속하는 단방향 통신일 수 있다.

[0095] 상기 확인 결과, 상기 복수의 테이블(또는 사서함) 중 적어도 하나의 테이블(또는 사서함)에 데이터가 등록된 상태인 경우, 상기 클라우드 포켓(300)은 해당 테이블(또는 사서함)에 등록된 데이터를 확인한다.

[0096] 즉, 상기 클라우드 포켓(300)은 루프(또는 스레드)를 돌면서 일정 시간 간격(또는 주기)으로 규칙적으로 해당 특정 게이트 서버(200)에 접속하고, 해당 클라우드 포켓(300)에서 처리할 작업(또는 데이터)이 있는지 여부를 확인한다. 여기서, 상기 클라우드 포켓(300)에서 처리할 작업은 임의의 사용자 단말(100) 등에서 상기 특정 게이트 서버(200) 내의 테이블에 등록된 데이터와 관련한 기능일 수 있다.

[0097] 또한, 상기 확인 결과, 상기 복수의 테이블(또는 사서함) 모두에 데이터가 등록되지 않은 상태인 경우, 상기 클라우드 포켓(300)은 다음 주기(또는 다음 스레드)에 다시 해당 특정 게이트 서버(200)와 연동하여, 해당 특정 게이트 서버(200) 내의 복수의 테이블에 데이터가 등록된 상태인지를 확인하는 과정을 수행한다.

[0098] 또한, 해당 데이터가 인증용 블록인 경우, 상기 클라우드 포켓(300)은 해당 특정 게이트 서버(200)와 연동하여, 상기 웹 서버에서 상기 특정 게이트 서버(200)에 등록한(또는 저장한) 인증용 블록과, 상기 사용자 단말(100)에서 상기 특정 게이트 서버(200)에 등록한(또는 저장한) 인증용 블록이 일치하는지 여부를 비교(또는 확인)한다. 여기서, 상기 클라우드 포켓(300)은 해당 데이터에 대해 구문 분석을 수행하고, 구문 분석 결과를 근거로 해당 데이터의 종류(또는 내용)를 확인하고, 상기 확인된 해당 데이터의 종류(또는 내용)를 근거로 해당 데이터가 아이디와 비밀번호를 포함하는 인증용 블록인지 여부를 확인할 수도 있다. 이때, 상기 클라우드 포켓(300)은 해당 데이터의 헤더(또는 해당 데이터에 포함된 추가 정보)를 근거로 해당 데이터가 인증용 블록인지 여부를 확인할 수도 있다.

[0099] 상기 비교 결과(또는 상기 확인 결과), 상기 웹 서버에서 해당 특정 게이트 서버(200)에 등록한(또는 저장한) 인증용 블록과 상기 사용자 단말(100)에서 해당 특정 게이트 서버(200)에 등록한(또는 저장한) 인증용 블록이 일치하지 않은 경우, 상기 클라우드 포켓(300)은 인증 실패 정보를 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록(또는 저장)하고, 해당 특정 게이트 서버(200)와의 연결을 종료한다. 여기서, 상기 클라우드 포켓(300)은 해당 특정 게이트 서버(200)의 해당 테이블에서 앞서 저장 중인 데이터(예를 들어 인증용 블록 등 포함)에 추가하여 상기 인증 실패 정보를 저장하거나 또는, 해당 테이블에 저장 중인 데이터를 삭제하고 상기 인증 실패 정보를 저장한다. 이때, 상기 클라우드 포켓(300)은 해당 특정 게이트 서버(200)의 복수의 테이블 중 서로 다른 테이블에 상기 인증 실패 정보, 상기 인증용 블록 등을 각각 저장할 수도 있다.

[0100] 또한, 상기 비교 결과(또는 상기 확인 결과), 상기 웹 서버에서 해당 특정 게이트 서버(200)에 등록한(또는 저장한) 인증용 블록과 상기 사용자 단말(100)에서 해당 특정 게이트 서버(200)에 등록한(또는 저장한) 인증용 블록이 일치하는 경우, 상기 클라우드 포켓(300)은 해당 인증용 블록에 포함된 아이디(또는 디바이스 아이디), 비밀번호 등을 확인한다.

[0101] 또한, 상기 클라우드 포켓(300)은 상기 확인된 아이디, 비밀번호, 현재 시각과 미리 설정된 유효 기간 등을 근거로 인증키를 생성(또는 발급)한다. 이때, 상기 인증키는 아이디(또는 디바이스 아이디), 비밀번호, 해당 인증키에 대한 유효 기간 정보를 포함하는 타임스탬프 등을 포함한다. 여기서, 상기 유효 기간은 미리 설정된 값(예를 들어 3분, 5분, 10분 등 포함)일 수 있다.

[0102] 또한, 상기 클라우드 포켓(300)은 사용자 계정 암호/복호키를 생성한다. 여기서, 상기 사용자 계정 암호/복호키는 미리 설정된 상태에서 사용하거나 또는 요청에 따라 생성하여 사용할 수 있으며, 열람 계정키(또는 복호키/복호화키), 수정 계정키(또는 암호키/암호화키), 연산키 등으로 구성(또는 포함)한다. 또한, 상기 사용자 계정 암호/복호키는 접속할 때 사용하는 계정키가 아니라, 암호화블록을 복호하거나 일반 데이터를 암호화할 때 사용하는 키이다. 또한, 클라우드 블록체인의 암호화 방법은 연산 처리 암호화 방법을 사용한다. 따라서, 2개의 키와 함께 연산키가 부가적으로 추가된다. 연산을 이용한 암호화 방법(또는 연산부호화 방식)은 이미 컴퓨터에서 많이 사용하는 방법으로 본 발명에서는 설명하지 않는다.

- [0103] 즉, 상기 클라우드 포켓(300)은 미리 설정된 크기(예를 들어 256 바이트*3)의 바이트 키(byte key)인 사용자 계정 암호/복호키를 생성하며, 해당 바이트 키는 키 단위가 바이트임을 나타낸다.
- [0104] 도 2에 도시된 바와 같이, 상기 클라우드 포켓(300)은 암호화된 데이터를 해석(또는 복호)하고자 할 때 사용하기 위한 미리 설정된 크기(예를 들어 256 바이트)의 열람 계정키와, 데이터를 암호화하고자 할 때 사용하기 위한 미리 설정된 크기(예를 들어 256 바이트)의 수정 계정키와, 연산부호화 방식을 사용하여 패턴으로 해석이 불가능하게 하기 위한 미리 설정된 크기(예를 들어 256 바이트)의 연산키로 구성된 상기 사용자 계정 암호/복호키를 생성한다.
- [0105] 본 발명의 실시예에서는 사용자 계정이 만들어지면(또는 해당 인증키가 생성되면/사용자 단말(100)에서 인증용 블록을 게이트 서버(200)에 등록하면), 상기 클라우드 포켓(300)에서 해당 사용자 계정 암호/복호키를 생성하는 것을 주로 설명하고 있으나, 이에 한정되는 것은 아니며, 상기 클라우드 포켓(300)은 전체 복수의 클라우드 포켓(300)에서 공용으로 사용하는 사용자 계정 암호/복호키를 미리 저장한 상태에서, 인증키 블록 생성에 해당 미리 저장된 사용자 계정 암호/복호키를 사용할 수도 있다.
- [0106] 또한, 상기 클라우드 포켓(300)은 상기 생성된 인증키와 상기 생성된 사용자 계정 암호/복호키를 포함하는 인증키 블록을 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록(또는 저장)한다. 여기서, 상기 클라우드 포켓(300)은 해당 특정 게이트 서버(200)의 해당 테이블에서 앞서 저장 중인 데이터(예를 들어 인증용 블록 등 포함)에 추가하여 상기 인증키 블록을 저장하거나 또는, 해당 테이블에 저장 중인 데이터를 삭제하고 상기 인증키 블록을 저장한다. 이때, 상기 클라우드 포켓(300)은 해당 특정 게이트 서버(200)의 복수의 테이블 중 서로 다른 테이블에 상기 인증키 블록, 상기 인증용 블록 등을 각각 저장할 수도 있다.
- [0107] 또한, 상기 클라우드 포켓(300)은 복수의 메인 서버(400) 중에서 해당 클라우드 포켓(300)과 연동하는 어느 하나의 메인 서버(400)와 연동하여, 해당 메인 서버(400)의 데이터베이스(미도시) 내의 복수의 테이블 중 어느 하나의 테이블 내의 어느 하나의 레코드에 해당 인증키 블록을 저장(또는 등록)한다. 이때, 상기 데이터베이스의 특정 테이블 내의 특정 레코드에 해당 인증키 블록이 저장됨에 따라, 상기 클라우드 포켓(300)은 해당 메인 서버(400)로부터 제공되는 사서함 번호(또는 해당 특정 테이블에 대응하는 사서함 번호)를 수신한다. 여기서, 상기 클라우드 포켓(300)은 미리 설정된 주기로 접속하는 상기 특정 게이트 서버(200) 내의 테이블에 상기 인증키 블록을 저장할 때, 상기 사서함 번호를 함께 저장할 수도 있다.
- [0108] 이와 같이, 상기 클라우드 포켓(300)과 상기 메인 서버(400)가 연결되어, 상기 클라우드 포켓(300)은 자신의 데이터 블록을 가지고 있고, 해당 데이터를 메인 서버(400)에 보내어 전체 흐름과 관리를 할 수 있다.
- [0109] 또한, 상기 클라우드 포켓(300)은 상기 미리 설정된 주기로 해당 특정 게이트 서버(200)와 연결(또는 통신/접속)한 후, 해당 특정 게이트 서버(200) 내의 복수의 테이블(또는 사서함)에 데이터(예를 들어 요구문 등 포함)가 등록된(또는 저장된) 상태인지 여부를 확인한다.
- [0110] 상기 확인 결과, 상기 복수의 테이블(또는 사서함) 중 적어도 하나의 테이블(또는 사서함)에 데이터가 등록된 상태인 경우, 상기 클라우드 포켓(300)은 해당 테이블(또는 사서함)에 등록된 데이터를 확인한다.
- [0111] 즉, 상기 클라우드 포켓(300)은 루프(또는 스레드)를 돌면서 일정 시간 간격(또는 주기)으로 규칙적으로 해당 특정 게이트 서버(200)에 접속하고, 해당 클라우드 포켓(300)에서 처리할 작업(또는 데이터)이 있는지 여부를 확인한다. 여기서, 상기 클라우드 포켓(300)에서 처리할 작업은 임의의 사용자 단말(100) 등에서 상기 특정 게이트 서버(200) 내의 테이블에 등록된 데이터와 관련한 기능일 수 있다.
- [0112] 또한, 상기 확인 결과, 상기 복수의 테이블(또는 사서함) 모두에 데이터가 등록되지 않은 상태인 경우, 상기 클라우드 포켓(300)은 다음 주기(또는 다음 스레드)에 다시 해당 특정 게이트 서버(200)와 연동하여, 해당 특정 게이트 서버(200) 내의 복수의 테이블에 데이터가 등록된 상태인지를 확인하는 과정을 수행한다.
- [0113] 또한, 해당 데이터가 요구문인 경우, 상기 클라우드 포켓(300)은 1차로 해당 요구문에 포함된 타임스탬프를 근거로 해당 데이터(또는 요구문)의 유효성을 검증(또는 판단)한다. 여기서, 상기 클라우드 포켓(300)은 해당 데이터에 대해 구문 분석을 수행하고, 구문 분석 결과를 근거로 해당 데이터의 종류(또는 내용)를 확인하고, 상기 확인된 해당 데이터의 종류(또는 내용)를 근거로 해당 데이터가 암호 블록, 인증키 등을 포함하는 요구문인지 여부를 확인할 수도 있다. 이때, 상기 클라우드 포켓(300)은 해당 데이터의 헤더(또는 해당 데이터에 포함된 추가 정보)를 근거로 해당 데이터가 요구문인지 여부를 확인할 수도 있다.
- [0114] 즉, 해당 데이터가 요구문인 경우, 상기 클라우드 포켓(300)은 해당 데이터(또는 요구문)의 유효성을 검증하기

위해서, 현재 시각과 해당 요구문에 포함된 타임스탬프를 근거로, 현재 시각과 해당 요구문에 포함된 타임스탬프 간의 시간 차이가 미리 설정된 기준값(예를 들어 3초, 5초, 10초 등 포함)을 지난 상태(또는 초과한 상태)인지 여부를 검증(또는 판단)한다.

[0115] 상기 데이터의 유효성 검증 결과(또는 상기 데이터/요구문의 유효성 판단 결과), 해당 요구문이 유효하지 않은 것으로 판단되는 경우, 상기 클라우드 포켓(300)은 해당 데이터의 유효성 검증이 실패한 상태임을 나타내는 정보를 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록(또는 저장)하고, 해당 특정 게이트 서버(200)와의 연결을 종료한다. 여기서, 상기 클라우드 포켓(300)은 해당 특정 게이트 서버(200)의 해당 테이블에서 앞서 저장 중인 데이터(예를 들어 인증 블록, 요구문 등 포함)에 추가하여 상기 데이터의 유효성 검증이 실패한 상태임을 나타내는 정보를 저장하거나 또는, 해당 테이블에 저장 중인 데이터를 삭제하고 상기 데이터의 유효성 검증이 실패한 상태임을 나타내는 정보를 저장한다. 이때, 상기 클라우드 포켓(300)은 해당 특정 게이트 서버(200)의 복수의 테이블 중 서로 다른 테이블에 상기 데이터의 유효성 검증이 실패한 상태임을 나타내는 정보, 상기 인증 블록, 상기 요구문 등을 각각 저장할 수도 있다.

[0116] 즉, 현재 시각과 해당 요구문에 포함된 타임스탬프 간의 시간 차이가 미리 설정된 기준값(예를 들어 3초, 5초, 10초 등 포함)을 지난 상태(또는 초과한 상태)인 경우, 상기 클라우드 포켓(300)은 해당 데이터의 유효성 검증이 실패한 상태임을 나타내는 정보를 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록(또는 저장)하고, 해당 특정 게이트 서버(200)와의 연결을 종료한다.

[0117] 또한, 상기 데이터의 유효성 검증 결과(또는 상기 데이터/요구문의 유효성 판단 결과), 해당 요구문이 유효한 것으로 판단되는 경우, 상기 클라우드 포켓(300)은 2차로 해당 요구문에 포함된 헤더값이 미리 설정된 규격(또는 조건)에 맞는지 여부(또는 충족하는지 여부)를 확인(또는 판단)한다. 여기서, 상기 헤더값은 해당 요구문에 포함된 암호 블록을 암호화하는 과정에서 생성된 값일 수 있다.

[0118] 즉, 현재 시각과 해당 요구문에 포함된 타임스탬프 간의 시간 차이가 미리 설정된 기준값(예를 들어 3초, 5초, 10초 등 포함)을 지나지 않은 상태(또는 초과하지 않은 상태)인 경우, 상기 클라우드 포켓(300)은 해당 요구문이 유효한 것으로 판단하고, 해당 요구문에 포함된 헤더값이 미리 설정된 규격(또는 조건)에 맞는지 여부를 2차로 확인(또는 판단)한다.

[0119] 상기 확인 결과(또는 상기 판단 결과), 해당 요구문에 포함된 헤더값이 미리 설정된 규격(또는 조건)에 맞지(또는 충족하지) 않는 경우, 상기 클라우드 포켓(300)은 해당 데이터의 규격 검증이 실패한 상태임을 나타내는 정보를 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록(또는 저장)하고, 해당 특정 게이트 서버(200)와의 연결을 종료한다. 여기서, 상기 클라우드 포켓(300)은 해당 특정 게이트 서버(200)의 해당 테이블에서 앞서 저장 중인 데이터(예를 들어 인증 블록, 요구문 등 포함)에 추가하여 상기 데이터의 규격 검증이 실패한 상태임을 나타내는 정보를 저장하거나 또는, 해당 테이블에 저장 중인 데이터를 삭제하고 상기 데이터의 규격 검증이 실패한 상태임을 나타내는 정보를 저장한다. 이때, 상기 클라우드 포켓(300)은 해당 특정 게이트 서버(200)의 복수의 테이블 중 서로 다른 테이블에 상기 데이터의 규격 검증이 실패한 상태임을 나타내는 정보, 상기 인증 블록, 상기 요구문 등을 각각 저장할 수도 있다.

[0120] 또한, 상기 확인 결과(또는 상기 판단 결과), 해당 요구문에 포함된 헤더값이 미리 설정된 규격(또는 조건)에 맞는지(또는 충족하는) 경우, 상기 클라우드 포켓(200)은 3차로 해당 요구문에 포함된 암호 블록을 미리 설정된 사용자 계정 암호/복호키(또는 앞서 해당 사용자 단말(100)과 관련한 인증용 블록을 근거로 생성된 사용자 계정 암호/복호키)를 이용해서 복호하여, 원본 데이터를 생성(또는 복원)한다.

[0121] 즉, 2차 해당 데이터의 규격 검증 결과, 해당 요구문에 포함된 헤더값이 미리 설정된 규격(또는 조건)에 맞는지(또는 충족하는) 경우, 상기 클라우드 포켓(200)은 해당 요구문을 인증키와 암호 블록으로 분리하고, 상기 분리된 암호 블록을 상기 사용자 계정 암호/복호키를 이용해서 복호하여, 원본 데이터를 생성(또는 복원)한다.

[0122] 또한, 상기 클라우드 포켓(300)은 해당 원본 데이터 등을 근거로 클라우드 블록체인에서 블록 생성 기능, 블록 수정 기능, 블록 조회 기능(또는 블록 내용 조회 기능) 등을 수행한다.

[0123] 즉, 상기 클라우드 포켓(300)은 해당 원본 데이터에 대해서 구문 분석(또는 파싱)을 수행하고, 구문 분석(또는 구문 분석 결과)에 따라 해당 원본 데이터의 의미(또는 내용)를 파악한다.

[0124] 또한, 상기 요구문에 포함된 요구사항이 새로운 블록 생성 요청인 경우(또는 해당 파악된 의미/내용이 새로운 블록 생성 요청인 경우), 상기 클라우드 포켓(300)은 해당 클라우드 포켓(300)에서 관리 중인 포켓 서버 리스트

중에서 해당 클라우드 포켓(300)에서의 블록 생성인지 확인한다.

- [0125] 즉, 상기 클라우드 포켓(300)은 해당 새로운 블록 생성 요청이 로컬 서버인 해당 클라우드 포켓(300)에서 수행해야 하는 작업(또는 기능)인지 여부를 상기 포켓 서버 리스트를 통해 확인한다. 여기서, 상기 포켓 서버 리스트는 사용자 계정에 대응하는 지갑(또는 암호화폐/가상화폐 지갑)이 어느 클라우드 포켓(300)에서 저장(또는 관리) 중인지에 대한 정보를 포함하며, 지갑 정보별 클라우드 포켓 정보(또는 클라우드 포켓(300)의 주소/URL)를 포함한다.
- [0126] 상기 확인 결과, 해당 클라우드 포켓(300)에서의 블록 생성인 경우, 상기 클라우드 포켓(300)은 클라우드 블록 체인에서 해당 원본 데이터를 근거로 블록 생성 기능을 수행한다.
- [0127] 즉, 상기 확인 결과, 해당 새로운 블록 생성 요청이 해당 요구문을 확인한 로컬 서버인 해당 클라우드 포켓(300)에서 수행해야 하는 작업(또는 기능)인 것으로 확인되는 경우, 상기 클라우드 포켓(300)은 해당 클라우드 포켓(300)에서 해당 원본 데이터를 근거로 블록 생성 기능을 수행한다. 이때, 상기 클라우드 포켓(300)은 해당 요구문과 관련한 사용자의 지갑을 새로 생성하고, 새로 생성된 지갑과 관련한 정보를 관리하는 블록 생성 기능을 수행할 수도 있다.
- [0128] 또한, 상기 클라우드 포켓(300)은 신규 블록 생성과 관련한 블록 생성 기능 수행 결과를 업데이트(또는 해당 클라우드 블록체인에서의 신규 블록 생성에 따른 업데이트)한다.
- [0129] 또한, 상기 클라우드 포켓(300)은 스레드를 이용해서, 전체 클라우드 포켓(300) 중에서 해당 클라우드 포켓(300)을 제외한 나머지 클라우드 포켓(300)에 해당 신규 블록 생성과 관련한 블록 생성 기능 수행 결과를 각각 업데이트한다.
- [0130] 또한, 상기 확인 결과, 다른 클라우드 포켓(300)에서의 블록 생성인 경우(또는 해당 요구문을 확인한 로컬 서버에서의 블록 생성이 아닌 경우), 상기 클라우드 포켓(300)은 해당 클라우드 포켓(300)에서 관리 중인 포켓 서버 리스트를 근거로 해당 블록 생성 기능 수행을 위한 담당인 다른 클라우드 포켓(300)을 확인하고, 상기 확인된 다른 클라우드 포켓(300)에 해당 요구문(또는 원본 데이터)을 제공한다.
- [0131] 이에 따라, 다른 클라우드 포켓(300)은 클라우드 블록체인에서 해당 요구문(또는 원본 데이터)을 근거로 블록 생성 기능을 수행한다. 이때, 상기 다른 클라우드 포켓(300)은 해당 요구문과 관련한 사용자의 지갑을 새로 생성하고, 새로 생성된 지갑과 관련한 정보를 관리하는 블록 생성 기능을 수행할 수도 있다.
- [0132] 또한, 블록 생성 기능 수행을 완료한 후, 상기 클라우드 포켓(300)은 신규 블록 생성과 관련한 블록 생성 기능 수행 결과(또는 상기 다른 클라우드 포켓(300)에서의 신규 블록 생성과 관련한 블록 생성 기능 수행 결과)를 업데이트(또는 해당 클라우드 블록체인에서의 신규 블록 생성에 따른 업데이트)한다. 이때, 상기 클라우드 포켓(300)은 해당 요구문에 따라 새로 생성한 사용자의 지갑에 대한 결과 정보를 업데이트할 수 있다.
- [0133] 또한, 상기 클라우드 포켓(300)은 스레드를 이용해서, 전체 클라우드 포켓(300) 중에서 해당 클라우드 포켓(300)을 제외한 나머지 클라우드 포켓(300)에 해당 신규 블록 생성과 관련한 블록 생성 기능 수행 결과를 각각 업데이트한다.
- [0134] 이때, 상기 다른 클라우드 포켓(300)은 해당 신규 블록 생성과 관련한 블록 생성 기능 수행 결과를 해당 다른 클라우드 포켓(300)에서 업데이트하고, 스레드를 이용해서, 전체 클라우드 포켓(300) 중에서 해당 다른 클라우드 포켓(300)을 제외한 나머지 클라우드 포켓(300)에 해당 신규 블록 생성과 관련한 블록 생성 기능 수행 결과를 각각 업데이트할 수도 있다.
- [0135] 또한, 상기 요구문에 포함된 요구사항이 블록 수정 요청인 경우(또는 해당 파악된 의미가 블록 수정 요청인 경우), 상기 클라우드 포켓(300)은 해당 클라우드 포켓(300)에서 관리 중인 포켓 서버 리스트를 근거로 1차 수정 클라우드 포켓(300)이 로컬인지 여부를 확인한다.
- [0136] 즉, 상기 클라우드 포켓(300)은 해당 블록 수정 요청과 관련해서 1차 수정 클라우드 포켓(300)이 로컬 서버인 해당 클라우드 포켓(300)에서 수행해야 하는 작업(또는 기능)인지 여부를 상기 포켓 서버 리스트를 통해 확인한다.
- [0137] 상기 확인 결과, 해당 클라우드 포켓(300)에서 1차 수정을 진행해야 하는 경우, 상기 클라우드 포켓(300)은 클라우드 블록체인에서 해당 원본 데이터를 근거로 1차 블록 수정 기능을 수행한다. 여기서, 상기 1차 블록 수정 기능은 대상자를 대상으로 하는 블록 수정 기능을 나타낸다.

- [0138] 즉, 상기 확인 결과, 1차 수정 클라우드 포켓(300)이 해당 요구문을 확인한 로컬 서버인 해당 클라우드 포켓(300)에서 수행해야 하는 작업(또는 기능)인 것으로 확인되는 경우, 상기 클라우드 포켓(300)은 해당 클라우드 블록체인에서 해당 원본 데이터를 근거로 1차 블록 수정 기능을 수행한다. 이때, 상기 클라우드 포켓(300)은 해당 요구문과 관련한 사용자의 지갑에서 해당 요구문에 포함된 암호화폐 수량만큼을 차감하는 블록 수정 기능을 수행할 수도 있다.
- [0139] 또한, 상기 확인 결과, 다른 클라우드 포켓(300)에서의 1차 수정을 진행해야 하는 경우(또는 해당 요구문을 확인한 로컬 서버에서의 1차 블록 수정이 아닌 경우), 상기 클라우드 포켓(300)은 해당 클라우드 포켓(300)에서 관리 중인 포켓 서버 리스트를 근거로 1차 블록 수정 기능 수행을 위한 담당인 다른 클라우드 포켓(300)을 확인하고, 상기 확인된 다른 클라우드 포켓(300)에 해당 요구문(또는 원본 데이터)을 제공한다.
- [0140] 이에 따라, 다른 클라우드 포켓(300)은 클라우드 블록체인에서 해당 요구문(또는 원본 데이터)을 근거로 1차 블록 수정 기능을 수행한다. 이때, 상기 다른 클라우드 포켓(300)은 해당 요구문과 관련한 사용자의 지갑에서 해당 요구문에 포함된 암호화폐 수량만큼을 차감하는 블록 수정 기능을 수행할 수도 있다.
- [0141] 또한, 상기 클라우드 포켓(300)은 상기 다른 클라우드 포켓(300)과 연동하여, 해당 다른 클라우드 포켓(300)에서의 1차 블록 수정 기능 수행의 완료 여부를 파악(또는 확인)한다.
- [0142] 또한, 해당 1차 블록 수정 기능이 완료된 후, 상기 클라우드 포켓(300)은 해당 클라우드 포켓(300)에서 관리 중인 포켓 서버 리스트를 근거로 2차 수정 클라우드 포켓(300)이 로컬인지 여부를 확인한다.
- [0143] 즉, 상기 클라우드 포켓(300)은 해당 블록 수정 요청과 관련해서 2차 수정 클라우드 포켓(300)이 로컬 서버인 해당 클라우드 포켓(300)에서 수행해야 하는 작업(또는 기능)인지 여부를 상기 포켓 서버 리스트를 통해 판단한다.
- [0144] 상기 판단 결과, 해당 클라우드 포켓(300)에서 2차 수정을 진행해야 하는 경우, 상기 클라우드 포켓(300)은 클라우드 블록체인에서 해당 원본 데이터를 근거로 2차 블록 수정 기능을 수행한다. 여기서, 상기 2차 블록 수정 기능은 피대상자를 대상으로 하는 블록 수정 기능을 나타낸다.
- [0145] 즉, 상기 판단 결과, 2차 수정 클라우드 포켓(300)이 해당 요구문을 확인한 로컬 서버인 해당 클라우드 포켓(300)에서 수행해야 하는 작업(또는 기능)인 것으로 판단되는 경우, 상기 클라우드 포켓(300)은 해당 클라우드 블록체인에서 해당 원본 데이터를 근거로 2차 블록 수정 기능을 수행한다. 이때, 상기 다른 클라우드 포켓(300)은 해당 요구문과 관련한 사용자의 지갑에서 해당 요구문에 포함된 암호화폐 수량만큼을 차감하는 블록 수정 기능을 수행할 수도 있다.
- [0146] 또한, 상기 판단 결과, 또 다른 클라우드 포켓(300)에서의 2차 수정을 진행해야 하는 경우(또는 해당 요구문을 확인한 로컬 서버에서의 2차 블록 수정이 아닌 경우), 상기 클라우드 포켓(300)은 해당 클라우드 포켓(300)에서 관리 중인 포켓 서버 리스트를 근거로 2차 블록 수정 기능 수행을 위한 담당인 또 다른 클라우드 포켓(300)을 확인하고, 상기 확인된 또 다른 클라우드 포켓(300)에 해당 요구문(또는 원본 데이터)을 제공한다.
- [0147] 이에 따라, 또 다른 클라우드 포켓(300)은 클라우드 블록체인에서 해당 요구문(또는 원본 데이터)을 근거로 2차 블록 수정 기능을 수행한다. 이때, 상기 또 다른 클라우드 포켓(300)은 해당 요구문과 관련한 사용자의 지갑에서 해당 요구문에 포함된 암호화폐 수량만큼을 차감하는 블록 수정 기능을 수행할 수도 있다.
- [0148] 또한, 상기 클라우드 포켓(300)은 상기 또 다른 클라우드 포켓(300)과 연동하여, 해당 또 다른 클라우드 포켓(300)에서의 2차 블록 수정 기능 수행의 완료 여부를 파악(또는 확인)한다.
- [0149] 또한, 1차 및 2차에 걸친 블록 수정 기능 수행을 완료한 후, 상기 클라우드 포켓(300)은 블록 수정과 관련한 블록 수정 기능 수행 결과(또는 해당 클라우드 포켓(300), 해당 다른 클라우드 포켓(300), 해당 또 다른 클라우드 포켓(300) 등에서의 블록 수정 기능 수행 결과)를 업데이트(또는 해당 클라우드 블록체인에서의 블록 수정에 따른 업데이트)한다. 이때, 상기 클라우드 포켓(300)은 해당 요구문을 근거로 암호화폐의 이체에 따라 대상자와 피대상자의 지갑에 대한 변동 사항에 대한 결과 정보를 업데이트할 수 있다.
- [0150] 또한, 상기 클라우드 포켓(300)은 스레드를 이용해서, 전체 클라우드 포켓(300) 중에서 해당 클라우드 포켓(300)을 제외한 나머지 클라우드 포켓(300)에 해당 블록 수정과 관련한 블록 수정 기능 수행 결과를 각각 업데이트한다.
- [0151] 이와 같이, 상기 요구문에 포함된 요구사항이 블록 수정 요청인 경우(또는 해당 파악된 의미가 블록 수정 요청

인 경우/코인을 송신하고자 하는 경우), 송신자 블록이 저장된 클라우드 포켓(300)과 수신자 블록이 저장된 클라우드 포켓(300)에서 우선적으로 수정할 수 있게 블록체인 연결 순서를 정한 후, 송신자 블록이 저장된 클라우드 포켓(300)과 수신자 블록이 저장된 클라우드 포켓(300)에서의 수정 기능이 완료되면, 상기 복수의 클라우드 포켓(300) 중 나머지 모든 클라우드 포켓(300)에서 해당 블록 수정 기능 수행 결과를 각각 업데이트하도록 구성하여, 불특정 다수의 랜덤 PtoP 방식의 기존 블록체인 연결과는 다른 방법을 적용한다.

- [0152] 또한, 상기 요구문에 포함된 요구사항이 블록 조회 요청인 경우(또는 해당 파악된 의미가 블록 조회 요청인 경우), 상기 클라우드 포켓(300)은 해당 클라우드 포켓(300)에서 관리 중인 포켓 서버 리스트 중에서 해당 클라우드 포켓(300)에서의 블록 조회인지 확인한다.
- [0153] 즉, 상기 클라우드 포켓(300)은 해당 블록 조회 요청이 로컬 서버인 해당 클라우드 포켓(300)에서 수행해야 하는 작업(또는 기능)인지 여부를 상기 포켓 서버 리스트를 통해 확인한다.
- [0154] 상기 확인 결과, 해당 클라우드 포켓(300)에서의 블록 조회인 경우, 상기 클라우드 포켓(300)은 클라우드 블록체인에서 해당 블록 조회 요청에 대응하는 정보(또는 해당 블록 내의 정보/데이터)를 확인하는 기능을 수행한다.
- [0155] 즉, 상기 확인 결과, 해당 블록 조회 요청이 해당 요구문을 확인한 로컬 서버인 해당 클라우드 포켓(300)에서 수행해야 하는 작업(또는 기능)인 것으로 확인되는 경우, 상기 클라우드 포켓(300)은 해당 클라우드 블록체인에서 해당 원본 데이터를 근거로 블록 조회 기능을 수행한다. 이때, 상기 클라우드 포켓(300)은 해당 요구문과 관련한 사용자의 지갑에 남아 있는 잔액을 확인하는 조회 기능을 수행할 수 있다.
- [0156] 또한, 상기 클라우드 포켓(300)은 블록 조회와 관련한 블록 조회 기능 수행 결과를 업데이트(또는 해당 클라우드 블록체인에서의 블록 조회에 따른 업데이트)한다.
- [0157] 또한, 상기 클라우드 포켓(300)은 스레드를 이용해서, 전체 클라우드 포켓(300) 중에서 해당 클라우드 포켓(300)을 제외한 나머지 클라우드 포켓(300)에 해당 블록 조회와 관련한 블록 조회 기능 수행 결과를 각각 업데이트한다.
- [0158] 또한, 상기 확인 결과, 다른 클라우드 포켓(300)에서의 블록 조회인 경우(또는 해당 요구문을 확인한 로컬 서버에서의 블록 조회가 아닌 경우), 상기 클라우드 포켓(300)은 해당 클라우드 포켓(300)에서 관리 중인 포켓 서버 리스트를 근거로 해당 블록 조회 기능 수행을 위한 담당인 다른 클라우드 포켓(300)을 확인하고, 상기 확인된 다른 클라우드 포켓(300)에 해당 요구문(또는 원본 데이터)을 제공한다.
- [0159] 이에 따라, 다른 클라우드 포켓(300)은 클라우드 블록체인에서 해당 요구문(또는 원본 데이터)을 근거로 블록 조회 기능을 수행한다. 이때, 상기 다른 클라우드 포켓(300)은 해당 요구문과 관련한 사용자의 지갑에 남아 있는 잔액을 확인하는 조회 기능을 수행할 수 있다.
- [0160] 또한, 블록 조회 기능 수행을 완료한 후, 상기 클라우드 포켓(300)은 블록 조회와 관련한 블록 조회 기능 수행 결과를 업데이트(또는 상기 다른 클라우드 포켓(300)에서의 블록 조회와 관련한 블록 조회 기능 수행 결과)를 업데이트(또는 해당 클라우드 블록체인에서의 블록 조회에 따른 업데이트)한다. 이때, 상기 클라우드 포켓(300)은 해당 요구문에 따라 해당 사용자의 지갑에 남아 있는 잔액에 대한 정보를 업데이트할 수 있다.
- [0161] 또한, 상기 클라우드 포켓(300)은 스레드를 이용해서, 전체 클라우드 포켓(300) 중에서 해당 클라우드 포켓(300)을 제외한 나머지 클라우드 포켓(300)에 해당 블록 조회와 관련한 블록 조회 기능 수행 결과를 각각 업데이트한다.
- [0162] 이때, 상기 다른 클라우드 포켓(300)은 해당 블록 조회와 관련한 블록 조회 기능 수행 결과를 해당 다른 클라우드 포켓(300)에서 업데이트하고, 스레드를 이용해서, 전체 클라우드 포켓(300) 중에서 해당 다른 클라우드 포켓(300)을 제외한 나머지 클라우드 포켓(300)에 해당 블록 조회와 관련한 블록 조회 기능 수행 결과를 각각 업데이트할 수도 있다.
- [0163] 이와 같이, 상기 클라우드 포켓(300)은 블록체인(또는 클라우드 블록체인)을 복수의 클라우드 포켓(300)을 통해 구현하여, 해킹 등의 위험성을 줄일 수 있다.
- [0164] 또한, 상기 클라우드 포켓(300)은 미리 설정된 주기로 해당 특정 게이트 서버(200)와 연결(또는 통신/접속)한 후, 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 해당 요구문에 대응하는 기능 수행 결과(예를 들어 블록 생성 기능 수행 결과, 블록 수정 기능 수행 결과, 블록 조회 기능 수행 결과 등 포함)를 등록(또는

저장)한다. 여기서, 상기 클라우드 포켓(300)은 해당 특정 게이트 서버(200) 내의 복수의 테이블 중에서 앞서 사용자 단말(100과 관련하여 데이터(예를 들어 인증용 블록, 인증키 블록, 요구문 등 포함)를 등록한 테이블에 해당 기능 수행 결과를 저장하거나 또는, 해당 테이블에 저장 중인 데이터를 삭제하고 해당 요구문에 대응하는 기능 수행 결과를 저장한다. 이때, 상기 클라우드 포켓(300)은 해당 특정 게이트 서버(200)의 복수의 테이블 중 서로 다른 테이블에 상기 인증용 블록, 상기 인증키 블록, 상기 요구문, 상기 기능 수행 결과 등을 각각 저장할 수도 있다.

[0165] 이와 같이, 현재의 블록체인 기반 가상화폐의 경우 화폐의 기능을 하기에 다소 부적절한 반면, 상기 클라우드 포켓(300)(또는 클라우드 블록체인 시스템(10))은 블록체인의 장점을 가지면서, 화폐의 기능이 가능하게 구성하였다.

[0166] 또한, 상기 클라우드 블록체인 시스템(10)은 실시간 수정, 송신, 생성할 수 있고, 통화량 제어가 가능하고, 화폐의 흐름을 추적할 수 있다.

[0167] 또한, 상기 클라우드 포켓(300)은 복수의 메인 서버(400) 중에서 어느 하나의 메인 서버(400)와 연결(또는 접속/통신)하고, 상기 연결된 메인 서버(400)에 기능 수행 결과(예를 들어 블록 생성 기능 수행 결과, 블록 수정 기능 수행 결과, 블록 조회 기능 수행 결과 등 포함)를 해당 메인 서버(400) 내의 데이터베이스(미도시) 내의 특정 테이블에 저장(또는 등록)한다.

[0168] 또한, 상기 클라우드 포켓(300)은 상기 메인 서버(400)로부터 제공되는 해당 기능 수행 결과가 저장된 특정 테이블과 관련한 특정 사서함 번호를 수신한다.

[0169] 또한, 상기 클라우드 포켓(300)은 미리 설정된 주기로 해당 특정 게이트 서버(200)와 연결(또는 통신/접속)한 후, 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 해당 특정 사서함 번호를 등록(또는 저장)한다. 여기서, 상기 클라우드 포켓(300)은 상기 특정 게이트 서버(200) 내의 복수의 테이블(또는 사서함) 중에서 앞서 사용자 단말(100)과 관련해서 데이터(예를 들어 인증용 블록, 인증키 블록, 요구문 등 포함)를 등록한 테이블에 해당 특정 사서함 번호를 누적하여 저장하거나 또는, 해당 테이블을 초기화하고 해당 특정 사서함 번호를 저장할 수도 있다. 이때, 상기 클라우드 포켓(300)은 해당 특정 게이트 서버(200)의 복수의 테이블 중에서 서로 다른 테이블에 상기 인증용 블록, 상기 인증키 블록, 상기 요구문, 상기 특정 사서함 번호 등을 각각 저장할 수도 있다.

[0170] 상기 메인 서버(400)는 상기 복수의 클라우드 포켓(300)과 통신한다. 여기서, 상기 메인 서버(400)는 복수로 구성하며, 복수의 메인 서버(400)는 각 메인 서버(400)에 저장되는 데이터를 공유한다. 이때, 상기 복수의 메인 서버(400)는 각각의 메인 서버(400)에 저장(또는 등록)하는 데이터에 대해서, 서로 공유(또는 데이터 동기화)할 수 있다.

[0171] 또한, 상기 메인 서버(400)는 데이터베이스 서버(미도시)로 구성(또는 포함)한다.

[0172] 또한, 상기 메인 서버(400)는 상기 복수의 클라우드 포켓(300) 중 적어도 하나의 클라우드 포켓(300)과 연결(또는 접속/통신)한다. 여기서, 상기 클라우드 포켓(300)과 상기 메인 서버(400) 간의 연결은 양방향 통신으로 구성하고, 미리 설정된 TCP/IP 프로토콜을 이용하여 통신한다. 이때, 해당 TCP/IP 프로토콜은 자체 제작하여 프로토콜 정보를 비공개이다.

[0173] 또한, 상기 메인 서버(400)는 일반 공인 서버(예를 들어 HTTP, TELNET, FTP 등 포함)를 절대 사용하지 않아, 외부에서 공인된 프로토콜로 접속할 수 없도록 구성한다.

[0174] 또한, 상기 메인 서버(400)는 상기 클라우드 포켓(300)과 양방향 통신으로 연결되며, 서버-클라이언트 구조에서 서버는 메인 서버(400)이고, 클라이언트는 클라우드 포켓(300)으로 구성한다.

[0175] 또한, 상기 메인 서버(400)는 TCP/IP로 연결할 때, 연결 포트 번호도 비공개한다.

[0176] 즉, 상기 메인 서버(400)는 상기 클라우드 포켓(300) 외에 다른 접속을 허가하지 않는다.

[0177] 또한, 상기 메인 서버(400)에서 보안 기능을 하는 것은 해당 메인 서버(400)의 IP 주소와 포트 번호, 상기 클라우드 포켓(300)의 디바이스 인증과 프로토콜 등이다.

[0178] 또한, 상기 메인 서버(400)는 외부에서 접속이 되지 않기에, 데이터를 암호화하지 않은 상태에서, 상기 클라우드 포켓(300)과 데이터(또는 정보)를 송/수신한다.

- [0179] 또한, 도 3에 도시된 바와 같이, 상기 메인 서버(400)는 사서함 번호와 해당 사서함 번호에 대응하는 테이블로 구성된 데이터베이스를 관리한다.
- [0180] 즉, 상기 메인 서버(400)는 어느 데이터베이스의 어느 테이블의 어디 레코드를 읽거나 수정하는 기능을 수행한다.
- [0181] 예를 들어, 상기 도 3에 도시된 바와 같이, 상기 메인 서버(400)는 1번 사서함 번호(또는 제 1 사서함에 대응하는 사서함 번호)와 관련해서 member 테이블을 매칭하고, 외부의 장치(300)에서 해당 member 테이블명을 사용하지 않고, 사서함 번호 1번을 이용하여 해당 메인 서버(400)의 member 테이블의 레코드에 접근하도록 구성하고, 해당 메인 서버(400) 내에서는 해당 사서함 번호에 대응하는 테이블(또는 테이블명)을 사용하도록 구성한다.
- [0182] 또한, 상기 메인 서버(400)는 상기 클라우드 포켓(300)과 연동하여, 해당 클라우드 포켓(300)에서의 특정 요구문에 대한 기능 수행 결과(예를 들어 블록 생성 기능 수행 결과, 블록 수정 기능 수행 결과, 블록 조회 기능 수행 결과 등 포함)를 해당 메인 서버(400) 내의 데이터베이스 내의 특정 테이블에 저장(또는 등록)한다.
- [0183] 또한, 상기 메인 서버(400)는 해당 기능 수행 결과가 저장된 특정 테이블에 대응하는 특정 사서함 번호를 상기 클라우드 포켓(300)에 제공한다. 이때, 상기 메인 서버(400)는 해당 메인 서버(400)의 데이터베이스에서의 기능 수행 결과가 저장된 테이블과 관련한 정보를 상기 클라우드 포켓(300)에 직접 제공하는 대신에, 해당 테이블에 대응하여 미리 설정된 사서함 번호를 상기 클라우드 포켓(300)에 제공하여, 해당 클라우드 포켓(300)에서는 상기 메인 서버(400)의 데이터베이스에 저장되는 데이터(또는 기능 수행 결과)와 관련한 직접적인 정보를 확인하지 못하도록 구성할 수 있다.
- [0184] 또한, 상기 메인 서버(400)는 복수의 메인 서버(400) 중에서 해당 어느 하나의 메인 서버(400)를 제외한 나머지 메인 서버(400)와 각각 연동하여, 기능 수행 결과(예를 들어 블록 생성 기능 수행 결과, 블록 수정 기능 수행 결과, 블록 조회 기능 수행 결과 등 포함)를 나머지 메인 서버(400)에 각각 구성된 데이터베이스에 각각 저장(또는 공유/등록/업데이트)한다.
- [0185] 이와 같이, 상기 메인 서버(400)는 다음과 같은 특징으로 외부 해킹의 침입을 막을 수 있다.
- [0186] 1. 메인 서버는 1개의 포트만 열어두며, 해당 포트 번호는 비공개로 외부에서 알 수 없다.
- [0187] 2. 메인 서버는 외부에 알려지지 않은 자체 프로토콜을 사용한다.
- [0188] 3. 메인 서버는 클라우드 포켓 연결 외에 다른 TCP/IP 통신이 연결되어 있지 않다. SSH, TFTP조차 연결되어 있지 않기에, 외부 해킹이 공인 프로토콜을 사용하여 접근할 수 없다.
- [0189] 4. 메인 서버 간의 통신은 하나의 포트를 이용하여 한다. 단, 이 통신은 메인 서버 URL만 허용하고, 다른 외부 접속은 원천 차단한다.
- [0190] 이와 같이, 사용자 단말에서 원본 데이터를 인증키를 이용해서 암호화하여 암호 블록을 생성하고, 암호 블록과 타임스탬프를 포함하는 요구 정보를 게이트 서버에 등록하고, 클라우드 포켓에서 게이트 서버에 접속하여 요구 정보를 확인한 후, 요구 정보에 포함된 암호 블록을 복호하여 원본 데이터를 복원하고, 블록체인에 새로운 블록으로 해당 원본 데이터를 저장하거나, 기존 데이터를 해당 원본 데이터로 수정할 수 있다.
- [0191] 또한, 이와 같이, 사용자 단말에서 웹 서버로 아이디와 비밀번호를 이용해서 로그인한 후, 요청에 따라 웹 서버에서 제공하는 인증용 블록을 수신하고, 수신된 인증용 블록을 게이트 서버에 등록한 후, 클라우드 포켓에서 사용자 단말이 게이트 서버에 등록한 인증용 블록과 웹 서버가 게이트 서버에 등록한 인증용 블록 간의 일치 여부 확인에 따라 인증 여부를 확인한 후, 인증에 성공한 경우 유효 기간이 설정된 인증키를 생성하여 게이트 서버에 등록하고, 사용자 단말에서 게이트 서버에 등록된 인증키를 이용해서 게이트 서버 및 클라우드 포켓과 연동하여 원본 데이터를 블록 형태로 클라우드 블록체인에 등록할 수 있다.
- [0192] 이하에서는, 본 발명에 따른 클라우드 블록체인 시스템의 제어 방법을 도 1 내지 도 6을 참조하여 상세히 설명한다.
- [0193] 도 4 내지 도 6은 본 발명의 실시예에 따른 클라우드 블록체인 시스템의 제어 방법을 나타낸 흐름도이다.
- [0194] 먼저, 사용자 단말(100)은 웹 서버(미도시)로 아이디(또는 해당 사용자 단말(100)의 디바이스 아이디)와 비밀번호(또는 패스워드)를 이용해서 로그인(또는 접속/연결)한다. 이때, 상기 사용자 단말(100)은 해당 웹 서버에서 제공하는 서비스를 이용하기 위한 사용자로 회원 가입한 상태일 수 있다.

- [0195] 또한, 상기 사용자 단말(100)은 해당 사용자 단말(100)의 사용자의 요청에 따른 상기 웹 서버로 인증용 블록 생성을 요청한다.
- [0196] 또한, 상기 웹 서버는 상기 사용자 단말(100)의 인증용 블록 생성 요청(또는 인증용 블록 생성 요청 정보)에 따라, 상기 사용자 단말(100)과 관련한 아이디(또는 해당 사용자 단말(100)의 디바이스 아이디)와 비밀번호로 구성된 인증용 블록을 생성하고, 상기 생성된 인증용 블록을 상기 사용자 단말(100)에 제공(또는 전송)한다.
- [0197] 또한, 상기 웹 서버는 상기 생성된 인증용 블록을 해당 웹 서버와 연동하는 게이트 서버(200)(또는 해당 게이트 서버(200) 내의 복수의 테이블 중 임의의 테이블)에 등록(또는 저장)한다. 이때, 상기 게이트 서버(200)는 해당 웹 서버로부터 제공되는 인증용 블록을 해당 게이트 서버(200) 내의 복수의 테이블(또는 복수의 사서함) 중에서도 어느 하나의 테이블에 등록(또는 저장)한다.
- [0198] 또한, 상기 게이트 서버(200)는 전체 복수의 게이트 서버(200) 중에서 해당 게이트 서버(200)를 제외한 나머지 게이트 서버(200)와 각각 연동하여, 상기 인증용 블록을 나머지 게이트 서버(200)에 각각 저장(또는 등록/업데이트)하도록 구성한다.
- [0199] 일 예로, 제 1 사용자 단말(100)은 가상화폐(또는 암호화폐)를 거래하는 제 1 웹 서버(미도시)에 해당 제 1 사용자 단말의 제 1 아이디와 제 1 비밀번호를 이용해서 로그인하고, 제 1 인증용 블록 생성 요청 정보를 상기 제 1 웹 서버에 전송한다.
- [0200] 또한, 상기 제 1 웹 서버는 상기 제 1 사용자 단말로부터 전송되는 제 1 인증용 블록 생성 요청 정보를 수신하고, 상기 수신된 제 1 인증용 블록 생성 요청 정보를 근거로 상기 제 1 아이디 및 제 1 비밀번호로 구성된 제 1 인증용 블록을 생성하고, 상기 생성된 제 1 인증용 블록을 상기 제 1 사용자 단말에 전송한다.
- [0201] 또한, 상기 제 1 웹 서버는 상기 생성된 제 1 인증용 블록을 복수의 게이트 서버(200) 중에서 해당 제 1 웹 서버와 연동하는 제 2 게이트 서버(200)에 저장한다.
- [0202] 다른 일 예로, 제 2 사용자 단말(100)은 가상화폐(또는 암호화폐)를 거래하는 제 2 웹 서버에 해당 제 2 사용자 단말의 제 2 아이디와 제 2 비밀번호를 이용해서 로그인하고, 제 2 인증용 블록 생성 요청 정보를 상기 제 2 웹 서버에 전송한다.
- [0203] 또한, 상기 제 2 웹 서버는 상기 제 2 사용자 단말로부터 전송되는 제 2 인증용 블록 생성 요청 정보를 수신하고, 상기 수신된 제 2 인증용 블록 생성 요청 정보를 근거로 상기 제 2 아이디 및 제 2 비밀번호로 구성된 제 2 인증용 블록을 생성하고, 상기 생성된 제 2 인증용 블록을 상기 제 2 사용자 단말에 전송한다.
- [0204] 또한, 상기 제 2 웹 서버는 상기 생성된 제 2 인증용 블록을 복수의 게이트 서버(200) 중에서 해당 제 2 웹 서버와 연동하는 제 23 게이트 서버(200)에 저장한다(S410).
- [0205] 이후, 상기 사용자 단말(100)은 앞선 인증용 블록 생성 요청(또는 인증용 블록 생성 요청 정보)에 응답하여 상기 웹 서버로부터 제공되는(또는 전송되는) 인증용 블록을 수신한다.
- [0206] 또한, 상기 사용자 단말(100)은 클라우드 포켓(300)으로부터 인증키(또는 인증키 블록)를 발급받기 위해서, 복수의 게이트 서버(200) 중 어느 하나의 특정 게이트 서버(200)에 접속(또는 연결)한다. 이때, 상기 사용자 단말(100)과 상기 게이트 서버(200)는 미리 설정된 HTTP 프로토콜(또는 HTTPS 프로토콜)을 사용하여 통신한다.
- [0207] 또한, 상기 사용자 단말(100)은 상기 수신된 인증용 블록을 상기 접속된 특정 게이트 서버(200)에 등록(또는 저장)한다.
- [0208] 즉, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200) 내의 복수의 테이블(또는 사서함) 중 어느 하나의 특정 테이블(또는 특정 사서함)에 해당 인증용 블록을 등록(또는 저장)한다.
- [0209] 일 예로, 상기 제 1 사용자 단말은 앞선 제 1 인증용 블록 생성 요청에 응답하여 상기 제 1 웹 서버로부터 전송되는 제 1 인증용 블록을 수신한다.
- [0210] 또한, 상기 제 1 사용자 단말은 상기 복수의 게이트 서버(200) 중에서 상기 제 2 게이트 서버에 접속한다.
- [0211] 또한, 상기 제 1 사용자 단말은 상기 제 2 게이트 서버에서 관리하는 복수의 테이블 중에서 제 2 테이블에 상기 제 1 인증용 블록을 등록한다.
- [0212] 다른 일 예로, 상기 제 2 사용자 단말은 앞선 제 2 인증용 블록 생성 요청에 응답하여 상기 제 2 웹 서버로부터

전송되는 제 2 인증용 블록을 수신한다.

- [0213] 또한, 상기 제 2 사용자 단말은 상기 복수의 게이트 서버(200) 중에서 상기 제 23 게이트 서버에 접속한다.
- [0214] 또한, 상기 제 2 사용자 단말은 상기 제 23 게이트 서버에서 관리하는 복수의 테이블 중에서 제 23 테이블에 상기 제 2 인증용 블록을 등록한다(S420).
- [0215] 이후, 클라우드 포켓(300)은 미리 설정된 주기로 해당 특정 게이트 서버(200)와 연결(또는 통신/접속)한 후, 해당 특정 게이트 서버(200) 내의 복수의 테이블(또는 사서함)에 데이터(예를 들어 인증용 블록 등 포함)가 등록된(또는 저장된) 상태인지 여부를 확인한다. 여기서, 상기 클라우드 포켓(300)은 복수의 클라우드 포켓(300) 중 어느 하나이고, 해당 특정 게이트 서버(200)와 통신하도록 미리 설정된 상태이며, 해당 클라우드 포켓(300)과 해당 특정 게이트 서버(200) 간의 연결은 해당 클라우드 포켓(300)에서만 해당 특정 게이트 서버(200)로 접속하는 단방향 통신일 수 있다.
- [0216] 상기 확인 결과, 상기 복수의 테이블(또는 사서함) 중 적어도 하나의 테이블(또는 사서함)에 데이터가 등록된 상태인 경우, 상기 클라우드 포켓(300)은 해당 테이블(또는 사서함)에 등록된 데이터를 확인한다.
- [0217] 즉, 상기 클라우드 포켓(300)은 루프(또는 스레드)를 돌면서 일정 시간 간격(또는 주기)으로 규칙적으로 해당 특정 게이트 서버(200)에 접속하고, 해당 클라우드 포켓(300)에서 처리할 작업(또는 데이터)이 있는지 여부를 확인한다. 여기서, 상기 클라우드 포켓(300)에서 처리할 작업은 임의의 사용자 단말(100) 등에서 상기 특정 게이트 서버(200) 내의 테이블에 등록된 데이터와 관련한 기능일 수 있다.
- [0218] 일 예로, 제 3 클라우드 포켓(300)은 미리 설정된 주기로 해당 제 2 게이트 서버에 접속하고, 상기 제 2 게이트 서버에서 관리하는 복수의 테이블에 임의의 데이터가 등록된 상태인지 여부를 확인한다.
- [0219] 다른 일 예로, 제 3 클라우드 포켓(300)은 미리 설정된 주기로 해당 제 23 게이트 서버에 접속하고, 상기 제 23 게이트 서버에서 관리하는 복수의 테이블에 임의의 데이터가 등록된 상태인지 여부를 확인한다(S430).
- [0220] 이후, 해당 데이터가 인증용 블록인 경우, 상기 클라우드 포켓(300)은 해당 특정 게이트 서버(200)와 연동하여, 상기 웹 서버에서 상기 특정 게이트 서버(200)에 등록한(또는 저장한) 인증용 블록과, 상기 사용자 단말(100)에서 상기 특정 게이트 서버(200)에 등록한(또는 저장한) 인증용 블록이 일치하는지 여부를 비교(또는 확인)한다.
- [0221] 일 예로, 상기 제 2 게이트 서버에서 관리하는 복수의 테이블 중에서 제 2 테이블에 상기 제 1 인증용 블록이 등록된 상태일 때, 상기 제 3 클라우드 포켓은 앞서 상기 제 1 웹 서버에서 상기 제 2 게이트 서버에 등록한 제 1 인증용 블록과, 상기 제 1 사용자 단말에서 상기 제 2 게이트 서버의 제 2 테이블에 등록한 제 1 인증용 블록이 일치하는지 여부를 비교한다.
- [0222] 다른 일 예로, 상기 제 23 게이트 서버에서 관리하는 복수의 테이블 중에서 제 23 테이블에 상기 제 2 인증용 블록이 등록된 상태일 때, 상기 제 3 클라우드 포켓은 앞서 상기 제 2 웹 서버에서 상기 제 23 게이트 서버에 등록된 제 2 인증용 블록과, 상기 제 2 사용자 단말에서 상기 제 23 게이트 서버의 제 23 테이블에 등록한 제 2 인증용 블록이 일치하는지 여부를 비교한다(S440).
- [0223] 상기 비교 결과(또는 상기 확인 결과), 상기 웹 서버에서 해당 특정 게이트 서버(200)에 등록한(또는 저장한) 인증용 블록과 상기 사용자 단말(100)에서 해당 특정 게이트 서버(200)에 등록한(또는 저장한) 인증용 블록이 일치하지 않은 경우, 상기 클라우드 포켓(300)은 인증 실패 정보를 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록(또는 저장)하고, 해당 특정 게이트 서버(200)와의 연결을 종료한다. 여기서, 상기 클라우드 포켓(300)은 해당 특정 게이트 서버(200)의 해당 테이블에서 앞서 저장 중인 데이터(예를 들어 인증용 블록 등 포함)에 추가하여 상기 인증 실패 정보를 저장하거나 또는, 해당 테이블에 저장 중인 데이터를 삭제하고 상기 인증 실패 정보를 저장한다.
- [0224] 또한, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록된(또는 저장된) 인증 실패 정보를 확인(또는 표시/출력)한다. 이때, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)와 접속한 상태에서, 해당 특정 게이트 서버(200)의 해당 테이블에 새롭게 정보(예를 들어 인증 실패 정보 등 포함)가 등록됨에 따라, 해당 특정 게이트 서버(200)로부터 전송되는 알림 정보(또는 안내 정보)를 수신하고, 상기 수신된 알림 정보를 근거로 해당 특정 게이트 서버(200) 내의 해당 테이블에 등록된 인증 실패 정보를 확인할 수도 있다. 또한, 상기 사용자 단말(100)은 앞선 단계들을 통해 인증 블록을 새로 발급받아야 함을 포함하는 안내 정보를 추가로 표시할 수도 있다.

- [0225] 일 예로, 상기 비교 결과, 상기 제 1 웹 서버에서 상기 제 2 게이트 서버에 등록한 제 1 인증용 블록과, 상기 제 1 사용자 단말에서 상기 제 2 게이트 서버의 제 2 테이블에 등록한 제 1 인증용 블록이 일치하지 않을 때, 상기 제 3 클라우드 포켓은 인증 실패 정보를 상기 제 2 게이트 서버의 제 2 테이블에 누적하여 저장하고, 상기 제 2 게이트 서버와의 연결을 종료한다.
- [0226] 또한, 상기 제 1 사용자 단말은 상기 접속 중인 제 2 게이트 서버 내의 제 2 테이블에 등록된 인증 실패 정보를 표시한다.
- [0227] 다른 일 예로, 상기 비교 결과, 상기 제 2 웹 서버에서 상기 제 23 게이트 서버에 등록된 제 2 인증용 블록과, 상기 제 2 사용자 단말에서 상기 제 23 게이트 서버의 제 23 테이블에 등록한 제 2 인증용 블록이 일치하지 않을 때, 상기 제 2 클라우드 포켓은 인증 실패 정보를 상기 제 23 게이트 서버의 제 23 테이블에 저장하고, 상기 제 23 게이트 서버와의 연결을 종료한다.
- [0228] 또한, 상기 제 2 사용자 단말은 상기 접속 중인 제 23 게이트 서버 내의 제 23 테이블에 등록된 인증 실패 정보를 표시한다(S450).
- [0229] 또한, 상기 비교 결과(또는 상기 확인 결과), 상기 웹 서버에서 해당 특정 게이트 서버(200)에 등록한(또는 저장한) 인증용 블록과 상기 사용자 단말(100)에서 해당 특정 게이트 서버(200)에 등록한(또는 저장한) 인증용 블록이 일치하는 경우, 상기 클라우드 포켓(300)은 해당 인증용 블록에 포함된 아이디(또는 디바이스 아이디), 비밀번호 등을 확인한다.
- [0230] 또한, 상기 클라우드 포켓(300)은 상기 확인된 아이디, 비밀번호, 현재 시각과 미리 설정된 유효 기간 등을 근거로 인증키를 생성(또는 발급)한다. 이때, 상기 인증키는 아이디(또는 디바이스 아이디), 비밀번호, 해당 인증키에 대한 유효 기간 정보를 포함하는 타임스탬프 등을 포함한다. 여기서, 상기 유효 기간은 미리 설정된 값(예를 들어 3분, 5분, 10분 등 포함)일 수 있다.
- [0231] 일 예로, 상기 비교 결과, 상기 제 1 웹 서버에서 상기 제 2 게이트 서버에 등록한 제 1 인증용 블록과, 상기 제 1 사용자 단말에서 상기 제 2 게이트 서버의 제 2 테이블에 등록한 제 1 인증용 블록이 일치할 때, 상기 제 3 클라우드 포켓은 상기 제 1 인증용 블록에 포함된 제 1 아이디, 제 1 비밀번호를 확인하고, 상기 확인된 제 1 아이디, 제 1 비밀번호 및 제 1 타임스탬프로 구성되는 제 1 인증키를 생성한다. 여기서, 상기 제 1 타임스탬프는 정수형으로 표시(또는 관리/구성)하며, 현재 시각(예를 들어 2025년 03월 01일 오후 1시 10분 20초)으로부터 미리 설정된 유효 기간(예를 들어 5분)이 적용된 값(예를 들어 2025년 03월 01일 오후 1시 15분 20초)일 수 있다.
- [0232] 다른 일 예로, 상기 비교 결과, 상기 제 2 웹 서버에서 상기 제 23 게이트 서버에 등록된 제 2 인증용 블록과, 상기 제 2 사용자 단말에서 상기 제 23 게이트 서버의 제 23 테이블에 등록한 제 2 인증용 블록이 일치할 때, 상기 제 3 클라우드 포켓은 상기 제 2 인증용 블록에 포함된 제 2 아이디, 제 2 비밀번호를 확인하고, 상기 확인된 제 2 아이디, 제 2 비밀번호 및 제 2 타임스탬프로 구성되는 제 2 인증키를 생성한다. 여기서, 상기 제 2 타임스탬프는 정수형으로 표시(또는 관리/구성)하며, 현재 시각(예를 들어 2025년 03월 01일 오후 7시 20분 30초)으로부터 미리 설정된 유효 기간(예를 들어 5분)이 적용된 값(예를 들어 2025년 03월 01일 오후 7시 25분 30초)일 수 있다(S460).
- [0233] 이후, 상기 클라우드 포켓(300)은 사용자 계정 암호/복호키를 생성한다. 여기서, 상기 사용자 계정 암호/복호키는 미리 설정된 상태에서 사용하거나 또는 요청에 따라 생성하여 사용할 수 있으며, 열람 계정키(또는 복호키/복호화키), 수정 계정키(또는 암호키/암호화키), 연산키 등으로 구성(또는 포함)한다.
- [0234] 즉, 상기 클라우드 포켓(300)은 미리 설정된 크기(예를 들어 256 바이트*3)의 바이트 키(byte key)인 사용자 계정 암호/복호키를 생성하며, 해당 바이트 키는 키 단위가 바이트임을 나타낸다.
- [0235] 일 예로, 상기 제 3 클라우드 포켓은 암호화된 데이터를 해석(또는 복호)하고자 할 때 사용하기 위한 미리 설정된 크기(예를 들어 256 바이트)의 제 1 열람 계정키와, 데이터를 암호화하고자 할 때 사용하기 위한 미리 설정된 크기(예를 들어 256 바이트)의 제 1 수정 계정키와, 연산부호화 방식을 사용하여 패턴으로 해석할 수 없게 하기 위한 미리 설정된 크기(예를 들어 256 바이트)의 제 1 연산키로 구성된 제 1 사용자 계정 암호/복호키를 생성한다.
- [0236] 다른 일 예로, 상기 제 3 클라우드 포켓은 암호화된 데이터를 해석(또는 복호)하고자 할 때 사용하기 위한 미리 설정된 크기(예를 들어 256 바이트)의 제 2 열람 계정키와, 데이터를 암호화하고자 할 때 사용하기 위한 미리

설정된 크기(예를 들어 256 바이트)의 제 2 수정 계정키와, 연산부호화 방식을 사용하여 패턴으로 해석할 수 없게 하기 위한 미리 설정된 크기(예를 들어 256 바이트)의 제 2 연산키로 구성된 제 2 사용자 계정 암호/복호키를 생성한다(S470).

[0237] 이후, 상기 클라우드 포켓(300)은 상기 생성된 인증키와 상기 생성된 사용자 계정 암호/복호키를 포함하는 인증키 블록을 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록(또는 저장)한다. 여기서, 상기 클라우드 포켓(300)은 해당 특정 게이트 서버(200)의 해당 테이블에서 앞서 저장 중인 데이터(예를 들어 인증용 블록 등 포함)에 추가하여 상기 인증키 블록을 저장하거나 또는, 해당 테이블에 저장 중인 데이터를 삭제하고 상기 인증키 블록을 저장한다.

[0238] 또한, 상기 클라우드 포켓(300)은 복수의 메인 서버(400) 중에서 해당 클라우드 포켓(300)과 연동하는 어느 하나의 메인 서버(400)와 연동하여, 해당 메인 서버(400)의 데이터베이스(미도시) 내의 복수의 테이블 중 어느 하나의 테이블 내의 어느 하나의 레코드에 해당 인증키 블록을 저장(또는 등록)한다. 이때, 상기 데이터베이스의 특정 테이블 내의 특정 레코드에 해당 인증키 블록이 저장됨에 따라, 상기 클라우드 포켓(300)은 해당 메인 서버(400)로부터 제공되는 사서함 번호(또는 해당 특정 테이블에 대응하는 사서함 번호)를 수신한다. 여기서, 상기 클라우드 포켓(300)은 미리 설정된 주기로 접속하는 상기 특정 게이트 서버(200) 내의 테이블에 상기 인증키 블록을 저장할 때, 상기 사서함 번호를 함께 저장할 수도 있다.

[0239] 또한, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록된(또는 저장된) 인증키 블록을 확인(또는 표시/출력/다운로드)한다. 이때, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)와 접속한 상태에서, 해당 특정 게이트 서버(200)의 해당 테이블에 새롭게 정보(예를 들어 인증키 블록 등 포함)가 등록됨에 따라, 해당 특정 게이트 서버(200)로부터 전송되는 알림 정보(또는 안내 정보)를 수신하고, 상기 수신된 알림 정보를 근거로 해당 특정 게이트 서버(200) 내의 해당 테이블에 등록된 인증키 블록을 확인할 수도 있다.

[0240] 일 예로, 상기 제 3 클라우드 포켓은 상기 생성된 제 1 인증키와 상기 생성된 제 1 사용자 계정 암호/복호키를 포함하는 제 1 인증키 블록을 생성하고, 상기 생성된 제 1 인증키 블록을 상기 제 2 게이트 서버의 제 2 테이블에 누적하여 저장한다.

[0241] 또한, 상기 제 3 클라우드 포켓은 복수의 메인 서버(400) 중에서 제 14 메인 서버(400)와 연동하여, 상기 제 14 메인 서버의 데이터베이스 내의 복수의 테이블 중에서 제 4 테이블 내의 제 14 레코드에 상기 제 1 인증키 블록을 저장한다.

[0242] 또한, 상기 제 14 메인 서버는 해당 제 1 인증키 블록이 저장된 제 4 테이블에 대응하는 제 4 사서함 번호를 상기 제 3 클라우드 포켓에 전송한다.

[0243] 또한, 상기 제 3 클라우드 포켓은 상기 제 14 메인 서버로부터 전송되는 제 4 사서함 번호를 수신한다.

[0244] 또한, 상기 제 1 사용자 단말은 상기 접속 중인 제 2 게이트 서버 내의 제 2 테이블에 등록된 제 1 인증키 블록을 확인하고, 해당 제 1 인증키 블록을 다운로드하여 임시 저장한다.

[0245] 다른 일 예로, 상기 제 3 클라우드 포켓은 상기 생성된 제 2 인증키와 상기 생성된 제 2 사용자 계정 암호/복호키를 포함하는 제 2 인증키 블록을 생성하고, 상기 생성된 제 2 인증키 블록을 상기 제 23 게이트 서버의 제 23 테이블에 저장한다.

[0246] 또한, 상기 제 3 클라우드 포켓은 복수의 메인 서버(400) 중에서 제 14 메인 서버(400)와 연동하여, 상기 제 14 메인 서버의 데이터베이스 내의 복수의 테이블 중에서 제 34 테이블 내의 제 34 레코드에 상기 제 2 인증키 블록을 저장한다.

[0247] 또한, 상기 제 14 메인 서버는 해당 제 2 인증키 블록이 저장된 제 34 테이블에 대응하는 제 34 사서함 번호를 상기 제 3 클라우드 포켓에 전송한다.

[0248] 또한, 상기 제 3 클라우드 포켓은 상기 제 14 메인 서버로부터 전송되는 제 34 사서함 번호를 수신한다.

[0249] 또한, 상기 제 2 사용자 단말은 상기 접속 중인 제 23 게이트 서버 내의 제 23 테이블에 등록된 제 2 인증키 블록을 확인하고, 해당 제 2 인증키 블록을 다운로드하여 임시 저장한다(S480).

[0250] 이후, 상기 사용자 단말(100)은 클라우드 포켓(300)에서 관리하는 클라우드 블록체인에 데이터(또는 정보)를 저장(또는 생성/수정)하거나 또는 해당 클라우드 블록체인에 등록된 데이터(또는 정보)를 조회하기 위해서, 클라

우드 블록체인에 등록하고자 하는 원본 데이터를 상기 인증키 블록에 포함된 사용자 계정 암호/복호키를 이용해서 암호화하여, 암호 블록(또는 암호화된 데이터)을 생성한다. 여기서, 상기 원본 데이터(또는 목적 블록/목적 데이터/암호화하고자 하는 데이터 블록)는 내용(또는 정보/데이터)뿐만 아니라, 요구사항(예를 들어 생성 요청 정보, 수정 요청 정보, 조회 요청 정보 등 포함) 등을 포함한다. 또한, 상기 암호 블록에는 원본 데이터뿐만 아니라, 헤더값(또는 암호화와 관련한 헤더값)이 포함될 수 있다.

- [0251] 일 예로, 상기 제 1 사용자 단말은 해당 제 1 사용자 단말의 제 1 사용자인 철수와 관련해서 암호화폐 지갑에 잔액이 얼마인지를 확인하기 위한 정보를 포함하는 제 1 원본 데이터(예를 들어 내 지갑에 있는 총금액을 알고 싶다)를 상기 제 1 인증키 블록에 포함된 제 1 사용자 계정 암호/복호키를 이용해서 암호화하여, 제 1 암호 블록을 생성한다.
- [0252] 다른 일 예로, 상기 제 2 사용자 단말은 해당 제 2 사용자 단말의 제 2 사용자와 관련해서 해당 제 2 사용자인 영희의 암호화폐 지갑에 보관 중인 1 비트코인을 홍길동의 암호화폐 지갑에 이체하기 위한 정보를 포함하는 제 2 원본 데이터(예를 들어 내 지갑에 있는 비트코인 중에서 1 비트코인을 홍길동의 암호화폐 지갑에 이체해줘)를 상기 제 2 인증키 블록에 포함된 제 2 사용자 계정 암호/복호키를 이용해서 암호화하여, 제 2 암호 블록을 생성한다(S490).
- [0253] 이후, 상기 사용자 단말(100)은 상기 생성된 암호 블록, 상기 인증키 블록에 포함된 인증키 등을 포함하는 요구문(또는 명령문/요청문/요구문 블록)을 생성한다.
- [0254] 또한, 상기 사용자 단말(100)은 상기 복수의 게이트 서버(200) 중 어느 하나의 특정 게이트 서버(200)에 접속(또는 통신/연결)한다.
- [0255] 또한, 상기 사용자 단말(100)은 상기 생성된 요구문을 상기 접속된 특정 게이트 서버(200)에 등록(또는 저장)한다.
- [0256] 즉, 상기 사용자 단말(100)은 상기 특정 게이트 서버(200) 내의 복수의 테이블(또는 사서함) 중 어느 하나의 다른 특정 테이블(또는 다른 특정 사서함)에 해당 요구문을 등록(또는 저장)한다.
- [0257] 일 예로, 상기 제 1 사용자 단말은 상기 생성된 제 1 암호 블록, 상기 제 1 인증키 블록에 포함된 제 1 인증키 등을 포함하는 제 1 요구문을 생성한다.
- [0258] 또한, 상기 제 1 사용자 단말은 상기 복수의 게이트 서버(200) 중 상기 제 2 게이트 서버에 접속한다.
- [0259] 또한, 상기 제 1 사용자 단말은 상기 생성된 제 1 요구문을 상기 접속된 제 2 게이트 서버에서 관리하는 복수의 테이블 중에서 제 2 테이블에 등록한다.
- [0260] 다른 일 예로, 상기 제 2 사용자 단말은 상기 생성된 제 2 암호 블록, 상기 제 2 인증키 블록에 포함된 제 2 인증키 등을 포함하는 제 2 요구문을 생성한다.
- [0261] 또한, 상기 제 2 사용자 단말은 상기 복수의 게이트 서버(200) 중 상기 제 23 게이트 서버에 접속한다.
- [0262] 또한, 상기 제 2 사용자 단말은 상기 생성된 제 2 요구문을 상기 접속된 제 23 게이트 서버에서 관리하는 복수의 테이블 중에서 제 24 테이블에 등록한다(S500).
- [0263] 이후, 상기 클라우드 포켓(300)은 상기 미리 설정된 주기로 해당 특정 게이트 서버(200)와 연결(또는 통신/접속)한 후, 해당 특정 게이트 서버(200) 내의 복수의 테이블(또는 사서함)에 데이터(예를 들어 요구문 등 포함)가 등록된(또는 저장된) 상태인지 여부를 확인한다.
- [0264] 상기 확인 결과, 상기 복수의 테이블(또는 사서함) 중 적어도 하나의 테이블(또는 사서함)에 데이터가 등록된 상태인 경우, 상기 클라우드 포켓(300)은 해당 테이블(또는 사서함)에 등록된 데이터를 확인한다.
- [0265] 즉, 상기 클라우드 포켓(300)은 루프(또는 스레드)를 돌면서 일정 시간 간격(또는 주기)으로 규칙적으로 해당 특정 게이트 서버(200)에 접속하고, 해당 클라우드 포켓(300)에서 처리할 작업(또는 데이터)이 있는지 여부를 확인한다. 여기서, 상기 클라우드 포켓(300)에서 처리할 작업은 임의의 사용자 단말(100) 등에서 상기 특정 게이트 서버(200) 내의 테이블에 등록한 데이터와 관련한 기능일 수 있다.
- [0266] 일 예로, 상기 제 3 클라우드 포켓은 미리 설정된 주기로 해당 제 2 게이트 서버에 접속하고, 상기 제 2 게이트 서버에서 관리하는 복수의 테이블에 임의의 데이터가 등록된 상태인지 여부를 확인한다.
- [0267] 다른 일 예로, 상기 제 3 클라우드 포켓은 미리 설정된 주기로 해당 제 23 게이트 서버에 접속하고, 상기 제 23

게이트 서버에서 관리하는 복수의 테이블에 임의의 데이터가 등록된 상태인지 여부를 확인한다(S510).

- [0268] 이후, 해당 데이터가 요구문인 경우, 상기 클라우드 포켓(300)은 1차로 해당 요구문에 포함된 타임스탬프를 근거로 해당 데이터(또는 요구문)의 유효성을 검증(또는 판단)한다.
- [0269] 즉, 해당 데이터가 요구문인 경우, 상기 클라우드 포켓(300)은 해당 데이터(또는 요구문)의 유효성을 검증하기 위해서, 현재 시각과 해당 요구문에 포함된 타임스탬프를 근거로, 현재 시각과 해당 요구문에 포함된 타임스탬프 간의 시간 차이가 미리 설정된 기준값(예를 들어 3초, 5초, 10초 등 포함)을 지난 상태(또는 초과한 상태)인지 여부를 검증(또는 판단)한다.
- [0270] 일 예로, 상기 제 2 게이트 서버에서 관리하는 복수의 테이블 중에서 제 2 테이블에 상기 제 1 요구문이 등록된 상태일 때, 상기 제 3 클라우드 포켓은 현재 시각과 상기 제 1 요구문에 포함된 제 1 타임스탬프(예를 들어 2025년 03월 01일 오후 1시 15분 20초) 간의 제 1 시간 차이를 산출하고, 상기 산출된 제 1 시간 차이가 미리 설정된 제 1 기준값(예를 들어 5초)을 지난 상태인지 여부를 판단한다.
- [0271] 다른 일 예로, 상기 제 23 게이트 서버에서 관리하는 복수의 테이블 중에서 제 24 테이블에 상기 제 2 요구문이 등록된 상태일 때, 상기 제 3 클라우드 포켓은 현재 시각과 상기 제 2 요구문에 포함된 제 2 타임스탬프(예를 들어 2025년 03월 01일 오후 7시 25분 30초) 간의 제 2 시간 차이를 산출하고, 상기 산출된 제 2 시간 차이가 미리 설정된 제 2 기준값(예를 들어 3초)을 지난 상태인지 여부를 판단한다(S520).
- [0272] 상기 데이터의 유효성 검증 결과(또는 상기 데이터/요구문의 유효성 판단 결과), 해당 요구문이 유효하지 않은 것으로 판단되는 경우, 상기 클라우드 포켓(300)은 해당 데이터의 유효성 검증이 실패한 상태임을 나타내는 정보를 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록(또는 저장)하고, 해당 특정 게이트 서버(200)와의 연결을 종료한다. 여기서, 상기 클라우드 포켓(300)은 해당 특정 게이트 서버(200)의 해당 테이블에서 앞서 저장 중인 데이터(예를 들어 인증 블록, 요구문 등 포함)에 추가하여 상기 데이터의 유효성 검증이 실패한 상태임을 나타내는 정보를 저장하거나 또는, 해당 테이블에 저장 중인 데이터를 삭제하고 상기 데이터의 유효성 검증이 실패한 상태임을 나타내는 정보를 저장한다.
- [0273] 즉, 현재 시각과 해당 요구문에 포함된 타임스탬프 간의 시간 차이가 미리 설정된 기준값(예를 들어 3초, 5초, 10초 등 포함)을 지난 상태(또는 초과한 상태)인 경우, 상기 클라우드 포켓(300)은 해당 데이터의 유효성 검증이 실패한 상태임을 나타내는 정보를 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록(또는 저장)하고, 해당 특정 게이트 서버(200)와의 연결을 종료한다.
- [0274] 또한, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록된(또는 저장된) 해당 데이터의 유효성 검증이 실패한 상태임을 나타내는 정보를 확인(또는 표시/출력)한다. 이때, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)와 접속한 상태에서, 해당 특정 게이트 서버(200)의 해당 테이블에 새롭게 정보(예를 들어 해당 데이터의 유효성 검증이 실패한 상태임을 나타내는 정보 등 포함)가 등록됨에 따라, 해당 특정 게이트 서버(200)로부터 전송되는 다른 알림 정보(또는 다른 안내 정보)를 수신하고, 상기 수신된 다른 안내 정보를 근거로 해당 특정 게이트 서버(200) 내의 해당 테이블에 등록된 해당 데이터의 유효성 검증이 실패한 상태임을 나타내는 정보를 확인할 수도 있다. 또한, 상기 사용자 단말(100)은 앞선 단계들을 통해 인증키를 새로 발급받아야 함을 포함하는 안내 정보를 추가로 표시할 수도 있다.
- [0275] 일 예로, 상기 제 1 요구문에 대한 유효성 판단 결과, 상기 산출된 제 1 시간 차이가 미리 설정된 제 1 기준값(예를 들어 5초)을 지난 상태일 때, 상기 제 3 클라우드 포켓은 상기 제 1 요구문의 유효성 검증이 실패한 상태임을 나타내는 정보를 상기 제 2 게이트 서버의 제 2 테이블에 누적하여 저장하고, 상기 제 2 게이트 서버와의 연결을 종료한다.
- [0276] 또한, 상기 제 1 사용자 단말은 상기 접속 중인 제 2 게이트 서버 내의 제 2 테이블에 등록된 상기 제 1 요구문의 유효성 검증이 실패한 상태임을 나타내는 정보를 표시한다.
- [0277] 다른 일 예로, 상기 제 2 요구문에 대한 유효성 판단 결과, 상기 산출된 제 2 시간 차이가 미리 설정된 제 2 기준값(예를 들어 3초)을 지난 상태일 때, 상기 제 3 클라우드 포켓은 상기 제 2 요구문의 유효성 검증이 실패한 상태임을 나타내는 정보를 상기 제 23 게이트 서버의 제 24 테이블에 저장하고, 상기 제 23 게이트 서버와의 연결을 종료한다.
- [0278] 또한, 상기 제 2 사용자 단말은 상기 접속 중인 제 23 게이트 서버 내의 제 24 테이블에 등록된 상기 제 2 요구문의 유효성 검증이 실패한 상태임을 나타내는 정보를 표시한다(S530).

- [0279] 또한, 상기 데이터의 유효성 검증 결과(또는 상기 데이터/요구문의 유효성 판단 결과), 해당 요구문이 유효한 것으로 판단되는 경우, 상기 클라우드 포켓(300)은 2차로 해당 요구문에 포함된 헤더값이 미리 설정된 규격(또는 조건)에 맞는지 여부(또는 충족하는지 여부)를 확인(또는 판단)한다. 여기서, 상기 헤더값은 해당 요구문에 포함된 암호 블록을 암호화하는 과정에서 생성된 값일 수 있다.
- [0280] 즉, 현재 시각과 해당 요구문에 포함된 타임스탬프 간의 시간 차이가 미리 설정된 기준값(예를 들어 3초, 5초, 10초 등 포함)을 지나지 않은 상태(또는 초과하지 않은 상태)인 경우, 상기 클라우드 포켓(300)은 해당 요구문이 유효한 것으로 판단하고, 해당 요구문에 포함된 헤더값이 미리 설정된 규격(또는 조건)에 맞는지 여부를 2차로 확인(또는 판단)한다.
- [0281] 일 예로, 상기 제 1 요구문에 대한 유효성 판단 결과, 상기 산출된 제 1 시간 차이가 미리 설정된 제 1 기준값(예를 들어 5초)을 지나지 않은 상태일 때, 상기 제 3 클라우드 포켓은 상기 제 1 요구문에 포함된 제 1 헤더값이 상기 미리 설정된 규격에 맞는지 여부를 확인한다.
- [0282] 다른 일 예로, 상기 제 2 요구문에 대한 유효성 판단 결과, 상기 산출된 제 2 시간 차이가 미리 설정된 제 2 기준값(예를 들어 3초)을 지나지 않은 상태일 때, 상기 제 3 클라우드 포켓은 상기 제 2 요구문에 포함된 제 2 헤더값이 상기 미리 설정된 규격에 맞는지 여부를 확인한다(S540).
- [0283] 상기 확인 결과(또는 상기 판단 결과), 해당 요구문에 포함된 헤더값이 미리 설정된 규격(또는 조건)에 맞지(또는 충족하지) 않는 경우, 상기 클라우드 포켓(300)은 해당 데이터의 규격 검증이 실패한 상태임을 나타내는 정보를 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록(또는 저장)하고, 해당 특정 게이트 서버(200)와의 연결을 종료한다. 여기서, 상기 클라우드 포켓(300)은 해당 특정 게이트 서버(200)의 해당 테이블에서 앞서 저장 중인 데이터(예를 들어 인증 블록, 요구문 등 포함)에 추가하여 상기 데이터의 규격 검증이 실패한 상태임을 나타내는 정보를 저장하거나 또는, 해당 테이블에 저장 중인 데이터를 삭제하고 상기 데이터의 규격 검증이 실패한 상태임을 나타내는 정보를 저장한다.
- [0284] 또한, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록된(또는 저장된) 해당 데이터의 규격 검증이 실패한 상태임을 나타내는 정보를 확인(또는 표시/출력)한다. 이때, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)와 접속한 상태에서, 해당 특정 게이트 서버(200)의 해당 테이블에 새롭게 정보(예를 들어 해당 데이터의 규격 검증이 실패한 상태임을 나타내는 정보 등 포함)가 등록됨에 따라, 해당 특정 게이트 서버(200)로부터 전송되는 다른 알림 정보(또는 다른 안내 정보)를 수신하고, 상기 수신된 다른 안내 정보를 근거로 해당 특정 게이트 서버(200) 내의 해당 테이블에 등록된 해당 데이터의 규격 검증이 실패한 상태임을 나타내는 정보를 확인할 수도 있다. 또한, 상기 사용자 단말(100)은 앞선 단계들을 통해 인증키를 새로 발급받아야 함을 포함하는 안내 정보를 추가로 표시할 수도 있다.
- [0285] 일 예로, 상기 제 1 요구문에 포함된 제 1 헤더값이 상기 미리 설정된 규격을 충족하지 않을 때, 상기 제 3 클라우드 포켓은 상기 제 1 요구문의 규격 검증이 실패한 상태임을 나타내는 정보를 상기 제 2 게이트 서버의 제 2 테이블에 누적하여 저장하고, 상기 제 2 게이트 서버와의 연결을 종료한다.
- [0286] 또한, 상기 제 1 사용자 단말은 상기 접속 중인 제 2 게이트 서버 내의 제 2 테이블에 등록된 상기 제 1 요구문의 규격 검증이 실패한 상태임을 나타내는 정보를 표시한다.
- [0287] 다른 일 예로, 상기 제 2 요구문에 포함된 제 2 헤더값이 상기 미리 설정된 규격을 충족하지 않을 때, 상기 제 3 클라우드 포켓은 상기 제 2 요구문의 규격 검증이 실패한 상태임을 나타내는 정보를 상기 제 23 게이트 서버의 제 24 테이블에 저장하고, 상기 제 23 게이트 서버와의 연결을 종료한다.
- [0288] 또한, 상기 제 2 사용자 단말은 상기 접속 중인 제 23 게이트 서버 내의 제 24 테이블에 등록된 상기 제 2 요구문의 규격 검증이 실패한 상태임을 나타내는 정보를 표시한다(S550).
- [0289] 또한, 상기 확인 결과(또는 상기 판단 결과), 해당 요구문에 포함된 헤더값이 미리 설정된 규격(또는 조건)에 맞지(또는 충족하는) 경우, 상기 클라우드 포켓(200)은 3차로 해당 요구문에 포함된 암호 블록을 미리 설정된 사용자 계정 암호/복호키(또는 앞서 해당 사용자 단말(100)과 관련한 인증용 블록을 근거로 생성된 사용자 계정 암호/복호키)를 이용해서 복호하여, 원본 데이터를 생성(또는 복원)한다.
- [0290] 즉, 2차 해당 데이터의 규격 검증 결과, 해당 요구문에 포함된 헤더값이 미리 설정된 규격(또는 조건)에 맞지(또는 충족하는) 경우, 상기 클라우드 포켓(200)은 해당 요구문을 인증키와 암호 블록으로 분리하고, 상기 분리된 암호 블록을 상기 사용자 계정 암호/복호키를 이용해서 복호하여, 원본 데이터를 생성(또는 복원)한다.

- [0291] 일 예로, 상기 제 1 요구문에 포함된 제 1 헤더값이 상기 미리 설정된 규격을 충족할 때, 상기 제 3 클라우드 포켓은 상기 제 1 요구문을 상기 제 1 인증키와 상기 제 1 암호 블록으로 분리한다.
- [0292] 또한, 상기 제 3 클라우드 포켓은 상기 분리된 제 1 암호 블록을 상기 제 1 사용자 계정 암호/복호키를 이용해서 복호하여, 상기 제 1 원본 데이터(예를 들어 내 지갑에 있는 총금액을 알고 싶다)를 생성한다.
- [0293] 다른 일 예로, 상기 제 2 요구문에 포함된 제 2 헤더값이 상기 미리 설정된 규격을 충족할 때, 상기 제 3 클라우드 포켓은 상기 제 2 요구문을 상기 제 2 인증키와 상기 제 2 암호 블록으로 분리한다.
- [0294] 또한, 상기 제 3 클라우드 포켓은 상기 분리된 제 2 암호 블록을 상기 제 2 사용자 계정 암호/복호키를 이용해서 복호하여, 상기 제 2 원본 데이터(예를 들어 내 지갑에 있는 비트코인 중에서 1 비트코인을 홍길동의 암호화폐 지갑에 이체해줘)를 생성한다(S560).
- [0295] 이후, 상기 클라우드 포켓(300)은 해당 원본 데이터 등을 근거로 클라우드 블록체인에서 블록 생성 기능, 블록 수정 기능, 블록 조회 기능(또는 블록 내용 조회 기능) 등을 수행한다.
- [0296] 즉, 상기 클라우드 포켓(300)은 해당 원본 데이터에 대해서 구문 분석(또는 파싱)을 수행하고, 구문 분석(또는 구문 분석 결과)에 따라 해당 원본 데이터의 의미(또는 내용)를 파악한다.
- [0297] 또한, 상기 요구문에 포함된 요구사항이 새로운 블록 생성 요청인 경우(또는 해당 파악된 의미/내용이 새로운 블록 생성 요청인 경우), 상기 클라우드 포켓(300)은 해당 클라우드 포켓(300)에서 관리 중인 포켓 서버 리스트 중에서 해당 클라우드 포켓(300)에서의 블록 생성인지 확인한다.
- [0298] 즉, 상기 클라우드 포켓(300)은 해당 새로운 블록 생성 요청이 로컬 서버인 해당 클라우드 포켓(300)에서 수행해야 하는 작업(또는 기능)인지 여부를 상기 포켓 서버 리스트를 통해 확인한다. 여기서, 상기 포켓 서버 리스트는 사용자 계정에 대응하는 지갑(또는 암호화폐/가상화폐 지갑)이 어느 클라우드 포켓(300)에서 저장(또는 관리) 중인지에 대한 정보를 포함하며, 지갑 정보별 클라우드 포켓 정보(또는 클라우드 포켓(300)의 주소/URL)를 포함한다.
- [0299] 상기 확인 결과, 해당 클라우드 포켓(300)에서의 블록 생성인 경우, 상기 클라우드 포켓(300)은 클라우드 블록체인에서 해당 원본 데이터를 근거로 블록 생성 기능을 수행한다.
- [0300] 즉, 상기 확인 결과, 해당 새로운 블록 생성 요청이 해당 요구문을 확인한 로컬 서버인 해당 클라우드 포켓(300)에서 수행해야 하는 작업(또는 기능)인 것으로 확인되는 경우, 상기 클라우드 포켓(300)은 해당 클라우드 포켓(300)에서 해당 원본 데이터를 근거로 블록 생성 기능을 수행한다. 이때, 상기 클라우드 포켓(300)은 해당 요구문과 관련한 사용자의 지갑을 새로 생성하고, 새로 생성된 지갑과 관련한 정보를 관리하는 블록 생성 기능을 수행할 수도 있다.
- [0301] 또한, 상기 클라우드 포켓(300)은 신규 블록 생성과 관련한 블록 생성 기능 수행 결과를 업데이트(또는 해당 클라우드 블록체인에서의 신규 블록 생성에 따른 업데이트)한다.
- [0302] 또한, 상기 클라우드 포켓(300)은 스레드를 이용해서, 전체 클라우드 포켓(300) 중에서 해당 클라우드 포켓(300)을 제외한 나머지 클라우드 포켓(300)에 해당 신규 블록 생성과 관련한 블록 생성 기능 수행 결과를 각각 업데이트한다.
- [0303] 또한, 상기 확인 결과, 다른 클라우드 포켓(300)에서의 블록 생성인 경우(또는 해당 요구문을 확인한 로컬 서버에서의 블록 생성이 아닌 경우), 상기 클라우드 포켓(300)은 해당 클라우드 포켓(300)에서 관리 중인 포켓 서버 리스트를 근거로 해당 블록 생성 기능 수행을 위한 담당인 다른 클라우드 포켓(300)을 확인하고, 상기 확인된 다른 클라우드 포켓(300)에 해당 요구문(또는 원본 데이터)을 제공한다.
- [0304] 이에 따라, 다른 클라우드 포켓(300)은 클라우드 블록체인에서 해당 요구문(또는 원본 데이터)을 근거로 블록 생성 기능을 수행한다. 이때, 상기 다른 클라우드 포켓(300)은 해당 요구문과 관련한 사용자의 지갑을 새로 생성하고, 새로 생성된 지갑과 관련한 정보를 관리하는 블록 생성 기능을 수행할 수도 있다.
- [0305] 또한, 블록 생성 기능 수행을 완료한 후, 상기 클라우드 포켓(300)은 신규 블록 생성과 관련한 블록 생성 기능 수행 결과(또는 상기 다른 클라우드 포켓(300)에서의 신규 블록 생성과 관련한 블록 생성 기능 수행 결과)를 업데이트(또는 해당 클라우드 블록체인에서의 신규 블록 생성에 따른 업데이트)한다. 이때, 상기 클라우드 포켓(300)은 해당 요구문에 따라 새로 생성한 사용자의 지갑에 대한 결과 정보를 업데이트할 수 있다.

- [0306] 또한, 상기 클라우드 포켓(300)은 스레드를 이용해서, 전체 클라우드 포켓(300) 중에서 해당 클라우드 포켓(300)을 제외한 나머지 클라우드 포켓(300)에 해당 신규 블록 생성과 관련한 블록 생성 기능 수행 결과를 각각 업데이트한다.
- [0307] 또한, 상기 요구문에 포함된 요구사항이 블록 수정 요청인 경우(또는 해당 파악된 의미가 블록 수정 요청인 경우), 상기 클라우드 포켓(300)은 해당 클라우드 포켓(300)에서 관리 중인 포켓 서버 리스트를 근거로 1차 수정 클라우드 포켓(300)이 로컬인지 여부를 확인한다.
- [0308] 즉, 상기 클라우드 포켓(300)은 해당 블록 수정 요청과 관련해서 1차 수정 클라우드 포켓(300)이 로컬 서버인 해당 클라우드 포켓(300)에서 수행해야 하는 작업(또는 기능)인지 여부를 상기 포켓 서버 리스트를 통해 확인한다.
- [0309] 상기 확인 결과, 해당 클라우드 포켓(300)에서 1차 수정을 진행해야 하는 경우, 상기 클라우드 포켓(300)은 클라우드 블록체인에서 해당 원본 데이터를 근거로 1차 블록 수정 기능을 수행한다. 여기서, 상기 1차 블록 수정 기능은 대상자를 대상으로 하는 블록 수정 기능을 나타낸다.
- [0310] 즉, 상기 확인 결과, 1차 수정 클라우드 포켓(300)이 해당 요구문을 확인한 로컬 서버인 해당 클라우드 포켓(300)에서 수행해야 하는 작업(또는 기능)인 것으로 확인되는 경우, 상기 클라우드 포켓(300)은 해당 클라우드 블록체인에서 해당 원본 데이터를 근거로 1차 블록 수정 기능을 수행한다. 이때, 상기 클라우드 포켓(300)은 해당 요구문과 관련한 사용자의 지갑에서 해당 요구문에 포함된 암호화폐 수량만큼을 차감하는 블록 수정 기능을 수행할 수도 있다.
- [0311] 또한, 상기 확인 결과, 다른 클라우드 포켓(300)에서의 1차 수정을 진행해야 하는 경우(또는 해당 요구문을 확인한 로컬 서버에서의 1차 블록 수정이 아닌 경우), 상기 클라우드 포켓(300)은 해당 클라우드 포켓(300)에서 관리 중인 포켓 서버 리스트를 근거로 1차 블록 수정 기능 수행을 위한 담당인 다른 클라우드 포켓(300)을 확인하고, 상기 확인된 다른 클라우드 포켓(300)에 해당 요구문(또는 원본 데이터)을 제공한다.
- [0312] 이에 따라, 다른 클라우드 포켓(300)은 클라우드 블록체인에서 해당 요구문(또는 원본 데이터)을 근거로 1차 블록 수정 기능을 수행한다. 이때, 상기 다른 클라우드 포켓(300)은 해당 요구문과 관련한 사용자의 지갑에서 해당 요구문에 포함된 암호화폐 수량만큼을 차감하는 블록 수정 기능을 수행할 수도 있다.
- [0313] 또한, 상기 클라우드 포켓(300)은 상기 다른 클라우드 포켓(300)과 연동하여, 해당 다른 클라우드 포켓(300)에서의 1차 블록 수정 기능 수행의 완료 여부를 파악(또는 확인)한다.
- [0314] 또한, 해당 1차 블록 수정 기능이 완료된 후, 상기 클라우드 포켓(300)은 해당 클라우드 포켓(300)에서 관리 중인 포켓 서버 리스트를 근거로 **2차** 수정 클라우드 포켓(300)이 로컬인지 여부를 확인한다.
- [0315] 즉, 상기 클라우드 포켓(300)은 해당 블록 수정 요청과 관련해서 **2차** 수정 클라우드 포켓(300)이 로컬 서버인 해당 클라우드 포켓(300)에서 수행해야 하는 작업(또는 기능)인지 여부를 상기 포켓 서버 리스트를 통해 판단한다.
- [0316] 상기 판단 결과, 해당 클라우드 포켓(300)에서 2차 수정을 진행해야 하는 경우, 상기 클라우드 포켓(300)은 클라우드 블록체인에서 해당 원본 데이터를 근거로 2차 블록 수정 기능을 수행한다. 여기서, 상기 2차 블록 수정 기능은 피대상자를 대상으로 하는 블록 수정 기능을 나타낸다.
- [0317] 즉, 상기 판단 결과, 2차 수정 클라우드 포켓(300)이 해당 요구문을 확인한 로컬 서버인 해당 클라우드 포켓(300)에서 수행해야 하는 작업(또는 기능)인 것으로 판단되는 경우, 상기 클라우드 포켓(300)은 해당 클라우드 블록체인에서 해당 원본 데이터를 근거로 2차 블록 수정 기능을 수행한다. 이때, 상기 다른 클라우드 포켓(300)은 해당 요구문과 관련한 사용자의 지갑에서 해당 요구문에 포함된 암호화폐 수량만큼을 차감하는 블록 수정 기능을 수행할 수도 있다.
- [0318] 또한, 상기 판단 결과, 또 다른 클라우드 포켓(300)에서의 2차 수정을 진행해야 하는 경우(또는 해당 요구문을 확인한 로컬 서버에서의 2차 블록 수정이 아닌 경우), 상기 클라우드 포켓(300)은 해당 클라우드 포켓(300)에서 관리 중인 포켓 서버 리스트를 근거로 2차 블록 수정 기능 수행을 위한 담당인 또 다른 클라우드 포켓(300)을 확인하고, 상기 확인된 또 다른 클라우드 포켓(300)에 해당 요구문(또는 원본 데이터)을 제공한다.
- [0319] 이에 따라, 또 다른 클라우드 포켓(300)은 클라우드 블록체인에서 해당 요구문(또는 원본 데이터)을 근거로 2차 블록 수정 기능을 수행한다. 이때, 상기 또 다른 클라우드 포켓(300)은 해당 요구문과 관련한 사용자의 지갑에

서 해당 요구문에 포함된 암호화폐 수량만큼을 차감하는 블록 수정 기능을 수행할 수도 있다.

- [0320] 또한, 상기 클라우드 포켓(300)은 상기 또 다른 클라우드 포켓(300)과 연동하여, 해당 또 다른 클라우드 포켓(300)에서의 2차 블록 수정 기능 수행의 완료 여부를 파악(또는 확인)한다.
- [0321] 또한, 1차 및 2차에 걸친 블록 수정 기능 수행을 완료한 후, 상기 클라우드 포켓(300)은 블록 수정과 관련한 블록 수정 기능 수행 결과(또는 해당 클라우드 포켓(300), 해당 다른 클라우드 포켓(300), 해당 또 다른 클라우드 포켓(300) 등에서의 블록 수정 기능 수행 결과)를 업데이트(또는 해당 클라우드 블록체인에서의 블록 수정에 따른 업데이트)한다. 이때, 상기 클라우드 포켓(300)은 해당 요구문을 근거로 암호화폐의 이체에 따라 대상자와 피대상자의 지갑에 대한 변동 사항에 대한 결과 정보를 업데이트할 수 있다.
- [0322] 또한, 상기 클라우드 포켓(300)은 스레드를 이용해서, 전체 클라우드 포켓(300) 중에서 해당 클라우드 포켓(300)을 제외한 나머지 클라우드 포켓(300)에 해당 블록 수정과 관련한 블록 수정 기능 수행 결과를 각각 업데이트한다.
- [0323] 또한, 상기 요구문에 포함된 요구사항이 블록 조회 요청인 경우(또는 해당 파악된 의미가 블록 조회 요청인 경우), 상기 클라우드 포켓(300)은 해당 클라우드 포켓(300)에서 관리 중인 포켓 서버 리스트 중에서 해당 클라우드 포켓(300)에서의 블록 조회인지 확인한다.
- [0324] 즉, 상기 클라우드 포켓(300)은 해당 블록 조회 요청이 로컬 서버인 해당 클라우드 포켓(300)에서 수행해야 하는 작업(또는 기능)인지 여부를 상기 포켓 서버 리스트를 통해 확인한다.
- [0325] 상기 확인 결과, 해당 클라우드 포켓(300)에서의 블록 조회인 경우, 상기 클라우드 포켓(300)은 클라우드 블록체에서 해당 블록 조회 요청에 대응하는 정보(또는 해당 블록 내의 정보/데이터)를 확인하는 기능을 수행한다.
- [0326] 즉, 상기 확인 결과, 해당 블록 조회 요청이 해당 요구문을 확인한 로컬 서버인 해당 클라우드 포켓(300)에서 수행해야 하는 작업(또는 기능)인 것으로 확인되는 경우, 상기 클라우드 포켓(300)은 해당 클라우드 블록체에서 해당 원본 데이터를 근거로 블록 조회 기능을 수행한다. 이때, 상기 클라우드 포켓(300)은 해당 요구문과 관련한 사용자의 지갑에 남아 있는 잔액을 확인하는 조회 기능을 수행할 수 있다.
- [0327] 또한, 상기 클라우드 포켓(300)은 블록 조회와 관련한 블록 조회 기능 수행 결과를 업데이트(또는 해당 클라우드 블록체인에서의 블록 조회에 따른 업데이트)한다.
- [0328] 또한, 상기 클라우드 포켓(300)은 스레드를 이용해서, 전체 클라우드 포켓(300) 중에서 해당 클라우드 포켓(300)을 제외한 나머지 클라우드 포켓(300)에 해당 블록 조회와 관련한 블록 조회 기능 수행 결과를 각각 업데이트한다.
- [0329] 또한, 상기 확인 결과, 다른 클라우드 포켓(300)에서의 블록 조회인 경우(또는 해당 요구문을 확인한 로컬 서버에서의 블록 조회가 아닌 경우), 상기 클라우드 포켓(300)은 해당 클라우드 포켓(300)에서 관리 중인 포켓 서버 리스트를 근거로 해당 블록 조회 기능 수행을 위한 담당인 다른 클라우드 포켓(300)을 확인하고, 상기 확인된 다른 클라우드 포켓(300)에 해당 요구문(또는 원본 데이터)을 제공한다.
- [0330] 이에 따라, 다른 클라우드 포켓(300)은 클라우드 블록체에서 해당 요구문(또는 원본 데이터)을 근거로 블록 조회 기능을 수행한다. 이때, 상기 다른 클라우드 포켓(300)은 해당 요구문과 관련한 사용자의 지갑에 남아 있는 잔액을 확인하는 조회 기능을 수행할 수 있다.
- [0331] 또한, 블록 조회 기능 수행을 완료한 후, 상기 클라우드 포켓(300)은 블록 조회와 관련한 블록 조회 기능 수행 결과를 업데이트(또는 상기 다른 클라우드 포켓(300)에서의 블록 조회와 관련한 블록 조회 기능 수행 결과)를 업데이트(또는 해당 클라우드 블록체인에서의 블록 조회에 따른 업데이트)한다. 이때, 상기 클라우드 포켓(300)은 해당 요구문에 따라 해당 사용자의 지갑에 남아 있는 잔액에 대한 정보를 업데이트할 수 있다.
- [0332] 또한, 상기 클라우드 포켓(300)은 스레드를 이용해서, 전체 클라우드 포켓(300) 중에서 해당 클라우드 포켓(300)을 제외한 나머지 클라우드 포켓(300)에 해당 블록 조회와 관련한 블록 조회 기능 수행 결과를 각각 업데이트한다.
- [0333] 일 예로, 상기 제 3 클라우드 포켓은 상기 제 1 요구문에 포함된 제 1 원본 데이터에 대해서 구문 분석을 수행하고, 구문 분석에 따라 해당 제 1 원본 데이터(예를 들어 내 지갑에 있는 총금액을 알고 싶다)의 제 1 의미(예를 들어 잔액 조회)를 파악한다.

- [0334] 또한, 상기 제 1 요구문에 포함된 제 1 요구사항이 블록 조회일 때, 상기 제 3 클라우드 포켓은 해당 제 3 클라우드 포켓에서 관리 중인 제 3 포켓 서버 리스트 중에서 해당 제 3 클라우드 포켓에서의 블록 조회(또는 해당 제 1 요구문과 관련한 철수의 암호화폐 지갑이 해당 제 3 클라우드 포켓에 설정된 상태)인지 확인한다.
- [0335] 상기 확인 결과, 해당 제 3 클라우드 포켓에서의 블록 조회(또는 해당 철수의 암호화폐 지갑이 해당 제 3 클라우드 포켓에 설정된 상태)일 때, 상기 제 3 클라우드 포켓은 클라우드 블록체인에서 해당 블록 조회 요청에 대응하는 제 4 데이터(예를 들어 잔액은 철수의 지갑 0.5 비트코인입니다)를 확인한다.
- [0336] 또한, 상기 제 3 클라우드 포켓은 블록 조회와 관련한 블록 조회 기능 수행 결과를 업데이트한다.
- [0337] 또한, 상기 제 3 클라우드 포켓은 스레드를 이용해서, 전체 클라우드 포켓(300) 중에서 해당 제 3 클라우드 포켓을 제외한 나머지 클라우드 포켓(300)에 해당 블록 조회와 관련한 블록 조회 기능 수행 결과를 각각 업데이트한다.
- [0338] 다른 일 예로, 상기 제 3 클라우드 포켓은 상기 제 2 요구문에 포함된 제 2 원본 데이터에 대해서 구문 분석을 수행하고, 구문 분석에 따라 해당 제 2 원본 데이터(예를 들어 내 지갑에 있는 비트코인 중에서 1 비트코인을 홍길동의 암호화폐 지갑에 이체해줘)의 제 2 의미(예를 들어 블록 수정)를 파악한다.
- [0339] 또한, 상기 파악된 제 2 의미가 블록 수정일 때, 상기 제 3 클라우드 포켓은 해당 블록 수정 요청과 관련하여 1차 수정이 해당 로컬 서버에서 수행해야 하는 작업인지 여부를 해당 제 3 클라우드 포켓에서 관리 중인 제 3 포켓 서버 리스트를 통해 확인(또는 이체하는 영희의 암호화폐 지갑이 해당 제 3 클라우드 포켓에 설정된 상태인지 확인)한다.
- [0340] 상기 확인 결과, 해당 제 3 클라우드 포켓에서 1차 수정을 진행해야 할 때(또는 해당 이체하는 영희의 암호화폐 지갑이 해당 제 3 클라우드 포켓에 설정된 상태일 때), 상기 제 3 클라우드 포켓은 클라우드 블록체인에서 해당 제 2 원본 데이터를 근거로 1차 블록 수정 기능(예를 들어 영희와 관련한 지갑에 있는 비트코인 중에서 1 비트코인 차감에 따른 블록 수정 기능)을 수행한다.
- [0341] 또한, 상기 제 3 클라우드 포켓은 해당 제 3 클라우드 포켓에서 관리 중인 포켓 서버 리스트를 근거로 해당 블록 수정 요청과 관련하여 2차 수정이 해당 로컬 서버에서 수행해야 하는 작업인지 여부를 판단(또는 이체받는 홍길동의 암호화폐 지갑이 해당 제 3 클라우드 포켓에 설정된 상태인지 판단)한다.
- [0342] 상기 판단 결과, 다른 클라우드 포켓에서 2차 수정을 진행해야 할 때, 상기 제 3 클라우드 포켓은 해당 제 3 클라우드 포켓에서 관리 중인 포켓 서버 리스트를 근거로 2차 블록 수정 기능 수행을 위한 담당인 제 7 클라우드 포켓(300)을 확인하고, 상기 확인된 제 7 클라우드 포켓으로 상기 제 2 요구문(또는 제 2 원본 데이터)을 전송한다.
- [0343] 또한, 상기 제 7 클라우드 포켓은 상기 제 3 클라우드 포켓으로부터 전송되는 제 2 요구문(또는 제 2 원본 데이터)을 수신하고, 상기 수신된 제 2 요구문(또는 제 2 원본 데이터)을 근거로 2차 블록 수정 기능(예를 들어 홍길동과 관련한 지갑에 1 비트코인 추가에 따른 블록 수정 기능)을 수행한다.
- [0344] 또한, 상기 제 3 클라우드 포켓은 블록 수정과 관련한 블록 수정 기능 수행 결과를 업데이트한다.
- [0345] 또한, 상기 제 3 클라우드 포켓은 스레드를 이용해서, 전체 클라우드 포켓(300) 중에서 해당 제 3 클라우드 포켓을 제외한 나머지 클라우드 포켓(300)에 해당 블록 수정과 관련한 블록 수정 기능 수행 결과를 각각 업데이트한다(S570).
- [0346] 이후, 상기 클라우드 포켓(300)은 미리 설정된 주기로 해당 특정 게이트 서버(200)와 연결(또는 통신/접속)한 후, 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 해당 요구문에 대응하는 기능 수행 결과(예를 들어 블록 생성 기능 수행 결과, 블록 수정 기능 수행 결과, 블록 조회 기능 수행 결과 등 포함)를 등록(또는 저장)한다. 여기서, 상기 클라우드 포켓(300)은 해당 특정 게이트 서버(200) 내의 복수의 테이블 중에서 앞서 사용자 단말(100과 관련하여 데이터(예를 들어 인증용 블록, 인증키 블록, 요구문 등 포함)를 등록한 테이블에 해당 기능 수행 결과를 저장하거나 또는, 해당 테이블에 저장 중인 데이터를 삭제하고 해당 요구문에 대응하는 기능 수행 결과를 저장한다.
- [0347] 또한, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록된(또는 저장된) 기능 수행 결과를 확인(또는 표시/출력)한다. 이때, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)와 접속한 상태에서, 해당 특정 게이트 서버(200)의 해당 테이블에 새롭게 정보(예를 들어 기능 수행 결과

등 포함)가 등록됨에 따라, 해당 특정 게이트 서버(200)로부터 전송되는 알림 정보(또는 안내 정보)를 수신하고, 상기 수신된 알림 정보를 근거로 해당 특정 게이트 서버(200) 내의 해당 테이블에 등록된 기능 수행 결과를 확인할 수도 있다.

- [0348] 일 예로, 상기 제 3 클라우드 포켓은 미리 설정된 주기로 제 2 게이트 서버에 접속하고, 블록 조회 기능 수행 결과(예를 들어 철수의 지갑 잔액은 0.5 비트코인입니다)를 상기 제 2 게이트 서버의 제 2 테이블에 누적하여 저장한다.
- [0349] 또한, 상기 제 1 사용자 단말은 상기 접속 중인 제 2 게이트 서버 내의 제 2 테이블에 저장된 블록 조회 기능 수행 결과(예를 들어 철수의 지갑 잔액은 0.5 비트코인입니다)를 표시한다.
- [0350] 다른 일 예로, 상기 제 3 클라우드 포켓은 미리 설정된 주기로 해당 제 23 게이트 서버에 접속하고, 블록 수정 기능 수행 결과(예를 들어 영희의 지갑에서 1 비트코인을 홍길동에게 정상적으로 이체하였고, 영희의 지갑 잔액은 12 비트코인입니다)를 상기 제 23 게이트 서버의 제 24 테이블에 저장한다.
- [0351] 또한, 상기 제 2 사용자 단말은 상기 접속 중인 제 23 게이트 서버 내의 제 24 테이블에 저장된 블록 수정 기능 수행 결과(예를 들어 영희의 지갑에서 1 비트코인을 홍길동에게 정상적으로 이체하였고, 영희의 지갑 잔액은 12 비트코인입니다)를 표시한다(S580).
- [0352] 이후, 상기 클라우드 포켓(300)은 복수의 메인 서버(400) 중에서 어느 하나의 메인 서버(400)와 연결(또는 접속/통신)하고, 상기 연결된 메인 서버(400)에 기능 수행 결과(예를 들어 블록 생성 기능 수행 결과, 블록 수정 기능 수행 결과, 블록 조회 기능 수행 결과 등 포함)를 해당 메인 서버(400) 내의 데이터베이스(미도시) 내의 특정 테이블에 저장(또는 등록)한다. 여기서, 상기 클라우드 포켓(300)과 상기 메인 서버(400) 간의 연결은 양방향 통신으로 구성하고, 미리 설정된 TCP/IP 프로토콜을 이용하여 통신한다. 이때, 해당 TCP/IP 프로토콜은 자체 제작하여 프로토콜 정보를 비공개이다.
- [0353] 또한, 상기 클라우드 포켓(300)은 상기 메인 서버(400)로부터 제공되는 해당 기능 수행 결과가 저장된 특정 테이블과 관련한 특정 사서함 번호를 수신한다.
- [0354] 또한, 상기 클라우드 포켓(300)은 미리 설정된 주기로 해당 특정 게이트 서버(200)와 연결(또는 통신/접속)한 후, 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 해당 특정 사서함 번호를 등록(또는 저장)한다. 여기서, 상기 클라우드 포켓(300)은 상기 특정 게이트 서버(200) 내의 복수의 테이블(또는 사서함) 중에서 앞서 사용자 단말(100)과 관련해서 데이터(예를 들어 인증용 블록, 인증키 블록, 요구문 등 포함)를 등록한 테이블에 해당 특정 사서함 번호를 누적하여 저장하거나 또는, 해당 테이블을 초기화하고 해당 특정 사서함 번호를 저장할 수도 있다. 이때, 상기 클라우드 포켓(300)은 해당 특정 게이트 서버(200)의 복수의 테이블 중에서 서로 다른 테이블에 상기 인증용 블록, 상기 인증키 블록, 상기 요구문, 상기 특정 사서함 번호 등을 각각 저장할 수도 있다.
- [0355] 또한, 상기 메인 서버(400)는 복수의 메인 서버(400) 중에서 해당 어느 하나의 메인 서버(400)를 제외한 나머지 메인 서버(400)와 각각 연동하여, 기능 수행 결과(예를 들어 블록 생성 기능 수행 결과, 블록 수정 기능 수행 결과, 블록 조회 기능 수행 결과 등 포함)를 나머지 메인 서버(400)에 각각 구성된 데이터베이스에 각각 저장(또는 등록/업데이트)한다.
- [0356] 또한, 상기 사용자 단말(100)은 해당 특정 게이트 서버(200)의 해당 테이블(또는 사서함)에 등록된(또는 저장된) 특정 사서함 번호를 확인(또는 표시/출력)한다.
- [0357] 또한, 상기 사용자 단말(100)은 추후 해당 건과 관련한 정보(또는 데이터)에 대해서 수정 기능, 조회 기능 등을 수행하고자 하는 경우, 해당 특정 사서함 번호를 이용한다.
- [0358] 일 예로, 상기 제 3 클라우드 포켓은 복수의 메인 서버(400) 중에서 제 4 메인 서버와 연결하고, 상기 연결된 제 4 메인 서버에 블록 조회 기능 수행 결과를 전송한다.
- [0359] 또한, 상기 제 4 메인 서버는 상기 제 3 클라우드 포켓으로부터 전송되는 블록 조회 기능 수행 결과를 수신한다.
- [0360] 또한, 상기 제 4 메인 서버는 해당 제 4 메인 서버에서 관리하는 복수의 테이블 중에서 제 44 테이블에 상기 수신된 블록 조회 기능 수행 결과를 저장하고, 해당 블록 조회 기능 수행 결과가 저장된 제 44 테이블에 대응하는 제 44 사서함 번호를 상기 제 3 클라우드 포켓에 전송한다.

- [0361] 또한, 상기 제 4 메인 서버는 상기 복수의 메인 서버(400) 중에서 상기 제 4 메인 서버를 제외한 나머지 모든 메인 서버(400)와 각각 연동하여, 상기 블록 조회 기능 수행 결과를 공유하여, 각각의 나머지 메인 서버(400)에서 해당 블록 조회 기능 수행 결과를 각각 저장하도록 구성한다.
- [0362] 또한, 상기 제 3 클라우드 포켓은 상기 제 4 메인 서버로부터 전송되는 제 44 사서함 번호를 수신한다.
- [0363] 또한, 상기 제 3 클라우드 포켓은 미리 설정된 주기로 해당 제 2 게이트 서버와 연결한 후, 상기 제 2 게이트 서버 내의 복수의 테이블 중에서 제 2 테이블에 상기 제 44 사서함 번호를 저장한다. 이때, 상기 제 3 클라우드 포켓은 스레드를 이용해서, 전체 클라우드 포켓(300) 중에서 해당 제 3 클라우드 포켓을 제외한 나머지 클라우드 포켓(300)에 해당 제 44 사서함 번호를 각각 업데이트한다.
- [0364] 또한, 상기 제 1 사용자 단말은 상기 접속 중인 제 2 게이트 서버 내의 제 2 테이블에 등록된 제 44 사서함 번호를 표시한다.
- [0365] 다른 일 예로, 상기 제 3 클라우드 포켓은 복수의 메인 서버(400) 중에서 제 4 메인 서버와 연결하고, 상기 연결된 제 4 메인 서버에 블록 수정 기능 수행 결과를 전송한다.
- [0366] 또한, 또한, 상기 제 4 메인 서버는 상기 제 3 클라우드 포켓으로부터 전송되는 블록 수정 기능 수행 결과를 수신한다.
- [0367] 또한, 상기 제 4 메인 서버는 해당 제 4 메인 서버에서 관리하는 복수의 테이블 중에서 제 55 테이블에 상기 수신된 블록 수정 기능 수행 결과를 저장하고, 해당 블록 수정 기능 수행 결과가 저장된 제 55 테이블에 대응하는 제 55 사서함 번호를 상기 제 3 클라우드 포켓에 전송한다.
- [0368] 또한, 상기 제 4 메인 서버는 상기 복수의 메인 서버(400) 중에서 상기 제 4 메인 서버를 제외한 나머지 모든 메인 서버(400)와 각각 연동하여, 상기 블록 수정 기능 수행 결과를 공유하여, 각각의 나머지 메인 서버(400)에서 해당 블록 수정 기능 수행 결과를 각각 저장하도록 구성한다.
- [0369] 또한, 상기 제 3 클라우드 포켓은 상기 제 4 메인 서버로부터 전송되는 제 55 사서함 번호를 수신한다.
- [0370] 또한, 상기 제 3 클라우드 포켓은 미리 설정된 주기로 해당 제 23 게이트 서버와 연결한 후, 상기 제 23 게이트 서버 내의 복수의 테이블 중에서 제 24 테이블에 상기 제 55 사서함 번호를 저장한다. 이때, 상기 제 3 클라우드 포켓은 스레드를 이용해서, 전체 클라우드 포켓(300) 중에서 해당 제 3 클라우드 포켓을 제외한 나머지 클라우드 포켓(300)에 해당 제 55 사서함 번호를 각각 업데이트한다.
- [0371] 또한, 상기 제 2 사용자 단말은 상기 접속 중인 제 23 게이트 서버 내의 제 24 테이블에 등록된 제 55 사서함 번호를 표시한다(S590).
- [0372] 본 발명의 실시예는 앞서 설명된 바와 같이, 사용자 단말에서 원본 데이터를 인증키를 이용해서 암호화하여 암호 블록을 생성하고, 암호 블록과 타임스탬프를 포함하는 요구 정보를 게이트 서버에 등록하고, 클라우드 포켓에서 게이트 서버에 접속하여 요구 정보를 확인한 후, 요구 정보에 포함된 암호 블록을 복호하여 원본 데이터를 복원하고, 블록체인에 새로운 블록으로 해당 원본 데이터를 저장하거나, 기존 데이터를 해당 원본 데이터로 수정하여, 블록체인을 개인 PC나 디바이스에 구성하는 것이 아니라, 네트워크에 연결되어 있는 클라우드 포켓에 구성함에 따라 개인 디바이스에는 아무 정보도 보관하지 않고, 사용자와 클라우드 포켓 간에 연결하는 암호화 블록 프로토콜만 존재하는 상태에서, 수많은 클라우드 포켓들이 서로 네트워크상에 PtoP로 연결되어 실시간 처리를 통해 화폐의 기능이 가능하며, 실시간 수정, 송신, 생성할 수 있고, 통화량 제어가 가능하고, 가상화폐의 흐름을 추적할 수 있다.
- [0373] 또한, 본 발명의 실시예는 앞서 설명된 바와 같이, 사용자 단말에서 웹 서버로 아이디와 비밀번호를 이용해서 로그인한 후, 요청에 따라 웹 서버에서 제공하는 인증용 블록을 수신하고, 수신된 인증용 블록을 게이트 서버에 등록한 후, 클라우드 포켓에서 사용자 단말이 게이트 서버에 등록된 인증용 블록과 웹 서버가 게이트 서버에 등록된 인증용 블록 간의 일치 여부 확인에 따라 인증 여부를 확인한 후, 인증에 성공한 경우 유효 기간이 설정된 인증키를 생성하여 게이트 서버에 등록하고, 사용자 단말에서 게이트 서버에 등록된 인증키를 이용해서 게이트 서버 및 클라우드 포켓과 연동하여 원본 데이터를 블록 형태로 클라우드 블록체인에 등록하여, 사용자 단말에서는 유효 기간이 설정된 인증키를 이용해서 블록을 생성, 수정 등을 효율적으로 수행할 수 있다.
- [0374] 전술된 내용은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시예들은 본 발명의 기술 사상

을 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.

부호의 설명

- [0375]
- 10: 클라우드 블록체인 시스템

100: 사용자 단말

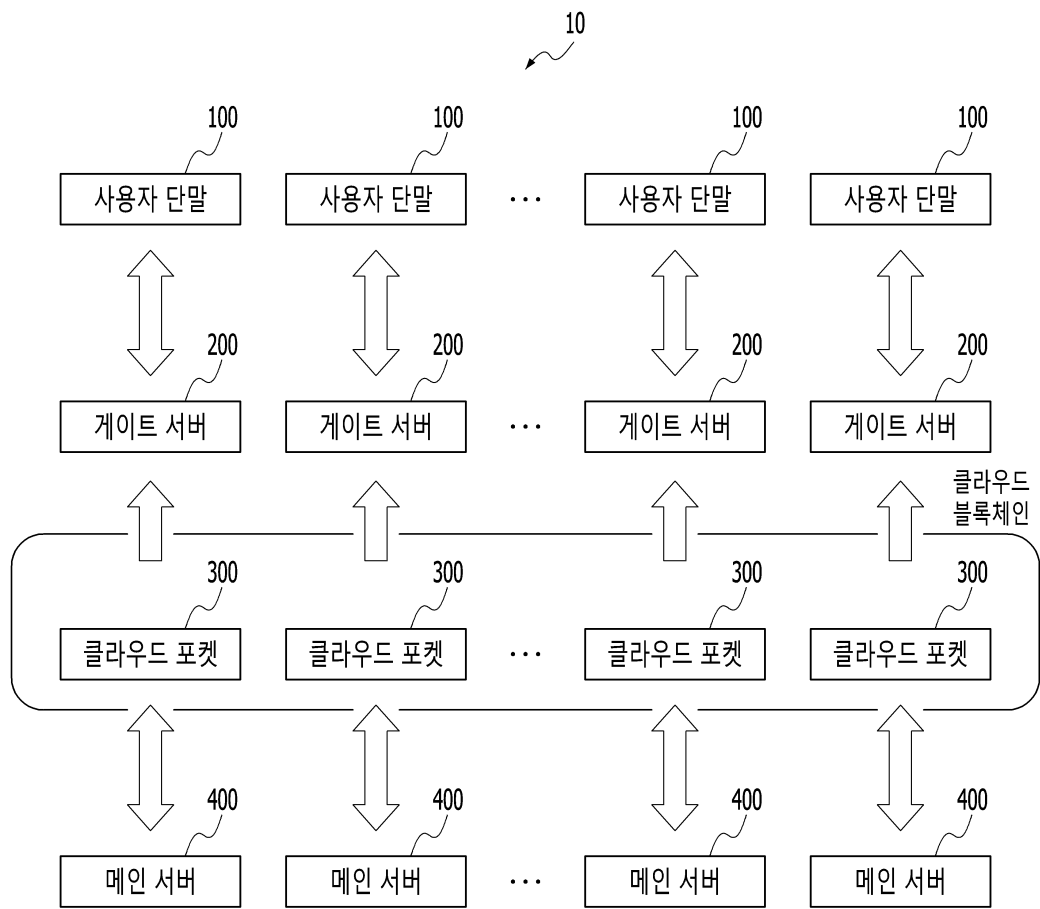
200: 복수의 게이트 서버

300: 복수의 클라우드 포켓

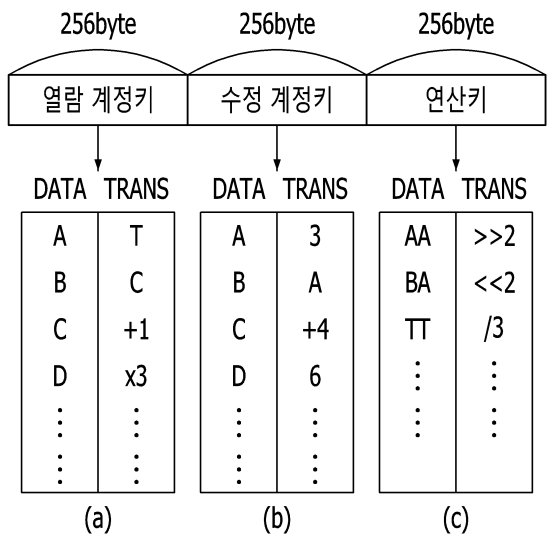
400: 복수의 메인 서버

도면

도면1



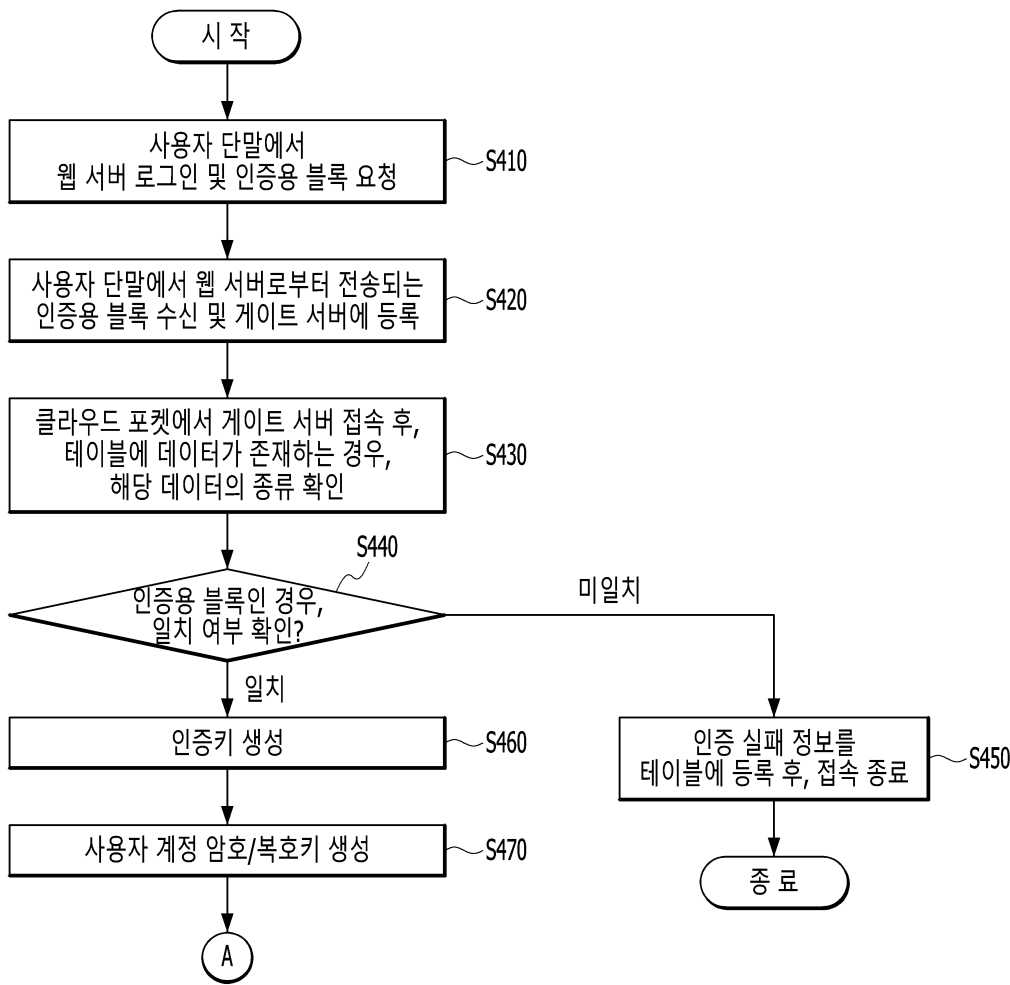
도면2



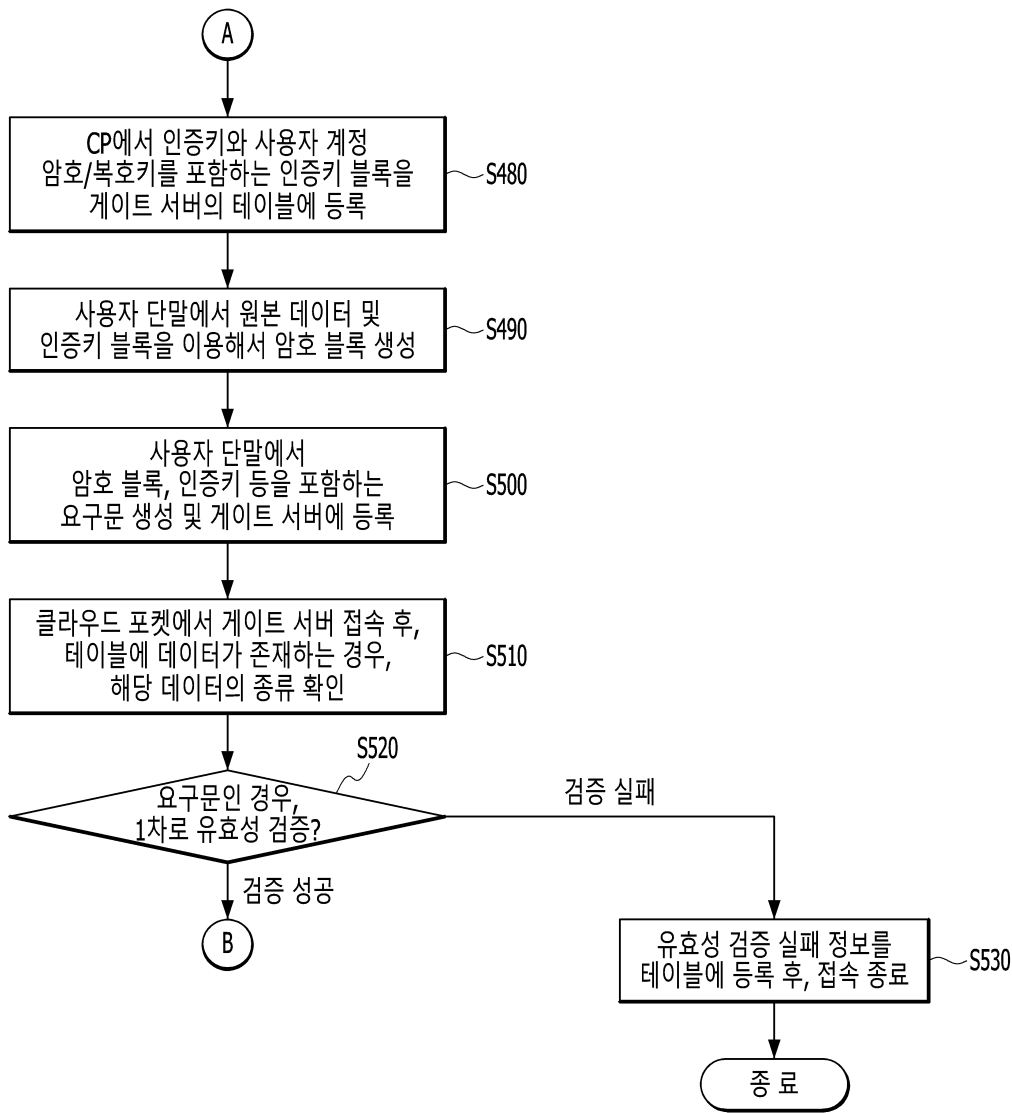
도면3

사서함 번호	테이블
1	member
2	bbs
3	info
4	content
...	...

도면4



도면5



도면6

