

명세서

발명의 명칭: 고위험 가상자산 지갑주소 관리장치 및 이를 이용한 고위험 지갑주소 조회 서비스 제공방법 기술분야

- [1] 본 발명은 금융거래 및 보안기술에 관한 것이다.

배경기술

- [2] 가상자산은 지폐·동전 등의 실물이 없고 온라인에서 거래되는 자산을 말한다. 가상자산 거래소는 가상자산을 직접 사고 파는 일을 돕기 위해 가상자산을 가진 사람과 그것을 사고자 하는 사람을 기능적으로 연결시켜 주는 역할을 한다. 우선, 가상자산을 거래하기 위해서는 고객이 거래소 홈페이지에 들어가 회원가입을 한 뒤 실명 확인한 계좌로 자금을 이체한다. 그리고 이체된 자금으로 가상자산을 매매할 수 있고, 또한, 가상자산 거래소가 지급하는 개인 전자지갑을 이용하여 가상자산을 다른 전자지갑 주소로 전송하거나 전송 받을 수 있다.
- [3] 일반적으로, 가상자산 전자지갑은 암호화 키를 보관하고 있으며, 보관된 암호화 키(또는 개인 키)를 이용한 신원 증명을 통해 가상자산에 접근할 수 있다. 또한, 이러한 가상자산 전자지갑은 가상자산에 접근하여 사용자 간 가상자산을 보내거나 받고, 거래를 수행할 수 있도록 한다. 또한, 가상자산 전자지갑은 해당 지갑 생성 시 지갑주소가 생성되며, 이러한 지갑주소는 다른 사용자에게 가상자산 전송하거나 거래시 사용될 수 있다.
- [4] 그런데, 고객이 가상자산 거래소 전자지갑에서 보유 가상자산을 다른 가상자산 거래소로 전송하고자 할 때, 수신자 전자지갑의 위험성을 파악할 수 없어 범죄 위험성이 있는 전자지갑으로 가상자산을 전송하고자 하는 고객을 통제할 수 없는 문제점이 있었다.
- [5] 따라서, 가상자산 거래소는 고객이 이용하는 전자지갑 주소의 위험성을 파악할 수 있는 현실적인 기술이 필요하다.

발명의 상세한 설명

기술적 과제

- [6] 일 실시 예에 따라, 가상자산 거래소 고객의 가상자산 전송 요청 시 사용되는 가상자산 지갑주소의 위험성 여부를 조회하여 제공함에 따라 고위험 전자지갑주소나 이상거래가 탐지된 전자지갑주소를 대상으로 부정사용을 사전에 차단하고 거래소를 보호할 수 있는 고위험 가상자산 지갑주소 관리장치 및 이를 이용한 고위험 지갑주소 조회 서비스 제공방법을 제안한다.

과제 해결 수단

- [7] 본 발명의 실시예에 따른 고위험 가상자산 지갑주소 데이터베이스 관리장치는, 복수의 가상자산 거래소 서버로부터 복수의 위험 지갑주소를 수집하는 데이터 수집부와, 수집된 복수의 위험 지갑주소를 데이터베이스에 저장하고, 가상자

산 거래소 서버로부터 특정 지갑주소에 대한 조회 요청을 수신하면, 상기 복수의 가상자산 거래소 서버로부터 수집된 복수의 위험 지갑주소를 데이터베이스에서 조회하여 해당 지갑주소가 위험 지갑주소인지 여부를 상기 가상자산 거래소 서버에 응답하는 데이터 관리부를 포함한다.

- [8] 데이터 수집부는, 복수의 금융기관 서버 및 복수의 공공기관 서버로부터 복수의 위험 지갑주소를 수집할 수 있고, 데이터 관리부는, 수집된 복수의 위험 지갑주소를 데이터베이스에 저장하고, 가상자산 거래소 서버로부터 특정 지갑주소에 대한 조회 요청을 수신하면, 복수의 금융기관 서버 및 공공기관 서버로부터 수집된 복수의 위험 지갑주소를 데이터베이스에서 조회하여 해당 지갑주소의 위험성 여부를 상기 가상자산 거래소 서버에 응답할 수 있다.
- [9] 데이터 수집부는, 웹 크롤링을 통해 서피스 웹(Surface web), 딥 웹(Deep web), 다크 웹(Dark web), SNS 중 적어도 하나를 포함하는 복수의 웹페이지로부터 복수의 고위험 지갑주소를 수집할 수 있고, 데이터 관리부는, 수집된 복수의 위험 지갑주소를 데이터베이스에 저장하고, 가상자산 거래소 서버로부터 특정 지갑주소에 대한 조회를 수신하면, 복수의 웹페이지로부터 수집된 복수의 위험 지갑주소를 데이터베이스에서 조회하여 해당 지갑주소의 위험성 여부를 상기 가상자산 거래소 서버에 응답할 수 있다.
- [10] 데이터 수집부는, 지갑주소에서 블록체인에 저장된 거래 내역, 전송량, 전송대상, 전송시간을 포함하는 지갑 정보를 수집하는 블록체인 탐색기와, 웹페이지에 노출된 지갑주소를 수집하는 웹 크롤러를 포함할 수 있다.
- [11] 데이터 수집부는, 위험 지갑주소의 카테고리를 정의하고, 위험 지갑주소 수집 방식을 구분하되, 제1 카테고리는 웹 크롤러를 통해 위험 지갑주소를 수집하고, 제2 카테고리는 수집된 지갑주소의 거래내역 분석을 통해 위험 지갑주소를 수집하며, 제3 카테고리는 공공기관의 웹사이트 접속을 통해 위험 지갑주소를 수집하도록 수집 방식을 구분할 수 있다.
- [12] 지갑주소 관리장치는, 데이터 수집부로부터 수집된 복수의 지갑주소를 분석하여 위험 지갑주소를 필터링 하는 데이터 분석부를 더 포함할 수 있다.
- [13] 데이터 분석부는, 수집된 지갑주소 정보를 이용하여 위험행위 패턴을 분석하고, 분석된 위험행위 패턴을 기초로 1차 위험 지갑주소를 분류하고 분류된 지갑주소를 위험도에 따라 위험도 레벨 별로 분류한 후 분류된 1차 위험 지갑주소를 데이터베이스에 저장하는 제1 분석부를 포함할 수 있다.
- [14] 데이터 분석부는, 위험 지갑주소 카테고리 별로 검색 키워드를 이용하여 1차 위험 지갑주소를 추출한 후 분류된 1차 위험 지갑주소를 데이터베이스에 저장하는 제1 데이터 분석부를 포함할 수 있다.
- [15] 제1 데이터 분석부는, 추출된 1차 위험 지갑주소의 의심 범죄 유형에 따라 유관 법령 및 관련 기관 규정을 적용하여 위험요소 평가 기준을 정의하고, 위험요소 평가 기준에 따라 지갑주소의 위험도를 수치화하고 가중치를 할당할 수 있다.

- [16] 데이터 분석부는, 1차 위험 지갑주소를 로딩하여 1차 위험 지갑주소의 거래내역 정보 분석 및 위험성 예측 모델을 통해 2차 위험 지갑주소를 추출하는 제2 데이터 분석부를 포함할 수 있다.
- [17] 다른 예에 따른 고위험 지갑주소 조회 서비스 제공방법은, 복수의 가상자산 거래소 서버로부터 위험 지갑주소 등록을 요청받아 등록하는 단계; 웹 크롤링을 통해 위험 지갑주소 카테고리 별 검색 키워드를 이용하여 1차 위험 지갑주소를 추출하는 단계와, 추출된 1차 위험 지갑주소를 데이터베이스에 저장하여 등록하는 단계와, 등록된 1차 위험 지갑주소의 거래내역을 분석하여 2차 위험 지갑주소를 추출하여 데이터베이스에 저장하는 단계를 포함한다.
- [18] 다른 실시 예에 따른 고위험 지갑주소 조회 서비스 제공방법은, 복수의 가상자산 거래소 서버로부터 위험 지갑주소 등록을 요청받아 등록하는 단계와, 가상자산 거래소 서버로부터 특정 지갑주소에 대한 조회 요청을 수신하는 단계와, 복수의 가상자산 거래소 서버로부터 등록된 위험 지갑주소를 조회하여 해당 지갑주소가 위험 지갑주소인지 여부를 확인하는 단계와, 위험 지갑주소 여부를 가상자산 거래소 서버에 응답하는 단계를 포함한다.
- [19] 지갑주소 조회 서비스 제공방법은, 복수의 공공기관 서버 및 복수의 금융기관 서버로부터 위험 지갑주소 등록을 요청받아 등록하는 단계를 더 포함하며, 해당 지갑주소가 위험 지갑주소인지 여부를 확인하는 단계에서, 복수의 공공기관 서버 및 복수의 금융기관 서버로부터 등록된 위험 지갑주소를 조회하여 해당 지갑주소가 위험 지갑주소인지 여부를 확인할 수 있다.
- [20] 지갑주소 조회 서비스 제공방법은, 웹 크롤링을 통해 위험 지갑주소를 수집하는 단계를 더 포함하며, 해당 지갑주소가 위험 지갑주소인지 여부를 확인하는 단계에서, 웹 크롤링을 통해 수집된 위험 지갑주소를 조회하여 해당 지갑주소가 위험 지갑주소인지 여부를 확인할 수 있다.
- [21] 지갑주소 조회 서비스 제공방법은, 웹 크롤링을 통해 위험 지갑주소 카테고리 별 검색 키워드를 이용하여 1차 위험 지갑주소를 추출하는 단계와, 추출된 1차 위험 지갑주소를 데이터베이스에 저장하여 등록하는 단계를 더 포함하며, 해당 지갑주소가 위험 지갑주소인지 여부를 확인하는 단계에서, 데이터베이스에 저장된 1차 위험 지갑주소를 조회하여 해당 지갑주소가 위험 지갑주소인지 여부를 확인할 수 있다.
- [22] 지갑주소 조회 서비스 제공방법은, 등록된 1차 위험 지갑주소의 거래내역을 분석하여 2차 위험 지갑주소를 추출하여 데이터베이스에 저장하는 단계를 더 포함하며, 해당 지갑주소가 위험 지갑주소인지 여부를 확인하는 단계에서, 데이터베이스에 저장된 2차 위험 지갑주소를 조회하여 해당 지갑주소가 위험 지갑주소인지 여부를 확인할 수 있다.

발명의 효과

- [23] 일 실시 예에 따른 고위험 가상자산 지갑주소 관리장치 및 이를 이용한 고위험 지갑주소 조회 서비스 제공방법은, 고객이 가상자산 거래소에 가상자산 전송 요청 시 가상자산 전송을 위한 지갑주소의 위험성 여부를 조회하여 조회결과를 제공할 수 있다.
- [24] 이에 따라, 이상거래가 탐지된 전자지갑 주소를 대상으로 부정사용을 사전에 차단하고 해당 가상자산 거래소를 금융범죄 위험으로부터 보호할 수 있다. 이때, 지갑주소 관리장치는 고객이 이용하는 가상자산 거래소뿐만 아니라, 지갑주소 관리장치와 제휴된 모든 가상자산 거래소가 등록 요청한 위험 지갑주소를 관리하고 있다가 위험성 여부를 해당 가상자산 거래소에게 알려줄 수 있으므로, 보다 안전하게 해당 가상자산 거래소를 금융범죄 위험으로부터 보호할 수 있다.
- [25] 또한, 일 실시 예에 따른 고위험 지갑주소 관리장치는 다크 웹, 서피스 웹, SNS 등으로부터 웹 크롤링을 통해 위험 지갑주소를 수집할 수 있다. 또한, 복수의 공공기관, 복수의 금융기관 등으로부터 위험 지갑주소를 수집하여 이를 가상자산 거래소에게 알려줄 수 있으므로, 보다 안전하게 해당 가상자산 거래소를 금융범죄 위험으로부터 보호할 수 있다.
- [26] 나아가, 일 실시 예에 따른 지갑주소 관리장치는 위험 지갑주소 카테고리 별로 검색 키워드를 이용하여 1차 위험 지갑주소를 추출할 수 있고, 1차 위험 지갑주소의 거래내역 정보 분석 및 위험성 예측 모델을 통해 2차 위험 지갑주소를 추출할 수 있다. 이에 따라, 위험 지갑주소 분석과정을 거치므로 보다 정확하게 위험 지갑주소를 추출할 수 있다.

도면의 간단한 설명

- [27] 도 1은 본 발명의 일 실시 예에 따른 고위험 가상자산 지갑주소 관리시스템의 구성을 도시한 도면,
- [28] 도 2는 본 발명의 일 실시 예에 따른 도 1의 지갑주소 관리장치의 세부 구성을 도시한 도면,
- [29] 도 3은 본 발명의 일 실시 예에 따른 프로세서의 세부 구성을 도시한 도면,
- [30] 도 4는 본 발명의 일 실시 예에 따른 블록체인 탐색기를 통해 수집된 정보를 분석하여 1차 위험 지갑주소를 추출하는 프로세스를 도시한 도면,
- [31] 도 5는 본 발명의 일 실시 예에 따른 웹 크롤러를 통해 수집된 정보를 분석하여 1차 위험 지갑주소를 추출하는 프로세스를 도시한 도면,
- [32] 도 6은 본 발명의 일 실시 예에 따른 2차 위험 지갑주소를 추출하는 프로세스를 도시한 도면,
- [33] 도 7은 본 발명의 일 실시 예에 따른 고위험 지갑주소 등록 및 등록 해지 프로세스를 도시한 도면,
- [34] 도 8은 본 발명의 일 실시 예에 따른 고위험 지갑주소 조회 서비스 제공방법의 흐름을 도시한 도면이다.

발명의 실시를 위한 최선의 형태

- [35] 이상의 본 발명의 목적들, 다른 목적들, 특징들 및 이점들은 첨부된 도면과 관련된 이하의 바람직한 실시 예들을 통해서 쉽게 이해될 것이다. 그러나 본 발명은 여기서 설명되는 실시 예들에 한정되지 않고 다른 형태로 구체화될 수도 있다. 오히려, 여기서 소개되는 실시 예들은 개시된 내용이 철저하고 완전해질 수 있도록 그리고 당업자에게 본 발명의 사상이 충분히 전달될 수 있도록 하기 위해 제공되는 것이다.
- [36] 본 명세서에서, 어떤 구성요소가 다른 구성요소 상에 있다고 언급되는 경우에는 그것은 다른 구성요소 상에 직접 형성될 수 있거나 또는 그들 사이에 제3의 구성요소가 개재될 수도 있다는 것을 의미한다.
- [37] 본 명세서에서 제1, 제2 등의 용어가 구성요소들을 기술하기 위해서 사용된 경우, 이들 구성요소들이 이 같은 용어들에 의해서 한정되어서는 안 된다. 이들 용어들은 단지 어느 구성요소를 다른 구성요소와 구별시키기 위해서 사용되었을 뿐이다. 여기에 설명되고 예시되는 실시 예들은 그것의 상보적인 실시 예들도 포함한다.
- [38] 또한, 제1 엘리먼트(또는 구성요소)가 제2 엘리먼트(또는 구성요소) 상(ON)에서 동작 또는 실행된다고 언급될 때, 제1 엘리먼트(또는 구성요소)는 제2 엘리먼트(또는 구성요소)가 동작 또는 실행되는 환경에서 동작 또는 실행되거나 또는 제2 엘리먼트(또는 구성요소)와 직접 또는 간접적으로 상호 작용을 통해서 동작 또는 실행되는 것으로 이해되어야 할 것이다.
- [39] 어떤 엘리먼트, 구성요소, 장치, 또는 시스템이 프로그램 또는 소프트웨어로 이루어진 구성요소를 포함한다고 언급되는 경우, 명시적인 언급이 없더라도, 그 엘리먼트, 구성요소, 장치, 또는 시스템은 그 프로그램 또는 소프트웨어가 실행 또는 동작하는데 필요한 하드웨어(예를 들면, 메모리, CPU 등)나 다른 프로그램 또는 소프트웨어(예를 들면 운영체제나 하드웨어를 구동하는데 필요한 드라이버 등)를 포함하는 것으로 이해되어야 할 것이다.
- [40] 또한, 어떤 엘리먼트(또는 구성요소)가 구현됨에 있어서 특별한 언급이 없다면, 그 엘리먼트(또는 구성요소)는 소프트웨어, 하드웨어, 또는 소프트웨어 및 하드웨어 어떤 형태로도 구현될 수 있는 것으로 이해되어야 할 것이다.
- [41] 또한, 본 명세서에서 사용된 용어는 실시 예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 '포함한다(comprises)' 및/또는 '포함하는(comprising)'은 언급된 구성요소는 하나 이상의 다른 구성요소의 존재 또는 추가를 배제하지 않는다.
- [42] 이하, 아래의 특정 실시 예들을 기술하는데 있어서, 여러 가지의 특정적인 내용들은 발명을 더 구체적으로 설명하고 이해를 돕기 위해 작성되었다. 하지만 본 발명을 이해할 수 있을 정도로 이 분야의 지식을 갖고 있는 독자는 이러한 여러 가지의 특정적인 내용들이 없어도 사용될 수 있다는 것을 인지할 수 있다.

- [43] 어떤 경우에는, 발명을 기술하는 데 있어서 흔히 알려졌으면서 발명과 크게 관련 없는 부분들은 본 발명을 설명하는 데 있어 별 이유 없이 혼돈이 오는 것을 막기 위해 기술하지 않음을 미리 언급해 둔다.
- [44] 이하, 본 명세서의 실시 예를 첨부된 도면을 참조하여 설명한다. 본 명세서에 따른 동작 및 작용을 이해하는 데 필요한 부분을 중심으로 상세히 설명한다. 본 명세서의 실시 예를 설명하면서, 본 명세서가 속하는 기술 분야에 익히 알려졌고 본 명세서와 직접적으로 관련이 없는 기술 내용에 대해서는 설명을 생략한다. 이는 불필요한 설명을 생략함으로써 본 명세서의 요지를 흐리지 않고 더욱 명확히 전달하기 위함이다.
- [45] 또한, 본 명세서의 구성 요소를 설명하는 데 있어서, 동일한 명칭의 구성 요소에 대하여 도면에 따라 다른 참조부호를 부여할 수도 있으며, 서로 다른 도면임에도 동일한 참조부호를 부여할 수도 있다. 그러나 이와 같은 경우라 하더라도 해당 구성 요소가 실시 예에 따라 서로 다른 기능을 갖는다는 것을 의미하거나, 서로 다른 실시 예에서 동일한 기능을 갖는다는 것을 의미하는 것은 아니며, 각각의 구성 요소의 기능은 해당 실시 예에서의 각각의 구성 요소에 대한 설명에 기초하여 판단하여야 할 것이다.
- [46] 본 명세서에서 각각의 구성들은 기능 및/또는 논리적으로 분리될 수 있음을 나타내는 것이며, 반드시 각각의 구성이 별도의 물리적 장치로 구분되거나 별도의 코드로 작성됨을 의미하는 것은 아님을 본 발명의 기술분야의 평균적 전문가가 용이하게 추론할 수 있을 것이다.
- [47] 또한, 본 명세서에서 각각의 구성들은, 본 발명의 기술적 사상을 수행하기 위한 하드웨어 및 하드웨어를 구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미할 수 있다. 예컨대, 소정의 코드와 소정의 코드가 수행되기 위한 하드웨어 리소스의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된 코드를 의미하거나, 한 종류의 하드웨어를 의미하는 것이 아님은 본 발명의 기술분야의 평균적 전문가에게는 용이하게 추론될 수 있다.
- [48] 본 발명의 실시 예에서 가상자산을 전송하는 것은 블록체인 네트워크 상에서 가상자산이 거래되는 트랜잭션을 의미하는 것으로 사용될 수 있다.
- [49] 이하, 도면을 참조하여 본 발명의 실시 예를 설명한다.
- [50] 도 1은 본 발명의 일 실시 예에 따른 가상자산 지갑주소 관리 시스템의 구성을 도시한 도면이다.
- [51] 도 1을 참조하면, 가상자산 지갑주소 관리시스템(1)은 고객 단말(10), 복수의 가상자산 거래소 서버(11), 지갑주소 관리장치(12), 복수의 공공기관 서버(13), 복수의 금융기관 서버(14) 및 복수의 웹 서버(15)를 포함한다.
- [52] 지갑주소 관리장치(12)는 가상자산을 전송 하기 위한 지갑주소를 수집하고 관리한다. 지갑주소 관리장치(12)는 자금세탁, 범죄 관련 의심이 되는 고위험 지갑주소를 수집하여 관리하고 있다가 소정의 가상자산 거래소 서버(11)의 요청 시 위험성을 조회하여 조회 결과를 제공한다.

- [53] 각 자산자산 거래소 서버(11)는 고객이 고객 단말(10)을 통해 가상자산 전송 요청 시 고객이 가상자산을 전송하고자 하는 지갑주소가 위험 지갑주소에 해당하면 해당 고객의 가상자산 전송 요청을 거부할 수 있다.
- [54] 지갑주소 관리장치(12)는 복수의 가상자산 거래소 서버(11), 복수의 공공기관 서버(13) 및 복수의 금융기관 서버(14), 복수의 웹 서버(15)로부터 제공되는 지갑주소를 수집할 수 있다. 도 1에서는 각 서버 별로 3개를 한정하고 있으나, 이는 설명의 이해를 돕기 위한 것일 뿐, 이에 한정되지는 않는다.
- [55] 공공기관의 예로는 은행연합회, 경찰청, 금융감독원, 국세청, 관세청, 기획재정부, 법무부, 금융위원회 등이 있다. 금융기관의 예로는 은행, 증권사 등의 금융회사가 있다. 웹 서버(13)가 제공하는 웹페이지의 예로는 서피스 웹(Surface web), 딥 웹(Deep web), 다크 웹(Dark web), SNS 등이 있다. SNS는 텔레그램, 디스코드 등이 있다.
- [56] 지갑주소 관리장치(12)는 소정의 가상자산 거래소 서버, 예를 들어, 제1 가상자산 거래소 서버(11-1)로부터 지갑주소 조회를 요청받으면, 조회를 요청받은 제1 가상자산 거래소 서버(11-1)뿐만 아니라, 지갑주소 관리장치(12)와 연결된 다른 가상자산 거래소 서버(11-2, 11-3)로부터 등록된 지갑주소를 조회하여 해당 지갑주소의 위험성 여부를 통보해 줄 수 있다.
- [57] 예를 들어, 고객 단말(10)이 제1 가상자산 거래소 서버(11-1)에 가상자산 전송을 요청한다. 그러면, 제1 가상자산 거래소 서버(11-1)는 지갑주소 관리장치(12)에 해당 가상자산을 전송 하기 위한 지갑주소가 위험 지갑주소인지 여부를 지갑주소 관리장치(12)에 조회한다. 이어서, 지갑주소 관리장치(12)는 데이터베이스에서 조회하여 다른 가상자산 거래소 서버(11-2, 11-3)로부터 등록받아 저장된 지갑주소를 조회하여 위험 지갑주소인지 여부를 확인하고, 위험 지갑주소 확인 결과를 제1 가상자산 거래소 서버(11-1)에 제공한다.
- [58] 고객 단말(10)은 가상자산 거래소 서버(11)에 접속하여 가상자산 거래소 서버(11)의 서비스를 제공받는다. 고객은 가상자산 거래소 서버(11)의 서비스를 이용하는 고객 단말(10) 사용자이다. 고객 단말(10)은 고객이 사용 가능한 모든 단말을 포함하며, 특히 휴대폰과 PC단말일 수 있다.
- [59] 지갑주소 관리장치(12)는 가상자산 거래소 서버(11)와 전산 상으로 연결되어 고객의 가상자산 거래소 서버(11)로의 전송을 관리한다.
- [60] 금융기관 서버(14)는, 불법 재산의심거래 보고, 고액현금거래 보고, 고객확인, 수사기관 정보제공을 처리한다.
- [61] 도 2는 본 발명의 일 실시 예에 따른 도 1의 지갑주소 관리장치의 세부 구성을 도시한 도면이다.
- [62] 도 1 및 도 2를 참조하면, 지갑주소 관리장치(12)는 프로세서(120) 및 데이터베이스(125)를 포함한다. 프로세서(120)는 데이터 수집부(121), 데이터 관리부(122) 및 데이터 분석부(123)를 포함한다.

- [63] 데이터 수집부(121)는 복수의 가상자산 거래소 서버(11)로부터 위험 지갑주소 등록 요청을 수신할 수 있다. 또는, 데이터 수집부(121)는 복수의 공공기관 서버(13)로부터 위험 지갑주소에 대한 등록 요청을 수신할 수 있다. 또는 데이터 수집부(20)는 복수의 금융기관 서버(14)로부터 위험 지갑주소에 대한 등록 요청을 수신할 수도 있다. 다른 예로, 데이터 수집부(121)는 복수의 가상자산 거래소 서버(11), 복수의 공공기관 서버(13), 복수의 금융기관 서버(14) 등으로부터 수집할 수 없는 위험 지갑주소를 서퍼스 웹, 딥 웹, 다크 웹, SNS 등으로부터 수집할 수도 있다.
- [64] 데이터 관리부(122)는 제휴한 복수의 가상자산 거래소에 대한 지갑주소 위험 여부를 관리한다.
- [65] 데이터 관리부(122)는 데이터 수집부(121)를 통해 수집된 복수의 위험 지갑주소를 데이터베이스(125)에 저장한다. 이때, 수집 경로는 복수의 가상자산 거래소 서버, 복수의 금융기관 서버, 복수의 공공기관 서버, 웹 페이지(서퍼스 웹, 딥 웹, 다크 웹, SNS) 등이 있다.
- [66] 이후, 데이터 관리부(122)가 소정의 가상자산 거래소 서버로부터 특정 지갑주소에 대한 조회 요청을 수신하면, 데이터베이스(125)에 저장된 복수의 위험 지갑주소를 데이터베이스(125)에서 조회하여 해당 지갑주소가 위험 지갑주소인지 여부를 확인하고, 위험 지갑주소 여부를 소정의 가상자산 거래소 서버에 응답할 수 있다.
- [67] 데이터베이스(125)는 각종 저장매체로서, 프로세서(120) 동작 시 생성되는 정보 또는 프로세서(120) 동작을 위해 필요한 정보 및 명령이 저장된다. 데이터베이스(125)에는 데이터 수집부(121)를 통해 수집된 복수의 위험 지갑주소가 저장된다.
- [68] 도 3은 본 발명의 일 실시 예에 따른 프로세서의 세부 구성을 도시한 도면이다.
- [69] 도 2 및 도 3을 참조하면, 프로세서(12)의 데이터 수집부(121)는 블록체인 탐색기(1211) 및 웹 크롤러(1212)를 포함한다.
- [70] 블록체인 탐색기(1211)는 지갑주소에서 지갑주소 정보를 수집할 수 있다. 지갑주소 정보는 블록체인에 저장된 거래(트랜잭션) 내역, 거래량, 거래 대상, 거래 시간 등을 포함한다. 웹 크롤러(1212)는 웹페이지에 노출된 지갑주소를 수집한다. 이때, 웹페이지는 다크 웹, 서피스 웹, 텔레그램과 같은 SNS 등이 있다.
- [71] 데이터 분석부(123)는 데이터 수집부(121)로부터 수집된 복수의 지갑주소를 분석하여 위험 지갑주소를 필터링 한다. 데이터 분석부(123)는 제1 데이터 분석부(1231) 및 제2 데이터 분석부(1232)를 포함할 수 있다.
- [72] 제1 데이터 분석부(1231)는 지갑주소 정보를 분석 및 분류한다. 이때, 제1 데이터 분석부(1231)는 1차 위험 지갑주소를 추출하여 도면에 도시된 바와 같이 데이터 관리부(122)를 통해 데이터베이스(125)에 저장하고, 1차 위험 지갑주소에서 확인할 수 있는 지갑주소 정보를 데이터베이스(125)에 저장할 수 있다. 제1 데이터

분석부(1231)의 1차 위험 지갑주소 추출 프로세스는 도 4 및 도 5를 참조로 하여 후술한다.

- [73] 제2 데이터 분석부(1232)는 1차 위험 지갑주소를 로딩하여 1차 위험 지갑주소의 거래내역 정보 분석 및 위험성 예측 모델을 통해 2차 위험 지갑주소를 추출한다. 예를 들어, 제2 데이터 분석부(1232)는 이전 거래의 거래내역을 분석하여 불법, 사기 행위 및 기 분류된 위험 주소와 거래 여부를 확인할 수 있다. 다른 예로, 제2 데이터 분석부(1232)는 단기간에 많은 코인이 거래되거나, 다수의 거래가 이루어진 경우와 같은 이상거래를 확인할 수 있다. 제2 데이터 분석부(1232)의 위험성 예측 모델을 통한 2차 위험 지갑주소 추출 프로세스는 도 6을 참조로 하여 후술한다.
- [74] 도 4는 본 발명의 일 실시 예에 따른 블록체인 탐색기를 통해 수집된 정보를 분석하여 1차 위험 지갑주소를 추출하는 프로세스를 도시한 도면이다.
- [75] 도 1, 도 3 및 도 4를 참조하면, 데이터 수집부(121)는 크롤링 할 지갑주소 대상을 선택한다(410). 대상이 되는 지갑주소는 대상 그룹(범죄자, 위험한 개인, 조직 등)이 보유하고 있는 지갑주소, 과거 범죄사례가 발생한 지갑주소, 유해 콘텐츠와 연결되어 있는 지갑주소 등이 포함될 수 있다.
- [76] 이어서, 데이터 수집부(121)는 블록체인 탐색기(1211)를 통해, 선택된 지갑주소에서 블록체인에 저장된 지갑주소 정보를 수집한다(420). 지갑주소 정보는 거래(트랜잭션) 내역, 거래량, 거래 대상, 거래 시간 등이 있다.
- [77] 이어서, 제1 데이터 분석부(1231)는 수집된 지갑주소 정보를 이용하여 위험 행위 패턴을 분석한다(430). 이상거래는 예를 들어, 주기적 또는 단기간에 큰 금액 또는 다수의 거래가 이루어지는 행위, 기 분류된 위험 지갑주소와의 거래 여부 등을 포함한다.
- [78] 이어서, 제1 데이터 분석부(1231)는 분석된 위험행위 패턴을 이용하여 1차 위험 지갑주소를 분류한다(440). 이때, 제1 데이터 분석부(1231)는 위험도에 따라 분류된 지갑주소를 위험도 레벨 별로 분류할 수 있다.
- [79] 이어서, 제1 데이터 분석부(1231)는 분류된 1차 위험 지갑주소를 데이터 관리부(122)를 통해 데이터베이스에 저장한다(450). 이때, 제1 데이터 분석부(1231)는 추가 위험요소, 패턴을 찾아 최종 학습 데이터로 정의할 수 있다.
- [80] 도 5는 본 발명의 일 실시 예에 따른 웹 크롤러를 통해 수집된 정보를 분석하여 1차 위험 지갑주소를 추출하는 프로세스를 도시한 도면이다.
- [81] 도 1, 도 3 및 도 5를 참조하면, 데이터 수집부(121)는 위험 지갑주소 카테고리를 정의한다(510). 카테고리는 블랙리스트, 사이버범죄, 금융범죄, 기타범죄, 자금세탁위험, 일반범죄, 무역경제범죄, 조세범죄 등일 수 있다.
- [82] 이어서, 데이터 수집부(121)는 위험 지갑주소의 수집 방식을 구분한다(520). 예를 들어, 블랙리스트, 사이버범죄, 금융범죄, 기타범죄 카테고리의 경우, 웹 크롤러(1212)를 통해 위험 지갑주소를 수집 가능하다. 자금세탁위험 카테고리의 경우, 수집된 지갑주소의 거래내역 분석을 통해 위험 지갑주소를 수집 가능하다.

일반범죄, 무역경제범죄, 조세범죄 등의 카테고리의 경우 웹 크롤링을 통해 수집 불가능하다. 이 경우, 공공기관의 웹사이트 접속을 통해 위험 지갑주소를 수집 가능하다.

- [83] 이어서, 제1 데이터 분석부(1231)는 블랙리스트, 사이버범죄, 금융범죄, 기타범죄 카테고리의 경우, 웹 크롤러(1212)를 통해 위험 지갑주소 카테고리 별 검색 키워드를 이용하여 1차 위험 지갑주소를 자동으로 추출한다(530). 이때, 서피스 웹, 다크 웹, SNS 등을 이용할 수 있다.
- [84] 이어서, 제1 데이터 분석부(1231)는 추출된 1차 위험 지갑주소의 연루 범죄 유형에 따라 유관 법령, 관련 기관 규정을 적용하여 위험요소 평가 기준을 정의하고, 위험요소 평가 기준에 따라 지갑주소의 위험도를 수치화하고 가중치를 할당하여 고위험 지갑주소를 추출할 수 있다(540).
- [85] 이어서, 제1 데이터 분석부(1231)는 추출된 1차 위험 지갑주소를 데이터관리부(122)를 통해 데이터베이스(125)에 저장한다(550).
- [86] 도 6은 본 발명의 일 실시 예에 따른 2차 위험 지갑주소를 추출하는 프로세스를 도시한 도면이다.
- [87] 도 1, 도 3 및 도 6을 참조하면, 제2 데이터 분석부(1232)는 1차 수집된 1차 위험 지갑주소를 로딩한다(610).
- [88] 이어서, 제2 데이터 분석부(1232)는 블록과 지갑의 전송자, 수신자, 전송량, 수수료, 거래 시간, 이전 거래 블록, 전자서명 및 거래 해시 등과 같은 거래내역 정보를 추출하는 전처리 과정을 수행한다(620).
- [89] 이어서, 제2 데이터 분석부(1232)는 모델을 학습하기 위해 그래프를 생성한다(630). 그래프 생성 단계(630)에서, 제2 데이터 분석부(1232)는 모든 지갑주소와 거래 정보를 그래프 노드로 만들고, 각 거래 정보에 대해 연결선을 추가할 수 있다.
- [90] 이어서, 제2 데이터 분석부(1232)는 위험 행위 패턴을 학습할 때 사용할 라벨링을 추가한다(640). 예를 들어, 대량 거래가 발생하는 지갑주소에 대한 라벨을 추가할 수 있다.
- [91] 이어서, 제2 데이터 분석부(1232)는 모델을 학습한다(650). 모델 학습 단계(650)에서 제2 데이터 분석부(1232)는 학습 데이터를 모델에 제공하고, 모델이 위험 행위 패턴을 탐지할 수 있다.
- [92] 이어서, 제2 데이터 분석부(1232)는 학습된 모델을 사용하여 새로운 지갑주소에 대한 위험 가능성을 예측한다(660). 예측 단계(660)에서, 제2 데이터 분석부(1232)는 모델이 학습하지 않은 지갑주소를 입력으로 제공하고, 모델이 해당 주소가 위험 행위 패턴과 연관되어 있는지 여부를 예측할 수 있다.
- [93] 이어서, 제2 데이터 분석부(1232)는 모델이 생성한 예측 결과를 평가한다(670). 평가 단계(670)에서, 제2 데이터 분석부(1232)는 모델이 생성한 예측이 정확하게 이루어졌는지 확인하고, 모델의 성능을 평가할 수 있다.

- [94] 도 7은 본 발명의 일 실시 예에 따른 지갑주소 등록 및 등록 해지 프로세스를 도시한 도면이다.
- [95] 도 2 및 도 7을 참조로 하여 위험 지갑주소 등록 프로세스에 대해 후술한다.
- [96] 가상자산 거래소 서버(11)는 위험 지갑주소 사유가 발생하면, 등록사유 별 코드를 분리하고 해당 지갑주소 관련 가상자산 거래를 금지한다(710).
- [97] 이어서, 가상자산 거래소 서버(11)는 위험 지갑주소 등록을 데이터 관리부(122)에 요청한다(711). 이때, 코인명, 지갑주소, 등록사유 코드 등을 함께 전송할 수 있다.
- [98] 이어서, 데이터 관리부(122)는 가상자산 거래소 서버(11)로부터 요청받은 위험 지갑주소를 등록(712) 하고, 거래소 코드 별로 지갑주소를 관리한다.
- [99] 이어서, 데이터 관리부(122)는 가상자산 거래소 서버(11)에 위험 지갑주소 등록 응답 메시지를 전송한다(713).
- [100] 나아가, 데이터 수집부(121)는 웹 크롤링을 통해 위험 지갑주소 카테고리 별 검색 키워드를 이용하여 1차 위험 지갑주소를 추출한다(721).
- [101] 이어서, 데이터 수집부(121)는 추출된 1차 위험 지갑주소를 데이터 관리부(122)에 전송하고 데이터 관리부(122)가 이를 데이터베이스에 저장한다(722).
- [102] 이어서, 데이터 관리부(122)는 등록된 1차 위험 지갑주소를 데이터베이스에 등록하고, 1차 위험 지갑주소를 통한 거래내역 분석을 데이터 분석부(123)에 요청한다(723).
- [103] 이어서, 데이터 분석부(123)는 1차 위험 지갑주소의 거래내역을 분석하여 2차 위험 지갑주소를 추출한다(724).
- [104] 이어서, 데이터 분석부(123)는 추출된 2차 위험 지갑주소를 데이터 관리부(122)에 전송하여 데이터베이스에 저장한다(725).
- [105] 이하, 위험 지갑주소 등록 해지 프로세스에 대해 후술한다.
- [106] 가상자산 거래소 서버(11)는 등록된 위험 지갑주소의 해지 사유가 발생하면, 해당 지갑주소 관련 가상자산의 거래 금지를 해제한다(731).
- [107] 이어서, 가상자산 거래소 서버(11)는 데이터 관리부(122)에 위험 지갑주소 해지를 요청한다(732). 이때, 등록 거래번호 등을 함께 전송할 수 있다.
- [108] 이어서, 데이터 관리부(122)는 위험 지갑주소 등록을 해지(733) 하고, 거래소 코드 별 지갑주소를 관리한다(733).
- [109] 이어서, 데이터 관리부(122)는 가상자산 거래소 서버(11)에 위험 지갑주소 해지 응답 메시지를 전송한다(734).
- [110] 도 8은 본 발명의 일 실시 예에 따른 지갑주소 조회 서비스 제공방법의 흐름을 도시한 도면이다.
- [111] 도 1 및 도 8을 참조하면, 고객 단말(10)이 가상자산 거래소 서버(11)에 고객 가상자산 거래 요청을 전송한다(811).
- [112] 이어서, 가상자산 거래소 서버(11)는 지갑주소 관리장치(12)에 소정의 지갑주소에 대한 조회를 요청한다(812).

- [113] 이어서, 지갑주소 관리장치(12)는 데이터베이스에 저장된 위험 지갑주소를 조회하여 해당 지갑주소 위험성 여부를 확인한다(813). 데이터베이스에 저장된 위험 지갑주소는, 복수의 가상자산 거래소 서버, 복수의 금융기관 서버, 복수의 공공기관 서버, 웹 페이지(서피스 웹, 딥 웹, 다크 웹, SNS) 등으로부터 수집되어 저장된 것들이다.
- [114] 이어서, 위험 지갑주소이면 위험 지갑주소임을 알리는 응답 메시지를 가상자산 거래소 서버(11)에 전송한다(814). 그러면, 가상자산 거래소 서버(11)는 고객 단말(10)에 가상자산 거래를 거부하거나 고객 확인을 요청할 수 있다(815).
- [115] 이에 비해, 위험 지갑주소가 아니면, 위험 지갑주소가 아님을 알리는 응답 메시지를 가상자산 거래소 서버(11)에 전송한다(816).
- [116] 응답 메시지는 응답 값(정상, 오류), 오류코드, 블랙리스트 등록기관 코드 등을 포함할 수 있다.
- [117] 상기와 같이, 본 발명에 따른 고위험 가상자산 지갑주소 관리장치 및 이를 이용한 고위험 지갑주소 조회 서비스 제공방법은, 고객이 가상자산 거래소에 가상자산 전송 요청 시 가상자산 전송을 위한 지갑주소의 위험성 여부를 조회하여 조회 결과를 제공할 수 있다.
- [118] 이에 따라, 이상거래가 탐지된 전자지갑 주소를 대상으로 부정사용을 사전에 차단하고 해당 가상자산 거래소를 금융범죄 위험으로부터 보호할 수 있다. 이때, 지갑주소 관리장치는 고객이 이용하는 가상자산 거래소뿐만 아니라, 지갑주소 관리장치와 제휴된 모든 가상자산 거래소가 등록 요청한 위험 지갑주소를 관리하고 있다가 위험성 여부를 해당 가상자산 거래소에게 알려줄 수 있으므로, 보다 안전하게 해당 가상자산 거래소를 금융범죄 위험으로부터 보호할 수 있다.
- [119] 또한, 일 실시 예에 따른 고위험 지갑주소 관리장치는 다크 웹, 서피스 웹, SNS 등으로부터 웹 크롤링을 통해 위험 지갑주소를 수집할 수 있다. 또한, 복수의 공공기관, 복수의 금융기관 등으로부터 위험 지갑주소를 수집하여 이를 가상자산 거래소에게 알려줄 수 있으므로, 보다 안전하게 해당 가상자산 거래소를 금융범죄 위험으로부터 보호할 수 있다.
- [120] 나아가, 일 실시 예에 따른 지갑주소 관리장치는 위험 지갑주소 카테고리 별로 검색 키워드를 이용하여 1차 위험 지갑주소를 추출할 수 있고, 1차 위험 지갑주소의 거래내역 정보 분석 및 위험성 예측 모델을 통해 2차 위험 지갑주소를 추출할 수 있다. 이에 따라, 위험 지갑주소 분석과정을 거치므로 보다 정확하게 위험 지갑주소를 추출할 수 있다.
- [121] 이제까지 본 발명에 대하여 그 실시 예들을 중심으로 살펴보았다. 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시 예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나

타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

청구범위

- [청구항 1] 복수의 가상자산 거래소 서버로부터 복수의 위험 지갑주소를 수집하는 데이터 수집부; 및
수집된 복수의 위험 지갑주소를 데이터베이스에 저장하고, 특정 가상자산 거래소 서버로부터 특정 지갑주소에 대한 조회 요청을 수신하면, 상기 복수의 가상자산 거래소 서버로부터 수집된 복수의 위험 지갑주소를 데이터베이스에서 조회하여 해당 지갑주소가 위험 지갑주소인지 여부를 상기 특정 지갑주소에 대한 조회를 요청한 가상자산 거래소 서버에 응답하는 데이터 관리부;
를 포함하는 것을 특징으로 하는 지갑주소 관리장치.
- [청구항 2] 제 1 항에 있어서, 데이터 수집부는
복수의 금융기관 서버 및 복수의 공공기관 서버로부터 복수의 위험 지갑주소를 수집하고,
데이터 관리부는
수집된 복수의 위험 지갑주소를 데이터베이스에 저장하고, 가상자산 거래소 서버로부터 특정 지갑주소에 대한 조회를 수신하면, 복수의 금융기관 서버 및 공공기관 서버로부터 수집된 복수의 위험 지갑주소를 데이터베이스에서 조회하여 해당 지갑주소의 위험성 여부를 해당 가상자산 거래소 서버에 응답하는 것을 특징으로 하는 지갑주소 관리장치.
- [청구항 3] 제 1 항에 있어서, 데이터 수집부는
웹 크롤링을 통해 서피스 웹(Surface web), 딥 웹(Deep web), 다크 웹(Dark web), SNS 중 적어도 하나를 포함하는 복수의 웹페이지로부터 복수의 고위험 지갑주소를 수집하고,
데이터 관리부는
수집된 복수의 위험 지갑주소를 데이터베이스에 저장하고, 가상자산 거래소 서버로부터 특정 지갑주소에 대한 조회를 수신하면, 복수의 웹페이지로부터 수집된 복수의 위험 지갑주소를 데이터베이스에서 조회하여 해당 지갑주소의 위험성 여부를 상기 가상자산 거래소 서버에 응답하는 것을 특징으로 하는 지갑주소 관리장치.
- [청구항 4] 제 1 항에 있어서, 데이터 수집부는
선택된 지갑주소에서 블록체인에 저장된 거래 내역, 전송량, 전송 대상, 전송 시간을 포함하는 지갑 정보를 수집하는 블록체인 탐색기; 및
웹페이지에 노출된 지갑주소를 수집하는 웹 크롤러;
를 포함하는 것을 특징으로 하는 지갑주소 관리장치.
- [청구항 5] 제 1 항에 있어서, 데이터 수집부는
위험 지갑주소의 카테고리를 정의하고,

위험 지갑주소 수집 방식을 구분하되, 제1 카테고리는 웹 크롤러를 통해 위험 지갑주소를 수집하고, 제2 카테고리는 수집된 지갑주소의 거래내역 분석을 통해 위험 지갑주소를 수집하며, 제3 카테고리는 공공기관의 웹사이트 접속을 통해 위험 지갑주소를 수집하도록 수집 방식을 구분하는 것을 특징으로 하는 지갑주소 관리장치.

- [청구항 6] 제 1 항에 있어서, 지갑주소 관리장치는
데이터 수집부로부터 수집된 복수의 지갑주소를 분석하여 위험 지갑주소를 필터링 하는 데이터 분석부;
를 더 포함하는 것을 특징으로 하는 지갑주소 관리장치.
- [청구항 7] 제 6 항에 있어서, 데이터 분석부는
수집된 지갑주소 정보를 이용하여 위험행위 패턴을 분석하고, 분석된 위험행위 패턴을 기초로 1차 위험 지갑주소를 분류하고 분류된 지갑주소를 위험도에 따라 위험도 레벨 별로 분류한 후 분류된 1차 위험 지갑주소를 데이터베이스에 저장하는 제1 데이터 분석부;
를 포함하는 것을 특징으로 하는 지갑주소 관리장치.
- [청구항 8] 제 6 항에 있어서, 데이터 분석부는
블랙리스트, 사이버범죄, 금융범죄 및 기타범죄 카테고리를 포함하는 위험 지갑주소 카테고리 별로 검색 키워드를 이용하여 1차 위험 지갑주소를 추출한 후 분류된 1차 위험 지갑주소를 데이터베이스에 저장하는 제1 데이터 분석부;
를 포함하는 것을 특징으로 하는 지갑주소 관리장치.
- [청구항 9] 제 8 항에 있어서, 제1 데이터 분석부는
추출된 1차 위험 지갑주소의 의심 범죄 유형에 따라 유관 법령 및 관련 기관 규정을 적용하여 위험요소 평가 기준을 정의하고, 위험요소 평가 기준에 따라 지갑주소의 위험도를 수치화하고 가중치를 할당하는 것을 특징으로 하는 지갑주소 관리장치.
- [청구항 10] 제 6 항에 있어서, 데이터 분석부는
상기 데이터베이스에서 1차 위험 지갑주소를 로딩하여 1차 위험 지갑주소의 거래내역 정보 분석 및 위험성 예측 모델을 통해 2차 위험 지갑주소를 추출하는 제2 데이터 분석부;
를 포함하는 것을 특징으로 하는 지갑주소 관리장치.
- [청구항 11] 가상자산을 거래하기 위한 복수의 지갑주소를 관리하는 지갑주소 관리장치를 이용한 지갑주소 조회 서비스 제공방법에 있어서,
복수의 가상자산 거래소 서버로부터 위험 지갑주소 등록을 요청받아 등록하는 단계;
웹 크롤링을 통해, 블랙리스트, 사이버범죄, 금융범죄 및 기타범죄 카테고리를 포함하는 위험 지갑주소 카테고리 별 검색 키워드를 이용하여 1차 위험 지갑주소를 추출하는 단계;

추출된 1차 위험 지갑주소를 데이터베이스에 저장하여 등록하는 단계; 및
 상기 데이터베이스에서 등록된 1차 위험 지갑주소를 로딩하여 1차 위험 지갑주소의 거래내역 정보 분석 및 위험성 예측 모델을 통해 2차 위험 지갑주소를 추출하여 데이터베이스에 저장하는 단계;
 를 포함하는 것을 특징으로 하는 지갑주소 조회 서비스 제공방법.

[청구항 12] 가상자산을 거래하기 위한 복수의 지갑주소를 관리하는 지갑주소 관리장치를 이용한 지갑주소 조회 서비스 제공방법에 있어서,
 블랙리스트, 사이버범죄, 금융범죄 및 기타범죄 카테고리를 포함하는 위험 지갑주소 카테고리 별 검색 키워드를 이용하여 1차 위험 지갑주소를 추출하고 추출된 1차 위험 지갑주소를 데이터베이스에 저장하여 등록하는 단계; 및
 상기 데이터베이스에 등록된 1차 위험 지갑주소를 로딩하여 1차 위험 지갑주소의 거래내역 정보 분석 및 위험성 예측 모델을 통해 2차 위험 지갑주소를 추출하여 데이터베이스에 저장하여 등록하는 단계;
 복수의 가상자산 거래소 서버로부터 위험 지갑주소 등록을 요청받아 등록하는 단계;
 가상자산 거래소 서버로부터 특정 지갑주소에 대한 조회 요청을 수신하는 단계;
 복수의 가상자산 거래소 서버로부터 등록된 위험 지갑주소를 상기 데이터베이스에서 조회하여 해당 지갑주소가 1차 또는 2차 위험 지갑주소인지 여부를 확인하는 단계; 및
 위험 지갑주소 여부를 해당 가상자산 거래소 서버에 응답하는 단계;
 를 포함하는 것을 특징으로 하는 지갑주소 조회 서비스 제공방법.

[청구항 13] 제 12 항에 있어서, 지갑주소 조회 서비스 제공방법은
 복수의 공공기관 서버 및 복수의 금융기관 서버로부터 위험 지갑주소 등록을 요청받아 등록하는 단계; 를 더 포함하며,
 해당 지갑주소가 위험 지갑주소인지 여부를 확인하는 단계는
 복수의 공공기관 서버 및 복수의 금융기관 서버로부터 등록된 위험 지갑주소를 조회하여 해당 지갑주소가 위험 지갑주소인지 여부를 확인하는 것을 특징으로 하는 지갑주소 조회 서비스 제공방법.

[청구항 14] 제 12 항에 있어서, 지갑주소 조회 서비스 제공방법은
 웹 크롤링을 통해 위험 지갑주소를 수집하는 단계; 를 더 포함하며,
 해당 지갑주소가 위험 지갑주소인지 여부를 확인하는 단계는
 웹 크롤링을 통해 수집된 위험 지갑주소를 조회하여 해당 지갑주소가 위험 지갑주소인지 여부를 확인하는 것을 특징으로 하는 지갑주소 조회 서비스 제공방법.

[청구항 15] 제 12 항에 있어서, 지갑주소 조회 서비스 제공방법은

웹 크롤링을 통해 위험 지갑주소 카테고리 별 검색 키워드를 이용하여 1차 위험 지갑주소를 추출하는 단계; 및
추출된 1차 위험 지갑주소를 데이터베이스에 저장하여 등록하는 단계; 를 더 포함하며,
해당 지갑주소가 위험 지갑주소인지 여부를 확인하는 단계는
데이터베이스에 저장된 1차 위험 지갑주소를 조회하여 해당 지갑주소가 위험 지갑주소인지 여부를 확인하는 것을 특징으로 하는 지갑주소 조회 서비스 제공방법.

[청구항 16] 제 15 항에 있어서, 지갑주소 조회 서비스 제공방법은
등록된 1차 위험 지갑주소의 거래내역을 분석하여 2차 위험 지갑주소를 추출하여 데이터베이스에 저장하는 단계; 를 더 포함하며,
해당 지갑주소가 위험 지갑주소인지 여부를 확인하는 단계는
데이터베이스에 저장된 2차 위험 지갑주소를 조회하여 해당 지갑주소가 위험 지갑주소인지 여부를 확인하는 것을 특징으로 하는 지갑주소 조회 서비스 제공방법.