(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년02월19일
(11) 등록번호 10-2078566
(24) 등록일자 2020년02월12일

(51) 국제특허분류(Int. Cl.)
G06Q 20/36 (2012.01) *G06Q 20/06* (2012.01)
G06Q 20/38 (2012.01)
(52) CPC특허분류
G06Q 20/3678 (2013.01)
G06Q 20/065 (2013.01)
(21) 출원번호 10-2019-0031026
(22) 출원일자 2019년03월19일
심사청구일자 2019년03월19일
(56) 선행기술조사문헌
KR101904208 B1*
KR101922567 B1*
KR101673073 B1
KR101681002 B1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
크립토 주식회사
전라남도 순천시 충효로 15, 232호(덕암동)
(72) 발명자
한재영
전라남도 순천시 서면 배들이길 17, 101동 703호 (선평배들마을아파트)
이경백
전라남도 여수시 문수7길 14, 205호 (문수동)
(74) 대리인
강창원

전체 청구항 수 : 총 1 항 심사관 : 권태헌

(54) 발명의 명칭 **암호화폐 분실 방지 방법 및 시스템**

(57) 요 약

본 발명의 목적은, 사용자 단말기에 보관된 암호화폐가 사용자에 의해 기 설정된 계약실행 대기기간 동안 사용되지 않으면, 상기 사용자 단말기에 보관된 암호화폐를 관리 시스템의 트리거계좌의 서명을 통해 자산보호계약을 실행해 상기 암호화폐와 토큰을 사용자자산 임시보호계좌로 이체시키는, 암호화폐 분실 방지 방법을 제공하는 것이다.

대 표 도 - 도1

(52) CPC특허분류
G06Q 20/3829 (2013.01)
G06Q 20/385 (2013.01)

명 세 서

청구범위

청구항 1

사용자 단말기로부터 사용자 정보가 수신되면, 관리 시스템이, 상기 사용자 정보를 이용하여 생성된 Seed 정보를, 상기 사용자 단말기로 전송하는 단계;

상기 사용자 단말기가 암호화폐와 토큰 이용을 위한 개인키 및 공개키를 생성하는 단계;

상기 Seed 정보와 상기 사용자 단말기를 통해 입력된 사용자 등록암호를 이용하여, 상기 사용자 단말기가 관리용 개인키를 생성하며, 상기 사용자 단말기가 암호화폐와 토큰을 관리하는 일반계좌를 생성하는 단계;

상기 사용자 단말기가 상기 사용자 단말기의 암호화폐나 토큰이 지속적으로 사용되지 않는 계약실행 대기기간을 이용하여 보호계좌 생성을 요청하면, 블럭체인이 보호계좌를 생성하는 단계;

상기 사용자 단말기가 상기 일반계좌에서 관리되는 암호화폐 및 토큰을 상기 보호계좌로 전송하는 단계;

상기 계약실행 대기기간이 경과하기 전에 상기 보호계좌에서 입/출금이 발생되면, 상기 사용자 단말기가 상기 계약실행 대기기간을 초기화시키는 단계;

사용자에 의해 설정된 상기 계약실행 대기기간이 경과하면, 상기 계약실행 대기기간과 관련된 계약이 실행되어, 상기 관리 시스템이, 상기 보호계좌에서 관리되는 암호화폐와 토큰을 상기 관리 시스템의 사용자자산 임시보호계좌로 이체시키는 단계; 및

상기 암호화폐와 토큰이 상기 사용자자산 임시보호계좌로 이체된 후, 상기 사용자 또는 상기 사용자의 법적 승계인으로부터 상기 암호화폐와 토큰에 대한 반환이 요청되면, 상기 관리 시스템이 상기 사용자 또는 상기 법적 승계인이 요청한 암호화폐 계좌로 상기 암호화폐와 토큰을 반환하는 단계를 포함하고,

상기 보호계좌를 생성하는 단계는,

상기 계약실행 대기기간이 입력되면, 상기 관리시스템이 자산보호계약을 작성해 상기 사용자 단말기에 전달하고, 상기 사용자 단말기가 상기 계약에 따른 상기 보호계좌 생성을 상기 블럭체인에 요청하면, 상기 블럭체인이 상기 보호계좌를 생성하여, 상기 보호계좌에 대한 정보를 상기 관리 시스템으로 전송하는 단계; 및

상기 사용자 단말기가 상기 일반계좌에서 관리되는 암호화폐와 토큰을 상기 보호계좌로 전송하여 관리하는 단계를 포함하고,

상기 암호화폐와 토큰이 상기 사용자자산 임시보호계좌로 이체되는 단계는,

상기 계약실행 대기기간이 경과하면, 상기 관리 시스템이 상기 사용자 정보에 포함된 정보들을 이용하여 상기 사용자와 연락을 시도하는 단계;

상기 시도 후 상기 사용자 또는 상기 사용자의 법적 승계인으로부터 정상적인 응답이 수신되면, 상기 관리 시스템이 상기 이체를 중지하는 단계; 및

상기 시도 후 상기 사용자로부터 정상적인 응답이 수신되지 않으면, 상기 관리 시스템이 상기 이체를 실행하는 단계를 포함하고,

상기 사용자 단말기에는 암호화폐와 토큰이 저장되어 있지 않고,

사용자자산 임시보호계좌로의 상기 암호화폐 이체는, 상기 이체와 관련된 권한을 갖는 트리거 계좌에 의해 상기 보호계좌로부터 상기 사용자자산 임시보호계좌로 이체되며,

사용자자산 임시보호계좌로의 상기 토큰의 이체는, 상기 이체와 관련된 권한을 갖는 트리거 계좌에 의해 일반계좌에서 상기 보호계좌로 이체 후 상기 사용자자산 임시보호계좌로 이체되는 암호화폐 분실 방지 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

청구항 12

삭제

청구항 13

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 암호화폐의 분실을 방지하는 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 블럭 체인(Block Chain)을 기반으로하는 암호화폐를 이용하기 위해, 일반적으로 전자지갑이 이용되고 있다. 특히, 사용자의 공개키 및 개인키를 이용하여, 암호화폐의 송금 또는 결제가 이루어진다.

[0003] 암호화폐의 공개키는 사용자가 암호화폐를 전달받을 공개주소를 의미하며, 개인키는 실제 거래를 위한 인증 정보로 사용된다.

[0004] 특히, 개인키(Private Key)는 거래내용의 작성을 위해 서명(암호화)을 해주는 기능을 수행하기 때문에, 암호화폐의 보안성은 개인키의 관리에 의해 좌우된다.

[0005] 종래의 암호화폐 시스템에서는, 개인키의 관리를 위해 Mnemonic이라는 복구단어가 이용되고 있다. 즉, 암호화

폐 지갑이 물리적으로 훼손되거나 분실되었을때, 복구단어를 이용해 새로운 암호화폐 지갑속에 기존에 사용하던 개인키가 복원될 수 있다. 그러나, 복구단어가 타인에게 노출되거나 훼손될 경우, 자산을 잃어버릴 위험이 발생한다.

[0006] 또한, 개인키(복구단어)가 장기간 보관되는 중에, 암호화폐 지갑의 사용자의 부재상황이 발생되면, 자산이 손실될 가능성이 높아진다. 예를 들어, 암호화폐 지갑의 사용자가 치매나 사고로 인해 자신의 암호화폐 지갑을 장기간 관리하지 못하는 경우가 발생되면, 보유한 자산이 잊혀질 수도 있으며, 가족에게 개인키가 전달되지 못하거나 전달받은 가족의 이용방법 미숙지로 인해, 자산이 분실될 수도 있다.

[0007] 이 외에도, 자연재해나 인재로 인한 개인키(복구단어)의 손실, 암호화폐 거래소에 대한 해킹, 거래소의 고객 자산 횡령, 거래소 이용고객 계정의 해킹, 클라우드 계정의 해킹, 웹 암호화폐 지갑의 DNS 변조에 의한 개인키 유출 등과 같은 다양한 원인들에 의해, 암호화폐가 분실될 수 있다.

[0008] 그러나, 종래에는 상기한 바와 같은 암호화폐의 분실을 방지할 수 있는 방법이 제공되지 못하고 있다.

선행기술문헌

특허문헌

(특허문헌 0001) 1. 등록번호 10-1922567호: 암호화폐 거래소의 해킹을 차단하기 위해 서로 다른기능을 하는 복수 개의 서버 시스템과 폐쇄코인을 이용한 전자지갑 관리 시스템

(특허문헌 0002) 2. 등록번호 10-1904208호: 블록체인 기반의 암호화폐와 전자지갑 관리 시스템

(특허문헌 0003) 3. 등록번호 10-1673073호: 블록체인 구조를 사용하는 암호화화폐 거래방법

발명의 내용

해결하려는 과제

[0009] 상술한 문제점을 해결하기 위해 제안된 본 발명의 목적은, 사용자 단말기에 보관된 암호화폐가 사용자에 의해기 설정된 계약실행 대기기간 동안 사용되지 않으면, 트리거 계좌의 서명을 통해 자산보호계약을 실행해 상기 사용자 단말기에 보관된 암호화폐를 미리 지정된 계약내용에 따라 사용자자산 임시보호계좌로 이체를 실행할 수 있는, 암호화폐 분실 방지 방법 및 시스템을 제공하는 것이다.

과제의 해결 수단

[0010] 상술한 기술적 과제를 달성하기 위한 본 발명에 따른 암호화폐 분실 방지 방법은, 사용자 단말기를 이용하는 사용자의 사용자 정보를 이용하여 생성된 Seed 정보를 관리 시스템으로부터 수신하는 단계; 상기 사용자 단말기가 암호화폐와 토큰 이용을 위한 개인키 및 공개키를 생성하는 단계; 상기 Seed 정보와 상기 사용자 단말기를 통해 입력된 사용자 등록암호를 이용하여, 상기 사용자 단말기가 관리용 개인키를 생성하며, 암호화폐와 토큰을 관리하는 일반계좌를 생성하는 단계; 상기 사용자 단말기가 상기 사용자 단말기의 암호화폐나 토큰이 지속적으로 사용되지 않는 계약실행 대기기간을 이용하여 보호계좌를 생성하는 단계; 및 상기 계약실행 대기기간이 경과하면, 상기 계약실행 대기기간과 관련된 계약이 실행되어, 상기 관리 시스템의 사용자자산 임시보호계좌로 상기 암호화폐와 토큰이 이체되는 단계를 포함한다.

[0011] 상술한 기술적 과제를 달성하기 위한 본 발명에 따른 또 다른 암호화폐 분실 방지 방법은, 관리 시스템이, 사용자 단말기로부터 수신된 사용자 정보를 이용하여 Seed 정보를 생성하며, 상기 Seed 정보를 상기 사용자 단말기로 전송하는 단계; 상기 사용자 단말기로부터 상기 사용자 단말기에 의해 관리되는 암호화폐와 토큰이 지속적으로 사용되지 않는 계약실행 대기기간 및 계약요청이 수신되면 상기 관리 시스템이 보호계좌에 대한 정보를 생성하여 상기 사용자 단말기로 전송하거나, 또는 상기 관리 시스템이 상기 사용자 단말기에서 생성된 보호계좌에 대한 정보를 상기 사용자 단말기로부터 수신하여 관리하는 단계; 및 상기 계약실행 대기기간이 경과하면, 상기 관리 시스템이 상기 계약실행 대기기간과 관련된 계약을 실행하여, 상기 보호계좌에서 관리되는 상기 암호화폐를 사용자자산 임시보호계좌로 이체하는 단계를 포함한다.

[0012] 상술한 기술적 과제를 달성하기 위한 본 발명에 따른 암호화폐 분실 방지 시스템은, 암호화폐 이용을 위한 개인

키 및 공개키를 생성하는 사용자 단말기; 및 상기 사용자 단말기로부터 전송된 상기 공개키와 상기 사용자 단말기를 이용하는 사용자의 사용자 정보를 이용하여 Seed 정보를 생성하는 관리 시스템을 포함하고, 상기 사용자 단말기는 상기 Seed 정보를 상기 관리 시스템으로부터 수신하고, 상기 Seed 정보와 상기 사용자 단말기를 통해 입력된 사용자 등록암호를 이용하여, 관리용 개인키를 생성하고, 암호화폐를 관리하는 일반계좌를 생성하며, 상기 사용자 단말기는 상기 사용자 단말기의 암호화폐가 지속적으로 사용되지 않는 계약실행 대기기간을 이용하여 보호계좌를 생성하며, 상기 계약실행 대기기간이 경과하면, 상기 계약실행 대기기간과 관련된 계약이 실행되어, 상기 관리 시스템이 상기 관리 시스템의 사용자자산 임시보호계좌로 상기 암호화폐와 토큰을 이체시킨다.

발명의 효과

[0013] 본 발명에 의하면 다음과 같은 효과가 기대될 수 있다,

[0014] 첫째, 사용자는 자신의 개인키(복구단어)가 유출될 상황에 대해 우려할 필요가 없다.

[0015] 둘째, 사용자는 언제 어디서든 하드웨어 월렛(암호화폐 지갑)과 같은 불편함 없이 스마트폰이나 테블릿PC에 암호화폐를 담아 보관할 수 있다.

[0016] 셋째, 사용자는 암호화폐 송금의 불편함 없이 암호화폐를 결제에 이용할 수 있다.

[0017] 넷째, 사용자는 암호화폐 지갑의 암호를 잃어버리거나 스마트폰을 잃어버리거나 도난당해도 암호화폐(자산)를 99.9% 찾아 돌려받을 수 있으며, 사용자의 연락두절시에는 사용자의 가족에게 암호화폐가 전달될 수 있다.

[0018] 다섯째, 암호화폐 지갑의 개인키는 사용자의 앱과 사용자의 클라우드 서버에만 보관될 수 있다.

[0019] 여섯째, 관리 시스템의 관리자는 사용자의 개인키에 대한 정보를 보유하지 않기 때문에, 관리자에 의한 암호화폐의 해킹은 발생되지 않는다.

[0020] 일곱째, 사용자는 암호화폐를 매우 안전하고, 편리하게 관리할 수 있으며, 장기적으로 보유할 수도 있다.

[0021] 여덟째, 사용자가 설정한 자산보호계약실행 대기기간이 만료되기 전까지의 모든 자산의 통제권은 오직 사용자에게만 있다.

도면의 간단한 설명

[0022] 도 1은 본 발명에 따른 암호화폐 분실 방지 시스템을 나타낸 일실시예 구성도.

도 2는 본 발명에 따른 암호화폐 분실 방지 방법이 적용되는 사용자 단말기와 관리 시스템의 일실시예 구성도.

도 3은 본 발명에 따른 암호화폐 분실 방지 방법의 일실시예 흐름도.

도 4는 본 발명에 따른 암호화폐 분실 방지 방법을 실행하는 서비스앱이 표시된 사용자 단말기를 나타낸 예시도.

도 5는 도 3에 도시된 단계들 중 개인키 및 공개키를 생성하는 단계와 관리용 개인키를 생성하는 단계를 구체적으로 설명한 예시도.

도 6은 블럭체인에서 거래기록이 블럭에 기록되는 과정을 구체적으로 설명한 예시도.

도 7은 도 3에 도시된 단계들 중 관리시스템의 주도로 자산보호계약(보호계좌)를 생성하는 단계를 구체적으로 설명한 또 다른 예시도.

도 8는 도 7에 대한 상세한 예시도.

도 9는 도 3에 도시된 단계들 중 단말기의 주도로 자산보호계약(보호계좌)을 생성하는 단계를 구체적으로 설명한 또 다른 예시도.

도 10은 도 9에 대한 상세한 예시도.

도 11은 도 3에 도시된 단계들 중 관리시스템의 보조에 의한 단말기 주도로 자산보호계약(보호계좌)을 생성하는 단계를 구체적으로 설명한 또 다른 예시도.

도 12는 도 11에 대한 상세한 예시도.

도 13은 도 3에 도시된 단계들 중 트리거 서버(또는 계좌)를 이용하여 자산보호계약을 실행해 암호화폐를 사용

자자산 임시보호계좌로 이체시키는 단계를 구체적으로 설명한 예시도.

도 14는 본 발명에 따른 자산보호계약(보호계좌)이 사용자의 토큰 자산을 보호하기 위한 권한을 획득하는 방법을 나타낸 예시도.

도 15는 본 발명에 따른 자산보호계약(보호계좌)이 실행되어 사용자의 자산이 보호되는 절차를 나타낸 예시도.

발명을 실시하기 위한 구체적인 내용

[0023] 이하, 첨부된 도면을 참조하여 본 발명의 실시 예에 대해 상세히 설명한다.

[0024] 도 1은 본 발명에 따른 암호화폐 분실 방지 시스템을 나타낸 일실시예 구성도이며, 도 2는 본 발명에 따른 암호화폐 분실 방지 방법이 적용되는 사용자 단말기와 관리 시스템의 일실시예 구성도이다.

[0025] 본 발명에 따른 암호화폐 분실 방지 시스템은, 도 1에 도시된 바와 같이, 암호화폐를 이용하는 사용자가 이용하는 사용자 단말기(10), 기 설정된 계약(이하의 설명에서 계약이란 사용자를 위한 자산보호계약을 의미함. 이하에서는, 간단히 보호계좌라고 함) 실행 기간이 경과하면 상기 사용자 단말기(10)에서 관리되는 암호화폐를 사용자 자산 임시보호계좌(콜드월렛이라고도 함)로 이체시켜 관리하는 관리 시스템(30), 상기 사용자에 의해 이용되는 클라우드 서버(20) 및 상기 암호화폐를 이용하는 이용자들에 의해 이용되는 암호화폐 단말기(40)들을 포함한다.

[0026] 상기 사용자 단말기(10) 및 상기 암호화폐 단말기(40)는, 컴퓨터, 테블릿 PC, 스마트폰과 같은 유선 단말기 또는 무선 단말기가 될 수 있다. 이하에서는, 상기 사용자 단말기(10)가 스마트폰인 경우를 일예로 하여 본 발명이 설명된다.

[0027] 상기 사용자 단말기(10)는, 도 2에 도시된 바와 같이, 무선통신 또는 유선통신을 수행하는 통신부(15), 각종 정보를 입력받는 입력부(17), 각종 정보를 출력하는 출력부(18), 각종 정보를 저장하는 저장부(19) 및 상기 각 구성요소들의 기능을 제어하는 제어부(16)를 포함한다. 상기에서 설명된 바와 같이, 상기한 바와 같은 구성들을 포함하는 상기 사용자 단말기(10)는 스마트폰이 될 수 있다.

[0028] 상기 사용자 단말기(10) 및 상기 암호화폐 단말기(40) 각각은, 암호화폐를 관리하는 암호화폐지갑의 기능을 수행할 수 있다.

[0029] 상기 관리 시스템(30)은 현재 일반적으로 이용되는 네트워크 서버가 될 수 있다. 상기 관리 시스템(30)은 상기 사용자 단말기(10)에서 실행되는 암호화폐 지갑에 보호계좌를 생성할 수 있으며, 기 설정된 계약실행 기간이 경과하면, 상기 보호계좌에 포함된 암호화폐들을 상기 관리 시스템(30)에서 관리되는 트리거 계좌를 통해 사용자 자산 임시보호계좌로 이체시킬 수 있다.

[0030] 상기 관리 시스템(30) 역시, 도 2에 도시된 바와 같이, 무선통신 또는 유선통신을 수행하는 통신부(15), 각종 정보를 입력받는 입력부(17), 각종 정보를 출력하는 출력부(18), 각종 정보를 저장하는 저장부(19) 및 상기 각 구성요소들의 기능을 제어하는 제어부(16)를 포함할 수 있다.

[0031] 상기 클라우드 서버(20) 역시 현재 일반적으로 이용되는 네트워크 서버가 될 수 있다. 상기 클라우드 서버(20)는 예를 들어, 구글, 삼성, 네이버 등과 같은 업체에 의해 관리될 수 있으며, 사용자의 각종 정보들을 저장하는 기능을 수행할 수 있다.

[0032] 도 3은 본 발명에 따른 암호화폐 분실 방지 방법의 일실시예 흐름도이다.

[0033] 본 발명에 따른 암호화폐 분실 방지 방법은, 도 3에 도시된 바와 같이, 사용자 단말기(10)가 상기 사용자 단말기를 이용하는 사용자의 사용자 정보를 이용하여 생성된 Seed 정보를 관리 시스템(30)으로부터 수신하는 단계(302), 사용자 단말기에서 암호화폐 이용을 위한 개인키 및 공개키를 생성하는 단계(304), 상기 Seed 정보와 상기 사용자 단말기를 통해 입력된 사용자 등록암호를 이용하여, 상기 사용자 단말기가 관리용 개인키(암호화된 개인키)(이하, 간단히 관리용 개인키라 함)를 생성하며, 암호화폐를 관리하는 일반계좌를 생성하는 단계(306), 상기 사용자 단말기의 암호화폐가 지속적으로 사용되지 않는 계약실행 대기기간을 이용하여 보호계좌를 생성하는 단계(308), 사용자가 암호화폐를 이용하는 단계(310), 상기 계약실행 대기기간이 경과하면, 상기 관리 시스템의 트리거 계좌의 서명을 통해 계약, 즉, 자산보호계약을 실행하여 상기 보호계좌속 암호화폐와 토큰이 사용자자산 임시보호계좌로 이체되는 단계(312) 및 상기 사용자 또는 상기 사용자의 법적 승계인으로부터 반환 요청이 수신되면 상기 암호화폐를 반환하는 단계(314)를 포함한다.

[0034] 암호화폐와 토큰은 좁은 의미로는 서로 다른 것일 수도 있으나, 넓은 의미로는 암호화폐에 토큰이 포함된다고 볼 수 있다. 따라서, 이하의 설명에서는 암호화폐와 토큰이 독립적으로 설명될 수도 있으며, 토큰이 암호화폐로서 설명될 수도 있다.

[0035] 이하에서는, 도 1 내지 도 15를 참조하여, 도 3에 도시된 암호화폐 분실 방지 방법이 구체적으로 설명된다.

[0036] 도 4는 본 발명에 따른 암호화폐 분실 방지 방법을 실행하는 서비스앱이 표시된 사용자 단말기를 나타낸 예시도이고, 도 5는 도 3에 도시된 단계들 중 개인키 및 공개키를 생성하는 단계와 관리용 개인키를 생성하는 단계를 구체적으로 설명한 예시도이고, 도 6은 블럭체인에서 거래기록이 블럭에 기록되는 과정을 구체적으로 설명한 예시도이고, 도 7은 도 3에 도시된 단계들 중 관리시스템의 주도로 자산보호계약(보호계좌)를 생성하는 단계를 구체적으로 설명한 또 다른 예시도이고, 도 8은 도 7에 대한 상세한 예시도이고, 도 9는 도 3에 도시된 단계들 중 단말기의 주도로 자산보호계약(보호계좌)을 생성하는 단계를 구체적으로 설명한 또 다른 예시도이고, 도 10은 도 9에 대한 상세한 예시도이고, 도 11은 도 3에 도시된 단계들 중 관리시스템의 보조에 의한 단말기 주도로 자산보호계약(보호계좌)을 생성하는 단계를 구체적으로 설명한 또 다른 예시도이고, 도 12는 도 11에 대한 상세한 예시도이며, 도 13은 도 3에 도시된 단계들 중 트리거 서버(또는 계좌)를 이용하여 자산보호계약을 실행해 암호화폐를 사용자자산 임시보호계좌로 이체시키는 단계를 구체적으로 설명한 예시도이다.

[0037] 특히, 도 6은 퍼블릭 블럭체인(개방형 블럭체인)에서의 거래(암호화폐이체,계약생성)를 검증하고 기록하는 절차에 대한 예시도이고, 도 7, 도 9 및 도 11은 도 3에 도시된 단계들 중 보호계좌를 생성하는 단계를 3가지 방법으로 설명한 또 다른 예시도이고, 도 8, 도 10 및 도 12는 보호계좌를 생성하는 절차를 상세하게 설명한 예시도이며, 도 13은 도 3에 도시된 단계들 중 트리거 서버(또는 계좌)를 이용하여 자산보호계약을 실행해 암호화폐와 토큰을 사용자자산 임시보호계좌로 이체시키는 단계를 구체적으로 설명한 예시도이다.

[0038] < 1. 관리시스템이 Seed 정보를 생성하는 단계(302) >

[0039] 본 발명을 이용하고자 하는 사용자는 우선 자신이 이용하는 사용자 단말기(10)에, 상기 관리 시스템(30)에 의해 제공되는 서비스앱(11)을 다운로드 받아 수행한다.

[0040] 상기 서비스앱(11)이 수행되면, 사용자는 상기 사용자 단말기(10)를 이용하여 상기 관리 시스템(30)으로 자신에 대한 정보, 즉, 사용자 정보를 전송한다.

[0041] 상기 사용자 정보에는 이름, 성별, 생년월일, 신분증, 전화번호, 이메일, 비상 연락처, 주소 등이 포함될 수 있다.

[0042] 상기 사용자 정보는 사용자가 상기 사용자 단말기를 분실하거나 상기 사용자 단말기가 파손되었을 때, 정상적인 사용자인지의 여부를 판단하기 위한 목적으로 이용될 수도 있다.

[0043] 이러한 사용자 정보를 모아 하나의 데이터 형태로 구성하고, 관리시스템은 이 사용자정보 데이터를 기반으로 Seed 정보를 생성해 사용자 단말기(10)에 전달한다.

[0044] < 2. 개인키 및 공개키 생성 단계(304) >

[0045] 상기 사용자 단말기(10)는 예를 들어 랜덤으로 생성되는 64byte의 HEX 코드를 이용하여 개인키를 생성한다.

[0046] 상기 공개키는 상기 개인키에 ECDSA(타원곡선 전자서명 알고리즘)를 적용해 추출될 수 있다. 즉, 상기 공개키는 상기 개인키를 통해 생성된다. 이렇게 생성된 공개키는 상기 관리시스템(30)으로 전송한다.

[0047] < 3. Seed 정보를 이용해 관리용 개인키파일 생성(306) >

[0048] 상기 사용자 단말기(10)는 상기 Seed 정보와 상기 사용자 단말기(10)를 통해 사용자로부터 입력된 사용자 등록 암호를 이용하여 관리용 개인키를 생성한다. (306).

[0049] 사용자는 상기 관리용 개인키를 자신이 이용하는 클라우드 서버(20)에 전송하여 관리할 수 있다.

[0050] 사용자는 상기 사용자 단말기(10)를 분실하였거나, 상기 사용자 단말기(10)가 파손된 경우, 상기 클라우드 서버(20)로부터 상기 관리용 개인키를 다운로드받아 새로운 사용자 단말기에 저장할 수 있다. 이 경우, 상기 새로운 사용자 단말기는 다운로드 받은 상기 관리용 개인키를 이용하여 일반계좌를 다시 생성할 수 있다.

[0051] < 4. 보호계좌 생성 단계(308) >

[0052] 사용자는 상기 사용자 단말기의 암호화폐가 지속적으로 사용되지 않는 계약실행 대기기간을 설정한다. 상기 계

약실행 대기기간이란, 상기 암호화폐가 상기 사용자자산 임시보호계좌로 이체되기전 최소한의 기간을 의미한다.

[0053] 상기 계약실행 대기기간은 예를 들어, 일주일, 한 달, 60일, 90일, 100일, 1년, 2년 등으로 다양하게 설정될 수 있다.

[0054] 상기 계약실행 대기기간 동안 상기 암호화폐가 지속적으로 사용되지 않으면, 상기 관리 시스템(30)에 의해 관리되는 상기 트리거 계좌의 서명을 통해 자산보호계약이 실행되며, 이에 따라, 상기 사용자 단말기(10)에서 관리되는 상기 암호화폐가 사용자자산 임시보호계좌로 이체된다.

[0055] 상기 사용자 단말기(10)는 상기 계약실행 대기기간을 이용하여 보호계좌를 생성한다.

[0056] 아래의 [표 1]은 보호계좌를 생성하기 위한 Smart Contract Code를 나타낸 예시도이다.

표 1

[0057]

자산보호 작동기 = 보호계좌를 생성하기 위한 Smart Contract Code	
조건	값
계약계좌의 자산을 옮길 수 있는 권한은 보호계좌에 등록된 A와 B에게만 있다. (보호계좌에 등록하는 사용자의 일반계좌는 다수가 될 수 있다.) (자산보호계약실행 대기기간 동안에는 보호계좌에 등록된 A에게만 자산을 옮길 수 있는 권한이 있다.)	A: 사용자 단말기(10)에서 생성된 일반계좌 공개키 B: 관리시스템(30)의 트리거 계좌 공개키 C: 관리시스템(30)의 사용자자산 임시보호계좌 공개키 D: 자산보호계약실행 대기기간은 사용자가 입력하는 값이며 일단위로 등록가능.
사용자가 입력하는 자산보호계약실행 대기기간 D 는 일(하루) 단위로 설정한다. (카운트기간은 보호계좌의 마지막 입금/출금 일에 다시 카운트된다.)	
대기기간 만료 후 자산보호계약을 실행할 권한은 B 에게만 있다.	
자산보호계약 실행 시 사용자의 자산을 보관하는 곳은 C 이다	

[0058] 상기 보호계좌는 세 가지 방법들에 의해 생성될 수 있다.

[0059] 첫 번째 방법은 도 7에 도시된 바와 같이, 상기 사용자 단말기(10)로부터 상기 사용자 단말기에 의해 관리되는 암호화폐가 지속적으로 사용되지 않는 계약실행 대기기간 및 계약요청이 수신되면 상기 관리시스템(30)이 자산보호계약을 구성하고 블럭체인에 전달한다. 블럭체인은 전달받은 자산보호계약에 따라 보호계좌를 생성한다. 관리시스템(30)은 보호계좌 생성결과를 확인후 저장하고 사용자 단말기(10)에 전달한다.

[0060] 상세한 절차는 도 8 및 이하에 기재된 바와 같다.

[0061] 1. 상기 사용자 단말기(10)에 계약항목을 입력하고 일반계좌를 생성한다.

[0062] 2. 상기 사용자 단말기(10)가 계약항목과 일반계좌정보를 관리시스템에 전송한다.

[0063] 3. 상기 관리시스템(30)이 사용자자산 임시보호계좌 정보, 트리거계좌 정보, 자산보호작동기 정보, 계약항목, 일반계좌정보를 모아 자산보호계약을 구성한다.

[0064] 4. 관리시스템(30)이 자산보호계약구성을 블럭체인으로 전달한다.

[0065] 5. 블럭체인이 자산보호계약이 담긴 보호계좌를 생성한다.

[0066] 6. 처리된 보호계좌 정보를 상기 관리시스템(30)이 사용자 정보와 묶어 저장한다.

[0067] 7. 상기 관리시스템(30)이 보호계좌 정보를 상기 사용자 단말기(10)에 전달한다.

[0068] 8. 상기 사용자 단말기(10)는 상기 관리시스템(30)으로부터 전달받은 보호계좌 정보를 등록한다.

[0069] 상기 보호계좌가 생성되면, 상기 사용자 단말기(10)는 상기 일반계좌에서 관리되는 암호화폐를 상기 보호계좌로 전송하여 관리할 수 있다.

[0070] 두 번째 방법은 도 9 에 도시된 바와 같이, 상기 사용자 단말기(10)로부터 상기 사용자 단말기에 의해 관리되는 암호화폐가 지속적으로 사용되지 않는 계약실행 대기기간을 입력받은후 자산보호계약내용을 상기관리시스템(30)에 요청하면 상기 관리시스템(30)이 가지고있는 자산보호계약내용을 상기 사용자 단말기(10)에 전달한다. 상

기 사용자 단말기(10)는 자산보호계약을 구성하고 블럭체인에 전달한다. 블럭체인은 전달받은 자산보호계약에 따라 보호계좌를 생성한다. 사용자 단말기(10)는 보호계좌 생성결과를 확인후 저장하고 관리시스템(30)에 전달한다.

[0071] 상세한 절차는 도 9 및 이하에 기재된 바와 같다.

[0072] 1. 상기 사용자 단말기(10)에 계약항목을 입력하고 일반계좌를 생성한다.

[0073] 2. 상기 관리시스템(30)이 사용자자산 임시보호계좌 정보, 트리거계좌 정보, 자산보호작동기 정보를 상기 사용자 단말기(10)에 전달한다.

[0074] 3. 상기 사용자 단말기(10)가 상기 관리시스템(30)의 사용자자산 임시보호계좌 정보, 트리거계좌 정보, 자산보호작동기 정보, 상기 사용자 단말기(10)의 계약항목, 일반계좌정보를 모아 자산보호계약을 구성한다.

[0075] 4. 상기 사용자 단말기(10)가 자산보호계약구성을 블럭체인으로 전달한다.

[0076] 5. 블럭체인이 자산보호계약이 담긴 보호계좌를 생성한다.

[0077] 6. 처리된 보호계좌 정보를 상기 관리시스템(30)이 사용자 정보와 묶어 저장한다.

[0078] 7. 상기 관리시스템(30)이 보호계좌 정보를 상기 사용자 단말기(10)에 전달한다.

[0079] 8. 상기 사용자 단말기(10)는 상기 관리시스템(30)으로부터 전달받은 보호계좌 정보를 등록한다.

[0080] 상기 보호계좌가 생성되면, 상기 사용자 단말기(10)는 상기 일반계좌에서 관리되는 암호화폐를 상기 보호계좌로 전송하여 관리할 수 있다.

[0081] 세 번째 방법은 도 11에 도시된 바와 같이, 상기 사용자 단말기(10)로부터 상기 사용자 단말기(10)에 의해 관리되는 암호화폐가 지속적으로 사용되지 않는 계약실행 대기기간을 입력받은 후 상기 관리시스템(30)이 자산보호계약구성을 하고 상기 사용자 단말기(10)에 전달하고, 상기 사용자 단말기(10)는 자산보호계약구성을 완성후 블럭체인에 보호계좌생성 요청을 한다. 블럭체인은 생성된 보호계좌 정보를 상기 관리시스템(30)에 전송하고, 상기 관리시스템(30)은 보호계좌 정보를 저장후 상기 사용자 단말기(10)에 전달한다.

[0082] 상세한 절차는 도 12 및 이하에 기재된 바와 같다.

[0083] 1. 상기 사용자 단말기(10)에 계약항목을 입력하고 일반계좌를 생성한다.

[0084] 2. 상기 관리시스템(30)이 사용자자산 임시보호계좌 정보, 트리거계좌 정보, 자산보호작동기 정보로 자산보호계약을 구성한다.

[0085] 3. 상기 관리시스템(30)이 자산보호계약구성을 상기 사용자 단말기(10)에 전달한다.

[0086] 4, 상기 사용자 단말기(10)의 계약항목, 일반계좌정보를 모아 자산보호계약을 구성한다.

[0087] 5. 상기 사용자 단말기(10)가 자산보호계약구성을 블럭체인으로 전달한다.

[0088] 6. 블럭체인이 자산보호계약이 담긴 보호계좌를 생성한다.

[0089] 7. 생성된 보호계좌 정보를 상기 관리시스템(30)이 저장한다.

[0090] 8. 상기 관리시스템(30)이 보호계좌 정보를 상기 사용자 단말기(10)에 전달한다.

[0091] 상기 보호계좌가 생성되면, 상기 사용자 단말기(10)는 상기 일반계좌에서 관리되는 암호화폐를 상기 보호계좌로 전송하여 관리할 수 있다.

[0092] 상기 일반계좌와 보호계좌는 적어도 하나 이상 생성될 수 있다. 상기 보호계좌가 두 개 이상 생성된 경우, 상기 보호계좌들 각각에는 서로 다른 종류의 토큰들과 한종류의 암호화폐가 보관될 수 있다.

[0093] < 5. 암호화폐를 이용하는 단계(310) >

[0094] 상기 일반계좌 및 상기 보호계좌가 생성되면, 사용자는 상기 보호계좌에 저장된 암호화폐를 이용할 수 있다. 상기 암호화폐가 이용되는 방법은 현재 일반적으로 이용되는 암호화폐 이용 방법이 적용될 수 있다. 따라서, 암호화폐가 이용되는 방법에 대한 상세한 설명은 생략된다.

[0095] 이 경우, 상기 사용자 단말기는 암호화폐 지갑이 될 수 있다.

[0096] 암호화폐가 사용될 때, 상기 일반계좌 및 상기 보호계좌는 구분되지 않는다.

[0097] 즉, 암호화폐가 이용될 때, 상기 보호계좌에 저장되어 있는 상기 암호화폐는 상기 일반계좌를 통해 타 계좌로 이체되며, 타 계좌로부터 이체되온 암호화폐는 상기 일반계좌를 통해 상기 보호계좌로 전송되어 관리된다.

[0098] 따라서, 사용자는 상기 일반계좌를 통해 암호화폐가 관리되는 것으로 인식할 수 있다.

[0099] < 6. 계약실행 대기기간 경과 후 트리거 계좌의 서명을 통해 자산보호계약이 실행되어 상기 암호화폐와 토큰이 사용자자산 임시보호계좌로 이체되는 단계(312) >

[0100] 상기 계약실행 대기기간이 경과하면, 상기 관리 시스템(30)의 사용자자산 임시보호계좌로 상기 암호화폐와 토큰이 이체된다.

[0101] 즉, 상기 계약실행 대기기간이 경과하면, 상기 관리 시스템(30)은 상기 보호계좌에서 관리되는 암호화폐와 토큰을 사용자자산 임시보호계좌로 이체할 수 있다.

[0102] 이 경우, 상기 이체를 요청하는 정보가 상기 관리 시스템(30)으로부터 수신되면, 상기 암호화폐는 상기 사용자 단말기(10)에 의해 상기 관리 시스템(30)으로 전송될 수 있다.

[0103] 또 다른 방법으로서, 상기 관리 시스템(30)이 상기 사용자 단말기(10)로부터 상기 암호화폐와 토큰을 강제로 상기 사용자자산 임시보호계좌로 이체할 수도 있다.

[0104] 또 다른 방법으로서, 상기 서비스앱에 의해 상기 암호화폐에 대한 정보를 지속적으로 관리하고 있는 상기 관리 시스템(30)에서, 상기 암호화폐에 대한 이체가 자동적으로 수행될 수도 있다. 예를 들어, 상기 보호계좌에 대한 정보는 상기 관리 시스템(30)에서 지속적으로 관리될 수 있다. 따라서, 상기 보호계좌를 통한 송금 또는 입금이 수행되면, 상기 관리 시스템(30) 역시, 상기 서비스앱을 통해 상기 보호계좌를 통한 송금 또는 입금에 대한 정보를 수신하여 관리할 수 있다. 따라서, 상기 관리 시스템(30)은 상기 보호계좌에서 관리되는 암호화폐에 대한 정보와 동일한 정보를 지속적으로 관리할 수 있다. 이에 따라, 상기 계약실행 대기기간이 경과하면 상기 사용자 단말기(10)를 통한 상기 암호화폐의 거래가 보호계좌 내용에 따라 차단되며, 상기 관리 시스템(30)은 상기 관리 시스템(30)에 의해 관리되는 사용자자산 임시보호계좌를 통해 상기 암호화폐와 토큰의 이체(자산이동)를 관리할 수 있다.

[0105] 상기 계약실행 대기기간이 경과하기 전에 상기 보호계좌로부터 타 계좌로 출금이 발생되거나, 상기 보호계좌로 입금이 발생되면, 상기 사용자 단말기(10)는 상기 계약실행 대기기간은 자동으로 초기화된다.

[0106] 즉, 상기 계약실행 대기기간이 경과하였는지를 판단하는 시점은, 상기 보호계좌에 대한 입/출금이 발생된 시점이 된다.

[0107] 예를 들어, 상기 계약실행 대기기간이 7일로 설정되고, 2월1일에 마지막으로 상기 보호계좌에 대한 입/출금이 발생되었다면, 상기한 바와 같은 이체는 2월8일 이후에 실행될 수 있다.

[0108] 이 경우, 만약, 2월6일에 상기 보호계좌에서 입/출금이 발생되었다면, 상기 계약실행 대기기간이 경과하였는지를 판단하는 시점은 2월6일로 초기화된다. 이 경우, 2월12일까지 지속적으로 상기 보호계좌에서 입/출금이 발생되지 않으면, 상기한 바와 같은 이체는 2월13일 이후에 실행될 수 있다. 즉, 블럭체인에서는 계좌열람에 대한 기록이 남지 않기 때문에, 본 발명은 입/출금 기록을 이용하여, 상기 계약실행 대기기간의 경과 여부를 판단할 수 있다.

[0109] 상기 계약실행 대기기간이 경과하더라도, 사용자에 대한 확인절차 후에 상기 이체가 실행될 수 있다.

[0110] 예를 들어, 상기 계약실행 대기기간이 경과하면(312a), 상기 관리 시스템(30)은 상기 사용자 정보에 포함된 정보들을 이용하여 상기 사용자와 연락을 시도하여, 계약실행, 즉, 사용자 연락불가시 암호화폐와 토큰이 사용자자산 임시보호계좌로 이체가 실행된다는 이체정보를 통지할 수 있다(312b).

[0111] 예를 들어, 상기 사용자 정보에 포함된 전화번호, 이메일, 비상 연락처, 주소 등으로 상기 이체가 실행될 수 있음을 알리는 정보를 전송할 수 있다.

[0112] 이 경우, 상기 관리 시스템(30)은 일차적으로 상기 사용자 단말기의 전화번호로 상기 이체정보를 전송할 수 있다.

[0113] 상기 통지에 의한 응답이 없으면, 상기 관리 시스템(30)은 상기 이메일, 또는 적어도 하나의 비상 연락처 또는

상기 주소로 동시에 또는 순차적으로 상기 이체정보를 전송할 수 있다.

[0114] 상기 이체정보를 전송하는 상기 시도 후 상기 사용자 또는 상기 사용자의 법적 승계인으로부터 정상적인 응답이 수신되면, 상기 관리 시스템(30)은 상기 이체를 실행하고, 이체된 암호화폐와 토큰 자산을 되돌려 줄 수 있다.(312c).

[0115] 상기 법적 승계인이란, 상기 사용자의 부모 또는 자녀가 될 수 있으며, 일반적으로 인식되어 있는 법적 승계인과 동일한 자가 될 수 있다.

[0116] 예를 들어, 상기 사용자가 사망하거나 연락을 취할 수 없는 경우, 상기 이체정보를 수신한 법적 승계인이 상기 사용자를 대리하여 상기 관리 시스템(30)에 정상적인 응답을 제공할 수 있다.

[0117] 상기 이체정보를 전송하는 상기 시도 후 상기 사용자 또는 법적 승계인으로부터 정상적인 응답이 수신되지 않으면, 상기 관리 시스템(30)은 상기 이체를 실행할 수 있다(312d).

[0118] < 7. 암호화폐와 토큰 반환 단계(314) >

[0119] 상기 암호화폐와 토큰이 상기 사용자자산 임시보호계좌로 이체된 후, 상기 사용자 또는 상기 사용자의 법적 승계인으로부터 반환 요청이 수신되면 상기 관리 시스템(30)은 상기 암호화폐와 토큰을 상기 사용자 또는 상기 사용자의 법적 승계인에게 반환할 수 있다.

[0120] 예를 들어, 상기 암호화폐와 토큰이 상기 사용자자산 임시보호계좌로 이체된 후, 상기 사용자 또는 상기 사용자의 법적 승계인으로부터 상기 암호화폐와 토큰에 대한 반환이 요청되면, 상기 관리 시스템(30)은, 상기 사용자 또는 상기 법적 승계인이 요청한 암호화폐 계좌로 상기 암호화폐와 토큰을 반환할 수 있다.

[0121] 즉, 상기 사용자 또는 상기 법적 승계인은 자신이 이용하는 단말기에서 관리되는 암호화폐 계좌로 상기 암호화폐와 토큰을 반환받은 후, 상기 암호화폐와 토큰을 이용할 수 있다.

[0122] < 관리 시스템 관점에서의 본 발명의 실행 방법 >

[0123] 상기 관리 시스템의 관점에서의 본 발명의 실행 방법을 간단히 정리하면 다음과 같다.

[0124] 우선, 상기 관리 시스템(30)은, 상기 사용자 단말기(10)로부터 수신된 사용자 정보를 이용하여 Seed 정보를 생성하며, 상기 Seed 정보를 상기 사용자 단말기(10)로 전송한다.

[0125] 다음, 상기 사용자 단말기(10)로부터 상기 사용자 단말기에 의해 관리되는 암호화폐와 토큰이 지속적으로 사용되지 않는 계약실행 대기기간 및 계약요청이 수신되면 상기 관리 시스템(30)은 보호계좌에 대한 정보를 생성하여 상기 사용자 단말기(10)로 전송할 수 있으며, 또는 상기 관리 시스템(30)은 상기 사용자 단말기(10)에서 생성된 보호계좌에 대한 정보를 상기 사용자 단말기로부터 수신하여 관리할 수 있다.

[0126] 다음, 상기 계약실행 대기기간이 경과하면, 상기 관리 시스템(30)은 상기 보호계좌에서 관리되는 암호화폐와 토큰을 상기 사용자자산 임시보호계좌로 이체할 수 있다.

[0127] 마지막으로, 상기 암호화폐와 토큰이 상기 사용자자산 임시보호계좌로 이체된 후, 상기 사용자 또는 상기 사용자의 법적 승계인으로부터 반환 요청이 수신되면 상기 관리 시스템(30)은 상기 암호화폐와 토큰을 상기 사용자 또는 상기 사용자의 법적 승계인에게 반환할 수 있다.

[0128] 이하에서, 상기에서 설명된 본 발명에 따른 암호화폐와 토큰의 분실 방지 방법이 도 14 및 도 15를 참조하여 다시 한 번 설명된다.

[0129] 도 14는 본 발명에 따른 자산보호계약(보호계좌)이 사용자의 토큰 자산을 보호하기 위한 권한을 획득하는 방법을 나타낸 예시도이다. 즉, 도 14는 본 발명에 따른 암호화폐 분실 방지 방법이 적용되는 관리 시스템에서 일반계좌의 토큰을 보호하기 위해 필요한 승인획득 과정을 나타낸 예시도이며, 특히, 도 14는 타 기업이나 기관에서 생성시킨 토큰에 대한 보호권한을 보호계좌에게 부여하는 절차를 설명한 예시도이다.

[0130] 관리 시스템(30)은 타기관/타사에서 생성된 토큰발행계약을 수정할 권한이 없다. 따라서 관리 시스템(30)은 사용자의 일반계좌의 토큰을 보호계좌로 토큰을 이동할 수 없다.

[0131] 상기한 바와 같은 이유로 인해, 일반계좌에서 보호계좌로 이동된 토큰은 일반계좌로 다시 보낼수가 없다. 즉, 보호계좌에 있는 토큰은 보호될 수 있지만, 일반계좌와 보호계좌 사이에 자유로운 이동이 불가능한 상황이다.

[0132] 이러한 이유 때문에, 일반계좌에 토큰을 두어야 하며, 비상시에 보호계좌로 토큰이 이동될 수 있어야 한다.

[0133] 도 14의 예시도에 따른 권한획득 과정은 아래에 나열한 것과 같다.

[0134] 1. 상기 사용자가 단말기(10)의 일반계좌에 토큰을 전송한다.

[0135] 2. 상기 사용자 단말기(10) 일반계좌에 존재하는 토큰을 계약실행대기기간 만료시 보호계좌로 옮길 수 있는 자산보호권한을 트리거계좌에 부여하는 구성을 한다.

[0136] 3. 블럭체인 내의 토큰발행계좌에 자산보호권한구성을 요청한다.

[0137] 4. 자산보호권한이 트리거계좌에 있음을 토큰발행계좌가 승인하고, 사용자 단말기에도 정보를 갱신한다.

[0138] 5. 토큰계좌(토큰을 보유중인 일반계좌)에 자산보호계약이 적용된다.

[0139] 6. 관리시스템에 토큰보호를 위한 보호계좌정보를 기록한다.

[0140] 도 15는 본 발명에 따른 자산보호계약(보호계좌)이 실행되어 사용자의 자산이 보호되는 절차를 나타낸 예시도이다. 즉, 도 15는 본 발명에 따른 암호화폐와 토큰 분실 방지 방법에 의한 계약이 실행되어 암호화폐와 토콘이 이체되는 방법을 나타낸 예시도이며, 특히, 도 15는 암호화폐와 토큰 각각에 대한 자산보호계약의 실행 절차를 설명한 예시도이다.

[0141] 우선, 다음과 같은 과정들이 수행된다.

[0142] 1. 사용자가 사용자 단말기 일반계좌로 자산(암호화폐와 토큰)을 입금한다. 암호화폐는 보호계좌로 이동 보호된다.

[0143] 2. 단말기는 블럭체인의 자산보호대기기간이 만료되었는지 확인한다.

[0144] 3.자산보호기간이 만료되면 단말기는 사용자에게 알린다.

[0145] 또한, 다음과 같은 과정들이 수행된다.

[0146] 1. 관리시스템의 자산보호대기기간을 확인한다.

[0147] 2. 관리시스템의 사용자 자산보호대기기간과 블럭체인의 자산보호계약에 기록된 사용자의 자산보호대기기간을 비교한다.

[0148] 3. 자산보호대기기간 확인 후 일치하면 자산보호실행명령에 의해 트리거계좌가 생성된다.

[0149] 4. 자산보호실행명령을 블럭체인에 전달한다.

[0150] 5. 블럭체인은 자산보호실행을 명령하기 전 자산보호대기기간이 경과되었는지 확인한다.

[0151] 6. 보호계좌의 자산보호계약이 실행된다.

[0152] 7. 사용자 일반계좌의 토큰을 보호계좌로 옮긴다.

[0153] 8. 보호계좌의 토큰을 사용자자산임시보호계좌로 옮긴다.

[0154] 9. 암호화폐를 위한 자산보호계약이 실행된다.

[0155] 10. 보호계좌의 암호화폐를 사용자자산 임시보호계좌로 옮긴다.

[0156] 11. 보호계좌의 처리결과가 관리시스템에 전달된다.

[0157] 12. 자산보호실행완료 확인후 보호계좌 정보와 사용자 정보가 갱신된다.

[0158] 본 발명이 속하는 기술분야의 당업자는 본 발명이 그 기술적 사상이나 필수적 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로, 이상에서 기술한 실시 예들은 모든 면에서 예시적인 것이며 한정적인 것이 아닌 것으로 이해해야만 한다. 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 등가 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

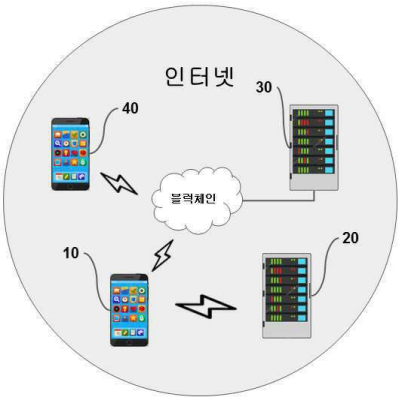
부호의 설명

[0159] 10: 사용자 단말기 20: 클라우드 서버

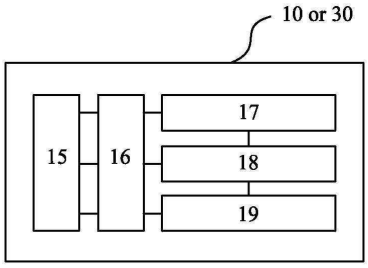
30: 관리 시스템 40: 암호화폐 단말기

도면

도면1

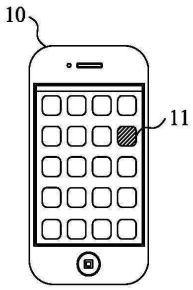


도면2

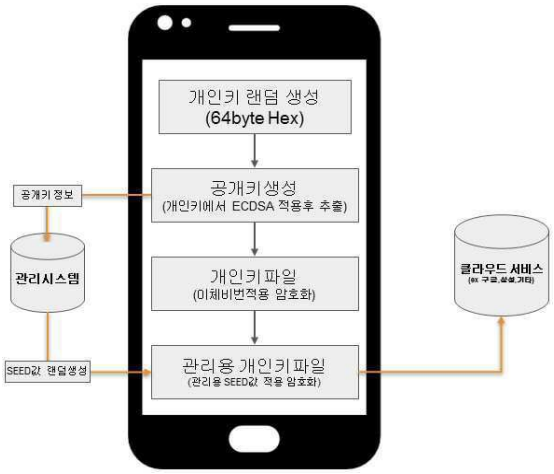


도면3

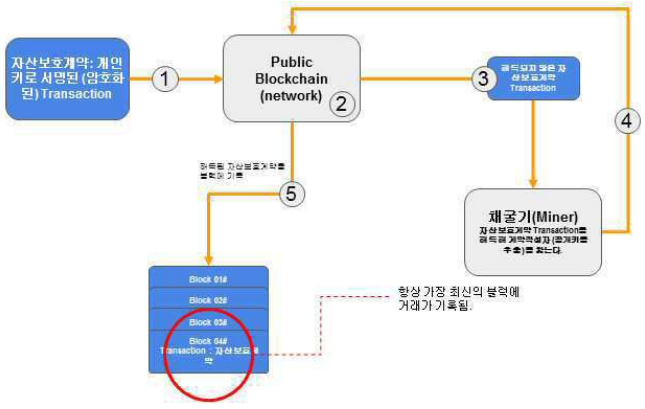
도면4


10
11

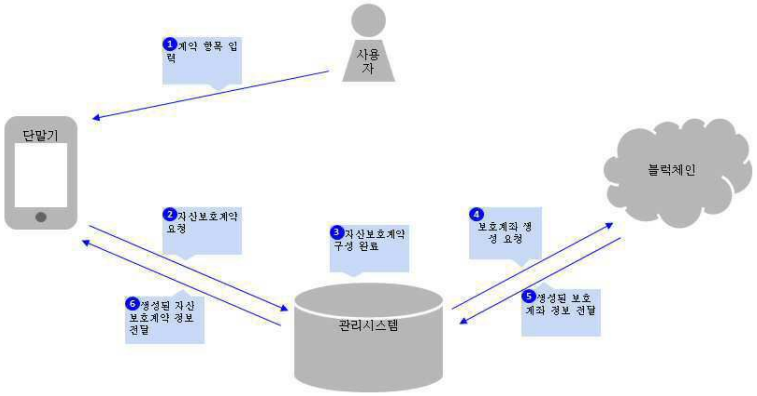
도면5


개인키 랜덤 생성
(64byte Hex)
공개키생성
(개인키에서 ECDSA 적용후 추출)
개인키파일
(이체비번적용 암호화)
관리용 개인키파일
(관리용 SEED값 적용 암호화)
공개키 정보
관리시스템
SEED값 랜덤생성
클라우드 서비스

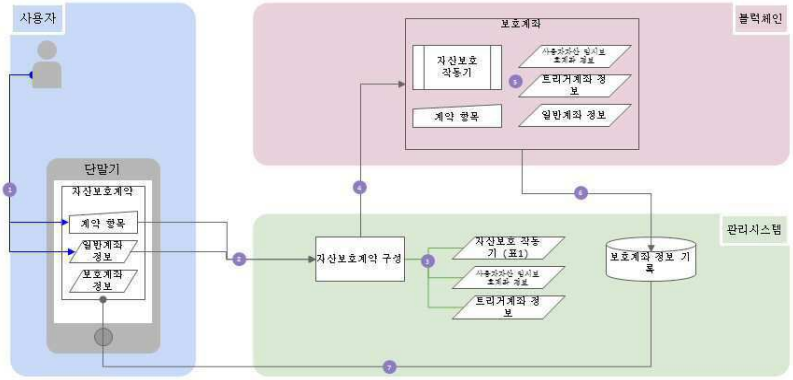
도면6


자산보호계약: 계인키로 서명된 (암호화된) Transaction
1
Public Blockchain (network)
2
3
4
5
채굴기(Miner)
Block 01#
Block 02#
Block 03#
Block 04#
항상 가장 최신의 블럭에 거래가 기록됨.

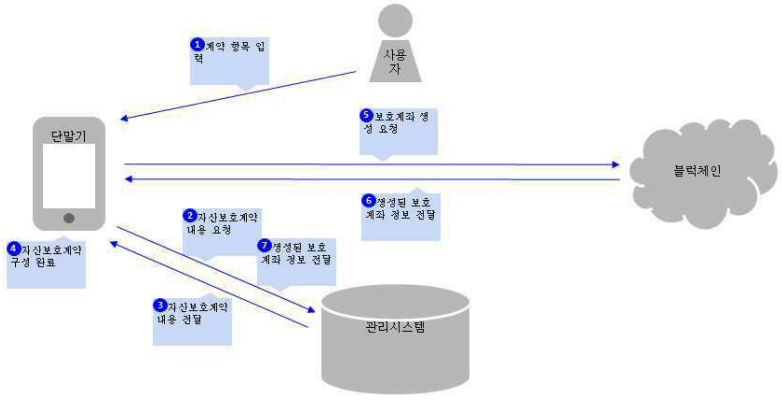
도면7


1계약 항목 입력
사용자
단말기
블럭체인
2자산보호계약 요청
3자산보호계약 구성 완료
4보호계좌 생성 요청
6생성된 자산 보호계약 정보 전달
관리시스템
5생성된 보호 계좌 정보 전달

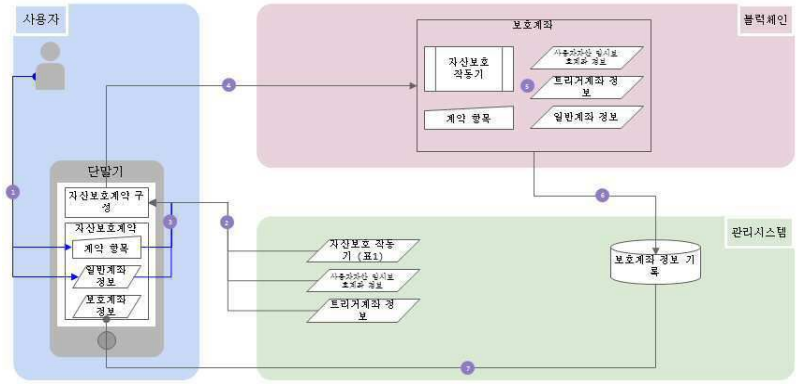
도면8


사용자
단말기
자산보호계약
계약 항목
일반계좌 정보
보호계좌 정보
보호계좌
자산보호 작동기
계약 항목
트리거계좌 정보
일반계좌 정보
블럭체인
자산보호계약 구성
자산보호 작동기 (표1)
트리거계좌 정보
보호계좌 정보 기록
관리시스템

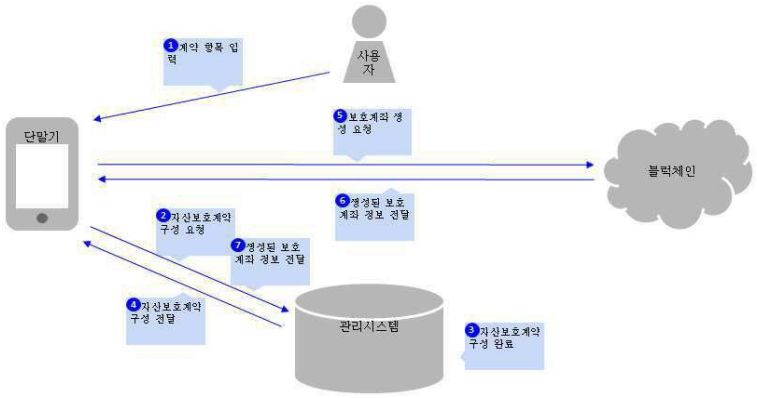
도면9


1계약 항목 입력
사용자
단말기
5보호계좌 생성 요청
블럭체인
6생성된 보호 계좌 정보 전달
2자산보호계약 내용 요청
4자산보호계약 구성 완료
7생성된 보호 계좌 정보 전달
3자산보호계약 내용 전달
관리시스템

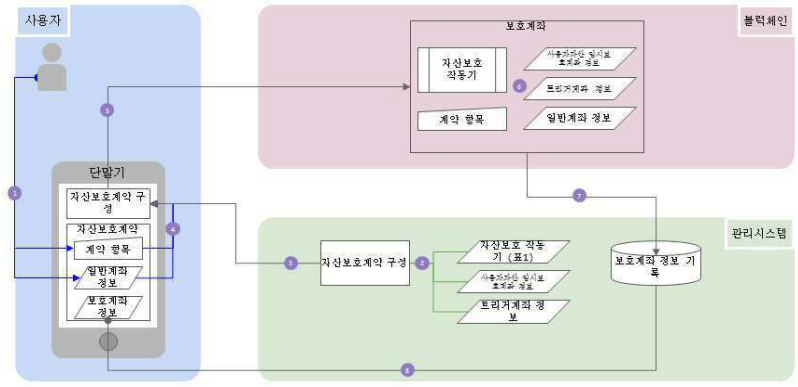
도면10



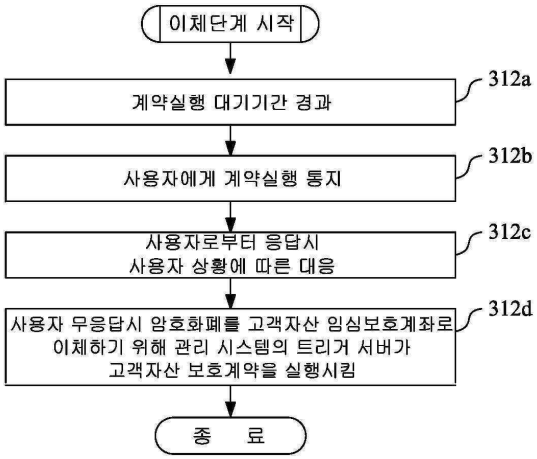
도면11



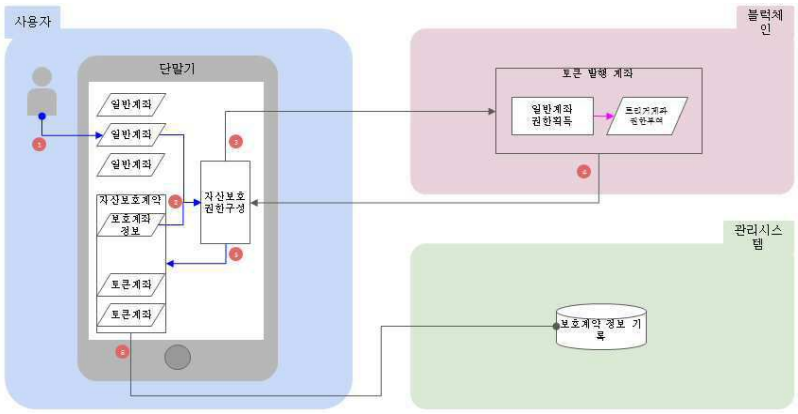
도면12



도면13



도면14



도면15