(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0065182
(43) 공개일자 2023년05월11일

(51) 국제특허분류(Int. Cl.)
G06Q 20/38 (2012.01) *G06Q 20/06* (2012.01)
G06Q 20/10 (2012.01) *H04L 9/00* (2022.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
G06Q 20/382 (2013.01)
G06Q 20/065 (2013.01)
(21) 출원번호 10-2022-0145237
(22) 출원일자 2022년11월03일
심사청구일자 2022년11월03일
(30) 우선권주장
1020210149772 2021년11월03일 대한민국(KR)

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
김형중
서울특별시 서초구
김범중
경기도 군포시 수리산로 244, 996동 1301호 (산본동, 한양백두아파트)
(74) 대리인
김등용

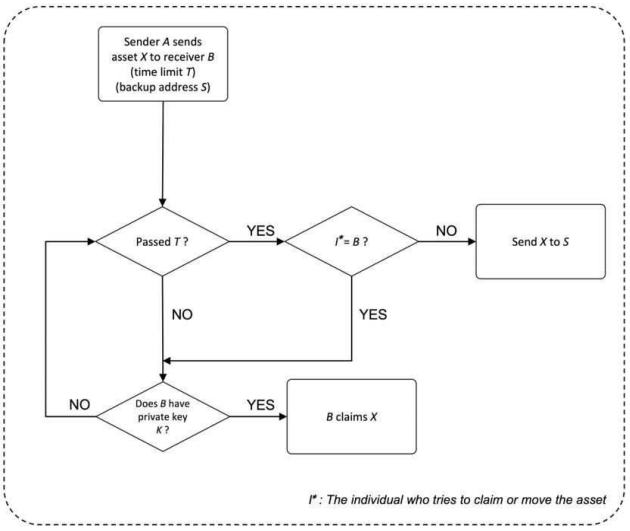
전체 청구항 수 : 총 7 항

(54) 발명의 명칭 **스마트 컨트랙트 기반 가상 자산 회생 방법**

(57) 요 약

스마트 컨트랙트를 이용한 가상 자산 회생 방법이 개시된다. 상기 가상 자산 회생 방법은 송신자의 단말이 가상 자산의 전송에 대한 스마트 컨트랙트를 생성하는 단계, 상기 송신자의 단말이 상기 스마트 컨트랙트를 포함하는 블록을 블록체인에 업로드하는 단계, 및 상기 가상 자산이 상기 가상 자산의 송신자의 계좌 또는 상기 가상 자산의 수신자의 계좌로 이동하는 단계를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
G06Q 20/10 (2013.01)
H04L 9/0825 (2013.01)
H04L 9/50 (2022.05)
H04L 2209/56 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1465032658
과제번호 HI19C0785010021
부처명 보건복지부
과제관리(전문)기관명 한국보건산업진흥원
연구사업명 의료데이터보호·활용기술개발(R&D)
연구과제명 블록체인 기술을 활용한 임상시험 데이터의 보호 및 역동적 동의 체계 알고리즘 개발
기 여 율 1/1
과제수행기관명 고려대학교산학협력단
연구기간 2019.07.25 ~ 2021.12.31

명 세 서

청구범위

청구항 1

송신자의 단말이 가상 자산의 전송에 대한 스마트 컨트랙트를 생성하는 단계;

상기 송신자의 단말이 상기 스마트 컨트랙트를 포함하는 블록을 블록체인에 업로드하는 단계; 및

상기 가상 자산이 상기 가상 자산의 송신자의 계좌 또는 상기 가상 자산의 수신자의 계좌로 이동하는 단계를 포함하는 가상 자산의 회생 방법.

청구항 2

제1항에 있어서,

상기 업로드하는 단계 이후에,

상기 스마트 컨트랙트의 실행에 따라 상기 가상 자산이 미리 정해진 계좌로 전송되는 단계를 더 포함하는,

가상 자산의 회생 방법.

청구항 3

제2항에 있어서,

상기 스마트 컨트랙트는 상기 수신자의 계좌의 주소, 상기 가상 자산을 환수할 환수 주소, 및 데드라인(deadline)에 대한 정보를 포함하는,

가상 자산의 회생 방법.

청구항 4

제3항에 있어서,

상기 이동하는 단계는,

상기 스마트 컨트랙트가 생성된 이후 상기 데드라인이 경과한 경우, 상기 가상 자산이 상기 환수 주소로 이동하는 단계를 포함하는,

가상 자산의 회생 방법.

청구항 5

제4항에 있어서,

상기 환수 주소로 이동하는 단계는,

상기 송신자의 단말에 의해 블록체인 네트워크를 구성하는 적어도 하나의 노드로 전송되는 환수 요청에 응답하여 실행되는,

가상 자산의 회생 방법.

청구항 6

제3항에 있어서,

상기 이동하는 단계는,

상기 스마트 컨트랙트가 생성된 이후 상기 데드라인이 경과하기 전에, 상기 가상 자산이 상기 수신자의 계좌로 이동하는 단계를 포함하는,

가상 자산의 회생 방법.

청구항 7

제6항에 있어서,

상기 수신자의 계좌로 이동하는 단계는,

상기 수신자의 단말에 의해 블록체인 네트워크를 구성하는 적어도 하나의 노드로 전송되는 요청에 응답하여 실행되는,

가상 자산의 회생 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 암호화폐나 각 국가의 중앙은행이 발행하는 디지털 화폐 등의 가장 자산의 회생 방법에 관한 것이다.

배 경 기 술

[0002] 블록체인에서 잘못된 주소로 자산을 전송하면 전송된 자산을 환수할 수 없다. 또한, 제대로 된 주소로 전송하더라도 수신자가 비밀키를 분실하는 경우 동일한 일이 발생한다. 이와 유사한 일이 발생할 경우, 의도하지 않은 실수로부터 자산을 안전하게 회수하는 방법이 필요하다.

[0003] 비트코인의 경우 TimeLock 등의 스마트 컨트랙트 프리미티브(nLockTime 등)를 내장하고 있엇, 특정한 시간 동안 전송한 자산을 잠기게 하거나 특정한 조건 하에서 자산을 환수할는 데 활용하고 있다. 존재하지 않는 주소로 자산을 전송하면 비밀키가 없어서 자산을 찾을 수 없다. 또한, 존재하는 주소로 전송이 이루어지더라도 수신자가 비밀키를 분실해서 많은 자산을 찾지 못하는 사례가 있다. 이더리움에서 많은 양의 자산을 보내거나 받을 때, 불의의 사고를 신속히 중지시키기 위해 유가능한(suspendable) 스마트 컨트랙트를 작성하도록 권장한다. 그러나, 이 경우 문제를 인지한 순간부터 자산의 이동을 중지시킬 뿐 회수하는 기능을 포함하고 있지 않다.

[0004] 일반적으로, 수신자가 송신자에게 자산을 수신할 주소를 보내면 송신자가 그 주소로 자산을 보낸다. 이때, 송신자 또는 수신자의 실수로 존재하지 않는 주소로 자산을 보낼 수 있다. 수신자가 착오로 잘못된 주소를 보내줘서 송신자가 그 주소로 보내는 것과 수신자가 바른 주소를 보내줬는데 송신자가 실수로 잘못된 주소로 보내는 경우를 상정해 볼 수 있다. 잘못된 주소로 보냈더라도 그 주소에 해당하는 비밀키를 지닌 제3자가 존재하는 경우에는 제3자의 처분을 따라야 하지만 논의할 여지를 마련할 수 있으면 좋다.

[0005] 실수로 보내진 자산은 그 주소에 대응하는 비밀키를 모르면 회수가 불가능하다. 송신자가 악의적으로 실수를 가장하여 자산을 전송한 후 대응하는 비밀키로 자산을 되찾아 가는 사기 행위는 여기에 해당하지 않는다. 본 발명에서 다루는 내용은 실제하지 않는 주소로 전송한 자산 또는 실제하는 주소이지만 해당 비밀키의 분실 등으로 회수할 수 없는 자산 등을 회생하는 방법이다.

[0006] 하지만, 존재하지 않는 주소란 없다. 주소가 존재하므로 자산 전송이 이루어 진다. 다만, 그 주소에 해당하는 비밀키를 모르기 때문에 자산을 찾을 수 없고, 그래서 통칭 존재하지 않는 주소라고 말한다. 존재하지 않는 주소로 송금하면 나타는 현상 가운데 하나가 자산이 영구히 이동하지 않는 것이다. 그렇지만, 자산이 이동하지 않는다고 해서 그 주소가 존재하지 않는 것은 아니다. 수신자가 자산을 이동시키지 않아서 그럴 수 있다. 수신자의 주소로 정확하게 전송이 되어도, 수신자가 비밀키를 분실하거나 비밀키를 공개하지 않고 사망하면, 자산을 찾을 수 없다. 이 경우 또한 본 발명에서 제안하는 방법을 통해 해결할 수 있다.

[0007] 일정 시간 이상 자산이 이동하지 않는 경우, 위에서 설명된 경우들에 따라 자산을 찾을 수 없다고 판단할 수 있다. 그러므로, 스마트 컨트랙트를 통해 자산을 관리하고 이러한 사건들에 대해 대비할 필요가 있다.

발명의 내용

해결하려는 과제

[0008] 본 발명이 이루고자 하는 기술적인 과제는 스마트 컨트랙트에 기반한 가상 자산 회생 방법을 제공하는 것이다.

과제의 해결 수단

[0009] 본 발명의 일 실시예에 따른 가상 자산 회생 방법은 송신자의 단말이 가상 자산의 전송에 대한 스마트 컨트랙트를 생성하는 단계, 상기 송신자의 단말이 상기 스마트 컨트랙트를 포함하는 블록을 블록체인에 업로드하는 단계, 및 상기 가상 자산이 상기 가상 자산의 송신자의 계좌 또는 상기 가상 자산의 수신자의 계좌로 이동하는 단계를 포함한다.

발명의 효과

[0010] 본 발명의 실시예들에 의할 경우, 상술한 사례에 대한 해결책을 제시하여 안전하게 가상 자산을 회생(또는 회수)할 수 있다.

도면의 간단한 설명

[0011] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시예에 따른 가상 자산 환수 방법을 설명하기 위한 흐름도이다.

도 2는 본 발명에서 제안하는 스마트 컨트랙트의 수도 코드(pseudo-code)를 도시한다.

도 3은 본 발명의 일 실시예에 따른 스마트 컨트랙트의 동작을 설명하기 위한 흐름도이다.

도 4는 본 발명의 일 실시예에 따른 가상 자산 회생 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0012] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시예들에 대해서 특정한 구조적 또는 기능적 설명들은 단지 본 발명의 개념에 따른 실시예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시예들에 한정되지 않는다.

[0013] 본 발명의 개념에 따른 실시예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

[0014] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

[0015] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.

[0016] 본 명세서에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0017] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의

미로 해석되지 않는다.

[0018] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시예들을 상세히 설명한다. 그러나, 특허출원의 범위가 이러한 실시예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[0019] 본 발명에서는 가상 자산(Cryptoasset, 암호 자산, 암호 화폐, 블록 자산, 블록체인 자산, 디지털 자산, 디지털 화폐, 가상 화폐 등으로 명명될 수도 있음)의 분실을 피하기 위해 KSC(Kim smart contract)로 불리는 스마트 컨트랙트(smart contract)를 이용한 회생가능한 트랜잭션(transaction) 방법(recoverable transaction method)을 제안한다. 트랜잭션은 가상 자산이 예기치 않게 소멸되거나 분실되는 것을 방지기 위하여 회생가능하여야 한다. 제안 기법은, 블록체인의 불변성(blockchain's immutability)을 위반하지 않고, 일정 시간이 경과한 후에 송신자가 가상 자산을 회복할 수 있도록 한다.

[0020] 가상 자산이 일정 시간이 경과한 후에도 이동하지 않는 적어도 두가지 이유가 있다. 첫째로, 가상 자산을 즉시 이용할 필요성이 없기 때문이다. 예컨대, 가상 자산의 가치가 상승할 것으로 예측하는 가상 자산의 보유자는 보유한 가상 자산을 바로 이용하지 않고 기다림을 택할 수 있다. 이는 대부분의 케이스에 해당하는 이유이다. 둘째로, 비밀키(private key, 개인키로 명명될 수도 있음)의 분실이다. 따라서, 가상 자산이 특정 시간 구간이 경과한 후에 이동하지 않으면, 가상 자산을 특정 주소로 환수할 수 있도록 하는 스마트 컨트랙트를 제안한다.

[0021] 본 발명에는 두 가지 키 포인트가 존재한다. 하나는 특정 시간, 즉 데드라인(deadline)을 설정하는 것이고, 다른 하나는 오리지널 수신자의 비밀키 없이 가상 자산을 환수할 수 있도록 하는 스마트 컨트랙트이다. 원래, 비밀키가 없으면 가상 자산은 이동될 수 없다. 그러나, 데드라인이 경과한 후, KSC와 같은 스마트 컨트랙트에 의해 비밀키가 없는 상태에서도 가상 자산은 이동될 수 있다. 여기서, 시간은 인계철선(wripwire)의 역할을 수행한다. 이는 제안 기법의 키 포인트 중 하나이다.

[0022] 가상 자산이 계좌(account)에 위치한 후에, 가상 자산의 상태(status)는 완결된다. 계좌에 존재하는 가상 자산은, 해당 계좌의 비밀키를 이용할 수 있을 때에만 철회되거나(withdrawn) 이동될(moved) 수 있다. 그러나, 가상 자산이 스마트 컨트랙트에 존재하면(즉, 미리 지정된 계좌에 존재하면), 비밀키를 이용할 수 없는 경우라도 스마트 컨트랙트에 따라 가상 자산은 철회되거나 이동될 수 있다. 가상 자산에 대한 보안을 향상시키기 위하여, 가상 자산은 일시적으로(temporarily) 스마트 컨트랙트(의 계좌)에 저장(또는 이동)될 수 있다. 이는 제안 기법의 또다른 키 포인트이다.

[0023] 트랜잭션은, 트랜잭션 그 자체는 철회할 수 없지만(irreversible), 가상 자산을 회생할(reversible) 수 있도록 하여야 한다. 또한, 가상 자산은 특정 시간 이후에 환불가능(refundable)하기 때문에, 잘못된 트랜잭션 문제를 해결할 수 있다. 가상 자산이 존재하지 않는 주소로 전송된 경우라도, 또는 비밀키가 분실된 경우라도, 제안 기법을 이용하면 가상 자산을 송신자가 회복(또는 회수)할 수 있다. 데드라인이 경과한 이후라도, KSC를 실행되지 않았다면 비밀키의 소유자는 가상 자산을 철회할 수 있다. 이때, KSC를 실행하는 자는 송신자, 수신자, 또는 제3자(대부분의 경우, 송신자 또는 수신자일 수 있음)를 의미할 수 있다.

[0024] 실시예에 따라, 백업 계좌 주소(backup account address, 환수 주소)를 사용함으로써, 트랜잭션의 안전성을 더욱 향상시킬 수 있다. 송신자와 수신자 사이에서 사전에 합의된 백업 계좌 주소는 특정 시간 구간이 경과한 후에 가상 자산을 유지(즉, 가상 자산을 수신)할 계좌의 주소이다. 본 발명에서 제안하는 백업 계좌 주소는 송신자의 계좌 주소일 수 있다. 그러나, 본 발명이 이에 제한되는 것은 아니며, 실시예에 따라, 백업 계좌 주소는 제3자의 계좌 주소로 구현 가능하다.

[0025] 송신자의 계좌 주소를 백업 계좌 주소로 제안하는 이유는 간단하다. 송신자가 가상 자산을 존재하지 않는 주소로 송신하면, 가상 자산은 송신자에게 환수되어야 한다. 수신자가 비밀키를 분실한 경우, 송신자와 수신자는 그들 사이의 트랜잭션 히스토리를 알고 있기 때문에, 가상 자산은 송신자에게 환수되어야 한다. 수신자가 비밀키를 가족이나 친인척 등에게 알려주지 않은 채 사망한 경우, 트랜잭션의 참여자들은 그들 사이의 트랜잭션 히스토리를 알고 있기 때문에, 가상 자산은 유사하게 송신자에게 환수되어야 한다.

[0026] 요컨대, 제안 기법은 의도치 않은 가상 자산의 분실을 예방할 수 있다. 이러한 기법을 통해, Alice(계좌 주소 A를 갖는 송신자)는, 가상 자산 X를 Bob(계좌 주소 B를 갖는 수신자)에게 송신하기 전에, 제한 시간(time limit) T를 설정하고 백업 계좌의 주소(환수 주소) S(A와 동일할 수 있음)를 명세할 수 있다. KSC를 이용할 때, 두 당사자는 사전에 데드라인 T와 백업 계좌 주소 S에 동의(합의)하여야 한다. 데드라인 T는 정당한 수신자인 Bob을 위한 유예 기간(grace period)으로 동작한다. 데드라인이 경과한 후라도, 가상 자산이 백업 계좌로 이동하지 않

았다면, Bob은 비밀키를 보유하고 있는 한 가상 자산을 요청(claim)할 수도 있다.

[0027] KSC에서는 3 가지의 함수들이 이용된다. 첫번째 함수는 데드라인을 설정하고 백업 계좌의 주소를 명세한다. 첫번째 함수는 가상 자산 X를 Alice의 계좌로부터, 수신자가 X를 요구할 수 있는 KSC 자체(예컨대, KSC의 계좌)로 전송한다. KSC(의 계좌)는 주소 K에 존재한다. 두번째 함수는 요구된 가상 자산 X를 KSC로부터 수신자의 계좌로 이동시킨다. 세번째 함수는 요구되지 않은 가상 자산 X를 KSC로부터 백업 계좌로 이동시킨다.

[0028] Alice와 Bob의 합의에 따라, Alice는 X를 Bob에게 전송한다. 그러나, X는 Bob의 계좌로 바로 전송되지 않고, 우선 KSC(즉, 미리 정해진 계좌)로 전송된다. Alice와 Bob은 Alice의 주소를 S(백업 계좌의 주소)로 설정하는 것에 대해 합의할 수 있기 때문에, KSC는 환수에 대한 자유도를 준다. KSC가 없는 경우(즉, 종래의 트랜잭션의 경우), X가 일단 수신자의 계좌로 이동하면, 이동된 X는 비밀키가 없는 한 환수될 수 없다.

[0029] 수신자 Bob은 가상 자산 X를 스마트 컨트랙트로부터 자신의 계좌로 전송하기 위한 함수 *Claim*을 실행하여야 한다. 이러한 실행은 데드라인의 경과 여부와는 무관하게 진행되거나 처리될 수도 있다.

[0030] 데드라인 경과 후, 가상 자산이 요구되지 않은 상태인 한, KSC의 가상 자산을 백업 계좌(주소 S를 갖음)로 이동하기 위한 함수 *Move*가 실행될 수 있다. 함수 *Move*가 실행된 이후에는, KSC로부터 이동된 가상 자산 X에 대한 Bob의 요구는 충족될 수 없다.

[0031] Alice는 A와 S를 설정함으로써, 가상 자산이 자신에게 회수(환수 또는 이동)될 수 있도록 할 수 있다. 제안하는 기법의 흐름도는 도 1에 도시되어 있다. 제안하는 기법은 체인 솔루션 상에(on-cahin solution) 탑재될 수 있고, 스마트 컨트랙트를 지원하는 모든 블록체인 플랫폼에 적용가능하다. 또한, 제안 기법은 스마트 컨트랙트를 지원하지 않는 어떠한 블록체인 플랫폼에도, 비트코인의 *nLockTime* 파라미터와 같은 시간 제한 기능들(time-limiting functionalities)을 가지고 있다면, 적용이 가능하다. 체인 상에 구현이 불가능한 경우, 부채널(side channels)의 이용이 고려될 수 있다. 이하에서는, KSC에 대해 보다 구체적으로 설명한다.

[0032] 1. 초기화(Initialization)

[0033] KSC를 초기화하기 위해, TTP(a trusted third party)가 KSC를 채용하는 것이 필요하다. KSC의 수도코드는 도 2에 도시되어 있고, KSC의 동작을 설명하기 위한 흐름도은 도 3에 도시되어 있다. 스마트 컨트랙트는 개인들이 그들 사이에서 회생가능한 트랜잭션을 생성하도록 한다. 사전에 생성된 KSC가 재사용될 수도 있다. TTP는 컨트랙트의 취약성을 식별하여 손실을 최소화하도록 스마트 컨트랙트를 감사할 필요가 있다. 또한, 도 2의 수도코드에서 활용된 용어에 대한 정의는 표 1에 나타나 있다.

[0034] [표 1]

Symbol	Meaning
K	Address of Kim smart contract
A	Address of a sender's account
B	Address of a receiver's account
S	Address of a backup account
$I(f)$	Address of the individual who calls the function f
X	Amount of cryptoasset
T	Value of a deadline
C	Value of the current time
R	Value of the receipt

[0035]

[0036] 다시 말하면, 본 발명의 일 실시예에 따른 가상 자산 회생 시스템(블록체인 자산 회생 시스템이나 시스템 등으로 명명될 수도 있음)은 송신자의 단말과 수신자의 단말 이외에 스마트 컨트랙트를 생성하는 TTP(스마트 컨트랙트 생성 서버로 명명될 수도 있음)를 더 포함할 수 있다. 일 예에 의하면, 스마트 컨트랙트 생성 서버는 스마트 컨트랙트를 생성하고자 하는 단말(송신자의 단말 및/또는 수신자의 단말일 수 있음)로부터 스마트 컨트랙트의 생성에 필요한 정보를 수신하고 수신된 정보에 기초하여 스마트 컨트랙트를 생성할 수 있다. 스마트 컨트랙트는 블록체인 기술을 이용한 중요 기능으로 일정 조건을 만족시키면 거래가 자동으로 실행되도록 하는 프로그램을 의미할 수 있다. 스마트 컨트랙트는 스마트 컨트랙트 코드를 포함한다. 스마트 컨트랙트 생성 서버는 스마트 컨트랙트를 컴파일하여 바이트 코드(즉, 스마트 컨트랙트 실행 프로그램)을 생성하고, 생성된 바이트 코드를 블록

에 삽입하여 블록체인(또는 블록체인 네트워크)에 업로드한다. 블록체인에 올려진 블록의 유효성은 블록체인 내부에서 분산 합의 절차를 통하여 검증될 수 있다. 여기서, 스마트 컨트랙트의 생성에 필요한 정보는 송신자의 주소, 수신자의 주소, 전송할 가상 자산의 양, 환수 주소, 데드라인, 및 현재 시간 중 적어도 하나를 포함할 수 있다.

[0037] 다만, 스마트 컨트랙트는 송신자의 단말 및/또는 수신자의 단말에 의해 생성될 수도 있고, 이 경우 스마트 컨트랙트 생성 서버는 생략될 수 있다. 즉, 스마트 컨트랙트는 소정의 단말의 사용자로부터 스마트 컨트랙트의 생성에 필요한 정보를 수신하고, 스마트 컨트랙트 생성 서버와 동일한 동작을 수행함으로써 스마트 컨트랙트를 생성할 수 있다.

[0038] 2. 가상 자산의 전송(Sending the Cryptoasset)

[0039] 가상 자산을 전송하기 위하여, 송신자는 *Send* 함수를 콜(call)함으로써 가상 자산 X를 KSC의 주소로 전송하는 트랜잭션을 생성하여야 한다. 송신자는 B, S, 및 T의 값을 설정하여야 한다. 콜을 수신함에 따라, 함수는 수신자의 주소, 백업 계좌 주소, 데드라인, 및 가상 자산의 양(amount)을 설정한다. 또한, 함수는 트랜잭션에 대응하는 *false(거짓)*의 불리언 값(Boolean value)을 설정할 수 있다. 이러한 불리언 값은 가상 자산이 이미 요구되었는지 또는 이동되었는지 여부를 판단하기 위해 이용될 수 있다.

[0040] 즉, 송신자의 단말은 미리 정해진 정보를 포함하는 스마트 컨트랙트에 대한 블록을 생성하고, 생성된 블록을 블록체인에 업로드함으로써 스마트 컨트랙트를 생성할 수 있다.

[0041] 함수 콜이 완료된 후(즉, 함수 콜에 대한 트랜잭션이 블럭에 기재된 경우), 송신자는 A, B, S, C, T, 및 X에 기초한 해쉬값(hash value)인 리시트(receipt) R을 수신한다. 이러한 리시트는 특정한 트랜잭션 데이터를 식별하기 위해 이용될 수 있다. 여기서, C는 보통 블록체인에 기초하여 계산될 수 있는 현재 시간 값(value of the current time)이다(Solidity 내의 *block.timestamp*).

[0042] 3. 통신(Communication)

[0043] 가상 자산 X를 요구하거나 이동시키기를 원하는 개인(주소 *I(f)*를 가짐)은 R을 이용하여 KSC의 *Claim* 또는 *Move* 함수를 콜할 필요가 있다. 여기서, *I(f)*는 함수 *f*를 콜하기를 원하는 개인의 주소이다. R을 찾기 위해, 개인은 (1) 임의의 통신 채널을 통해 송신자에게 R에 대해 문의하거나 (2) KSC 계좌를 살펴볼 수 있다. 계좌의 주소(K)는 잘 알려진 주소에 해당할 수 있다.

[0044] 즉, 수신자의 단말은 송신자의 단말 및/또는 KSC 계좌로부터 스마트 컨트랙트에 대한 리시트 R을 수신할 수 있다.

[0045] 4. 가상 자산의 요청(Claiming the Cryptoasset)

[0046] B(B는 주소 *I(Claim)*과 동일한 값을 가짐)의 소유자만이 *Claim* 함수를 실행할 수 있고, 리시트에 대응하는 불리언 값은 *false(거짓)*이어야 한다. 그렇지 않으면, 컨트랙트는 *REVERT*를 실행한다. 모든 조건이 충족되면, 컨트랙트는 불리언 값을 *true*로 변경하고 X를 B로 전송한다. *I(Claim)*은 보통 블록체인에 기초하여 계산가능한 값(Solidity 에서의 *msg.sender*)이기 때문에, 이러한 파라미터의 사용은 구현이 용이하다.

[0047] 5. 가상 자산의 이동(Moving the Cryptoasset)

[0048] 데드라인이 경과한 경우에만(C가 T 보다 클 때), *Move* 함수를 실행할 수 있다. 또한, 리시트에 대응하는 불리언 값은 *false*이어야 한다. 그렇지 않으면, 컨트랙트는 *REVERT*를 실행한다. 모든 조건이 충족되면, 컨트랙트는 불리언 값을 *true*로 변경하고 X를 S로 전송한다.

[0049] 도 4는 본 발명의 일 실시예에 따른 가상 자산 회생 방법을 설명하기 위한 흐름도이다. 상기 방법을 설명함에 있어, 앞선 기재와 중복되는 내용에 관하여는 그 구체적인 설명을 생략하기로 한다.

[0050] 도 4를 참조하면, 스마트 컨트랙트가 생성되어 블록체인에 업로드될 수 있다(S100). 스마트 컨트랙트는 송신자의 단말이나 스마트 컨트랙트 생성 서버에 의해 생성될 수 있다. 생성된 스마트 컨트랙트를 포함하는 블록은 블록체인에 업로드된다. 다시 말하면, 생성된 스마트 컨트랙트를 포함하는 블록은 블록체인 네트워크를 구성하는 적어도 하나의 노드로 전송됨으로서 블록체인에 업로드될 수 있다.

[0051] 스마트 컨트랙트에 의해, 가상 자산은 스마트 컨트랙트에 대응하는 주소 K로 이동할 수 있다(S200). 여기서 스마트 컨트랙트에 대응하는 주소 K는 미리 정해진 주소로써, 가상 자산이 의도치 않게 소멸되는 것을 방지하기

위해 일시적으로 가상 자산을 보유하는 계좌의 주소로 이해될 수 있다.

[0052] 다음으로, S300 단계 또는 S400 단계가 실행될 수 있다.

[0053] S300 단계는 가상 자산이 주소 K에서 주소 B로 이동하는 단계를 의미한다. 주소 B는 수신자의 계좌 주소를 의미한다. 즉, 스마트 컨트랙트가 생성된 시점으로부터 데드라인이 경과되지 전까지 수신자는 자신의 비밀키를 증명함으로써 가상 자산이 자신의 계좌로 전송되도록 할 수 있다. 실시예에 따라, 데드라인이 경과하였더라도, 송신자가 가상 자산을 환수하지 않은 경우 수신자는 가상 자산이 자신의 계좌로 전송되도록 할 수 있다. 물론, 이 경우에도 수신자는 자신이 비밀키를 알고 있음을 증명하여야 한다.

[0054] 일 예로써, 수신자는 수신자의 단말에 설치된(또는 구현된) 디지털 자산 지갑 앱(예컨대, Metamask) 등을 통해 KSC의 "Claim" 함수를 실행시킬 수 있다. 다시 말해, 수신자의 단말은 블록체인 네트워크를 구성 중인 적어도 하나의 노드에게 "Claim" 함수에 대한 함수 콜(function call) 데이터를 담은 트랜잭션 발생을 요청할 수 있다. 이때, 수신자가 자산을 수신하기 위한 조건으로는 1) 송신 단계에서 정의된 "정당한 수신자"이어야 할 것과 2) 수신자가 해당 자산을 이미 획득했거나 송신자가 자산 회생을 하지 않았을 것을 만족하여야 한다. 위 조건을 만족하는지 여부는 스마트 컨트랙트의 Claim 함수의 If 조건문을 통해 자동으로 확인(또는 검증)될 수 있다.

[0055] S400 단계는 가상 자산이 주소 K에서 주소 S로 이동하는 단계를 의미한다. 주소 S는 송신자와 수신자의 합의에 의해 결정된 가상 자산의 환수 주소로써, 실시예에 따라 송신자의 계좌의 주소와 동일할 수도 있다. 즉, 스마트 컨트랙트가 생성된 시점으로부터 데드라인이 경과된 후에, 송신자는 가상 자산이 환수 주소로 이동하도록 할 수 있다. 물론, 실시예에 따라 데드라인이 경과한 경우라도, 가상 자산이 수신자의 계좌로 송신된 경우, 송신자는 가상 자산을 환수할 수는 없다.

[0056] 일 예로써, 송신자 또는 제3자는 자신의 단말에 설치된 디지털 자산 지갑 등을 통해 KSC의 "Move" 함수를 실행시킬 수 있다. 다시 말해, 송신자 또는 제3자의 단말은 블록체인 네트워크를 구성 중인 적어도 하나의 노드에게 "Move" 함수에 대한 함수 콜 데이터를 담은 트랜잭션 발생을 요청할 수 있다. 이때, 자산을 환수하기 위한 조건으로는 1) 현재의 시간이 "데드라인"을 경과하였을 것과 2) 수신자가 해당 자산을 이미 획득하였거나 송신자 또는 제3자가 자산 회생을 하지 않았을 것을 만족하여야 한다. 위 조건을 만족하는지 여부는 스마트 컨트랙트의 Move 함수의 If 조건문을 통해 자동으로 확인(또는 검증)될 수 있다.

[0057] 이상에서 설명된 장치는 하드웨어 구성 요소, 소프트웨어 구성 요소, 및/또는 하드웨어 구성 요소 및 소프트웨어 구성 요소의 집합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성 요소는, 예를 들어, 프로세서, 콘트롤러, ALU(Arithmetic Logic Unit), 디지털 신호 프로세서(Digital Signal Processor), 마이크로컴퓨터, FPA(Field Programmable array), PLU(Programmable Logic Unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(Operation System, OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술 분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(Processing Element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(Parallel Processor)와 같은, 다른 처리 구성(Processing Configuration)도 가능하다.

[0058] 소프트웨어는 컴퓨터 프로그램(Computer Program), 코드(Code), 명령(Instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(Collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성 요소(Component), 물리적 장치, 가상 장치(Virtual Equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(Signal Wave)에 영구적으로, 또는 일시적으로 구체화(Embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

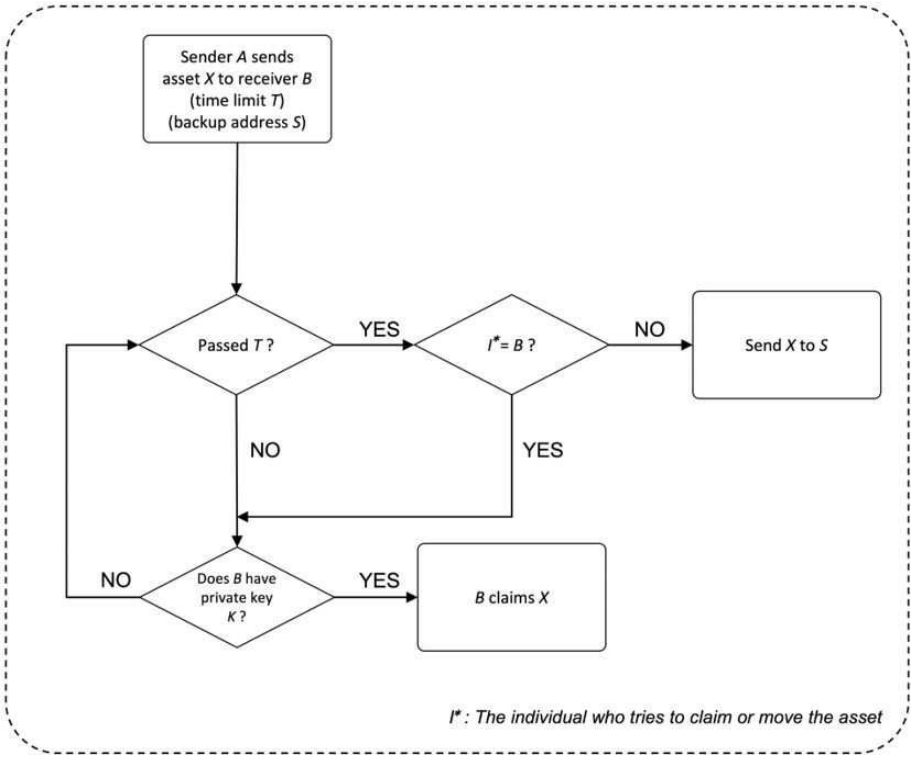
[0059] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계

되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM, DVD와 같은 광기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-optical Media), 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0060] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성 요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

도면

도면1



도면2

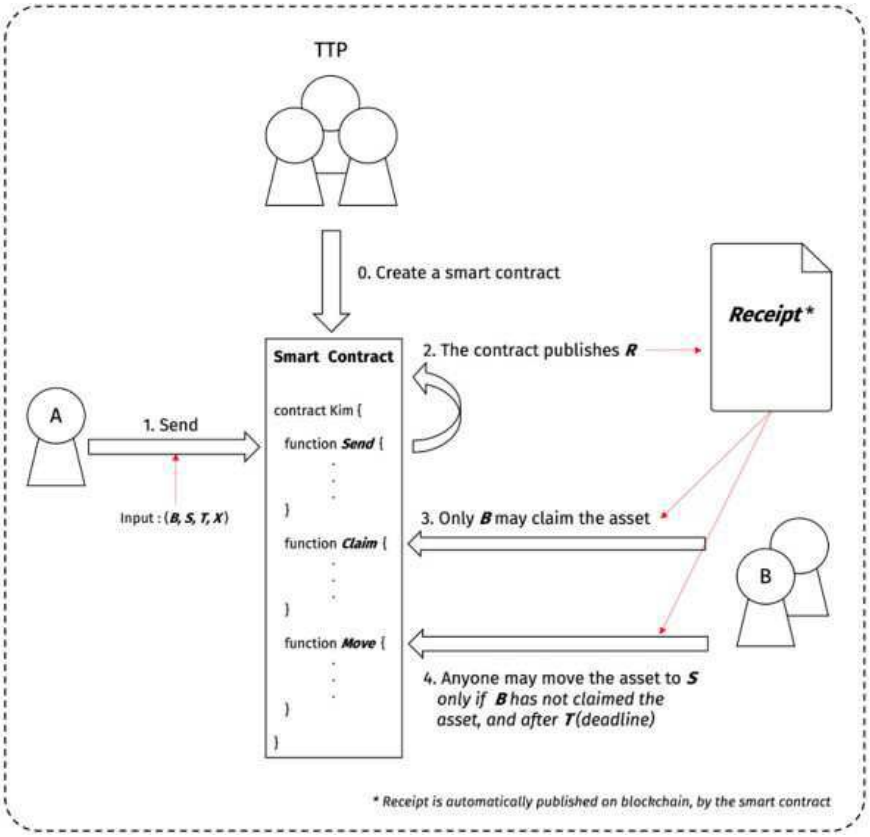
```
Global Variables: B(R), S(R), T(R), X(R), and Bool(R) map a receipt to the receiver's
                  address, backup address, deadline, amount of cryptoasset, and Bool-
                  ean value, respectively. R is a value of the receipt.

Function Send (b, s, t, x) :
    R ← hash( A || b || s || C || t || x )   // The address of the sender's account A and the
                                             current time value C are blockchain-native calcu-
                                             lable values.
    B(R) ← b
    S(R) ← s
    T(R) ← t
    X(R) ← X(R) + x
    Bool(R) ← false
return R

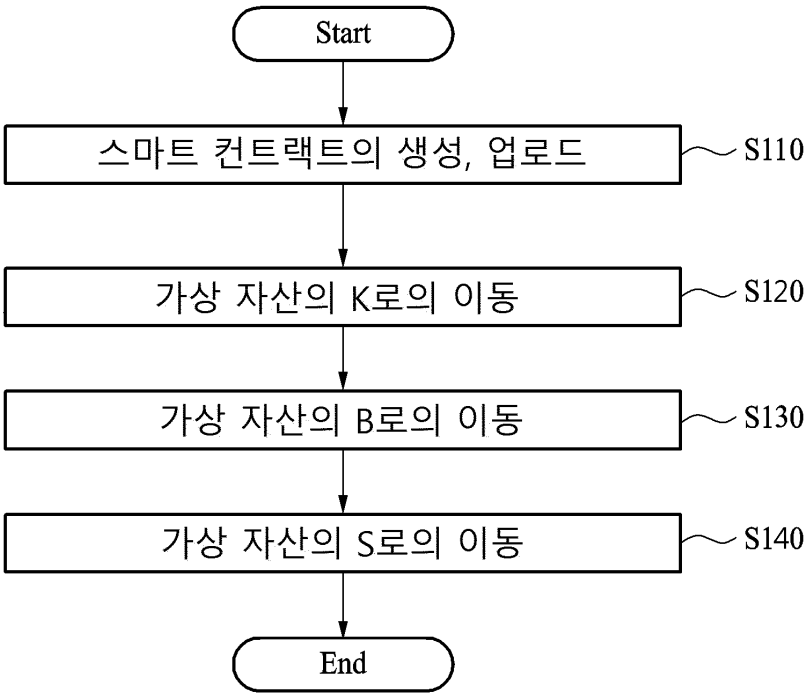
Function Claim (R) :
    if I (Claim) ≠ B(R) then
        REVERT
    else
        if Bool(R) ≠ false then
            REVERT
        else
            Bool(R) ← true
            Send X(R) to B(R)
        end
    end
return

Function Move (R) :
    if C ≤ T(R) then
        REVERT
    else
        if Bool(R) ≠ false then
            REVERT
        else
            Bool(R) ← true
            Send X(R) to S(R)
        end
    end
return
```

도면3


TTP
0. Create a smart contract
Receipt*
Smart Contract
2. The contract publishes R
contract Kim {
function Send {
}
function Claim {
}
function Move {
}
}
A
1. Send
Input : (B, S, T, X)
3. Only B may claim the asset
B
4. Anyone may move the asset to S only if B has not claimed the asset, and after T(deadline)
* Receipt is automatically published on blockchain, by the smart contract

도면4


Start
스마트 컨트랙트의 생성, 업로드
S110
가상 자산의 K로의 이동
S120
가상 자산의 B로의 이동
S130
가상 자산의 S로의 이동
S140
End