(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0107109
(43) 공개일자 2019년09월18일

(51) 국제특허분류(Int. Cl.)
G06Q 20/06 (2012.01) *G06Q 20/32* (2012.01)
G06Q 20/36 (2012.01)
(52) CPC특허분류
G06Q 20/065 (2013.01)
G06Q 20/322 (2013.01)
(21) 출원번호 10-2019-7024104
(22) 출원일자(국제) 2018년01월29일
심사청구일자 없음
(85) 번역문제출일자 2019년08월16일
(86) 국제출원번호 PCT/IB2018/050517
(87) 국제공개번호 WO 2018/142260
국제공개일자 2018년08월09일
(30) 우선권주장
1701605.6 2017년01월31일 영국(GB)
1701608.0 2017년01월31일 영국(GB)

(71) 출원인
엔체인 홀딩스 리미티드
안티구아바부다 세인트존스, 처치 스트리트 44, 피츠제럴드 하우스
(72) 발명자
세웰, 마틴
영국, 씨에프10 2에이치에이치 카디프, 처칠 웨이, 처칠 하우스 7층, 어커트-디키스 앤 로드 엘엘피
비세볼로지스키, 베라
영국, 씨에프10 2에이치에이치 카디프, 처칠 웨이, 처칠 하우스 7층, 어커트-디키스 앤 로드 엘엘피
(74) 대리인
특허법인다나

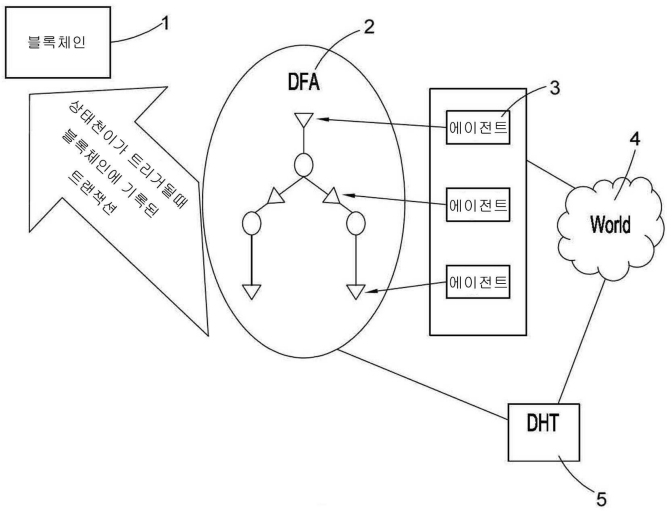
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **블록체인 상에 저장된 사용자 관련 데이터를 생성하고 추출하기 위한 컴퓨터 구현 시스템 및 방법**

(57) 요 약

트랜잭션들에 관련된 블록체인의 사용자들에 대한, 평판 정보와 같은 사용자 관련 데이터를 제공하기 위한 컴퓨터 구현 시스템 및 방법이 상세히 설명된다. 이 방법은 특히 계약의 컨텍스트(context)에서 트랜잭션들의 이행을 평가한 다음, 평판 정보를 통해 블록체인에 기록을 제공하는 접근법을 포함한다. 결과적으로, 늦은 시간에 이 평판 정보가 검색될 수 있다. 다른 트랜잭션들에 대한 유사한 평판 정보가 사용자에 대한 마스터 공개 키의 해시의 사용에 기초하여 검색될 수 있으며 동일한 사용자에게 연결될 수 있다. 집합된 평판 정보는 검색된 평판 정보의 조각들로부터 컴퓨팅될 수 있다.

대 표 도 - 도5



(52) CPC특허분류
G06Q 20/3678 (2013.01)

명 세 서

청구범위

청구항 1

집합된 사용자 관련 데이터(aggregated user related data)를 컴퓨팅하는 방법에 있어서,

a. 사용자 관련 데이터 트랜잭션을 구성하는 단계, 상기 사용자 관련 데이터 트랜잭션은 사용자와 관련된 이전 트랜잭션으로부터의 사용자 관련 데이터의 표현(expression)을 포함한다;

b. 상기 사용자 관련 데이터 트랜잭션을 상기 블록체인으로 브로드캐스팅하는 단계;

c. 복수의 이전 트랜잭션들 및/또는 복수의 사용자들에 대해 단계 a) 및 b)를 반복하는 단계;

d. 선택된 사용자를 얻기 위하여, 집합된 사용자 관련 데이터가 요구되는 사용자를 선택하는 단계;

e. 선택된 사용자와 관련된 필터를 생성하는 단계;

f. 상기 필터가 적용되는 사용자 관련 데이터 트랜잭션에 대한 블록체인을 검색하는 단계;

g. 상기 필터가 적용되는 상기 사용자 관련 데이터 트랜잭션들로부터 상기 선택된 사용자에 대한 집합된 사용자 관련 데이터를 컴퓨팅하는 단계를 포함하는 방법.

청구항 2

제1항에 있어서,

a. 적어도 하나의 사용자와 적어도 하나의 다른 사용자 사이의 트랜잭션을 정의하는 단계;

b. 상기 트랜잭션을 실행하는 단계;

c. 적어도 하나의 사용자들 또는 적어도 하나의 다른 사용자들에 대해 상기 트랜잭션으로부터 사용자 관련 데이터를 제공함으로써, 사용자 관련 데이터 표현을 제공하는 단계; 중 하나 이상을 더 제공하며,

사용자 관련 데이터 트랜잭션을 구성하는데 사용하기 위한 사용자 관련 데이터 표현을 제공하며, 상기 사용자 관련 데이터 트랜잭션은 사용자 관련 데이터 표현을 포함하는 방법.

청구항 3

집합된 사용자 관련 데이터를 컴퓨팅하는 방법에 있어서,

a. 선택된 사용자를 얻기 위하여, 집합된 사용자 관련 데이터가 요구되는 사용자를 선택하는 단계;

b. 선택된 사용자와 관련된 필터를 생성하는 단계;

c. 상기 필터가 적용되는 사용자 관련 데이터 트랜잭션에 대한 블록체인을 검색하는 단계;

d. 상기 필터가 적용되는 상기 사용자 관련 데이터 트랜잭션들로부터 상기 선택된 사용자에 대한 집합된 사용자 관련 데이터를 컴퓨팅하는 단계를 포함하는 방법.

청구항 4

제1항 내지 제3항 중 어느 한 항에 있어서,

컴퓨팅된 집합된 사용자 관련 데이터의 평가를 더 제공하며, 상기 평가는 결정(decision) 및/또는 동작(action) 및/또는 수정(modification)을 제공하는 방법.

청구항 5

제4항에 있어서,

결정 및/또는 액션 및/또는 수정은

a. 블록체인 트랜잭션들과 같은 하나 이상의 추가 트랜잭션에 대한 하나 이상의 입력으로 변경;

b. 블록체인 트랜잭션들과 같은 하나 이상의 추가 트랜잭션으로부터의 하나 이상의 출력으로 변경;

c. 하나 이상의 추가 트랜잭션을 구현하는 DFA와 같은 DFA로 변경

중 하나 이상을 발생시키는 방법.

청구항 6

제4항 또는 제5항에 있어서,

결정 및/또는 액션 및/또는 수정은

a. 서비스 및/또는 제품의 설계 및/또는 생산 및/또는 저장 및/또는 분배 및/또는 소비를 수정 및/또는 최적화하기 위한 피드백;

b. 서비스 및/또는 제품의 설계 및/또는 생산 및/또는 저장 및/또는 분배 및/또는 소비를 위한 프로세스와 같은 프로세스를 수정 및/또는 최적화하기 위한 피드백

중 하나 이상을 제공하는 방법.

청구항 7

제4항 내지 제6항 중 어느 한 항에 있어서,

결정 및/또는 액션 및/또는 수정은 스마트 계약과 같은 계약을 수정 및/또는 최적화하기 위한 피드백을 제공하는 방법.

청구항 8

제1항 내지 제7항 중 어느 한 항에 있어서,

상기 사용자는 트랜잭션을 제공하는 사용자들로부터 선택되는 방법.

청구항 9

제1항 내지 제8항 중 어느 한 항에 있어서,

상기 필터는 상기 선택된 사용자의 공개 키로부터 발생하는 주소 해시로부터 구성되는 방법.

청구항 10

제1항 내지 제9항 중 어느 한 항에 있어서,

상기 필터는 상기 선택된 사용자의 공개 키로부터 발생하는 서명 스크립트로부터 구성되는 방법.

청구항 11

제1항 내지 제10항 중 어느 한 항에 있어서,

상기 필터는 상기 선택된 사용자의 마스터 공개 키의 해시인 방법.

청구항 12

제1항 내지 제11항 중 어느 한 항에 있어서,

상기 필터는 선택된 사용자에 대한 마스터 공개 키 및 그들의 모든 후손(decendant) 공개 키에 관한 메타데이터를 포함하는 모든 평판(reputation) 트랜잭션들을 수집하는 방법.

청구항 13

제1항 내지 제12항 중 어느 한 항에 있어서,

선택은 사용자의 디지털 지갑을 이용하여 만들어지는 방법.

청구항 14

제16항 또는 제16항을 인용하는 항에 있어서,

상기 방법은 복수의 사용자를 선택하는 단계 및 복수의 사용자들 각각에 대한 집합된 사용자 관련 데이터를 컴퓨팅하는 단계를 포함하는 방법.

청구항 15

제1항 또는 제2항의 방법을 구현하도록 설정된 시스템.

청구항 16

제15항에 있어서,

상기 시스템은:

a. 사용자 디지털 지갑;

b. 블록체인을 통하여 DFA를 구현하도록 설정된 적어도 하나의 컴퓨팅 에이전트;

c. 블록체인 플랫폼을 포함하는 시스템.

청구항 17

제3항 내지 제14항 중 어느 한 항에 따른 방법을 구현하도록 설정된 시스템.

청구항 18

제17항에 있어서,

상기 시스템은:

c) 블록체인을 통하여 DFA를 구현하도록 설정된 적어도 하나의 컴퓨팅 에이전트;

d) 블록체인 플랫폼을 포함하는 시스템

청구항 19

사용자 관련 데이터의 기록을 만드는 방법에 있어서,

a. 적어도 하나의 사용자 및 적어도 하나의 다른 사용자 간 트랜잭션을 정의하는 단계;

b. 상기 트랜잭션을 구현하는 단계;

c. 적어도 하나의 사용자 또는 적어도 하나의 다른 사용자에 의해 상기 트랜잭션으로부터 사용자 관련 데이터를 제공함으로써, 사용자 관련 데이터 표현을 제공하는 단계;

d. 상기 사용자 관련 데이터 표현을 포함하는 사용자 관련 데이터 트랜잭션을 구성하는 단계;

e. 사용자 관련 데이터 트랜잭션을 상기 블록체인으로 브로드캐스팅하는 단계를 포함하는 방법.

청구항 20

제19항의 방법을 구현하도록 설정된 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 일반적으로 컴퓨터 구현 시스템 및 방법에 관한 것으로, 보다 상세하게는 트랜잭션들과 관련된 사용자에 대한 데이터를 제공하기 위한 컴퓨터 구현 시스템 및 방법에 관한 것이다. 본 발명은 블록체인(blockchain) 상에서 트랜잭션들의 측면들과 관련하여 스코어, 정확도 또는 품질 측정과 같은 데이터를 제공하는 용도로 특히 적합하지만, 이에 한정되는 것은 아니다. 예를 들어 트랜잭션들과 관련된 사용자들에 대한 평판 정보를 제공하며, 특히 블록체인 상에서 구현되는 스마트 계약들의 사용자에 대한 평판 정보를 제공하는

것이나, 이로 제한되는 것은 아니다.

배 경 기 술

[0002] 본 문서에서 모든 형태의 전자, 컴퓨터 기반의, 분산 원장을 포함하는 용어로 '블록체인'을 사용한다. 이는 허가된 및 허가되지 않은 원장, 공유 원장 및 그들의 변형을 포함하지만, 블록체인 및 트랜잭션 체인 기술에 한정되지 않는다. 블록체인 기술에서 가장 널리 알려진 애플리케이션은 비트코인 원장이지만, 다른 블록체인 구현도 제안되고 개발되었다. 본 명세서에서 편의 및 설명을 위해 비트코인이 언급될 수 있지만, 본 발명은 비트코인 블록체인으로 사용하는 것에 제한되지 않으며, 다른 블록체인 구현 및 프로토콜도 본 발명의 범위 내에 있음을 알아야 한다.

[0003] 블록체인(blockchain)은 컨센서스 기반의 전자 원장으로, 트랜잭션들로 차례대로 구성된 블록들로 이루어진 컴퓨터 기반의 분산형(decentralised) 분산(distributed) 시스템으로 구현된다. 각 트랜잭션은 블록체인 시스템의 참여자들 간 디지털 자산의 제어의 트랜스퍼를 부호화하는 데이터 구조이며, 적어도 하나의 입력 및 저경도 하나의 출력을 포함한다. 블록들이 시작 이래로 블록체인에 기록된 모든 트랜잭션들의 영구적이고 변경 불가능한 기록을 생성하기 위하여 서로 연결되도록, 각 블록은 이전 블록의 해시를 포함한다. 트랜잭션들은 그들의 입력들 및 출력들로 임베드된 스크립트들로 알려진 작은 프로그램들을 포함하며, 이는 트랜잭션들의 출력이 어떻게 그리고 누구에 의하여 액세스될 수 있는지를 나타낸다. 비트코인 플랫폼에서, 이들 스크립트들은 스택 기반 스크립팅 언어를 사용하여 작성된다.

[0004] 트랜잭션이 블록체인에 기록되도록 하기 위하여, "인증(validated)"되어야만 한다. 네트워크 노드(채굴자, miner)는 유효하지 않은(invalid) 트랜잭션들을 네트워크에서 거부하여, 각 트랜잭션이 유효한(valid) 것을 보장하기 위한 작업을 수행한다. 노드에 설치된 소프트웨어 클라이언트들은 잠금(locking) 및 잠금 해제(unlocking) 스크립트를 실행하는 것에 의하여 사용되지 않은(unspent) 트랜잭션(UTXO)에 대한 인증 작업(validation work)을 수행한다. 잠금 및 잠금 해제 스크립트의 실행이 참(TRUE)인 것으로 평가되면, 트랜잭션이 유효하며 트랜잭션이 블록체인에 기록된다. 그러므로, 트랜잭션이 블록체인에 기록되도록 하기 위하여, i) 트랜잭션을 수신하는 첫 번째 노드에서 인증되어야 하며, 트랜잭션이 유효한 경우 상기 노드는 이를 네트워크 내 다른 노드로 전달하고; ii) 채굴자에 의하여 세워진 새로운 블록에 추가되며; iii) 과거 트랜잭션의 공개 원장에 채굴, 즉 추가된다.

[0005] 블록체인 기술이 암호화폐 구현의 용도로 가장 널리 알려져 있음에도 불구하고, 디지털 기업들은 비트코인이 기반되는 암호화 보안 시스템 및 새로운 시스템들을 구현하기 위해 블록체인에 저장될 수 있는 데이터의 사용을 모색하기 시작했다. 블록체인이 암호화폐의 영역에 국한되지 않는 자동화된 업무 및 프로세스에 사용될 수 있다면 매우 유용할 것이다. 이러한 솔루션은 그들의 애플리케이션에서 더욱 다양하게 사용되는 동안 (예를 들어, 이벤트의 영구적인, 위변조방지(temper proof) 기록, 분산 프로세싱 등의) 블록체인의 장점을 이용할 수 있다.

[0006] 현재 연구의 한 분야는 "스마트 계약"의 구현을 위해 블록체인을 사용하는 것이다. 이들은 기계가 읽을 수 있는 계약 또는 계약조건의 실행을 자동화하도록 설계된 컴퓨터 프로그램이다. 자연어로 작성된 전통적인 계약과는 달리, 스마트 계약은 결과를 산출하기 위해 입력을 처리할 수 있는 규칙을 포함하는 기계가 실행 가능한 프로그램으로, 그 결과에 따라 동작(action)이 수행될 수 있다.

[0007] 블록체인과 관련된 또 다른 영역은 블록체인을 통해 실제 엔티티를 표현하고 전달하기 위하여 '토큰'(또는 '컬러 동전')을 사용하는 것이다. 잠재적으로 민감한 또는 비밀 아이템은 식별 가능한 의미 또는 값이 없는 토큰으로 나타내어질 수 있다. 따라서 토큰은 실제 아이템이 블록체인에서 참조될 수 있도록 하는 식별자의 역할을 한다.

[0008] 네트워크 내 평판 데이터 또는 신용 정보와 같은 사용자 관련 데이터를 관리하기 위한 다양한 종래 기술 방법론이 알려져 있다. 이러한 종래 기술 방법론의 예가 아래에 간략하게 설명되어 있다.

[0009] Chris Pacia et al. "OpenBazaar - Ratings, reviews and reputation"의 프리젠테이션은 블록체인 기반 레이팅 시스템을 개시한다. 슬라이드 55에서, 아이템이 수신되면, 바이어(Buyer)는 벤더(Vendor)에게 자금을 방출하기 직전에 레이팅을 생성한다. 레이팅 데이터는 Ricardian 계약에 첨부되어 있다. 레이팅 데이터는 다음 파라미터를 기반으로 바이어에 의해 제공된 스코어를 포함한다: 피드백; 품질; 상세설명; 딜리버리 시간; 고객 서비스; 및 리뷰. 슬라이드 63에서, OP_RETURN은 벤더의 전역고유식별자(GUID, Globally Unique Identifier)를 가지며, 이는 레이팅을 스캔할 때 블록체인으로부터 관련된 복수의 서명 트랜잭션들을 필터링하는데 사용된다. 또한, 이러한 태그가 붙은 다중 서명 트랜잭션 중 스크립트서명(scriptsig) 내 벤더의 GUID 서명이 유효한 것으

로 간주되는 경우에만 "벤더가 트랜잭션에 관련되었다는 위조없는 증거"임을 나타낸다.

[0010] OpenBazaar에 개시된 시스템에서, 레이팅 데이터는 사용자(Buyer)에 의해 제공되는 점에 유의해야 한다. 이 등급 정보는 원칙적으로 (예를 들어, 열악한 등급 정보를 넣는 경쟁자에 의하여) 남용될 수 있다. OpenBazaar에서 레이팅 시스템의 남용을 방지하기 위해, 시스템은 벤더에 의해 서명된 트랜잭션들만 사용하므로, 실제 트랜잭션들을 나타낸다. 그러나, 이는 경쟁자가 벤더에 의해 서명된 트랜잭션에서 합법적으로 제품이나 서비스를 구매하지 못하도록 하지만 제3자가 벤더로부터 제품이나 서비스를 구매하지 못하도록 하기 위해 열악한 등급 정보를 제공하지는 않는다.

[0011] WO 2015/085393은 디지털 통화의 트랜잭션 히스토리를 평가하는 등급 시스템을 개시한다. 등급 시스템은 디지털 통화의 트랜잭션 정보를 저장하는 저장 시스템; 디지털 통화와 연관된 적어도 하나의 계좌의 식별자 및 상기 적어도 하나의 계좌의 트랜잭션 히스토리를 평가하기 위한 요청을 수신하기 위한 인터페이스; 및 상기 저장 시스템 및 상기 인터페이스와 통신하는 프로세서를 포함한다. 프로세서는 저장 시스템에 저장된 트랜잭션 정보로부터 적어도 하나의 계좌의 트랜잭션을 식별하고 식별된 트랜잭션의 목적지를 평가하여 적어도 하나의 계좌에 대한 등급을 생성한다. 등급 시스템이 식별된 트랜잭션의 양 및 연령을 평가할 수 있으며, 등급 시스템이, 예를 들어 피어-투-피어 디지털 통화에 유용할 수 있음이 더 개시되어 있다. 저장 시스템이 블록체인을 포함하는 것으로 나타나 있지는 않으며, 단지 사용자 별 트랜잭션들이 식별된 트랜잭션들의 양, 날짜 및 목적지를 포함한다.

[0012] US2006149745는 전자 상거래 시스템의 분산 피드백 시스템 내에서 피드백 데이터를 제공하는 시스템 및 방법을 개시한다. 전자 상거래 트랜잭션을 설명하는 피드백 데이터는 상품 및 서비스의 바이어와 해당 상품 및 서비스의 셀러(seller)에 의해 생성된다. 피드백 데이터는 분산 장치의 피어-투-피어(P2P) 네트워크로 구성된 피드백 서버 집합 내에 저장되고 관리된다. 피드백 데이터는 각각의 P2P 네트워크 노드와 연관된 데이터베이스 저장소 상에 저장된 피드백 데이터의 그룹핑으로 구성된다. 바이어와 셀러는 이러한 분산 데이터 소스들로부터 피드백 데이터를 검색하여 상품 및 서비스에 대한 새로운 트랜잭션들로 제안하는 당사자들과 연관된 평판 데이터를 얻을 수 있다. 사용자 관련 데이터가 전송, 저장, 검색 및 추출되는 블록 체인 시스템은 개시되어 있지 않다.

[0013] US2015302400은 분산된 암호화폐 평판 시스템 및 암호화폐 공공 원장을 모니터링하는 것을 포함하는 방법을 개시한다. 현재의 암호화폐 트랜잭션은 암호화폐 공공 원장에서 검출되며, 이에 따라 평판 마커가 현재의 암호화폐 트랜잭션에 포함되는 지불자(payer) 및 수취자(payee) 모두에게 할당될 수 있다. 그러면, 평판 마커들 중 적어도 일부는 지불자로부터 수취자에게, 그리고 수취자로부터 지불자에게 이전되는 것으로 결정된다. 수취자 또는 지불자에 대한 평판 정보를 위한 요청이 수신될 때, 지불자로부터 수취자에게, 또는 수취자로부터 지불자에게 평판 마크들의 적어도 일부를 이전하는 것과 관련되는 정보가 제공될 수 있다.

[0014] CN106230808은 많은 상이한 기관들로부터의 개인 신용 정보를 블록체인 상에 저장하는 것을 개시한다.

발명의 내용

해결하려는 과제

[0015] 시스템 사용자에 대한 평판 정보와 같은 데이터를 제공하기 위한 기존의 시스템 및 방법에 관한 문제는 시스템 및 데이터가 공격 및 조작에 취약하거나 분산 시스템에서 구현하기에 부적합하다는 것이다.

[0016] 따라서, 공격 및 조작에 대해 보다 강인한 시스템 및/또는 방법을 목적으로 하는 해결책을 제공하고자 한다.

[0017] 따라서, 분산 시스템에서 구현하기에 적합한 시스템 및/또는 방법을 목적으로 하는 해결책을 제공하고자 한다.

[0018] 따라서, 블록체인(blockchain) 또는 비트코인 블록체인(bitcoin blockchain)을 구현하기에 적합한 시스템 및/또는 방법을 목적으로 하는 해결책을 제공하고자 한다.

[0019] 사용자 관련 정보를 생성하는 관점에서 보다 객관적인 해결책을 제공하고자 한다.

[0020] 또 다른 목적은 블록체인에서 사용자 관련 데이터를 생성, 저장 및 검색하는 효과적이고 효율적인 방법을 제공하는 것이다.

과제의 해결 수단

[0021] 이를 개선한 시스템이 여기에서 개시된다. 본 발명은 첨부된 청구항 및/또는 본 명세서 및/또는 이 문서 내에서

설명된 특징, 옵션 및 가능성들로 정의된다.

[0022] 본 발명의 제1 실시예에 따른 집합된 사용자 관련 데이터(aggregated user related data)를 컴퓨팅하는 방법은

[0023] a. 사용자 관련 데이터 트랜잭션을 구성하는 단계, 상기 사용자 관련 데이터 트랜잭션은 사용자와 관련된 이전 트랜잭션으로부터의 사용자 관련 데이터의 표현(expression)을 포함한다;

[0024] b. 상기 사용자 관련 데이터 트랜잭션을 상기 블록체인으로 브로드캐스팅하는 단계;

[0025] c. 복수의 이전 트랜잭션들 및/또는 복수의 사용자들에 대해 단계 a) 및 b)를 반복하는 단계;

[0026] d. 선택된 사용자를 얻기 위하여, 집합된 사용자 관련 데이터가 요구되는 사용자를 선택하는 단계;

[0027] e. 선택된 사용자와 관련된 필터를 생성하는 단계;

[0028] f. 상기 필터가 적용되는 사용자 관련 데이터 트랜잭션에 대한 블록체인을 검색하는 단계;

[0029] g. 상기 필터가 적용되는 상기 사용자 관련 데이터 트랜잭션들로부터 상기 선택된 사용자에 대한 집합된 사용자 관련 데이터를 컴퓨팅하는 단계를 포함한다.

[0030] 이 방법은 집합된 사용자 관련 데이터가 집합된 평판 정보임을 제공할 수 있다. 사용자 관련 데이터 트랜잭션은 평판 트랜잭션일 수 있다. 사용자 관련 데이터 트랜잭션은 사용자와 관련된 이전 트랜잭션의 이행의 표현을 포함할 수 있다. 이전 트랜잭션으로부터의 사용자 관련 데이터는 사용자에 관한 이전 트랜잭션의 이행의 표현일 수 있다.

[0031] 이 방법은 컴퓨팅된 집합된 사용자 관련 데이터가 바람직하게는 평가를 통해 결정(decision)을 내리고, 가장 바람직하게는 결정에 따라 액션(action) 및/또는 수정(modification)이 이루어질 수 있다. 하나 이상의 평가가 이루어질 수 있다. 하나 이상의 결정이 발생할 수 있다. 하나 이상의 동작이 행해질 수 있다. 하나 이상의 수정이 이루어질 수 있다.

[0032] 컴퓨팅된 집합된 사용자 관련 데이터는 임계값 및/또는 범위에 따라 평가될 수 있다. 임계값의 제1 측에 대한 값은 제1 결정을 야기할 수 있다. 임계값의 제2 측에 대한 값은 제2 결정을 야기할 수 있으며, 바람직하게는 제1 결정과 상이할 수 있다. 범위 내 값은 제1 결정을 야기할 수 있고, 범위 밖 값은 제2 결정을 야기할 수 있다.

[0033] 결정 및/또는 액션 및/또는 수정은 블록체인 트랜잭션과 같은 하나 이상의 추가 트랜잭션에 대한 하나 이상의 입력을 변경시킬 수 있다. 결정 및/또는 액션 및/또는 수정은 블록체인 트랜잭션과 같은 하나 이상의 추가 트랜잭션으로부터의 하나 이상의 출력을 변경시킬 수 있다. 결정 및/또는 액션 및/또는 수정은 결정 유한 오토머턴(deterministic finite automaton, DFA)을 변경시킬 수 있으며, 예를 들어 DFA는 하나 이상의 추가 트랜잭션을 구현한다.

[0034] 결정 및/또는 액션 및/또는 수정은 DFA, 예를 들어 DFA의 성능을 수정 및/또는 최적화하기 위한 피드백을 제공할 수 있다.

[0035] 결정 및/또는 액션 및/또는 수정은 서비스 및/또는 제품의 설계 및/또는 생산 및/또는 저장 및/또는 분배 및/또는 소비를 수정 및/또는 최적화하기 위한 피드백을 제공할 수 있다.

[0036] 결정 및/또는 액션 및/또는 수정은 서비스 및/또는 제품의 설계 및/또는 생산 및/또는 저장 및/또는 분배 및/또는 소비를 위한 프로세스와 같은 프로세스를 수정 및/또는 최적화하기 위한 피드백을 제공할 수 있다.

[0037] 결정 및/또는 액션 및/또는 수정은 스마트 계약과 같은 계약을 수정 및/또는 최적화하기 위한 피드백을 제공할 수 있다.

[0038] 사용자 관련 데이터는 시간일 수 있다. 시간은 이벤트가 발생한 시간일 수 있다. 이벤트는 트랜잭션 또는 상태 전이 또는 DFA로부터 발생한 블록체인 트랜잭션의 완료 시간 및/또는 DFA 작업을 구현할 때 DFA 내 상태 변경 시간이 될 수 있다.

[0039] 사용자 관련 데이터는 정확도 및/또는 정밀도의 표현일 수 있다. 정확도 및/또는 정밀도는 DFA에 입력되거나 DFA에 의해 사용되거나 DFA에 의해 출력되는 측정값으로부터 얻을 수 있다. 측정값은 크기, 부피, 형상, 질량, 면적 또는 다른 정량적 값과 같은 하나 이상의 물리적 파라미터일 수 있다. 물리적 파라미터에 대한 정확도 및/또는 정밀도, 예를 들어 미리 결정된 허용 가능한 범위가 평가 및 기록될 수 있다. 평가는 실제값 및/또는 목표 및/또는 실제값에 대한 편차 및/또는 에러에 상대적일 수 있다. 평가는 결함 또는 기타 바람직하지 않은 특징들

의 존재 또는 부재일 수 있다.

[0040] 사용자 관련 데이터는 물리적 형태와 관련될 수 있다. 물리적 형태는 DFA에 입력되거나 DFA에 의해 사용되거나 DFA에 의해 출력되는 물리적 형태와 관련될 수 있고, 예를 들어 물리적 형태 자체 및/또는 크기, 부피, 모양, 질량, 면적 등과 같은 다른 정량적인 값으로 물리적 형태를 정량화한 것일 수 있다. 사용자 관련 데이터는 상품 또는 서비스의 유형일 수 있다.

[0041] 사용자 관련 데이터는, 예를 들어 트랜잭션, 잠재적으로 DFA를 통해 구현되는 트랜잭션을 사용하여 제공되는 상품 및/또는 서비스와 같은 품질에 관련될 수 있다. 품질은 트랜잭션 자체의 구현과 관련될 수 있다. 품질은 사양 품질 및/또는 적합성 품질일 수 있다. 품질은 다음 트랜잭션에서의 하나 이상의 변수 및/또는 DFA에 대한 다음 형태 및/또는 DFA에 의한 구현에 영향을 주는 피드백을 제공하는 것에 의하여, 품질 관리 프로세스에서 사용될 수 있다. 피드백은 결함; 이슈; 결점; 실패한 작업; 실패한 상태 전이 중 하나 이상의 존재 또는 부재일 수 있다. 품질은 다음 트랜잭션에서의 설계 및/또는 동작 및/또는 DFA에 대한 다음 형태 및/또는 DFA에 의한 구현에 영향을 주는 피드백을 제공하는 것에 의하여, 품질 관리 프로세스에서 사용될 수 있다. 품질 관리 프로세스는 품질 보증 프로세스일 수 있다. 피드백은 프로세스 및 프로세스 단계의 강도; 프로세스 및 프로세스 단계의 안정성; 프로세스 및 프로세스 단계의 포맷 중 하나 이상에 영향을 줄 수 있다. 피드백은 트랜잭션이 미래의 트랜잭션 구성에서 목적 및/또는 처음으로 적합하게 되는 범위를 증가시킬 수 있다.

[0042] 사용자 관련 데이터는 사용자의 능력, 예를 들어 트랜잭션의 일부 및/또는 DFA를 통하여 일반적이고, 잠재적으로 구현되는 트랜잭션을 완료할 수 있는 능력에 관한 것일 수 있다. 능력은 다음 중 하나 이상의 기록일 수 있다: 기능(competence)의 증거; 지식(knowledge)의 증거; 기술(skills)의 증거; 경험(experience)의 증거; 자격(qualifications)의 증거; 인증(certification)의 증거; 특히, 이들 중 하나 이상의 평가(assessment)에 대한 증거. 능력은 조직 및/또는 규제 기관의 회원; 규제 기관 또는 무역 기관과 같은 제3 자에 의한 보증 및/또는 승인; 제3자 운영 레지스터(register)에 존재 중 하나 이상일 수 있다.

[0043] DFA에 의해 잠재적으로 표현/구현될 수 있는 계약의 맥락에서, 계약은 다양한 금융 상품과 관련될 수 있다. 잠재적 금융 상품은 현금, 소유의 증서, 현금을 수령 또는 제공할 계약 상의 권리(예: 채권)가 포함될 수 있다. 잠재적 금융 상품은 현금 상품을 포함할 수 있고, 잠재적으로 다음 중 하나 이상을 포함할 수 있다: 주식(shares); 증권(securities); 청구서(bills); 주식자본(stocks); 옵션(options); 선물(futures); 시장 가치 자산(market valued assets). 잠재적 금융 상품은 파생 상품을 포함할 수 있으며, 잠재적으로는 다음 중 하나 이상을 포함할 수 있다: 자산(assets); 인덱스(indexes); 금리(interest rates); 대출(loans); 보증금(deposits); 양도성 예금 증서(certificates of deposit); 직물 환율(spot rates); 직물 환산장(spot exchange rates).

[0044] 트랜잭션에 관련된 블록체인의 사용자들에 대한 평판 정보와 같은, 사용자 관련 데이터를 제공하기 위한 컴퓨터 구현 시스템 및 방법이 제공된다. 이 방법은 특히 계약의 맥락에서 트랜잭션의 이행을 평가한 다음, 평판 정보를 통해 블록체인 상에 이를 기록하는 접근 방식을 포함한다. 결과적으로, 이 평판 정보가 늦게 검색될 수 있다. 다른 트랜잭션들에 대한 유사한 평판 정보는, 예를 들어 사용자에 대한 마스터 공개 키의 해시의 사용에 기초하여 동일한 사용자에게 검색되고 연결될 수 있다. 집합된 평판 정보는 검색된 평판 정보의 단편들로부터 컴퓨팅될 수 있다.

[0045] 바람직한 실시예에서, 특히 계약의 맥락에서, 평가 및 기록 제공은 결정 유한 오토머턴(DFA)을 사용하여 구현될 수 있다. 이 방법은 각 스마트 계약에 관련된 각 사용자에 대해 DFA가 스마트 계약을 구성하고 구현할 뿐만 아니라, 스마트 계약의 조건의 이행 정도도 고려할 수 있다. 따라서 DFA는 각 스마트 계약의 각 사용자에 관한 평판 정보를 생성한다. 파생 상품의 예에서, 이는 사실상 신용 등급 정보이다. DFA는 이 평판 정보가 블록 체인에 게시되고 저장되도록 한다.

[0046] 따라서, 소정의 구성에 따르면, 등급 정보(ratings information)와 같은 사용자 관련 데이터는 사용자에 의해서라기 보다 시스템 자체에 의해 생성된다. 이러한 자동화된 시스템의 한 예는 위에서 설명한 DFA의 사용이다. 그러나, 원칙적으로, 이는 사용자가 아닌 시스템이 등급 데이터를 제공하는 자동화된 블록체인 시스템에 의해 구현될 수 있다. 예를 들어, 등급 데이터는 블록체인 시스템 상에서 디지털 스마트 계약을 구현할 때 사용자가 조건을 어떻게 충족시키는가에 따라 블록체인 시스템에 의해 생성될 수 있다. 이 방법론은 사용자 입력 데이터와 비교할 때보다 객관적인 데이터를 제공하며 보다 효율적이고 믿을 수 있는 방식으로 생성 및 저장된다.

[0047] 본 방법은 다음의 하나 이상을 더 제공할 수 있다:

[0048] a. 적어도 하나의 사용자와 적어도 하나의 다른 사용자 사이의 트랜잭션을 정의하는 단계;

[0049] b. 상기 트랜잭션을 실행하는 단계;

[0050] c. 적어도 하나의 사용자들 또는 적어도 하나의 다른 사용자들에 대해 트랜잭션의 이행의 표현과 같은, 상기 트랜잭션으로부터 사용자 관련 데이터를 제공함으로써, 사용자 이행 표현과 같은, 사용자 관련 데이터 표현을 제공하는 단계;

[0051] 예를 들어, 사용자와 관련된 이전 트랜잭션의 이행의 표현과 같은, 사용자 관련 데이터 표현을 포함하는, 평판 트랜잭션과 같은 사용자 관련 데이터 트랜잭션을 구성하는데 사용하기 위하여, 사용자 이행 표현과 같은 사용자 관련 데이터 표현을 제공한다.

[0052] 본 발명의 제2 실시예에 따르면, 다음의 단계를 포함하는 사용자 관련 데이터의 기록을 만드는 방법이 제공된다:

[0053] a. 적어도 하나의 사용자 및 적어도 하나의 다른 사용자 간 트랜잭션을 정의하는 단계;

[0054] b. 상기 트랜잭션을 구현하는 단계;

[0055] c. 적어도 하나의 사용자 또는 적어도 하나의 다른 사용자에 대해 상기 트랜잭션으로부터 사용자 관련 데이터를 제공함으로써, 사용자 관련 데이터 표현을 제공하는 단계;

[0056] d. 상기 사용자 관련 데이터 표현을 포함하는 사용자 관련 데이터 트랜잭션을 구성하는 단계;

[0057] e. 사용자 관련 데이터 트랜잭션을 상기 블록체인으로 브로드캐스팅하는 단계.

[0058] 이 방법은 사용자 관련 데이터가 평판 정보임을 제공할 수 있다. 트랜잭션으로부터의 사용자 관련 데이터는 사용자에 관한 트랜잭션의 이행의 표현일 수 있다. 사용자 관련 데이터 트랜잭션은 평판 트랜잭션일 수 있다. 사용자 관련 데이터 트랜잭션은 사용자와 관련된 이전 트랜잭션의 이행의 표현을 포함할 수 있다. 사용자 관련 데이터 표현은 사용자 이행 표현일 수 있다.

[0059] 본 발명의 제2 실시예는 본 발명의 제1 실시예에 제시된 특징, 옵션 및 가능성 중 임의의 것을 포함할 수 있다.

[0060] 본 발명의 제3 실시예에 따르면, 집합된 사용자 관련 데이터를 컴퓨팅하는 방법이 제공되며, 이 방법은 다음을 포함한다:

[0061] a. 선택된 사용자를 얻기 위하여, 집합된 사용자 관련 데이터가 요구되는 사용자를 선택하는 단계;

[0062] b. 선택된 사용자와 관련된 필터를 생성하는 단계;

[0063] c. 상기 필터가 적용되는 사용자 관련 데이터 트랜잭션에 대한 블록체인을 검색하는 단계;

[0064] d. 상기 필터가 적용되는 상기 사용자 관련 데이터 트랜잭션들로부터 상기 선택된 사용자에 대한 집합된 사용자 관련 데이터를 컴퓨팅하는 단계.

[0065] 이 방법은 집합된 사용자 관련 데이터가 집합된 평판 정보임을 제공할 수 있다. 사용자 관련 데이터 트랜잭션은 평판 트랜잭션일 수 있다. 사용자 관련 데이터 트랜잭션은 사용자와 관련된 이전 트랜잭션의 이행의 표현을 포함할 수 있다. 이전 트랜잭션으로부터의 사용자 관련 데이터는 사용자에 관한 이전 트랜잭션의 이행의 표현일 수 있다.

[0066] 본 발명의 제3 실시예는 본 발명의 제1 실시예에 제시된 특징, 옵션 및 가능성 중 임의의 것을 포함할 수 있다.

[0067] 본 발명의 제4 실시예에 따르면, 본 발명의 제1 실시예의 방법을 구현하도록 설정된 컴퓨터 구현 시스템, 잠재적으로는 본 문서 내의 다른 곳에 제시된 특징, 옵션 및 가능성 중 어느 것을 수행하도록 설정된 시스템을 포함한다.

[0068] 시스템은 다음을 더 포함할 수 있다:

[0069] a. 사용자 디지털 지갑;

[0070] b. 블록체인을 통하여 DFA를 구현하도록 설정된 적어도 하나의 컴퓨팅 에이전트;

[0071] c. 블록체인 플랫폼.

[0072] 본 발명의 제4 실시예는 본 발명의 제1 실시예에 제시된 특징, 옵션 및 가능성 중 임의의 것을 포함할 수 있다.

[0073] 본 발명의 제5 실시예에 따르면, 본 발명의 제2 실시예의 방법을 구현하도록 설정된 컴퓨터 구현 시스템, 잠재적으로는 본 문서 내에 제시된 특징, 옵션 및 가능성 중 어느 것을 수행하도록 설정된 시스템을 포함한다.

[0074] 시스템은 다음을 더 포함할 수 있다:

[0075] a) 블록체인을 통하여 DFA를 구현하도록 설정된 적어도 하나의 컴퓨팅 에이전트;

[0076] b) 블록체인 플랫폼.

[0077] 본 발명의 제5 실시예는 본 발명의 제1 실시예에 제시된 특징, 옵션 및 가능성 중 임의의 것을 포함할 수 있다.

[0078] 본 발명의 제6 실시예에 따르면, 본 발명의 제3 실시예의 방법을 구현하도록 설정된 시스템, 바람직하게는 컴퓨터 구현 시스템, 잠재적으로는 본 문서 내에 제시된 특징, 옵션 및 가능성 중 어느 것을 수행하도록 설정된 시스템을 포함한다.

[0079] 시스템은 다음을 더 포함할 수 있다:

[0080] a. 사용자 디지털 지갑;

[0081] b. 블록체인을 통하여 DFA를 구현하도록 설정된 적어도 하나의 컴퓨팅 에이전트;

[0082] c. 블록체인 플랫폼.

[0083] 본 발명의 제6 실시예는 본 발명의 제1 실시예에 제시된 특징, 옵션 및 가능성 중 임의의 것을 포함할 수 있다.

[0084] 그러므로, 본 발명에 따르면 다음 중의 옵션들, 가능성들 및 특징들이 제공되거나 더 제공될 수 있다.

[0085] 본 발명은 특히 본 발명의 제1, 제2, 제4 및 제5 실시예와 관련하여, 또한 일반적으로 다음으로부터 제공될 수 있다. 평판 정보(reputational information)라는 용어는 본 출원 내의 사용자 관련 데이터라는 용어로 대체될 수 있다. 평판 트랜잭션은 본 출원 내의 사용자 관련 데이터 트랜잭션이라는 용어로 대체될 수 있다. 이전 트랜잭션의 이행의 표현은 사용자 관련 데이터의 표현이라는 용어로 대체될 수 있다.

[0086] 사용자 이행 표현은 사용자에 의한 트랜잭션의 이행 정도를 정량화하는 이행 점수로서 정의될 수 있다. 사용자 이행 표현은 트랜잭션이 완료되었는지를 반영할 수 있다. 사용자 이행 표현은 이행 값(fulfilment value)일 수 있다. 사용자 이행 표현은 이행 스코어, 예를 들어 이진 스코어일 수 있다.

[0087] 평판 트랜잭션은 사용자 이행 표현이 관련된 사용자에 대한 기여 정보(attributable information)를 더 포함한다. 사용자에 대한 기여 정보는 사용자에 대한 비트코인 주소와 같은 주소일 수 있다. 기여 정보는 사용자에 대한 서명 스크립트 또는 그의 해시일 수 있다. 사용자에 대한 기여 정보는 사용자에 대한 비트코인 주소와 같은 주소 및/또는 사용자에 대한 서명 스크립트 또는 그의 해시일 수 있다. 기여 정보는 사용자를 위해 및/또는 사용자를 대신하여 수행된 결정론적 키 생성으로부터 나올 수 있다.

[0088] 평판 트랜잭션은 사용자 이행 표현이 획득된 트랜잭션에 대한 트랜잭션 유형을 더 포함할 수 있다. 트랜잭션 유형은 트랜잭션의 내용을 자세히 설명할 수 있다. 트랜잭션 유형은 사용된 트랜잭션 템플릿을 자세히 설명할 수 있다. 트랜잭션 유형은 계약 유형, 예를 들어 스마트 계약 유형일 수 있다. 트랜잭션 유형은 트랜잭션 유형에 따른 트랜잭션 유형의 공지의 목록 중 하나일 수 있다.

[0089] 사용자 이행 표현은 평판 트랜잭션의 메타데이터에 포함될 수 있다. 사용자 이행 표현 및/또는 기여 정보 및/또는 트랜잭션 유형은 평판 트랜잭션의 메타데이터에 포함될 수 있다.

[0090] 평판 트랜잭션은 P2SH(Pays To Script Hash) 트랜잭션일 수 있다. 평판 트랜잭션은 다중 서명 트랜잭션일 수 있다. 평판 트랜잭션은 제3자에 의해 제어, 예를 들어 DFA에 의해 제어되는 주소로 전달될 수 있다. 평판 트랜잭션(transaction)은 더스트(dust)를 보낼 수 있다.

[0091] 평판 트랜잭션은 도 1을 구현할 수 있다. 평판 트랜잭션을 위한 리딤 스크립트(redeem script)는 도 2를 구현할 수 있다.

[0092] 평판 트랜잭션은 결정 유한 오토머턴(DFA)에 의해 구현될 수 있다.

[0093] 방법 또는 시스템은 다음 중 하나 이상에 대해 결정 유한 오토머턴을 사용하는 것을 포함할 수 있다: 트랜잭션을 정의; 트랜잭션을 구현; 이행의 표현을 제공; 평판 트랜잭션을 구성. 방법 또는 시스템은 트랜잭션을 정의하

고, 트랜잭션을 구현하며, 이행의 표현을 제공하고 평판 트랜잭션을 구성하기 위해 공통 결정 유한 오토머턴(DFA)을 사용하는 것을 포함할 수 있다.

[0094] 하나 이상의 트랜잭션은 계약, 예를 들어 스마트 계약일 수 있다.

[0095] 본 발명은 특히 본 발명의 제1, 제3 및 제6 실시예와 관련하여, 또한 일반적으로 다음 중 하나를 더 제공할 수 있다.

[0096] 사용자는 트랜잭션을 제공하는 사용자들로부터 선택될 수 있다. 사용자는 선택 사용자에 의해 선택될 수 있다. 복수의 사용자들은, 예를 들어 선택 사용자에 의해 선택될 수 있다. 선택 사용자는 하나 이상의 트랜잭션을 시작하는 것을 고려하는 사용자일 수 있다.

[0097] 사용자의 디지털 지갑을 사용하여 선택이 이루어질 수 있다. 디지털 지갑에는 사용자 선택을 위한 인터페이스가 제공될 수 있다. 디지털 지갑에는 집합된 평판 정보 및/또는 그의 추가로 처리된 형태의 디스플레이를 위한 인터페이스와 함께 제공될 수 있다.

[0098] 집합된 평판 정보를 컴퓨팅하는 것은 하나 이상 또는 모든 선택된 사용자에 대해 컴퓨팅될 수 있다.

[0099] 필터는 선택된 사용자로부터 어드레스 해시 및/또는 선택된 사용자로부터 서명 스크립트를 획득함으로써 구성될 수 있다. 필터는 선택된 사용자의 공개 키로부터 발생하는 어드레스 해시 및/또는 선택된 사용자의 공개 키로부터 발생하는 서명 스크립트로부터 구성될 수 있다. 필터는 선택된 사용자의 마스터 공개 키의 해시를 제공하도록 구성될 수 있다.

[0100] 방법 및/또는 시스템은 사용자가 블록체인에 액세스 및/또는 블록체인을 파싱하는 것을 더 제공할 수 있다.

[0101] 방법 및/또는 시스템은 블록체인에서의 평판 트랜잭션이 필터를 사용하는 것이 고려되는 것을 더 제공할 수 있다. 바람직하게는, 필터에 의해 픽업된 모든 평판 트랜잭션을 수집하기 위해, 예를 들어 필터에 의해 픽업된 메타데이터를 포함하는 모든 평판 트랜잭션을 수집하기 위해, 가장 바람직하게는 선택된 사용자에 대한 마스터 공개 키 및 그로부터의 모든 후손 공개 키(descendant public keys)와 관련하여 필터에 의해 픽업된 모든 평판 트랜잭션을 수집하는 것이다.

[0102] 집합된 평판 정보에는 추가 프로세싱이 적용될 수 있고, 추가 프로세싱은 다음 중 하나 이상을 컴퓨팅한다: 수치 평판 점수; 평판 점수; 다른 사용자에 대한 평판 등급.

[0103] 집합된 평판 정보 및/또는 그의 추가로 처리된 형태는 선택 시 및/또는 사용자로부터의 제안으로 점수를 제시하기 위해 및/또는 임의의 선택 전 및/또는 사용자에 의한 트랜잭션 제안 전에 컴퓨팅될 수 있다.

[0104] 집합된 평판 정보를 컴퓨팅하는 방법은 집합된 평판 정보를 사용자, 특히 지갑이 집합된 평판 정보를 계산한 사용자에게 제시하는 단계를 더 포함할 수 있다.

[0105] 집합된 평판 정보를 계산하는 방법은 사용자가 결정을 내리는 단계를 더 포함하는 방법을 제공할 수 있으며, 결정은 집합된 평판 정보의 고려를 포함한다. 결정은 선택된 사용자와 트랜잭션을 시작하기로 하는 결정을 포함할 수 있다.

[0106] 집합된 평판 정보를 컴퓨팅하는 방법은 사용자 및/또는 선택된 사용자가 액션을 수행하는 단계를 더 포함하는 방법을 제공할 수 있다. 액션은 선택된 사용자에게 정보를 제공하는 단계; 선택된 사용자로부터 정보를 수신하는 단계; 선택된 사용자가 사용자를 위한 상품을 생산하는 단계; 사용자가 선택된 사용자를 위한 상품을 생산하는 단계; 선택된 사용자가 사용자에게 상품을 제공하는 단계; 사용자가 선택된 사용자에게 상품을 제공하는 단계; 선택된 사용자가 사용자에게 상품을 발송, 배송 또는 운송하는 단계; 사용자가 선택된 사용자에게 상품을 발송, 배송 또는 운송하는 단계 중 하나 이상을 포함할 수 있다. 상품은 서비스 및/또는 물건일 수 있다.

도면의 간단한 설명

[0107] 본 발명의 이들 및 다른 실시예는 본 명세서에 기술된 실시예를 참조하여 명백해지고 설명될 것이다. 본 발명의 실시예는 이제 단지 예로서 그리고 첨부 도면을 참조하여 설명될 것이다:

도 1은 비트코인 트랜잭션의 구현을 도시한다;

도 2는 도 1 비트코인 트랜잭션과 관련된 비트코인 거래 리딤 스크립트(redeem script)를 도시한다;

도 3은 트랜잭션들 사이의 링크 및 트랜잭션들의 유효성을 도시한다;

도 4는 트랜잭션으로부터 블록체인까지, 그리고 지갑 조회로의 정보 흐름을 도시한다;

도 5는 본 발명이 포함될 수 있는 시스템의 개요를 도시한다;

도 6은 블록체인 기반 DFA 구현을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0108] 제안된 발명은 블록체인, 보다 구체적으로는 비트코인 블록체인 상에서의 사용자 관련 데이터 기록 시스템의 구현 및 블록체인으로부터 사용자 관련 데이터 기록 및 프로세싱이다.

[0109] 이 방법은 사용자 관련 데이터 평가를 위한 접근법을 포함하거나 제공하며, 사용자 관련 데이터 기록을 통해 블록체인 상에서 그의 기록을 제공하는 것이다.

[0110] 바람직한 실시 예에서, 평가 및 기록 제공은 결정 유한 오토머턴(DFA)을 사용하여 구현될 수 있다. 아래에서 제시된 상세한 예에서, 이는 피어-투-피어 파생 상품 거래 플랫폼을 특징으로 하는 특정 실시예에서 예시되지만, 사용자 관련 데이터가 관련된 다른 상황도 동일하게 적용될 수 있다.

[0111] 이 방법은 각 트랜잭션에 관련된 각 사용자에 대해 DFA가 트랜잭션의 구현을 설정하고 가능하게 할 뿐만 아니라, 트랜잭션으로부터 발생하는 사용자 관련 데이터를 고려하도록 한다. 따라서 DFA는 각 트랜잭션에서 사용자 관련 데이터를 생성한다. DFA는 이러한 사용자 관련 데이터가 블록체인에 게시되고 저장되도록 한다.

[0112] 결과적으로, 이 사용자 관련 데이터를 늦게 검색될 수 있다. 또한, 후술되는 바와 같이, 다른 트랜잭션에 대한 유사한 사용자 관련 데이터가 검색되어 동일한 사용자에게 링크될 수 있다. 바람직한 실시예에서, 이는 사용자에 대한 마스터 공개 키의 해시의 사용에 기초한다. 집합된 사용자 관련 데이터는 해당 사용자에 대한 사용자 값을 주기 위하여 처리될 수 있다. 그 후, 사용자 값은 후속 평가 및/또는 결정 및/또는 수정에 사용될 수 있다.

[0113] 한 실시예에서, 각각의 사용자는 그들의 비트코인 지갑을 이용하여 블록체인으로부터 사용자 관련 데이터를 검색한 다음 집합된 사용자 관련 데이터를 처리할 수 있으며, 이는 지갑 인터페이스를 통해 사용자에게 표시될 수 있다. 이는 사용자, 실질적으로 고객 사용자에게 상대방 사용자, 벤더 사용자에 대한 유용한 정보를 제공하며, 이는 사용자로 하여금 다른 가능한 혜택 중에서도 제공된 트랜잭션에 참여할지 여부를 결정하는 것을 돕는다.

[0114] 제공되는 솔루션은 강력하고 효율적이며 분산형이며 익명성이 있다.

[0115] 제안된 발명은 다음의 잠재적 이점을 제공한다:

[0116] * 분산되어 대규모 단일 지점에서의 장애를 방지하고, 공격에 취약하지 않음;

[0117] * 수수료 없음(일반적으로 비트코인 프로토콜에서는 적은 트랜잭션 수수료만 예상됨);

[0118] * 전 세계적이며 인터넷에 액세스할 수 있는 사람이라면 언제든지 참여할 수 있음;

[0119] * 투명하므로, 데이터가 블록체인에 기록되면 누구나 볼 수 있음;

[0120] * 불변이므로, 데이터가 블록체인에 기록되면 변경할 수 없음; 그리고

[0121] * 분산적 데이터의 기록, 저장 및 검색 시스템.

[0122] 아래에서 상세하게 설명되는 구현은 평판의 맥락에서 사용자 관련 데이터의 중요한 유형이 제공되지만, 본 발명은 광범위한 사용자 관련 데이터에 적용될 수 있다.

[0123] 사용자 관련 데이터는 블록체인 트랜잭션에 대한 입력의 결과(예: 사용자의 존재 및 참여) 및 블록체인 트랜잭션에 대한 출력의 결과 (예: 행동 및 결과에 대한 사용자의 영향)로 인해 발생한다. 이들은 사용자 관련 데이터가 처리될 수 있도록 하고, 사용자 관련 데이터 평가는 (사용자 관련 데이터 블록체인 트랜잭션에서) 블록체인에 기록될 가치가 있는 사용자 관련 데이터를 획득할 수 있게 한다. 따라서, 사용자 관련 데이터의 이러한 개별적 단편들은 후속 검색 및 수집을 위해 블록체인에서 쉽게 이용 가능하여 집합된 사용자 관련 데이터를 제공한다. 이 집합된 사용자 관련 데이터는 처리의 대상이 될 수 있다. 처리는 다음을 포함하는 다양한 후속 단계를 일으킬 수 있다:

[0124] 집합된 사용자 관련 데이터의 잠재적 평가; 및/또는

[0125] 집합된 사용자 관련 데이터에 기초한 하나 이상의 결정; 및/또는

[0126] 미래 블록체인 트랜잭션 또는 프로세스 변수, 잠재적으로 미래 블록체인 트랜잭션에 미치는 영향에 대한 수정

[0127] 결정 및/또는 수정은 잠재적으로 미래 트랜잭션을 개선할 수 있고 및/또는 이전 트랜잭션과 비교하여 성공적인 또는 보다 성공적인 결과를 갖도록 할 수 있다.

[0128] 다양한 실시예에서, 예를 들어, 사용자 관련 데이터는 시간과 관련될 수 있다. 이는 DFA로 인해 블록체인 트랜잭션이 완료되는 시간 및/또는 DFA 작업을 구현할 때 DFA 내에서 상태가 변경되는 시간일 수 있다. DFA의 작업에 따라 이와 같은 시간이 여러 개 존재할 수 있다. 시간을 포함하여, 이러한 사용자 관련 데이터의 복수의 기록의 검색은 (집합된 사용자 관련 데이터로서) DFA의 사용을 분석하고 및/또는 구현하는 동작을 포함하여 DFA의 성능을 최적화하는데 사용될 수 있다. 이는, 예를 들어 프로세스 용량을 개선하기 위하여, 작업을 통과하는 서비스 또는 제품의 타이밍을 최적화하는 것이 포함된다. 최적화는 작업에서 변수들을 제어하여 타이밍을 변경함으로써 위치 등에 접근하는 사람들과 관련될 수 있다. 시간은 작업의 신뢰성, 이용 가능한 경우 유지 보수 또는 서비스가 제공되어야 하는 상황 등에 관한 정보를 제공할 수 있다.

[0129] 다양한 실시예들에서, 예를 들어, 사용자 관련 데이터는 정확성 및/또는 정밀도에 관한 것일 수 있다. 따라서, 사용자 기여의 정확성 및/또는 정밀도에 관한 사용자 관련 데이터가 수집되고 기록될 수 있다. 정확성 및/또는 정밀도는 DFA에 입력되거나 DFA에 의해 사용되거나 DFA에 의해 출력된 측정, 예를 들어 크기, 부피, 형상, 질량, 면적 또는 다른 정량적 값과 같은 물리적 파라미터와 관련될 수 있다. 따라서, 상품 또는 서비스를 수용 또는 거부하는 스크리닝 프로세스를 구현하는 DFA의 맥락에서, 물리적 파라미터가 고려될 수 있다. 물리적 파라미터에 대한 정확도 또는 정밀도, 예를 들어 소정의 허용 가능한 범위가 평가 및 기록될 수 있다. 평가는 실제 값에 대한 것일 수도 있고, 목표 또는 실제 값 등에 대한 편차 또는 오차일 수도 있다. 평가는 결함 또는 다른 바람직하지 않은 특징의 존재 또는 부재일 수 있다. 예를 들어, 여러 프로세스에 대한 거부율을 밝히거나 및/또는 향후 프로세스를 개선하기 위해 해당 프로세스의 제어에 피드백을 제공하기 위해 이러한 여러 결과가 (집합된 사용자 관련 데이터로) 함께 고려될 수 있다.

[0130] 다양한 실시예들에서, 예를 들어, 사용자 관련 데이터는 물리적 형태와 관련될 수 있다. 따라서, 사용자 기여의 물리적 형태에 대한 사용자 관련 데이터가 수집되고 기록될 수 있다. 물리적 형태는 DFA에 입력되거나 DFA에 의해 사용되거나 DFA에 의해 출력되는 물리적 형태, 예를 들어 물리적 형태 자체 및/또는 크기, 부피, 형상, 질량, 면적 또는 다른 정량적 값과 같은 물리적 형태의 정량화와 관련 될 수 있다. 따라서, 물류 운영을 구현하는 DFA의 맥락에서, 물리적 형태가 고려될 수 있다. 특정 물리적 형태는 물류 작업 내에서 작업에 영향을 미치거나 제어할 수 있으며, 예를 들어 특정 크기의 단위 및/또는 재고 레벨로 처리될 수 있는 (집합된 사용자 관련 데이터로서) 최대 질량일 수 있다. 상품 또는 서비스의 유형인 사용자 관련 데이터에도 유사한 원칙이 적용될 수 있다. 따라서, 사용자 관련 데이터는 (집합된 사용자 관련 데이터로서) 재고 레벨을 제공하기 위해 상품에 대해 나가는 판매 및 들어오는 보충 공급을 반영할 수 있다.

[0131] 다양한 실시 예에서, 예를 들어, 사용자 관련 데이터는 예를 들어 트랜잭션, 잠재적으로는 DFA를 통하여 구현되는 트랜잭션을 사용하여 제공되는 상품 및/또는 서비스의 품질에 관한 것일 수 있다. 품질은 트랜잭션 자체의 구현과 관련될 수 있다. 품질은 사양 품질 및/또는 적합성 품질일 수 있다. 품질은, 예를 들어, 이후 트랜잭션 및/또는 DFA에 대한 다음 형태 및/또는 DFA에 의한 구현에서 하나 이상의 변수에 영향을 주는 피드백을 제공함으로써 품질 제어 프로세스에서 사용될 수 있다. 피드백은 다음 중 하나 이상의 존재 또는 부재일 수 있다: 결함; 이슈; 결점; 실패한 작업; 실패한 상태 전이. 품질은 다음 트랜잭션에서의 설계 및/또는 동작 및/또는 DFA에 대한 다음 형태 및/또는 DFA에 의한 구현에 영향을 주는 피드백을 제공하는 것에 의하여, 품질 관리 프로세스에서 사용될 수 있다. 품질 관리 프로세스는 품질 보증 프로세스일 수 있다. 피드백은 프로세스 및 프로세스 단계의 강도; 프로세스 및 프로세스 단계의 안정성; 프로세스 및 프로세스 단계의 포맷 중 하나 이상에 영향을 줄 수 있다. 피드백은 트랜잭션이 미래의 트랜잭션 구성에서 목적에 따라 및/또는 처음으로 적합하게 되는 범위를 증가시킬 수 있다.

[0132] 다양한 실시예에서, 사용자 관련 데이터는 사용자의 능력, 예를 들어 트랜잭션의 일부 및/또는 DFA를 통하여 일반적이고, 잠재적으로 구현되는 트랜잭션을 완료할 수 있는 능력에 관한 것일 수 있다. 능력은 다음 중 하나 이상의 기록일 수 있다: 기능(competence)의 증거; 지식(knowledge)의 증거; 기술(skills)의 증거; 경험(experience)의 증거; 자격(qualifications)의 증거; 인증(certification)의 증거; 특히, 이들 중 하나 이상의 평가(assessment)에 대한 증거. 능력은 조직 및/또는 규제 기관의 회원; 규제 기관 또는 무역 기관과 같은 제3

자에 의한 보증 및/또는 승인; 제3자 운영 레지스터(register)에 존재 중 하나 이상일 수 있다.

[0133] DFA에 의해 잠재적으로 표현/구현될 수 있는 계약의 맥락에서, 계약은 다양한 금융 상품과 관련될 수 있다. 잠재적 금융 상품은 현금, 소유의 증서, 현금을 수령 또는 제공할 계약 상의 권리(예: 채권)가 포함될 수 있다. 잠재적 금융 상품은 현금 상품을 포함할 수 있고, 잠재적으로 다음 중 하나 이상을 포함할 수 있다: 주식(shares); 증권(securities); 청구서(bills); 주식자본(stocks); 옵션(options); 선물(futures); 시장 가치 자산(market valued assets). 잠재적 금융 상품은 파생 상품을 포함할 수 있으며, 잠재적으로는 다음 중 하나 이상을 포함할 수 있다: 자산(assets); 인덱스(indexes); 금리(interest rates); 대출(loans); 보증금(deposits); 양도성 예금 증서(certificates of deposit); 직물 환율(spot rates); 직물 환산장(spot exchange rates).

[0134] 평판 시스템의 맥락에서, 사용자 관련 데이터는 평판 정보일 수 있다; 및/또는 사용자 관련 데이터 트랜잭션 고려는 트랜잭션의 이행을 평가하는 것을 포함할 수 있다; 및/또는 트랜잭션은 계약일 수 있다; 및/또는 집합된 사용자 정보는 집합된 평판 정보일 수 있다; 및/또는 사용자 값은 평판 표시 또는 스코어일 수 있다.

[0135] 평판의 맥락에서, 공개 키와 관련된 평판 정보의 사용으로부터 이점이 발생하는 다양한 다른 상황들이 있다. 평판 정보 또는 스코어가 의미하는 것은 전후 사정에 따른다. 예를 들어, 이는 온라인 게임을 플레이하는 것에 관한 스코어일 수 있다.

[0136] 평판 스코어와 같은 평판 정보는 호텔, 식당, 전자 상거래 판매자, 계약자 또는 동료에게 적용될 수 있다. 이는 회사, 부서, 팀 또는 개인 수준에서 적용될 수 있다. 사용자의 모든 제품(서비스 또는 상품) 또는 해당 제품 세트 또는 단일 제품에 적용될 수 있다. 예를 들어, 올바른 데이터를 이용하여, 과학적 연구 영향 지수인 h-인덱스를 계산할 수 있다.

[0137] 평판 정보, 예를 들어 평판 스코어는 정수 또는 실수일 수 있다. 이는 최근성에 의해 가중치가 부여될 수 있다. 이는 절대 등급이거나 동료에 대한 순위일 수 있다.

[0138] 위에서 예시된 바와 같이, 본 발명의 원리는 사용자와 관련된 광범위한 데이터에 적용될 수 있다. 아래의 상세한 구현은 평판이 중요한 유형의 데이터라는 맥락에서 제공되지만, 본 발명은 다른 데이터에 대해서도 유사하게 구현되므로 본 실시예는 본 발명의 범위 또는 그 구현을 제한하지 않는다.

[0139] 신뢰는 사회 및 경제 생활의 많은 측면의 기초가 된다. 화폐는 실제 자본의 한 형태인 것처럼 신뢰는 사회 자본의 한 형태로서 매우 중요하다. 그러나, 알지 못하지만 인터넷을 통해 거래하고자 하는 사람을 신뢰하는 방법을 어떻게 배울 수 있을까?

[0140] 평판 시스템은 평판을 통해 신뢰를 정량화하고 신뢰할 수 있는 행동을 장려하기 위해 사용자가 온라인 커뮤니티에서 서로를 평가할 수 있도록 하는 프로그램이다.

[0141] 평판 시스템은, 전자 상거래 웹 사이트와 같이 사용자들이 서로를 신뢰해야 하는 분산 응용 프로그램에 중요하다. 평판은 커뮤니티가 당신을 얼마나 많이 신뢰 하는지를 측정하며, 커뮤니티 및/또는 생태계의 다른 사용자들과의 이전 거래 및 상호 작용을 기반으로 계산된다.

[0142] 평판의 한 측면은 다른 사용자들, 상대방들과 체결한 계약을 이행함으로써 측정될 수 있다. 평판이 높을수록 네트워크 상에서 당신의 신뢰도가 높아진다. 이는 당신과의 상호 작용을 장려한다. 또한, 온라인 상에서 사용자의 평판으로 인해, 대부분의 사용자는 네트워크에서 보다 정직하게 행동하도록 선택할 것이다.

[0143] 평판 시스템은 평판 정보를 컴퓨팅하고 게시한다. 평판 정보는 스코어, 신용 평가, 신용 스코어, 등급과 같은 여러 형태를 취할 수 있다. 평판 정보는 일련의 서비스와 연관될 수 있다.

[0144] 평판은 eBay 또는 블록체인 기반 경매와 같은 온라인 마켓 플레이스와 같이 매우 다양한 환경에서 협력을 촉진하는데 탁월한 실적을 가지고 있다. 따라서, 많은 P2P(Peer-to-Peer) 시스템이 동료의 좋은 행동을 보상하고 및/또는 나쁜 행동을 처벌하기 위해 어떤 형태의 평판 체계를 채택한 것은 놀라운 일이 아니다.

[0145] 그러나, 이러한 평판 시스템의 신뢰성, 공격 또는 조작에 대한 취약성 및 사용 가능한 상황의 폭에 관한 이슈가 있다.

[0146] 여기서 기술되는 특정 실시예는 P2P 파생 상품 평판 생태계의 일부로서 비트코인 블록체인에서의 옵션, 선물 또는 선물 거래와 같은 P2P 파생 상품에 관한 것이다. 이 특정 실시예에서, DFA는 평판 정보를 블록체인에 제공하지만, 사용자의 지갑은 집합된 평판 정보를 생성한 다음, 이를 사용자에게 제공할 신뢰의 척도인 정량화된 평판

으로 처리한다.

[0147] 본 발명의 구현은 다음의 단계를 통해 설명된다:

[0148] 기여 정보(attributable information)를 포함하는 트랜잭션의 발생;

[0149] 기여 정보와 함께, 블록체인 상에서 평판 정보를 포함하는 평판 트랜잭션의 처리 및 기록;

[0150] 선택된 사용자에 대한 기여 정보, 결과적으로 고객 사용자의 지갑에 의한 선택된 사용자에 대한 평판 정보의 추출;

[0151] 평판 정보를 처리하여 집합된 평판 정보를 제공하고, 이에 따라 고객 사용자의 지갑에 의한 수량화된 평판을 획득.

[0152] *벤더 지갑 및 기여 정보의 출처*

[0153] 예를 들어, 파생 상품에 기초하여, 다른 사용자가 선택할 수 있는 일련의 사용자 제공 계약이 있을 수 있다. 계약을 제공하는 사용자는 벤더 사용자로 지정되고 계약을 선택하는 사용자는 식별의 용이를 위하여 고객 사용자로 지정된다. 물론, 두 사용자 모두가 계약 조건 내에서 제공하고 수신할 수 있으며, 계약은 둘 이상의 사용자와 관련될 수 있으므로, 이러한 지정은 본 발명의 범위를 제한하는 것이 아니다.

[0154] 벤더 사용자는 지갑을 가지고 있으며 벤더 사용자의 지갑에는 트랜잭션을 수행하는데 필요한 정보가 들어있다. 이는 계약과 같은 트랜잭션에 필요한 공개 키 및 개인 키 쌍을 포함한다. 벤더의 디지털 지갑은 소프트웨어의 일부로 개인 키들 및 공개 키들의 제공을 위한 컨테이너의 역할을 하며, 일반적으로 구조화된 파일 또는 간단한 데이터베이스로 구현된다.

[0155] 키들의 쌍들을 생성하는 일반적인 방법은 결정론적 키 생성이다. 이를 통해 단일의 "시드(seed)"로부터 많은 키들을 쉽게 생성할 수 있게 된다. 프로덕션은 시드를 사용하여 마스터 키를 생성한다. 마스터 키는 일련의 자식 키(child key)를 생성하기 위하여 사용될 수 있으며, 각 자식 키는 여러 세대를 걸쳐 일련의 손자 키(grandchild key)를 생성할 수 있다. 모든 키들은 계층 구조로 연결된다. 키의 전체 계층 구조를 생성하기 위하여, 오직 하나의 단일 마스터 키가 필요하다.

[0156] 결정론적 키 생성 및 계층적 결정론적 키 생성을 사용하면 많은 장점이 있으며, 그의 채택 및 사용을 장려한다. 따라서, 본 발명이 기초로 하는 특성은 사용 중인 키의 많은 부분에 존재한다.

[0157] 이러한 방식으로 키를 생성하기에 적합한 접근 방식에 대한 자세한 내용은 BIP0032 표준, Wuille, P. (2012), BIP 32: Hierarchical deterministic wallets, GitHub에 설명된 방법에서 확인할 수 있다.

[0158] *DFA 구현 트랜잭션*

[0159] 위에서 언급된 바와 같이, 이 실시예는 평판 정보에 대한 본 발명의 역할과 함께 관련 사용자에 의한 구성 및 성능을 포함하는 스마트 계약에 관한 것이다. 결정 유한 오토머턴(DFA)은 비트코인 블록체인을 통한 P2P 파생 상품 거래에 참여하는 각 사용자에 대해 스마트 계약을 실행할 수 있는 한 가지 방법을 나타낸다.

[0160] 스마트 계약 구현에서 DFA 사용에 대한 더욱 자세한 내용은 이 문서의 끝 부분에 제공된 스마트 계약에서 DFA의 사용(*Use of a DFA in Smart Contracts*) 섹션에서 제공된다.

[0161] 여기서는 DFA를 사용했지만, 이는 (재무) 계약의 상태를 관리하는 데 유용한 도구이기 때문에, DFA를 사용하지 않고 본 발명의 기능을 비트코인 지갑에 추가할 수 있다.

[0162] DFA를 사용하여 구조화되고 구현된 계약에는 많은 사용자가 참여할 수 있다. 각 사용자는 트랜잭션을 촉진하는 데 사용되는 개인 및 공개 키의 쌍과 연관된다. 이전 섹션에서는 이들이 결정론적 지갑에 의해 생성될 수 있으므로 마스터 키와 관련이 있다고 설명하고 있다.

[0163] 벤더 사용자의 경우, 시드는 마스터 개인 키를 생성하기 위하여 사용되며, 마스터 개인 키는 마스터 공개 키를 생성하기 위하여 사용되고, 마스터 공개 키는 다른 공개 키들을 생성하는데 사용된다. 벤더 사용자의 지갑은 다른 공개 키들 중 하나를 선택하여 계약이 나타내는 트랜잭션을 촉진한다. 수신자인 벤더 사용자는 비트코인 주소를 제공해야 한다.

[0164] 비트코인 주소는 사용될 다른 공개 키를 가져 와서 암호화 해싱 알고리즘에 이를 적용하여 다른 공개 키의 해시를 얻는 것에 의하여 획득된다. 보다 구체적으로, 이는 SHA256 해시 연산과 RIPEMD160 해시의 연산에 의해 수행

된다. 다른 공개 키에 따른 해시는 일반적으로 트랜잭션으로의 계약에 사용하기 위한 다른 공개 키에 대한 비트코인 주소와 같이, 실제 사용하기 전에 Base58Check를 사용하여 인코딩된다.

[0165] 계약을 구성하면, 계약의 구현 및 결과는 시간이 지남에 따라 발생한다. 결과로부터, 계약에 관련된 사용자 X가 계약에 의해 부과된 조건을 충족시켰는지 아니면 사용자 X가 계약에 의해 부과된 조건을 충족시키지 않았는지를 알 수 있다. 이러한 계약은 복잡하고, 여러 사용자가 관련될 수 있으므로, 이행 결과는 모든 당사자에게 보여질 수도 있다.

[0166] 트랜잭션의 구성, 구현 및 결과 외에도, DFA는 해당 계약과 관련하여 사용자에 대하여 관찰된 이행 위치를 반영하기 위해 추가 트랜잭션을 구현할 수도 있다.

[0167] 이행은 이행 값 또는 바람직하게는 이행 스코어에 반영된다. 선호되는 형태에서, 이는 해당 사용자의 해당 계약에 대한 이진 스코어이다.

[0168] 벤더 사용자에게 적용될 수 있는 계약 조건이 이행되면, 스코어 1이 생성된다. 벤더 사용자에게 적용될 수 있는 계약 조건 중 하나 이상이 이행되지 않으면, 스코어 0이 생성된다. 이행, 본 실시예에서 보다 구체적으로는 스코어는 계약의 처리와 함께 DFA에 의해 결정될 수 있다.

[0169] 또한, DFA는 예를 들어 트랜잭션의 세부 사항 또는 사용된 트랜잭션 템플릿을 통해 트랜잭션 유형을 결정할 수 있다. 이 특정 실시예에서, 트랜잭션은 계약이지만, 트랜잭션 유형은, 예를 들어 특정 형태의 P2P 파생 계약이 트랜잭션 유형으로 사용될 수 있는 것보다 더욱 구체적일 수 있다.

[0170] 결국, DFA는 계약의 구현을 위해 벤더 사용자의 비트코인 주소와 함께 제공된다. 이는 벤더 사용자와 연결되어 있다는 의미에서 비트코인 주소의 특성인 기여 정보를 구성한다. 사용자가 지불 사용자, 고객 사용자인 경우, DFA는 고객 사용자와 연결되어 있다는 의미에서 기여 정보인 공개 키 또는 서명 스크립트와 함께 제공될 것이다.

[0171] 이 트랜잭션 정보가 주어지면, 이 방법은 추가 트랜잭션인 평판 트랜잭션을 수행하기 위하여 DFA를 사용한다. 평판 트랜잭션에서, DFA는 평판 트랜잭션의 메타 데이터가 메타 데이터 내에 3 개의 메타 데이터를 포함하도록 제공한다: 계약에 대한 트랜잭션 유형; 해당 계약과 관련된 기여 정보(예: 비트코인 주소 또는 서명 스크립트); 및 벤더 사용자에 대한 해당 계약의 이행(예: 스코어).

[0172] 이후, DFA는 평판 트랜잭션을 생성하는데, 이 실시예에서, 이는 비트코인 트랜잭션 T_1이며, 4 개의 P2SH 다중 서명 출력 중 하나와 함께, '더스트'(무시할만한 양의 비트코인)를 DFA 에이전트에 의해 제어되는 주소로 보내는 메타데이터를 포함한다. 도 1은 비트코인 트랜잭션의 구현을 도시한다. 도 2는 비트코인 트랜잭션 리딤 스크립트를 도시한다. 도 3은 다양한 트랜잭션들 간의 연결을 도시한다. 모든 트랜잭션들이 표준 P2PKH 또는 P2SH 다중 서명 트랜잭션이며 유효함을 알 수 있다.

[0173] 이러한 평판 트랜잭션 및 블록체인에 포함되는 평판 정보를 저장하는 주요 이점은 블록체인이 변경될 수 없으므로, 불공정한 등급 공격의 가능성을 줄이는 것이다. 평판 트랜잭션은 그 자체로는 유용한 중간 형태이지만, 하지만 본 발명의 후속 이점을 허용하기도 한다.

[0174] 일반적으로, 제안된 발명을 채택하기 전에 트랜잭션 브로드캐스트가 DFA 메커니즘에 의해 고려되어 해당 트랜잭션들로부터 평판 정보를 결정하는데 사용될 수는 없다. 그러나, 비트코인 트랜잭션이 잠금해제 될 때마다, 공개 키가 서명 스크립트에 노출되므로, 특정 공개 키와 관련된 트랜잭션 내역은 항상 이용 가능하다.

[0175] *추출 및 처리를 위해 고객 지갑 사용(Customer Wallet Use to Extract and Process)*

[0176] 실시예는 이제 고객 사용자의 관점으로 돌아간다. 이 실시예에서 고객은 비트코인 블록체인에 대한 P2P 파생 상품 거래에 관심이 있다. 이와 같이, 위의 실시예에서 검토된 벤더 사용자를 포함하여, 이들은 다수의 사용자로부터 다수의 거래를 제공받을 수 있다. 제공되는 계약은 포맷, 리스크 프로파일, 가격 및 트랜잭션을 제공하는 서로 다른 사용자들 간의 기타 변수의 측면에서 동일하거나 매우 유사할 수 있다.

[0177] 고객 사용자의 디지털 지갑을 통해, 고객 사용자는 하나 이상의 여러 문의를 할 수 있다. 이들은 거래를 제공하는 특정 사용자 또는 동일한 유형의 거래를 제공하는 각 사용자와 관련될 수 있다. 단일 사용자에 대한 문의의 예를 사용하여, 고객 사용자는 벤더 사용자가 제공한 계약에 관심이 있다. 따라서, 고객 사용자는 벤더 사용자의 평판에 대한 조사를 시작하기 위해 고객 사용자의 지갑에 있는 지갑 기능을 통해 해당 벤더 사용자를 선택할 수 있다.

[0178] 고객 사용자의 지갑은 제공되는 계약의 일부이므로 트랜잭션을 제공하는 벤더 사용자의 비트코인 주소를 알고 있다. 비트코인 주소는 해당 계약에서 제공되는 특정 공개 키의 해시이므로 마스터 공개 키와 관련이 있다. 결과적으로 고객 사용자의 지갑이 벤더 사용자의 마스터 공개 키 해시를 결정할 수 있으며, 마스터 공개 키는 특정 다른 공개 키 뒤에 있다. 이와 관련하여 SHA-256과 같은 해시 함수를 사용하여 마스터 공개 키를 해시할 수 있다.

[0179] 이후, 고객 사용자의 지갑은 블록체인에 액세스하고 구문 분석하여 블록체인에서 과거 평판 트랜잭션을 검색하고 선택된 벤더 사용자에 대해 얻어진 마스터 키의 해시에 의해 해당 트랜잭션을 필터링할 수 있다. 고객 사용자에 의한 문의 시에 선택된 벤더 사용자와 연관된 공통 마스터 공개 키의 후손(descendant)을 사용하는 블록체인의 각 평판 트랜잭션은 이러한 방식으로 찾아질 수 있다. 따라서, 지갑은 해당 마스터 공개 키 및 이에 따른 벤더 사용자에게 연결된 각 트랜잭션에 대한 평판 정보를 블록체인으로부터 추출한다.

[0180] 평판 정보를 추출한 후, 고객 사용자의 지갑은 해당 정보를 추가로 처리할 수 있다. 예를 들어, 평판 계산 알고리즘은 검색된 평판 정보에 대한 계산을 수행할 수 있으며, 이는 사용자(들)에 대한 집합된 평판 스코어를 산출할 수 있고, 그 결과는 고객 사용자의 지갑에 표시된다. 예를 들어, 선택된 단일 사용자에 대한 대한 평판 정보의 경우, 지갑은 트랜잭션으로부터 긍정적인 평판 결과를 기록하는 사전 평판 트랜잭션의 총 수 및 트랜잭션로부터 부정적인 평판 결과를 기록하는 사전 평판 트랜잭션의 총 수를 고려할 수 있다. 지갑은 고객 사용자에 대한 긍정 및 부정의 균형을 신용 점수로 표시할 수 있다. 처리는 선택되지 않은 다른 사용자에 대한 정보를 고려하여 상대적 등급을 부여할 수 있다. 처리는 (수가 적어서 덜 강건한 경우에) 결과를 야기하는 평판 트랜잭션의 총 수를 고려하고, 스코어에 가중치를 부여하거나 및/또는 스코어의 신뢰도를 표시할 수 있다.

[0181] 마스터 공개 키의 해시를 통해 사용자에 기초한 집합된 평판 점수는 소정 시점, 예를 들어 선택 시, 사용자로부터의 제안과 함께 점수를 제시하기 위한 시간, 또는 선택이나 사용자가 고객 사용자에게 트랜잭션을 제공하기 전에 미리 컴퓨팅될 수 있다. 타이밍은 속도 및 정확도 사이의 선택된 밸런스 또는 트래이드 오프 및/또는 스코어의 최근성을 반영할 수 있다.

[0182] 정보 흐름은 도 4에 도시되어 있다. DFA에 의한 트랜잭션의 성능의 결과, DFA는 추가의 새로운 평판 트랜잭션을 통해 평판 정보의 기록을 블록체인으로 제공한다. 요구 또는 요청 시, 평판 정보는 처리를 위해 블록체인으로부터 고객 사용자의 지갑으로 흐른다.

[0183] 본 발명의 구현이 공통 마스터 공개 키로부터 계층적으로 도출된 공개 키의 맥락에서 위에서 기술되고 있지만, 본 발명은 결정론적 지갑이 아닌 다른 지갑의 관점에서 구현될 수 있다. 예를 들어, 사용자에게는 접근을 용이하게 하는 여러 가지 옵션이 있다. 이들은: 1) 각 트랜잭션에 대해 동일한 공개 키를 사용하여 이를 마스터 키로 사용할 수 있지만, (복수의 트랜잭션에 대하여 동일한 비트코인 주소를 재사용하는 것이 보안 상의 이유로 권장되지 않는 경우) 각 트랜잭션에 대해 별도의 주소를 생성하는 것이 바람직하고; 2) (매번 동일한 '마스터 키'로 식별되는) 임의의 공개 키를 사용하는 것을 포함한다. 그러나, 사용자는 계층적 결정론적 지갑을 가지는 것이 바람직하다. 왜냐하면 그 와트에는 자동적으로 마스터 키가 있기 때문에, 사용자가 백업할 양이 적은 지갑과 같은 고유한 이점이 있기 때문이다).

[0184] *스마트 계약에서 DFA 사용(Use of a DFA in Smart Contracts)*

[0185] 이 섹션은 DFA가 스마트 계약을 구현하는 방법에 대한 배경 지식을 제공하기 위한 것이다. 이 예시적인 맥락에서, 계약과 같은 프로세스 또는 작업을 모델링하는 DFA에 대한 정의가 제공된다. DFA는 컴퓨팅 에이전트 또는 "봇"으로 일컬어지는 컴퓨팅 리소스와 관련된 시스템과 상호작용한다. 이 컴퓨팅 에이전트는 트랜잭션을 생성하고 이를 블록체인에 제출하도록 구성된다. 이 DFA 실시예가 계약에 관한 것이지만, DFA의 사용은 계약에 한정되지 않는다.

[0186] 도 5를 참조하면, 실시예는 하드웨어 및 소프트웨어 컴포넌트를 포함하는 컴퓨팅 플랫폼-블록 체인-상에 구현된 관념적인 DFA로서 프로세스의 실현을 제공한다.

[0187] 도 5는 본 발명의 예시적인 실시예에 따라 구성된 시스템의 개요를 제공한다. 이 시스템은 명령을 수신하기 위해 다른 엔티티들 4(예를 들어, 인간 또는 다른 컴퓨터들)과 상호 작용할 수 있는 컴퓨팅 에이전트 3를 포함한다. 이러한 명령은 예를 들어 스마트 계약을 생성하고 실행할 수 있다. 따라서, 컴퓨팅 에이전트 3는 물리적인 세계와 상호 작용하여 "실세계"에서 외부의 이벤트에 응답하고 그 원인으로 본 발명을 구현한다.

[0188] 계약 자체의 사양은 소정의 기계 실행 형식, 예를 들어 xBRL으로 제공될 수 있으며, 안전하고 분산된 방식, 예

를 들어 토런트 네트워크(torrent network)의 분산 해시 테이블(DHT) 5에 저장된다. 계약의 사양으로부터, 컴퓨팅 에이전트는 DFA 2를0 구성하며, 이는 이후 하나 이상의 에이전트에 의해 블록체인 1에서 구현된다.

[0189] DFA 2 자체는 유한 세트{S, I, t, s0, F}로 지정되며, 여기서 S는 계약/DFA가 될 수 있는 가능한 (유한) 세트의 상태를 나타내고; I는 (알파벳으로도 알려진)의 (유한) 입력 세트이며, 계약과 관련하여 발생할 수 있는 소정의 이벤트 또는 조건, 예를 들어 지불, 기기의 성숙도, 상대방의 불이행 등을 의미하고; 우리의 메커니즘에서 이러한 입력 신호들은 하나 이상의 에이전트에 의해 수신/생산되며 시스템의 다음 상태(가능하면 동일한 상태)를 결정한다.

[0190] DFA의 세 번째 구성 요소는 전이 함수 t: SXI→S이다. "DFA"에서 "결정론적"이라는 용어는 결정의 고유성을 나타낸다: 상태와 입력이 주어지면 오직 하나의 새로운 상태(아마도 동일한 것). 따라서, 초기 상태(S_0)와 입력 히스토리가 주어지면 계산(계약)의 결과는 모든 가능한 최종 결과 세트(F⊆S)중 하나로 고유하다. 이러한 모든 요소가 설정되면, 모든 가능한 현재 상태 및 입력 신호들에 대하여 미래 상태를 지정하는 전이 테이블에 의해 DFA가 완전히 정의된다. DFA의 상태는 블록체인에서 사용되지 않은 트랜잭션 출력(UTXO)과 관련이 있다. 당 업계에 알려진 바와 같이, 비트코인 네트워크는 이용 가능한 모든 UTXO를 지속적으로 추적한다. 실시예에 따르면, DFA가 한 상태에서 다른 상태로 이동하는 메커니즘은 본 발명에 따라 블록체인 트랜잭션에 의해 구현(실행)된다. 효과적으로, 블록체인의 트랜잭션은 한 상태 (이전 트랜잭션의 입력)와 관련된 UTXO를 소비하고 다음 상태 (출력)와 관련된 UTXO를 생성한다.

[0191] *예: 할인(제로-쿠폰) 채권(Example: Discount (Zero-Coupon) Bond)*

[0192] 설명을 위해, 우리는 이제 (일반적으로 액면가에 대하여 할인된) 가격으로 구입하고 원금이 만기에 반환될 때까지 보유하는 단순 공채인 할인 (제로-쿠폰) 채권을 고려한다. 우리가 고려하는 가능한 상태는 각각 S={s_0, f_0, f_1}이며, 각각 보유 상태(s_0), (행복한 경로를 따르는 경우) 계약의 정상적인 결론 또는 행복한 결말(f_0), 소송과 같은 상황이 잘못되는 상태(f_1)를 나타낸다. 이에 따라, 시스템의 최종 상태는 F={f_0, f_1}이다. 우리가 고려할 알파벳은 I={r, d, e}로, 각각 만기 시 (또는 그 이전에) 원금의 상환(r), 만기 시 (또는 그 이전에) 발행자의 불이행(d), 상환하지 않고 계약의 만료(e)를 나타낸다. 이와 같은 간단한 계약의 전이 매트릭스는 표 1에 나와 있다.

표 1

[0193]

t	r	d	e
s_0	f_0	f_1	f_1

[0194] 표 1은 제로-쿠폰 채권을 나타내는 DFA에 대한 전이 테이블이다.

[0195] 최종 상태는 계약의 완료를 나타내므로 더 이상 상태를 지정할 필요가 없다(현재는 전이 테이블에서 '-'로 표시되지만 줄은 생략될 수 있음). 원칙적으로, 본 기기에 대해 (액션들뿐만 아니라) 더 많은 상태들 및/또는 입력들이 정의될 수 있지만, 복잡한 계약에 관한 상세한 내용을 넣기보다 본 발명의 근본적인 발명 측면을 간결하고 명확하게 설명하기 위해 수행하지 않았다.

[0196] 도 6은 (비트코인) 블록체인 상의 제로-쿠폰 채권 DFA의 실시예를 나타낸다. 삼각형으로 한 상태에서 다른 상태로 기계를 이동시키는 비트코인 트랜잭션 및 원에 의해 상태가 표시된다. 에이전트에 의해 수신된 입력은 도 6에서 생략되었지만 각 상태에서 이러한 입력에 따라 하나 또는 다른 전이가 발생해야 한다. 이는 하나 또는 다른 비트코인 트랜잭션(예: 상태 s_0에서 t_0 또는 t_1)의 구성에 의한 다이어그램에 반영된다; 상태를 변경하지 않는 전이에서는 트랜잭션이 필요하지 않으므로 생략되었다. DFA의 전이 트랜잭션(t_i)에 더하여, 초기 원래의 트랜잭션(o) 및 계약의 완료에 해당하는 트랜잭션(ci)이 고려된다.

[0197] 우리는 이제 트랜잭션(출발, 전이 및 완료)에서 자금의 흐름에 주의를 돌린다. 중요한 관찰은 DFA 및 (금융) 계약의 유한한 특성으로 인해 여러 번의 전이 후에 프로세스가 완료된다는 것이다. 이는 필수적으로 (관련 컴퓨팅 에이전트 및 비트코인 채굴자에 대한 약간의 수수료를 가정하며) 계약의 성립 및 실행의 최대 비용이 정해져 있으며, DFA의 성립 시에 미리 결정될 수 있음을 의미한다. 상상할 수 있는 가장 긴 경로를 따라 계약을 실행하는 데 필요한 총 금액으로 제공된다. 물론 이것은 실행에서 무한 루프의 가능성을 배제한 것이다. 그러나, 이는 현

재 (금융) 계약과 관련이 없으며, 심지어 그들의 이름에도 불구하고 영구적인 계약이 미래 어느 시점에 완료될 수 있다; 예를 들어, 부채가 있는 엔티티가 더이상 존재하지 않거나 인플레이션으로 인해 지불이 무시될 수 있는 경우이다.

[0198] 전술한 실시예들은 본 발명을 제한하기보다는 예시하는 것이고, 당업자는 첨부된 청구항에 의해 정의된 본 발명의 범위를 벗어나지 않는 범위에서 많은 대안적인 실시예들을 설계할 수 있음을 알아야 한다. 청구항에서, 괄호 안의 임의의 참조 번호는 청구 범위를 제한하는 것으로 해석되어서는 안 된다. "포함하는(comprising)" 및 "포함하다(comprises)" 라는 단어 등은 청구항 또는 명세서 전체에 열거된 구성 또는 단계의 존재를 배제하지 않는다. 본 명세서에서, "포함하다(comprises)"는 "포함하거나 구성되다(includes or consist of)"를 의미하고 "포함하는(comprising)"는 "포함하거나 구성되는(including or consisting of)"를 의미한다. 구성의 단일 참조 번호는 이러한 구성의 복수 참조 번호를 배제하지 않으며 반대의 경우도 마찬가지이다. 본 발명은 몇몇 구별되는 구성들을 포함하는 하드웨어에 의해 그리고 적절하게 프로그래밍된 컴퓨터에 의해 구현될 수 있다. 여러 수단을 열거하는 장치 청구항에서, 이들 수단 중 몇 개는 하나의 동일한 하드웨어 항목에 의해 구현될 수 있다. 특정 측정 값이 서로 다른 종속 항에 인용되어 있다는 단순한 사실만으로 이 측정 값의 조합을 활용할 수 없다는 것을 의미하지는 않는다.

도면

도면1

버전번호			
입력의 수			1
입력 (잠금 해제)	이전 트랜잭션	해시	T_0
		출력 인덱스	
	서명 스크립트의 길이		
	서명 스크립트 [P2PKH]		<DFA's signature> <DFA's public key>
	시퀀스번호		
출력의 수			1
출력 (잠금)	값		dust
	공개 키 스크립트의 길이		
	공개 키 스크립트 [P2SH multisig]		OP_HASH160 <hash160(redeem script)> OP_EQUAL
잠금시간			0

도면2

리딤 스크립트 [P2SH multisig]	OP_1 <transaction type> <hash(master public key)> <DFA state-zero or one> <DFA public key> OP_4 OP_CHECKMULTISIG

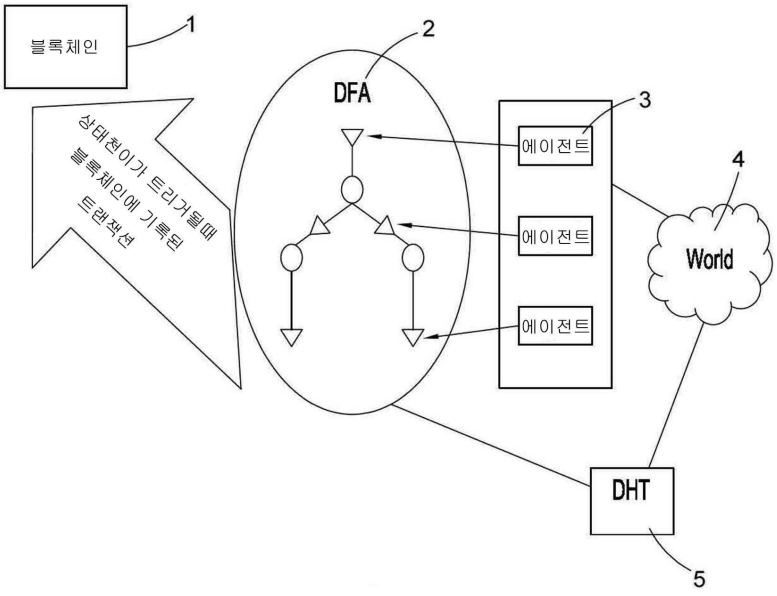
도면3

P2PKH				T_0	<DFA's signature> <DFA's public key>
P2SH multisig	T_1	OP_HASH160 <hash160(redeem script)> OP_EQUAL	OP_1 <transaction type> <hash(master public key)> <DFA state (0 or 1)> <DFA public key> OP_4 OP_CHECKMULTISIG		

도면4


DFA
지갑
T1
블록체인

도면5


블록체인
1
2
DFA
3
에이전트
에이전트
에이전트
4
World
상태전이가 트리거될때
블록체인에 기록된
트랜잭션
DHT
5

도면6