(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년07월01일
(11) 등록번호 10-2272008
(24) 등록일자 2021년06월28일

(51) 국제특허분류(Int. Cl.)
G06F 21/56 (2013.01) *H04L 29/06* (2006.01)
(52) CPC특허분류
G06F 21/563 (2013.01)
H04L 63/14 (2013.01)
(21) 출원번호 10-2019-0132250
(22) 출원일자 2019년10월23일
심사청구일자 2019년10월23일
(65) 공개번호 10-2021-0048241
(43) 공개일자 2021년05월03일
(56) 선행기술조사문헌
Santiago Bragagnolo et al, "SmartInspect: Solidity Smart Contract Inspector"(2018.03.)*
(뒷면에 계속)

(73) 특허권자
전북대학교산학협력단
전라북도 전주시 덕진구 백제대로 567 (덕진동1가)
(72) 발명자
김순태
전라북도 전주시 덕진구 백제대로 567 전북대 공대 5호관 511호 (금암동, 전북대학교)
홍준기
전라북도 전주시 덕진구 백제대로 567 전북대 공대 5호관 512호 (금암동, 전북대학교)
(74) 대리인
박종한

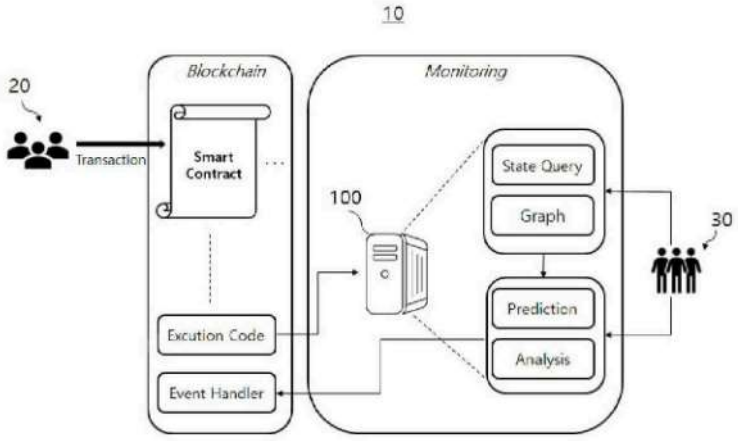
전체 청구항 수 : 총 13 항 심사관 : 정성훈

(54) 발명의 명칭 **스마트 컨트랙트에 대한 관제 장치 및 방법**

(57) 요 약

스마트 컨트랙트에 대한 관제 장치 및 방법이 개시되며, 본원의 일 실시예에 따른 스마트 컨트랙트에 대한 관제 방법은, 발행된 스마트 컨트랙트의 소스코드를 파싱하여 상기 스마트 컨트랙트와 연계된 변수를 추출하는 단계, 상기 스마트 컨트랙트의 주소 정보에 기초하여 상기 스마트 컨트랙트와 연계된 상태값을 추출하는 단계, 추출된 상기 변수 및 상기 상태값을 매핑하는 단계 및 매핑된 상기 변수 및 상기 상태값을 시각화하여 표시하는 단계를 포함할 수 있다.

대 표 도 - 도1



(56) 선행기술조사문헌

Bogdan Habic, "Debugging Ethereum transactions just got a whole lot easier"(2019.08.)*

Pouyan Momeni et al, "Machine Learning Model for Smart Contracts Security Analysis"(2019.08.)*

KR102024377 B1

KR102004511 B1

*는 심사관에 의하여 인용된 문헌

이 발명을 지원한 국가연구개발사업

과제고유번호	201739036.01
부처명	미래창조과학부
과제관리(전문)기관명	정보통신기술진흥센터(IITP)
연구사업명	대학ICT연구센터지원
연구과제명	적응형 블록체인 플랫폼 기술 개발 및 전문 인력 양성
기 여 율	1/1
과제수행기관명	서강대학교 산학협력단
연구기간	2017.06.01 ~ 2020.12.31

공지예외적용 : 있음

명 세 서

청구범위

청구항 1

스마트 컨트랙트에 대한 관제 방법에 있어서,

발행된 스마트 컨트랙트의 소스코드를 파싱하여 상기 스마트 컨트랙트와 연계된 변수를 추출하는 단계;

상기 스마트 컨트랙트의 주소 정보에 기초하여 상기 스마트 컨트랙트와 연계된 상태값을 추출하는 단계;

추출된 상기 변수 및 상기 상태값을 매핑하는 단계; 및

매핑된 상기 변수 및 상기 상태값을 시각화하여 표시하는 단계;를 포함하고,

상기 표시하는 단계는,

상기 매핑된 변수 및 상태값을 타임라인 형태로 표시하되,

상기 타임라인 상에서 상기 상태값이 변화된 시점에 대응하는 지점들을 상기 상태값이 유지된 영역과 구분되도록 표시하고,

사용자 입력에 의해 상기 지점들 중 어느 하나가 선택되는 경우, 해당 지점에 대응되는 상태값 변화 정보를 제공하는 것인, 스마트 컨트랙트 관제 방법.

청구항 2

제1항에 있어서,

상기 변수를 추출하는 단계는,

상기 소스코드에 대한 파싱 결과에 기초하여 추상 구문 트리를 생성하는 단계; 및

상기 추상 구문 트리에 기초하여 상기 스마트 컨트랙트와 연계된 변수 각각의 데이터 유형 및 변수명을 추출하는 단계,

를 포함하는 것인, 스마트 컨트랙트 관제 방법.

청구항 3

제2항에 있어서,

상기 상태값을 추출하는 단계는,

상기 스마트 컨트랙트의 주소 정보에 기초하여 Blockchain API를 통해 부호화된 데이터를 획득하는 단계; 및

상기 부호화된 데이터를 상기 상태값으로 변환하는 단계,

를 포함하는 것인, 스마트 컨트랙트 관제 방법.

청구항 4

제1항에 있어서,

상기 상태값 변화 정보는,

현재 블록 번호(Block Number), Tx 정보, 상태값이 변화하기 이전의 블록(PreBlock)에 포함된 상태값 정보, 상태값이 변화한 후의 블록(CurrentBlock)에 포함된 상태값 정보 중 적어도 하나를 포함하는 것인, 스마트 컨트랙트 관제 방법.

청구항 5

제1항에 있어서,

상기 표시하는 단계는,

소정의 변수에 대한 시간에 따른 상태값 변화를 나타낸 그래프 형태로 매핑된 상기 변수 및 상기 상태값을 표시하는 것인, 스마트 컨트랙트 관제 방법.

청구항 6

제1항에 있어서,

상기 스마트 컨트랙트의 이상을 탐지하는 단계를 더 포함하는 것인, 스마트 컨트랙트 관제 방법.

청구항 7

제6항에 있어서,

상기 이상을 탐지하는 단계는,

기 학습된 인공 지능 알고리즘에 기초하여 상기 상태값의 변화 패턴이 비정상적인 것으로 판단되는 경우 이상을 탐지하는 것인, 스마트 컨트랙트 관제 방법.

청구항 8

제7항에 있어서,

상기 이상을 탐지하는 단계는,

복수의 발행된 스마트 컨트랙트 각각에 대하여 수행되는 것인, 스마트 컨트랙트 관제 방법.

청구항 9

제8항에 있어서,

소정의 상기 스마트 컨트랙트에 대한 이상이 탐지된 경우, 경고 및 알림 신호를 생성하는 단계를 더 포함하는 것인, 스마트 컨트랙트 관제 방법.

청구항 10

스마트 컨트랙트에 대한 관제 장치에 있어서,

발행된 스마트 컨트랙트의 소스코드를 파싱하여 상기 스마트 컨트랙트와 연계된 변수를 추출하는 변수 추출부;

상기 스마트 컨트랙트의 주소 정보에 기초하여 상기 스마트 컨트랙트와 연계된 상태값을 추출하는 상태 추출부;

추출된 상기 변수 및 상기 상태값을 매핑하는 매핑부; 및

매핑된 상기 변수 및 상기 상태값을 시각화하여 표시하는 표시부;를 포함하고,

상기 표시부는,

상기 매핑된 변수 및 상태값을 타임라인 형태로 표시하되,

상기 타임라인 상에서 상기 상태값이 변화된 시점에 대응하는 지점들을 상기 상태값이 유지된 영역과 구분되도록 표시하고,

사용자 입력에 의해 상기 지점들 중 어느 하나가 선택되는 경우, 해당 지점에 대응되는 상태값 변화 정보를 제공하는 것인, 스마트 컨트랙트 관제 장치.

청구항 11

제10항에 있어서,

상기 변수 추출부는,

상기 소스코드에 대한 파싱 결과에 기초하여 추상 구문 트리를 생성하고, 상기 추상 구문 트리에 기초하여 상기 스마트 컨트랙트와 연계된 변수 각각의 데이터 유형 및 변수명을 추출하는 것인, 스마트 컨트랙트 관제 장치.

청구항 12

제11항에 있어서,

상기 상태 추출부는,

상기 스마트 컨트랙트의 주소 정보에 기초하여 Blockchain API를 통해 부호화된 데이터를 획득하고, 상기 부호화된 데이터를 상기 상태값으로 변환하는 것인, 스마트 컨트랙트 관제 장치.

청구항 13

제12항에 있어서,

기 학습된 인공 지능 알고리즘에 기초하여 적어도 하나 이상의 스마트 컨트랙트에 대하여 상기 상태값의 변화 패턴이 비정상적인 것으로 판단되는 경우 해당 스마트 컨트랙트의 이상을 탐지하는 이상 탐지부를 더 포함하는 것인, 스마트 컨트랙트 관제 장치.

발명의 설명

기 술 분 야

[0001] 본원은 스마트 컨트랙트에 대한 관제 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 최근 들어, 가상화폐에 대한 관심이 고조되면서 블록체인을 기반으로 한 다양한 어플리케이션이 생산 및 소비되고 있다. 가상화폐를 포함하는 블록체인 중 하나인 이더리움은 스마트 컨트랙트(Smart Contract)라는 기술을 활용하여 가상화폐의 기능을 넘어선 서비스를 제공하고 있다.

[0003] 이에 따라, 많은 개발자들은 이더리움에서 활용할 수 있는 스마트 컨트랙트를 개발하여 관련 서비스를 제공하고 있으며, 개발자뿐만 아니라 일반 사용자에 의해서도 스마트 컨트랙트가 배포되거나 사용될 수 있는데, 이러한 일반 사용자가 자신이 배포한 스마트 컨트랙트 혹은 사용하고자 하는 스마트 컨트랙트에 대한 정보를 획득하기 위해서는 별도의 수수료를 지급해야 하거나 해당 스마트 컨트랙트에 대한 Bytecode를 직접 분석하여야 하는 한계가 있다.

[0004] 전술한 개발자와 일반 사용자의 편의성 측면 외에도, 정부, 민간단체, 이더리움 관계자 등의 주체는 블록체인 네트워크 내의 악의적인 사용(예를 들면, 자금 세탁, DDoS 공격 등)에 대한 발생 여부 및 상황을 신속히 파악하고 대처하여 이더리움 생태계를 지속적으로 관리할 책임과 필요성이 높아지고 있다.

[0005] 또한, 가상화폐에 대한 전세계적인 활용 증가 추세를 고려하면, 다양한 국가의 사정에 맞는 규제와 법률이 적용되어야 할 필요성이 높음에도 이더리움 등의 블록체인 시스템에 대한 규제 또는 제어를 위한 도구는 아직 제대로 마련되지 않은 실정이다.

[0006] 본원의 배경이 되는 기술은 한국공개특허공보 제10-2019-0048227호에 개시되어 있다.

발명의 내용

해결하려는 과제

[0007] 본원은 전술한 종래 기술의 문제점을 해결하기 위한 것으로서, 이더리움 등의 블록체인 시스템에서 제공되는 스마트 컨트랙트에 대한 소스코드 분석, 상태 값 정보 추출 등을 통해 사용자가 쉽게 이해할 수 있도록 스마트 컨트랙트에 대한 정보를 제공하는 스마트 컨트랙트에 대한 관제 장치 및 방법을 제공하는 것을 목적으로 한다.

[0008] 본원은 전술한 종래 기술의 문제점을 해결하기 위한 것으로서, 이더리움 등의 블록체인 시스템에서 제공되는 복수의 스마트 컨트랙트의 이상 상황 또는 악의적인 사용을 감지하여 즉각적인 조치가 가능하도록 하는 스마트 컨트랙트에 대한 관제 장치 및 방법을 제공하는 것을 목적으로 한다.

[0009] 다만, 본원의 실시예가 이루고자 하는 기술적 과제는 상기된 바와 같은 기술적 과제들로 한정되지 않으며, 또 다른 기술적 과제들이 존재할 수 있다.

과제의 해결 수단

[0010] 상기한 기술적 과제를 달성하기 위한 기술적 수단으로서, 본원의 일 실시예에 따른 스마트 컨트랙트에 대한 관제 방법은, 발행된 스마트 컨트랙트의 소스코드를 파싱하여 상기 스마트 컨트랙트와 연계된 변수를 추출하는 단계, 상기 스마트 컨트랙트의 주소 정보에 기초하여 상기 스마트 컨트랙트와 연계된 상태값을 추출하는 단계, 추출된 상기 변수 및 상기 상태값을 매핑하는 단계 및 매핑된 상기 변수 및 상기 상태값을 시각화하여 표시하는 단계를 포함할 수 있다.

[0011] 또한, 상기 변수를 추출하는 단계는, 상기 소스코드에 대한 파싱 결과에 기초하여 추상 구문 트리를 생성하는 단계 및 상기 추상 구문 트리에 기초하여 상기 스마트 컨트랙트와 연계된 변수 각각의 데이터 유형 및 변수명을 추출하는 단계를 포함할 수 있다.

[0012] 또한, 상기 상태값을 추출하는 단계는, 상기 스마트 컨트랙트의 주소 정보에 기초하여 Blockchain API를 통해 부호화된 데이터를 획득하는 단계 및 상기 부호화된 데이터를 상기 상태값으로 변환하는 단계를 포함할 수 있다.

[0013] 또한, 상기 표시하는 단계는, 매핑된 상기 변수 및 상기 상태값을 타임라인 형태로 표시하되, 상기 타임라인 상에는 상기 상태값이 변화한 시점에 대응하는 지점이 상기 상태값이 유지된 영역과 구분되도록 표시될 수 있다.

[0014] 또한, 상기 표시하는 단계는, 소정의 변수에 대한 시간에 따른 상태값 변화를 나타낸 그래프 형태로 매핑된 상기 변수 및 상기 상태값을 표시할 수 있다.

[0015] 또한, 본원의 일 실시예에 따른 스마트 컨트랙트에 대한 관제 방법은, 상기 스마트 컨트랙트의 이상을 탐지하는 단계를 포함할 수 있다.

[0016] 또한, 상기 이상을 탐지하는 단계는, 기 학습된 인공 지능 알고리즘에 기초하여 상기 상태값의 변화 패턴이 비정상적인 것으로 판단되는 경우 이상을 탐지할 수 있다.

[0017] 또한, 상기 이상을 탐지하는 단계는, 복수의 발행된 스마트 컨트랙트 각각에 대하여 수행되는 것일 수 있다.

[0018] 또한, 본원의 일 실시예에 따른 스마트 컨트랙트에 대한 관제 방법은, 소정의 상기 스마트 컨트랙트에 대한 이상이 탐지된 경우, 경고 및 알림 신호를 생성하는 단계를 포함할 수 있다.

[0019] 한편, 본원의 일 실시예에 따른 스마트 컨트랙트에 대한 관제 장치는, 발행된 스마트 컨트랙트의 소스코드를 파싱하여 상기 스마트 컨트랙트와 연계된 변수를 추출하는 변수 추출부, 상기 스마트 컨트랙트의 주소 정보에 기초하여 상기 스마트 컨트랙트와 연계된 상태값을 추출하는 상태 추출부, 추출된 상기 변수 및 상기 상태값을 매핑하는 매핑부 및 매핑된 상기 변수 및 상기 상태값을 시각화하여 표시하는 표시부를 포함할 수 있다.

[0020] 또한, 상기 변수 추출부는, 상기 소스코드에 대한 파싱 결과에 기초하여 추상 구문 트리를 생성하고, 상기 추상 구문 트리에 기초하여 상기 스마트 컨트랙트와 연계된 변수 각각의 데이터 유형 및 변수명을 추출할 수 있다.

[0021] 또한, 상기 상태 추출부는, 상기 스마트 컨트랙트의 주소 정보에 기초하여 Blockchain API를 통해 부호화된 데이터를 획득하고, 상기 부호화된 데이터를 상기 상태값으로 변환할 수 있다.

[0022] 또한, 본원의 일 실시예에 따른 스마트 컨트랙트에 대한 관제 장치는, 기 학습된 인공 지능 알고리즘에 기초하여 적어도 하나 이상의 스마트 컨트랙트에 대하여 상기 상태값의 변화 패턴이 비정상적인 것으로 판단되는 경우 해당 스마트 컨트랙트의 이상을 탐지하는 이상 탐지부를 포함할 수 있다.

[0023] 상술한 과제 해결 수단은 단지 예시적인 것으로서, 본원을 제한하려는 의도로 해석되지 않아야 한다. 상술한 예시적인 실시예 외에도, 도면 및 발명의 상세한 설명에 추가적인 실시예가 존재할 수 있다.

발명의 효과

[0024] 전술한 본원의 과제 해결 수단에 의하면, 이더리움 등의 블록체인 시스템에서 제공되는 스마트 컨트랙트에 대한 소스코드 분석, 상태 값 정보 추출 등을 통해 사용자가 쉽게 이해할 수 있도록 스마트 컨트랙트에 대한 정보를 제공하는 스마트 컨트랙트에 대한 관제 장치 및 방법을 제공할 수 있는 효과가 있다.

[0025] 전술한 본원의 과제 해결 수단에 의하면, 스마트 컨트랙트에 대한 정보를 그래프, 타임라인 형태 등으로 시각화하여 제공함으로써, 사용자가 용이하게 스마트 컨트랙트의 상태를 확인할 수 있다.

[0026] 전술한 본원의 과제 해결 수단에 의하면, 이더리움 등의 블록체인 시스템에서 제공되는 복수의 스마트 컨트랙트의 이상 상황 또는 악의적인 사용을 감지하여 즉각적인 조치가 가능하며 지속적인 추적이 가능하도록 하는 스마트 컨트랙트에 대한 관제 장치 및 방법을 제공할 수 있다.

[0027] 전술한 본원의 과제 해결 수단에 의하면, 개발자, 사용자 등의 여러 이해관계자들에게 스마트 컨트랙트에 대한 다양한 상태 정보를 제공하여 스마트 컨트랙트 동작에 대한 이해도를 높임으로써, 개발자는 다음 스마트 컨트랙트 개발 시 향상된 품질의 스마트 컨트랙트를 제작하도록 유도하고, 사용자는 모니터링 정보를 기반으로 하여 신뢰도 및 안정성이 향상된 거래를 수행하도록 할 수 있다.

[0028] 다만, 본원에서 얻을 수 있는 효과는 상기된 바와 같은 효과들로 한정되지 않으며, 또 다른 효과들이 존재할 수 있다.

도면의 간단한 설명

[0029] 도 1은 본원의 일 실시예에 따른 스마트 컨트랙트에 대한 관제 장치를 포함하는 블록체인 관제 시스템의 개략적인 구성도이다.

도 2는 Blockchain API를 통해 스마트 컨트랙트에 대한 상태값을 추출하는 것을 설명하기 위한 개념도이다.

도 3은 Level DB를 통해 스마트 컨트랙트에 대한 상태값을 추출하는 것을 설명하기 위한 개념도이다.

도 4는 추출된 변수 및 상태값을 매핑하는 것을 설명하기 위한 개념도이다.

도 5는 본원의 일 실시예에 따른 매핑된 변수 및 상태값을 타임라인 형태로 표시하는 화면을 나타낸 도면이다.

도 6은 본원의 일 실시예에 따른 매핑된 변수 및 상태값을 포함하여 스마트 컨트랙트와 연계된 정보를 표시하는 화면을 나타낸 도면이다.

도 7은 본원의 일 실시예에 따른 스마트 컨트랙트에 대한 관제 장치가 복수의 발행된 스마트 컨트랙트 중 비정상적인 것으로 판단된 스마트 컨트랙트에 대한 이상을 탐지하는 것을 설명하기 위한 도면이다.

도 8은 본원의 일 실시예에 따른 스마트 컨트랙트에 대한 관제 장치의 개략적인 구성도이다.

도 9는 본원의 일 실시예에 따른 스마트 컨트랙트에 대한 관제 방법의 동작 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0030] 아래에서는 첨부한 도면을 참조하여 본원이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본원의 실시예를 상세히 설명한다. 그러나 본원은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본원을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0031] 본원 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결" 또는 "간접적으로 연결"되어 있는 경우도 포함한다.

[0032] 본원 명세서 전체에서, 어떤 부재가 다른 부재 "상에", "상부에", "상단에", "하에", "하부에", "하단에" 위치하고 있다고 할 때, 이는 어떤 부재가 다른 부재에 접해 있는 경우뿐 아니라 두 부재 사이에 또 다른 부재가 존재하는 경우도 포함한다.

[0033] 본원 명세서 전체에서, 어떤 부분이 어떤 구성 요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성 요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있는 것을 의미한다.

[0034] 본원은 스마트 컨트랙트에 대한 관제 장치 및 방법에 관한 것이다.

[0035] 도 1은 본원의 일 실시예에 따른 스마트 컨트랙트에 대한 관제 장치를 포함하는 블록체인 관제 시스템의 개략적인 구성도이다.

[0036] 도 1을 참조하면, 본원의 일 실시예에 따른 블록체인 관제 시스템(10)은, 스마트 컨트랙트가 배포되고, 사용자(20)에 의해 발생한 트랜잭션(Transaction)에 의해 배포된 스마트 컨트랙트가 변동되는 블록 체인(Blockchain) 영역과 스마트 컨트랙트에 대한 관제 장치(100)를 포함하고 배포된 스마트 컨트랙트에 대한 모니터링이 이루어

지는 관제(Monitoring) 영역을 포함할 수 있다.

[0037] 본원에서의 '스마트 컨트랙트'는 블록체인 기술을 이용하여 대금 결제, 송금 등의 금융거래뿐만 아니라 임의의 유형의 계약을 처리할 수 있도록 확장된 것을 의미할 수 있다. 달리 말해, 스마트 컨트랙트는 코드를 활용한 디지털 계약서로 이해될 수 있으며, 계약 조건이 충족되면 코드 순서대로 계약이 자동적으로 이행될 수 있다. 특히, 본원에서의 스마트 컨트랙트는 가상화폐의 유형 중 스마트 컨트랙트의 개념을 가장 활발히 적용한 이더리움(Ethereum)을 대상으로 하는 것일 수 있으나, 이에만 한정되는 것은 아니고 블록체인을 통해 임의의 계약 기능을 제공하는 종래의 공지되었거나 향후 개발되는 모든 가상화폐 유형, 플랫폼 등(예를 들면, 넥스레저(NexLedger) 등)에 적용되는 것일 수 있다.

[0038] 특히, 이더리움을 대상으로 하는 스마트 컨트랙트는 Solidity 코드를 컴파일 한 Bytecode의 형태로 블록체인 네트워크(이더리움 네트워크)에 배포될 수 있으며, 사용자(네트워크 참여자)는 배포된 스마트 컨트랙트를 활용하여 거래를 진행할 수 있다.

[0039] 이하에서는, 도 2 내지 도 6을 참조하여, 본원의 일 실시예에 따른 스마트 컨트랙트에 대한 관제 장치(100)가 스마트 컨트랙트에 대한 소스코드 분석, 상태 값 정보 추출 등을 통해 배포된 스마트 컨트랙트에 대한 정보를 획득(분석)하고 이를 사용자에게 제공하는 실시예에 관하여 상세히 서술하도록 한다.

[0040] 본원의 일 실시예에 따른 스마트 컨트랙트에 대한 관제 장치(100)(이하, '관제 장치(100)'라 한다.)는, 발행된 스마트 컨트랙트의 소스코드를 파싱하여 스마트 컨트랙트와 연계된 변수(1)를 추출할 수 있다.

[0041] 참고로, 본원의 일 실시예에 따른 스마트 컨트랙트의 소스코드는 해당 스마트 컨트랙트의 배포를 위하여 Bytecode 형태로 컴파일된 Solidity 코드를 의미하는 것일 수 있다. 실시예에 따라, 본원에서의 소스코드는 실행 코드(Execution Code) 등으로 달리 지칭될 수 있다.

[0042] 본원의 일 실시예에 따르면, 관제 장치(100)는 Antlr-js 등의 솔리디티 파서(Solidity Parser)를 활용하여 소스코드를 파싱할 수 있다.

[0043] 구체적으로 본원의 일 실시예에 따르면, 관제 장치(100)는 소스코드에 대한 파싱 결과에 기초하여 추상 구문 트리(Abstract Syntax Tree, AST)를 생성할 수 있다. 또한, 관제 장치(100)는 생성된 추상 구문 트리에 기초하여 스마트 컨트랙트와 연계된 변수(1) 각각의 데이터 유형(1a) 및 변수명(1b)를 추출할 수 있다.

[0044] 또한, 관제 장치(100)는 스마트 컨트랙트의 주소 정보에 기초하여 스마트 컨트랙트와 연계된 상태값(2)을 추출할 수 있다. 여기서, 스마트 컨트랙트와 연계된 상태값(2)이란, 배포된 스마트 컨트랙트의 전역 변수(global variable)에 대하여 할당된 값을 의미하는 것일 수 있다.

[0045] 도 2는 Blockchain API를 통해 스마트 컨트랙트에 대한 상태값을 추출하는 것을 설명하기 위한 개념도이다.

[0046] 도 2를 참조하면, 본원의 일 실시예에 따른 관제 장치(100)는 스마트 컨트랙트의 주소 정보에 기초하여 Blockchain API를 통해 부호화된 데이터(Encoded data, 2')를 획득할 수 있다. 또한, 관제 장치(100)는 부호화된 데이터(2')를 상태값(2)으로 변환할 수 있다. 여기서, API는 본원에서의 스마트 컨트랙트와 연계된 블록체인 네트워크에서 활용 가능한 Application Programming Interface를 지칭하는 것으로, API에 관한 사항은 통상의 기술자에게 자명한 것이므로 구체적인 설명은 생략한다.

[0047] 또한, 실시예에 따라 관제 장치(100)는 스마트 컨트랙트의 주소 정보에 기초하여 getStorageAt 함수를 통해 부호화된 데이터(Encoded data, 2')를 획득하도록 구현될 수 있다. 참고로, getStorageAt 함수는 스마트 컨트랙트의 상태값과 관련하여 EVM 메모리 구조에 적합한 16진수의 형태로 변환된 부호화된 데이터(예를 들면, 0Xfab242534234030001 등의 형태)를 출력하는 함수일 수 있다. 아울러, getStorageAt 함수를 통해 부호화된 데이터(2')를 획득하는 방식은 본원이 적용되는 블록 체인의 유형이 이더리움과 연계된 것일 때 특히 활용될 수 있다.또한, 부호화된 데이터(2')에 대한 상태값(2)으로의 변환과 관련하여, 본원의 일 실시예에 따른 관제 장치(100)는 획득된 부호화된 데이터(Encoded data, 2')(달리 말해, 부호화된 값)을 가져오고, 파서에 의해 추출한 데이터를 활용하여 부호화된 데이터(2')를 상태값(2)으로 변환하는 것일 수 있다.

[0048] 도 3은 Level DB를 통해 스마트 컨트랙트에 대한 상태값을 추출하는 것을 설명하기 위한 개념도이다.

[0049] 도 3을 참조하면, 본원의 다른 실시예에 따른 관제 장치(100)는 스마트 컨트랙트의 주소 정보에 기초하여 Level DB를 통해 상태값을 추출할 수 있다. 구체적으로, 본원의 다른 실시예에 따른 관제 장치(100)는 Geth에 의해 저장된 블록체인 Level DB를 복사할 수 있다. 또한, 관제 장치(100)는 복사된 Level DB(Replicated Level DB)로

부터 Storage Trie(예를 들어, 도 3의 Contract Storage Merkle Patricia Trie)를 추출할 수 있다. 또한, 관제 장치(100)는 추출된 Storage Trie에 RLP 디코딩(RLP Decode)을 수행하여 부호화된 데이터(Encoded data, 2')를 획득할 수 있다. 또한, 관제 장치(100)는 부호화된 데이터(2')를 상태값(2)으로 변환할 수 있다.

[0050] 참고로, Level DB는 오픈 소스(Open-Source) 기반 온-디스크(on-disk) 키/밸류 저장소일 수 있다. 구체적으로, Level DB는 키값 및 밸류값을 임의의 바이트 배열로 저장하고, 데이터가 키별로 정렬되어 저장되는 특징을 갖는 데이터베이스일 수 있다. 또한, Geth는 Go 언어로 개발된 이더리움 기반의 블록체인 클라이언트 소프트웨어(Goetherium)를 의미할 수 있다. 또한, 상기의 Storage Trie는 스마트 컨트랙트의 상태(예를 들면, 변수의 값)를 저장하는 머클 패트리샤 트리(Merkle Patricia Trie)일 수 있다. 이러한, Stroage Trie는 이더리움의 경우 솔리디티 코드의 전역 변수(global variable)를 저장할 수 있다. 또한, 상술한 RLP는 이더리움 등에서 상태, 트랙잭션 정보 등이 머클 패트리샤 트리에 키(Key)/밸류(Value) 형태로 저장되는 경우, 밸류(Value) 주소와 연계된 여러 정보들을 직렬화하여 삽입하기 위하여 사용되는 인코딩/디코딩 방법을 지칭하는 것일 수 있다.

[0051] 또한, 관제 장치(100)는 추출된 변수(1) 및 상태값(2)을 매핑할 수 있다.

[0052] 도 4는 추출된 변수 및 상태값을 매핑하는 것을 설명하기 위한 개념도이다.

[0053] 도 4를 참조하면, 본원의 일 실시예에 따른 관제 장치(100)는 추출된 변수(1) 각각에 대하여 변수(1)와 추출된 상태값(2) 간의 대응 관계를 매핑을 통해 파악할 수 있다. 예시적으로 도 4를 참조하면, 관제 장치(100)는 제1 변수인 이름(데이터 유형: String, 변수명: name)에 대응되는 상태값인 'Hong'을 제1 변수에 대하여 매핑하고, 제2 변수인 나이(데이터 유형: int, 변수명: age)에 대응되는 상태값인 '28'을 제2 변수에 대하여 매핑하도록 동작할 수 있다.

[0054] 본원의 일 실시예에 따르면, 관제 장치(100)는 도 4와 같이 매핑된 변수(1)와 상태값(2)을 등호(=)를 통해 대응 관계를 표시한 테이블 형태로 매핑 결과를 도출하여 저장할 수 있으나, 이에만 한정되는 것은 아니다. 본원의 일 실시예에 따르면, 매핑 결과가 저장되는 테이블은 복수의 슬롯(Slot)을 포함하고, 각각의 슬롯(Slot)의 크기는 256bit일 수 있다. 이 때, 관제 장치(100)는 추출된 변수(1)의 데이터 유형(1a)에 따라 매핑된 상태값(2)을 하나 이상의 슬롯(Slot)에 할당할 수 있다.

[0055] 예를 들어, 관제 장치(100)는 추출된 변수(1)의 데이터 유형(1a)이 int인 경우, int 형의 변수(1)는 256bit이므로 하나의 슬롯(Slot)에 매핑된 상태값(2)이 저장할 수 있다. 이와 달리, 변수(1)의 데이터 유형(1a)이 int64인 경우, int64 형의 변수(1)는 64bit를 사용하므로, 관제 장치(100)는 4개의 int64 형의 상태값(2)을 하나의 슬롯(Slot)에 저장하여 관리하도록 동작할 수 있다.

[0056] 또한, 관제 장치(100)는 매핑된 변수(1) 및 상태값(2)을 시각화하여 표시할 수 있다. 본원의 일 실시예에 따르면, 관제 장치(100)는 매핑된 변수(1) 및 상태값(2)을 시각화한 화면을 출력(표시)하는 디스플레이 모듈을 구비하여 구비된 디스플레이 모듈을 통해 매핑된 변수(1) 및 상태값(2)을 시각화한 화면을 출력하도록 동작할 수 있으나, 이에만 한정되는 것은 아니다. 다른 예로, 관제 장치(100)는 매핑된 변수(1) 및 상태값(2)에 대한 시각화 결과 정보를 별도의 사용자 단말(미도시)로 전송하고, 시각화 결과 정보를 수신한 사용자 단말에 구비된 디스플레이 상에서 해당 매핑된 변수(1) 및 상태값(2)을 시각화한 화면이 출력되도록 구현될 수 있다.

[0057] 도 5는 본원의 일 실시예에 따른 매핑된 변수 및 상태값을 타임라인 형태로 표시하는 화면을 나타낸 도면이다.

[0058] 도 5를 참조하면, 관제 장치(100)는 매핑된 변수(1) 및 상태값(2)을 타임라인 형태로 표시할 수 있다. 여기서, 관제 장치(100)에 의해 생성된 타임라인 상에는 상태값(2)이 변화한 시점(예를 들어, 해당 스마트 컨트랙트의 상태가 임의의 사용자에 의한 트랜잭션(Transaction)에 의해 변동된 시점)에 대응하는 지점이 상태값(2)이 변화하지 않고 유지된 다른 영역과 구분되도록 표시될 수 있다.

[0059] 본원의 일 실시예에 따르면, 타임라인 형태의 화면은 시간의 흐름을 가로 축으로 하는 막대 형태로 구비(블록의 시간 순 배열)되고, 상태값(2)이 변화한 시점에 대응하는 막대 내의 소정의 위치에 다른 영역과 구분되게 식별될 수 있는 식별 표지(예를 들면, 도형 형태, 색상 변화, 마크 등)가 삽입될 수 있다. 사용자가 타임라인 형태의 화면에서 관제 장치(100) 또는 시각화 화면을 출력하는 별도의 사용자 단말(미도시)에 소정의 식별 표지를 선택하는 사용자 입력을 인가(예를 들어, 식별 표지를 클릭하거나 터치하는 등의 동작)하는 경우, 해당 식별 표지에 대응하는 스마트 컨트랙트의 상태값 변화 정보가 표시될 수 있다.

[0060] 본원의 일 실시예에 따르면, 스마트 컨트랙트의 상태값 변화 정보는 현재 블록 번호(Block Number), Tx 정보, 상태값이 변화하기 이전의 블록(PreBlock)에 포함된 상태값 정보, 상태값이 변화한 후의 블록(CurrentBlock)에

포함된 상태값 정보 등을 포함할 수 있다. 다만, 이에만 한정되는 것은 아니며, 스마트 컨트랙트의 상태 변화와 연계된 다양한 정보가 표시되도록 구현될 수 있다.

[0061] 예시적으로 도 5를 참조하면, 관제 장치(100)가 사용자가 마우스 커서를 갖다대거나 클릭한 식별 표지에 대응하는 상태값 변화 정보를 제공함으로써, 사용자는 스마트 컨트랙트의 상태값 중 제1변수인 이름과 관련하여 기존 블록에서는 'Kim' 이었다가 해당 식별 표지에 대응하는 시점에 변화하여 현재 블록에서는 'Hong'으로 변동되었음을 확인할 수 있고, 제2변수인 나이와 관련하여 기존 블록에서는 '10'이었다가 해당 식별 표지에 대응하는 시점에 변화하여 현재 블록에서는 '28'로 변동되었음을 확인할 수 있다.

[0062] 또한, 본원의 일 실시예에 따르면, 관제 장치(100)는 소정의 변수에 대한 시간에 따른 상태값 변화를 나타낸 그래프 형태로 매핑된 변수(1) 및 상태값(2)을 표시할 수 있다. 예를 들어, 사용자가 관제 장치(100) 또는 시각화된 화면을 출력하는 별도의 사용자 단말(미도시)에 소정의 변수(1)를 선택하는 사용자 입력을 인가하는 경우, 선택된 변수(1)에 대한 매핑된 상태값(2)의 시간에 따른 변화 추이를 나타내는 그래프가 관제 장치(100) 또는 사용자 단말(미도시)에 표시되도록 구현될 수 있다.

[0063] 도 6은 본원의 일 실시예에 따른 매핑된 변수 및 상태값을 포함하여 스마트 컨트랙트와 연계된 정보를 표시하는 화면을 나타낸 도면이다.

[0064] 도 6을 참조하면, 관제 장치(100)는 매핑된 변수(1) 및 상태값(2)을 포함하여 스마트 컨트랙트와 연계된 다양한 정보를 표시하는 화면을 관제 장치(100)의 디스플레이 모듈(예를 들면, 표시부(140))을 통해 출력하거나 스마트 컨트랙트와 연계된 다양한 정보를 표시하는 시각화 결과 정보를 사용자 단말(미도시)로 전송할 수 있다.

[0065] 본원의 일 실시예에 따르면, 매핑된 변수(1) 및 상태값(2)을 포함하는 스마트 컨트랙트와 연계된 정보 표시 화면에는, 스마트 컨트랙트 주소 정보(a), 스마트 컨트랙트의 컴파일러 버전 정보(b), 스마트 컨트랙트의 소스 코드(예를 들면, Solidity 코드) 정보(c), 스마트 컨트랙트의 전체 변수(1) 별 상태값(2) 정보(d), 스마트 컨트랙트의 숫자 타입의 데이터 유형을 가지는 소정의 변수(1)에 대한 상태값(2) 변화 추이 그래프(e), 문자 타입의 데이터 유형을 가지는 소정의 변수(1)에 대한 상태값(2) 변화 추이 그래프(f), 지역별 스마트 컨트랙트 사용 빈도 정보(g) 등이 포함될 수 있으나, 이에만 한정되는 것은 아니고, 변수 및 상태 변화, 트랜잭션 발생 정보, 사용 패턴, 함수별 사용 빈도, 가상화폐 수량(이더량) 변동 정보, 가상화폐 거래 정보 등 배포된 스마트 컨트랙트와 연계된 다양한 정보가 표시될 수 있다.

[0066] 이더리움을 통해 발행되는 스마트 컨트랙트의 경우, get 함수를 활용하여 사용자 등이 변수의 상태를 확인할 수 있지만, 이는 해당 변수가 발행(배포) 시에 Public으로 선언되었을 것을 전제 조건으로 하며, Public으로 선언되지 않은 변수의 경우 get function 기능을 활용해야 하나 이러한 방식의 경우 Tx를 발행해야 하므로 사용자 등에게 별도의 수수료 부담이 부과되는 한계가 있었다. 이와 달리, 본원의 관제 장치(100)는 스마트 컨트랙트에 대한 다양한 상태 정보를 사용자(20), 개발자(30) 등을 포함하는 여러 이해 관계인이 손쉽게 확인할 수 있도록 시각화하여 제공하는 이점이 있다.

[0067] 또한, 관제 장치(100)는 스마트 컨트랙트의 이상을 탐지할 수 있다. 본원의 일 실시예에 따르면, 관제 장치(100)는 기 학습된 인공 지능 알고리즘에 기초하여 소정의 변수(1)에 대한 상태값(2)의 변화 패턴이 비정상적인 것으로 판단되는 경우 이상을 탐지하도록 동작할 수 있다. 특히, 본원에서의 기 학습된 인공 지능 알고리즘은 Txs, Balance 등의 지표들을 활용하여 비정상적인 상황을 식별하도록 학습된 것일 수 있다.

[0068] 본원의 일 실시예에 따르면, 스마트 컨트랙트의 이상을 탐지하기 위한 기 학습된 인공 지능 알고리즘은 로지스틱 회귀 분석(Logistic Regression), 랜덤 포레스트(Random Forest), 딥 러닝(Deep Learning), 서포트 벡터 머신(Supprot Vector Machine, SVM), 인공신경망(Artificial Neural Network, ANN), 강화 학습(Reinforcement Learning) 등 종래에 공지되었거나 향후 개발되는 모든 종류의 기계 학습 방식을 통해 생성(학습)된 것일 수 있다.

[0069] 특히, 본원의 일 실시예에 따르면, 관제 장치(100)는 복수의 발행된 스마트 컨트랙트 각각에 대하여 이상을 탐지할 수 있다. 나아가, 관제 장치(100)는 소정의 스마트 컨트랙트에 대한 이상이 탐지된 경우, 경고 및 알림 신호를 생성할 수 있다. 블록체인 네트워크 상에 배포되고 트랜잭션에 의해 다양한 형태로 변동되는 스마트 컨트랙트 각각의 상태를 사람이 확인하고 전체 스마트 컨트랙트를 감시하는 것은 실질적으로 불가능에 가까운 일이다. 따라서, 본원의 관제 장치(100)는 스마트 컨트랙트 각각의 상태 정보(변수 및 변수에 대응되는 상태값의 변화)를 획득하고, 기 학습된 인공 지능 알고리즘을 활용하여 여러 스마트 컨트랙트에 대한 이상을 즉각적으로 탐지할 수 있다.

[0070] 본원의 일 실시예에 따르면, 관제 장치(100)에 의해 생성된 경고 및 알림 신호는 해당 스마트 컨트랙트와 연계된 사용자(20) 및 개발자(30) 중 적어도 하나의 단말로 전송될 수 있다. 또한, 관제 장치(100)는 해당 스마트 컨트랙트와 연계된 사용자(20) 및 개발자(30) 중 적어도 하나의 단말뿐만 아니라, 블록체인 네트워크와 관련된 이해관계인(예를 들면, 정부 관계자 등)의 단말에 함께 경고 및 알림 신호를 전송하도록 동작할 수 있다.

[0071] 도 7은 본원의 일 실시예에 따른 스마트 컨트랙트에 대한 관제 장치가 복수의 발행된 스마트 컨트랙트 중 비정상적인 것으로 판단된 스마트 컨트랙트에 대한 이상을 탐지하는 것을 설명하기 위한 도면이다.

[0072] 도 7을 참조하면, 본원의 일 실시예에 따른 관제 장치(100)는 예시적으로 복수의 스마트 컨트랙트(Smart Contract 1 내지 Smart Contract 9) 각각의 소정의 변수(1)(예를 들어, Balance, Txs, Term)에 대한 상태값(2) 변화 추이를 입력으로 하는 기 학습된 인공 지능 알고리즘에 기초하여 소정의 스마트 컨트랙트에 대한 이상을 탐지할 수 있다. 도 7을 참조하면, 예시적으로 Smart Contract 5에 대한 상태값(2)의 변화 패턴이 비정상적인 것으로 판단될 수 있다.

[0073] 본원의 일 실시예에 따르면, 관제 장치(100)에 의해 수행되는 스마트 컨트랙트에 대한 상태 정보 획득, 획득된 상태 정보에 대한 시각화 및 스마트 컨트랙트에 대한 이상 탐지 중 적어도 하나의 프로세스는 기 설정된 모니터링 주기 마다 반복적으로 수행되는 것일 수 있다. 예를 들어, 관제 장치(100)와 연계된 블록체인 네트워크 상에 새로운 블록이 연결될 때마다 전술한 프로세스가 수행되도록 구현될 수 있다.

[0074] 도 8은 본원의 일 실시예에 따른 스마트 컨트랙트에 대한 관제 장치의 개략적인 구성도이다.

[0075] 도 8을 참조하면, 관제 장치(100)는, 변수 추출부(110), 상태 추출부(120), 매핑부(130), 표시부(140) 및 이상 탐지부(150)를 포함할 수 있다.

[0076] 변수 추출부(110)는, 발행된 스마트 컨트랙트의 소스코드를 파싱하여 해당 스마트 컨트랙트와 연계된 변수(1)를 추출할 수 있다.

[0077] 본원의 일 실시예에 따르면, 변수 추출부(110)는, 소스코드에 대한 파싱 결과에 기초하여 추상 구문 트리(AST)를 생성하고, 생성된 추상 구문 트리(AST)에 기초하여 스마트 컨트랙트와 연계된 변수(1) 각각의 데이터 유형(1a) 및 변수명(1b)을 추출할 수 있다.

[0078] 상태 추출부(120)는, 스마트 컨트랙트의 주소 정보에 기초하여 스마트 컨트랙트와 연계된 상태값(2)을 추출할 수 있다.

[0079] 본원의 일 실시예에 따르면, 상태 추출부(120)는, 스마트 컨트랙트의 주소 정보에 기초하여 Blockchain API를 통해 부호화된 데이터(2', Encoded data)를 획득하고, 부호화된 데이터(2')를 상태값(2)으로 변환할 수 있다. 다만, 이에만 한정되는 것은 아니며, 실시예에 따라 상태 추출부(120)는, 스마트 컨트랙트의 주소 정보에 기초하여 getStorageAt 함수를 통해 부호화된 데이터(2', Encoded data)를 획득하도록 동작할 수 있다. 또 다른 예로, 상태 추출부(120)는, Level DB를 통해 상태값(2)을 추출할 수 있다.

[0080] 매핑부(130)는, 추출된 변수(1) 및 상태값(2)을 매핑할 수 있다.

[0081] 표시부(140)는, 매핑된 변수(1) 및 상태값(2)을 시각화하여 표시할 수 있다.

[0082] 본원의 일 실시예에 따르면, 변수 추출부(110), 상태 추출부(120), 매핑부(130) 및 표시부(140)를 포괄하여 관찰부(Observer) 등으로 달리 지칭할 수 있다

[0083] 이상 탐지부(150)는, 기 학습된 인공 지능 알고리즘에 기초하여 적어도 하나 이상의 스마트 컨트랙트에 대하여 상태값(2)의 변화 패턴이 비정상적인 것으로 판단되는 경우 해당 스마트 컨트랙트의 이상을 탐지할 수 있다. 실시예에 따라 이상 탐지부(150)는 분석부(Analyzer) 등으로 달리 지칭될 수 있다.

[0084] 이하에서는 상기에 자세히 설명된 내용을 기반으로, 본원의 동작 흐름을 간단히 살펴보기로 한다.

[0085] 도 9는 본원의 일 실시예에 따른 스마트 컨트랙트에 대한 관제 방법의 동작 흐름도이다.

[0086] 도 9에 도시된 스마트 컨트랙트에 대한 관제 방법은 앞서 관제 장치(100)에 의하여 수행될 수 있다. 따라서, 이하 생략된 내용이라고 하더라도 관제 장치(100)에 대하여 설명된 내용은 스마트 컨트랙트에 대한 관제 방법에 대한 설명에도 동일하게 적용될 수 있다.

[0087] 도 9를 참조하면, 단계 S910에서 변수 추출부(110)는, 발행된 스마트 컨트랙트의 소스코드를 파싱하여 스마트

컨트랙트와 연계된 변수(1)를 추출할 수 있다.

[0088] 구체적으로, 단계 S910에서 변수 추출부(110)는, 소스코드에 대한 파싱 결과에 기초하여 추상 구문 트리(AST)를 생성할 수 있다. 또한, 변수 추출부(110)는 생성된 추상 구문 트리(AST)에 기초하여 스마트 컨트랙트와 연계된 변수(1) 각각의 데이터 유형(1a) 및 변수명(1b)을 추출할 수 있다.

[0089] 다음으로, 단계 S920에서 상태 추출부(120)는, 스마트 컨트랙트의 주소 정보에 기초하여 스마트 컨트랙트와 연계된 상태값(2)을 추출할 수 있다.

[0090] 구체적으로, 단계 S920에서 상태 추출부(120)는, 스마트 컨트랙트의 주소 정보에 기초하여 Blockchain API를 통해 부호화된 데이터(2', Encoded data)를 획득하고, 부호화된 데이터(2')를 상태값(2)으로 변환할 수 있다. 다만, 이에만 한정되는 것은 아니며, 실시예에 따라 단계 S920에서 상태 추출부(120)는, 스마트 컨트랙트의 주소 정보에 기초하여 getStorageAt 함수를 통해 부호화된 데이터(2', Encoded data)를 획득하도록 구현될 수 있다. 또 다른 예로, 단계 S920에서 상태 추출부(120)는, 스마트 컨트랙트의 주소 정보에 기초하여 Level DB를 통해 상태값(2)을 추출할 수 있다.

[0091] 다음으로, 단계 S930에서 매핑부(130)는, 추출된 변수(1) 및 상태값(2)을 매핑할 수 있다.

[0092] 다음으로, 단계 S940에서 표시부(140)는, 매핑된 변수(1) 및 상태값(2)을 시각화하여 표시할 수 있다.

[0093] 본원의 일 실시예에 따르면, 단계 S940에서 표시부(140)는, 매핑된 변수(1) 및 상태값(2)을 타임라인 형태로 표시하되, 타임라인 상에는 상태값(2)이 변화한 시점에 대응하는 지점이 상태값(2)이 유지된 영역과 구분되도록 표시될 수 있다.

[0094] 또한, 본원의 일 실시예에 따르면, 단계 S940에서 표시부(140)는, 소정의 변수(1)에 대한 시간에 따른 상태값(2) 변화를 나타낸 그래프 형태로 매핑된 변수(1) 및 상태값(2)을 표시할 수 있다.

[0095] 다음으로, 단계 S950에서 이상 탐지부(150)는, 스마트 컨트랙트의 이상을 탐지할 수 있다.

[0096] 본원의 일 실시예에 따르면, 단계 S950은 복수의 발행된 스마트 컨트랙트 각각에 대하여 수행되는 것일 수 있다.

[0097] 또한, 본원의 일 실시예에 따르면, 단계 S950에서 이상 탐지부(150)는, 기 학습된 인공 지능 알고리즘에 기초하여 상태값(2)의 변화 패턴이 비정상적인 것으로 판단되는 경우 이상을 탐지할 수 있다.

[0098] 다음으로, 단계 S960에서 이상 탐지부(160)는, 소정의 스마트 컨트랙트에 대한 이상이 탐지된 경우, 경고 및 알림 신호를 생성할 수 있다.

[0099] 상술한 설명에서, 단계 S910 내지 S960은 본원의 구현예에 따라서, 추가적인 단계들로 더 분할되거나, 더 적은 단계들로 조합될 수 있다. 또한, 일부 단계는 필요에 따라 생략될 수도 있고, 단계 간의 순서가 변경될 수도 있다.

[0100] 본원의 일 실시 예에 따른 스마트 컨트랙트에 대한 관제 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 본 발명을 위하여 특별히 설계되고 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), 및 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 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0101] 또한, 전술한 스마트 컨트랙트에 대한 관제 방법은 기록 매체에 저장되는 컴퓨터에 의해 실행되는 컴퓨터 프로그램 또는 애플리케이션의 형태로도 구현될 수 있다.

[0102] 전술한 본원의 설명은 예시를 위한 것이며, 본원이 속하는 기술분야의 통상의 지식을 가진 자는 본원의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을

것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

[0103] 본원의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본원의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

[0104] 10: 블록체인 관제 시스템

20: 사용자

30: 개발자

100: 스마트 컨트랙트에 대한 관제 장치

110: 변수 추출부

120: 상태 추출부

130: 매핑부

140: 표시부

150: 이상 탐지부

1: 변수

1a: 데이터 유형

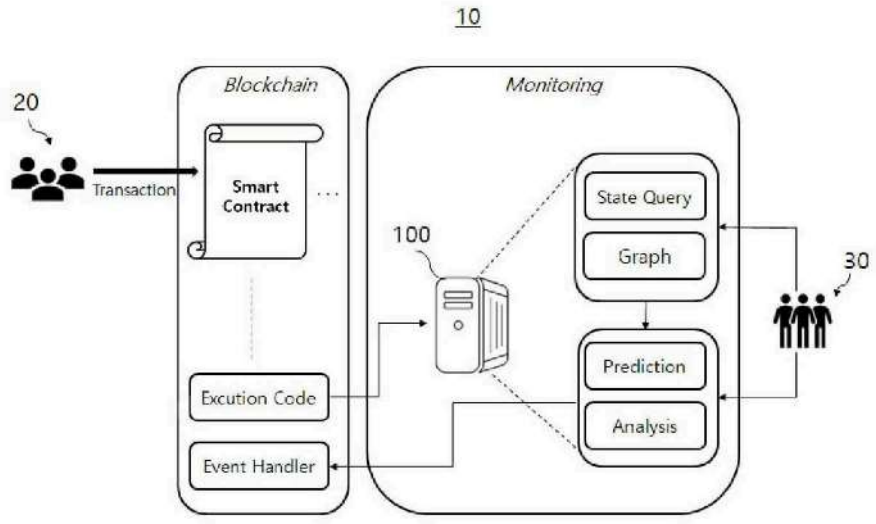
1b: 변수명

2: 상태값

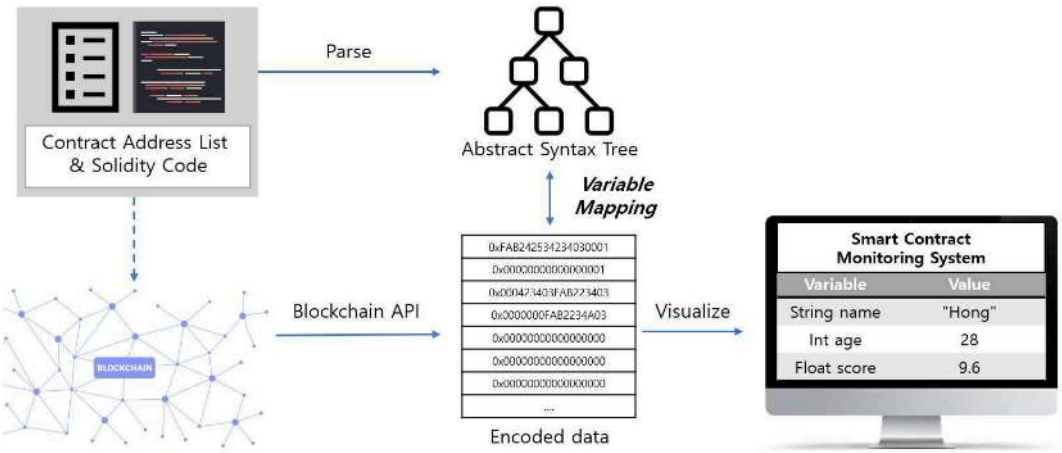
2': 부호화된 데이터

도면

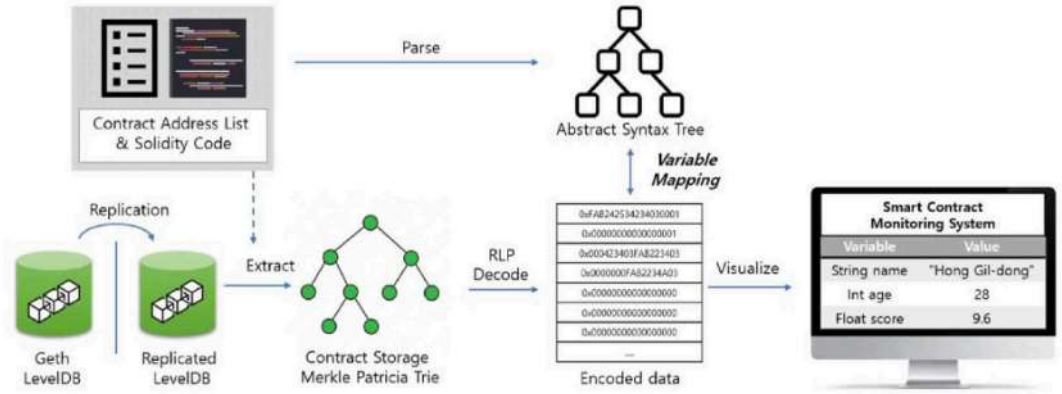
도면1



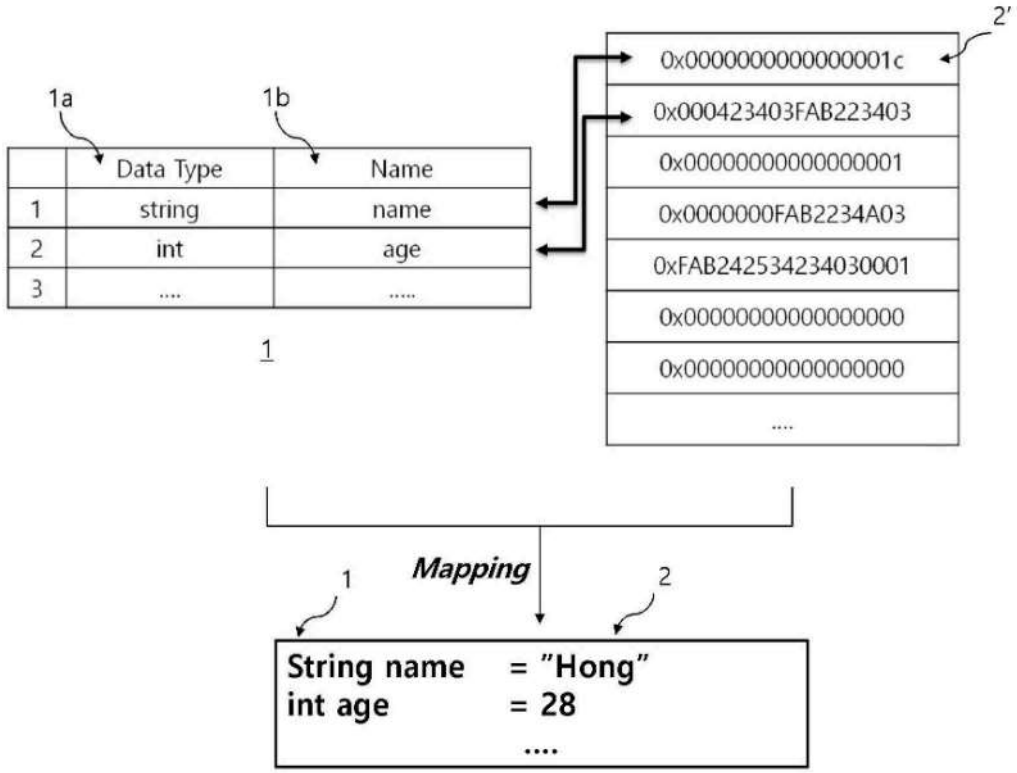
도면2


Contract Address List
& Solidity Code
Parse
Abstract Syntax Tree
Variable
Mapping
Blockchain API
Visualize
Encoded data
Smart Contract
Monitoring System
Variable
Value
String name
"Hong"
Int age
28
Float score
9.6

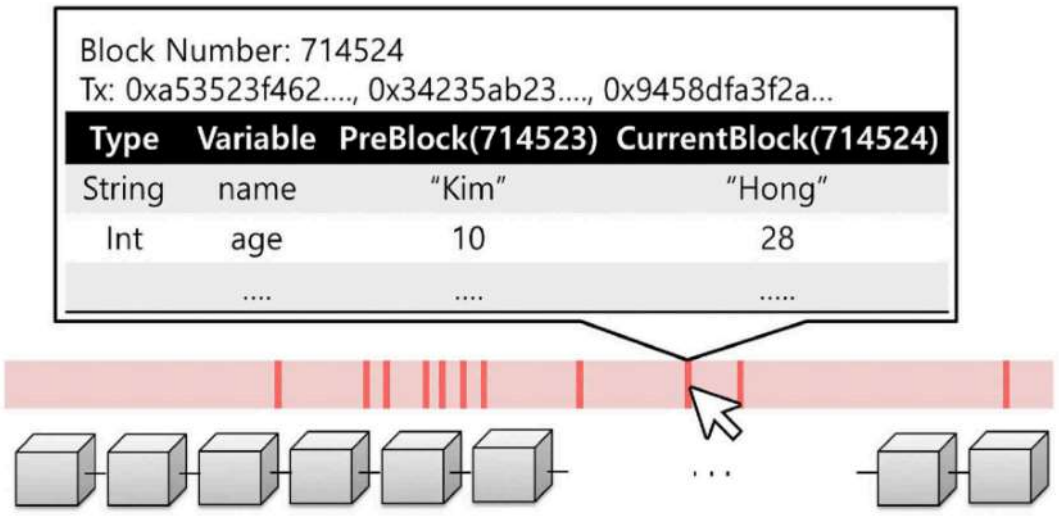
도면3


Contract Address List
& Solidity Code
Parse
Abstract Syntax Tree
Variable
Mapping
Replication
Extract
RLP
Decode
Visualize
Geth
LevelDB
Replicated
LevelDB
Contract Storage
Merkle Patricia Trie
Encoded data
Smart Contract
Monitoring System
Variable
Value
String name
"Hong Gil-dong"
Int age
28
Float score
9.6

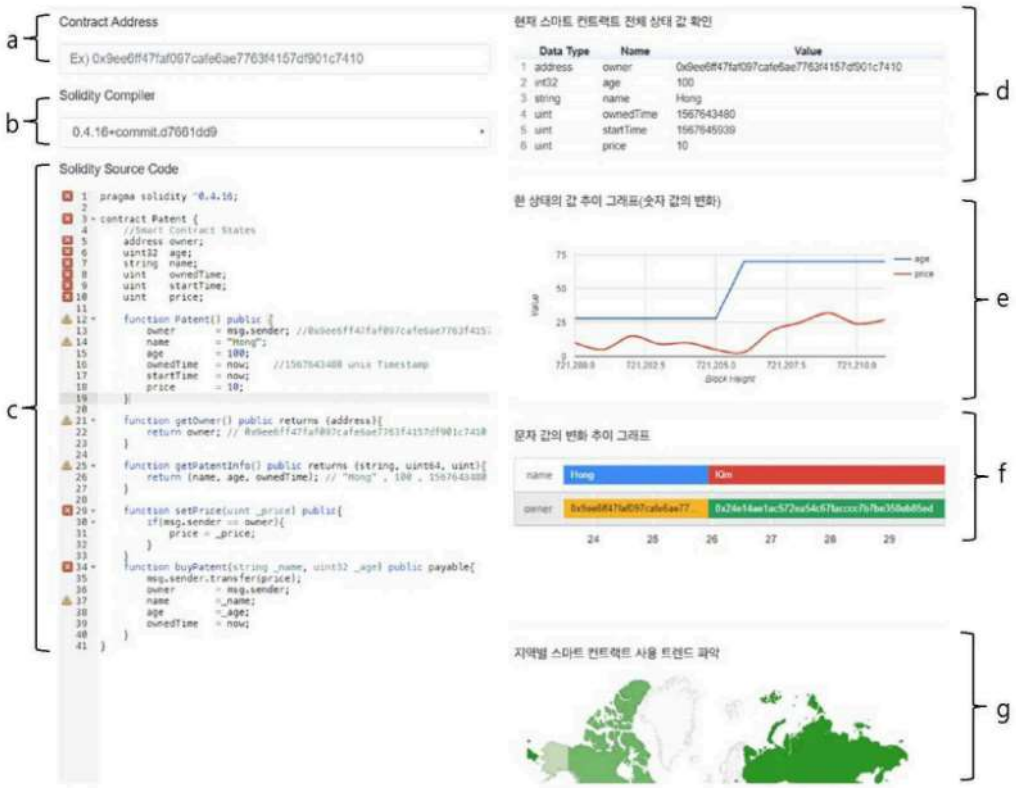
도면4


2'
0x000000000000001c
0x000423403FAB223403
0x0000000000000001
0x0000000FAB2234A03
0xFAB242534234030001
0x0000000000000000
0x0000000000000000
....
1a
1b
Data Type
Name
1
string
name
2
int
age
3
....
.....
1
Mapping
1
2
String name = "Hong"
int age = 28
....

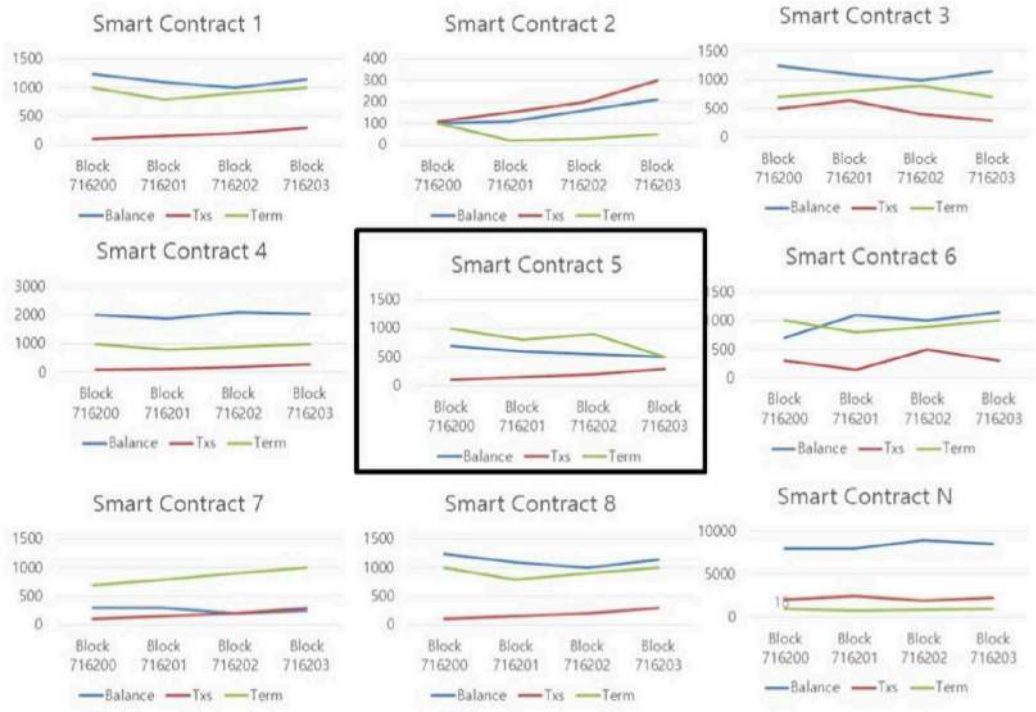
도면5


Block Number: 714524
Tx: 0xa53523f462...., 0x34235ab23...., 0x9458dfa3f2a...
Type
Variable
PreBlock(714523)
CurrentBlock(714524)
String
name
"Kim"
"Hong"
Int
age
10
28
....
....
.....

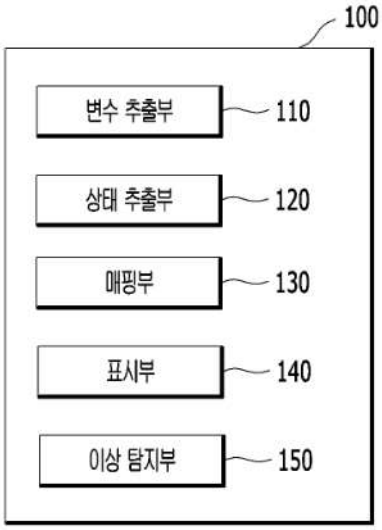
도면6


a
Contract Address
Ex) 0x9ee6ff47faf097cafe6ae7763f4157df901c7410
b
Solidity Compiler
0.4.16+commit.d7661dd9
c
Solidity Source Code
d
현재 스마트 컨트랙트 전체 상태 값 확인
Data Type
Name
Value
e
f
문자 값의 변화 추이 그래프
g
지역별 스마트 컨트랙트 사용 트렌드 파악

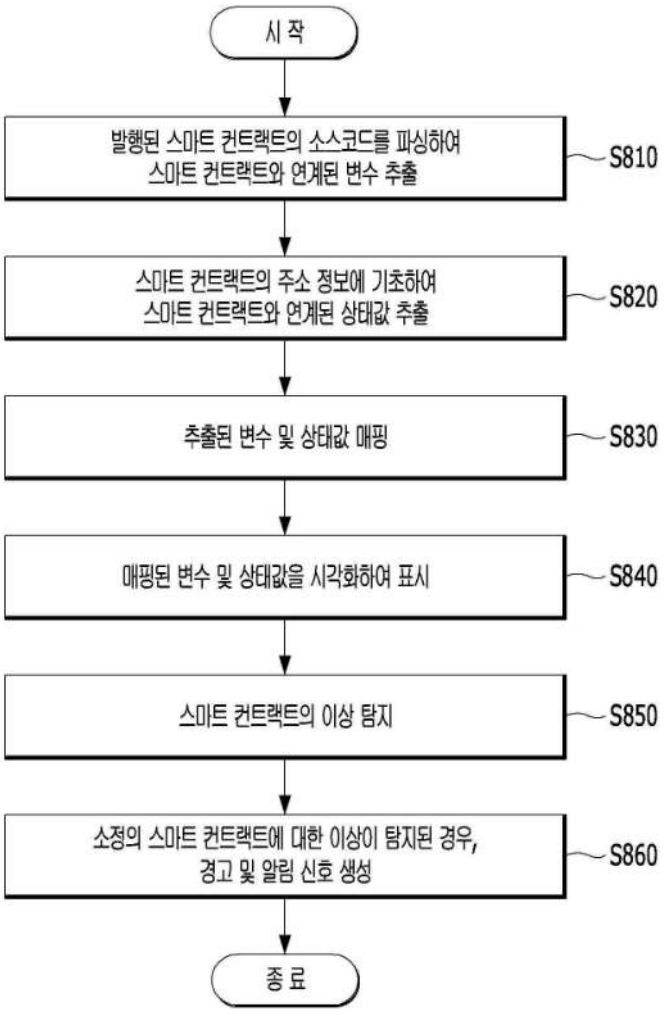
도면7


Smart Contract 1
Smart Contract 2
Smart Contract 3
Smart Contract 4
Smart Contract 5
Smart Contract 6
Smart Contract 7
Smart Contract 8
Smart Contract N
Block 716200
Block 716201
Block 716202
Block 716203
Balance
Txs
Term

도면8


100
변수 추출부
110
상태 추출부
120
매핑부
130
표시부
140
이상 탐지부
150

도면9


시 작
발행된 스마트 컨트랙트의 소스코드를 파싱하여
스마트 컨트랙트와 연계된 변수 추출
S810
스마트 컨트랙트의 주소 정보에 기초하여
스마트 컨트랙트와 연계된 상태값 추출
S820
추출된 변수 및 상태값 매핑
S830
매핑된 변수 및 상태값을 시각화하여 표시
S840
스마트 컨트랙트의 이상 탐지
S850
소정의 스마트 컨트랙트에 대한 이상이 탐지된 경우,
경고 및 알림 신호 생성
S860
종 료