



(19) 대한민국특허청(KR)  
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0123957  
(43) 공개일자 2024년08월16일

(51) 국제특허분류(Int. Cl.)  
G06F 21/62 (2013.01) G06F 8/41 (2018.01)  
H04L 9/40 (2022.01)  
(52) CPC특허분류  
G06F 21/6245 (2013.01)  
G06F 8/41 (2013.01)  
(21) 출원번호 10-2023-0016591  
(22) 출원일자 2023년02월08일  
심사청구일자 2023년02월08일

(71) 출원인  
충남대학교산학협력단  
대전광역시 유성구 대학로 99 (궁동, 충남대학교)  
(72) 발명자  
조은선  
대전광역시 유성구 어은로 57, 110동 1504호(어은  
동, 한빛아파트)  
김지수  
대전광역시 유성구 대학로 169, 301호  
(74) 대리인  
이은철, 김재문

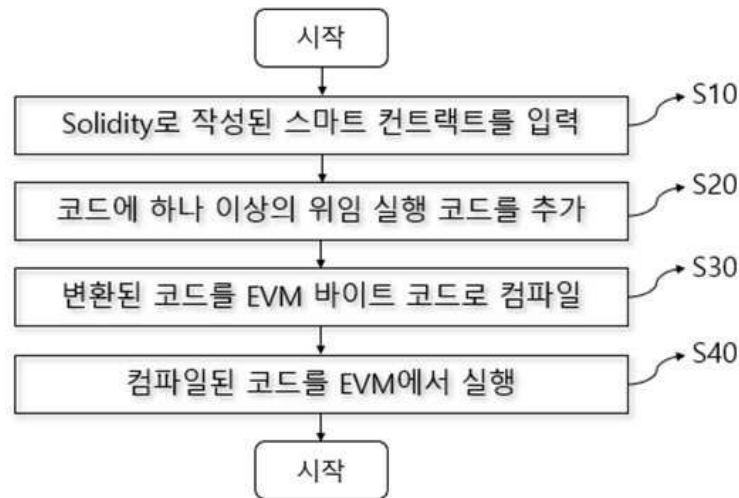
전체 청구항 수 : 총 7 항

(54) 발명의 명칭 동적 정책 기반 스마트 컨트랙트 개인정보보호 방법 및 시스템

(57) 요약

본 발명은, Solidity로 작성된 스마트 컨트랙트를 입력받는 (a)단계; 상기 스마트 컨트랙트 코드에 하나 이상의 위임 실행 코드를 추가하여 중간언어로 변환하는 (b)단계; 상기 중간언어 변환단계에서 변환된 코드를 EVM(Ethereum Virtual Machine) 바이트 코드로 컴파일하는 (c)단계; 및 상기 컴파일하는 단계에서 컴파일된 코드를 EVM에서 실행시키는 (d)단계;를 포함하는 것을 일 특징으로 한다.

대표도 - 도1



(52) CPC특허분류

**H04L 63/0428** (2013.01)

이 발명을 지원한 국가연구개발사업

|             |                                |
|-------------|--------------------------------|
| 과제고유번호      | 1711157470                     |
| 과제번호        | 2020R1A2C2008864               |
| 부처명         | 과학기술정보통신부                      |
| 과제관리(전문)기관명 | 한국연구재단                         |
| 연구사업명       | 개인기초연구(과기정통부)                  |
| 연구과제명       | 영지식 증명을 지원하는 스마트 컨트랙트 프레임워크 연구 |
| 기 여 율       | 1/1                            |
| 과제수행기관명     | 충남대학교                          |
| 연구기간        | 2020.03.01 ~ 2023.02.28        |

---

## 명세서

### 청구범위

#### 청구항 1

Solidity로 작성된 스마트 컨트랙트를 입력받는 (a)단계;

상기 스마트 컨트랙트 코드에 하나 이상의 위임 실행 코드를 추가하여 중간언어로 변환하는 (b)단계;

상기 중간언어 변환단계에서 변환된 코드를 EVM(Ethereum Virtual Machine) 바이트 코드로 컴파일하는 (c)단계;  
및

상기 컴파일하는 단계에서 컴파일된 코드를 EVM에서 실행시키는 (d)단계;

를 포함하는 동적 정책 기반 스마트 컨트랙트 개인정보보호 방법.

#### 청구항 2

제 1 항에 있어서,

상기 (b)단계는,

데이터 소유자를 나타내는 소유권 매개변수를 함수의 각 필드 및 각 인수에 첨부하는 (b-1)단계 및

코드를 타입 기반으로 분석하여 블록체인상에서 정보가 공개될 수 있는 코드에 공개식을 삽입하는 (b-2)단계를  
포함하는 것을 특징으로 하는 동적 정책 기반 스마트 컨트랙트 개인정보보호 방법.

#### 청구항 3

제 1 항에 있어서,

상기 (b)단계는,

상기 스마트 컨트랙트 코드를 암호화된 형태로 변환하는 것을 특징으로 하는 동적 정책 기반 스마트 컨트랙트  
개인정보보호 방법.

#### 청구항 4

제 1 항에 있어서,

상기 (a)단계 이후에 개인정보보호 정책을 기술한 JSON을 입력받는 (e)단계 및 JSON을 스마트 컨트랙트 내에서  
개인정보보호에 적용할 수 있도록 확장된 타입으로 결합하는 (f)단계를 더 포함하는 것을 특징으로 하는 동적  
정책 기반 스마트 컨트랙트 개인정보보호 방법.

#### 청구항 5

제 4 항에 있어서,

상기 (d)단계는,

컴파일된 코드에서 JSON으로 나타난 정책 파일을 인식하여 정보 접근 권한을 확인하는 것을 특징으로 하는 동적  
정책 기반 스마트 컨트랙트 개인정보보호 방법.

**청구항 6**

Solidity로 작성된 스마트 컨트랙트를 입력받는 입력부;  
 상기 스마트 컨트랙트 코드에 하나 이상의 위임 실행 코드를 추가하여 중간언어로 변환하는 변환부;  
 상기 변환부에서 변환된 코드를 EVM(Ethereum Virtual Machine) 바이트 코드로 컴파일하는 컴파일부; 및  
 상기 컴파일부에서 컴파일된 코드를 EVM에서 실행시키는 실행부;  
 를 포함하는 동적 정책 기반 스마트 컨트랙트 개인정보보호 시스템.

**청구항 7**

제 6 항에 있어서,  
 상기 변환부는,

데이터 소유자를 나타내는 소유권 매개변수를 함수의 각 필드 및 각 인수에 첨부하는 소유권 매개변수 첨부모듈 및 코드를 타입 기반으로 분석하여 블록체인상에서 정보가 공개될 수 있는 코드에 공개식을 삽입하는 공개식 삽입모듈을 포함하는 것을 특징으로 하는 동적 정책 기반 스마트 컨트랙트 개인정보보호 시스템.

**발명의 설명****기술 분야**

[0001] 본 발명은 스마트 컨트랙트 개인정보보호 방법 및 시스템에 관한 것으로서, 특히 블록체인 참여자에게 모든 데이터가 잠재적으로 공개되는 스마트 컨트랙트에서 프라이버시가 중요한 데이터들을 보호하기 위한 스마트 컨트랙트 개인정보보호 방법 및 시스템에 관한 것이다.

**배경 기술**

[0003] 블록체인 기술은 분산된 방식으로 데이터 저장을 약속한다. 데이터는, 블록들의 체인을 형성하는, 서로 선행 관계를 갖는 일련의 데이터 블록에 저장될 수 있다. 블록들의 체인은, 데이터를 블록들에 저장하기 전에 그 데이터의 유효성을 확인하는 것을 담당하는 노드들의 네트워크에 의해 유지된다. 노드들에 의해 사용되는 암호 및 합의 기술을 사용함으로써, 블록체인에 저장된 데이터가 거의 변경되지 않는다. 따라서, 노드들의 네트워크는 블록체인 합의 네트워크라고도 한다.

[0004] 최근 블록체인을 기반으로 하는 스마트 컨트랙트(Smart contract) 기술이 주목받고 있다. 스마트 컨트랙트란 블록체인을 기반으로 금융거래, 부동산 계약, 공증 등 다양한 형태의 계약을 체결하고 이행하는 것을 말하는 것으로 1994년에 제안되었다.

[0005] 스마트 컨트랙트는 블록체인에서 실행되지만, 이는 개인정보보호 관점에서 데이터에 잠재적으로 해를 끼칠 수 있다. 블록체인 위에서 구동되는 스마트 컨트랙트는 블록체인 참여자에게 모든 데이터가 잠재적으로 공개되므로, privacy가 중요한 데이터들은 스마트 컨트랙트에서 다루기 어렵다는 문제점이 있다.

[0006] 이와 같은 개인정보보호 문제를 해결하기 위해 스마트 컨트랙트에 개인정보보호 정책을 별도로 지원하는 시스템이 대두되고 있다. 개인정보보호 정책이 컴파일 시간에 제공되는 기술은 Zkay, ZeeStar, Stone 등에서 지원된다. 그러나 스마트 컨트랙트가 컴파일될 때 아직 개인정보보호 정책이 제공되지 않거나, 컴파일 시간과 런타임에 개인정보보호 정책이 달라지는 경우가 존재한다는 문제점이 있다. 따라서, 동적으로 변하는 개인정보보호 정책을 스마트 컨트랙트에서 지원할 수 있는 시스템이 요구되고 있는 실정이다.

**선행기술문헌****특허문헌**

[0008] (특허문헌 0001) 한국등록특허 제10-2021-0039691호

## 발명의 내용

### 해결하려는 과제

[0009] 본 발명은 스마트 컨트랙트가 컴파일될 때 개인정보보호 정책이 제공되지 않거나, 컴파일 시간과 런타임 중에 개인정보보호 정책이 변경되는 경우에도 프라이버시가 중요한 데이터를 보호할 수 있는 동적 정책 기반 스마트 컨트랙트 개인정보보호 방법 및 시스템을 제공하는 것을 목적으로 한다.

### 과제의 해결 수단

[0011] 상기 목적을 달성하기 위하여 본 발명은, Solidity로 작성된 스마트 컨트랙트를 입력받는 (a)단계; 상기 스마트 컨트랙트 코드에 하나 이상의 위임 실행 코드를 추가하여 중간언어로 변환하는 (b)단계; 상기 중간언어 변환단계에서 변환된 코드를 EVM(Ethereum Virtual Machine) 바이트 코드로 컴파일하는 (c)단계; 및 상기 컴파일하는 단계에서 컴파일된 코드를 EVM에서 실행시키는 (d)단계;를 포함하는 것을 일 특징으로 한다.

[0012] 바람직하게는, 상기 (b)단계는, 데이터 소유자를 나타내는 소유권 매개변수를 함수의 각 필드 및 각 인수에 첨부하는 (b-1)단계 및 코드를 타입 기반으로 분석하여 블록체인상에서 정보가 공개될 수 있는 코드에 공개식을 삽입하는 (b-2)단계를 포함할 수 있다.

[0013] 바람직하게는, 상기 (b)단계는, 상기 스마트 컨트랙트 코드를 암호화된 형태로 변환할 수 있다.

[0014] 바람직하게는, 상기 (a)단계 이후에 개인정보보호 정책을 기술한 JSON을 입력받는 (e)단계 및 JSON을 스마트 컨트랙트 내에서 개인정보보호에 적용할 수 있도록 확장된 타입으로 결합하는 (f)단계를 더 포함할 수 있다.

[0015] 바람직하게는, 상기 (d)단계는, 컴파일된 코드에서 JSON으로 나타난 정책 파일을 인식하여 정보 접근 권한을 확인할 수 있다.

[0016] 또한 본 발명은, Solidity로 작성된 스마트 컨트랙트를 입력받는 입력부; 상기 스마트 컨트랙트 코드에 하나 이상의 위임 실행 코드를 추가하여 중간언어로 변환하는 변환부; 상기 변환부에서 변환된 코드를 EVM(Ethereum Virtual Machine) 바이트 코드로 컴파일하는 컴파일부; 및 상기 컴파일부에서 컴파일된 코드를 EVM에서 실행시키는 실행부;를 포함하는 것을 다른 특징으로 한다.

[0017] 바람직하게는, 상기 변환부는, 데이터 소유자를 나타내는 소유권 매개변수를 함수의 각 필드 및 각 인수에 첨부하는 소유권 매개변수 첨부모듈 및 코드를 타입 기반으로 분석하여 블록체인상에서 정보가 공개될 수 있는 코드에 공개식을 삽입하는 공개식 삽입모듈을 포함할 수 있다.

### 발명의 효과

[0019] 본 발명은 스마트 컨트랙트의 life cycle 동안 개인정보보호 정책에 변화가 있는 경우에도 새로운 개인정보보호 정책에 따라 데이터 공개 범위가 변화되므로, 연속성을 잃지 않고 갱신된 개인정보보호 정책을 적용하여 프라이버시가 중요한 데이터를 보호할 수 있다는 이점이 있다.

### 도면의 간단한 설명

[0021] 도 1은 본 발명의 실시예에 따른 동적 정책 기반 스마트 컨트랙트 개인정보보호 방법의 흐름도를 나타낸다.

도 2는 본 발명의 실시예에 따른 (b)단계의 흐름도를 나타낸다.

도 3은 본 발명의 실시예에 따른 (e)단계와 (f)단계가 포함된 동적 정책 기반 스마트 컨트랙트 개인정보보호 방법의 흐름도를 나타낸다.

도 4는 본 발명의 실시예에 따른 동적 정책 기반 스마트 컨트랙트 개인정보보호 시스템의 구성도를 나타낸다.

### 발명을 실시하기 위한 구체적인 내용

- [0022] 이하, 첨부된 도면들에 기재된 내용들을 참조하여 본 발명을 상세히 설명한다. 다만, 본 발명이 예시적 실시 예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일 참조부호는 실질적으로 동일한 기능을 수행하는 부재를 나타낸다.
- [0023] 본 발명의 목적 및 효과는 하기의 설명에 의해서 자연스럽게 이해되거나 보다 분명해 질 수 있으며, 하기의 기재만으로 본 발명의 목적 및 효과가 제한되는 것은 아니다. 또한, 본 발명을 설명함에 있어서 본 발명과 관련된 공지 기술에 대한 구체적인 설명이, 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다.
- [0024] 도 1은 본 발명의 실시예에 따른 동적 정책 기반 스마트 컨트랙트 개인정보보호 방법의 흐름도를 나타낸다. 도 1을 참조하면, 동적 정책 기반 스마트 컨트랙트 개인정보보호 방법은 (a)단계, (b)단계, (c)단계, (d)단계, (e)단계 및 (f)단계를 포함할 수 있다.
- [0025] 스마트 컨트랙트는 블록체인 위에서 구동되는 경우 블록체인 참여자에게 모든 데이터가 공개되므로 프라이버시가 중요한 데이터들을 다루기에는 어려움이 있다. 이를 해결하기 위해, 스마트 컨트랙트에 개인정보보호 정책을 별도로 지원하는 요구가 있었다. Zkay, ZeeStar, Stone 등은 컴파일 시간에 개인정보보호 정책을 제공한다. 그러나, 스마트 컨트랙트가 컴파일될 때 아직 개인정보보호 정책이 제공되지 않거나, 컴파일 시간과 런타임에 개인정보보호 정책이 달라지는 경우에는 프라이버시가 노출될 우려가 여전히 존재한다.
- [0026] GDPR(General Data Protection Regulation)과 같이 법령 개정 또는 상황 변화 등으로 개인정보보호 정책이 변경되는 경우는 일상적인 데이터 관리에서 적지 않게 일어난다. 그러나, 최근 스마트 컨트랙트에 개인정보보호 정책을 구현하는 기법들은 이러한 정책의 변화를 고려하지 않고, 컴파일 시간에 제공되는 정책으로 고정된다. 동적 정책 기반 스마트 컨트랙트 개인정보보호 방법은 스마트 컨트랙트의 life cycle 동안 개인정보보호 정책에 변화가 있는 경우에도 새로운 개인정보보호 정책에 따라 데이터 공개 범위가 변화되므로, 연속성을 잃지 않고 갱신된 개인정보보호 정책을 적용하여 프라이버시가 중요한 데이터를 보호할 수 있다.
- [0027] 동적 정책 기반 스마트 컨트랙트 개인정보보호 방법은 DeFi, 중고 물품, NFT 등에 대한 거래 앱에서 개인정보를 보호할 수 있으며, 특히 개인정보보호 정책이 변화되는 경우에도 연속성을 잃지 않고 갱신된 개인정보보호 정책이 적용될 수 있다. 동적 정책 기반 스마트 컨트랙트 개인정보보호 방법은 스마트 컨트랙트로 데이터를 관리하거나 금전적인 거래가 일어나는 경우, 불필요한 상황에서 부적절하게 데이터가 유출되는 상황을 막을 수 있다.
- [0028] (a)단계는 Solidity로 작성된 스마트 컨트랙트를 입력받을 수 있다.
- [0029] Solidity 프로그램은 계약 지향 프로그래밍 언어로 다양한 블록체인 플랫폼의 스마트 컨트랙트 작성 및 구현에 사용될 수 있다. Solidity 프로그램은 dapp을 프로그래밍할 수 있다. Solidity 프로그램은 이더리움 블록체인 플랫폼에서 스마트 계약을 정의할 수 있다.
- [0030] (b)단계는 스마트 컨트랙트 코드에 하나 이상의 위임 실행 코드를 추가하여 중간언어로 변환할 수 있다. (b)단계는 모든 가능한 위치에 위임(delegation) 실행 코드를 추가할 수 있다. (b)단계에서 추가된 위임 실행 코드가 삽입된 정보는 컴파일된 이후 해당 코드가 실행될 때, 개인정보보호 정책에 따라 공개가 가능한 것인지 판단될 수 있다.
- [0031] 도 2는 본 발명의 실시예에 따른 (b)단계의 흐름도를 나타낸다. 도 2를 참조하면, (b)단계는 데이터 소유자를 나타내는 소유권 매개변수를 함수의 각 필드 및 각 인수에 첨부하는 (b-1)단계와 코드를 타입 기반으로 분석하여 블록체인상에서 정보가 공개될 수 있는 코드에 공개식을 삽입하는 (b-2)단계를 더 포함할 수 있다. (b-1)단계에서 첨부된 복수개의 소유권 매개변수는 각각 독립적일 수 있다.
- [0032] (b)단계는 스마트 컨트랙트 코드를 암호화된 형태로 변환할 수 있다. (b)단계는 위임 실행 코드를 추가하는 과정에서 접근이 허용되는 않는 위치에는 위임 실행 코드를 추가할 수 없다. 이때, 접근이 허용되지 않는 위치에 있는 정보보다 중요한 개인정보인 경우 런타임 중에 보호받을 수 없는 문제가 발생한다. 따라서, (b)단계는 스마트 컨트랙트 코드를 암호화된 형태로 변환하여 이중 보호 효과를 달성할 수 있다.
- [0033] (b)단계는 스마트 컨트랙트 코드를 암호화된 형태로 변환하는 방법으로 영지식 증명을 사용할 수 있다. 영지식 증명이란 암호학에서 누군가가 상대방에게 어떤 사항이 참이라는 것을 증명할 때, 그 문장의 참 거짓 여부를 제

외한 어떤 것도 노출되지 않는 절차를 뜻한다.

- [0034] (c)단계는 중간언어 변환단계에서 변환된 코드를 EVM(Ethereum Virtual Machine) 바이트 코드로 컴파일할 수 있다. 이더리움에서 스마트 컨트랙트 코드를 실행하는 프로그램을 EVM이라고 한다. EVM은 스마트 컨트랙트를 컴파일해서 얻어진 바이트 코드를 실행할 수 있다. 바이트 코드란 EVM에서 정의하는 명령어, 즉 OP 코드들의 집합을 의미한다. (c)단계는 변환된 코드가 EVM에서 실행되도록 EVM 바이트 코드로 변환하는 역할을 수행할 수 있다. (c)단계에서는 변환된 코드가 EVM 바이트 코드로 변환되고, 스마트 컨트랙트 계약에 주석이 달린 데이터를 새 메타데이터로 추가될 수 있다.
- [0035] (d)단계는 컴파일하는 단계에서 컴파일된 코드를 EVM에서 실행시킬 수 있다. (d)단계에서는 컴파일된 코드가 EVM에 실행될 수 있고, 이때 위임 실행 코드의 시작/종료 지점에서 정책 파일이 검사될 수 있다. (d)단계는 컴파일된 코드에서 JSON으로 나타낸 정책 파일을 인식하여 정보 접근 권한을 확인할 수 있다. 따라서, 컴파일 시점에 제공되는 정책으로 고정되지 않고 실제 코드가 실행될 때에도 스마트 컨트랙트 데이터의 개인정보보호 정책이 제공 및 적용될 수 있다.
- [0036] JSON(JavaScript Object Notation)은 속성-값 쌍(attribute-value pairs and array data types) 또는 키-값 쌍으로 이루어진 데이터 오브젝트를 전달하기 위해 인간이 읽을 수 있는 텍스트를 사용하는 개방형 표준 포맷이다. JSON은 비동기 브라우저/서버 통신을 위해, 넓게는 XML을 대체하는 주요 데이터 포맷이다. JSON은 인터넷에서 자료를 주고 받을 때 그 자료를 표현하는 방법이다. JSON은 자바스크립트 언어로부터 파생되어 자바스크립트의 구문 형식을 따르지만 언어 독립형 데이터 포맷이다. JSON은 프로그래밍 언어나 플랫폼에 독립적이므로, 구문 분석 및 JSON 데이터 생성을 위한 코드는, C, C++, C#, 자바, 자바스크립트, 펄, 파이썬 등 수많은 프로그래밍 언어에서 쉽게 사용될 수 있다.
- [0037] 도 3은 본 발명의 실시예에 따른 (e)단계와 (f)단계가 포함된 동적 정책 기반 스마트 컨트랙트 개인정보보호 방법의 흐름도를 나타낸다.
- [0038] 도 3을 참조하면, (e)단계는 (a)단계 이후에 개인정보보호 정책을 기술한 JSON을 입력받을 수 있다. (f)단계는 스마트 컨트랙트 내에서 개인정보보호에 적용할 수 있도록 확장된 타입으로 결합할 수 있다. Solidity로 작성된 스마트 컨트랙트와 개인정보보호 정책을 기술한 JSON이 입력되면 단일 스마트 계약으로 결합할 수 있다. 다음 단계에서 proof 및 기타 부산물을 포함한 결과값으로 출력될 수 있다. 확장된 타입은 최종 사용자 언어가 아니라 중간 표현이므로 복잡성은 개발자를 괴롭히지 않는다.
- [0039] 도 4는 본 발명의 실시예에 따른 동적 정책 기반 스마트 컨트랙트 개인정보보호 시스템(10)의 구성도를 나타낸다. 도 4를 참조하면, 스마트 컨트랙트 개인정보보호 시스템(10)은 입력부(100), 변환부(300), 컴파일부(500), 및 출력부(700)를 포함할 수 있다.
- [0040] 입력부(100)는 Solidity로 작성된 스마트 컨트랙트를 입력받을 수 있다. 입력부(100)는 전술한 (a)단계의 동작을 수행할 수 있다.
- [0041] 변환부(300)는 스마트 컨트랙트 코드에 하나 이상의 위임 실행 코드를 추가하여 중간언어로 변환할 수 있다. 변환부(300)는 전술한 (b)단계의 동작을 수행할 수 있다.
- [0042] 변환부(300)는 소유권 매개변수 첨부모듈(310)과 공개식 삽입모듈(330)을 포함할 수 있다. 소유권 매개변수 첨부모듈(310)은 데이터 소유자를 나타내는 소유권 매개변수를 함수의 각 필드 및 각 인수에 첨부할 수 있다. 소유권 매개변수 첨부모듈(310)은 전술한 (b-1)단계의 동작을 수행할 수 있다. 공개식 삽입모듈(330)은 코드를 타입 기반으로 분석하여 블록체인상에서 정보가 공개될 수 있는 코드에 공개식을 삽입할 수 있다. 공개식 삽입모듈(330)은 전술한 (b-2)단계의 동작을 수행할 수 있다.
- [0043] 컴파일부(500)는 변환부(300)에서 변환된 코드를 EVM(Ethereum Virtual Machine) 바이트 코드로 컴파일할 수 있다. 컴파일부(500)는 전술한 (c)단계의 동작을 수행할 수 있다.
- [0044] 출력부(700)는 컴파일부(500)에서 컴파일된 코드를 EVM에서 실행시킬 수 있다. 출력부(700)는 전술한 (d)단계의 동작을 수행할 수 있다.
- [0045] 동적 정책 기반 스마트 컨트랙트 개인정보보호 시스템(10)은 개인정보보호 정책을 기술한 JSON을 입력받는 JSON 입력부와 JSON을 스마트 컨트랙트 내에서 개인정보보호에 적용할 수 있도록 확장된 타입으로 결합하는 결합부를 더 포함할 수 있다. JSON 입력부는 전술한 (e)단계의 동작을 수행할 수 있고, 결합부는 전술한 (f)단계의 동작

을 수행할 수 있다.

[0046]

이상에서 대표적인 실시예를 통하여 본 발명을 상세하게 설명하였으나, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리 범위는 설명한 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허청구범위뿐만 아니라 특허청구범위와 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태에 의하여 정해져야 한다.

## 부호의 설명

[0048]

10 : 동적 정책 기반 스마트 컨트랙트 개인정보보호 시스템

100 : 입력부

300 : 변환부

310 : 소유권 매개변수 첨부모듈

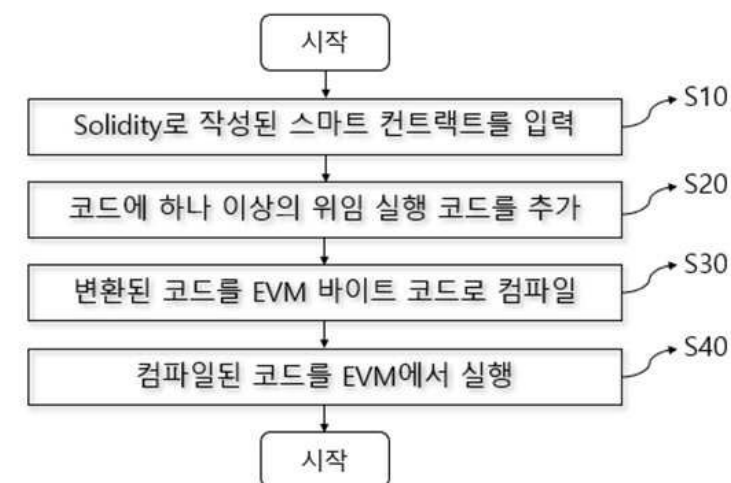
330 : 공개식 삽입모듈

500 : 컴파일부

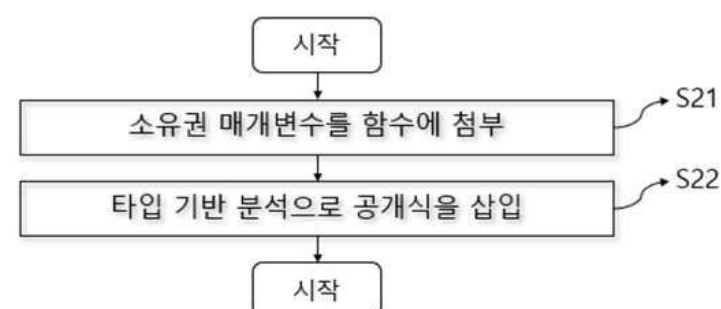
700 : 출력부

## 도면

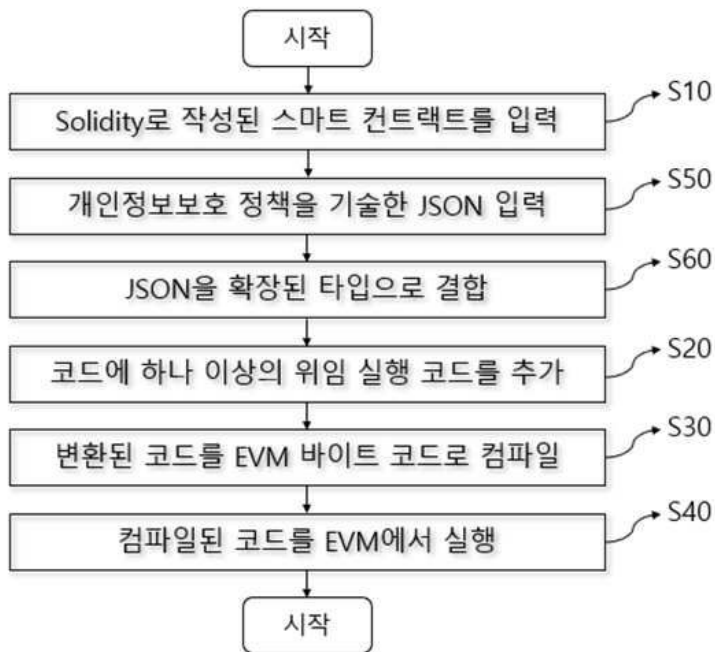
### 도면1



### 도면2



도면3



도면4

