



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0117975
(43) 공개일자 2023년08월10일

(51) 국제특허분류(Int. Cl.)
G06F 21/62 (2013.01) G06F 21/57 (2013.01)
(52) CPC특허분류
G06F 21/6245 (2013.01)
G06F 21/577 (2013.01)
(21) 출원번호 10-2022-0014402
(22) 출원일자 2022년02월03일
심사청구일자 2022년02월03일

(71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
조은선
대전광역시 유성구 어은로 57 한빛아파트, 110동 1504호
김지현
경상남도 진주시 정촌면 삼일로106번길 8 대경과미르 105동 1004호
(뒷면에 계속)
(74) 대리인
이은철, 김재문

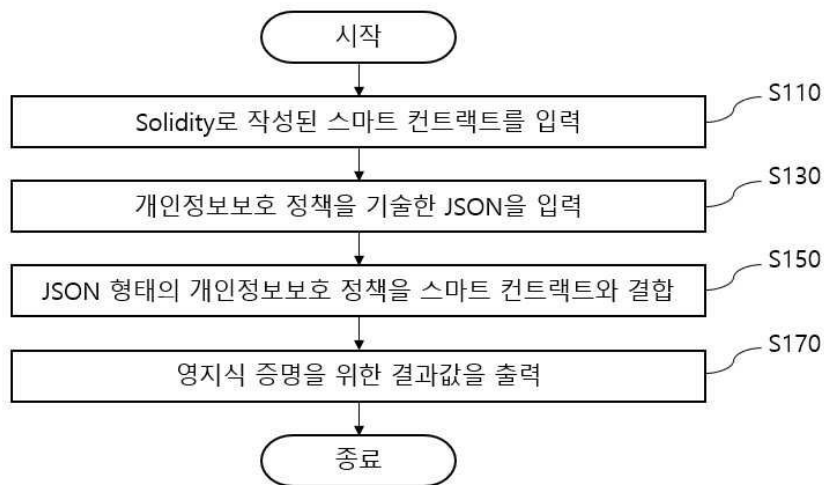
전체 청구항 수 : 총 8 항

(54) 발명의 명칭 스마트 컨트랙트 개인정보보호 방법 및 이를 이용한 시스템

(57) 요약

본 발명은, Solidity로 작성된 스마트 컨트랙트를 입력받는 단계; 개인정보보호 정책을 기술한 JSON을 입력받는 단계; JSON을 스마트 컨트랙트 내에서 개인정보보호에 적용할 수 있도록 확장된 타입으로 결합하는 단계; 및 변환된 Solidity 컨트랙트, 증명 컨트랙트, 키, 구동을 위한 API, 또는 메타정보 파일을 포함하는 영지식 증명을 위한 결과값을 출력하는 단계;를 포함하는 것을 특징으로 한다.

대표도 - 도1



(72) 발명자

김지수

대전광역시 유성구 대학로 169, 301호

정다현

울산광역시 울주군 청량읍 율리영해2길 7 문수데시
앙2단지아파트 203동 1403호

이 발명을 지원한 국가연구개발사업

과제고유번호 1711111605

과제번호 2020R1A2C2008864

부처명 과학기술정보통신부

과제관리(전문)기관명 한국연구재단

연구사업명 개인기초연구(과기정통부)(R&D)

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 단계;

개인정보보호 정책을 기술한 JSON을 입력받는 단계;

JSON을 스마트 컨트랙트 내에서 개인정보보호에 적용할 수 있도록 확장된 타입으로 결합하는 단계; 및

변환된 Solidity 컨트랙트, 증명 컨트랙트, 키, 구동을 위한 API, 또는 메타정보 파일을 포함하는 영지식 증명을 위한 결과값을 출력하는 단계;를 포함하는 스마트 컨트랙트 개인정보보호 방법.

청구항 2

제 1 항에 있어서,

상기 결과값을 출력하는 단계는,

스마트 컨트랙트가 JSON의 개인정보보호 정책에 위배되는지 검사하는 단계를 포함하는 것을 특징으로 하는 스마트 컨트랙트 개인정보보호 방법.

청구항 3

제 2 항에 있어서,

상기 결과값을 출력하는 단계는,

스마트 컨트랙트가 JSON의 개인정보보호 정책에 위배되는 경우 결과값을 출력하지 않고 종료하는 것을 특징으로 하는 스마트 컨트랙트 개인정보보호 방법.

청구항 4

제 2 항에 있어서,

상기 결과값을 출력하는 단계는,

스마트 컨트랙트가 JSON의 개인정보보호 정책에 위배되지 않는 경우 영지식 증명을 위한 결과값을 출력하는 것을 특징으로 하는 스마트 컨트랙트 개인정보보호 방법.

청구항 5

Solidity로 작성된 스마트 컨트랙트를 입력받는 제 1 입력단;

개인정보보호 정책을 기술한 JSON을 입력받는 제 2 입력단;

JSON을 스마트 컨트랙트 내에서 개인정보보호에 적용할 수 있도록 확장된 타입으로 결합하는 프론트 엔드 단; 및

상기 프론트 엔드 단에서 결합된 파일을 변환된 Solidity 컨트랙트, 증명 컨트랙트, 키, 구동을 위한 API, 또는 메타정보 파일을 포함하는 영지식 증명을 위한 결과값으로 출력하는 백 엔드 단;을 포함하는 스마트 컨트랙트 개인정보보호 시스템.

청구항 6

제 5 항에 있어서,

상기 백 엔드 단은,

스마트 컨트랙트가 JSON의 개인정보보호 정책에 위배되는지 검사하는 리졸버를 포함하는 것을 특징으로 하는 스마트 컨트랙트 개인정보보호 시스템.

청구항 7

제 6 항에 있어서,

상기 리졸버는,

스마트 컨트랙트가 JSON의 개인정보보호 정책에 위배되는 경우 결과값을 출력하지 않고 종료하는 것을 특징으로 하는 스마트 컨트랙트 개인정보보호 시스템.

청구항 8

제 6 항에 있어서,

상기 백 엔드 단은,

스마트 컨트랙트가 JSON의 개인정보보호 정책에 위배되지 않는 경우 영지식 증명을 위한 결과값을 출력하는 영지식 증명 생성부를 더 포함하는 것을 특징으로 하는 스마트 컨트랙트 개인정보보호 시스템.

발명의 설명

기술 분야

[0001] 본 발명은 개인정보보호 방법 및 이를 이용한 시스템에 관한 것으로서, 특히 스마트 컨트랙트의 특성을 고려한 스마트 컨트랙트 개인정보보호 방법 및 이를 이용한 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. 최근, 블록체인 기술은 스마트 컨트랙트의 실행을 위한 프레임워크를 제공하도록 확장되었다. 스마트 컨트랙트는, 사용자가 만든 비즈니스 로직을 달성하도록 블록체인 합의 네트워크에서 실행될 수 있는 코드이다. 스마트 컨트랙트는 디지털 형식으로 정의된 일련의 약속을 포함할 수 있고, 관련 약속이 코드로 설명되어 있는 당사자들 간의 합의를 포함할 수 있다. 스마트 컨트랙트는 향후 서명 또는 트리거 이벤트에 따라 자동으로 정산될 수 있다.

[0004] 최근 스마트 컨트랙트는 블록체인에서 실행되지만 이는 개인 정보 보호 관점에서 데이터에 잠재적으로 해를 끼칠 수 있다. 블록체인에서 프로그램의 비공개 변수와 암호화 프로토콜을 지원하는 기존의 개인정보보호 기법은 스마트 컨트랙트의 특성을 충분히 고려하지 않고 있다. 기존의 타입 기반 개인 정보 보호는 생산성을 감소시킬 수 있고, 암호화된 데이터에 대한 프로토콜 기반 지원은 오버헤드로 인해 현실적으로 제한된 종류의 개인 정보 데이터에만 적용된다. 따라서, 이를 극복하기 위해서 컨트랙트 코드가 다루는 모든 종류의 개인 정보 데이터

를 의도한 대로 보호하는 다른 기법이 요구되고 있는 실정이다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 한국공개특허 제10-2020-0066261호

발명의 내용

해결하려는 과제

[0007] 본 발명은 상기와 같은 문제를 해결하기 위한 것으로서, 기존의 스마트 컨트랙트 개인정보보호 기법의 한계를 극복할 수 있는 스마트 컨트랙트 개인정보보호 방법 및 이를 이용한 시스템을 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0009] 상기 목적을 달성하기 위하여 본 발명은, Solidity로 작성된 스마트 컨트랙트를 입력받는 단계; 개인정보보호 정책을 기술한 JSON을 입력받는 단계; JSON을 스마트 컨트랙트 내에서 개인정보보호에 적용할 수 있도록 확장된 타입으로 결합하는 단계; 및 변환된 Solidity 컨트랙트, 증명 컨트랙트, 키, 구동을 위한 API, 또는 메타정보 파일을 포함하는 영지식 증명을 위한 결과값을 출력하는 단계;를 포함하는 것을 일 특징으로 한다.

[0010] 바람직하게는, 상기 결과값을 출력하는 단계는, 스마트 컨트랙트가 JSON의 개인정보보호 정책에 위배되는지 검사하는 단계를 포함할 수 있다.

[0011] 바람직하게는, 상기 결과값을 출력하는 단계는, 스마트 컨트랙트가 JSON의 개인정보보호 정책에 위배되는 경우 결과값을 출력하지 않고 종료할 수 있다.

[0012] 바람직하게는, 상기 결과값을 출력하는 단계는, 스마트 컨트랙트가 JSON의 개인정보보호 정책에 위배되지 않는 경우 영지식 증명을 위한 결과값을 출력할 수 있다.

[0013] 또한 본 발명은, Solidity로 작성된 스마트 컨트랙트를 입력받는 제 1 입력단; 개인정보보호 정책을 기술한 JSON을 입력받는 제 2 입력단; JSON을 스마트 컨트랙트 내에서 개인정보보호에 적용할 수 있도록 확장된 타입으로 결합하는 프론트 엔드 단; 및 상기 프론트 엔드 단에서 결합된 파일을 변환된 Solidity 컨트랙트, 증명 컨트랙트, 키, 구동을 위한 API, 또는 메타정보 파일을 포함하는 영지식 증명을 위한 결과값으로 출력하는 백 엔드 단;을 포함하는 것을 다른 특징으로 한다.

[0014] 바람직하게는, 상기 백 엔드 단은, 스마트 컨트랙트가 JSON의 개인정보보호 정책에 위배되는지 검사하는 리졸버를 포함할 수 있다.

[0015] 바람직하게는, 상기 리졸버는, 스마트 컨트랙트가 JSON의 개인정보보호 정책에 위배되는 경우 결과값을 출력하지 않고 종료할 수 있다.

[0016] 바람직하게는, 상기 백 엔드 단은, 스마트 컨트랙트가 JSON의 개인정보보호 정책에 위배되지 않는 경우 영지식 증명을 위한 결과값을 출력하는 영지식 증명 생성부를 더 포함할 수 있다.

발명의 효과

[0018] 본 발명은 일반적인 Solidity 프로그램에 별도의 JSON 정책을 결합하여 스마트 컨트랙트의 민감한 개인 정보 저장 데이터가 블록체인으로 유출되는 것을 막을 수 있다는 이점이 있다.

[0019] 또한, 본 발명은 스마트 컨트랙트에 대한 개인정보보호를 지원하면서도 스마트 컨트랙트의 생산성이 부담이 적으며, 재사용성을 높일 수 있다는 이점이 있다.

도면의 간단한 설명

- [0021] 도 1은 본 발명의 실시예에 따른 스마트 컨트랙트 개인정보보호 방법의 흐름도를 나타낸다.
- 도 2는 본 발명의 실시예에 따른 스마트 컨트랙트 개인정보보호 방법의 구체적인 세부 흐름도를 나타낸다.
- 도 3은 본 발명의 실시예에 따른 스마트 컨트랙트 개인정보보호 시스템의 구성도를 나타낸다.
- 도 4는 본 발명의 실시예에 따른 백 엔드 단의 구성도를 나타낸다.
- 도 5는 본 발명의 실시예에 따른 스마트 컨트랙트 개인정보보호 시스템의 구체적인 세부 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] 블록체인은 네트워크 참여자들의 합의 프로토콜에 의해 탈중앙화 환경에서 원장을 구성할 수 있다. 스마트 컨트랙트는 계약 조건을 블록체인에 기록하고 조건이 충족됐을 경우 자동으로 계약이 실행되게 한다. 스마트 컨트랙트는 블록체인에서 실행되는 프로그램으로 Solidity와 같은 언어로 개발될 수 있다. 스마트 컨트랙트는 블록체인에서 실행되지만 개인 정보 보호 관점에서 문제가 발생할 수 있으므로 이하에서는 이를 해결하기 위한 스마트 컨트랙트 개인정보보호 방법을 제시한다.
- [0025] 스마트 컨트랙트 개인정보보호 방법은 스마트 컨트랙트의 특성을 고려하지 않은 기존의 개인정보보호 기법과 달리 스마트 컨트랙트의 특성을 반영할 수 있다. 스마트 컨트랙트 개인정보보호 방법은 기존의 스마트 컨트랙트 개인정보보호 기법의 한계를 극복하기 위해 일반적인 Solidity 프로그램에 별도의 JSON 정책을 결합하여 컨트랙트의 민감한 개인 정보 저장 데이터가 체인으로 유출되는 것을 막을 수 있다.
- [0026] 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.
- [0027] 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.
- [0028] 제안하는 스마트 컨트랙트 개인정보보호 방법은 별도로 정의된 JSON 형태의 개인정보보호 정책을 Solidity로 작성된 스마트 컨트랙트와 결합시키는 단계를 포함할 수 있다.
- [0029] 제안하는 스마트 컨트랙트 개인정보보호 방법은 기존의 개인정보보호 기법에서 타입 시스템의 수명이 프로그램의 수명과 달라 발생하는 생산성 부담을 적게 할 수 있다. 제안하는 스마트 컨트랙트 개인정보보호 방법은 블록체인상에 배포되어 있는 스마트 컨트랙트의 보안분야에서 널리 사용될 수 있다. 제안하는 스마트 컨트랙트 개인정보보호 방법은 Solidity 형식의 스마트 컨트랙트와 JSON 형식의 정책에서 낮은 수준의 증명 메커니즘으로의 자동 변환을 정교하게 하여 정적 및 동적으로 개인 정보 보호를 보장할 수 있다.
- [0030] 도 1은 본 발명의 실시예에 따른 스마트 컨트랙트 개인정보보호 방법의 흐름도를 나타낸다. 도 1을 참조하여 본 발명에 따른 스마트 컨트랙트 개인정보보호 방법에 대해 살펴보면 아래와 같다.

- [0031] 먼저, Solidity로 작성된 스마트 컨트랙트 및 개인정보보호 정책을 기술한 JSON을 입력받을 수 있다. 여기서, 스마트 컨트랙트와 JSON이 입력되는 순서는 무관하다.
- [0032] 뒤이어, JSON을 스마트 컨트랙트 내에서 개인정보보호에 적용할 수 있도록 확장된 타입으로 결합할 수 있다. Solidity로 작성된 스마트 컨트랙트와 개인정보보호 정책을 기술한 JSON이 입력되면 Stone internal representation(SIR)이라 칭하는 단일 스마트 계약으로 결합할 수 있다. 변환된 SIR은 다음 단계에서 proof 및 기타 부산물을 포함한 결과값으로 출력될 수 있다. SIR은 최종 사용자 언어가 아니라 중간 표현이므로 복잡성은 개발자를 괴롭히지 않는다.
- [0033] 다음으로, 변환된 Solidity 컨트랙트, 증명 컨트랙트, 키, 구동을 위한 API, 또는 메타정보 파일을 포함하는 영지식 증명을 위한 결과값을 출력할 수 있다.
- [0034] 도 2는 본 발명의 실시예에 따른 스마트 컨트랙트 개인정보보호 방법의 구체적인 세부 흐름도를 나타낸다. 도 2를 참조하면, 결과값을 출력하는 단계에서는 스마트 컨트랙트가 JSON의 개인정보보호 정책에 위배되는지 검사할 수 있다.
- [0035] 결과값을 출력하는 단계에서는 스마트 컨트랙트가 JSON의 개인정보보호 정책에 위배되는 경우 결과값을 출력하지 않고 종료할 수 있다. 즉, 기존 Solidity 컨트랙트를 조사하여 주어진 정책에 위배되어 개인정보가 유출되는 경우 타입 오류를 내고 결과값 출력을 종료할 수 있다.
- [0036] 결과값을 출력하는 단계에서는 스마트 컨트랙트가 JSON의 개인정보보호 정책에 위배되지 않는 경우 영지식 증명을 위한 결과값을 출력할 수 있다. 즉, 기존 Solidity 컨트랙트를 조사하여 주어진 정책에 위배되지 않아 개인정보가 보호되는 것이 확인된 스마트 컨트랙트는 영지식 증명을 위한 결과값을 출력할 수 있다.
- [0037] 영지식 증명이란 암호학에서 누군가가 상대방에게 어떤 사항이 참이라는 것을 증명할 때, 그 문장의 참 거짓 여부를 제외한 어떤 것도 노출되지 않는 절차를 뜻한다.
- [0038] 도 3은 본 발명의 실시예에 따른 스마트 컨트랙트 개인정보보호 시스템(10)의 구성도를 나타낸다. 도 3을 참조하면, 스마트 컨트랙트 개인정보보호 시스템(10)은 제 1 입력단(100), 제 2 입력단(300), 프론트 엔드 단(500), 및 백 엔드 단(700)을 포함할 수 있다.
- [0039] 제 1 입력단(100)은 Solidity로 작성된 스마트 컨트랙트를 입력받을 수 있다.
- [0040] 제 2 입력단(300)은 개인정보보호 정책을 기술한 JSON을 입력받을 수 있다.
- [0041] 프론트 엔드 단(500)은 JSON을 스마트 컨트랙트 내에서 개인정보보호에 적용할 수 있도록 확장된 타입으로 결합할 수 있다. 프론트 엔드 단(500)은 Stonizer로 명명될 수 있다. 프론트 엔드 단(500)은 입력된 스마트 컨트랙트와 JSON을 중간언어(Stone internal representation, SIR)로 변환할 수 있다. 프론트 엔드 단(500)은 중간언어를 백 엔드 단(700)으로 전달할 수 있다.
- [0042] JSON의 개인정보보호 정보 정책에는 필드, 생성자 및 함수에 대한 항목이 포함될 수 있다. JSON은 각 필드, 생성자의 각 인수, 함수의 각 인수 및 변수에 대해 속성 ‘이름’, ‘유형’, 또는 기타 필수 사항을 제공할 수 있다. ‘유형’에는 기본 Solidity 유형, 데이터 소유자 및 위임 정보가 포함될 수 있다. 필드에는 ‘!’ 기호가 이끄는 제한된 유형 변수가 필요한 복잡한 유형 매핑이 있을 수 있다.
- [0043] 프론트 엔드 단(500)은 JSON 개인정보보호 정책을 ‘유형’ 표기법으로 변환하는 것이 주요 작업일 수 있다. 프론트 엔드 단(500)은 Solidity 프로그램을 파싱하고 JSON 정책과 내용을 비교하는 것을 수반할 수 있다. 프론트 엔드 단(500)은 먼저 유형 및 이름이 JSON 정책과 일치하는 Solidity 함수를 차례로 검사할 수 있다. 다음으로 프론트 엔드 단(500)은 소유권 및 위임 정보를 SIR에 삽입시킬 수 있다.
- [0044] 도 4는 본 발명의 실시예에 따른 백 엔드 단(700)의 구성도를 나타낸다. 도 4를 참조하면, 백 엔드 단(700)은 리졸버(710)와 영지식 증명 생성부(730)를 포함할 수 있다.
- [0045] 백 엔드 단(700)은 상기 프론트 엔드 단에서 결합된 파일을 변환된 Solidity 컨트랙트, 증명 컨트랙트, 키, 구동을 위한 API, 또는 메타정보 파일을 포함하는 영지식 증명을 위한 결과값으로 출력할 수 있다.
- [0046] 리졸버(710)는 스마트 컨트랙트가 JSON의 개인정보보호 정책에 위배되는지 검사할 수 있다.
- [0047] 리졸버(710)는 스마트 컨트랙트가 JSON의 개인정보보호 정책에 위배되는 경우 결과값을 출력하지 않고 종료할 수 있다. 리졸버(710)는 기존 Solidity 컨트랙트를 조사하여 주어진 정책에 위배되어 개인 정보가 유출되는 경

우 타입 오류를 내고 결과값 출력을 종료할 수 있다.

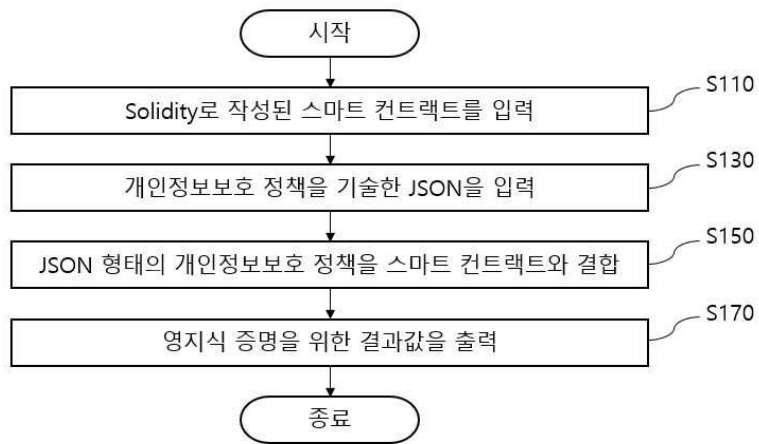
- [0048] 영지식 증명 생성부(730)는 스마트 컨트랙트가 JSON의 개인정보보호 정책에 위배되지 않는 경우 영지식 증명을 위한 결과값을 출력할 수 있다. 영지식 증명 생성부(730)는 기존 Solidity 컨트랙트를 조사하여 주어진 정책에 위배되지 않아 개인정보가 보호되는 것이 확인된 스마트 컨트랙트는 영지식 증명을 위한 결과값을 출력할 수 있다. 영지식 증명 생성부(730)는 zkay v0.2를 사용할 수 있다. 이는 jsnark 및 zksnark와 같은 다양한 영지식 도구를 지원할 수 있음을 의미한다.
- [0049] 도 5는 본 발명의 실시예에 따른 스마트 컨트랙트 개인정보보호 시스템(10)의 구체적인 세부 구성도를 나타낸다. 도 5를 참조하여, 본 발명의 일 실시예를 설명한다.
- [0050] Solidity 스마트 컨트랙트와 개인 정보 보호 정책이 기술된 JSON은 Stonizer Frontend로 입력될 수 있다. 입력된 스마트 컨트랙트와 JSON은 확장된 타입으로 결합되어 중간언어인 SIR(Stone internal representation)으로 변환될 수 있다. 변환된 SIR은 Backend로 입력될 수 있다.
- [0051] 입력된 SIR은 Stone Type Resolver에서 스마트 컨트랙트가 JSON의 개인정보보호 정책에 위배되는지 검사될 수 있다. 스마트 컨트랙트가 개인정보보호 정책에 위배되는 경우에는 알고리즘은 그대로 종료될 수 있다. 스마트 컨트랙트가 개인정보보호 정책에 위배되지 않는 경우에는 ZK Proof Generator에서 proof 및 부산물을 출력할 수 있다. 여기서, 출력되는 값은 transformed contract, verifier contract, keys, auxiliaries 등으로 영지식 증명을 위해 사용되는 것이다.
- [0052] 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

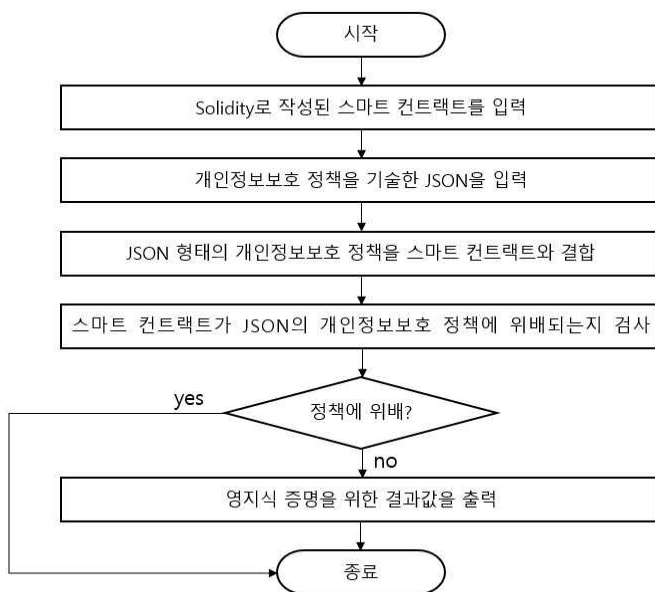
- [0054] 10 : 스마트 컨트랙트 개인정보보호 시스템
- 100 : 제 1 입력단
- 300 : 제 2 입력단
- 500 : 프론트 엔드 단
- 700 : 백 엔드 단
- 710 : 리졸버
- 730 : 영지식 증명 생성부

도면

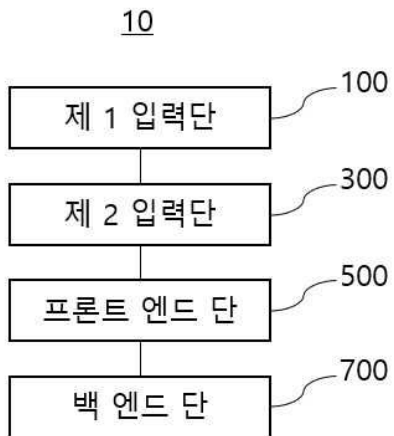
도면1



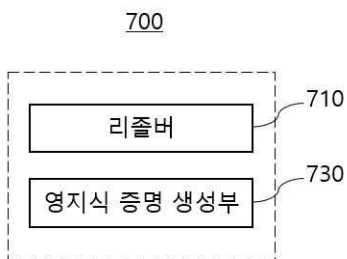
도면2



도면3



도면4



도면5

