(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0002663
(43) 공개일자 2024년01월05일

(51) 국제특허분류(Int. Cl.)
G06F 9/455 (2018.01) *G06F 9/54* (2018.01)
(52) CPC특허분류
G06F 9/45558 (2013.01)
G06F 9/45504 (2013.01)
(21) 출원번호 10-2022-0140328
(22) 출원일자 2022년10월27일
심사청구일자 2022년10월27일
(30) 우선권주장
1020220079974 2022년06월29일 대한민국(KR)

(71) 출원인
포항공과대학교 산학협력단
경상북도 포항시 남구 청암로 77 (지곡동)
(72) 발명자
박찬익
경상북도 포항시 남구 청암로 77
정문현
경상북도 포항시 남구 청암로 77
(74) 대리인
특허법인이상

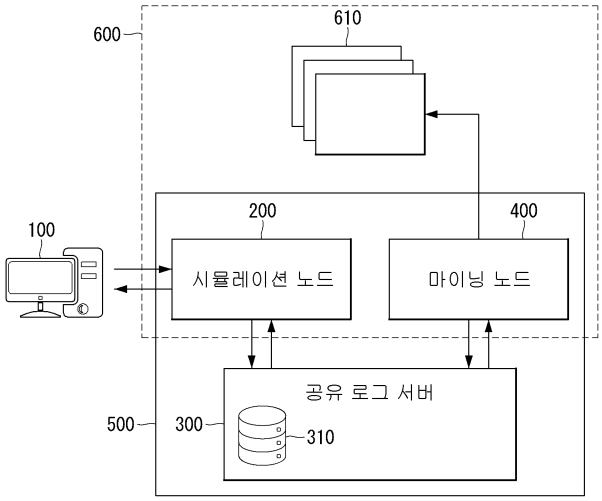
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **공유로그 기반 솔리디티 스마트 컨트랙트 실행 방법 및 장치**

(57) 요 약

공유로그 기반 솔리디티 스마트 컨트랙트 실행 방법 및 시스템이 개시된다. 솔리디티 스마트 컨트랙트 실행 시스템은, 이더리움 네트워크로부터 솔리디티 스마트 컨트랙트의 주소와 데이터를 받고 솔리디티 스마트 컨트랙트를 시뮬레이션하는 시뮬레이션 노드, 시뮬레이션 노드로부터 받은 시뮬레이션 결과들의 순서를 결정하여 나열하고 공유로그의 쓰기 요청이 성공하였음을 시뮬레이션 노드로 전달하는 시퀀서, 및 시퀀서가 결정한 순서대로 저장된 공유로그 항목들의 마지막 항목 다음에 새로운 공유로그 항목을 추가하고, 정해진 개수의 공유로그 항목이 추가되거나 정해진 시간이 경과하는 경우에 새로 추가된 공유로그 항목들을 마이닝 노드로 전달하는 공유로그 서버를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
G06F 9/544 (2013.01)
G06F 9/546 (2013.01)
H04L 67/1087 (2022.05)
G06F 2009/45562 (2013.01)
G06F 2009/45595 (2019.08)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711160099
과제번호	2018-0-01441-005
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보통신방송혁신인재양성
연구과제명	크로스 도메인 호환성을 위한 블록체인 플랫폼 및 비즈모델 개발
기 여 율	1/1
과제수행기관명	포항공과대학교 산학협력단
연구기간	2022.01.01 ~ 2022.12.31

명 세 서

청구범위

청구항 1

공유로그 기반 솔리디티(Solidity) 스마트 컨트랙트 실행 시스템으로서,

이더리움 네트워크로부터 솔리디티 스마트 컨트랙트의 주소와 데이터를 받고 상기 솔리디티 스마트 컨트랙트를 시뮬레이션하는 시뮬레이션 노드;

상기 시뮬레이션 노드로부터 받은 시뮬레이션 결과들의 순서를 결정하여 나열하고, 공유로그의 쓰기 요청이 성공하였음을 상기 시뮬레이션 노드로 전달하는 시퀀서; 및

상기 시퀀서가 결정한 순서대로 상기 공유로그에 저장된 공유로그 항목들의 마지막 항목 다음에 새로운 공유로그 항목을 추가하고, 정해진 개수의 공유로그 항목이 추가되거나 정해진 시간이 경과하는 경우, 새로 추가된 공유로그 항목들을 마이닝 노드로 전달하는 공유로그 서버;

를 포함하는 솔리디티 스마트 컨트랙트 실행 시스템.

청구항 2

청구항 1에 있어서,

상기 솔리디티 스마트 컨트랙트의 주소와 데이터는 사용자 단말에서 미리 설정된 형식에 맞게 작성되어 상기 이더리움 네트워크로 전송된 것인, 솔리디티 스마트 컨트랙트 실행 시스템.

청구항 3

청구항 1에 있어서,

상기 시뮬레이션 노드는, 상기 이더리움 네트워크에 접속하여 상기 솔리디티 스마트 컨트랙트의 실행을 요청하는 사용자 요청에 따라 상기 공유로그 서버로부터 최신의 데이터를 읽어 자신의 상태를 업데이트하는, 솔리디티 스마트 컨트랙트 실행 시스템.

청구항 4

청구항 1에 있어서,

상기 시뮬레이션 노드는 상기 솔리디티 스마트 컨트랙트의 실행을 위한 모듈인 가상 머신(Virtual Machine)을 복사하고, 복사된 가상 머신 복사 모듈에서 상기 솔리디티 스마트 컨트랙트를 시뮬레이션하는, 솔리디티 스마트 컨트랙트 실행 시스템.

청구항 5

청구항 4에 있어서,

상기 시뮬레이션의 실행 결과는 소비된 가스의 총량, 변경된 계정 및 그 데이터를 포함하는, 솔리디티 스마트 컨트랙트 실행 시스템.

청구항 6

청구항 1에 있어서,

상기 시뮬레이션 노드는,

상기 솔리디티 스마트 컨트랙트의 실행을 위한 모듈인 가상 머신,

상기 가상 머신을 복사하여 상기 솔리디티 스마트 컨트랙트를 시뮬레이션하는 가상 머신 복사 모듈, 및

상기 공유로그 서버와 데이터 송수신을 수행하고 상기 공유로그 서버의 공유로그에 시뮬레이션 결과를 기록하고

상기 공유로그에 기록된 최신의 데이터를 읽는 공유로그 런타임 모듈을 구비하는, 솔리디티 스마트 컨트랙트 실행 시스템.

청구항 7

청구항 1에 있어서,

상기 공유로그 서버는,

상기 시뮬레이션 노드의 시뮬레이션 결과들을 받아 순서를 결정하여 나열하는 상기 시퀀서; 및

상기 시퀀서가 결정한 순서대로 상기 시뮬레이션 결과들에 대응하는 공유로그 항목들을 저장하고, 기저장된 공유로그 항목들의 마지막 항목 다음에 새로운 공유로그 항목을 추가하여 저장하는 상기 공유로그;

를 포함하는 솔리디티 스마트 컨트랙트 실행 시스템.

청구항 8

청구항 1에 있어서,

상기 공유로그 서버로부터 받은 데이터를 이용하여 블록을 생성하고, 생성된 블록을 이더리움 네트워크 또는 블록체인 네트워크에 참여하는 다른 노드들에게 전파하는 마이닝 노드를 더 포함하는, 솔리디티 스마트 컨트랙트 실행 시스템.

청구항 9

솔리디티(Solidity) 스마트 컨트랙트 실행 시스템의 시뮬레이션 노드에 의해 수행되는 공유로그 기반 솔리디티(Solidity) 스마트 컨트랙트 실행 방법으로서,

이더리움 네트워크로부터 솔리디티 스마트 컨트랙트의 주소와 데이터를 받는 단계-상기 솔리디티 스마트 컨트랙트의 주소와 데이터는 사용자 단말에서 미리 설정된 형식에 맞게 작성되어 상기 이더리움 네트워크로 전송된 것임-;

상기 솔리디티 스마트 컨트랙트의 실행을 위한 모듈인 가상 머신(Virtual Machine)을 복사하는 단계;

상기 가상 머신을 복사한 가상 머신 복사 모듈에서 상기 솔리디티 스마트 컨트랙트를 시뮬레이션하는 단계;

상기 시뮬레이션의 실행 결과를 공유로그 서버의 공유로그에 기록하는 단계; 및

상기 공유로그 서버로부터 상기 공유로그의 쓰기 요청에 대한 성공 메시지를 수신하는 단계를 포함하는, 솔리디티 스마트 컨트랙트 실행 방법.

청구항 10

청구항 9에 있어서,

상기 이더리움 네트워크에 접속하여 상기 솔리디티 스마트 컨트랙트의 실행을 요청하는 사용자 요청에 따라 상기 공유로그 서버로부터 최신의 데이터를 읽어 자신의 상태를 업데이트하는 단계를 더 포함하는, 솔리디티 스마트 컨트랙트 실행 방법.

청구항 11

청구항 9에 있어서,

상기 시뮬레이션의 실행 결과는 소비된 가스의 총량, 변경된 계정 및 그 데이터를 포함하는, 솔리디티 스마트 컨트랙트 실행 방법.

청구항 12

청구항 9에 있어서,

상기 공유로그 서버는 상기 시뮬레이션의 실행 결과를 받아 정해진 순서대로 나열하여 공유로그에 저장하고, 상기 공유로그의 마지막 항목에 새로운 공유로그 항목을 추가하고, 정해진 개수의 공유로그 항목이 추가되거나 정해진 시간이 경과하는 경우, 새로 추가된 공유로그 항목들을 마이닝 노드로 전달하는, 솔리디티 스마트 컨트랙

트 실행 방법.

청구항 13

청구항 12에 있어서,

상기 마이닝 노드는 상기 공유로그 서버로부터 받은 데이터를 이용하여 블록을 생성하고, 생성된 블록을 이더리움 네트워크 또는 블록체인 네트워크에 참여하는 다른 노드들에게 전파하는, 솔리디티 스마트 컨트랙트 실행 방법.

청구항 14

솔리디티(Solidity) 스마트 컨트랙트 실행 시스템의 공유로그 서버에 의해 수행되는 공유로그 기반 솔리디티 스마트 컨트랙트 실행 방법으로서,

시뮬레이션 노드로부터 시뮬레이션의 실행 결과를 받는 단계-상기 시뮬레이션 노드는 이더리움 네트워크로부터 솔리디티 스마트 컨트랙트의 주소와 데이터를 받고 상기 솔리디티 스마트 컨트랙트를 시뮬레이션함-;

상기 시뮬레이션의 실행 결과를 정해진 순서대로 나열하는 단계;

상기 순서대로 나열되고 공유로그에 저장된 공유로그 항목들의 마지막 항목에 새로운 공유로그 항목을 추가하는 단계; 및

상기 공유로그에 정해진 개수의 공유로그 항목이 추가되거나 정해진 시간이 경과하는 경우, 새로 추가된 공유로그 항목들을 마이닝 노드로 전달하는 단계;

를 포함하는 솔리디티 스마트 컨트랙트 실행 방법.

청구항 15

청구항 14에 있어서,

상기 공유로그의 쓰기 요청이 성공하였음을 상기 시뮬레이션 노드들로 전달하는 단계를 더 포함하는, 솔리디티 스마트 컨트랙트 실행 방법.

청구항 16

청구항 14에 있어서,

상기 시뮬레이션의 실행 결과는 소비된 가스의 총량, 변경된 계정 및 그 데이터를 포함하는, 솔리디티 스마트 컨트랙트 실행 방법.

청구항 17

청구항 14에 있어서,

상기 솔리디티 스마트 컨트랙트의 주소와 데이터는 사용자 단말에서 미리 설정된 형식에 맞게 작성되어 상기 이더리움 네트워크로 전송된 것인, 솔리디티 스마트 컨트랙트 실행 방법.

청구항 18

청구항 17에 있어서,

상기 시뮬레이션 노드는, 상기 이더리움 네트워크에 접속하여 솔리디티 스마트 컨트랙트 실행을 요청하는 사용자 요청에 따라 상기 공유로그 서버로부터 최신의 데이터를 읽어 자신의 상태를 업데이트하는, 솔리디티 스마트 컨트랙트 실행 방법.

청구항 19

청구항 18에 있어서,

상기 시뮬레이션 노드는 상기 솔리디티 스마트 컨트랙트의 실행을 위한 모듈인 가상 머신(Virtual Machine)을 복사하고, 복사된 가상 머신 복사 모듈에서 상기 솔리디티 스마트 컨트랙트를 시뮬레이션하고, 상기 공유로그

서버의 공유로그에 시뮬레이션 결과를 기록하는, 솔리디티 스마트 컨트랙트 실행 방법.

청구항 20

청구항 19에 있어서,

상기 마이닝 노드는 상기 공유로그 서버로부터 받은 데이터를 이용하여 블록을 생성하고, 생성된 블록을 블록체인 네트워크에 참여하는 다른 노드들로 전파하는, 솔리디티 스마트 컨트랙트 실행 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 공유로그 기반 솔리디티 스마트 컨트랙트 실행 방법 및 장치에 관한 것으로, 보다 상세하게는 공유로그 기반 솔리디티 스마트 컨트랙트 실행 환경 및 네트워크 구성을 위한 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 블록체인은 사용자 간의 신뢰 없이도 거래가 가능한 최초의 탈중앙화 서비스로 비트코인(Bitcoin)의 등장과 함께 큰 인기를 얻었다. 그 중 이더리움(Ethereum)은 솔리디티 스마트 컨트랙트(Solidity smart contract)를 지원하여 단순 화폐 거래뿐만 아니라 소셜 네트워크, 게임 등 사용자가 원하는 기능을 분산 어플리케이션으로 구현할 수 있는 블록체인 플랫폼이다. 이더리움은 Order-Execute 모델을 사용하기 때문에, 솔리디티 스마트 컨트랙트는 먼저 실행 순서가 정해진 뒤, 순서에 맞게 실행되게 된다. 따라서 동시에 복수의 트랜잭션을 실행할 수 없고, 이는 솔리디티 스마트 컨트랙트 처리 속도를 제한하게 된다.

[0003] 구체적으로, Order-Execute 모델은 많은 블록체인 플랫폼에서 사용되고 있는 트랜잭션 실행 모델로, 이름과 같이 먼저 트랜잭션의 실행 순서를 결정한 다음 각 트랜잭션을 실행하는 모델이다. Order-Execute 모델은 개념적으로 단순하여 구현이 쉽다는 장점이 있으나 단점도 많다.

[0004] Order-Execute 모델의 첫 번째 단점은 모든 트랜잭션이 순서대로 실행되어야 한다는 점이다. 사전에 정해진 순서대로 실행이 이루어져야 하는 모델의 특성상 이전 트랜잭션의 실행이 완료될 때까지 다음 트랜잭션은 실행될 수 없으며, 이는 트랜잭션 처리 속도를 하나의 노드의 트랜잭션 처리 속도로 제한하고 있다. 또한, 실행에 많은 시간이 필요한 트랜잭션을 고의로 추가하여 Denial-of-Service (DoS) 공격을 유도할 수 있다.

[0005] Order-Execute 모델의 두 번째 단점은 모든 트랜잭션이 결정적(deterministic)이어야 한다는 점이다. 이는 블록체인에 속한 모든 노드가 같은 순서로 트랜잭션을 실행하면 같은 결과를 얻어야 해서 필요한 성질이다. 이로 인해 이더리움의 경우, 솔리디티(Solidity)와 같은 특정 언어로 스마트 컨트랙트를 구현하도록 제한되어 있다.

[0006] 한편, 공유로그는 분산 시스템에서의 데이터 일관성 제공, 실행 기록 보관 등을 수행하는 기술이다. 공유로그는 읽기와 쓰기의 두 가지 동작만을 수행할 수 있으며, 모든 동작은 공유로그에 저장된다. 또한 공유로그의 내용은 변경 불가능하며, 공유로그에서 추가는 가능하지만, 삭제는 불가능하다.

[0007] 공유로그는 블록체인의 원장 구조와 유사한 형태를 띠고 있다. 둘의 공통점으로는 쓰인 데이터의 변경 불가, 기존 항목의 삭제 불가, 모든 사용자가 조회 가능하고 같은 데이터를 유지함 등이 있다. 따라서 블록체인 플랫폼에 공유로그를 적용하여 공유로그의 장점을 얻을 수 있다. 하지만, 공유로그를 블록체인 플랫폼에 적용한 방안은 아직까지 제안되고 있지 않다.

발명의 내용

해결하려는 과제

[0008] 이에 본 발명에서는 Order-Execute 모델이 아닌 Execute-Order 모델을 사용하여 솔리디티(Solidity) 스마트 컨트랙트가 병렬적으로 실행되고 그 결과를 이용해 순서를 결정함으로써 솔리디티 스마트 컨트랙트의 병렬적 실행을 가능하게 하는, 공유로그 기반 솔리디티 스마트 컨트랙트 실행 방법 및 장치를 제공하는데 있다.

[0009] 본 발명의 다른 목적은, 솔리디티 스마트 컨트랙트를 위한 시뮬레이션 노드, 공유로그, 마이닝 노드를 도입함으로써, 솔리디티 스마트 컨트랙트 실행 구조로 인한 속도 저하를 해결할 수 있는, 공유로그 기반 솔리디티 스마트 컨트랙트 실행 방법 및 장치를 제공하는데 있다.

[0010] 본 발명의 또 다른 목적은 이더리움 사용자의 동작에 영향을 주지 않으면서 솔리디티 스마트 컨트랙트의 병렬적 실행을 가능하게 하기 위해 Order-Execute 모델을 변경하여 기존 이더리움 동작을 모두 수행할 수 있는, 공유로그 기반 솔리디티 스마트 컨트랙트 실행 방법 및 장치를 제공하는데 있다.

과제의 해결 수단

[0011] 상기 기술적 과제를 해결하기 위한 본 발명의 일 측면에 따른 공유로그 기반 솔리디티 스마트 컨트랙트 실행 방법은, 솔리디티(Solidity) 스마트 컨트랙트를 실행하는 모델을 Execute-Order 모델로 변경하고, 공유로그 서버를 이용하여 솔리디티 스마트 컨트랙트가 실행 가능한 기존 사용자들이 같은 동작으로 결과를 얻을 수 있도록 구성된다.

[0012] 상기 솔리디티 스마트 컨트랙트 실행 방법은, 마이닝 노드의 구성 방법을 포함한다. 마이닝 노드의 구성 방법은, 사용자의 요청을 받아 가상 머신 복사 모듈을 통해 솔리디티 스마트 컨트랙트를 시뮬레이션하여 그 결과를 얻는 시뮬레이션 노드와 공유로그에 새로 추가된 항목들을 받아 이더리움 네트워크에 블록을 생성하고 전파하도록 구성될 수 있다.

[0013] 상기 솔리디티 스마트 컨트랙트 실행 방법은, 공유로그 서버의 구성 방법을 포함한다. 공유로그 서버는 시뮬레이션 노드들의 시뮬레이션 결과를 받아 정해진 순서대로 나열하는 시퀀서와 그 결과들을 저장하는 공유로그를 포함할 수 있다.

[0014] 상기 솔리디티 스마트 컨트랙트 실행 방법은 스마트 컨트랙트 실행 모델을 Execute-Order 모델로 변경하기 위해 솔리디티 스마트 컨트랙트를 실행한 결과를 시뮬레이션으로 얻는 모듈과, 시뮬레이션의 실행 결과를 모두 모아 순서를 결정하는 모듈과, 결정된 순서에 따라 블록을 생성하고 전파하는 모듈을 포함할 수 있다.

[0015] 상기 기술적 과제를 해결하기 위한 본 발명의 다른 측면에 따른 공유로그 기반 솔리디티(Solidity) 스마트 컨트랙트 실행 시스템은, 이더리움 네트워크로부터 솔리디티 스마트 컨트랙트의 주소와 데이터를 받고 상기 솔리디티 스마트 컨트랙트를 시뮬레이션하는 시뮬레이션 노드; 상기 시뮬레이션 노드로부터 받은 시뮬레이션 결과들의 순서를 결정하여 나열하고, 공유로그의 쓰기 요청이 성공하였음을 상기 시뮬레이션 노드로 전달하는 시퀀서; 및 상기 시퀀서가 결정한 순서대로 상기 공유로그에 저장된 공유로그 항목들의 마지막 항목 다음에 새로운 공유로그 항목을 추가하고, 정해진 개수의 공유로그 항목이 추가되거나 정해진 시간이 경과하는 경우, 새로 추가된 공유로그 항목들을 마이닝 노드로 전달하는 공유로그 서버를 포함한다.

[0016] 상기 시뮬레이션 노드는, 상기 이더리움 네트워크에 접속하여 상기 솔리디티 스마트 컨트랙트의 실행을 요청하는 사용자 요청에 따라 상기 공유로그 서버로부터 최신의 데이터를 읽어 자신의 상태를 업데이트할 수 있다.

[0017] 상기 시뮬레이션 노드는 상기 솔리디티 스마트 컨트랙트의 실행을 위한 모듈인 가상 머신(Virtual Machine)을 복사하고, 복사된 가상 머신 복사 모듈에서 상기 솔리디티 스마트 컨트랙트를 시뮬레이션할 수 있다.

[0018] 상기 시뮬레이션의 실행 결과는 소비된 가스의 총량, 변경된 계정 및 그 데이터를 포함한다.

[0019] 상기 시뮬레이션 노드는, 상기 솔리디티 스마트 컨트랙트의 실행을 위한 모듈인 가상 머신, 상기 가상 머신을 복사하여 상기 솔리디티 스마트 컨트랙트를 시뮬레이션하는 가상 머신 복사 모듈, 및 상기 공유로그 서버와 데이터 송수신을 수행하고 상기 공유로그 서버의 공유로그에 시뮬레이션 결과를 기록하고 상기 공유로그에 기록된 최신의 데이터를 읽는 공유로그 런타임 모듈을 구비할 수 있다.

[0020] 상기 공유로그 서버는, 상기 시뮬레이션 노드의 시뮬레이션 결과들을 받아 순서를 결정하여 나열하는 시퀀서; 및 상기 시퀀서가 결정한 순서대로 상기 시뮬레이션 결과들에 대응하는 공유로그 항목들을 저장하고, 기저장된 공유로그 항목들의 마지막 항목 다음에 새로운 공유로그 항목을 추가하여 저장하는 공유로그를 포함한다.

[0021] 상기 솔리디티 스마트 컨트랙트 실행 시스템은, 상기 공유로그 서버로부터 받은 데이터를 이용하여 블록을 생성하고, 생성된 블록을 이더리움 네트워크 또는 블록체인 네트워크에 참여하는 다른 노드들에게 전파하는 마이닝 노드를 더 포함할 수 있다.

[0022] 상기 기술적 과제를 해결하기 위한 본 발명의 또 다른 측면에 따른 공유로그 기반 솔리디티(Solidity) 스마트 컨트랙트 실행 방법은, 솔리디티 스마트 컨트랙트 실행 시스템의 시뮬레이션 노드에 의해 수행되는 공유로그 기반 솔리디티 스마트 컨트랙트 실행 방법으로서, 이더리움 네트워크로부터 솔리디티 스마트 컨트랙트의 주소와 데이터를 받는 단계-상기 솔리디티 스마트 컨트랙트의 주소와 데이터는 사용자 단말에서 미리 설정된 형식에 맞게 작성되어 상기 이더리움 네트워크로 전송된 것임-; 상기 솔리디티 스마트 컨트랙트의 실행을 위한 모듈인 가

상 머신(Virtual Machine)을 복사하는 단계; 상기 가상 머신을 복사한 가상 머신 복사 모듈에서 상기 솔리디티 스마트 컨트랙트를 시뮬레이션하는 단계; 상기 시뮬레이션의 실행 결과를 공유로그 서버의 공유로그에 기록하는 단계; 및 상기 공유로그 서버로부터 상기 공유로그의 쓰기 요청에 대한 성공 메시지를 수신하는 단계를 포함한다.

[0023] 상기 솔리디티 스마트 컨트랙트 실행 방법은, 상기 이더리움 네트워크에 접속하여 상기 솔리디티 스마트 컨트랙트의 실행을 요청하는 사용자 요청에 따라 상기 공유로그 서버로부터 최신의 데이터를 읽어 자신의 상태를 업데이트하는 단계를 더 포함할 수 있다.

[0024] 상기 공유로그 서버는 상기 시뮬레이션의 실행 결과를 받아 정해진 순서대로 나열하여 공유로그에 저장하고, 상기 공유로그의 마지막 항목 다음에 새로운 공유로그 항목을 추가하고, 정해진 개수의 공유로그 항목이 추가되거나 정해진 시간이 경과하는 경우, 새로 추가된 공유로그 항목들을 마이닝 노드로 전달하도록 구성될 수 있다.

[0025] 상기 마이닝 노드는 상기 공유로그 서버로부터 받은 데이터를 이용하여 블록을 생성하고, 생성된 블록을 이더리움 네트워크 또는 블록체인 네트워크에 참여하는 다른 노드들에게 전파하도록 구성될 수 있다.

[0026] 상기 기술적 과제를 해결하기 위한 본 발명의 또 다른 측면에 따른 공유로그 기반 솔리디티(Solidity) 스마트 컨트랙트 실행 방법은, 솔리디티 스마트 컨트랙트 실행 시스템의 공유로그 서버에 의해 수행되는 공유로그 기반 솔리디티 스마트 컨트랙트 실행 방법으로서, 시뮬레이션 노드로부터 시뮬레이션의 실행 결과를 받는 단계-상기 시뮬레이션 노드는 이더리움 네트워크로부터 솔리디티 스마트 컨트랙트의 주소와 데이터를 받고 상기 솔리디티 스마트 컨트랙트를 시뮬레이션함-; 상기 시뮬레이션의 실행 결과를 정해진 순서대로 나열하는 단계; 상기 순서대로 나열되고 공유로그에 저장된 공유로그 항목들의 마지막 항목에 새로운 공유로그 항목을 추가하는 단계; 및 상기 공유로그에 정해진 개수의 공유로그 항목이 추가되거나 정해진 시간이 경과하는 경우, 새로 추가된 공유로그 항목들을 마이닝 노드로 전달하는 단계를 포함한다.

[0027] 상기 솔리디티 스마트 컨트랙트 실행 방법은 상기 공유로그의 쓰기 요청이 성공하였음을 상기 시뮬레이션 노드들로 전달하는 단계를 더 포함할 수 있다.

[0028] 상기 시뮬레이션 노드는, 상기 이더리움 네트워크에 접속하여 솔리디티 스마트 컨트랙트 실행을 요청하는 사용자 요청에 따라 상기 공유로그 서버로부터 최신의 데이터를 읽어 자신의 상태를 업데이트하도록 구성될 수 있다.

[0029] 상기 시뮬레이션 노드는 상기 솔리디티 스마트 컨트랙트의 실행을 위한 모듈인 가상 머신(Virtual Machine)을 복사하고, 복사된 가상 머신 복사 모듈에서 상기 솔리디티 스마트 컨트랙트를 시뮬레이션하고, 상기 공유로그 서버의 공유로그에 시뮬레이션 결과를 기록하도록 구성될 수 있다.

[0030] 상기 마이닝 노드는 상기 공유로그 서버로부터 받은 데이터를 이용하여 블록을 생성하고, 생성된 블록을 블록체인 네트워크에 참여하는 다른 노드들로 전파하도록 구성될 수 있다.

[0031] 상기 시뮬레이션의 실행 결과는 소비된 가스의 총량, 변경된 계정 및 그 데이터를 포함할 수 있다.

[0032] 상기 솔리디티 스마트 컨트랙트의 주소와 데이터는 사용자 단말에서 미리 설정된 형식에 맞게 작성되어 상기 이더리움 네트워크로 전송된 것일 수 있다.

발명의 효과

[0033] 전술한 본 발명에 의하면, 스마트 컨트랙트 실행 환경에 공유로그 기술을 적용함으로써, 이더리움과 같은 솔리디티(Solidity) 스마트 컨트랙트를 병렬적으로 실행할 수 있고, 솔리디티 스마트 컨트랙트 실행 구조로 인한 속도 저하를 해결할 수 있고, 솔리디티 스마트 컨트랙트 사용자의 동작을 영향을 주지 않으면서 기존의 솔리디티 스마트 컨트랙트 동작을 모두 수행할 수 있으며, 그에 의해 트랜잭션 처리 성능을 향상시키는 솔리디티 스마트 컨트랙트 실행 환경을 제공할 수 있다.

[0034] 이러한 본 발명의 효과를 나열하면 다음과 같다.

[0035] 첫째, 이더리움 사용자의 사용 방법과 완벽하게 호환되어, 사용자는 기존 이더리움의 방식과 같은 방법으로 트랜잭션을 제출하여 그 실행 결과를 얻을 수 있다.

[0036] 둘째, Order-Execute 모델이 아닌 Execute-Order 모델을 사용하여 복수의 솔리디티 스마트 컨트랙트를 병렬적으로 실행할 수 있으며 처리 속도의 향상을 얻을 수 있다.

[0037] 셋째, 이더리움만이 아닌 솔리디티 스마트 컨트랙트를 실행할 수 있는 다른 블록체인에서도 적용 가능하다.

[0038] 넷째, 현재 모든 솔리디티 스마트 컨트랙트의 실행 순서를 결정하는 공유로그의 시퀀서를 하나만 사용하는 것으로 예시하고 있으나, 모든 솔리디티 스마트 컨트랙트의 실행 순서를 결정하는 공유로그의 시퀀서에 복수의 시퀀서들을 사용할 수 있으며, 그 경우 각 시퀀서의 부담을 줄여 트랜잭션 처리 성능을 용이하게 증가시킬 수 있다.

도면의 간단한 설명

[0039] 도 1은 본 발명의 일실시예에 따른 공유로그 기반 솔리디티(Solidity) 스마트 컨트랙트의 실행 시스템을 설명하기 위한 개략적인 블록도이다.

도 2는 도 1의 솔리디티 스마트 컨트랙트 실행 시스템에 채용할 수 있는 시뮬레이션 노드의 구성을 설명하기 위한 블록도이다.

도 3은 도 1의 솔리디티 스마트 컨트랙트 실행 시스템에 채용할 수 있는 공유로그 서버의 구조와 그 작동 원리를 설명하기 위한 블록도이다.

도 4는 본 발명의 다른 실시예에 따른 공유로그 기반 솔리디티 스마트 컨트랙트의 실행 시스템을 설명하기 위한 개략적인 블록도이다.

도 5는 본 발명의 또 다른 실시예에 따른 공유로그 기반 솔리디티 스마트 컨트랙트의 실행 방법에 대한 흐름도이다.

도 6은 본 발명의 또 다른 실시예에 따른 공유로그 기반 솔리디티 스마트 컨트랙트의 실행 방법의 또 다른 형태에 대한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0040] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0041] 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0042] 본 출원의 실시예들에서, 'A 및 B 중에서 적어도 하나'는 'A 또는 B 중에서 적어도 하나' 또는 'A 및 B 중 하나 이상의 조합들 중에서 적어도 하나'를 의미할 수 있다. 또한, 본 출원의 실시예들에서, 'A 및 B 중에서 하나 이상'은 'A 또는 B 중에서 하나 이상' 또는 'A 및 B 중 하나 이상의 조합들 중에서 하나 이상'을 의미할 수 있다.

[0043] 어떤 구성요소가 다른 구성요소에 '연결되어' 있다거나 '접속되어' 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 '직접 연결되어' 있다거나 '직접 접속되어'있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0044] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, '포함한다' 또는 '가진다' 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0045] 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 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가진 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0046] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 본 발명을 설명함에 있어 전체적인 이해를 용이하게 하기 위하여 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다.

[0047] 도 1은 본 발명의 일실시예에 따른 공유로그 기반 솔리디티(Solidity) 스마트 컨트랙트의 실행 시스템을 설명하기 위한 개략적인 블록도이다.

[0048] 도 1을 참조하면, 솔리디티 스마트 컨트랙트 실행 시스템(500)은, 이더리움 네트워크(600)에 접속하여 솔리디티 스마트 컨트랙트의 실행을 요청하는 사용자 또는 사용자 단말(100)로부터 요청을 받아 시뮬레이션을 진행하는 시뮬레이션 노드(200)와, 시뮬레이션 노드(200)가 전송한 시뮬레이션 결과의 순서를 결정하는 시퀀서(310) 및 결정된 순서에 대한 시뮬레이션 결과 즉, 공유로그 항목들이 쓰여지는 공유로그를 포함하는 공유로그 서버(300)와, 공유로그에 새로 추가된 항목들로 블록을 생성하여 전파하는 마이닝 노드(400)를 포함할 수 있다.

[0049] 시뮬레이션 노드(200)는 이더리움 네트워크(600)로부터 솔리디티 스마트 컨트랙트(Solidity smart contract, SSC)의 주소와 데이터를 받고, 이를 토대로 획득한 SSC를 시뮬레이션한다. SSC의 주소와 데이터는 사용자 단말에서 미리 설정된 형식에 맞게 작성되어 이더리움 네트워크로 전송된 것일 수 있다.

[0050] 시뮬레이션 노드(200)는 이더리움 네트워크(600)에 접속하여 SSC의 실행을 요청하는 사용자의 사용자 요청에 따라 공유로그 서버(300)로부터 최신의 데이터를 읽어 자신의 상태를 업데이트할 수 있다. 이러한 시뮬레이션 노드(200)는 복수의 사용자 단말들에 각각 대응하는 복수의 시뮬레이션 노드들을 포함할 수 있다.

[0051] 시퀀서(310)는 공유로그 서버(300)에 탑재될 수 있다. 시퀀서(310)는 시뮬레이션 노드(200)로부터 받은 시뮬레이션 결과들의 순서를 결정하여 나열하고, 공유로그의 쓰기 요청이 성공하였음을 시뮬레이션 노드(200)로 전달할 수 있다.

[0052] 또한, 시퀀서(310)는 시뮬레이션 노드들로부터 트랜잭션 시뮬레이션 결과를 공유로그에 작성하는 요청을 받을 수 있다. 시퀀서(310)는 해당 요청들을 처리할 때, 요청 사이의 충돌(conflict)을 분석하여 최소한의 중지(abort)를 일으킬 수 있도록 충돌 분석 및 해결(conflict analysis & resolve)을 위한 알고리즘으로 동작할 수 있다. 여기서, 충돌 분석(conflict analysis) 방법은 요청들을 이용하여 충돌 DAG(Directed Acyclic Graph)를 그리고, 사이클(cycle)이 생기는 부분을 확인하고, 그 중에서 가장 많은 사이클에 포함된 특정 요청(TX)을 제거하며 사이클이 없어질 때까지 반복하도록 구성될 수 있다. 여기서 제거된 요청들(TX)만 중지되면 요청들 간에 충돌은 일어나지 않는다.

[0053] 공유로그 서버(300)는 시퀀서(310)가 결정한 순서대로 공유로그에 저장된 공유로그 항목들의 마지막 항목 다음에 새로운 공유로그 항목을 추가하고, 정해진 개수의 공유로그 항목이 추가되거나 정해진 시간이 경과하는 경우에 새로 추가된 공유로그 항목들을 마이닝 노드(400)로 전달할 수 있다.

[0054] 마이닝 노드(400)는 공유로그 서버(300)로부터 받은 데이터를 이용하여 블록을 생성하고, 생성된 블록을 이더리움 네트워크(600) 또는 블록체인 네트워크에 참여하는 다른 노드들(610)에게 전파할 수 있다.

[0055] SSC 실행 시스템(500)은 이더리움(Ethereum) 네트워크(600)에 존재하는 레거시(Legacy) 이더리움 클라이언트 노드(610)에 블록을 전파하도록 구성될 수 있다.

[0056] 이더리움 네트워크(600)는, 블록체인 네트워크 참여자를 특별히 제한할 필요가 없으므로, 비허가형 블록체인으로 구성될 수 있다. 이러한 이더리움 네트워크(600)는 솔리디티 스마트 컨트랙트를 이용하는 블록체인 네트워크의 일종을 의미할 수 있다. SSC 실행 시스템(500)의 시뮬레이션 노드(200)와 마이닝 노드(400)는 이더리움 네트워크(600)에 포함되거나 이더리움 네트워크(600)의 일부 노드들로서 기능할 수 있다.

[0057] SSC의 실행을 요청하는 사용자는 기존 이더리움 네트워크를 사용하는 사용자를 포함하며, 기존 사용자와 같은 동작으로 SSC의 실행 결과를 확인할 수 있다.

[0058] SSC 실행 시스템(500)은 SSC를 시뮬레이션 노드(200)에서 실행하고, 시뮬레이션 결과로 정해진 순서에 맞게 공유로그 서버(300)에 시뮬레이션 결과를 저장하고, 마이닝 노드(400)에서 블록을 직접 생성하는 기존 방식과 다르게, 마이닝 노드(400)가 공유로그 서버(300)의 데이터만으로 블록을 생성하고 이를 이더리움 네트워크(600)로 전파하여 이더리움 네트워크(600)에 존재하는 레거시 이더리움 클라이언트 노드들(610)이 업데이트될 수 있도록 한다.

[0059] 도 2는 도 1의 솔리디티 스마트 컨트랙트 실행 시스템에 채용할 수 있는 시뮬레이션 노드의 구성을 설명하기 위

한 블록도이다.

[0060] 도 2를 참조하면, 공유로그 기반 솔리디티 실행 환경에 속한 시뮬레이션 노드(200)는 가상 머신(210), 가상 머신 복사 모듈(220) 및 공유로그 런타임 모듈(230)을 포함할 수 있다.

[0061] 가상 머신(210)은 이더리움 가상머신(Ethereum virtual machine, EVM)을 포함할 수 있다. 가상 머신(210)은 SSC 실행을 위해 필요한 모듈로서 기존 이더리움 네트워크의 이더리움 노드로도 존재할 수 있다. 가상 머신(210)은 이더리움 네트워크로부터 SSC의 주소와 데이터를 받을 수 있다. SSC의 주소와 데이터는 사용자 단말(100)에서 미리 설정된 형식에 맞게 작성되어 이더리움 네트워크로 전송된 것일 수 있다.

[0062] 또한, 가상 머신(210)은 사용자 요청에 따라 공유로그 서버로부터 최신의 데이터를 읽어 자신의 상태를 업데이트할 수 있다. 이때, 사용자는 이더리움 네트워크에 접속하여 SCC의 실행을 요청하는 사용자 단말(100)을 포함할 수 있다.

[0063] 가상 머신 복사 모듈(220)은 이더리움 가상머신 복사모듈을 포함할 수 있다. 가상 머신 복사 모듈(220)은 가상 머신(210)를 복사하여 SSC를 시뮬레이션하고 그 실행 결과를 확인하기 위한 모듈이다. 시뮬레이션의 실행 결과는 소비된 가스(Gas)의 총량, 변경된 계정 및 그 데이터를 포함할 수 있다. 가스는 이더리움 상에서 트랜잭션의 발생 수수료를 책정하기 위한 단위이며 그 사용량은 정해져 있다.

[0064] 공유로그 런타임 모듈(230)은 시뮬레이션 노드와 공유로그 서버와의 데이터 간의 데이터 송수신을 위한 모듈이다. 공유로그 런타임 모듈(230)은 가상 머신 복사 모듈(230)의 시뮬레이션 결과를 시퀀서(310)에 전달할 수 있다. 또한, 공유로그 런타임 모듈(230)은 공유로그 서버의 공유로그에 시뮬레이션 결과를 기록하고 공유로그에 기록된 최신의 데이터를 읽도록 구성될 수 있다.

[0065] 도 3은 도 1의 솔리디티 스마트 컨트랙트 실행 시스템에 채용할 수 있는 공유로그 서버의 구조와 그 작동 원리를 설명하기 위한 블록도이다.

[0066] 도 3을 참조하면, 공유로그 서버(300)는 시퀀서(310) 및 공유로그(330)를 포함할 수 있다.

[0067] 시퀀서(310)는 시뮬레이션 노드(200)로부터 SSC를 시뮬레이션하여 얻은 시뮬레이션 결과를 받아 사전에 정의된 순서대로 정렬하여 공유로그(330)에 쓰일 위치를 토큰의 형태로 공유로그(330)에 전달하는 모듈이다. 다시 말해서, 시퀀서(310)는 시뮬레이션 노드(200)의 시뮬레이션 결과들을 받아 순서를 결정하여 나열하도록 구성될 수 있다.

[0068] 공유로그(330)는 시퀀서(310)에 모인 시뮬레이션 결과들을 순서에 맞게 기저장된 공유로그 항목들의 가장 끝에서부터 새로운 공유로그 항목을 추가하는 모듈이다. 다시 말해서, 공유로그(330)는 시퀀서(310)가 결정한 순서대로 시뮬레이션 결과들에 대응하는 공유로그 항목들을 저장하고, 기저장된 공유로그 항목들의 마지막 항목 다음에 새로운 공유로그 항목을 추가하여 저장하도록 구성될 수 있다.

[0069] 공유로그 서버(300)는, 공유로그(330)에 미리 정해진 개수의 공유로그 항목이 추가되거나 정해진 시간이 경과하는 경우, 새로 추가된 공유로그 항목들을 마이닝 노드(400)로 전달할 수 있다.

[0070] 도 4는 본 발명의 다른 실시예에 따른 공유로그 기반 솔리디티 스마트 컨트랙트의 실행 시스템을 설명하기 위한 개략적인 블록도이다.

[0071] 도 4를 참조하면, SSC 실행 시스템(400)은, 적어도 하나의 프로세서(410)를 포함할 수 있다. 이 경우, 적어도 하나의 프로세서(410)는 시뮬레이션 노드를 포함하거나, 시뮬레이션 노드와 마이닝 노드를 포함하거나, 공유로그 서버를 포함하거나, 공유로그 서버와 시뮬레이션 노드를 포함하거나, 시뮬레이션 노드와 공유로그 서버 및 마이닝 노드를 포함하도록 구성될 수 있다. 이때, 시뮬레이션 노드, 공유로그 서버 및 마이닝 노드 각각 또는 이들의 조합은 적어도 하나의 소프트웨어 모듈이나 적어도 하나의 프로그램 명령으로 구현되어 프로세서(410)에 탑재될 수 있다.

[0072] 또한, SSC 실행 시스템(400)은, 선택적으로 메모리(420), 송수신 장치(430)입력 인터페이스 장치(440), 출력 인터페이스 장치(450), 저장 장치(460) 또는 이들의 조합 구성을 더 포함할 수 있다. SSC 실행 시스템(400)에 포함된 각각의 구성 요소들은 버스(bus, 470)에 의해 연결되어 서로 통신을 수행할 수 있다.

[0073] 프로세서(410)는 메모리(420) 및 저장 장치(460) 중에서 적어도 하나에 저장된 프로그램 명령(program command)을 실행할 수 있다. 프로그램 명령은 적어도 하나의 소프트웨어 모듈을 구비할 수 있다. 프로세서(410)는 중앙 처리 장치(central processing unit, CPU), 그래픽 처리 장치(graphics processing unit, GPU), 또는 본 발

명의 실시예에 따른 방법들 중 적어도 하나의 방법이 수행되는 전용의 프로세서를 의미할 수 있다. 메모리(420) 및 저장 장치(460) 각각은 휘발성 저장 매체 및 비휘발성 저장 매체 중에서 적어도 하나로 구성될 수 있다. 예를 들어, 메모리(420)는 읽기 전용 메모리(read only memory, ROM) 및 랜덤 액세스 메모리(random access memory, RAM) 중에서 적어도 하나로 구성될 수 있다.

[0074] 송수신 장치(430)는 이더리움 네트워크와의 연결, 이더리움 네트워크 또는 다른 통신 네트워크를 통한 사용자 단말과의 연결을 지원하는 수단이나 이러한 수단에 상응하는 기능을 수행하는 구성부를 포함한다. 송수신 장치(430)는 유선, 무선 또는 유무선 서브통신시스템을 포함할 수 있다.

[0075] 입력 인터페이스 장치(440)는 키보드, 마이크, 터치패드, 터치스크린 등의 입력 수단들과, 입력 수단들 중에서 선택되는 적어도 하나와 적어도 하나의 입력 수단을 통해 입력되는 신호를 기저장된 명령과 매핑하거나 처리하여 프로세서(410)로 전달하는 입력 신호 처리부를 포함할 수 있다.

[0076] 출력 인터페이스 장치(450)는 프로세서(410)의 제어에 따라 출력되는 신호를 기저장된 신호 형태나 레벨로 매핑하거나 처리하는 출력 신호 처리부와, 출력 신호 처리부의 신호에 따라 진동, 빛 등의 형태로 신호나 정보를 출력하는 적어도 하나의 출력 수단을 포함할 수 있다. 적어도 하나의 출력 수단은 스피커, 디스플레이 장치, 프린터, 광 출력 장치, 진동 출력 장치 등의 출력 수단들에서 선택되는 적어도 하나를 포함할 수 있다.

[0077] 명세서 전체에서 SSC 실행 시스템(400)은 퍼스널 컴퓨터, 웹 서버, 컴퓨팅 서버, 애플리케이션 서버, 데이터베이스 서버, 파일 서버, 게임 서버, 메일 서버, 프록시 서버 또는 이들의 조합 형태를 의미할 수 있으며, 각 장치의 전부 또는 일부의 기능을 포함할 수 있다.

[0078] 또한, 컴퓨팅 서버는 무선 단말, 유선 단말 또는 이들의 혼합 형태인 유무선 단말을 포함할 수 있다. 무선 단말은 이동 단말(mobile terminal), 이동국(mobile station), 진보된 이동국(advanced mobile station), 고신뢰성 이동국(high reliability mobile station), 가입자국(subscriber station), 휴대 가입자국(portable subscriber station), 접근 단말(access terminal), 사용자 장비(user equipment) 등을 지칭할 수 있고, 각 장치의 전부 또는 일부의 기능을 포함할 수 있다. 그리고, 유선 단말은 네트워크에 연결되어 신호 및 데이터를 송수신하고 공유로그 기반으로 스마트 컨트랙트 실행 환경을 구성할 수 있는 기존의 단말 장치, 네트워크 터미널, 컴퓨팅 장치를 모두 포함할 수 있다.

[0079] 도 5는 본 발명의 또 다른 실시예에 따른 공유로그 기반 솔리디티 스마트 컨트랙트의 실행 방법에 대한 흐름도이다.

[0080] 도 5를 참조하면, SSC 실행 시스템의 시뮬레이션 노드에 의해 수행되는 공유로그 기반 SSC 실행 방법은, 먼저 이더리움 네트워크로부터 SSC의 주소와 데이터를 받을 수 있다(S510). 여기서 SSC의 주소와 데이터는 사용자 단말에서 미리 설정된 형식에 맞게 작성되어 이더리움 네트워크로 전송된 것일 수 있다.

[0081] 다음, 사용자 요청에 따라 공유로그 서버로부터 최신의 데이터를 읽어 자신의 상태를 업데이트할 수 있다(S520). 여기서 사용자 요청은 사용자가 이더리움 네트워크에 접속하여 SSC의 실행을 요청하는 것을 의미할 수 있다.

[0082] 다음, SSC의 실행을 위한 모듈인 가상 머신(Virtual Machine)을 복사할 수 있다(S530).

[0083] 다음, 가상 머신을 복사한 가상 머신 복사 모듈에서 SSC를 시뮬레이션할 수 있다(S540).

[0084] 다음, 시뮬레이션의 실행 결과를 공유로그 서버의 시퀀서에 전달하거나 공유로그에 기록할 수 있다(S550).

[0085] 다음, 공유로그 서버로부터 공유로그의 쓰기 요청에 대한 성공 메시지를 수신할 수 있다(S560). 공유로그의 쓰기 요청에 대한 성공은 시뮬레이션 결과가 정해진 순서대로 공유로그에 정상적으로 쓰여진 것을 의미할 수 있다.

[0086] 한편, 공유로그의 쓰기 요청이 실패하면, 시뮬레이션 노드는 공유로그 서버로부터 최신의 데이터를 읽어 자신의 상태를 업데이트하는 단계(S520)부터 그 이하의 단계들을 다시 수행할 수 있다.

[0087] 전술한 과정 후에, 공유로그 서버는 정해진 순서대로 공유로그에 저장된 공유로그 항목들의 마지막 항목 다음에 새로운 공유로그 항목을 추가하고, 정해진 개수의 공유로그 항목이 추가되거나 정해진 시간이 경과하는 경우에 새로 추가된 공유로그 항목들을 마이닝 노드로 전달할 수 있다. 그리고, 마이닝 노드는 공유로그 서버로부터 받은 데이터를 이용하여 블록을 생성하고, 생성된 블록을 이더리움 네트워크 또는 블록체인 네트워크에 참여하는 다른 노드들에게 전파할 수 있다.

[0088] 도 6은 본 발명의 또 다른 실시예에 따른 공유로그 기반 솔리디티 스마트 컨트랙트의 실행 방법의 또 다른 형태에 대한 흐름도이다.

[0089] 도 6을 참조하면, SSC 실행 시스템의 공유로그 서버에 의해 수행되는 공유로그 기반 솔리디티 스마트 컨트랙트 실행 방법은, 먼저 시뮬레이션 노드로부터 시뮬레이션의 실행 결과를 받을 수 있다(S610). 여기서 시뮬레이션 노드는 이더리움 네트워크로부터 SSC의 주소와 데이터를 받고 SSC를 시뮬레이션할 수 있다.

[0090] 다음, 시뮬레이션의 실행 결과를 정해진 순서대로 나열할 수 있다(S620). 정해진 순서는 시뮬레이션 결과에 따른 공유로그 항목들을 공유로그에 쓰일 위치를 토큰의 형태로 정의한 것일 수 있다.

[0091] 정해진 순서대로 시뮬레이션 결과가 공유로그에 정상적으로 저장되면, 즉 공유로그의 쓰기 요청이 성공하면, 해당 신호나 성공 메시지를 시뮬레이션 노드들로 전달할 수 있다. 시뮬레이션의 실행 결과는 소비된 가스의 총량, 변경된 계정 및 그 데이터를 포함할 수 있다.

[0092] 다음, 상기 순서대로 나열되고 공유로그에 저장된 공유로그 항목들의 마지막 항목 다음에 새로운 공유로그 항목을 추가할 수 있다(S630). 즉, 공유로그는 시퀀서에 모인 시뮬레이션 결과들을 순서에 맞게 공유로그에 저장하고, 저장된 시뮬레이션 결과들에 대응하는 공유로그 항목들의 가장 끝에서부터 새로운 공유로그 항목을 추가하도록 동작할 수 있다.

[0093] 다음, 공유로그에 정해진 개수의 새로운 공유로그 항목이 추가되거나 정해진 시간이 경과하였는지를 판단할 수 있다(S640).

[0094] 위의 판단 단계(S640)의 판단 결과, 정해진 개수의 새로운 공유로그 항목이 추가되었거나 정해진 시간이 경과한 경우에, 새로 추가된 공유로그 항목들을 마이닝 노드로 전달할 수 있다(S650). 마이닝 노드는 공유로그 서버로부터 받은 데이터를 이용하여 블록을 생성하고, 생성된 블록을 블록체인 네트워크에 참여하는 다른 노드들로 전파할 수 있다.

[0095] 본 실시예에 의하면, 이더리움과 같은 솔리디티 스마트 컨트랙트를 병렬적으로 실행하여 트랜잭션 처리 성능을 향상시키는 실행 환경을 제공할 수 있다. SSC 실행 환경은 좁은 의미에서 SSC 실행 시스템을 지칭할 수 있다.

[0096] 본 발명의 실시 예에 따른 방법의 동작은 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 프로그램 또는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의해 읽혀질 수 있는 정보가 저장되는 모든 종류의 기록장치를 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산 방식으로 컴퓨터로 읽을 수 있는 프로그램 또는 코드가 저장되고 실행될 수 있다.

[0097] 또한, 컴퓨터가 읽을 수 있는 기록매체는 롬(rom), 램(ram), 플래시 메모리(flash memory) 등과 같이 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치를 포함할 수 있다. 프로그램 명령은 컴파일러(compiler)에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터(interpreter) 등을 사용해서 컴퓨터에 의해 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

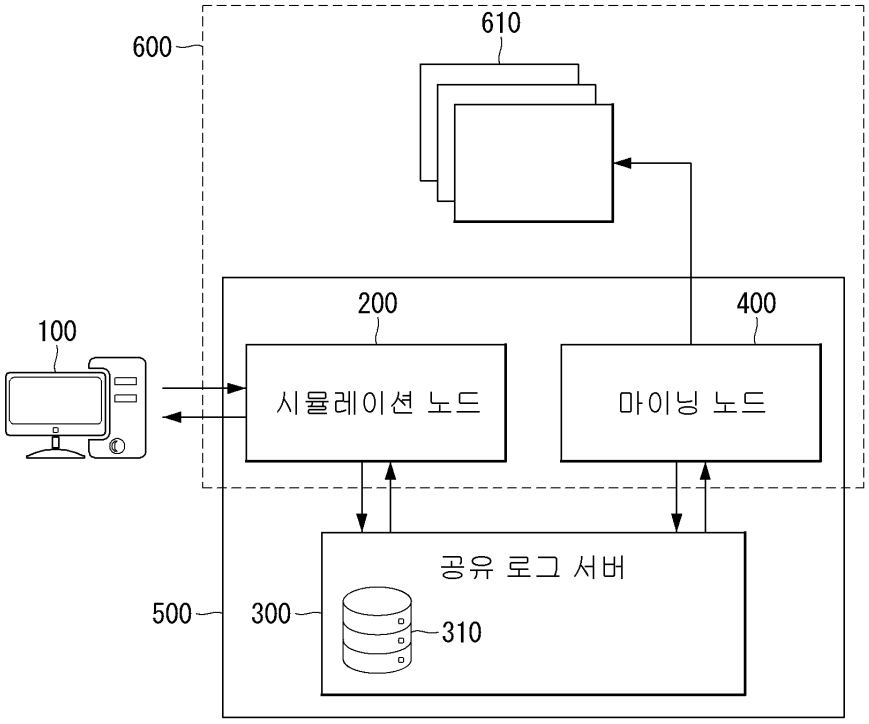
[0098] 본 발명의 일부 측면들은 장치의 문맥에서 설명되었으나, 그것은 상응하는 방법에 따른 설명 또한 나타낼 수 있고, 여기서 블록 또는 장치는 방법 단계 또는 방법 단계의 특징에 상응한다. 유사하게, 방법의 문맥에서 설명된 측면들은 또한 상응하는 블록 또는 아이템 또는 상응하는 장치의 특징으로 나타낼 수 있다. 방법 단계들의 몇몇 또는 전부는 예를 들어, 마이크로프로세서, 프로그램 가능한 컴퓨터 또는 전자 회로와 같은 하드웨어 장치에 의해(또는 이용하여) 수행될 수 있다. 몇몇의 실시 예에서, 가장 중요한 방법 단계들의 적어도 하나 이상은 이와 같은 장치에 의해 수행될 수 있다.

[0099] 실시 예들에서, 프로그램 가능한 로직 장치(예를 들어, 필드 프로그래머블 게이트 어레이)가 여기서 설명된 방법들의 기능의 일부 또는 전부를 수행하기 위해 사용될 수 있다. 실시 예들에서, 필드 프로그래머블 게이트 어레이(field-programmable gate array)는 여기서 설명된 방법들 중 하나를 수행하기 위한 마이크로프로세서(microprocessor)와 함께 작동할 수 있다. 일반적으로, 방법들은 어떤 하드웨어 장치에 의해 수행되는 것이 바람직하다.

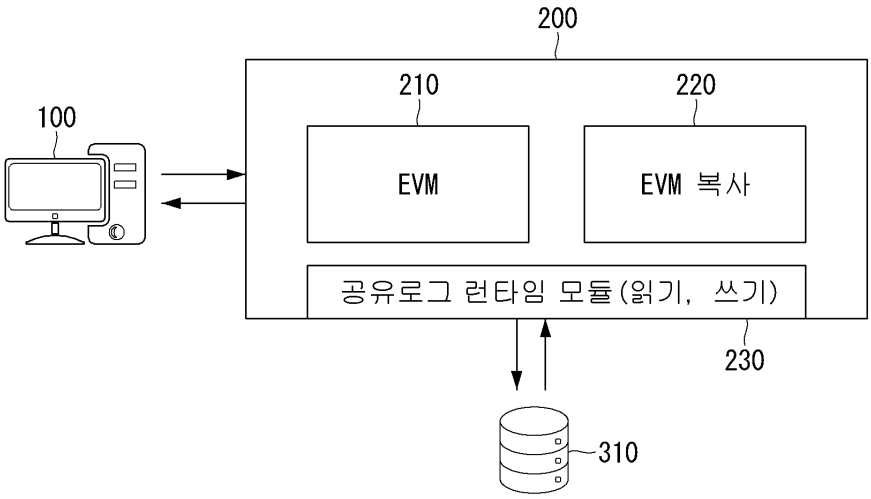
[0100] 이상 본 발명의 바람직한 실시 예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

도면

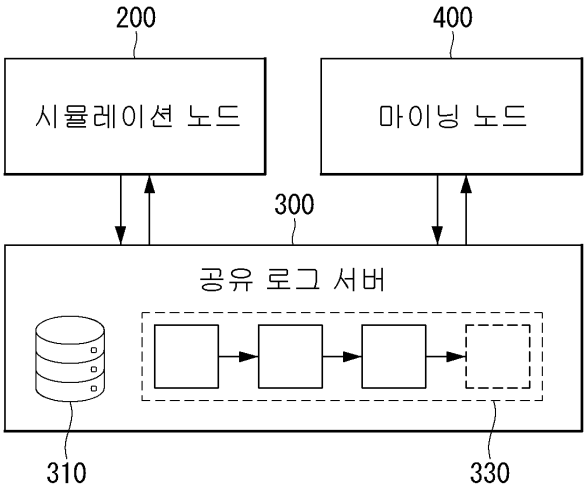
도면1


600
610
200
400
100
시뮬레이션 노드
마이닝 노드
공유 로그 서버
500
300
310

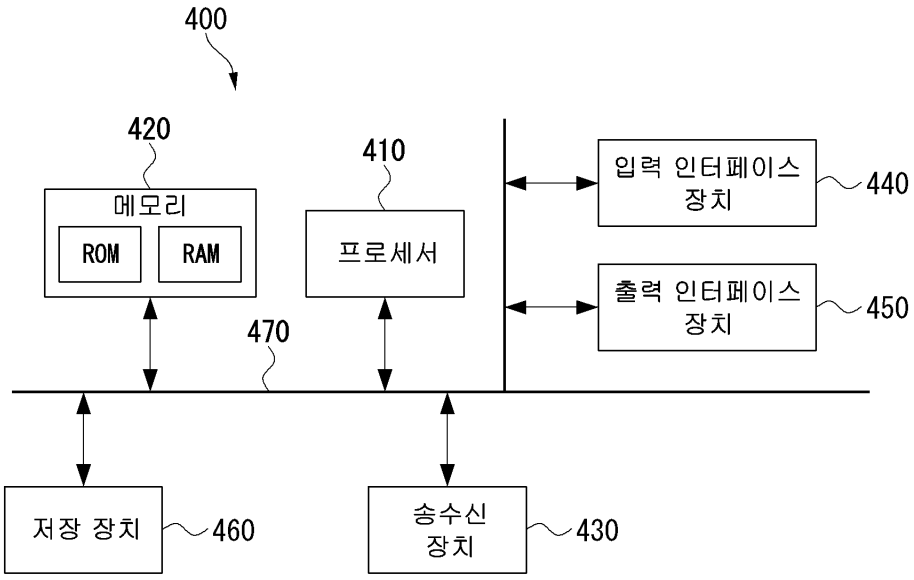
도면2


200
210
220
100
EVM
EVM 복사
공유로그 런타임 모듈(읽기, 쓰기)
230
310

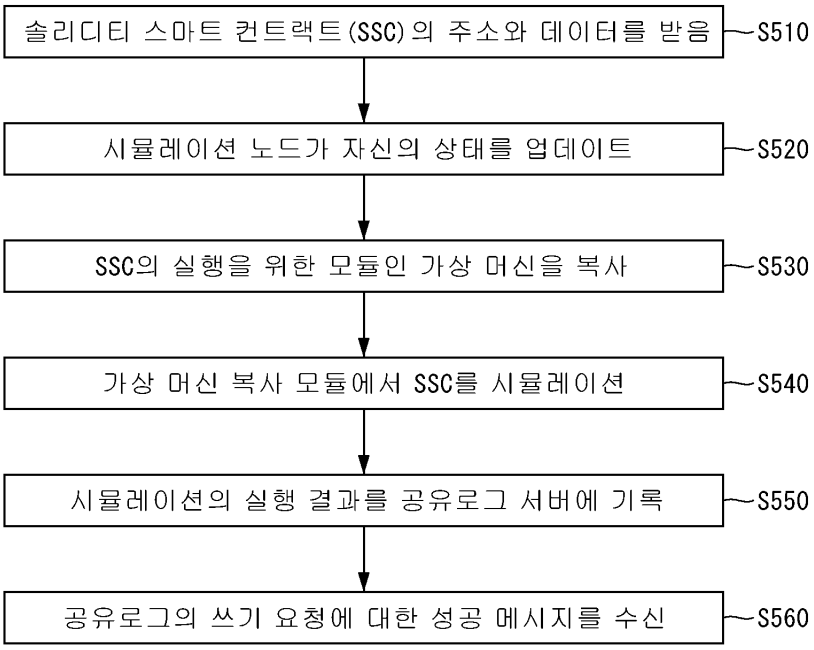
도면3


200
400
시뮬레이션 노드
마이닝 노드
300
공유 로그 서버
310
330

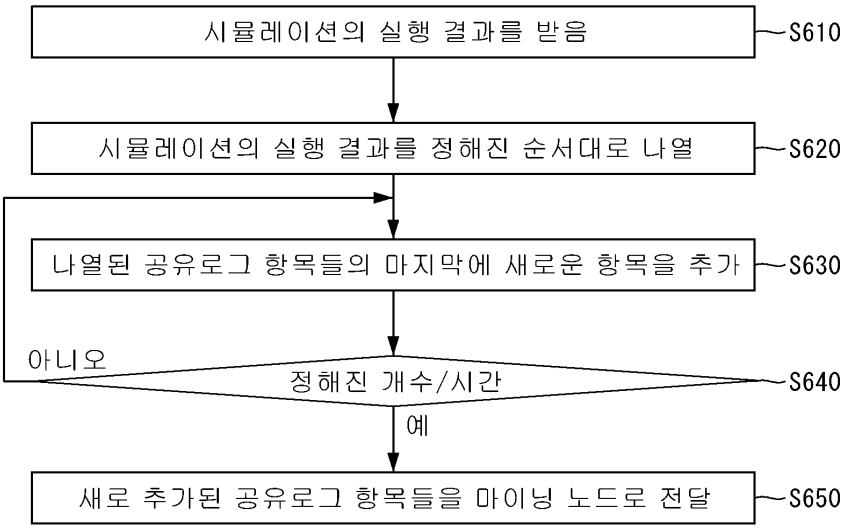
도면4


400
420
메모리
ROM
RAM
410
프로세서
입력 인터페이스 장치
440
출력 인터페이스 장치
450
470
저장 장치
460
송수신 장치
430

도면5


솔리디티 스마트 컨트랙트(SSC)의 주소와 데이터를 받음
S510
시뮬레이션 노드가 자신의 상태를 업데이트
S520
SSC의 실행을 위한 모듈인 가상 머신을 복사
S530
가상 머신 복사 모듈에서 SSC를 시뮬레이션
S540
시뮬레이션의 실행 결과를 공유로그 서버에 기록
S550
공유로그의 쓰기 요청에 대한 성공 메시지를 수신
S560

도면6


시뮬레이션의 실행 결과를 받음
S610
시뮬레이션의 실행 결과를 정해진 순서대로 나열
S620
나열된 공유로그 항목들의 마지막에 새로운 항목을 추가
S630
아니오
정해진 개수/시간
S640
예
새로 추가된 공유로그 항목들을 마이닝 노드로 전달
S650