(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2023년01월09일
(11) 등록번호 10-2485970
(24) 등록일자 2023년01월03일

(51) 국제특허분류(Int. Cl.)
H04L 65/40 (2022.01) *H04L 69/40* (2022.01)
(52) CPC특허분류
H04L 67/1095 (2022.05)
H04L 67/1093 (2022.05)
(21) 출원번호 10-2021-0066732
(22) 출원일자 2021년05월25일
심사청구일자 2021년05월25일
(65) 공개번호 10-2022-0035823
(43) 공개일자 2022년03월22일
(30) 우선권주장
1020200117921 2020년09월14일 대한민국(KR)
(56) 선행기술조사문헌
KR102002509 B1*
"hyperledger-fabricdocs Documentation", https://hyperledger-fabric.readthedocs.io/_/downloads/en/release-1.3/pdf/(2020.09.02)*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
포항공과대학교 산학협력단
경상북도 포항시 남구 청암로 77 (지곡동)
(72) 발명자
박찬익
경상북도 포항시 남구 지곡로 155, 6동 1105호
마정현
경기도 안산시 단원구 당곡2로 30, 903동 301호
(74) 대리인
특허법인이상

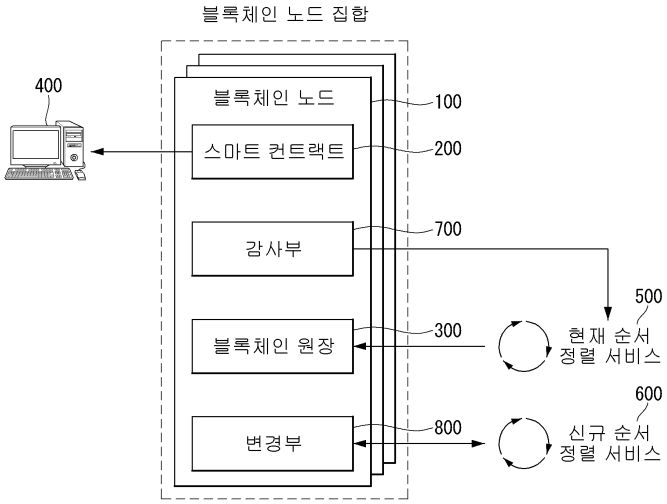
전체 청구항 수 : 총 14 항 심사관 : 이주민

(54) 발명의 명칭 **비잔틴 장애를 감내하는 블록체인 시스템 및 그 시스템 내의 블록체인 노드의 동작 방법**

(57) 요 약

본 발명의 블록체인 플랫폼에서 비잔틴 장애 감내 방법은, 블록체인 순서 정렬 서비스의 동작을 분석하는 감사 트랜잭션 분석 방법에 있어서, 적어도 하나의 수신한 블록내에 포함되어 있는 각 블록체인 노드가 제출한 감사 트랜잭션 분석을 통해 수신한 각 블록의 합의 수준을 결정하는 단계 및 블록체인 노드에서 감사 트랜잭션 분석 과정의 오류 분석과 합의 수준 업데이트 지연 시간을 기반으로 순서 정렬 서비스의 악의적 공격 여부 및 오동작을 검출하는 단계를 포함한다.

대 표 도 - 도2



(52) CPC특허분류
H04L 67/51 (2022.05)
H04L 69/40 (2022.05)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711116985
과제번호	2020-0-00936-001
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	블록체인융합기술개발
연구과제명	5G 초저지연 서비스를 위한 무선 단말용 블록체인 기술 개발
기 여 율	1/1
과제수행기관명	포항공과대학교 산학협력단
연구기간	2020.04.01 ~ 2020.12.31

명 세 서

청구범위

청구항 1

비잔틴 장애를 감내하는 블록체인 시스템에 있어서,

복수의 순서 정렬 서비스 후보군; 및

상기 복수의 순서 정렬 서비스 후보군 중 현재 순서 정렬 서비스에 의하여 생성된 블록을 수신하고, 상기 수신된 블록을 감사한 결과를 제1 감사 트랜잭션으로서 생성하는 블록체인 노드;

를 포함하고,

상기 제1 감사 트랜잭션은 다른 블록체인 노드들로 전파되고,

상기 블록체인 노드는 적어도 상기 제1 감사 트랜잭션을 분석한 결과에 기반하여 상기 복수의 순서 정렬 서비스 후보군 중 상기 현재 순서 정렬 서비스를 대체할 다른 신규 순서 정렬 서비스를 위한 변경 제안 트랜잭션을 생성하는,

블록체인 시스템.

청구항 2

청구항 1에 있어서,

상기 블록체인 노드는 상기 제1 감사 트랜잭션, 및 상기 다른 블록체인 노드들로부터 수신된 제2 감사 트랜잭션의 분석 결과에 기반하여 상기 현재 순서 정렬 서비스를 변경하도록 제안하는 제1 변경 요청 메시지를 생성하고,

상기 제1 변경 요청 메시지는 상기 다른 블록체인 노드들로 전파되는,

블록체인 시스템.

청구항 3

청구항 2에 있어서,

상기 블록체인 노드는 상기 다른 블록체인 노드들로부터 상기 현재 순서 정렬 서비스를 변경하도록 제안하는 제2 변경 요청 메시지들이 수신된 개수가 임계값 이상이면 상기 변경 제안 트랜잭션을 생성하고,

상기 변경 제안 트랜잭션은 상기 신규 순서 정렬 서비스에 제출되고, 상기 변경 제안 트랜잭션은 상기 신규 순서 정렬 서비스에 의하여 상기 다른 블록체인 노드로 전파되는,

블록체인 시스템.

청구항 4

청구항 2에 있어서,

상기 블록체인 노드는 상기 제1 감사 트랜잭션 및 상기 제2 감사 트랜잭션의 분석 결과에 기반하여 각 블록의 합의 수준을 결정하고,

상기 블록체인 노드는 상기 제1 감사 트랜잭션 및 상기 제2 감사 트랜잭션의 분석 결과에 기반하여 얻어지는 오류 분석 결과와 합의 수준 업데이트 지연 시간을 기반으로 상기 현재 순서 정렬 서비스의 악의적 공격 여부 및 오동작을 검출하는,

블록체인 시스템.

청구항 5

청구항 4에 있어서,

상기 블록체인 노드가 상기 제1 감사 트랜잭션 및 상기 제2 감사 트랜잭션의 분석 결과에 기반하여 각 블록의 합의 수준을 결정함에 있어서,

블록체인 구조에서 모든 블록들이 해시 체인으로 연결되어 있는 특징을 활용하여, 해시 체인으로 연결된 두 블록에 중에서 블록의 높이가 더 높은 블록에 대한 감사 트랜잭션을, 블록의 높이가 더 낮은 블록에 대한 감사 트랜잭션으로 해석하는 블록 합의 수준 결정 기법을 이용하는,

블록체인 시스템.

청구항 6

청구항 4에 있어서,

상기 블록체인 노드가 상기 현재 순서 정렬 서비스의 악의적 공격 여부 및 오동작을 검출함에 있어서,

상기 블록체인 노드는 상기 현재 순서 정렬 서비스의 공격으로 인한 안정성(safety), 생존성(liveness), 그리고 공정성(fairness) 위반을 검출하고,

안정성(safety) 위반의 검출은, 블록체인상 동일한 높이의 블록에 대해 블록체인 노드들이 서로 다른 해시 값을 갖는 감사 트랜잭션을 제출한 경우를 판단함으로써 수행되고,

생존성(liveness) 위반의 검출은, 블록의 합의 수준이 유한하게 정해진 시간 동안 업데이트 되지 않는 경우를 판단함으로써 수행되고,

공정성(fairness) 위반의 검출은, 블록체인상 동일한 범위 내에 위치한 블록들에서 확인되는 감사 트랜잭션 개수가 각 블록체인 노드들 간에 불균형이 확인되는 경우를 판단함으로써 수행되는,

블록체인 시스템.

청구항 7

비잔틴 장애를 감내하는 블록체인 시스템 내의 블록체인 노드의 동작 방법에 있어서,

블록체인 노드가 순서 정렬 서비스 변경을 제안하는 변경 요청 메시지를 생성하고 다른 블록체인 노드들로 전파하는 단계;

각 블록체인 노드로부터 수신한 변경 요청 메시지를 분석하여, 소정의 수 이상의 블록체인 노드들이 변경에 동의한다고 판단하는 경우, 신규 순서 정렬 서비스를 위한 변경 제안 트랜잭션을 생성하여 이를 변경될 순서 정렬 서비스에 제출하는 단계;

블록체인 노드가 신규 순서 정렬 서비스로부터 변경 제안 트랜잭션이 포함된 블록을 수신하고, 해당 블록에 대한 변경 제안 합의를 위한 감사 트랜잭션을 생성하고 제출하는 단계; 및

블록체인 노드가 신규 순서 정렬 서비스로부터 수신하는 블록에 포함되어 있는 각 블록체인 노드들이 제출한 변경 제안 합의를 위한 감사 트랜잭션을 분석하여 신규 순서 정렬 서비스로의 변경을 합의하는 단계; 를 포함하는,

비잔틴 장애를 감내하는 블록체인 시스템 내의 블록체인 노드의 동작 방법.

청구항 8

청구항 7에 있어서, 변경 요청 메시지는,

준비(prepared) 합의 수준을 갖는 블록 중 가장 높은 블록 높이인 준비 높이를 갖는 블록을 기준으로 생성한 정보를 포함하고,

준비 높이를 갖는 블록을 기준으로 생성한 정보는, 신규 순서 정렬 서비스 식별 정보, 현재 제공받고 있는 순서 정렬 서비스 식별 정보, 준비 높이, 준비 높이에 위치한 블록 해시 값, 해당 블록의 합의 수준인 준비(prepared)를 검증하는데 필요한 다른 블록체인 노드들의 감사 트랜잭션을 포함하는 후속 블록 정보 리스트, 및 블록체인 노드의 신원을 포함하는,

비잔틴 장애를 감내하는 블록체인 시스템 내의 블록체인 노드의 동작 방법.

청구항 9

청구항 7에 있어서, 변경 제안 트랜잭션은,

신규 순서 정렬 서비스 식별 정보, 타 블록체인 노드들로부터 수신한 변경 요청 메시지 집합, 수신한 변경 요청 메시지들 중에서 최신의 순서 정렬 서비스 식별 정보, 최신 순서 정렬 서비스에서 확인되는 최고 준비 높이 정보, 최고의 준비 높이에 위치한 블록 해시 값, 최고의 준비 높이에 대한 검증을 위한 블록체인 노드들의 감사 트랜잭션을 포함하는 후속 블록 리스트, 최고의 준비 높이 블록까지 고려하여 생성된 블록체인 상태 정보, 및 블록체인 노드의 신원을 포함하는,

비잔틴 장애를 감내하는 블록체인 시스템 내의 블록체인 노드의 동작 방법.

청구항 10

청구항 7에 있어서, 변경 제안 합의를 위한 감사 트랜잭션은,

블록의 높이, 블록의 해시 값, 현재 순서 정렬 서비스 식별 정보, 블록 내의 변경 제안 트랜잭션 위치 오프셋 정보, 및 블록체인 노드의 신원을 포함하는,

비잔틴 장애를 감내하는 블록체인 시스템 내의 블록체인 노드의 동작 방법.

청구항 11

청구항 7에 있어서, 상기 방법은,

해시 체인으로 연결된 두 블록에 대해 블록의 높이가 더 높은 블록에 대한 감사 트랜잭션을 블록의 높이가 더 낮은 블록에 대한 감사 트랜잭션으로 해석하고, 각 블록체인 노드가 판단한 유효한 변경 제안 트랜잭션의 위치 오프셋 정보 단위로 나누어 감사 트랜잭션을 해석하여 정하는 변경 제안 합의를 위한 감사 트랜잭션 분석 방법인 변경 제안 트랜잭션을 포함하는 블록의 합의 수준을 정하는 단계를 더 포함하는,

비잔틴 장애를 감내하는 블록체인 시스템 내의 블록체인 노드의 동작 방법.

청구항 12

청구항 7에 있어서, 상기 방법은,

하이퍼레저 패브릭의 피어(peer) 노드상 기존 모듈과 연동하는 하이퍼레저 패브릭에서의 순서 정렬 서비스 비잔틴 장애 감내 방법인 감사부 및 변경부를 하이퍼레저 패브릭으로 적용하는 단계를 더 포함하는,

비잔틴 장애를 감내하는 블록체인 시스템 내의 블록체인 노드의 동작 방법.

청구항 13

청구항 7 내지 청구항 12 중 어느 한 항의 비잔틴 장애를 감내하는 블록체인 시스템 내의 블록체인 노드의 동작 방법을 구현하기 위한 컴퓨터 판독 가능한 기록매체에 저장된 컴퓨터 프로그램.

청구항 14

청구항 7 내지 청구항 12 중 어느 한 항의 비잔틴 장애를 감내하는 블록체인 시스템 내의 블록체인 노드의 동작 방법을 구현하기 위한 프로그램이 저장된 컴퓨터 판독 가능한 기록매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 블록체인 플랫폼을 위한 비잔틴 장애를 감내하는 방법에 관한 것으로, 더욱 상세하게는 블록체인 노드의 기능 확장을 통해 블록을 생성하고 전파하는 기능을 담당하는 순서 정렬 서비스의 비잔틴 장애를 감내하는 방법에 관한 것이며, 본 발명은 순서 정렬 서비스를 제공하는 모든 블록체인 플랫폼에 적용될 수 있다.

배 경 기 술

[0002] 일반적으로 블록체인 플랫폼은 순서 정렬 서비스를 제공하는 노드들과 스마트 컨트랙트 및 원장 서비스를 제공하는 노드들로 구성된다. 순서 정렬 서비스를 제공하는 노드들은 합의 프로토콜을 통해 클라이언트에서 제출된 트랜잭션의 순서를 정하고 블록 단위로 묶어 스마트 컨트랙트 및 원장 서비스를 제공하는 노드들에 전달한다. 스마트 컨트랙트 및 원장 서비스를 제공하는 노드들은 블록체인 노드라고 불리며, 순서 정렬 서비스에서 생성된 트랜잭션 실행 순서에 따라 클라이언트에게 스마트 컨트랙트 실행 결과 및 원장에 대한 정보를 제공한다. 즉, 블록체인 노드가 유지하고 관리하는 원장 및 상태 정보는 순서 정렬 서비스에서 정한 트랜잭션 실행 순서에 의해 결정된다. 각 서비스는 복제 기술을 이용해 여러 노드로 구성될 수 있다.

[0003] 블록체인 플랫폼 구조에서 순서 정렬 서비스가 일관성 없는(inconsistent) 블록들을 블록체인 노드로 전파하는 경우 스마트 컨트랙트 실행 및 원장 관리에 있어 안정성(safety) 문제가 발생할 수 있으며, 순서 정렬 서비스가 블록을 블록체인 노드로 전파하지 않는 경우엔 생존성(liveness) 문제가 발생할 수 있다. 이는 블록체인 플랫폼을 이용하는 클라이언트에 더 이상 올바른 서비스를 제공할 수 없음을 의미한다.

[0004] 하이퍼레저 패브릭은 블록체인 플랫폼 중 대표적인 플랫폼으로 엔터프라이즈 환경에서 가장 많이 사용된다. 하이퍼레저 패브릭은 순서 정렬 서비스(ordering service)와 피어(peer)로 구성된다. 클라이언트는 트랜잭션을 순서 정렬 서비스(ordering service)에 제출하고 순서 정렬 서비스(ordering service)는 클라이언트에서 제출한 트랜잭션의 순서를 정하고 블록단위로 묶어 피어(peer)에게 전달한다. 이 후 피어(peer)는 순서 정렬 서비스(ordering service)에서 전달받은 블록을 이용하여 원장 및 상태(state) 정보를 업데이트하고 클라이언트에 결과를 전달한다. 이와 같은 구조는 순서 정렬 서비스(ordering service)의 악의적인 공격이나 오동작으로 인해 안정성(safety)및 생존성(liveness) 문제가 발생할 수 있는 구조이다. 따라서, 하이퍼레저 패브릭은 순서 정렬 서비스(ordering service)가 올바르게 동작한다고 가정한다.

[0005] 분산 노드 환경에서 임의의 노드가 악의적이거나 오동작 하더라도 이를 감내하고 노드 간 올바르게 상태를 복제할 수 있는 기술을 비잔틴 장애 감내(BFT; Byzantine Fault Tolerance) 기술이라고 부른다. 기술 중 실용적 비잔틴 장애 감내(PBFT)가 가장 대표적이다. 실용적 비잔틴 장애 감내(PBFT)기술에서 노드들은 크게 하나의 주 노드와 복제 노드로 구분되는데, 주 노드는 업데이트할 데이터에 대해 순서를 정하고 다른 복제 노드들에게 데이터와 정해진 순서를 전파한다. 복제 노드는 주 노드로부터 데이터와 순서를 전달받으면 정보를 다른 복제 노드들이 전달 받은 정보와 일치하는지 비교하고 정보가 일치하면 데이터와 순서를 이용하여 상태를 업데이트 한다(데이터 일치 확인 과정). 만약 복제 노드들이 전달 받은 정보가 일치하지 않으면 주 노드를 다른 노드로 변경 한다(주 노드 변경 과정). 실용적 비잔틴 장애 감내(PBFT) 기술에서 프로토콜을 올바르게 동작시키기 위해선, 전체 노드 개수가 n, 감내 가능한 결함 노드들의 최대 개수가 f 일 때, 결함 노드의 수 f 는 전체 노드 수 n의 1/3 보다 작아야 한다. 또한 데이터 일치 확인 과정과 주 노드 변경 과정은 최소 전체 노드 수 n의 2/3 이상이 동의해야 한다.

발명의 내용

해결하려는 과제

[0006] 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은, 블록체인 플랫폼에서 올바르지 않은 순서 정렬 서비스의 동작으로 인해 발생할 수 있는 안정성(safety)혹은 생존성(liveness) 문제를 블록체인 노드에서 대응하는 블록체인 플랫폼에서 비잔틴 장애 감내 장치 및 방법을 제공하는데 있다.

[0007] 기존의 블록체인 플랫폼들은 순서 정렬 서비스로 인해 발생할 수 있는 안정성(safety)혹은 생존성(liveness) 문제를 해결하기 위해 순서 정렬 서비스 자체를 올바르게 동작시키는데 목적을 두고 있다. 예를 들어, 순서 정렬 서비스를 여러 개의 노드로 구성하고 임의의 합의 프로토콜을 기반으로 복제 기술을 적용한다. 하지만, 위와 같은 구조는 다수의 순서 정렬 서비스의 노드가 악의적으로 동작하거나 해킹될 수 있는 환경에선 블록체인 노드는 더 이상 순서 정렬 서비스를 신뢰할 수 없다.

[0008] 본 발명은 순서 정렬 서비스가 악의적이거나 오동작 할 수 있음을 고려하여 블록체인 노드의 기능을 확장하여 대응한다. 확장된 블록체인 노드는 순서 정렬 서비스를 감사하고 순서 정렬 서비스의 악의적 공격이나 오동작을 탐지할 경우 신규 순서 정렬 서비스로 변경한다. 이러한 방법을 통하여 기존 블록체인 플랫폼에서 블록체인 노드가 순서 정렬 서비스에 의존적인 동작으로 인해 생길 수 있는 문제를 해결하고자 한다.

과제의 해결 수단

[0009] 상기 목적을 달성하기 위한 본 발명의 블록체인 플랫폼에서 비잔틴 장애 감내 장치는, 블록체인 순서 정렬 서비스의 동작을 감사하는 블록체인 플랫폼에서 비잔틴 장애 감내 장치에 있어서, 블록을 수신한 블록체인 노드가 감사 트랜잭션을 생성하고 현재 순서 정렬 서비스에 제출하는 것을 특징으로 하는 감사 트랜잭션 생성 장치일 수 있다.

[0010] 감사 트랜잭션은, 블록체인 노드가 자체적으로 유지하는 블록체인 정보에 기반하여, 블록의 높이, 블록의 해시 값, 현재 순서 정렬 서비스 식별 정보, 그리고 블록체인 노드의 신원을 포함하여 구성될 수 있다.

[0011] 감사 트랜잭션 생성은, 블록체인 노드가 현재 순서 정렬 서비스를 감사하는 주기에 따라 생성하며, 주기는 현재 순서 정렬 서비스로부터 수신한 블록의 개수를 기반으로 정해질 수 있다.

[0012] 본 발명의 다른 목적을 달성하기 위한 블록체인 플랫폼에서 비잔틴 장애 감내 방법은, 블록체인 순서 정렬 서비스의 동작을 분석하는 감사 트랜잭션 분석 방법에 있어서, 적어도 하나의 수신한 블록내에 포함되어 있는 각 블록체인 노드가 제출한 감사 트랜잭션 분석을 통해 수신한 각 블록의 합의 수준을 결정하는 단계; 및 블록체인 노드에서 감사 트랜잭션 분석 과정의 오류 분석과 합의 수준 업데이트 지연 시간을 기반으로 순서 정렬 서비스의 악의적 공격 여부 및 오동작을 검출하는 단계; 를 포함할 수 있다.

[0013] 적어도 하나의 수신한 블록내에 포함되어 있는 각 블록체인 노드가 제출한 감사 트랜잭션 분석을 통해 수신한 각 블록의 합의 수준을 결정하는 단계는, 블록체인 구조에서 모든 블록들이 해시 체인으로 연결되어 있는 특징을 활용하여, 해시 체인으로 연결된 두 블록에 중에서 블록의 높이가 더 높은 블록에 대한 감사 트랜잭션을, 블록의 높이가 더 낮은 블록에 대한 감사 트랜잭션으로 해석하는 블록 합의 수준 결정 방법일 수 있다.

[0014] 블록체인 노드에서 감사 트랜잭션 분석 과정의 오류 분석과 합의 수준 업데이트 지연 시간을 기반으로 순서 정렬 서비스의 악의적 공격 여부 및 오동작을 검출하는 단계는, 순서 정렬 서비스의 공격으로 인한 안정성(safety), 생존성(liveness), 그리고 공정성(fairness) 위반을 검출하는 단계; 를 더 포함하고, 안정성(safety) 위반의 검출은, 블록체인상 동일한 높이의 블록에 대해 블록체인 노드들이 서로 다른 해시 값을 갖는 감사 트랜잭션을 제출한 경우를 판단하고, 생존성(liveness) 위반의 검출은, 블록의 합의 수준이 유한하게 정해진 시간 동안 업데이트 되지 않는 경우를 판단하며, 공정성(fairness) 위반의 검출은, 블록체인상 동일한 범위내에 위치한 블록들에서 확인되는 감사 트랜잭션 개수가 각 블록체인 노드들 간에 불균형이 확인되는 경우를 판단할 수 있다.

[0015] 본 발명의 다른 목적을 달성하기 위한 블록체인 플랫폼에서 비잔틴 장애 감내 방법은, 블록체인 노드가 순서 정렬 서비스 오동작이 확인되는 경우 블록체인 순서 정렬 서비스를 변경하는 방법에 있어서, 블록체인 노드가 순서 정렬 서비스 변경을 제안하는 변경 요청 메시지를 생성하고 다른 블록체인 노드들로 전파하는 단계; 각 블록체인 노드로부터 수신한 변경 요청 메시지를 분석하여, 소정의 수 이상의 블록체인 노드들이 변경에 동의한다고 판단하는 경우, 신규 순서 정렬 서비스를 위한 변경 제안 트랜잭션을 생성하여 이를 변경될 순서 정렬 서비스에 제출하는 단계; 블록체인 노드가 신규 순서 정렬 서비스로부터 변경 제안 트랜잭션이 포함된 블록을 수신하고, 해당 블록에 대한 변경 제안 합의를 위한 감사 트랜잭션을 생성하고 제출하는 단계; 및 블록체인 노드가 신규 순서 정렬 서비스로부터 수신하는 블록에 포함되어 있는 각 블록체인 노드들이 제출한 변경 제안 합의를 위한 감사 트랜잭션을 분석하여 신규 순서 정렬 서비스로의 변경을 합의하는 단계; 를 포함할 수 있다.

[0016] 변경 요청 메시지는, 준비(prepared) 합의 수준을 갖는 블록 중 가장 높은 블록 높이인 준비 높이를 갖는 블록을 기준으로 생성한 정보를 포함하고, 준비 높이를 갖는 블록을 기준으로 생성한 정보는, 신규 순서 정렬 서비스 식별 정보, 현재 제공받고 있는 순서 정렬 서비스 식별 정보, 준비 높이, 준비 높이에 위치한 블록 해시 값, 해당 블록의 합의 수준인 준비(prepared)를 검증하는데 필요한 다른 블록체인 노드들의 감사 트랜잭션을 포함하는 후속 블록 정보 리스트, 및 블록체인 노드의 신원을 포함할 수 있다.

[0017] 변경 제안 트랜잭션은, 신규 순서 정렬 서비스 식별 정보, 타 블록체인 노드들로부터 수신한 변경 요청 메시지 집합, 수신한 변경 요청 메시지들 중에서 최신의 순서 정렬 서비스 식별 정보, 최신 순서 정렬 서비스에서 확인되는 최고 준비 높이 정보, 최고의 준비 높이에 위치한 블록 해시 값, 최고의 준비 높이에 대한 검증을 위한 블록체인 노드들의 감사 트랜잭션을 포함하는 후속 블록 리스트, 최고의 준비 높이 블록까지 고려하여 생성된 블록체인 상태 정보, 및 블록체인 노드의 신원을 포함할 수 있다.

[0018] 변경 제안 합의를 위한 감사 트랜잭션은, 블록의 높이, 블록의 해시 값, 현재 순서 정렬 서비스 식별 정보, 블

록 내의 변경 제안 트랜잭션 위치 오프셋 정보, 및 블록체인 노드의 신원을 포함할 수 있다.

[0019] 상기 방법은, 해시 체인으로 연결된 두 블록에 대해 블록의 높이가 더 높은 블록에 대한 감사 트랜잭션을 블록의 높이가 더 낮은 블록에 대한 감사 트랜잭션으로 해석하고, 각 블록체인 노드가 판단한 유효한 변경 제안 트랜잭션의 위치 오프셋 정보 단위로 나누어 감사 트랜잭션을 해석하여 정하는 변경 제안 합의를 위한 감사 트랜잭션 분석 방법인 변경 제안 트랜잭션을 포함하는 블록의 합의 수준을 정하는 단계를 더 포함할 수 있다.

[0020] 상기 방법은, 하이퍼레저 패브릭의 피어(peer) 노드상 기존 모듈과 연동하는 하이퍼레저 패브릭에서의 순서 정렬 서비스 비잔틴 장애 감내 방법인 감사부 및 변경부를 하이퍼레저 패브릭으로 적용하는 단계를 더 포함할 수 있다.

[0021] 본 발명의 또 다른 목적을 달성하기 위한 블록체인 플랫폼에서 비잔틴 장애 감내 방법을 구현하기 위한 컴퓨터 판독 가능한 기록매체에 저장된 컴퓨터 프로그램일 수 있다.

[0022] 본 발명의 또 다른 목적을 달성하기 위한 블록체인 플랫폼에서 비잔틴 장애 감내 방법의 프로그램을 구현하기 위한 컴퓨터 판독 가능한 기록매체일 수 있다.

발명의 효과

[0023] 상기와 같은 본 발명에 따른 블록체인 플랫폼에서 비잔틴 장애 감내 장치 및 방법은, 실용적 비잔틴 장애 감내(PBFT)에 기초하여 감내 가능한 장애 블록체인 노드들의 최대 개수가 f인 환경에서도 순서 정렬 서비스의 안정성(safety)과 생존성(liveness) 문제에 대응할 수 있다.

[0024] 본 발명에 따른 블록체인 플랫폼에서 비잔틴 장애 감내 장치 및 방법의 전술한 특징은, 블록체인 플랫폼에서 순서 정렬 서비스의 장애를 감내하는 최초의 발명이다.

[0025] 또한, 해시 체인으로 연결된 두 블록이 주어졌을 때, 반드시 하나의 해시 체인 경로만 존재한다는 블록체인의 해시 체인 특성을 활용하여 블록체인 노드의 감사 및 변경 비용을 줄일 수 있다는 장점을 가진다.

[0026] 또한, 순서 정렬 서비스의 변경은 특정 블록체인 노드에 의해 주도적으로 수행되는 것이 아닌 모든 노드가 독립적으로 변경 요청 메시지 및 변경 제안 트랜잭션을 생성하고, 변경 제안 트랜잭션에 동의하는 탈중앙화 형태로 수행된다는 장점을 가진다.

도면의 간단한 설명

[0027] 도 1은 일반적인 블록체인 플랫폼의 시스템 구성도이다.

도 2는 본 발명의 일 실시예의 블록체인 플랫폼을 위한 비잔틴 장애 감내(BFT; Byzantine Fault Tolerance) 장치의 전체 시스템 구성도이다.

도 3은 본 발명의 일 실시예의 블록체인 플랫폼을 위한 비잔틴 장애 감내(BFT; Byzantine Fault Tolerance) 장치의 감사부 구성도이다.

도 4는 본 발명의 일 실시예의 블록체인 플랫폼을 위한 비잔틴 장애 감내(BFT; Byzantine Fault Tolerance) 장치의 변경부 구성도이다.

도 5는 본 발명의 일 실시예의 순서 정렬 서비스 감사를 위한 감사 트랜잭션 생성 및 분석 순서도이다.

도 6은 본 발명의 일 실시예의 순서 정렬 서비스 변경을 위한 변경 제안 트랜잭션 생성 및 제출 순서도이다.

도 7은 본 발명의 일 실시예의 변경 제안 트랜잭션 수신 및 변경 제안 트랜잭션에 대한 감사 트랜잭션 제출 순서도이다.

도 8은 본 발명의 일 실시예의 변경 제안 트랜잭션에 대한 합의 순서도이다.

도 9는 본 발명의 일 실시예의 하이퍼레저 패브릭으로의 감사부 적용 구성도이다.

도 10은 본 발명의 일 실시예의 하이퍼레저 패브릭으로의 변경부 적용 구성도이다.

발명을 실시하기 위한 구체적인 내용

[0028] 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.

[0029] 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.

[0030] 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.

[0031] 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, "포함하다" 또는 "가지다" 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.

[0032] 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.

[0033] 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.

[0034] 실용적 비잔틴 장애 감내 (PBFT) 알고리즘을 활용하기 위하여, 전체 블록체인 노드의 개수는 n, 감내 가능한 장애 블록체인 노드들의 최대 개수는 f를 기준으로 설명한다.

[0036] 도 1은 일반적인 블록체인 플랫폼의 시스템 구성도이다.

[0037] 도 1에 도시된 바와 같이, 블록체인 플랫폼의 시스템의 구성을 설명하면, 블록체인 노드(100)는 스마트 컨트랙트 서비스(200) 및 블록체인 원장(300)을 클라이언트(400)에게 제공하는 노드이고, 순서 정렬 서비스(500)는 블록체인 노드(100)에 블록을 제공하는 서비스이다.

[0038] 블록체인 플랫폼의 시스템의 전체적인 수행 흐름은 다음과 같다.

[0039] 먼저, 클라이언트(400)는 트랜잭션을 순서 정렬 서비스(500)에 제출한다. 트랜잭션은 순서 정렬 서비스(500)가 실행 순서를 정하고 블록으로 묶어 블록체인 노드(100)로 전파한다. 전파된 블록은 블록체인 노드(100)의 블록체인 원장(300)에 기록되고 블록 내 트랜잭션 순서를 기반으로 스마트 컨트랙트(200)가 실행된 후 클라이언트에 실행 결과가 전달된다.

[0041] 도 2는 본 발명의 일 실시예의 블록체인 플랫폼을 위한 비잔틴 장애 감내(BFT; Byzantine Fault Tolerance) 장치의 전체 시스템 구성도이고, 도 3은 감사부 구성도이고, 도 4는 변경부 구성도이다.

[0042] 도 2에 도시된 바와 같이, 본 발명의 블록체인 플랫폼을 위한 비잔틴 장애 감내(BFT; Byzantine Fault Tolerance) 장치의 시스템의 구성에서, 블록체인 노드(100)는, 도 1의 일반적인 블록체인 플랫폼과 동일하게 블록체인 노드(100), 스마트 컨트랙트 서비스를 제공하는 스마트 컨트랙트(200) 및 순서 정렬 서비스로부터 수신한 일련의 블록들을 담고 있는 블록체인 원장(300)을 가진다.

[0043] 본 발명의 블록체인 플랫폼을 위한 비잔틴 장애 감내(BFT; Byzantine Fault Tolerance) 장치는 전술한 도 1의 구성에 추가적으로 순서 정렬 서비스(500, 600)의 비잔틴 장애를 감내하기 위한 감사부(700) 및 변경부(800)를 추가로 채택함으로써 순서 정렬 서비스(500, 600)의 비잔틴 고장 감내를 지원한다.

[0044] 순서 정렬 서비스(500, 600)는 블록체인 노드(100)가 현재 서비스를 제공받고 있는 현재 순서 정렬 서비스(50

0)와 현재 순서 정렬 서비스(500)의 올바르지 않은 동작이 탐지되는 경우 새롭게 사용될 신규 순서 정렬 서비스(600)를 포함한다.

[0045] 블록체인 노드(100)의 감사부(700)는 현재 순서 정렬 서비스(500)의 동작을 감사하기 위한 정보를 생성하는 생성부(710)와, 각 블록체인 노드(100)들에서 생성된 감사 정보를 기반으로 순서 정렬 서비스의 동작을 분석하는 분석부(720)로 구성된다.

[0046] 생성부(710)에서 생성하는 정보는, 현재 순서 정렬 서비스(500)를 감사하기 위하여 블록체인 노드(100)가 자체적으로 유지하는 블록체인 정보에 기반한 블록의 높이, 블록의 해시 값, 현재 순서 정렬 서비스(500) 식별 정보, 그리고 블록을 수신한 블록체인 노드(100)의 신원을 포함하는 트랜잭션으로 구성된다. 여기서, 트랜잭션을 감사 트랜잭션이라 부르며, 감사 트랜잭션은 블록을 수신한 블록체인 노드(100)에서 개별적으로 생성되고, 현재 순서 정렬 서비스(500)로 제출된다.

[0047] 감사 트랜잭션은 블록체인 노드(100)가 각자 유지하는 블록체인 정보를 다른 블록체인 노드(100)들에게 공지하기 위한 정보이다. 감사 트랜잭션은 블록체인 노드(100)가 현재 순서 정렬 서비스(500)를 감사하는 주기에 따라 생성되며, 주기는 현재 순서 정렬 서비스(500)로부터 수신한 블록의 개수를 기반으로 정해진다. 즉, 감사 트랜잭션은 블록을 수신할 때마다 생성할 수도 있고, 여러 개의 블록을 수신했을 때 생성할 수도 있다.

[0048] 블록체인 노드(100)는 생성한 감사 트랜잭션을 현재 순서 정렬 서비스(500)에 제출하며, 제출된 감사 트랜잭션은 현재 순서 정렬 서비스(500)에 의해 일반 트랜잭션들과 함께 순서가 정해지고 블록으로 생성되어 블록체인 노드(100)로 전파된다.

[0049] 분석부(720)는 수신한 블록 내에 포함되어 있는 감사 트랜잭션을 추출하고 분석하여, 블록체인 노드(100)들이 동일한 블록들을 관찰했는지 여부를 바탕으로 블록체인 원장(300)내에 있는 블록들의 합의 수준을 증가시킨다. 각 블록의 합의 수준은 실용적 비잔틴 장애 감내(PBFT)에 기초하여 '무합의(none)', '준비(prepared)', '확정(committed)'으로 구분된다.

[0050] '무합의(none)' 합의 수준은 블록체인 원장에 블록은 연결되었지만, 해당 블록의 순서는 보장할 수 없는 상태이다.

[0051] '준비(prepared)' 합의 수준은 n-f 개 이상의 블록체인 노드(100)들이 동일한 '무합의(none)' 합의 수준을 갖는 블록을 관찰했을 때 전환된다.

[0052] '확정(committed)' 합의 수준은 n-f 개 이상의 블록체인 노드(100)들이 동일한 '준비(prepared)' 합의 수준을 갖는 블록을 관찰했을 때 전환된다.

[0053] 또한, 해시 체인으로 연결된 임의의 두 블록이 주어졌을 때, 반드시 하나의 해시 체인 경로만 존재한다는 블록체인의 해시 체인 특성을 활용하여, 임의의 블록 높이 g 와 g 보다 높은 블록 높이 g'을 갖는 두 블록이 해시 체인으로 연결된다면, 블록 높이 g'을 임의의 블록체인 노드(100)가 관찰한 것은 블록 높이 g도 블록체인 노드(100)가 관찰한 것으로 간주 할 수 있다. 따라서 특정 블록 높이 g를 갖는 블록의 합의 수준은 블록 높이 g를 포함하는 감사 트랜잭션과 블록 높이 g 보다 높은 블록 높이 g'을 포함하는 감사 트랜잭션을 이용하여 합의 수준을 전환할 수 있다.

[0054] 분석부(720)는 위의 내용을 기반으로 현재 순서 정렬 서비스(500)의 올바르지 않은 동작을 안정성(safety), 생존성(liveness), 그리고 공정성(fairness) 관점에서 분석한다.

[0055] 안정성(safety) 위반은 블록체인상 동일한 높이의 블록에 대해 블록체인 노드(100)들이 서로 다른 해시 값을 관찰한 경우에 해당한다.

[0056] 생존성(liveness) 위반은 블록의 합의 수준이 유한하게 정해진 시간 동안 업데이트되지 않는 경우에 해당한다. 생존성(liveness) 위반은 시간제한(timeout)에 의해 탐지된다.

[0057] 공정성(fairness) 위반은 블록체인상 동일한 범위 내에 위치한 블록들에서 확인되는 감사 트랜잭션 개수가 각 블록체인 노드(100)들 간에 불균형이 확인되는 경우에 해당한다.

[0058] 변경부(800)는 현재 순서 정렬 서비스(500)의 오동작이 확인되는 경우 순서 정렬 서비스를 변경하는 과정을 진행한다.

[0059] 제안부(810)는 순서 정렬 서비스 변경을 제안하는 변경 요청 메시지를 생성하고 다른 블록체인 노드(100)들로

전파한다. 또한 다른 블록체인 노드(100)로부터 수신한 변경 요청 메시지를 분석하여, 일정 수 이상의 블록체인 노드(100)들이 변경에 동의한다고 판단하는 경우, 신규 순서 정렬 서비스(600)를 위한 변경 제안 트랜잭션을 생성하고 신규 순서 정렬 서비스(600)에 제출한다. 동의부(820)는 신규 순서 정렬 서비스(600)로부터 수신하는 블록에 포함되어 있는 각 블록체인 노드(100)들이 제출한 변경 제안 합의를 위한 감사 트랜잭션을 분석하여 신규 순서 정렬 서비스(600)로의 변경을 합의한다.

[0060] 제안부(810)는 블록체인 노드(100)가 유지하는 블록체인 원장(300)에 존재하는 일련의 블록들 중에 '준비(prepared)' 합의 수준을 갖는 블록 중 가장 높은 블록 높이를 갖는 블록을 기준으로 순서 정렬 서비스 변경 요청 메시지를 생성하여 다른 블록체인 노드(100)들에 전파한다. 이하 한 블록체인 노드(100) 내에서 '준비(prepared)' 합의 수준을 갖는 블록 중 가장 높은 블록 높이는 준비 높이 라고 부른다. 각 블록체인 노드(100)는 서로 다른 준비 높이를 가질 수 있다.

[0061] 블록체인 노드(100)의 변경 요청 메시지는 신규 순서 정렬 서비스(600) 식별 정보, 현재 제공받고 있는 순서 정렬 서비스(500) 식별 정보, 준비 높이, 준비 높이에 위치한 블록 해시 값, 해당 블록의 합의 수준인 '준비(prepared)'를 검증하는데 필요한 다른 블록체인 노드(100)들의 감사 트랜잭션을 포함하는 후속 블록 정보 리스트, 그리고 블록체인 노드(100)의 신원을 포함한다.

[0062] 블록체인 노드(100)는 현재 순서 정렬 서비스(500)의 올바르지 않은 동작을 탐지한 타 블록체인 노드(100)들의 변경 요청 메시지를 n-f 개 이상 수신하면 변경 제안 트랜잭션을 생성하여 신규 순서 정렬 서비스(600)에 제출한다.

[0063] 변경 제안 트랜잭션은 신규 순서 정렬 서비스(600) 식별 정보, 타 블록체인 노드(100)들로부터 수신한 변경 요청 메시지 집합(n-f 개 이상), 수신한 변경 요청 메시지들 중에서 최신의 순서 정렬 서비스 식별 정보, 최신 순서 정렬 서비스에서 확인되는 최고 준비 높이 정보, 최고의 준비 높이에 위치한 블록 해시 값, 최고의 준비 높이에 대한 검증을 위한 블록체인 노드(100)들의 감사 트랜잭션을 포함하는 후속 블록 리스트, 최고의 준비 높이 블록까지 고려하여 생성된 블록체인 상태(950)(state) 정보, 그리고 블록체인 노드(100)의 신원을 포함하며, 트랜잭션 형태로 구성된다.

[0064] 동의부(820)는 임의의 블록체인 노드(100)의 제안부(810)에서 제출된 변경 제안 트랜잭션이 신규 순서 정렬 서비스(600)에서 블록으로 생성되어 블록체인 노드(100)들로 전파되면, 이를 추출하여 검증하고 첫 번째 유효한 변경 제안 트랜잭션을 찾는다.

[0065] 첫 번째 유효한 변경 제안 트랜잭션을 찾으면, 변경 제안 합의를 위해 블록 내의 첫 번째 유효한 변경 제안 트랜잭션 위치 오프셋 정보를 추가한 감사 트랜잭션을 신규 순서 정렬 서비스(600)로 제출한다. 즉, 변경 제안 합의를 위한 감사 트랜잭션은 블록의 높이, 블록의 해시 값, 신규 순서 정렬 서비스(600), 식별 정보, 블록 내의 변경 제안 트랜잭션 위치 오프셋 정보, 그리고 블록체인 노드(100)의 신원을 포함한다.

[0066] 신규 순서 정렬 서비스(600)는 변경 제안 합의를 위한 감사 트랜잭션들을 블록으로 생성하여 블록체인 노드(100)로 전파한다. 각 블록체인 노드(100)는 변경 제안 트랜잭션의 위치 오프셋 정보 단위로 나누어 감사 트랜잭션을 해석하고 블록의 합의 수준을 결정한다.

[0067] 합의 수준의 결정 과정은 감사부(700)의 분석부(720)와 동일하다. 첫 번째 유효한 변경 제안 트랜잭션을 포함한 블록의 합의 수준이 '확정(committed)' 되면 변경 제안 트랜잭션 내에 포함된 상태(950)(state) 정보로 로컬 상태를 업데이트하고 순서 정렬 서비스 변경 절차를 종료한다.

[0069] 도 5는 본 발명의 일 실시예에 따른 블록체인 플랫폼에서 비잔틴 장애 감내 방법의 현재 순서 정렬 서비스(500) 감사를 위한 감사 트랜잭션 생성 및 분석 순서도이다.

[0070] 도 5를 참조하면, 본 발명의 일 실시예의 블록체인 플랫폼에서 비잔틴 장애 감내 방법은, 현재 순서 정렬 서비스(500) 감사를 위한 감사 트랜잭션 생성 및 분석 의 S701 내지 S705 단계를 포함한다.

[0071] 블록체인 노드(100)는 현재 순서 정렬 서비스(500)에서 생성한 블록 내 감사 트랜잭션을 추출한다(S701). 감사 트랜잭션은 각 블록체인 노드(100)가 관찰한 블록의 정보를 포함하고 있으며 각 블록체인 노드(100)의 개인키로 서명된다. 즉, 임의의 블록체인 노드(100)가 타 블록체인 노드(100)가 관찰한 정보를 임의로 생성할 수 없다.

[0072] 서명 정보 및 블록체인 노드(100) 자신이 관찰한 블록의 해시 값과 타 블록체인 노드(100)가 관찰한 블록의 해시 값이 일치하는지 감사 트랜잭션 검증 단계에서 확인한다(S702).

[0073] 이후 감사 트랜잭션에 포함된 블록의 높이보다 낮은 각 블록의 관찰 노드 정보를 업데이트 한다(S703).

[0074] 블록의 관찰 노드 정보가 합의 수준 업데이트 조건에 해당하는 경우 블록의 합의 수준을 업데이트(S704)한다.

[0075] 블록체인 노드(100)가 현재 분석하고 있는 블록에 대응되는 감사 트랜잭션을 현재 순서 정렬 서비스에 제출한다(S705).

[0076] 감사 트랜잭션은 현재 순서 정렬 서비스(500)에 의해 새로운 블록으로 생성되고 블록체인 노드(100)로 전파되며 블록체인 노드(100)는 새로운 블록을 수신하면 S701 단계부터 동일한 과정을 반복한다.

[0078] 도 6는 본 발명의 일 실시예에 따른 블록체인 플랫폼에서 비잔틴 장애 감내 방법의 순서 정렬 서비스 변경을 위한 변경 제안 트랜잭션 생성 및 제출 순서도이다.

[0079] 도 6를 참조하면, 본 발명의 일 실시예에 따른 블록체인 플랫폼에서 비잔틴 장애 감내 방법은, 순서 정렬 서비스 변경을 위한 변경 제안 트랜잭션 생성 및 제출의 S801 내지 S805 단계를 포함한다.

[0080] 블록체인 노드(100)는 순서 정렬 서비스 변경 절차가 시작되면 변경 요청 메시지를 생성하고 타 블록체인 노드(100)들에 전파한다(S801). 변경 요청 메시지는 블록체인 노드(100)의 준비 높이를 기준으로 생성되고 블록체인 노드(100)의 개인키를 이용해 서명한다.

[0081] 블록체인 노드(100)는 자신과 동일한 방법으로 생성된 변경 요청 메시지를 타 블록체인 노드(100)들로부터 수신하며 이를 검증하고 수집한다(S802). 검증은 변경 요청 메시지의 서명 정보를 확인하고 준비 높이에 해당하는 블록의 합의 수준이 '준비(prepared)' 가 맞는지 확인한다. n-f 개 이상의 블록체인 노드(100)들에서 제출한 감사 트랜잭션들이 후속 블록 리스트에 있다면 변경 요청 메시지의 검증 과정은 완료된다.

[0082] 블록체인 노드(100)는 n-f 개 이상의 유효한 변경 요청 메시지를 수집하면 시간제한(timeout)을 설정한다(S803). 이는 신규 순서 정렬 서비스(600)에서도 생존성(liveness) 문제가 발생할 수 있기 때문이다.

[0083] 이후 블록체인 노드(100)는 변경 제안 트랜잭션을 생성한다(S804). 변경 제안 트랜잭션은 n-f 개 이상의 노드들이 본 준비 높이 중 최고의 준비 높이를 기준으로 생성된다. 변경 제안 트랜잭션은 어떤 상태(950)(state) 정보를 기준으로 신규 순서 정렬 서비스(600)에서 블록체인을 재개할 것인지에 대한 모든 증거를 포함한다.

[0084] 블록체인 노드(100)는 변경 제안 트랜잭션을 생성하면 이를 신규 순서 정렬 서비스(600)에 제출한다(S805).

[0086] 도 7은 본 발명의 일 실시예에 따른 블록체인 플랫폼에서 비잔틴 장애 감내 방법의 변경 제안 트랜잭션 수신 및 변경 제안 트랜잭션에 대한 감사 트랜잭션 제출 순서도이다.

[0087] 도 7을 참조하면, 본 발명의 일 실시예에 따른 블록체인 플랫폼에서 비잔틴 장애 감내 방법은, 변경 제안 트랜잭션 수신 및 변경 제안 트랜잭션에 대한 감사 트랜잭션 제출의 S811 내지 S813 단계를 포함한다.

[0088] 블록체인 노드(100)는 신규 순서 정렬 서비스(600)에서 생성한 블록을 수신하면 블록 내의 변경 제안 트랜잭션을 추출한다(S811).

[0089] 블록체인 노드(100)는 추출된 변경 제안 트랜잭션을 검증한다(S812). 변경 제안 트랜잭션 추출 및 검증은 블록체인 노드(100)가 첫 번째 유효한 변경 제안 트랜잭션을 찾을 때까지 수행된다.

[0090] 블록체인 노드(100)는 첫 번째 유효한 변경 제안 트랜잭션을 찾으면, 변경 제안 트랜잭션의 블록체인 내 위치 오프셋 정보를 추가한 감사 트랜잭션을 신규 순서 정렬 서비스에 제출한다(S813).

[0092] 도 8은 본 발명의 일 실시예에 따른 블록체인 플랫폼에서 비잔틴 장애 감내 방법의 특정 변경 제안 트랜잭션에 대한 합의 순서도이다.

[0093] 도 8을 참조하면, 본 발명의 일 실시예에 따른 블록체인 플랫폼에서 비잔틴 장애 감내 방법은, 특정 변경 제안 트랜잭션에 대한 합의의 S821 내지 S825 단계를 포함한다.

[0094] 블록체인 노드(100)는 신규 순서 정렬 서비스(600)에서 생성한 블록을 수신하면 변경 제안 트랜잭션 합의를 위한 감사 트랜잭션을 추출한다(S821).

[0095] 블록체인 노드(100)는 추출된 감사 트랜잭션을 검증한다(S822).

[0096] 이후 감사 트랜잭션에 포함된 블록의 높이보다 낮은 각 블록의 관찰 노드 정보를 업데이트한다(S823). 이 때, 각 블록별로 블록체인 노드(100)들이 관찰한 첫 번째 유효한 변경 제안 트랜잭션의 블록체인 내 위치 오프셋 정

보를 구분하여 관찰 노드 정보를 업데이트한다.

[0097] 여기서, 첫 번째 유효한 변경 제안 트랜잭션을 포함한 블록의 합의 수준이 '확정(committed)' 되면(S824), 신규 순서 정렬 서비스(600)로의 변경 절차는 종료되고, 그렇지 않은 경우 현재 분석한 블록의 정보(블록의 높이, 블록의 해시)와 자신이 확인했던 첫 번째 유효한 변경 제안 트랜잭션의 블록체인 내 위치 오프셋 정보를 포함하여 감사 트랜잭션을 제출한다(S825).

[0098] 이 후 후속 블록에 포함된 감사 트랜잭션을 분석하여 첫 번째 유효한 변경 제안 트랜잭션을 포함한 블록의 합의 수준이 '확정(committed)'될 때까지 S821 내지 S825 과정을 반복한다.

[0100] 도 9는 본 발명의 일 실시예에 따른 블록체인 플랫폼에서 비잔틴 장애 감내 장치의 하이퍼레저 패브릭으로의 감사부(700) 적용 구성도이다.

[0101] 도 9를 참조하면, 본 발명의 일 실시예에 따른 블록체인 플랫폼에서 비잔틴 장애 감내 장치는, 피어(peer)의 블록 수신부(910)(block provider)가 현재 순서 정렬 서비스(500)(ordering service)에서 전파된 블록을 수신하면, 블록 버퍼부(payload buffer)(920)에 수신된 블록을 삽입한 후, 블록 연결부(committer)(930)에 블록 수신을 통보한다.

[0102] 블록 연결부(committer)(930)는 블록 버퍼부(payload buffer)(920)에 삽입된 블록을 순차적으로 가져와 블록체인 원장(300)(ledger)에 저장한 후 감사부(700)에 블록 연결을 통보한다.

[0103] 감사부(700)의 분석부(710)는 블록체인 원장(300)에서 읽은 블록 내 감사 트랜잭션을 추출하고, 이를 기반으로 블록의 합의 수준을 계산한다. 블록의 합의 수준이 '확정(committed)'이되면, 블록 내 트랜잭션 정보를 이용해 상태(950)를 업데이트한다.

[0104] 이 후 감사부(700)의 생성부(720)는 현재 분석한 블록의 정보를 이용하여 감사 트랜잭션을 현재 순서 정렬 서비스(500)(ordering service)에 제출한다.

[0106] 도 10은 본 발명의 일 실시예에 따른 블록체인 플랫폼에서 비잔틴 장애 감내 장치의 하이퍼레저 패브릭으로의 변경부(800) 적용 구성도이다.

[0107] 도 10을 참조하면, 본 발명의 일 실시예에 따른 블록체인 플랫폼에서 비잔틴 장애 감내 장치의 변경부(800)의 제안부(820)는 타 피어로부터 충분한 변경 요청 메시지를 수신하면, 상태(950)를 추출하고 이를 기반으로 변경 제안 트랜잭션을 생성하여 신규 순서 정렬 서비스(600)(ordering service)에 제출한다.

[0108] 신규 순서 정렬 서비스(600)(ordering service)는 전달받은 변경 제안 트랜잭션을 블록으로 생성하고 피어들에게 전파한다.

[0109] 블록 수신부(block provider)(910)가 신규 순서 정렬 서비스(600)(ordering service)에서 전파된 블록을 수신하면 블록 버퍼부(payload buffer)(920)에 삽입한 후 블록 연결부(committer)(930)에 통보한다.

[0110] 블록 연결부(committer)(930)는 블록 버퍼부(payload buffer)(920)에 삽입된 블록을 순차적으로 가져와 블록체인 원장(ledger)(300)에 저장한 후 변경부(800)에 블록 연결을 통보한다.

[0111] 변경부(800)의 동의부(810)는 블록체인 원장(300)에서 읽은 블록 내 유효한 변경 제안 트랜잭션을 발견하면 감사 트랜잭션을 신규 순서 정렬 서비스(600)(ordering service)에 제출한다.

[0112] 감사 트랜잭션은 신규 순서 정렬 서비스(600)(ordering service)에 의해 블록으로 생성되고 피어로 전파된다.

[0113] 변경부(800)의 동의부(810)는 새롭게 전달받은 블록 내 감사 트랜잭션을 추출하고 이를 기반으로 변경 제안 트랜잭션을 포함한 블록의 합의 수준을 계산한다.

[0114] 블록의 합의 수준이 '확정(committed)' 되면, 블록 내 변경 제안 트랜잭션의 상태(950) 정보를 이용해 상태를 업데이트 한다.

[0116] 본 발명의 일 실시예의 블록체인 플랫폼에서 비잔틴 장애 감내 장치의 구성을 작동과 관련하여 설명하면 다음과 같다.

[0117] 본 발명의 일 실시예의 블록체인 플랫폼에서 비잔틴 장애 감내 장치는, 블록체인 노드의 기능을 확장하여, 순서 정렬 서비스의 비잔틴 장애를 감내할 수 있도록 구성된다. 현재 순서 정렬 서비스가 블록체인 노드에 블록을 전파하면 블록체인 노드는 자신이 수신한 블록의 정보를 메시지로 구성하고 이를 서명하여 현재 순서 정렬 서비스

에 제출한다. 현재 순서 정렬 서비스는 메시지를 새로운 블록에 포함하여 블록체인 노드로 전파하고 블록체인 노드는 자신이 수신한 블록 정보와 타 블록체인 노드가 수신한 블록 정보를 비교하여 현재 순서 정렬 서비스의 오동작을 검출한다. 블록체인 노드는 현재 순서 정렬 서비스가 유한하게 정해진 시간 동안 블록을 전파하지 않는 경우도 오동작으로 판단한다. 블록체인 노드는 현재 순서 정렬 서비스의 오동작을 검출하면 타 블록체인 노드와 자신이 갖고 있는 블록체인 원장 정보를 주고 받고 이를 기반으로 신규 순서 정렬 서비스에서 시작할 상태 정보와 상태 정보에 대한 증거를 포함하여 변경 제안 트랜잭션으로 생성하고 신규 정렬 서비스에 제출한다. 이후 블록체인 노드들은 변경 제안 트랜잭션에 합의하고 신규 순서 정렬 서비스에서 블록체인 서비스를 재개한다. 블록체인 노드의 순서 정렬 서비스 감사 및 변경은 블록 단위로 비잔틴 장애 감내 프로토콜을 적용한다.

[0119] 본 발명의 일 실시예에 따른 블록체인 플랫폼에서 비잔틴 장애 감내 방법은, 실용적 비잔틴 장애 감내(PBFT)에 기초하여 감내 가능한 장애 블록체인 노드들의 최대 개수가 f 인 환경에서도 순서 정렬 서비스의 안정성(safety)과 생존성(liveness) 문제에 대응할 수 있다.

[0120] 본 발명에 따른 블록체인 플랫폼에서 비잔틴 장애 감내 방법의 전술한 특징은, 블록체인 플랫폼에서 순서 정렬 서비스의 장애를 감내하는 최초의 발명이다.

[0121] 또한, 해시 체인으로 연결된 두 블록이 주어졌을 때, 반드시 하나의 해시 체인 경로만 존재한다는 블록체인의 해시 체인 특성을 활용하여 블록체인 노드의 감사 및 변경 비용을 줄일 수 있다는 장점을 가진다.

[0122] 또한, 순서 정렬 서비스의 변경은 특정 블록체인 노드에 의해 주도적으로 수행되는 것이 아닌 모든 노드가 독립적으로 변경 요청 메시지 및 변경 제안 트랜잭션을 생성하고, 변경 제안 트랜잭션에 동의하는 탈중앙화 형태로 수행된다는 장점을 가진다.

[0124] 본 발명의 실시예들에 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 데이터가 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.

[0125] 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.

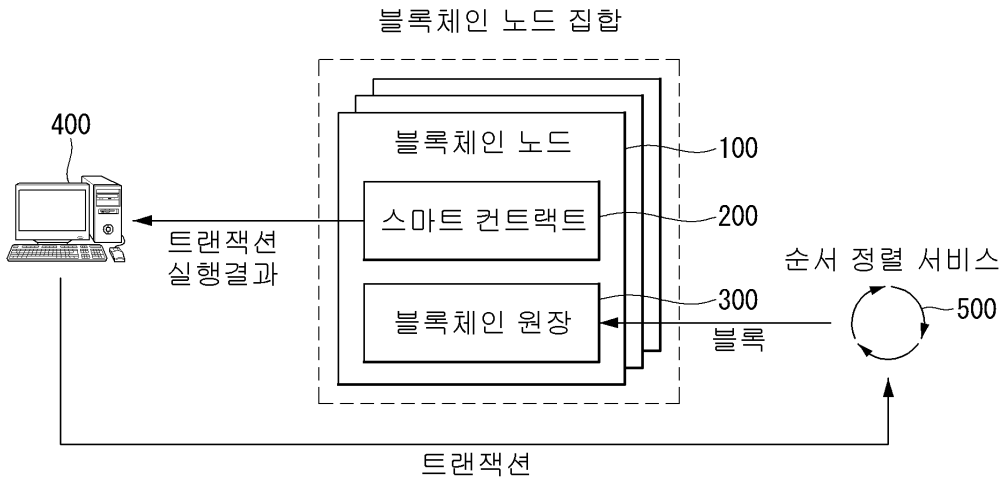
[0126] 본 발명의 일부 측면들은 장치의 문맥에서 설명되었으나, 그것은 상응하는 방법에 따른 설명 또한 나타낼 수 있고, 여기서 블록 또는 장치는 방법 단계 또는 방법 단계의 특징에 상응한다. 유사하게, 방법의 문맥에서 설명된 측면들은 또한 상응하는 블록 또는 아이템 또는 상응하는 장치의 특징으로 나타낼 수 있다. 방법 단계들의 몇몇 또는 전부는 예를 들어, 마이크로프로세서, 프로그램 가능한 컴퓨터 또는 전자 회로와 같은 하드웨어 장치에 의해(또는 이용하여) 수행될 수 있다. 몇몇의 실시예에서, 가장 중요한 방법 단계들의 하나 이상은 이와 같은 장치에 의해 수행될 수 있다.

[0127] 실시예들에서, 프로그램 가능한 로직 장치(예를 들어, 필드 프로그머블 게이트 어레이)가 여기서 설명된 방법들의 기능의 일부 또는 전부를 수행하기 위해 사용될 수 있다. 실시예들에서, 필드 프로그머블 게이트 어레이는 여기서 설명된 방법들 중 하나를 수행하기 위한 마이크로프로세서와 함께 작동할 수 있다. 일반적으로, 방법들은 어떤 하드웨어 장치에 의해 수행되는 것이 바람직하다.

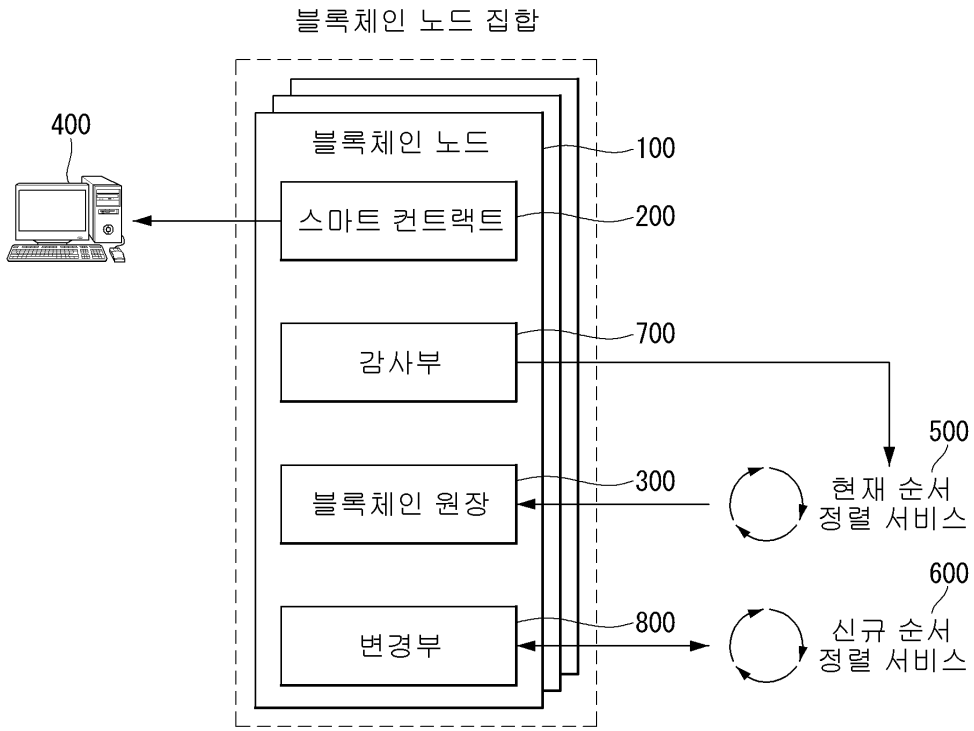
[0128] 이상 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

도면

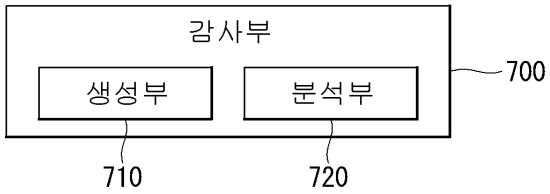
도면1


블록체인 노드 집합
400
블록체인 노드
100
스마트 컨트랙트
200
트랜잭션
실행결과
순서 정렬 서비스
300
블록
블록체인 원장
500
트랜잭션

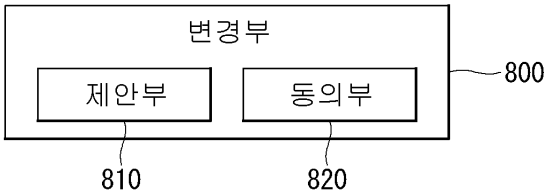
도면2


블록체인 노드 집합
400
블록체인 노드
100
스마트 컨트랙트
200
감사부
700
500
300
블록체인 원장
현재 순서
정렬 서비스
600
800
변경부
신규 순서
정렬 서비스

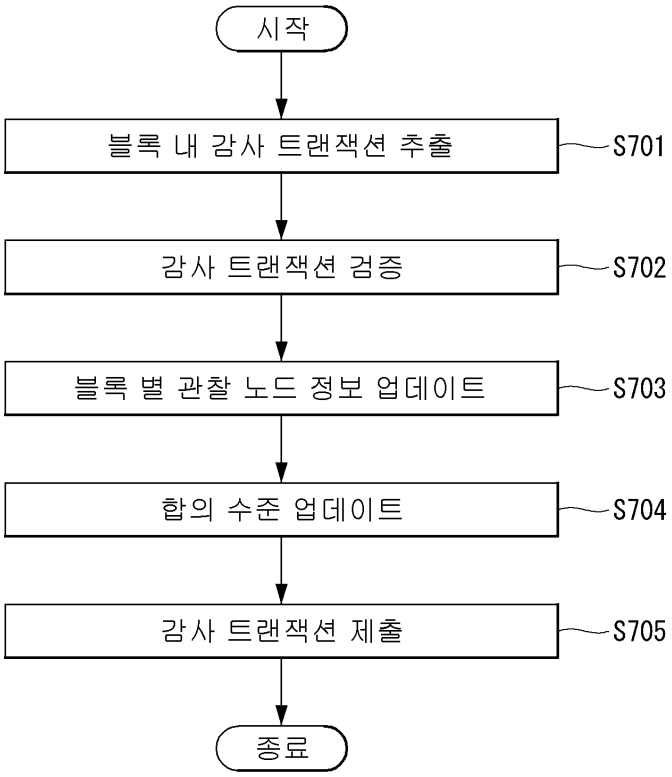
도면3


감사부
생성부
분석부
700
710
720

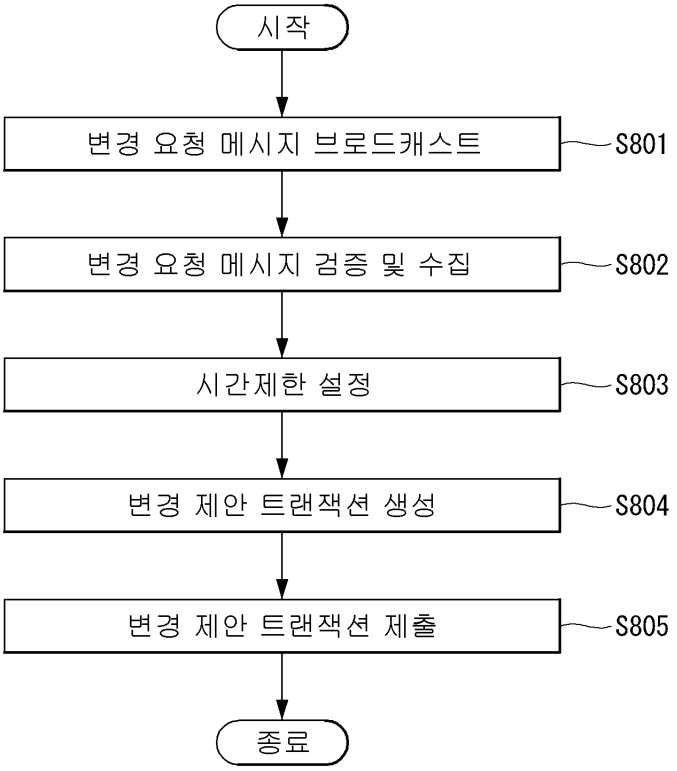
도면4


변경부
제안부
동의부
800
810
820

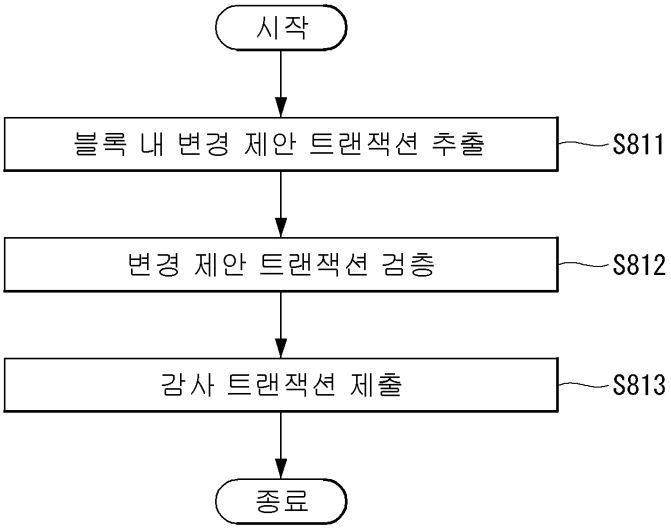
도면5


시작
블록 내 감사 트랜잭션 추출
S701
감사 트랜잭션 검증
S702
블록 별 관찰 노드 정보 업데이트
S703
합의 수준 업데이트
S704
감사 트랜잭션 제출
S705
종료

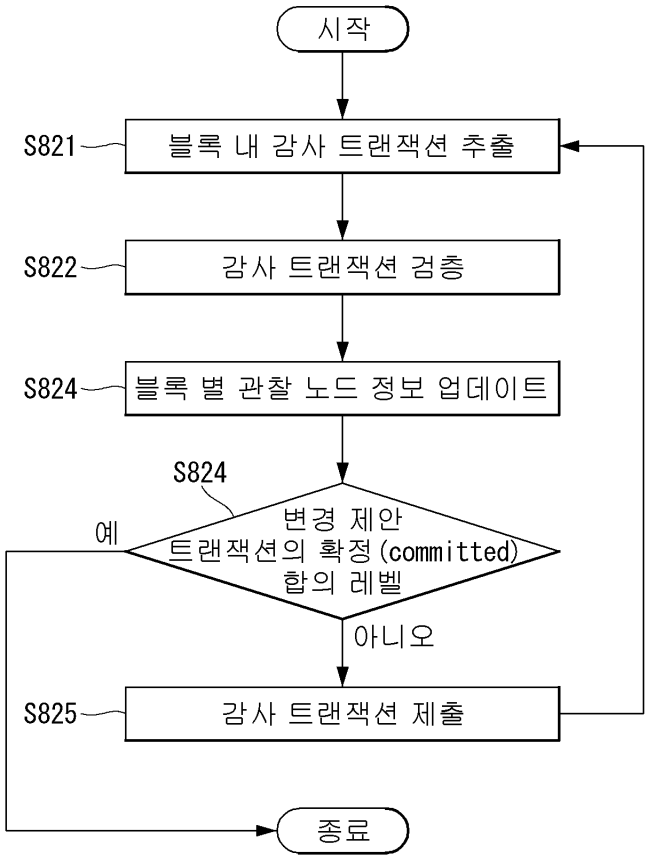
도면6


시작
변경 요청 메시지 브로드캐스트
S801
변경 요청 메시지 검증 및 수집
S802
시간제한 설정
S803
변경 제안 트랜잭션 생성
S804
변경 제안 트랜잭션 제출
S805
종료

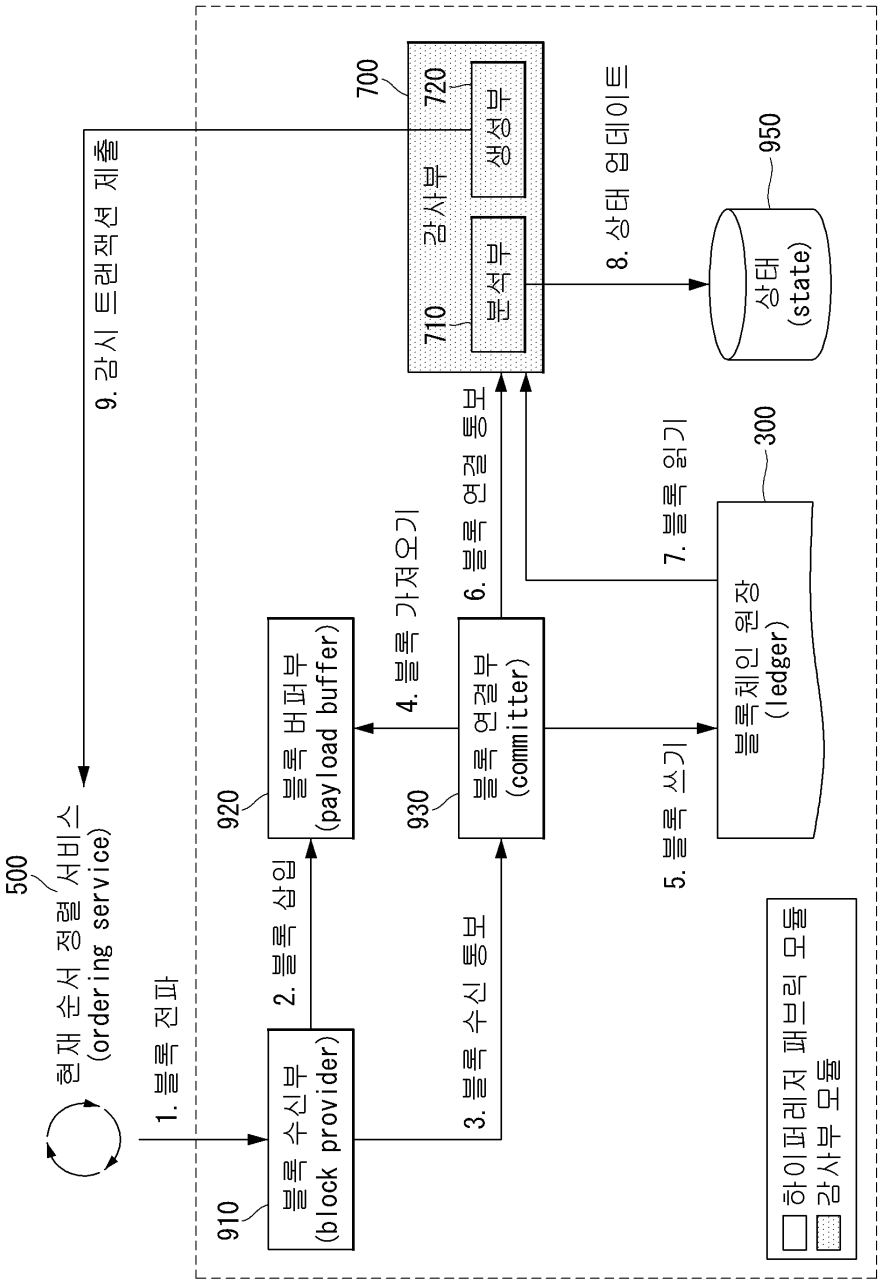
도면7


시작
블록 내 변경 제안 트랜잭션 추출
S811
변경 제안 트랜잭션 검증
S812
감사 트랜잭션 제출
S813
종료

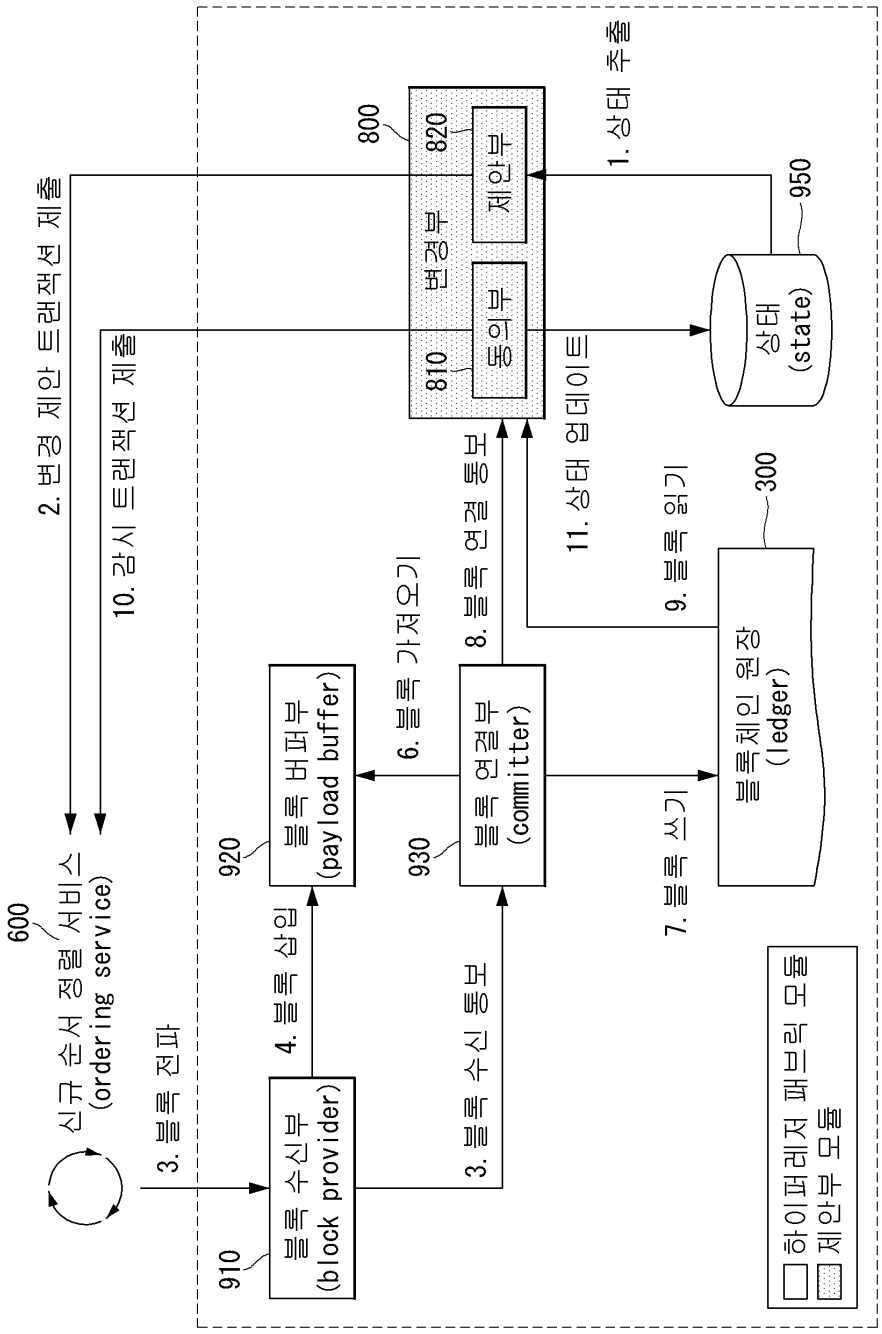
도면8


시작
S821
블록 내 감사 트랜잭션 추출
S822
감사 트랜잭션 검증
S824
블록 별 관찰 노드 정보 업데이트
S824
변경 제안
트랜잭션의 확정(committed)
합의 레벨
예
아니오
S825
감사 트랜잭션 제출
종료

도면9


500
현재 순서 정렬 서비스
(ordering service)
1. 블록 전파
910
블록 수신부
(block provider)
2. 블록 삽입
920
블록 버퍼부
(payload buffer)
3. 블록 수신 통보
930
블록 연결부
(committer)
4. 블록 가져오기
5. 블록 쓰기
블록체인 원장
(ledger)
300
6. 블록 연결 통보
7. 블록 읽기
700
감사부
710
분석부
720
생성부
8. 상태 업데이트
950
상태
(state)
9. 감시 트랜잭션 제출
하이퍼레저 패브릭 모듈
감사부 모듈

도면10


1. 상태 추출
2. 변경 제안 트랜잭션 제출
10. 감시 트랜잭션 제출
11. 상태 업데이트
800
820
제안부
변경부
810
동의부
950
상태
(state)
600
신규 순서 정렬 서비스
(ordering service)
3. 블록 전파
4. 블록 삽입
920
블록 버퍼부
(payload buffer)
910
블록 수신부
(block provider)
6. 블록 가져오기
3. 블록 수신 통보
8. 블록 연결 통보
930
블록 연결부
(committer)
9. 블록 읽기
7. 블록 쓰기
300
블록체인 원장
(ledger)
하이퍼레저 패브릭 모듈
제안부 모듈