



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2024년12월20일
(11) 등록번호 10-2745042
(24) 등록일자 2024년12월17일

(51) 국제특허분류(Int. Cl.)
H04L 9/00 (2022.01) H04L 9/06 (2006.01)

(52) CPC특허분류
H04L 9/50 (2022.05)
H04L 9/0643 (2013.01)

(21) 출원번호 10-2023-0182257

(22) 출원일자 2023년12월14일

심사청구일자 2023년12월14일

(56) 선행기술조사문헌

KR1020190065876 A*

(뒷면에 계속)

(73) 특허권자

국립부경대학교 산학협력단

부산광역시 남구 용소로 45, 부경대학교내 (대연동)

(72) 발명자

이경현

부산광역시 남구 신선로 566, 308동 2903호

현지연

부산광역시 사상구 대동로64번길 22, 102동 112호

(74) 대리인

김성현

전체 청구항 수 : 총 7 항

심사관 : 나용수

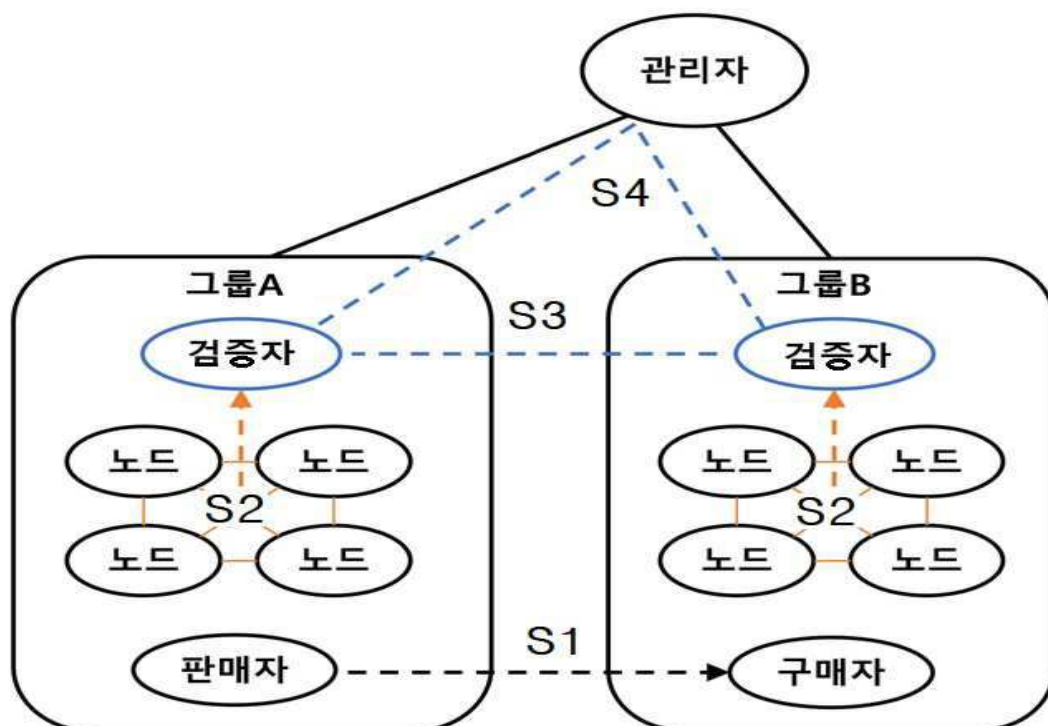
(54) 발명의 명칭 공급망에 최적화된 허가형 블록체인 시스템 및 그 운영방법

(57) 요약

본 발명은 다수의 노드가 구성된 그룹이 다수 구비되며, 상기 다수 그룹을 관리하는 관리자 노드가 구비된 허가형 블록체인 시스템에서 최초 거래가 발생하면, (a) 상기 각 그룹 내에서 검증을 위한 투표가 진행되며, 상기 투표 결과 가장 많은 추천인을 확보한 노드가 그 그룹의 검증자 노드로 채택되는 단계와; (b) 상기 그룹 중 그룹A

(뒷면에 계속)

대표도 - 도3



에 속한 검증자 노드, 그룹B에 속한 검증자 노드, 관리자 노드는 해당 거래에 대한 유효성을 검증하되, 유효성 검증 결과가 올바르다면 True를, 아니라면 False를 반환하는 단계와; (c) 상기 단계 (b)에서, 과반수 이상이 True를 반환하였다면 해당 거래에 대한 합의가 성립하게 되며, 해당 거래에 대한 거래검증 결과에 대한 key값을 HASH(ID, 판매자, 구매자)를 통해 생성하고 거래검증key에 저장하는 단계와; (d) 블록체인상에서 직전 블록에 존재하는 원장과 현재 거래검증 결과에 대한 key값의 HASH값을 구해 현재 거래 블록의 HASH값으로 기록하는 단계; 를 진행하는 공급망에 최적화된 허가형 블록체인 시스템 운영방법을 제공한다.

(56) 선행기술조사문헌

KR1020190100733 A*

KR1020220061296 A*

KR102485525 B1*

W02022240906 A1*

*는 심사관에 의하여 인용된 문헌

이 발명을 지원한 국가연구개발사업

과제고유번호	1711202494
과제번호	2023-DD-RD-0152-01
부처명	과학기술정보통신부
과제관리(전문)기관명	(재단)연구개발특구진흥재단
연구사업명	연구개발특구육성
연구과제명	블록체인 기반 스마트 물류 기술사업화 협업플랫폼 구축사업
과제수행기관명	재단법인부산테크노파크
연구기간	2023.04.01 ~ 2025.12.31

명세서

청구범위

청구항 1

허가형 블록체인 네트워크의 관리자 노드는, 대리점 노드들의 참여 권한을 부여하고 그룹을 지정 가능하게 구비되며,

상기 허가형 블록체인 네트워크에 참가한 노드들은, 블록체인 DB와 블록체인 프로그램으로 구성되며, 상기 블록체인 프로그램을 통해 거래내역에 대한 검증 과정에 참가하고, 검증을 통해 획득한 블록을 저장 가능하며,

상기 블록체인 DB는, 블록번호, 해당거래ID, 판매자ID, 구매자ID, 이전블록HASH, 거래검증key, 직전거래리스트, 필요정보HASH를 포함하되,

상기 블록번호는 블록체인상에서 현재 블록이 몇 번째로 생성되었는지를 알려주고, 이를 통해 현재 블록의 이전 블록이나 n번째 블록에 접근하는 것이 가능한 것을 특징으로 하는 공급망에 최적화된 허가형 블록체인 시스템.

청구항 2

제1항에 있어서,

상기 블록체인 네트워크상에서 상기 노드들이 그룹에 속하는 기준은 취급하는 제품에 따라 결정되되,

각 그룹 내의 노드들은 동일한 종류의 제품을 구매 및 판매하는 것을 원칙으로 하는 것을 특징으로 하는 공급망에 최적화된 허가형 블록체인 시스템.

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 해당거래ID는 현재 블록에 기록될 거래에 부여한 식별번호이고, 상기 판매자ID와 구매자ID는 각각 판매자와 구매자의 식별번호이며, 상기 이전블록HASH는 HASH의 결과값이고, 상기 거래검증key는 합의알고리즘을 통해 생성되는 key값인 것을 특징으로 하는 공급망에 최적화된 허가형 블록체인 시스템.

청구항 5

제1항에 있어서,

상기 직전거래리스트는, 판매자가 현재 판매하려는 제품과 관련되어 제시해야 하는 직전거래 내역들의 ID를 리스트로 생성한 것인 것을 특징으로 하는 공급망에 최적화된 허가형 블록체인 시스템.

청구항 6

제1항에 있어서,

상기 필요정보HASH는, 판매자가 현재 판매하려는 제품과 관련되어 제시해야 하는 직전거래 품목의 필요한 정보들에 대하여 진위성을 판별하기 위해 등록해둔 HASH값들을 리스트로 생성한 것인 것을 특징으로 하는 공급망에 최적화된 허가형 블록체인 시스템.

청구항 7

청구항 1항의 공급망에 최적화된 허가형 블록체인 시스템을 이용한 운영방법에 있어서,

다수의 노드가 구성된 그룹이 다수 구비되며, 상기 다수 그룹을 관리하는 관리자 노드가 구비된 허가형 블록체인 시스템에서 최초 거래가 발생하면,

- (a) 상기 각 그룹 내에서 검증을 위한 투표가 진행되며, 상기 투표 결과 가장 많은 추천인을 확보한 노드가 그 그룹의 검증자 노드로 채택되는 단계와;
- (b) 상기 그룹 중 그룹A에 속한 검증자 노드, 그룹B에 속한 검증자 노드, 관리자 노드는 해당 거래에 대한 유효성을 검증하되, 유효성 검증 결과가 올바르다면 True를, 아니라면 False를 반환하는 단계와;
- (c) 상기 단계 (b)에서, 과반수 이상이 True를 반환하였다면 해당 거래에 대한 합의가 성립하게 되며, 해당 거래에 대한 거래검증 결과에 대한 key값을 HASH(ID, 판매자, 구매자)를 통해 생성하고 거래검증key에 저장하는 단계와;
- (d) 블록체인상에서 직전 블록에 존재하는 원장과 현재 거래검증 결과에 대한 key값의 HASH값을 구해 현재 거래 블록의 HASH값으로 기록하는 단계;를 진행하는 것을 특징으로 하는 공급망에 최적화된 허가형 블록체인 시스템 운영방법.

청구항 8

제7항에 있어서,

상기 단계 (d)는, HASH(직전블록 데이터, 현재 거래 검증key)를 블록HASH에 저장하고, 블록 데이터를 생성하여 블록체인에 등록하는 것을 특징으로 하는 공급망에 최적화된 허가형 블록체인 시스템 운영방법.

청구항 9

삭제

청구항 10

삭제

발명의 설명

기술 분야

[0001] 본 발명은 공급망에 최적화된 허가형 블록체인 시스템 및 그 운영방법에 관한 것으로서, 보다 상세하게는 공급망에 최적화된 블록체인 시스템이되 비용이 절감되고 실제로 거래 대상이 되는 제품의 진위성이 반드시 검증되도록 개선된 공급망에 최적화된 허가형 블록체인 시스템 및 그 운영방법에 관한 것이다.

배경 기술

[0002] 일반적으로 공급망은 원재료를 획득하는 과정에서부터 중간과정을 거쳐 소비자에게 유통하기까지의 과정을 조직적으로 관리하기 위해 형성되는 기업 간의 비즈니스 프로세스 네트워크이다.

[0003] 이러한 공급망의 과정에는 원재료를 중간재나 최종재로 변환하는 제조 과정과 실제 소비자에게 공급하기 위한 유통과정이 포함된다.

[0004] 또한, 공급망은 제품 제공 및 서비스 과정을 원천부터 소비까지 이르도록 공급업체, 제조공장, 유통센터, 소매할인점, 고객을 연결한다.

[0005] 그리고 공급망에서 물질, 정보, 지불은 양방향으로 흐른다.

[0006] 또한, 공급 사슬의 상류(upstream) 지역에는 공급업체 간의 거래, 즉 업체 간의 관계를 관리하기 위한 B2B 프로세스가 포함되고, 하류(downstream) 지역은 최종 고객에게 제품을 유통하고 전달하기 위해 조직과 프로세스를 구성된다.

[0007] 한편, 블록체인 기술은, 탈중앙화된 분산형 네트워크 위에서 구축된 분산원장 시스템(DLT; Distributed Ledger Technology)으로써, 네트워크에 참가하고 있는 모든 노드들이 데이터를 공유받아 원장에 기록하는 데이터 분산 관리 기술이다.

[0008] 이러한 블록체인은 상호 신뢰하기 어려운 노드들 사이에서 데이터를 관리해야 할 때, 투명성과 신뢰성을 확보하려는 경우 적용 가능한 기술이다. 네트워크에 참가하고 있는 DB(Database)에 데이터를 반영하기 위해서는 합의 알고리즘을 통해 다른 노드들의 승인을 얻어야 한다.

- [0009] 그리고 허가형 블록체인이란, 권한을 가진 관리자에 의해 허가된 참가자들로 구성된 블록체인 네트워크로, 따라서 허가된 참가자 이외에는 블록체인 네트워크에 기록된 데이터에 접근하는 것이 불가능하다.
- [0010] 또한, 자동화된 공급망상에서 데이터가 기록되고 유지되는 동안 외부적인 요인에 의해 변조가 발생할 가능성이 항상 존재하기 때문에, 그것을 감시하고 추적하기 위한 기능을 구현해야한다.
- [0011] 이와 동시에 무수한 거래내역이 발생하는 공급망상에서는 비용을 절감하기 위해서는 반드시 검증에 필요한 과정을 최적화해야 할 필요가 있다.

선행기술문헌

특허문헌

- [0012] (특허문헌 0001) 1. 등록특허 제10-2433504호(2022년 08월 12일 등록)의 허가된 블록체인 네트워크를 위한 에러 정정 코드에 기초하는 블록체인 데이터 저장
- (특허문헌 0002) 2. 등록특허 제10-2507732호(2023년 03월 03일 등록)의 허가형 블록체인에서의 분리형 보증 처리 방법 및 시스템
- (특허문헌 0003) 3. 등록특허 제10-2419853호(2022년 07월 07일 등록)의 블록체인에 기반한 DID 인증서를 이용한 허가형 블록체인 플랫폼 인증 방법 및 시스템
- (특허문헌 0004) 4. 등록특허 제10-2294571호(2021년 08월 23일 등록)의 대체 불가능 토큰을 지원하는 허가형 블록체인 시스템

발명의 내용

해결하려는 과제

- [0013] 본 발명은 상기와 같은 문제점을 해결하기 위하여 창출된 것으로서, 공급망에 최적화된 블록체인 시스템이되 비용이 절감되고 실제로 거래 대상이 되는 제품의 진위성이 반드시 검증되도록 한 공급망에 최적화된 허가형 블록체인 시스템 및 그 운영방법을 제공하는데 그 목적이 있다.

과제의 해결 수단

- [0014] 상기와 같은 목적을 달성하기 위한 본 발명의 공급망에 최적화된 허가형 블록체인 시스템은,
- [0015] 허가형 블록체인 네트워크의 관리자 노드는, 대리점 노드들의 참여 권한을 부여하고 그룹을 지정 가능하게 구비되며,
- [0016] 상기 허가형 블록체인 네트워크에 참가한 노드들은, 블록체인 DB와 블록체인 프로그램으로 구성되며, 상기 블록체인 프로그램을 통해 거래내역에 대한 검증 과정에 참가하고, 검증을 통해 획득한 블록을 저장 가능하게 구비된 것을 그 특징으로 한다.
- [0017] 본 발명에 있어서, 상기 블록체인 네트워크상에서 상기 노드들이 그룹에 속하는 기준은 취급하는 제품에 따라 결정되되, 각 그룹 내의 노드들은 동일한 종류의 제품을 구매 및 판매하는 것을 원칙으로 한다.
- [0018] 본 발명에 있어서, 상기 블록체인 DB는, 블록번호, 해당거래ID, 판매자ID, 구매자ID, 이전블록HASH, 거래검증key, 직전거래리스트, 필요정보HASH를 포함하되, 상기 블록번호는 블록체인상에서 현재 블록이 몇 번째로 생성되었는지를 알려주고, 이를 통해 현재 블록의 이전 블록이나 n번째 블록에 접근하는 것이 가능하다.
- [0019] 본 발명에 있어서, 상기 해당거래ID는 현재 블록에 기록될 거래에 부여한 식별번호이고, 상기 판매자ID와 구매자ID는 각각 판매자와 구매자의 식별번호이며, 상기 이전블록HASH는 HASH의 결과값이고, 상기 거래검증key는 합의알고리즘을 통해 생성되는 key값이다.
- [0020] 본 발명에 있어서, 상기 전거래리스트는, 판매자가 현재 판매하려는 제품과 관련되어 제시해야하는 직전거래 내역들의 ID를 리스트로 생성한다.
- [0021] 본 발명에 있어서, 상기 필요정보HASH는, 판매자가 현재 판매하려는 제품과 관련되어 제시해야 하는 직전거래

품목의 필요한 정보들에 대하여 진위성을 판별하기 위해 등록해둔 HASH값들을 리스트로 생성한다.

- [0022] 상기와 같은 목적을 달성하기 위한 본 발명의 공급망에 최적화된 허가형 블록체인 시스템 운영방법은,
- [0023] 다수의 노드가 구성된 그룹이 다수 구비되며, 상기 다수 그룹을 관리하는 관리자 노드가 구비된 허가형 블록체인 시스템에서 최초 거래가 발생하면,
- [0024] (a) 상기 각 그룹 내에서 검증을 위한 투표가 진행되며, 상기 투표 결과 가장 많은 추천인을 확보한 노드가 그 그룹의 검증자 노드로 채택되는 단계와;
- [0025] (b) 상기 그룹 중 그룹A에 속한 검증자 노드, 그룹B에 속한 검증자 노드, 관리자 노드는 해당 거래에 대한 유효성을 검증하되, 유효성 검증 결과가 올바르다면 True를, 아니라면 False를 반환하는 단계와;
- [0026] (c) 상기 단계 (b)에서, 과반수 이상이 True를 반환하였다면 해당 거래에 대한 합의가 성립하게 되며, 해당 거래에 대한 거래검증 결과에 대한 key값을 HASH(ID, 판매자, 구매자)를 통해 생성하고 거래검증key에 저장하는 단계와;
- [0027] (d) 블록체인상에서 직전 블록에 존재하는 원장과 현재 거래검증 결과에 대한 key값의 HASH값을 구해 현재 거래 블록의 HASH값으로 기록하는 단계;를 진행하는 것을 그 특징으로 한다.
- [0028] 본 발명에 있어서, 상기 단계 (d)는, HASH(직전블록 데이터, 현재 거래 검증key)를 블록HASH에 저장하고, 블록 데이터를 생성하여 블록체인에 등록한다.
- [0029] 상기와 같은 목적을 달성하기 위한 다른 본 발명의 공급망에 최적화된 허가형 블록체인 시스템 운영방법은,
- [0030] 다수의 노드가 구성된 그룹이 다수 구비되며, 상기 다수 그룹을 관리하는 관리자 노드가 구비된 허가형 블록체인 시스템에서 직전 거래 내역이 존재한 상태에서 거래가 발생하면,
- [0031] (A) 상기 그룹 내에서 검증을 위한 투표가 진행되며, 이때 가장 많은 추천인을 확보한 노드가 해당 그룹의 검증자 노드로 채택되는 단계와;
- [0032] (B) 제품의 진위성 검증을 위해서 상기 직전거래에서 제출했던 자료를 직전거래자 노드를 통해 제공받는 단계와;
- [0033] (C) 상기 그룹 중 그룹A에 속한 검증자 노드, 그룹B에 속한 검증자 노드, 관리자 노드는 제공받은 제출 자료를 토대로 해당 거래에 대한 유효성을 검증하되, 유효성 검증 결과가 올바르다면 True를, 아니라면 False를 반환하는 단계와;
- [0034] (D) 상기 단계 (C)에서, 과반수 이상이 True를 반환하였다면, 해당 거래에 대한 합의가 성립하게 되며, 해당 거래에 대한 거래검증 결과에 대한 key값을 HASH(ID, 판매자, 구매자)를 통해 생성하고 거래검증key에 저장하는 단계와;
- [0035] (E) 상기 블록체인상에서 직전 블록에 존재하는 원장과 현재 거래검증 결과에 대한 key값의 HASH값을 구해 현재 거래 블록의 HASH값으로 기록하는 단계;를 진행한다.
- [0036] 본 발명에 있어서, 상기 단계 (E)는, HASH(직전블록 데이터, 현재 거래 검증key)를 블록HASH에 저장하고, 블록 데이터를 생성하여 블록체인에 등록한다.

발명의 효과

- [0037] 본 발명의 실시예에 따르면, 거래에 직접 연관된 그룹 사이에서 발생하는 내역에 관한 데이터만을 블록체인으로 유지하여 데이터베이스(DB)를 유지하기 위해 필요한 비용을 직접 줄였다.
- [0038] 또한, 특정 제품의 거래가 진행되는 경우, 해당 제품의 직전거래에 참가한 판매자의 검증을 통해 직접 진위성을 보장받을 수 있다.

도면의 간단한 설명

- [0039] 도 1은 본 발명에 따른 공급망에 최적화된 허가형 블록체인 시스템 및 그 운영방법이 적용된 허가형 블록체인 네트워크의 구조도.
- 도 2는 본 발명이 적용된 네트워크에 참가한 노드에 속한 블록체인 DB에 대한 구조도.

도 3은 본 발명에 따른 공급망에 최적화된 허가형 블록체인 시스템 운영방법의 일 실시예로 허가형 블록체인 시스템에서의 합의 알고리즘 프로세스 도면.

도 4는 본 발명에 따른 공급망에 최적화된 허가형 블록체인 시스템 운영방법의 다른 실시예로 허가형 블록체인 시스템에서의 합의 알고리즘 프로세스 도면.

발명을 실시하기 위한 구체적인 내용

- [0040] 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 실시예를 상세히 설명하기로 한다.
- [0041] 설명에 앞서, 후술하는 본 발명의 환경 및 용어 정의는, 먼저, 관리자와 거래참가자의 각 포인트를 노드라 부르고, 노드a와 노드b의 거래를 거래ab라 칭한다.
- [0042] 또한, 허가형 블록체인 네트워크(이하, 네트워크라 한다.)상에는 같은 거래품목을 다루는 노드들을 모은 그룹이 형성되어있다.
- [0043] 그리고 그룹 중 그룹A에 속한 노드와 그룹B에 속한 노드가 거래를 진행하는 경우, 이것을 거래AB라 한다.
- [0044] 또한, 상기 거래는 거래ab, 거래bc, ..., 거래fg와 같이, 단방향으로 진행되는 것으로 하고, 특정 거래의 전단계에서 진행한 거래를 직전거래라고 한다. 예를 들면, 거래bc가 진행되었다면, 직전거래는 거래ab가 된다.
- [0045] 도 1에는 본 발명에 따른 공급망에 최적화된 허가형 블록체인 시스템 및 그 운영방법이 적용된 허가형 블록체인 네트워크의 구조도가 도시되어 있다.
- [0046] 도 1을 참조하면, 본 발명에 따른 공급망에 최적화된 허가형 블록체인 시스템에서 모든 노드는 블록체인 DB(Database)와 블록체인 프로그램으로 구성된다.
- [0047] 그리고 네트워크의 관리자 노드는 대리점 노드들의 참여 권한을 부여하는 것과 그룹을 지정하는 것이 가능하다.
- [0048] 또한, 네트워크에 참가한 노드들은 상기 블록체인 프로그램을 통해 거래내역에 대한 검증 과정에 참가하고, 검증을 통해 획득한 블록을 저장하는 것이 가능하다.
- [0049] 그리고 네트워크상에서 노드들이 그룹에 속하는 기준은 취급하는 제품에 따라 결정되고, 각 그룹 내의 노드들은 동일한 종류의 제품을 구매 및 판매하는 것을 원칙으로 한다.
- [0050] 또한, 하나의 기업이 여러 개의 그룹에 동시에 소속되는 것도 가능하지만, 별개의 노드와 별개의 식별번호를 받게 된다.
- [0051] 도 2에는 본 발명이 적용된 네트워크에 참가한 노드에 속한 블록체인 DB에 대한 구조도가 도시되어 있다.
- [0052] 즉, 도 2는 블록체인 노드가 보유한 블록체인 DB의 구조도이다.
- [0053] 도 2를 참조하면, 블록체인 DB(10)에서 유지되는 원장의 내역은, 블록번호(11), 해당거래ID(12), 판매자ID(13), 구매자ID(14), 이전블록HASH(15), 거래검증key(16), 직전거래리스트(17), 필요정보HASH(18)를 포함한다.
- [0054] 구체적으로는, 상기 블록번호(11)는 블록체인상에서 현재 블록이 몇 번째로 생성되었는지를 알려준다. 이를 통해 현재 블록의 이전 블록이나 n번째 블록에 접근하는 것이 가능하다.
- [0055] 그리고 상기 해당거래ID(12)는 현재 블록에 기록될 거래에 부여한 식별번호이고, 상기 판매자ID(13)와 구매자ID(14)는 각각 판매자와 구매자의 식별번호이다.
- [0056] 또한, 상기 이전블록HASH(15)는 HASH(이전블록에 저장된 데이터)의 결과값이고, 상기 거래검증key(16)는 합의 알고리즘을 통해 생성되는 key값이다.
- [0057] 그리고 상기 직전거래리스트(17)는 판매자가 현재 판매하려는 제품과 관련되어 제시해야하는 직전거래 내역들의 ID를 리스트로 생성한 것이다.
- [0058] 또한, 상기 필요정보HASH(18)는 판매자가 현재 판매하려는 제품과 관련되어 제시해야 하는 직전거래 품목의 필요한 정보들에 대하여 진위성을 판별하기 위해 등록해둔 HASH값들을 리스트로 생성한 것이다.
- [0059] 도 3에는 본 발명에 따른 공급망에 최적화된 허가형 블록체인 시스템 운영방법의 일 실시예로, 허가형 블록체인 시스템에서의 합의 알고리즘 프로세스이다.

- [0060] 특히, 도 3은 공급망상에서 원료를 생산한 뒤, 최초로 거래하는 거래ab에 대한 합의 과정이다.
- [0061] 먼저, 거래ab가 발생한다면 거래를 수행하는 노드에 속해있는 그룹A와 그룹B의 각각에 대해 다음 과정을 거친다.(단계 S1)
- [0062] 이어서, 상기 그룹 내에서 검증을 위한 투표가 진행되며, 이때 가장 많은 추천인을 확보한 노드가 해당 그룹의 검증자 노드로 채택된다.(단계 S2)
- [0063] 그리고 상기 그룹A에 속한 검증자 노드, 그룹B에 속한 검증자 노드, 관리자 노드는 해당 거래에 대한 유효성을 검증한다.(단계 S3)
- [0064] 상기 단계 S3에서, 유효성 검증 결과가 올바르다면 True를, 아니라면 False를 반환한다.
- [0065] 또한, 과반수 이상이 True를 반환하였다면, 해당 거래에 대한 합의가 성립하게 되며, 해당 거래에 대한 거래검증 결과에 대한 key값을 HASH(ID, 판매자, 구매자)를 통해 생성하고, 거래검증key에 저장한다.(단계 S4)
- [0066] 이때, 블록체인상에서 직전 블록에 존재하는 원장과 현재 거래검증 결과에 대한 key값의 HASH값을 구해 현재 거래 블록의 HASH값으로 기록한다. 즉, HASH(직전블록 데이터, 현재 거래 검증key)를 블록HASH에 저장한다.
- [0067] 그리고 블록 데이터를 생성하여 블록체인에 등록한다.
- [0068] 도 4에는 본 발명에 따른 공급망에 최적화된 허가형 블록체인 시스템 운영방법의 다른 실시예로, 도 3의 일 실시예와는 달리, 거래bc, 거래cd, ..., 등 최초 거래 이후의 거래 과정에서 적용되는 합의 알고리즘이다.
- [0069] 도 4의 합의 프로세스에서는 반드시 직전 거래(거래ab) 내역이 존재하여야 성립한다.
- [0070] 예를 들어, 거래bc가 성립하려면, 이에 대응하는 직전거래ab가 존재하여야 한다.
- [0071] 해당 거래는 거래ab 이후에 대한 모든 거래에 해당되며, 설명을 위해 임의로 거래bc를 기준으로 하여 하였다.
- [0072] 도 4를 참조하면, 먼저, 거래bc가 발생한다면, 거래를 수행하는 노드에 속해있는 그룹B(또는 그룹N)와 그룹C(또는 그룹N+1)의 각각에 대해 프로세스를 진행한다.(단계 S11)
- [0073] 이어서, 상기 그룹 내에서 검증을 위한 투표가 진행되며, 이때 가장 많은 추천인을 확보한 노드가 해당 그룹의 검증자 노드로 채택된다.(단계 S12)
- [0074] 그리고 제품의 진위성 검증을 위해서 직전거래에서 제출했던 자료를 직전거래자 노드를 통해 제공받는다.(단계 S13)
- [0075] 또한, 상기 그룹A에 속한 검증자 노드, 그룹B에 속한 검증자 노드, 관리자 노드는 제공받은 제출 자료를 토대로 해당 거래에 대한 유효성을 검증한다.(단계 S14)
- [0076] 이때, 상기 유효성 검증 결과가 올바르다면 True를, 아니라면 False를 반환한다.
- [0077] 이어서, 과반수 이상이 True를 반환하였다면, 해당 거래에 대한 합의가 성립하게 되며, 해당 거래에 대한 거래검증 결과에 대한 key값을 HASH(ID, 판매자, 구매자)를 통해 생성하고, 거래검증key에 저장한다.(단계 S15)
- [0078] 그리고 이때, 블록체인상에서 직전 블록에 존재하는 원장과 현재 거래검증 결과에 대한 key값의 HASH값을 구해 현재 거래 블록의 HASH값으로 기록한다. 즉 HASH(직전블록 데이터, 현재 거래 검증key)를 블록HASH에 저장한다.
- [0079] 또한, 블록 데이터를 생성하여 블록체인에 등록한다.
- [0080] 상기한 바와 같은 구성을 갖는 본 발명에 따른 공급망에 최적화된 허가형 블록체인 시스템 및 그 운영방법은, 공급망상에서 발생하는 거래는 외부에 공개되는 것이 아니므로, 관리자 노드를 통해 운영되는 네트워크상에서 허가형 블록체인 시스템이 작동할 수 있도록 한 것이다.
- [0081] 그리고 거래자 간의 상품 내역이 중요한 공급망에서 추적 가능하고 신뢰할 수 있는 데이터 관리는 가장 중요한 과제이다.
- [0082] 따라서 본 발명은 다음 두 가지 문제를 해결하는 것에 초점을 맞추고 있다.
- [0083] 첫 번째는, 공급망에 속해있는 모든 그룹이 모든 거래 내역을 유지할 필요는 없다.
- [0084] 이를 위해서 거래에 직접 연관된 그룹 사이에서 발생하는 내역에 관한 데이터만을 블록체인으로 유지하는 것으

로 하여, DB를 유지하기 위해 필요한 비용을 직접 줄이고자 하였다.

[0085] 두 번째는, 거래내역의 진실성을 위해서는 실제로 거래 대상이 되는 제품의 진위성이 반드시 검증되어야한다.

[0086] 이를 위해 특정 제품의 거래가 진행되는 경우, 해당 제품의 직전거래에 참가한 판매자의 검증을 통해 직접 진위성을 보장받고자 하였다.

[0087] 상술한 바와 같이 본 발명은 도면에 도시된 일 실시예를 참고로 설명되었으나, 이는 예시적인 것에 불과하며, 당해 기술분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 실시예가 가능하다는 점을 이해할 것이다.

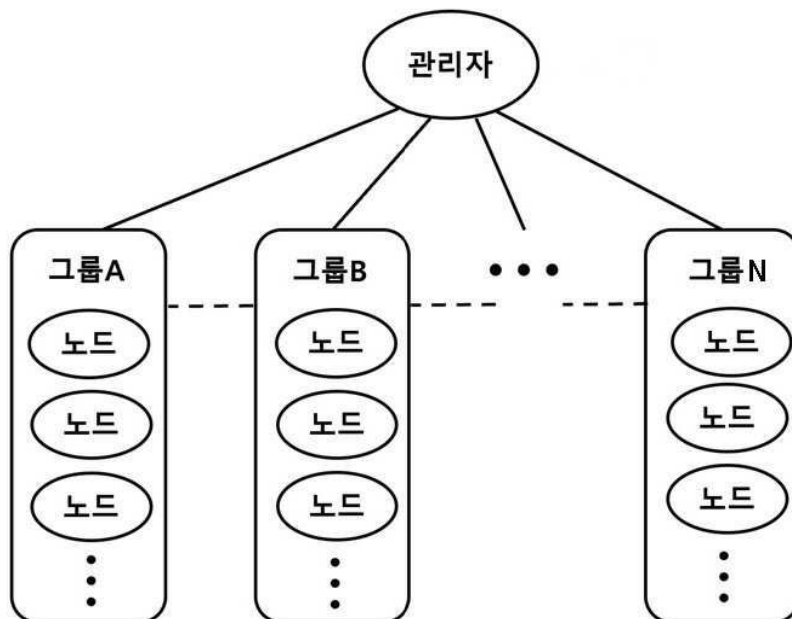
[0088] 따라서 본 발명의 진정한 보호 범위는 첨부된 청구범위에 의해서만 정해져야 할 것이다.

부호의 설명

- [0089]
- 10. 블록체인 DB
 - 11. 블록번호
 - 12. 해당거래ID
 - 13. 판매자ID
 - 14. 구매자ID
 - 15. 이전블록HASH
 - 16. 거래검증key
 - 17. 직전거래리스트
 - 18. 필요정보HASH

도면

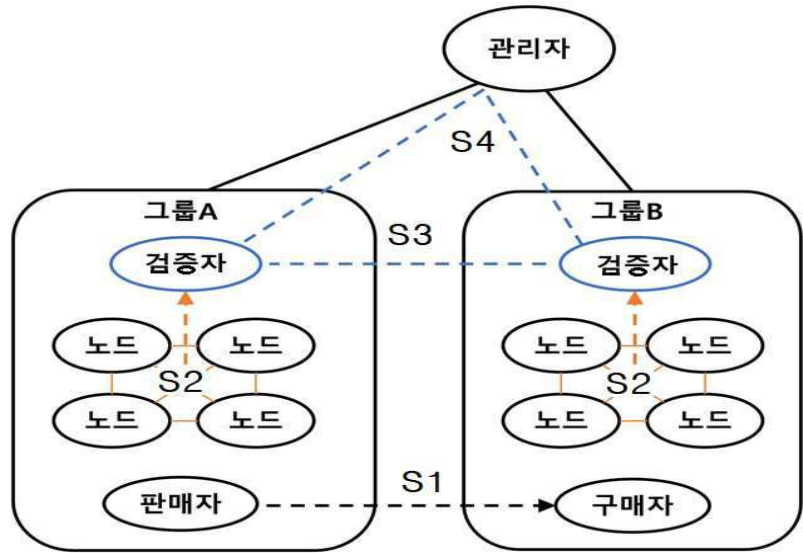
도면1



도면2



도면3



도면4

