



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0089250
(43) 공개일자 2022년06월28일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) G06F 16/22 (2019.01)
H04L 65/40 (2022.01)
(52) CPC특허분류
H04L 9/3236 (2013.01)
G06F 16/2246 (2019.01)
(21) 출원번호 10-2020-0179700
(22) 출원일자 2020년12월21일
심사청구일자 2020년12월21일

(71) 출원인
계명대학교 산학협력단
대구광역시 달서구 달구벌대로 1095, 계명대학교
산학협력관 201호(신당동)
(72) 발명자
박기현
대구광역시 달서구 도원로 45(도원동, 대곡강산타운)
박준수
대구광역시 달서구 와룡로 112-13, 202호(본리동)
(74) 대리인
특허법인 무한

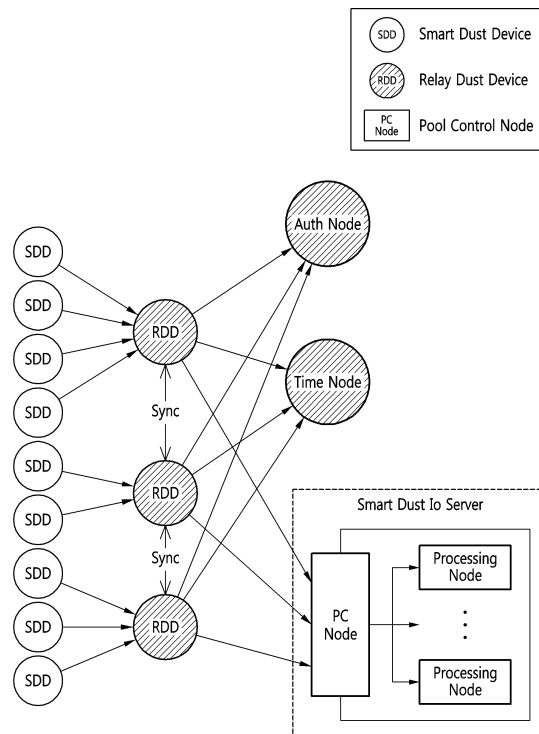
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 스마트 더스트 IoT 환경을 위한 경량화 블록체인 제공 방법 및 장치

(57) 요약

스마트 더스트 IoT 환경을 위한 경량화 블록체인 제공 방법 및 장치가 개시된다. 스마트 더스트(Smart Dust) 시스템의 제1 중계 더스트 장치(Relay Dust Device, RDD)가 수행하는 경량화 블록체인 제공 방법은 스마트 더스트 장치(Smart Dust Device, SDD)로부터 인증 요청이 수신된 경우, 신규 블록을 생성한 후 생성된 신규 블록의 해더(뒷면에 계속)

대표도 - 도1



(Header)에 상기 SDD의 기기 정보 및 이전 블록의 해시 값을 기록하는 단계; 상기 SDD의 인증에 필요한 인증 로우 데이터를 인증 노드로부터 수신하여 상기 SDD의 인증을 수행한 후 인증 결과를 상기 신규 블록의 헤더에 기록하는 단계; 상기 신규 블록의 헤더에 기록된 내용들에 해시 알고리즘을 적용하여 도출된 해시 값을 상기 신규 블록의 바디(Body)에 기록하는 단계; 상기 신규 블록을 다른 제2 RDD들과 동기화하여 관리하기 위해 타임 노드에 커밋 타임(Commit time)을 요청한 후 상기 신규 블록의 바디에 기록하는 단계; 및 상기 신규 블록을 다른 제2 RDD들로 전송한 후 대기 원장에 기록하였다가 상기 커밋 타임에 다른 RDD들과 동시에 상기 신규 블록을 커밋 원장에 기록하는 단계를 포함할 수 있다.

(52) CPC특허분류

H04L 67/1097 (2022.05)

H04L 67/12 (2022.05)

H04L 9/50 (2022.05)

이 발명을 지원한 국가연구개발사업

과제고유번호	1345317632
과제번호	2018R1D1A1B07043982
부처명	교육부
과제관리(전문)기관명	한국연구재단
연구사업명	기본연구
연구과제명	접근이 어려운 열악한 환경에서의 사물인터넷 시스템 연구
기 여 율	1/1
과제수행기관명	계명대학교
연구기간	2020.03.01 ~ 2021.02.28

명세서

청구범위

청구항 1

스마트 더스트(Smart Dust) 시스템의 제1 중계 더스트 장치(Relay Dust Device, RDD)가 수행하는 경량화 블록체인 제공 방법에 있어서,

스마트 더스트 장치(Smart Dust Device, SDD)로부터 인증 요청이 수신된 경우, 신규 블록을 생성한 후 생성된 신규 블록의 헤더(Header)에 상기 SDD의 기기 정보 및 이전 블록의 해시 값을 기록하는 단계;

상기 SDD의 인증에 필요한 인증 로우 데이터를 인증 노드로부터 수신하여 상기 SDD의 인증을 수행한 후 인증 결과를 상기 신규 블록의 헤더에 기록하는 단계;

상기 신규 블록의 헤더에 기록된 내용들에 해시 알고리즘을 적용하여 도출된 해시 값을 상기 신규 블록의 바디(Body)에 기록하는 단계;

상기 신규 블록을 다른 제2 RDD들과 동기화하여 관리하기 위해 타임 노드에 커밋 타임(Commit time)을 요청한 후 상기 신규 블록의 바디에 기록하는 단계; 및

상기 신규 블록을 다른 제2 RDD들로 전송한 후 대기 원장에 기록하였다가 상기 커밋 타임에 다른 RDD들과 동시에 상기 신규 블록을 커밋 원장에 기록하는 단계

를 포함하는 경량화 블록체인 제공 방법.

청구항 2

제1항에 있어서,

상기 다른 제2 RDD들은,

상기 제1 RDD로부터 수신된 신규 블록을 대기 원장에 기록하였다가 상기 신규 블록의 바디에 기록된 커밋 타임에 상기 신규 블록을 커밋 원장에 기록하는 경량화 블록체인 제공 방법.

청구항 3

제1항에 있어서,

상기 인증을 요청한 SDD의 인증을 수행하기 위하여 하위 노드에 대응하는 제2 RDD들에 원장 검증을 요청하는 단계

를 더 포함하는 경량화 블록체인 제공 방법.

청구항 4

제3항에 있어서,

상기 원장 검증은,

상기 제1 RDD 및 제2 RDD들이 바이너리 트리 구조의 형태로 검증이 수행되는 경량화 블록체인 제공 방법.

청구항 5

제4항에 있어서,

상기 원장 검증은,

원장 검증을 요청한 제1 RDD의 바이너리 트리 구조 최하위 노드에 루트(Root) RDD로의 오버레이 패스(Overlay path)를 임시로 연결하는 경량화 블록체인 제공 방법.

청구항 6

경량화 블록체인 제공 방법에 있어서,

스마트 더스트 장치(Smart Dust Device, SDD)로부터 인증 요청을 수신한 제1 중계 더스트 장치(Relay Dust Device, RDD)가 원장 검증을 위한 바이너리 트리 구조를 식별하는 단계;

상기 식별된 바이너리 트리 구조를 이용하여 원장 검증에 참여 가능한 다른 제2 RDD들이 과반 이상인지의 여부를 판단하는 단계;

상기 원장 검증에 참여 가능한 다른 제2 RDD들이 과반 미만으로 판단된 경우, 상기 바이너리 트리 구조를 변경하는 단계; 및

상기 변경된 바이너리 트리 구조에 기초하여 원장 검증을 수행하는 단계

를 포함하는 경량화 블록체인 제공 방법.

청구항 7

제6항에 있어서,

상기 바이너리 트리 구조를 변경하는 단계는,

상기 제2 RDD들에 원장 검증을 요청하는 제1 RDD의 바이너리 트리 구조 최하위 노드에 루트(Root) RDD로의 오버레이 패스(Overlay path)를 임시로 연결하는 경량화 블록체인 제공 방법.

청구항 8

경량화 블록체인 제공 방법을 제공하는 스마트 더스트(Smart Dust) 시스템의 제1 중계 더스트 장치(Relay Dust Device, RDD)에 대응하는 경량화 블록체인 제공 장치에 있어서,

프로세서를 포함하고,

상기 프로세서는,

스마트 더스트 장치(Smart Dust Device, SDD)로부터 인증 요청이 수신된 경우, 신규 블록을 생성한 후 생성된 신규 블록의 헤더(Header)에 상기 SDD의 기기 정보 및 이전 블록의 해시 값을 기록하고,

상기 SDD의 인증에 필요한 인증 로우 데이터를 인증 노드로부터 수신하여 상기 SDD의 인증을 수행한 후 인증 결과를 상기 신규 블록의 헤더에 기록하며,

상기 신규 블록의 헤더에 기록된 내용들에 해시 알고리즘을 적용하여 도출된 해시 값을 상기 신규 블록의 바디(Body)에 기록하고,

상기 신규 블록을 다른 제2 RDD들과 동기화하여 관리하기 위해 타임 노드에 커밋 타임(Commit time)을 요청한 후 상기 신규 블록의 바디에 기록하며,

상기 신규 블록을 다른 제2 RDD들로 전송한 후 대기 원장에 기록하였다가 상기 커밋 타임에 다른 RDD들과 동시에 상기 신규 블록을 커밋 원장에 기록하는 경량화 블록체인 제공 장치.

청구항 9

제8항에 있어서,

상기 다른 제2 RDD들은,

상기 제1 RDD로부터 수신된 신규 블록을 대기 원장에 기록하였다가 상기 신규 블록의 바디에 기록된 커밋 타임에 상기 신규 블록을 커밋 원장에 기록하는 경량화 블록체인 제공 장치.

청구항 10

제8항에 있어서,

상기 프로세서는,

상기 인증을 요청한 SDD의 인증을 수행하기 위하여 하위 노드에 대응하는 제2 RDD들에 원장 검증을 요청하는 경

량화 블록체인 제공 장치.

청구항 11

제10항에 있어서,

상기 원장 검증은,

상기 제1 RDD 및 제2 RDD들이 바이너리 트리 구조의 형태로 검증이 수행되는 경량화 블록체인 제공 장치.

청구항 12

제11항에 있어서,

상기 프로세서는,

원장 검증을 요청한 제1 RDD의 바이너리 트리 구조 최하위 노드에 루트(Root) RDD로의 오버레이 패스(Overlay path)를 임시로 연결하는 경량화 블록체인 제공 장치.

청구항 13

경량화 블록체인 제공 방법을 제공하는 스마트 더스트(Smart Dust) 시스템의 제1 중계 더스트 장치(Relay Dust Device, RDD)에 대응하는 경량화 블록체인 제공 장치에 있어서,

프로세서를 포함하고,

상기 프로세서는,

스마트 더스트 장치(Smart Dust Device, SDD)로부터 인증 요청이 수신된 경우, 원장 검증을 위한 바이너리 트리 구조를 식별하고,

상기 식별된 바이너리 트리 구조를 이용하여 원장 검증에 참여 가능한 다른 제2 RDD들이 과반 이상인지의 여부를 판단하며,

상기 원장 검증에 참여 가능한 다른 제2 RDD들이 과반 미만으로 판단된 경우, 상기 바이너리 트리 구조를 변경하고,

상기 변경된 바이너리 트리 구조에 기초하여 원장 검증을 수행하는 경량화 블록체인 제공 장치.

청구항 14

제13항에 있어서,

상기 프로세서는,

상기 제2 RDD들에 원장 검증을 요청하는 제1 RDD의 바이너리 트리 구조 최하위 노드에 루트(Root) RDD로의 오버레이 패스(Overlay path)를 임시로 연결함으로써 상기 바이너리 트리 구조를 변경하는 경량화 블록체인 제공 장치.

발명의 설명

기술 분야

[0001] 본 발명은 스마트 더스트 IoT 환경을 위한 경량화 블록체인 제공 방법 및 장치에 관한 것으로, 보다 구체적으로는 기존 블록 체인의 선형 블록 구조를 바이너리 트리 구조로 재구성함으로써 스마트 더스트 IoT 환경에서 블록 체인의 운영을 효율적으로 간소화하는 방법 및 장치에 관한 것이다.

배경 기술

[0002] 스마트 더스트(Smart Dust)는 먼지처럼 매우 작은 센서들을 건물, 도로, 의복, 인체 등 물리적 공간에 먼지처럼 뿌려 주위의 온도, 습도, 가속도, 압력 등의 정보를 무선 네트워크로 감지, 관리할 수 있는 기술을 의미한다. 이와 같은 스마트 더스트는 최근 포춘지에 의해 2년 안에 전세계를 휩쓸 10대 신기술 중 하나로 선정된 바 있을

만큼 주목받는 기술 중 하나이다.

- [0003] 사물인터넷(Internet of Things, IoT)는 현실의 세계와 온라인 세계의 긴밀한 연결을 포함하는 개념으로 주변의 사물 및 사람이 네트워크로 연결되는 차세대 통신을 의미한다. IoT는 이미 주목받는 기술을 넘어 우리 주변의 많은 분야 (e.g. 교통, 스마트 시티, 스마트 홈, 전자 거버넌스, 전자 교육, 개인 건강, 소매, 물류, 농업, 제조 산업 및 비즈니스 등)에서 실제로 사용되고 있으며, 심지어 최근 출시되는 전자 제품 등의 상당 수는 IoT 기능을 기본적으로 탑재하고 있다.
- [0004] 스마트 더스트는 아주 작은 크기의 디바이스들이 서로 유기적으로 통신하는 네트워크로써, 아주 작은 크기의 디바이스를 다루는 IoT라고 생각될 수 있다. 즉, 스마트 더스트 IoT 시스템은 매우 작은 크기로 인해 매우 낮은 컴퓨팅 파워를 지니는 스마트 더스트를 관리 대상 기기로 다루는 특수한 IoT 환경을 의미할 수 있다.
- [0005] 스마트 더스트 IoT 시스템을 구성하는 환경은 상상하기 힘든 숫자의 디바이스들이 있을 수 있다. 이 숫자는 적게는 수천에서 많게는 수 억에 달할 수 있다. 따라서, 이와 같은 대규모의 디바이스들을 인증하거나 그들로부터 수집되는 데이터의 무결성을 유지하는 일은 결코 쉽지 않은 일이다.
- [0006] 이 작은 기기들(Smart Dust Devices)은 일반적으로 널리 알려진 공격 방법들에 노출될 수 있지만, 이에 대한 해결책들은 많은 연구자들에 의해 연구되었다. 하지만, 그들이 가지는 특수한 취약점들은 거의 연구가 된 적이 없다.
- [0007] 아주 방대한 수의 기기들이 데이터를 수집하는 스마트 더스트 IoT 시스템에는 인증되지 않은 노드들이 데이터 수집에 참여하여 데이터 수집을 오염시킬 수 있을 뿐만 아니라 많은 수에서 기인하는 데이터 지연 문제는 같은 데이터를 여러 번 수집, 기록하여 데이터 통계에 대한 정확성을 떨어뜨릴 수 있다.
- [0008] 일반적으로 블록체인은 데이터 위조, 변조 같은 데이터 신뢰성 문제에 대한 좋은 솔루션 중 하나로 여겨진다. 이와 같은 블록체인은 원장의 검증을 위해 선형적인 체이닝을 구성하며, 불행히도 원장의 검증 속도는 체인에 참여한 노드 수에 비례할 수 있다.
- [0009] 따라서, 수 억에 달하는 디바이스들을 가정하는 스마트 더스트 IoT 시스템에 일반적인 블록체인을 적용하는 것은 불가능하므로 스마트 더스트 IoT 시스템에 사용 가능한 새로운 블록체인 기술이 요구되고 있다.

발명의 내용

해결하려는 과제

- [0010] 본 발명은 기존 블록 체인의 선형 블록 구조를 바이너리 트리 구조로 재구성함으로써 스마트 더스트 IoT 환경에서 블록체인의 운영을 효율적으로 간소화하는 방법 및 장치를 제공한다.

과제의 해결 수단

- [0011] 본 발명의 일 실시예에 따른 스마트 더스트(Smart Dust) 시스템의 제1 중계 더스트 장치(Relay Dust Device, RDD)가 수행하는 경량화 블록체인 제공 방법은 스마트 더스트 장치(Smart Dust Device, SDD)로부터 인증 요청이 수신된 경우, 신규 블록을 생성한 후 생성된 신규 블록의 헤더(Header)에 상기 SDD의 기기 정보 및 이전 블록의 해시 값을 기록하는 단계; 상기 SDD의 인증에 필요한 인증 로우 데이터를 인증 노드로부터 수신하여 상기 SDD의 인증을 수행한 후 인증 결과를 상기 신규 블록의 헤더에 기록하는 단계; 상기 신규 블록의 헤더에 기록된 내용들에 해시 알고리즘을 적용하여 도출된 해시 값을 상기 신규 블록의 바디(Body)에 기록하는 단계; 상기 신규 블록을 다른 제2 RDD들과 동기화하여 관리하기 위해 타임 노드에 커밋 타임(Commit time)을 요청한 후 상기 신규 블록의 바디에 기록하는 단계; 및 상기 신규 블록을 다른 제2 RDD들로 전송한 후 대기 원장에 기록하였다가 상기 커밋 타임에 다른 RDD들과 동시에 상기 신규 블록을 커밋 원장에 기록하는 단계를 포함할 수 있다.
- [0012] 상기 다른 제2 RDD들은 상기 제1 RDD로부터 수신된 신규 블록을 대기 원장에 기록하였다가 상기 신규 블록의 바디에 기록된 커밋 타임에 상기 신규 블록을 커밋 원장에 기록할 수 있다.
- [0013] 상기 인증을 요청한 SDD의 인증을 수행하기 위하여 하위 노드에 대응하는 제2 RDD들에 원장 검증을 요청하는 단계를 더 포함할 수 있다.
- [0014] 상기 원장 검증은 상기 제1 RDD 및 제2 RDD들이 바이너리 트리 구조의 형태로 검증이 수행될 수 있다.
- [0015] 상기 원장 검증은 원장 검증을 요청한 제1 RDD의 바이너리 트리 구조 최하위 노드에 루트(Root) RDD로의 오버레

이 패스(Overlay path)를 임시로 연결할 수 있다.

- [0016] 본 발명의 일실시예에 따른 경량화 블록체인 제공 방법은 스마트 더스트 장치(Smart Dust Device, SDD)로부터 인증 요청을 수신한 제1 중계 더스트 장치(Relay Dust Device, RDD)가 원장 검증을 위한 바이너리 트리 구조를 식별하는 단계; 상기 식별된 바이너리 트리 구조를 이용하여 원장 검증에 참여 가능한 다른 제2 RDD들이 과반 이상인지의 여부를 판단하는 단계; 상기 원장 검증에 참여 가능한 다른 제2 RDD들이 과반 미만으로 판단된 경우, 상기 바이너리 트리 구조를 변경하는 단계; 및 상기 변경된 바이너리 트리 구조에 기초하여 원장 검증을 수행하는 단계를 포함할 수 있다.
- [0017] 상기 바이너리 트리 구조를 변경하는 단계는 상기 제2 RDD들에 원장 검증을 요청하는 제1 RDD의 바이너리 트리 구조 최하위 노드에 루트(Root) RDD로의 오버레이 패스(Overlay path)를 임시로 연결할 수 있다.
- [0018] 본 발명의 일실시예에 따른 경량화 블록체인 제공 방법을 제공하는 스마트 더스트(Smart Dust) 시스템의 제1 중계 더스트 장치(Relay Dust Device, RDD)에 대응하는 경량화 블록체인 제공 장치는 프로세서를 포함하고, 상기 프로세서는 스마트 더스트 장치(Smart Dust Device, SDD)로부터 인증 요청이 수신된 경우, 신규 블록을 생성한 후 생성된 신규 블록의 헤더(Header)에 상기 SDD의 기기 정보 및 이전 블록의 해시 값을 기록하고, 상기 SDD의 인증에 필요한 인증 로우 데이터를 인증 노드로부터 수신하여 상기 SDD의 인증을 수행한 후 인증 결과를 상기 신규 블록의 헤더에 기록하며, 상기 신규 블록의 헤더에 기록된 내용들에 해시 알고리즘을 적용하여 도출된 해시 값을 상기 신규 블록의 바디(Body)에 기록하고, 상기 신규 블록을 다른 제2 RDD들과 동기화하여 관리하기 위해 타임 노드에 커밋 타임(Commit time)을 요청한 후 상기 신규 블록의 바디에 기록하며, 상기 신규 블록을 다른 제2 RDD들로 전송한 후 대기 원장에 기록하였다가 상기 커밋 타임에 다른 RDD들과 동시에 상기 신규 블록을 커밋 원장에 기록할 수 있다.
- [0019] 상기 다른 제2 RDD들은 상기 제1 RDD로부터 수신된 신규 블록을 대기 원장에 기록하였다가 상기 신규 블록의 바디에 기록된 커밋 타임에 상기 신규 블록을 커밋 원장에 기록할 수 있다.
- [0020] 상기 프로세서는 상기 인증을 요청한 SDD의 인증을 수행하기 위하여 하위 노드에 대응하는 제2 RDD들에 원장 검증을 요청할 수 있다.
- [0021] 상기 원장 검증은 상기 제1 RDD 및 제2 RDD들이 바이너리 트리 구조의 형태로 검증이 수행될 수 있다.
- [0022] 상기 프로세서는 원장 검증을 요청한 제1 RDD의 바이너리 트리 구조 최하위 노드에 루트(Root) RDD로의 오버레이 패스(Overlay path)를 임시로 연결할 수 있다.
- [0023] 본 발명의 일실시예에 따른 경량화 블록체인 제공 방법을 제공하는 스마트 더스트(Smart Dust) 시스템의 제1 중계 더스트 장치(Relay Dust Device, RDD)에 대응하는 경량화 블록체인 제공 장치는 프로세서를 포함하고, 상기 프로세서는 스마트 더스트 장치(Smart Dust Device, SDD)로부터 인증 요청이 수신된 경우, 원장 검증을 위한 바이너리 트리 구조를 식별하고, 상기 식별된 바이너리 트리 구조를 이용하여 원장 검증에 참여 가능한 다른 제2 RDD들이 과반 이상인지의 여부를 판단하며, 상기 원장 검증에 참여 가능한 다른 제2 RDD들이 과반 미만으로 판단된 경우, 상기 바이너리 트리 구조를 변경하고, 상기 변경된 바이너리 트리 구조에 기초하여 원장 검증을 수행할 수 있다.
- [0024] 상기 프로세서는 상기 제2 RDD들에 원장 검증을 요청하는 제1 RDD의 바이너리 트리 구조 최하위 노드에 루트(Root) RDD로의 오버레이 패스(Overlay path)를 임시로 연결함으로써 상기 바이너리 트리 구조를 변경할 수 있다.

발명의 효과

- [0025] 본 발명은 기존 블록 체인의 선형 블록 구조를 바이너리 트리 구조로 재구성함으로써 스마트 더스트 IoT 환경에서 블록체인의 운영을 효율적으로 간소화할 수 있다.
- [0026] 또한, 본 발명은 블록체인의 인증 과정과 동기화 과정에서 발생할 수 있는 부하를 성능이 충분한 다른 노드로 이전함으로써 스마트 더스트 IoT 환경에서 블록체인을 구현할 수 있다.

도면의 간단한 설명

- [0027] 도 1은 본 발명의 일실시예에 따른 스마트 더스트 IoT 시스템의 물리적 장치의 구성을 나타낸 도면이다.

도 2는 본 발명의 일실시예에 따른 블록체인을 적용한 스마트 더스트 IoT 시스템의 구성도를 나타낸 도면이다.

도 3은 본 발명의 일실시예에 따른 스마트 더스트 IoT 시스템을 위한 경량 블록체인에 사용되는 블록을 시각화한 도면이다.

도 4는 본 발명의 일실시예에 따른 스마트 더스트 IoT 시스템의 SDD 인증 절차의 흐름을 나타낸 도면이다.

도 5a 및 도 5b는 본 발명의 일실시예에 따른 바이너리 트리 구조의 원장 검증 방법을 나타낸 도면이다.

도 6은 본 발명의 일실시예에 따른 스마트 더스트 IoT 시스템을 구성하는 장치들의 소프트웨어 모듈 구성을 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

[0028]

이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0029]

도 1은 본 발명의 일실시예에 따른 스마트 더스트 IoT 시스템의 물리적 장치의 구성을 나타낸 도면이다.

[0030]

스마트 더스트는 MEMS(Micro Electro Mechanical Systems), 광수신기, 신호처리 및 제어 회로, 후막 배터리, 태양 전지 등의 기술을 통합한 기술이다. 이러한 스마트 더스트의 가장 큰 특징은 디바이스의 크기가 먼지처럼 작다는 것이다. 먼지처럼 작은 디바이스는 대부분 사람의 접근이 힘든 지역(e.g. 아마존 우림, 달표면, 극지방 등)에 항공장치(e.g. 드론, 항공기 등)를 이용해 초대량으로 살포되는 특징이 있다. 초대량으로 배포되는 특징은 스마트 더스트 장치(Smart Dust Devices, SDD)가 아주 저렴한 가격으로 생산되어야 하는 이유이며, 저렴한 가격은 낮은 컴퓨팅 파워 및 리소스를 동반할 수 있다. 또한, 사람의 접근이 힘든 지역에 배포되는 특성은 스마트 더스트 장치의 사후 관리가 어려운 문제를 동반할 수 있다. 요약하자면, 스마트 더스트 장치는 초대량의 기기수, 낮은 컴퓨팅 파워 및 힘든 사후 관리와 같은 특징을 가질 수 있다.

[0031]

넓은 의미에서 스마트 더스트는 IoT의 범주에 속할 수 있다. 단지, 아주 낮은 컴퓨팅 파워 및 리소스를 지니는 초대량의 디바이스가 대상이라는 점이 기존의 IoT와는 차이가 있다.

[0032]

도 1을 참고하면, 스마트 더스트 IoT 시스템(100)은 다층 형태로 구성될 수 있다. 도 1의 SDD는 데이터를 수집하는 센싱 디바이스인 스마트 더스트 장치를 의미하며, 앞서 설명한 스마트 더스트 장치의 모든 특징을 가질 수 있다. RDD는 SDD를 통해 수집된 데이터를 릴레이 하고, 블록체인을 구성하는 중계 더스트 장치를 의미하며, 병목현상을 제거하기 위해 데이터를 통합하거나 변환, 압축하는 역할 혹은 버퍼의 역할을 수행함으로써 방대한 수의 SDDs/RDDs로부터 발생하는 부하를 분산하는 역할을 수행할 수 있다. Auth Node는 인증을 수행하는 인증 노드를 의미하고, Time Node는 RDD들의 동기화를 위한 커밋 타임(commit time)을 지정하는 타임 노드를 의미할 수 있다. 그리고, 스마트 더스트 IoT 서버의 Processing Node는 수집된 데이터를 처리하는 노드로써 일반적인 IoT의 시각에서 어플리케이션 엔티티(Application Entities)에 매핑될 수 있으며, PC Node는 Processing Node를 관리하는 노드로서 동적 분할 알고리즘에 따라 처리 부하를 여러 Processing Node에 효율적으로 분해하는 노드이다.

[0034]

도 2는 본 발명의 일실시예에 따른 블록체인을 적용한 스마트 더스트 IoT 시스템의 구성도를 나타낸 도면이다.

[0035]

블록체인으로 대변되는 체인 알고리즘의 잘 알려진 문제 중 하나는 느린 처리 속도이다. 하나의 트랜잭션이 발생하면 즉시 처리하지 못하고 블록을 구성할 때까지 기다려야 하고 블록이 구성된 이후에도 네트워크에 분산된 여러 노드들의 원장을 검증하고 확인하는데 많은 시간이 소요된다. 블록체인의 구현체 중 가장 잘 알려진 비트코인은 새로운 블록을 구성할 때, 약 10분의 시간이 걸리고, 블록을 검증받기 위해서는 1시간 이상의 시간이 소요되는 경우가 있다.

[0036]

스마트 더스트 IoT 시스템(100)의 주요 특징은 방대한 수의 디바이스와 낮은 컴퓨팅 파워를 포함할 수 있다. 이 두 가지 주요 특징은 스마트 더스트 IoT 환경에서 일반적인 블록체인이 사용되기 어렵도록 만드는 이유로 작용한다. 매우 제한된 컴퓨팅 파워 및 리소스를 지니는 SDD는 태생적으로 블록체인의 원장을 소유하거나 원장 비교 등의 연산을 수행할 능력을 지니지 않는다. SDD에 비해 보다 나은 컴퓨팅 파워 및 리소스를 지니는 RDD 또한 여유가 있지는 않다. 따라서, 본 발명의 스마트 더스트 IoT 시스템(100)은 RDD에서 동작하지만, 아주 경량화된 형태로 개량된 블록체인을 제공할 수 있다.

[0037]

또한, 스마트 더스트 IoT 시스템(100)의 방대한 수의 디바이스에 블록체인이 적용될 경우 원장 검증이 실제로

이루어진다고 보기 힘들 정도로 느려 질 수 있다. 이러한 블록체인의 느린 처리 속도 문제와 스마트 더스트 IoT 환경의 특징은 서로에게 악영향을 미쳐 스마트 더스트 IoT 환경에 블록체인이 적용되는 것을 더욱 힘들게 할 수 있다.

- [0038] 따라서, 본 발명에서 제공하는 스마트 더스트 IoT 시스템(100)은 블록체인의 느린 처리 속도를 개선하고 스마트 더스트 IoT 환경에서 사용할 수 있을 정도로 경량화한 블록체인을 디자인하기 위해 RDD의 컴퓨팅 파워 및 리소스를 고려한 간단한 인증 절차와 선형적인 보통의 블록체인보다 빠른 속도로 이루어지는 원장 검증을 고려하였다.
- [0039] 도 2를 참고하면, 본 발명에서 제공하는 스마트 더스트 IoT 시스템(100)은 인증의 대상이 되는 스마트 더스트 장치인 SDD, 인증을 수행하는 중계 더스트 장치인 RDD, 인증 정보를 제공하는 인증 노드인 Authentication Node 및 각 원장의 동기화를 위한 커밋 타임(Commit time)을 제공하는 타임 노드인 Time Node로 구성될 수 있다. 이때, Authentication Node는 데이터를 전달하는 서버, 즉 도 1의 PC Node 및 Processing Node이 포함된 스마트 더스트 IoT 서버와는 독립적인 노드이다.
- [0040] 스마트 더스트 IoT 시스템(100)은 RDD의 제한된 컴퓨팅 파워로도 충분히 동작할 수 있도록 인증절차 중 필수적이지 않은 부분이 배제되었다. 또한, 스마트 더스트 IoT 시스템(100)은 모든 RDD가 모든 SDD에 대한 인증 정보를 가지게 됐을 때 발생할 수 있는 RDD의 성능 부족 현상과 새로운 보안 이슈에서 자유로워지기 위해 각 RDD가 가질 수 있는 인증 정보를 제한하였다. 따라서, 스마트 더스트 IoT 시스템(100)은 RDD가 필드에 배포된 후, 자신에게 인증을 요청하는 SDD에 관한 인증 정보만 Authentication Node에 요청하도록 제한하였다.
- [0042] 도 3은 본 발명의 일실시예에 따른 스마트 더스트 IoT 시스템을 위한 경량 블록체인에 사용되는 블록을 시각화한 도면이다.
- [0043] 도 3을 참고하면, 경량 블록체인에 사용되는 블록(300)은 헤더(Header) 영역과 바디(Body) 영역을 포함할 수 있다. 이 중 헤더 영역은 인증을 요청한 SDD의 인증 결과 정보(Authentication Information), 인증을 요청한 SDD의 기기 정보(Device's Information) 및 이전 블록의 해시 값(Prev. Hash)이 기록될 수 있고, 바디 영역은 헤더를 포함한 필드의 해시 값(Hash(Header)), 타임 노드에서 설정한 블록의 동기화 시간 정보(Sync Time) 및 SDD가 감지한 정보(Transaction)가 기록될 수 있다.
- [0045] 도 4는 본 발명의 일실시예에 따른 스마트 더스트 IoT 시스템의 SDD 인증 절차의 흐름을 나타낸 도면이다.
- [0046] 먼저, 스마트 더스트 IoT 시스템(100)을 구성하는 각 디바이스들이 필드에 배포되면, 가장 처음으로 단계(402)에서 RDD A는 Authentication Node에 사전 인증을 요청할 수 있으며, 단계(404)에서 Authentication Node는 자신에게 사전 인증을 요청한 RDD에 인증 결과를 회신할 수 있다. 이러한 사전 인증 과정은 일반적인 공개키 방식을 진행될 수 있으며, 단계(406)에서 Authentication Node는 자신에게 인증을 요청한 첫 번째 RDD A의 기기 정보 및 인증 결과를 바탕으로 최초의 블록인 Genesis Block을 생성할 수 있다. Genesis Block의 Prev. Hash는 Authentication Node에 최초 인증이 요청된 시간에 대한 해시 값(SHA256)이 기록될 수 있다. 이와 같이 Genesis Block이 생성되면, 단계(408)에서 Authentication Node는 생성된 Genesis Block을 모든 RDD들에 전파할 수 있다. 전파된 Genesis Block이 모든 RDD들에서 동기화되면 스마트 더스트 IoT 시스템(100)은 SDD에 대한 인증을 수행할 준비를 마친 상태가 된다.
- [0047] 인증을 수행할 준비가 된 RDD A는 단계(410)에서 SDD가 인증을 요청하면, 단계(412)과 같이 인증 요청을 수신한 RDD A가 신규 블록을 생성함으로써 인증을 시작할 수 있다. 이때, RDD A는 인증을 요청한 SDD의 기기 정보를 Device's Information에 기록하고, 이전 블록의 해시 값을 Prev. Hash에 기록할 수 있다.
- [0048] 단계(414)에서 RDD A는 SDD의 인증을 위해 필요한 인증 로우 데이터를 Authentication Node에게 요청하고, 단계(416)에서 Authentication Node는 RDD A가 요청한 인증 로우 데이터를 회신할 수 있다.
- [0049] 단계(418)에서, RDD A는 수신된 인증 로우 데이터를 이용하여 SDD를 인증하고, 인증 결과를 신규 블록의 헤더 영역을 구성하는 Authentication Information에 기록할 수 있다. 그리고 헤더 영역에 정보를 모두 기록한 RDD A는 헤더 영역의 내용을 해시 알고리즘을 적용(e.g. SHA256 알고리즘)하여 해시 값을 도출한 뒤, 도출된 해시 값을 Hash(Header)에 기록할 수 있다.

- [0050] 현재 개별 로컬 RDD들에 기록된 정보들은 다른 RDD들과 동기화되어 관리될 필요가 있다. 따라서, 단계(420)에서 RDD A는 동기화 시간을 지정할 Time Node에게 commit time을 요청할 수 있으며, Time Node는 단계(422)에서 자신의 스케줄에 commit time T를 할당한 후, 단계(424)와 같이 할당된 commit time T를 RDD A에 회신할 수 있다.
- [0051] commit time T를 회신 받은 RDD A가 단계(426)과 같이 이를 신규 블록의 바디 영역을 구성하는 Sync time에 기록하여 단계(428)과 같이 다른 RDD들(RDD B, RDD C)로 신규 블록을 전파하면, 이를 수신한 다른 RDD들은 자신의 커밋 원장에 신규 블록을 기록하는 것이 아니라, 대기 원장에 신규 블록을 기록할 수 있다. 이때 대기 원장은 인증은 수행됐지만 인증 여부에 대한 동기화가 이루어지기 전의 신규 블록들이 기록된 원장을 의미하고, 커밋 원장은 모든 RDD들에 동기화된 블록들이 기록된 원장을 의미할 수 있다. 그리고, 신규 블록을 전파한 RDD A 역시 자신의 대기 원장에 신규 블록을 기록할 수 있다.
- [0052] 이후 commit time T가 되면 Time Node는 단계(430)에서, 스마트 더스트 IoT 시스템의 모든 RDD들로 commit time T가 되었음을 통지하며, 이를 수신한 RDD들은 단계(430)에서, 대기 원장에 기록된 신규 블록을 자신의 커밋 원장에 기록함으로써 커밋 원장을 업데이트할 수 있다.
- [0053] 상술한 단계를 거치고 나면, 각 RDD들의 인증 정보는 모두 블록으로 커밋 원장에 기록될 수 있다. 이 후 데이터를 수집할 때도 데이터에 대한 기록이 블록단위로 커밋 원장에 기록되며, 기록된 결과는 원장 검증을 통해 검증됨으로 중복 기록, 데이터 위, 변조 공격, 데이터 삽입 공격 등으로부터 수집 데이터를 보호할 수 있다.
- [0055] 도 5a 및 도 5b는 본 발명의 일실시예에 따른 바이너리 트리 구조의 원장 검증 방법을 나타낸 도면이다.
- [0056] 일반적인 블록체인은 특유의 선형적인 구성으로 인해 스마트 더스트 IoT 환경과 같은 초대량의 디바이스가 존재하는 시스템에서 치명적일 수 있다. 예를 들어, 100,000,000개의 디바이스가 존재하는 스마트 더스트 IoT 환경의 커밋 원장을 검증하기 위해 50,000,001번 이상의 통신이 요구될 뿐만 아니라, 모든 작업이 선형적이어서 매우 큰 시간이 소요될 수 있다.
- [0057] 이러한 문제를 해결하기 위하여 본 발명의 스마트 더스트 IoT 시스템(100)은 도 5a와 같이 검증에 참여하는 RDD들을 바이너리 트리 구조로 배치함으로써 기존의 선형 구조에 비해 검증 시간을 감소시킬 수 있다.
- [0058] 커밋 원장에 대한 검증은 RDD에 대한 중복된 인증을 통한 공격을 방지하기 위해서 인증이 수행될 때 마다, 지속적으로 발생할 수 있다. 또한, 데이터를 수집하고 전달할 때도, 중복된 데이터를 방지하고 데이터를 삽입하는 공격을 방지하기 위해, 지속적으로 원장 검증이 수행되어야 한다. 이는 원장 검증이 빈번하게 발생함을 의미하며, 임의의 RDD의 위치에서 요청될 수 있음을 의미할 수 있다. 그러나 도 5a의 RDD D에서 검증 요청이 발생할 경우, 단방향 트리 구조의 특성상 RDD H와 RDD I에만 검증 요청이 가능하여 과반 이상의 검증을 수행할 수 없는 문제가 발생할 수 있다. 또한, 단방향 트리 구조를 취할 때, 발생할 수 있는 문제 중 하나는 경량화 블록체인을 이용한 인증 절차 중 하나인 대기 원장의 전파가 불가능하다는 문제를 야기한다. 따라서, 이 두가지 문제점을 해결하기 위해서는 검증 수행이 요청될 때 마다 트리 구조가 유연하기 변경될 수 있어야 한다.
- [0059] 일례로, RDD D에 RDD가 등록(인증)을 요청하는 상황이 발생하면, 해당 RDD에 대해 인증을 수행하기 위해 하위 노드들을 통해 원장 검증을 수행해야 한다. 하지만, 도 5a의 구조에서는 RDD D가 RDD H, RDD I의 정보만 검증할 수 있기 때문에 이 요청을 수행할 수 없다. 도 5b는 이러한 문제를 해결하기 위하여 본 발명의 스마트 더스트 IoT 시스템(100)이 제공하는 트리 변환의 예를 나타낸 도면이다.
- [0060] 보다 구체적으로 스마트 더스트 IoT 시스템(100)은 각 RDD들이 루트 RDD(Genesis Block의 생성에 참여한 RDD A)에 대한 오버레이 패스(Overlay path)를 가지도록 구조를 변경할 수 있다. 일례로, 스마트 더스트 IoT 시스템(100)은 도 5b와 같이 RDD의 등록(인증)을 요청받은 RDD D가 자신이 루트인 트리의 최하단에 루트 노드인 RDD A를 임시로 연결하도록 트리 변환을 수행할 수 있다. 이때, 음영 표시된 부분은 변경된 트리를 의미한다.
- [0061] 이는 마치 트리가 변하는 듯 보이지만, 전파를 위해 일시적으로 하나의 패스만 연결되었다 사라지므로 아무리 트리에 노드가 많아져도 트리 변경에 들어가는 오버헤드가 일정할 수 있다. 오버헤드가 일정하다는 뜻은 1,000개의 노드가 참여한 트리를 변경하는 비용과 10개의 노드가 참여한 트리를 한번 변경하는 비용이 동일함을 의미한다.
- [0062] 당연히게도 변경의 횟수가 많아지면 (인증되는 횟수가 많아지거나, 원장 검증 요청이 많아지면) 선형적으로 비

용이 증가하지만, 검증이 병렬적으로 수행되며, 최대 깊이는 전체 노드의 수가 N 일 때, $\log N$ (트리의 최대 높이)까지 늘어남으로 장치의 수가 늘어날수록 일반적인 블록체인에 비해 효율성이 증대될 수 있다.

[0063] 즉, 원장 비교 검증은 SDD의 유효성 검사를 원하는 RDD가 다른 RDD들에게 커밋 원장을 비교하도록 요청(Step 1)하고, 요청을 수신한 RDD의 최하단에 루트 노드로의 논리적 연결 경로를 일시적으로 생성(Step 2) 한 후 요청을 수신된 RDD로부터 최하위 노드까지 검증을 수행(Step 3)하고, 하위 노드들이 요청을 수신한 RDD로 검증 결과를 전송(Step 4)하는 네 단계로 수행될 수 있다.

[0065] 도 6은 본 발명의 일실시예에 따른 스마트 더스트 IoT 시스템을 구성하는 장치들의 소프트웨어 모듈 구성을 나타낸 도면이다.

[0066] 본 발명에서 제공하는 스마트 더스트 IoT 시스템(100)은 SDD, RDD, Authentication Node, Time Node 등과 같이 크게 4개의 물리적 장치로 구분될 수 있다. 이와 같은 4가지 물리적 장치의 소프트웨어 중 공통적으로 탑재되는 모듈은 Init Module, Sending Module 및 Receiving Module이다. 먼저, Init Module은 각 장치의 역할에 맞는 초기화를 수행하는 모듈이고, Sending Module은 장치로부터 발생되거나 가공한 데이터를 다른 장치로 송신하는 모듈이며, Receiving Module은 다른 장치로부터 데이터를 수신하는 모듈이다.

[0067] 이에 더불어 SDD는 Session Module 및 Sensing Module을 더 포함할 수 있으며, 이때, Session Module은 자신과 연결되는 장치에 대한 연결을 유지하고 관리하는 모듈이고, Sensing Module은 외부로부터 데이터를 수집하는 모듈이다.

[0068] 그리고, RDD는 BlockMng Module, TransMng Module, Auth Module 및 Broadcast Module을 더 포함할 수 있으며, 이때, BlockMng Module은 블록을 생성, 관리하는 모듈이고, TransMng Module은 인증, 데이터 수집 등의 트랜잭션을 블록에 기록하는 모듈이며, Auth Module은 인증 데이터를 처리하거나 인증을 수행하는 모듈이고, Broadcast Module은 대기 원장을 전파하는 모듈이다.

[0069] Auth Node는 Auth Module을 더 포함할 수 있으며, 이때, Auth Module은 인증 로우 데이터를 관리하는 모듈이다.

[0070] 마지막으로 Time Node는 TaskRegister Module, TimeCheck Module 및 Notification Module을 더 포함할 수 있으며, 이때, TaskRegister Module은 작업을 스케줄에 등록하는 모듈이고, TimeCheck Module은 동기화를 위한 작업 시간을 결정하는 모듈이며, Notification Module은 작업 시간에 도달했을 때, 동기화를 통지하는 모듈이다.

[0072] 한편, 본 발명에 따른 방법은 컴퓨터에서 실행될 수 있는 프로그램으로 작성되어 마그네틱 저장매체, 광학적 판독매체, 디지털 저장매체 등 다양한 기록 매체로도 구현될 수 있다.

[0073] 본 명세서에 설명된 각종 기술들의 구현들은 디지털 전자 회로조직으로, 또는 컴퓨터 하드웨어, 펌웨어, 소프트웨어로, 또는 그들의 조합들로 구현될 수 있다. 구현들은 데이터 처리 장치, 예를 들어 프로그램가능 프로세서, 컴퓨터, 또는 다수의 컴퓨터들의 동작에 의한 처리를 위해, 또는 이 동작을 제어하기 위해, 컴퓨터 프로그램 제품, 즉 정보 캐리어, 예를 들어 기계 판독가능 저장 장치(컴퓨터 판독가능 매체) 또는 전파 신호에서 유형적으로 구체화된 컴퓨터 프로그램으로서 구현될 수 있다. 상술한 컴퓨터 프로그램(들)과 같은 컴퓨터 프로그램은 컴파일된 또는 인터프리트된 언어들을 포함하는 임의의 형태의 프로그래밍 언어로 기록될 수 있고, 독립형 프로그램으로서 또는 모듈, 구성요소, 서브루틴, 또는 컴퓨팅 환경에서의 사용에 적절한 다른 유닛으로서 포함하는 임의의 형태로 전개될 수 있다. 컴퓨터 프로그램은 하나의 사이트에서 하나의 컴퓨터 또는 다수의 컴퓨터들 상에서 처리되도록 또는 다수의 사이트들에 걸쳐 분배되고 통신 네트워크에 의해 상호 연결되도록 전개될 수 있다.

[0074] 컴퓨터 프로그램의 처리에 적절한 프로세서들은 예로서, 범용 및 특수 목적 마이크로프로세서들 둘 다, 및 임의의 종류의 디지털 컴퓨터의 임의의 하나 이상의 프로세서들을 포함한다. 일반적으로, 프로세서는 판독 전용 메모리 또는 랜덤 액세스 메모리 또는 둘 다로부터 명령어들 및 데이터를 수신할 것이다. 컴퓨터의 요소들은 명령어들을 실행하는 적어도 하나의 프로세서 및 명령어들 및 데이터를 저장하는 하나 이상의 메모리 장치들을 포함할 수 있다. 일반적으로, 컴퓨터는 데이터를 저장하는 하나 이상의 대량 저장 장치들, 예를 들어 자기, 자기-광 디스크들, 또는 광 디스크들을 포함할 수 있거나, 이것들로부터 데이터를 수신하거나 이것들에 데이터를 송신하거나 또는 양쪽으로 되도록 결합될 수도 있다. 컴퓨터 프로그램 명령어들 및 데이터를 구체화하는데 적절한 정

보 캐리어들은 예로서 반도체 메모리 장치들, 예를 들어, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM(Compact Disk Read Only Memory), DVD(Digital Video Disk)와 같은 광 기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-Optical Media), 롬(ROM, Read Only Memory), 램(RAM, Random Access Memory), 플래시 메모리, EPROM(Erasable Programmable ROM), EEPROM(Electrically Erasable Programmable ROM) 등을 포함한다. 프로세서 및 메모리는 특수 목적 논리 회로조직에 의해 보충되거나, 이에 포함될 수 있다.

[0075] 또한, 컴퓨터 판독가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용매체일 수 있고, 컴퓨터 저장매체 및 전송매체를 모두 포함할 수 있다.

[0076] 본 명세서는 다수의 특정한 구현물의 세부사항들을 포함하지만, 이들은 어떠한 발명이나 청구 가능한 것의 범위에 대해서도 제한적인 것으로서 이해되어서는 안되며, 오히려 특정한 발명의 특정한 실시형태에 특유할 수 있는 특징들에 대한 설명으로서 이해되어야 한다. 개별적인 실시형태의 문맥에서 본 명세서에 기술된 특정한 특징들은 단일 실시형태에서 조합하여 구현될 수도 있다. 반대로, 단일 실시형태의 문맥에서 기술한 다양한 특징들 역시 개별적으로 혹은 어떠한 적절한 하위 조합으로도 복수의 실시형태에서 구현 가능하다. 나아가, 특징들이 특정한 조합으로 동작하고 초기에 그와 같이 청구된 바와 같이 묘사될 수 있지만, 청구된 조합으로부터의 하나 이상의 특징들은 일부 경우에 그 조합으로부터 배제될 수 있으며, 그 청구된 조합은 하위 조합이나 하위 조합의 변형물로 변경될 수 있다.

[0077] 마찬가지로, 특정한 순서로 도면에서 동작들을 묘사하고 있지만, 이는 바람직한 결과를 얻기 위하여 도시된 그 특정한 순서나 순차적인 순서대로 그러한 동작들을 수행하여야 한다거나 모든 도시된 동작들이 수행되어야 하는 것으로 이해되어서는 안 된다. 특정한 경우, 멀티태스킹과 병렬 프로세싱이 유리할 수 있다. 또한, 상술한 실시형태의 다양한 장치 컴포넌트의 분리는 그러한 분리를 모든 실시형태에서 요구하는 것으로 이해되어서는 안되며, 설명한 프로그램 컴포넌트와 장치들은 일반적으로 단일의 소프트웨어 제품으로 함께 통합되거나 다중 소프트웨어 제품에 패키징 될 수 있다는 점을 이해하여야 한다.

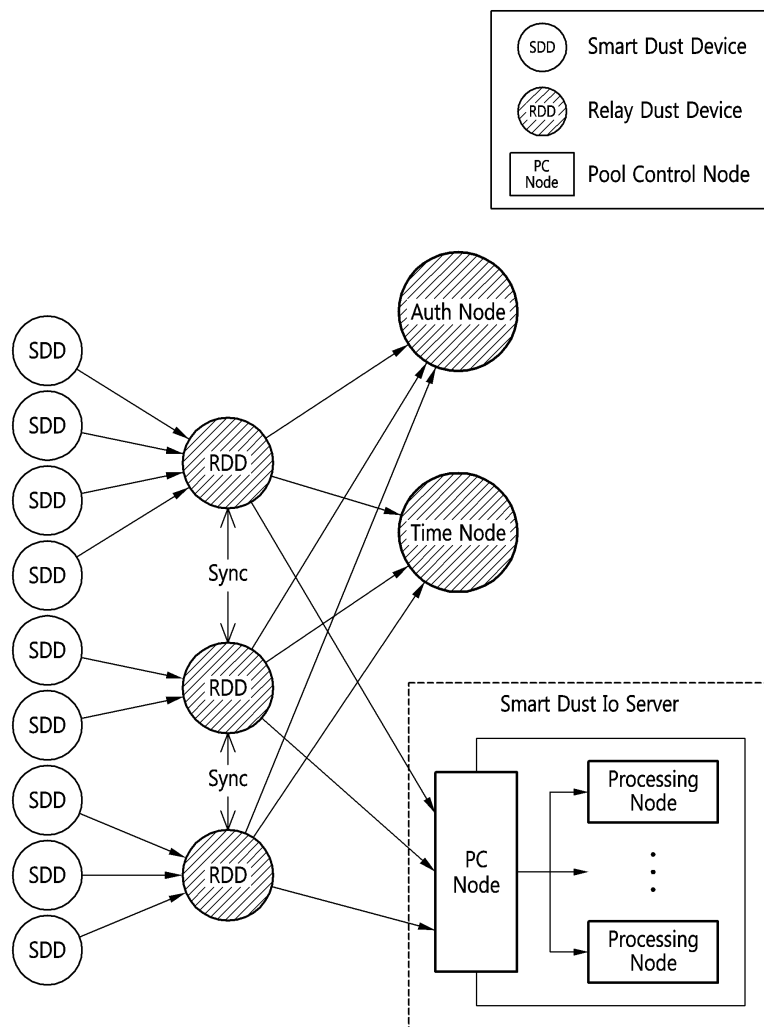
[0078] 한편, 본 명세서와 도면에 개시된 본 발명의 실시 예들은 이해를 돕기 위해 특정 예를 제시한 것에 지나지 않으며, 본 발명의 범위를 한정하고자 하는 것은 아니다. 여기에 개시된 실시 예들 이외에도 본 발명의 기술적 사상에 바탕을 둔 다른 변형 예들이 실시 가능하다는 것은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 자명한 것이다.

부호의 설명

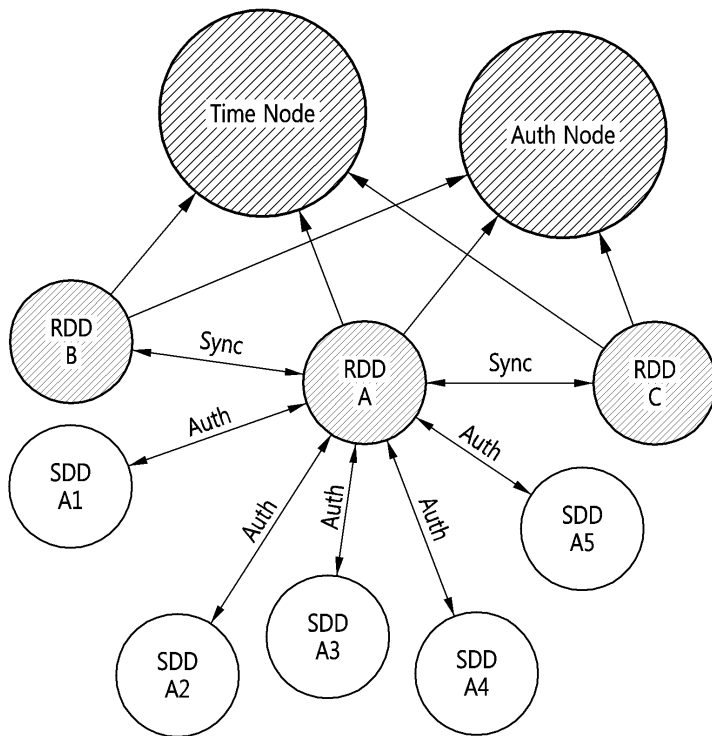
[0079] 100 : 스마트 더스트 IoT 시스템

도면

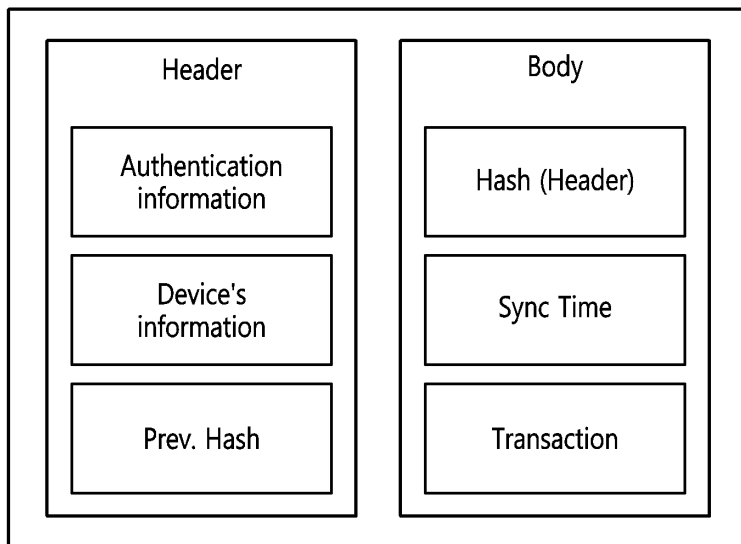
도면1



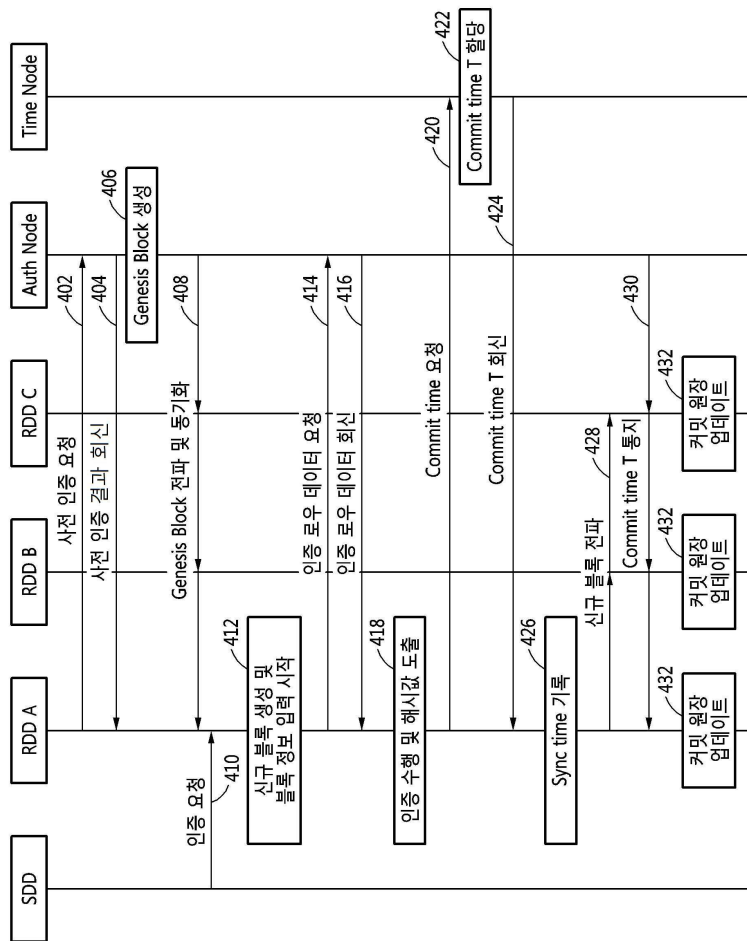
도면2



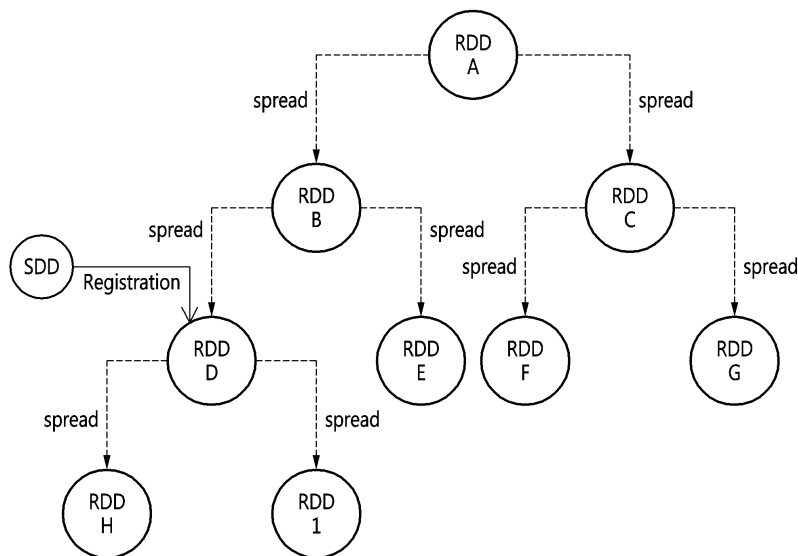
도면3



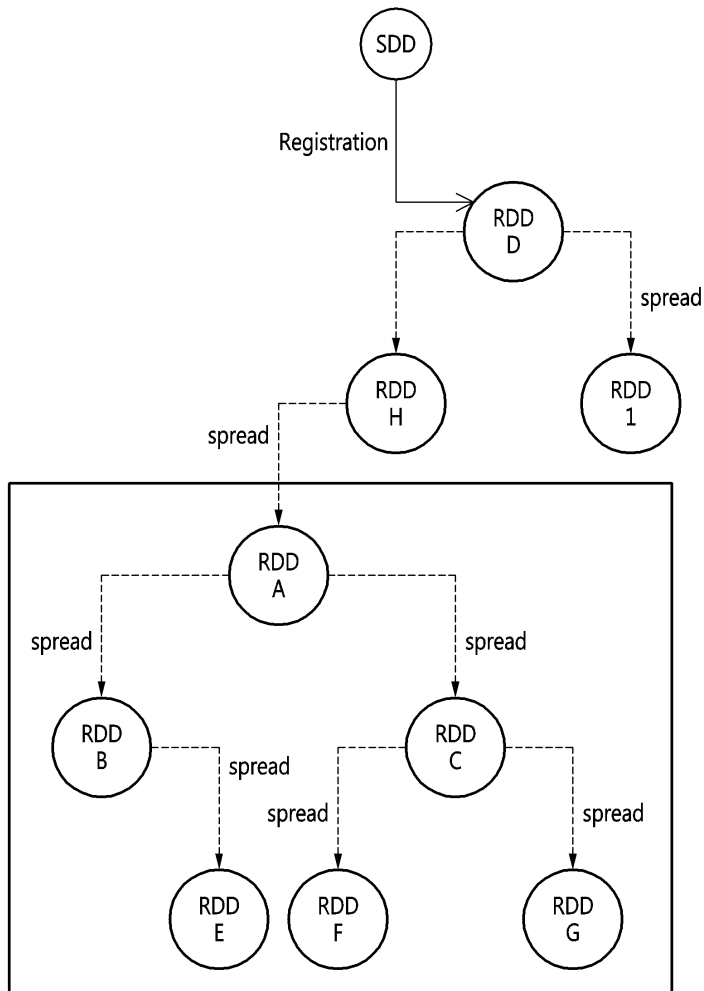
도면4



도면5a



도면5b



도면6

