(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년10월28일
(11) 등록번호 10-2319416
(24) 등록일자 2021년10월25일

(51) 국제특허분류(Int. Cl.)
G06F 21/64 (2013.01) *G06F 16/182* (2019.01)
G06F 16/27 (2019.01) *G06F 21/62* (2013.01)
(52) CPC특허분류
G06F 21/64 (2013.01)
G06F 16/1834 (2019.01)
(21) 출원번호 10-2020-0105452
(22) 출원일자 2020년08월21일
심사청구일자 2020년08월21일
(56) 선행기술조사문헌
JP2019145925 A*
JP2020522919 A*
KR101787900 B1*
KR1020170141976 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
신지선
서울특별시 송파구 올림픽로 435, 311동 2001호(신천동, 파크리오)
최서윤
서울특별시 관악구 은천로33길 5, 102동 1301호(봉천동, 관악동부센트레빌아파트)
(74) 대리인
두호특허법인

전체 청구항 수 : 총 17 항 심사관 : 구대성

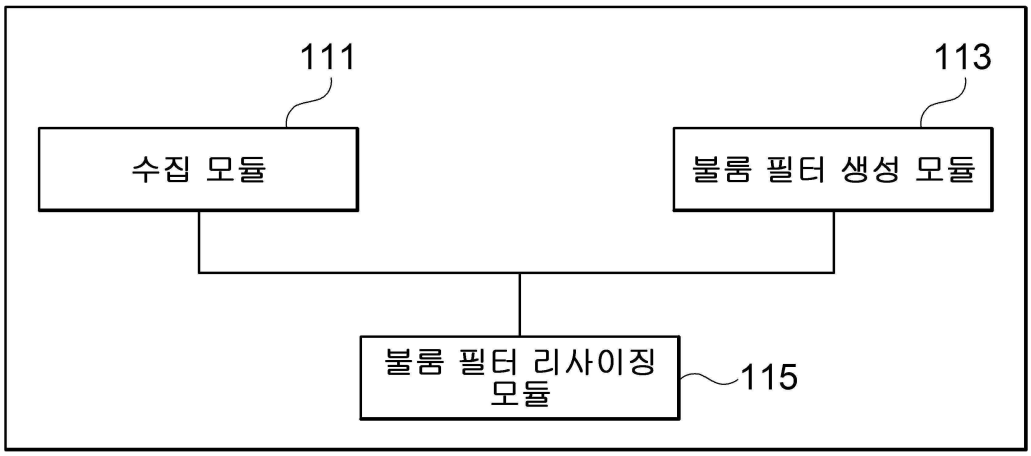
(54) 발명의 명칭 **블록체인 기반의 블룸 필터 생성 방법과 이를 수행하기 위한 컴퓨팅 장치 및 시스템**

(57) 요 약

블록체인 기반의 블룸 필터 생성 방법과 이를 수행하기 위한 컴퓨팅 장치 및 시스템이 개시된다. 개시되는 일 실시예에 따른 컴퓨팅 장치는, 하나 이상의 프로세서들, 및 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하며, 블록체인 망을 구성하는 노드(Node)로 동작되는 컴퓨팅 장치로서, 복수 개의 사용자 단말들로부터 사용자 관련 정보를 포함하는 트랜잭션을 수집하는 수집 모듈 및 수집된 트랜잭션에 기반하여 블록체인을 구성하는 각 블록을 생성하고, 해당 블록을 구성하는 트랜잭션들에 포함된 사용자 관련 정보를 기반으로 블룸 필터(Bloom Filter)를 생성하는 블룸 필터 생성 모듈을 포함한다.

대 표 도 - 도3

104



(52) CPC특허분류
G06F 16/27 (2019.01)
G06F 21/6245 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711117818
과제번호 2020R1F1A1072275
부처명 과학기술정보통신부
과제관리(전문)기관명 한국연구재단
연구사업명 개인기초연구(과기정통부)(R&D)
연구과제명 무인항공기를 위한 블록체인 기반 보안 강화 기술 개발
기 여 율 1/2
과제수행기관명 세종대학교
연구기간 2020.06.01 ~ 2021.02.28
이 발명을 지원한 국가연구개발사업
과제고유번호 1345321135
과제번호 2020R1A6A1A03038540
부처명 교육부
과제관리(전문)기관명 한국연구재단
연구사업명 이공학학술연구기반구축(R&D)
연구과제명 자율지능무인비행체연구소
기 여 율 1/2
과제수행기관명 세종대학교
연구기간 2020.06.01 ~ 2021.02.28

명 세 서

청구범위

청구항 1

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하며, 블록체인 망을 구성하는 노드(Node)로 동작되는 컴퓨팅 장치로서,

복수 개의 사용자 단말들로부터 사용자 관련 정보를 포함하는 트랜잭션을 수집하는 수집 모듈; 및

상기 수집된 트랜잭션에 기반하여 블록체인을 구성하는 각 블록을 생성하고, 해당 블록을 구성하는 트랜잭션들에 포함된 사용자 관련 정보를 기반으로 블룸 필터(Bloom Filter)를 생성하는 블룸 필터 생성 모듈을 포함하며,

상기 블록은, N(N은 2이상의 자연수)개의 트랜잭션을 포함하고,

상기 블룸 필터 생성 모듈은, 첫 번째 트랜잭션부터 N-1번째 트랜잭션에 포함된 사용자 관련 정보를 기반으로 블룸 필터를 생성하고, 생성한 블룸 필터를 상기 블록의 N번째 트랜잭션으로 하는, 컴퓨팅 장치.

청구항 2

청구항 1에 있어서,

상기 사용자 관련 정보는,

사용자의 가명(Pseudonym), 사용자의 공개키, 사용자의 아이디, 및 사용자 단말의 식별 번호 중 하나를 포함하는, 컴퓨팅 장치.

청구항 3

삭제

청구항 4

청구항 1에 있어서,

상기 블룸 필터 생성 모듈은,

해당 블록을 블록체인에 연결하는 경우, 상기 블록체인에서 이전 블록의 블룸 필터에 해당 블록의 첫 번째 트랜잭션부터 N-1번째 트랜잭션에 포함된 사용자 관련 정보를 추가하여 해당 블록의 블룸 필터를 생성하는, 컴퓨팅 장치.

청구항 5

청구항 4에 있어서,

상기 컴퓨팅 장치는,

상기 이전 블록의 블룸 필터의 긍정 오류를 산출하고, 산출한 긍정 오류가 기 설정된 임계 값을 초과하는지에 따라 블룸 필터의 크기를 리사이징 하는 블룸 필터 리사이징 모듈을 더 포함하는, 컴퓨팅 장치.

청구항 6

청구항 5에 있어서,

상기 블룸 필터 리사이징 모듈은,

상기 산출한 긍정 오류가 상기 임계 값을 초과하는 경우 블룸 필터의 크기를 상기 이전 블록의 블룸 필터의 크기보다 크게 리사이징하는, 컴퓨팅 장치.

청구항 7

청구항 6에 있어서,

상기 블룸 필터 생성 모듈은,

상기 블룸 필터의 크기를 리사이징 한 경우, 상기 블록체인의 모든 트랜잭션에 포함된 사용자 관련 정보를 기반으로 블룸 필터를 재구성하는, 컴퓨팅 장치.

청구항 8

청구항 1에 있어서,

상기 블룸 필터는, 카운팅 블룸 필터(Counting Bloom Filter)이고,

상기 트랜잭션은, 멤버의 삽입 요청 또는 삭제 요청을 나타내는 필드를 포함하며,

상기 블룸 필터 생성 모듈은,

상기 필드의 삽입 요청 또는 삭제 요청을 확인하여 상기 카운팅 블룸 필터의 해당 셀에서 해당 멤버의 해쉬 값에 대응하는 카운트를 증가하거나 감소시키는, 컴퓨팅 장치.

청구항 9

청구항 1에 있어서,

상기 블룸 필터는, 유효 멤버 블룸 필터 및 취소 멤버 블룸 필터를 포함하고,

상기 트랜잭션은, 멤버의 삽입 요청 또는 삭제 요청을 나타내는 필드를 포함하며,

상기 블룸 필터 생성 모듈은,

상기 필드의 삽입 요청 또는 삭제 요청을 확인하여 해당 트랜잭션의 사용자 관련 정보를 상기 유효 멤버 블룸 필터에 추가하거나 상기 취소 멤버 블룸 필터에 추가하는, 컴퓨팅 장치.

청구항 10

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하며, 블록체인 망을 구성하는 노드(Node)로 동작되는 컴퓨팅 장치에서 수행되는 방법으로서,

복수 개의 사용자 단말로부터 사용자 관련 정보를 포함하는 트랜잭션을 수집하는 단계; 및

상기 수집된 트랜잭션에 기반하여 블록체인을 구성하는 각 블록을 생성하는 단계를 포함하고,

상기 블록을 생성하는 단계는, 상기 블록을 구성하는 트랜잭션들에 포함된 사용자 관련 정보를 기반으로 블룸 필터(Bloom Filter)를 생성하는 단계를 포함하며,

상기 블록은, N(N은 2이상의 자연수)개의 트랜잭션을 포함하고,

상기 블룸 필터를 생성하는 단계는, 첫 번째 트랜잭션부터 N-1번째 트랜잭션에 포함된 사용자 관련 정보를 기반

으로 블룸 필터를 생성하고, 생성한 블룸 필터를 상기 블록의 N번째 트랜잭션으로 하는, 블록체인 기반의 블룸 필터 생성 방법.

청구항 11

청구항 10에 있어서,

상기 사용자 관련 정보는,

사용자의 가명(Pseudonym), 사용자의 공개키, 사용자의 아이디, 및 사용자 단말의 식별 번호 중 하나를 포함하는, 블록체인 기반의 블룸 필터 생성 방법.

청구항 12

삭제

청구항 13

청구항 10에 있어서,

상기 블룸 필터를 생성하는 단계는,

해당 블록을 블록체인에 연결하는 경우, 상기 블록체인에서 이전 블록의 블룸 필터에 해당 블록의 첫 번째 트랜잭션부터 N-1번째 트랜잭션에 포함된 사용자 관련 정보를 추가하여 해당 블록의 블룸 필터를 생성하는, 블록체인 기반의 블룸 필터 생성 방법.

청구항 14

청구항 13에 있어서,

상기 블룸 필터를 생성하는 단계는,

상기 이전 블록의 블룸 필터의 긍정 오류를 산출하는 단계; 및

산출한 긍정 오류가 기 설정된 임계 값을 초과하는지에 따라 블룸 필터의 크기를 리사이징 하는 단계를 더 포함하는, 블록체인 기반의 블룸 필터 생성 방법.

청구항 15

청구항 14에 있어서,

상기 블룸 필터의 크기를 리사이징 하는 단계는,

상기 산출한 긍정 오류가 상기 임계 값을 초과하는 경우 블룸 필터의 크기를 상기 이전 블록의 블룸 필터의 크기보다 크게 하는 단계를 포함하는, 블록체인 기반의 블룸 필터 생성 방법.

청구항 16

청구항 15에 있어서,

상기 블룸 필터 생성 방법은,

상기 블룸 필터의 크기를 리사이징 한 경우, 상기 블록체인의 모든 트랜잭션에 포함된 사용자 관련 정보를 기반으로 블룸 필터를 재구성하는 단계를 더 포함하는, 블록체인 기반의 블룸 필터 생성 방법.

청구항 17

청구항 10에 있어서,

상기 블룸 필터는, 카운팅 블룸 필터(Counting Bloom Filter)이고,

상기 트랜잭션은, 멤버의 삽입 요청 또는 삭제 요청을 나타내는 필드를 포함하며,

상기 블룸 필터를 생성하는 단계는,

상기 필드의 삽입 요청 또는 삭제 요청을 확인하여 상기 카운팅 블룸 필터의 해당 셀에서 해당 멤버의 해쉬 값에 대응하는 카운트를 증가하거나 감소시키는, 블록체인 기반의 블룸 필터 생성 방법.

청구항 18

청구항 10에 있어서,

상기 블룸 필터는, 유효 멤버 블룸 필터 및 취소 멤버 블룸 필터를 포함하고,

상기 트랜잭션은, 멤버의 삽입 요청 또는 삭제 요청을 나타내는 필드를 포함하며,

상기 블룸 필터를 생성하는 단계는,

상기 필드의 삽입 요청 또는 삭제 요청을 확인하여 해당 트랜잭션의 사용자 관련 정보를 상기 유효 멤버 블룸 필터에 추가하거나 상기 취소 멤버 블룸 필터에 추가하는, 블록체인 기반의 블룸 필터 생성 방법.

청구항 19

사용자 관련 정보를 포함하는 트랜잭션을 생성하고, 상기 생성한 트랜잭션을 서명하여 전송하는 복수 개의 사용자 단말; 및

상기 복수 개의 사용자 단말로부터 상기 트랜잭션을 수집하고, 상기 수집된 트랜잭션에 기반하여 블록체인을 구성하는 각 블록을 생성하는 마이너 노드를 포함하고,

상기 마이너 노드는, 상기 블록을 구성하는 트랜잭션들에 포함된 사용자 관련 정보를 기반으로 블룸 필터(Bloom Filter)를 생성하며,

상기 블록은, N(N은 2이상의 자연수)개의 트랜잭션을 포함하고,

상기 마이너 노드는, 첫 번째 트랜잭션부터 N-1번째 트랜잭션에 포함된 사용자 관련 정보를 기반으로 블룸 필터를 생성하고, 생성한 블룸 필터를 상기 블록의 N번째 트랜잭션으로 하는, 블록체인 기반의 블룸 필터 생성 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예는 블록체인 기반의 블룸 필터 생성 기술과 관련된다.

배 경 기 술

[0003] 분산 원장 기술인 블록체인(Blockchain)은 스마트 그리드(Smart Grid)와 같은 중요 인프라를 포함하는 다양한 분야에서 사용되고 있다. 최근, 스마트 그리드에서 개인 정보 보호를 다루는 연구가 진행되고 있는데, 그 중 하나가 스마트 그리드에서 블록체인 기술을 사용하여 무결성 및 익명성을 제공하는 개인 정보 보호 집계 시스템에 대한 연구이다.

[0004] 이전의 연구에서는 블록체인에서 빠른 인증을 위해 블룸 필터(Bloom Filter)가 사용되었으며, 사용자 키 관리에 별도의 키 관리 센터가 사용되었다. 그러나, 키 관리 센터에 대한 의존도가 높기 때문에, 분산된 환경을 제공할 수 없었고 연결성(Linkability) 문제가 있었다. 또한, 블룸 필터를 통한 키 해지 및 업데이트 기능을 제공할 수

없다는 한계가 있다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 한국등록특허공보 제10-1321080호(2013.10.23)

발명의 내용

해결하려는 과제

[0007] 개시되는 실시예는 블록체인 환경에서 분산 및 탈 중앙화된 블룸 필터 생성 기법을 제공하기 위한 것이다.

과제의 해결 수단

[0009] 개시되는 일 실시예에 따른 컴퓨팅 장치는, 하나 이상의 프로세서들, 및 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하며, 블록체인 망을 구성하는 노드(Node)로 동작되는 컴퓨팅 장치로서, 복수 개의 사용자 단말들로부터 사용자 관련 정보를 포함하는 트랜잭션을 수집하는 수집 모듈; 및 상기 수집된 트랜잭션에 기반하여 블록체인을 구성하는 각 블록을 생성하고, 해당 블록을 구성하는 트랜잭션들에 포함된 사용자 관련 정보를 기반으로 블룸 필터(Bloom Filter)를 생성하는 블룸 필터 생성 모듈을 포함한다.

[0010] 상기 사용자 관련 정보는, 사용자의 가명(Pseudonym), 사용자의 공개키, 사용자의 아이디, 및 사용자 단말의 식별 번호 중 하나를 포함할 수 있다.

[0011] 상기 블록은, N(N은 2이상의 자연수)개의 트랜잭션을 포함하고, 상기 블룸 필터 생성 모듈은, 첫 번째 트랜잭션부터 N-1번째 트랜잭션에 포함된 사용자 관련 정보를 기반으로 블룸 필터를 생성하고, 생성한 블룸 필터를 상기 블록의 N번째 트랜잭션으로 할 수 있다.

[0012] 상기 블룸 필터 생성 모듈은, 해당 블록을 블록체인에 연결하는 경우, 상기 블록체인에서 이전 블록의 블룸 필터에 해당 블록의 첫 번째 트랜잭션부터 N-1번째 트랜잭션에 포함된 사용자 관련 정보를 추가하여 해당 블록의 블룸 필터를 생성할 수 있다.

[0013] 상기 컴퓨팅 장치는, 상기 이전 블록의 블룸 필터의 긍정 오류를 산출하고, 산출한 긍정 오류가 기 설정된 임계값을 초과하는지에 따라 블룸 필터의 크기를 리사이징 하는 블룸 필터 리사이징 모듈을 더 포함할 수 있다.

[0014] 상기 블룸 필터 리사이징 모듈은, 상기 산출한 긍정 오류가 상기 임계 값을 초과하는 경우 블룸 필터의 크기를 상기 이전 블록의 블룸 필터의 크기보다 크게 리사이징 할 수 있다.

[0015] 상기 블룸 필터 생성 모듈은, 상기 블룸 필터의 크기를 리사이징 한 경우, 상기 블록체인의 모든 트랜잭션에 포함된 사용자 관련 정보를 기반으로 블룸 필터를 재구성할 수 있다.

[0016] 상기 블룸 필터는, 카운팅 블룸 필터(Counting Bloom Filter)이고, 상기 트랜잭션은, 멤버의 삽입 요청 또는 삭제 요청을 나타내는 필드를 포함하며, 상기 블룸 필터 생성 모듈은, 상기 필드의 삽입 요청 또는 삭제 요청을 확인하여 상기 카운팅 블룸 필터의 해당 셀에서 해당 멤버의 해쉬 값에 대응하는 카운트를 증가하거나 감소시킬 수 있다.

[0017] 상기 블룸 필터는, 유효 멤버 블룸 필터 및 취소 멤버 블룸 필터를 포함하고, 상기 트랜잭션은, 멤버의 삽입 요청 또는 삭제 요청을 나타내는 필드를 포함하며, 상기 블룸 필터 생성 모듈은, 상기 필드의 삽입 요청 또는 삭제 요청을 확인하여 해당 트랜잭션의 사용자 관련 정보를 상기 유효 멤버 블룸 필터에 추가하거나 상기 취소 멤버 블룸 필터에 추가할 수 있다.

[0018] 개시되는 일 실시예에 따른 블록체인 기반의 블룸 필터 생성 방법은, 하나 이상의 프로세서들, 및 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하며, 블록체인 망을 구성하는 노드(Node)로 동작되는 컴퓨팅 장치에서 수행되는 방법으로서, 복수 개의 사용자 단말로부터 사용자 관련 정보를 포함하는 트랜잭션을 수집하는 단계; 및 상기 수집된 트랜잭션에 기반하여 블록체인을 구성하는 각 블록

을 생성하는 단계를 포함하고, 상기 블록을 생성하는 단계는, 상기 블록을 구성하는 트랜잭션들에 포함된 사용자 관련 정보를 기반으로 블룸 필터(Bloom Filter)를 생성하는 단계를 포함한다.

[0019] 상기 사용자 관련 정보는, 사용자의 가명(Pseudonym), 사용자의 공개키, 사용자의 아이디, 및 사용자 단말의 식별 번호 중 하나를 포함할 수 있다.

[0020] 상기 블록은, N(N은 2이상의 자연수)개의 트랜잭션을 포함하고, 상기 블룸 필터를 생성하는 단계는, 첫 번째 트랜잭션부터 N-1번째 트랜잭션에 포함된 사용자 관련 정보를 기반으로 블룸 필터를 생성하고, 생성한 블룸 필터를 상기 블록의 N번째 트랜잭션으로 할 수 있다.

[0021] 상기 블룸 필터를 생성하는 단계는, 해당 블록을 블록체인에 연결하는 경우, 상기 블록체인에서 이전 블록의 블룸 필터에 해당 블록의 첫 번째 트랜잭션부터 N-1번째 트랜잭션에 포함된 사용자 관련 정보를 추가하여 해당 블록의 블룸 필터를 생성할 수 있다.

[0022] 상기 블룸 필터를 생성하는 단계는, 상기 이전 블록의 블룸 필터의 긍정 오류를 산출하는 단계; 및 산출한 긍정 오류가 기 설정된 임계 값을 초과하는지에 따라 블룸 필터의 크기를 리사이징 하는 단계를 더 포함할 수 있다.

[0023] 상기 블룸 필터의 크기를 리사이징 하는 단계는, 상기 산출한 긍정 오류가 상기 임계 값을 초과하는 경우 블룸 필터의 크기를 상기 이전 블록의 블룸 필터의 크기보다 크게 하는 단계를 포함할 수 있다.

[0024] 상기 블룸 필터 생성 방법은, 상기 블룸 필터의 크기를 리사이징 한 경우, 상기 블록체인의 모든 트랜잭션에 포함된 사용자 관련 정보를 기반으로 블룸 필터를 재구성하는 단계를 더 포함할 수 있다.

[0025] 상기 블룸 필터는, 카운팅 블룸 필터(Counting Bloom Filter)이고, 상기 트랜잭션은, 멤버의 삽입 요청 또는 삭제 요청을 나타내는 필드를 포함하며, 상기 블룸 필터를 생성하는 단계는, 상기 필드의 삽입 요청 또는 삭제 요청을 확인하여 상기 카운팅 블룸 필터의 해당 셀에서 해당 멤버의 해쉬 값에 대응하는 카운트를 증가하거나 감소시킬 수 있다.

[0026] 상기 블룸 필터는, 유효 멤버 블룸 필터 및 취소 멤버 블룸 필터를 포함하고, 상기 트랜잭션은, 멤버의 삽입 요청 또는 삭제 요청을 나타내는 필드를 포함하며, 상기 블룸 필터를 생성하는 단계는, 상기 필드의 삽입 요청 또는 삭제 요청을 확인하여 해당 트랜잭션의 사용자 관련 정보를 상기 유효 멤버 블룸 필터에 추가하거나 상기 취소 멤버 블룸 필터에 추가할 수 있다.

[0027] 개시되는 일 실시예에 따른 블록체인 기반의 블룸 필터 생성 시스템은, 사용자 관련 정보를 포함하는 트랜잭션을 생성하고, 상기 생성한 트랜잭션을 서명하여 전송하는 복수 개의 사용자 단말; 및 상기 복수 개의 사용자 단말로부터 상기 트랜잭션을 수집하고, 상기 수집된 트랜잭션에 기반하여 블록체인을 구성하는 각 블록을 생성하는 마이너 노드를 포함하고, 상기 마이너 노드는, 상기 블록을 구성하는 트랜잭션들에 포함된 사용자 관련 정보를 기반으로 블룸 필터(Bloom Filter)를 생성한다.

발명의 효과

[0029] 개시되는 실시예에 의하면, 사용자 단말이 사용자 관련 정보를 포함하는 트랜잭션을 서명하여 블록체인 망에 브로드캐스팅 하고, 블록체인 망의 마이너 노드에서 트랜잭션을 기반으로 각 블록에 대해 블룸 필터를 생성함으로써, 탈 중앙화된(Decentralized) 방식으로 블룸 필터를 생성할 수 있게 된다.

[0030] 또한, 블록체인의 각 블록에서 이전 블록의 블룸 필터를 누적시킴으로써, 블록체인의 마지막 블록의 블룸 필터를 확인하면 해당 블록체인 망에 대해 멤버쉽 체크를 용이하게 수행할 수 있게 된다. 또한, 블룸 필터를 통해 사용자 멤버쉽의 삭제 및 추가 기능을 제공할 수 있게 된다.

도면의 간단한 설명

[0032] 도 1은 본 발명의 일 실시예에 따른 블록체인 기반의 블룸 필터 생성 시스템을 나타낸 도면

도 2는 개시되는 일 실시예에서 블록에 블룸 필터를 생성하는 상태를 나타낸 도면

도 3은 본 발명의 일 실시예에 따른 마이너 노드의 구성을 나타낸 블록도

도 4는 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도

발명을 실시하기 위한 구체적인 내용

[0033] 이하, 도면을 참조하여 본 발명의 구체적인 실시형태를 설명하기로 한다. 이하의 상세한 설명은 본 명세서에서 기술된 방법, 장치 및/또는 시스템에 대한 포괄적인 이해를 돕기 위해 제공된다. 그러나 이는 예시에 불과하며 본 발명은 이에 제한되지 않는다.

[0034] 본 발명의 실시예들을 설명함에 있어서, 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다. 상세한 설명에서 사용되는 용어는 단지 본 발명의 실시예들을 기술하기 위한 것이며, 결코 제한적이어서는 안 된다. 명확하게 달리 사용되지 않는 한, 단수 형태의 표현은 복수 형태의 의미를 포함한다. 본 설명에서, "포함" 또는 "구비"와 같은 표현은 어떤 특성들, 숫자들, 단계들, 동작들, 요소들, 이들의 일부 또는 조합을 가리키기 위한 것이며, 기술된 것 이외에 하나 또는 그 이상의 다른 특성, 숫자, 단계, 동작, 요소, 이들의 일부 또는 조합의 존재 또는 가능성을 배제하도록 해석되어서는 안 된다.

[0035] 이하의 설명에 있어서, 신호 또는 정보의 "전송", "통신", "송신", "수신" 기타 이와 유사한 의미의 용어는 일 구성요소에서 다른 구성요소로 신호 또는 정보가 직접 전달되는 것뿐만이 아니라 다른 구성요소를 거쳐 전달되는 것도 포함한다. 특히 신호 또는 정보를 일 구성요소로 "전송" 또는 "송신"한다는 것은 그 신호 또는 정보의 최종 목적지를 지시하는 것이고 직접적인 목적지를 의미하는 것이 아니다. 이는 신호 또는 정보의 "수신"에 있어서도 동일하다. 또한 본 명세서에 있어서, 2 이상의 데이터 또는 정보가 "관련"된다는 것은 하나의 데이터(또는 정보)를 획득하면, 그에 기초하여 다른 데이터(또는 정보)의 적어도 일부를 획득할 수 있음을 의미한다.

[0036] 또한, 제1, 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로 사용될 수 있다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성 요소는 제2 구성 요소로 명명될 수 있고, 유사하게 제2 구성 요소도 제1 구성 요소로 명명될 수 있다.

[0038] 도 1은 본 발명의 일 실시예에 따른 블록체인 기반의 블룸 필터 생성 시스템을 나타낸 도면이다.

[0039] 도 1을 참조하면, 블록체인 기반의 블룸 필터 생성 시스템(100)은 사용자 단말(102) 및 마이너(Miner) 노드(104)를 포함할 수 있다. 사용자 단말(102)은 마이너 노드(104)와 통신 네트워크(150)를 통해 상호 통신 가능하게 연결된다.

[0040] 몇몇 실시예들에서, 통신 네트워크(150)는 인터넷, 하나 이상의 로컬 영역 네트워크(local area networks), 광역 네트워크(wide area networks), 셀룰러 네트워크, 모바일 네트워크, 그 밖에 다른 종류의 네트워크들, 또는 이러한 네트워크들의 조합을 포함할 수 있다.

[0041] 개시되는 실시예에서, 블록체인은 프라이빗(Private) 블록체인일 수 있으나, 이에 한정되는 것은 아니며, 퍼블릭(Public) 블록체인 또는 컨소시움(Consortium) 블록체인일 수도 있다.

[0042] 사용자 단말(102)은 사용자 관련 정보를 포함하여 트랜잭션(Transaction)을 생성할 수 있다. 예시적인 실시예에서, 사용자 관련 정보는 사용자의 가명(Pseudonym), 사용자 아이디, 사용자의 공개키, 및 사용자 단말의 식별번호(예를 들어, MAC Address, IP 등) 중 어느 하나일 수 있으나, 이에 한정되는 것은 아니며 그 이외에 사용자를 식별할 수 있는 다양한 정보가 포함될 수 있다.

[0043] 구체적으로, 사용자 단말(102)은 트랜잭션을 위한 공개키 및 비밀키를 랜덤하게 각각 생성할 수 있다. 사용자 단말(102)은 사용자 관련 정보를 포함하는 트랜잭션을 상기 생성한 비밀키로 서명(Signature)하여 복수 개의 노드(Node)를 포함하는 블록체인 망으로 브로드캐스팅(Broadcasting) 할 수 있다.

[0044] 마이너 노드(104)는 블록체인 망을 구성하는 노드(Node) 중 하나를 의미할 수 있다. 블록체인 망은 복수 개의 노드를 포함하며, 복수 개의 노드 중 하나 이상이 마이너 노드(104)로 동작할 수 있다.

[0045] 마이너 노드(104)는 사용자 단말(102)로부터 트랜잭션을 수신할 수 있다. 예시적인 실시예에서, 마이너 노드(104)는 비밀키로 서명된 사용자 관련 정보를 포함하는 트랜잭션을 수신할 수 있다.

[0046] 마이너 노드(104)는 블록체인 망에서 각 사용자 단말(102)들이 전송하는 트랜잭션들을 수집하여 블록(Block)을 생성할 수 있다. 마이너 노드(104)는 생성한 블록을 블록체인(Blockchain)에 연결할 수 있다. 예시적인 실시예

에서, 마이너 노드(104)가 수집하는 트랜잭션에는 각 사용자의 사용자 관련 정보가 포함될 수 있다.

[0047] 마이너 노드(104)는 블록을 구성하는 각 트랜잭션에 포함된 사용자 관련 정보를 이용하여 블룸 필터(Bloom Filter)를 생성할 수 있다. 즉, 마이너 노드(104)는 각 트랜잭션에 포함된 사용자 관련 정보(예를 들어, 사용자의 가명(Pseudonym) 등)를 블룸 필터의 멤버(Member)로 하여 블룸 필터를 생성할 수 있다. 블룸 필터(Bloom Filter)는 소정 멤버가 집합에 속하는지 여부를 검사하기 위해 사용되는 확률적 자료 구조를 의미할 수 있다.

[0048] 마이너 노드(104)는 각 트랜잭션에 포함된 사용자 관련 정보에 대해 기 설정된 해쉬 함수를 적용하여 해쉬 값을 산출하고, 산출한 각 해쉬 값을 기반으로 블룸 필터를 생성할 수 있다. 마이너 노드(104)는 해당 블록을 구성하는 각 트랜잭션에 포함된 사용자 관련 정보를 기반으로 생성한 블룸 필터를 해당 블록의 마지막 트랜잭션으로 할 수 있다. 예를 들어, 블록이 6개의 트랜잭션으로 구성되는 경우, 마이너 노드(104)는 5개의 트랜잭션에 포함된 사용자 관련 정보를 기반으로 블룸 필터를 생성하고, 생성한 블룸 필터를 6번째 트랜잭션으로 할 수 있다.

[0049] 마이너 노드(104)는 블록체인에 각 블록을 연결하는 경우, 블록체인의 이전 블록에 포함된 블룸 필터에 해당 블록의 트랜잭션에 포함된 사용자 관련 정보를 추가하여 블룸 필터를 생성하고, 생성한 블룸 필터를 해당 블록의 마지막 트랜잭션으로 할 수 있다. 이에 대해 도 2를 참조하여 설명하기로 한다.

[0051] 도 2는 개시되는 일 실시예에서 블록에 블룸 필터를 생성하는 상태를 나타낸 도면이다. 도 2를 참조하면, 블록체인의 첫 번째 블록(S1)이 6개의 트랜잭션으로 구성되고, 마지막 트랜잭션은 5개의 트랜잭션(T1 ~ T5)에 포함된 사용자 관련 정보를 기반으로 생성된 제1 블룸 필터(BF1)일 수 있다.

[0052] 여기서, 두 번째 블록(S2)을 첫 번째 블록(S1)에 연결하는 경우, 마이너 노드(104)는 첫 번째 블록(S1)의 제1 블룸 필터(BF1)에 두 번째 블록(S2)의 5개의 트랜잭션(T1 ~ T5)에 포함된 사용자 관련 정보를 추가하여 제2 블룸 필터(BF2)를 생성할 수 있다. 이때, 제2 블룸 필터(BF2)는 두 번째 블록(S2)의 마지막 트랜잭션일 수 있다.

[0053] 그리고, 세 번째 블록(S3)을 두 번째 블록(S2)에 연결하는 경우, 마이너 노드(104)는 두 번째 블록(S2)의 제2 블룸 필터(BF2)에 세 번째 블록(S3)의 5개의 트랜잭션(T1 ~ T5)에 포함된 사용자 관련 정보를 추가하여 제3 블룸 필터(BF3)를 생성할 수 있다. 이때, 제3 블룸 필터(BF3)는 세 번째 블록(S3)의 마지막 트랜잭션일 수 있다.

[0054] 이러한 방식으로 블룸 필터를 생성하면, 블록체인에서 각 블록의 블룸 필터는 이전 블록의 블룸 필터가 누적된 값을 가지게 된다. 이 경우, 블록체인의 마지막 블록의 블룸 필터는 블록체인에 포함된 각 트랜잭션들에 포함된 사용자 관련 정보들을 멤버로 하게 되므로, 멤버쉽 체크가 필요한 경우 블록체인의 마지막 블록의 블룸 필터를 이용하여 용이하게 수행할 수 있게 된다.

[0055] 즉, 블록체인 내에서 소정 사용자에 대한 멤버쉽 체크가 필요한 경우, 블록체인의 마지막 블록의 블룸 필터를 조회하고, 소정 사용자의 사용자 관련 정보(예를 들어, 사용자의 가명(Pseudonym) 등)에 대해 블룸 필터가 예스(Yes) 또는 노(No)를 보고하는지를 확인하여 멤버쉽 체크를 진행할 수 있다. 블룸 필터가 예스(Yes)로 보고하는 경우, 마이너 노드(104)는 해당 사용자가 유효한 멤버인 것으로 판단할 수 있다. 블룸 필터가 노(No)로 보고하는 경우, 마이너 노드(104)는 해당 사용자가 유효하지 않은 멤버인 것으로 판단할 수 있다.

[0056] 여기서, 각 블록의 블룸 필터는 이전 블록의 블룸 필터가 누적된 상태이므로, 어떤 시점에서는 블룸 필터의 긍정 오류(False Positive)가 무시할 수 없는 수준에 도달할 수 있게 된다. 이에, 마이너 노드(104)는 블룸 필터의 긍정 오류가 기 설정된 임계 값을 초과하는 경우, 블룸 필터의 크기를 키울 수 있다.

[0057] 구체적으로, 마이너 노드(104)는 소정 블록에 대해 블룸 필터를 생성하는 경우, 이전 블록의 블룸 필터를 조회하여 긍정 오류(False Positive)를 산출할 수 있다. 여기서, 긍정 오류(FP)는 하기의 수학식을 통해 산출할 수 있다.

[0058] (수학식)

[0059] $$FP = (1 - (1 - \frac{1}{M})^{l \cdot N})^{l}$$

[0060] 여기서, M은 현재 블룸 필터의 크기를 나타내고, l은 블룸 필터를 위한 해쉬 함수의 수를 나타내며, N은 블룸 필터의 축적된 수를 나타낸다.

[0061] 마이너 노드(104)는 산출된 긍정 오류(FP)가 기 설정된 임계 값을 초과하는 경우, 블룸 필터의 크기를 리사이징(Resizing) 할 수 있다. 즉, 블룸 필터의 크기를 현재 블룸 필터의 크기보다 크게 리사이징 할 수 있다. 이때, 마이너 노드(104)는 블록체인의 모든 트랜잭션(즉, 첫 번째 블록에서 현재 블록에 포함된 모든 트랜잭션)들에

포함된 사용자 관련 정보들을 사용하여 블룸 필터를 재구성할 수 있다. 블룸 필터의 크기는 블룸 필터의 크기의 성장 속도에 따라 조정될 수 있다.

[0062] 한편, 개시되는 실시예에서는 블룸 필터로 카운팅 블룸 필터(Counting Bloom Filter)를 사용할 수도 있다. 일반적인 블룸 필터는 멤버의 삭제가 불가능하나, 카운팅 블룸 필터는 멤버의 삭제가 가능하다.

[0063] 예시적인 실시예에서, 사용자 단말(102)은 특정 사용자 관련 정보의 삭제를 마이너 노드(104)에 요청할 수 있다. 이를 위해, 블록체인의 트랜잭션은 멤버의 삽입 요청인지 삭제 요청인지를 나타내는 필드를 포함할 수 있다. 마이너 노드(104)는 트랜잭션의 해당 필드에서 멤버의 삽입 요청인지 삭제 요청인지를 확인하여 삭제 요청인 경우 해당 셀에서 해당 멤버의 해쉬값에 대응하는 카운트를 줄일 수 있다. 만약, 멤버의 삽입 요청인 경우, 마이너 노드(104)는 해당 멤버의 해쉬 값에 해당하는 각 셀의 카운트를 증가시킬 수 있다.

[0064] 또한, 개시되는 실시예에서는 취소된 멤버를 위한 블룸 필터를 별도로 사용할 수도 있다. 이 경우, 2개의 블룸 필터가 존재할 수 있다. 즉, 유효한 멤버를 위한 블룸 필터(유효 멤버 블룸 필터)와 취소된 멤버를 위한 블룸 필터(취소 멤버 블룸 필터)가 있을 수 있다.

[0065] 사용자 단말(102)은 특정 사용자 관련 정보에 대해 삭제 또는 추가를 마이너 노드(104)에 요청할 수 있다. 마이너 노드(104)는 트랜잭션에서 멤버의 삽입 요청인지 삭제 요청인지를 나타내는 필드를 확인하여 삭제 요청이면 해당 사용자 관련 정보를 취소 멤버 블룸 필터에 추가하고, 삽입 요청이면 해당 사용자 관련 정보를 유효 멤버 블룸 필터에 추가할 수 있다.

[0066] 개시되는 실시예에 의하면, 사용자 단말(102)이 사용자 관련 정보를 포함하는 트랜잭션을 서명하여 블록체인 망에 브로드캐스팅 하고, 블록체인 망의 마이너 노드(104)에서 트랜잭션을 기반으로 각 블록에 대해 블룸 필터를 생성함으로써, 탈 중앙화된(Decentralized) 방식으로 블룸 필터를 생성할 수 있게 된다.

[0067] 또한, 블록체인의 각 블록에서 이전 블록의 블룸 필터를 누적시킴으로써, 블록체인의 마지막 블록의 블룸 필터를 확인하면 해당 블록체인 망에 대해 멤버쉽 체크를 용이하게 수행할 수 있게 된다. 또한, 블룸 필터를 통해 사용자 멤버쉽의 삭제 및 추가 기능을 제공할 수 있게 된다.

[0069] 도 3은 본 발명의 일 실시예에 따른 마이너 노드의 구성을 나타낸 블록도이다.

[0070] 도 3을 참조하면, 마이너 노드(104)는 수집 모듈(111), 블룸 필터 생성 모듈(113), 및 블룸 필터 리사이징 모듈(115)을 포함할 수 있다.

[0071] 수집 모듈(111)은 블록체인 망에서 각 사용자 단말(102)들이 전송하는 트랜잭션을 수집할 수 있다. 수집 모듈(111)이 수집하는 트랜잭션에는 각 사용자의 사용자 관련 정보가 포함될 수 있다.

[0072] 블룸 필터 생성 모듈(113)은 수집된 트랜잭션에 기반하여 블록체인을 구성하는 각 블록을 생성할 수 있다. 블룸 필터 생성 모듈(113)은 블록을 구성하는 각 트랜잭션에 포함된 사용자 관련 정보에 기반하여 블룸 필터를 생성할 수 있다. 블룸 필터 생성 모듈(113)은 해당 블록을 구성하는 각 트랜잭션에 포함된 사용자 관련 정보를 기반으로 블룸 필터를 생성하고, 생성한 블룸 필터를 해당 블록의 마지막 트랜잭션으로 할 수 있다.

[0073] 또한, 블룸 필터 생성 모듈(113)은 블록체인에 각 블록을 연결하는 경우, 블록체인의 이전 블록에 포함된 블룸 필터에 해당 블록의 트랜잭션에 포함된 사용자 관련 정보를 추가하여 블룸 필터를 생성하고, 생성한 블룸 필터를 해당 블록의 마지막 트랜잭션으로 할 수 있다.

[0074] 블룸 필터 리사이징 모듈(115)은 블룸 필터의 긍정 오류(False Positive)가 기 설정된 임계 값을 초과하는지 여부에 따라 블룸 필터의 크기를 키울 수 있다. 블룸 필터 리사이징 모듈(115)은 소정 블록에 대해 블룸 필터를 생성하는 경우, 이전 블록의 블룸 필터를 조회하여 긍정 오류(False Positive)를 산출할 수 있다. 블룸 필터 리사이징 모듈(115)은 산출된 긍정 오류(FP)가 기 설정된 임계 값을 초과하는 경우, 블룸 필터의 크기를 현재 블룸 필터의 크기보다 크게 리사이징(Resizing) 할 수 있다

[0075] 블룸 필터의 크기를 리사이징 한 경우, 블룸 필터 생성 모듈(113)은 블록체인의 모든 트랜잭션(즉, 첫 번째 블록에서 현재 블록에 포함된 모든 트랜잭션)들에 포함된 사용자 관련 정보들을 사용하여 블룸 필터를 재구성할 수 있다.

[0076] 본 명세서에서 모듈이라 함은, 본 발명의 기술적 사상을 수행하기 위한 하드웨어 및 상기 하드웨어를 구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미할 수 있다. 예컨대, 상기 "모듈"은 소정의 코드와 상기 소정의 코드가 수행되기 위한 하드웨어 리소스의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된 코드를

의미하거나, 한 종류의 하드웨어를 의미하는 것은 아니다.

[0078] 도 4는 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경(10)을 예시하여 설명하기 위한 블록도이다. 도시된 실시예에서, 각 컴포넌트들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술된 것 이외에도 추가적인 컴포넌트를 포함할 수 있다.

[0079] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 일 실시예에서, 컴퓨팅 장치(12)는 사용자 단말(102)일 수 있다. 또한, 컴퓨팅 장치(12)는 마이너 노드(104)일 수 있다.

[0080] 컴퓨팅 장치(12)는 적어도 하나의 프로세서(14), 컴퓨터 판독 가능 저장 매체(16) 및 통신 버스(18)를 포함한다. 프로세서(14)는 컴퓨팅 장치(12)로 하여금 앞서 언급된 예시적인 실시예에 따라 동작하도록 할 수 있다. 예컨대, 프로세서(14)는 컴퓨터 판독 가능 저장 매체(16)에 저장된 하나 이상의 프로그램들을 실행할 수 있다. 상기 하나 이상의 프로그램들은 하나 이상의 컴퓨터 실행 가능 명령어를 포함할 수 있으며, 상기 컴퓨터 실행 가능 명령어는 프로세서(14)에 의해 실행되는 경우 컴퓨팅 장치(12)로 하여금 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.

[0081] 컴퓨터 판독 가능 저장 매체(16)는 컴퓨터 실행 가능 명령어 내지 프로그램 코드, 프로그램 데이터 및/또는 다른 적합한 형태의 정보를 저장하도록 구성된다. 컴퓨터 판독 가능 저장 매체(16)에 저장된 프로그램(20)은 프로세서(14)에 의해 실행 가능한 명령어의 집합을 포함한다. 일 실시예에서, 컴퓨터 판독 가능 저장 매체(16)는 메모리(랜덤 액세스 메모리와 같은 휘발성 메모리, 비휘발성 메모리, 또는 이들의 적절한 조합), 하나 이상의 자기 디스크 저장 디바이스들, 광학 디스크 저장 디바이스들, 플래시 메모리 디바이스들, 그 밖에 컴퓨팅 장치(12)에 의해 액세스되고 원하는 정보를 저장할 수 있는 다른 형태의 저장 매체, 또는 이들의 적합한 조합일 수 있다.

[0082] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

[0083] 컴퓨팅 장치(12)는 또한 하나 이상의 입출력 장치(24)를 위한 인터페이스를 제공하는 하나 이상의 입출력 인터페이스(22) 및 하나 이상의 네트워크 통신 인터페이스(26)를 포함할 수 있다. 입출력 인터페이스(22) 및 네트워크 통신 인터페이스(26)는 통신 버스(18)에 연결된다. 입출력 장치(24)는 입출력 인터페이스(22)를 통해 컴퓨팅 장치(12)의 다른 컴포넌트들에 연결될 수 있다. 예시적인 입출력 장치(24)는 포인팅 장치(마우스 또는 트랙패드 등), 키보드, 터치 입력 장치(터치패드 또는 터치스크린 등), 음성 또는 소리 입력 장치, 다양한 종류의 센서 장치 및/또는 촬영 장치와 같은 입력 장치, 및/또는 디스플레이 장치, 프린터, 스피커 및/또는 네트워크 카드와 같은 출력 장치를 포함할 수 있다. 예시적인 입출력 장치(24)는 컴퓨팅 장치(12)를 구성하는 일 컴포넌트로서 컴퓨팅 장치(12)의 내부에 포함될 수도 있고, 컴퓨팅 장치(12)와는 구별되는 별개의 장치로 컴퓨팅 장치(12)와 연결될 수도 있다.

[0085] 이상에서 본 발명의 대표적인 실시예들을 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0087] 100 : 블록체인 기반의 블룸 필터 생성 시스템

102 : 사용자 단말

104 : 마이너 노드

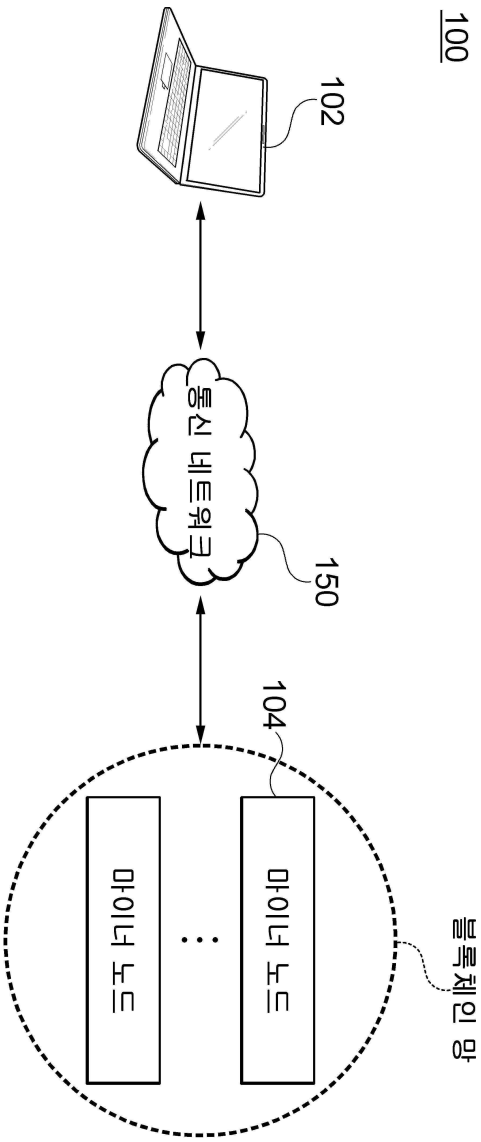
111 : 수집 모듈

113 : 블룸 필터 생성 모듈

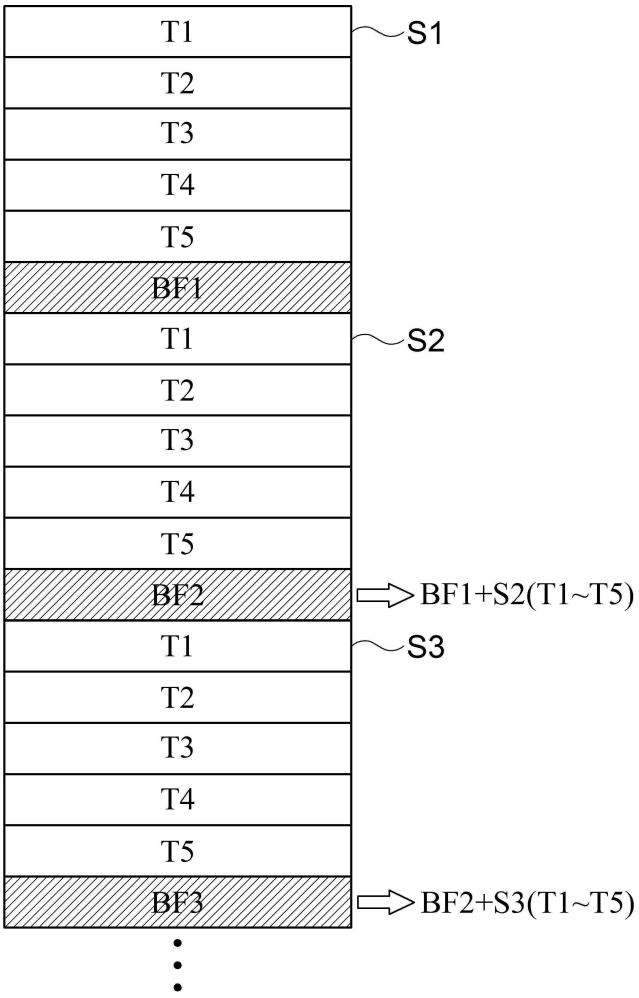
115 : 블룸 필터 리사이징 모듈

도면

도면1

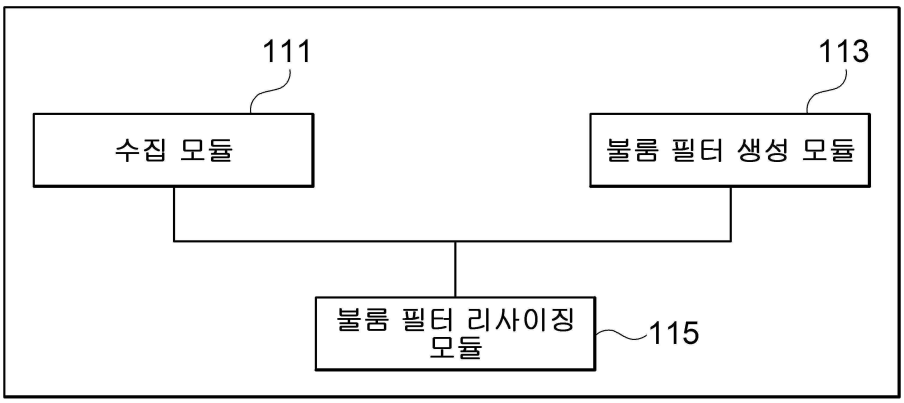


도면2

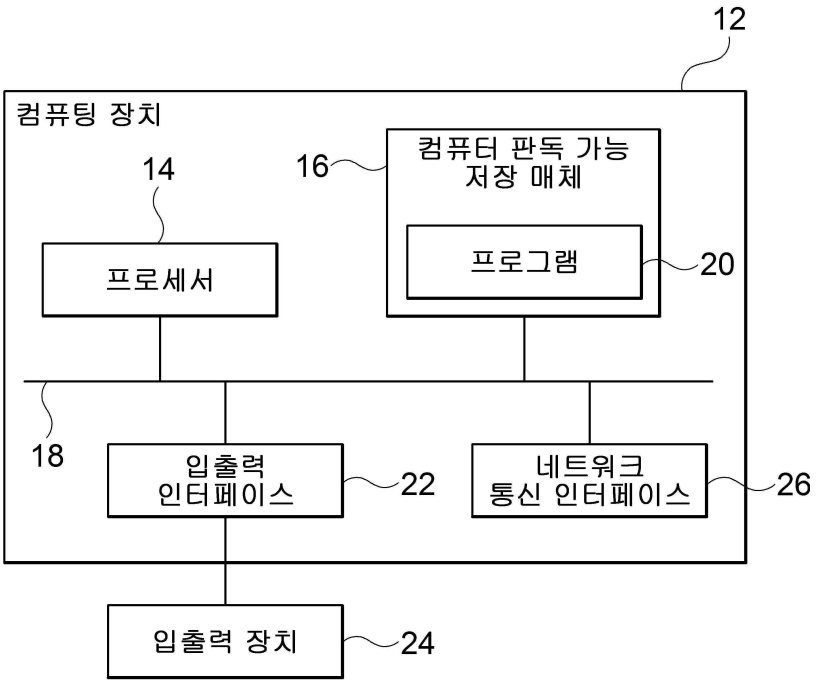

T1
T2
T3
T4
T5
BF1
T1
T2
T3
T4
T5
BF2
T1
T2
T3
T4
T5
BF3
S1
S2
S3
BF1+S2(T1~T5)
BF2+S3(T1~T5)

도면3

104


111
113
수집 모듈
불룸 필터 생성 모듈
불룸 필터 리사이징 모듈
115

도면4


10
12
컴퓨팅 장치
14
프로세서
16
컴퓨터 판독 가능
저장 매체
프로그램
20
18
입출력
인터페이스
22
네트워크
통신 인터페이스
26
입출력 장치
24