



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0079218
(43) 공개일자 2020년07월02일

(51) 국제특허분류(Int. Cl.)
G06F 21/64 (2013.01) G06F 21/60 (2013.01)
G06F 21/62 (2013.01) H04L 9/06 (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
G06F 21/64 (2013.01)
G06F 21/602 (2013.01)
(21) 출원번호 10-2019-7022198
(22) 출원일자(국제) 2018년12월21일
심사청구일자 2019년08월09일
(85) 번역문제출일자 2019년07월26일
(86) 국제출원번호 PCT/CN2018/122559
(87) 국제공개번호 WO 2019/072301
국제공개일자 2019년04월18일

(71) 출원인
알리바바 그룹 홀딩 리미티드
케이만군도, 그랜드 케이만, 피오박스 847, 원 캐
피탈 플레이스 4층
(72) 발명자
청 룽
중국 저지앙 311121 항저우 유 향 디스트릭트 웨
스트 웨 이 로드 넘버 969 빌딩 3 알리바바 그룹
리갈 디파트먼트 5층
리 안펑
중국 저지앙 311121 항저우 유 향 디스트릭트 웨
스트 웨 이 로드 넘버 969 빌딩 3 알리바바 그룹
리갈 디파트먼트 5층
펑 지위안
중국 저지앙 311121 항저우 유 향 디스트릭트 웨
스트 웨 이 로드 넘버 969 빌딩 3 알리바바 그룹
리갈 디파트먼트 5층
(74) 대리인
김태홍, 김진희

전체 청구항 수 : 총 20 항

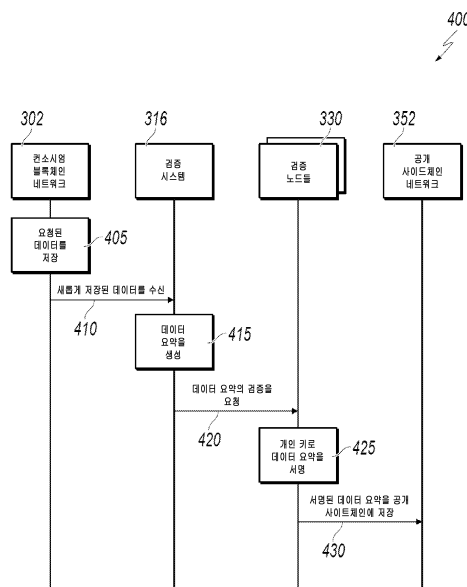
(54) 발명의 명칭 퍼블릭 사이드체인을 사용하여 컨소시엄 블록체인에 저장된 데이터의 무결성 검증

(57) 요약

본 명세서의 구현예는 데이터 항목을 컨소시엄 블록체인에서 저장하는 것; 저장된 데이터 항목에 기초하여 제 1 데이터 요약을 생성하는 것; 제 1 데이터 요약, 제 1 데이터 요약을 암호 방식으로 서명하고 설명된 제 1 데이터 요약을 공개 블록체인에서 저장하기 위한 검증 노드로 전송하는 것; 저장된 데이터 항목을 리트리브하기 위한

(뒷면에 계속)

대표도 - 도4



요청을 수신하는 것; 컨소시엄 블록체인으로부터 요청된 데이터 항목을 리트리브하는 것; 리트리브된 데이터 항목에 기초하여 제 2 데이터 요약을 생성하는 것; 각각의 검증 노드가 제 2 데이터 요약을 서명하도록, 제 2 데이터 요약을 검증 노드로 전송하는 것; 복수의 검증 노드로부터 서명된 제 2 데이터 요약을 수신하는 것; 공개 블록체인으로부터 서명된 제 1 데이터 요약을 리트리브하는 것; 서명된 제 1 데이터 요약이 서명된 제 2 데이터 요약과 정합하는 것으로 결정하는 것; 및 저장된 데이터 항목을 리트리브하기 위한 요청에 대한, 저장된 데이터 항목이 변경되지 않는다는 것을 표시하는 응답을 전송하는 것을 포함한다.

(52) CPC특허분류

G06F 21/62 (2013.01)

H04L 9/0643 (2013.01)

H04L 9/3247 (2013.01)

명세서

청구범위

청구항 1

컴퓨터 구현(computer-implemented) 방법에 있어서,

데이터 항목(data item)을 컨소시엄 블록체인 네트워크에 의해 유지되는 컨소시엄 블록체인에 저장하는 단계;

상기 저장된 데이터 항목에 기초하여 제 1 데이터 요약(data digest)을 생성하는 단계;

각각의 검증(verification) 노드가 상기 제 1 데이터 요약을 암호 방식으로 서명하고 자신의 서명된 제 1 데이터 요약을 공개 블록체인 네트워크에 의해 유지되는 공개 블록체인에 저장하도록, 상기 제 1 데이터 요약을 복수의 검증 노드로 전송하는 단계;

상기 저장된 데이터 항목을 리트리브하기 위한 요청을 수신하는 단계;

상기 요청을 수신하는 것에 응답하여, 상기 컨소시엄 블록체인으로부터 상기 요청된 데이터 항목을 리트리브(retrieve)하는 단계;

상기 리트리브된 데이터 항목에 기초하여 제 2 데이터 요약을 생성하는 단계;

각각의 검증 노드가 상기 제 2 데이터 요약을 암호 방식으로 서명하고 자신의 서명된 제 2 데이터 요약을 반환(return)하도록, 상기 제 2 데이터 요약을 상기 복수의 검증 노드로 전송하는 단계;

상기 복수의 검증 노드로부터 상기 서명된 제 2 데이터 요약을 수신하는 단계;

상기 공개 블록체인으로부터 상기 서명된 제 1 데이터 요약을 리트리브하는 단계;

상기 서명된 제 1 데이터 요약이 상기 서명된 제 2 데이터 요약과 매칭됨(match)을 결정하는 단계; 및

상기 결정하는 것에 응답하여, 저장된 데이터 항목을 리트리브하기 위한 상기 요청에 대한 응답 - 상기 응답은 상기 저장된 데이터 항목이 그것이 저장된 이래로 변경되지 않았다는 것을 표시함 - 을 전송하는 단계

를 포함하는, 컴퓨터 구현 방법.

청구항 2

제 1 항에 있어서,

상기 복수의 검증 노드는 상기 공개 블록체인 네트워크에 참여하는 컴퓨팅 디바이스인 것인, 컴퓨터 구현 방법.

청구항 3

제 1 항에 있어서,

스마트 계약을 상기 공개 블록체인에 저장하는 단계를 더 포함하고, 상기 스마트 계약은, 상기 검증 노드로부터 상기 요청된 서명된 제 2 데이터 요약을 수신하는 것에 응답하여 금전적 보상을 상기 검증 노드에 제공하도록 구성되는 것인, 컴퓨터 구현 방법.

청구항 4

제 1 항에 있어서,

상기 제 1 데이터 요약을 생성하는 단계는 상기 저장된 데이터 항목의 해시(hash)를 계산하는 단계를 포함하는 것인, 컴퓨터 구현 방법.

청구항 5

제 1 항에 있어서,

각각의 검증 노드는 그 검증 노드와 연관된 개인 키(private key)를 사용하여 상기 제 1 데이터 요약을 암호 방

식으로 서명하도록 구성되는 것인, 컴퓨터 구현 방법.

청구항 6

제 1 항에 있어서,

상기 제 1 데이터 요약을 상기 복수의 검증 노드로 전송하는 단계는, 상기 제 1 데이터 요약을 상기 공개 블록체인 네트워크로 브로드캐스팅하는 단계를 포함하는 것인, 컴퓨터 구현 방법.

청구항 7

제 1 항에 있어서,

상기 공개 블록체인으로부터 상기 서명된 제 1 데이터 요약을 리트리브하는 단계는, 상기 저장된 데이터 항목과 연관되며 상기 공개 블록체인에 저장된 식별자에 기초하여, 상기 서명된 제 1 데이터 요약을 식별하는 단계를 포함하는 것인, 컴퓨터 구현 방법.

청구항 8

비-일시적 컴퓨터-판독가능 저장 매체에 있어서,

하나 이상의 컴퓨터에 결합되며,

데이터 항목을 컨소시엄 블록체인 네트워크에 의해 유지되는 컨소시엄 블록체인에 저장하고;

상기 저장된 데이터 항목에 기초하여 제 1 데이터 요약을 생성하고;

각각의 검증 노드가 상기 제 1 데이터 요약을 암호 방식으로 서명하고 자신의 서명된 제 1 데이터 요약을 공개 블록체인 네트워크에 의해 유지되는 공개 블록체인에 저장하도록, 상기 제 1 데이터 요약을 복수의 검증 노드로 전송하고;

상기 저장된 데이터 항목을 리트리브하기 위한 요청을 수신하고;

상기 요청을 수신하는 것에 응답하여, 상기 컨소시엄 블록체인으로부터 상기 요청된 데이터 항목을 리트리브하고;

상기 리트리브된 데이터 항목에 기초하여 제 2 데이터 요약을 생성하고;

각각의 검증 노드가 상기 제 2 데이터 요약을 암호 방식으로 서명하고 자신의 서명된 제 2 데이터 요약을 반환하도록, 상기 제 2 데이터 요약을 상기 복수의 검증 노드로 전송하고;

상기 복수의 검증 노드로부터 상기 서명된 제 2 데이터 요약을 수신하고;

상기 공개 블록체인으로부터 상기 서명된 제 1 데이터 요약을 리트리브하고;

상기 서명된 제 1 데이터 요약이 상기 서명된 제 2 데이터 요약과 매칭됨을 결정하고;

상기 결정하는 것에 응답하여, 상기 저장된 데이터 항목을 리트리브하기 위한 상기 요청에 대한 응답 - 상기 응답은 상기 저장된 데이터 항목이 그것이 저장된 이래로 변경되지 않았다는 것을 표시함 - 을 전송하도록

상기 하나 이상의 컴퓨터에 의해 실행가능한 명령들로 구성(configure)된, 비-일시적 컴퓨터-판독가능 저장 매체.

청구항 9

제 8 항에 있어서,

상기 복수의 검증 노드는 상기 공개 블록체인 네트워크에 참여하는 컴퓨팅 디바이스인 것인, 비-일시적 컴퓨터-판독가능 저장 매체.

청구항 10

제 8 항에 있어서,

스마트 계약을 상기 공개 블록체인에 저장하도록, 상기 하나 이상의 컴퓨터에 의해 실행가능한 명령들로 또한

구성되며, 상기 스마트 계약은, 상기 검증 노드로부터 상기 요청된 서명된 제 2 데이터 요약을 수신하는 것에 응답하여 금전적 보상을 상기 검증 노드에 제공하도록 구성되는 것인, 비-일시적 컴퓨터-판독가능 저장 매체.

청구항 11

제 8 항에 있어서,

상기 제 1 데이터 요약을 생성하는 것은 상기 저장된 데이터 항목의 해시를 계산하는 것을 포함하는 것인, 비-일시적 컴퓨터-판독가능 저장 매체.

청구항 12

제 8 항에 있어서,

각각의 검증 노드는 그 검증 노드와 연관된 개인 키를 사용하여 상기 제 1 데이터 요약을 암호 방식으로 서명하도록 구성되는 것인, 비-일시적 컴퓨터-판독가능 저장 매체.

청구항 13

제 8 항에 있어서,

상기 제 1 데이터 요약을 상기 복수의 검증 노드로 전송하는 것은, 상기 제 1 데이터 요약을 상기 공개 블록체인 네트워크로 브로드캐스팅하는 것을 포함하는 것인, 비-일시적 컴퓨터-판독가능 저장 매체.

청구항 14

제 8 항에 있어서,

상기 공개 블록체인으로부터 상기 서명된 제 1 데이터 요약을 리트리브하는 것은, 상기 저장된 데이터 항목과 연관되며 상기 공개 블록체인에 저장된 식별자에 기초하여, 상기 서명된 제 1 데이터 요약을 식별하는 것을 포함하는 것인, 비-일시적 컴퓨터-판독가능 저장 매체.

청구항 15

시스템에 있어서,

하나 이상의 컴퓨터; 및

하나 이상의 컴퓨터-판독가능 메모리를 포함하고,

상기 컴퓨터-판독가능 메모리는, 상기 하나 이상의 컴퓨터에 결합되며,

데이터 항목을 컨소시엄 블록체인 네트워크에 의해 유지되는 컨소시엄 블록체인에 저장하고;

상기 저장된 데이터 항목에 기초하여 제 1 데이터 요약을 생성하고;

각각의 검증 노드가 상기 제 1 데이터 요약을 암호 방식으로 서명하고 자신의 서명된 제 1 데이터 요약을 공개 블록체인 네트워크에 의해 유지되는 공개 블록체인에 저장하도록, 상기 제 1 데이터 요약을 복수의 검증 노드로 전송하고;

상기 저장된 데이터 항목을 리트리브하기 위한 요청을 수신하고;

상기 요청을 수신하는 것에 응답하여, 상기 컨소시엄 블록체인으로부터 상기 요청된 데이터 항목을 리트리브하고;

상기 리트리브된 데이터 항목에 기초하여 제 2 데이터 요약을 생성하고;

각각의 검증 노드가 상기 제 2 데이터 요약을 암호 방식으로 서명하고 자신의 서명된 제 2 데이터 요약을 반환하도록, 상기 제 2 데이터 요약을 상기 복수의 검증 노드로 전송하고;

상기 복수의 검증 노드로부터 상기 서명된 제 2 데이터 요약을 수신하고;

상기 공개 블록체인으로부터 상기 서명된 제 1 데이터 요약을 리트리브하고;

상기 서명된 제 1 데이터 요약이 상기 서명된 제 2 데이터 요약과 매칭됨을 결정하고;

상기 결정하는 것에 응답하여, 상기 저장된 데이터 항목을 리트리브하기 위한 상기 요청에 대한 응답 - 상기 응답은 상기 저장된 데이터 항목이 그것이 저장된 이래로 변경되지 않았다는 것을 표시함 - 을 전송하도록

상기 하나 이상의 컴퓨터에 의해 실행가능한 명령들로 구성된 것인, 시스템.

청구항 16

제 15 항에 있어서,

상기 복수의 검증 노드는 상기 공개 블록체인 네트워크에 참여하는 컴퓨팅 디바이스인 것인, 시스템.

청구항 17

제 15 항에 있어서,

상기 컴퓨터-관독가능 메모리는 또한, 스마트 계약을 상기 공개 블록체인에 저장하도록, 상기 하나 이상의 컴퓨터에 의해 실행가능한 명령들로 구성되며, 상기 스마트 계약은, 상기 검증 노드로부터 상기 요청된 서명된 제 2 데이터 요약을 수신하는 것에 응답하여 금전적 보상을 상기 검증 노드에 제공하도록 구성되는 것인, 시스템.

청구항 18

제 15 항에 있어서,

상기 제 1 데이터 요약을 생성하는 것은 상기 저장된 데이터 항목의 해시를 계산하는 것을 포함하는 것인, 시스템.

청구항 19

제 15 항에 있어서,

각각의 검증 노드는 그 검증 노드와 연관된 개인 키를 사용하여 상기 제 1 데이터 요약을 암호 방식으로 서명하도록 구성되는 것인, 시스템.

청구항 20

제 15 항에 있어서,

상기 제 1 데이터 요약을 상기 복수의 검증 노드로 전송하는 것은, 상기 제 1 데이터 요약을 상기 공개 블록체인 네트워크로 브로드캐스팅하는 것을 포함하는 것인, 시스템.

발명의 설명

기술 분야

배경 기술

[0001] 컨센서스 네트워크(consensus network)들 및/또는 블록체인 네트워크(blockchain network)들로서 또한 지칭될 수 있는 분산된 원장 시스템(distributed ledger system; DLS)들은 참여하는 엔티티(entity)들이 데이터를 보안성 있게 그리고 변경할 수 없게 저장하는 것을 가능하게 한다. DLS들은 임의의 특정한 사용자 경우를 참조하지 않으면서, 블록체인 네트워크들로서 통상적으로 지칭된다. 블록체인 네트워크들의 유형들의 예들은 공개 블록체인 네트워크(public blockchain network)들, 사적 블록체인 네트워크(private blockchain network)들, 및 컨소시엄 블록체인 네트워크(consortium blockchain network)들을 포함할 수 있다. 공개 블록체인 네트워크는 모든 엔티티들이 DLS를 이용하고 컨센서스 프로세스에 참여하기 위하여 개방된다. 사적 블록체인 네트워크는 관독 및 기입 허가들을 중앙 제어하는 특정한 엔티티를 위하여 제공된다. 컨소시엄 블록체인 네트워크는 컨센서스 프로세스를 제어하는 엔티티들의 선택된 그룹을 위하여 제공되고, 액세스 제어 계층(access control layer)을 포함한다.

[0002] 블록체인은 탈중앙화된(decentralized) 그리고 템퍼-방지 분산된(temper-proof distributed) 데이터 저장 기술이다. 사용자 데이터 및 계약들은 논리적으로 동작되고, 공개 방식으로 체인(chain) 상에서 저장된다. 많은

시나리오들에서, 사용자들은 프라이버시 보호(privacy protection) 요건들을 충족시키는 것을 필요로 하고, 그 데이터 및 로직(logic)들이 비인가된 당사자들에게 누설되는 것을 원하지 않는다.

[0003] 암호법(cryptography)은 일부 특정 시나리오 설계들을 위한 프라이버시 보호를 개량하기 위하여 이용될 수 있지만, 블록체인 동작들의 현존하는 프라이버시 쟁점들을 해결하기 위하여, 더 다목적이고 효율적인 해결책이 희망된다.

발명의 내용

[0004] 본 명세서의 구현예들은 블록체인 네트워크의 노드들과 연관된 검증되어야 할 데이터를 저장하고 리트리브(retrieve)하기 위한 컴퓨터-구현된 방법들을 포함한다. 더 상세하게는, 본 명세서의 구현예들은 다수의 검증 노드들을 이용하는 하나 이상의 컨소시엄 블록체인 네트워크 노드들과 연관된 검증되어야 할 데이터의 데이터 요약(data digest)을 저장하는 것과, 검증되어야 할 데이터 및 저장된 데이터 요약들을 리트리브하는 것에 관한 것이다.

[0005] 일부 구현예들에서, 액션들은 데이터 항목(data item)을 컨소시엄 블록체인 네트워크에 의해 유지된 컨소시엄 블록체인에 저장하는 것; 저장된 데이터 항목에 기초하여 제 1 데이터 요약을 생성하는 것; 각각의 검증 노드가 제 1 데이터 요약을 암호 방식으로 서명하고, 그 서명된 제 1 데이터 요약을 공개 블록체인 네트워크에 의해 유지된 공개 블록체인에 저장하도록, 제 1 데이터 요약을 검증 노드들로 전송하는 것; 저장된 데이터 항목을 리트리브하기 위한 요청을 수신하는 것; 요청을 수신하는 것에 응답하여, 컨소시엄 블록체인으로부터 요청된 데이터 항목을 리트리브하는 것; 리트리브된 데이터 항목에 기초하여 제 2 데이터 요약을 생성하는 것; 각각의 검증 노드가 제 2 데이터 요약을 암호 방식으로 서명하고 그 서명된 제 2 데이터 요약을 반환하도록, 제 2 데이터 요약을 검증 노드들로 전송하는 것; 검증 노드들로부터 서명된 제 2 데이터 요약들을 수신하는 것; 공개 블록체인으로부터 서명된 제 1 데이터 요약들을 리트리브하는 것; 서명된 제 1 데이터 요약들이 서명된 제 2 데이터 요약들과 정합하는 것으로 결정하는 것; 및 결정하는 것에 응답하여, 저장된 데이터 항목을 리트리브하기 위한 요청에 대한 응답 - 응답은 저장된 데이터 항목이 그것이 저장된 이후로 변경되지 않았다는 것을 표시함 - 을 전송하는 것을 포함한다. 다른 구현예들은 대응하는 시스템들, 장치, 및 컴퓨터 저장 디바이스들 상에서 인코딩된, 방법들의 액션들을 수행하도록 구성된 컴퓨터 프로그램들을 포함한다.

[0006] 일부 구현예들에서, 비-일시적 컴퓨터-판독가능 저장 매체는 하나 이상의 컴퓨터들에 결합되고, 그리고 데이터 항목을 컨소시엄 블록체인 네트워크에 의해 유지된 컨소시엄 블록체인에 저장하고; 저장된 데이터 항목에 기초하여 제 1 데이터 요약을 생성하고; 각각의 검증 노드가 제 1 데이터 요약을 암호 방식으로 서명하고, 그 서명된 제 1 데이터 요약을 공개 블록체인 네트워크에 의해 유지된 공개 블록체인에 저장하도록, 제 1 데이터 요약을 검증 노드들로 전송하고; 저장된 데이터 항목을 리트리브하기 위한 요청을 수신하고; 요청을 수신하는 것에 응답하여, 컨소시엄 블록체인으로부터 요청된 데이터 항목을 리트리브하고; 리트리브된 데이터 항목에 기초하여 제 2 데이터 요약을 생성하고; 각각의 검증 노드가 제 2 데이터 요약을 암호 방식으로 서명하고 그 서명된 제 2 데이터 요약을 반환하도록, 제 2 데이터 요약을 검증 노드들로 전송하고; 검증 노드들로부터 서명된 제 2 데이터 요약들을 수신하고; 공개 블록체인으로부터 서명된 제 1 데이터 요약들을 리트리브하고; 서명된 제 1 데이터 요약들이 서명된 제 2 데이터 요약들과 정합하는 것으로 결정하고; 그리고 결정하는 것에 응답하여, 저장된 데이터 항목을 리트리브하기 위한 요청에 대한 응답 - 응답은 저장된 데이터 항목이 그것이 저장된 이후로 변경되지 않았다는 것을 표시함 - 을 전송하도록 하나 이상의 컴퓨터들에 의해 실행가능한 명령들로 구성된다.

[0007] 일부 구현예들에서, 시스템은 하나 이상의 컴퓨터들; 및 하나 이상의 컴퓨터들에 결합되고, 그리고 데이터 항목을 컨소시엄 블록체인 네트워크에 의해 유지된 컨소시엄 블록체인에 저장하고; 저장된 데이터 항목에 기초하여 제 1 데이터 요약을 생성하고; 각각의 검증 노드가 제 1 데이터 요약을 암호 방식으로 서명하고, 그 서명된 제 1 데이터 요약을 공개 블록체인 네트워크에 의해 유지된 공개 블록체인에 저장하도록, 제 1 데이터 요약을 검증 노드들로 전송하고; 저장된 데이터 항목을 리트리브하기 위한 요청을 수신하고; 요청을 수신하는 것에 응답하여, 컨소시엄 블록체인으로부터 요청된 데이터 항목을 리트리브하고; 리트리브된 데이터 항목에 기초하여 제 2 데이터 요약을 생성하고; 각각의 검증 노드가 제 2 데이터 요약을 암호 방식으로 서명하고 그 서명된 제 2 데이터 요약을 반환하도록, 제 2 데이터 요약을 검증 노드들로 전송하고; 검증 노드들로부터 서명된 제 2 데이터 요약들을 수신하고; 공개 블록체인으로부터 서명된 제 1 데이터 요약들을 리트리브하고; 서명된 제 1 데이터 요약들이 수신되는 서명된 제 2 데이터 요약들과 정합하는 것으로 결정하고; 그리고 결정하는 것에 응답하여, 저장된 데이터 항목을 리트리브하기 위한 요청에 대한 응답 - 응답은 저장된 데이터 항목이 그것이 저장된 이후로 변경되지 않았다는 것을 표시함 - 을 전송하도록 하나 이상의 컴퓨터들에 의해 실행가능한 명령들로 구성된

하나 이상의 컴퓨터-판독가능 메모리들을 포함한다. 이러한 그리고 다른 구현예들은 다음의 특징들 중의 하나 이상을 각각 임의적으로 포함할 수도 있다:

- [0008] 다음의 특징들 중의 임의의 것과 조합가능한 제 1 특징으로서, 여기서, 검증 노드들은 공개 블록체인 네트워크에 참여하는 컴퓨팅 디바이스들이다.
- [0009] 다음의 특징들 중의 임의의 것과 조합가능한 제 2 특징은 스마트 계약(smart contract) - 스마트 계약은 검증 노드들로부터 요청된 서명된 제 2 데이터 요약들을 수신하는 것에 응답하여 금전적 보상(monetary reward)을 검증 노드들에 제공하도록 구성됨 - 을 공개 블록체인에 저장하는 것을 더 포함한다.
- [0010] 다음의 특징들 중의 임의의 것과 조합가능한 제 3 특징으로서, 여기서, 제 1 데이터 요약을 생성하는 것은 저장된 데이터 항목의 해시(hash)를 계산하는 것을 포함한다.
- [0011] 다음의 특징들 중의 임의의 것과 조합가능한 제 4 특징으로서, 여기서, 각각의 검증 노드는 검증 노드와 연관된 개인 키(private key)를 사용하여 제 1 데이터 요약을 암호 방식으로 서명하도록 구성된다.
- [0012] 다음의 특징들 중의 임의의 것과 조합가능한 제 5 특징으로서, 여기서, 제 1 데이터 요약을 검증 노드들로 전송하는 것은 제 1 데이터 요약을 공개 블록체인 네트워크로 브로드캐스팅(broadcasting)하는 것을 포함한다.
- [0013] 다음의 특징들 중의 임의의 것과 조합가능한 제 6 특징으로서, 여기서, 공개 블록체인으로부터 서명된 제 1 데이터 요약들을 리트리브하는 것은 저장된 데이터 항목과 연관되고 공개 블록체인에 저장된 식별자에 기초하여 서명된 제 1 데이터 요약들을 식별하는 것을 포함한다.
- [0014] 본 명세서는, 하나 이상의 프로세서들에 결합되고, 그리고 하나 이상의 프로세서들에 의해 실행될 때, 하나 이상의 프로세서들로 하여금, 본원에서 제공된 방법들의 구현예들에 따라 동작들을 수행하게 하는 명령들을 그 상에 저장한 하나 이상의 비-일시적 컴퓨터-판독가능 저장 매체들을 또한 제공한다.
- [0015] 본 명세서는 본원에서 제공된 방법들을 구현하기 위한 시스템을 추가로 제공한다. 시스템은 하나 이상의 프로세서들, 및 하나 이상의 프로세서들에 의해 실행될 때, 하나 이상의 프로세서들로 하여금, 본원에서 제공된 방법들의 구현예들에 따라 동작들을 수행하게 하는 명령들을 그 상에 저장한, 하나 이상의 프로세서들에 결합된 컴퓨터-판독가능 저장 매체를 포함한다.
- [0016] 설명된 블록체인 네트워크는 블록체인 네트워크에 저장된 데이터의 무결성(integrity)을 검증하기 위하여 이용될 수 있다. 그것은 컨센서스 프로세스에 참여할 수 있는 큰 수의 노드들을 수반함으로써, 데이터의 무결성을 보장한다. 추가적으로, 설명된 기법들은 공개 사이드체인(public sidechain)에서의 노드 참여를 증가시키기 위하여 스마트 계약들에 기초한 인센티브 메커니즘(incentive mechanism)을 제공한다.
- [0017] 본 명세서에 따른 방법들은 본원에서 설명된 양태들 및 특징들의 임의의 조합을 포함할 수도 있다는 것이 인식된다. 즉, 본 명세서에 따른 방법들은 본원에서 구체적으로 설명된 양태들 및 특징들의 조합들로 제한되는 것이 아니라, 제공된 양태들 및 특징들의 임의의 조합을 또한 포함한다.
- [0018] 본 명세서의 하나 이상의 구현예들의 세부사항들은 동반 도면들 및 이하의 설명에서 기재된다. 본 명세서의 다른 특징들 및 장점들은 설명 및 도면들로부터, 그리고 청구항들로부터 분명할 것이다.

도면의 간단한 설명

- [0019] 도 1은 본 명세서의 구현예들을 실행하기 위하여 이용될 수 있는 환경의 예를 도시한다.
- 도 2는 본 명세서의 구현예들에 따라, 개념적인 아키텍처의 예를 도시한다.
- 도 3은 본 명세서의 구현예들에 따라, 본 명세서의 구현예들을 실행하기 위하여 이용될 수 있는 시스템의 예를 도시한다.
- 도 4는 본 명세서의 양태들에 따라, 컨소시엄 블록체인 네트워크 및 연관된 공개 사이드체인 네트워크에서 데이터를 저장하는 프로세스의 예를 도시한다.
- 도 5는 본 명세서의 양태들에 따라, 컨소시엄 블록체인 네트워크로부터 데이터를 리트리브하고 공개 사이드체인 네트워크에 기초하여 리트리브된 데이터를 검증하는 프로세스의 예를 도시한다.
- 도 6은 본 명세서의 구현예들에 따라, 실행될 수 있는 프로세스의 예를 도시한다.

도 7은 명세서의 구현예들에 따라, 장치의 모듈들을 예시하는 도면의 예를 도시한다.

다양한 도면들에서의 유사한 참조 기호들은 유사한 구성요소들을 표시한다.

발명을 실시하기 위한 구체적인 내용

- [0020] 본 명세서의 구현예들은 블록체인 네트워크의 노드들과 연관된 검증되어야 할 데이터를 저장하고 리트리브하기 위한 컴퓨터-구현된 방법들을 포함한다. 더 상세하게는, 본 명세서의 구현예들은 다수의 검증 노드들을 이용하는 하나 이상의 컨소시엄 블록체인 네트워크 노드들과 연관된 검증되어야 할 데이터의 데이터 요약을 저장하는 것과, 검증되어야 할 데이터 및 저장된 데이터 요약들을 리트리브하는 것에 관한 것이다.
- [0021] 명세서의 구현예들을 위한 추가의 맥락을 제공하기 위하여, 그리고 위에서 소개된 바와 같이, (예컨대, 피어-투-피어(peer-to-peer) 노드들로 이루어진) 컨센서스 네트워크들 및 블록체인 네트워크들로서 또한 지칭될 수 있는 분산된 원장 시스템(DLS)들은 참여하는 엔티티들이 트랜잭션(transaction)들을 보안성 있게 그리고 변경할 수 없게 행하고 데이터를 저장하는 것을 가능하게 한다. 용어 블록체인은 임의의 특정한 이용의 경우를 참조하지 않으면서, DLS를 일반적으로 지칭하기 위하여 본원에서 이용된다.
- [0022] 블록체인은, 트랜잭션들이 변경될 수 없고 추후에 검증될 수 있는 방법으로 트랜잭션들을 저장하는 데이터 구조이다. 블록체인은 하나 이상의 블록들을 포함한다. 체인에서의 각각의 블록은 이전의 블록의 암호 해시(cryptographic hash)를 포함함으로써, 체인에서의 각각의 블록 직전에 이전의 블록에 링크된다. 각각의 블록은 타임스탬프(timestamp), 그 자신의 암호 해시, 및 하나 이상의 트랜잭션들을 또한 포함한다. 블록체인 네트워크의 노드들에 의해 이미 검증되었던 트랜잭션들은 해싱(hash)되고 머클 트리(Merkle tree)로 인코딩된다. 머클 트리는, 트리의 리프 노드(leaf node)들에서의 데이터가 해싱되고 트리의 각각의 가지(branch)에서의 모든 해시들이 가지의 루트(root)에서 연결(concatenate)되는 데이터 구조이다. 이 프로세스는 트리 위에서, 트리에 있는 모든 데이터를 나타내는 해시를 저장하는 전체 트리의 루트까지 계속된다. 트리에서 저장된 트랜잭션임을 의도하는 해시는 해시가 트리의 구조와 일치하는지 여부를 결정함으로써 신속하게 검증될 수 있다.
- [0023] 블록체인이 트랜잭션들을 저장하기 위한 데이터 구조이기 때문에, 블록체인 네트워크는 하나 이상의 블록체인들을 관리하고, 업데이트하고, 유지하는 컴퓨팅 노드들의 네트워크이다. 위에서 소개된 바와 같이, 블록체인 네트워크는 공개 블록체인 네트워크, 사적 블록체인 네트워크, 또는 컨소시엄 블록체인 네트워크로서 제공될 수 있다.
- [0024] 공개 블록체인 네트워크에서, 컨센서스 프로세스는 컨센서스 네트워크의 노드들에 의해 제어된다. 예를 들어, 수백, 수천, 심지어 수백만 개의 엔티티들은 공개 블록체인 네트워크와 협력할 수 있고, 엔티티들의 각각은 공개 블록체인 네트워크에서의 적어도 하나의 노드를 동작시킨다. 따라서, 공개 블록체인 네트워크는 참여하는 엔티티들에 대한 공개 네트워크로 고려될 수 있다. 일부 예들에서, 대다수의 엔티티들(노드들)은 블록이 유효하도록 하고 블록체인 네트워크의 블록체인(분산된 원장)에 추가되도록 하기 위하여 매 블록을 서명해야 한다. 일 예의 공개 블록체인 네트워크들은 블록체인으로서 지칭된 분산된 원장을 활용하는 특정한 피어-투-피어 지분 네트워크들을 포함한다. 위에서 언급된 바와 같이, 그러나, 용어 블록체인은 임의의 특정한 블록체인 네트워크를 특히 참조하지 않으면서, 분산된 원장들을 일반적으로 지칭하기 위하여 이용된다.
- [0025] 일반적으로, 공개 블록체인 네트워크는 공개 트랜잭션들을 지원한다. 공개 트랜잭션은 공개 블록체인 네트워크 내의 노드들의 전부와 공유되고, 글로벌 블록체인(global blockchain)에서 저장된다. 글로벌 블록체인은 모든 노드들에 걸쳐 복제(replicate)되는 블록체인이다. 즉, 모든 노드들은 글로벌 블록체인에 대한 완벽한 상태 컨센서스(state consensus)에 있다. 컨센서스(예컨대, 블록체인으로의 블록의 추가에 대한 협정)를 달성하기 위하여, 컨센서스 프로토콜은 공개 블록체인 네트워크 내에서 구현된다. 컨센서스 프로토콜들의 예들은 작업-증명(proof-of-work; POW), 지분-증명(proof-of-stake; POS), 및 권위-증명(proof-of-authority; POA)을 제한 없이 포함한다. POW는 비-제한적인 예로서 본원에서 추가로 참조된다.
- [0026] 일반적으로, 사적 블록체인 네트워크는 판독 및 기입 허가들을 중앙 제어하는 특정한 엔티티를 위하여 제공된다. 엔티티는 어느 노드들이 블록체인 네트워크에 참여할 수 있는지를 제어한다. 결과적으로, 사적 블록체인 네트워크들은 누가 네트워크에 참여하도록 허용되는지와, (예컨대, 오직 어떤 트랜잭션들에서의) 그 참여의 레벨에 대해 한정들을 설정하는 허가된 네트워크들로서 일반적으로 지칭된다. 다양한 유형들의 액세스 제어 메커니즘들이 이용될 수 있다(예컨대, 현존하는 참여자들은 새로운 엔티티들을 추가하는 것에 투표하고, 규제 기관은 승인을 제어할 수 있음).

- [0027] 일반적으로, 컨소시엄 블록체인 네트워크는 참여하는 엔티티들 사이에서 사적이다. 컨소시엄 블록체인 네트워크에서, 컨센서스 프로세스는 노드들의 인가된 세트에 의해 제어되고, 하나 이상의 노드들은 개개의 엔티티(예컨대, 금융 기관(financial institution), 보험 회사(insurance company))에 의해 동작된다. 예를 들어, 10개(10)의 엔티티들(예컨대, 금융 기관들, 보험 회사들)의 컨소시엄은 컨소시엄 블록체인 네트워크를 동작시킬 수 있고, 엔티티들의 각각은 컨소시엄 블록체인 네트워크에서의 적어도 하나의 노드를 동작시킨다. 따라서, 컨소시엄 블록체인 네트워크는 참여하는 엔티티들에 대한 사적 네트워크로 고려될 수 있다. 일부 예들에서, 각각의 엔티티(노드)는 블록이 유효하도록 하고 블록체인에 추가되도록 하기 위하여 매 블록을 서명해야 한다. 일부 예들에서, 엔티티들(노드들)의 적어도 서브-세트(sub-set)(예컨대, 적어도 7 개의 엔티티들)는 블록이 유효하도록 하고 블록체인에 추가되도록 하기 위하여 매 블록을 서명해야 한다.
- [0028] 블록체인은 공개 또는 사적 피어-투-피어 네트워크에서의 트랜잭션들을 레코딩하는 탬퍼-방지(tamper-proof) 공유된 디지털 원장이다. 원장(ledger)은 네트워크에서의 모든 멤버 노드(member node)들로 분산되고, 네트워크에서 발생하는 자산 트랜잭션(asset transaction)들의 이력은 블록에서 영구적으로 레코딩된다. 트랜잭션에 참여하기 이전에, 블록체인 상의 노드는 다양한 기법들을 이용하여 연산들을 실행하는 것을 필요로 할 수도 있다. 현재의 해결책들 하에서는, 각각의 블록체인이 독립적이므로, 하나의 블록체인의 노드는 다른 체인들과 통신할 수 없다. 예를 들어, 노드는 다른 블록체인들로부터 데이터를 판독할 수 없거나, 다른 블록체인들과 데이터를 교환할 수 없다. 추가적으로, 노드가 연산을 실행하기 위하여 다른 블록체인들로부터의 데이터를 필요로 하지 않더라도, 완전히 블록체인 상에서 이러한 연산들을 수행하는 것은 그것이 복잡한 연산 로직들 및 프로토콜들을 요구할 경우에, 많은 시간 및 블록체인의 연산 자원들을 소비할 수 있다.
- [0029] 명세서의 구현예들은 참여하는 엔티티들 사이에서 공개적인 컨소시엄 블록체인 네트워크를 참조하여 본원에서 더 상세하게 설명된다. 그러나, 명세서의 구현예들은 임의의 적절한 유형의 블록체인 네트워크에서 실현될 수 있다는 것이 고려된다.
- [0030] 명세서의 구현예들은 위의 맥락을 감안하여 본원에서 더 상세하게 설명된다. 더 상세하게는, 그리고 위에서 소개된 바와 같이, 명세서의 구현예들은 신뢰된 실행 환경에서 교차-체인 데이터를 동작시킬 수 있는 오프-체인 스마트 계약 서비스를 제공하는 것에 관한 것이다.
- [0031] 구체적으로, 설명된 기법들은 컨소시엄 블록체인에서 저장된 데이터의 무결성을 검증하기 위하여 이용되는 공개 보조 블록체인(public auxiliary blockchain)("사이드체인"으로서 또한 지칭됨)을 소개한다. 사이드체인은 공개적이므로, 큰 수의 노드들이 컨센서스 프로세스에 참여할 수 있음으로써, 사이드체인에서의 데이터의 무결성을 보장할 수 있다. 컨소시엄 블록체인 상에서의 각각의 트랜잭션의 표현은 사이드체인에서 저장된다. 이에 따라, 컨소시엄 블록체인에서의 데이터를 변경하기 위하여, 공격자는 또한, 공개 사이드체인에 대한 대응하는 변경을 행해야 한다. 공개 사이드체인에서 이러한 변경을 행하는 것은 공개 사이드체인에 대한 컨센서스 프로세스에서 수반된 노드들의 수로 인해, 컨소시엄 블록체인에서보다 훨씬 더 어려울 것이다. 이러한 방법으로, 컨소시엄 블록체인에서의 데이터의 무결성은 보장될 수도 있다. 추가적으로, 설명된 기법들은 공개 사이드체인에서의 노드 참여를 증가시키기 위하여 스마트 계약들에 기초한 인센티브 메커니즘을 제공한다. 스마트 계약은 정보적 방식으로 계약들을 유효시키거나, 검증하거나, 집행하도록 설계된 컴퓨터 협정일 수 있다. 스마트 계약들은 신뢰된 트랜잭션들이 제 3 자 개입(third-party involvement) 없이 수행되는 것을 허용한다. 이 트랜잭션들은 추적가능하고 비가역적이다.
- [0032] 설명된 기법들은 다양한 애플리케이션들을 가질 수 있다. 예를 들어, 저작권 침해 소송(copyright infringement litigation) 동안에, 원고(plaintiff)는 그녀가 원래의 작품을 창작한 정확한 시간을 도시하기 위하여 일부 유형의 디지털 증거를 법원에 제공하는 것을 필요로 한다. 원고에 의해 제출된 디지털 증거가 컨소시엄 블록체인에서 원래 저장될 경우에, 법원은 디지털 증거가 탬퍼링되지 않은 것으로 결정할 수 없으므로, 디지털 증거는 요구된 증명의 부담을 충족시킬 수 없을 수도 있다. 법원에 의해 수용될 증거에 입각한 레코드(evidentiary record)를 확립하기 위하여, 원고는 검증 시스템을 통해 설명된 기법들을 이용하여 데이터 증거를 저장할 수 있다. 증거 제출 시에, 원고는 검증 노드들에 의해 제출된 디지털 증거의 복사본들과 함께, 컨소시엄 블록체인에서 저장된 디지털 증거를 제출할 수 있다. 이러한 방법으로, 큰 수의 검증 노드들이 디지털 증거의 진본성(authenticity)을 입증하고 있으므로, 법원은 디지털 증거의 진본성을 인식할 가능성이 더 많을 것이다.
- [0033] 위에서 논의된 예를 제외하고도, 설명된 기법들은 블록체인 기술을 이용하는 많은 다른 애플리케이션들에 유익할 수 있다.

- [0034] 도 1은 명세서의 구현예들을 실행하기 위하여 이용될 수 있는 환경(100)의 예를 도시한다. 일부 예들에서, 환경(100)은 엔티티들이 블록체인 네트워크(102)에 참여하는 것을 가능하게 한다. 환경(100)은 컴퓨팅 디바이스들(106, 108) 및 네트워크(110)를 포함한다. 일부 예들에서, 네트워크(110)는 로컬 영역 네트워크(local area network; LAN), 광역 네트워크(wide area network; WAN), 인터넷, 또는 그 조합을 포함하고, 웹 사이트(web site)들, 사용자 디바이스들(예컨대, 컴퓨팅 디바이스들), 및 백-엔드 시스템(back-end system)들을 접속시킨다. 일부 예들에서, 네트워크(110)는 유선 및/또는 무선 통신 링크 상에서 액세스될 수 있다. 일부 예들에서, 네트워크(110)는 블록체인 네트워크(102)와의, 그리고 블록체인 네트워크(102) 내에서의 통신을 가능하게 한다. 일반적으로, 네트워크(110)는 하나 이상의 통신 네트워크들을 표현한다. 일부 경우에는, 컴퓨팅 디바이스들(106, 108)이 클라우드 컴퓨팅 시스템(도시되지 않음)의 노드들일 수 있거나, 각각의 컴퓨팅 디바이스(106, 108)는 네트워크에 의해 상호접속된 다수의 컴퓨터들을 포함하고 분산된 프로세싱 시스템으로서 기능하는 별도의 클라우드 컴퓨팅 시스템일 수 있다.
- [0035] 도시된 예에서, 컴퓨팅 시스템들(106, 108)은 블록체인 네트워크(102)에서의 노드로서의 참여를 가능하게 하는 임의의 적절한 컴퓨팅 시스템을 각각 포함할 수 있다. 컴퓨팅 디바이스들의 예들은 서버, 데스크톱 컴퓨터, 랩톱 컴퓨터, 태블릿 컴퓨팅 디바이스, 및 스마트폰을 제한 없이 포함한다. 일부 예들에서, 컴퓨팅 시스템들(106, 108)은 블록체인 네트워크(102)와 상호작용하기 위한 하나 이상의 컴퓨터-구현된 서비스들을 호스팅(host)한다. 예를 들어, 컴퓨팅 시스템(106)은 제 1 엔티티가 하나 이상의 다른 엔티티들(예컨대, 다른 참여자들)과의 그 트랜잭션들을 관리하기 위하여 이용하는 트랜잭션 관리 시스템과 같이, 제 1 엔티티(예컨대, 참여자 A)의 컴퓨터-구현된 서비스들을 호스팅할 수 있다. 컴퓨팅 시스템(108)은 제 2 엔티티가 하나 이상의 다른 엔티티들(예컨대, 다른 참여자들)과의 그 트랜잭션들을 관리하기 위하여 이용하는 트랜잭션 관리 시스템과 같이, 제 2 엔티티(예컨대, 참여자 B)의 컴퓨터-구현된 서비스들을 호스팅할 수 있다. 도 1의 예에서, 블록체인 네트워크(102)는 노드들의 피어-투-피어 네트워크로서 표현되고, 컴퓨팅 시스템들(106, 108)은 블록체인 네트워크(102)에 참여하는 제 1 엔티티 및 제 2 엔티티의 노드들을 각각 제공한다.
- [0036] 도 2는 명세서의 구현예들에 따라, 개념적인 아키텍처(200)의 예를 도시한다. 개념적인 아키텍처(200)의 예는 참여자 A, 참여자 B, 및 참여자 C에 각각 대응하는 참여자 시스템들(202, 204, 206)을 포함한다. 각각의 참여자(예컨대, 사용자, 기업)는 다수의 노드들(214)을 포함하는 피어-투-피어 네트워크로서 제공된 블록체인 네트워크(212)에 참여하고, 다수의 노드들(214)의 적어도 일부는 블록체인(216)에서의 정보를 변경할 수 없게 레코딩한다. 단일 블록체인(216)이 블록체인 네트워크(212) 내에서 개략적으로 도시되지만, 블록체인(216)의 다수의 복사본들은 본원에서 더 상세하게 설명된 바와 같이, 블록체인 네트워크(212)에 걸쳐 제공되고 유지된다.
- [0037] 도시된 예에서, 각각의 참여자 시스템(202, 204, 206)은 각각 참여자 A, 참여자 B, 및 참여자 C에 의해, 또는 이를 대신하여 제공되고, 블록체인 네트워크 내에서 개개의 노드(214)로서 기능한다. 본원에서 이용된 바와 같이, 노드는, 블록체인 네트워크(212)에 접속되고, 개개의 참여자가 블록체인 네트워크에 참여하는 것을 가능하게 하는 개별적인 시스템(예컨대, 컴퓨터, 서버)을 일반적으로 지칭한다. 도 2의 예에서, 참여자는 각각의 노드(214)에 대응한다. 그러나, 참여자는 블록체인 네트워크(212) 내에서 다수의 노드들(214)을 동작시킬 수 있고, 및/또는 다수의 참여자들은 노드(214)를 공유할 수 있다는 것이 고려된다. 일부 예들에서, 참여자 시스템들(202, 204, 206)은 프로토콜(예컨대, 하이퍼텍스트 전송 프로토콜 보안(hypertext transfer protocol secure; HTTPS))을 이용하여, 및/또는 원격 절차 호출(remote procedure call; RPC)들을 이용하여 블록체인 네트워크(212)와 통신하거나, 또는 블록체인 네트워크(212)를 통해 통신한다.
- [0038] 노드들(214)은 블록체인 네트워크(212) 내에서 변동하는 참여도를 가질 수 있다. 예를 들어, 일부 노드들(214)은 (예컨대, 블록들을 블록체인(216)에 추가하는 마인더 노드(minder node)들로서) 컨센서스 프로세스에 참여할 수 있는 반면, 다른 노드들(214)은 컨센서스 프로세스에 참여하지 않는다. 또 다른 예로서, 일부 노드들(214)은 블록체인(216)의 완전한 복사본을 저장하는 반면, 다른 노드들(214)은 블록체인(216)의 부분들의 복사본들을 오직 저장한다. 예를 들어, 데이터 액세스 특권들은 개개의 참여자가 그 개개의 시스템 내에서 저장하는 블록체인 데이터를 제한할 수 있다. 도 2의 예에서, 참여자 시스템들(202, 204, 206)은 블록체인(216)의 개개의 완전한 복사본들(216', 216'', 216''')을 저장한다.
- [0039] 블록체인(예컨대, 도 2의 블록체인(216))은 블록들의 체인으로 이루어지고, 각각의 블록은 데이터를 저장한다. 데이터의 예들은 2 이상의 참여자들 사이의 트랜잭션을 나타내는 트랜잭션 데이터를 포함한다. 트랜잭션들은 비-제한적인 예로서 본원에서 이용되지만, 임의의 적절한 데이터가 블록체인에서 저장될 수 있다는 것(예컨대, 문서들, 이미지들, 비디오들, 오디오)이 고려된다. 트랜잭션들의 예들은 가치 있는 어떤 것(예컨대, 자산들, 제품들, 서비스들, 및 통화)의 교환들을 제한 없이 포함할 수 있다. 트랜잭션 데이터는 블록체인 내에서 변경

할 수 없게 저장된다. 즉, 트랜잭션 데이터는 변경될 수 없다.

- [0040] 블록에서 저장하기 전에, 트랜잭션 데이터는 해싱된다. 해싱은 (스트링 데이터(string data)로서 제공된) 트랜잭션 데이터를 (스트링 데이터로서 또한 제공된) 고정된-길이 해시 값으로 변환하는 프로세스이다. 트랜잭션 데이터를 획득하기 위하여 해시 값을 역-해싱(un-hash)하는 것은 가능하지 않다. 해싱은 트랜잭션 데이터에서의 사소한 변경조차도 완전히 상이한 해시 값으로 귀착된다는 것을 보장한다. 또한, 그리고 위에서 언급된 바와 같이, 해시 값은 고정된 길이이다. 즉, 트랜잭션 데이터의 크기에 관계 없이, 해시 값의 길이는 고정된다. 해싱은 해시 값을 생성하기 위한 해시 함수(hash function)를 통해 트랜잭션 데이터를 프로세싱하는 것을 포함한다. 해시 함수의 예들은 256-비트 해시 값들을 출력하는 보안 해시 알고리즘(secure hash algorithm; SHA)-256을 제한 없이 포함한다.
- [0041] 다수의 트랜잭션들의 트랜잭션 데이터는 해싱되고 블록에서 저장된다. 예를 들어, 2 개의 트랜잭션들의 해시 값들이 제공되고, 또 다른 해시를 제공하기 위하여 자체적으로 해싱된다. 이 프로세스는 블록에서 저장되어야 할 모든 트랜잭션들에 대하여, 단일 해시 값이 제공될 때까지 반복된다. 이 해시 값은 머클 루트 해시(Merkle root hash)로서 지칭되고, 블록의 헤더(header)에서 저장된다. 트랜잭션들 중의 임의의 것에서의 변경은 그 해시 값에서의 변경, 그리고 궁극적으로, 머클 루트 해시에서의 변경으로 귀착될 것이다.
- [0042] 블록들은 컨센서스 프로토콜을 통해 블록체인에 추가된다. 블록체인 네트워크 내에서의 다수의 노드들은 컨센서스 프로토콜에 참여하고, 블록체인에 추가된 블록을 가지기 위하여 경쟁한다. 이러한 노드들은 마이너(miner)들(또는 마인더 노드들)로서 지칭된다. 위에서 소개된 POW는 비-제한적인 예로서 이용된다.
- [0043] 마이너 노드들은 트랜잭션들을 블록체인에 추가하기 위하여 컨센서스 프로세스를 실행한다. 다수의 마이너 노드들이 컨센서스 프로세스에 참여하지만, 오직 하나의 마이너 노드는 블록을 블록체인에 기입할 수 있다. 즉, 마이너 노드들은 블록체인에 추가된 그 블록을 가지기 위하여 컨센서스 프로세스에서 경쟁한다. 더 상세하게, 마이너 노드는 트랜잭션 풀(transaction pool)로부터 (예컨대, 만약 있다면, 블록 내에 포함될 수 있는 트랜잭션들의 수에 대한 미리 정의된 제한에 이르기까지) 계류 중인 트랜잭션들을 주기적으로 수집한다. 트랜잭션 풀은 블록체인 네트워크에서의 참여자들로부터의 트랜잭션 메시지들을 포함한다. 마이너 노드는 블록을 구축하고, 트랜잭션들을 블록에 추가한다. 트랜잭션들을 블록에 추가하기 전에, 마이너 노드는 트랜잭션들 중의 임의의 것이 블록체인의 블록 내에 이미 포함되는지 여부를 체크한다. 트랜잭션이 이미 또 다른 블록 내에 포함될 경우에, 트랜잭션은 폐기된다.
- [0044] 마이너 노드는 블록 헤더를 생성하고, 블록에서의 트랜잭션들의 진부를 해싱하고, 단일 해시 값이 블록에서의 모든 트랜잭션들에 대하여 제공될 때까지(머클 루트 해시), 추가의 해시 값들을 생성하기 위하여 해시 값을 쌍들로 조합한다. 이 해시는 블록 헤더에 추가된다. 마이너는 또한, 블록체인에서의 가장 최근의 블록(즉, 블록체인에 추가된 최후의 블록)의 해시 값을 결정한다. 마이너 노드는 또한, 논스 값 nonce value) 및 타임스탬프를 블록 헤더에 추가한다. 마인딩 프로세스에서, 마이너 노드는 요구된 파라미터들을 충족시키는 해시 값을 발견하는 것을 시도한다. 마이너 노드는 요구된 파라미터들을 충족시키는 해시 값을 발견할 때까지, 논스 값을 변경하는 것을 계속한다.
- [0045] 블록체인 네트워크에서의 모든 마이너는 요구된 파라미터들을 충족시키는 해시 값을 발견하는 것을 시도하고, 이러한 방법으로, 서로 경쟁한다. 결국, 마이너 노드들 중의 하나는 요구된 파라미터들을 충족시키는 해시 값을 발견하고, 이것을 블록체인 네트워크에서의 모든 다른 마이너 노드들에 알린다. 다른 마이너 노드들은 해시 값을 검증하고, 올바른 것으로 결정될 경우에, 블록에서의 각각의 트랜잭션을 검증하고, 블록을 수용하고, 블록을 블록체인의 그 복사본에 첨부한다. 이러한 방식으로, 블록체인의 글로벌 상태는 블록체인 네트워크 내에서의 모든 마이너 노드들에 걸쳐 일치한다. 위에서 설명된 프로세스는 POW 컨센서스 프로토콜이다.
- [0046] 비-제한적인 예는 도 2를 참조하여 제공된다. 이 예에서, 참여자 A는 자금의 양을 참여자 B에게 전송하기를 원한다. 참여자 A는 (예컨대, From, To, 및 Value 필드들을 포함하는) 트랜잭션 메시지를 생성하고, 트랜잭션 메시지를 블록체인 네트워크로 전송하고, 블록체인 네트워크는 트랜잭션 메시지를 트랜잭션 풀에 추가한다. 블록체인 네트워크에서의 각각의 마이너 노드는 블록을 생성하고, 트랜잭션 풀로부터 (예컨대, 만약 있다면, 블록에 추가될 수 있는 트랜잭션의 수에 대한 미리 정의된 제한에 이르기까지) 모든 트랜잭션들을 취하고, 트랜잭션들을 블록에 추가한다. 이러한 방식으로, 참여자 A에 의해 발행된 트랜잭션은 마이너 노드들의 블록들에 추가된다.
- [0047] 일부 트랜잭션 네트워크들에서, 암호법은 트랜잭션들의 프라이버시를 유지하도록 구현된다. 예를 들어, 2 개의

노드들이 트랜잭션을 사적인 것으로 유지하기를 원하여, 블록체인 네트워크에서의 다른 노드들이 트랜잭션의 세부사항들을 파악할 수 없을 경우에, 노드들은 트랜잭션 데이터를 암호화할 수 있다. 암호 방법들의 예들은 대칭적 암호화 및 비대칭적 암호화를 제한 없이 포함한다. 대칭적 암호화는 (평문(plaintext)으로부터 암호문을 생성하는) 암호화 및 (암호문으로부터 평문을 생성하는) 복호화의 양자를 위하여 단일 키를 이용하는 암호화 프로세스를 지칭한다. 대칭적 암호화에서, 동일한 키는 다수의 노드들에 이용가능하므로, 각각의 노드는 트랜잭션 데이터를 암호화/복호화할 수 있다.

[0048] 비대칭적 암호화는 개인 키 및 공개 키(public key)를 각각 포함하는 키 쌍들을 사용하고, 개인 키는 개개의 노드에 오직 알려지고, 공개 키는 블록체인 네트워크에서의 임의의 또는 모든 다른 노드들에 알려진다. 노드는 데이터를 암호화하기 위하여 또 다른 노드의 공개 키를 이용할 수 있고, 암호화된 데이터는 다른 노드의 개인 키를 사용하여 복호화될 수 있다. 예를 들어, 그리고 도 2를 다시 참조하면, 참여자 A는 데이터를 암호화하고 암호화된 데이터를 참여자 B에게 전송하기 위하여 참여자 B의 공개 키를 이용할 수 있다. 참여자 B는 암호화된 데이터(암호문)를 복호화하고 원래의 데이터(평문)를 추출하기 위하여 그 개인 키를 사용할 수 있다. 노드의 공개 키로 암호화된 메시지들은 노드의 개인 키를 사용하여 오직 복호화될 수 있다.

[0049] 비대칭적 암호화는 디지털 서명들을 제공하기 위하여 이용되고, 이는 트랜잭션에서의 참여자들이 트랜잭션에서의 다른 참여자들 뿐만 아니라, 트랜잭션의 유효성(validity)을 확인하는 것을 가능하게 한다. 예를 들어, 노드는 메시지를 디지털 방식으로 서명할 수 있고, 또 다른 노드는 참여자 A의 디지털 서명에 기초하여, 메시지가 노드에 의해 전송되었다는 것을 확인할 수 있다. 디지털 서명들은 또한, 메시지들이 전송 중에 탬퍼링되지 않는다는 것을 보장하기 위하여 이용될 수 있다. 예를 들어, 그리고 도 2를 다시 참조하면, 참여자 A는 메시지를 참여자 B에게 전송한다. 참여자 A는 메시지의 해시를 생성하고, 그 다음으로, 그 개인 키를 사용하여, 디지털 서명을 암호화된 해시로서 제공하기 위하여 해시를 암호화한다. 참여자 A는 디지털 서명을 메시지에 첨부하고, 디지털 서명을 갖는 메시지를 참여자 B에게 전송한다. 참여자 B는 참여자 A의 공개 키를 이용하여 디지털 서명을 복호화하고, 해시를 추출한다. 참여자 B는 메시지를 해싱하고, 해시들을 비교한다. 해시들이 동일할 경우에, 참여자 B는 메시지가 실제로 참여자 A로부터의 것이었고, 탬퍼링되지 않았다는 것을 확인할 수 있다.

[0050] 도 3은 본 명세서의 구현예들에 따라, 본 명세서의 구현예들을 실행하기 위하여 이용될 수 있는 시스템(300)의 예를 도시한다.

[0051] 도 3에서 예시된 바와 같이, 시스템(300)은 컨소시엄 블록체인(306)을 유지하는 노드들(304a 내지 304e)을 포함하는 컨소시엄 블록체인 네트워크(302)를 포함한다. 시스템(300)은 검증 시스템(316), 인센티브 시스템(320), 및 공개 사이드체인 네트워크(352)를 포함한다. 공개 사이드체인 네트워크(352)는 복수의 검증 노드들(330), 공개 블록체인(356), 및 공개 블록체인(356)을 유지하는 공개 블록체인 노드들(예컨대, 354)을 포함한다.

[0052] 동작 시에, 컨소시엄 블록체인 네트워크(302)(즉, 노드들(304a 내지 304e))는 데이터를 저장하기 위한 요청들(360)을 수신한다. 노드들(304a 내지 304e)은 위에서 설명된 메커니즘들에 따라 데이터를 컨소시엄 블록체인(306)에서 저장한다. 검증 시스템(316)은 (362에서) 일단 저장된 데이터가 블록체인(306)에 추가되면, 저장된 데이터를 수신한다. 예를 들어, 검증 시스템은 컨소시엄 블록체인 네트워크(302)를 모니터링할 수 있고, 컨센서스가 데이터를 포함하는 체인 상의 노드들(304a 내지 304e)에 의해 도달되면, 데이터가 저장된 것으로 결정할 수 있다.

[0053] 일부 구현예들에서, 검증 시스템(316)은 컨소시엄 블록체인 네트워크(302)와 공개 사이드체인 네트워크(352) 사이의 상호작용을 담당한다. 동작 시에, 검증 시스템(316)은 (366에서) 저장된 데이터의 데이터 요약들 검증 노드들(330)로 전송한다. 일부 구현예들에서, 검증 노드들(330)은 공개 사이드체인 네트워크(352)에 참여하는 컴퓨팅 디바이스들이다. 큰 수(예컨대, 수천 개)의 검증 노드들(330)이 있을 수도 있다. 일부 경우에는, 검증 시스템(316)이 데이터 요약을 공개 사이드체인 네트워크(352)로 브로드캐스팅할 수도 있다. 검증 노드들(330)은 데이터 요약을 수신할 시에, 그 개인 키를 사용하여 데이터를 암호 방식으로 서명한다. 각각의 검증 노드는 그 다음으로, 그 서명된 데이터 요약을 공개 블록체인(356)에서 저장하는 것을 시도한다. 일부 구현예들에서, 검증 노드들(330)에 의해 생성된 모든 서명된 데이터 요약들은 공개 블록체인(356)에서 저장된다. 일부 경우에는, 어떤 수의 설명된 데이터 요약들이 공개 블록체인(356)에서 저장되고, 다른 것들은 폐기된다. 이 수는 공개 사이드체인 네트워크(352)에서 이용된 컨센서스 메커니즘들의 함수일 수 있다.

[0054] 시스템(300)은 인센티브 시스템(320)을 또한 포함할 수도 있다. 일부 구현예들에서, 인센티브 시스템(320)은 공개 블록체인(356)에서 저장되어야 할 스마트 계약을 생성할 수도 있다. 스마트 계약은 공개 사이드체인 네트워크에 의해 실행될 때, 금전적 보상을 저장된 데이터의 검증에 참여하는 검증 노드들(330)에 제공하도록 구성

될 수도 있다. 예를 들어, 공개 블록체인(356)에서 그 서명된 데이터 요약을 성공적으로 포함하는 검증 노드(330)는 스마트 계약의 실행을 통해 금전적 보상을 자동적으로 수신할 수도 있다. 일부 경우에는, 컨소시엄 블록체인(이하, 도 5 참조)으로부터 요청된 데이터의 검증에 참여하는 검증 노드(330)가 스마트 계약의 실행을 통해 금전적 보상을 자동적으로 수신할 수도 있다.

[0055] 도 4는 본 명세서의 양태들에 따라, 컨소시엄 블록체인 네트워크 및 연관된 공개 사이드체인 네트워크에서 데이터를 저장하는 일 예의 프로세스(400)를 도시한다.

[0056] 405에서, 데이터 항목은 컨소시엄 블록체인 네트워크(302)에서 저장된다. 410에서, 검증 시스템(316)은 네트워크에 참여하는 노드들과 통신하는 것에 의한 것과 같이, 컨소시엄 블록체인 네트워크(302)로부터 새롭게 저장된 데이터를 수신한다. 415에서, 검증 시스템(316)은 새롭게 저장된 데이터 항목의 데이터 요약을 생성한다. 예를 들어, 검증 시스템(316)은 예를 들어, 보안 해시 알고리즘(Secure Hash Algorithm) 1(SHA-1), SHA-256, 리베스트-샤미르-애들만(Rivest-Shamir-Adleman; RSA), 또는 다른 알려진 알고리즘들과 같은 해싱 알고리즘(hashing algorithm)을 이용하여 저장된 데이터 항목의 해시를 생성함으로써 데이터 요약을 생성할 수도 있다.

[0057] 420에서, 검증 시스템(316)은 검증 노드들(330)에 의한 데이터 요약의 검증을 요청한다. 이에 응답하여, 425에서, 검증 노드들(330)은 그 개인 키들을 사용하여 데이터 요약을 암호 방식으로 서명한다. 430에서, 검증 노드들(330)은 그 개별적인 서명된 데이터 요약들을 공개 사이드체인 네트워크(352)에 의해 관리된 공개 블록체인(356)에서 저장한다. 위에서 설명된 바와 같이, 일부 구현예들에서, 오직 어떤 수의 데이터 요약들은 공개 사이드체인 네트워크(352)에 의해 채용된 컨센서스 메커니즘들에 따라 공개 블록체인(356)에서 저장될 것이다.

[0058] 도 5는 컨소시엄 블록체인 네트워크(302)로부터 데이터를 리트리브하고, 공개 사이드체인 네트워크(352)에 기초하여 리트리브된 데이터를 검증하는 일 예의 프로세스를 도시한다. 505에서, 데이터를 리트리브하기 위한 요청은 컨소시엄 블록체인 네트워크(302)에 의해(즉, 컨소시엄 블록체인 네트워크에 참여하는 노드에 의해) 수신된다. 일부 구현예들에서, 이 요청은 검증 시스템(316)에 의해 수신될 수도 있다.

[0059] 510에서, 검증 시스템(316)은 컨소시엄 블록체인(306)의 컨센서스 버전으로부터 요청된 데이터를 획득하는 것에 의한 것과 같이, 컨소시엄 블록체인 네트워크(302)로부터 요청된 데이터를 리트리브한다. 515에서, 검증 시스템(316)은 공개 사이드체인 네트워크(352)로부터, 요청된 데이터와 연관된 서명된 데이터 요약들을 리트리브한다. 일부 경우에는, 서명된 요약들이 검증 노드들(330)에 의한 서명된 데이터 요약들과 함께, 공개 블록체인(356)에서 저장된 타임스탬프 또는 다른 식별자와 같은, 저장된 데이터와 연관된 식별자에 기초하여 리트리브될 수도 있다.

[0060] 520에서, 검증 시스템(316)은 검증 노드들(330)로부터 리트리브된 데이터의 서명된 데이터 요약을 요청한다. 검증 시스템(316)은 위에서 설명된 해싱 알고리즘들을 이용하여 리트리브된 데이터의 데이터 요약을 생성할 수도 있다. 525에서, 검증 시스템(316)은 검증 노드들(330)이 리트리브된 데이터의 데이터 요약을 암호 방식으로 각각 서명할 수 있고, 530에서, 데이터 요약의 그 서명된 버전을 검증 시스템(316)으로 반환할 수 있도록, 데이터 요약들을 검증 노드들(330)로 전송한다.

[0061] 535에서, 검증 시스템(316)은 검증 노드들(330)로부터 수신된 리트리브된 데이터의 서명된 데이터 요약들을 (도 4 참조, 데이터가 컨소시엄 블록체인 네트워크에서 원래 저장되었을 때에 생성되었던) 공개 블록체인(356)으로부터 리트리브된 서명된 데이터 요약들과 비교한다. 검증 노드들(330)로부터 수신된 리트리브된 데이터의 서명된 데이터 요약들이 공개 블록체인(356)으로부터 리트리브된 서명된 데이터 요약들과 정합할 경우에, 컨소시엄 블록체인 네트워크(302)에서의 저장된 데이터는 그것이 원래 저장된 이후로 변경되지 않았다(540).

[0062] 이 프로세스는 요청된 데이터가 변경되지 않았을 경우에, 검증 노드들(330)에 의해 생성된 리트리브된 데이터의 서명된 데이터 요약들의 값이 데이터가 원래 저장되었을 때에 생성되었던 이전에 저장된 데이터 서명들과 정합할 것이므로, 요청된 데이터가 변경되지 않았다는 것을 검증한다. 데이터가 컨소시엄 블록체인에서 저장된 후에 변경되었을 경우에, 리트리브된 데이터의 서명된 데이터 요약들은 데이터가 원래 저장되었을 때에 공개 블록체인(356)에서 저장되었던 것들과 정합하지 않을 것이다.

[0063] 일부 경우에는, 검증 시스템(316)이 그 서명된 데이터 요약들을 공개 블록체인(356)으로 성공적으로 삽입하였던 검증 노드들로부터, 520에서, 서명된 데이터 요약들을 오직 요청할 수도 있다. 예를 들어, 검증 노드들(330)은 데이터 요약과 함께, 특정한 노드를 식별하는 고유한 식별자(예컨대, 공개 키)를 저장하는 것을 각각 시도할 수 있다. 공개 블록체인(356)의 컨센서스 버전 내에 포함되는 엔트리(entry)들만이 이에 따라 질의(query)될 것이다.

- [0064] 일부 경우에는, 검증 시스템(316)이 데이터를 컨소시엄 블록체인(306)에 저장할 때, 검증 노드들(330)의 특정한 세트로부터의 검증을 오직 요청할 수도 있다. 이러한 경우에는, 검증 시스템(316)이 컨소시엄 블록체인(306)으로부터의 리트리브된 데이터가 변경되지 않았다는 것을 검증할 때, 서명된 데이터 요약들에 대하여 노드들의 특정한 세트에 오직 질의할 수도 있다.
- [0065] 도 6은 본 명세서의 구현예들에 따라, 실행될 수 있는 프로세스(600)의 예를 도시한다. 일부 구현예들에서, 프로세스(600)의 예는 하나 이상의 컴퓨팅 디바이스들을 이용하여 실행된 하나 이상의 컴퓨터-실행가능 프로그램들을 이용하여 수행될 수도 있다. 제시의 명확함을 위하여, 뒤따르는 설명은 이 설명에서의 다른 도면들의 맥락에서 프로세스(600)를 일반적으로 설명한다. 그러나, 프로세스(600)는 예를 들어, 임의의 적당한 시스템, 환경, 소프트웨어, 및 하드웨어, 또는 시스템들, 환경들, 소프트웨어, 및 하드웨어의 조합에 의해 적절한 바와 같이 수행될 수도 있다는 것이 이해될 것이다. 일부 구현예들에서, 프로세스(600)의 다양한 단계들은 병렬로, 조합하여, 루프(loop)들로, 또는 임의의 순서로 작동될 수 있다.
- [0066] 602에서, 데이터 항목은 컨소시엄 블록체인 네트워크에 의해 유지된 컨소시엄 블록체인에서 저장된다.
- [0067] 604에서, 제 1 데이터 요약은 저장된 데이터 항목에 기초하여 생성된다.
- [0068] 606에서, 각각의 검증 노드가 제 1 데이터 요약을 암호 방식으로 서명하고, 그 서명된 제 1 데이터 요약을 공개 블록체인 네트워크에 의해 유지된 공개 블록체인에서 저장하도록, 제 1 데이터 요약은 검증 노드들로 전송된다. 일부 구현예들에서, 검증 노드들은 공개 블록체인 네트워크에 참여하는 컴퓨팅 디바이스들이다. 일부 구현예들에서, 각각의 검증 노드는 그 검증 노드와 연관된 개인 키를 사용하여 제 1 데이터 요약을 암호 방식으로 서명하도록 구성된다. 일부 구현예들에서, 제 1 데이터 요약을 검증 노드들로 전송하는 것은 제 1 데이터 요약을 공개 블록체인 네트워크로 브로드캐스팅하는 것을 포함한다.
- [0069] 608에서, 요청은 저장된 데이터 항목을 리트리브하기 위하여 수신된다.
- [0070] 610에서, 요청을 수신하는 것에 응답하여, 요청된 데이터 항목은 컨소시엄 블록체인으로 부터 리트리브된다.
- [0071] 612에서, 제 2 데이터 요약은 리트리브된 데이터 항목에 기초하여 생성된다. 일부 구현예들에서, 제 1 데이터 요약을 생성하는 것은 저장된 데이터 항목의 해시를 계산하는 것을 포함한다.
- [0072] 614에서, 제 2 데이터 요약은 각각의 검증 노드가 제 2 데이터 요약들을 암호 방식으로 서명할 수 있고 그 서명된 제 2 데이터 요약을 반환할 수 있도록, 검증 노드들로 전송된다.
- [0073] 616에서, 서명된 제 2 데이터 요약들은 검증 노드들로부터 수신된다.
- [0074] 618에서, 서명된 제 1 데이터 요약들은 공개 블록체인으로 부터 리트리브된다. 일부 구현예들에서, 공개 블록체인으로 부터 서명된 제 1 데이터 요약들을 리트리브하는 것은 저장된 데이터 항목과 연관되고 공개 블록체인에서 저장된 식별자에 기초하여 서명된 제 1 데이터 요약들을 식별하는 것을 포함한다.
- [0075] 620에서는, 서명된 제 1 데이터 요약들이 서명된 제 2 데이터 요약들과 정합하는 것으로 결정된다.
- [0076] 622에서는, 결정하는 것에 응답하여, 응답은 저장된 데이터 항목을 리트리브하기 위하여 전송되고, 응답은 저장된 데이터 항목이 그것이 저장된 이후로 변경되지 않았다는 것을 표시한다.
- [0077] 일부 구현예들에서, 프로세스(600)는 스마트 계약을 공개 블록체인에서 저장하는 것을 더 포함하고, 여기서, 스마트 계약은 검증 노드들로부터 요청된 서명된 제 2 데이터 요약들을 수신하는 것에 응답하여 금전적 보상을 검증 노드들에 제공하도록 구성된다.
- [0078] 도 7을 참조하면, 도 7은 명세서의 구현예들에 따라, 장치(700)의 모듈들을 예시하는 도면의 예를 도시한다. 장치(700)는 블록체인 네트워크의 노드들과 연관된 검증되어야 할 데이터를 저장하고 리트리브하기 위한 일 예의 구현예일 수 있다. 장치(700)는 도 3 내지 도 5에서 도시된 구현예에 대응할 수 있고, 장치(700)는 다음: 데이터 항목을 컨소시엄 블록체인 네트워크에 의해 유지된 컨소시엄 블록체인에서 저장하도록 구성된 스토리지(storage) 또는 저장 유닛(705); 저장된 데이터 항목에 기초하여 제 1 데이터 요약을 생성하도록 구성된 제 1 생성기 또는 생성 유닛(710); 제 1 데이터 요약을 검증 노드들 - 각각의 검증 노드는 그 제 1 데이터 요약을 암호 방식으로 서명하고, 그 서명된 제 1 데이터 요약을 공개 블록체인 네트워크에 의해 유지된 공개 블록체인에서 저장하도록 구성된 - 로 전송하도록 구성된 제 1 송신기 또는 송신 유닛(715); 저장된 데이터 항목을 리트리브하기 위한 요청을 수신하도록 구성된 수신기 또는 수신 유닛(720); 요청을 수신하는 것에 응답하여 컨소시엄 블록체인으로 부터 요청된 데이터 항목을 리트리브하도록 구성된 제 1 리트리브 유닛(725); 리트리브된 데이터

항목에 기초하여 제 2 데이터 요약을 생성하도록 구성된 제 2 생성기 또는 생성 유닛(730); 검증 노드들로부터 요청된 서명된 제 2 데이터 요약들을 수신하는 것에 응답하여 검증 노드들로부터 배정된 제 2 데이터 요약들을 요청하도록 구성된 요청기 또는 요청 유닛(735); 공개 블록체인으로부터 서명된 제 1 데이터 요약들을 리트리브하도록 구성된 제 2 리트리브 유닛(740); 공개 블록체인으로부터의 서명된 제 1 데이터 요약들이 검증 노드들로부터 수신된 서명된 제 2 데이터 요약들과 정합하는 것으로 결정하도록 구성된 결정 유닛(745); 결정하는 것에 응답하여 저장된 데이터 항목을 포함하는 저장된 데이터를 리트리브하기 위한 요청에 대한 응답 - 응답은 저장된 데이터 항목이 그것이 저장된 이후로 변경되지 않았다는 것을 표시함 - 을 전송하도록 구성된 제 2 송신기 또는 송신 유닛(750)을 포함한다.

- [0079] 임의적인 구현예에서, 검증 노드들은 공개 블록체인 네트워크에 참여하는 컴퓨팅 디바이스들이다.
- [0080] 임의적인 구현예에서, 장치(700)는 다음: 스마트 계약 - 스마트 계약은 검증 노드들로부터 요청된 서명된 제 2 데이터 요약들을 수신하는 것에 응답하여 금전적 보상을 검증 노드들에 제공하도록 구성됨 - 을 공개 블록체인에서 저장하도록 구성된 스토리지 또는 저장 서브-유닛(sub-unit)을 더 포함한다.
- [0081] 임의적인 구현예에서, 장치(700)는 다음: 저장된 데이터 항목의 해시를 계산하도록 구성된 계산기 또는 계산 서브-유닛을 더 포함한다.
- [0082] 임의적인 구현예에서, 각각의 검증 노드는 그 검증 노드와 연관된 개인 키를 사용하여 제 1 데이터 요약을 암호 방식으로 서명하도록 구성된다.
- [0083] 임의적인 구현예에서, 장치(700)는 다음: 제 1 데이터 요약을 공개 블록체인 네트워크로 브로드캐스팅하도록 구성된 브로드캐스팅 서브-유닛을 더 포함한다.
- [0084] 임의적인 구현예에서, 장치(700)는 다음: 저장된 데이터 항목과 연관되고 공개 블록체인에서 저장된 식별자에 기초하여 서명된 제 1 데이터 요약들을 식별하도록 구성된 식별기 또는 식별 서브-유닛을 더 포함한다.
- [0085] 이전의 구현예들에서 예시된 시스템, 장치, 모듈, 또는 유닛은 컴퓨터 칩 또는 엔티티를 이용함으로써 구현될 수 있거나, 어떤 기능을 가지는 제품을 이용함으로써 구현될 수 있다. 전형적인 구현예의 디바이스는 컴퓨터이고, 컴퓨터는 개인용 컴퓨터, 랩톱 컴퓨터, 셀룰러 전화, 카메라 전화, 스마트폰, 개인 정보 단말(personal digital assistant), 미디어 플레이어(media player), 내비게이션 디바이스, 이메일 수신 및 전송 디바이스, 게임 콘솔(game console), 태블릿 컴퓨터, 웨어러블 디바이스, 또는 이 디바이스들의 임의의 조합일 수 있다.
- [0086] 장치에서의 각각의 유닛의 기능들 및 역할들의 구현 프로세스에 대하여, 이전의 방법에서의 대응하는 단계들의 구현 프로세스에 대해 참조들이 행해질 수 있다. 세부사항들은 간략화를 위하여 여기에서 생략된다.
- [0087] 장치 구현예는 방법 구현예에 기본적으로 대응하므로, 관련된 부분들에 대하여, 방법 구현예에서의 관련된 설명들에 대해 참조들이 행해질 수 있다. 이전에 설명된 장치 구현예는 단지 예이다. 별도의 부분들로서 설명된 유닛들은 물리적으로 별도일 수도 있거나 아닐 수도 있고, 유닛들로서 디스플레이된 부분들은 물리적 유닛들일 수도 있거나 아닐 수도 있거나, 하나의 포지션에서 위치될 수도 있거나, 다수의 네트워크 유닛들 상에서 분산될 수도 있다. 모듈들의 일부 또는 전부는 명세서의 해결책들의 목적들을 달성하기 위하여 실제적인 요구들에 기초하여 선택될 수 있다. 당해 분야의 당업자는 창조적인 노력들 없이 본 출원의 구현예들을 이해할 수 있고 구현할 수 있다.
- [0088] 도 7은 컨소시엄 블록체인 네트워크 장치의 내부 기능적 모듈 및 구조를 예시하는 개략도이다. 실행 본체는 본질적으로 전자 디바이스일 수 있고, 전자 디바이스는 다음: 하나 이상의 프로세서들; 및 하나 이상의 프로세서들의 실행가능 명령을 저장하도록 구성된 메모리를 포함한다.
- [0089] 하나 이상의 프로세서들은 데이터 항목을 컨소시엄 블록체인 네트워크에 의해 유지된 컨소시엄 블록체인에서 저장하고; 저장된 데이터 항목에 기초하여 제 1 데이터 요약을 생성하고; 제 1 데이터 요약을 검증 노드들 - 각각의 검증 노드는 제 1 데이터 요약을 암호 방식으로 서명하고, 그 서명된 제 1 데이터 요약을 공개 블록체인 네트워크에 의해 유지된 공개 블록체인에서 저장하도록 구성됨 - 로 전송하고; 저장된 데이터 항목을 리트리브하기 위한 요청을 수신하고; 요청을 수신하는 것에 응답하여, 컨소시엄 블록체인으로부터 요청된 데이터 항목을 리트리브하고; 리트리브된 데이터 항목에 기초하여 제 2 데이터 요약을 생성하고; 노드들로부터 요청된 서명된 제 2 데이터 요약들을 수신하는 것에 응답하여 검증 노드들로부터 서명된 제 2 데이터 요약들을 요청하고; 공개 블록체인으로부터 서명된 제 1 데이터 요약들을 리트리브하고; 공개 블록체인으로부터의 서명된 제 1 데이터 요약들이 검증 노드들로부터 수신된 서명된 제 2 데이터 요약들과 정합하는 것으로 결정하고; 그리고 결정하는 것

에 응답하여, 저장된 데이터 항목을 포함하는 저장된 데이터를 리트리브하기 위한 요청에 대한 응답 - 응답은 저장된 데이터 항목이 그것이 저장된 이후로 변경되지 않았다는 것을 표시함 - 을 전송하도록 구성된다.

- [0090] 임의적으로, 검증 노드들은 공개 블록체인 네트워크에 참여하는 컴퓨팅 디바이스들이다.
- [0091] 임의적으로, 하나 이상의 프로세서들은 스마트 계약을 공개 블록체인에서 저장하도록 구성되고, 여기서, 스마트 계약은 검증 노드들로부터 요청된 서명된 제 2 데이터 요약들을 수신하는 것에 응답하여 금전적 보상을 검증 노드들에 제공하도록 구성된다.
- [0092] 임의적으로, 하나 이상의 프로세서들은 저장된 데이터 항목의 해시를 계산하도록 구성된다.
- [0093] 임의적으로, 각각의 검증 노드는 그 검증 노드와 연관된 개인 키를 사용하여 제 1 데이터 요약을 암호 방식으로 서명하도록 구성된다.
- [0094] 임의적으로, 하나 이상의 프로세서들은 제 1 데이터 요약을 공개 블록체인 네트워크로 브로드캐스팅하도록 구성된다.
- [0095] 임의적으로, 하나 이상의 프로세서들은 저장된 데이터 항목과 연관되고 공개 블록체인에서 저장된 식별자에 기초하여 서명된 제 1 데이터 요약들을 식별하도록 구성된다.
- [0096] 이 명세서에서 설명된 발명 요지 및 액션들 및 동작들의 구현예들은 디지털 전자 회로부로, 유형적으로-구체화된 컴퓨터 소프트웨어 또는 펌웨어로, 이 명세서에서 개시된 구조들 및 그 구조적 등가물들을 포함하는 컴퓨터 하드웨어로, 또는 이들 중의 하나 이상의 조합들로 구현될 수 있다. 이 명세서에서 설명된 발명 요지의 구현예들은 하나 이상의 컴퓨터 프로그램들, 예컨대, 데이터 프로세싱 장치에 의한 실행을 위하여, 또는 데이터 프로세싱 장치의 동작을 제어하기 위하여, 컴퓨터 프로그램 캐리어(computer program carrier) 상에서 인코딩된 컴퓨터 프로그램 명령들의 하나 이상의 모듈들로서 구현될 수 있다. 캐리어는 유형의 비-일시적 컴퓨터 저장 매체일 수도 있다. 대안적으로 또는 추가적으로, 캐리어는 인공적으로 생성된 전파된 신호, 예컨대, 데이터 프로세싱 장치에 의한 실행을 위하여 적당한 수신기 장치로의 송신을 위한 정보를 인코딩하기 위하여 생성되는 머신-생성된 전기적, 광학적, 또는 전자기적 신호일 수도 있다. 컴퓨터 저장 매체는 컴퓨터-판독가능 저장 디바이스, 머신-판독가능 저장 기관, 랜덤 또는 직렬 액세스 메모리 디바이스, 또는 이들 중의 하나 이상의 조합일 수 있거나, 그 일부일 수 있다. 컴퓨터 저장 매체는 전파된 신호가 아니다.
- [0097] 용어 "데이터 프로세싱 장치"는 프로그래밍가능 프로세서, 컴퓨터, 또는 다수의 프로세서들 또는 컴퓨터들을 예로서 포함하는, 데이터를 프로세싱하기 위한 모든 종류의 장치, 디바이스들, 및 머신들을 망라한다. 데이터 프로세싱 장치는 특수-목적 로직 회로부, 예컨대, FPGA(field programmable gate array; 필드 프로그래밍가능 게이트 어레이), ASIC(application specific integrated circuit; 애플리케이션 특정 집적 회로), 또는 GPU(graphics processing unit; 그래픽 프로세싱 유닛)를 포함할 수 있다. 장치는 또한, 하드웨어에 추가적으로, 컴퓨터 프로그램들을 위한 실행 환경을 생성하는 코드, 예컨대, 프로세서 펌웨어, 프로토콜 스택, 데이터베이스 관리 시스템, 오퍼레이팅 시스템, 또는 이들 중의 하나 이상의 조합을 구성하는 코드를 포함할 수 있다.
- [0098] 프로그램, 소프트웨어, 소프트웨어 애플리케이션, 앱(app), 모듈, 소프트웨어 모듈, 엔진, 스크립트, 또는 코드로서 또한 지칭될 수도 있거나 설명될 수도 있는 컴퓨터 프로그램은 컴파일링된 또는 해독된 언어들, 또는 선언적 또는 절차적 언어들을 포함하는 임의의 형태의 프로그래밍 언어로 기입될 수 있고; 컴퓨터 프로그램은 단독형 프로그램 또는 모듈로서, 컴포넌트, 엔진, 서브루틴, 또는 그 환경이 하나 이상의 위치들에서 데이터 통신 네트워크에 의해 상호접속된 하나 이상의 컴퓨터들을 포함할 수도 있는 컴퓨팅 환경에서 실행하기 위하여 적당한 다른 유닛을 포함하는 임의의 형태로 전개될 수 있다.
- [0099] 컴퓨터 프로그램은 파일 시스템에서의 파일에 대응할 필요는 없지만, 파일 시스템에서의 파일에 대응할 수도 있다. 컴퓨터 프로그램은 다른 프로그램들 또는 데이터, 예컨대, 마크업 언어 문서에서 저장된 하나 이상의 스크립트들을 유지하는 파일의 부분에서, 논의 중인 프로그램에 전용인 단일 파일에서, 또는 다수의 조정된 파일들, 예컨대, 하나 이상의 모듈들, 서브 프로그램들, 또는 코드의 부분들을 저장하는 파일들에서 저장될 수 있다.
- [0100] 이 명세서에서 설명된 프로세스들 및 로직 흐름들은 입력 데이터에 대해 동작함으로써 그리고 출력을 생성함으로써, 동작들을 수행하기 위한 하나 이상의 컴퓨터 프로그램들을 실행하는 하나 이상의 컴퓨터들에 의해 수행될 수 있다. 프로세스들 및 로직 흐름들은 또한, 특수-목적 로직 회로부, 예컨대, FPGA, ASIC, 또는 GPU에 의해, 또는 특수-목적 로직 회로부 및 하나 이상의 프로그래밍된 컴퓨터들의 조합에 의해 수행될 수 있다.
- [0101] 컴퓨터 프로그램의 실행을 위하여 적당한 컴퓨터들은 일반 또는 특수-목적 마이크로프로세서들 또는 양, 또는

임의의 다른 종류의 중앙 프로세싱 유닛에 기초할 수 있다. 일반적으로, 중앙 프로세싱 유닛은 판독 전용 메모리 또는 랜덤 액세스 메모리 또는 양자로부터 명령들 및 데이터를 수신할 것이다. 컴퓨터의 엘리먼트들은 명령들을 실행하기 위한 중앙 프로세싱 유닛, 및 명령들 및 데이터를 저장하기 위한 하나 이상의 메모리 디바이스들을 포함할 수 있다. 중앙 프로세싱 유닛 및 메모리는 특수-목적 로직 회로부에 의해 보충될 수 있거나, 특수-목적 로직 회로부 내에 편입될 수 있다.

[0102] 일반적으로, 컴퓨터는 적어도 하나의 비-일시적 컴퓨터-판독가능 저장 매체(컴퓨터-판독가능 메모리로서 또한 지칭됨)에 결합될 것이다. 컴퓨터에 결합된 저장 매체는 컴퓨터의 내부 컴포넌트(예컨대, 통합된 하드 드라이브) 또는 외부 컴포넌트(예컨대, 유니버설 직렬 버스(universal serial bus; USB) 하드 드라이브 또는 네트워크 상에서 액세스된 저장 시스템)일 수 있다. 저장 매체들의 예들은 예를 들어, 자기적, 자기 광학적, 또는 광학적 디스크들, 솔리드 스테이트 드라이브(solid state drive)들, 클라우드 저장 시스템들과 같은 네트워크 저장 자원들, 또는 다른 유형들의 저장 매체들을 포함할 수 있다. 그러나, 컴퓨터는 이러한 디바이스들을 가질 필요가 없다. 또한, 컴퓨터는 또 다른 디바이스, 예컨대, 몇몇을 거명하면, 이동 전화, 개인 정보 단말(personal digital assistant; PDA), 이동 오디오 또는 비디오 플레이어, 게임 콘솔, 글로벌 포지셔닝 시스템(Global Positioning System; GPS) 수신기, 또는 휴대용 저장 디바이스, 예컨대, 유니버설 직렬 버스(USB) 플래시 드라이브(flash drive)에서 내장될 수 있다.

[0103] 사용자와의 상호작용을 제공하기 위하여, 이 명세서에서 설명된 발명 요지의 구현예들은, 정보를 사용자에게 디스플레이하기 위한 디스플레이 디바이스, 예컨대, LCD(liquid crystal display; 액정 디스플레이) 모니터, 및 사용자가 입력을 컴퓨터에 제공할 수 있게 하는 입력 디바이스, 예컨대, 키보드 및 포인팅 디바이스(pointing device), 예컨대, 마우스(mouse), 트랙볼(trackball), 또는 터치패드(touchpad)를 가지는 컴퓨터 상에서 구현될 수 있거나, 컴퓨터와 통신하도록 구성될 수 있다. 다른 종류들의 디바이스들은 마찬가지로 사용자와의 상호작용을 제공하기 위하여 이용될 수 있고; 예를 들어, 사용자에게 제공된 피드백은 임의의 형태의 센서류 피드백, 예컨대, 시각적 피드백, 청각적 피드백, 또는 촉각적 피드백일 수 있고; 사용자로부터의 입력은 음향, 스피치, 또는 촉각적 입력을 포함하는 임의의 형태로 수신될 수 있다. 추가적으로, 컴퓨터는 문서들을 사용자에게 의해 이용되는 디바이스로 전송함으로써 그리고 이러한 디바이스로부터 문서들을 수신함으로써; 예를 들어, 웹 브라우저(web browser)로부터 수신된 요청들에 응답하여 웹 페이지들을 사용자의 디바이스 상의 웹 브라우저로 전송함으로써, 또는 사용자 디바이스, 예컨대, 스마트폰 또는 전자 태블릿 상에서 작동하는 앱과 상호작용함으로써 사용자와 상호작용할 수 있다. 또한, 컴퓨터는 텍스트 메시지들 또는 다른 형태들의 메시지들을, 개인용 디바이스, 예컨대, 메시징 애플리케이션을 작동시키고 있는 스마트폰으로 전송함으로써, 반환 시에 사용자로부터 응답 메시지들을 수신함으로써 사용자와 상호작용할 수 있다.

[0104] 이 명세서는 시스템들, 장치, 및 컴퓨터 프로그램 컴포넌트들과 관련하여 용어 "~하도록 구성된"을 이용한다. 하나 이상의 컴퓨터들의 시스템이 특정한 동작들 또는 액션들을 수행하도록 구성되는 것은 시스템이, 동작 시에, 시스템으로 하여금, 동작들 또는 액션들을 수행하게 하는 소프트웨어, 펌웨어, 하드웨어, 또는 이들의 조합을 컴퓨터 상에서 설치한 것을 의미한다. 하나 이상의 컴퓨터 프로그램들이 특정한 동작들 또는 액션들을 수행하도록 구성되는 것은, 하나 이상의 프로그램들이, 데이터 프로세싱 장치에 의해 실행될 때, 장치로 하여금, 동작들 또는 액션들을 수행하게 하는 명령들을 포함한다는 것을 의미한다. 특수-목적 로직 회로부가 특정한 동작들 또는 액션들을 수행하도록 구성되는 것은 회로부가 동작들 또는 액션들을 수행하는 전자 로직을 가진다는 것을 의미한다.

[0105] 이 명세서는 특정 구현예 세부사항들을 포함하지만, 이들은 청구항들 자체에 의해 정의되는, 청구되고 있는 것의 범위에 대한 제한들로서 해석되어야 하는 것이 아니라, 오히려, 특정한 구현예들에 특정적일 수도 있는 특징들의 설명들로서 해석되어야 한다. 별도의 구현예들의 맥락에서 이 명세서에서 설명되는 어떤 특징들은 또한, 단일 구현예에서 조합으로 실현될 수 있다. 반대로, 단일 구현예들의 맥락에서 설명되는 다양한 특징들은 또한, 다수의 구현예들에서 별도로, 또는 임의의 적당한 하위조합으로 실현될 수 있다. 또한, 특징들은 어떤 조합들로 작동하고 심지어 이와 같이 초기에 청구되는 것으로서 위에서 설명될 수도 있지만, 청구된 조합으로부터의 하나 이상의 특징들은 일부 경우에는, 조합으로부터 삭제될 수 있고, 청구항은 하위조합 또는 하위조합의 변형에 관한 것일 수도 있다.

[0106] 유사하게, 동작들은 특정한 순서로 도면들에서 도시되고 청구항들에서 기재되어 있지만, 이것은 바람직한 결과들을 달성하기 위하여, 이러한 동작들이 도시된 특정한 순서로 또는 순차적인 순서로 수행되거나, 모든 예시된 동작들이 수행될 것을 요구하는 것으로서 이해되어야 하는 것은 아니다. 어떤 상황들에서는, 멀티태스킹 및 병렬 프로세싱이 유리할 수도 있다. 또한, 위에서 설명된 구현예들에서의 다양한 시스템 모듈들 및 컴포넌트들의

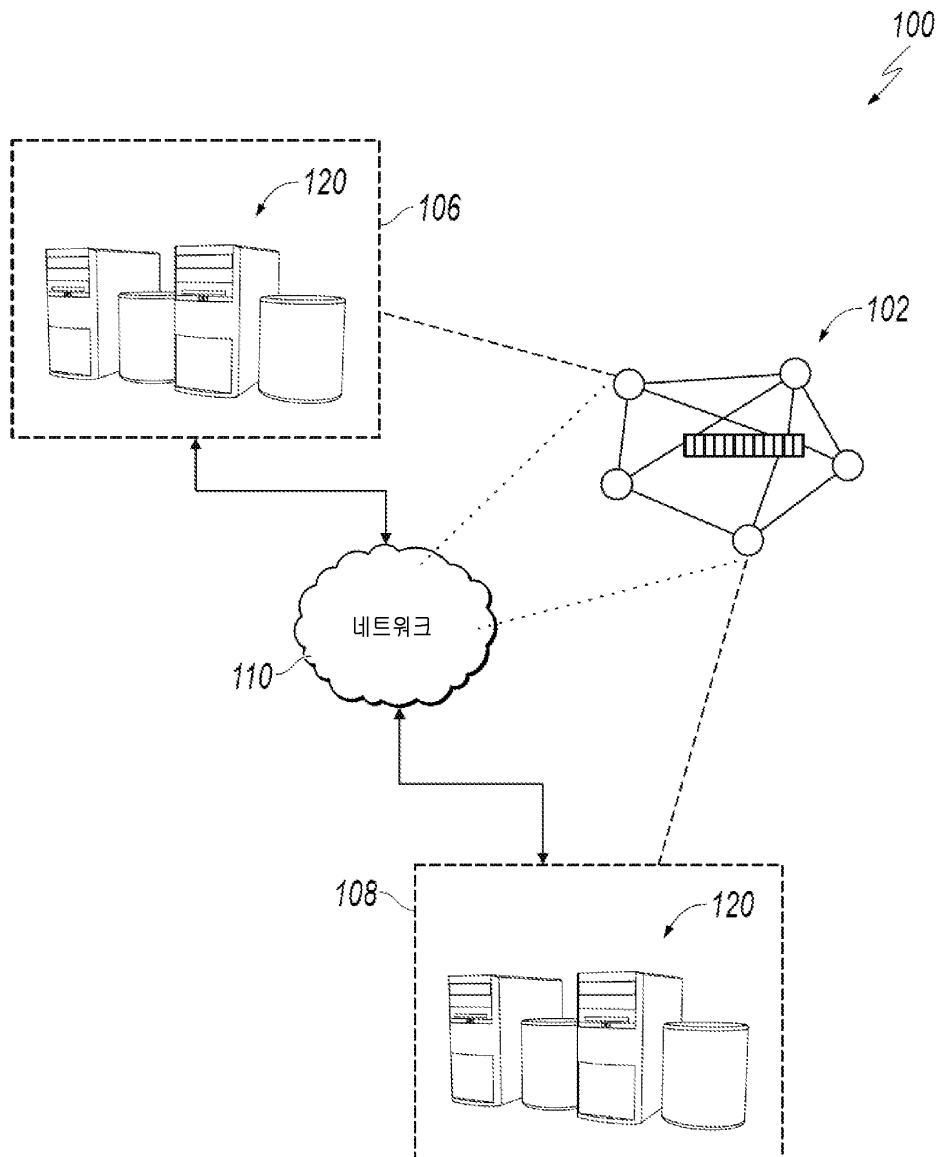
분리는 모든 구현예들에서 이러한 분리를 요구하는 것으로서 이해되지 않아야 하고, 설명된 프로그램 컴포넌트들 및 시스템들은 단일 소프트웨어 제품에서 일반적으로 함께 통합될 수 있거나 다수의 소프트웨어 제품들로 패키징될 수 있다는 것이 이해되어야 한다.

[0107]

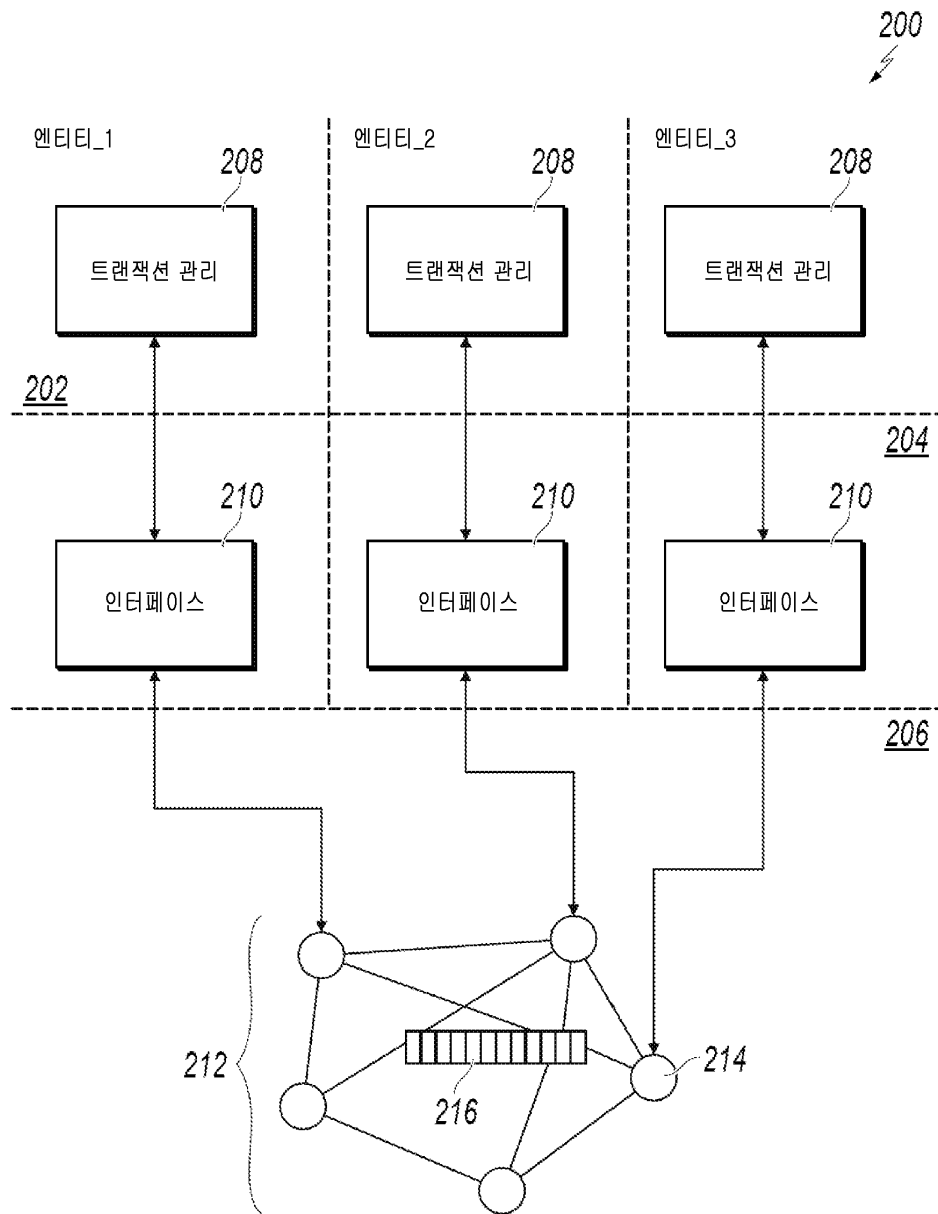
발명 요지의 특정한 구현예들이 설명되었다. 다른 구현예들은 다음의 청구항들의 범위 내에 있다. 예를 들어, 청구항들에서 기재된 액션들은 상이한 순서로 수행될 수 있고, 바람직한 결과들을 여전히 달성할 수 있다. 하나의 예로서, 동반 도면들에서 도시된 프로세스들은 바람직한 결과들을 달성하기 위하여 도시된 특정한 순서 또는 순차적인 순서를 반드시 요구하지는 않는다. 일부 경우에는, 멀티태스킹 및 병렬 프로세싱이 유리할 수도 있다.

도면

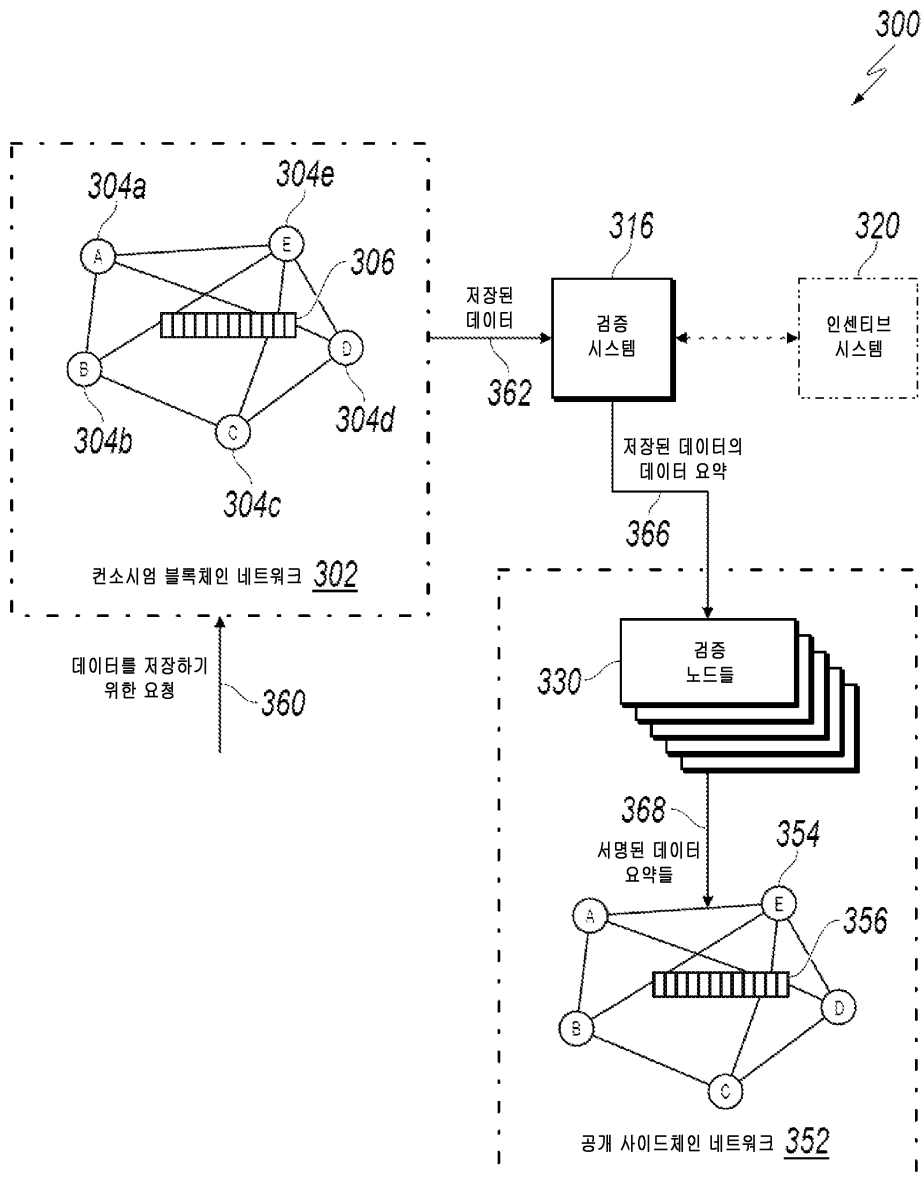
도면1



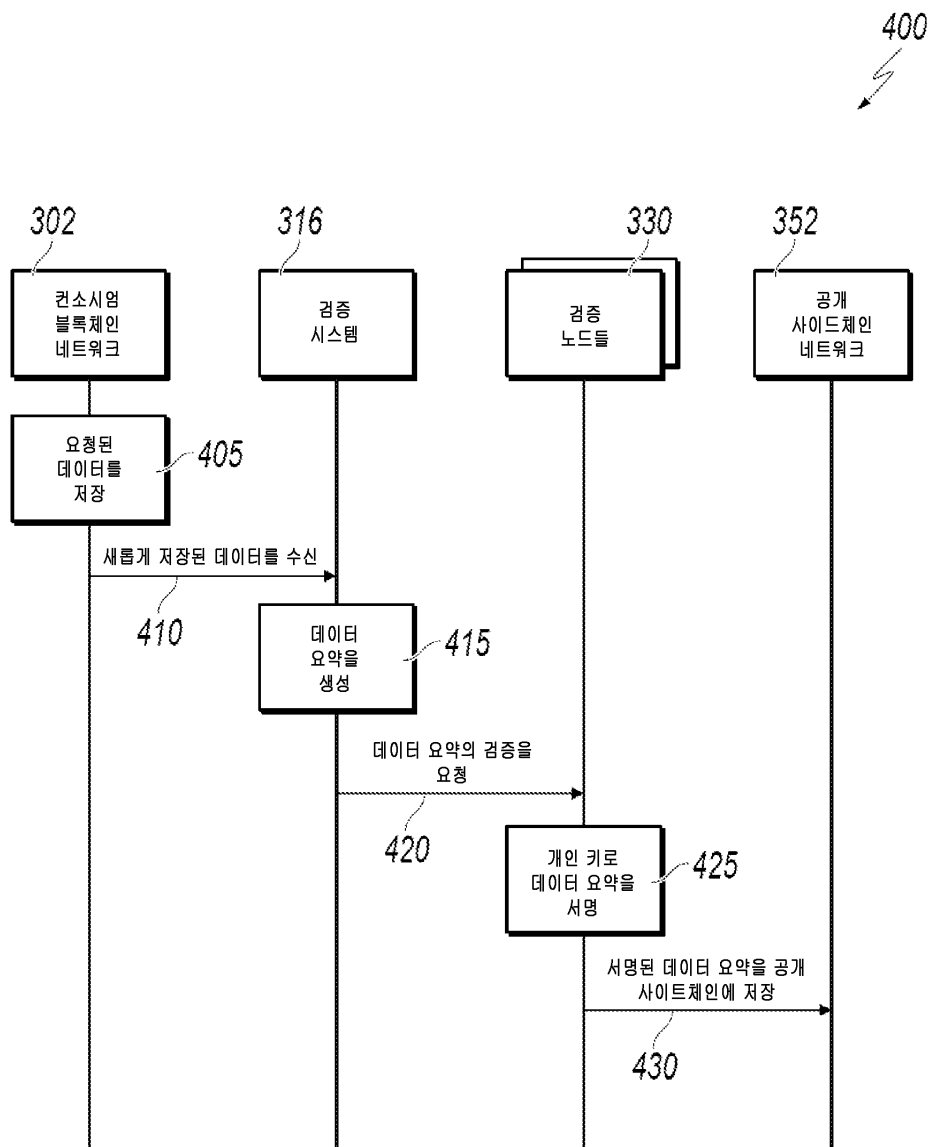
도면2



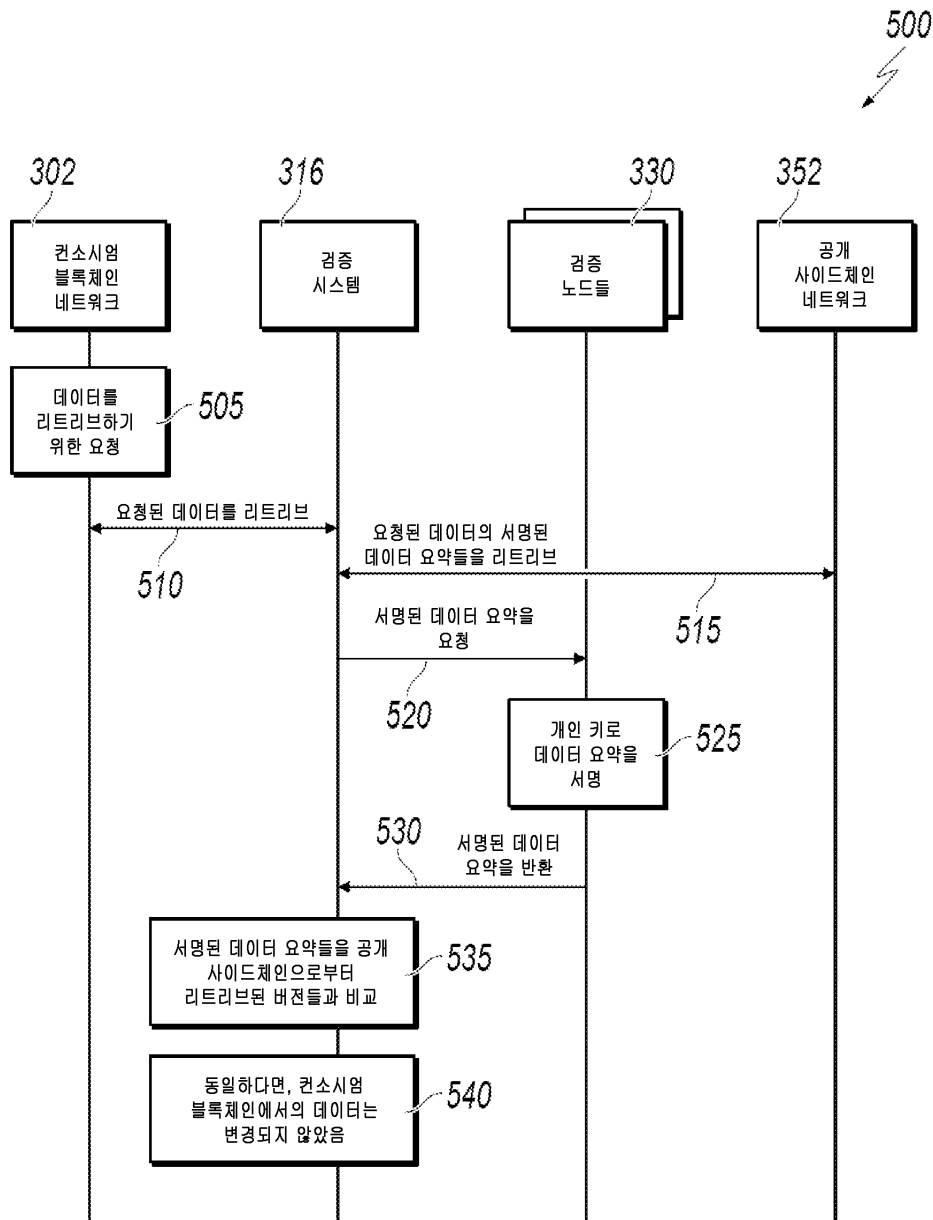
도면3



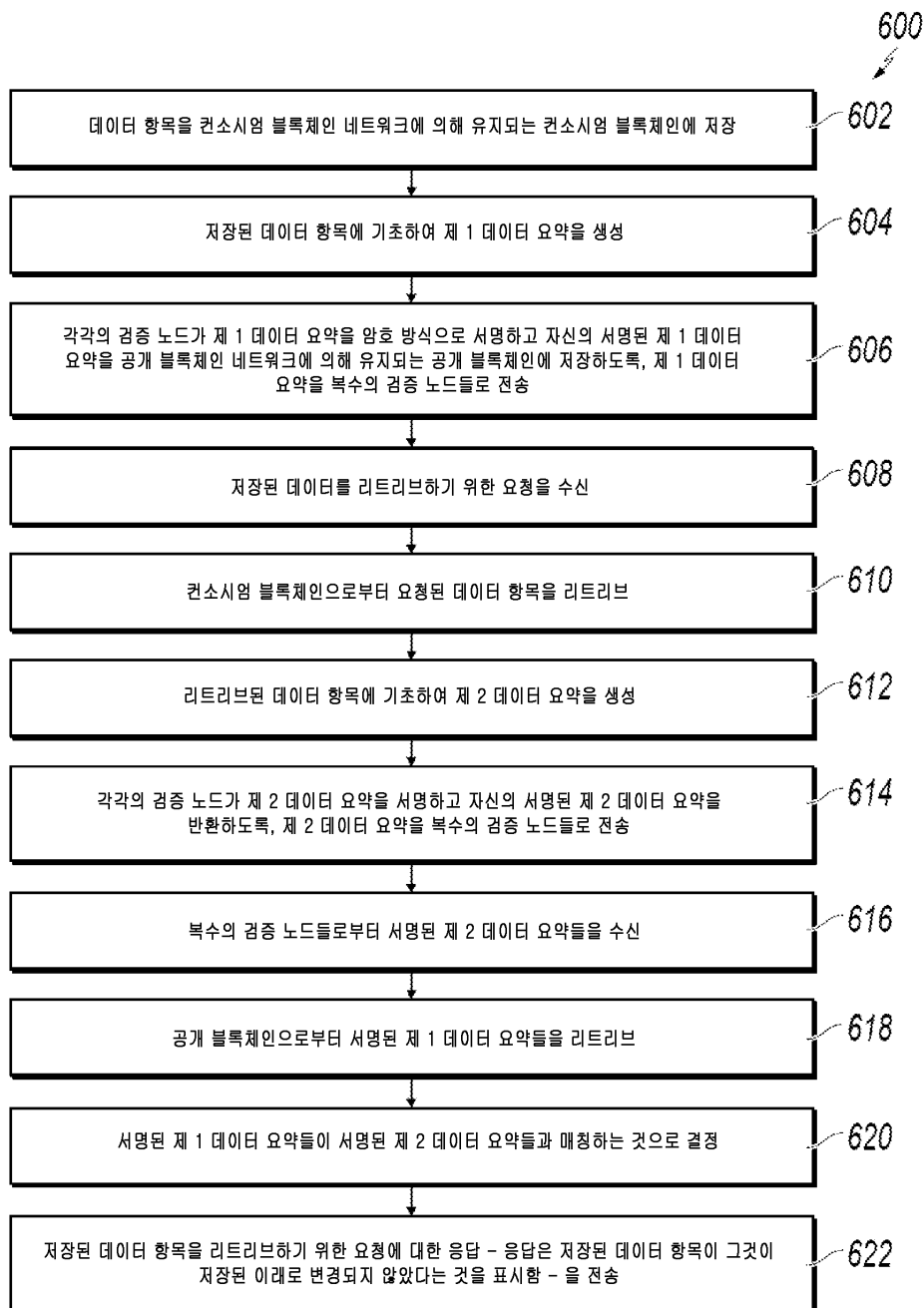
도면4



도면5



도면6



도면7

