



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0077674
(43) 공개일자 2024년06월03일

(51) 국제특허분류(Int. Cl.)
G06Q 10/06 (2012.01) G06Q 10/10 (2023.01)
H04L 9/00 (2022.01) H04L 9/32 (2006.01)
(52) CPC특허분류
G06Q 10/06311 (2013.01)
G06Q 10/0633 (2023.01)
(21) 출원번호 10-2022-0159802
(22) 출원일자 2022년11월24일
심사청구일자 2022년11월24일

(71) 출원인
인하대학교 산학협력단
인천광역시 미추홀구 인하로 100(용현동, 인하대 학교)
(72) 발명자
신병석
서울특별시 서초구
양이화이
인천광역시 미추홀구 재념이길 67-5, 401호(용현동, 금성하이츠빌라)
이연
인천광역시 부평구 주부토로 78, 902호(부평동, 뉴에이스)
(74) 대리인
양성보

전체 청구항 수 : 총 9 항

(54) 발명의 명칭 공개 블록체인 기반의 분산형 클라우드소싱을 위한 신뢰 인증용 AHC 트리 및 프로토콜

(57) 요약

공개 블록체인 기반의 분산형 클라우드소싱을 위한 신뢰 인증용 AHC 트리 및 프로토콜이 개시된다. 공개 블록체인 기반의 분산형 HIT(Human Intelligence Tasks) 클라우드소싱 방법은, 요청자(requester)의 작업(task)을 블록체인의 스마트 계약(smart contract)에 기록하는 단계; 및 상기 적어도 하나의 프로세서의 의해, 상기 작업에 대해 상기 스마트 계약에 기록된 작업자(worker)의 답안을 검증하는 단계를 포함하고, 상기 검증하는 단계는, 상기 스마트 계약에 기록된 데이터를 트리 형태로 표현한 AHC(Additively Homomorphic-based Commitment) 트리를 이용하여 상기 작업자의 답안을 검증할 수 있다.

대표도 - 도4



(52) CPC특허분류

G06Q 10/06398 (2013.01)

G06Q 10/10 (2023.01)

H04L 9/3239 (2013.01)

H04L 9/50 (2022.05)

H04L 2463/102 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1415177413
과제번호	P0017157
부처명	산업통상자원부
과제관리(전문)기관명	한국산업기술진흥원
연구사업명	산업혁신기반구축사업
연구과제명	AI 기반 OLED 제조용 OCR 잉크젯 기술을 적용한 Lamination 장비 개발(2차년도)
기 여 율	1/2
과제수행기관명	지에스아이
연구기간	2022.01.01 ~ 2022.12.31

이 발명을 지원한 국가연구개발사업

과제고유번호	1711174118
과제번호	RS-2022-00155915
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	인공지능융합혁신인재양성(R&D)
연구과제명	인공지능융합혁신인재양성(인하대학교)
기 여 율	1/2
과제수행기관명	인하대학교 산학협력단
연구기간	2022.07.01 ~ 2022.12.31

명세서

청구범위

청구항 1

컴퓨터 장치에서 수행되는 분산형 HIT(Human Intelligence Tasks) 클라우드소싱 방법에 있어서,
 상기 컴퓨터 장치는 메모리에 포함된 컴퓨터 판독가능한 명령들을 실행하도록 구성된 적어도 하나의 프로세서를 포함하고,
 상기 분산형 HIT 클라우드소싱 방법은,
 상기 적어도 하나의 프로세서의 의해, 요청자(requester)의 작업(task)을 블록체인의 스마트 계약(smart contract)에 기록하는 단계; 및
 상기 적어도 하나의 프로세서의 의해, 상기 작업에 대해 상기 스마트 계약에 기록된 작업자(worker)의 답안을 검증하는 단계
 를 포함하고,
 상기 검증하는 단계는,
 상기 스마트 계약에 기록된 데이터를 트리 형태로 표현한 AHC(Additively Homomorphic-based Commitment) 트리를 이용하여 상기 작업자의 답안을 검증하는 것
 을 특징으로 하는 분산형 HIT 클라우드소싱 방법.

청구항 2

제1항에 있어서,
 상기 분산형 HIT 클라우드소싱 방법은,
 상기 적어도 하나의 프로세서의 의해, 상기 작업에 대한 표준 답안(gold-standard answer)을 공개하는 단계
 를 더 포함하고,
 상기 작업자 측에서 상기 표준 답안을 이용하여 답안 품질을 평가하는 것
 을 특징으로 하는 분산형 HIT 클라우드소싱 방법.

청구항 3

제1항에 있어서,
 상기 분산형 HIT 클라우드소싱 방법은,
 상기 적어도 하나의 프로세서의 의해, 상기 작업자의 답안이 상기 요청자의 요구사항을 충족하지 않으면 상기 스마트 계약을 종료하는 단계
 를 더 포함하는 분산형 HIT 클라우드소싱 방법.

청구항 4

제1항에 있어서,
 상기 분산형 HIT 클라우드소싱 방법은,
 상기 적어도 하나의 프로세서의 의해, 상기 작업자의 답안이 상기 요청자의 요구사항을 충족하지 않으면 불일치 증명(PoM)을 생성하여 상기 스마트 계약에 기록하는 단계
 를 더 포함하는 분산형 HIT 클라우드소싱 방법.

청구항 5

제1항에 있어서,
상기 검증하는 단계는,
상기 작업자의 답안이 지정된 데이터 구조로 구성 및 인코딩되었는지 확인하는 단계
를 포함하는 분산형 HIT 클라우드소싱 방법.

청구항 6

제1항에 있어서,
상기 검증하는 단계는,
상기 작업자의 답안으로 인코딩된 데이터와 상기 작업자로부터 노출된 보안 키를 수신한 후 상기 보안 키를 통해 상기 인코딩된 데이터를 디코딩하여 상기 작업자의 답안을 검증하는 단계
를 포함하는 분산형 HIT 클라우드소싱 방법.

청구항 7

제1항에 있어서,
상기 검증하는 단계는,
상기 AHC 트리에 포함된 각 노드에 대해 자식 노드의 해시 값을 이용하여 해당 노드의 해시 값을 계산하는 단계; 및
상기 AHC 트리에 포함된 리프 노드(leaf node)의 해시 값을 이용하여 상기 작업자의 답안을 검증하는 단계
를 포함하는 분산형 HIT 클라우드소싱 방법.

청구항 8

제1항에 있어서,
상기 검증하는 단계는,
상기 AHC 트리의 루트 해시 값을 상기 작업에 대한 보안 키로 사용하여 상기 작업자의 답안을 검증하는 것을 특징으로 하는 분산형 HIT 클라우드소싱 방법.

청구항 9

컴퓨터 장치에 있어서,
메모리에 포함된 컴퓨터 판독가능한 명령들을 실행하도록 구성된 적어도 하나의 프로세서
를 포함하고,
상기 적어도 하나의 프로세서는,
요청자(requester)의 작업(task)을 블록체인의 스마트 계약(smart contract)에 기록하는 과정; 및
상기 작업에 대해 상기 스마트 계약에 기록된 작업자(worker)의 답안을 검증하는 과정을 처리하고,
상기 적어도 하나의 프로세서는,
상기 스마트 계약에 기록된 데이터를 트리 형태로 표현한 AHC(Additively Homomorphic-based Commitment) 트리를 이용하여 상기 작업자의 답안을 검증하는 것을 특징으로 하는 컴퓨터 장치.

발명의 설명

기술 분야

[0001] 아래의 설명은 공개 블록체인 환경에서 분산형 HIT(Human Intelligence Tasks) 클라우드소싱 기술에 관한 것이다.

배경 기술

[0002] HIT(Human Intelligence Tasks)를 위한 클라우드소싱은 기계 학습을 위한 이미지 주석과 같은 인간 지식을 크라우드소싱(crowdsourcing)하는 데 널리 사용되고 있다.

[0003] 일례로, 한국 공개특허공보 제10-2015-0140644호(공개일 2015년 12월 16일)에는 기계학습 표정 분류기를 위한 훈련 사례를 발생시키는 크라우드소싱 파이프라인을 구현하는 기술이 개시되어 있다.

[0004] HIT에서 요청자는 질문을 게시하고 해당 질문에 대한 답변을 제공하는 작업자에게 비용을 지불한다. 그러나, 인터넷 환경에서는 양 당사자가 서로를 신뢰하지 않는다고 가정하는 것이 합리적이다. 이에 따라 신뢰의 문제가 발생한다. 요청자는 허위 신고를 방지하기 위해 양질의 답변을 얻기를 기대하고, 작업자의 경우 무임승차(free-riding) 방지를 위해 답변이 미리 설정된 요구 사항을 충족하면 비용을 받을 수 있다.

[0005] 답변 품질을 결정하기 위해 표준 답안(gold-standard answer) 또는 알려진 답변의 질문을 작업자가 답변해야 하는 질문과 혼합하는 것이 대부분의 HIT를 캡처할 수 있는 일반적인 매커니즘이다.

[0006] 요청자와 작업자 간의 신뢰 문제를 해결하기 위한 한 가지 접근 방식은 신뢰할 수 있는 제3자(예를 들어, ATM(Amazon's MTurk) 등)에 의존하는 것이다.

[0007] 그러나, 제3자에 의존하는 방식은 디도스(DDos) 공격에 취약하다. 중앙 집중식 서버 또는 대규모 클라우드 플랫폼에서 HIT 시스템을 실행하는 것은 가동 중단 및 불법 행위 등으로 인해 실제 사용 환경이 취약하다. 또한, 중앙 집중식 서버는 준정직한 플랫폼(semi-honest platform)으로 모델링되어 규정된 프로토콜을 실행할 것으로 예상되지만 개인정보 유출 위험이 있다.

발명의 내용

해결하려는 과제

[0008] 공개 블록체인을 사용하여 블록체인이 암호화폐 지불을 처리하고 분산된 환경에서 작업자와 요청자 간의 분쟁을 해결하는 역할을 하여 잘못된 보고와 무임 승차를 방지하는 중앙 집중식 HIT 시스템을 제공할 수 있다.

[0009] 영지식 증명(zero-knowledge proof)과 같은 값비싼 암호화 도구를 사용하거나 작업자의 답변을 블록체인에 보내지 않고 온체인 비용(on-chain cost)을 크게 줄일 수 있는 접근 방식을 제공한다.

[0010] 블록체인에 의한 오버헤드를 줄이기 위해 오프라인에서의 AHC 트리(Additively Homomorphic-based Commitment Tree) 구조를 사용하고 이를 따르는 크라우드소싱 프로토콜을 제공한다.

과제의 해결 수단

[0011] 컴퓨터 장치에서 수행되는 분산형 HIT(Human Intelligence Tasks) 클라우드소싱 방법에 있어서, 상기 컴퓨터 장치는 메모리에 포함된 컴퓨터 관독가능한 명령들을 실행하도록 구성된 적어도 하나의 프로세서를 포함하고, 상기 분산형 HIT 클라우드소싱 방법은, 상기 적어도 하나의 프로세서의 의해, 요청자(requester)의 작업(task)을 블록체인의 스마트 계약(smart contract)에 기록하는 단계; 및 상기 적어도 하나의 프로세서의 의해, 상기 작업에 대해 상기 스마트 계약에 기록된 작업자(worker)의 답안을 검증하는 단계를 포함하고, 상기 검증하는 단계는, 상기 스마트 계약에 기록된 데이터를 트리 형태로 표현한 AHC(Additively Homomorphic-based Commitment) 트리를 이용하여 상기 작업자의 답안을 검증하는 것을 특징으로 하는 분산형 HIT 클라우드소싱 방법을 제공한다.

[0012] 일 측면에 따르면, 상기 분산형 HIT 클라우드소싱 방법은, 상기 적어도 하나의 프로세서의 의해, 상기 작업에 대한 표준 답안(gold-standard answer)을 공개하는 단계를 더 포함하고, 상기 작업자 측에서 상기 표준 답안을 이용하여 답안 품질을 평가할 수 있다.

- [0013] 다른 측면에 따르면, 상기 분산형 HIT 클라우드소싱 방법은, 상기 적어도 하나의 프로세서의 의해, 상기 작업자의 답안이 상기 요청자의 요구사항을 충족하지 않으면 상기 스마트 계약을 종료하는 단계를 더 포함할 수 있다.
- [0014] 또 다른 측면에 따르면, 상기 분산형 HIT 클라우드소싱 방법은, 상기 적어도 하나의 프로세서의 의해, 상기 작업자의 답안이 상기 요청자의 요구사항을 충족하지 않으면 불일치 증명(PoM)을 생성하여 상기 스마트 계약에 기록하는 단계를 더 포함할 수 있다.
- [0015] 또 다른 측면에 따르면, 상기 검증하는 단계는, 상기 작업자의 답안이 지정된 데이터 구조로 구성 및 인코딩되었는지 확인하는 단계를 포함할 수 있다.
- [0016] 또 다른 측면에 따르면, 상기 검증하는 단계는, 상기 작업자의 답안으로 인코딩된 데이터와 상기 작업자로부터 노출된 보안 키를 수신한 후 상기 보안 키를 통해 상기 인코딩된 데이터를 디코딩하여 상기 작업자의 답안을 검증하는 단계를 포함할 수 있다.
- [0017] 또 다른 측면에 따르면, 상기 검증하는 단계는, 상기 AHC 트리에 포함된 각 노드에 대해 자식 노드의 해시 값을 이용하여 해당 노드의 해시 값을 계산하는 단계; 및 상기 AHC 트리에 포함된 리프 노드(leaf node)의 해시 값을 이용하여 상기 작업자의 답안을 검증하는 단계를 포함할 수 있다.
- [0018] 또 다른 측면에 따르면, 상기 검증하는 단계는, 상기 AHC 트리의 루트 해시 값을 상기 작업에 대한 보안 키로 사용하여 상기 작업자의 답안을 검증할 수 있다.
- [0019] 컴퓨터 장치에 있어서, 메모리에 포함된 컴퓨터 판독가능한 명령들을 실행하도록 구성된 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는, 요청자(requester)의 작업(task)을 블록체인의 스마트 계약(smart contract)에 기록하는 과정; 및 상기 작업에 대해 상기 스마트 계약에 기록된 작업자(worker)의 답안을 검증하는 과정을 처리하고, 상기 적어도 하나의 프로세서는, 상기 스마트 계약에 기록된 데이터를 트리 형태로 표현한 AHC(Additively Homomorphic-based Commitment) 트리를 이용하여 상기 작업자의 답안을 검증하는 것을 특징으로 하는 컴퓨터 장치를 제공한다.

발명의 효과

- [0020] 본 발명의 실시예들에 따르면, 요청자와 작업자 간의 신뢰 문제를 해결하기 위한 제3자를 사용하지 않고 허가가 필요하지 않은 블록체인의 스마트계약에 의존하여 분산형 HIT를 효율적으로 수행할 수 있는 프로토콜로 AHC 트리 구조를 따르는 클라우드소싱 프로토콜을 제공한다.
- [0021] 본 발명의 실시예들에 따르면, 단순히 리프 노드의 값 합계를 간단히 커밋하고 효율적으로 확인할 수 있는 AHC 트리를 사용함으로써 오프체인(off-chain) 계산과 같은 암호화 도구를 피하고 온체인 비용을 크게 줄일 수 있다.
- [0022] 본 발명의 실시예들에 따르면, UC(Universal Compensability) 프레임워크에서 bHIT(블록체인 기반 HIT)의 공식 정의를 제공하고 잘못된 보고 및 무임승차를 방지하는 분산형 HIT 기능을 구현할 수 있다.

도면의 간단한 설명

- [0023] 도 1은 본 발명의 일실시예에 따른 컴퓨터 장치의 예를 도시한 블록도이다.
- 도 2는 본 발명의 일실시예에 있어서 AHC(Additively Homomorphic-based Commitment) 트리 구조 예시를 도시한 것이다.
- 도 3은 본 발명의 일실시예에 있어서 블록체인 기반 HIT(Human Intelligence Tasks) 프로토콜의 개요를 설명하기 위한 도면이다.
- 도 4는 본 발명의 일실시예에 있어서 블록체인 기반 HIT 실행 예시를 도시한 것이다.
- 도 5는 본 발명의 일실시예에 있어서 표준 답안과 조건자를 사용하여 HIT에 AHC 트리를 적용하는 예시를 도시한 것이다.
- 도 6은 본 발명의 일실시예에 있어서 AHC 트리의 리프 노드의 값을 계산하는 과정의 예시를 도시한 것이다.
- 도 7은 본 발명의 일실시예에 있어서 작업자의 데이터에 대해 스마트 계약에 중재를 요청하는 예시를 도시한 것이다.

발명을 실시하기 위한 구체적인 내용

- [0024] 이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.
- [0026] 본 발명의 실시예들은 공개 블록체인 환경에서 분산형 HIT(Human Intelligence Tasks) 클라우드소싱 기술에 관한 것이다.
- [0027] 본 명세서에서 구체적으로 개시되는 것들을 포함하는 실시예들은 영지식 증명과 같은 책임 있고 계산 비용이 많이 드는 암호화 기술을 사용하지 않고 블록체인에 의한 보안 오버헤드를 줄이기 위해 오프라인에서의 AHC 트리 구조를 사용하며, 이에 따르는 클라우드소싱 프로토콜을 제공할 수 있다.
- [0028] 본 발명의 실시예들에 따른 분산형 HIT 클라우드소싱 시스템은 적어도 하나의 컴퓨터 장치에 의해 구현될 수 있으며, 본 발명의 실시예들에 따른 분산형 HIT 클라우드소싱 방법은 분산형 HIT 클라우드소싱 시스템에 포함되는 적어도 하나의 컴퓨터 장치를 통해 수행될 수 있다. 이때, 컴퓨터 장치에는 본 발명의 일실시예에 따른 컴퓨터 프로그램이 설치 및 구동될 수 있고, 컴퓨터 장치는 구동된 컴퓨터 프로그램의 제어에 따라 본 발명의 실시예들에 따른 분산형 HIT 클라우드소싱 방법을 수행할 수 있다. 상술한 컴퓨터 프로그램은 컴퓨터 장치와 결합되어 분산형 HIT 클라우드소싱 방법을 컴퓨터에 실행시키기 위해 컴퓨터 판독 가능한 기록매체에 저장될 수 있다.
- [0029] 도 1은 본 발명의 일실시예에 따른 컴퓨터 장치의 예를 도시한 블록도이다. 예를 들어, 본 발명의 실시예들에 따른 분산형 HIT 클라우드소싱 시스템은 도 1을 통해 도시된 컴퓨터 장치(100)에 의해 구현될 수 있다.
- [0030] 도 1에 도시된 바와 같이 컴퓨터 장치(100)는 본 발명의 실시예들에 따른 분산형 HIT 클라우드소싱 방법을 실행하기 위한 구성요소로서, 메모리(110), 프로세서(120), 통신 인터페이스(130) 그리고 입출력 인터페이스(140)를 포함할 수 있다.
- [0031] 메모리(110)는 컴퓨터에서 판독 가능한 기록매체로서, RAM(random access memory), ROM(read only memory) 및 디스크 드라이브와 같은 비소멸성 대용량 기록장치(permanent mass storage device)를 포함할 수 있다. 여기서 ROM과 디스크 드라이브와 같은 비소멸성 대용량 기록장치는 메모리(110)와는 구분되는 별도의 영구 저장 장치로서 컴퓨터 장치(100)에 포함될 수도 있다. 또한, 메모리(110)에는 운영체제와 적어도 하나의 프로그램 코드가 저장될 수 있다. 이러한 소프트웨어 구성요소들은 메모리(110)와는 별도의 컴퓨터에서 판독 가능한 기록매체로부터 메모리(110)로 로딩될 수 있다. 이러한 별도의 컴퓨터에서 판독 가능한 기록매체는 플로피 드라이브, 디스크, 테이프, DVD/CD-ROM 드라이브, 메모리 카드 등의 컴퓨터에서 판독 가능한 기록매체를 포함할 수 있다. 다른 실시예에서 소프트웨어 구성요소들은 컴퓨터에서 판독 가능한 기록매체가 아닌 통신 인터페이스(130)를 통해 메모리(110)에 로딩될 수도 있다. 예를 들어, 소프트웨어 구성요소들은 네트워크(160)를 통해 수신되는 파일들에 의해 설치되는 컴퓨터 프로그램에 기반하여 컴퓨터 장치(100)의 메모리(110)에 로딩될 수 있다.
- [0032] 프로세서(120)는 기본적인 산술, 로직 및 입출력 연산을 수행함으로써, 컴퓨터 프로그램의 명령을 처리하도록 구성될 수 있다. 명령은 메모리(110) 또는 통신 인터페이스(130)에 의해 프로세서(120)로 제공될 수 있다. 예를 들어, 프로세서(120)는 메모리(110)와 같은 기록 장치에 저장된 프로그램 코드에 따라 수신되는 명령을 실행하도록 구성될 수 있다.
- [0033] 통신 인터페이스(130)는 네트워크(160)를 통해 컴퓨터 장치(100)가 다른 장치와 서로 통신하기 위한 기능을 제공할 수 있다. 일례로, 컴퓨터 장치(100)의 프로세서(120)가 메모리(110)와 같은 기록 장치에 저장된 프로그램 코드에 따라 생성한 요청이나 명령, 데이터, 파일 등이 통신 인터페이스(130)의 제어에 따라 네트워크(160)를 통해 다른 장치들로 전달될 수 있다. 역으로, 다른 장치로부터의 신호나 명령, 데이터, 파일 등이 네트워크(160)를 거쳐 컴퓨터 장치(100)의 통신 인터페이스(130)를 통해 컴퓨터 장치(100)로 수신될 수 있다. 통신 인터페이스(130)를 통해 수신된 신호나 명령, 데이터 등은 프로세서(120)나 메모리(110)로 전달될 수 있고, 파일 등은 컴퓨터 장치(100)가 더 포함할 수 있는 저장 매체(상술한 영구 저장 장치)로 저장될 수 있다.
- [0034] 통신 방식은 제한되지 않으며, 네트워크(160)가 포함할 수 있는 통신망(일례로, 이동통신망, 유선 인터넷, 무선 인터넷, 방송망)을 활용하는 통신 방식뿐만 아니라 기기들 간의 근거리 유선/무선 통신 역시 포함될 수 있다. 예를 들어, 네트워크(160)는, PAN(personal area network), LAN(local area network), CAN(campus area network), MAN(metropolitan area network), WAN(wide area network), BBN(broadband network), 인터넷 등의 네트워크 중 하나 이상의 임의의 네트워크를 포함할 수 있다. 또한, 네트워크(160)는 버스 네트워크, 스타 네트워크, 링 네트워크, 메쉬 네트워크, 스타-버스 네트워크, 트리 또는 계층적(hierarchical) 네트워크 등을 포함

하는 네트워크 토폴로지 중 임의의 하나 이상을 포함할 수 있으나, 이에 제한되지 않는다.

[0035] 입출력 인터페이스(140)는 입출력 장치(150)와의 인터페이스를 위한 수단일 수 있다. 예를 들어, 입력 장치는 마이크, 키보드, 카메라 또는 마우스 등의 장치를, 그리고 출력 장치는 디스플레이, 스피커와 같은 장치를 포함할 수 있다. 다른 예로 입출력 인터페이스(140)는 터치스크린과 같이 입력과 출력을 위한 기능이 하나로 통합된 장치와의 인터페이스를 위한 수단일 수도 있다. 입출력 장치(150)는 컴퓨터 장치(100)와 하나의 장치로 구성될 수도 있다.

[0036] 또한, 다른 실시예들에서 컴퓨터 장치(100)는 도 1의 구성요소들보다 더 적은 혹은 더 많은 구성요소들을 포함할 수도 있다. 그러나, 대부분의 종래기술적 구성요소들을 명확하게 도시할 필요성은 없다. 예를 들어, 컴퓨터 장치(100)는 상술한 입출력 장치(150) 중 적어도 일부를 포함하도록 구현되거나 또는 트랜시버(transceiver), 카메라, 각종 센서, 데이터베이스 등과 같은 다른 구성요소들을 더 포함할 수도 있다.

[0037] 이하에서는 공개 블록체인 기반의 분산형 클라우드소싱을 위한 신뢰 인증용 AHC 트리 및 프로토콜의 구체적인 실시예를 설명하기로 한다.

[0038] 본 발명의 실시예들에 따른 분산형 HIT 클라우드소싱 시스템은 블록체인의 계산 및 저장 오버헤드를 줄이고 효율적으로 요청자의 무임승차 부정행위와 작업자의 잘못된 작업을 방지하고 블록체인의 스마트 계약에 의해 작업자 데이터의 품질을 자동 평가할 수 있다.

[0039] 도 2는 본 발명의 일실시예에 있어서 AHC 트리 구조 예시를 도시한 것이다.

[0040] 도 2를 참조하면, AHC 트리는 (m_i, v_i) 의 데이터 셋을 입력으로 구축한다. 다시 말해, 표 1의 알고리즘 1의 Ctree 함수는 (m_i, v_i) 목록을 입력으로 받아 AHC 트리를 구축할 수 있다. 여기서, m_i 는 임의 길이의 문자열이고, 리프 노드의 값인 v_i 는 $v_i \in 0 \cup \mathbb{N}$ 을 만족한다.

[0041] [표 1]

Algorithm 1: CTree, to build an AHCTree

Input: $\{(m_1, v_1), \dots, (m_n, v_n)\}$ ▷ n is a power of 2

1 **for** $i = 1$ **to** n **do**

2 $hom_i \leftarrow \text{Hom}(v_i);$

3 $h_i \leftarrow \mathcal{H}(m_i || hom_i);$ ▷ hash value of a leaf node

4 append (h_i, hom_i) to *ctree*;

5 **for** $i = 1$ **to** $n - 1$ **do**

6 $hom_{i+n} \leftarrow hom_{2i-1} + hom_{2i};$ ▷ non-leaf nodes

7 $h_{i+n} \leftarrow \mathcal{H}(h_{2i-1} || h_{2i} || hom_{i+n});$

8 append (h_{i+n}, hom_{i+n}) to *ctree*;

Output: *ctree* with root (h_{2n-1}, hom_{2n-1})

[0042]

[0043] AHC 트리는 블록체인에서 블록 하나에 포함된 모든 거래 정보를 요약하여 트리 형태로 표현한 데이터 구조인 머클 트리(Merkle tree)와 유사하게, 자식 노드의 해시를 입력으로 받아 재귀적으로 자신의 해시 값을 계산한다. 각 노드는 동형 암호화된 값을 가진다.

[0044] 각 노드에 대한 동형 값 hom_i (즉, Pedersen Commitment)는 수학적 식 1을 통해 재귀적으로 계산된다.

[0045] [수학적 식 1]

[0046]
$$hom_i = hom_{lchild} + hom_{rchild}$$

[0047] 여기서, hom_{lchild} 는 i 번째 노드의 바로 왼쪽 자식 노드의 Hom 값을 의미하고, hom_{rchild} 는 i 번째 노드의 바로 오른쪽 자식 노드의 Hom 값을 의미한다. 수학적 식 1에 따른 hom_i 를 i 번째 노드에 대한 해시 계산을 위한 입력의 일부로 취할 수 있다.

- [0048] 예를 들어, AHC 트리 구조 중 5번째 루트 h_5 는 $h_5=H(h_1||h_2||Hom_5)$ 와 같다. 여기서, $Hom_5=Hom(v_1)+Hom(v_2)$. h_6 은 $h_6=H(h_3||h_4||Hom_6)$ 와 같고, $Hom_6=Hom(v_3)+Hom(v_4)$ 와 같다.
- [0049] 리프 노드의 값 v_i 를 은닉하기 위해 새로운 임의의 값을 생성하고 $Hom(v_i)$ 을 계산하는 데 사용한다. AHC 트리에 있는 모든 리프 노드의 합을 빠르고 쉽게 계산할 수 있어 빠른 보안 검증에 사용 가능하다.
- [0050] 예를 들어, AHC 트리에서 보증일방이 모든 리프 노드의 합이 $S_v=v_1+v_2+v_3+v_4$ 와 같다고 주장할 때, 검증일방은 AHC 트리가 올바르게 구성되었음을 확인하고 알려진 h_7 이 계산식 $h_7=Hash(h_5||h_6||Hom(S_v))$ 의 결과와 일치한다면 보증일방의 주장을 검증 완료한 것으로 간주한다.
- [0051] 또한, AHC 트리 (m_i , v_i)값을 모르는 상황에서 $h_i=Hash(h_{child}||h_{rchild}||hom_i)$ 식과 $hom_i=hom_{child}+hom_{rchild}$ 식으로 트리가 정확히 구축되었는지를 검증할 수 있다.
- [0052] 인증 솔루션으로 사용 가능한 AHC 트리에서 루트 값 h_{root} 를 약속 키(promise key)로 사용한다. 검증을 위해 $\{(m_1, v_2), \dots, (m_n, v_n)\}$ 및 페테르센(Pedersen) 인증의 랜덤 값을 오픈하고, 검증일방은 $h_{root}=CTree(\{(m_1, v_2), \dots, (m_n, v_n)\})$ 가 맞는지 확인한다.
- [0053] 만약, $h'_{root}=h_{root}$ 가 정확할 경우 검증이 정확하다고 판단한다.
- [0054] 도 3은 본 발명의 일실시예에 있어서 블록체인 기반 HIT(즉, bHIT) 프로토콜의 개요를 설명하기 위한 도면이다.
- [0055] bHIT 프로토콜은 요청자(310)와 작업자(320) 간의 분쟁을 해결하기 위한 프로토콜로 표준 답안을 기준으로 작업자 답변의 품질을 평가한다. bHIT 프로토콜에서 요청자(310)는 우선 작업자(320)를 낙관적으로 신뢰한다. 최종 과정에서 요청자(310)가 작업자(320)를 부정직하다고 판단하면 요청자(310)는 서버(300) 상의 스마트 계약에게 불공정성을 신청하고 중재를 요청하며 요구사항 불일치 증명(PoM)을 생성한다.
- [0056] 이러한 bHIT 프로토콜이 원활히 작동하기 위해 보안 시스템은 2가지 기능을 지원해야 한다. (1) 작업자(320)의 모든 (인코딩된 데이터) 데이터가 규칙(요구사항)에 부합됨을 증명할 수 있어야 한다. (2) 작업자(320)의 임의의 인코딩된 데이터가 요구사항에 부합되지 않음을 증명할 수 있어야 한다.
- [0057] 도 3을 참조하면, 요청자(310)는 정보 수집을 위해 서버(300)에 스마트 계약에 기록할 작업, 예치금 및 표준 답안(gold-standard answers) 및 약속보안키, 기타 파라미터들을 발행한다(S301). 또한, 수집 작업의 요구사항 및 보조 데이터를 작업자(320)가 액세스할 수 있는 웹 페이지와 같은 장소에 배포한다.
- [0058] 작업자(320)는 요청된 정보 수집을 완성하고 약속보안키 및 페테르센의 약속보안솔루션을 서버(300)의 스마트 계약에 전송한다(S302).
- [0059] 요청자(310)가 약속한 표준 답안을 공개한다(S303).
- [0060] 작업자(320)는 표준 답안을 사용하여 자신의 답안 품질을 평가하고 답안을 암호화 및 인코딩한다(S304). 답안이 품질 요구 사항을 충족하지 않으면 서버(300)는 계약을 종료한다.
- [0061] 요청자(310)는 작업자(320)의 답안을 확인하지 않은 상태에서 작업자(320)의 인코딩된 데이터가 지정된 데이터 구조를 사용하여 구성 및 인코딩되었는지 확인한다(S305). 검증 통과 후 요청자(310)는 서버(300)의 스마트 계약에 ACK를 전송하여 작업자(320)의 인코딩 데이터 수신 신호를 전송한다(S306).
- [0062] 작업자(320)는 보안키를 노출한다(S307).
- [0063] 요청자(310)는 작업자(320)로부터 보안키를 받은 후 작업자(320)의 답변 데이터를 디코딩하고 답안을 검증한다(S308).
- [0064] 요청자(310)의 검증 결과 작업자(320)의 데이터가 요구사항에 부합되지 않을 경우 불일치 증명(PoM)을 생성하여 생성된 PoM을 서버(300)의 스마트 계약에 기록함에 따라 작업자(320)의 성실 여부를 중재하도록 한다(S309). 작업자(320)가 정직하지 않을 경우 서버(300)의 스마트 계약은 보증금을 요청자(310)에게 반환한다. 요청자(310)가 검증 기간 내에 스마트 계약에 불만 신고를 하지 않을 경우 서버(300)의 스마트 계약은 작업이 성공적으로 진행된 것으로 간주하고 요청자(310)의 보증금을 작업자(320)에게 보상으로 지급한다.

- [0065] 도 4는 본 발명의 일실시예에 있어서 bHIT 실행 예시를 도시한 것이다.
- [0066] 도 4의 예시에는 빨간 색 아이디로 표시된 4개의 표준 이미지가 포함되어 있다. 작업자가 레이블링 작업을 진행하게 되는데, 이때 작업자에 의한 작업 결과는 회색 텍스트 배경으로 표시되어 있다.
- [0067] 도 4는 제안 보안 매커니즘을 사용하는 클라우드소싱의 사례를 나타내고 있다. 예를 들어, 레이블링 작업에서는 작업자가 각 이미지에 대해 '실내' 또는 '실외' 태그를 지정해야 한다. 4개의 표준 이미지를 포함하여 주석 처리 가능 이미지는 총 30개이다. 표준 이미지 데이터의 ID와 레이블은 $\{(0,1), (4,2), (20,2), (29,1)\}$ 이며 이 데이터를 표준 이미지 레이블링 데이터라고 한다. 작업자가 모든 이미지에 레이블을 지정 및 제출한 후 요청자는 표준 이미지의 레이블 지정 데이터를 공개한다. 이때, 작업자의 데이터에 기반하여 도 5에 도시한 바와 같이 AHC 트리의 리프 노드가 계산된다. 도 5에 도시한 바와 같이, 표준 답안과 조건자(predicate) $P(s_i, a_i) \rightarrow 0/1$ 를 포함하여 AHC 트리를 HIT에 제출할 수 있다. 각 리프 노드는 튜플(sid_i, s_i, a_i)이며, 여기서 a_i 는 표준 이미지에 해당하는 작업자 레이블의 결과를 나타낸다. 다음 튜플들을 사용하여 작업자는 인코딩된 데이터를 생성하고 도 5와 도 6에 표시된 프로세스에 따라 bHIT 프로토콜의 추가 처리를 위해 요청자에게 전송한다. 도 6에 도시한 바와 같이, 머클 트리의 리프 노드들의 값은 도 5를 통해 설명한 AHC 트리의 노드 값으로 계산할 수 있다. 도 6에서 sk 는 암호화된 비밀 키(secret key)를 의미하고, z 는 암호문(ciphertext)을 의미한다.
- [0068] 도 6과 도 7에 도시한 바와 같이, 요청자가 작업자의 인코딩된 데이터를 복호화한 후 도 7의 머클 트리의 리프 노드가 정확하지 않은 경우, (1) 응답 a 가 지정된 범위 내에 있지 않거나 (2) 해시 값이 올바르지 않는, 즉 작업자의 데이터가 정확하지 않으면 작업자가 성실하지 않음을 의미한다. 이 경우 요청자는 정확하지 않은 리프 노드와 검증결과를 스마트 계약에 전송한다. 작업자의 키 및 관련 보안 약속이 스마트 계약에 저장되기 때문에 스마트 계약은 요청자의 부정 신고가 사실인지 확인할 수 있다.
- [0069] 이처럼 본 발명의 실시예들에 따르면, 요청자와 작업자 간의 신뢰 문제를 해결하기 위한 제3자를 사용하지 않고 허가가 필요하지 않은 블록체인의 스마트계약에 의존하여 분산형 HIT를 효율적으로 수행할 수 있는 프로토콜로 AHC 트리 구조를 따르는 클라우드소싱 프로토콜을 제공한다. 더욱이, 본 발명의 실시예들에 따르면, 단순히 리프 노드의 값 합계를 간단히 커밋하고 효율적으로 확인할 수 있는 AHC 트리를 사용함으로써 오프체인 계산과 같은 암호화 도구를 피하고 온체인 비용을 크게 줄일 수 있다. 또한, 본 발명의 실시예들에 따르면, UC 프레임워크에서 bHIT의 공식 정의를 제공하고 잘못된 보고 및 무임승차를 방지하는 분산형 HIT 기능을 구현할 수 있다.
- [0070] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 프로세서, 컨트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 어플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 컨트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.
- [0071] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 컴퓨터 저장 매체 또는 장치에 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.
- [0072] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 이때, 매체는 컴퓨터로 실행 가능한 프로그램을 계속 저장하거나, 실행 또는 다운로드를 위해 임시 저장하는 것일 수도 있다. 또한, 매체는 단일 또는 수 개의 하드웨어가 결합된 형태의 다

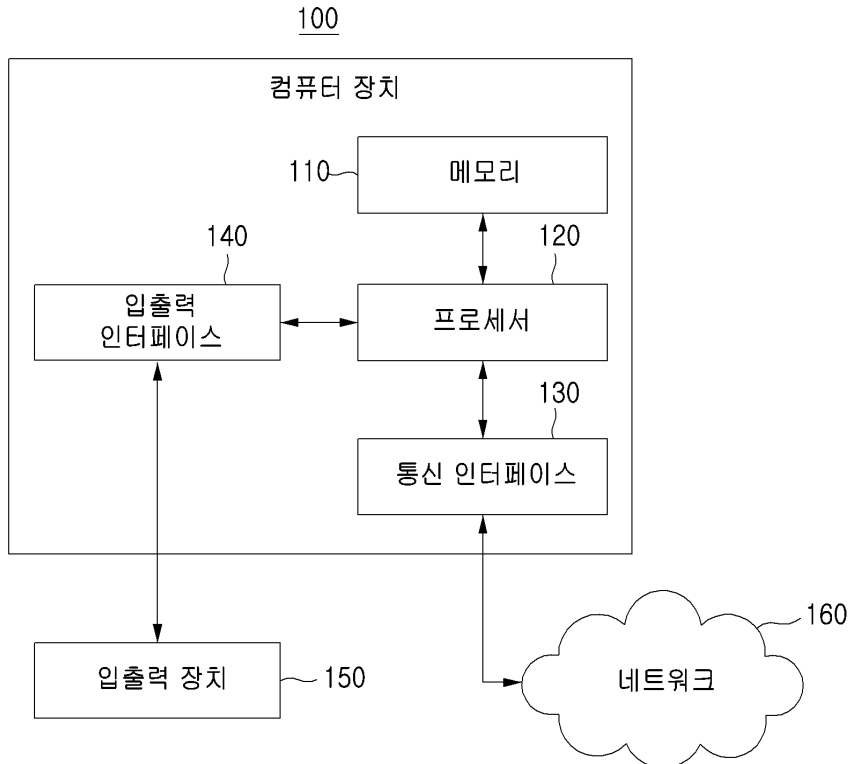
양한 기록수단 또는 저장수단일 수 있는데, 어떤 컴퓨터 시스템에 직접 접속되는 매체에 한정되지 않고, 네트워크 상에 분산 존재하는 것일 수도 있다. 매체의 예시로는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM 및 DVD와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical medium), 및 ROM, RAM, 플래시 메모리 등을 포함하여 프로그램 명령어가 저장되도록 구성된 것이 있을 수 있다. 또한, 다른 매체의 예시로, 어플리케이션을 유통하는 앱 스토어나 기타 다양한 소프트웨어를 공급 내지 유통하는 사이트, 서버 등에서 관리하는 기록매체 내지 저장매체도 들 수 있다.

[0073] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

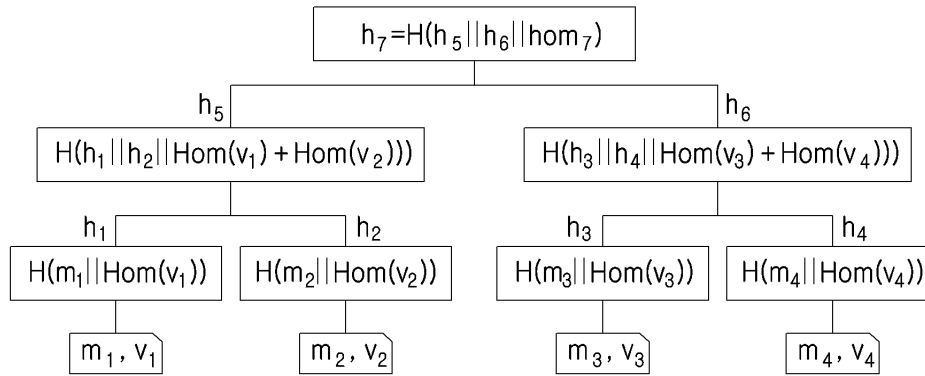
[0074] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

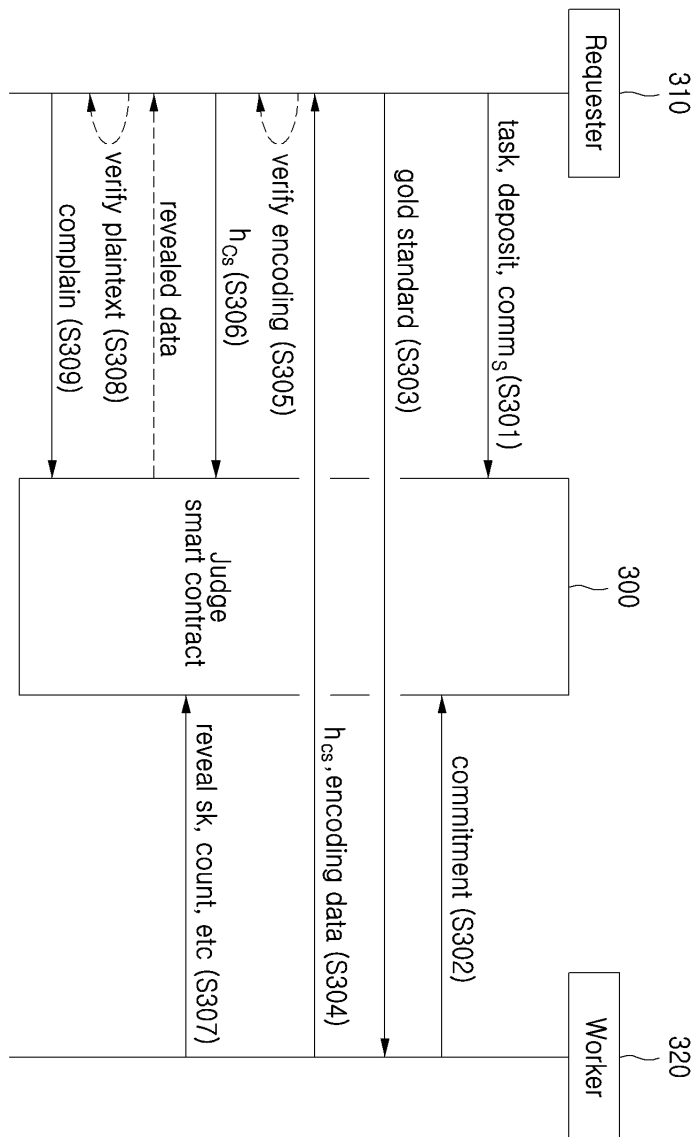
도면1



도면2



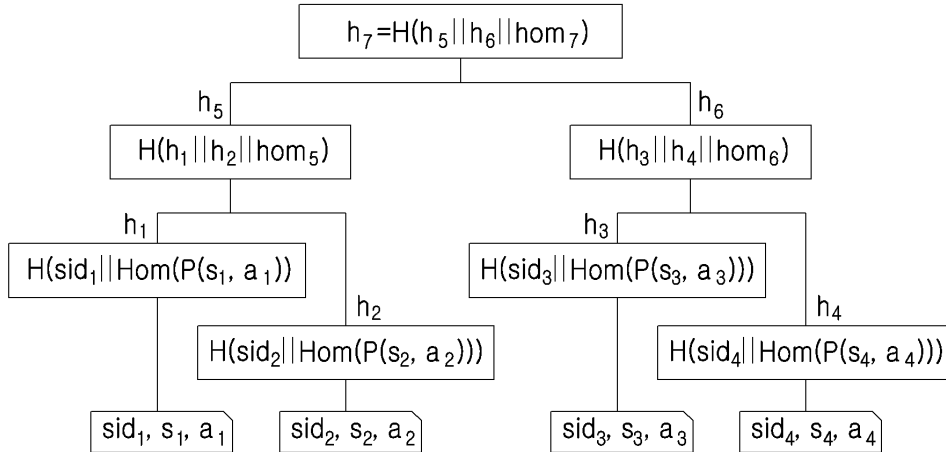
도면3



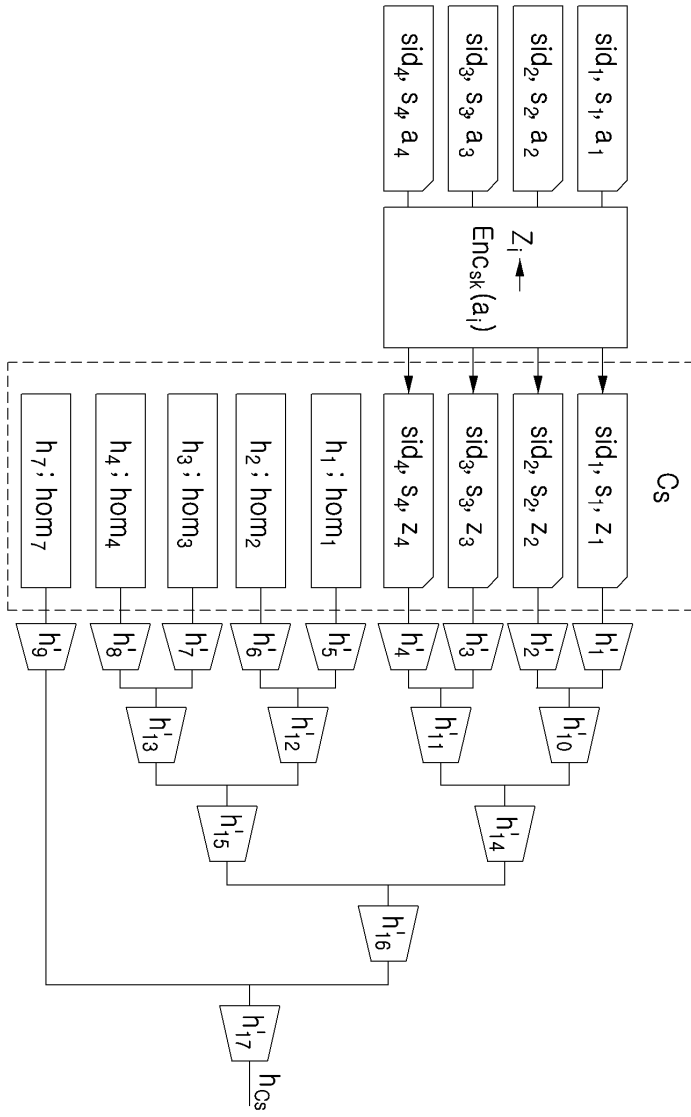
도면4



도면5



도면6



도면7

