(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년12월08일
(11) 등록번호 10-2337760
(24) 등록일자 2021년12월06일

(51) 국제특허분류(Int. Cl.)
H04L 29/08 (2006.01) *G06F 16/23* (2019.01)
G06F 16/27 (2019.01) *G06F 9/46* (2006.01)
H04L 29/06 (2006.01)
(52) CPC특허분류
H04L 67/1002 (2013.01)
G06F 16/2365 (2019.01)
(21) 출원번호 10-2020-0108628
(22) 출원일자 2020년08월27일
심사청구일자 2020년08월27일
(56) 선행기술조사문헌
KR1020190067581 A
KR1020200083145 A

(73) 특허권자
연세대학교 산학협력단
서울특별시 서대문구 연세로 50 (신촌동, 연세대학교)
(72) 발명자
정종문
서울특별시 용산구 이촌로 181, 104동 101호(이촌동, 한강대우아파트)
윤주식
서울특별시 서대문구 신촌로7길 49-6, 202호(창천동, 청송빌)
고윤영
서울특별시 서대문구 신촌로7길 49-15(창천동)
(74) 대리인
민영준

전체 청구항 수 : 총 19 항 심사관 : 황철규

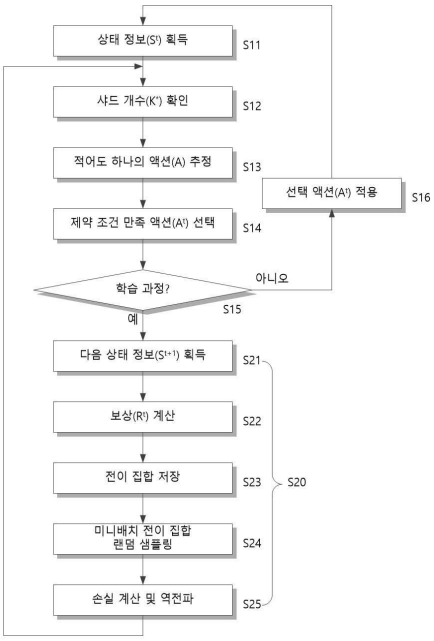
(54) 발명의 명칭 **심층강화학습 기반 적응적 샤드 블록체인 네트워크 관리 장치 및 방법**

(57) 요 약

본 발명은 N개의 노드가 적어도 하나의 샤드에 분배되는 샤드 기반 블록체인 네트워크의 현재 에포크에서의 노드 간 데이터 전송률과 각 노드들의 연산 자원, 각 샤드에서 각 노드들의 합의 과정 기록 및 악의적 노드 비율이 포함된 상태 정보를 획득하고, 패턴 추정 방식이 미리 학습된 인공 신경망을 이용하여, 상태 정보에 대응하는 블록

(뒷면에 계속)

대 표 도 - 도6



사이즈, 블록 간격 및 샤드 개수를 각각 포함하는 적어도 하나의 액션를 추정하며, 추정된 적어도 하나의 액션 중 레이턴시가 연속되는 블록 간격 이하인 제1 제약 조건과 샤드 개수가 보안성을 유지하기 위해 요구되는 기지정된 최대 보안 샤드 개수 이내인 제2 제약 조건을 만족하면서 처리 속도를 최대로 하는 하나의 액션을 선택하여 샤드 기반 블록체인 네트워크에 적용하여, 악의적 노드가 존재하는 경우에도 보안성을 유지하면서 처리 성능을 향상시킬 수 있어 블록체인 네트워크의 확장성을 개선할 수 있는 샤드 블록체인 네트워크 관리 장치 및 방법을 제공할 수 있다.

(52) CPC특허분류
G06F 16/278 (2019.01)
G06F 9/466 (2013.01)
H04L 63/0815 (2013.01)
H04L 67/1097 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711116181
과제번호	IITP-2020-2018-0-01799
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	대학ICT연구센터지원사업
연구과제명	블록체인 비즈니스 서비스 기술 개발 및 인력양성
기 여 율	1/1
과제수행기관명	중앙대학교 산학협력단
연구기간	2020.01.01 ~ 2020.12.31

공지예외적용 : 있음

명 세 서

청구범위

청구항 1

N개의 노드가 적어도 하나의 샤드에 분배되는 샤드 기반 블록체인 네트워크의 현재 에포크(t)에서의 노드간 데이터 전송률(R)과 각 노드들의 연산 자원(c), 각 샤드에서 각 노드들의 합의 과정 기록(H) 및 악의적 노드 비율($\bar{p}$)이 포함된 상태 정보(S^t)를 획득하고, 패턴 추정 방식이 미리 학습된 인공 신경망을 이용하여, 상기 상태 정보(S^t)에 대응하는 블록 사이즈(B), 블록 간격(T^I) 및 샤드 개수(K)를 각각 포함하는 적어도 하나의 액션(A)을 추정하며, 추정된 적어도 하나의 액션(A) 중 레이턴시($T_{latency}$)가 연속되는 블록 간격(uT^I) 이하인 제1 제약 조건과 샤드 개수(K)가 보안성을 유지하기 위해 요구되는 기지정된 최대 보안 샤드 개수($\dot{K}$) 이내인 제2 제약 조건을 만족하면서 처리 속도(TPS)를 최대로 하는 하나의 액션(A^t)을 선택하여 상기 샤드 기반 블록체인 네트워크에 적용하는 샤드 블록체인 네트워크 관리 장치.

청구항 2

제1항에 있어서, 상기 레이턴시($T_{latency}$)는

블록 간격(T^I)과 k개의 샤드 블록을 갖는 샤드 블록 체인 네트워크에서 소모되는 전체 합의 시간(T^k_{con})의 합으로 계산되고,

전체 합의 시간(T^k_{con})은 샤드내 합의 시간(T^k_{intra})과 최종 샤드 합의 시간(T^k_{final})의 합으로 계산되는 샤드 블록체인 네트워크 관리 장치.

청구항 3

제2항에 있어서, 상기 샤드내 합의 시간(T^k_{intra})은

샤드내 합의 과정에서의 메시지 전파 시간($T^k_{in\_prop}$)과 샤드내 합의 과정에서의 검증 시간($T^k_{in\_val}$)의 합으로 계산되고,

상기 최종 샤드 합의 시간(T^k_{final})은

최종 합의 과정에서의 메시지 전파 시간($T^k_{f\_prop}$)과 최종 합의 과정에서의 검증 시간의 합($T^k_{f\_prop}$)으로 계산되는 샤드 블록체인 네트워크 관리 장치.

청구항 4

제3항에 있어서, 상기 전체 합의 시간(T^k_{con})은

수학식

$$
\begin{aligned}
T_{con}^{k} = T_{intra}^{k} + T_{final}^{k} &= (T_{in\_prop}^{k} + T_{in\_val}^{k}) \\
&\quad + (T_{f\_prop}^{k} + T_{f\_val}^{k}) \\
&= \frac{1}{\mathcal{M}} \Big(\max_{i=1,\cdots,k} (T_{in\_replica}^{i}, T_{in\_primary}^{i}) \\
&\quad + \max(T_{f\_primary}^{k}, T_{f\_replica}^{k}) \Big) \\
&\quad + \frac{1}{\mathcal{M}} \max_{i=1,\cdots,k} \Big(\min \left\{ \max_{j \neq p} \frac{\mathcal{M}B}{R_{n_{i,p},n_{i,j}}}, \zeta \right\} \\
&\quad + \min \left\{ \max_{j \neq l} \frac{\mathcal{M}B}{R_{n_{i,j},n_{i,l}}}, \zeta \right\} \\
&\quad + \min \left\{ \max_{j \neq l} \frac{\mathcal{M}B}{R_{n_{i,j},n_{i,l}}}, \zeta \right\} \Big) \\
&\quad + \frac{1}{\mathcal{M}} \Big(\min \left\{ \max_{i=1,\cdots,k; j=1,\cdots,N_i; l=1,\cdots,C} \frac{\mathcal{M}B}{R_{n_{i,j},n_{f,l}}}, \zeta \right\} \\
&\quad + \min \left\{ \max_{l \neq p} \frac{\mathcal{M}B}{R_{n_{f,p},n_{f,l}}}, \zeta \right\} \\
&\quad + \min \left\{ \max_{u \neq p; u,l=1,\cdots,C} \frac{\mathcal{M}B}{R_{n_{f,u},n_{f,l}}}, \zeta \right\} \\
&\quad + \min \left\{ \max_{u \neq l} \frac{\mathcal{M}B}{R_{n_{f,u},n_{f,l}}}, \zeta \right\} \\
&\quad + \min \left\{ \max_{i=1,\cdots,k} \frac{k\mathcal{M}B}{R_{n_{f,u},n_{i,j}}}, \zeta \right\} \Big)
\end{aligned}
$$

(여기서 M은 요청된 블록의 배치 크기(Batch size), $T^{i}_{in\_primary}$ 와 $T^{i}_{in_replica}$는 i번째 샤드내 우선 노드와 복제 노드의 처리 시간, $T^{k}_{f\_primary}$ 와 $T^{k}_{f_replica}$는 k개의 샤드 각각의 샤드내 합의에서 승인된 블록들에 대해 최종 합의를 수행하는 DC(Directory Committee)의 우선 노드와 복제 노드의 처리 시간, $n_{f,p}$ 와 $n_{f,r}$ 는 DC에서의 우선 노드와 복제 노드 번호, $R_{n_{i,j},n_{f,l}}$, $R_{n_{f,p},n_{f,l}}$, $R_{n_{f,u},n_{f,l}}$, $R_{n_{f,u},n_{f,l}}$, $R_{n_{f,u},n_{i,j}}$ 는 첨자로 지정되는 노드들 사이의 전송률을 나타내고, ζ는 기지정된 노드의 응답 제한 시간이다.)

으로 계산되는 샤드 블록체인 네트워크 관리 장치.

청구항 5

제1항에 있어서, 상기 샤드 기반 블록체인 네트워크는

실용적 비잔틴 장애 허용 알고리즘 기법에 따라 합의를 수행하는 샤드 블록체인 네트워크 관리 장치.

청구항 6

제5항에 있어서, 상기 최대 보안 샤드 개수($\dot{K}$)는

각 샤드에서 악의적 노드 비율이 1/3미만이 되도록 하는 샤드 개수를 나타내는 제1 보안성 조건(S_1)과

각 샤드에서 악의적 노드 비율이 2/3미만이 되도록 하는 샤드 개수를 나타내는 제2 보안성 조건(S_2) 각각보다 작은 값 중 최대값으로 설정되는 샤드 블록체인 네트워크 관리 장치.

청구항 7

제6항에 있어서, 상기 제1 보안성 조건(S_1)은

수학식

$$S_1 = \frac{N(1-3p)-1}{3Np+1}$$

(여기서 N은 전체 노드 수, p는 악의적 노드 비율을 나타낸다)

로 계산되고,

상기 제2 보안성 조건(S_2)은

수학식

$$S_2 = \frac{2N}{3(Np+1)} - 1$$

로 계산되는 샤드 블록체인 네트워크 관리 장치.

청구항 8

제1항에 있어서, 상기 샤드 블록체인 네트워크 관리 장치는

패턴 추정 방식이 미리 학습된 인공 신경망을 포함하여 상기 상태 정보(S^t)에 대응하는 다수의 액션(A)을 추정하고, 추정된 다수의 액션(A) 중 상기 제1 및 제2 제약 조건을 만족하며, TPS 를 최대로 하는 액션(A^t)을 선택하는 에이전트부; 및

선택된 액션(A^t)을 상기 샤드 블록체인 네트워크에 적용하여 다음 에포크(t+1)에서의 상태 정보(S^{t+1})와 보상(R^t)을 추정하는 환경 분석부를 포함하는 샤드 블록체인 네트워크 관리 장치.

청구항 9

제8항에 있어서, 상기 샤드 블록체인 네트워크 관리 장치는

상기 상태 정보(S^t)와 선택된 액션(A^t), 선택된 액션(A^t)에 따른 다음 에포크(t+1)에서의 상태 정보(S^{t+1}) 및 보상(R^t)이 전이 집합($[S^t, A^t, R^t, S^{t+1}]$)으로 매칭되어 저장되는 메모리부를 더 포함하고,

상기 에이전트부의 학습시에 상기 메모리부에 저장된 다수의 전이 집합($[S^x, A^x, R^x, S^{x+1}]$)의 미니배치(minibatch)를 기지정된 방식으로 샘플링하고, 샘플링된 전이 집합의 보상(R^x)과 각 상태 정보(S^x, S^{x+1})에 따라 선택되는 액션(A^x, A')에 의한 TPS 차를 기반으로 손실을 추정하고, 추정된 손실을 역전파하는 샤드 블록체인 네트워크 관리 장치.

청구항 10

제1항에 있어서, 상기 TPS는

수학식

$$\mathcal{T}(B, T^I) = \frac{k\lfloor B/b \rfloor}{T^I}$$

(여기서 k는 샤드 개수를 나타내고, b는 평균 트랜잭션 크기를 나타내며, $\lfloor\ \rfloor$는 바닥 함수(floor funciton)를 나타낸다.)으로 계산되는 샤드 블록체인 네트워크 관리 장치.

청구항 11

N개의 노드가 적어도 하나의 샤드에 분배되는 샤드 기반 블록체인 네트워크의 현재 에포크(t)에서의 노드간 데이터 전송률(R)과 각 노드들의 연산 자원(c), 각 샤드에서 각 노드들의 합의 과정 기록(H) 및 악의적 노드 비율

($\bar{p}$)이 포함된 상태 정보(S^t)를 획득하는 단계;

패턴 추정 방식이 미리 학습된 인공 신경망을 이용하여, 상기 상태 정보(S^t)에 대응하는 블록 사이즈(B), 블록 간격(T^I) 및 샤드 개수(K)를 각각 포함하는 적어도 하나의 액션(A)을 추정하는 단계;

추정된 적어도 하나의 액션(A) 중 레이턴시($T_{latency}$)가 연속되는 블록 간격(uT^I) 이하인 제1 제약 조건과 샤드 개수(K)가 보안성을 유지하기 위해 요구되는 기지정된 최대 보안 샤드 개수($\dot{K}$) 이내인 제2 제약 조건을 만족하면서 처리 속도(TPS)를 최대로 하는 하나의 액션(A^t)을 선택하는 단계; 및

선택된 액션(A^t)의 블록 사이즈(B), 블록 간격(T^I) 및 샤드 개수(K^*) 상기 샤드 기반 블록체인 네트워크에 적용하는 단계를 포함하는 샤드 블록체인 네트워크 관리 방법.

청구항 12

제11항에 있어서, 상기 레이턴시($T_{latency}$)는

블록 간격(T^I)과 k개의 샤드 블록을 갖는 샤드 블록 체인 네트워크에서 소모되는 전체 합의 시간(T^k_{con})의 합으로 계산되고,

전체 합의 시간(T^k_{con})은 샤드내 합의 시간(T^k_{intra})과 최종 샤드 합의 시간(T^k_{final})의 합으로 계산되는 샤드 블록체인 네트워크 관리 방법.

청구항 13

제12항에 있어서, 상기 샤드내 합의 시간(T^k_{intra})은

샤드내 합의 과정에서의 메시지 전파 시간($T^k_{in\_prop}$)과 샤드내 합의 과정에서의 검증 시간($T^k_{in\_val}$)의 합으로 계산되고,

상기 최종 샤드 합의 시간(T^k_{final})은

최종 합의 과정에서의 메시지 전파 시간($T^k_{f\_prop}$)과 최종 합의 과정에서의 검증 시간의 합($T^k_{f\_prop}$)으로 계산되는 샤드 블록체인 네트워크 관리 방법.

청구항 14

제13항에 있어서, 상기 전체 합의 시간(T^k_{con})은

수학식

$$
\begin{aligned}
T_{con}^{k} = T_{intra}^{k} + T_{final}^{k} &= (T_{in\_prop}^{k} + T_{in\_val}^{k}) \\
&\quad + (T_{f\_prop}^{k} + T_{f\_val}^{k}) \\
&= \frac{1}{\mathcal{M}} \Big(\max_{i=1,\cdots,k} (T_{in\_replica}^{i}, T_{in\_primary}^{i}) \\
&\quad + \max(T_{f\_primary}^{k}, T_{f\_replica}^{k}) \Big) \\
&\quad + \frac{1}{\mathcal{M}} \max_{i=1,\cdots,k} \Big(\min \left\{ \max_{j \neq p} \frac{\mathcal{M}B}{R_{n_{i,p},n_{i,j}}}, \zeta \right\} \\
&\quad + \min \left\{ \max_{j \neq l} \frac{\mathcal{M}B}{R_{n_{i,j},n_{i,l}}}, \zeta \right\} \\
&\quad + \min \left\{ \max_{j \neq l} \frac{\mathcal{M}B}{R_{n_{i,j},n_{i,l}}}, \zeta \right\} \Big) \\
&\quad + \frac{1}{\mathcal{M}} \Big(\min \left\{ \max_{i=1,\cdots,k; j=1,\cdots,N_i; l=1,\cdots,C} \frac{\mathcal{M}B}{R_{n_{i,j},n_{f,l}}}, \zeta \right\} \\
&\quad + \min \left\{ \max_{l \neq p} \frac{\mathcal{M}B}{R_{n_{f,p},n_{f,l}}}, \zeta \right\} \\
&\quad + \min \left\{ \max_{u \neq p; u,l=1,\cdots,C} \frac{\mathcal{M}B}{R_{n_{f,u},n_{f,l}}}, \zeta \right\} \\
&\quad + \min \left\{ \max_{u \neq l} \frac{\mathcal{M}B}{R_{n_{f,u},n_{f,l}}}, \zeta \right\} \\
&\quad + \min \left\{ \max_{i=1,\cdots,k} \frac{k\mathcal{M}B}{R_{n_{f,u},n_{i,j}}}, \zeta \right\} \Big)
\end{aligned}
$$

(여기서 M은 요청된 블록의 배치 크기(Batch size), $T^{i}_{in\_primary}$ 와 $T^{i}_{in_replica}$는 i번째 샤드내 우선 노드와 복제 노드의 처리 시간, $T^{k}_{f\_primary}$ 와 $T^{k}_{f_replica}$는 k개의 샤드 각각의 샤드내 합의에서 승인된 블록들에 대해 최종 합의를 수행하는 DC(Directory Committee)의 우선 노드와 복제 노드의 처리 시간, $n_{f,p}$ 와 $n_{f,r}$ 는 DC에서의 우선 노드와 복제 노드 번호, $R_{n_{i,j},n_{f,l}}$, $R_{n_{f,p},n_{f,l}}$, $R_{n_{f,u},n_{f,l}}$, $R_{n_{f,u},n_{f,l}}$, $R_{n_{f,u},n_{i,j}}$ 는 첨자로 지정되는 노드들 사이의 전송률을 나타내고, ζ는 기지정된 노드의 응답 제한 시간이다.)

으로 계산되는 샤드 블록체인 네트워크 관리 방법.

청구항 15

제11항에 있어서, 상기 샤드 기반 블록체인 네트워크는

실용적 비잔틴 장애 허용 알고리즘 기법에 따라 합의를 수행하는 샤드 블록체인 네트워크 관리 방법.

청구항 16

제15항에 있어서, 상기 최대 보안 샤드 개수($\dot{K}$)는

각 샤드에서 악의적 노드 비율이 1/3미만이 되도록 하는 샤드 개수를 나타내는 제1 보안성 조건(S_1)과

각 샤드에서 악의적 노드 비율이 2/3미만이 되도록 하는 샤드 개수를 나타내는 제2 보안성 조건(S_2) 각각보다 작은 값 중 최대값으로 설정되는 샤드 블록체인 네트워크 관리 방법.

청구항 17

제16항에 있어서, 상기 제1 보안성 조건(S_1)은

수학식

$$S_1 = \frac{N(1-3p)-1}{3Np+1}$$

(여기서 N은 전체 노드 수, p는 악의적 노드 비율을 나타낸다)

로 계산되고,

상기 제2 보안성 조건(S_2)은

수학식

$$S_2 = \frac{2N}{3(Np+1)} - 1$$

로 계산되는 샤드 블록체인 네트워크 관리 방법.

청구항 18

제11항에 있어서, 상기 샤드 블록체인 네트워크 관리 방법은

상기 인공 신경망을 학습시키기 위한 학습 단계를 더 포함하고,

상기 학습 단계는

상기 상태 정보(S^t)와 선택된 액션(A^t), 선택된 액션(A^t)에 따른 다음 에포크(t+1)에서의 상태 정보(S^{t+1}) 및 보상(R^t)이 전이 집합([S^t, A^t, R^t, S^{t+1}])으로 매칭하여 저장하는 단계;

저장된 다수의 전이 집합의 미니배치(minibatch)를 기지정된 방식으로 샘플링하는 단계;

다수의 전이 집합([S^x, A^x, R^x, S^{x+1}])의 미니배치(minibatch)를 기지정된 방식으로 샘플링하고, 샘플링된 전이 집합의 보상(R^x)과 각 상태 정보(S^x, S^{x+1})에 따라 선택되는 액션(A^x, A')에 의한 TPS 차를 기반으로 손실을 추정하는 단계; 및

추정된 손실을 역전파하는 단계를 포함하는 샤드 블록체인 네트워크 관리 방법.

청구항 19

제11항에 있어서, 상기 TPS는

수학식

$$\mathcal{T}(B, T^I) = \frac{k\lfloor B/b \rfloor}{T^I}$$

(여기서 k는 샤드 개수를 나타내고, b는 평균 트랜잭션 크기를 나타내며, $\lfloor\ \rfloor$는 바닥 함수(floor funciton)를 나타낸다.)으로 계산되는 샤드 블록체인 네트워크 관리 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 샤드 블록체인 네트워크 관리 장치 및 방법에 관한 것으로, 심층강화학습에 기반하여 보안성을 유지하면서 트랜잭션 처리 속도 네트워크 상황에 따라 적응적으로 향상시킬 수 있는 샤드 블록체인 네트워크 관리 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 블록체인은 기존의 중앙화된 기관이 거래 내용을 단일 위치(single point)에 저장하는 중앙화된 방식을 탈피하

고자 등장한 탈중앙화 분산 트랜잭션 관리 기술이다. 블록체인에서는 거래내역 및 장부에 대한 트랜잭션들을 모든 검증인 노드들이 P2P (Peer to Peer) 방식으로 검사하고, 과반수 노드들에 의해 합의를 얻은 경우 각 검증 노드들은 해당 거래내역모음을 해시 체인(Hash-chain)형태로 저장한다. 이는 분산데이터 저장의 한 기술로서 악의적 노드에 의한 데이터, 거래내역 조작이 불가능하도록 고안되었다. 블록체인 기술은 현재 암호화폐에서 주로 사용되고 있다. 블록체인에서 데이터를 조작하려면, 검증인자로 참여하는 다수의 노드의 과반수 이상의 블록들 모두를 제한된 시간 내에 수정해야 하므로, 실질적으로 데이터 조작이 거의 불가능한 것으로 알려져 있다.

[0003] 다만 블록체인에서는 다수의 노드 각각이 블록을 검증함에 따라 트랜잭션에 대한 낮은 처리 속도(transactions per second: 이하 TPS)로 인해, 사물 인터넷(IoT)과 같이 대규모 데이터를 생성하는 다수의 사용자가 참여하는 네트워크에서 적용되기에는 어려움이 있다. 즉 IoT와 같은 대규모의 사용자 그룹이 합의 과정에 참여하게 되면, 블록을 체인에 연결하는 인증과정에서 복잡성으로 인해 TPS가 낮아지게 되고, 원장의 크기가 증가하고 블록체인 크기가 증가함에 따라 확장성(Scalability) 문제가 발생하여 분산 방식으로 블록체인을 관리하기 어려워진다.

[0004] 또한, 5G 통신의 활용과 IoT 장치의 비약적인 성장으로 IoT 네트워크에서 방대한 양의 대규모 데이터 트랜잭션을 처리하기 위해서는 신뢰할 수 있는 높은 TPS를 가지는 성능이 필수적이다. 따라서, IoT 네트워크를 지원하는 미래의 블록체인 시스템은 기존의 블록체인 시스템보다 더 향상된 확장성을 가져야 한다.

[0005] 그러나 기존의 대표적인 합의 알고리즘인 작업증명(Proof of Work: 이하 PoW) 알고리즘을 이용하는 블록체인에서는 7 ~ 10 TPS의 낮은 처리속도를 가진다. 이러한 낮은 TPS는 IoT 네트워크에서 데이터 처리하는데 적합하지 않다. 특히 작업증명 알고리즘은 반복되는 해시 연산이 필요하기 때문에 많은 에너지와 시간이 소모된다.

[0006] 이에 현재는 PoW 알고리즘을 지분증명(Proof of Stake: 이하 PoS)이나 실용적 비잔틴 장애 허용(Practical Byzantine Fault Tolerance: 이하 PBFT) 알고리즘 체계로 대체함으로써 복잡한 해시 연산의 계산 비용을 감소시키는 방법이 제안되어 주로 이용되고 있다.

[0007] 한편, 상기한 합의 알고리즘 이외에도, 블록체인 시스템의 확장성 문제를 해결하기 위한 다양한 솔루션들이 연구되었으며, 크게 온-체인(on-chain) 솔루션과 오프-체인(off-chain) 솔루션으로 구분될 수 있다.

[0008] 이중 온-체인 솔루션은 블록크기, 블록생성주기, 블록생성자 등 블록체인 변수들을 조정하여 TPS를 향상시키는 방법을 사용한다. 예를 들어, 온 체인 솔루션에서는 합의에 참여하는 노드들의 수를 줄임으로써 메시지 복잡도를 줄여 합의에 도달하는 시간을 짧게하여 TPS를 향상시킬 수 있다. 특히 샤딩(Sharding) 기법에서는 트랜잭션을 병렬처리하는 개념을 도입하여, 블록체인 검증 노드들을 여러 개의 샤드 그룹으로 임의로 분배하고, 다수의 샤드가 각각 트랜잭션을 병렬 처리하도록 하여 TPS가 샤드의 개수에 비례하여 향상되도록 한다. 다만 샤딩 기법의 경우, 악의적 노드가 하나의 샤드에 다수를 차지 하기 더 쉬워지는 문제가 생기기 때문에 보안 레벨은 감소될 수 있다.

[0009] 블록체인 트릴레마(trilemma)에 따르면, 블록체인 시스템에서는 블록체인의 3가지 특징(탈중앙화, 보안성, 확장성) 중 2가지만 가질 수 있다. 즉 한 가지 특징을 극대화하게 되면 다른 특징이 급격히 감소하게 된다.

[0010] 따라서, 보안성을 유지하거나 향상시키면서도 TPS를 향상시켜 블록체인의 확장성을 개선할 수 있는 방안이 요구되고 있다.

선행기술문헌

특허문헌

[0011] (특허문헌 0001) 한국 공개 특허 제10-2020-0059136호 (2020.05.28 공개)

발명의 내용

해결하려는 과제

[0012] 본 발명의 목적은 블록체인 네트워크의 트랜잭션 처리 속도를 향상시켜 확장성을 개선할 수 있는 샤드 블록체인 네트워크 관리 장치 및 방법을 제공하는데 있다.

[0013] 본 발명의 다른 목적은 블록체인 네트워크의 확장성을 개선하면서도 보안성을 유지하거나 향상시킬 수 있는 샤드 블록체인 네트워크 관리 장치 및 방법을 제공하는데 있다.

과제의 해결 수단

[0014] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 샤드 블록체인 네트워크 관리 장치는 N개의 노드가 적어도 하나의 샤드에 분배되는 샤드 기반 블록체인 네트워크의 현재 에포크(t)에서의 노드간 데이터 전송률(R)과 각 노드들의 연산 자원(c), 각 샤드에서 각 노드들의 합의 과정 기록(H) 및 악의적 노드 비율($\bar{p}$)이 포함된 상태 정보(S^t)를 획득하고, 패턴 추정 방식이 미리 학습된 인공 신경망을 이용하여, 상기 상태 정보(S^t)에 대응하는 블록 사이즈(B), 블록 간격(T^I) 및 샤드 개수(K)를 각각 포함하는 적어도 하나의 액션(A)을 추정하며, 추정된 적어도 하나의 액션(A) 중 레이턴시($T_{latency}$)가 연속되는 블록 간격(uT^I) 이하인 제1 제약 조건과 샤드 개수(K)가 보안성을 유지하기 위해 요구되는 기지정된 최대 보안 샤드 개수($\dot{K}$) 이내인 제2 제약 조건을 만족하면서 처리 속도(transactions per second: 이하 TPS)를 최대로 하는 하나의 액션(A^t)을 선택하여 상기 샤드 기반 블록체인 네트워크에 적용한다.

[0015] 상기 레이턴시($T_{latency}$)는 블록 간격(T^I)과 k개의 샤드 블록을 갖는 샤드 블록 체인 네트워크에서 소모되는 전체 합의 시간(T^k_{con})의 합으로 계산되고, 전체 합의 시간(T^k_{con})은 샤드내 합의 시간(T^k_{intra})과 최종 샤드 합의 시간(T^k_{final})의 합으로 계산될 수 있다.

[0016] 상기 샤드내 합의 시간(T^k_{intra})은 샤드내 합의 과정에서의 메시지 전파 시간($T^k_{in\_prop}$)과 샤드내 합의 과정에서의 검증 시간($T^k_{in\_val}$)의 합으로 계산되고, 상기 최종 샤드 합의 시간(T^k_{final})은 최종 합의 과정에서의 메시지 전파 시간($T^k_{f\_prop}$)과 최종 합의 과정에서의 검증 시간의 합($T^k_{f\_prop}$)으로 계산될 수 있다.

[0017] 상기 샤드 기반 블록체인 네트워크는 실용적 비잔틴 장애 허용 알고리즘 기법에 따라 합의를 수행할 수 있다.

[0018] 상기 최대 보안 샤드 개수($\dot{K}$)는 각 샤드에서 악의적 노드 비율이 1/3미만이 되도록 하는 샤드 개수를 나타내는 제1 보안성 조건(S_1)과 각 샤드에서 악의적 노드 비율이 2/3미만이 되도록 하는 샤드 개수를 나타내는 제2 보안성 조건(S_2) 각각보다 작은 값 중 최대값으로 설정될 수 있다.

[0019] 상기 샤드 블록체인 네트워크 관리 장치는 패턴 추정 방식이 미리 학습된 인공 신경망을 포함하여 상기 상태 정보(S^t)에 대응하는 다수의 액션(A)을 추정하고, 추정된 다수의 액션(A) 중 상기 제1 및 제2 제약 조건을 만족하며, TPS 를 최대로 하는 액션(A^t)을 선택하는 에이전트부; 및 선택된 액션(A^t)을 상기 샤드 블록체인 네트워크에 적용하여 다음 에포크(t+1)에서의 상태 정보(S^{t+1})와 보상(R^t)을 추정하는 환경 분석부를 포함할 수 있다.

[0020] 상기 샤드 블록체인 네트워크 관리 장치는 상기 상태 정보(S^t)와 선택된 액션(A^t), 선택된 액션(A^t)에 따른 다음 에포크(t+1)에서의 상태 정보(S^{t+1}) 및 보상(R^t)이 전이 집합([S^t, A^t, R^t, S^{t+1}])으로 매칭되어 저장되는 메모리부를 더 포함하고, 상기 에이전트부의 학습시에 상기 메모리부에 저장된 다수의 전이 집합([S^x, A^x, R^x, S^{x+1}])의 미니배치(minibatch)를 기지정된 방식으로 샘플링하고, 샘플링된 전이 집합의 보상(R^x)과 각 상태 정보(S^x, S^{x+1})에 따라 선택되는 액션(A^x, A')에 의한 TPS 차를 기반으로 손실을 추정하고, 추정된 손실을 역전파할 수 있다.

[0021] 상기 목적을 달성하기 위한 본 발명의 다른 실시예에 따른 샤드 블록체인 네트워크 관리 방법은 N개의 노드가 적어도 하나의 샤드에 분배되는 샤드 기반 블록체인 네트워크의 현재 에포크(t)에서의 노드간 데이터 전송률(R)과 각 노드들의 연산 자원(c), 각 샤드에서 각 노드들의 합의 과정 기록(H) 및 악의적 노드 비율($\bar{p}$)이 포함된 상태 정보(S^t)를 획득하는 단계; 패턴 추정 방식이 미리 학습된 인공 신경망을 이용하여, 상기 상태 정보

(S^t)에 대응하는 블록 사이즈(B), 블록 간격(T^I) 및 샤드 개수(K)를 각각 포함하는 적어도 하나의 액션(A)을 추정하는 단계; 추정된 적어도 하나의 액션(A) 중 레이턴시($T_{latency}$)가 연속되는 블록 간격(uT^I) 이하인 제1 제약조건과 샤드 개수(K)가 보안성을 유지하기 위해 요구되는 기지정된 최대 보안 샤드 개수($\dot{K}$) 이내인 제2 제약조건을 만족하면서 처리 속도(transactions per second: 이하 TPS)를 최대로 하는 하나의 액션(A^t)을 선택하는 단계; 및 선택된 액션(A^t)의 블록 사이즈(B), 블록 간격(T^I) 및 샤드 개수(K^*) 상기 샤드 기반 블록체인 네트워크에 적용하는 단계를 포함한다.

발명의 효과

[0022] 따라서, 본 발명의 실시예에 따른 샤드 블록체인 네트워크 관리 장치 및 방법은 심층강화학습에 기반하여 학습되어, 네트워크의 상황에 따라 적응적으로 블록 사이즈, 블록 간격 및 샤드의 개수를 조절함으로써 악의적 노드가 존재하는 경우에도 보안성을 유지하면서 처리 성능을 향상시킬 수 있다. 그러므로 블록체인 네트워크의 확장성을 개선할 수 있어, IoT 네트워크와 같이 대규모 트랜잭션이 처리되어야 하는 환경에서도 블록체인이 용이하게 이용되도록 할 수 있다.

도면의 간단한 설명

[0023] 도 1은 IoT 네트워크 환경에서의 샤드 기반 블록체인 네트워크의 개략적 구조를 나타낸다.

도 2는 본 발명의 일 실시예에 따른 네트워크 관리 장치의 개략적 구조를 나타낸다.

도 3은 도 2의 네트워크 설정부의 개략적 구조를 나타낸다.

도 4는 도 3의 에이전트부를 구성하는 인공 신경망의 일 예를 나타낸다.

도 5는 샤드 블록체인 네트워크의 합의 과정을 설명하기 위한 도면이다.

도 6은 본 발명의 일 실시예에 따른 블록체인 네트워크 관리 방법을 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0024] 본 발명과 본 발명의 동작상의 이점 및 본 발명의 실시에 의하여 달성되는 목적을 충분히 이해하기 위해서는 본 발명의 바람직한 실시예를 예시하는 첨부 도면 및 첨부 도면에 기재된 내용을 참조하여야만 한다.

[0025] 이하, 첨부한 도면을 참조하여 본 발명의 바람직한 실시예를 설명함으로써, 본 발명을 상세히 설명한다. 그러나, 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 설명하는 실시예에 한정되는 것이 아니다. 그리고, 본 발명을 명확하게 설명하기 위하여 설명과 관계없는 부분은 생략되며, 도면의 동일한 참조부호는 동일한 부재임을 나타낸다.

[0026] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라, 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "...부", "...기", "모듈", "블록" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[0027] 도 1은 IoT 네트워크 환경에서의 샤드 기반 블록체인 네트워크의 개략적 구조를 나타낸다.

[0028] 도 1을 참조하면, 스마트 홈, 스마트 차량 등 다양한 IoT 기기가 배치된 IoT 네트워크(10)에서 각 기기는 지정된 동작을 수행하며, 상호 통신함으로써 다양한 트랜잭션 데이터들을 생성한다. 그리고 생성된 트랜잭션들은 블록체인 네트워크(20)를 통해서 각 도메인에서 서로 공유될 수 있다.

[0029] 블록체인 네트워크(20)는 IoT 네트워크(10)로부터 트랜잭션을 받아 분산원장의 역할을 하는 블록에 기록해 신뢰성 있는 데이터 관리를 한다. 다만 IoT 네트워크(10)로부터 대량의 트랜잭션이 인가되므로, 인가된 트랜잭션을 신속하게 처리할 수 있어야 한다. 즉 트랜잭션 처리 속도(Transactions Per Second: 이하 TPS)가 향상되어야 한다.

[0030] 이에 블록체인 네트워크(20)는 IoT 네트워크(10)로부터 인가되는 대량의 트랜잭션을 병렬적으로 처리하는 샤드 기반 블록체인 네트워크로 구성될 수 있다.

[0031] 도 1에 도시된 바와 같이, 샤드 기반 블록체인 네트워크(20)는 다수의 노드를 다수의 샤드(shard)(shard 1 ~ shard K)으로 분배하고, 분배된 각 샤드에서 다수의 트랜잭션을 분할하여 병렬로 처리함으로써 TPS를 향상시킬 수 있다.

[0032] 샤드 블록체인 네트워크(20)에서 트랜잭션을 처리하는 과정은 먼저 블록체인 검증자에 해당하는 다수의 노드가 다수의 샤드(shard 1 ~ shard K)로 분배된다. 그리고 각 샤드(shard 1 ~ shard K)에서 검증자들은 샤드 내 합의를 통해서 독립적으로 블록을 만들고 블록의 무결성을 검증한다. 이후 각 샤드에서 생성된 블록은 마지막 합의를 통해 합쳐지고 합쳐진 새로운 블록이 블록체인에 연결된다.

[0033] 블록체인 네트워크(20)의 다수의 노드는 상기한 바와 같이 기본적으로 블록의 유효성을 검증하는 검증 노드로서 기능하며, 다수의 노드 중 적어도 하나의 노드는 네트워크 관리 장치로 기능할 수 있다.

[0034] 본 실시예에서 네트워크 관리 장치로 기능하는 노드는 블록체인 네트워크(20)의 상태에 따라 블록체인 네트워크(20)의 TPS를 향상시킬 수 있으며, TPS가 향상됨에도 블록체인 네트워크의 보안성이 유지되거나 더욱 향상될 수 있도록 관리한다. 즉 블록체인 네트워크를 최적화하여 블록체인 네트워크의 확장성이 개선되도록 할 수 있다. 특히 본 실시예에 따른 네트워크 관리 장치는 심층강화학습 방식으로 학습되어 블록체인 네트워크의 상태에 따라 적응적으로 블록체인 네트워크를 최적화하여 관리할 수 있다.

[0035] 상기에서는 설명의 편의를 위하여 IoT 네트워크(10)와 블록체인 네트워크(20)를 구분하였으나, IoT 네트워크(10)의 다수의 IoT 기기들은 블록체인 네트워크(20)의 노드로 동작할 수 있다.

[0036] 도 2는 본 발명의 일 실시예에 따른 네트워크 관리 장치의 개략적 구조를 나타낸다.

[0037] 도 2를 참조하면, 본 실시예에 따른 네트워크 관리 장치는 통신부(110), 제어부(120), 블록 생성부(130), 신뢰도 계산부(140), 블록 저장부(150) 및 네트워크 설정부(160)를 포함할 수 있다.

[0038] 통신부(110)는 네트워크 관리 장치가 블록체인 네트워크 상의 다른 노드들과 통신을 수행할 수 있도록 한다. 그리고 제어부(120)는 노드의 각 구성요소를 제어하여 내부에서 각 구성 요소 사이의 데이터를 전달할 뿐만 아니라 통신부(110)를 제어하여 다른 노드와 데이터를 송수신한다.

[0039] 블록 생성부(130)는 노드가 블록 생성권자로 선택되면, 처리해야할 트랜잭션을 수집하고 기록 및 검증하여 블록을 생성한다. 여기서 블록 생성부(130)는 다수의 노드가 이미 다수의 샤드에 분배된 상태라면, 블록 생성부(130)는 해당 노드가 포함된 샤드에서 처리해야할 트랜잭션을 수집하여 블록을 생성할 수 있다. 그리고 생성된 블록을 통신부(110)를 통해 블록체인 네트워크에 전파한다.

[0040] 블록 생성권자는 작업 증명(Proof of Work: PoW) 또는 지분 증명(Proof of Stake: PoS) 기법에 따라 선택될 수 있다. 작업 증명(PoW) 기법에서는 매번 블록을 생성하기에 앞서 모든 검증 노드들은 특정 난이도 미만의 해시(hash)값을 찾는 작업을 수행하고, 특정 난이도 미만의 해시값 중 가장 낮은 해시값을 제안한 노드에게 블록 생성권자로 선택된다. 여기서 생성된 블록은 블록체인 네트워크의 다수의 노드에 의한 합의 과정을 거쳐 과반수 이상의 동의를 받게 되면 최종 블록으로 선언되어 각 노드에 이전 저장된 블록체인에 연결된다.

[0041] 한편 지분 증명(PoS) 기법은 작업 증명(PoW) 기법에서의 과도한 해시 연산 부담을 줄이기 위해 제안된 기법으로 각 노드가 보유한 지분(Stake) 및 지분의 보유기간에 따라 블록 생성권자가 확률적으로 선택된다. 만약 모든 노드들의 지분과 보유기간이 동일하다면, 블록 생성권자는 다수의 노드가 동일 확률로 랜덤하게 선택될 수 있다.

[0042] 본 실시예에서 블록 생성권자는 작업 증명(PoW) 또는 지분 증명(PoS) 기법 또는 다른 기법으로도 선택될 수 있으나, 여기서는 일 예로 작업 증명(PoW) 기법을 기반으로 블록 생성권자가 결정되는 것으로 가정한다.

[0043] 신뢰도 계산부(140)는 블록 생성권자로 선택된 노드에서 생성되고 전파된 블록의 유효성을 검증하고, 다른 노드들의 블록 검증 결과를 함께 고려하여 블록합의 결과를 판별하여 승인 여부를 결정한다. 이때 신뢰도 계산부(140)는 노드가 특정 샤드에 포함된 상태이면 해당 샤드 내의 블록 생성권자에서 생성된 블록과 다른 노드들의 블록 검증 결과를 인가받을 수 있다.

[0044] 블록 저장부(150)는 신뢰도 계산부(140)에서 유효한 것으로 판별된 블록을 인가받아 저장한다. 이때 블록 저장부(150)는 이전 저장된 블록체인에 인가된 블록을 연결하여 저장한다. 그리고 저장된 블록체인을 블록체인 네트워크의 다른 노드들로 전파할 수 있다.

[0045] 상기에서는 노드가 블록체인 네트워크에서 제안된 블록의 유효성을 검증하는 검증자로 기능을 수행하는 경우의

구성을 설명하였다. 그러나 상기한 바와 같이 블록체인 네트워크의 다수의 노드 중 적어도 하나의 노드는 네트워크 관리자로도 기능할 수 있으며, 특정 샤드의 샤드 매니저로도 기능할 수 있다.

[0046] 노드가 샤드 매니저인 경우, 신뢰도 계산부(140)는 샤드에 포함된 다수의 노드에서 획득된 신뢰도를 인가받아 로컬 합의 결과를 획득하고, 획득된 로컬 합의 결과에 기반하여 각 노드에 대한 평균 신뢰도를 획득할 수 있다.

[0047] 한편 노드가 네트워크 관리자인 경우, 해당 노드는 네트워크 설정부(160)를 더 포함할 수 있다. 여기서 네트워크 설정부(160)는 통신부(110)를 통해 수집되는 블록체인 네트워크(20)의 상태 정보(state)(S)를 기반으로 블록체인 네트워크를 관리하기 위한 동작(action)(A)을 설정할 수 있다. 여기서 네트워크 설정부(160)는 심층강화학습(deep reinforcement learning: DRL) 방식으로 미리 학습되는 인공 신경망을 포함하여 구현될 수 있다. 일 예로 본 실시예에서 네트워크 설정부(160)는 인공 신경망 중에서 DRL 방식으로 학습되는 심층 Q 네트워크(Deep Q Network) 모듈을 포함하여 구성될 수 있다.

[0048] 네트워크 설정부(160)는 블록체인 네트워크(20)의 상태 정보(S)로서 블록체인 네트워크(20)의 노드간 데이터 전송률(R)과 각 노드들의 연산 자원(c) 및 각 샤드에서 각 노드들의 합의 과정 기록(H)을 수집하고, 악의적 노드 확률($\bar{p}$)을 추정한다. 즉 데이터 전송률(R)과 연산 자원(c), 합의 과정 기록(H) 및 악의적 노드 확률($\bar{p}$)이 상태 정보(S = [R, c, H, $\bar{p}$])에 포함된다.

[0049] 블록체인 네트워크(20)에서 검증자(validator)로서 N개의 노드(n)가 존재하고 N개의 노드는 샤딩 기법에 따라 k개의 샤드로 분배될 수 있다. 그리고 샤드 구성이 완료된 후 블록체인 네트워크(20)는 합의가 수행되도록 정의된 기간을 나타내는 에포크 구간 동안 다수의 노드들의 블록 합의가 수행되어야 한다. 그리고 특정 노드가 특정 샤드에 장기간 참여하는 것을 방지하기 위해 매 에포크 구간마다 샤드는 새로이 재구성될 수 있다.

[0050] t번째 에포크에서 i번째 노드(n_i)와 j번째 노드(n_j) 사이의 전송률($R_{i,j}$)은 유한 상태 마르코프 채널 모델을 기반으로 H 개의 레벨로 양자화(R = {R_1, R_2, …, R_H})될 수 있으며, 상태 전이 확률 행렬($[p_R(t)]_{H\times H}$)은 H 시 H 크기로 $p_{\mathcal{R}}(t)=\Pr[R_{i,j}(t+1) = \mathcal{R}_b \mid R_{i,j}(t) = \mathcal{R}_a]$ 로 계산될 수 있다.

[0051] 네트워크 설정부(160)는 블록체인 네트워크(20)의 상태 정보(S)로서 데이터 전송률(R)과 연산 자원(c), 합의 과정 기록(H) 및 악의적 노드 확률($\bar{p}$)을 획득하고, 획득된 상태 정보(S)에 기반하여 미리 학습된 방식에 따라 블록체인 네트워크(20)를 최적화하기 위한 액션(A)을 결정한다. 여기서 네트워크 설정부(160)는 보안성을 유지하면서 시간 지연 및 TPS를 개선하여 블록체인 네트워크(20)의 확장성을 향상시킬 수 있도록 액션(A)을 결정함으로써, 다양한 환경 변화에도 블록체인 네트워크(20)가 최적화될 수 있도록 한다. 네트워크 설정부(160)가 블록체인 네트워크(20)를 최적화하기 위해 결정하는 액션(A = [B, T^I, K^*])에는 블록 사이즈(B), 블록 간격(T^I) 및 샤드 개수(K^*)가 포함될 수 있다.

[0052] 그리고 네트워크 설정부(160)는 블록체인 네트워크(20) 상의 다수의 노드를 결정된 개수(K^*)의 샤드에 분배할 수 있으며, 분배된 샤드 블록의 다수의 노드들은 결정된 블록 사이즈(B) 및 블록 간격(T^I)에 따라 블록을 전달할 수 있다.

[0053] 이에 블록체인 네트워크(20)의 현재 상태 정보(S^t)는 결정된 액션(A^t)에 의해 새로운 다음 상태 정보(S^{t+1})로 변경되고, 네트워크 설정부(160)는 변경된 다음 상태 정보(S^{t+1})와 다음 상태 정보(S^{t+1}) 따른 보상(Reward)(R^t)을 관측할 수 있다.

[0054] 즉 네트워크 설정부(160)는 블록체인 네트워크(20)가 합의에 도달하도록 미리 정의된 기간을 나타내는 단위인 에포크 중 현재 에포크(t)에서의 상태 정보(S^t = [R, c, H, $\bar{p}$]^t)에 포함된 데이터 전송률(R)과 연산 자원(c), 합의 과정 기록(H) 및 악의적 노드 확률($\bar{p}$)을 기반으로 블록체인 네트워크(20)의 액션(A^t = [B, T^I, K^*]^t)에 포함될 노드 사이에 전송될 블록 사이즈(B), 블록 간격(T^I) 및 다수의 노드가 분배될 샤드 개수(K^*)를 결정한다. 그리고 결정된 액션(A^t)에 따른 다음 에포크(t+1)에서의 상태 정보(S^{t+1})와 보상(R^t)을 관측하여 다음 액션(A^{t+1})

을 설정하는 과정을 보상(R^t)을 관측함으로써 블록체인 네트워크(20)를 최적화시킬 수 있다.

[0055] 도 3은 도 2의 네트워크 설정부의 개략적 구조를 나타내고, 도 4는 도 3의 에이전트부를 구성하는 인공 신경망의 일 예를 나타낸다.

[0056] 상기한 바와 같이, 본 실시예에 따른 네트워크 관리 장치에서 네트워크 설정부(160)는 심층강화학습 방식으로 학습되는 인공 신경망을 포함하여 구현될 수 있다. 도 3을 참조하면, 네트워크 설정부(160)는 메모리부(161)와 에이전트부(162) 및 환경 분석부(163)를 포함할 수 있다.

[0057] 메모리부(161)는 블록체인 네트워크(20)의 환경으로, 노드간 데이터 전송률(R)과 각 노드의 연산 자원(c), 합의 과정 기록(H) 및 악의적 노드 확률($\bar{p}$)을 포함하는 다수의 상태 정보(S^t = [R, c, H, $\bar{p}$]^t)를 저장할 수 있다.

[0058] 그리고 메모리부(161)는 다수의 상태 정보(S) 각각에 대응하여 에이전트부(162)에서 결정된 블록 사이즈(B), 블록 간격(T^I) 및 샤드 개수(K^*)를 포함하는 액션(A^t = [B, T^I, K^*]^t])을 함께 매칭시켜 저장할 수 있다.

[0059] 뿐만 아니라 메모리부(161)는 특정 에포크(t)에서의 상태 정보(S^t)와 이에 대응하여 결정되는 액션(A^t)에 의해 환경 분석부(163)에서 판별되는 다음 에포크(t+1)에서의 상태 정보(S^{t+1} = [R, c, H, $\bar{p}$]$^{t+1}$) 및 다음 상태 정보(S^{t+1})에 대응하는 보상(R^t)이 함께 저장될 수 있다.

[0060] 즉 메모리부(161)는 각 에포크 간격으로 블록체인 네트워크(20)의 상태 정보(S^t)와 이에 대응하는 액션(A^t) 및 액션(A^t)에 따른 다음 상태 정보(S^{t+1}) 및 보상(R^t)을 매칭하여 함께 저장할 수 있다. 여기서 메모리부(161)에 매칭되어 함께 저장되는 상태 정보(S^t)와 액션(A^t), 다음 상태 정보(S^{t+1}) 및 보상(R^t)은 전이 집합(Transition set)이라 한다.

[0061] 에이전트부(162)는 도 4에 도시된 바와 같이, 강화학습 방식으로 학습되는 인공 신경망으로 구현되어 메모리부(161)에서 인가되는 특정 에포크(t)에서의 상태 정보(S^t)에 대응하는 액션(A^t)을 결정한다. 에이전트부(162)는 상태 정보(S^t)에 포함된 노드간 데이터 전송률(R)과 각 노드의 연산 자원(c), 합의 과정 기록(H) 및 악의적 노드 확률($\bar{p}$)에 대해 학습된 패턴 추정 방식에 따른 최적의 블록 사이즈(B), 블록 간격(T^I) 및 샤드 개수(K^*)를 추정하여 출력한다.

[0062] 에이전트부(162)는 데이터 전송률(R)과 연산 자원(c), 합의 과정 기록(H) 및 악의적 노드 확률($\bar{p}$)을 기지정된 크기로 크기 변환 및 결합(concatenate)하여 입력 데이터로 인가받고, 입력 데이터에 대응하는 블록 사이즈(B), 블록 간격(T^I) 및 샤드 개수(K)를 포함하는 적어도 하나의 액션(A)을 추정하여 출력할 수 있다.

[0063] 그리고 에이전트부(162)는 추정된 적어도 하나의 액션(A) 중 하나의 액션을 액션(A^t)을 수학식 1에 따라 선택할 수 있다.

수학식 1

[0064] $$\max_{A} Q(S, A)$$

[0065] 여기서 Q는 에이전트부(162)가 수행하는 동작을 나타내는 액션 가치 함수(action-value function)로서, 상태 정보(S)에 응답하여 에이전트부(162)에서 결정될 수 있는 다수의 액션(A) 각각의 가치를 출력하는 함수이다.

[0066] 이때 에이전트부(162)는 학습에 의해 미리 지정된 가중치(ω)를 추가로 적용하여 현재 에포크(t)에서의 상태 정보(S^t)에 대응하는 액션(A^t)을 $\max_{A} Q(S^t, A^t; \omega)$로 선택할 수도 있다.

[0067] 환경 분석부(163)는 미리 학습된 인공 신경망으로 구현되어 현재 에포크(t)에서의 상태 정보(S^t)와 상태 정보

(S^t)에 따라 에이전트부(162)에서 결정된 액션(A^t)을 기반으로 다음 상태 정보(S^{t+1})와 다음 상태 정보(S^{t+1})에 대응하는 보상(R^t)을 추정한다.

[0068] 본 실시예의 네트워크 관리 장치는 블록체인 네트워크(20)의 처리 속도(transactions per second: 이하 TPS)를 최대로 하여 블록체인 네트워크(20)의 확장성을 향상시키는 것을 목적으로 하며, 블록체인 네트워크의 TPS(T)는 수학식 2에 따라 계산될 수 있다.

수학식 2

[0069] $$\mathcal{T}(B,T^I)=\frac{k\lfloor B/b\rfloor}{T^I}$$

[0070] 여기서 k는 샤드 개수를 나타내고, b는 평균 트랜잭션 크기를 나타내며, $\lfloor\ \rfloor$는 바닥 함수(floor funciton)를 나타낸다.

[0071] 즉 에이전트부(162)는 상태 정보(S^t)에 대응하여 결정 가능한 다수의 액션(A) 중 수학식 2에 따른 TPS가 최대가 되는 액션(A^t)을 결정하도록 학습된다.

[0072] 다만 에이전트부(162)가 단순히 TPS를 최대로 하는 경우, 트랜잭션이 블록체인 네트워크에 인가된 후 합의과정을 거쳐 비가역적인 상태가 될 때까지의 시간을 나타내는 레이턴시($T_{latency}$) 또는 보안성이 저하될 가능성이 있다.

[0073] 이에 환경 분석부(163)는 레이턴시($T_{latency}$)와 기지정된 두 가지 보안성 조건(S_1, S_2)을 유지하기 위해 요구되는 최대 보안 샤드 개수($\dot{K}$)의 2가지 제약 조건을 추가하여, 에이전트부(162)가 수학식 3과 같이 2가지 제약 조건을 만족하면서 액션(A^t)을 결정하도록 한다.

수학식 3

[0074] $$Objective:\ \max_{A} Q(S,A)$$
$$Constraint\ 1:\ T_{latency}=T^I+T_{con}^k\le uT^I$$
$$Constraint\ 2:\ \dot{K}<S_l, l=1,2$$

[0075] 여기서 T^k_{con} 는 k개의 샤드 블록을 갖는 샤드 블록체인 네트워크에서 소모되는 전체 합의 시간을 나타내고, u 는 연속된 블록 간격을 나타낸다. 그리고 2가지 보안성 조건(S_l, l = 1,2)은 샤드 블록체인 네트워크가 실용적 비잔틴 장애 허용(Practical Byzantine Fault Tolerance: 이하 PBFT) 알고리즘에 따라 합의를 수행하는 경우 보안성을 유지하기 위한 제약 조건을 나타낸다.

[0076] 도 5는 샤드 블록체인 네트워크의 합의 과정을 설명하기 위한 도면이다.

[0077] 상기한 바와 같이 레이턴시($T_{latency}$)는 트랜잭션이 블록체인 네트워크에 인가된 후 합의과정을 거쳐 비가역적인 상태가 될 때까지의 시간을 나타낸다. 블록체인 네트워크에 인가된 트랜잭션은 다수의 샤드 중 하나에 배치될 수 있다. 일 예로 트랜잭션은 샤드 분배 기법에 따라 송신자 주소의 마지막 비트에 따라 샤드에 배치될 수 있다. 그리고 도 5에 도시된 바와 같이 트랜잭션은 배치된 샤드 내에서 1차로 샤드내 합의(intra shard consensus)를 거친 후, 다수의 샤드들에 의한 최종 샤드 합의(final shard consensus) 과정을 통해 블록체인에 결합될 수 있다.

[0078] 트랜잭션의 레이턴시($T_{latency}$)는 수학식 3에 나타난 바와 같이, 블록 간격(T^{I})과 전체 합의 시간(T^{k}_{con})의 합으로 계산될 수 있다. 그리고 도 5를 참조하면, 전체 합의 시간(T^{k}_{con})은 샤드내 합의 시간(T^{k}_{intra})과 최종 샤드 합의 시간(T^{k}_{final})의 합으로 수학식 4에 따라 계산될 수 있다.

수학식 4

[0079] $$T^{k}_{con} = T^{k}_{intra} + T^{k}_{final}$$

[0080] 그리고 샤드내 합의 시간(T^{k}_{intra})과 최종 샤드 합의 시간(T^{k}_{final}) 각각에는 메시지 전파 시간과 메시지 검증 시간이 포함되어 수학식 5 및 6으로 계산될 수 있다.

수학식 5

[0081] $$T^{k}_{intra} = T^{k}_{in\_prop} + T^{k}_{in\_val}$$

수학식 6

[0082] $$T^{k}_{final} = T^{k}_{f\_prop} + T^{k}_{f\_val}$$

[0083] $T^{k}_{in\_prop}$ 와 $T^{k}_{in\_val}$ 는 각각 샤드내 합의 과정에서의 메시지 전파 시간과 검증 시간이고, $T^{k}_{f\_prop}$ 와 $T^{k}_{f\_val}$ 는 각각 최종 합의 과정에서의 메시지 전파 시간과 검증 시간이다.

[0084] 도 5를 참조하면, 샤드내 합의 시간(T^{k}_{intra})은 선 준비 단계(Pre-Prepare)와 준비 단계(Prepare) 및 승인 단계(Commit)로 구성된다.

[0085] 선 준비 단계에서 각 샤드의 우선 노드(Primary node, 또는 리더 노드라함)는 기지정된 배치 크기(Batch size)의 M개의 요청(request)을 인가받아 선 준비 메시지를 생성하고, 샤드 내 N_i-1 개의 복제 노드(Replica node)들로 각각 하나의 선 준비 메시지를 전파한다. 그리고 우선 노드는 N_i-1 개의 메시지 인증 코드(Message Authentication Code: 이하 MAC)를 생성하고, 각 복제 노드들은 블록을 검증하기 위해 MAC에 대한 연산을 수행한다.

[0086] 준비 단계에서 각 복제 노드들은 선 준비 메시지가 타당한지에 대한 검증 메시지를 다른 복제 노드들과 교환한다. 이때 각 복제 노드들은 N_i-1 개의 MAC를 생성하고, N_i-2 개의 MAC를 검증한다.

[0087] 승인 단계에서는 샤드내 모든 노드들이 검증을 위해 메시지를 교환한다. 특히 우선 노드는 각 메시지의 송수신에 대해 N_i-1 개의 메시지를 처리한다.

[0088] 승인 단계 이후, 우선 노드와 복네 노드들은 샤드내 합의 결과를 최종 합의를 위해 디렉토리 커미티(Directory Committee: 이하 DC)로 응신(reply)한다. 이때 우선 노드와 복제 노드들은 각 요청당 DC 의 수인 C 개의 MAC를 생성한다. 즉 우선노드는 전체 M개의 서명 확인과 M(1+C)+4(N_i-1)개의 MAC 연산을 수행하고 복제 노드는 M개의 서명 확인과 CM+4(N_i-1)개의 MAC 연산을 수행한다.

[0089] 따라서 i번째 샤드의 우선 노드의 전체 처리 시간은 $T^{i}_{in\_primary} = \frac{\mathcal{M}\theta + [\mathcal{M}(1+C)+4(N_i-1)]\alpha}{c_{i,p}}$ 이고, 복제 노드의

전체 처리 시간은 $T^{i}_{in\_replica} = \frac{\mathcal{M}\theta+[C\mathcal{M}+4(N_i-1)]\alpha}{c_{i,r}}$ 이다. 여기서 $c_{i,p}$ 와 $c_{i,r}$ 은 i번째 샤드의 우선 노드와 복제 노드의 연산 속도이다. 한편, 샤드 내 합의는 각 샤드에서 병렬로 처리되기 때문에, 지연 시간은 샤드 내 합의를 가장 늦게 처리한 샤드에 의해서 결정되고, 우선 노드와 복제 노드들의 검증 과정 또한 병렬로 처리된다. 따라서, 샤드 내 합의에서 각 요청 메시지에 대한 검증 시간($T^{k}_{in\_val}$)은 수학식 7로 계산될 수 있다.

수학식 7

[0090]
$$T^{k}_{in\_val} = \frac{1}{\mathcal{M}} \max_{i=1,\cdots,k}(T^{i}_{in\_replica}, T^{i}_{in\_primary})$$

[0091] 또한, 메시지 전파 시간은 합의 과정 동안에 목적 노드에게 메시지를 전달하는데 걸리는 시간이다. 이때 각 합의 단계에서 노드들이 무응답해서 합의 과정이 과도히 길어지는 것을 방지하기 위해서 제한 시간(ζ)이 설정될 수 있다. 제한 시간(ζ) 내에 응답을 하지 않는 복제 노드들은 해당 합의 단계에서 거절의 의견을 가진다고 여겨진다. 그러므로 샤드 내 각 합의 단계에서 전파 시간($T^{k}_{in\_prop}$)은 수학식 8로 계산될 수 있다.

수학식 8

[0092]
$$\begin{aligned} T^{k}_{in\_prop} &= \frac{1}{\mathcal{M}}(T^{k}_{in\_preprepare} + T^{k}_{in\_prepare} + T^{k}_{in\_commit}) \\ &= \frac{1}{\mathcal{M}} \max_{i=1,\cdots,k}(\min\left\{\max_{j\neq p}\frac{\mathcal{M}B}{R_{n_{i,p},n_{i,j}}}, \zeta\right\} \\ &\quad + \min\left\{\max_{j\neq l}\frac{\mathcal{M}B}{R_{n_{i,j},n_{i,l}}}, \zeta\right\} \\ &\quad + \min\left\{\max_{j\neq l}\frac{\mathcal{M}B}{R_{n_{i,j},n_{i,l}}}, \zeta\right\}) \end{aligned}$$

[0093] k 개의 샤드 각각의 샤드내 합의에서 승인된 블록들은 최종 합의를 위해 DC로 전파된다. DC는 각 샤드로부터 받은 kM개의 서명과 MAC를 검증을 시행한다. 이때 DC 노드들은 샤드내 합의와 마찬가지로 PBFT 합의를 다시 진행하고 합쳐진 블록을 모든 노드에게 전파한다. DC의 우선 노드와 복제 노드들의 검증 시간은 수학식 9와 같다.

수학식 9

[0094]
$$\begin{aligned} T^{k}_{f\_primary} &= \frac{k\mathcal{M}\theta + [k\mathcal{M} + 4(C-1) + (N-C)\mathcal{M}]\alpha}{c_{f,p}} \\ T^{k}_{f\_replica} &= \frac{k\mathcal{M}\theta + [4(C-1) + (N-C)\mathcal{M}]\alpha}{c_{f,r}} \end{aligned}$$

[0095] 여기서 $c_{f,p}$ 와 $c_{f,r}$ 은 DC의 우선 노드와 복제 노드의 연산 속도이다.

[0096] 따라서 최종 합의에서 각 요청에 대한 검증 시간($T^{k}_{f\_val}$)은 수학식 10으로 계산된다.

수학식 10

[0097]
$$T^{k}_{f\_val} = \frac{1}{\mathcal{M}} \max(T^{k}_{f\_primary}, T^{k}_{f\_replica})$$

[0098] 그리고 DC에서의 메시지 전파 시간은 샤드 내 합의에서의 전파 시간($T^{k}_{f\_prop}$)과 동일한 방식으로 수학식 11과 같이 계산될 수 있다.

수학식 11

[0099]
$$
\begin{aligned}
T_{f\_prop^k} = \frac{1}{\mathcal{M}}(&T^k_{f\_request} + T^k_{f\_preprepare} + T^k_{f\_prepare} \\
&+ T^k_{f\_commit} + T^k_{reply}) \\
= \frac{1}{\mathcal{M}}(&\min\left\{\max_{i=1,\cdots,k;j=1,\cdots,N_i;l=1,\cdots,C} \frac{\mathcal{M}B}{R_{n_{i,j},n_{f,l}}}, \zeta\right\} + \\
&\min\left\{\max_{l\neq p} \frac{\mathcal{M}B}{R_{n_{f,p},n_{f,l}}}, \zeta\right\} + \\
&\min\left\{\max_{u\neq p;u,l=1,\cdots,C} \frac{\mathcal{M}B}{R_{n_{f,u},n_{f,l}}}, \zeta\right\} + \\
&\min\left\{\max_{u\neq l} \frac{\mathcal{M}B}{R_{n_{f,u},n_{f,l}}}, \zeta\right\} + \\
&\min\left\{\max_{i=1,\cdots,k} \frac{k\mathcal{M}B}{R_{n_{f,u},n_{i,j}}}, \zeta\right\})
\end{aligned}
$$

[0100] 여기서 $n_{f,p}$ 와 $n_{f,r}$ 는 DC에서의 우선 노드와 복제 노드 번호를 나타내고, $R_{n_{i,j},n_{f,l}}$ $R_{n_{f,p},n_{f,l}}$ $R_{n_{f,u},n_{f,l}}$, $R_{n_{f,u},n_{f,l}}$, $R_{n_{f,u},n_{i,j}}$ 는 첨자로 지정되는 노드들 사이의 전송률을 나타낸다.

[0101] $T^{k}_{f_request}$는 DC가 샤드 내 합의 과정에서 만든 블록들을 수신하는데 소모되는 전파 시간이며, $T^{k}_{f\_reply}$ 는 최종적으로 합쳐진 블록을 전체 블록체인 네트워크로 브로드캐스팅 하는데 소모되는 시간이다.

[0102] 최종적으로, 샤드 블록체인 네트워크에서 소모되는 전체 합의 시간(T^{k}_{con})은 수학식 12로 계산될 수 있다.

수학식 12

$$
\begin{aligned}
T_{con}^{k} = T_{intra}^{k} + T_{final}^{k} &= (T_{in\_prop}^{k} + T_{in\_val}^{k}) \\
&\quad + (T_{f\_prop}^{k} + T_{f\_val}^{k}) \\
&= \frac{1}{\mathcal{M}}\Big(\max_{i=1,\cdots,k}(T_{in\_replica}^{i}, T_{in\_primary}^{i}) \\
&\quad + \max(T_{f\_primary}^{k}, T_{f\_replica}^{k})\Big) \\
&\quad + \frac{1}{\mathcal{M}}\max_{i=1,\cdots,k}\Big(\min\left\{\max_{j\neq p}\frac{\mathcal{M}B}{R_{n_{i,p},n_{i,j}}}, \zeta\right\} \\
&\quad + \min\left\{\max_{j\neq l}\frac{\mathcal{M}B}{R_{n_{i,j},n_{i,l}}}, \zeta\right\} \\
&\quad + \min\left\{\max_{j\neq l}\frac{\mathcal{M}B}{R_{n_{i,j},n_{i,l}}}, \zeta\right\}\Big) \\
&\quad + \frac{1}{\mathcal{M}}\Big(\min\left\{\max_{i=1,\cdots,k;j=1,\cdots,N_i;l=1,\cdots,C}\frac{\mathcal{M}B}{R_{n_{i,j},n_{f,l}}}, \zeta\right\} \\
&\quad + \min\left\{\max_{l\neq p}\frac{\mathcal{M}B}{R_{n_{f,p},n_{f,l}}}, \zeta\right\} \\
&\quad + \min\left\{\max_{u\neq p;u,l=1,\cdots,C}\frac{\mathcal{M}B}{R_{n_{f,u},n_{f,l}}}, \zeta\right\} \\
&\quad + \min\left\{\max_{u\neq l}\frac{\mathcal{M}B}{R_{n_{f,u},n_{f,l}}}, \zeta\right\} \\
&\quad + \min\left\{\max_{i=1,\cdots,k}\frac{k\mathcal{M}B}{R_{n_{f,u},n_{i,j}}}, \zeta\right\}\Big)
\end{aligned}
$$

[0103]

[0104] 그리고 트랙잭션의 합의 지연 시간은 블록체인의 완결성(finality) 특징을 만족하기 위해서 연속된 블록 간격(u) 내에 완료되어야 하므로, 상기한 수학식 3의 첫번째 제약 사항(Constraint1)을 만족해야한다.

[0105] 한편, PBFT 를 기반으로 하는 합의 알고리즘에서는 전체 N개의 블록체인 노드가 있을 때, (3f+1) ≤ N 의 조건을 만족하는 f개의 악의적 노드가 있더라도 정상적으로 합의과정이 작동될 수 있다. 그리고 샤딩이 적용된 샤드 블록체인 네트워크에서는, 전체 노드들이 k개의 샤드로 분배되고, 최종 합의를 담당하는 DC는 C(C = |N/(k+1)|) 개의 노드로 구성된다. 즉, N명의 검증자들이 전체 k+1개로 균등하게 분배되어 PBFT 알고리즘을 따른다.

[0106] PBFT 알고리즘에서 2가지 보안성 조건(S_l, l = 1,2) 중 제1 보안성 조건(S_1)은 모든 샤드 내에서 악의적 노드가 각 샤드에서 1/3이상의 비율을 형성하는 것을 막아 정상적인 블록들이 모두 생성되도록 하는 조건으로 수학식 13으로 정의될 수 있다.

수학식 13

[0107]
$$S_1 = \frac{N(1-3p)-1}{3Np+1}$$

[0108] 여기서 p는 악의적 노드 비율이다.

[0109] PBFT 알고리즘에서 샤드 내의 전체 노드 수(N_i)와 악의적 노드 수(f_i) 및 DC 의 악의적 노드 수(f_{DC})에 대해 ($3f_i + 1$) ≤ N_i 의 조건과 ($3f_{iC} + 1$) ≤ C 의 조건을 만족해야 한다.

[0110] 전체 네트워크에 Np개의 악의적 노드가 있을 때, 가장 심각한 경우는 모든 악의적 노드가 DC에 집중되었을 때이다. 이 경우 각 샤드와 DC는 3Np+1 ≤ N_i와 3Np+1 ≤ N_i의 조건을 만족해야 한다. 그리고 C = |N/(k+1)|, N_i ≥ |(N-C)/k| 로서, N_i가 C보다 크므로, 3Np+1 ≤ |N/(k+1)| < N/(k+1)가 보안성 조건이 된다. 그리고 이를 k

에 대해서 정리하면 k < (N(1-3p)-1)/(3Np+1)이 되고, 따라서 제1 보안성 조건(S_1)은 수학식 13과 같이 유도될 수 있다.

[0111] 그리고 제2 보안성 조건(S_2)은 모든 샤드내에서 악의적 노드가 2/3이상의 비율을 형성하는 것을 막아 변조된 블록 형성이 이루어지지 않도록 하는 조건으로 수학식 14로 정의될 수 있다.

수학식 14

[0112] $$S_2 = \frac{2N}{3(Np+1)} - 1$$

[0113] 상기한 바와 같이, PBFT 알고리즘에서는 악의적 노드가 각 샤드와 DC에서 2/3 이상의 비율을 점유해서는 안된다. 따라서 Np ≤ (2/3)N_i-1 와 Np ≤ (2/3)C-1를 만족해야 하고, 최종적으로 Np ≤ (2/3)C-1 = (2/3)|N/(k+1)|-1 < 2N/3(k+1) -1 조건에 의해서 k < 2N/(3(Np+1))-1의 식이 유도된다. 따라서 제2 보안성 조건(S_2)은 수학식 14와 같이 유도될 수 있다.

[0114] 한편, 각 노드가 악의적으로 행동할 확률(p)에 따라 평균 Np 개의 악의적 노드가 블록체인 네트워크(20)에 존재한다고 가정할 수 있다. 그러나 본 실시예에 따른 네트워크 관리 장치에서 네트워크 설정부(160)는 어떠한 노드가 악의적 노드인지 판별할 수 없다. 따라서 네트워크 설정부(160)의 에이전트부(162)는 이전 획득된 합의 과정 기록(H)에 기초하여 악의적 노드 비율을 추정하고, 보안성 조건(S_1, S_2)에 따라 샤드 개수를 조정할 필요가 있다.

[0115] 악의적 노드 확률(p)을 추정하기 위해서 먼저, 합의 과정 기록(H)을 기반으로 정규화된 엔트로피 값을 이용해 샤드의 합의 불일치도를 계산한다. 만약, 블록이 정상인지 비정상인지 검증하는 과정에서 검증자들이 정확히 반반의 의견을 제시했다면 불일치도는 1이 된다. 만약 합의 결과가 만장일치로 이루어진다면 불일치도는 0이 된다. p^i_m와 p^i_M를 각각 소수의 합의 의견의 비율과 다수의 합의 의견의 비율이라고 하면, 다수 합의 의견 비율(p^i_M)은 1-p^i_m 로 계산된다. 따라서, i번째 샤드의 합의 과정에서 엔트로피 값은 수학식 15로 계산될 수 있다.

수학식 15

[0116] $$I_i = -p_m^i log_2(p_m^i) - (1-p_m^i) log_2(1-p_m^i)$$
$$I_{DC} = -p_m^{DC} log_2(p_m^{DC}) - (1-p_m^{DC}) log_2(1-p_m^{DC})$$

[0117] 여기서 I_i와 I_{DC}는 각각 i번째 샤드와 DC에서 합의의 불일치도를 나타낸다.

[0118] 그리고 각 샤드들의 정규화된 엔트로피 값을 평균한 값인 전체 합의 신뢰도 U는 수학식 16과 같이 계산된다.

수학식 16

[0119] $$U = \frac{1}{k+1}((\sum_{i=1}^{k} I_i) + I_{DC})$$

[0120] 다만 전체 블록체인 네트워크에서 악의적 노드 비율은 어떠한 노드가 정직한지 악의적인지에 대한 정확한 정보가 없기 때문에, 각 샤드 별로 소수와 다수의 의견의 비율만을 알 수 있다. 그러므로, 각 샤드의 불일치도의 평균값은 전체 네트워크의 불일치도와 거의 비슷하다고 가정하여 전체 악의적 노드 비율($\bar{p}$)을 수학식 17과 같

이 추정할 수 있다.

수학식 17

[0121] $$U \approx -\dot{p}log_2\dot{p} - (1-\dot{p})log_2(1-\dot{p})$$
$$\bar{p} = \min\{\dot{p}, (1-\dot{p})\}$$

[0122] 추정 값은 악의적이지 않은 정상적인 노드들이 전체 네트워크에서 과반수 이상을 차지한다고 가정하여, $\dot{p}$와 (1-$\dot{p}$) 중 작은 값이 악의적 노드 비율($\bar{p}$)로 추정될 수 있다.

[0123] 상기한 수학식 3의 2가지 제약 조건은 TPS를 최대로 함에 따라 발생할 수 있는 레이턴시($T_{latency}$) 또는 보안성이 저하를 방지하기 위해 이용되기도 하지만, 에이전트부(162)가 무의미한 액션(A)을 선택하지 않도록 하여, 인공신경망으로 구현되는 에이전트부(162)가 강화 학습 시에 더욱 빨리 수렴할 수 있도록 하는 장점이 있다. 즉 에이전트부(162)의 학습 속도를 향상시킬 수 있다.

[0124] 환경 분석부(163)는 에이전트부(162)에서 결정된 액션(A^t)이 2가지 제약 조건을 만족하는 경우, 에포크(t)에서의 보상(R^t)을 수학식 2의 TPS에 기반하여 수학식 18과 같이 계산하는 반면, 결정된 액션(A^t)이 2가지 제약 조건을 만족하지 못하는 경우 보상(R^t)을 0으로 계산한다.

수학식 18

[0125] $$\mathfrak{R}^t = \mathfrak{R}(S^t, A^t) = \frac{k\lfloor (B-B_H)/b \rfloor}{T^I}$$

[0126] 여기서 B_H는 블록 헤더 크기이다.

[0127] 에이전트부(162)는 수학식 18에 따른 보상(R^t)이 최대가 되도록 강화 학습이 수행될 수도 있다. 여기서 보상(R^t)은 수학식 3의 액션 가치 함수(Q)일 수 있다.

[0128] 그러나 이 경우, 에이전트부(162)의 업데이트가 매우 빈번하게 발생될 뿐만 아니라, 학습 시에 결과가 진동하거나 발산되어 수렴되지 않는 경우도 발생할 수 있다.

[0129] 이에 심층 Q 네트워크의 구조를 에이전트부(162)에 적용하여 에이전트부(162)가 매 에포크마다 업데이트되는 메인 Q 네트워크와 기지정된 주기로 업데이트되는 타겟 Q 네트워크를 포함하도록 구성할 수 있다.

[0130] 이와 같이, 에이전트부(162)가 메인 Q 네트워크와 타겟 Q 네트워크를 포함하는 경우, 메인 Q 네트워크는 현재 에포크(t)에서 설정된 샤드 개수(K^*)와 상태 정보(S^t)에서의 액션(A^t)을 수학식 3을 수정한 수학식 19에 따라 선택한다.

수학식 19

[0131] $$A^t = \arg\max_A Q(S^t, A^t; \omega)$$

[0132] 여기서 ω는 메인 Q 네트워크의 가중치이다.

[0133] 이때 메인 Q 네트워크는 수학식 3의 2가지 제약 조건을 만족하도록 액션(A^t)을 선택해야한다. 또한 메인 Q 네트워크는 강화 학습이 완전하게 수행되지 않은 상태로 임의의 액션을 선택할 랜덤 액션 확률(p_ε)이 미리 지정된 랜덤 선택 확률(ε) 이상이면, 액션(A = [B, T^I, K^*])에 포함되는 블록 사이즈(B), 블록 간격(T^I) 및 샤드 개수

(K^*)를 임의로 선택할 수 있다. 즉 랜덤 액션을 선택할 수도 있다. 다만 샤드 개수(K^*)는 수학식 3의 2가지 제약 조건을 만족하도록 선택되어야 한다.

[0134] 이에 환경 분석부(163)는 메인 Q 네트워크에서 선택된 액션(A^t)을 실행한 보상(R^t)과 다음 에포크(t+1)에서의 상태 정보(S^{t+1})를 관측한다. 그리고 관측된 상태 정보(S^{t+1})로부터 악의적 노드 비율($\bar{p}$)을 추정하고, 샤드 개수(K^*)를 업데이트하여 다시 메인 Q 네트워크로 전달할 수 있다.

[0135] 여기서는 에이전트부(162)가 추정된 다수의 액션(A) 중 2가지 제약 조건을 만족하면서 TPS를 최대로 하는 액션(A^t)을 선택하는 것으로 설명하였으나, 경우에 따라서는 환경 분석부(163)가 하나의 액션(A^t)을 선택할 수도 있다.

[0136] 상태 정보(S^t)와 메인 Q 네트워크에서 선택된 액션(A^t)과 환경 분석부(163)에서 획득된 보상(R^t) 및 다음 에포크(t+1)에서의 상태 정보(S^{t+1})는 전이 집합([S^t, A^t, R^t, S^{t+1}])으로서 메모리부(161)에 저장된다.

[0137] 그리고 메모리부(161)에 이전 저장된 다수의 전이 집합([S^x, A^x, R^x, S^{x+1}])의 미니배치(minibatch)를 기지정된 방식(예를 들면 랜덤하게)으로 샘플링하고, 타겟 Q 네트워크를 최적화하기 위한 함수(y^x)를 수학식 20으로 설정한다.

수학식 20

[0138]
$$y^x = \begin{cases} \mathcal{R}^x & if\ episode\ terminates\ at\ step\ x+1 \\ \mathcal{R}^x + \gamma \max_{A'} Q^*(S^{x+1}, A'; \omega^*) & otherwise \end{cases}$$

[0139] 여기서 ω^*은 타겟 Q 네트워크의 가중치이고, A'은 타겟 Q 네트워크에서 선택된 액션을 나타내며, Q^* 는 타겟 Q 네트워크의 액션 가치 함수로서, $Q^*(S,A) = \max_\pi \mathbb{E}[\sum_{t=0}^{\infty} \gamma^t \mathfrak{R}(S^t, A^t) \mid S^{(0)} = S, A^{(0)} = A, \pi]$ 로 계산될 수 있다.

[0140] 여기서 γ($\gamma \in (0,1)$)는 디스카운트 팩터(discount factor)이고, π는 행동 정책(behavior policy)을 나타낸다.

[0141] 타겟 Q 네트워크는 기지정된 주기로 메인 Q 네트워크는 수학식 21로 계산되는 손실($L(\omega)$)이 최소화되도록 역전파되어 업데이트될 수 있다.

수학식 21

[0142]
$$L(w) = E[(\mathfrak{R}^x + \gamma \max_{A'} Q^*(S^{x+1}, A'; \omega^*) - Q(S^x, A^x; \omega))^2]$$

[0143] 수학식 21에 따르면, 손실($L(\omega)$)은 상기 메모리부에 저장된 다수의 전이 집합([S^x, A^x, R^x, S^{x+1}])의 미니배치(minibatch)를 기지정된 방식으로 샘플링하고, 샘플링된 전이 집합의 보상(R^x)과 각 상태 정보(S^x, S^{x+1})에 따라 선택되는 액션(A^x, A')에 의한 TPS 차를 기반으로 에너지 함수의 형태로 획득될 수 있다.

[0144] 그리고 손실이 역전파되어 학습된 타겟 Q 네트워크는 메인 Q 네트워크로 복제됨으로써 메인 Q 네트워크 또한 업데이트 될 수 있다.

[0145] 도 6은 본 발명의 일 실시예에 따른 블록체인 네트워크 관리 방법을 나타낸다.

[0146] 도 2 내지 도 5를 참조하여 도 6의 블록체인 네트워크 관리 방법을 설명하면, 우선 현재 에포크(t)에서의 상태 정보(S^t)를 획득한다(S11). 여기서 상태 정보(S^t)는 블록체인 네트워크(20)의 환경으로, 노드간 데이터 전송률

(R)과 각 노드의 연산 자원(c), 합의 과정 기록(H) 및 악의적 노드 비율($\bar{p}$)을 포함한다. 여기서 악의적 노드 비율($\bar{p}$)은 합의 과정 기록(H)을 기반으로 정규화된 엔트로피 값을 이용해 샤드의 합의 불일치도를 계산하여 추정될 수 있다.

[0147] 그리고 현재 블록체인 네트워크(20)에 설정된 샤드 개수(K^*)를 확인한다(S12).

[0148] 패턴 추정 방식이 학습되는 인공 신경망에 상태 정보(S^t)를 입력 데이터로 입력하여, 상태 정보(S^t)에 대응하는 적어도 하나의 액션(A)을 추정하여 획득한다(S13). 이때, 상태 정보(S^t)에 포함된 각 요소는 인공 신경망의 입력 데이터로 이용될 수 있도록 크기 변환 및 결합될 수 있다. 그리고 인공 신경망은 심층 강화 학습 방식에 따라 학습될 수 있으며 일 예로 심층 Q 네트워크로 구성될 수 있다.

[0149] 여기서 적어도 하나의 액션(A) 각각에는 블록 사이즈(B), 블록 간격(T^I) 및 샤드 개수(K)가 포함된다.

[0150] 적어도 하나의 액션(A)이 획득되면, 획득된 적어도 하나의 액션(A) 중 하나의 액션(A^t)을 수학식 3에 따라 선택한다(S14). 수학식 3에 따르면, 레이턴시($T_{latency}$)와 기지정된 두 가지 보안성 조건(S_1, S_2)을 유지하기 위해 요구되는 최대 보안 샤드 개수($\dot{K}$)의 2가지 제약 조건을 만족시키면서 TPS 를 최대로 할 수 있는 액션(A^t)을 선택한다.

[0151] 액션(A^t)이 선택되면, 인공 신경망이 학습되어야 하는 학습 과정인지 판별한다(S15). 만일 학습 과정이 아닌 것으로 판별되면, 선택된 액션(A^t)에 포함된 블록 사이즈(B), 블록 간격(T^I) 및 샤드 개수(K^*)를 블록 체인 네트워크(20)에 적용한다(S16).

[0152] 그러나 만일 현재 블록체인 네트워크 관리 방법이 학습되는 학습 과정인 경우, 선택된 액션(A^t)이 적용됨에 따라 변화하는 블록체인 네트워크(20)의 다음 에포크(t+1)에서의 상태 정보(S^{t+1})를 획득한다(S21). 그리고 보상(R^t)을 계산한다(S22).

[0153] 이에 각 에포크 간격으로 획득되는 블록 체인 네트워크(20)의 상태 정보(S^t)와 이에 대응하는 액션(A^t) 및 액션(A^t)에 따른 다음 상태 정보(S^{t+1}) 및 보상(R^t)을 매칭하여 전이 집합($[S^t, A^t, R^t, S^{t+1}]$)으로써 함께 저장한다(S23).

[0154] 그리고 저장된 다수의 전이 집합($[S^x, A^x, R^x, S^{x+1}]$)에서 기지정된 방식으로 미니배치(minibatch)를 샘플링한다(S24). 미니배치로 샘플링된 전이 집합($[S^x, A^x, R^x, S^{x+1}]$)가 획득되면, 미니배치로 샘플링된 전이 집합($[S^x, A^x, R^x, S^{x+1}]$)의 상태 정보(S^x)에 대응하는 액션(A')을 추정하여 보상과 손실을 수학식 20 및 수학식 21에 따라 계산하고, 계산된 손실을 역전파하여 액션을 추정하는 인공 신경망을 학습시킨다(S25).

[0155] 이때, 인공 신경망이 심층 Q 네트워크로 구현되는 경우, 현재 에포크(t)에서의 상태 정보(S^t)로부터 액션(A^t)을 선택하는 신경망과 미니배치로 샘플링된 전이 집합($[S^x, A^x, R^x, S^{x+1}]$)으로부터 기지정된 방식으로 손실을 추정하여 학습되는 신경망을 각각 메인 Q 네트워크와 타겟 Q 네트워크로 구분할 수 있다. 여기서 손실이 역전파되어 학습된 타겟 Q 네트워크는 메인 Q 네트워크로 복제됨으로써 메인 Q 네트워크 또한 업데이트 될 수 있다.

[0156] 본 발명에 따른 방법은 컴퓨터에서 실행시키기 위한 매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다. 여기서 컴퓨터 판독가능 매체는 컴퓨터에 의해 액세스 될 수 있는 임의의 가용 매체일 수 있고, 또한 컴퓨터 저장 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함하며, ROM(판독 전용 메모리), RAM(랜덤 액세스 메모리), CD(컴팩트 디스크)-ROM, DVD(디지털 비디오 디스크)-ROM, 자기 테이프, 플로피 디스크, 광데이터 저장장치 등을 포함할 수 있다.

[0157] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다.

[0158] 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0159] 10: IoT 네트워크 20: 블록체인 네트워크

110: 통신부 120: 제어부

130: 블록 생성부 140: 신뢰도 계산부

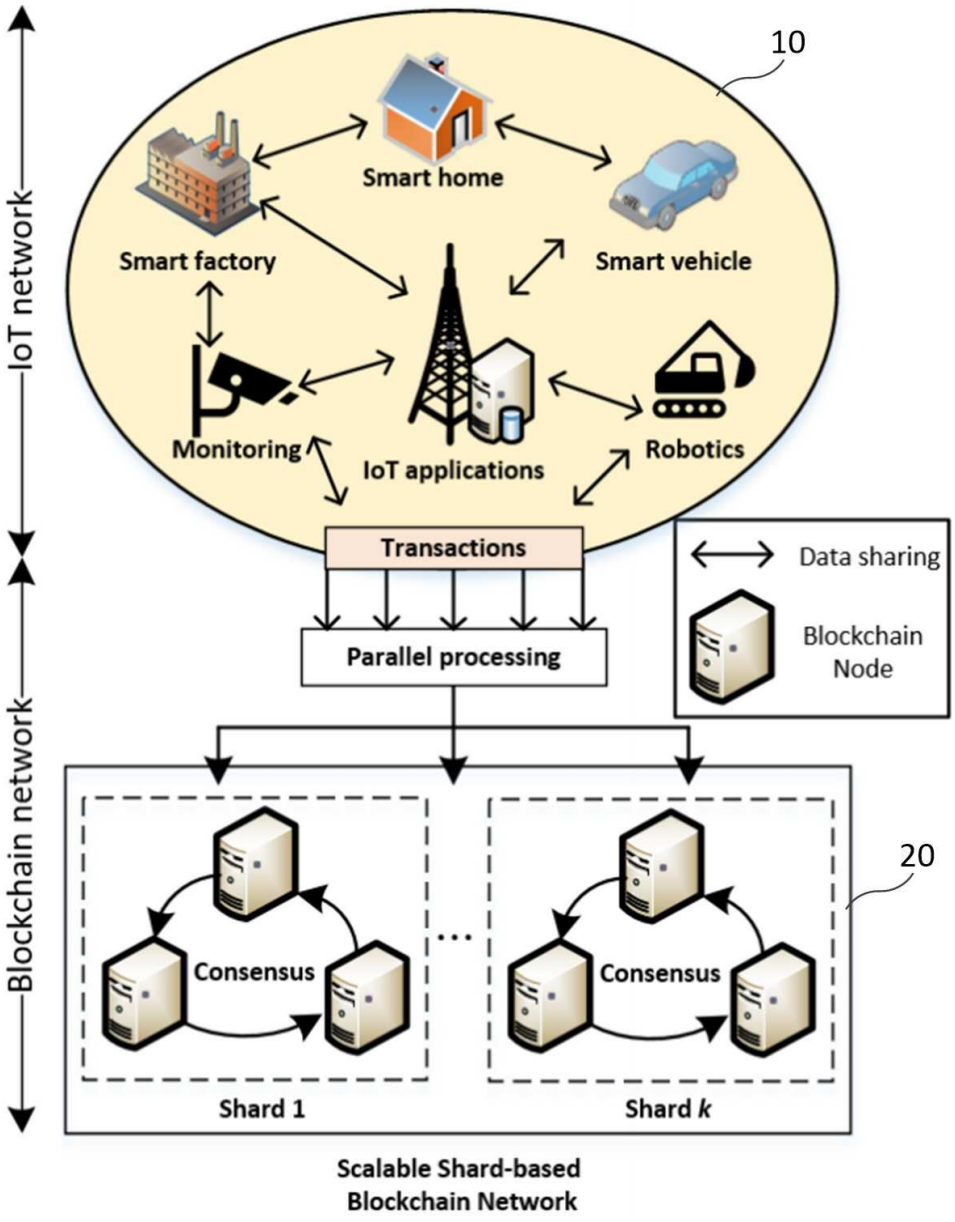
150: 블록 저장부 160: 네트워크 설정부

161: 메모리부 162: 에이전트부

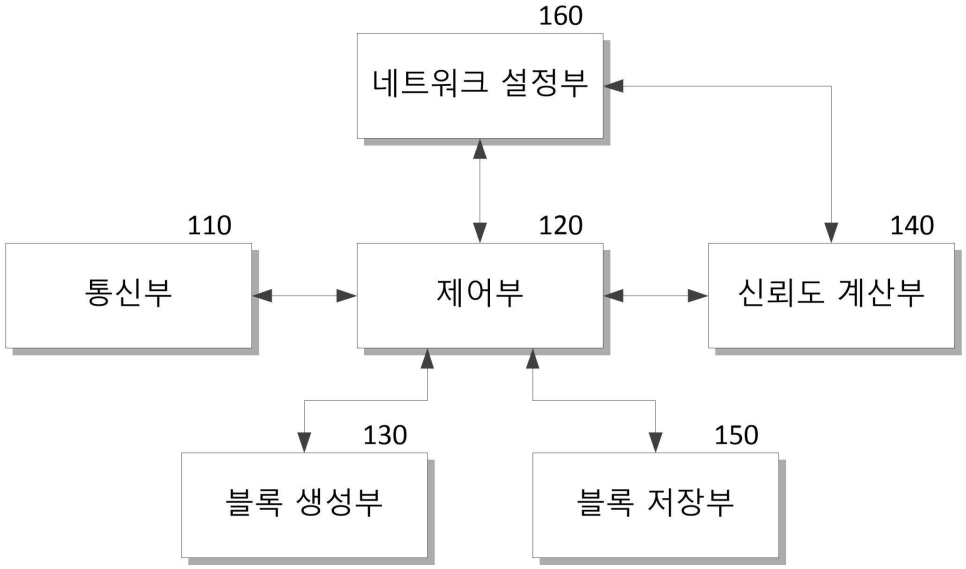
163: 환경 분석부

도면

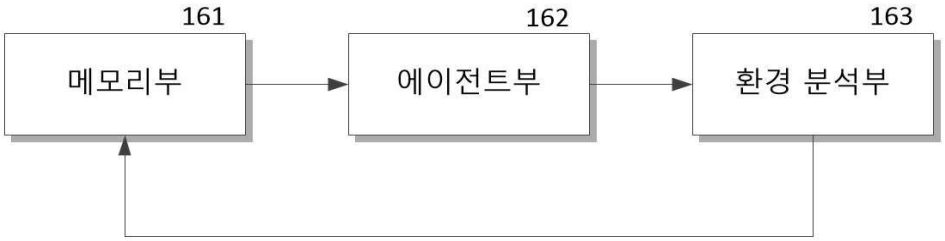
도면1



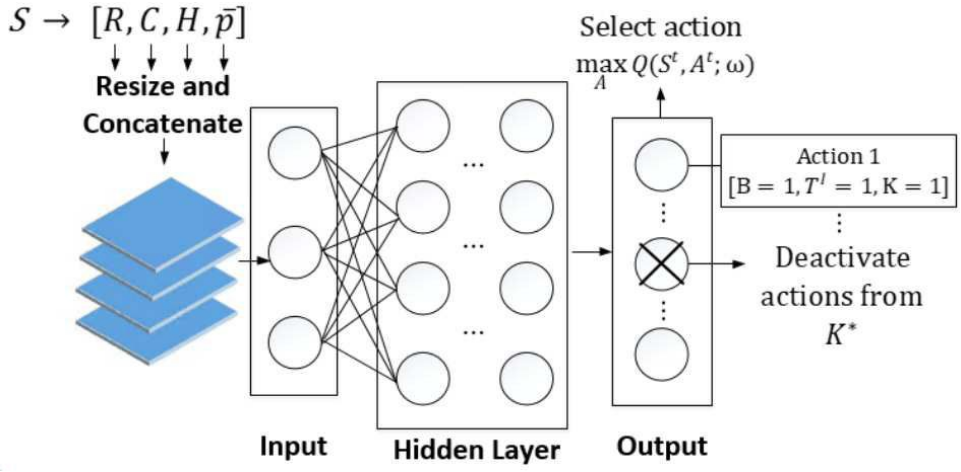
도면2


160
네트워크 설정부
110
통신부
120
제어부
140
신뢰도 계산부
130
블록 생성부
150
블록 저장부

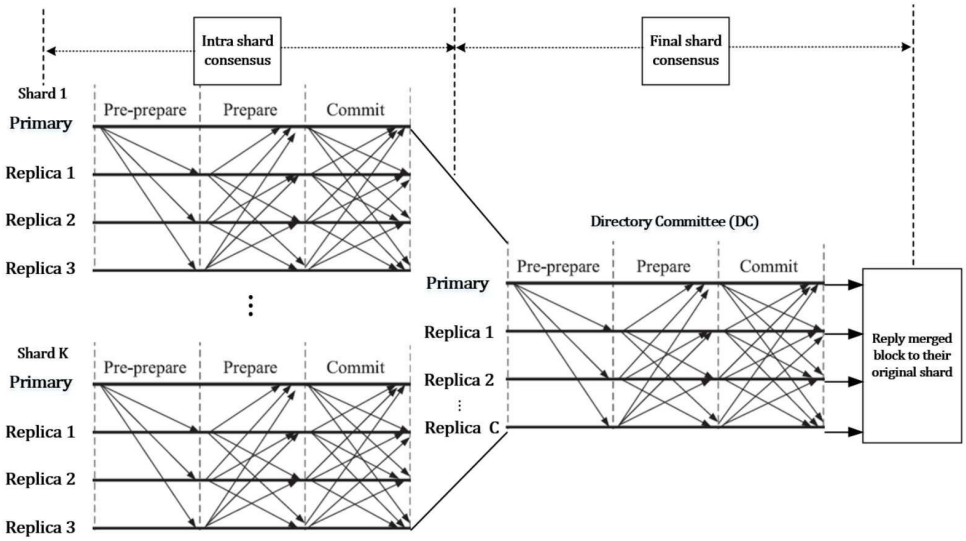
도면3


161
메모리부
162
에이전트부
163
환경 분석부

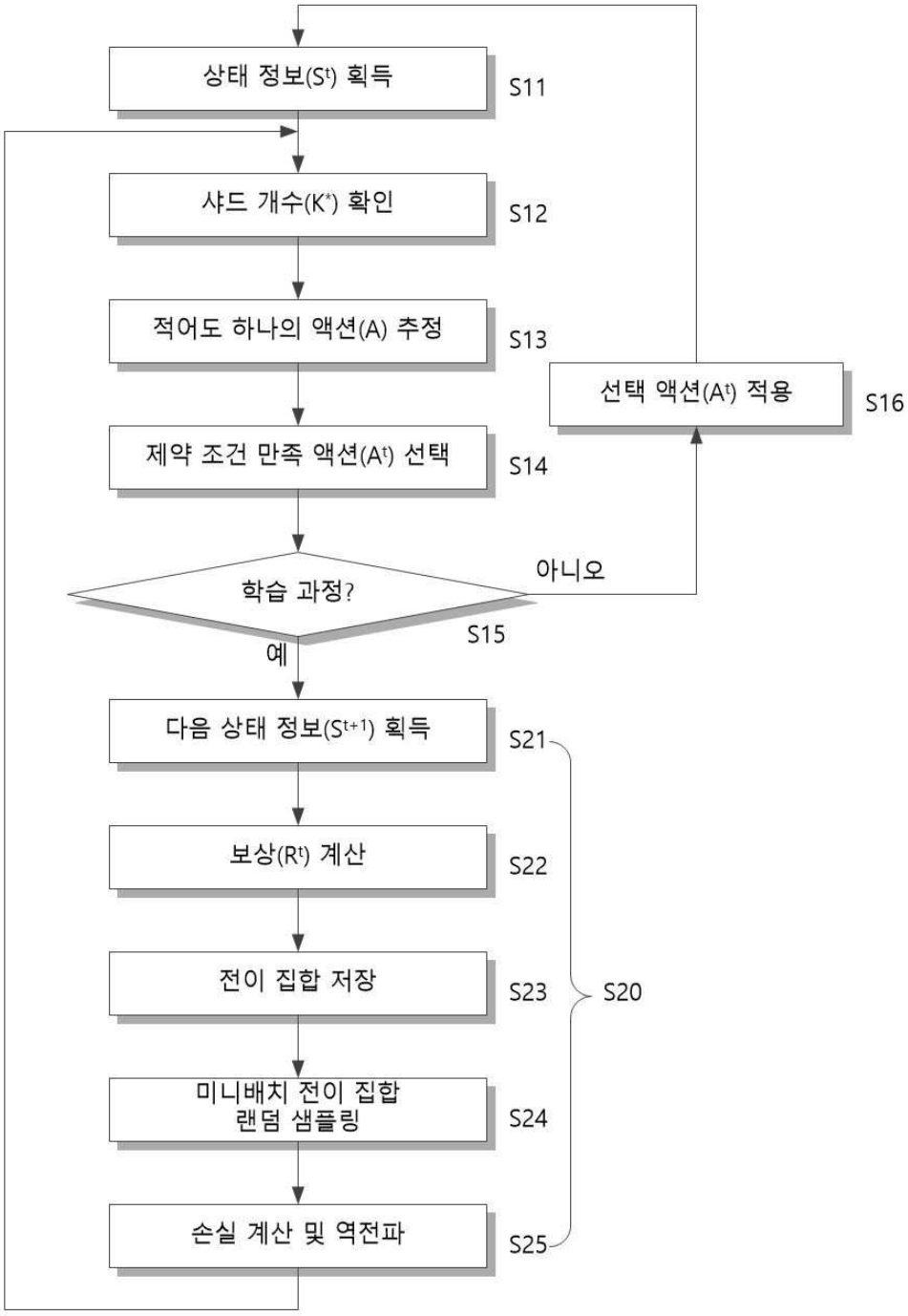
도면4


$S \rightarrow [R, C, H, \bar{p}]$
Resize and
Concatenate
Select action
$\max_A Q(S^t, A^t; \omega)$
Action 1
$[B = 1, T^l = 1, K = 1]$
Deactivate
actions from
K^*
Input
Hidden Layer
Output

도면5


Intra shard consensus
Final shard consensus
Shard 1
Primary
Replica 1
Replica 2
Replica 3
Pre-prepare
Prepare
Commit
Shard K
Primary
Replica 1
Replica 2
Replica 3
Pre-prepare
Prepare
Commit
Directory Committee (DC)
Primary
Replica 1
Replica 2
Replica C
Pre-prepare
Prepare
Commit
Reply merged block to their original shard

도면6


상태 정보(S^t) 획득
S11
샤드 개수(K*) 확인
S12
적어도 하나의 액션(A) 추정
S13
제약 조건 만족 액션(A^t) 선택
S14
학습 과정?
아니오
S15
예
선택 액션(A^t) 적용
S16
다음 상태 정보(S^t+1) 획득
S21
보상(R^t) 계산
S22
전이 집합 저장
S23
미니배치 전이 집합
랜덤 샘플링
S24
손실 계산 및 역전파
S25
S20