

플록(FLock.io)

해당 번역본은 이용자가 디지털자산 관련 정보를 편리하게 확인할 수 있도록 단순 참고용으로 번역된 것이며, 투자 권유를 목적으로 하지 않습니다.

그 내용이 정확하지 않을 수 있으므로 정확한 정보 습득을 위해서는 원문을 참고하시거나 원문 작성 주체 측에 문의하시기 바랍니다.

두나무는 해당 번역본 내용의 진실성 및 정확성을 보장하지 않고, 제공된 정보에 의한 투자 결과에 대하여 어떠한 책임도 지지 않으며, 투자 손실은 투자자에게 귀속됩니다.

FLock: 블록체인 기반 연합 머신러닝

데이터, 연산, 모델의 분산화를 통한 AI 민주화

FLock 팀

초록

AI 개발의 급속한 진전은, 그 생성과 배포 과정에서 중요한 문제들을 부각시켰습니다. 이는 주로 소수의 대기업이 유지하고 있는 중앙집중적 통제에서 기인합니다. 이러한 접근 방식은 효과적인 거버넌스와 감독의 부재로 인해 AI 모델 내 편향성을 심화시키며, 공공의 참여를 저해하고 심각한 데이터 보호 문제를 야기합니다. 또한 데이터와 모델 결과물에 대한 독점적 통제는 사용자들이 자신도 모르는 사이에 대기업의 이익을 위한 데이터셋에 기여하게 만들며, 혁신과 공정한 데이터 활용에 대한 위협이 됩니다.

FLock은 온체인 인센티브 메커니즘을 통해 AI 개발과 정렬(alignment)의 민주화를 실현합니다. 오픈 소스 개발과 데이터 소유권을 촉진함으로써, FLock은 참가자들이 모델, 데이터, 컴퓨팅 자원을 기여하고 온체인 합의에 따라 보상을 받는 개방적이고 협력적인 환경을 조성합니다. 이러한 접근은 중앙집중 기관에서 발생하는 편향 없이 투명성과 대규모 협업을 증진시킵니다. 궁극적으로, FLock은 다양한 커뮤니티가 그들의 특정한 요구에 맞춘 목적지향적 AI 모델을 개발할 수 있도록 하며, AI 개발과 배포의 패러다임을 혁신합니다.

I. 서론

모든 분야를 아우르며, 협업은 역사적으로 혁신의 촉매 역할을 해왔습니다. 이는 과학과 디지털 영역에서 특히 명확하게 드러납니다. 집단의 전문성을 모음으로써, 우리는 빠르게 파괴적인 혁신을 이루어냈습니다. 그러나 이러한 이상은 현재 AI 개발 및 배포에 적용될 때 여러 장애물에 직면하고 있습니다. 특히 공공의 참여 저하, 통제 집중에 대한 만연한 우려, 그리고 소수 대기업에 의한 데이터 보호 통제가 대표적입니다. 한편, 블록체인 기술^{1 2}은 탈중앙화된 금융³, 투표 및 거버넌스 등 분산된 조직이 필요한 여러 영역에서 그 효용성을 입증해왔습니다. 이제 블록체인을 활용한 AI 개발의 혁신에 대한 연구와 배치가 진행 중입니다.

Flock은 커뮤니티의 참여와 데이터 보호에 대한 확고한 헌신을 바탕으로, 블록체인을 활용하여 AI 생태계의 민주화를 선도할 준비가 되어 있습니다.

A. AI 개발에 대한 중앙집중적 통제의 문제점

오늘날 AI 분야 혁신의 주요 장애물은 중앙집중적 통제입니다. 이 중앙화 구조는 모든 AI 훈련, 의사결정 과정, 데이터 저장에 하나의 기관 또는 위치에 의해 통제됨을 의미합니다⁴. 이로 인해 다음과 같은 문제점들이 발생합니다:

- **단일 실패 지점(Single Point of Failure):** 기술적 문제나 사이버 공격으로 인한 중단에 취약함.
- **가치의 다양성 결여(Value Plurality):** 단일 기관의 편향이 AI에 그대로 반영됩니다. 중앙화된 기관이 모델에 대해 절대적인 통제권을 행사할 경우^{1 2}, 결과물인 모델의 가치 또한 중앙집중적으로 설정됩니다³. 예를 들어, 구글의 생성형 AI 도구인 Gemini가 재구성한 세계는 광범위한 비판을 받고 있습니다⁴.

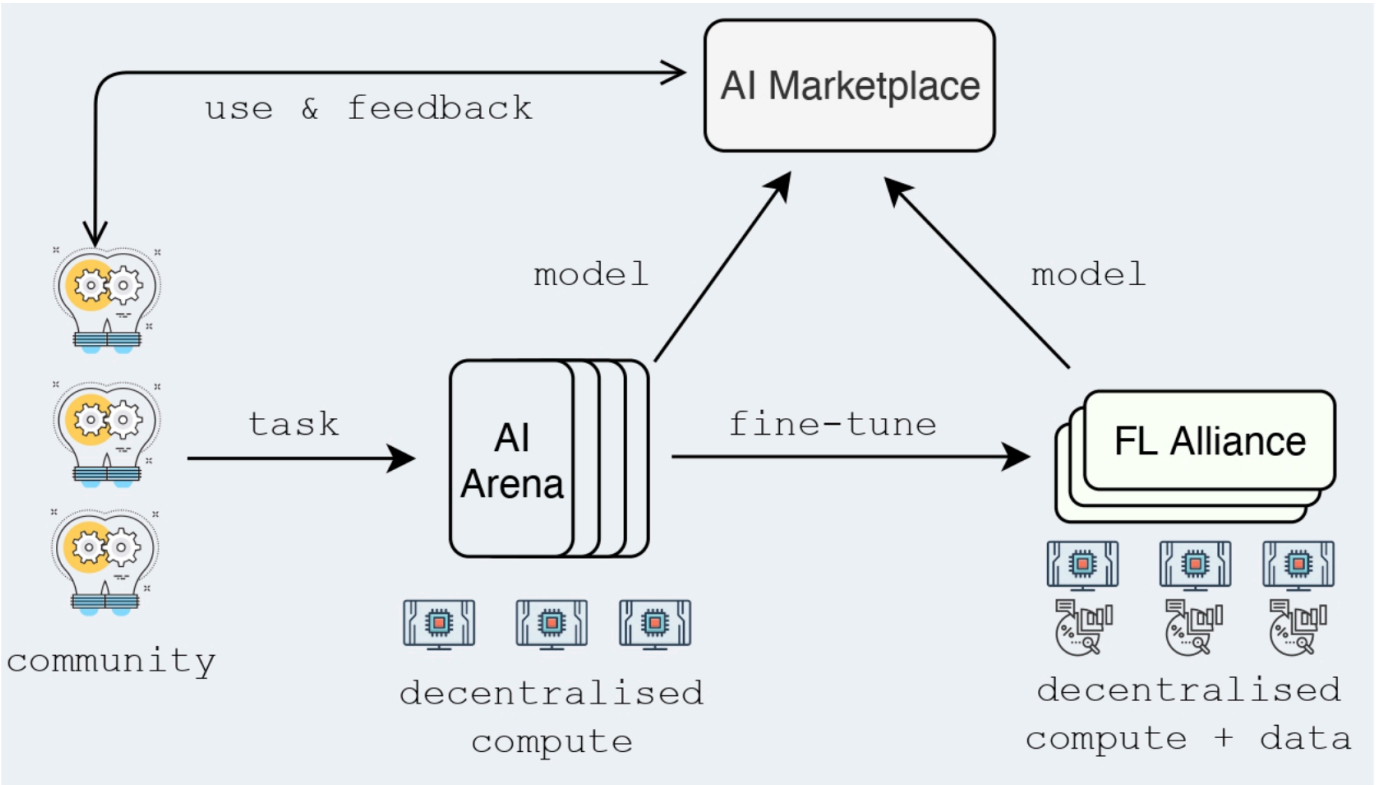


그림 1: Flock 시스템 로직. 태스크가 생성되면, 모델은 먼저 블록체인 기반 분산 훈련 플랫폼인 AI Arena에서 학습 및 검증되고, 이후 선택적으로 참가자들의 로컬 데이터를 활용하여 FL Alliance에서 추가 미세 조정됩니다. 최종적으로 해당 모델은 AI Marketplace의 애플리케이션에 의해 배포되며, 이곳에서 얻은 피드백은 모델의 지속적인 개선에 활용됩니다.

- **데이터 보호:** OpenAI와 같은 폐쇄형 LLM 제공업체⁵는 모델과의 모든 사용자 상호작용을 모니터링할 수 있는 능력을 보유하고 있어, 심각한 데이터 보호 우려를 야기합니다. 또한 이러한 중앙집중형 구조에서는, LLM과 상호작용하는 모든 사용자가 자신도 모르게 모델을 소유한 대기업에 데이터를 제공하는 기여자가 됩니다. 사용자 기여 데이터의 가치 평가를 보다 정확히 수행하고, 기여에 대한 보상 인센티브의 공정성을 제고할 필요성이 시급합니다.
- **거버넌스:** 최근의 연구들^{6 7 8}은, 거버넌스 부재가 모델 내 편향성과 부정확성을 심화시키는 우려스러운 추세를 지적하고 있습니다.
- **확장성:** 데이터의 양과 태스크의 복잡도가 증가함에 따라, 제한된 처리 능력이 병목현상으로 작용합니다.
- **혁신:** 실험을 수행할 수 있는 권한이 소수 기관에만 집중된 환경에서는, 혁신이 저해됩니다.

B. FLock 솔루션

FLock^{9 10}은 블록체인 기반 분산형 AI 플랫폼입니다. 그림 1 및 그림 2에서 볼 수 있듯이, FLock은 AI 시스템에 대한 활발한 참여를 가로막는 장애 요소를 제거하고, 커뮤니티가 모델, 데이터, 컴퓨팅 자원을 모뮬화된 분산 방식으로 기여할 수 있도록 지원합니다. AI 모델은 AI Arena에서 학습 및 검증될 수 있으며, 이후 연합 학습(FL) Alliance에서 추가적으로 정제됩니다. FLock은 블록체인 기술을 활용하여 참가자를 위한 인센티브 메커니즘을 도입하고, 협력적인 환경을 조성합니다. 이로써 커뮤니티에 의해, 커뮤니티와 함께, 커뮤니티를 위해 개발되는 다양한 목적 기반 모델이 생성되며, 특정한 요구를 충족하는 맞춤형 솔루션을 제공합니다.

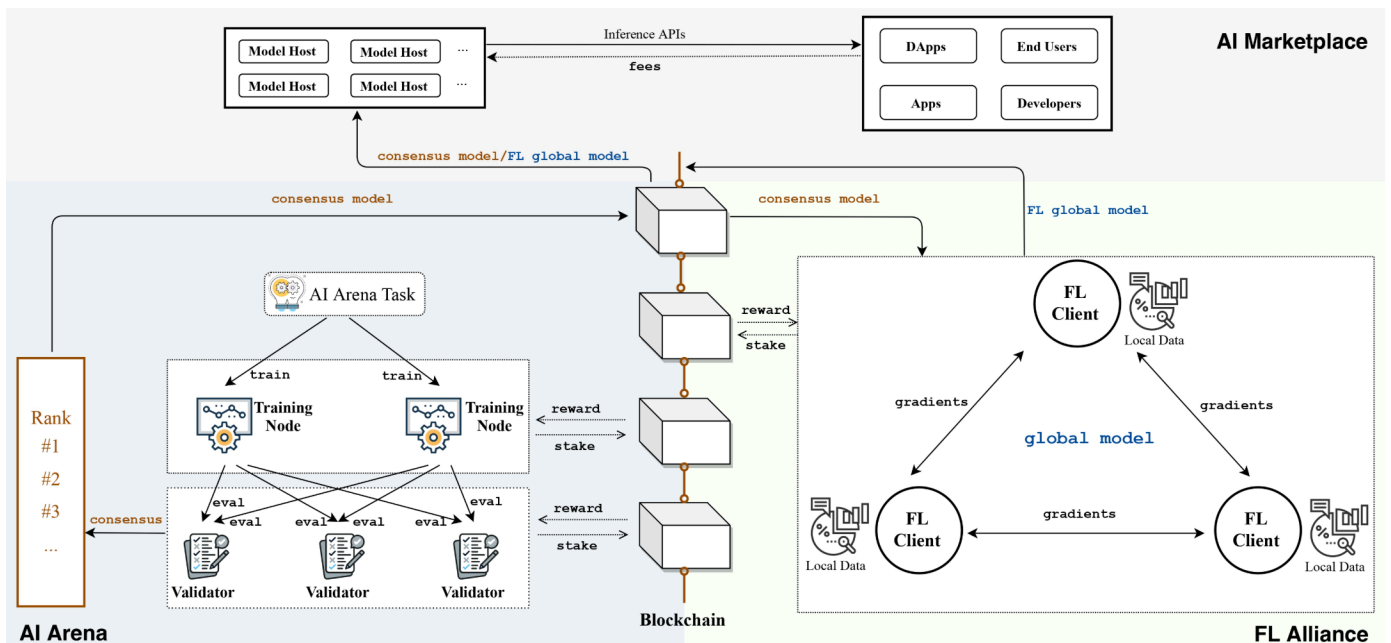


그림 2: FLock 시스템 개요. AI Arena에서 태스크가 생성되면, 학습 노드들이 먼저 모델을 학습시킵니다. 이들 노드는 학습된 모델을 검증자에게 제출하며, 검증자는 각 제출물에 대해 평가 및 점수를 제안합니다. 검증자들은 이 점수에 대해 합의를 도출하고, 제출된 모델들의 순위를 결정합니다. 합의된 모델은 FL 클라이언트에게 할당되어, 이들의 로컬 데이터를 활용해 미세 조정 및 개선이 이루어지며, 최종적으로 FL 글로벌 모델이 완성됩니다. AI Arena 합의 모델 또는 FL 글로벌 모델은 AI Marketplace에 배포 및 호스팅될 수 있으며, 다양한 애플리케이션과의 인터페이스를 제공합니다. AI Arena 학습 노드, 검증자, FL 클라이언트는 시스템에 참여하기 위해 스테이킹을 해야 하며, 성과에 따라 보상을 받습니다.

II. FLock 시스템 개요

FLock 시스템은 블록체인 레이어, AI 레이어, 그리고 다양한 참여자로 구성됩니다. 각 구성 요소는 시스템의 기능성과 보안을 보장하는 데 필수적인 역할을 수행합니다.

A. 블록체인 레이어

FLock의 토크노믹스는 악의적인 사용자 공격에 대한 회복력을 강화하기 위해 설계된 블록체인 기반 보상 메커니즘을 포함합니다. 이러한 강력한 보안 기능은 정교하게 설계된 인센티브 메커니즘에 의해 뒷받침됩니다. 블록체인 레이어는 이해관계자의 참여와 보상 분배의 기반 역할을 합니다. 이 레이어는 스마트 계약을 활용하여 참가자들이 자신의 스테이크를 안전하게 잠글 수 있도록 하며, 신뢰와 투명성이 보장되는 환경을 조성합니다. 이 프로세스는 기여도에 따라 보상을 할당함으로써, 보다 적극적이고 활발한 커뮤니티 참여를 장려하도록 설계되어 있습니다. 블록체인 레이어의 고유한 보안 기능은 사기 행위를 방지하며, 스테이킹과 보상 분배의 무결성을 손상 없이 유지합니다. 이는 모델의 안전성을 지원하고 악의적인 사용자 공격에 대한 회복력을 강화하는 데 있어 중요한 구성 요소입니다. 스마트 계약을 활용함으로써, 시스템은 효율적이고 공정한 보상 절차를 자동화합니다. 자동화는 인간 오류를 줄이고, 보상이 시의적절하고 공정하게 분배되도록 보장합니다.

B. AI 레이어

AI 레이어는 분산 학습을 위한 인프라를 제공하며, 데이터로부터 지식을 추출하고 이를 수익화할 수 있는 구조를 제공합니다. 이 레이어는 커뮤니티로부터의 연산 및 데이터 기여를 장려하며, 블록체인을 활용하여 기여도 기반 보상을 제공합니다.

- **AI Arena.** AI 레이어는 기존의 머신러닝(ML) 모델 학습 패러다임을 지원하며, 사용자의 기기에서 자체 또는 공개 데이터를 사용해 모델을 직접 최적화할 수 있도록 합니다. 최종 학습 모델의 일반화 능력과 성능을 극대화하기 위해, 이 레이어는 커뮤니티 구성원들이 다양한 공개 또는 로컬 데이터를 기여하도록 설계되었습니다. 커뮤니티의 집단 역량을 활용함으로써, 블록체인은 데이터가 모델 개선에 미치는 정량적 영향을 기준으로 지속적인 참여와 보상이 이루어지도록 합니다.
- **FL Alliance.** FL ¹¹ 접근법을 활용하여, AI 레이어는 수천 명의 참여자가 협업을 통해 글로벌 모델을 학습할 수 있도록 합니다. 이 과정에서 데이터 주권은 철저히 보장되며, 학습 과정 중 어떤 단계에서도 로컬 데이터가 전송되지 않습니다. AI 레이어 내에는 모델 집계 구성 요소가 포함되어 있어, 참가자들은 자신들의 고유한 로컬 데이터로 학습된 모델의 가중치를 업로드할 수 있습니다. 이 가중치들은 집계되어 최적의 글로벌 모델을 구축하는 데 사용되며, 결과적으로 모델의 일반화 능력과 성능을 향상시킵니다. 학습 태스크 자동화 및 배포 조정 구성 요소의 통합은 사용자가 태스크에 참여하고 자신의 데이터로부터 추출한 유용한 지식을 기여하는 과정을 간소화합니다.

FLock에서는 AI Arena 태스크를 통해, 공개 데이터셋을 사용하여 모델을 학습 및 검증할 수 있는 컴퓨팅 자원을 보유한 Web2 AI 커뮤니티의 참가자들이 참여하게 됩니다. 이들이 학습한 모델은 이후 FL Alliance 태스크를 통해, 자신의 로컬 데이터를 기여할 수 있는 참여자들에 의해 추가적으로 정제될 수 있습니다.

C. AI 마켓플레이스

모델이 AI Arena와 FL Alliance를 통해 학습 및 미세 조정된 후, 해당 모델은 FLock 플랫폼에 호스팅될 수 있습니다. 이 플랫폼은 머신러닝(ML) 모델의 배포를 위한 종합적인 환경을 제공하며, 블록체인 기반 가상 머신(VM) 네트워크 내에서 접근 가능하도록 합니다. 이러한 네트워크와의 통합을 통해, 플랫폼은 복잡한 ML 모델의 원활한 실행 및 추론을 가능하게 하며, 실시간성, 확장성, 보안성이 확보된 솔루션을 제공합니다.

모델 관리 인프라는 버전 관리, 모델 모니터링, 자동 업데이트 기능을 포함하여, 시간이 지나도 모델의 정확성과 효율성이 유지되도록 보장합니다. 이 플랫폼은 추론(inference) API 또는 SDK를 제공할 수 있어, 개발자들이 해당 모델을 자신들의 애플리케이션에 쉽게 통합할 수 있습니다.

모델 호스트는 기여의 품질과 빈도에 따라 보상을 받습니다. 이들은 추론을 생성하고 인프라를 유지하는 데 중요한 역할을 수행합니다.

D. 참여자

FLock에는 다양한 유형의 참여자가 존재합니다.

1. 태스크 생성자(Task Creators):

태스크 생성자는 학습 태스크를 정의하는 역할을 합니다. 시스템에 충분한 자산을 스테이킹하거나 이미 기여한 이력이 있는 참가자라면 누구나 태스크 생성자로 선정될 수 있습니다. 이는 이해관계자의 범위를 넓히고, 소유 의식과 적극적 참여를 유도합니다.

2. 학습 노드(Training Nodes):

학습 노드는 AI 태스크 학습에 경쟁적으로 참여하며, 자격을 얻기 위해 토큰을 스테이킹해야 합니다. 이 요건은 네트워크 무결성에 대한 책임을 보장하며, 분산되고 신뢰 기반의 태스크 할당 메커니즘을 가능하게 합니다. 스테이킹은 높은 품질 기준을 유지하기 위한 진입 장벽이자, 네트워크 보안 프로토콜의 핵심 요소로 작용하며, 노드가 정확한 실행과 생태계 전반의 건전성에 이해관계를 갖도록 합니다.

3. 검증자(Validators):

검증자는 학습 노드의 작업을 평가하고, 보상 분배에 영향을 미치는 검증 점수를 제출하는 역할을 맡습니다. 이들은 토큰을 스테이킹함으로써 태스크 검증 권한을 얻으며, 하드웨어 호환성과 지분에 비례한 공정한 태스크 분배가 이루어지도록 합니다. 태스크 완료 후, 검증자는 스테이킹을 회수하고 성과 및 기대 결과에 따른 보상을 청구할 수 있습니다. 이 설계는 검증자가 정확하고 정직한 평가를 수행할 유인을 제공하며, 네트워크의 계산 태스크 품질과 신뢰성을 유지합니다.

4. 위임자(Delegators):

위임자는 직접 태스크 학습이나 검증에 참여하지 않고, 다른 참여자의 스테이킹 과정을 지원함으로써 FLock 시스템에 기여합니다. 이를 통해 네트워크의 검증 역량이 향상됩니다. 위임자는 자신이 지원한 대상자의 성과에 기반하여 보상을 공유받으며, 이는 사전에 정의된 알고리즘에 따라 스테이킹 기여도를 반영합니다. 학습 노드 및 검증자는 위임을 수락할 경우, 위임자와의 보상 분배 비율을 자유롭게 설정할 수 있습니다. 이 비율이 높을수록 위임자가 받는 보상 몫이 커집니다. 위임자는 직접 학습이나 검증을 수행할 기술 역량 없이도, 자신의 토큰을 활용하여 시스템의 학습, 검증, 경제 활동에 참여할 수 있습니다.

5. FL 클라이언트(FL Clients):

FL(연합 학습) 프레임워크를 기반으로, FL 클라이언트는 AI Arena 태스크에서 학습된 모델을 향상시키기 위해 자신의 로컬 데이터를 기여합니다. 각 FL 태스크에서 참가자는 무작위로 제안자(proposer) 또는 투표자(voter)로 지정됩니다. 제안자는 FL 프레임워크 내에서 모델 학습을 수행하며, 투표자는 제안자가 생성한 학습 결과를 평가합니다. 제안자와 투표자 모두, 그들의 성과에 따라 보상을 받거나 페널티를 받게 됩니다. FLock은 모든 참가자가 모델 개선에 효과적으로 기여할 수 있

도록 동기를 부여합니다.

6. 모델 호스트(Model Hosts):

AI 마켓플레이스에서 모델 호스트는 학습된 모델을 배포하고 관리하는 역할을 수행합니다. 이들은 안전하고 확장 가능한 실행을 위한 인프라를 제공하며, API와 SDK를 통해 접근성을 제공합니다. 호스트는 모델을 최신 상태로 유지하고, 성능을 모니터링하며, 애플리케이션과의 통합을 지원합니다. 또한 추론을 생성하고 시스템 무결성을 유지한 기여에 대해 보상을 받습니다.

III. FLock 토크노믹스

FLock은 협업을 촉진하고 커뮤니티 내에서 장기적인 정렬(alignment)을 보장하기 위해, 공정하고 인센티브 친화적인 생태계를 구축하는 것을 목표로 합니다. 이러한 비전은 전략적으로 설계된 보상 분배 시스템, 책임성을 위한 효과적인 슬래싱(slashng) 메커니즘, 그리고 적극적인 토큰 수요의 조성을 통해 실현됩니다.

A. 토큰 공급

1. 발행(Emission):

FLock 생태계는 \$FLOCK¹ 토큰을 중심으로 구성되며, 초기 토큰 발행과 시간이 지남에 따라 전략적으로 설계된 보상 분배 시스템을 통해 다양한 이해관계자에게 분배됩니다. 참가자는 시스템에 대한 기여도에 따라 \$FLOCK 토큰으로 보상을 받습니다. FLock 시스템 내 학습 노드 및 검증자와 같은 참가자들은 모델 학습 및 검증을 완료하기 위해 컴퓨팅 또는 스토리지 자원을 기여해야 하며, 이에 따라 보상을 획득할 수 있습니다. 이는 \$FLOCK 토큰의 가치는 최소한 이러한 과정에서 소모된 자원의 가치에 해당함을 의미합니다.

2. 슬래시(Slash):

FLock은 시스템의 무결성과 신뢰성을 보장하기 위해 악의적인 행위를 한 참가자에게 패널티를 부과하는 강력한 메커니즘을 갖추고 있습니다. AI Arena에서, 만약 어떤 참가자가 시스템 규칙에 반하거나 악의적인 방식으로 시스템을 훼손하려는 시도가 확인될 경우, 해당 참가자는 “슬래싱”의 대상이 됩니다. 슬래싱된 토큰은 정직한 참가자에게 보상으로 분배됩니다. 슬래싱은 악의적인 행위자에게 강한 억제 효과를 제공함으로써 즉각적인 위협으로부터 시스템을 보호하며, 참여자 간 신뢰와 협력의 문화를 강화합니다.

B. 토큰 수요

생태계 내 순환 토큰의 가치를 보여주며, 다음과 같은 다각적인 접근을 통해 적극적인 토큰 수요가 유도됩니다.

1. 유틸리티(Utility):

참가자들은 어떤 역할을 수행하기 위해 \$FLOCK 토큰을 스테이킹해야 합니다. 이는 운영의 무결성과 성공에 대한 그들의 이해관계를 반영합니다. 모델 학습을 위해 최상급 학습자를 신속하게 모집해야 하거나 촉박한 마감 시한 하에 있는 태스크 생성자는, 추가적인 \$FLOCK을 현상금(bounty)으로 지불할 수 있습니다. 이 현상금은 해당 태스크에 참여하는 참가자에게 지급되어, 학습 프로세스를 우선 처리할 수 있도록 합니다. 참가자는 또한 \$FLOCK 토큰 위임을 통해 위임자(delegate)로부터 지원을 받을 수 있습니다. 이를 통해 시스템은 FLock 내 참가자의 스테이킹 규모를 증가시키고, 상호 이익 관계를 장려합니다. 위임자는 자신이 지원한 참가자의 보상에서 일정 지분을 공유함으로써, 잠재적 위임자

에게 매력적인 조건을 제공하려는 경쟁적 환경이 조성됩니다.

2. 결제(Payment):

커뮤니티 구성원은 AI Arena와 FL Alliance에서 학습 및 미세 조정된 후, AI 마켓플레이스에 호스팅된 우수 모델에 접근하고 이를 활용할 수 있습니다. 최종 사용자는 자신의 스테이킹 양에 따라 모델 접근에 대한 속도 제한(rate limit)을 적용받으며, 그 한도를 초과하면 \$FLOCK 토큰을 결제 수단으로 사용하게 됩니다. 한편, 모델 호스트는 우수 모델을 호스팅하기 위해 \$FLOCK을 스테이킹해야 합니다. 이들은 최종 사용자를 대상으로 요금을 부과할지 여부 및 방식에 대해 자유롭게 설정할 수 있습니다. 초기 단계에서는 모델 호스트에게 일일 토큰 발행량의 일부가 보상으로 제공되어 참여를 유도하지만, 이러한 인센티브는 시간이 지나면서 점차 감소할 것으로 예상됩니다. 전반적으로 이러한 설계는 수요와 공급이 역동적으로 균형을 이루는 지속 가능하고 경쟁적인 환경을 조성하여, 혁신을 촉진하고 최신 기술이 시장의 변화하는 수요를 지속적으로 충족하도록 합니다. 결제 메커니즘은 또한 모델 접근에 일정 수준의 금전적 장벽을 형성하여, 악의적인 참가자로부터의 서비스 거부(DoS) 공격을 완화하는 데 기여합니다.

3. 거버넌스 참여(Governance Participation):

\$FLOCK 토큰을 보유함으로써, 구성원은 탈중앙 자율 조직(DAO) 거버넌스를 통해 네트워크의 미래에 영향을 미칠 수 있는 권한을 가집니다. 이는 의사결정의 탈중앙화를 실현할 뿐만 아니라, 토큰에 생태계 발전을 설계하는 열쇠로서의 유틸리티와 가치를 부여합니다.

IV. FLock 인센티브 및 보안

A. 인센티브

FLock은 정교하게 설계된 인센티브 메커니즘을 활용하여 참가자에게 보상을 제공합니다. 새로 발행되는 토큰의 분배는 AI Arena 태스크와 FL Alliance 태스크 전반에 걸쳐 신중하게 조율되며, 각 태스크 카테고리 내 스테이킹 역학에 따라 전략적으로 할당됩니다.

우리 시스템에서는 검증된 태스크에 일일 보상의 일부가 배분되며, 이는 태스크 생성 생태계의 성장을 장려하기 위한 인센티브로 작용합니다. 이러한 보상 분배는 프로토콜이 낮은 품질이거나 악의적인 태스크에 의해 악용되어, 실질적인 가치 없이 보상을 소모하는 사태를 방지하기 위해 DAO의 승인을 받은 태스크로 제한됩니다.

새로 생성되는 각 AI Arena 및 FL Alliance 태스크는 커뮤니티 주도의 DAO에 의해 수행되는 검증 과정을 선택적으로 거칠 수 있습니다. 이 검증 절차는 태스크가 생태계의 목표에 부합하며, 요구되는 품질 기준을 충족하는지를 보장하기 위해 설계되었습니다. 태스크가 검증을 통과하면, 해당 태스크는 \$FLOCK의 일일 발행량(emission)으로부터 보상을 받을 자격을 얻게 되며, 태스크 생성자는 이를 통해 참여 및 협업을 유도할 추가 자원을 확보할 수 있습니다.

반면, FLock DAO의 검증 없이 퍼미션리스(permissionless) 방식으로 태스크가 생성될 경우, 해당 태스크에 대한 재정적 책임은 전적으로 태스크 생성자에게 있습니다. 이는 다양한 참가자에게 지급되는 보상과 관련된 비용을 자신의 \$FLOCK 토큰으로 충당해야 함을 의미합니다. 이러한 방식은 태스크 생성에 있어 더 큰 유연성과 탈중앙화를 허용하는 반면, 태스크 생태계를 지원하기 위한 재정적 부담을 생성자에게 전가합니다. 이 메커니즘은 창의성과 품질 통제를 균형 있게 조화시키기 위해 설계되었으며, 커뮤니티 지원 보상의 혜택은 구조적으로 잘 구성된 태스크에 한정되면서도 생태계 내 자유로운 실험을 허용합니다.

장기적으로 이 이중 구조는 고품질 태스크 생성을 유도하고, 활기차고 신뢰할 수 있는 생태계를 조성하며, 인센티브를 커뮤니티의 기준 및 목표와 정렬시킴으로써 \$FLOCK 보상 시스템의 무결성을 유지하는 것을 목표로 합니다.

태스크가 생성된 이후, DAO 검증을 통과한 AI Arena 및 FL Alliance 태스크 간의 보상 분배는 각각의 활성 태스크에 대한 상대적 스테이킹 양에 따라 결정됩니다. 이에 따라, 모든 활성 AI Arena 태스크에 할당되는 \$FLOCK 보상의 양은 다음과 같습니다:

$$R^{AI} = C_0 \cdot \frac{S^{AI}}{S^{AI} + S^{FL}}$$

그리고 모든 활성 FL Alliance 태스크의 경우에는 다음과 같습니다:

$$R^{FL} = C_0 \cdot \frac{S^{FL}}{S^{AI} + S^{FL}}$$

여기서 \$C_0\$는 \$FLOCK의 일일 발행량(emission), \$S^{AI}\$는 모든 활성 AI Arena 태스크의 총 스테이킹 금액, \$S^{FL}\$은 모든 활성 FL Alliance 태스크의 총 스테이킹 금액을 나타냅니다.

B. 보안 및 공격 완화

공격 유형	설명	FLock의 대응 방안
시빌 공격 (Sybil Attacks)	공격자가 여러 개의 가짜 참가자 신원을 생성 및 제어하여 FLock 시스템에서 과도한 영향력을 얻으려 할 수 있음.	- 자산 스테이킹은 다수의 학습 노드 또는 검증자를 제어하는 데 필요한 비용을 증가시켜 공격 난이도를 높입니다. - 블라인드 검증 메커니즘은 학습 노드와 검증자 간의 담합을 방지합니다. - 각 태스크에서 성능 상위 \$k_1\$개 학습 노드 및 \$k_2\$개 검증자에게만 보상이 주어지므로, 낮은 성능의 참가자는 보상을 받을 수 없습니다.
서비스 거부 공격(DoS Attacks)	공격자가 시스템 자원을 고갈시켜 정직한 참가자가 시스템을 사용할 수 없도록 만들 수 있음.	- 일정 시간 내 조치 빈도 및 볼륨을 제한하는 속도 제한(rate limiting)을 구현하여, 특정 참가자가 시스템을 과도하게 점유하는 것을 방지합니다.
무임승차 공격(Free-rider Attacks)	무임승차자는 공정한 기여 없이 시스템의 혜택을 누립니다. FLock에서는 학습하지 않은 모델을 무작위로 제출하는 학습 노드나, 평가 없이 무작위 점수를 주는 검증자가 이에 해당됩니다.	- 각 태스크에서 성능 상위 \$k_1\$개 학습 노드와 \$k_2\$개 검증자에게만 보상이 주어져, 낮은 성능의 참가자는 보상을 받을 수 없습니다. - FLock AI Arena의 합의 메커니즘은 성실하게 기여한 정직한 참가자가 적절히 인정받고 보상받도록 하여, 무임승차자가 시스템을 악용하지 못하게 합니다.
룩업 공격(Lookup Attacks)	학습 노드가 과거의 검증 점수 계산 방식을 학습하여 부정확한 방법으로 점수를 높이려 할 수 있음.	- 두 개의 데이터셋(Dataset A와 B)을 검증 세트로 사용하여 모델을 평가합니다. - 따라서, 학습 노드가 Dataset A에 최적화하더라도 Dataset B에서는 성능이 떨어질 수 있습니다. - Dataset A와 B 사이의 보상 균형을 정교하게 조정함으로써, FLock은 학습 노드가 진정으로 고품질 모델을 개발하도록 유도합니다.
FL 모델 오염 공격(FL Model Poisoning Attacks)	FL Alliance에서, 공격자가 편향되거나 손상된 데이터를 사용하여 모델 성능을 저하시킬 수 있음.	- 다수결 집계를 통해 악의적인 참가자 1인의 영향력을 최소화합니다. - 슬래싱 메커니즘은 악의적인 클라이언트에게 패널티를 부과하여, 모델 오염 공격을 억제하고 향후 공격을 방지합니다.

표 I: FLock 시스템의 잠재적 공격에 대한 완화 전략 요약.

초기 단계에서는 참여를 유도하기 위해, 태스크 생성자도 보상 토큰의 일부를 수령하게 됩니다. 그러나 이 보상은 시간이 지남에 따라 점진적으로 제거될 예정입니다.

AI Arena에서는 이 할당이 각 태스크에 대해 태스크 생성자, 학습 노드, 검증자, 위임자의 총 스테이킹 기여도를 기준으로 정밀하게 계산됩니다.

1. AI Arena 태스크 간 보상 분배:

하루 동안, M 개의 AI Arena 태스크가 존재하고 각각의 총 스테이킹 금액이 $(S_1, \dots, S_M)$ 라고 가정합니다.

각 태스크의 총 스테이킹 금액 S_i 는 해당 태스크에 참여하는 모든 유형의 사용자가 스테이킹한 토큰을 포함합니다.

즉, 어떤 유형의 사용자든 해당 태스크에 스테이킹한 금액은 보상 분배에 영향을 미치게 됩니다.

여기서 S_p 는 DAO 결정에 따라 조정 가능한 시스템 파라미터입니다.

AI Arena 전체에 대해 하루 동안 발행되는 $FLOCK$ 토큰의 양을 C_{AI} 라고 가정할 때, 스테이킹 총합이 S_i 인 AI Arena 태스크 i 에 대한 일일 보상액은 다음과 같이 정의됩니다:

$$R_i^{AI} = C_{AI} \cdot \frac{S_i^p}{\sum_{k=1}^M S_k^p}$$

각 AI Arena 태스크 내에서는 태스크 생성자, 학습 노드, 검증자, 위임자 간에 보상이 분배됩니다. FLock의 초기 버전에서는, 검증자에게 위임자가 존재할 경우 전체 보상의 $d_1\%$ 가 해당 위임자에게 배정됩니다.

이 분배 비율 파라미터는 유동적이며, FLock DAO 거버넌스를 통해 조정될 수 있습니다.

2. FL Alliance 태스크 간 보상 분배:

FL Alliance 태스크는 반드시 완료된 AI Arena 태스크를 기반으로 하여 추가적인 미세 조정을 목적으로 생성됩니다.

FL Alliance 태스크가 시작되면 자동으로 새로운 FL 스마트 계약이 생성됩니다.

생태계 내 활성 FL Alliance 태스크마다, 해당 태스크가 아직 진행 중이고 설정된 최대 생애 주기를 초과하지 않았다면,

일일 보상은 해당 FL 스마트 계약으로 이전됩니다.

이 초기 단계는 보상이 해당 태스크에 실제로 참여 중인 참가자들에게 안전하게 예약되도록 보장합니다.

이후, 사전에 정의된 조건을 충족하게 되면, FL 스마트 계약은 참가자의 기여도에 따라 보상을 자동으로 분배합니다.

B. 보안

표 I에서 보여지듯, FLock 시스템의 보안 설계는 다양한 공격에 대한 회복력을 갖추고 있습니다.

시빌(Sybil) 공격은 최소 자산 스테이킹 요건을 통해 완화되며, 이는 다수의 신원을 제어하는 데 높은 비용이 들게 만듭니다.

검증자는 모델의 출처를 알 수 없도록 설계되어 있어 담합의 위험이 줄어듭니다.

보상은 오직 상위 성과를 낸 학습 노드와 검증자에게만 지급되며, 이는 저조한 성능이나 조작 시도를 억제합니다.

DoS(서비스 거부) 공격을 완화하기 위해 시스템은 속도 제한(rate limiting)을 구현하여, 어느 한 참가자가 자원을 독점하는 것을 방지합니다.

무임승차(free-rider) 공격에 대해서는, 실질적 기여도가 높은 참가자만 보상을 받도록 하여 기여 없는 사용자가 이익을 얻지 못하게 합니다.

룩업(lookup) 공격을 방지하기 위해 두 개의 검증 데이터셋(Dataset A와 B)을 사용하며, 하나의 데이터셋에만 최적화하는 것이 성공을 보장하지 않도록 합니다.

FL 모델 오염 공격에 대해서는 다수결 집계와 슬래싱 메커니즘을 통해 모델 무결성을 보호하며, 악의적인 행위자에게 패널티를 부과하고 향후 공격을 억제합니다.

이러한 조치들은 FLock을 다양한 위협으로부터 강력히 방어하여, 참가자에게 안전하고 신뢰할 수 있는 탈중앙화 학습 환경을 제공합니다.

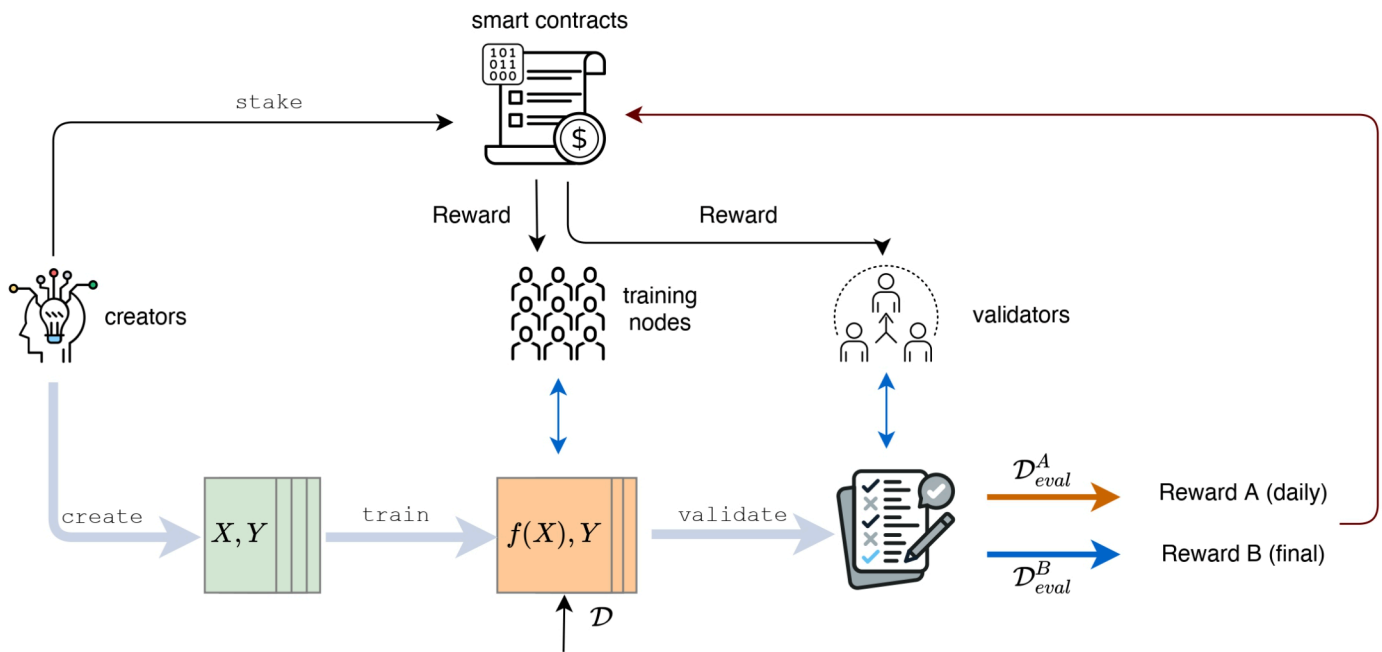


그림 3: FLock AI Arena 태스크의 워크플로우 개요. 검증자는 합의 점수(consensus score)에 기반하여 보상을 획득합니다.

학습 노드의 룩업/과적합(lookup/overfitting) 공격을 완화하기 위해 두 가지 유형의 보상이 사용됩니다.

V. FLock AI Arena의 합의 메커니즘

그림 3은 FLock AI Arena 태스크의 워크플로우 개요를 보여줍니다.

A. 태스크 생성자 (Task Creators)

태스크 생성은 학습 사이클의 가장 초기 단계입니다. 생성자는 원하는 모델을 정의하고 플랫폼에 태스크를 제출합니다.

자격 요건을 충족하는 누구든지 태스크 생성자가 될 수 있기 때문에, 시스템은 본질적으로 민주적이며 다양한 이해관계자에게 개방되어 있습니다.

이러한 포용성은 FLock 커뮤니티 내 소유 의식과 능동적 참여를 고취시킵니다.

태스크 생성 자격을 얻기 위해 사용자는 다음 기준 중 하나 이상을 충족해야 합니다:

- 충분한 양의 \$FLOCK\$을 스테이킹할 것
- 온체인 기록을 통해 입증된 과거 학습 또는 검증 태스크를 성공적으로 수행한 이력 보유
- 머신러닝 분야에서의 평판 또는 해당 분야의 도메인 전문가로서의 자격을 FLock 커뮤니티로부터 인정받은 경우

태스크 생성자와 해당 태스크가 FLock DAO에 의해 검증될 경우, 해당 태스크는 \$FLOCK\$ 일일 발행량 (emission)에 대한 보상 자격을 얻게 됩니다.

반면, 커뮤니티 주도 DAO의 검증을 선택하지 않을 경우, 태스크 생성자는 참가자 보상 분배에 필요한 \$FLOCK\$을 직접 지불하며 태스크를 자비로 운영해야 합니다.

태스크 생성자는 원하는 학습 모델에 접근할 수 있을 뿐 아니라, 기여에 대한 보상을 획득할 수도 있습니다. 다만 이러한 보상은 시간이 지남에 따라 점진적으로 축소될 예정입니다.

B. 학습 노드 및 검증자 선택 (Training Node and Validator Selection)

이 구조에서 각 참가자는 태스크 학습 또는 검증을 수행할 자격을 얻기 위해 먼저 시스템에 스테이킹해야 합니다.

실제 운영에서는, 각 태스크에 대해 참가자가 검증에 접근할 수 있는 횟수를 제한하기 위해 속도 제한(rate limiting)이 적용됩니다.

그림 4에서 볼 수 있듯이, 참가자가 특정 제출물을 검증 대상으로 선택될 확률은 자신의 스테이킹 양에 비례하여 증가합니다.

그러나 스테이킹 양이 많아질수록, 검증 빈도 증가율은 점차 완만해지는 경향을 보입니다.

C. AI Arena에서의 학습 (Training in AI Arena)

학습 노드가 보유한 데이터셋 $\mathcal{D}_{\text{local}}$ 을 고려합니다. 이 데이터셋은 로컬에서 수집된 데이터 샘플로 구성되며,

특징 집합 X 와 레이블 집합 Y 로 나뉘며, 각 샘플 $x_i \in X$ 는 레이블 $y_i \in Y$ 에 대응합니다.

예측 모델 f 는 $\mathcal{D}$ 내 패턴을 학습하여 $f(x_i) \approx y_i$ 를 만족하도록 설계됩니다.

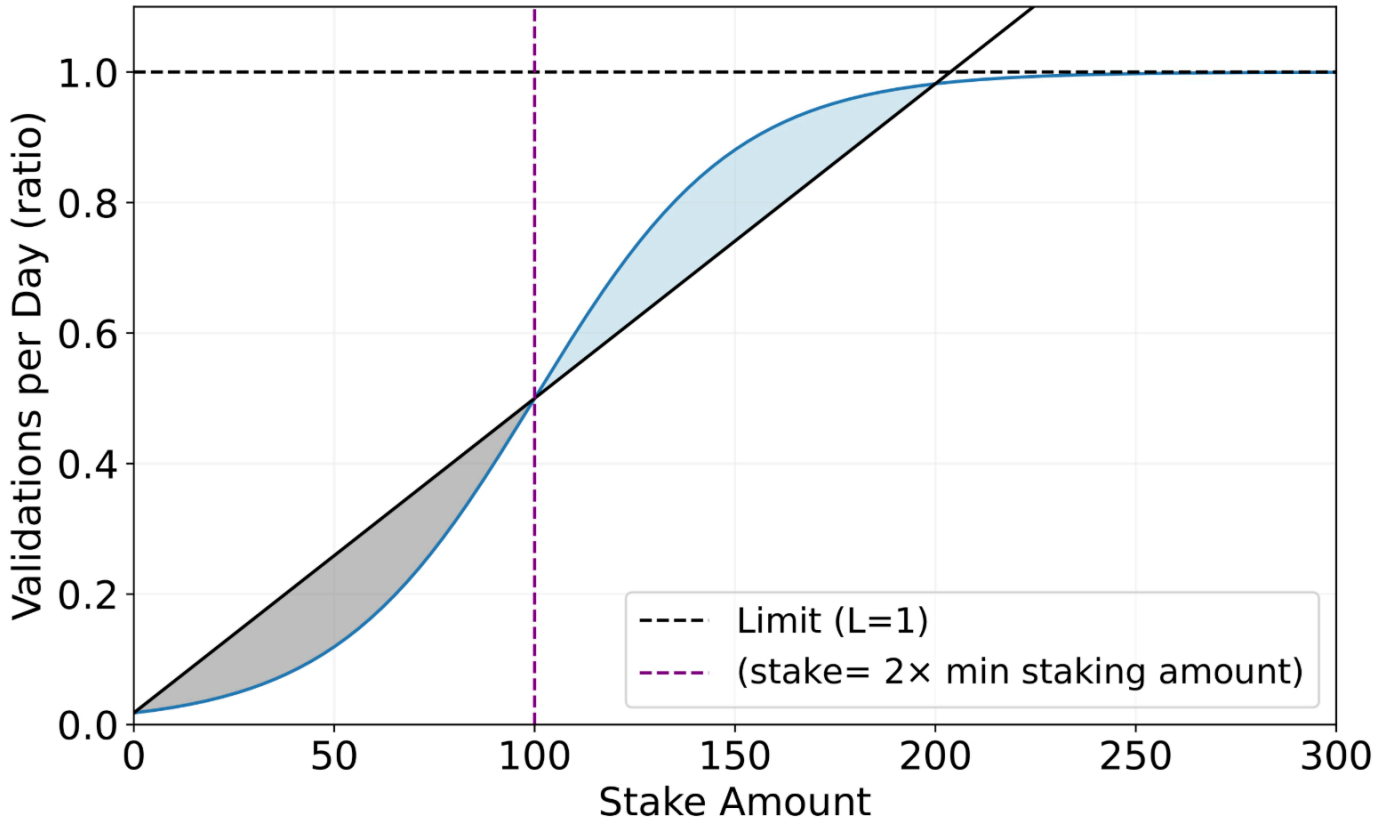


그림 4: 검증 빈도에 대한 속도 제한 예시.

예측 지표를 정량화하기 위해, 예를 들어 정확도(accuracy)를 사용할 경우, 태스크 트레이너는 손실 함수 $L(f(x_i), y_i)$ 를 도입하여 예측값 $f(x_i)$ 와 실제 레이블 y_i 간의 차이를 평가합니다. 이 손실 함수의 일반적인 표현은 다음과 같습니다:

$$L = \frac{1}{N} \sum_{i=1}^N l(f(x_i), y_i)$$

여기서 N 은 전체 샘플 수를 나타내며, l 은 문제 특화 손실 함수로서 평균 제곱 오차(mean squared error) 또는 크로스 엔트로피 손실(cross-entropy loss) 등이 될 수 있습니다.

최적화의 목표는 모델 파라미터 θ 를 조정하여 L 을 최소화하는 것입니다. 일반적으로는 경사 하강법(gradient descent)과 같은 알고리즘을 통해 이루어집니다:

$$\theta_{\text{new}} = \theta_{\text{old}} - \eta \nabla_{\theta} L$$

여기서 η 는 학습률(learning rate)을, $\nabla_{\theta} L$ 은 θ 에 대한 손실 함수 L 의 그래디언트를 의미합니다.

집계된 데이터셋 $\mathcal{D}$ 를 활용하여, 파라미터 θ 는 L 을 줄이기 위해 반복적으로 업데이트되며, 이로써 모델의 예측 정확도가 향상됩니다.

이러한 최적화 과정은 사전에 정의된 에폭(epoch) 수 E 동안 수행되며, 각 에폭은 전체 데이터셋 $\mathcal{D}$ 를 한 번 완전히 순회하는 과정으로 구성됩니다.

D. AI Arena에서의 검증

검증자 집합 V 중 선택된 일부 검증자를 $V_j \in V$ 라고 가정합니다. 이들은 태스크 생성자로부터 제공된 평가 데이터셋 $\mathcal{D}_{\text{eval}}$ 을 보유하고 있으며, 이 데이터셋은 (x_i, y_i) 쌍으로 구성되어 있습니다. 여기서 x_i 는 i 번째 샘플의 특징 벡터, y_i 는 그에 대응하는 실제 레이블입니다.

학습 노드에 의해 학습된 모델은 θ_p^{task} 로 표현됩니다. 이 모델의 주요 목적은 $\mathcal{D}_{\text{eval}}$ 에 포함된 각 입력 벡터 x_i 에 대한 예측 레이블 $\hat{y}_i$ 를 출력하는 것입니다.

$\mathcal{D}_{\text{eval}}$ 에서 θ_p^{task} 의 성능을 평가하기 위해, 일반적인 평가 지표 `eval`을 사용합니다.

예시로서 정확도(accuracy)는 다음과 같이 계산됩니다:

$$\text{eval}(\theta_p^{\text{task}}, \mathcal{D}_{\text{eval}}) = \frac{1}{|\mathcal{D}_{\text{eval}}|} \sum_{(x_i, y_i) \in \mathcal{D}_{\text{eval}}} \mathbf{1}(\hat{y}_i = y_i)$$

여기서 $\mathbf{1}$ 은 예측된 레이블 $\hat{y}_i$ 가 실제 레이블 y_i 와 일치하면 1을, 그렇지 않으면 0을 반환하는 지시 함수(indicator function)를 나타냅니다.

또한 $|\mathcal{D}_{\text{eval}}|$ 은 평가 데이터셋 내 샘플의 총 개수를 나타냅니다.

모델 θ_p^{task} 로부터 예측된 각 $\hat{y}_i$ 는 $\mathcal{D}_{\text{eval}}$ 내 해당 샘플의 실제 레이블 y_i 와 비교됩니다.

이 계산된 정확도 지표는, 평가 데이터셋 전반에 걸쳐 θ_p^{task} 가 얼마나 효과적으로 레이블을 예측하는지를 정량적으로 나타내는 지표입니다.

E. AI Arena에서 학습 노드에 대한 보상

하나의 AI Arena 태스크 내에서, 학습 노드와 검증자 간의 보상 분배는 상대적인 스테이킹 양에 따라 결정됩니다.

n 개의 학습 노드가 제출한 결과물 $(O_1, \dots, O_n)$ 과 m 명의 검증자 $(V_1, \dots, V_m)$ 가 존재한다고 가정하며, 각 검증자는 스테이킹 값 $(s_1, \dots, s_m)$ 을 보유하고 있다고 가정합니다.

이 스테이킹 값은 검증자의 책임감과 프로세스에 대한 신뢰를 나타내며, 평가 점수 집계 시 가중치에 영향을 미칩니다.

태스크에 할당된 일일 보상 총액을 R_0 라고 하고, 보상 분할 균형을 정의하는 파라미터 γ 는 고정 보상과 스테이킹 기반 보상 간의 비율을 조절합니다.

이에 따라 학습 노드 전체에 할당되는 보상은 다음과 같습니다:

$$R_0 \cdot \left(\gamma + (1 - 2\gamma) \cdot \frac{\sum_{i=1}^n t_i}{\sum_{i=1}^n t_i + \sum_{j=1}^m s_j} \right)$$

- 각 검증자 V_j ($1 \leq j \leq m$)는 학습 노드가 제출한 n 개의 모델을 평가하여 점수 벡터

$\vec{r} = (r_{j1}, \dots, r_{jn})$ 를 생성합니다.

이 점수는 사전 정의된 기준에 따라 각 모델의 정확도, 신뢰성 또는 성능을 반영합니다.

악의적인 검증자가 제안한 이상치 점수는 정직한 검증자들에 의해 무시되며, 이후 과정에서 고려되지 않습니다.

- 각 학습 노드 모델에 대한 최종 점수는 스테이킹 기반 가중 합산을 통해 결정됩니다:

$$\vec{r} = \left(\frac{\sum_j r_{j1} \cdot s_j}{\sum_j s_j}, \dots, \frac{\sum_j r_{jn} \cdot s_j}{\sum_j s_j} \right)$$

이는 스테이킹이 많은 검증자의 평가가 최종 결과에 더 큰 영향을 미친다는 것을 의미합니다.

- 이후 다음과 같은 기하급수 수열을 계산합니다:

$$g_k = \frac{1 - q}{1 - q^m} \cdot q^{k-1}$$

여기서 k 는 해당 태스크 내에서 특정 학습 노드의 순위를 나타내며, q 는 공비, m 은 해당 태스크에 참여한 학습 노드 수입니다.

Flock 시스템의 참가자인 학습 노드와 검증자는 보상을 받기 위해 모델 학습 및 검증을 수행하는 데 필요한 컴퓨팅 또는 스토리지 자원을 제공해야 합니다.

따라서 FLOCK 토큰의 가치는 최소한 이러한 과정에서 소모된 자원의 가치에 상응하게 됩니다.

- 마지막으로, 제출물의 품질과 총 스테이킹 금액에 기반하여 학습 노드 및 그 위임자에게 할당되는 총 보상을 다음과 같이 계산합니다:

$$f_i(g_i, t_i) = \frac{g_i \cdot t_i^{\alpha_i}}{\sum_{k=1}^n g_k \cdot t_k^{\alpha_k}}$$

여기서 α_i 는 보상 분배에서 스테이킹의 영향을 조절하는 시스템 파라미터이며, t_i 는 학습 노드 i 와 그에 연결된 위임자의 총 스테이킹 금액을 의미합니다.

- 학습 노드 i 가 설정한 보상 분배 비율을 σ 라고 가정합니다. 이는 해당 학습 노드와 위임자 간에 보상을 어떻게 나눌지를 결정합니다.
또한, 학습 노드 i 의 직접 스테이킹 금액을 t_n , 위임된 스테이킹 금액을 t_d 라고 할 때, 총 스테이킹 금액은 $t_i = t_n + \epsilon \cdot t_d$ 로 정의되며, 여기서 ϵ 은 유효 위임 비율을 결정하는 시스템 파라미터입니다.
그에 따라 학습 노드 i 의 실제 보상은 다음과 같이 계산됩니다:

$$f_i \cdot \left(\sigma + (1 - \sigma) \cdot \frac{t_n}{t_n + t_d} \right)$$

F. AI Arena에서 검증자 보상

학습 노드의 보상 계산과 유사하게, 동일한 AI Arena 태스크 내 모든 검증자에게 할당되는 보상은 다음과 같습니다:

$$R_0 \cdot \left(\gamma + (1 - 2\gamma) \cdot \frac{\sum_{j=1}^m s_j}{\sum_{i=1}^n t_i + \sum_{j=1}^m s_j} \right)$$

각 검증자 V_j 에 대해, 이들의 점수와 최종 집계 점수 간의 차이를 계산합니다:

$$\vec{\Delta}_j = (\Delta_{j1}, \dots, \Delta_{jn}) = \left(\left| \frac{\sum_j r_{j1} \cdot s_j}{\sum_j s_j} - r_{j1} \right|, \dots, \left| \frac{\sum_j r_{jn} \cdot s_j}{\sum_j s_j} - r_{jn} \right| \right)$$

다음 조건을 만족하는 분배 함수 f_i 를 정의합니다:

$$\begin{cases} f_i(\Delta_{1i}, s_1) + \dots + f_i(\Delta_{mi}, s_m) = 1, \\ f_i \text{는 거리 } \Delta_{ji} \text{가 커질수록 감소,} \\ f_i \text{는 스테이킹 양 } s_j \text{이 증가할수록 증가.} \end{cases}$$

이 세 가지 조건을 만족시키기 위해, Softmax 함수를 변형한 다음 함수를 사용할 수 있습니다:

$$f_i(\Delta_{ji}, s_j) = \frac{e^{-\lambda_i \Delta_{ji}} \cdot s_j^{\alpha_j}}{\sum_{k=1}^m e^{-\lambda_i \Delta_{ki}} \cdot s_k^{\alpha_k}}$$

여기서 파라미터 λ 와 α 는 다음과 같은 핵심적인 역할을 수행합니다:

- λ_v

- **목적:** 거리 Δ_{ji} 에 대한 함수의 민감도를 조절합니다. 이 거리는 검증자의 점수와 최종 집계 점수 간의 차이를 측정합니다.
- **효과:** λ_v 가 클수록 함수는 점수 정확도에 더 민감하게 반응하며, 정밀한 평가의 중요성이 강조됩니다.
- **선택 기준:** λ_v 의 설정은 부정확한 평가에 대한 패널티와 거의 정확한 평가에 대한 보상 사이의 균형을 맞추는 데 기반합니다.

- α_v

- **목적:** 보상 분배에서 스테이킹 금액 s_j 의 영향을 결정하여, 검증자의 재정적 기여에 부여되는 가중치를 조정합니다.
- **효과:** 검증자의 재정적 책임과 평가 정확성 간의 균형을 조절할 수 있습니다. α_v 가 높을수록 보상 계산에서 스테이킹 금액이 더 큰 영향을 미치게 됩니다.
- **선택 기준:** 이 값은 스테이킹의 중요성과 점수 정확도 간의 상대적 우선순위에 대한 시스템 철학을 반영합니다. $\alpha_v = 0$ 이면 스테이킹은 완전히 무시되고, 높은 값일수록 그 영향이 커집니다.

검증자가 여러 번(N 번) 검증 태스크를 완료했다면, 해당 검증자의 전체 보상 비율은 다음과 같이 계산됩니다:

$$\sum_{i=1}^N f_i(\Delta_{ji}, s_j)$$

검증자의 해당 태스크 내 스테이킹 금액을 s_v 라고 하고, 총 위임 받은 스테이킹 금액을 s_d 라고 할 때, 전체 누적 스테이킹은 다음과 같이 정의됩니다:

$$s_j = s_v + \epsilon \cdot s_d$$

여기서 ϵ 은 유효 위임 비율을 조정하는 시스템 파라미터입니다. 이때, 해당 검증자의 실제 보상 비율은 다음과 같이 계산됩니다:

$$\left(\sum_i f_i(\Delta_{ji}, s_j) \right) \cdot \left(\sigma + (1 - \sigma) \cdot \frac{s_v}{s_v + s_d} \right)$$

여기서 σ 는 검증자가 설정하는 보상 분배 비율로, 직접 스테이킹한 금액과 위임 받은 금액 간의 보상 분배 비율을 조절합니다.

G. 위임 스테이킹 (Delegate Staking)

위임자는 자신이 선택한 참가자에게 토큰을 위임함으로써 수동적인 투자 수익 흐름(passive income)을 얻을 수 있습니다.

수령자는 자신의 스테이킹 규모, 영향력, 투표권, 보상을 증대시킬 수 있으며, 이러한 보상은 위임자와 공유되어 협력을 더욱 촉진합니다.

이 메커니즘은 토큰은 보유하고 있지만 AI 모델 학습이나 검증에 필요한 기술적 전문성이 부족한 사용자들도 생태계에 참여할 수 있도록 확장합니다.

구체적으로, 위임자의 보상은 다음 두 요소에 따라 결정됩니다:

- 위임 대상으로 선택한 학습 노드 또는 검증자의 품질
- 위임자가 위임한 스테이킹 금액

형식적으로, ϵ 을 유효 위임 비율(effective delegation amount)로 가정할 때, 학습 노드에 토큰을 위임한 위임자의 보상은 다음과 같이 계산됩니다:

$$f_i \cdot (1 - \sigma) \cdot \frac{t_d}{t_n + t_d}$$

여기서:

- f_i 는 해당 학습 노드 i 의 제출물 품질을 기준으로 산정된 학습 노드 및 위임자에게 분배된 총 보상,
- t_d 는 위임자의 스테이킹 금액,
- t_n 은 학습 노드 i 의 자체 스테이킹 금액,
- σ 는 학습 노드 i 가 사전에 설정한 보상 분배 비율을 의미합니다.

유사하게, 검증자에게 위임한 위임자의 보상은 다음과 같이 계산됩니다:

$$\left(\sum_i f_i(\Delta_{ji}, s_j) \right) \cdot (1 - \sigma) \cdot \frac{s_d}{s_v + s_d}$$

여기서:

- $\sum_i f_i(\Delta_{ji}, s_j)$ 는 앞서 설명한 Softmax 함수 기반의 검증자 보상 분배 비율,
- s_d 는 해당 위임자의 스테이킹 금액,
- s_v 는 검증자의 자체 스테이킹 금액을 의미합니다.

향후 FLock의 위임 스테이킹은 기존의 리스테이킹(restaking) 플랫폼들과 통합될 수 있는 선택지를 제공하여, 보다 넓은 블록체인 커뮤니티의 사용자를 유입할 수 있도록 할 예정입니다.

H. 다양한 검증 데이터셋 (Various Validation Sets)

악의적인 학습 노드로부터의 룩업(lookup) 공격을 방지하기 위해, FLock의 검증자들은 다양한 검증 데이터셋을 채택합니다.

특히, x 일에 걸쳐 수행되는 AI Arena 태스크의 경우, 초기 $x - 1$ 일 동안 사용되는 검증 데이터셋은 마지막 날에 사용되는 데이터셋과 다릅니다.

이와 같은 상이한 검증 데이터셋은 **Reward A**(초기 기간)와 **Reward B**(최종일)에 각각 대응되는 두 가지 유형의 보상과 연계되어 있습니다.

이러한 전략적 설계는 학습 노드가 검증에 사용될 데이터를 예측하여 조작하는 시도를 복잡하게 만들어 보안을 강화합니다.

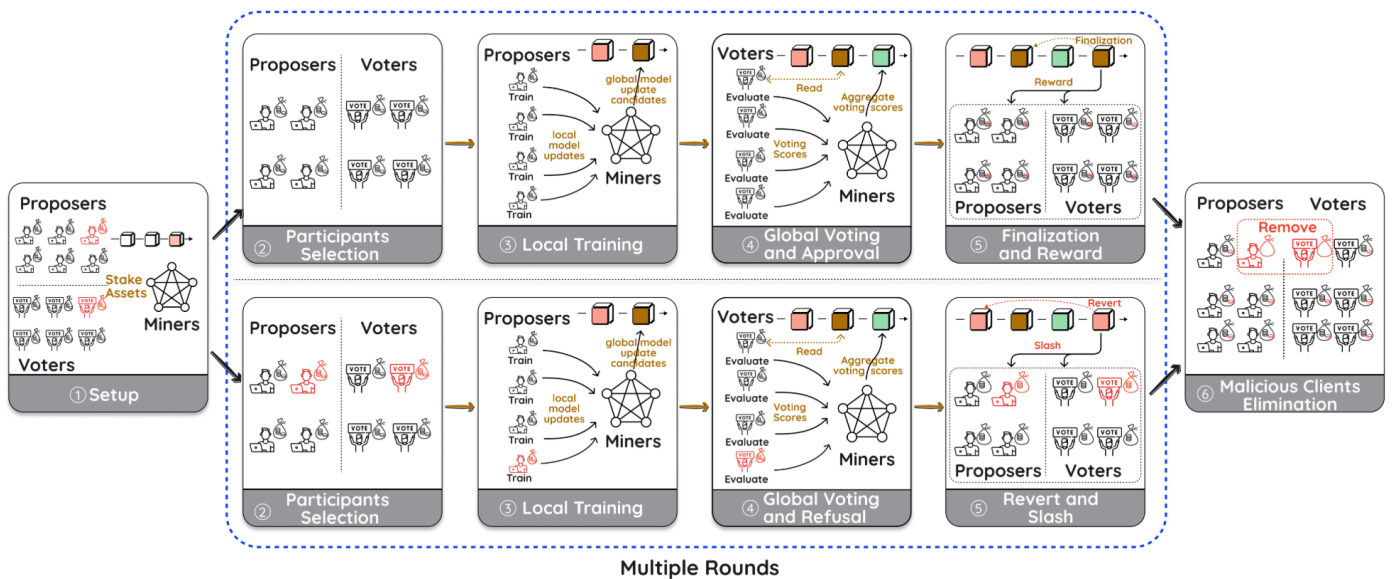


그림 5: FLock FL 태스크의 워크플로우 개요 (이전 연구¹⁰로부터 채택됨).

각 라운드마다 FL 클라이언트는 무작위로 제안자(proposer) 또는 투표자(voter)로 선택됩니다.

이들의 스테이킹 금액은 다수결 투표 결과에 따라 보상을 받을 수도, 슬래싱될 수도 있습니다.

악의적인 클라이언트는 궁극적으로 FL 시스템에서 제거됩니다.

- 생태계 내 각 AI Arena 태스크에 대해, 학습 노드를 위한 보상 메커니즘은 **Reward A**와 **Reward B**로 구성된 두 가지 독립적인 파트로 설계되어 있습니다.
 - **Reward A**는 일일 조건 기반 보상 체계로, 참가자가 AI Arena 태스크에 즉각적으로 몰입할 수 있도록 유도하는 보상입니다.
이러한 지속적인 보상 구조는 지속적인 피드백을 제공함으로써, 참가자의 참여를 장기적으로 유지하도록 만듭니다.
 - **Reward B**는 베스팅(vesting) 방식을 채택하여, 사전에 정의된 태스크 수명 내에서 성공적으로 완료되었을 경우에만 토큰이 지급됩니다.
이 보상 구조는 참가자가 태스크에 참여할 뿐 아니라, 정해진 기한 내에 효과적으로 완료하도록 유도합니다.
또한, 베스팅은 품질 관리 수단으로도 작용하여, 마감일에 맞춰 집중도 높은 기여를 장려합니다.
- AI Arena 태스크의 **Reward A**는 다음과 같습니다:

$$R_{i,A}^{AI} = \delta \cdot R_i^{AI}$$

- AI Arena 태스크의 **Reward B**는 다음과 같습니다:

$$R_{i,B}^{AI} = (1 - \delta) \cdot R_i^{AI}$$

여기서 δ 는 설정 가능한 시스템 파라미터입니다.

I. 예시 (Example)

태스크 1에 참여한 참가자들의 보상을 계산해 봅니다. 다음과 같은 조건을 가정합니다:

- 해당 날짜의 전체 AI Arena 태스크에 대한 일일 총 보상은 309,157.68 \$FLOCK입니다.
- 해당 태스크에는 학습 노드 2개와 검증자 3명이 참여합니다.
- 노드 A와 B는 각각 3,000 및 3,500 \$FLOCK을 스테이킹하였고, 검증자 A, B, C는 각각 3,000, 6,000, 3,000을 스테이킹하였습니다.
노드 A는 위임자로부터 추가로 1,000 \$FLOCK을 받아 총 스테이킹 금액 t_i 는 4,000이 됩니다.
- 계산 단순화를 위해 γ 는 0으로 가정합니다.
- σ 는 0.4, δ 는 0.1로 가정합니다.
- 노드 A, B, 검증자 A, B, C의 평가 점수는 각각 0.501435, 0.498565, 0.472768, 0.280226, 0.247006입니다.

우선, Day 1 기준 이 태스크에 대해 학습 노드 전체에 분배되는 보상은 다음과 같습니다:

$$309157.68 \times \frac{6500}{6500 + 12000} = 108623.7$$

다음으로 노드 A 및 해당 위임자에게 분배되는 보상을 계산합니다. $\alpha_t = 1$ 이라고 가정할 때, 노드 A (위임자 포함)의 보상은 다음과 같습니다:

$$\frac{0.501435 \times 4000}{(0.501435 \times 4000) + (0.498565 \times 3500)} \times 108623.7 = 58084$$

유사하게, 노드 B (위임자 포함)의 보상은 다음과 같습니다:

$$\frac{0.498565 \times 3500}{(0.501435 \times 4000) + (0.498565 \times 3500)} \times 108623.7 = 50539$$

\$\sigma = 0.4\$일 때, 노드 A가 실제로 수령하는 보상은:

$$58084 \times \left(0.4 + 0.6 \times \frac{3000}{4000} \right) = 49371$$

노드 B는 위임자가 없기 때문에 전체 보상(즉, 50,539)을 100% 수령합니다.

\$\delta = 0.1\$이므로, 학습 노드의 일일 보상 중 10%는 **Reward A**, 나머지 90%는 **Reward B**로 구분되며, Reward B는 태스크 종료 시까지 잠금됩니다.

따라서, Day 1 기준 노드 A의 Reward A는 4,937.1, Reward B는 44,433.9이며, 노드 B의 Reward A는 5,053.9, Reward B는 45,485.1입니다.

이제 검증자 보상을 계산해 봅시다. Day 1 기준 해당 태스크에 대해 전체 검증자에게 분배되는 보상은:

$$309157.68 \times \frac{12000}{6500 + 12000} = 200534.0$$

검증자 A의 점수가 0.472768이라고 가정하면, 검증자 A의 보상은 다음과 같습니다:

$$200534.0 \times 0.369 \times \left(0.4 + 0.6 \times \frac{3000}{3000 + 0} \right) = 73997$$

유사하게, Day 1 기준으로 검증자 B (점수 = 0.280226, 스테이킹 = 6000)는 87,834, 검증자 C (점수 = 0.247006, 스테이킹 = 3000)는 38,703의 보상을 수령합니다.

Node A에 1,000을 위임한 위임자 A의 보상은 다음과 같이 계산됩니다:

$$58084 \times \left(0.6 \times \frac{1000}{3000 + 1000} \right) = 8712.6$$

태스크 1에 대한 참가자별 5일간 보상 분포는 표 II에 제시됩니다.

AI Arena 태스크의 **Reward A**는 다음과 같이 정의됩니다:

$$R_{i,A}^{AI} = \delta \cdot R_i^{AI}$$

AI Arena 태스크의 **Reward B**는 다음과 같이 정의됩니다:

$$R_{i,B}^{AI} = (1 - \delta) \cdot R_i^{AI}$$

여기서 Δ 는 조정 가능한 시스템 파라미터입니다.

I. 예시 (Example)

태스크 1에 참여한 참가자들의 보상을 계산해 봅니다. 다음과 같은 조건을 가정합니다:

- 해당 날짜의 전체 AI Arena 태스크에 대한 일일 총 보상은 309,157.68 \$FLOCK입니다.
- 해당 태스크에는 학습 노드 2개와 검증자 3명이 참여합니다.
- 노드 A와 B는 각각 3,000 및 3,500 \$FLOCK을 스테이킹하였고, 검증자 A, B, C는 각각 3,000, 6,000, 3,000 \$FLOCK을 스테이킹하였습니다.
- 노드 A는 위임자로부터 1,000 \$FLOCK을 추가로 위임받아 $t_i = 4000$ 이 됩니다.
- $\gamma = 0$, $\sigma = 0.4$, $\Delta = 0.1$ 로 가정합니다.
- 점수: 노드 A = 0.501435, 노드 B = 0.498565, 검증자 A = 0.472768, 검증자 B = 0.280226, 검증자 C = 0.247006

학습 노드 보상 (Day 1):

노드의 총 스테이킹 = 3,000 + 3,500 = 6,500

검증자의 총 스테이킹 = 3,000 + 6,000 + 3,000 = 12,000

노드에 할당되는 보상 몫:

$$309157.68 \times \frac{6500}{6500 + 12000} = 108623.7$$

- 노드 A (위임자 포함):

$$\frac{0.501435 \times 4000}{0.501435 \times 4000 + 0.498565 \times 3500} \times 108623.7 = 58084$$

- 노드 A (자기 몫):

$$58084 \times \left(0.4 + 0.6 \times \frac{3000}{4000} \right) = 49371$$

- 위임자 A:

$$58084 \times \left(0.6 \times \frac{1000}{4000} \right) = 8712.6$$

- 노드 B:

$$\frac{0.498565 \times 3500}{0.501435 \times 4000 + 0.498565 \times 3500} \times 108623.7 = 50539$$

Reward A / B 분할 (Day 1):

- 노드 A: A = 4,937.1, B = 44,433.9
- 노드 B: A = 5,053.9, B = 45,485.1

검증자 보상 (Day 1):

검증자 몫:

$$309157.68 \times \frac{12000}{6500 + 12000} = 200534.0$$

- 검증자 A:

$$200534.0 \times 0.369 \times \left(0.4 + 0.6 \times \frac{3000}{3000} \right) = 73997$$

- 검증자 B: 87,834
- 검증자 C: 38,703

표 II: 최종 일일 보상 분배 (1일차~5일차)

일자	총 보상액	노드 A A	노드 A B	노드 B A	노드 B B	위임자 A	검증자 A	검증자 B	검증자 C
Day 1	309,157.68	4,937.1	44,433.9	5,053.9	45,485.1	8,712.6	73,997	87,834	38,703
Day 2	309,157.68	4,937.1	44,433.9	5,053.9	45,485.1	8,712.6	73,997	87,834	38,703
Day 3	309,157.68	4,937.1	44,433.9	5,053.9	45,485.1	8,712.6	73,997	87,834	38,703
Day 4	309,157.68	4,937.1	44,433.9	5,053.9	45,485.1	8,712.6	73,997	87,834	38,703
Day 5	309,157.68	4,937.1	44,433.9	5,053.9	45,485.1	8,712.6	73,997	87,834	38,703

표 II: 예시 — 1개의 태스크에 대한 5일간 보상 분배 내역. 참가자는 학습 노드 2개 (A, B), 위임자 A $(\sigma = 0.4)$, 검증자 3명 (A, B, C). 보상 구조는 $(\delta = 0.1)$, 즉 Reward A는 10%, Reward B는 90%.

VII. FLock 거버넌스

FLock 토큰 보유자는 DAO(탈중앙화 자율 조직)를 통해 시스템의 민주적 거버넌스에 참여할 수 있는 권한을 가집니다.

거버넌스 참여를 위해서는 일반적으로 토큰을 스마트 계약에 잠금(lock)해야 하며, 각 토큰은 1표의 투표권을 나타내어 사용자 보유 지분에 비례한 권한을 부여합니다.

사용자는 다음과 같은 다양한 개발 및 운영 측면에 대해 제안하고, 토론하고, 투표할 수 있습니다:

- 기술 업데이트
- 프로토콜 변경

- 재무/금고(treasury) 관리
- 커뮤니티 주도 프로젝트 및 이니셔티브

- **제안(Proposing):**

Flock 커뮤니티는 모든 토큰 보유자가 참여할 수 있는 제안 시스템을 통해 프로토콜의 미래를 적극적으로 설계합니다.

제안은 버그 수정, 알고리즘 최적화 등 기술적 이슈부터, 연구를 위한 금고 자금 배분, 교육 프로그램 개설 등

커뮤니티 전체에 영향을 미치는 사안에 이르기까지 다양합니다.

- **토론(Debating):**

제출된 제안은 이후 Flock 커뮤니티 내에서 자유롭게 토론되고 비판의 대상이 됩니다.

토큰 보유자는 포럼, 커뮤니티 토론, 개발자와의 직접 소통 등을 통해 제안의 타당성과 잠재적 영향력을 검토할 수 있습니다.

이와 같은 토론 과정은 투명성을 촉진하고, 다양한 관점에서 충분히 고려된 정보에 기반한 의사결정을 가능하게 합니다.

- **투표(Voting):**

제안이 충분히 논의된 후, 토큰 보유자들은 투표를 통해 제안의 채택 여부를 결정합니다.

이 투표 시스템은 공정한 대표성을 보장하기 위해 가중 투표(보유량에 비례한 투표력), 혹은 쿼드라틱 보팅(quadratic voting: 깊이 있는 참여를 유도하고 조작을 억제하는 방식)과 같은 메커니즘을 활용할 수 있습니다.

Flock의 거버넌스 모델은 플랫폼과 탈중앙화 AI 환경이 진화함에 따라 지속적인 적응이 가능함을 강조합니다:

- **정책 적응(Policy Adaptation):**

새로운 도전과 기회가 등장할 때, 토큰 보유자는 기존 정책을 수정하거나 완전히 새로운 정책을 도입하기 위해

투표 시스템을 사용할 수 있습니다. 이를 통해 Flock은 커뮤니티와 광범위한 AI 생태계의 변화하는 요구에 민감하게 대응할 수 있습니다.

- **기능 구현(Feature Implementation):**

새로운 기능 도입에 대한 제안이 제출되고 투표될 수 있으며, 이를 통해 Flock 플랫폼은 사용자 수요 및 피드백에 기반하여 성장하고 진화할 수 있습니다.

이는 혁신을 촉진하고 Flock을 탈중앙화 AI 개발의 최전선에 유지시킵니다.

- **위기 대응(Responding to Challenges):**

정책을 빠르게 조정하고 변화를 구현할 수 있는 능력은 Flock이 보안 취약점, 규제 변화, 시장 변동성 등

예기치 못한 도전에 효과적으로 대응할 수 있도록 합니다.

Flock과 탈중앙화 AI 생태계가 성숙함에 따라, 토큰 보유자들은 정책을 조정하고, 기능을 도입하며, 새로운 과제에 능동적으로 대응해 나갈 수 있습니다.

VIII. Flock 활용 사례 (Flock Applications)

Flock 시스템은 중앙집중형 AI 구축에도 활용될 수 있으며, 다음과 같은 사례들에서 그 적용 가능성이 입증되었습니다.

A. LLM을 위한 탈중앙화 AI

- **LLM 사전 학습 (Pre-training of LLMs):**

FLock은 탈중앙화 네트워크를 활용하여 LLM의 사전 학습을 가능하게 합니다.

참가자들은 컴퓨팅 자원과 다양한 데이터셋을 기여할 수 있으며, 이는 기존 중앙집중형 오픈소스 개발 방식으로는 접근하거나 활용할 수 없었던 독점적 데이터를 개방하는 효과를 가집니다.

다양한 데이터셋은 LLM의 다재다능함을 보장하며, 언어적·문화적 뉘앙스, 그리고 커뮤니티가 정의한 가치들이 더 넓게 반영된 모델을 구현할 수 있게 합니다.

- **LLM 미세 조정 (Fine-tuning of LLMs):**

미세 조정은 사전 학습된 모델을 특정 작업에 적합하도록 조정하거나 특정 유형의 데이터에서 정확도를 높이는 과정입니다.

FLock은 다음과 같은 방식으로 미세 조정을 지원합니다:

- *금융 거래를 위한 미세 조정:*

LLM은 암호화폐 거래를 위한 지능형 에이전트 역할을 하도록 미세 조정될 수 있습니다.

기능에는 송금, 스왑, 다양한 암호화폐 간 브리징 등이 포함됩니다.

FLock은 **Morpheus Network**, **Oxscope** 등의 플랫폼과의 협업을 통해 이러한 AI 모델을 호스팅하며,

커뮤니티가 안전하고 효율적으로 사용할 수 있도록 지원합니다.

- *AI 동반자(AI Companions)를 위한 미세 조정:*

AI 모델은 **Character.ai**와 같은 플랫폼의 사례처럼, 사용자와 더욱 개인화되고 몰입감 있는 방식으로 상호작용할 수 있도록 미세 조정될 수 있습니다.

FLock은 이러한 고도화된 AI 동반자를 호스팅함으로써, 보다 자연스럽게 맥락을 인식하는 사용자 경험을 제공합니다.

B. Stable Diffusion 모델을 위한 탈중앙화 AI

FLock 시스템은 텍스트-투-이미지 모델인 Stable Diffusion을 미세 조정하는 데에도 사용될 수 있습니다.

이 과정에서 핵심적인 구성요소는 **LoRA (Low-Rank Adaptation)**¹²이며, 이는 모델 아키텍처 내 일부 파라미터를 조정하여 대규모 재학습 없이도 특정 작업에 잘 적응할 수 있도록 합니다.

- **LoRA 미세 조정 (Fine-tuning LoRA):**

LoRA는 사전 학습된 모델에 대해 학습 가능한 저랭크 행렬을 도입함으로써, 효율적이고 경량화된 미세 조정을 가능하게 합니다.

이 기법은 적은 연산 비용과 제한된 수의 학습 파라미터로도 모델을 효과적으로 조정할 수 있게 합니다.

FLock이 Stable Diffusion 모델과 함께 LoRA를 적용하는 경우, 다음과 같은 이점이 있습니다:

- *커뮤니티 주도 개선:*

미세 조정 과정을 탈중앙화함으로써, FLock은 개별 사용자의 지식과 선호를 반영할 수 있는 참여를 확장합니다.

예술가, 디자이너 등 창작자들은 자신만의 스타일이나 기능을 반영하여 모델 출력 품질을 개선하고,

보다 다양한 문화적 맥락과 예술 표현에 부합하는 결과물을 이끌어낼 수 있습니다.

- **확장성 및 접근성:**

LoRA를 통한 미세 조정은 다수의 노드에 걸쳐 확장 가능하므로, 지속적이고 분산적인 개선이 용이합니다.

- **사용 사례 확장:**

Stable Diffusion 모델에 LoRA를 적용함으로써, 특정 산업이나 틈새 시장에 맞춤화할 수 있습니다.

예를 들어, 의학 교육용 삽화 생성, 부동산용 건축 시각화, 디지털 미디어를 위한 독창적인 아트 스타일 생성 등에 활용될 수 있습니다.

C. 선형 회귀 모델을 위한 탈중앙화 AI

선형 회귀 모델¹³은 변수 간 관계를 이해하기 위한 통계 분석 및 예측 모델링에서 널리 사용되는 기본 도구입니다.

FLock은 이러한 원리를 탈중앙화 환경에 적용하여, 당뇨병 관리와 같은 특정 의료 과제를 해결하고자 합니다.

당뇨병 관리는 혈당 수치, 식단, 운동, 약물 복용 순응도 등 다양한 입력 데이터를 기반으로 환자의 결과를 예측할 수 있는 선형 회귀 모델이 효과적으로 활용될 수 있는 중요한 분야입니다.

FL Alliance는 이러한 예측 모델을 탈중앙화된 데이터 소스를 통해 개발할 수 있도록 하며, 환자 데이터 보호를 철저히 준수하는 방식으로 운영됩니다.

- **데이터 보호 및 보안:**

FLock은 여러 의료 기관이 실제 데이터를 공유하지 않고도 모델 학습 과정에 협업할 수 있도록 지원합니다.

이 방식은 미국의 HIPAA와 같은 엄격한 건강 정보 보호 규제를 준수하는 데 필수적입니다.

참가자(예: 병원, 클리닉)는 자신들의 데이터를 로컬에서 보유한 채, 해당 데이터로 모델 업데이트를 계산합니다.

이렇게 생성된 업데이트만이 공유 모델 개선에 활용되며, 개별 환자 데이터는 외부에 노출되지 않습니다.

- **모델 정확도 및 신뢰도 향상:**

다양한 인구통계 및 지리적 배경에서 데이터를 통합함으로써, FLock은 보다 정확하고 일반화된 당뇨병 관리용

선형 회귀 모델 개발을 가능하게 합니다. 이는 환자 특성이 지역별로 크게 상이할 수 있는 의료 분야에서 특히 중요합니다.

- **협업 기반 혁신:**

서로 다른 의료 기관이 공동의 목표를 향해 협력함으로써, 당뇨병 관리 및 치료 전략에 대한 새로운 통찰을 이끌어내고, 혁신을 가속화할 수 있습니다.

IX. 결론 (Conclusion)

FLock은 AI Arena, FL Alliance, AI Marketplace를 통해 탈중앙화 AI 구축을 위한 솔루션을 제공합니다.

FLock은 AI 시스템 참여를 가로막는 장벽을 제거하며, 개발자들이 모델, 데이터, 또는 컴퓨팅 자원을 유연하고 모듈화된 방식으로 기여할 수 있도록 합니다.

FLock은 각 커뮤니티가 직접 만들고, 직접 사용할 수 있는 AI 모델을 정교하게 설계함으로써, 다양한 목적 지향형 모델 생성을 촉진합니다.

1. Reference 1 ↩ ↩ ↩

2. Reference 2 ↩ ↩

3. Reference 3 ↩ ↩

4. Reference 4 ↩ ↩

5. Reference 5 ↩

6. Reference 6 ↩

7. Reference 7 ↩

8. Reference 8 ↩

9. Reference 13 ↩

10. Reference 14 ↩ ↩

11. Reference 15 ↩

12. Reference 19 ↩

13. Reference 20 ↩