

엘프(aelf)

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.

내일의 AI+블록체인 경험하기

백서 2.0

요약문(Executive Summary)

엘프(aelf)는 2017년 12월에 출시된 첨단 멀티체인 블록체인 프레임워크로, C# 언어 기반으로 구축되었다. 메인체인(MainChain)과 디앱체인(dAppChain)으로 구성된 다층 구조를 통해 기존 블록체인 시스템이 겪는 성능 병목 현상과 데이터 복잡성 문제를 효과적으로 해결한다. 이 아키텍처는 여러 체인에 작업을 분산시켜 확장성을 높이고 네트워크 혼잡을 완화한다. 개발자 맞춤화와 병렬 처리(parallel processing)에 중점을 둔 aelf의 프레임워크는 디지털 자산 관리부터 디파이(DeFi)에 이르기까지 폭넓은 응용을 지원하는 다재다능한 구조를 갖추고 있다. aelf의 초기 기술 아키텍처에 대해서는 백서 v1.0을 참조하면 된다.

aelf 백서 2.0의 목표는 인공지능(AI)을 활용하여 운영 효율성을 극대화하는 것이다. AI 기반 머신러닝 모델은 스마트 컨트랙트 실행 효율과 가스 사용량을 최적화하고, 네트워크 혼잡을 예측하며, 자원을 동적으로 조정하여 높은 성능을 유지한다. 또한 AI는 지능형 부하 분산(load balancing)과 예측적 확장(predictive scaling)을 가능하게 하여, 네트워크 전반에서 효율적인 트래픽 분배와 자원 활용을 실현한다. aelf의 AI 오라클(AI Oracle)은 온체인 스마트 컨트랙트에 AI 기능을 결합한 신뢰성 높은 Web3 AI 프레임워크 구현을 목표로 하며, AI 중심의 탈중앙화 애플리케이션(AI-dApp) 생태계 형성을 촉진한다.

개발자를 위해 aelf는 자연어 처리(NLP)를 통해 스마트 컨트랙트 작성 과정을 단순화하고, AI 기반 챗봇을 통해 실시간 지원을 제공하는 AI 강화 개발 환경을 제공한다. 이러한 도구들은 비전문 사용자가 블록체인 기술에 쉽게 접근할 수 있도록 하고, 숙련된 개발자에게는 개발 과정을 더욱 효율적으로 만들어준다. aelf의 AI 기반 스마트 컨트랙트 감사를 통해 스마트 컨트랙트 코드는 사전 학습된 모델에 입력되어 문법과 논리 구조를 분석하며, 보안 취약점과 오류를 식별하고, 배포 전에 수정 제안이 포함된 상세 감사 보고서를 aelf 개발자에게 제공한다. AI의 도입으로 aelf는 사용자 경험을 개선할 뿐 아니라 이용자 저변을 확대하고, 블록체인 산업

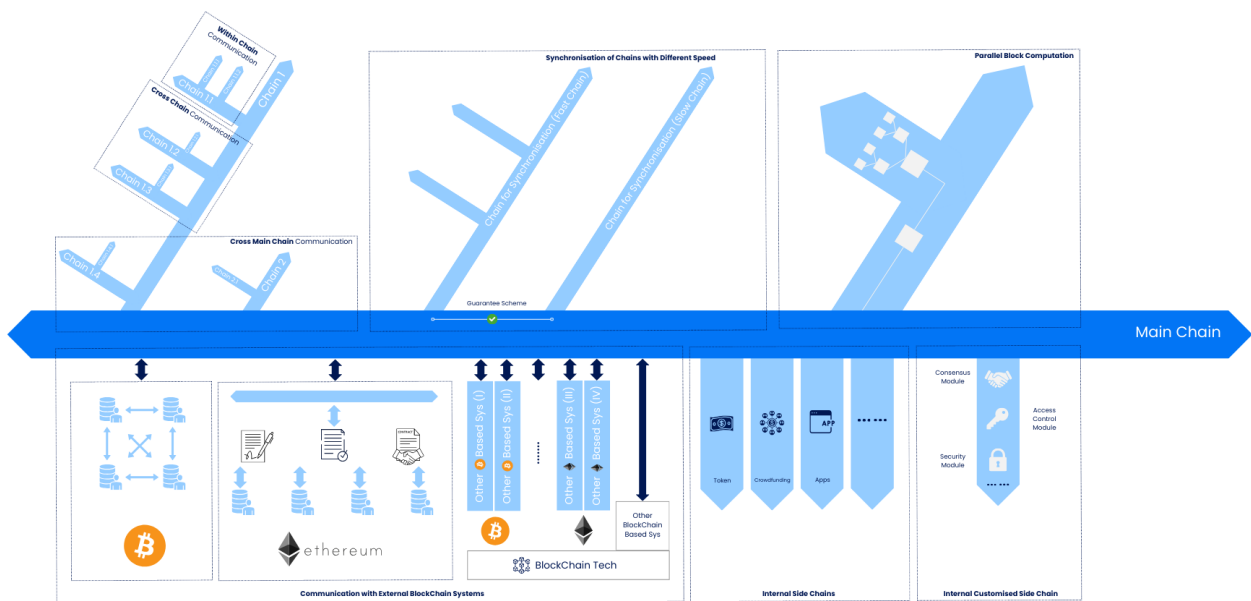
내 도입과 혁신을 촉진한다.

AI를 넘어, aelf는 성능, 확장성, 그리고 EVM 호환성을 대폭 향상시키는 새로운 모듈형 블록체인 기술을 도입할 예정이다. 이러한 접근 방식은 가스 저장 비용을 줄이고 사용자 거래 비용을 낮추며, 궁극적으로는 개인 정보 보호와 사용자 경험을 향상시킨다.

결국 aelf는 다층 아키텍처, AI 통합, 모듈형 구조를 통해 효율성과 확장성을 높인 다재다능한 멀티체인 블록체인 프레임워크로서, 높은 효율성과 보안성, 그리고 개발자 친화성을 함께 갖춘 플랫폼이다.

aelf의 배경(Background on aelf)

aelf의 이야기는 2017년 12월 10일, Coindesk 컨퍼런스에서 aelf의 비전과 계획이 전 세계 투자자들에게 처음 공개되면서 시작되었다. aelf는 [Binance](#), [Arrington Capital](#), [Draper Dragon](#), [Galaxy Digital](#) 등 유수 기관으로부터 투자를 유치하며, 예정된 일정보다 훨씬 앞서 자금 조달을 성공적으로 완료했다. 같은 달, ELF 토큰은 [Binance](#)와 [OKEX](#)를 포함한 6개의 주요 거래소에 상장되었다. 이후 2018년에는 aelf 테스트넷(Testnet)이, 2020년에는 메인넷(Mainnet)이 차례로 성공적으로 출시되었다.



aelf는 본질적으로 멀티체인 병렬 컴퓨팅 블록체인 프레임워크로, 기존 블록체인 시스템이 지닌 성능 병목 현상과 데이터 복잡성 등의 한계를 해결하기 위해 설계되었다. aelf의 비전은 최신 IT 설계 원칙을 통합하여 개발자가 자신의 필요에 맞게 체인을 자유롭게 맞춤화할 수 있는, 블록체인 분야의 “리눅스 생태계(Linux Ecosystem)”가 되는 것이다.

aelf의 핵심은 다음과 같은 주요 기능으로 구성된다.

1. 다양한 사용자 중심 시나리오를 처리하기 위한 메인체인(MainChain)과 다계층 디앱체인(dAppChain) 구조. 각 체인은 하나의 사용 사례에 맞게 설계되어 있으며, 여러 체인에 작업을 분산

시켜 처리 효율을 높인다.

2. 비트코인(Bitcoin)과 이더리움(Ethereum) 등 외부 블록체인 네트워크와 교차 체인 메시징 프로토콜(cross-chain messaging protocol)을 통해 상호 통신 가능.
3. 클라우드 기반 환경에서 경쟁되지 않는(non-competing) 트랜잭션의 병렬 처리(parallel processing) 지원.
4. 각 체인별로 최소 실행 블록(Minimum Viable Block)과 제네시스 스마트 컨트랙트 컬렉션(Genesis Smart Contract Collection)을 제공하여 데이터 복잡성을 줄이는 동시에 높은 수준의 맞춤화를 실현.
5. 이해관계자가 합의 프로토콜(Consensus Protocol)을 포함한 프로토콜 수정안을 승인할 수 있는 권한과, 디앱체인이 합의 프로토콜에 따라 메인체인에 동적으로 참여하거나 탈퇴할 수 있는 권한 제공.

aelf의 가장 큰 강점은 메인체인과 여러 디앱체인으로 구성된 다층 아키텍처에 있다. 이는 기존의 단일 체인(Single Chain) 시스템과 달리, 메인체인이 시스템의 중심축(backbone) 역할을 하며 여러 디앱체인과 연결되는 “분기형 생태계(Branched Ecosystem)” 구조를 채택한다. 기존의 “하나의 체인으로 모든 종류의 컨트랙트를 처리”하는 방식과 달리, aelf의 “하나의 체인에 하나의 컨트랙트 유형” 설계는 작업을 효율적으로 분산시키고 트랜잭션을 병렬 처리할 수 있게 하여, 확장성을 대폭 향상시키고 네트워크 혼잡을 줄인다. 동시에 디앱체인은 관리가 용이하며 특정 응용에 맞게 최적화할 수 있어, 성능 저하 없이 다양한 사용 사례를 지원할 수 있다.

aelf의 합의 메커니즘(consensus mechanism)은 위임지분증명(Delegated Proof of Stake, DPoS)을 채택하여 네트워크 전반의 효율성을 관리한다. DPoS는 작업증명(PoW) 등 다른 합의 메커니즘에 비해 속도와 에너지 효율성이 뛰어난 것으로 알려져 있다. 토큰 보유자가 거래 검증과 네트워크 유지를 담당할 대표자(delegate)를 투표로 선출함으로써, aelf는 높은 수준의 보안성과 탈중앙화를 유지하면서도 빠른 거래 속도를 달성한다. 또한 aelf의 동적 인덱싱(dynamic indexing)과 포괄적인 토큰 시스템은 디지털 자산 관리부터 디파이(DeFi) 플랫폼에 이르기까지 다양한 응용을 안정적으로 지원하며, 모든 유형의 개발자에게 유연하고 강력한 블록체인 솔루션을 제공한다.

마지막으로, C# 프로그래밍 언어는 aelf 블록체인의 기술적 기반을 형성하는 핵심 요소이다. C#은 강력한 형식 검사(type-checking)를 지원하는 견고한 객체 지향 언어로, 코드의 신뢰성을 높이고 런타임 오류를 최소화하는 데 중요한 역할을 한다. 또한 효율적인 메모리 관리와 높은 실행 속도 등 성능 특성이 블록체인의 까다로운 요구 사항을 충족한다. 더불어 C#의 비동기 프로그래밍(asynchronous programming) 및 병렬 처리 기능은 블록체인 노드의 성능을 최적화하여, 지연 없이 다수의 트랜잭션을 동시에 처리할 수 있도록 한다. 이러한 견고한 기술적 기반은 aelf가 대규모 트랜잭션과 복잡한 연산을 안정적으로 처리할 수 있는 역량을 뒷받침한다.

aelf의 초기 설계와 아키텍처에 대한 자세한 내용은 원본 백서 1.0을 참고하기 바란다.

진화하는 블록체인 환경(The evolving blockchain landscape)

블록체인 산업은 빠르게 진화하고 있으며, 2024년에는 여러 주요 흐름이 산업 전반을 형성하고 있다. 디파이(DeFi)는 여전히 선두에 있으며, 중개자를 제거하고 직접적이며 신뢰 불필요(trustless)한 거래를 가능하게 한다는 점에서 특징적이다. 여기에 AI 기반 리스크 관리 시스템이 통합되면서, 자동화된 자금세탁방지(AML) 및 고객확인(KYC) 절차를 통해 보안성과 규제 준수 수준을 높이고 있다. 또한, 크로스체인 상호운용성(cross-chain interoperability)의 중요성이 점점 커지고 있으며, 이를 통해 서로 다른 블록체인 네트워크 간에 자산 이전과 트랜잭션을 원활히 수행할 수 있게 되었다. 예를 들어, [체인링크\(Chainlink\)](#)의 CCIP(Cross-Chain Interoperability Protocol)은 크로스체인 유동성 풀(liquidity pool)과 상호운용 가능한 디파이 프로토콜을 지원하여, 이더리움(Ethereum)의 높은 유동성과 레이어2(Layer 2) 솔루션의 낮은 거래 수수료를 동시에 활용할 수 있게 한다. 이러한 상호운용성은 단일 블록체인의 한계를 넘어 디파이 서비스를 확장하고, 다양한 프로토콜 전반에서 유동성을 강화하며 사용자 수익률을 최적화하는 데 필수적이다.

NFT(대체불가능토큰) 역시 꾸준히 성장세를 이어가고 있으며, 주요 브랜드들의 도입과 함께 게임 및 부동산 등 다양한 산업 분야로 통합되고 있다. NFT를 활용한 실물자산의 토큰화(real-world asset tokenisation, RWA)는 물리적 자산을 디지털 형태로 표현함으로써 투자자에게 새로운 기회를 제공하고, 전통적으로 유동성이 낮았던 시장에서 새로운 유동성을 창출한다. 예를 들어, [Ondo Finance](#)는 토큰화된 미 재무부 채권 시장(tokenised treasury market)의 주요 플레이어로, 기관급 금융 상품을 암호화폐 생태계로 도입하고 있다. 이들은 미 재무부 단기채(Treasury Bills)를 토큰화하여 USDY 스테이블코인(stablecoin)을 통해 안정적인 수익을 제공한다. 이러한 흐름은 가치 있는 자산에 대한 접근성을 민주화하고, 글로벌 시장 참여를 촉진할 것으로 기대된다.

또한, 확장성과 지속 가능성을 동시에 달성하려는 수요가 증가함에 따라, 에너지 효율적인 합의 메커니즘(consensus mechanism)인 지분증명(PoS) 방식이 빠르게 채택되고 있다. 이는 글로벌 차원의 지속 가능성 이니셔티브와도 맞닿아 있다. 이더리움의 [Ethereum 2.0](#) 업그레이드는 샤드 체인(shard chain) 도입과 작업증명(PoW)에서 지분증명(PoS)으로의 전환을 통해 확장성을 크게 향상시키는 것을 목표로 한다. 샤딩(sharding)은 이더리움 네트워크를 더 작고 관리하기 쉬운 여러 조각으로 분할하여 병렬로 트랜잭션을 처리할 수 있게 하며, 이를 통해 전체 처리량을 대폭 증가시킨다. 이러한 혁신적 접근 방식은 블록체인 기술의 확장성 문제를 해결하고, 성능이나 보안을 저해하지 않으면서 증가하는 수요를 충족할 수 있도록 한다.

이처럼 블록체인 기술이 지속적으로 발전하고 성숙함에 따라, 다양한 활용 사례를 통해 투명성, 보안성, 그리고 효율성을 강화하며, 일상과 가까운 여러 산업 분야에서 그 잠재력이 더욱 부각되고 있다.

AI 혁명과 블록체인에 미치는 영향(The AI revolution and its impact on blockchain)

AI의 영향력은 때로는 미묘하지만, 그 변화의 폭은 깊고 근본적이다. AI는 우리의 일상과 업무 방식을 혁신적으로 재편하고 있다. 의료 분야에서는 의사들이 AI를 활용해 [진단 정확도](#)를 높이고, 맞춤형 치료 계획을 수립함으로써 환자 치료 품질을 개선하고 회복 속도를 높이고 있다. 또한 AI는 방대한 데이터를 분석하여 잠재적 신약 후보를 발굴함으로써, 전통적으로 많은 시간과 자원이 소요되던 [신약 개발 과정](#)을 획기적으로 단축하고 있다. 금융 부문에서도 금융기관들은 AI를 활용해 비정상적인 패턴을 탐지함으로써 인간이 놓칠 수 있는 [사기 행위](#)를 조기에 발견하고, 보안 수준을 강화하고 있다. 개인 금융 영역에서도 AI는 개인의 금융 행동을

분석해 맞춤형 금융 조언을 제공함으로써 자산 관리의 효율성을 높이고 있다. 즉, 로보어드바이저(Robo-advisor)와 같은 기술이 그 대표적인 사례다.

특히 블록체인 분야에서 AI는 보안성과 효율성을 동시에 강화할 수 있는 혁신적인 해결책을 제시한다. AI는 보안 침해를 사전에 예측하고 방지할 수 있으며, 트랜잭션 검증 과정을 최적화하고 온체인 활동에 대한 심층적 통찰을 제공한다. 스마트 컨트랙트 개발에서도 AI는 코드 생성, 최적화, 버그 탐지 등을 지원하여 개발 효율성을 높인다. 또한 AI는 트랜잭션 라우팅(transaction routing)과 네트워크 혼잡 예측을 최적화함으로써 블록체인의 확장성과 성능을 향상시켜, 트랜잭션을 더 빠르고 오류 없이 처리할 수 있도록 한다. 이를 통해 블록체인 기술은 실생활에서도 더욱 실용적인 형태로 발전하고 있다.

한편, 블록체인의 탈중앙화 인프라는 AI 개발의 새로운 가능성을 열고 있다. 블록체인은 AI 모델을 투명하고 불변의 형태로 저장하고 공유할 수 있는 플랫폼을 제공함으로써, 모델의 무결성을 보장하고 협업형 개발을 촉진한다. 스마트 컨트랙트 기반의 SingularityNet과 같은 탈중앙화 AI 마켓플레이스 개념은, 신뢰할 필요 없는 환경(trustless environment)에서 AI 서비스의 구매, 판매, 실행을 가능하게 한다. 또한 블록체인의 네이티브 암호화폐를 활용하여 AI 학습에 대한 인센티브를 제공함으로써, 고급 AI 역량에 대한 접근성을 민주화할 가능성도 있다. 블록체인 애플리케이션의 사용자 경험 측면에서도 AI는 디파이(DeFi) 플랫폼에서 개인화된 투자 추천을 제공하거나, 디지털 신원 관리(digital identity management)를 지원하여 데이터 보안을 유지하면서 사용자 접근성을 간소화할 수 있다.

AI와 블록체인 간의 시너지가 점차 확대됨에 따라, aelf는 이 두 기술의 융합을 통한 혁신을 적극적으로 수용하고 있다. 우리는 블록체인 기술이 일상 속으로 더 널리 확산되기를 기대하며, 이러한 협업이 보안성, 확장성, 그리고 사용자 경험 측면에서 Web3 생태계 전반에 실질적인 가치를 제공할 것이라 확신한다.

aelf의 AI 강화 아키텍처(aelf's AI-enhanced architecture)

앞서 언급했듯이, aelf의 기본 아키텍처는 근본적으로 C# 언어로 작성되어 있다. C#은 .NET 생태계와의 긴밀한 연계성을 통해 블록체인 개발에서 AI 통합을 위한 강력한 기반을 제공한다. .NET은 머신러닝 알고리즘, 자연어 처리(NLP), 데이터 분석 등을 포함한 고급 AI 모델 개발을 지원하는 다양한 라이브러리와 도구를 제공하며, 이는 블록체인 플랫폼의 기능성과 지능을 강화하는 데 핵심적인 역할을 한다. C#의 강력한 형식 시스템(strong typing)과 객체 지향(object-oriented) 구조는 코드의 안정성과 유지보수성을 보장하여, 보안에 영향을 미칠 수 있는 오류 발생 가능성을 최소화한다. 또한 Google Cloud의 AI 솔루션과 같은 클라우드 컴퓨팅 플랫폼 및 머신러닝 서비스와의 매끄러운 통합을 통해, aelf 개발자는 자동화된 스마트 컨트랙트 실행, 사기 탐지(fraud detection), 고급 암호화 기술을 통한 데이터 프라이버시 강화 등 다양한 AI 기능을 aelf 블록체인 내에 손쉽게 구현할 수 있다.

C#과 .NET의 광범위한 라이브러리를 활용함으로써, aelf 개발자는 네트워크 혼잡을 예측하고 합의 프로세스를 동적으로 조정하여 높은 성능을 유지하는 AI 모델을 통합할 수 있다. 이를 통해 효율적인 네트워크 관리가 가능해질 뿐 아니라, 트랜잭션 지연(latency)과 비용을 줄여 사용자 경험 또한 향상된다.

또한 aelf 위에서 개발을 진행하려는 개발자는 다양한 전문 개발 도구의 폭넓은 지원을 활용해 여러 AI 기능을 구현할 수 있으며, 이를 통해 개발 과정이 더욱 간소화되고, 금융 디앱(dApp)이나 탈중앙화 마켓플레이스(decentralised marketplace)와 같은 AI 기반 블록체인 솔루션의 신속한 프로토타이핑과 배포가 가능해진다.

종합적으로, C#은 .NET 생태계의 강점을 기반으로 한 폭넓은 라이브러리, 최고 수준의 클라우드 AI 서비스와의 원활한 통합, 그리고 강력한 개발 도구를 통해 aelf와 같은 블록체인 플랫폼에서 AI 통합을 위한 견고한 기반을 제공한다. 이러한 기술적 조합은 안전하고 확장 가능하며, 지능적인 블록체인 애플리케이션을 구현하는 데 핵심적인 역할을 한다.

aelf 생태계 내 AI 통합 지점(AI integration points in the aelf ecosystem)

AI의 통합은 aelf 생태계의 운영 역량을 한층 진화시킨 중대한 전환점으로, 성능과 보안을 최적화할 뿐만 아니라, 전반적인 사용자 및 개발자 경험을 크게 향상시켜 대규모 Web2 사용자의 Web3 전환을 촉진하는 핵심 역할을 한다.

aelf 생태계 내 AI 통합은 크게 두 가지 주요 영역으로 구분할 수 있으며, 각각의 영역은 다음과 같다.

1. 운영 우수성(Operational Excellence)
2. 개발자 및 사용자 경험(Developer and user experience)

운영 우수성(Operational Excellence)

i) 스마트 컨트랙트 최적화를 위한 머신러닝 모델(Machine Learning Models for Smart Contract Optimisation)

머신러닝 모델을 aelf 블록체인에 통합함으로써 가스 사용량과 실행 효율성을 획기적으로 최적화할 수 있다. aelf는 기존 롤업(Rollup) 기술에서 영감을 얻되, 이를 고도화된 예측 모델링(predictive modelling)을 통해 한 단계 발전시켰다.

가스 사용 최적화(Optimising Gas Usage)

머신러닝 모델은 스마트 컨트랙트 실행의 과거 데이터를 분석하여 패턴을 식별하고, 향후 트랜잭션에 대한 최적의 가스 가격을 예측할 수 있다. 이러한 접근 방식은 금융 시장에서 자산 가격과 거래량을 예측하기 위해 사용되는 예측 모델과 유사하며, aelf 네트워크에서의 트랜잭션을 비용 효율적이면서도 신속하게 수행하도록 돕는다.

또한 머신러닝 모델은 스마트 컨트랙트 코드 내에서 과도한 가스를 소모하는 비효율적인 패턴을 탐지하고 최소화하는 데에도 활용될 수 있다. aelf는 머신러닝 알고리즘을 활용해 불필요하게 많은 가스를 사용하는 비효율적인 코드 패턴을 분석하고 식별하는 도구를 적용하고 있다. 예를 들어, 반복(iteration)이 필요하지 않은 경우 배열(array) 대신 매핑(mapping)을 사용하는 것은 가스 비용을 상당히 절감할 수 있는데, 이는 매핑이 일반적으로 배열보다 가스 소모량이 적기 때문이다. 이러한 패턴을 지속적으로 모니터링하고 최적화함으로써, aelf는 스마트 컨트랙트가 최소한의 가스 비용으로 실행되도록 보장할 수 있다. 이는 [이더리움 네트워크](#)

크에서 개발자들이 사용하는 AI 기반 최적화 기법과 유사한 접근이다.

더 나아가, 머신러닝은 예측된 연산 요구량에 따라 자원 할당(resource allocation)을 동적으로 조정함으로써 스마트 컨트랙트의 실행 효율을 최적화할 수 있다. 예를 들어, 변수를 더 적은 스토리지 슬롯에 배치하여 저장 공간을 효율화하는 변수 패킹(variable packing) 기술은 머신러닝 알고리즘에 의해 자동으로 식별되고 적용될 수 있다. 이를 통해 필요한 스토리지 연산 횟수가 줄어들고, 결과적으로 가스 소비가 감소한다. 또한 온체인(on-chain)과 오프체인(off-chain) 데이터 저장 간의 최적 분배를 머신러닝으로 관리함으로써, 메모리 및 스토리지 활용을 극대화하고 전반적인 가스 효율을 향상시킬 수 있다.

실행 효율성 향상(Enhancing Execution Efficiency)

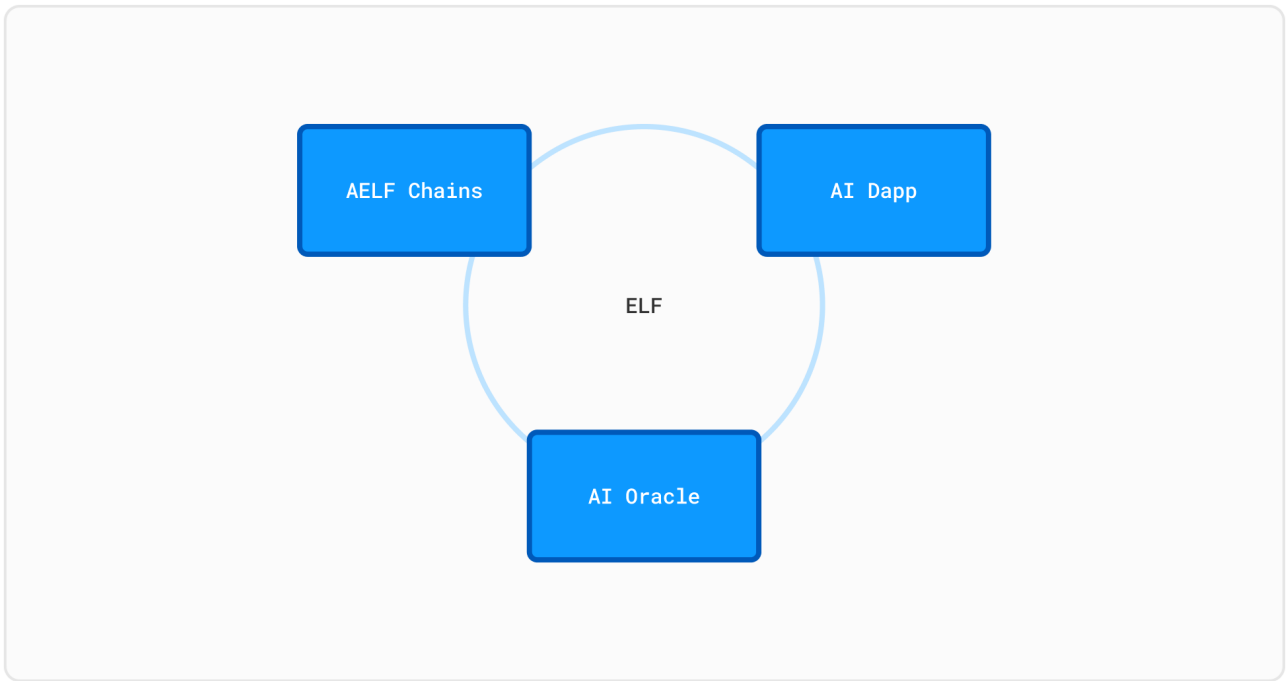
가스 최적화뿐만 아니라, AI는 aelf에서 스마트 컨트랙트의 실행 효율성 또한 향상시킬 수 있다. 예측 모델링을 활용하면 AI는 복잡한 스마트 컨트랙트의 자원 요구량과 실행 경로를 미리 예측할 수 있다. 이러한 예측 기능은 시스템이 연산 자원을 보다 효과적으로 배분하도록 하여, 불필요한 지연 없이 원활한 컨트랙트 실행을 가능하게 한다.

이 개념은 Google Cloud의 AI가 클라우드 서비스에서 자원 할당을 최적화하는 방식에서도 확인할 수 있다. Google Cloud는 머신러닝 모델을 활용해 수요를 예측하고, 사용자 요청에 맞춰 자원을 동적으로 조정함으로써 효율성을 극대화한다. aelf에서도 이와 유사하게, AI가 트랜잭션 볼륨을 예측하고 연산 자원을 실시간으로 조정함으로써 네트워크의 안정적인 성능을 유지한다. 예를 들어, 디파이(DeFi) 트랜잭션 급증 시기에 AI 모델은 거래량 증가를 미리 감지하고, 네트워크 지연 없이 이를 처리할 수 있도록 추가 연산 자원을 사전에 배분한다.

예측 모델은 서로 다른 스마트 컨트랙트의 실행 패턴을 평가하여, 실행 시간과 자원 소비를 줄일 수 있는 코드 최적화 방안을 제시할 수도 있다. 이는 컴파일러 설계(compiler design)에서 코드 성능을 개선하기 위해 수행되는 분석 및 재구조화 기법과 유사하다. 실제 사례로, 이더리움 재단(Ethereum Foundation)은 AI를 활용해 스마트 컨트랙트 바이트코드(bytecode)를 분석하고, 비효율적인 반복문이나 중복 계산을 탐지하여 실행 시간을 단축하고 가스 사용을 줄이는 최적화 방안을 제안해왔다. aelf 또한 이와 유사한 기술을 적용함으로써 스마트 컨트랙트의 전반적인 실행 효율을 크게 높일 수 있다.

ii) aelf의 AI 오라클(AI Oracle on aelf)

aelf의 AI 오라클(AI Oracle)은 Web3의 AI 계층(AI layer)으로 자리매김하고 있으며, 오라클 기술과 보안 연산(security compute) 기술을 결합하여 AI 기반 디앱(dApp)의 개발을 지원한다. 이는 aelf의 핵심 아키텍처 내에서 중요한 역할을 담당하며, aelf 체인, AI 오라클 네트워크, AI 애플리케이션으로 구성된 구조 속에서 AI 기능을 블록체인에 통합하는 연결 허브(bridge and hub)로 작동한다.



온체인 AI(On-chain AI)

현재 AI 오라클 분야는 주로 연산 및 추론 과정의 무결성을 보장하기 위해 영지식증명(ZKP, Zero-Knowledge Proofs)을 각 계산 단계에 통합하는 방식(예: ORA)에 초점을 맞추고 있다. 이러한 접근 방식은 추론 과정이 인간의 개입이 아닌 대형 언어 모델(LLM, Large Language Model) 자체로부터 도출되었음을 보장한다. 그러나 단순히 AI 추론 과정의 무결성만 보장하는 것으로는 충분하지 않으며, 상위 계층의 AI 에이전트(AI Agent) 애플리케이션 또한 변조 불가능해야 한다는 점이 중요하다.

또한 ChatGPT와 같은 대형 모델이나 IO와 같은 탈중앙화 컴퓨팅 네트워크는 고유한 연산 및 운영 메커니즘을 가지고 있어 ZKP 프로세스를 직접 내장하기가 현실적으로 어렵다. 따라서 aelf는 AI 추론 과정 자체보다, 대형 모델이 호출하는 API 및 상위 AI 에이전트 애플리케이션의 무결성을 보장하는 것이 더 중요하고 실질적 가치가 있다고 판단한다.

aelf에서의 구현(Implementation on aelf)

aelf는 다음과 같은 메커니즘을 통해 AI 오라클 네트워크를 구현한다.

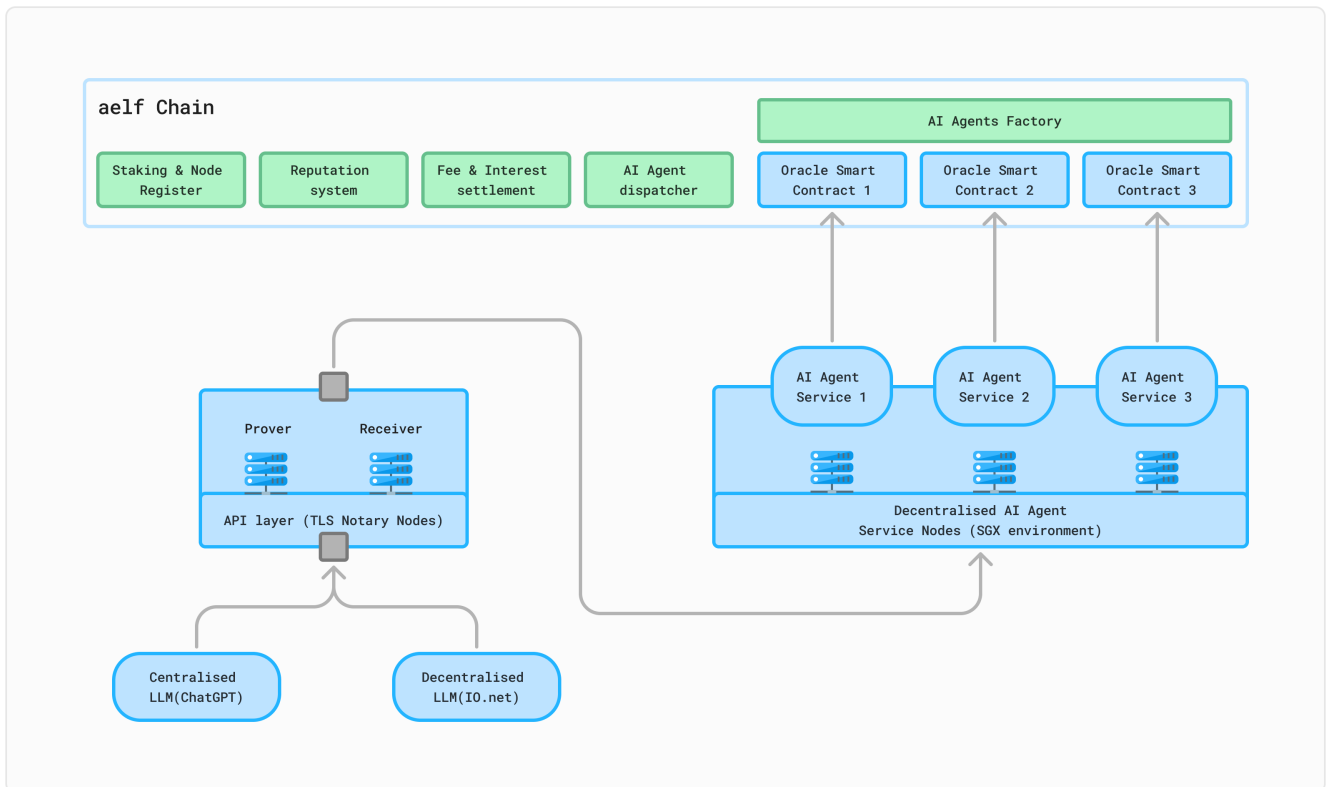
1. **TLSNotary 메커니즘**: 중앙화 또는 탈중앙화된 LLM이 제공하는 API가 데이터 소스에서 로컬 엔드포인트까지 변조되지 않았음을 보장한다.
2. **SGX 및 탈중앙화 컴퓨팅 네트워크**: AI 에이전트의 신뢰할 수 있는 실행 환경을 보장한다.

aelf 오라클 아키텍처는 크게 **1) 온체인(on-chain)** 과 **2) 오프체인(off-chain)** 두 구성 요소로 나뉜다.

1. 온체인 구성요소(On-Chain Components)

온체인 구성요소(현재는 aelf 체인에 구축되어 있으며, 향후 이더리움(Ethereum) 등 다른 체인으로 확장 가능)는 노드 예치 관리(Node Pledge Management), 평판 시스템(Reputation System), 수수료 및 정산 관리(Cost and Revenue Settlement), AI 에이전트 스케줄러(AI Agent Scheduler), AI 에이전트 팩토리(AI Agent Factory)로 구성된다. 이들은 AI 오라클의 기본 프레임워크 컨트랙트를 구성하며, 오프체인 노드들과 결합되어 aelf 오라클 네트워크를 완성한다. 특히, 개발자가 정의한 AI 오라클 컨트랙트는 사용자가 지정한 로직에 따라 AI 에이전트 팩토리 컨트랙트가 자동으로 생성한다.

1. **노드 예치 관리(Node Pledge Management)**: AI 에이전트 서비스 노드를 관리하며, 네트워크에 참여하려는 모든 노드는 일정량의 ELF를 예치해야 한다.
2. **평판 시스템(Reputation System)**: 위원회의 평가와 연동되어 노드의 운영 상태를 평가하며, 오프라인 노드의 등급을 강등하는 등의 역할을 수행한다.
3. **비용 및 수익 정산(Cost and Revenue Settlement)**: AI 에이전트 스케줄러와 연동되어, 노드의 수익 정산 및 디앱 호출 수수료 청구를 담당한다.
4. **AI 에이전트 스케줄러(AI Agent Scheduler)**: 네트워크의 컴퓨팅 부하 상태에 따라 AI 에이전트 서비스 코드를 배포하고 스케줄링한다.
5. **AI 에이전트 팩토리(AI Agent Factory)**: 사용자 정의 AI 에이전트 로직에 따라 맞춤형 컨트랙트를 생성한다. 이는 기본 프레임워크 컨트랙트와 사용자 정의 컨트랙트 간의 중개자 역할을 수행하며, 디앱 호출 인터페이스를 전달하고 수수료 정산 컨트랙트와 상호작용한다. 또한 AI 에이전트 서비스와 사용자 정의 컨트랙트 간의 모든 호출 및 추론 결과를 통합적으로 처리한다.



2. 오프체인 구성요소(Off-Chain Components)

오프체인 구성요소는 TLS 노터리 노드(TLS Notary Nodes)와 SGX 환경에서 실행되는 탈중앙화 AI 에이전트 서비스 노드(Decentralised AI Agent Service Nodes)로 이루어진다.

TLS 노터리 노드(TLS Notary Nodes)

TLS Notary는 신뢰할 수 없는 참가자 간의 네트워크 통신 무결성과 보안을 보장하기 위한 인증 메커니즘이다. 이는 클라이언트와 서버 간 통신을 암호화하는 TLS(Transport Layer Security) 프로토콜을 기반으로 하며, “노터리(Notary)”는 해당 TLS 세션이 변조되지 않았음을 검증하는 신뢰된 제3자 또는 노드를 의미한다. TLS Notary는 암호화된 핸드셰이크(handshake)와 세션 키(session key) 등 주요 세션 정보를 캡처하고 기록하여, 신뢰되지 않은 참여자조차 세션 무결성을 검증할 수 있도록 한다. 이 메커니즘을 통해 상위 AI 에이전트 서비스는 외부 서버로부터 데이터를 완전하게 신뢰하지 않고도 인증할 수 있으며, TLS Notary의 증거는 온체인 검증 과정에서 활용되어 AI 에이전트 서비스가 안전하고 신뢰할 수 있는 데이터를 처리하도록 보장한다. aelf는 현재 수신자(Receiver)와 노터리(Notary) 두 개의 독립 노드를 통해 TLS Notary 메커니즘을 운영하고 있다.

탈중앙화 AI 에이전트 서비스 노드(Decentralised AI Agent Service Nodes)

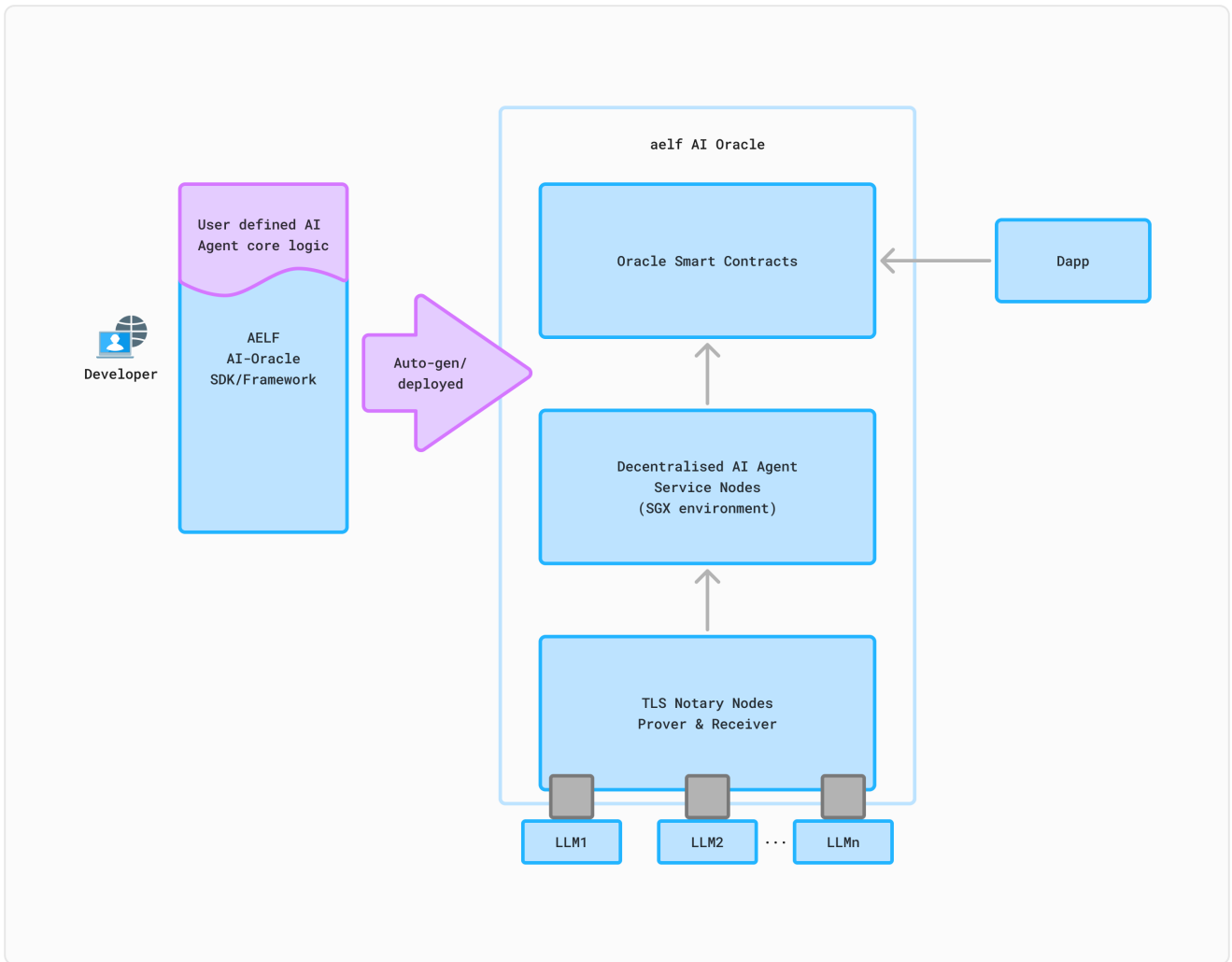
탈중앙화 AI 에이전트 서비스 노드는 인텔(Intel)의 SGX(Software Guard Extensions) 기술을 활용한 분산형 AI 에이전트 컴퓨팅 네트워크를 구성한다. SGX는 프로세서 수준에서 “신뢰 실행 환경(trusted execution environment)”을 생성하여 안전하고 신뢰할 수 있는 데이터 처리 기능을 제공한다. aelf 오라클 네트워크에서 AI 에이전트 서비스는 SGX 실행 환경 내에서 작동하므로, 노드 운영자조차 서비스 실행의 세부 내용을 확인할 수 없다. 이 SGX 기반 기술은 AI 에이전트 코드 실행의 보안을 보장하고 변조로부터 보호하며, 블록체인 기술과 결합될 경우 변조 불가능한 기록과 탈중앙화 신뢰를 동시에 제공한다. 개발자는 이러한 보안 계층 위에서 자신의 AI 에이전트 서비스를 배포하고 실행할 수 있다.

aelf에서의 AI 오라클 활용(AI Oracle Use on aelf)

aelf는 완전한 SDK 및 프레임워크를 제공하여, 개발자는 핵심 로직과 상호작용 인터페이스만 개발하면 된다. 프레임워크는 관련 AI 에이전트 서비스를 자동으로 생성, 스케줄링, 배포하고, AI 에이전트 팩토리를 트리거(trigger)하여 연관된 AI 스마트 컨트랙트를 자동으로 생성한다.

단순한 AI 호출 로직의 경우, 이 과정은 완전히 자동화된다. 그러나 메모리 관리나 임베딩(embedding)과 같은 복잡한 AI 에이전트 서비스(현재 프레임워크는 ChatGPT API와 통합되어 있으며, 향후 추가적인 LLM과 연동 가능)를 개발하려는 경우, 개발자는 제공된 인터페이스 문서를 참고하여 직접 서비스를 구현해야 한다.

또한 aelf AI 오라클은 가격 피드(price feed), 난수 생성(random number generation) 등 전통적인 오라클 서비스도 제공한다. 개발자는 aelf AI 오라클 SDK를 활용해 무한한 온체인 AI 애플리케이션 시나리오를 구현할 수 있다.



aelf AI 오라클은 aelf 상의 AI 디앱 생태계 발전을 적극적으로 지원한다. 이를 위해 SDK와 프레임워크를 지속적으로 최적화하여 AI 디앱과 AI 간의 상호작용 기능을 강화하고, AI 에이전트 플랫폼과의 협업을 확대할 계획이다. 현재 aelf AI 오라클은 ChatGPT API와 통합되어 있으며, 향후에는 더 많은 중앙화 LLM과의 연동 및 다른 탈중앙화 AI 컴퓨팅 네트워크와의 협력을 통해 개발자들의 다양한 요구를 충족할 예정이다.

aelf 체인을 넘어, aelf AI 오라클은 이더리움(Ethereum) 등 주요 블록체인으로 확장되어 Web3의 진정한 AI 계층으로 발전하는 것을 목표로 하고 있다.

iii) aelf를 위한 지능형 부하 분산(Intelligent Load Balancing for aelf)

지능형 부하 분산(Intelligent Load Balancing)은 aelf 블록체인의 확장성과 성능을 향상시키는 핵심 요소이다. AI와 머신러닝을 활용하여 네트워크 전반의 작업 부하를 보다 효율적으로 분산함으로써, 단일 노드에 병목 현상이 발생하는 것을 방지하고 높은 트랜잭션 처리량과 낮은 지연(latency)을 유지할 수 있다.

동적 트래픽 분배(Dynamic Traffic Distribution)

머신러닝 알고리즘은 실시간 네트워크 트래픽과 과거 트랜잭션 패턴을 분석하여 작업 부하를 동적으로 분배할 수 있다. AI 모델은 현재 및 과거의 성능 데이터를 기반으로 과부하가 예상되는 노드를 예측하고, 트래픽을 사용률이 낮은 노드로 자동 재분배함으로써 네트워크 혼잡을 방지하고 안정적인 운영을 유지한다.

이러한 개념은 블록체인 외부의 콘텐츠 전송 네트워크(CDN)에서도 확인할 수 있다. 예를 들어, [Akamai](#)와

[Cloudflare](#)는 AI를 활용해 전 세계 서버 네트워크 전반의 트래픽을 관리한다. 이 시스템들은 서버 부하, 지연 시간, 네트워크 상태 등의 지표를 지속적으로 모니터링하여 콘텐츠를 가장 빠르고 효율적으로 전달한다. aelf 역시 유사한 AI 기반 부하 분산 기술을 적용하여 노드 간 트랜잭션 처리 효율을 극대화할 계획이다.

자원 활용 최적화(Resource Utilisation Optimisation)

AI는 네트워크의 연산 자원을 균형 있게 배분함으로써 효율적인 자원 활용을 가능하게 한다. 이는 스마트 컨트랙트 실행과 트랜잭션 검증 작업을 네트워크 전반에 고르게 분산하는 것을 의미한다. 머신러닝 모델은 여유 연산 용량이 있는 노드를 식별하고, 해당 노드로 작업을 재배치함으로써 모든 자원이 효율적으로 활용되도록 한다.

예를 들어, [Google의 Borg 시스템](#)은 대규모 데이터센터에서 가용 자원에 따라 작업을 동적으로 할당하여 높은 활용률을 유지하고 유휴 시간을 최소화한다. aelf 역시 이와 유사한 전략을 평가 및 적용하여 네트워크 내 작업 부하를 균형 있게 분산함으로써, 특정 노드의 과부하나 미활용 상태를 방지하고 있다.

예측적 확장(Predictive Scaling)

예측적 확장은 지능형 부하 분산의 핵심 요소 중 하나로, AI 모델이 미래의 네트워크 수요를 예측하고 이에 따라 자원을 선제적으로 확장하는 개념이다. 트랜잭션 볼륨의 추세와 패턴을 분석함으로써 AI는 트래픽 증가가 예상되는 시점을 미리 파악하고, 필요한 연산 자원을 사전에 배분한다. 이러한 사전 대응적 접근 방식은 피크 시간대에도 네트워크의 응답성을 유지하도록 돕는다.

예를 들어, [AWS Auto Scaling](#)은 예측 알고리즘을 사용하여 예상 부하에 따라 서버 수를 자동으로 조정함으로써 응답 시간을 최소화하고 서비스 품질 저하를 방지한다. aelf 또한 이와 유사한 예측적 확장 기술을 활용하여 트랜잭션 볼륨 변동에도 성능 저하 없이 안정적으로 네트워크를 운영할 수 있도록 하고 있다.

장애 허용성과 중복성(Fault Tolerance and Redundancy)

지능형 부하 분산은 네트워크의 장애 허용성(fault tolerance)과 중복성(redundancy)을 강화하는 역할도 수행한다. AI는 노드의 상태와 성능을 지속적으로 모니터링하며, 장애 조치이나 성능 저하를 보이는 노드를 식별하고 격리한다. 이후 트래픽을 정상적으로 작동하는 노드로 재분배함으로써 네트워크의 가용성과 안정성을 유지한다.

[Netflix의 Chaos Monkey](#)는 이러한 개념을 기반으로 인프라 내 의도적인 장애를 유발하여 시스템의 복원력을 테스트하며, AI 기반 부하 분산 시스템을 통해 트래픽을 자동으로 재조정하여 서비스 연속성을 보장한다. aelf 역시 AI 기반 장애 복원 메커니즘을 도입해 개별 노드 장애 상황에서도 네트워크 전체가 견고하게 유지되도록 설계하고 있다.

AI와 머신러닝 기반의 지능형 부하 분산은 aelf 블록체인의 확장성과 성능을 대폭 향상시키는 핵심 기술이다. 트래픽을 동적으로 분배하고, 자원을 효율적으로 활용하며, 수요를 예측해 자원을 확장하고, 장애에 대응하는 능력을 강화함으로써, AI 기반 부하 분산은 aelf 네트워크가 증가하는 트랜잭션 볼륨을 안정적이고 효율적으로 처리할 수 있도록 보장한다.

iv) aelf를 위한 AI 기반 크로스체인 상호운용성(AI-Facilitated Cross-Chain Interoperability for aelf)

AI를 aelf의 크로스체인 상호운용성(cross-chain interoperability) 프레임워크에 통합함으로써, 데이터 전송과 검증 프로세스의 효율성과 보안을 크게 향상시킬 수 있다. AI 기반 최적화 기술을 활용하면 aelf 내부(MainChain과 dAppChain 간)뿐만 아니라 다양한 외부 블록체인 네트워크와의 통신에서도 원활하고 안정적인 상호운용성을 보장할 수 있다.

데이터 전송 최적화(Optimising Data Transfer)

AI는 aelf와 연결된 다양한 블록체인 간 데이터 전송 과정을 간소화하는 데 핵심적인 역할을 한다. 머신러닝 알고리즘은 과거 데이터와 현재 네트워크 상태를 분석하여 데이터 패킷의 최적 라우팅 경로를 예측할 수 있다. 이를 통해 데이터는 혼잡이 가장 적고 효율성이 가장 높은 경로를 따라 전송되어, 지연(latency)을 최소화하고 전송 속도를 높일 수 있다.

예를 들어, AI 모델은 실시간 네트워크 트래픽에 따라 라우팅 경로를 동적으로 조정할 수 있으며, 이는 구글(Google)이나 아마존(Amazon)과 같은 대형 클라우드 컴퓨팅 네트워크에서 데이터 흐름을 최적화하는 방식과 유사하다. 또한 AI는 예측 분석(predictive analytics)을 통해 네트워크 혼잡을 사전에 예측하고 데이터 전송 프로토콜을 선제적으로 조정할 수 있다. 이를 통해 aelf는 잠재적인 병목 현상을 방지하고, 크로스체인 트랜잭션이 효율적으로 처리되도록 보장할 수 있다.

AI 알고리즘은 네트워크 동작으로부터 지속적으로 학습함으로써 예측 정확도를 점차 개선하고, 시간이 지남에 따라 전반적인 성능과 신뢰성을 높인다.

데이터 검증 강화(Enhanced Data Validation)

AI는 크로스체인 트랜잭션 검증의 보안성과 정확성을 강화할 수도 있다. 방대한 트랜잭션 이력 데이터를 학습한 머신러닝 모델은 사기 가능성이나 오류를 나타내는 비정상적인 패턴을 식별할 수 있다. AI 기반 검증 도구는 비정상적으로 큰 규모의 송금이나 동일 노드에서 반복적으로 발생하는 트랜잭션 등 일반적인 패턴과 다른 이상 행위를 탐지하여, 이중 지출(double-spending) 또는 보안 침해 가능성을 조기에 경고한다.

aelf는 이러한 AI 기반 검증 메커니즘을 구현하기 위해 여러 전략적 파트너와 협력하고 있으며, 이를 통해 크로스체인 상호작용의 무결성과 보안을 보장할 계획이다.

v) aelf를 위한 AI 기반 노드 선택 및 검증(AI-Driven Node Selection and Validation for aelf)

장기적 연구 과제의 일환으로, aelf 연구팀은 현재 AI를 노드 선택(node selection) 및 검증(validation) 프로세스에 통합하는 방안을 탐색하는 초기 단계에 있다. 이 연구가 본격적으로 추진될 경우, aelf의 합의 메커니즘(consensus mechanism)에서 속도와 보안성을 모두 크게 향상시킬 잠재력을 지니고 있다.

노드 선택 최적화(Optimising Node Selection)

머신러닝은 과거 데이터를 분석하여 신뢰성과 안정성이 높은 노드를 예측하는 데 활용될 수 있다. AI 모델은 과거 성능, 네트워크 지연(latency), 자원 가용성(resource availability) 등의 요인을 평가하여 합의 프로세스에 참여하기에 가장 적합한 노드를 우선순위화할 수 있다. 예를 들어, 신경망(neural network)을 학습시켜 가동 시간(uptime), 트랜잭션 검증 속도, 과거 정확도 등의 지표를 기반으로 노드의 신뢰도를 예측함으로써, 합의에 참여하는 노드가 높은 성능과 안정성을 갖추도록 보장할 수 있다.

이러한 최적화를 구현하는 실질적인 접근 방식 중 하나는 유전 알고리즘(genetic algorithm)의 활용이다. 유전 알고리즘은 자연 선택(natural selection)의 원리를 모방하여, 미리 정의된 적합도(fitness) 기준에 따라 반복적으로 전략을 진화시키고 개선함으로써 최적의 노드 선택 방식을 도출한다. 예를 들어, 과거 트랜잭션에서 높은 신뢰성과 낮은 지연을 보인 노드에는 더 높은 우선순위를 부여하여, 합의 과정이 효율적이면서도 보안성을 유지하도록 한다. 이러한 방식은 엣지 컴퓨팅(edge computing)이나 작업 스케줄링(task scheduling)과 같은 다른 분야에서도 자원 할당과 성능 최적화를 위해 효과적으로 활용된 바 있다.

합의 보안성 강화(Enhancing Consensus Security)

AI는 실시간 네트워크 상태와 잠재적 위협을 기반으로 노드 선택 기준을 동적으로 조정함으로써 합의 프로세스의 보안성을 강화할 수도 있다. 예를 들어, 머신러닝 모델은 시빌 공격(Sybil attack)과 같이 단일 주체가 여러 노드를 제어하여 네트워크를 장악하려는 시도를 탐지할 수 있다. AI는 이러한 비정상적 패턴을 실시간으로 식별하고 대응함으로써, 합의 메커니즘의 견고함과 신뢰성을 유지한다.

이 개념의 구체적 구현으로는 이상 탐지 알고리즘(anomaly detection algorithm)의 적용이 가능하다. 이 알고리즘은 네트워크 활동을 모니터링하여, 갑작스러운 노드 참여 증가나 비정상적인 트랜잭션 패턴 등 평소와 다른 행위를 감지한다. 이러한 이상 현상이 탐지되면, AI 시스템은 해당 노드를 검증 대상으로 표시하거나 합의 과정에서 제외함으로써 네트워크를 잠재적 공격으로부터 보호한다. 이 접근 방식은 AI의 대규모 데이터 실시간 분석 능력을 활용하여 블록체인 보안을 선제적으로 강화하는 것이다.

노드 선출(node election)은 네트워크 합의와 보안의 핵심 절차이기 때문에, 향후 aelf는 AI 오라클(AI Oracle)을 통합하여 이러한 선출 과정이 개방적이고 투명하며 신뢰성 있게 운영되도록 할 계획이다.

개발자 및 사용자 경험(Developer and User Experience)

i) NLP를 통한 비전문가의 스마트 컨트랙트 생성 지원(Enabling Non-Technical Users to Create Smart Contracts with NLP on aelf)

aelf에서 스마트 컨트랙트를 생성하는 과정은 비기술 사용자뿐만 아니라 Web3 환경에 익숙하지 않은 기술 사용자에게도 상당한 도전 과제가 될 수 있다. 사용자는 프로그래밍 언어의 이해, 개발 환경의 활용, 그리고 컨트랙트의 보안성과 기능 보장을 동시에 처리해야 하는 어려움을 겪는다.

aelf는 자연어 처리(NLP, Natural Language Processing) 기술을 활용하여 이러한 복잡한 과정을 단순화하고, 사용자가 직관적인 자연어 입력만으로 엔드투엔드(end-to-end) 스마트 컨트랙트를 생성할 수 있도록 지원한다.

스마트 컨트랙트 생성 단순화(Simplifying Smart Contract Creation)

NLP는 비전문가가 블록체인 기술과 상호작용하는 방식을 근본적으로 변화시킨다. 자연어로 작성된 설명을 해석하여 실행 가능한 스마트 컨트랙트 코드로 변환할 수 있기 때문이다. 예를 들어, 사용자가 “앨리스가 10 ELF를 예치하고, 밥이 특정 조건 X를 충족하면 이를 받는 에스스로 컨트랙트를 생성해줘”라고 입력하면, NLP 모델은 이를 해석하고 관련 엔터티와 조건을 추출해 해당하는 스마트 컨트랙트 코드를 자동으로 생성한다.

이 과정에는 GPT-4 및 OpenAI의 Codex와 같은 고급 NLP 모델의 기능이 활용된다. 이러한 모델은 자연어 설명을 이해하고 코드로 변환하도록 학습되어 있으며, 사용자 입력을 미리 정의된 템플릿에 매핑하거나 사용자의 요구에 맞는 코드 구조를 동적으로 생성할 수 있다. 이를 통해 비전문 사용자도 단 한 줄의 코드 작성

없이 복잡한 스마트 계약을 구현할 수 있다.

접근성과 사용성 향상(Enhancing Accessibility and Usability)

aelf는 NLP를 플랫폼에 통합함으로써 블록체인 기술의 접근성과 사용성을 획기적으로 개선하고자 한다. 이러한 기술의 민주화는 더 폭넓은 사용자층이 블록체인 생태계에 참여할 수 있도록 하여, 채택률과 혁신을 동시에 촉진한다.

예를 들어, 한 사용자가 단순한 디파이(DeFi) 토큰 스테이킹 계약을 생성하려 할 때, 개발자를 고용하는 대신 NLP 기반 인터페이스에 계약 조건을 자연어로 입력할 수 있다. 시스템은 이러한 입력을 해석하여 다양한 스테이킹 기능을 수행하는 스마트 계약을 자동으로 생성하며, 프로토콜이 의도한 대로 작동하도록 보장한다. 무엇보다 이 과정은 보안을 유지하면서 사용자 경험을 크게 향상시킨다.

실시간 피드백 및 검증(Real-Time Feedback and Validation)

aelf에서의 NLP 기반 스마트 계약 생성의 또 다른 주요 장점은 실시간 피드백 및 검증 기능이다. 사용자가 계약 요구사항을 입력하는 동안 NLP 시스템은 잠재적인 문제를 강조 표시하거나, 최적화 방안을 제안하고, 복잡한 로직을 쉽게 이해할 수 있는 언어로 설명할 수 있다.

예를 들어, 사용자가 보안 취약점으로 이어질 수 있는 계약 설명을 입력할 경우, 시스템은 이를 즉시 감지하여 수정 제안을 제공한다. 이와 같은 인터랙티브한 과정은 계약의 보안을 강화할 뿐만 아니라, 사용자가 스마트 계약 개발의 모범 사례를 자연스럽게 학습하도록 돕는다.

사용자 기반 확장(Broadening the User Base)

스마트 계약 생성을 위한 NLP 도입은 비기술적 배경을 가진 개인 및 기업이 블록체인 기술을 활용할 수 있도록 하여, aelf의 사용자 기반을 대폭 확장한다. 이러한 포용성은 블록체인의 대중적 확산에 핵심적이며, 진입 장벽을 낮추고 과정을 단순화함으로써, 다양한 사용자가 블록체인의 자동화와 보안성을 전문가 수준의 기술 없이도 누릴 수 있게 된다.

ii) aelf 개발자를 위한 AI 기반 스마트 계약 감사(AI based Smart Contract Audit for Developers on aelf)

AI 기반 스마트 계약 감사는 GPT-4 및 BERT와 같은 대규모 사전 학습(pre-trained) 모델을 활용하여 감사 과정을 자동화한다. 기존의 감사 방식이 수동 코드 리뷰나 정적 분석 도구에 의존했던 것과 달리, AI 감사는 자연어 처리(NLP)와 딥러닝(deep learning)을 통해 보다 포괄적이고 정확한 감사 보고서를 제공한다.

AI 감사에서는 스마트 계약 코드를 사전 학습된 모델에 입력하여 코드의 문법(syntax) 및 논리 구조(logical structure)를 분석하고, 보안 취약점 및 논리적 오류를 식별한다. 사용자는 “이 스마트 계약에 재진입 공격(reentrancy attack) 취약점이 있는지 확인해줘”와 같은 프롬프트(prompt)를 입력해 분석을 유도할 수 있다. 모델은 이에 따라 상세 분석을 수행하고, 잠재적 취약점과 수정 방안을 포함한 감사 보고서를 생성한다.

AI 기반 스마트 계약 감사의 주요 측면(Key Aspects of AI based Smart Contract Audits)

이 프로세스의 주요 목적은 배포 이전에 코드를 검토하고 분석하여 취약점, 비효율성 또는 잠재적 누수를 식별하는 것이다. 이는 결함이 심각한 재정 손실이나 보안 침해로 이어질 수 있기 때문에 필수적이다. 예를 들어, 디파이(DeFi) 애플리케이션 컨트랙트의 감사에서는 사용자 자금을 보호하기 위해 익스플로잇

(exploit) 테스트가 엄격히 수행된다.

- **취약점 평가(Vulnerability Assessment):**

코드 내 잠재적 보안 문제를 식별한다. 예를 들어, 토큰 발행 컨트랙트 감사 과정에서 자금 탈취 가능성을 가진 취약점이 발견되어, 개발자가 배포 전 해당 문제를 수정할 수 있었다.

- **코드 최적화(Code Optimisation):**

효율성을 개선하고 가스 수수료를 절감한다. 예를 들어, 게임 디앱(DApp) 컨트랙트의 감사에서 트랜잭션 비용을 크게 줄이고 접근성과 경제성을 높이기 위한 최적화 방안이 제안되었다.

- **규제 준수 검증(Compliance Check):**

법적 및 규제 기준 준수를 보장한다. 감사 과정에서 스마트 컨트랙트가 최신 규제 요건을 충족하는지 검증하여, 디파이 플랫폼이 규정에 부합하도록 보장한다.

aelf에서의 기술 구현(Technical Implementation on aelf)

AI 기반 스마트 컨트랙트 감사는 일반적으로 두 가지 접근법으로 구현된다: **프롬프트 설계 접근법(Prompt Design Approach)**과 **자동화된 미세 조정 접근법(Automated Fine-Tuning Approach)**이다.

1. 프롬프트 설계 접근법(Prompt Design Approach)

프롬프트 설계 접근법은 모델을 재학습시키지 않고, 특정 작업을 최적으로 수행할 수 있도록 지시문(prompt)을 구성하는 방식이다. 스마트 컨트랙트 감사를 위한 단계는 다음과 같다.

1. **목표 작업 정의(Define the Target Task):**

감사를 수행할 특정 이슈를 명확히 정의하고, 감사 규칙 라이브러리를 구축한다.

예:

- 재진입 공격 취약점(Reentrancy Attack Vulnerability): 외부 컨트랙트가 반복 호출을 통해 다중 자금 이체를 유발할 가능성이 있는지 확인.

2. **프롬프트 설계(Design Prompts):**

모델의 분석 방향을 유도할 수 있는 정밀한 프롬프트를 작성한다.

예:

- “이 스마트 컨트랙트에 재진입 공격 취약점이 있는지 확인해줘.”

3. **프롬프트 및 코드 입력(Input Prompts and Contract Code):**

설계된 프롬프트와 스마트 컨트랙트 코드를 GPT-4와 같은 대형 모델에 입력한다.

- 코드 분석을 지원하는 모델 선택
- 확인할 구체적 항목을 지정하는 프롬프트 입력

4. **감사 보고서 생성(Generate Audit Report):**

모델은 입력된 코드와 프롬프트를 분석하여 다음과 같은 내용을 포함한 감사 보고서를 생성한다.

- **취약점 설명(Vulnerability Description):** 발견된 취약점의 구체적 위치와 유발 조건을 상세히 기술.
- **위험 평가(Risk Assessment):** 취약점의 심각도 및 잠재적 영향 평가.
- **수정 제안(Remediation Suggestions):** 코드 로직 수정, 접근 제어 추가, 보안 라이브러리 사용 등 구체적 개선 방안 제시.

이 방법의 장점은 대규모 데이터나 연산 자원이 필요하지 않아 빠르게 배포 및 적용할 수 있다는 점이다.

2. 자동화된 미세 조정 접근법(Automated Fine-Tuning Approach)

미세 조정(fine-tuning) 접근법은 대형 모델을 특정 작업에 더욱 최적화하도록 재학습하는 방식이다. 이를 위해 과거 감사 데이터와 수정 사례 등 대규모 학습 데이터셋이 필요하다. 주요 단계는 다음과 같다.

1. **데이터 수집(Data Collection):**
스마트 컨트랙트 코드, 감사 보고서, 수정 사례 등의 대규모 데이터셋을 수집한다.
2. **데이터 전처리(Data Preprocessing):**
학습 효과를 높이기 위해 데이터를 정제하고 표준화한다.
3. **모델 미세 조정(Model Fine-Tuning):**
전처리된 데이터셋을 기반으로 대형 모델을 재학습시켜 분석 및 감사 능력을 강화한다.
4. **검증 및 최적화(Validation and Optimisation):**
검증 세트를 활용해 모델 성능을 평가하고 필요 시 최적화한다.
5. **모델 배포(Model Deployment):**
미세 조정된 모델을 실제 감사 환경에 배포하여 실시간 감사에 활용한다.

이 접근법은 특정 작업에 대한 모델의 성능을 크게 향상시킬 수 있지만, 많은 연산 자원과 시간이 요구된다. 그러나 이렇게 미세 조정된 모델은 복잡한 취약점을 보다 정확하게 식별하고, 구체적이고 효과적인 수정 방안을 제시할 수 있다.

궁극적으로, 이 모델은 스마트 컨트랙트 감사 도구에 통합되어 aelf 및 디앱(dApp) 개발자들이 스마트 컨트랙트를 aelf 체인에 배포하기 전 철저한 감사를 수행할 수 있도록 지원할 예정이다.

iii) AI 기반 챗봇을 통한 사용자 및 개발자 경험 향상(Enhancing User and Developer Experience with AI-Powered Chatbots on aelf)

AI 기반 챗봇(chatbot)을 aelf 블록체인 생태계에 통합함으로써, 실시간 지원 제공, 반복 업무 자동화, 정보 접근성 향상을 통해 사용자와 개발자 모두의 경험을 획기적으로 개선할 수 있다.

사용자 경험 개선(User Experience Improvement)

AI 기반 챗봇은 즉각적인 지원과 개인화된 도움을 제공함으로써 사용자 경험을 대폭 향상시킬 수 있다. aelf 생태계에 처음 진입하는 사용자들은 지갑 설정, 트랜잭션 수행, 블록체인 기능 이해 등에서 어려움을 겪는 경우가 많다. aelf는 업계 선도 전략 파트너인 [ChainGPT](#)와 협력하여, 24시간 상시 지원이 가능한 AI 챗봇을 개발하고 있다.

이 챗봇은 자주 묻는 질문에 답변하고, 단계별 가이드를 제공하며, 실시간으로 문제 해결을 지원한다. 이러한 즉각적인 지원은 사용자 불편을 줄이고 만족도를 높인다.

이는 전통 산업에서도 이미 널리 활용되고 있는 방식으로, 예를 들어 [Bank of America](#)는 ‘Erica’라는 AI 챗봇을 도입하여 고객에게 거래 내역 조회, 알림 전송, 금융 조언 등의 맞춤형 서비스를 제공하고 있다.

마찬가지로, aelf의 AI 챗봇은 토큰 잔액, 트랜잭션 상태, 스마트 컨트랙트 기능 등에 대한 정보를 즉시 제공하며, 사용자가 플랫폼을 보다 효율적으로 탐색할 수 있도록 돕는다.

또한 AI 챗봇은 사용자 행동과 선호도를 분석하여 개인화된 추천을 제공함으로써 사용자 참여도를 높인다. 예를 들어, [Amazon](#)이 AI 챗봇을 통해 사용자의 구매 이력과 검색 기록을 분석해 맞춤형 상품을 추천하듯, aelf의 챗봇도 사용자의 활동 데이터를 기반으로 새로운 디앱(dApp)이나 관심을 가질 만한 기능을 제안할 수 있다. 이를 통해 플랫폼 내 상호작용이 한층 풍부해지고, 신규 및 기존 사용자 모두에게 더 매력적인 경험을 제공한다.

개발자 경험 향상(Developer Experience Enhancement)

개발자에게 AI 기반 챗봇은 반복적인 작업을 자동화하고 코드 작성 지원을 제공함으로써 개발 효율성을 높인다. aelf는 실시간 코드 도움, 디버깅 제안, 문서 접근 기능을 제공하는 통합형 개발자용 챗봇을 개발 중이다. 예를 들어, 개발자가 C#으로 스마트 컨트랙트를 작성하던 중 오류를 발견하면, 챗봇이 즉시 해결책을 제안하거나, 관련 문서의 코드 스니펫(snippet)을 제공하며, 모범 사례(best practice)를 안내할 수 있다. [GitHub Copilot](#)은 이러한 기능의 대표적 사례로, OpenAI와 GitHub이 공동 개발한 AI 기반 코드 보조 도구이다. 이 도구는 코드 문맥을 이해하고 함수나 구문을 자동으로 완성해 개발자의 생산성을 높인다. aelf는 이와 유사한 AI 기능을 통합하여 개발자가 문제 해결에 소요하는 시간을 줄이고, 더 많은 시간을 혁신적 애플리케이션 개발과 가치 창출에 집중할 수 있도록 돕고자 한다.

온보딩 및 교육 효율화(Efficient Onboarding and Education)

AI 챗봇은 사용자와 개발자 모두에게 효율적인 온보딩(onboarding)과 지속적 교육(continuous education)을 제공할 수 있다. 신규 사용자는 챗봇과의 대화형 상호작용을 통해 초기 설정을 안내받고, 주요 기능과 서비스에 대해 학습할 수 있다. 개발자 역시 챗봇을 통해 튜토리얼, 모범 사례, 최신 개발 도구 및 프로토콜 관련 업데이트를 실시간으로 제공할 수 있다. 예를 들어, [Coursera](#)는 AI 챗봇을 활용하여 학습자에게 과정 추천, 질의응답, 맞춤형 피드백 제공을 수행한다. 이와 유사하게, aelf의 챗봇은 멘토 역할을 수행하며 사용자와 개발자가 원활하고 체계적인 학습 경험을 얻도록 지원한다. 이를 통해 블록체인 기술의 진입 장벽을 낮추고, 학습 곡선을 완화하여 생태계 참여를 촉진한다.

AI를 넘어 - 모듈형 블록체인(Beyond AI - A Modular Blockchain)

[모듈형 블록체인\(modular blockchain\)](#)은 블록체인의 일부 핵심 기능만 직접 처리하고, 나머지 기능은 하나 이상의 독립적인 계층(layer)에 위임하는 설계 방식이다. 즉, 블록체인의 다양한 작업과 기능을 각각의 독립된 계층 또는 모듈로 분리함으로써, 성능, 확장성, 그리고 맞춤화(customisation)를 개선할 수 있다.

실행 계층(Execution Layer):

이 계층은 트랜잭션과 상태 변화(state change)가 발생하는 영역으로, 예를 들어 지갑 잔액 변경과 같은 연산이 수행된다. 사용자는 트랜잭션 수행, 자산 전송, 스마트 컨트랙트 배포 등을 통해 이 계층과 상호작용한다.

정산 계층(Settlement Layer):

모듈형 블록체인에서 선택적으로 존재하는 계층으로, 롤업(rollup) 트랜잭션을 검증하고 정산(settle)하는 역할을 담당한다. 롤업은 여러 개의 트랜잭션을 하나로 묶어 처리 효율을 높이는 기술이다.

합의 계층(Consensus Layer):

이 계층은 네트워크 내 전체 노드(full node)를 통해 블록 순서(ordering)와 최종성(finality)을 제공한다. 전체 노드는 블록의 내용을 다운로드하고 실행하여 상태 전이(state transition)의 유효성에 대한 합의(consensus)에 도달한다.

데이터 가용성 계층(Data Availability Layer):

이 계층에는 이미 유효성 검증을 마친 데이터가 저장된다. 상태 전이 검증에 필요한 데이터가 언제든지 접근 가능하고 쉽게 검증될 수 있도록 보장하는 역할을 한다.

이러한 기능 분리를 통해, 모듈형 블록체인은 각 계층을 독립적으로 최적화할 수 있으며, 이는 전체적인 성능과 확장성을 비약적으로 향상시킨다. 그 결과, 보다 확장 가능하고 조합성(composability) 및 탈중앙성이 강화된 시스템을 구축할 수 있다. 이러한 이유로 모듈형 블록체인은 차세대 블록체인 기술의 방향으로 평가받고 있다.

aelf의 현재 상태(The present status of aelf)

앞서 설명했듯이, aelf는 메인체인(MainChain)과 디앱체인(dAppChain)으로 구성된 아키텍처를 기반으로 운영된다. aelf의 디앱체인은 코스모스(Cosmos)의 컨슈머 체인(consumer chain)이나 폴카닷(Polkadot)의 패러체인(parachain)과 유사하다. 이러한 플랫폼들과 마찬가지로, aelf는 소프트웨어 공학 원리에 기반한 모듈형(modular) 또는 분해형(deconstructed) 접근 방식을 채택하여 코드 수준에서 기능을 분리한다.

이 아키텍처의 주요 목적은 aelf 생태계 내에서 모듈형 플러그인(plugin)을 개발할 수 있도록 하고, 다양한 모듈을 플러그인 형태로 로드할 수 있게 하여 확장성과 유연성을 강화하는 데 있다. 예를 들어, 합의 기능(consensus functionality)을 교체 가능한 코드 패키지로 취급하여 개발자가 손쉽게 커스터마이징할 수 있다.

그러나 이러한 구조에도 불구하고, 현재 aelf의 메인체인-디앱체인 아키텍처는 특히 TPS(Transaction Per Second) 처리 용량 측면에서 성능 병목 현상을 겪고 있다. 이에 따라 aelf는 성능, 확장성, 그리고 타 블록체인 가상 머신(Virtual Machine, VM)과의 호환성을 대폭 향상시키는 새로운 **모듈형 체인 구조(Modular Chain Structure)**를 도입할 예정이다.

이에 맞춰, aelf는 이러한 한계를 해결하고 차세대 확장형 블록체인으로 도약하기 위한 **모듈형 블록체인 프로젝트(Modular Blockchain Project)**를 본격적으로 추진하고 있다.

aelf의 솔루션(The aelf solution)

aelf는 [Polygon CDK](#)를 기반으로 한 **ZK-롤업(ZK-rollup)**을 구축하고 있으며, 이는 **밸리디움(validium)** 모드로 동작한다.

주요 구성 요소는 다음과 같다.

1. **Executor/Verifier:** zkEVM / ZKProver
 2. **Data Availability:** 외부 데이터 가용성(External DA) + 데이터 가용성 위원회(Data Availability Committee, DAC)
 3. **Consensus:** 온체인 스마트 컨트랙트(On-chain Smart Contracts)
 4. **Sequencer**
 5. **Bridge**
-

검증 프로세스(Verification Process)

aelf ZK-롤업은 Polygon CDK를 활용한다. Polygon CDK는 이더리움(Ethereum) 위에서 ZK 기반 레이어2(L2) 블록체인을 신속하게 배포할 수 있도록 설계된 고급 오픈소스 프레임워크이며, aelf는 이를 대폭 수정 및 최적화하여 자체 구조에 맞게 구현하고 있다.

aelf ZK-롤업은 밸리디움(validium) 모드로 운영되며, 동시에 모든 EVM 체인과의 원활한 상호운용성을 유지한다. 트랜잭션 데이터는 aelf 메인넷에 저장되지 않고 오프체인(off-chain)에서 실행 및 저장되므로, 확장성이 크게 향상된다.

밸리디움은 보안을 전제로 하면서 L1 가스 저장 비용을 절감하고, 이를 통해 L2 사용자들의 거래 비용을 낮추며, 프라이버시와 사용자 경험을 동시에 개선한다.

전통적인 롤업(rollup)이나 디앱체인(dAppChain)과 달리, aelf ZK-롤업은 실제 트랜잭션 데이터를 공유하지 않고 **유효성 증명(validity proof)**만을 레이어1에 제출한다.

작동 방식은 다음과 같다: 검증자 스마트 컨트랙트(verifier smart contract)가 aelf 레이어1에 배포되고, 밸리디움은 해당 컨트랙트에 유효성 증명을 제출한다.

이 증명은 본질적으로 영지식(Zero-Knowledge) 구조를 가지며, 개별 트랜잭션 세부 내용을 공개하지 않고 결과만을 포함한다.

검증자 스마트 컨트랙트는 제출된 증명의 유효성을 검증하며, 만약 밸리디움이 제출한 배치(batch)가 유효하지 않은 것으로 판정되면 해당 배치는 거부되고 aelf 레이어1에 저장되지 않는다.

합의 컨트랙트(Consensus Contract)

ZkEVM.cs는 유효성 증명(validity proof)을 사용하여 상태 변화(state transition)의 정확성을 보장하는 기본 프로토콜이다.

상태 전이 규칙이 미리 정의된 기준에 따라 올바르게 수행되었는지 확인하기 위해, 합의 컨트랙트(Consensus Contract, ZkEVM.cs)가 aelf 레이어1에 배포되어 작동한다.

ZkEVM.cs는 **ZK-SNARK 회로**를 활용해 각 트랜잭션이 정확히 실행되었는지를 검증한다. 이 시스템이 정상적으로 작동하기 위해서는 두 가지 핵심 프로세스가 필요하다: **트랜잭션 배치(transaction batching)** 및 **트랜잭션 검증(transaction verification)**.

이를 수행하기 위해 aelf ZK-롤업은 두 유형의 참여자를 포함한다:

1. **시퀀서(Sequencer):** 트랜잭션 요청을 그룹화하여 네트워크에 배치(batch)로 제안하고, 이를 ZkEVM.cs에 추가한다.

2. **애그리게이터(Aggregator):** 트랜잭션 배치의 유효성을 검토하고, 해당 유효성 증명을 생성하여 제출한다. 허가가 필요 없는(permissionless) 애그리게이터는 상태 전이 계산의 정확성을 입증하는 증명을 제출할 수 있다.

데이터 가용성(Data Availability)

aelf ZK-롤업의 밸리디움 모드는 **데이터 가용성 위원회(DAC, Data Availability Committee)**가 관리하는 보안 데이터 가용성 계층을 포함한다. 이 계층은 다음과 같은 역할을 수행한다.

1. 특정 블록체인 블록과 관련된 데이터의 가용성을 검증한다.
2. aelf ZK-롤업의 데이터 안정성과 연산 효율성을 보장한다.

DAC의 주요 장점은 다음과 같다.

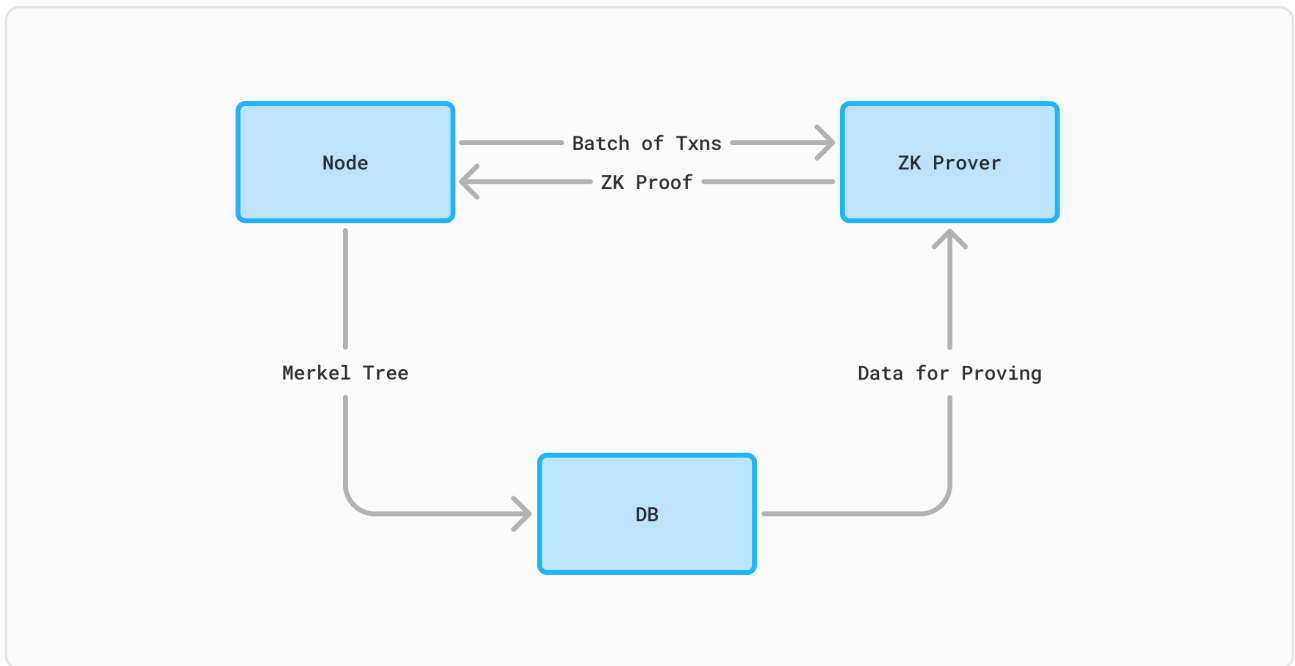
1. **거래 수수료 절감(Reduced Transaction Fees):** 연산량이 줄어들어 따라 비용이 낮아진다.
2. **상태 프라이버시(State Privacy):** 상태 변화의 안전한 기록을 유지하여 데이터 무결성을 보장한다.

zkEVM / ZKProver

aelf ZK-롤업의 노드 핵심 기능 중 하나는 **zkEVM**과 **ZKProver**이다.

일반적인 동작 흐름은 다음과 같다. zkEVM / ZKProver는 레이어2(Layer 2)에서 전달받은 대규모 트랜잭션 배치를 실행하고, 영지식증명(ZK, Zero-Knowledge) 기술을 활용하여 해당 트랜잭션의 유효성을 입증하는 **제로 지식 증명(ZK Proof)**을 생성한다. 증명 생성 과정은 다음과 같다.

1. 노드는 머클 트리(Merkle Tree)의 내용을 데이터베이스에 저장한다.
2. 이후 노드는 트랜잭션 배치를 ZKProver 구성요소로 전송한다.
3. ZKProver는 데이터베이스에 접근하여, 노드가 전송한 트랜잭션에 대한 검증 가능한 증명을 생성하는 데 필요한 정보를 가져온다. 이 정보에는 머클 루트(Merkle Root), 키(keys), 그리고 관련 형제 노드의 해시(hash) 값이 포함된다.
4. 마지막으로 ZKProver는 트랜잭션에 대한 증명을 생성하고 이를 다시 노드로 전송한다.



시퀀서(Sequencer)

시퀀서는 트랜잭션의 순서를 정하고, 글로벌 상태(global state)를 지속적으로 업데이트하는 역할을 한다.

1. **트랜잭션 정렬(Transaction Ordering)**: 풀(pool)에서 트랜잭션을 가져와 상태(state)에 추가한다.
2. **상태 전이(State Transition)**: 실행기(Executor)와 협력하여 트랜잭션을 처리하고 상태를 업데이트한다.
3. **신뢰 가능한 최종성(Trustworthy Finality)**: 시퀀서가 트랜잭션을 상태에 추가하면, 해당 정보를 다른 노드와 공유함으로써 트랜잭션이 최종적으로 확정된다.
다른 노드는 데이터 가용성(DA, Data Availability) 및 유효성(ZKP, Zero-Knowledge Proof) 확인을 받을 때까지, 해당 트랜잭션이 상태에 추가되었다는 점을 신뢰해야 한다. (자세한 내용은 [aelf ZK-Rollup의 트랜잭션 여정\(Transaction Journey on aelf ZK-Rollup\)](#) 참고)

애그리게이터(Aggregator)

애그리게이터는 레이어2의 상태 유효성(validity)을 증명하는 **ZK Proof**를 생성하여 레이어1에 제출하는 역할을 한다. 이를 위해 시퀀서가 정렬한 트랜잭션 배치를 받아 프로버(Prover)와 상호작용하여 영지식증명(ZKP)을 생성한다. 효율적인 운영을 위해 애그리게이터는 다음을 수행한다.

1. 하나 이상의 프로버(Prover)와 협력한다.
2. 여러 트랜잭션 배치에 대한 증명을 집계(aggregate)하여, 하나의 증명으로 여러 배치를 검증할 수 있도록 한다.

브리지(Bridge)

aelf의 레이어2와 레이어1 간의 **토큰 자산 접근 및 컨트랙트 호출(메시지 전달, message passing)**은 **zkEVM 브리지 스마트 컨트랙트(ZkEVMBridge.cs)**를 통해 수행된다.

이 브리지는 레이어1과 레이어2 양쪽에 존재하는 **Global Exit Tree Root Manager** 두 개와의 연동을 통해 네트워크 상호운용성을 실현한다.

가스 요금(Gas Fees)

aelf ZK-롤업에는 **시퀀서(Sequencer)**와 **애그리게이터(Aggregator)** 두 주요 참여자가 있으며, 이들은 ELF 토큰으로 가스 요금을 지불하거나 보상으로 획득한다.

- **시퀀서(Sequencer):**

- 트랜잭션 배치를 생성 및 제안할 때 가스 요금을 지불한다.
- 유효한 트랜잭션이 포함된 배치를 성공적으로 제안할 경우, 트랜잭션 요청자 또는 네트워크 사용자가 지불한 수수료를 보상으로 받는다.

- **애그리게이터(Aggregator):**

- 시퀀서가 제안하고 배치한 트랜잭션을 검증한다.
- aelf ZK-롤업의 ZKNode 소프트웨어에서 실행되며, ZKProver를 사용해 영지식 유효성 증명을 생성한다.
- 트랜잭션을 검증하고 유효성 증명을 제공함으로써, 시퀀서가 각 검증 성공 시 지불하는 ELF 수수료를 보상으로 획득한다.

aelf ZK-롤업의 트랜잭션 진행 과정(Transaction Journey on aelf ZK-rollup)

레이어2(Layer 2) 트랜잭션을 수행하기 전에, 사용자는 가스 요금 지불을 위해 aelf ZK-롤업 브리지를 통해 일부 ELF 토큰을 레이어1(L1)에서 레이어2(L2)로 전송해야 한다.

이후의 단계는 다음과 같다.

1. 사용자는 자신의 지갑(예: [Portkey](#))에서 트랜잭션을 생성하고 이를 시퀀서(Sequencer)에 전송한다.
2. 시퀀서가 해당 트랜잭션을 추가(commit)하기로 확정하면, 해당 트랜잭션은 L2에서 최종화(finalised)된다.
3. 이 시점에서 트랜잭션은 L2 상에서 정산(settled)되었지만, 그 상태(state)는 아직 L1로 전파되지 않았다. 이 상태를 **사전 검증 상태(Pre-validated State)**라 한다.
4. 시퀀서는 트랜잭션 배치 데이터를 L1의 스마트 컨트랙트로 전송하여, 모든 노드가 L1로부터 안전하고 신뢰 불필요(trustless)한 방식으로 상태를 동기화할 수 있도록 한다. 이 상태를 **커밋 상태(Committed State)**라 부른다.
5. 애그리게이터(Aggregator)는 검증을 위해 대기 중인 트랜잭션을 수집하고, 증명(proof)을 구성하여 L1에서 최종성을 확보한다.
6. 증명이 검증되면, 사용자의 트랜잭션은 L1에서도 최종화(finality)에 도달하며, 이는 출금(withdrawal) 등 기타 연산을 수행하기 위한 핵심 단계이다. 이 상태를 **검증 완료 상태(Verified State)**라 한다.

로드맵(Roadmap)



aelf 2025 로드맵: 개요(aelf 2025 Roadmap: Introduction)

본 로드맵은 aelf의 핵심 블록체인 기술 발전 방향을 제시하며, **모듈화(modularity)**, **분산 컴퓨팅(distributed computing)**, 그리고 **AI 통합(AI integration)**에 초점을 맞춘 전략적 로드맵이다.

2025년 1분기(Q1 2025)

핵심 모듈: 합의 및 데이터 가용성(Core Modules: Consensus and Data Availability)

aelf는 합의(consensus)와 데이터 가용성(data availability) 기능을 모듈형 컴포넌트로 추상화(abstraction)할 예정이다.

이를 통해 개발자는 기본 구현체를 그대로 사용하거나, 표준화된 인터페이스를 활용하여 맞춤형 솔루션을 구축할 수 있는 유연성을 확보하게 된다.

첨단 블록체인 아키텍처 탐색 및 통합(Exploring and Integrating Cutting-Edge Blockchain Architectures)

aelf는 **BlockDAG**(탐색 중인 잠재적 기술 계층)를 비롯한 첨단 블록체인 아키텍처를 모듈형 프레임워크에 통합할 계획이다.

이러한 아키텍처는 기존 블록체인이 직면했던 확장성(scalability) 및 동시성(concurrency) 문제를 해결할 수 있는 혁신적 접근법을 제공한다.

2025년 2분기(Q2 2025)

모듈형 실행 및 합의(Modular Execution and Consensus)

합의 계층(consensus layers)과 실행 계층(execution layer) 모두에 모듈화를 확장하여, 개발자가 기본 구현체를 사용하거나 표준화된 인터페이스를 통해 맞춤형 솔루션을 구축할 수 있도록 한다. 이를 통해 유연성이 강화되고, 차세대 Web3 AI 기술 발전에 대비한 확장성을 확보한다.

맞춤형 블록체인 조립(Customisable Blockchain Assembly)

런타임(runtime)에서 구성 파일(configuration file)을 통해 사용자 정의 모듈 컴포넌트를 동적으로 로드할 수 있는 **PoC(Proof-of-Concept)** 검증을 수행한다. 이를 통해 개발자는 특정 사용 사례에 맞춘 블록체인을 구성하고, 새로운 설정을 실험적으로 적용할 수 있게 된다.

AI 인텐트 인식 및 자동 실행(AI Intent Recognition and Automated Execution)

복잡한 Web3 및 암호화폐 상호작용을 자동화하는 AI 기반 계층을 도입한다. 사용자의 '의도(intent)'를 인식하여, 서명(signing), 컨트랙트 호출(contract call), 수수료 정산(fee settlement) 등의 작업을 수동 개입 없이 자동으로 수행함으로써 사용자 경험과 효율성을 향상시킨다.

2025년 3분기(Q3 2025)

완전한 모듈형 블록체인 구현(Fully Operational Modular Blockchain)

실행, 합의, 데이터 가용성, 정산(settlement) 모듈의 핵심 기능을 완성하고 확장 기능을 포함하여, 완전한 운영 가능한 블록체인을 구축한다.

플러그형 모듈 통합(Pluggable Module Integration)

개발자가 모듈형 블록체인 아키텍처에 커스텀 및 확장 모듈을 원활히 통합할 수 있도록 하여, 유연성과 맞춤화를 한층 강화한다.

클라우드 네이티브 배포(Cloud-Native Deployment)

확장 가능한 분산 컴퓨팅 리소스를 활용하는 클라우드 네이티브 아키텍처 상에 모듈형 블록체인을 배포하여, 성능과 자원 할당을 최적화한다.

AI 프라이버시 및 보안(AI Privacy and Security)

영지식증명(ZKP, Zero-Knowledge Proof) 및 동형 암호화(homomorphic encryption) 기술을 통합하여, 자동화된 AI 연산 환경에서도 사용자 데이터의 보안성과 프라이버시를 보장한다.

2025년 4분기(Q4 2025)

완전한 모듈형 블록체인(Complete Modular Blockchain)

거버넌스(governance), 경제 모델(economic model), 권한(permission), 보안(security) 등 남은 모든 모듈의 개발을 완료하여 완전한 기능의 모듈형 블록체인 시스템을 완성한다.

클라우드 네이티브 AI 통합(Cloud-Native AI Integration)

AI 통합을 통해 DevOps 상호운용성을 강화하고, AI 기반 모니터링 및 자동 확장을 도입하여 클라우드 네이티브 환경에서 효율성을 극대화하고 고가용성(high availability)을 보장한다.

플러그형 AI 엔진(Pluggable AI Engine)

개발자가 [LLM\(Large Language Model\)](#)이나 그래프 신경망(Graph Neural Network, GNN)과 같은 다양한 AI 모델을 통합할 수 있도록 지원한다.

이를 통해 복잡한 크로스체인 상호작용, 스마트 컨트랙트 로직 추천 등 고도화된 시나리오에서 AI 활용이 가능해진다.

참고문헌 및 추가 자료(References and Further Readings)

1. aelf. Whitepaper V 1.7.0. October 25th, 2022. [[Link](#)]
2. Blockchain Council. "How Blockchain and AI Can Work Together." Blockchain Council, January 22, 2024. Retrieved from [[Link](#)]
3. Buterin, V. (2024, January 30). Crypto AI. Retrieved from [[Link](#)]
4. Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. Journal of Business Venturing Insights, 13, e00151. [[Link](#)]
5. Christos Smiliotopoulos, Ryan Benton, Georgios Kambourakis, Dimitrios Damopoulos. "Blockchain and Artificial Intelligence: Synergies and Conflicts." *arXiv*, 2024. [[Link](#)]
6. Christos Smiliotopoulos, Ryan Benton, Georgios Kambourakis, Dimitrios Damopoulos. "The Convergence of Artificial Intelligence and Blockchain: The State of Play and the Road Ahead." *MDPI Information*, vol. 15, no. 5, 2024. [[Link](#)]
7. Cointelegraph. "EU Commission Urged to Prepare for Blockchain and AI Integration." Cointelegraph, May 24, 2024. Retrieved from [[Link](#)]
8. Dinh, T. N., & Thai, M. T. (2018). AI and blockchain: A disruptive integration. Computer, 51(9), 48–53. [[Link](#)]
9. ETH Research. (2024). How AI Revolutionizes Ethereum: Another View on AI & Blockchain. Retrieved from [[Link](#)]
10. Pandl, K. D., Thiebes, S., Schmidt-Kraepelin, M., & Sunyaev, A. (2020). On the convergence of artificial intelligence and distributed ledger technology: A scoping review and future research agenda. IEEE Access, 8, 57075–57095. [[Link](#)]
11. Polygon Technology. (2024). Polygon CDK Documentation. Retrieved from [[Link](#)]
12. Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. IEEE Access, 7, 10127–10149. [[Link](#)]
13. Techopedia. (2024). Why Is the Future of Blockchain Modular? Retrieved from [[Link](#)]
14. World Economic Forum. "How Immersive Technology, Blockchain and AI Are Converging." World Economic Forum, June 2024. Retrieved from [[Link](#)]
15. Xiong, Z., Zhang, Y., Niyato, D., Wang, P., & Han, Z. (2018). When mobile

blockchain meets edge computing. IEEE Communications Magazine, 56(8), 33–39. [[Link](#)]

16. Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems, 105, 475–491. [[Link](#)]