

# 아즈텍(Aztec)

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.

## 서론

비트코인(2008)과 이더리움(2014)이 출시된 지 10년이 넘는 지금까지도, 블록체인이 글로벌 금융과 상거래에 미친 영향은 여전히 제한적이다. 문제는 확장성이나 사용성만이 아니다. 한 때 미덕으로 여겨졌던 강제된 투명성이 오히려 주류 채택을 가로막는 장애물로 드러났다.

인터넷 역시 1990년대에 유사한 병목 현상을 겪었다. 열성 사용자 단계에서 대중 시장으로 전환하기 위해서는, 사용자들이 온라인 거래와 정보가 비공개적이고 안전하다는 보장을 필요로 했다. 이러한 돌파구는 두 가지 암호학적 인프라 혁신, 즉 SSL과 HTTPS를 통해 마련되었으며, 이는 인터넷의 상업화 시대를 열어 수조 달러 규모의 가치를 창출했다.

Aztec의 프로그래머블 프라이버시는 블록체인을 위한 SSL에 해당하며, 블록체인이 현실 세계에서 채택되기 위해 부족했던 핵심 기능이다.

Aztec은 2017년에 단순한 목표로 시작했다. 바로 현실 세계 자산을 블록체인으로 가져오는 것이었다. 초기에는 비공개 부채를 토큰화하려는 시도를 했으나, 투명한 원장이 가진 근본적인 한계를 드러냈다. 어떤 기관도 자사의 포트폴리오와 거래 데이터가 온체인에 불변적으로 공개되는 것을 원하지 않았던 것이다. 이후 Aztec은 이 문제 해결에 일관되게 집중해 왔으며, 프로그래머블 온체인 프라이버시를 가능하게 하는 데 필요한 암호학적 인프라를 개발하는 데 전념해 왔다.

지난 8년 동안 Aztec은 여러 핵심적인 혁신을 제공해 왔다. 여기에는 이더리움 상 최초의 프라이빗 전송 시스템(2018)<sup>1</sup>, 성능이 뛰어난 범용 SNARK인 PLONK(2019)<sup>2</sup>, 그리고 범용 영지식 언어인 Noir가 포함된다. Aztec Network는 이러한 모든 작업의 결실로서, 이더리움 위

에 구축된 zk-SNARK 기반의 프라이버시 및 확장성 레이어 2로, Noir와 자체 스마트 컨트랙트 프레임워크인 Aztec.nr을 통해 프라이버시, 확장성, 완전한 프로그래머빌리티를 결합한다.

Aztec Network는 개발자, 기관, 전 세계의 개인 사용자 등 서로 다른 기대와 요구를 가진 다양한 이해관계자를 지원하도록 설계되었다. Aztec은 프로토콜 수준에서는 최대한 중립적이고 검증 가능하도록 구축되었으며, 애플리케이션 수준에서는 사용자에게 강력한 통제권과 프라이버시를 제공한다. 이 네트워크는 출범 초기부터 탈중앙화되어 있으며, 단일 주체가 네트워크의 진화를 좌우하지 않는 상태에서 이러한 모든 이해관계자의 요구가 충족될 수 있도록 보장한다.

이 네트워크의 핵심에는 탈중앙화된 프라이버시 레이어를 구동하는 네이티브 자산인 AZTEC 토큰(AZTEC token)이 있다.

- 스테이킹(Staking): 이 토큰은 Aztec 내에서 블록 생성을 담당하는 시퀀서(Sequencers)의 스테이킹을 통해 네트워크를 보안한다. 시퀀서는 블록 제안 권한을 획득하기 위해 토큰을 스테이킹해야 하며, 자신이 제안한 블록이 이더리움 레이어 1(Ethereum L1)에서 성공적으로 증명될 경우 토큰 형태의 블록 보상을 받을 수 있다.
- 거버넌스(Governance): 시퀀서와 토큰 보유자는 온체인 거버넌스에 참여하여 업그레이드, 파라미터, 토큰 이코노미를 관리한다.
- 사용자 수수료 시장(User Fee Market): 이 토큰은 Aztec Network 내 거래 수수료의 매개체로 사용되며, 실행 환경이 활성화되는 경우 및 그 시점에 따라 블록 공간에 대한 수요에 기반해 인플레이션과 디플레이션이 발생할 수 있도록 한다.

## Aztec 토큰

Aztec Network는 블록 생성을 탈중앙화하고, 최종 확정성(finality) 이전의 빠른 사전 확인(pre-confirmation)이 이루어지는 대기 체인에 경제적 보안을 제공하기 위해 지분증명(proof-of-stake, PoS) 시스템을 활용한다(이하 “Aztec Network” 또는 “Aztec”). Aztec의 네이티브 자산인 (“AZTEC” 또는 “토큰”)은 이 메커니즘의 핵심에 위치하며, 이더리움 레이어 1(Ethereum L1) 상에서 Aztec 시퀀서(Aztec Sequencers)에 의한 스테이킹을 통해 Aztec Network를 보안하는 데 사용된다. 이들은 “시퀀서(Sequencers)”라고도 불리며, Aztec 내에서 블록 생성을 담당한다. 이 토큰은 블록을 제안하고 증명하는 행위에 대한 인센티브로 발행되며, 사용자는 거래 수수료로 토큰을 지불해야 하고, 이는 Aztec 거버넌스 시스템에서의 의결권을 산정하는 기준이 된다.

AZTEC은 이더리움 상에서 ERC-20 토큰으로 발행된다. 이는 불변적이며 프라이버시 보존 기능은 포함하지 않는다. 거버넌스 시스템을 통해 AZTEC 보유자는 Aztec Network의 연가

레이드와 AZTEC의 토크노믹스에 대한 통제권을 가진다. 이들은 토큰을 발행할 수 있으며, 최대 인플레이션 비율을 설정하고, 블록 생성 보상을 정하며, 거래 수수료 계산에 사용되는 파라미터를 구성할 수 있다. AZTEC의 거버넌스 시스템과 롤업(Rollup)은 모두 이더리움에 배포된다.

## 탈중앙화된 출시

이더리움 위의 롤업(Rollup)은 사용자 거래 수수료를 낮추기 위한 목적의 일환으로 확산되어 왔다. 그러나 대부분은 탈중앙화를 “점진적(progressive)”으로 접근하며, 궁극적으로 네트워크를 통제하는 중앙화된 회사 소유 시퀀서(Sequencer)를 운영한다. 이에 반해 Aztec은 탈중앙화 프로토콜이 어떻게 출시되어야 하는지에 대한 새로운 기준을 제시한다. 즉, 완전히 탈중앙화된 블록 생성과 실질적인 유틸리티, 거버넌스, 그리고 건전한 경제 구조를 갖춘 토큰을 기반으로 한다.

탈중앙화된 네트워크로서 Aztec은 단일 주체가 거래를 검열하거나, 프라이버시를 침해하거나, 거버넌스 결과를 좌우할 수 없도록 보장한다. Aztec Network에 대한 통제는 독립적인 행위자들 사이에 분산되어 있으며, 이를 통해 Aztec은 누구나 검증하고, 참여하고, 그 위에서 구축할 수 있는 진정으로 중립적인 공공재가 된다. 이러한 중립성은 광범위한 채택을 위한 토대이며, 사용자는 자신이 의존하는 인프라가 탈취되거나, 장악되거나, 훼손될 수 없고, 어떠한 중앙 운영자도 시스템을 편향시키거나 사용자 이익에 반하는 행위를 할 수 없다는 신뢰를 가질 수 있어야 한다.

Aztec Network의 신뢰 가능한 탈중앙화를 확고히 하기 위해, Aztec Foundation과 Aztec Labs의 직원 및 투자자는 네트워크 출시 이후 1년 동안 스테이킹과 거버넌스에 참여할 수 없도록 제한된다. 이를 통해 특정 주체가 아닌 커뮤니티의 손에 통제권이 귀속되도록 보장한다.

Aztec Network 출시와 함께, Aztec Foundation은 이더리움 상에서 새로운 방식의 토큰 세일(“토큰 세일(Token Sale)”)을 통해 커뮤니티에 토큰을 배포한다. 이 토큰 세일은 수요에 따라 가격이 동적으로 조정되는 연속 청산 경매(continuous clearing auction)를 사용하여, 투명한 가격 발견과 공정한 할당을 보장한다. 해당 경매는 아래에서 정의되는 총 공급량(Total Supply)의 최대 14.95%를 판매하며, 완전 희석 가치 기준 \$350M의 최저 가격(floor price)을 설정한다. 이는 Aztec Labs의 최근 지분 투자 라운드를 기준으로 한 가장 최근의 암시적 네트워크 가치 대비 약 75% 할인된 수준에 해당한다.

토큰 세일의 주요 목적은 노드 운영자, 생태계 기여자, 그리고 더 넓은 커뮤니티 전반에 토큰 총 공급량을 분배하여, 이들이 토큰을 스테이킹하고, Aztec Network를 운영하며, Aztec 거버

스태이킹을 통해, 시퀀서(Sequencer)가 네트워크 업그레이드와 관련된 제안에 참여할 수 있도록 하는 데 있다.

Aztec 거버넌스는 시퀀서가 특정 네트워크 파라미터 및 네트워크 업그레이드와 관련된 제안을 게시할 수 있도록 허용한다. 제안이 시퀀서에 의해 온체인 시그널링 메커니즘을 통해 충분한 지지를 확보하면, 해당 제안은 비준(ratification) 단계로 진입한다. 이후 토큰 보유자는 투표 기간 동안 토큰을 락업함으로써 제안에 대해 투표할 수 있다. 기본적으로 토큰이 스테이킹되면, 이에 수반되는 의결권은 시퀀서 시그널링을 통과한 모든 제안을 승인하는 롤업 인스턴스에 위임된다. 그러나 토큰 보유자는 이 기본 설정을 재정의하여, 자신의 주소를 포함한 어떠한 다른 주소로도 의결권을 재위임할 수 있다.

토큰 세일의 부차적인 목적은 Foundation이 비영리적 책무를 이행할 수 있도록 하는 데 있다. 여기에는 Aztec 프로토콜 및 관련 기술의 개발, 홍보, 채택을 지원하기 위한 부수적 지원을 제공하는 것과, Aztec 프로토콜을 사용하는 애플리케이션 및/또는 서비스에 대한 부수적 지원을 제공하는 것이 포함된다.

## 스테이킹 요건

Aztec의 지분증명(proof-of-stake, PoS) 네트워크에서는 시퀀서(Sequencer)로서 블록 생성에 참여하기 위해 최소 200,000 AZTEC의 스테이킹이 요구된다. 이 스테이크는 시빌 저항 메커니즘(sybil-resistance mechanism)으로서의 역할과 함께, 생성된 블록에 대한 경제적 보안을 제공한다. 시퀀서가 지속적으로 성과가 저조하거나 부정직하게 행동할 경우, 해당 시퀀서의 스테이크는 정직한 시퀀서들에 의해 슬래시(slashing)된다.

노드를 운영하기 위한 머신 요구 사항은 여기에서 확인할 수 있다.

이더리움 방식의 진입 큐(entry queue)는 정직한 시퀀서가 과도한 부담을 받지 않도록 방지하며, 출구 지연(exit delay)은 부정직한 시퀀서가 슬래시가 집행되기 전에 스테이크를 회수하는 것을 방지한다.

사용자는 스테이킹을 위해 직접 시퀀서를 운영할 필요가 없으며, 자신의 토큰과 의결권에 대한 완전한 통제권을 유지한 채 전문적인 제3자에게 시퀀서 운영을 위임할 수 있다. 전체 최소 요구량인 200,000 AZTEC보다 적은 수량으로 스테이킹하는 분할 스테이킹(fractional staking)은 Aztec에서 네이티브하게 지원되지 않지만, 제3자 프로토콜을 통해 가능해질 것으로 예상된다.

# 네트워크 수수료 및 블록 보상

Aztec에서 시간은 이산적인 “슬롯(slot)”으로 구분되며, 이는 다시 “에포크(epoch)”로 묶인다. 각 에포크마다 시퀀서(Sequencer)로 구성된 위원회가 무작위로 선정되어 블록 제안을 담당한다. 하나의 슬롯에는 해당 슬롯에 배정된 시퀀서의 가용성에 따라 블록 제안이 포함될 수도 있고 포함되지 않을 수도 있다. 생성된 각 블록은 Aztec의 스테이킹 집합이 제공하는 경제적 보안을 기반으로 하는 대기 체인(pending chain)에 추가된다.

대기 체인에 포함된 블록은 관련된 모든 거래의 정확성을 증명하는 유효성 증명(Validity proof)을 제출함으로써 이더리움(Ethereum) 상에서 최종 확정되어야 한다. 이러한 증명은 각 에포크가 종료되기 전까지 제출되어야 한다. 이더리움 상의 최종 확정성은 약 30분이 소요될 것으로 예상되며, 실행에 대한 사전 확인(pre-confirmation)은 Aztec의 거버넌스 설정에 따라 약 1~4초 이내에 제공될 수 있다.

시퀀서와 프로버(Prover, 이더리움 레이어 1에 게시되는 유효성 증명을 계산하는 주체)는 거래 수수료와 블록 보상을 통해 AZTEC으로 보상을 받는다. 시퀀서는 특정 슬롯에 대해 자신이 시퀀싱한 블록 집합이 증명되어 최종화된 체인에 추가될 때 AZTEC을 누적한다. 에포크에 대한 유효성 증명을 성공적으로 제출한 프로버 역시 서비스 품질에 따라 AZTEC을 누적한다.

체인의 라이브니스(liveness)를 보장하기 위해, 하나의 에포크에 대해 여러 개의 유효성 증명이 제출될 수 있다. 보상은 해당 에포크에서 가장 높은 연속 블록 구간을 최종화하는 각 증명을 제출한 주체에게 지급된다. 프로버의 독점을 방지하고 과점 구조를 유도하기 위해, 프로토콜은 초기 설정에서 에포크당 최소 두 개의 증명에 대해 사실상 보조금을 지급하도록 구성된다. 또한, 장기간에 걸쳐 지속적으로 에포크를 증명하는 프로버는 서비스 품질을 장려하기 위해 더 높은 보상 비중을 받게 된다. 반대로 프로버가 한 에포크를 놓칠 경우, 해당 프로버의 보상 비중은 신규 프로버 수준으로 감소하여, 일관된 증명 참여를 유도한다.

사용자는 거래 수수료를 직접 AZTEC으로 지불할 필요가 없다. Aztec은 독립적인 개발자가 배포한 수수료 지불 계약(Fee-Paying Contracts, FPCs)을 통해 네이티브 수수료 추상화 기능을 지원한다. FPC는 AZTEC 준비금을 유지하며, ETH나 USDC와 같은 다른 자산과의 환율을 관리한다. 사용자는 FPC가 지원하는 자산 중 하나를 제공할 수 있으며, FPC는 보유한 AZTEC 준비금을 사용해 시퀀서에게 수수료를 지불한다.

## 인플레이션

초기 토큰 분배의 일환으로 네트워크 보상에 해당하는 첫 1년치 물량이 사전 발행되었으며, 이에 따라 1년 차에는 AZTEC 총 공급량(Total Supply)의 2.41%에 해당하는 실질적인 연간 블록 보상이 적용된다. 처리량과 소각 마진이 증가함에 따라, 이러한 인플레이션은 자연스럽게 상쇄되며 디플레이션으로 전환될 수 있다(이더리움의 EIP-1559와 유사한 구조를 의도함). 첫 해 이후에는 Aztec 거버넌스를 통해 거버넌스 투표에 따라 네트워크 보상을 목적으로 신규 토큰을 발행함으로써 총 공급량을 조정할 수 있으며, 연간 최대 20%의 공급량 상한이 적용된다. 이 상한은 Aztec 거버넌스가 블록 보상을 위한 재원을 조성하고 비상 상황에 대응할 수 있도록 하면서도, 발행자 계약(issuer contract)의 악의적이거나 오류로 인한 과도한 토큰 발행을 방지하기 위한 제한으로 설정되었다.

이와 같은 절제된 인플레이션 비율은 시퀀서(Sequencer)에 대한 인센티브 제공과 네트워크 보안을 통해 탈중앙화를 유지하는 동시에, 장기적인 희석을 최소화하도록 설계되었다. 보다 광범위한 공급 일정의 맥락에서 보면, 팀 및 투자자 연락은 아래의 “토큰 공급 및 분배(Token Supply and Distribution)”에서 추가로 설명되듯이 점진적으로 이루어지며, 네트워크 활동과 수수료 규모의 증가와 맞물릴 것으로 예상된다. 통제된 인플레이션과 계획된 연락은 함께 토큰의 건전한 분배를 뒷받침하고, 네트워크 보안을 유지하며, 네트워크를 위한 지속 가능한 경제 구조를 강화한다.

## 대기 중 거래의 보안성

Aztec에서 최종 확정된 거래의 보안성은 각 에포크(epoch)에 대해 제출되는 유효성 증명(validity proof)을 통해 모든 거래가 암호학적으로 정확함이 입증됨으로써, 이더리움의 지분 증명(proof-of-stake, PoS) 네트워크로부터 제공된다. 대기 체인(pending chain)을 통해 제공되는 저지연 실행 사전 확인(pre-confirmation)은, 해당 에포크에 대해 무작위로 선정된 시퀀서(Sequencer) 위원회의 구성원 수에 기반한 최소 수준의 보안을 가진다. 시퀀서당 최소 스테이크가 200,000 AZTEC이고 위원회 크기가 48인 경우, 필요한 스테이크에 대한 대략적인 하한은  $\approx 33 \times 200,000 = 6.6M$  AZTEC으로 계산된다(조정 할인(coordination discounts)은 고려하지 않음).

## 수수료 메커니즘

Aztec은 연산 작업량을 마나(Mana) 단위로 계량하며, 이는 이더리움 레이어 1(Ethereum L1)의 “가스(gas)”에 대체로 상응한다. 사용자가 거래에서 소비되는 각 마나 단위에 대해 지불해야 하는 마나당 최소 수수료(AZTEC 기준)는 다음의 합으로 구성된다.

- I. 블록당 마나 목표치(Mana target)에 걸쳐 상각되는 레이어 1 게시 오버헤드(L1 posting overhead)
- II. 오라클(oracle)에 의해 보고되는 마나당 프로버 비용(Prover-cost-per-Mana)

마나당 최소 수수료는 보상 구성 요소와 혼잡 구성 요소로 이루어진다. 보상 구성 요소는 시퀀서(Sequencer)와 프로버(Prover)가 각 에포크(epoch) 종료 시 보상을 받기 전까지 각각 부담하는 비용을 상쇄하기 위한 것이며, 혼잡 구성 요소는 마진 또는 ‘프라이버시 프리미엄(Privacy Premium)’을 반영하도록 설정될 수 있다. 설정 가능한 마나 한도(Mana limit)와 마나 목표치(Mana target)를 기반으로, 프로토콜은 프로토콜 파라미터와 소각되는 혼잡 구성 요소를 구성할 수 있는 폭넓은 설정 권한을 부여한다.

## L2 블록에 대한 시퀀서 비용

시퀀서(Sequencer)가 부담해야 하는 L2 블록 제안에 대한 레이어 1(L1) 비용은 다음과 같다:

$$\begin{aligned} \text{Sequencer L1 cost per L2 block} = & (\text{L1\_GAS\_PER\_BLOCK\_PROPOSED} \\ & + \text{BLOBS\_PER\_BLOCK} * \text{POINT\_EVALUATION\_PRECOMPILE\_GAS}) \\ & * \text{wei\_per\_l1\_gas} \\ & + \text{BLOBS\_PER\_BLOCK} * \text{L1\_GAS\_PER\_BLOB} * \text{wei\_per\_l1\_blob\_gas} \end{aligned}$$

## L2 블록에 대한 프로버 비용

프로버(Prover)가 부담하는 L2 블록에 대한 레이어 1(L1) 비용이다. 여기서는 해당 계산을 위해 하나의 에포크(epoch)가 모두 사용된다고 가정한다. 일부 구성 요소는 상각되며(예를 들어, 제출 비용은 전체 에포크에 걸쳐 공유된다).

$$\begin{aligned} \text{Prover L1 cost per L2 block} = & \left\lceil \frac{\text{L1\_GAS\_PER\_EPOCH\_VERIFIED}}{\text{L2\_SLOTS\_PER\_L2\_EPOCH}} \right\rceil * \text{wei\_per\_l1\_gas} \\ & + \text{proving\_cost\_per\_mana} * \text{TARGET\_MANA\_PER\_BLOCK} \end{aligned}$$

## minimum\_fee 도출

제안자(proposer)가 L2 블록을 생성할 때, 시퀀서(Sequencer) 구성 요소와 프로버(Prover) 구성 요소, 그리고 혼잡 승수(congestion multiplier)를 계산하며, 이를 바탕으로 사용자가 부담해야 하는 기본 수수료(base fee)를 산출한다.

$$\begin{aligned} \text{sequencer cost per mana} &= \frac{\text{Sequencer L1 cost per L2 block}}{\text{TARGET\_MANA\_PER\_BLOCK}} \\ \text{prover cost per mana} &= \frac{\text{Prover L1 cost per L2 block}}{\text{TARGET\_MANA\_PER\_BLOCK}} \\ \text{minimum\_fee\_in\_wei} &= (\text{sequencer cost per mana} + \text{prover cost per mana}) \times \text{minimum fee congestion multiplier} \\ \text{minimum\_fee\_in\_fee\_asset} &= [\text{minimum\_fee\_in\_wei} \times \text{fee asset per wei}] \end{aligned}$$

이 최종 값은 L2 블록 헤더에 포함되는 minimum\_fee\_per\_mana 필드에 해당한다.

minimum\_fee는 ETH/Mana 단위로 계산되며, 시퀀서가 업데이트하는 AZTEC/ETH 환율 파라미터를 통해 온체인에서 AZTEC/Mana로 변환된다. 사용자는 수수료 지불 계약(Fee-Paying Contracts, FPCs)을 통해 ETH, USDC 등으로도 계속 수수료를 지불할 수 있으며, FPC는 AZTEC 준비금을 보유하고 변환을 처리한다. Aztec Network는 L2에서 수수료 전용 자산으로 AZTEC을 사용할 수 있도록 하는 단방향 정식 브리지(one way canonical bridge)를 지원한다.

## 토큰 이코노믹스(Token Economics)

다음 섹션에서는 점화 체인(Ignition chain) 및 알파(Alpha) 출시를 통해 Aztec의 이코노믹스를 살펴본다.

## 점화 체인의 이코노믹스(Economics of the Ignition Chain)

Aztec Network는 초기 단계에서 점화 체인과 함께 출시된다. 이는 머지(Merge) 당시 이더리움의 비콘 체인(Beacon Chain)과 유사하게, 탈중앙화된 시퀀서 집합을 부트스트랩하고 커뮤니티 주도의 거버넌스가 자리 잡을 수 있는 시간을 확보하는 것을 목적으로 한다. 이 단계에서는 사용자 거래가 처리되지 않는다.

시퀀서(Sequencer)와 프로버(Prover)는 위의 수수료 메커니즘(Fee Mechanism) 섹션에서 설명된 공식에 따라, 빈 블록을 사용해 대기 체인(pending chain)과 증명된 체인(proven chain)을 구축하는 데 비용을 부담한다.

(proven claim)를 구축하는 데 비용을 부담한다.

시퀀서 측면에서 하드웨어 비용은 비교적 낮으며, 1,000 달러 미만으로 충분히 조달 가능하다. 시퀀서를 운영하는 데 드는 주요 비용은 대기 체인에 블록을 제안하기 위해 이더리움 가스 수수료를 지불하는 것이다. 최근 평균 이더리움 가스 가격은 3 gwei였으며, EIP-7918 이후에는 블롭(blob) 가스 가격이 보수적으로 약 1 gwei 수준에서 형성될 것으로 예상된다. 점화 체인은 72초 슬롯을 사용하며, 에포크당 32개의 슬롯으로 구성된다. 각 제안된 블록은 대략 200,000 가스와 1개의 블롭(이는  $2^{17}$  블롭 가스에 해당함)을 소모한다.

따라서 시퀀서는 블록당 다음과 같은 ETH 비용을 지불한다.

$$\frac{(2^{17} \times 1) + (200000 \times 3)}{10^9} = 0.000731072 \text{ ETH}$$

1 ETH = \$4,500이라고 가정하면,

$$\text{블록당 USD 비용} = \$4500 \times 0.000731072 = \$3.29$$

연간 슬롯 수가 438,055개임을 고려하면, 이는 연간 비용 \$1,441,203에 해당하며, 해당 비용은 시퀀서 집합 전체에 균등하게 분배된다.

프로버(Prover) 측면에서도, 프로버는 자신의 증명을 온체인에서 검증받기 위해 이더리움 가스를 지불해야 하며, 이는 유효성 증명(validity proof) 1건당 약 250만 가스가 소요된다. 연간 13,689개의 에포크(epoch)를 기준으로 할 때, 이는 프로버 1인당 연간 비용 462,000 달러에 해당한다. 프로토콜은 초기 설정에서 에포크당 최소 2개의 증명이 생성되도록 사실상 보조금을 지급하도록 구성되며, 이에 따라 프로토콜이 부담하는 총 증명 비용은 \$923,900이 된다.

거버넌스는 블록 보상(Block Reward)의 규모와, 그중 시퀀서에게 지급되는 비율을 모두 설정할 수 있는 권한을 가진다. 아래의 “토큰 공급 및 분배(Token Supply and Distribution)” 섹션을 기준으로 볼 때, 점화(Ignition) 단계에서 전체 토큰 공급량 중 최대 20%가 스테이킹될 것으로 가정하는 것이 합리적이다.

가상의 예시로,

AZTEC의 완전 희석 가치(FDV)가

500M 인 경우, 거버넌스는 블록 보상을 615 AZTEC (FDV 기준 29.71에 해당)으로 설정할 수 있으며, 이 중 92.5%를 시퀀서에게 지급하도록 할 수 있다. 이 경우 모든 시퀀서 비

용이 회수될 뿐만 아니라, 스테이킹된 AZTEC에 대해 연 10%의 수익률이 제공되면서도 연간 인플레이션율은 2.47%로 유지된다. 이러한 가정하에서는 프로버에게 연간 **976,000 이분배된다. 이분식은 ETH 가격이 10,000까지 상승하더라도** 유효하나, 이 경우 인플레이션율은 3.05%로 상승하게 된다. 전체 모델은 Github<sup>3</sup>에 공개되어 있으며, 사용자가 자체적인 시나리오를 실행할 수 있도록 설정 가능하다.

점화 단계에서의 실제 파라미터는 거버넌스 결정에 따라 변경될 수 있다.

## 알파 단계의 이코노믹스(Economics at Alpha)

알파 단계에서는 인플레이션이 아닌 수수료가 운영자의 주요 수익원이 되는 것을 목표로 하며, 이는 다음의 예시를 통해 가장 잘 설명된다. 마나(Mana)는 Aztec 거래가 측정되는 작업 단위로, EVM의 가스(gas)에 대응한다. 블록에는 마나 목표치(Mana target)와 마나 한도(Mana limit)가 존재한다. 가득 찬 블록, 즉 마나 목표치를 초과하는 마나를 사용하는 거래를 포함한 블록의 경우, 다음 블록에서 혼잡 승수(congestion multiplier)를 최대 12.5%까지 증가시켜 최소 수수료(minimum\_fee)를 인상하며, 이로 인해 순 토큰 발행량이 자동으로 감소한다. 이 최소 수수료는 소각된다.

Aztec 거버넌스는 단순 송금 기준 사용자 비용을 약 0.05 0.15 수준(초당 5~10 TPS)으로 목표 설정하면서도, 우선순위 수수료(priority fees)를 통해 운영자에게는 양의 마진을 유지하도록 이코노믹스를 구성할 수 있다.

MEV. 블록이 지속적으로 마나 목표치(Mana target)를 초과할 경우, 거버넌스는 인센티브를 훼손하지 않으면서 처리량을 확장하기 위해 해당 목표치를 상향 조정할 수 있다.

거래에서 수수료로 지불되어야 하는 AZTEC의 양은 해당 거래의 마나 비용에 현재의 “마나당 최소 수수료(minimum fee per mana)”, 또는 간단히 “minimum\_fee”를 곱한 값이다. minimum\_fee는 여러 구성 요소로 계산되며, 시퀀서(Sequencer) 구성 요소, 프로버(Prover) 구성 요소, 그리고 혼잡 승수(congestion multiplier)로 이루어진다.

시퀀서 구성 요소는 먼저 ETH/Mana 단위로 다음과 같이 계산된다.

$$\frac{(200,000 \times \text{L1BaseFee}) + (\text{BlobsPerBlock} \times 2^{17} \times \text{L1BlobFee})}{\text{TARGET\_MANA\_PER\_BLOCK}}$$

마찬가지로, 프로버 구성 요소 역시 ETH/Mana 단위로 먼저 계산된다.

$$\frac{2 \times 2,500,000 \times \text{L1BaseFee}}{\text{SlotsPerEpoch} \times \text{TARGET\_MANA\_PER\_BLOCK}} + (\text{ProverCostPerMana})$$

첫 번째 항은 이더리움 상에서 증명을 게시하고 검증하는 데 필요한 프로버 2명의 마나당 비용을 포함한다. ProverCostPerMana는 wei 단위로 표시되며, 거버넌스에 의해 설정될 수 있고, Aztec 블록을 증명하는 실제 비용의 동학에 수수료 메커니즘이 대응할 수 있도록 한다. 이는 블록이 더 많은 마나를 포함할수록 증가하며, 하드웨어와 증명 시스템이 개선될수록 감소한다.

혼잡 승수(congestion multiplier)는 다음과 같이 정의되는 누적 값이다.

$$\text{excess mana} = \begin{cases} 0 & \text{if parent.excess + parent.spent} < \text{TARGET\_MANA\_PER\_BLOCK} \\ \text{parent.excess + parent.spent} - \text{TARGET\_MANA\_PER\_BLOCK} & \text{otherwise} \end{cases}$$

마나당 최소 수수료 혼잡 승수(minimum fee congestion multiplier)는 다음과 같이 정의된다.

$$\text{minimum fee congestion multiplier} = \text{MINIMUM\_CONGESTION\_MULTIPLIER} \times \exp\left(\frac{\text{excess mana}}{\text{CONGESTION\_MULTIPLIER\_UPDATE\_FRACTION}}\right)$$

MINIMUM\_CONGESTION\_MULTIPLIER가 1 이상( $\geq 1$ )으로 설정될 경우, 이는 프라이버시 프리미엄(Privacy Premium) 또는 시퀀서 마진(Sequencer margin)으로 작용한다는 점에 유의해야 한다. 만약 해당 값이 1로 설정되고 excess\_mana가 존재하지 않는다면, 이는 블록을 제안하고 검증하는 데 필요한 ETH 비용만을 단순히 총당한다. 알파(Alpha) 단계에서는 이 프리미엄이 거버넌스에 의해 조정되거나, 예를 들어 지속적으로 가득 찬 블록과 같은 상황에 반응하는 자기 조정(self-governing) 메커니즘을 사용할 수 있을 것으로 예상된다.

지수 함수 형태는 블록 간 혼잡 승수가 약 12.5%를 초과하여 변동하지 않도록 제한한다.

사용자가 AZTEC으로 지불하는 마나당 최종 유효 최소 수수료(effective minimum fee per Mana)를 계산하기 위해, 시퀀서에 의해 유지되는 AZTEC과 ETH 간의 현재 환율이 사용되며, 이는  $\alpha$ 로 표기된다. 이후 다음과 같이 계산된다.

$$\text{Effective Minimum Fee (\$AZTEC/mana)} = \alpha \times \text{Minimum Fee Congestion Multiplier} \times$$

따라서 사용자의 거래가 10 마나를 소비하는 경우, 추가될 수 있는 우선순위 수수료(priority fee)를 제외하면, 사용자가 지불하는 총 AZTEC 수수료는 유효 최소 수수료의 10배가 된다. 다만, 혼잡 승수로 인해 발생한 수수료의 일부는 소각되며, 이는 누구도 접근할 수 없고 회수 불가능한 주소로 전송됨을 의미한다. 블록이 마나 목표치(Mana target)를 초과하여 마나를 소비할 경우, 또는 거버넌스가 MINIMUM\_CONGESTION\_MULTIPLIER를 1보다 크게 설정한 경우, 해당 수수료는 소각된다.

이에 따라 시퀀서는 거래를 블록에 포함시켜 마나 목표치를 달성하도록 항상 유인되는데, 이는 해당 거래들로부터 기본 수수료(base fee)의 자신에게 할당된 몫을 수취하기 때문이다. 동시에 시퀀서는 마나 목표치를 초과하도록 블록을 확장하고 소각을 발생시켜, 우선순위 수수료(priority fees)와 MEV 기회를 확보하도록 유인된다. 마나 목표치가 지속적으로 달성되거나 초과되는 경우, 거버넌스에 의해 해당 목표치는 상향 조정될 수 있다.

예를 들어, 알파(Alpha) 단계에서 한 개발자가 관련 법률을 모두 준수하면서도, 이더리움의 \$500억 규모 생태계로의 프라이빗 브리징(private bridging)을 Venmo나 Revolut만큼 매끄럽게 만드는 애플리케이션을 배포했다고 가정하자.

- 은행 계정으로 로그인하여 Aztec으로 온램프(onramp)한다 - 지갑이 필요 없다.
- Aztec의 계정 추상화(account abstraction)를 통해 에스크로 계약(escrow contract)에서 자금을 수령한다.
- 에스크로에서 크로스체인 브리지(cross chain bridge)로 자금을 이동하며, 수수료 추상화(fee abstraction)로 가스를 직접 다룰 필요가 없다.
- 퍼미션리스 KYC 검사(permissionless KYC check)를 통해 Arbitrum에서 Aave에 예치(lend)한다.

사용자가 지불하는 비용이 약 0.15 이하라고 가정하면, 초당 10건을 초과하는 거래 수요가 존재할 것이라고 상상하기는 쉽다. Aztec이 72초 슬롯과 에포크당 32개 슬롯으로 운영된다고 가정하고, 평균 거래가 블롭(blob) 1,200바이트를 소비하며, Aztec Network가 초당 평균 10건의 거래를 처리하고, 블록이 1,500만 마나(15M mana)의 마나 목표치(Mana target)에도 달한다고 가정하자. 또한  $1 \text{ ETH} = 4,500$ , *AZTEC*의 완전회석가치(FDV)는 500M, 이더리움 가스 가격은 3 gwei, 블롭 가스는 1 gwei라고 가정하자.

이는 제안된 블록 하나가 다음을 소비함을 의미한다.

$$\left\lceil \frac{10 \times 72 \times 1200}{4096 \times 32} \right\rceil = 7 \text{ blobs}$$

그리고 각 거래는 다음을 소비한다.

$$\frac{15 \times 10^6}{10 \times 72} = 20,833 \text{ mana}$$

위의 수수료 방정식은 부과되는 `minimum_fee`를 계산하는 데 사용할 수 있다. 시퀀서 구성 요소(Sequencer component)는 다음과 같다.

$$\frac{(200,000 \times 3 \times 10^{-9}) + (7 \times 2^{17} \times 1 \times 10^{-9})}{15 \times 10^6}$$

그리고 프로버(Prover) 구성 요소는 다음과 같다.

$$\frac{2 \times 2,500,000 \times 3 \times 10^{-9}}{32 \times 15 \times 10^6} + \text{ProverCostPerMana}$$

프라이버시 프리미엄(Privacy Premium)을  $3 \times 10^6$ 으로, `ProverCostPerMana`를 0으로 설정하면, ETH/Mana 기준 `minimum_fee`는  $7.32 \times 10^{-10}$ 이 된다.

이로부터 사용자의 거래 수수료를 달러 기준으로 계산할 수 있으며, 이는 다음과 같다.

$$\$4,500 \times 20,833 \times 7.32 \times 10^{-10} = \$0.0687$$

이는 프로토콜에 연간 \$21.67M의 수익을 창출한다.

프라이버시 프리미엄이 0으로 설정될 경우, 기본 수수료(base fee)는 거래당 \$0.012가 되며, 이는 시퀀서가 블록을 게시하기 위해 부담하는 비용을 정확히 총당하는 수준임을 유의할 필요가 있다.

알파(Alpha) 단계에서 토큰 총 공급량(Total Supply)의 50%가 스테이킹된다고 가정하자. 이러한 조건하에서 거버넌스는 블록 보상을 427 AZTEC(또는 \$20.28)으로 낮출 수 있으며, 시퀀서는 운영 비용이 상환된 이후에도 스테이킹된 AZTEC에 대해 달러 기준 연 10%의 수익률을 여전히 확보할 수 있다. 이 경우 연간 인플레이션율은 1.78%로 하락한다.

이 수수료 모델의 흥미로운 측면은 프라이버시 프리미엄이 0이 아닐 경우, 이더리움 가스 가격과 ETH 가격이 상승함에 따라 시퀀서와 프로버가 달러 기준으로 더 많은 수수료를 수취하게 된다는 점이다. 동일한 분석은 ETH 가격이 10,000 달러인 경우에도 적용될 수 있으며, 이 경우 시퀀서는 블록 보상을 0으로 설정하더라도 여전히 연 10%의 수익률을 확보할 수 있고, 12.8M

의 잔여 금액이 남게 된다. 이더리움 가스 가격이 7 gwei까지 상승하는 경우에도 유사한 시나리오가 전개된다. 두 경우 모두에서 사용자의 거래당 비용은 약 0.15 달러 수준을 유지한다. 이러한 상황에서 거버넌스는 사용자 수수료를 낮추기 위해 프라이버시 프리미엄을 줄이거나, minimum congestion multiplier를 증가시키는 선택을 할 수 있다. 만약 \$12.8M 전액을 소각하기로 선택할 경우, 이는 연간 2.56%의 디플레이션(deflation)을 초래하게 된다.

## 토큰 공급 및 분배(Token Supply and Distribution)

제네시스 시점의 AZTEC 총 공급량은 10,350,000,000(“총 공급량(Total Supply)”)이며, 아래의 차트와 표에 설명된 범주로 분배된다.

이 토큰들은 별도 명시가 없는 한 락업을 강제하기 위해, 이더리움 상의 토큰 금고(Token Vaults)로도 알려진 Aztec 토큰 포지션 계약(Aztec Token Position contracts, “ATPs”)에 보관된다.

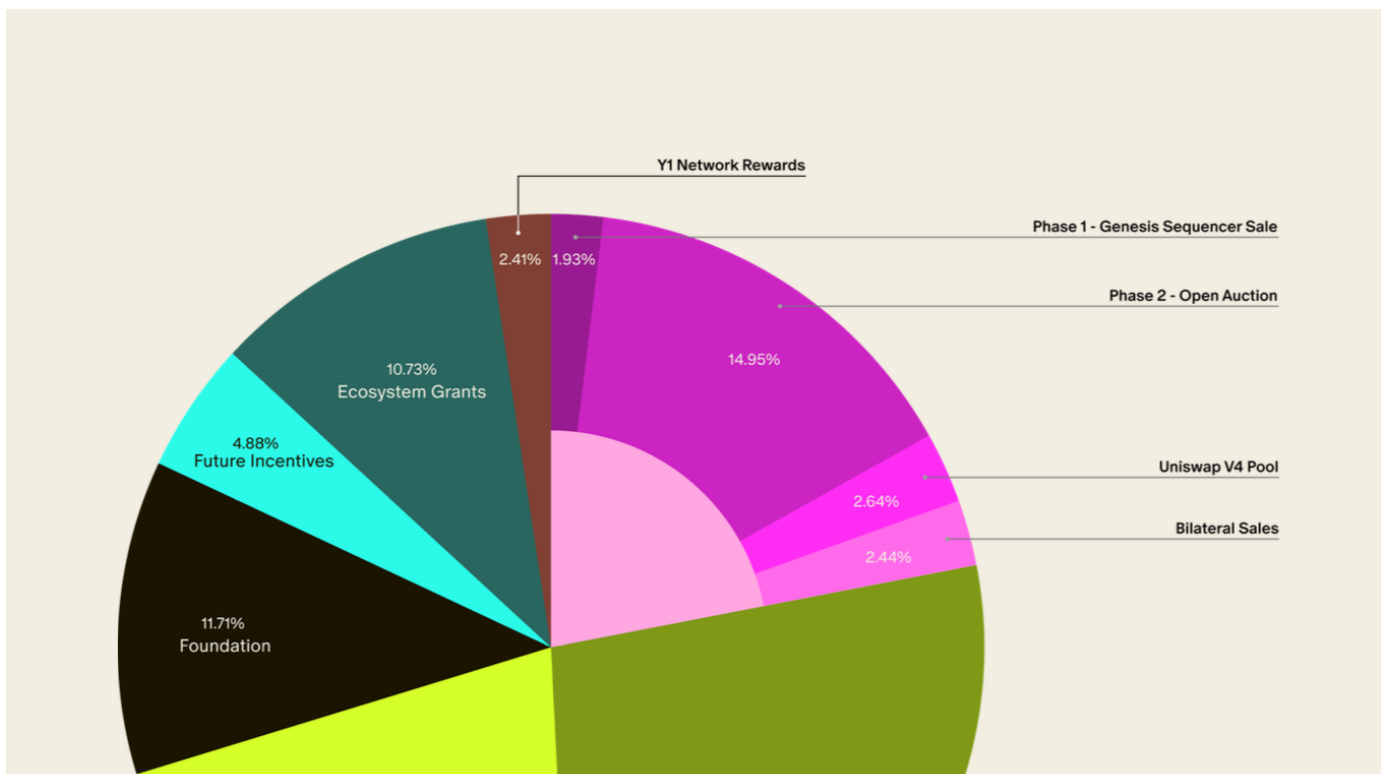
ATP는 다음 중 하나 이상을 가능하게 하도록 구성할 수 있는 유연한 계약이다.

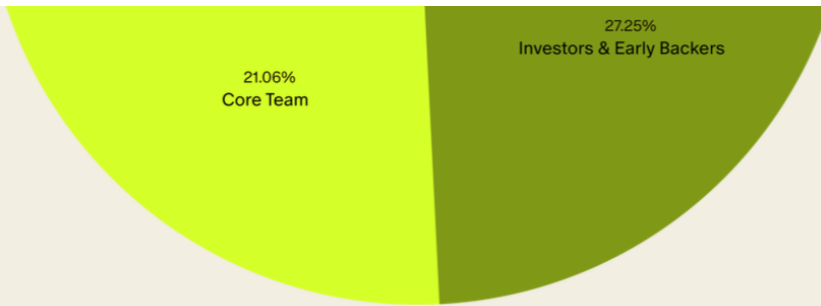
- 특정 날짜까지 ATP 내에서 토큰을 락업
- 특정 날짜까지 Aztec에서 토큰을 스테이킹
- ATP 내 토큰을 Aztec 거버넌스에 참여시키는 기능
- 특정 날짜 도달 이후 토큰을 점진적으로 언락
- 오프체인 이벤트에 대응하여 토큰을 언락
- 오프체인 이벤트에 대응하여 토큰을 회수(revoke)

Aztec Labs의 투자자 및 직원에게 배분되는 토큰은 점화 체인(Ignition chain) 출시 시점을 기준으로, 12개월 락업 이후 24개월에 걸친 선형 언락을 강제하는 ATP에 배분된다. 또한 이러한 ATP는 토큰 세일(Token Sale) 시작 이후 최초 12개월 동안 스테이킹과 거버넌스 참여를 제한하는 규칙도 함께 적용한다.

퍼블릭 세일에서 판매된 모든 토큰은 취소 불가능하며, 12개월 락업이 적용된다. 해당 락업 기간은 거버넌스 투표를 통해 최소 90일까지 단축될 수 있다. 정확한 락업 기간은 위에서 설명한 바와 같이 거버넌스 투표를 통해 결정된다. 초기 토큰 보유자는 토큰 세일 또는 스테이킹에 따른 블록 보상을 통해 토큰을 취득했으므로, 거버넌스는 최소 락업 기간을 선호할 것으로 예상하는 것이 합리적이다.







| Category   | Description                                                                                                  | %            | Token Amount                                                                                    | Owned By Whom Post-Ignition? |
|------------|--------------------------------------------------------------------------------------------------------------|--------------|-------------------------------------------------------------------------------------------------|------------------------------|
| Token Sale | <b>Total:</b><br>Sold by the Foundation through the following sales on or around Ignition (as defined below) | <b>21.96</b> | <b>2,272,500,000</b><br>(At Ignition (as defined below), owned by Token holders and Foundation) |                              |
|            | <b>Phase 1 – Genesis Sequencers Sale:</b>                                                                    | 1.93         | 200,000,000                                                                                     | Token holders                |

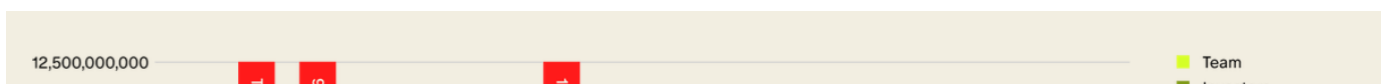
|  |                                                                                                                     |       |               |                                            |
|--|---------------------------------------------------------------------------------------------------------------------|-------|---------------|--------------------------------------------|
|  | onboard early network Sequencers.                                                                                   |       |               |                                            |
|  | <b>Phase 2 – Open Auction:</b><br>broaden participation among current and future Aztec users                        | 14.95 | 1,547,000,000 | Token holders participating in this offer. |
|  | <b>Uniswap V4 Liquidity Pool:</b><br>in connection with the “Phase 2 - Open Auction” the Foundation will contribute | 2.64  | 273,000,000   | Liquidity Pool owned by Aztec governance   |

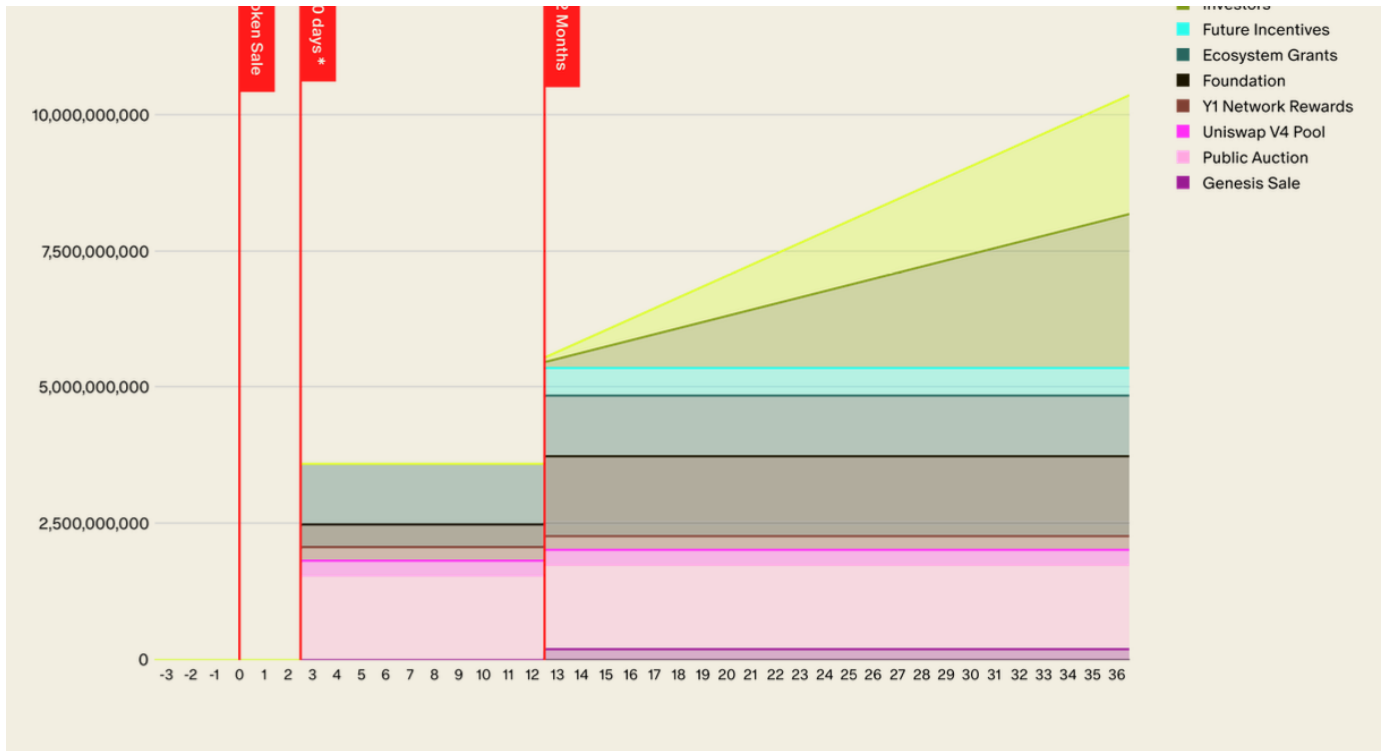
|                  |                                                                                                                                      |       |               |                                                                                                                          |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------|-------|---------------|--------------------------------------------------------------------------------------------------------------------------|
|                  | 273,000,000 Tokens to the auction contracts, that will be transferred autonomously to a Uniswap V4 pool upon completion of the sale. |       |               |                                                                                                                          |
|                  | <b>Bilateral Sales</b><br>- reserved for sale by the Foundation to strategic investors to benefit the ecosystem                      | 2.44  | 252,500,000   | Foundation. No bilateral sales are currently expected in 2025, but may be conducted at the Foundation's sole discretion. |
| Ecosystem Grants | The Foundation intends to allocate Tokens to certain                                                                                 | 10.73 | 1,111,000,000 | Grant recipients (~10.61%)<br>Foundation                                                                                 |

|                    |                                                                                                                                                                    |       |               |                  |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------------|------------------|
|                    | non-insider early contributors, community members, and aligned individuals, the majority of which will have been distributed and allocated by the Token Sale date. |       |               | (~0.12%)         |
| Future Incentives  | Controlled by Aztec governance; examples of usage include boosted rewards distributed over 24 months after Ignition (as defined below) or liquidity mining.        | 4.88  | 505,000,000   | Aztec governance |
| Y1 Network Rewards | Pre-minted first year staking and proving rewards.                                                                                                                 | 2.41  | 250,000,000   | Aztec governance |
| Foundation*        | Allocation to the                                                                                                                                                  | 11.71 | 1,211,500,000 | Foundation       |

|                           |                                                                                                           |             |                              |           |
|---------------------------|-----------------------------------------------------------------------------------------------------------|-------------|------------------------------|-----------|
|                           | Aztec Foundation to support ecosystem initiatives such as protocol ops, research, grants and partnerships |             |                              |           |
| Investors & Early Backers | Early supporters of Aztec                                                                                 | 27.25       | 2,820,330,869                | Labs      |
| Team                      | Members of Aztec Labs and the Aztec Foundation                                                            | 21.06       | 2,179,669,131                | Core Team |
| <b>Total:</b>             |                                                                                                           | <b>100%</b> | <b>10,350,000,000 Tokens</b> |           |

토큰 세일(Token Sale) 시점 전후로, Foundation은 초기 총 공급량의 최대 약 14.27%에 해당하는 1,477,455,000개의 토큰을 보유하게 될 것으로 예상된다. Foundation이 내부 정책에 따라 언락된 토큰을 보유하게 되는 범위 내에서는, Foundation은 Aztec 거버넌스에 참여하지 않는다.





핵심 팀(core team)의 언락은 위 일정에 따라 진행되지만, 이는 개별적인 로드맵 마일스톤에 종속된다. 해당 마일스톤이 지연될 경우, 핵심 팀 토큰은 계속해서 락업 상태로 유지된다. 위 차트는 가장 공격적인 언락 일정을 보여준다.

## Uniswap V4 풀(Uniswap V4 Pool)

토큰 세일은 경매에 할당된 토큰의 최대 15%(총 공급량의 약 2.64%에 해당)와, 경매의 최종 청산 가격(final clearing price)을 기준으로 매칭되는 ETH를 사용하여, Uniswap V4 유동성 풀을 자동으로 생성한다. 경매 스마트 컨트랙트는 ETH로 조달된 자금의 일부를 사용해 전 범위 유동성 풀(full range liquidity pool)을 구축한다.

LP 포지션은 Aztec 거버넌스가 소유하며, 초기에는 해당 풀을 통한 거래가 비활성화된다. 거래 활성화는 거버넌스 투표를 통해서만 가능하며, 이는 토큰 세일 날짜로부터 최소 90일 이후에만 이루어질 수 있다.

경매의 최종 청산 가격이 **750M** 일 경우, 해당 풀에는 약 20M 상당의 ETH와 \$20M 상당의 Aztec 토큰이 포함되며, 이는 V4 풀 기준 상위 10위권에 해당하는 규모가 된다.

이 풀은 거버넌스 투표에 따라, V4 훅(hook)을 통해 발생하는 LP 수수료를 토큰 바이백(token buyback)으로 전환하도록 구성될 수 있다.

## 면책 조항(Disclaimers)

연구 거즈자에 대한 정보(Information for Persons in the IIC).

영국 거주자에게만 제공되는 정보 (INFORMATION FOR PERSONS IN THE UK).

본 커뮤니케이션은 영국 외 지역의 개인만을 대상으로 한다. 영국 거주자는 토큰 세일에 참여할 수 없으며, 본 커뮤니케이션을 근거로 어떠한 행위도 해서는 안 된다.

할인 가격 관련 면책 조항(Discount Price Disclaimer):

이전 평가액 또는 할인율에 대한 언급은 토큰 세일의 초기 최저 가격이 어떻게 산정되었는지를 잠재적 구매자에게 설명하기 위한 목적에 한해 제공된다. 지분 투자(financing) 평가액은 본 토큰 제공과 비교할 수 없는 특정한 상황에서 산정된 것이다. 이는 토큰의 현재 또는 미래 시장 가치를 나타내지 않으며, 잠재적 수익에 대한 지표로 의존되어서는 안 된다. 토큰 가격은 크게 변동할 수 있고, 토큰은 일부 또는 전부의 가치를 상실할 수 있으며, 구매자는 과거 평가액에 의존하지 않고 독립적인 판단을 내려야 한다. 어떠한 구매자도 수익을 실현하거나 구매 대금을 회수할 수 있다는 보장이나 진술은 제공되지 않는다.

MiCA 면책 조항(MiCA Disclaimer):

본 가상자산 마케팅 커뮤니케이션은 유럽연합(EU) 회원국 내 어떠한 관할 당국에 의해서도 검토되거나 승인되지 않았다. 본 가상자산 마케팅 커뮤니케이션의 내용에 대한 책임은 전적으로 가상자산의 제공자에게 있다. Aztec Foundation은 토큰 세일과 관련하여 MiCA를 준수하는 백서를 발행하였으며, 이는 여기에서 확인할 수 있다.

기능 관련 면책 조항(Functionality Disclaimer):

프라이빗 실행 환경(Private Execution Environment) 또는 협업 증명(collaborative proving)을 포함하여, Aztec 내 수수료 구조에 영향을 미치는 어떠한 특정 기능도 출시 시점 또는 특정 기간 내에 제공될 것이라는 보장은 없다. 이는 이코노믹스 분석에 영향을 미칠 수 있다.