Aztec Token Economics

AZTEC

Introduction

More than a decade after the launch of Bitcoin (2008) and Ethereum (2014), the impact of blockchains on global finance and commerce remains muted. The problem is not scalability or usability alone. Instead, it is enforced transparency–once seen as a virtue–which has turned out to be a roadblock for mainstream adoption.

The Internet had to cope with a similar bottleneck in the 1990s. To transition from enthusiasts to mass-market adoption, users needed guarantees that their online transactions and information were private and secure. The breakthrough came with two cryptographic infrastructure innovations - SSL and HTTPS - that unleashed the commercialization era of the Internet, unlocking trillions in value.

Aztec's programmable privacy is SSL for blockchains – the missing feature that makes blockchain ready for real-world adoption.

Aztec began in 2017 with a simple goal: to bring real-world assets to blockchains. Our early attempts to tokenize private debt exposed the core limitation of transparent ledgers – no institution wanted its portfolios and trade data immutably published onchain. Since then, Aztec has been singularly focused on solving this problem: developing the cryptographic infrastructure needed to make programmable onchain privacy possible.

Over the past eight years, Aztec has delivered multiple foundational innovations – from the first private transfer system on Ethereum (2018)[1], to PLONK (2019), the performant universal SNARK[2], and Noir, the universal zero-knowledge language. The Aztec Network is the culmination of all of our work - a zk-SNARK-based privacy and scaling L2 built on Ethereum that brings together privacy, scalability, and full programmability through Noir and Aztec.nr, our smart-contract framework.

The Aztec Network is designed to serve a wide range of stakeholders – including developers, institutions, and individual users globally – each with different expectations and needs. Aztec is built to be maximally neutral and verifiable at the protocol level, while giving users strong control and privacy at the application level. The network is decentralized from day one, ensuring all of these stakeholders' needs can be met with no single entity to dictate the network's evolution.

---

[1] https://github.com/AztecProtocol/aztec-v1/blob/develop/AZTEC.pdf

[2] https://eprint.iacr.org/2019/953

At the heart of this network is the $AZTEC token, the native asset powering this decentralized privacy layer:

- Staking: The Token secures the network through staking by Sequencers, who are responsible for block production within Aztec. Sequencers must stake the Token to obtain the right to propose blocks and may receive block rewards in the form of Tokens when a block they propose is successfully proven on Ethereum L1.
- Governance: Sequencers and tokenholders participate in onchain governance to manage upgrades, parameters, and token economics.
- User Fee Market: The Token will serve as a medium for transaction fees within the Aztec Network allowing inflation and deflation depending on demand for block space, if and when the execution environment is enabled.

The Aztec Token

The Aztec Network leverages a proof-of-stake (PoS) system to decentralize block production and give economic security to a fast pre-confirmation pending chain before finality ("Aztec Network" or "Aztec"). Aztec's native asset, ("$AZTEC" or "Token"), is at the core of this mechanism: it will be used to secure the Aztec Network through staking by Aztec Sequencers on Ethereum (L1), also known as "Sequencers" ("Sequencers"), who will be responsible for the production of blocks within Aztec. The Token is minted as an incentive to propose and prove blocks, it must be paid by users for transaction fees, and it is the measure of voting power in Aztec's Governance System.

$AZTEC is issued as an ERC-20 token on Ethereum. It is immutable and has no privacy preserving features. Through the Governance System, $AZTEC holders have control over Aztec Network upgrades and the tokenomics of $AZTEC. They can mint the Token, set the maximum inflation rate, set block production rewards, and configure parameters used in the transaction fee calculations. $AZTEC's Governance System, and Rollup are all deployed to Ethereum.

Launching Decentralized

Rollups on Ethereum have proliferated in part to reduce transaction fees for users. However, most take a "progressive" approach to decentralization, and run a centralized company-owned Sequencer that ultimately controls the network. By contrast, Aztec is

setting a new standard for how decentralized protocols should launch: completely decentralized block production and a token with utility, governance and sound economics.

As a decentralized network, Aztec ensures that no single party can censor transactions, compromise privacy, or determine governance outcomes. Control of the Aztec Network is distributed among independent actors, making Aztec a genuinely neutral public good that anyone can verify, participate in, and build upon. This neutrality is the foundation for broad adoption as users must have confidence that the infrastructure they depend on cannot be co-opted, seized, or corrupted, and that no central operator can bias the system or act against their interests.

To cement the credible decentralization of the Aztec Network, the Aztec Foundation and Aztec Labs employees and investors will be prevented from participating in staking and governance for one year post-launch, ensuring that control rests in the hands of the community, rather than any specific entity.

Alongside the Aztec Network launch, the Aztec Foundation is distributing Tokens to the community via a novel token sale on Ethereum ("Token Sale"). The Token Sale will use a continuous clearing auction, which dynamically adjusts pricing based on demand, ensuring transparent price discovery and fair allocation. The auction will sell up to 14.95% of Total Supply (as defined below) with a floor price of $350M fully diluted valuation ("FDV"), representing approximately a 75% discount to the most recent implied network valuation based on Aztec Labs' latest equity financing.

The primary goal of the Token Sale is to distribute the Token Total Supply among node operators, ecosystem contributors, and the broader community to enable them to stake the Token, run the Aztec Network and participate in the Aztec governance.

Aztec governance allows Sequencers to initiate proposals related to certain network parameters and network upgrades. Once a proposal has sufficient support, expressed by Sequencers through an on-chain signaling mechanism, it advances to the ratification stage. Tokenholders will then be able to vote on proposals by locking Tokens for the duration of the vote. By default, when Tokens are staked, the associated voting rights are delegated to a rollup instance that votes to approve all proposals that pass Sequencer signalling. However, a tokenholder may override this default by redelegating their voting rights to any other address, including their own.

The secondary goal of the Token Sale is to enable the Foundation to fulfill its non-profit mandate. This includes providing ancillary support for the development, promotion and

adoption of the Aztec protocol and related technologies, and providing ancillary support for applications and/or services using the Aztec protocol.

Staking Requirements

Aztec's proof of stake network has a minimum stake of 200,000 $AZTEC, required to participate in block production as a Sequencer. The stake serves as both a "sybil-resistance mechanism", and economic security for blocks produced; if a Sequencer is consistently underperforming or dishonest, its stake will be slashed by the honest Sequencers.

Machine requirements for running a node can be found here.

An Ethereum-style entry queue prevents honest Sequencers from being overwhelmed, and an exit delay prevents dishonest Sequencers from retrieving their stake before a slash can be enacted.

Users do not need to run a Sequencer themselves in order to stake; they can delegate the operation of their Sequencer to a professional third-party while retaining full control of their tokens and voting rights. Fractional staking, that is staking with less than the full minimum 200,000 $AZTEC required to run a Sequencer, is not supported natively in Aztec, but is expected to be possible via third-party protocols.

Network Fees and Block Rewards

Time in Aztec is divided into discrete "slots", which are grouped into "epochs". Each epoch, a committee of Sequencers is randomly selected and tasked with proposing blocks. A slot may or may not have a block proposal associated with it, depending on the availability of the Sequencer which was assigned that slot. Each block produced gets added to a pending chain backed by the economic security of the staking set of Aztec.

Blocks included in the pending chain must be finalized on Ethereum through the submission of a validity proof that proves correctness of all relevant transactions. These proofs must be submitted by the end of any given epoch. Ultimate finality on Ethereum is expected to be ~30 minutes, whilst execution pre-confirmations can be given as quickly as 1-4 seconds depending on the governance configuration of Aztec.

Sequencers and Provers (who compute the validity proofs posted to Ethereum layer 1) are compensated for their services in $AZTEC via transaction fees and a block reward. Sequencers accrue $AZTEC when the set of blocks they sequenced for a given slot is proven

and added to the finalised chain. Provers who successfully submit a validity proof for an epoch also accrue $AZTEC depending on their quality of service.

Multiple validity proofs may be submitted for any epoch to ensure liveness of the chain. Rewards are paid to the submittors of validity proofs for an epoch, for each proof that finalizes the highest consecutive block range. To encourage an oligopoly rather than a monopoly of Provers, the protocol is initially configured to effectively subsidize at least two proofs per epoch and Provers who consistently prove epochs over time will receive a higher share of the reward to encourage quality of service. If a Prover misses an epoch, their share of the reward reduces to that of a new Prover, incentivising consistent proving.

Users do not need to pay for their transactions in $AZTEC directly. Aztec supports native fee abstraction through Fee-Paying Contracts (FPCs) deployed by independent developers. FPCs maintain a reserve of $AZTEC and exchange rates with other assets such as ETH or USDC. Users can provide one of the supported assets to the FPC, which uses its reserve of $AZTEC to pay the Sequencer.

Inflation

The first year's worth of network rewards has been pre-minted as part of the initial Token distribution giving an effective annual block reward of 2.41% of the $AZTEC Total Supply in year 1. As throughput and burned margin grow, this inflation is naturally offset and can turn deflationary (intended to be similar to Ethereum's EIP-1559). After the first year, Aztec governance will have the ability to adjust the Total Supply by minting new Tokens for network rewards through governance votes, up to a maximum cap of 20% of supply annually. This cap has been set to ensure that Aztec governance can create funds for block rewards and respond to any contingency, but still impose a limit to prevent malicious or bugged use of the issuer contract to mint an excessive amount of Tokens.

This modest inflation rate is designed to sustain decentralization by incentivizing Sequencers and securing the network, while minimizing long-term dilution. In the context of the broader supply schedule: team and investor unlocks (described further below in "Token Supply and Distribution") are gradual and expected to align with increased network activity and fee volume. Together, controlled inflation and scheduled unlocks support the healthy distribution of Tokens, maintain network security, and strengthen sustainable economics for the network.

Security of pending transactions

Aztec's security for finalized transactions comes from Ethereum's proof of stake network due to the validity proof that is submitted for each epoch, proving all transactions are correct cryptographically. Low latency execution pre-confirmations given by the pending chain have a minimum security based on the number of Sequencers in the randomly selected committee for a given epoch. With a minimum stake 200,000 $AZTEC per Sequencer and committee size of 48, a back-of-envelope bound for stake required is ≈ 33 × 200,000 = 6.6M $AZTEC (coordination discounts ignored).

Fee Mechanism

Aztec meters computation work in Mana, broadly equivalent to "gas" on Ethereum L1. The minimum fee in $AZTEC per Mana a user must pay for each unit of Mana consumed in a transaction is the sum of:

I. L1 posting overhead amortized over the Mana target per block and
II. a Prover-cost-per-Mana reported by an oracle;

The minimum fee per Mana consists of a compensation component, one that offsets the costs incurred by Sequencer and Provers respectively until they're paid at the end of each epoch and a congestion component, one that can be configured to bake in a margin or 'privacy premium' ("Privacy Premium"). Atop a configurable Mana limit & Mana target the protocol grants expressive rights to configure the protocol parameters and burnt congestion component.

Sequencer Cost of an L2 Block

The L1 cost to propose an L2 block that the Sequencer must cover is:

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

Prover Cost of an L2 Block

The L1 cost for an L2 block covered by the Prover. Here, we assume a full epoch for this computation. Some parts are amortized (for example the submission cost is shared across the full epoch).

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

Deriving the minimum_fee

When a proposer is building an L2 block, it calculates a Sequencer and a Prover component and a congestion multiplier and from there the base fee that the user must cover.

$$\text{sequencer cost per mana} = \frac{\text{Sequencer L1 cost per L2 block}}{\text{TARGET\_MANA\_PER\_BLOCK}}$$

$$\text{prover cost per mana} = \frac{\text{Prover L1 cost per L2 block}}{\text{TARGET\_MANA\_PER\_BLOCK}}$$

$$\text{minimum\_fee\_in\_wei} = (\text{sequencer cost per mana} + \text{prover cost per mana}) \times \text{minimum fee congestion multiplier}$$

$$\text{minimum\_fee\_in\_fee\_asset} = [\text{minimum\_fee\_in\_wei} \times \text{fee asset per wei}]$$

This final value is the minimum_fee_per_mana field in the L2 block header.

The minimum_fee is computed in ETH/Mana and converted on-chain to $AZTEC/Mana via a Sequencer-updated $AZTEC/ETH exchange rate parameter; users can still pay in ETH/USDC/etc. via Fee-Paying Contracts (“FPCs”) which hold $AZTEC reserves and handle conversion. The Aztec Network supports a one way canonical bridge to use $AZTEC on L2 as a fee-only asset.

Token Economics

The next section explores the Economics of Aztec through the launch of the Ignition chain & Alpha.

Economics of the Ignition Chain

The Aztec Network will initially launch with the Ignition chain. Similarly to Ethereum's Beacon Chain at the Merge, its purpose is to bootstrap a decentralized Sequencer set and allow time for community led governance to establish itself. No user transactions will be processed during this phase.

Sequencers and Provers face costs to build the pending and proven chains with empty blocks using the formula outlined in the Fee Mechanism section above.

On the Sequencer side, the hardware costs are modest, and are acquirable for well under $1,000. The main cost of running a Sequencer comes from paying Ethereum gas fees to propose blocks to the pending chain. Recently, the average Ethereum gas price has been 3 gwei, and after EIP-7918, blob gas prices will conservatively hover around 1 gwei. Ignition will run with 72 second slots, and 32 slots per epoch; each proposed block costs roughly 200,000 gas and 1 blob (which equates to 2^{17} blob gas).

So a Sequencer pays the following per block in ETH:

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

Assuming 1 ETH = $4,500

$$\text{USD per block} = \$4500 \times 0.000731072 = \$3.29$$

Considering there will be 438,055 slots per year, this comes out to an annualized cost of $1,441,203 which will be spread evenly over the Sequencer set.

On the Prover side, Provers too need to pay Ethereum to verify their proof on-chain, which will cost around 2.5M gas per validity proof. At 13,689 epochs per year this gives an annualized cost of $462,000 for each Prover. The protocol will be configured initially to effectively subsidize at least 2 proofs to be produced per epoch, bringing the total cost for proving to the protocol to $923,900.

Governance has the ability to set both the size of the Block Reward, and the portion of it paid to Sequencers. Based on the "Token Supply and Distribution" section below, it is reasonable to assume that at most 20% of the Token supply will be staked at Ignition.

As a hypothetical example:

If $AZTEC has a fully diluted value of $500M, governance could set the Block Reward to be 615 $AZTEC (equal to $29.71 at the given FDV), with 92.5% of it going to Sequencers. This would result in all Sequencer costs being recouped plus a 10% yield on staked $AZTEC while maintaining an annualized inflation rate of 2.47%. These assumptions would yield $976,000 per year to be split amongst Provers. The analysis holds even if the price of ETH climbs to $10K though a 3.05% inflation rate would be felt. The full model is available on Github[3] which is configurable for users to run their own scenarios.

Real parameters at Ignition may change in response to governance actions.

Economics at Alpha

At Alpha, fees, not inflation, are intended to become the primary operator revenue, best seen through an example: Mana, the unit of work by which Aztec transactions are measured, analogous to gas on the EVM. Blocks have a Mana target, and a Mana limit. Full blocks (blocks with transactions using more Mana than the Mana target) automatically reduce net token issuance by increasing the congestion multiplier by up to 12.5% in the following block, increasing the minimum_fee, which is burned.

Aztec governance can configure the economics to target user costs (~$0.05–$0.15 for simple transfers at 5–10 TPS) while preserving positive operator margin via priority fees and

[3] https://github.com/AztecProtocol/aztec-fee-model

MEV. If blocks consistently exceed the Mana target, governance may raise the target, scaling throughput without compromising incentives.

The $AZTEC required to be paid as a fee by a transaction is its Mana cost multiplied by the current “minimum fee per mana”, or simply “minimum_fee”. The minimum_fee is calculated out of several components: a Sequencer component, a Prover component, and a congestion multiplier.

The Sequencer component is calculated first in ETH/Mana as

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

Similarly, the Prover component is calculated first in ETH/Mana as

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

The first term covers 2 Provers’ costs per Mana for publishing and verifying their proof on Ethereum. ProverCostPerMana - denominated in wei - can be set by Governance, and allows the fee mechanism to respond to the real-world dynamics of the cost to prove Aztec blocks, which will increase as blocks contain more mana, but decrease as hardware and the proving system improve.

The congestion multiplier is a running value that is

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

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

Notice that the MINIMUM_CONGESTION_MULTIPLIER when set to values >= 1 acts as a Privacy Premium or Sequencer margin & if set to 1 and with no excess_mana simply covers the costs in ETH to propose & verify. At Alpha, it is expected that this premium will be adjustable by Governance or use a self-governing mechanism which responds to, e.g., persistently full blocks.

The form of the exponential prevents the multiplier from moving more than ~12.5% between blocks.

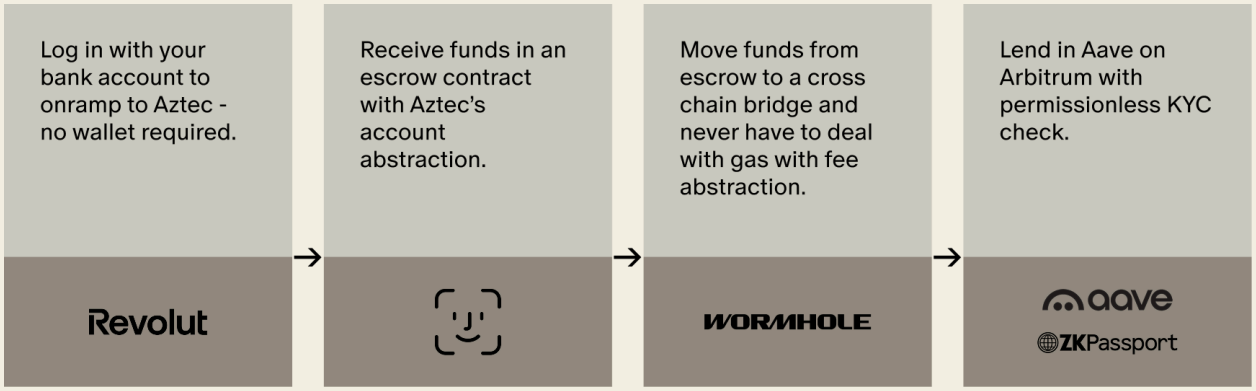
To compute the final effective minimum fee per Mana that the user pays in $AZTEC, the current exchange rate between $AZTEC and ETH is used, which is maintained by Sequencers, and denoted α. It may then be calculated as

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

So if a user's transaction consumes 10 mana, their total fee in $AZTEC (ignoring any priority fee which may be added) is 10 times the effective minimum fee. However, the portion of their fee that is due to the congestion multiplier is burned, meaning it is transferred to an address that is inaccessible to anyone, and irrecoverable; fees will be burned when blocks consume more Mana than the target, or when the MINIMUM_CONGESTION_MULTIPLIER is set by Governance to be greater than 1.

Sequencers are thus always incentivized to fill blocks with transactions to hit the Mana target, as they collect their portion of the base fee from these transactions; they are also incentivized to push beyond the Mana target and engage the burn in order to capture priority fees and MEV opportunities. When the Mana target is being persistently hit or exceeded, it may be raised by Governance.

For example, suppose that at Alpha a developer has deployed an application that makes private bridging to Ethereum's $50bn eco-system as seamless as Venmo or Revolut while remaining compliant with all relevant laws.



It is easy to imagine that there would be greater than 10 transactions per second in demand, assuming the cost paid by a user is under ~$0.15. Assume Aztec runs with 72 second slots and 32 slots per epoch, and assume the average transaction consumes 1,200 bytes of a blob, and the Aztec Network is averaging 10 transactions per second, and the blocks are hitting the Mana target of 15M mana. Assume 1 ETH= $4,500, the FDV of $AZTEC is $500M, the Ethereum gas price is 3 gwei, and blob gas is 1 gwei.

This implies that a block proposed consumes

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

And each transaction consumes

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

The fee equations above can be used to calculate the minimum_fee that is charged. The Sequencer component is

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

And the Prover component is

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

Setting the Privacy Premium to 3×10^{6}, and the ProverCostPerMana to 0 yields a minimum_fee in ETH/Mana of 7.32×10^{-10}.

From here, the user's transaction fee in dollars can be calculated as

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

This produces an annual revenue for the protocol of $21.67M.

It is worth noting that were the Privacy Premium set to 0, the base fee would result in $0.012 per transaction, which would exactly cover the costs borne by the Sequencer to publish the block.

Suppose that at Alpha 50% of the Token Total Supply is staked. Under these conditions, Governance could *reduce* the block rewards to 427 $AZTEC or $20.28, and Sequencers would still receive a 10% yield on their staked $AZTEC in dollar terms *after* costs of operations have been reimbursed; annualized inflation would fall to 1.78%.

An interesting aspect of the fee model is that when the Privacy Premium is non-zero, the Sequencers and Provers collect more fees in dollar terms as the Ethereum gas price and the price of ETH increase. The same analysis above can be performed with the price of ETH at $10,000; Sequencers could set the block reward to 0, *still* receive 10% annualized return, and there would still be $12.8M *leftover*. A similar scenario plays out if Ethereum gas prices increase to 7 gwei. In both circumstances, the user's cost per transaction remains around $0.15. In these cases, Governance could choose to reduce the Privacy Premium to cut user fees, or increase the minimum congestion multiplier; if they chose to burn the $12.8M, that would result in an annualized *deflation* of 2.56%.

Token Supply and Distribution

$AZTEC total supply at genesis is 10,350,000,000 (“Total Supply”), split across the categories described in the chart and table below.

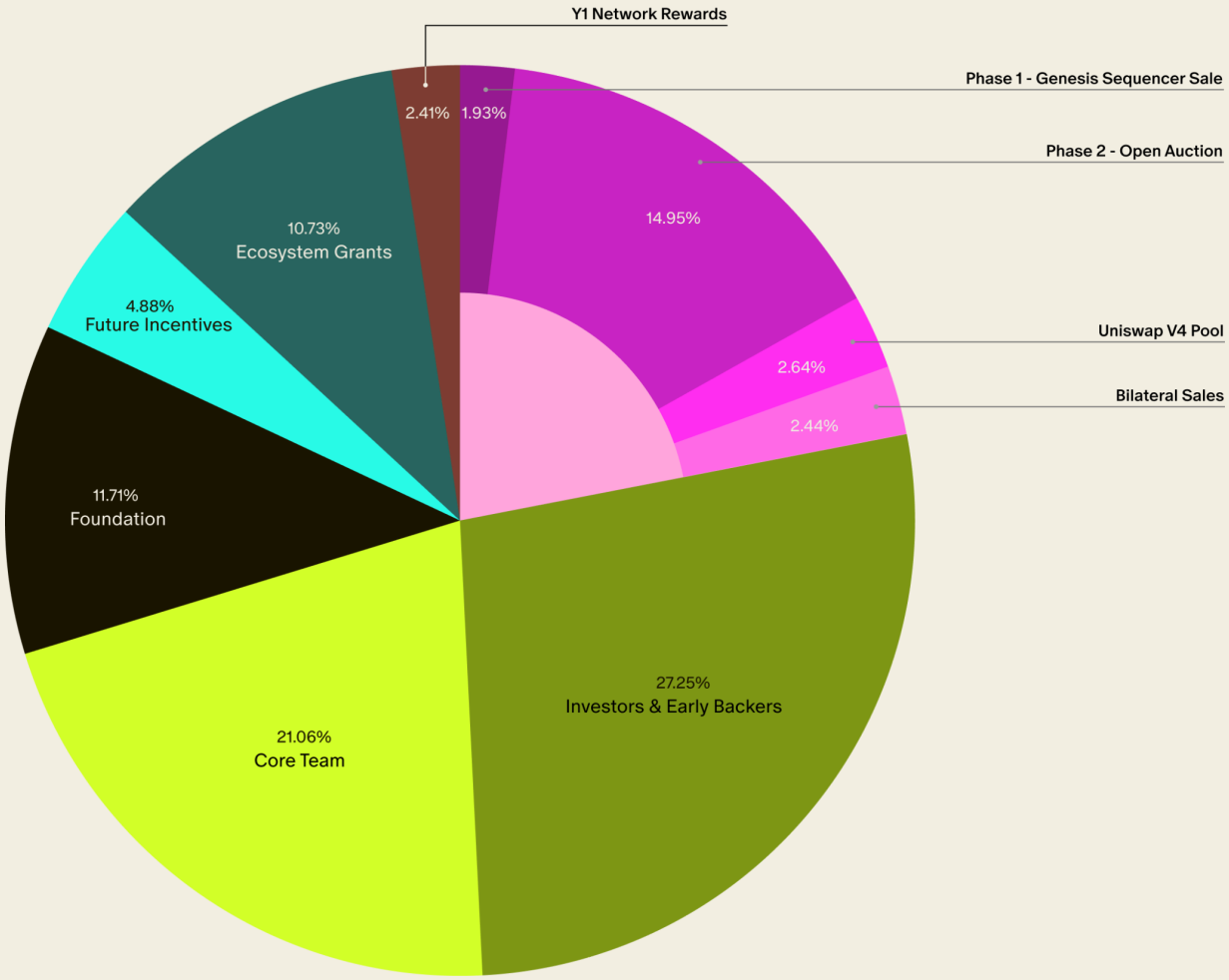
These tokens will be held in Aztec Token Position contracts (“ATPs”) otherwise known as Token Vaults on Ethereum to enforce lockups unless stated.

ATPs are flexible contracts that can be configured to enable any of the following:

- Tokens to be locked in the ATP until a certain date
- Tokens to be staked in Aztec until a certain date
- Tokens in the ATP to participate in Aztec governance
- Tokens to unlock gradually after a date is reached
- Tokens to unlock in response to an off-chain event
- Tokens to be revoked in response to an off-chain event

Tokens to Aztec Labs’ investors and employees will be distributed to ATPs that enforce a 12-month lock-up, followed by 24-month linear unlock from the launch of the Ignition chain. These ATPs will also enforce restrictions from participation in staking and governance for the first 12 months following the start of the Token Sale.

All Tokens sold in the public sale will be irrevocable and are subject to a 12 month lockup, that can be shortened to at least 90 days upon a governance vote. The exact lock duration will be determined through a governance vote, as described above. Since initial Token holders acquired Tokens through the sale or block rewards from staking, it is reasonable to expect that governance will favor the minimum lockup period.

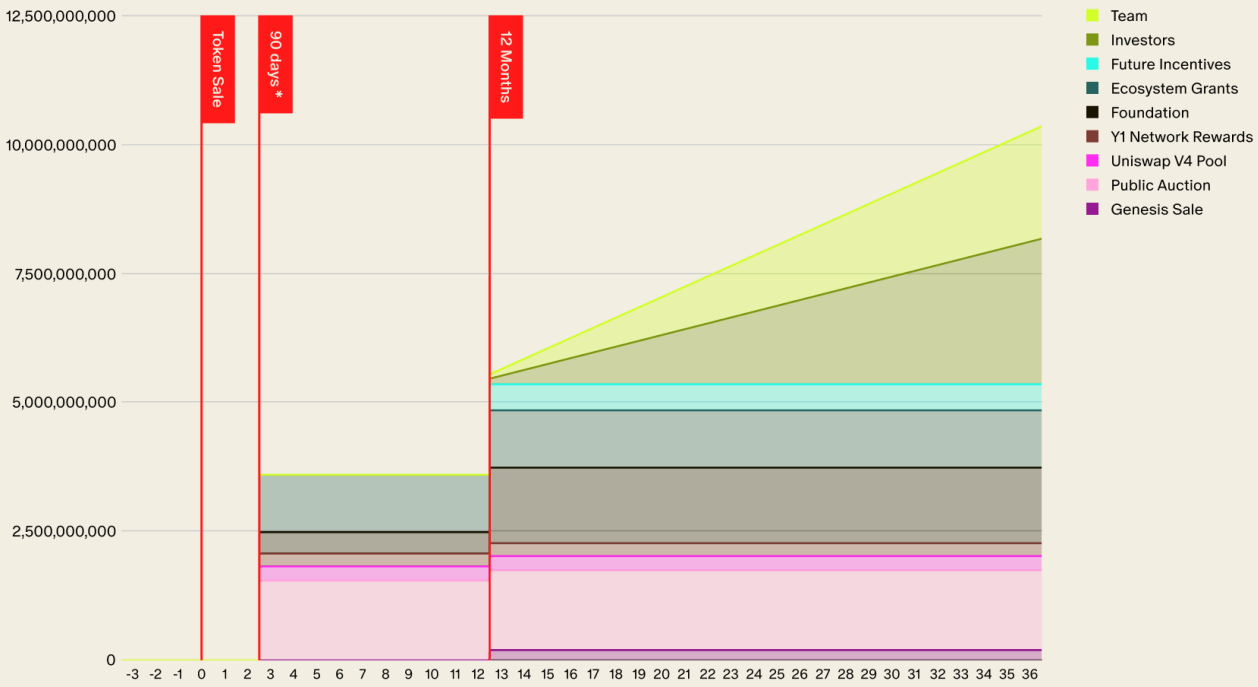


Category	Description	%	Token Amount	Owned By Whom Post-Ignition?
Token Sale	**Total:** Sold by the Foundation through the following sales on or around Ignition (as defined below)	**21.96**	**2,272,500,000** (At Ignition (as defined below), owned by Token holders and Foundation)	
	Phase 1 – Genesis Sequencers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

	onboard early network Sequencers.			
	Phase 2 – Open Auction: broaden participation among current and future Aztec users	14.95	1,547,000,000	Token holders participating in this offer.
	Uniswap V4 Liquidity Pool: in connection with the "Phase 2 - Open Auction" the Foundation will contribute 273,000,000 Tokens to the auction contracts, that will be transferred autonomously to a Uniswap V4 pool upon completion of the sale.	2.64	273,000,000	Liquidity Pool owned by Aztec governance
	Bilateral Sales - 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%) 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 Aztec Foundation to support ecosystem initiatives such as protocol ops, research, grants and partnerships	11.71	1,211,500,000	Foundation
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
Total:		**100%**	**10,350,000,000 Tokens**	

**On or around the Token Sale date, it is expected that the Foundation will control up to ~14.27% of the initial total supply, being 1,477,455,000 Tokens. To the extent the Foundation will have unlocked Tokens, in accordance with its internal policies, the Foundation will not participate in Aztec governance.*



Note the core team unlock will follow this schedule, but is subject to discrete roadmap milestones. If these milestones are delayed then the core team Tokens will remain locked. The above chart shows the most aggressive unlock schedule.

Uniswap V4 Pool

The Token Sale will create autonomously a Uniswap V4 liquidity pool funded with up to 15% of the Tokens allocated to the auction (equal to approximately 2.64% of the Total Supply) and a matching ETH amount at the final clearing price of the Auction. The Auction smart contracts will take a portion of the funds raised in ETH and deploy these against a full range liquidity pool.

The LP position will be owned by Aztec governance and any trading against the pool will be initially disabled. Only a governance vote can enable trading, which can't occur for-at least 90 days from the Token Sale date.

Based on a $750M final clearing price in the auction, the pool would have approximately $20M of ETH and $20M of Aztec Tokens, putting it inside the top 10 V4 Pools.

This pool, subject to governance votes, can be configured to direct any LP fees towards Token buybacks via a V4 hook.

Disclaimers:

Information for Persons in the UK: This communication is directed only at persons outside the UK. Persons in the UK are not permitted to participate in the token sale and must not act upon this communication.

Discount Price Disclaimer: Any reference to a prior valuation or percentage discount is provided solely to inform potential purchasers of how the initial floor price for the token sale was calculated. Equity financing valuations were determined under specific circumstances that are not comparable to this offering. They do not represent, and should not be relied upon as, the current or future market value of the tokens, nor as an indication of potential returns. The price of tokens may fluctuate substantially, the token may lose its value in part or in full, and purchasers should make independent assessments without reliance on past valuations. No representation or warranty is made that any purchaser will achieve profits or recover the purchase price.

MiCA Disclaimer: This crypto-asset marketing communication has not been reviewed or approved by any competent authority in any Member State of the European Union. The offeror of the crypto-asset is solely responsible for the content of this crypto-asset marketing communication. The Aztec Foundation has published a MiCA-compliant white paper in relation to the token sale which can be accessed here.

Functionality Disclaimer: No assurance is given that any particular functionality (including the Private Execution Environment or collaborative proving, which affects how fees work within Aztec) will be available at launch or within any specific timeframe, which may impact the economics analysis.