Aztec Network – MiCA Whitepaper

Contents:

No.	FIELD	CONTENT
01	Date of notification	2025-10-14
02	Statement in accordance with Article 6(3) of Regulation (EU) 2023/1114	This crypto-asset white paper has not been 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 white paper.
03	Compliance statement in accordance with Article 6(6) of Regulation (EU) 2023/1114	This crypto-asset white paper complies with Title II of Regulation (EU) 2023/1114 of the European Parliament and of the Council and, to the best of the knowledge of the management body, the information presented in the crypto-asset white paper is fair, clear and not misleading and the crypto-asset white paper makes no omission likely to affect its import.
04	Statement in accordance with Article 6(5), points (a), (b), (c), of Regulation (EU) 2023/1114	The crypto-asset referred to in this crypto-asset white paper may lose its value in part or in full, may not always be transferable and may not be liquid.
05	Statement in accordance with Article 6(5), point (d), of Regulation (EU) 2023/1114	Not applicable.

06	Statement in accordance with Article 6(5), points (e) and (f), of Regulation (EU) 2023/1114	The crypto-asset referred to in this white paper is not covered by the investor compensation schemes under Directive 97/9/EC of the European Parliament and of the Council or the deposit guarantee schemes under Directive 2014/49/EU of the European Parliament and of the Council.

1. Summary

07	Warning in accordance with Article 6(7), second subparagraph, of Regulation (EU) 2023/1114	**Warning** This summary should be read as an introduction to the crypto-asset white paper. The prospective holder should base any decision to purchase this crypto-asset on the content of the crypto-asset white paper as a whole and not on the summary alone. The offer to the public of this crypto-asset does not constitute an offer or solicitation to purchase financial instruments and any such offer or solicitation can be made only by means of a prospectus or other offer documents pursuant to the applicable national law. This crypto-asset white paper does not constitute a prospectus as referred to in Regulation (EU) 2017/1129 of the European Parliament and of the Council or any other offer document pursuant to Union or national law.
08	Characteristics of the crypto-asset	**Overview**. - The AZTEC token ("**AZTEC**" or "**Token**") is the native token of the Aztec Network, a Layer 2 rollup on Ethereum ("**Aztec Network**" or "**Aztec**"). - AZTEC is a fungible ERC20 token recorded on the Ethereum blockchain. - The staking of AZTEC and the payment of block rewards to Sequencers and provers will take place on Ethereum. - Public Offer Date as referred to throughout this document is the date at which the Token sale starts, expected to be 13 November 2025 subject to technical readiness ("**Public Offer Date**"). - **Key functionality**. The Token is intended to serve the following main functions on the Aztec Network: – ***Sequencer Staking***. The Token will be used to secure the Aztec Network through staking by Aztec validators on Ethereum (L1), also known as "sequencers" ("**Sequencers**"), who will be responsible for the production of blocks within Aztec. Sequencers will need to stake the Token and in return for doing so they will obtain the right to produce blocks and may be entitled to receive block rewards in the form of Tokens when a block they propose is successfully proven on Ethereum L1. – ***Governance***. Tokens will also enable participation in the governance of the Aztec Network through a two-stage process: (i) Sequencer signalling, followed by (ii) Token holder ratification, as follows: – ***Stage 1 - Sequencer Signalling***. By staking AZTEC, Sequencers will be able to initiate proposals related to certain network parameters and upgrades of the Aztec Network. Sequencers express support for such proposals through an on-chain signalling mechanism, and only proposals that meet the governance-set signalling threshold (m block proposers over a total of n blocks, with m = 600 and n = 1000 pre-set at launch; future governance proposals may change these variables) may advance to the ratification stage. Token holders may elect to delegate the operation of a Sequencer to a third party. Delegated operation of a Sequencer increases the Sequencer operator's signalling power for this purpose, but delegation does not transfer voting rights for the purposes

of Token holder ratification voting at stage 2. A delegator also does not obtain the right to initiate governance proposals as a result of delegating their Tokens.

– ***Stage 2 - Token Holder Ratification***. From Ignition (as defined below), holders of AZTEC that are operating Sequencers or have delegated the operation of a Sequencer to a third party, may participate in governance by voting on proposals that pass Sequencer signalling, which requires them to lock their Tokens for the duration of a vote. Only Tokens that are staked, either directly or through delegation to a Sequencer are eligible to vote. Token holders retain full and independent voting rights and may ratify or reject any proposal advanced by Sequencers. Sequencers have no ability to vote on behalf of delegators; their role in governance is limited to signaling proposals at stage 1.

– ***Voting Delegation***. Token holders may, in addition, delegate their voting rights separately, either to another Token holder, a third party, or a smart contract. 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 Token holder may override this default at any time by redelegating their voting rights to any other address, including their own.

(collectively, "**Aztec Governance**").

– ***Token Holders in Control***. As of the Public Offer Date (as defined above), Token holders will be in control of Aztec Governance. None of the Aztec Foundation (as defined below), the initial private investors & early backers in Aztec nor any member of the core team at Labs (as defined below), will have control over Aztec Governance. In addition, for at least 12 months from the Public Offer Date, to ensure control of Aztec Governance is as decentralised as possible, such parties' Token allocations will be locked from participating in Aztec Governance, subject to and as set out in the "Token Unlocks" table below.

– ***Execution Environment (future)***. If and when at a future date Aztec is upgraded by Aztec Governance to enable the smart contract execution environment ("**Execution Environment**"), the Token will serve as the means to pay for transaction fees within the Aztec Network. If and when the Execution Environment is enabled, the Token will likely have to (i) be bridged from Ethereum (L1) to Aztec (L2) for this purpose (i.e., to pay for transaction fees) and (ii) be non-transferrable once it is transferred to Aztec.

Token Supply.

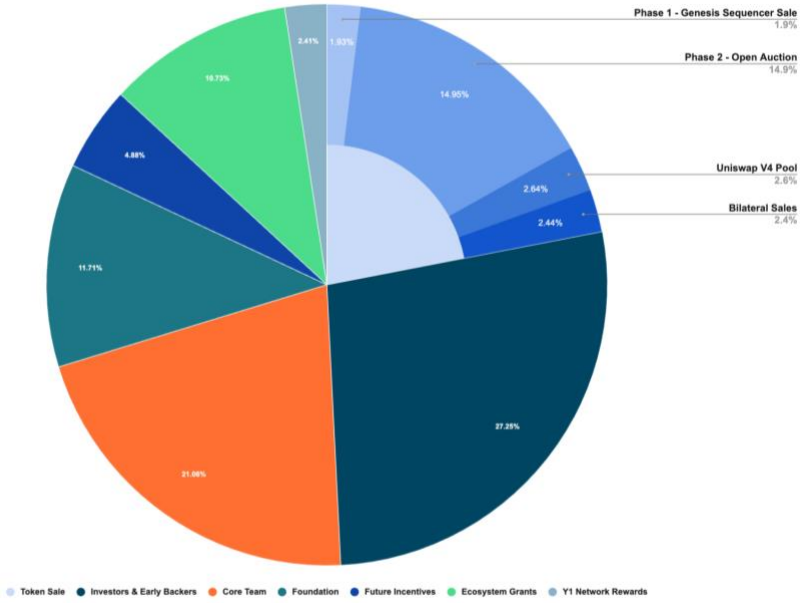
- ***Initial Supply at the Public Offer Date.*** At the Public Offer Date, the initial supply of AZTEC will be 10,350,000,000 Tokens (the "**Initial Total Supply**").

- ***Future Inflation***. From twelve (12) months after the Public Offer Date: (i) Aztec Governance will be able to change the total supply of the Aztec Token, including by increasing the Initial Total Supply by up to a capped percentage per annum as further described below in H.5 and (ii) if and when the Execution

Environment is enabled by Aztec Governance, fees will likely be regulated autonomously (intended to be similar to Ethereum's EIP-1559) by the Aztec Network.

Token Distribution Plan.

The Initial Total Supply as of the Public Offer Date is intended to be as set out below.



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: onboard early network Sequencers through whitelists, please see E.19 below for further details	1.93	200,000,000	Token holders

			Phase 2 – Open Auction: broaden participation among current and future Aztec users, please see 10 below for further details.	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 non-insider early contributors, community members, and aligned individuals, the	10.73	1,111,000,000	Grant recipients (~10.61%) Foundation (~0.12%)

	majority of which will have been distributed and allocated by the Public Offer Date.			
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**	

** Please see "Liquidity Pool" description in item 10 in the Summary below for further information. Final amounts subject to change.*
*** On or around the Public Offer 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.

Token Unlocks.

The Initial Total Supply as of the Public Offer Date will be subject to the below unlock schedules. ATPs (as defined below) and registries can be configured in multiple ways: for Tokens and unlocks to be immutable, or controlled by the Foundation, Labs, or Aztec Governance. Each ATP requires configuration to achieve its stated effect. Unlocks cannot be changed by Aztec Governance, unless specified below.

Category	**Unlock Schedule**	**Who Controls Unlock?**
Token Sale	**Phase 1 (Genesis Sequencer Auction)** - 12-month fixed lock-up from the Public Offer Date	Immutable
	Phase 2 (Open Auction) - 12-month fixed lock-up from the Public Offer Date	Immutable, but can be shortened to at least 90 days from the Public Offer Date via an Aztec Governance vote
Liquidity Pool	Locked. Requires a governance vote to enable tradability.	Immutable. No votes permitted for at least 90 days from the Public Offer Date, then subject to Aztec Governance
Ecosystem Grants	At least 90-day unlock from Public Offer Date, that may be longer based on individual grant milestones, set by the Foundation in its discretion	Foundation
Future Incentives	12-month fixed lock-up from Public Offer Date	Immutable for at least 12 months, then subject to Aztec Governance
Y1 Network Rewards	At least 90-day unlock from Public Offer Date	Immutable for at least 90 days from Public Offer Date, then subject to Aztec Governance

<table>
<tr><td></td><td></td><td>
<table>
<tr><td>Foundation</td><td>● 4% unlocked not subject to any restrictions – internal policies will not allow staking or participation in governance

● 7.71% locked for a 12-month period from Public Offer Date preventing staking and governance votes in this time</td><td>● Foundation for the 4%

● Immutable for the 7.71% (once issued into ATP)</td></tr>
<tr><td>Investors & Early Backers</td><td>12-month fixed lock-up, followed by 24-month linear unlock from Public Offer Date</td><td>Immutable</td></tr>
<tr><td>Team</td><td>12-month fixed lock-up, followed by 24-month linear unlock from Public Offer Date*</td><td>Immutable</td></tr>
</table>
*Team Tokens are also subject to vesting at certain milestones defined by reference to Aztec Network activity/adoption
Risks: Please refer to the risk disclosures in Part I – Information on risks.
</td></tr>
<tr><td>09</td><td></td><td>Not applicable.</td></tr>
<tr><td>10</td><td>Key information about the offer to the public or admission to trading</td><td>
Overview of Offer: Aztec Foundation (the “Foundation”) will offer up to 14.95% of the Initial Total Supply.

Primary Purpose of Offer:
● Decentralize ownership and control of the Aztec Network, placing governance and economic security in the hands of a broad, distributed set of participants rather than the Foundation or any other single entity, increasing censorship resistance and credible neutrality.
● Enable governance and staking participation such that if and when approximately 500 Sequencers or at least 100,000,000 Tokens are purchased and staked, block production will start on the Aztec Network and Ignition will occur (“Ignition”).

Secondary Purpose of Offer:
● Raise funds for the Foundation to enable it to fulfil its non-profit mandate, to (i) support the development and adoption of open and decentralized technologies in general, (ii) provide ancillary support for the development, promotion and
</td></tr>
</table>

adoption of the Aztec Network and related technologies, and (iii) provide ancillary support for applications and/or services using the Aztec Network.

Key details of Offer: The public offer will be for up to 14.95% of the Initial Total Supply. The public offer will be structured as an auction with the following key details:

- ***Public Auction*:** An open, price-discovery sale using the novel Uniswap Time-Weighted Uniform Clearing Auction ("**TWUCA**") format with a fully diluted valuation ("**FDV**") initial floor price set by the Foundation ahead of the sale. The TWUCA is a new and multi-period token sale format designed by Universal Navigation Inc. and/or its affiliates ("**Uniswap**") which intends to reduce price manipulation, promote fair access, and help fair market price discovery. The sale is divided into discrete time periods, with a portion of the total amount of Tokens to be sold in the auction allocated to each period, and an initial pre-set floor price that applies during the first auction period, each determined by the Foundation ahead of the sale. After the end of the first auction period, the minimum clearing price may increase as a result of increased demand. While the initial fixed price floor remains the same, actual clearing prices in later periods may rise above it and will not fall below the most recent clearing price once established. Bidders submitting prices below the prevailing clearing price may receive no allocation. Subject to the final design of the user interface launched ahead of the offer, it is intended that bidders will submit their total maximum commitment (in ETH) and either elect to buy Tokens at the market clearing price (clearing currently anticipated to be every 3 mins) or set a maximum price per Token/FDV at which they are willing to purchase Tokens. Their bids are automatically split pro rata across all remaining periods based on a supply schedule governing the number of Tokens allocated to each period (to be determined and finalised by the Foundation prior to the sale) ("**Supply Schedule**"). At the end of each period, Tokens are allocated to bidders based on a single uniform clearing price, which is the highest price at which there is demand that fills all available supply for the remaining periods. It is expected that periods will not have an equal supply of Tokens allocated to them. Additional Tokens may be allocated to the final periods to attempt to reduce risk of price manipulation (although this cannot be eliminated entirely) and any Tokens unsold in a period will be reallocated to remaining periods. Any Tokens allocated to the public offer that are unsold at the end of the auction (for whatever reason) may be claimed back by the Foundation.

- ***Subscription Goals***:

    1. *Minimum Subscription Goal:* No minimum subscription target is set for the auction.

    2. *Maximum Subscription Goal:* No maximum subscription target has been set for the auction in terms of value of funds raised, however the maximum number of Tokens sold via the auction will be up to 14.95% of the Initial Total Supply, as stated above.

- ***Public Auction Eligibility***:

    All sale participants will be required to qualify for the sale by passing sanctions checks and/or any other required KYC/KYB checks determined by the Foundation and its contractors administering such checks in their sole and

absolute discretion.

Access to the sale after qualification is split into two participation tracks:

1. *Contributor Track*: Whitelisted participants selected by the Foundation based on certain criteria, including:

    - testnet activity;
    - Aztec Connect usage;
    - Participation as an Ethereum solo staker;
    - Discord engagement; and/or
    - other community contributions at the discretion of the Foundation,

    (the "**Contributor Track**").

2. *Public Sale Track*: Open to all qualified participants (the "**Public Sale Track**").

- ***Public Auction Announcement***: Prior to the sale, the Foundation will communicate eligibility criteria, process to participate in the sale and final details on the sale on its websites (https://aztec.foundation/, https://aztec.network and/or their sub-domains, including, https://sale.aztec.network), Discord (https://discord.com/invite/aztec), X (https://x.com/aztecFND and/or https://x.com/aztecnetwork).

- ***Public Auction Process***:

    1. *Eligibility and Sanctions Checks.* Prospective participants are required to complete eligibility and sanctions checks and, once passed, will be able to mint a Soulbound NFT, which will entitle them to participate in the sale but will expire after 60 days. After expiration, prospective participants will be required to complete new eligibility and sanctions checks and mint another SoulBound NFT (incurring any additional applicable Ethereum gas fees).

    2. *Bid Auction Process*:

        - Contributor Track bids are accepted during the 18 days before the auction period and throughout the 5-day auction period itself.

        - Public Sale Track bids are accepted during the final 4 days of the 5-day auction period.

    3. *How Auction Bids Work:* Participants' bids will be split across all remaining periods of the auction, even if, in the case of Contributor Track bids, they are placed before the start of the 5-day auction period. However, Contributor Track participants who place bids before Public Sale Track bidding opens are expected to receive a lower average clearing price than Public Sale Track participants if the auction clears above the floor price (rather than at the floor price).

- ***Public Auction Period***: The auction will be open and clearing for 5 days, with bidding being open for the Contributor Track and Public Sale Track,

respectively, as follows:

1. Contributor Track bidding starts from 18 days before day 1 of the auction being open and clearing (the starting date for Contributor Track bidding currently expected to be 13 November 2025, subject to technical and operational readiness) until the end of the auction period.
2. Public Sale Track bidding starts from day 2 of the auction being open and clearing (currently expected to be 2 December 2025, subject to technical and operational readiness) until the end of the auction period.

- ***Subscription Fees***: No subscription fees will be charged by the Foundation in relation to the public offer.

- ***Gas Fees***: Participants ***will be required to pay for all*** Ethereum gas fees under or in connection with each transaction on the Ethereum blockchain required to participate in or take actions related to the public offer and deal with purchased Tokens, including, without limitation: minting of the SoulBound NFT to participate in the offer, placing bids, claiming Tokens, staking Tokens to run each Sequencer and/or electing to delegate the operation of a Sequencer to a third party, locking Tokens to participate in Aztec governance, claiming unspent ETH committed to the auction and/or any other actions. Gas fees vary and may be material, for example for participants that purchase large numbers of Tokens and/or run multiple Sequencers. For the avoidance of doubt, Ethereum gas fees are not charged by, set by or transferred to the Foundation; they are charged and set by the Ethereum blockchain, with a portion being burned and a portion being transferred to validators on the Ethereum blockchain.

- ***Public Auction Frontend***: sale.aztec.network

- ***Delivery of Tokens and Aztec Token Positions***: Immediately following the conclusion of the auction, Tokens allocated as a result of successful bids will be transferred to Aztec Token Positions ("**ATPs**"), which will be non-transferable smart contracts on Ethereum. Each Soulbound NFT minted by a participant will be able to create one ATP and Tokens allocated as a result of successful bids made by the Ethereum wallet address associated with the relevant Soulbound NFT ("**Bidding Address**") will be transferred to this ATP. As part of creating an ATP, a participant must designate an Ethereum address that will control the ATP (but this may only be the Ethereum wallet address associated with the Soulbound NFT or another Ethereum address specified by the participant that passes the sanctions / other screening checks determined by the Foundation and its contractors administering such checks in their sole and absolute discretion). Tokens in an ATP may be staked or delegated for staking by participants. Tokens in an ATP may also be unstaked, undelegated or "claimed" (i.e., transferred to the participant-designated Ethereum address that controls the ATP) by participants, subject to the mandatory staking requirement and lockup described below. For purchases of 200,000 Tokens or above, the ATP will not natively allow for the withdrawal of Tokens. Tokens in these locked ATPs will only become withdrawable if and when their owner stakes them.

- ***Mandatory Staking Requirement and Lockup***: The following requirements will apply to Tokens purchased in the offer:

  1. *Mandatory Staking Requirement*: Participants who purchase 200,000 or

		more Tokens will be required to stake at least one multiple of 200,000 Tokens. Until they meet this requirement, all purchased Tokens will remain locked in their ATP. 2. *Lockup*: All Tokens will be subject to the following restrictions (enforced autonomously via ATPs) for a 12-month period from the Public Offer Date unless amended to a shorter period of a minimum of 90 days from the Public Offer Date via Aztec Governance: o Staked or delegated Tokens may not be unstaked or undelegated; and o Tokens may not be claimed from ATPs. For the avoidance of doubt, all locked Tokens in multiples of 200,000 can be staked. ● ***Liquidity Pool:*** The smart contracts governing the auction will be programmed such that (i) a proportion of the ETH paid by purchasers in the auction, and (ii) a proportion of AZTEC determined by reference to the number of AZTEC allocated to the auction from the Initial Total Supply, will be autonomously transferred by the auction smart contract to the Liquidity Pool. With respect to the AZTEC to be transferred, the Foundation will fund the auction smart contract with sufficient Tokens at the outset to cover this transfer (meaning that participants will receive via ATPs 100% of the AZTEC they purchase in the auction). Out of the Tokens allocated to the auction for this offer, 15% of such Tokens will be transferred autonomously to the Liquidity Pool. The Liquidity Pool will be controlled by Aztec Governance and locked in an immutable smart contract for at least 90 days from the Public Offer Date, after which Aztec Governance can vote to lift such restrictions.

2. Part A - Information about the offeror or the person seeking admission to trading

A.1	Name	Aztec Foundation
A.2	Legal form	Refer to Legal Entity Identifier ("**LEI**") included in A.6. Aztec Foundation is a memberless, non-profit foundation (*Stiftung*) domiciled in Zug, Switzerland. It has no shareholders or equity owners and is governed by a Foundation Board. The Foundation's statutory purpose is to steward the development and governance of the Aztec Network and its ecosystem, including to (i) support the development and adoption of open and decentralized technologies in general, (ii) provide ancillary support for the development, promotion and adoption of the Aztec Network and related technologies, and (iii) provide ancillary support for applications and/or services using the Aztec Network. The Foundation does not engage in commercial profit-making activities; any surplus is reinvested into its statutory objectives.

A.3	Registered address	Gartenstrasse 6, 6300 Zug, Switzerland
A.4	Head office	Refer to Legal Entity Identifier ("**LEI**") included in A.6.
A.5	Registration date	2024-12-16
A.6	Legal entity identifier	506700JRDV5Z828A9D47
A.7	Another identifier required pursuant to applicable national law	Not applicable.
A.8	Contact telephone number	+41 41 710 16 70
A.9	E-mail address	sale@aztec.foundation
A.10	Response time (Days)	25
A.11	Parent company	Not applicable.
A.12	Members of the management body	Zachary Williamson, Chair and Founder; Arnaud Schenk, Executive Director and Board Member; and Herbert Sterchi, Board Member. Gartenstrasse 6, 6300 Zug, Switzerland.
A.13	Business activity	The Foundation's statutory purpose is to steward the development and governance of the Aztec Network and its ecosystem, including to (i) support the development and adoption of open and decentralized technologies in general, (ii) provide ancillary support for the development, promotion and adoption of the Aztec Network and related technologies, and (iii) provide ancillary support for applications and/or services using the Aztec Network.
A.14	Parent company business activity	Not applicable.
A.15	Newly established	Yes
A.16	Financial condition for the past three years	Not applicable. Established for less than three years.

A.17	Financial condition since registration	At the time of drafting this white paper the Foundation has been financially stable since its registration. The Foundation received a non-repayable ordinary course of business grant of CHF 265,000 in June 2025 from Spilsbury Holdings Limited (t/a Aztec Labs) to cover its ordinary course of business operating costs in the period prior to the launch of the Aztec Network and facilitate the deployment of Aztec Network testnets and the initial issuance and deployment of the native cryptoasset (i.e., AZTEC). In addition, the Aztec Foundation received a non-repayable CHF100,000 initial capital contribution by its Founder on or around the date of its establishment on December 16, 2024. Since its establishment the Foundation has only onboarded one full-time employee, the Executive Director. As an ownerless legal form, the Foundation does not have share capital. At the time of drafting this white paper, the Foundation has CHF 220,384.00 of cash or cash equivalents on its balance sheet. This amount is sufficient to cover the Foundation's current and expected expenditure between the date of this white paper and the completion of the public offer. In July of 2025, the Foundation sold 5,000,000,000 tokens that, once the Aztec Network is deployed, will become the AZTEC Token to Spilsbury Holdings Limited (t/a Aztec Labs) for US$792,500.00 and expects to set this amount off against future expenditure under relevant arrangements with Labs following the launch of the Aztec Network. The Foundation intends to raise additional funding through the offer to the public (as detailed in section 10 of the Summary of this white paper) in Q4 of 2025. The proceeds are expected to be applied towards the objectives of the Foundation detailed in section A.2 and to cover its general operational expenditure in pursuing its objectives. The Foundation will also retain ownership of ~11.71% of the AZTEC Initial Total Supply, which is intended to be used in support of ecosystem initiatives, including protocol operations, research, grants, and partnerships. The Foundation has no outstanding debt or other significant financial obligations at the time of drafting this white paper. In particular, the key offer expenses set out in Section E.37, whether already incurred or expected to be incurred prior to the offer to the public, have been or will be funded through the grants outlined above, applying offsets, or will only become due after the offer to the public.

3. Part B - Information about the issuer, if different from the offeror or person seeking admission to trading

Not applicable. The Foundation is the issuer and offeror.

Part C- Information about the operator of the trading platform in cases where it draws up the crypto-asset white paper and information about other persons drawing the crypto-asset white paper pursuant to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114

Not applicable.

4. Part D- Information about the crypto-asset project

D.1	Crypto-asset project name	Aztec
D.2	Crypto-assets name	AZTEC Token
D.3	Abbreviation	AZTEC
D.4	Crypto-asset project description	The Aztec Network is a Layer 2 blockchain built on Ethereum. The Aztec Network is intended to be a general-purpose layer 2 built on Ethereum. Compared to Ethereum and similar blockchains, the innovations of the Aztec network may in the future (if and when the Execution Environment is enabled by Aztec Governance) relate to how transaction data is stored, and the extent to which transaction data is accessible to third parties that are not involved in the transactions. These innovations are based on seminal research in applied mathematics and cryptography pioneered by Dr. Zachary Williamson and colleagues. AZTEC is a core part of the protocol, used to secure the network via staking, and participate in decentralized governance.
D.5	Details of all natural or legal persons involved in the implementation of the crypto-asset project	The Aztec Network has been developed by the Foundation, Spilsbury Holdings Limited ("**Labs**"), and various other independent community members, including through Request for Proposals (RFPs) and Requests for Comments (RFCs) set out in https://forum.aztec.network. The initial contracts for the Aztec Network will be deployed by the Foundation on the Public Offer Date, but the network Ignition and first live implementation of the Aztec Network will only occur directly as a result of Sequencers staking and launching block production.
D.6	Utility Token Classification	Not applicable.
D.7	Key Features of Goods/Services for Utility Token Projects	Not applicable.
D.8	Plans for the token	**Past Milestones** ● **2024**: ○ Launched the Aztec Sandbox, enabling developers to test and write programs for the upcoming network. ○ Released Noir Alpha, the first production-oriented iteration of " Noir", Aztec's privacy-focused programming language. Noir Alpha expanded

		standard library features, enabling developers to write, test, and debug zero-knowledge applications more efficiently. ○ Foundation launched to steward the development of the token and deploy testnets of the Aztec Network. ○ Completed certain (but not all) independent smart contract and protocol security audits, including Bigfield, SSA, Stdlib Field, and the token generation event smart contracts. ● **2025**: ○ Public testnets, including an adversarial testnet, launched. ○ Rollup circuits and sequencer logic finalized. ○ Governance contracts are audited and formally verified. ○ Rollup, ATP, and Sale contracts are audited. **Indicative Future Milestones** These anticipated future key milestones are tied to the technical and governance evolution of the Aztec Network and depend on actions by Aztec Network participants: ● Q4 2025 - Ignition: The Foundation will deploy network governance and staking system functionality, which will enable Sequencers to access the protocol, stake Tokens and enable block production, igniting the first instance of the Aztec Network. Once a sufficient threshold of Sequencers participate and join to secure the network economically, Ignition will occur. ● Q4 2025 - Staking and Governance Dashboards: The Foundation intends to fund the development of certain non-custodial staking and governance dashboards, which will provide a user interface for Sequencers and/or Token holders to stake AZTEC and/or participate in Aztec Governance. ● Q1+ 2026 - Alpha: If and when Aztec Governance upgrades the Aztec Network to enable the Execution Environment, this may enable: ○ the Token to serve as the means to pay for transaction fees within the Aztec Network; and/or ○ Transaction functionality on the Aztec Network which in turn may enable external dApps and smart contracts to be deployed on the Aztec Network, ("**Alpha**"). ● Q2 2026 - Mainnet Beta: Upgrade of Alpha, where state is migrated between upgrades and incentives may be introduced by Aztec Governance or otherwise for depositing funds into the Aztec Network. Full programmability may be enabled with enhanced stability and security. **Disclaimer**: Neither the Foundation nor Labs controls protocol upgrades nor the implementation of any future milestones into the Aztec Network. The milestones described above are indicative only and may not occur. By purchasing AZTEC, you

		acquire the current functionality of the Token and the Aztec Network as it exists at the time of purchase. The future of the Aztec Network will be determined by Token holders through the network's governance process. Further detail on the expected community driven roadmap is visible here: https://aztec.network/roadmap. None of the roadmap initiatives may occur and purchasers should be aware that any Tokens they purchase may only be used to secure the Aztec Network through staking and to participate in Aztec Governance, unless and until future milestones occur.
D.9	Resource allocation	On or around March 2025, the Foundation received an ordinary course of business grant of CHF 265,000 from Labs to cover the ordinary course of business operating costs and facilitate the deployment of Aztec Network testnets and the initial issuance and deployment of the native cryptoasset (i.e., AZTEC). In 2025, the Foundation is also expected to receive the following key resources: ● certain intellectual property, including trade marks related to Aztec and Noir; ● proceeds (denominated in ETH) from the sale conducted in connection with this offer; and/or ● prior to the date of this offer, potential further grants from Labs to cover general purpose expenses. In addition, the Foundation will also hold a dedicated Token treasury to finance ongoing operations, grants, and strategic initiatives aligned with its mission to support Aztec, Noir and other similar infrastructure. This amounts to the following: ● **Held for Bilateral Sales:** 252,500,000 Tokens (2.44% of Initial Total Supply) ● **Foundation Allocation:** 1,211,500,000 Tokens (11.71% of Initial Total Supply) ● **Ecosystem Grants:** ~ 13,455,000 Tokens of the total 1,111,000,000 tokens (10.73% of Initial Total Supply) allocated towards Ecosystem Grants. Of which ~10.61% of Initial Total Supply has already been allocated to third-party recipients leaving ~0.12% of Initial Total Supply in Foundation control. ● **Total:** 1,477,455,000 Tokens, being ~14.27% of the Initial Total Supply. Please see item 08 of the Summary for more details, including as to unlocks. **Disclaimer**: the above is indicative only as at the date of the white paper, not exhaustive and is subject to change.
D.10	Planned use of collected funds or crypto-assets	ETH collected by the Foundation through the public Token sale will be used in accordance with its Business Activity mandate described in A.13 above, and may include using the funds to: ● Support Aztec Network and governance infrastructure; ● Fund grants and initiatives to grow the Aztec Network developer ecosystem; ● Advance protocol security, audits, and technical development; ● Cover ordinary course expenditures related to operational, legal, regulatory and compliance costs under or in connection with the Foundation's activities. All ETH collected by the Foundation through the sale will be managed by the Foundation in line with its non-profit mandate to steward and further decentralize the Aztec Network.

5. Part E - Information about the offer to the public of crypto-assets or their admission to trading

E.1	Public offering or admission to trading	Offer to the public
E.2	Reasons for public offer or admission to trading	The primary reason for this offer is to decentralize the ownership and control of the Aztec Network, thus increasing Aztec's censorship resistance and credible neutrality, and enable the sale participants to launch the Aztec Network through Ignition. The second reason for this offer is to raise funds for the Foundation to enable it to fulfil its non-profit mandate, to support (i) the development and adoption of open and decentralized technologies in general, (ii) provide ancillary support for the development, promotion and adoption of the Aztec protocol and related technologies, and (iii) provide ancillary support for applications and/or services using the Aztec protocol.
E.3	Fundraising target	The Foundation intends to raise approximately US$50 million through the public Token sale, with the actual proceeds to be received denominated in Ether ("**ETH**"). The funds raised will depend on the clearing price achieved at the auction and is not pegged to any particular target. For example, if the auction clears at an average price implying an FDV of: ● US$300 million, the Foundation would be expected to raise approximately US$50 million (denominated in ETH). ● US$600 million, the Foundation would be expected to raise approximately US$100 million (denominated in ETH). In addition, the value of ETH may change against US$/USDC or equivalent stablecoins and that may impact the actual amounts raised in dollar terms.
E.4	Minimum subscription goals	No minimum subscription target is set for the offer.
E.5	Maximum subscription goals	No maximum subscription target has been set for the offer in terms of value of funds raised, however the maximum number of Tokens sold via the offer will be up to 14.95% of the Initial Total Supply, as stated above.
E.6	Oversubscription acceptance	Oversubscriptions are accepted mechanically in the auction, meaning total bid demand can exceed the total token auction supply, however, only bids equal to or above the clearing price (clearing is currently anticipated to be every 3 mins) will be allocated Tokens on a pro-rata basis.
E.7	Oversubscription allocation	In case of excess demand, Token allocations are made using Uniswap's auction model, where bids are cleared (currently anticipated to be every 3 mins) at the highest price

		that fills all available supply. Only clearing bids will be allocated Tokens. The auction does not reject or limit incoming bids based on a total sale cap, and clearing is handled per sub-period via a time-weighted, price-ranked allocation.
E.8	Issue price	The initial floor price will be set by the Foundation ahead of the offer at FDV value, which will subsequently be determined dynamically by auction mechanics (see E.11 below).
E.9	Official currency or any other crypto-assets determining the issue price	ETH DTI: X9J9K872S
E.10	Subscription fee	Not applicable.
E.11	Offer price determination method	The offer price will be determined via the Uniswap TWUCA format with an initial FDV floor price set by the Foundation ahead of the sale. After the end of the first auction period, the minimum clearing price may increase as a result of increased demand. While the initial fixed price floor remains the same, actual clearing prices in later periods may rise above it and will not fall below the most recent clearing price once established. Bidders submitting prices below the prevailing clearing price may receive no allocation. The TWUCA is a multi-period token sale format intended to promote fair access, fair price discovery, and resistance to manipulation. Please see item 10 in the Summary for further detail on price determination.
E.12	Total number of offered/traded crypto-assets	Up to 14.95% of the Initial Total Supply or 1,547,000,000 Tokens.
E.13	Targeted holders	The sale targets purchasers interested in staking and governance of the Aztec Network.
E.14	Holder restrictions	The following are excluded from participating: ● Persons and/or Ethereum wallet addresses sanctioned by the U.S. Office of Foreign Assets Control ("**OFAC**"), the European Union/European Economic Area, or Switzerland or persons in comprehensively sanctioned jurisdiction as determined by OFAC. ● Residents of other jurisdictions that the Foundation may exclude in its sole discretion (including the United Kingdom).
E.15	Reimbursement notice	Purchasers participating in the offer to the public will be able to be reimbursed if they exercise the right to withdrawal provided for in Article 13 of Regulation (EU) 2023/1114 of the European Parliament and of the Council or if the offer is cancelled.
E.16	Refund mechanism	Refunds will be processed manually by the Foundation, which will transfer a relevant amount of ETH to the relevant Bidding Address used by the participant in the auction. EU purchasers who are retail holders as defined in Article 3(1)(37) of Regulation (EU) 2023/1114 of the European Parliament and of the Council ("**MiCA**") may contact the Foundation directly to initiate a refund within the withdrawal period.

E.17	Refund timeline	Refunds will be processed within a reasonable time period and no later than 14 days after receipt of a valid withdrawal declaration by a retail holder.
E.18	Offer phases	The offer will be conducted in two phases, as described in item 10 in the Summary: a whitelisted Contributor Track for selected participants based on network contributions, followed by a Public Sale Track open to all qualified participants.
E.19	Early purchase discount	Yes. Discounted access to the public Token sale will be granted to contributors to the Aztec protocol and/or community selected by the Foundation via the Contributor Track, which allows relevant participants the opportunity of early bidding in the auction (as described in item 10 in the Summary), likely resulting in lower average prices. Contributor Track participants who place bids before Public Sale Track bidding opens are expected to receive a lower average clearing price than Public Sale Track participants if the auction clears above the floor price (rather than at the floor price). This early access will be granted in recognition of such participants' contributions to the development of the Aztec protocol or the Aztec community. Separate to the public offer (the Contributor Track and Public Sale Track), the Foundation currently intends to sell Tokens as follows: ● ***Genesis Sequencer Sale.*** The Foundation plans to sell 1.93% of the Initial Total Supply at a discount to the auction price in a private sale to purchasers the Foundation determines meet technical and alignment criteria relating to the operation of a genesis Sequencer. Participation in this private sale will be granted in recognition of such participants' ability and willingness to operate a genesis Sequencer for the Aztec Network. ● ***Bilateral Sales.*** The Foundation may also sell 2.44% of its treasury of AZTEC in bilateral private sales to strategic investors at prices determined by the Foundation. No bilateral sales are currently expected in 2025, but may be conducted at the Foundation's sole discretion.
E.20	Time-limited offer	Yes.
E.21	Subscription period beginning	Contributor Track: 18 days before day 1 of the auction being open and clearing, currently expected to be 13 November 2025, subject to technical and operational readiness. Public Track: day 2 of the auction being open and clearing, currently expected to be 2 December 2025, subject to technical and operational readiness.
E.22	Subscription period ends	Contributor Track: end of the last day of the auction, currently expected to be 6 December 2025, subject to technical and operational readiness. Public Track: end of the last day of the auction, currently expected to be 6 December

		2025, subject to technical and operational readiness.
E.23	Safeguarding arrangements for offered funds/crypto-Assets	ETH committed by participants in the auction will not be collected by the Foundation until after the end of the auction. During the auction, ETH committed by participants will be held in immutable, autonomous smart contracts governing the auction not controlled by the Foundation. Following the auction, the proportion of the ETH paid by purchasers in the auction transferred to the Foundation by the auction smart contract will be received into a crypto-asset account in the Foundation's name.
E.24	Payment methods for crypto-asset purchase	Purchasers must pay in ETH using their Bidding Address.
E.25	Value transfer methods for reimbursement	Reimbursements will be made in ETH to a participant's Bidding Address.
E.26	Right of withdrawal	During the subscription period, purchasers in the EU who are retail holders as defined in Article 3(1)(37) of MiCA will have a right to withdraw from their agreement to purchase Tokens without incurring any fees or costs and without being required to give reasons. To exercise it, they must contact the Foundation and request a refund before the end of the subscription period.
E.27	Transfer of purchased crypto-assets	Tokens will be transferred to ATPs and subject to the mandatory staking requirement (where relevant) and lockup, as described in item 10 of the Summary.
E.28	Transfer time schedule	Tokens will be transferred to ATPs as described in item 10 of the Summary immediately following the conclusion of the auction.
E.29	Purchaser's technical requirements	Purchasers must hold a wallet capable of interacting with Ethereum L1 and receiving ERC-20 tokens and have sufficient ETH to initiate required Ethereum L1 transactions.
E.30	Crypto-asset service provider (CASP) name	Not applicable.
E.31	CASP identifier	Not applicable.
E.32	Placement form	Not applicable.
E.33	Trading platforms name	Not applicable.
E.34	Trading platforms Market identifier code (MIC)	Not applicable.
E.35	Trading platforms access	Not applicable.
E.36	Involved costs	Not applicable.
E.37	Offer expenses	The following key offer expenses have been incurred (or are expected to be incurred) related to the preparation and/or implementation of this offer:

Expense Item	**Estimated Cost (US$)**

		<table><tr><td>Legal advisory</td><td>US$300,000</td></tr><tr><td>Compliance tooling integration</td><td>US$131,000</td></tr><tr><td>Token sale website development</td><td>US$131,000</td></tr><tr><td>Audit of Ignition and governance contracts</td><td>US$300,000</td></tr></table> **Disclaimer**: the above estimated key expenses are indicative only as at the date of the white paper, are not exhaustive and are subject to change, pending receipt of all final invoices from service providers and finalisation of the offer. Participants in the offer will also be required to pay for all Ethereum gas fees under or in connection with each transaction on the Ethereum blockchain required to participate in or take actions related to the public offer. Please see item 10 in the Summary for further information on this.
E.38	Conflicts of interest	To the Foundation's knowledge, there are no potential conflicts of interest of the persons involved in the offer to the public, arising in relation to the offer at the time of drawing up this white paper.
E.39	Applicable law	The applicable law governing participation in the offer will vary depending on where participants are located and what kind of participant they are (for example, because of mandatory jurisdiction-specific rules regarding the governing law relating to consumer contracts or conferring mandatory protections on consumers under the law of the jurisdiction in which they are located). The applicable law in any given case will therefore be as explained to participants in the terms and conditions governing participation in the sale, which participants will be required to actively agree to before being able to participate in the auction.
E.40	Competent court	The competent court for disputes arising in relation to the offer will vary depending on where participants are located and what kind of participant they are (for example, because of mandatory jurisdiction-specific rules relating to the ability for consumers to commence disputes in their local courts or governing the use of arbitration). The competent court for any given dispute will therefore be as explained to participants in the terms and conditions governing participation in the sale, which participants will be required to actively agree to before being able to participate in the auction.

6. Part F - Information about the crypto-assets

F.1	Crypto-asset type	AZTEC is a crypto-asset falling under Title II of MiCA, being a crypto-asset other than an asset-referenced token or e-money token. With respect to Switzerland, in its position letter dated 4 April 2025, the Swiss

		Financial Market Supervisory Authority ("**FINMA**") confirmed that AZTEC qualifies as a utility token under Swiss financial market laws. The Token is issued on Ethereum (ERC-20) and provides access to and enables use of the Aztec Network. Its functions are limited to: ● Staking to become a Sequencer and secure the Aztec Network; and ● Participating in Aztec Governance by voting on protocol upgrades and parameters. ● Paying for transaction execution and block space on the Aztec Network, if and when the Execution Environment is activated by Sequencers; AZTEC does not offer any other payment function, and is not intended to be used for the acquisition of goods or services, and/or as a means of money or value transfer. Further, it does not grant ownership rights, profit participation, repayment claims, or rights to financial returns, and is not backed by any underlying asset. On this basis, FINMA further confirmed that it is neither a payment token nor an investment token under Swiss financial market law and does not constitute a deposit or security.
F.2	Crypto-asset functionality	The Token is intended to serve the following main functions on the Aztec Network: – ***Sequencer Staking***. The Token will be used to secure the Aztec Network through staking by Sequencers, who will be responsible for the production of blocks within Aztec. Sequencers will need to stake the Token and in return for doing so they will obtain the right to produce blocks and may be entitled to receive block rewards in the form of Tokens when a block they proposed is successfully proven on Ethereum L1. – ***Governance***. Tokens will also enable participation in Aztec Governance through a two-stage process: (i) Sequencer signalling, followed by (ii) Token holder ratification, as described in item 08 of the Summary. – ***Execution Environment (future)***. If and when at a future date Aztec is upgraded by Aztec Governance to enable the Execution Environment, the Token will serve as the means to pay for transaction fees within the Aztec Network. If and when the Execution Environment is enabled, the Token will likely have to (i) be bridged from Ethereum (L1) to Aztec (L2) for this purpose (i.e., to pay for transaction fees) and (ii) be non-transferrable once it is transferred to Aztec.
F.3	Planned application of functionalities	Sequencer staking will be possible from the deployment of the smart contracts for the Aztec Network's governance and staking system functionality by the Foundation. Use of the Token to participate in Aztec Governance will be available if and when Ignition occurs. The use of Aztec to pay for transaction fees within the Aztec Network will only apply if and when at a future date Aztec is upgraded by Aztec Governance to enable the Execution Environment. **Disclaimer**: Neither the Foundation nor Labs controls protocol upgrades nor the

		implementation of any future milestones into the Aztec Network. The planned functionalities described above are indicative only and may not occur. By purchasing AZTEC, you acquire the current functionality of the Token based on the Aztec Network as it exists at the time of purchase. The future of the Aztec Network will be determined by Token holders through the Aztec Network's governance process.
A description of the characteristics of the crypto-asset, including the data necessary for classification of the crypto-asset white paper in the register referred to in Article 109 of Regulation (EU) 2023/1114, as specified in accordance with paragraph 8 of that Article		
F.4	Type of crypto-asset white paper	OTHR
F.5	The type of submission	NEWT
F.6	Crypto-asset characteristics	**Overview**. - AZTEC is the native crypto-asset of the Aztec Network. - AZTEC is a fungible ERC20 token recorded on the Ethereum blockchain. - The staking of AZTEC and the payment of block rewards to Sequencers and provers will take place on Ethereum. **Key functionality**. The Token is intended to serve the main functions on the Aztec Network described in F.2. **No profit rights, ownership, etc**. AZTEC does not confer any profit rights, ownership in the Foundation, rights to financial returns, and is not backed by any underlying asset. Its sole purpose is to facilitate decentralized participation in and usage of the Aztec protocol.
F.7	Commercial name or trading name	Not applicable.
F.8	Website of the issuer	https://aztec.foundation
F.9	Starting date of offer to the public or admission to trading	13 November 2025, subject to operational and technical readiness.
F.10	Publication date	12 November 2025
F.11	Any other services provided by the issuer	None. The Foundation does not provide services outside the scope of MiCA. It does not act as a CASP or financial service provider under other EU or national frameworks.
F.12	Language or languages of the crypto-asset white paper	English
F.13	Digital token	Not applicable.

	identifier code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates, where available	
F.14	Functionally fungible group digital token identifier, where available	Not applicable.
F.15	Voluntary data flag	False.
F.16	Personal data flag	True.
F.17	LEI eligibility	True.
F.18	Home Member State	Ireland
F.19	Host Member States	Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden.

7. *Part G - Information on the rights and obligations attached to the crypto-assets*

G.1	Purchaser rights and obligations	Purchasers of the Token obtain the rights to participate in staking (including delegated staking) and Aztec Governance. Purchasers do not acquire ownership, profit-sharing rights, or any entitlement to financial returns. The token does not represent a claim on any asset or obligation of the Foundation. Purchasers will also have the rights and obligations set out in the terms and conditions governing the public Token sale.
G.2	Exercise of rights and obligations	In order to exercise their rights, Token holders must: ● Use a compatible Ethereum wallet to interact with the Aztec protocol with sufficient ETH to initiate Ethereum transactions. ● Stake Tokens to participate as Sequencers. ● Delegate or lock tokens in order to vote in governance proposals.
G.3	Conditions for modifications of rights and obligations	Any modification to Token-related rights and obligations must be passed via Aztec Governance. Successful proposals may modify network parameters such as staking requirements, governance structure, certain unlock conditions, or Token supply.
G.4	Future public offers	As of the date of this white paper, there are no anticipated future public offers planned by the Foundation beyond this initial public Token sale.
G.5	Issuer retained crypto-assets	The Foundation will retain a portion of the AZTEC supply not allocated to the Labs team or the public sale. These retained tokens are intended to support protocol development, community initiatives, and other operational activities. See D.9 and item 08 of the Summary for more details, including the intended amount of Tokens that will be retained by the Foundation.

G.6	Utility token classification	False.
G.7	Key features of goods/services of utility tokens	Not applicable.
G.8	Utility tokens redemption	Not applicable.
G.9	Non-trading request	False.
G.10	Crypto-assets purchase or sale modalities	AZTEC is transferable and holders may therefore be able to transact in AZTEC on the secondary market, subject to applicable lock-up restrictions and governance votes. After the auction, secondary market liquidity may become available via the Liquidity Pool.The smart contracts governing the auction will be programmed such that (i) a proportion of the ETH paid by purchasers in the auction, and (ii) a proportion of AZTEC determined by reference to the number of AZTEC allocated to the auction from the Initial Total Supply, will be autonomously transferred by the auction smart contract to the Liquidity Pool. With respect to the AZTEC to be transferred, the Foundation will fund the auction smart contract with sufficient Tokens at the outset to cover this transfer (meaning that participants will receive via ATPs 100% of the AZTEC they purchase in the auction). Out of the Tokens allocated to the auction for this offer, 15% of such Tokens will be transferred autonomously to the Liquidity Pool. The Liquidity Pool will be controlled by Aztec Governance and locked in an immutable smart contract for at least 90 days from the Public Offer Date, after which Aztec Governance can vote to lift such restrictions.
G.11	Crypto-assets transfer restrictions	Tokens purchased in the auction will be subject to the mandatory staking requirement (where relevant) and lockup, as described in Section 10.
G.12	Supply adjustment protocols	True.
G.13	Supply adjustment mechanisms	On and from the Public Offer Date for the first twelve (12) months, the Initial Token Supply cannot increase. From twelve (12) months after the Public Offer Date: (i) Aztec Governance will be able to change the total supply of the Aztec Token, including by increasing the Initial Total Supply by up to a percentage capped per annum as further described below in H.5; and (ii) if and when the Execution Environment is enabled by Aztec Governance, fees will likely be regulated autonomously (intended to be similar to Ethereum's EIP-1559) by the Aztec Network.
G.14	Token value protection schemes	Not applicable.
G.15	Token value protection schemes description	Not applicable.
G.16	Compensation schemes	Not applicable.
G.17	Compensation schemes description	Not applicable.
G.18	Applicable law	Swiss law

G.19	Competent court	Zug, Switzerland.

8. Part H – Information on the underlying technology

H.1	Distributed ledger technology (DLT)	AZTEC is issued as an ERC-20 token on Ethereum Layer 1. The Aztec Network is a Layer 2 rollup built on Ethereum.
H.2	Protocols and technical standards	AZTEC adheres to the ERC-20 token standard on Ethereum Layer 1. Participants in the Aztec Network interact with the Aztec Layer 2 rollup via staking and governance. The Aztec Network is intended to be a general-purpose layer 2 built on Ethereum. Compared to Ethereum and similar blockchains, the innovations of the Aztec Network relate to how transaction data may be stored, and the extent to which transaction data is accessible to third parties that are not involved in the transactions, subject to the Execution Environment being live. These innovations are based on seminal research in applied mathematics and cryptography pioneered by Dr. Williamson and colleagues. The protocol at Ignition will consist of a decentralised network of sequencers and provers and a governance system. If and when the Aztec Network is upgraded by Aztec Governance to enable the Execution Environment, this may enable developers to deploy smart contracts with public and private transaction flows, account abstraction and fee abstraction. If any contracts are deployed, users may send transactions to these smart contracts.
H.3	Technology used	Ethereum blockchain, Solidity, Noir, Typescript, C++, Rust and other ancillary technologies.
H.4	Consensus mechanism	At Ignition, the consensus mechanism of Ethereum Layer 1 (Proof of Stake) is used for the issuance, storage and transfer of AZTEC.
H.5	Incentive mechanisms and applicable fees	On and from Ignition, 250,000,000 Tokens from the Initial Total Supply will be used to incentivise Sequencers to stake Tokens and produce blocks and as a result receive block rewards in the form of Tokens. This block reward is split between entities who participated in block production including those who compute and submit aggregation proofs to Ethereum, proving the correctness of a set of blocks. The exact split between Sequencers and provers is determined by the protocol when blocks are produced, factoring in market costs, subject to Aztec Governance directly setting out the basis point split of block rewards between Sequencers and provers. From twelve (12) months after the Public Offer Date: (i) Aztec Governance will also be able to change the total supply of the Aztec Token, including by increasing

		the existing Aztec Token supply at that time by up to a fixed percentage of the current Total Supply per annum ("**Token Mint Cap**") to create any Sequencer incentive mechanisms or otherwise and (ii) if and when the Execution Environment is enabled by Aztec Governance, fees will likely be regulated autonomously (intended to be similar to Ethereum's EIP-1559) by the Aztec Network. The Token Mint Cap cannot be changed by Aztec Governance once set, but actual network inflation does not have to fill the entire Token Mint Cap at the discretion of governance. The Token Mint Cap will be set immediately prior to the Public Offer Date and is expected to be between 10% and 30%. This has been set to ensure that Aztec Governance can create funds for block rewards and respond to any contingency that could be foreseen, but still impose a cap to prevent malicious or bugged use of the issuer contract to mint an excessive amount of Tokens.
H.6	Use of distributed ledger technology	AZTEC is issued, stored and transferred on Ethereum Layer 1, which is a public distributed ledger not operated by the issuer or a third party acting on its behalf.
H.7	DLT functionality description	Not applicable.
H.8	Audit	Third-party audits of the technology for all aspects of the contracts deployed at the Public Offer Date are ongoing and scheduled to be completed before the Public Offer Date. Future audits for Alpha are ongoing or yet to be started.
H.9	Audit outcome	Existing completed audits have identified bugs, in some cases material. At the time of preparing this white paper, for most of the relevant components, at least two independent audits have already been completed. These reviews identified issues ranging from routine bugs and optimisations to more serious vulnerabilities, all of which have since been remediated or are in the process of remediation. At the time of preparing this white paper, fixes are currently being applied to the smart contracts. At the time of preparing this white paper, audit reports are not public as publication before remediation could create unnecessary risks. Reports related to governance and rollup components may be released in due course, and any audits relating to the token sale contracts will only be published immediately prior to the sale to avoid alerting the public prematurely to the fact of the sale. Further security assessments for Ignition contracts are ongoing.

9. Part I – Information on risks

I.1	Offer-related risks	**Legal, regulatory and compliance risk**: The legal, regulatory and compliance environment relating to crypto-assets (including public offerings) varies across jurisdictions where the AZTEC public Token sale is conducted, may be uncertain, and is subject to change. Authorities in relevant jurisdictions could reach different conclusions about the application of legal, regulatory and compliance requirements to the AZTEC public Token sale, which could impact the Foundation's ability to execute the sale, the delivery of Tokens to purchasers, the value of the Token, or the ability for purchasers to stake, participate in governance, transfer or transact in the Token, including on secondary markets. Changes to legal, regulatory and

		compliance requirements, or changes to their application or interpretation, may also impact the offeror's ability to execute the sale or deliver Tokens or levels of participation in the sale. **Smart contract risks**: The successful completion of the AZTEC public Token sale depends on the correct design and operation of various smart contracts, including the smart contracts governing the auction and ATPs. Some of the smart contracts involved in the public Token sale (in particular, those relating to the auction) were not designed or deployed (for example, the Uniswap TWUCA contracts) by the Foundation and are not under its control. Those smart contracts relevant to the Token sale (including those necessary for Ignition) that have been designed by the Foundation are generally no longer subject to the Foundation's control once deployed. Any smart contract relevant to the Token sale or the Aztec Network may be exposed to technical vulnerabilities or issues (including errors in design or implementation or hacks) that could lead to unforeseen or adverse consequences, including but not limited to the Token sale (including, but not limited to, the auction) not operating as envisaged or at all, participants not being allocated Tokens as expected (including with respect to prices obtained by participants in the auction), participants not being able to participate in the auction, participants losing ETH committed via the auction, or participants being unable to access purchased AZTEC. **Network risks**: The AZTEC public token sale is conducted via the Ethereum network, which is a decentralized, public permissionless blockchain, not controlled by the Foundation. Any changes or interruptions to the accessibility, availability or operation of the Ethereum blockchain during or around the time of the Token sale could have adverse consequences for the Token sale, participants, or the Foundation. Participants may also be exposed to changes in the costs of executing transactions on the Ethereum blockchain (i.e., Ethereum gas fees), which may be material and will be necessary to (among other things) participate in the Token sale, access purchased AZTEC, and stake, transfer or transact in the Token. Participants should also be aware that information relating to their participation in the Token sale and other actions taken in relation to AZTEC on the Ethereum network may be public. **Lockup**: In some cases, the release of AZTEC from lockup restrictions depends on a vote to lift such restrictions being passed via Aztec Governance. This requires a relevant proposal to be initiated by a Sequencer and passed via a Token holder vote. The Foundation will not have control over the initiation of such a proposal or the outcome of any Token holder vote in relation to such a proposal, and there can be no guarantee that such a proposal will be initiated or, if initiated, passed.

		Insider vesting and unlocks: Tokens allocated to early stage investors in the project and the project team are subject to vesting schedules and/or lockups. When these Tokens are released into circulation, this may introduce additional selling pressure, which could impact the value of Token. **Participation risk**: Low rates of participation in the genesis Sequencer private sale or the AZTEC public Token sale may impact the success of the Aztec Network launch, including failure or delay of Ignition, which could adversely affect the value of the Token. **Concentration risk**: It is possible that the token distribution may not result in the intended broad dissemination of AZTEC across a diverse group of holders (for example, as a result of low levels of participation or a single entity purchasing large amounts of AZTEC at high prices in the auction or otherwise), which may impact the adoption, operations, success, and/or decentralisation of the Aztec Network. **No market in the Token**: Purchasers of AZTEC should be aware that there is currently no public market for the Token and there can be no assurance that a market will develop in the future. Consequently, purchasers may find it difficult or impossible to sell their Tokens at a desired time or price. The absence of a market may also adversely affect the value of the Token and purchasers may not be able to liquidate their Tokens readily or at all. The development of a market for the Tokens will depend on various factors, including the success of the Aztec Network, decisions taken or not taken via Aztec Governance, and overall market conditions. In particular, the activation of the Liquidity Pool which will be created with a portion of the proceeds of the public Token sale by purchasers depends on a vote to activate it being passed via the Aztec Governance mechanism. This requires a relevant proposal to be initiated by a Sequencer and passed via Aztec Governance. The Foundation will not have control over the initiation of such a proposal or the outcome of any Token holder vote in relation to such a proposal, and there can be no guarantee that such a proposal will be initiated or, if initiated, passed. Even if a market does develop, it may not be liquid and the price of the Tokens may be volatile. Purchasers should consider the potential illiquidity of the Tokens as a significant risk factor and be prepared to bear the economic risk of holding the Tokens for an indefinite period. **Auction mechanics risks**: User error in interacting with the auction smart contracts or a lack of understanding of the effects of the auction mechanics (including as to the effects of placing a bid or likely outcomes for the price of purchased AZTEC in different scenarios) could result in losses or unexpected outcomes for participants. In particular, participants should note that bids are binding once placed and that the Foundation will not have control over the auction smart contracts once deployed. Participants should only participate in the auction if they have an appropriate understanding of the auction mechanics, functioning of the auction smart contracts

		and are able to sustain any potential losses that may be incurred as a result of participating in the auction. **Taxation**: The tax treatment of the Token may vary by jurisdiction and based on the particular circumstances of participants or Token holders. Participants and Token holders are solely responsible for understanding their own tax position in relation to participation in the Token sale and holding or transacting in AZTEC, and complying with applicable tax laws.
I.2	Issuer-related risks	**No claim on the issuer**: Purchasers of AZTEC should note that it does not constitute or represent a claim against or any obligation of the Foundation or any other legal person. In particular, Token holders will not have rights or entitlements to share in ownership or profits of the Foundation, receive income or repayment of any sort from the Foundation, participate in the assets of the Foundation, or voting rights akin to those of shareholders in companies or partners in partnerships. **Ignition and lack of control**: Generally, the Foundation will not have control over the smart contracts relating to AZTEC, the public Token sale, the Aztec Network and the Liquidity Pool, once deployed. In particular, the Foundation will not have control over the occurrence or timing of Ignition or Alpha, which will depend, respectively, on a sufficient threshold of Sequencers staking Tokens to secure the network economically and a future Sequencer-initiated vote passed by Aztec Governance to upgrade the Aztec Network to enable the Execution Environment. **Foundation and/or board ceases to steward Aztec Network**: The ongoing and primary role of the Foundation and its existing management (which, as at the date of this white paper is Zachary Williamson, Arnaud Schenk and Herbert Sterchi) (each a "**Board Member**") is to steward the Aztec Network. While the Aztec Network at Ignition is intended to function without any control or manual input required from the Foundation or any one of its Board Members, the security, stability and future success of the Aztec Network may require involvement from the Foundation and its Board Members, including, in the short-term: ● scheduling and paying for audits of key components of the current Aztec Network and future versions that intend to ensure its security, stability and future success; ● funding grants for ongoing work on core components of the Aztec Network; ● maintaining certain open source cryptographic libraries and the programming language Noir, which is intended to be used by developers deploying applications on the Aztec Network, if and when the Execution Environment is enabled by Aztec Governance; ● funding and co-ordinating work on a staking and governance dashboard for Aztec Governance; ● funding developer events and educational content related to the Aztec Network and Noir; and

		● funding and/or organising any other activities / developments that may increase the security, stability, marketability and future success of the Aztec Network. If (1) the Foundation or any of its Board Members, management or contractors/employees ceases to provide, or decreases, the support for and stewardship of the Aztec Network and/or (2) any one of its Board Members leave or is unable to remain or continue to be on the Foundation board or involved with the Aztec Network, this may negatively impact the success of the Aztec Network, its utility and the value of the Token. **Labs (and other software developers) and/or founder / management cease to provide services and/or support to the Foundation and for the Aztec Network**: The ongoing and primary role of Labs (including its founder Joseph Andrews ("**Labs Founder**") and certain other management) at least until Alpha is currently intended to be limited to providing certain services / support to the Foundation / the Aztec Network. While the Aztec Network at Ignition is intended to function without any control or manual input required from Labs and its Founder, Labs will be providing certain services / support to the Foundation / the Aztec Network, including under: ● a services agreement for at least 12 months, for certain transition services to the Foundation, including, without limitation: ○ marketing services; ○ research and technical development activities, including to fix any bugs or improvement suggestions that are raised during the audit process; ○ services relating to ecosystem development and decentralisation initiatives; ○ certain finance, tax and accounting services and certain in-house counsel, policy, and other advisory and related administrative services; and ○ any other services agreed between the Foundation and Labs, ● a grant agreement for up to 5 years, for the development and maintenance of an Aztec typescript client for Sequencers; ● a grant agreement for up to 5 years, to maintain and improve certain developer tooling for writing and interacting with smart contracts on the network, including Aztec.nr and the Private Execution Environment ("**PXE**", pronounced "pixie"), a client-side library for the execution of private operations. In addition, the Foundation may also enter into similar contracts with other software developers. On and after Alpha, Labs may develop important applications on the Aztec Network which may showcase the power and functionality of the Aztec Network, which may have significant positive effects on the Aztec Network.

		If (1) the Foundation ceases to cooperate and/or pay for contracts / grants with Labs and/or any other software developer and Labs and/or any developer ceases to provide, or decreases, the support for the Aztec Network and/or Noir and/or (2) any one of the Labs Founder or any of the Labs management leave or are unable to remain or continue to be with Labs or involved with the Aztec Network, this may negatively impact the success of the Aztec Network, its utility and the value of the Token. **Third-party risks**: The Foundation relies on external service providers / third party infrastructure (including, without limitation, the Ethereum network, ZKPassport, Uniswap, SumSub, TRM Labs, FS Vector, Predicate, etc) to provide essential services and/or infrastructure in relation to the Token sale and the Aztec Network. Any issues faced by such third parties / infrastructure elements, or their failure to perform actions required to facilitate the Token sale or the Aztec Network could directly impact the Foundation's ability to execute the Token sale, the launch of the Aztec Network, and the value of the Token. **Reputational risks**: Negative publicity about the Foundation, its Board Members, management or contractors/employees could damage the Foundation's reputation and, by extension, impact confidence in or the adoption or use of the Aztec Network and the value of the Token.
I.3	Crypto-assets-related risks	**Loss of private keys**: A participant's ability to participate in the auction is subject to their safeguarding of relevant crypto-assets and private keys, in particular their Soulbound NFT and the private key to their Bidding Address. Similarly, a Token holder's ability to access AZTEC is subject to their safeguarding of their own private keys (including, with respect to AZTEC purchased in the Token sale, the private keys to their Bidding Address or another Ethereum address specified by the participant to control the ATP to which their Tokens will be transferred). AZTEC is vulnerable to the risk of loss where participants lose or expose their private keys, or rely on unproven or vulnerable wallet or custody services, and the Foundation will not be able to provide assistance or remedy to Token holders in such circumstances. **Irreversibility of blockchain transactions**: Transactions in AZTEC may be irreversible and users may lose some or all of their AZTEC if they execute a transfer to an unintended blockchain address. **Scam risk:** Malicious actors may set up fake or fraudulent websites (including fake frontends purporting to relate to the Token sale) or use other means to attempt to defraud purchasers before, during or after the public Token sale. Purchasers should ensure that they only act on information communicated by the Foundation in relation to the Token or Token sale via official channels and check that relevant frontends, blockchain addresses and transactions are legitimate before providing

		sensitive or personal data or authenticating any transactions. As Tokens become freely transferable, holders may be susceptible to scam or fraud attempts from malicious actors, leading to losses for holders of AZTEC where AZTEC is transferred from a holder's wallet or address.
I.4	Project implementation-related risks	**Launch and anticipated future milestones risk**: As at the date of publication of this white paper, the deployment of the Aztec protocol, Ignition of the Aztec Network, and other anticipated future milestones in relation to the Token and the Aztec Network have not occurred, and there can be no guarantee that these things will be completed as intended, in a timely fashion, or at all. Delays in development, changes to designs or technical specifications, delays or failure to complete necessary audits or required remediations, lack of participation by key ecosystem participants (including, but not limited to, Sequencers and provers) may result in delay, material change to, or non-occurrence of one or more of the following as contemplated in this white paper: deployment of the smart contracts for the Aztec Network's governance and staking system functionality; the public Token sale; Ignition; the Liquidity Pool, Alpha; and the expected features and functionality of Aztec, including, without limitation, the potential upgrade of the Aztec Network to enable the Execution Environment. Any forward-looking statements in this white paper and/or made by the Foundation or its employees/contractors on social media (X, Linkedin, Discord, Aztec Network website, etc) ("**Social Media**") about AZTEC or the Aztec Network (including, for example, statements using terms such as "may", "will", "expected", "anticipated", "intended", the negative of such terms, or similar expressions) are therefore only predictions, based largely on the Foundation's understanding and expectations about the plans for development and launch of the Aztec Network and AZTEC as at the date of this white paper, but which are inherently subject to known and unknown risks, uncertainties, and other important factors (which may be beyond the knowledge or control of the Foundation) that may impact the actual outcomes in each case. **Accordingly, any forward-looking statements in this white paper or on Social Media should not be relied on as reliable or accurate statements about future events. The events and circumstances set forth in any forward-looking statements may not be achieved or occur and actual results could differ materially from those stated.** **Competition risk**: There are an increasing number of crypto-asset projects (including those seeking to leverage privacy enhancing technologies such as zero-knowledge proofs, interactive multi-party computation, homomorphic encryption, trusted execution environments, and/or a combination of the foregoing to solve the same or similar problems or provide the same or similar functionality as the Aztec Network), which may compete with the Aztec Network for participants and adoption. Low participation or adoption due to competition from other projects may impact the launch of the Aztec Network, its continuing operation post-launch, or the overall success of the project. The project may be unable to compete with larger or better resourced projects, which may negatively impact the success of the project, its utility and the value of the Token.

		Participation risk: As a new network project, the success of the Aztec Network is dependent on participant involvement. Low rates of participation (including in the public Token sale) may impact the success of the Aztec Network launch or the implementation of anticipated future milestones, either of which could adversely impact the utility and value of AZTEC. In particular, the long-term success of the Aztec Network is dependent on widespread adoption of the Network by a broad group of ecosystem participants, including developers, users, infrastructure providers (such as Sequencers and provers), and other participants. Adoption will be influenced by various external factors, including user demand, competitive market conditions, and organic community-driven expansion. There is no guarantee of sufficient demand for, or continued adoption and operation of, the Aztec Network. If adoption of the Aztec Network fails to grow, or if key ecosystem participants do not continue to conduct activities necessary for the ongoing operation of the Network, the value of the Token may be significantly impacted.
I.5	Technology-related risks	**Reliance on Ethereum**: AZTEC is an ERC-20 token issued, stored and transferred via the Ethereum network. Congestion, disruptions, outages, or security breaches in the Ethereum network could therefore impact the availability or functionality of AZTEC, including the ability of Token holders to access, stake, transfer or transact in the Token. **Cryptography risks**: Any cryptography proving system relevant to the Aztec Network, AZTEC, Ignition and/or the Token sale at any time (including, without limitation, the use of cryptographic zero-knowledge proofs by ZKPassport for certain checks as part of the Token sale) may be exposed to technical vulnerabilities and/or issues (including errors in design and/or implementation and/or hacks) that could lead to unforeseen and/or adverse consequences for participants or Token holders. The technology and software involved in the Aztec Network, AZTEC, and/or the Token sale is new and untested at scale and any issues and/or vulnerabilities could adversely impact the utility and value of AZTEC. **Smart contract risks**: Any smart contract relevant to the Aztec Network, AZTEC, Ignition and/or the Token sale at any time (including, without limitation, Uniswap's smart contracts for novel auction mechanics and/or liquidity pool creation utilised for the Token sale) may be exposed to technical vulnerabilities and/or issues (including errors in design and/or implementation and/or hacks) that could lead to unforeseen and/or adverse consequences for participants or Token holders. The technology and software involved in the Aztec Network is new and untested at scale and any issues and/or vulnerabilities could adversely impact the utility and value of AZTEC. **Programming language risks**: Any programming language relevant to the Aztec Network, AZTEC, and/or the Token sale at any time (including, without limitation, the use of Noir, a new programming language initially developed by Labs) may be exposed to technical vulnerabilities and/or issues (including errors in design and/or

		implementation and/or hacks) that could lead to unforeseen and/or adverse consequences for participants or Token holders. The technology and software involved in the Aztec Network, AZTEC, and/or the Token sale is new and untested at scale and any issues and/or vulnerabilities could adversely impact the utility and value of AZTEC. **Network attacks and cyber security risks**: Blockchain networks can be vulnerable to a variety of cyber-attacks, including 51% attacks, where an attacker gains control of the majority of the network's consensus, Sybil attacks, or DDoS attacks. These can disrupt the network's operations and compromise data integrity, affecting its security and reliability. **Consensus Failures or Forks**: Faults in the consensus mechanism or schisms within the community can lead to network halts or forks (where multiple versions of the blockchain coexist, creating uncertainty around which version should be canonical) potentially destabilising the network, reducing trust among participants, and/or adversely impacting the utility and value of AZTEC.
I.6	Mitigation measures	With respect to various risks discussed in this Part I, the Foundation has taken or will take steps to mitigate certain of these risks as follows. 1. Mitigation measures concerning offer-related risks **Legal, regulatory and compliance risk:** The Foundation has engaged internal and external legal counsel and compliance experts to understand and address legal, regulatory and compliance requirements associated with the AZTEC public Token sale. **Smart contract risks:** The source code of all smart contracts that have or will be deployed by the Foundation will be publicly available in real time, and have or will be comprehensively and independently audited before deployment. The Foundation will not retain any rights over deployed smart contracts. They will either be fully immutable or owned and controlled through the Aztec Governance process. Where audits reveal potential vulnerabilities or issues, steps are taken to address these before deployment of the smart contracts. 2. Mitigation measures concerning issuer-related risks **Third-Party Risks:** When the Foundation relies on a third party to provide important services, it generally seeks to enter into an agreement containing specific clauses ensuring that the service provider cannot terminate the business relationship without notice. Third parties with whom the Foundation contracts may also be

		subject to due diligence procedures to ensure their financial viability and to limit any other risks of non-compliance. 3. Mitigation measures concerning crypto-assets-related risks **Scam Risk**: The Foundation cannot directly prevent scams related to AZTEC. At the same time, the Foundation will endeavour to educate users about AZTEC, how to participate in the public Token sale and how to use AZTEC, as well as about scam risks and how to avoid them via various channels. In addition, Labs is engaged with a service provider, Chainpatrol, that intends to automatically detect any Aztec-focused scam websites, accounts, channels and videos on popular platforms and reports them to platform owners of third-parties (e.g., wallet extensions) in case of fraudulent websites. **Irreversibility of blockchain transactions**: The Foundation cannot directly control for this possibility based on user error, but it will inform users about this risk in the context of the Token sale. 4. Mitigation measures concerning project implementation-related risks Steps taken to mitigate project implementation-related risks include: a. Distribution of the Ecosystem Grants pool to enable and incentivise participation by appropriately experienced and qualified persons in future development of the protocol. b. Implementation of certain internal / external policies and documents at the Foundation and Labs to mitigate various implementation, entity, and other risks. c. Entry into contractual arrangements with third parties (Predicate, ZKpassport and others) required for Ignition and the Token distribution that intend to detail all relevant steps contractors need to take to perform and implement their services. d. Obtaining D&O insurance for directors and officers at the Foundation and Labs for board members to mitigate personal risks for these key individuals, with a view to encouraging their ongoing participation in the project. e. Continued hiring for key security and engineering roles to mitigate risk and impact of key person departures.

		5. Mitigation measures concerning technology-related risks The software development process used to develop the Aztec protocol has used known best practices for engineering secure systems, has been coordinated by a highly skilled and experienced project team, and has been subject to scrutiny and testing by the Aztec community. Any changes to the code during development go through a multi-stage testing process before they are deployed. Labs is also engaged with security provider, Groom Lake, to ensure the operational security of the organisation. The software is also subject to comprehensive and independent code auditing, designed to detect potential vulnerabilities or issues prior to deployment. Additionally, to address any potential undiscovered issues Aztec intend to implement a Bug Bounty concerning deployed smart contracts. These practices include the following: **Assurance techniques and tooling (non-exhaustive):** ● Automated testing (including property- and fuzz-style tests with randomised inputs) across key codepaths. ● Invariant testing on critical components. ● Coverage-guided fuzzing built in-house, plus external fuzzing for Noir (by Fuzzing Labs and ConsenSys Diligence). ● Specialised static and dynamic analysis tooling aimed at detecting issues in zero-knowledge proof (ZKP) systems. ● Formal verification of selected ZKP primitives by an internal security team. ● Internal peer reviews by implementing teams with cross-team review. ● External audits by multiple independent firms (including Veridise, Cantina/Spearbit, Zellic, ZKSecurity, and independent researchers Igor Konnov and Thomas Pani). ● Formal verification of governance smart contracts by external experts. ● Fuzzing of smart contracts by external auditors (e.g., Veridise using its proprietary tool Orca).

		• Supply-chain security monitoring (e.g., via socket.dev) to detect dependency risks and potential supply-chain attacks. We have performed audits of the previous Aztec products: • Audit of Aztec Protocol by Trail of bits in 2019 (https://github.com/trailofbits/publications/blob/master/reviews/aztec.pdf) • Audit of Aztec Protocol by Consensys Diligence in 2019 (https://github.com/ConsenSysDiligence/aztec-audit-report-2019-04) • Audit of the cryptography library barretenberg in 2022 (https://github.com/AztecProtocol/aztec-connect/blob/master/audits/Security%20Audit%20%20Results%20-%20Aztec%20Protocol.pdf) **2024–2025 audit programme for the current Aztec Network:** To select ongoing partners for the current audit programme, multiple firms were engaged to audit the same primitives, including: • Cantina (Spearbit) • Zellic • ZKSecurity • Veridise **Recent and in-flight audits in preparation for Ignition (2025):** • Veridise: big-field ZKP circuit primitive. Fix review pending; final report intended to be published thereafter. • Cantina (Spearbit): field ZKP circuit primitive. • ZKSecurity: Token Generation Event (TGE) smart contracts. • Cantina (Spearbit): TGE smart contracts. • Igor Konnov (initial): governance smart contracts. • Igor Konnov & Thomas Pani: formal verification of governance smart contracts. Findings under review.

		• Cantina (Spearbit): governance smart contracts. • Veridise: governance smart contracts. • Cantina (Spearbit): rollup smart contracts. • Cantina (Spearbit): token sale & soulbound smart contracts. • Veridise: token sale & soulbound smart contracts. • Cantina (Spearbit): staking registry and staking extension smart contracts. • Veridise: staking registry and staking extension smart contracts. For all critical components, it is intended that at least two independent audit teams will be commissioned following internal reviews. **Website and ongoing audits:** Before the sale, it is intended that Cantina (Spearbit) will be engaged to audit the Token sale website. It is expected that Cantina (Spearbit) and Veridise and/or others will provide additional reviews across the stack as new functionality is released. Upcoming scopes include: • Veridise: parts of the Noir compiler. • Veridise: additional Noir compiler scope. **Disclaimer:** The above listed mitigation measures may not be implemented as contemplated or prove effective; no assurance is given that they will reduce or eliminate the risks described.

10. Part J – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts

J.1	Adverse impacts on climate and other environment-related adverse impacts	The operation of the Aztec Network relies on Ethereum Layer 1, which transitioned to a Proof-of-Stake consensus mechanism in 2022 and is widely recognized as having a low environmental footprint compared to Proof-of-Work systems. At Ignition, the Aztec Network itself is expected to rely on a distributed set of Sequencers, Full-nodes, and Provers. Energy use remains modest when compared to large-scale Proof-of-Work networks. No material adverse impacts on climate, natural resources, or waste generation have otherwise been identified in connection with the project.

S.1	Name	Aztec Foundation
S.2	Relevant Legal Entity Identifier	506700JRDV5Z828A9D47
S.3	Name of the Crypto-Asset	AZTEC Token
S.4	Consensus Mechanism	Finality of Aztec state is secured by Ethereum Layer 1 Proof-of-Stake, which validates and stores the cryptographic proofs which prove the validity of a set of Aztec Network blocks. These cryptographic proofs are computed by a set of provers (no more than 5 at any given time), and Aztec Network blocks are created by a distributed set of sequencers. Sequencers gain the right to produce blocks by staking AZTEC. The Aztec Network does not operate an independent consensus algorithm.
S.5	Incentive Mechanisms and Applicable Fees	See Section H.5
S.6	Beginning of the Period to Which the Disclosure Relates	12 November 2025
S.7	End of the Period to Which the Disclosure Relates	12 November 2026

S.8	Energy Consumption	**Scope** This disclosure covers the systems on which AZTEC relies during the period, being: (i) Ethereum Layer 1 (issuance, staking, rewards, and governance) and (ii) the Aztec Network, composed of Sequencers, Provers and Full-nodes. *Sequencers* are computers tasked with creating and attesting to Aztec Network blocks. *Full-nodes* are computers which keep an up-to-date copy of all Aztec Network-relevant data, but do not participate in block creation. *Provers* are computers which compute cryptographic proofs of correct execution of batches of Aztec Network blocks. **Method** We used a bottom-up accounting of device-level energy use for the Aztec Network, plus a base-layer share allocated to the token on Ethereum using the Crypto Carbon Ratings Institute's hybrid approach. Rollup postings and proof verifications are excluded by this method and are covered via Aztec Network node energy use. Further details on methodology and assumptions can be found in S.9. **Result (annualised)** ● Aztec Network subtotal: **~310,090.86 kWh per year** ○ Sequencers (1,000 machines) → average ≈ 33.36 W per host → ~292,233.6 kWh per year. ○ Full Nodes (50 machines) → average ≈ 31.47 W per host → ~13,783.86 kWh per year. ○ Provers (5 machines) → average ≈ 93 W per host → ~4,073.4 kWh per year. ● Ethereum L1 allocation to the token: **6,294.3 kWh per year** ***Combined total:*** **316,385.16 kWh per year.** Total energy is < 500,000 kWh/yr, so Table 3 (S.10–S.16) disclosures are out of scope for this period under the RTS. **Variance** Since the Aztec Network is decentralized and permissionless from day one, actual Sequencer participation could differ from our assumptions here and in S.9, potentially affecting energy consumption estimates. While some mature and long running networks like Ethereum have grown to tens of thousands of machines participating in block production over a period of years, far in excess of our assumptions, most networks comparable to Aztec Network (Ethereum-based layer-2s) never exceed 1 to 3 Sequencers. To pick a conservative middle ground, we have aligned ourselves with the number of nodes involved in block production on Solana. Solana is a mature blockchain, in operation for more than 5 years. At the time of drafting this white paper, Solana Beach reports 985 active validators (roughly equivalent to our count of unique machines). Additionally, if and when Aztec Governance upgrades the Aztec Network to

		enable the Execution Environment, the energy consumption associated with the Aztec Network may change. The primary impact will be on the power consumption of Provers, but we do not expect it to have a significant impact on the overall power consumption of the network (<10% increase).
S.9	Energy Consumption Sources and Methodologies	**Scope and system boundary** This disclosure covers the systems on which AZTEC relies during the period, being: (i) Ethereum Layer 1 (issuance, staking, rewards, and governance) and (ii) the Aztec Network, composed of Sequencers, Provers and Full-nodes. Definitions of these roles are set out in S.8. We set the boundary to nodes of the Aztec Network (Sequencers, Full-nodes, Provers) and attribute a proportionate share of Ethereum L1 using CCRI's hybrid allocation. Rollup posts and proof verifications are excluded from the token's L1 share to avoid double counting because corresponding activity is already captured in L2 node/prover energy. **Approach** We follow the Crypto Carbon Ratings Institute methodology for non-PoW systems: count relevant nodes (including full-nodes), assign representative device power, and integrate over time. Since the Aztec Network is a Layer 2, this total is combined with an allocated share of the base chain using CCRI's hybrid allocation for tokens. The base-layer allocation refer to the following activities on Ethereum: ● Sequencers staking/unstaking ● Sequencers claiming rewards ● Token holders participating in governance ● Execution of slashing votes against Sequencers ● Owner-to-owner transfers Rollup operations (posting blocks, verifying proofs, etc…) are excluded from the L1 transaction share under CCRI; they are accounted for via node/prover energy. Since, at the date of this white paper, the Aztec Network is not yet operational, estimates have been made based on reasonable assumptions for Sequencer counts, Full-node counts, Prover counts, device classes and power draw, hosting mix, computational load, and number of Ethereum L1 transactions assignable to the Aztec Network or to the AZTEC token, as such information does not yet exist. The sustainability indicators set out in S.8 are provided based on these estimates. In order to derive these estimates, we conducted additional research on comparable L2s, used third-party datasets/providers, and applied conservative, reasonable assumptions where direct measurements are unavailable. Energy accounting follows ESRS E1-5 (AR32–AR38), applied coherently with ESMA's MiCA RTS sustainability indicators. We include external datasets and provider names/links below. We do not include specific method for missing/un(der)reported metrics or offsetting methodology. No

		offsets are applied to the indicators. **Ethereum Layer 1 energy use allocation** We allocate a share of Ethereum's energy to AZTEC using CCRI's hybrid method applied to the token on L1. *Included transaction types* ● Sequencers staking/unstaking ● Sequencers claiming rewards ● Token holders participating in governance ● Execution of slashing votes against Sequencers ● Owner-to-owner transfers Rollup block posts and proof verifications are excluded from the token's L1 transaction share by design of the method. It is important to note that owner-to-owner transfers are dependent on an Aztec Network governance process enabling transferability of the AZTEC token. *Assumptions* ● 6.2943 Wh/tx on Ethereum L1 (CCRI measurement reported by the EU Blockchain Observatory). ● Sequencers staking/unstaking (12,000 txs per year, equivalent to 2 staking and 2 unstaking events per Sequencer per year); ● Sequencers claiming rewards (~739,125 txs per year, equivalent to 1 transaction per Sequencer in a committee per 32 block epoch); ● Token holders participating in governance (~19,680 txs per year) ● Execution of slashing votes against Sequencers (~7,699 tx per year, one transaction every 4 epochs); ● Owner-to-owner transfers (assuming 182,500 transfers, 500 transfers a day on average over a year assumed); We round the sum of all of the above transaction counts (961,004) to 1,000,000 transactions during the period covered by this disclosure. *Subtotal* 6,294.3 kWh per year **Aztec Network node energy use allocation** *Assumptions* ● 3,000 Sequencers run on ~1,000 physical machines (≈3 Sequencers per host) ● 5 active Provers ● 50 active Full-nodes ● Sequencers and Full-nodes are ~39% residential, ~61% data-centre/hosted (aligned to the current Ethereum validator landscape)

		● No user transactions on the Aztec Network during the measurement period ● Target specifications used for device classes (to anchor representative power): ○ Sequencer host: 8-core CPU, 16 GB RAM ○ Prover host: 32-core CPU, 128 GB RAM *Assigning representative device power* Values below bracket public measurements for devices that match the stated target specifications. The same figures are applied to Sequencer and Full-Node hosts, and weighted by the hosting mix. ● Residential host (8-core/16 GB class): 18 W low activity; 55 W burst ● Data-centre host (rack-mount server class): 40 W low activity; 85 W burst. ● Prover (32-core/128 GB class): 45 W low activity; 285 W burst. These levels conservatively reflect modern mini-PC/SFF devices and compact 1U servers at the stated target specifications. *Estimating activity levels across node types* <u>Sequencers</u> Every block on the Aztec Network (during Ignition), 24 Sequencers are called upon to form a committee. This committee will be solely responsible for producing blocks on the Aztec Network for 1024 seconds. With 3,000 sequencer instances and three instances per host, the chance a given host is selected in a block is roughly 2.38%. Allowing for brief pre-/post-committee overhead (networking, state updates, time spent syncing to latest state) roughly doubles the active window, yielding ~4.5% of wall-clock time in "burst" and ~95.5% of wall-clock time at low activity per host. <u>Full-nodes</u> Full-nodes may enter burst activity while syncing the Aztec Network's latest state, or when responding to API calls for data, but these burst windows are expected to be very short. Full-nodes are assumed to remain at low activity 100% of the time as a result. <u>Provers</u> During Ignition, the Aztec Network is not processing any user transactions. Provers are still computing the cryptographic proofs required by the Aztec Network to attest to the validity of included blocks, but without user transactions these proofs can be computed more quickly. We assume that Provers operate at burst activity levels during roughly 20% of wall-clock time. *Computation method* For each device class we: 1. compute average power per machine; 2. multiply by the number of machines;

		3. multiply by 8,760 h to annualise. Sequencers/Full-nodes average power per host = residential share × [low activity power × (1 – burst rate) + burst rate × (burst power)] + hosted share × [low activity power × (1 – burst rate) + burst rate × (burst power)] where residential share = 39%, hosted share = 61%, burst rate = 4.5% for Sequencers, 0% for Full-nodes. Provers average power per host = low activity power × (1 – burst rate) + full-compute power × burst rate burst rate = 20% (low-utilisation baseline consistent with no user transactions on L2). **Results** • Sequencers (1,000 machines) → average ≈ 33.36 W per host → ~292,233.6 kWh per year. • Full Nodes (50 machines) → average ≈ 31.47 W per host → ~13,783.86 kWh per year. • Provers (5 machines) → average ≈ 93 W per host → ~4,073.4 kWh per year. *Subtotal* ~310,090.86 kWh per year. ***Total*** 310,090.86 kWh + 6,294.3 kWh = **316,385.16 kWh per year** **Sources** https://carbon-ratings.com/dl/whitepaper-mica-methods-2024 https://solanabeach.io/validators https://blockchain-observatory.ec.europa.eu/document/download/3f78c885-d14e-47cb-b183-f22ef529a258_en?filename=EUBOF3.0_Ethereum_Merge_Trend_Report_final.pdf&prefLang=sl https://docs.api.carbon-ratings.com/v2/#/mica https://carbon-ratings.com/accounting-framework-2022 https://www.ethernodes.org/network-types?synced=1

		https://monitoreth.io/nodes https://www.servethehome.com/hpe-proliant-dl20-gen10-review-compact-and-nimble-server/5/ https://www.servethehome.com/dell-emc-poweredge-r240-review-1u-entry-server/4/ https://www.servethehome.com/beelink-ser6-pro-7735hs-edition-review-amd-ryzen-intel-arc-usb4-egpu/4/ https://www.servethehome.com/beelink-gtr6-review-an-improved-amd-ryzen-mini-pc/3/ https://www.servethehome.com/simplynuc-onyx-v9-review-an-intel-core-i9-13900h-nuc/4/ https://www.anandtech.com/Show/Index/15571?all=False&cPage=6&page=9&slug=intel-nuc10i7fnh-frost-canyon-review&sort=0 https://www.phoronix.com/review/amd-epyc-4005-server/11