EMBARGO UNTIL 12 NOON GREENWICH MEAN TIME FRIDAY 31 JANUARY 2020

London, U.K. – January 31, 2020: Today, Aztec announces the launch of its privacy network on Ethereum mainnet, following two major audits and the conclusion of the largest MPC ceremony in history.

Today, Aztec allows users to create, send, swap and pay income on confidential assets on Ethereum mainnet, allowing the private tokenisation of digital assets on the public blockchain. The protocol allows developers to easily achieve 'data privacy' – hiding the amount of each transaction, whilst allowing Ethereum to fully ratify the transaction logic. Aztec uses zero knowledge proving systems to achieve this.

As well as deploying the ACE (Aztec Cryptography Engine) to mainnet, the company has also released its Privacy SDK to make it easy for developers to integrate confidential transactions into their dapps, and to abstract away the complications of zkNote management from the user.

Aztec is also making a limited number of API keys available for free private mainnet transactions for 12 months, and is now welcoming applications from Ethereum-based software companies.

In December 2019 Aztec completed the largest MPC ("Multi-Party Computation") in history by number of participants. From over 600 applicants, a public list was deterministically generated, and 202 participants from 105 cities across 41 countries took part in this global computation. This has provided the network with important security guarantees. Over 170 of these participants successfully completed their part of the computation.

On 1st January 2020, Aztec appointed new Chief Scientist Ariel Gabizon (formerly Zcash and Protocol Labs). Gabizon is a renowned cryptographer and engineer, perhaps best-known for discovering a critical vulnerability in Zcash two years ago. In Summer 2019, Ariel collaborated with Aztec CTO Zachary Williamson to create PLONK, the superfast Universal ZK-SNARK. This mathematical technique will be key to both privacy and scaling in 2020, and Aztec will be integrating PLONK into its Cryptography Engine this year.

The company's 2020 roadmap includes the integration of anonymity (also known as 'user privacy') into its technology, as well as increasing transaction speed by an order of magnitude using cutting-edge mathematical techniques.

In preparation for launch, Aztec's smart contracts have undergone a highly rigorous sequence of audits, including a first audit by ConsenSys Diligence and a final audit by Trail of Bits, the documentation for which is available for inspection on the company's GitHub account.

Aztec CEO Tom Walton-Pocock said: "We're very excited to be deploying our Web3.0 privacy layer to Ethereum today. As public blockchain networks start to percolate into our everyday lives, privacy providers such as Aztec will enable the general public to transact safely on these networks, without broadcasting sensitive information about their financial activities to the whole world."

The company's CTO Zachary Williamson added, "Giving people the tools to perform confidential transactions on open Web3.0 networks is just the first milestone in our longer-term strategy. Our protocol provides 'data privacy', which encrypts values being transferred. Our next release will add 'user privacy', where identities are obscured. Our final-form protocol will include 'code privacy', where transaction logic is also encrypted. In this triptych of privacy, users will be protected from exploitation of their sensitive transaction data."

Other Resources
AZTEC Completes the Largest MPC Ceremony in History
The Hunting of the SNARK: A Brief History in 3 Parts
PLONK Benchmarks