Generating a proof for non-membership is a well-known scaling problem in zk-private projects.

How is Aztec going to solve this issue? Suppose 1B transactions, or more. Which party would generate a proof? Is it a user, like in Tornado? How much data would a user need to download?