Authors: Jakob Hackel @ BlockScience, Cooper Kunz @ Aztec Labs

Context

Aztec's community originally articulated a number of designs for decentralized proving protocols during anRFP facilitated during October 2023. These designs articulated a landscape that resulted in a variety of mechanisms, i.e. auctions, proof races, or cooperative solutions aiming to achieve traditional byzantine fault tolerance.

Examples: 1, 2, 3, 4, 5.

The current designs enable the currently randomly elected sequencer to outsource or subcontract their proof generation to any zero knowledge proving marketplace that supports the Aztec network.

Here we aim to articulate a new idea: zero-knowledge proving marketplaces may be able to offer an improved user (requester) experience, and an improved quality of service (QoS), by allowing the requester of a zero-knowledge proof to specify which mechanism best fits their specific needs. Alternatively, it may provide a nice user experience that abstracts away the mechanism and provides an explicit decision based off of a set of expressed preferences. Notably, this idea is not specific to or designed for Aztec, but informed by the many conversations we've had over the past few months with proving marketplaces.

Our thinking

Since the QoS desired from each zero knowledge proof requester is likely different from that of any other requester (with different preferences on semi-fungible attributes, such as timeliness, costs, guarantees, predictability, etc), any decentralized prover marketplace has two choices:

1. Choose one mechanism by which Provers coordinate, and hope that it roughly fits enough requesters requirements, or
2. Choose several mechanisms and find an allocation to requesters, that better maps to their requirements (lower loss of quality of service).

If several mechanisms are chosen, there exist again two choices:

1. Let requesters directly interface with any particular mechanism (as per their own understanding of the mechanism), or
2. Provide some UX abstraction mechanism that facilitates this choice (such as letting requesters specify QoS metrics / KPIs that are important, non-negotiable, etc) which are then matched with a particular mechanism for their requests.

These can then be enhanced/tuned over time: If a particular auction mechanism is first identified as best match, but a requester over time finds that particular QoS metrics are not resulting as needed, one can either move to a different mechanism, or tune that particular instance of the mechanism.

For example, Aztec could then have their own interface, which is tuned over time via QoS evaluation, and even though the mechanism was originally "general purpose", several instances of it later exist for different requesters with different parametrization within the same marketplace.

To the individual Provers for a given marketplace, a similar interface should exist. They should specify what they can commit to, with certain properties matchable to demand QoS. This should in theory allow anyone to connect, without caring who is on the other side, not breaking demand or supply constraints, but delivering more targetted (aka less lossy) QoS.

Any centralized marketplace will logically do such a routing internally anyways - a requester that interfaces with them will likely over time specify more and more QoS metrics they have, allowing the centralized marketplace to provide better service over time by adapating the internal routing/coordination.

We think that decentralized marketplaces may want to do something similar, even though it is more complex compared to a centralized marketplace. Forcing any one particular mechanism for coordination on all requesters will likely mean that some are happier than others, with the sad requesters moving somewhere else entirely - as any tuning of the one canonical mechanism might make life more happy for one requester, while at the same time another gets more sad.

While a future landscape of proving marketplaces might consist of different entities, each specializing in one mechanism for prover coordination, this could run into risks of fragmenting the market rather than making it more competitive - as each chosen mechanism fits well for one type of requesters, and less so for others, requesters might face a situation where most proofs are resulting from the one well fitting marketplace, increasing friction and switching costs especially when things go wrong. Instead, a healthy and competitive market could instead optimize quality of service for requesters and provers through a market of mechanisms, lowering costs while ensuring requesters specific needs are met better and better over time.