Summary

This proposal lays the foundation for upgrades by social consensus, while preserving the ability to quickly resolve issues while the network is still in development. In this proposal, infrastructure providers determine whether an upgrade goes into effect after receiving feedback from the community. By default, there is a 1000 block timelock to allow users to withdraw funds.

Importantly, this proposal applies training wheels in the form of a security council. This security council provides checks and balances in order to protect the long term health of the network. The security council is made up of eight technical experts who are elected by the community. The security council has the ability to veto upgrades and approve timelock overrides for urgent situations.

Once the network is stable and mature, upgrades will be determined by social consensus amongst the network participants (similar to Ethereum, where individual client teams work together to determine what improvements to prioritize based on the EIP process). The security council's role will be reduced and eventually eliminated.

Outside of the scope of this proposal is the mandate of the community beyond its role in upgrades. For example, the community may be able to vote on network mechanics such as the economics or funding public goods via grants. These are areas that are still under consideration and will not be addressed in this proposal.

Comparison

This proposal takes inspiration from The Empire Stakes Back in that it heavily relies on coordination and social consensus among those running the network.

Like Beskar Council, it introduces training wheels via a Security Council - though it differs in that it introduces token governance to vote in a Security Council, rather than relying on genesis stakers. It also extends the powers of the Security Council to be able to veto upgrades or approve overrides of the default timelock. However, it does not go as far as to allow the Security Council to act unilaterally - consensus from the infrastructure providers is required.

This proposal doesn't go into as much technical detail as The Republic, particularly around portal contract governance. At the moment, it's assumed that all portal contracts follow canonical governance.

Standard upgrade process

Aztec is being developed in the open with significant input from its community, which has submitted proposals on the network's sequencer selection and upgrade processes. This will continue when the network launches, so any network changes or upgrades take into account the interests of users, developers, and other ecosystem partners - following the process below for standard upgrades.

Potential upgrades are discussed publicly by users, developers, and infrastructure providers on Aztec's Discourse. Once there has been sufficient discussion (at least 1 week) and community feedback has been addressed, the proposed upgrade is distributed on Github for infrastructure providers to review. The upgrade will indicate the block height (activation block) when the contract registry will be updated.

To support the upgrade, infrastructure providers will download the updated software. To oppose the upgrade, infrastructure providers will continue running the same software they are already running. If infrastructure providers representing at least ⅔ of the stakeweight are running the updated software by the activation block and there is no veto from the security council, then the upgrade is confirmed.

By default, the activation block will be at least 1000 blocks after the first infrastructure provider is running this upgraded software (timelock). Users who disagree with the upgrade may withdraw funds before it goes into effect. The timelock also provides time for the security council to review and determine whether a malicious upgrade has been accepted by the infrastructure providers, and veto the upgrade.

Once the contract registry is updated, the incentive contract (as defined in The Empire Stakes Back) and protocol governed portals will be automatically updated. Users will not have to migrate funds.

Overriding the timelock for immediate upgrades

In extreme situations, like a critical bug in the system, there may be a need for an immediate update (overriding the timelock). In order to override the timelock, infrastructure providers can vote for an immediate upgrade. Once infrastructure providers representing at least 80% of the stakeweight have voted in favor of an immediate upgrade and the security council has approved the upgrade, then the upgrade will go into effect immediately and the contract registry will be updated. The

As part of the network launch, the foundation will establish a bug bounty to protect against catastrophic exploits. The bounty will define a responsible disclosure path to escalate potential issues via closed channels. If it is necessary to pause the network, the network will halt when infrastructure providers with 80% of the stakeweight vote in favor of halting the network over 1000 blocks. It will resume once ⅔ of the stakeweight votes is running the upgraded software and votes to resume the network.

Training wheels via security council

In the short term, it's necessary to establish a security council that is responsible for overseeing upgrades to ensure they are in line with the long-term direction and health of the protocol. The security council's mandate is to veto malicious upgrades and approve an override of the timelock for urgent upgrades via a multisig. The security council must provide a report explaining the rationale for their decisions within 48 hours.

The security council will consist of eight technical experts, at least two of which will come from Aztec Labs, who have the domain knowledge to review upgrades. Token holders will elect security council members every 6 months. A security council member can be removed with a 6 of 8 vote by the security council. Token holders also have the ability to remove security council members via governance vote with participation of at least 20% of all votable tokens, and at least 75% vote in favor of removal.

The security council will be phased out three years after the network's launch. Via token governance, the community can vote to extend the term for 6 months at a time if necessary. Once the security council is phased out, infrastructure providers will have sole discretion over upgrades.

Benefits

- Mostly relies on social consensus amongst infrastructure providers but introduces a security council with limited power as a counterbalance if the infrastructure providers aren't acting in the best interest of the network
- Introduces a mechanism to act quickly in the event of an urgent upgrade, or pause the network if necessary - but does not allow either the infrastructure providers or security council the ability to act unilaterally

Risks

- Security council doesn't get phased out because the community continues to extend its term
- Proposes security council is elected via token governance, which has notoriously low participation