CONCEPT PROPOSAL, FOR DISCUSSION PURPOSES ONLY - DOES NOT CONTAIN ALL TECHNICAL DETAILS

- Summary
- Description
- This is a high-level (non-technical) concept proposal only. It proposes a discussion around a potential modification

of the Empire Stakes Back proposal and proposes a “training wheels” (pause-only) multi-sig add-on for the first 12 months (the “Security Council

” or the “Beskar Council

”) layered on top of the existing governance structure as set out in theEmpire Strikes Back proposal whereby stakers participate and decide on Aztec governance (the “Stakers

”).

- If the Security Council pauses the network as a result of discovering a critical bug/vulnerabilty, this would enable the Stakers to upgrade the network to resolve the vulnerability, without any delay limitations although with a higher 75% activation threshold during pause period to activate the new rollup (cf. 51% in Empire Stakes Back - the 51% would still be retained for normal processes before / after new rollup activation), while retaining full control over the existence of the Security Council (Stakers can remove Security Council at any time). See below for more details.

- This is a high-level (non-technical) concept proposal only. It proposes a discussion around a potential modification

of the Empire Stakes Back proposal and proposes a “training wheels” (pause-only) multi-sig add-on for the first 12 months (the “Security Council

” or the “Beskar Council

”) layered on top of the existing governance structure as set out in theEmpire Strikes Back proposal whereby stakers participate and decide on Aztec governance (the “Stakers

”).

- If the Security Council pauses the network as a result of discovering a critical bug/vulnerabilty, this would enable the Stakers to upgrade the network to resolve the vulnerability, without any delay limitations although with a higher 75% activation threshold during pause period to activate the new rollup (cf. 51% in Empire Stakes Back - the 51% would still be retained for normal processes before / after new rollup activation), while retaining full control over the existence of the Security Council (Stakers can remove Security Council at any time). See below for more details.

- Rationale
- As a privacy-focused protocol at the cutting edge of innovation there is an argument that Aztec should have an interim “training wheels” mechanism in place to be able to mitigate risk in case of unforeseen engineering / cryptographic bugs, quicker than the Staker governance system allows.
- Given multi-sigs are a particular vector of attack (even more so as they relates to a privacy protocol), to limit this risk, this proposal recognises that a limited function (pause only) emergency multi-sig is considered as it may assist in resolving emergency situations as the network crystalizes and becomes battle tested, while limiting overall censorship risk to the network.
- The final and perhaps most important reason

behind this concept proposal is to highlight that any implementation of a multi-sig that contains any upgrade capability, creates a high risk for a judicial order (whether for political purposes or not) to impact the individuals who “control” the network, which may lead to a complete failure / censorship of the network. Upgrade multi-sigs may be fine for protocols which allow for scalability (such as Arbitrum or Optimism), but not for privacy protocols.

[

910×396 246 KB

](https://europe1.discourse-cdn.com/business20/uploads/aztec/original/1X/9c66d55444b5b3cc2cc1718bdfacb5dbd04551a4.png)

- As a privacy-focused protocol at the cutting edge of innovation there is an argument that Aztec should have an interim “training wheels” mechanism in place to be able to mitigate risk in case of unforeseen engineering / cryptographic bugs, quicker than the Staker governance system allows.
- Given multi-sigs are a particular vector of attack (even more so as they relates to a privacy protocol), to limit this risk,

this proposal recognises that a limited function (pause only) emergency multi-sig is considered as it may assist in resolving emergency situations as the network crystalizes and becomes battle tested, while limiting overall censorship risk to the network.

- The final and perhaps most important reason

behind this concept proposal is to highlight that any implementation of a multi-sig that contains any upgrade capability, creates a high risk for a judicial order (whether for political purposes or not) to impact the individuals who "control" the network, which may lead to a complete failure / censorship of the network. Upgrade multi-sigs may be fine for protocols which allow for scalability (such as Arbitrum or Optimism), but not for privacy protocols.

[

910×396 246 KB

](https://europe1.discourse-cdn.com/business20/uploads/aztec/original/1X/9c66d55444b5b3cc2cc1718bdfacb5dbd04551a4.png)

- Description

- This is a high-level (non-technical) concept proposal only. It proposes a discussion around a potential modification

of the Empire Stakes Back proposal and proposes a "training wheels" (pause-only) multi-sig add-on for the first 12 months (the "Security Council

" or the "Beskar Council

") layered on top of the existing governance structure as set out in theEmpire Strikes Back proposal whereby stakers participate and decide on Aztec governance (the "Stakers

").

- If the Security Council pauses the network as a result of discovering a critical bug/vulnerabilty, this would enable the Stakers to upgrade the network to resolve the vulnerability, without any delay limitations although with a higher 75% activation threshold during pause period to activate the new rollup (cf. 51% in Empire Stakes Back - the 51% would still be retained for normal processes before / after new rollup activation), while retaining full control over the existence of the Security Council (Stakers can remove Security Council at any time). See below for more details.

- This is a high-level (non-technical) concept proposal only. It proposes a discussion around a potential modification

of the Empire Stakes Back proposal and proposes a "training wheels" (pause-only) multi-sig add-on for the first 12 months (the "Security Council

" or the "Beskar Council

") layered on top of the existing governance structure as set out in theEmpire Strikes Back proposal whereby stakers participate and decide on Aztec governance (the "Stakers

").

- If the Security Council pauses the network as a result of discovering a critical bug/vulnerabilty, this would enable the Stakers to upgrade the network to resolve the vulnerability, without any delay limitations although with a higher 75% activation threshold during pause period to activate the new rollup (cf. 51% in Empire Stakes Back - the 51% would still be retained for normal processes before / after new rollup activation), while retaining full control over the existence of the Security Council (Stakers can remove Security Council at any time). See below for more details.

- Rationale

- As a privacy-focused protocol at the cutting edge of innovation there is an argument that Aztec should have an interim "training wheels" mechanism in place to be able to mitigate risk in case of unforeseen engineering / cryptographic bugs, quicker than the Staker governance system allows.

- Given multi-sigs are a particular vector of attack (even more so as they relates to a privacy protocol), to limit this risk, this proposal recognises that a limited function (pause only) emergency multi-sig is considered as it may assist in resolving emergency situations as the network crystalizes and becomes battle tested, while limiting overall censorship risk to the network.

- The final and perhaps most important reason

behind this concept proposal is to highlight that any implementation of a multi-sig that contains any upgrade capability, creates a high risk for a judicial order (whether for political purposes or not) to impact the individuals who "control" the network, which may lead to a complete failure / censorship of the network. Upgrade multi-sigs may be fine for protocols

which allow for scalability (such as Arbitrum or Optimism), but not for privacy protocols.

[

910×396 246 KB

](https://europe1.discourse-cdn.com/business20/uploads/aztec/original/1X/9c66d55444b5b3cc2cc1718bdfacb5dbd04551a4.png)

- As a privacy-focused protocol at the cutting edge of innovation there is an argument that Aztec should have an interim “training wheels” mechanism in place to be able to mitigate risk in case of unforeseen engineering / cryptographic bugs, quicker than the Staker governance system allows.
- Given multi-sigs are a particular vector of attack (even more so as they relates to a privacy protocol), to limit this risk, this proposal recognises that a limited function (pause only) emergency multi-sig is considered as it may assist in resolving emergency situations as the network crystalizes and becomes battle tested, while limiting overall censorship risk to the network.
- The final and perhaps most important reason

behind this concept proposal is to highlight that any implementation of a multi-sig that contains any upgrade capability, creates a high risk for a judicial order (whether for political purposes or not) to impact the individuals who “control” the network, which may lead to a complete failure / censorship of the network. Upgrade multi-sigs may be fine for protocols which allow for scalability (such as Arbitrum or Optimism), but not for privacy protocols.

[

910×396 246 KB

](https://europe1.discourse-cdn.com/business20/uploads/aztec/original/1X/9c66d55444b5b3cc2cc1718bdfacb5dbd04551a4.png)

- Comparisons
- This (pause-only) Security Council balances the benefits of having a quick response to prevent/limit vulnerabilities (i.e pause the network, to prevent exploits and loss of funds) while:
- (i) retaining Staker governance to implement protocol upgrades;
- (ii) limiting (but not eliminating) certain legal risk associated with multi-sigs (see below table); and
- (iii) retaining the ability for the Security Council members to reveal their identities (cf Optimism which has an anonymous multi-sig) and provide a certain level of accountability and comfort to users in the initial stages of the network.

- (i) retaining Staker governance to implement protocol upgrades;
- (ii) limiting (but not eliminating) certain legal risk associated with multi-sigs (see below table); and
- (iii) retaining the ability for the Security Council members to reveal their identities (cf Optimism which has an anonymous multi-sig) and provide a certain level of accountability and comfort to users in the initial stages of the network.
- This (pause-only) Security Council balances the benefits of having a quick response to prevent/limit vulnerabilities (i.e pause the network, to prevent exploits and loss of funds) while:
- (i) retaining Staker governance to implement protocol upgrades;
- (ii) limiting (but not eliminating) certain legal risk associated with multi-sigs (see below table); and
- (iii) retaining the ability for the Security Council members to reveal their identities (cf Optimism which has an anonymous multi-sig) and provide a certain level of accountability and comfort to users in the initial stages of the network.
- (i) retaining Staker governance to implement protocol upgrades;
- (ii) limiting (but not eliminating) certain legal risk associated with multi-sigs (see below table); and
- (iii) retaining the ability for the Security Council members to reveal their identities (cf Optimism which has an anonymous multi-sig) and provide a certain level of accountability and comfort to users in the initial stages of the network.

Here is a high level overview of the judicial order risk [^1] associated with certain upgrade mechanism models:

Certain Upgrade Mechanisms

Description

Other Similar Projects

Judicial Order Risk / Consequence

[^2]

Social Consensus

See Non-governance

Bitcoin / Ethereum 1.0

Low

Staker Based Consensus

See Empire Strikes Back

Ethereum 2.0

Low

(assuming Staking is not concentrated among a limited set of easily identifiable Stakers and Staker set continues to grow)

Staker Based Consensus + Pause Only Multi-Sig (Transparent)

See Empire Strikes Back + this concept proposal

N/A [^3]

Low/Medium

- a court order may force members of the Security Council to pause the network. However, the Stakers could remove the Security Council and ensure the network remains functional, live and censorship resistant, making any judicial requirement to pause the network inconsequential. A potentially greater risk here is that members of the Security Council / Foundation could be forced to reveal identities of the genesis Stakers (see below - genesis Stakers would participate in the selection / nomination of the Security Council members), which may lead to court action against the genesis Stakers, although this could be mitigated by ensuring a geographically / jurisdictionally diverse and growing set of Stakers (over and above the genesis Stakers) is joining the network on a permissionless basis.

Multi-Sig (Anonymous)

Upgrades conducted via an anonymous mult-sig

Optimism

Medium / High

- a court order may force the Security Council members to take an action, provided they are identified, impacting the whole network.

Multi-Sig (Transparent)

Emergency upgrades conducted via a transparent multi-sig

Arbitrum

High

- a court may force council members to take all necessary steps to take an action, impacting the whole network.

Senate (Transparent)

See The Republic

N/A but similar to Uniswap

High

- a court order may force Senators to take an action, impacting the whole network. However, a mitigating factor for the users is that the Senate cannot force an upgrade instantly, users can exit the network. Notwithstanding the consequence for the network itself remains high.

- Details

- The upgrade mechanism follows the Empire Stakes Back proposal, which requires Staker consensus, subject to the following modification(s):

- What?

In addition to Staker governance, a temporary Security Council would be responsible for an emergency multi-sig which would only be able to pause the Rollup Contract, in case of any suspected or actual unforeseen vulnerabilities.

- How?

(high-level, would require further technical / analysis to determine feasibility).

- A new voting contract would likely need to be implemented (which would be unpausable) in theEmpire Stakes Back proposal that would designate a Security Council address on L1 capable of disabling the Rollup Contract functionality (ideally just the “real roll-up” and not any previous contracts that used ungoverned portals).

- Used only in the event of an unforeseen vulnerability, the Security Council has one and only one ability: to disable a select set of functions regarding the functionality of the Rollup Contract (scope of pause functionality to be discussed, but assumption is that all functions could be paused other than the function to replace the Security Council / ability for Stakers to upgrade the network). The Security Council would not be able to unpause an action.

- Once a pause occurs as a result of any critical vulnerability:

- the Security Council would notify the community that a critical bug has been identified and emergency action has been taken to pause the Rollup Contract and that it and the Stakers are working on a fix which would be finalised asap, noting a report would be published explaining the reason behind the pause action following implementation.

- the Security Council would work with the Stakers to implement a solution in a timely manner.

- the normal 750/1000 blocks for a new rollup is ignored and anybody can propose a new rollup implementation.

- the Security Council would notify the community that a critical bug has been identified and emergency action has been taken to pause the Rollup Contract and that it and the Stakers are working on a fix which would be finalised asap, noting a report would be published explaining the reason behind the pause action following implementation.

- the Security Council would work with the Stakers to implement a solution in a timely manner.

- the normal 750/1000 blocks for a new rollup is ignored and anybody can propose a new rollup implementation.

- Upon initiation of any pause functionality by the Security Council, the 51% Staker activation threshold would be changed to 75% and at least 75% of the Stakers would be required to activate the new Rollup Contract which fixed vulnerabilities (higher threshold to decrease likelihood of malicious Staker behaviour during this sensitive period). If 75% of the stake has manually moved from implementation A (old Rollup Contract) to B (new Rollup Contract), implementation B will become canonical.

- Upon implementation of the solution by the Stakers:

- the Security Council would prepare a public report, explaining the rationale for triggering a pause and the solution implemented. The transparency of the individuals on the Security Council would incentivise good behaviour.

- The 75% activation threshold would revert to 51%.

- the Security Council would prepare a public report, explaining the rationale for triggering a pause and the solution implemented. The transparency of the individuals on the Security Council would incentivise good behaviour.

- The 75% activation threshold would revert to 51%.

- A new voting contract would likely need to be implemented (which would be unpausable) in theEmpire Stakes Back proposal that would designate a Security Council address on L1 capable of disabling the Rollup Contract functionality (ideally just the “real roll-up” and not any previous contracts that used ungoverned portals).

- Used only in the event of an unforeseen vulnerability, the Security Council has one and only one ability: to disable a select set of functions regarding the functionality of the Rollup Contract (scope of pause functionality to be discussed, but assumption is that all functions could be paused other than the function to replace the Security Council / ability for Stakers to upgrade the network). The Security Council would not be able to unpause an action.

- Once a pause occurs as a result of any critical vulnerability:

- the Security Council would notify the community that a critical bug has been identified and emergency action has been taken to pause the Rollup Contract and that it and the Stakers are working on a fix which would be finalised asap, noting a report would be published explaining the reason behind the pause action following implementation.
- the Security Council would work with the Stakers to implement a solution in a timely manner.
- the normal 750/1000 blocks for a new rollup is ignored and anybody can propose a new rollup implementation.

- the Security Council would notify the community that a critical bug has been identified and emergency action has been taken to pause the Rollup Contract and that it and the Stakers are working on a fix which would be finalised asap, noting a report would be published explaining the reason behind the pause action following implementation.
- the Security Council would work with the Stakers to implement a solution in a timely manner.
- the normal 750/1000 blocks for a new rollup is ignored and anybody can propose a new rollup implementation.

- Upon initiation of any pause functionality by the Security Council, the 51% Staker activation threshold would be changed to 75% and at least 75% of the Stakers would be required to activate the new Rollup Contract which fixed vulnerabilities (higher threshold to decrease likelihood of malicious Staker behaviour during this sensitive period). If 75% of the stake has manually moved from implementation A (old Rollup Contract) to B (new Rollup Contract), implementation B will become canonical.
- Upon implementation of the solution by the Stakers:
- the Security Council would prepare a public report, explaining the rationale for triggering a pause and the solution implemented. The transparency of the individuals on the Security Council would incentivise good behaviour.
- The 75% activation threshold would revert to 51%.

- the Security Council would prepare a public report, explaining the rationale for triggering a pause and the solution implemented. The transparency of the individuals on the Security Council would incentivise good behaviour.
- The 75% activation threshold would revert to 51%.

- When?
- The Security Council would be able to pause the Rollup Contract at any time.
- The Stakers, working with the Security Council, could upgrade to resolve any vulnerabilities immediately, without a 30 day window.

- The Security Council would be able to pause the Rollup Contract at any time.
- The Stakers, working with the Security Council, could upgrade to resolve any vulnerabilities immediately, without a 30 day window.

- For How Long?
- The Security Council multi-sig will automatically fall away after 12 months, unless an AZIP proposal is passed to upgrade the network to extend the period and/or alter the Security Council (for example, change individuals, etc).

- The Security Council multi-sig will automatically fall away after 12 months, unless an AZIP proposal is passed to upgrade the network to extend the period and/or alter the Security Council (for example, change individuals, etc).

- Who?
- The genesis Stakers (i.e. the initial Stakers participating in the Aztec network at mainnet) would designate a Security Council address on L1 and select and approve an independent and transparent council of 8 technical experts, which would operate the address held by the mult-sig.
- 6 out of 8 Security Council members would be required to operate the multi-sig, spread over all time-zones to ensure effective response time. Regular fire drills would be conducted by the community/Foundation to ensure Security Council members are operational and can react quickly.
- Bugs reported through the Foundation bug bounty program (closed channels) would be accessible by the Security Council members who could act on them quickly.
- The Security Council members could be changed (for example because they were not sufficiently reactive to a fire drill), or the Security Council could be removed in its entirety, by AZIP proposals / Stakers at any time.

- The genesis Stakers (i.e. the initial Stakers participating in the Aztec network at mainnet) would designate a Security Council address on L1 and select and approve an independent and transparent council of 8 technical experts, which

would operate the address held by the mult-sig.

- 6 out of 8 Security Council members would be required to operate the multi-sig, spread over all time-zones to ensure effective response time. Regular fire drills would be conducted by the community/Foundation to ensure Security Council members are operational and can react quickly.
- Bugs reported through the Foundation bug bounty program (closed channels) would be accessible by the Security Council members who could act on them quickly.
- The Security Council members could be changed (for example because they were not sufficiently reactive to a fire drill), or the Security Council could be removed in its entirety, by AZIP proposals / Stakers at any time.
- What?

In addition to Staker governance, a temporary Security Council would be responsible for an emergency multi-sig which would only be able to pause the Rollup Contract, in case of any suspected or actual unforeseen vulnerabilities.

- How?

(high-level, would require further technical / analysis to determine feasibility).

- A new voting contract would likely need to be implemented (which would be unpausable) in theEmpire Stakes Back proposal that would designate a Security Council address on L1 capable of disabling the Rollup Contract functionality (ideally just the “real roll-up” and not any previous contracts that used ungoverned portals).
- Used only in the event of an unforeseen vulnerability, the Security Council has one and only one ability: to disable a select set of functions regarding the functionality of the Rollup Contract (scope of pause functionality to be discussed, but assumption is that all functions could be paused other than the function to replace the Security Council / ability for Stakers to upgrade the network). The Security Council would not be able to unpause an action.
- Once a pause occurs as a result of any critical vulnerability:
- the Security Council would notify the community that a critical bug has been identified and emergency action has been taken to pause the Rollup Contract and that it and the Stakers are working on a fix which would be finalised asap, noting a report would be published explaining the reason behind the pause action following implementation.
- the Security Council would work with the Stakers to implement a solution in a timely manner.
- the normal 750/1000 blocks for a new rollup is ignored and anybody can propose a new rollup implementation.

- the Security Council would notify the community that a critical bug has been identified and emergency action has been taken to pause the Rollup Contract and that it and the Stakers are working on a fix which would be finalised asap, noting a report would be published explaining the reason behind the pause action following implementation.
- the Security Council would work with the Stakers to implement a solution in a timely manner.
- the normal 750/1000 blocks for a new rollup is ignored and anybody can propose a new rollup implementation.

- Upon initiation of any pause functionality by the Security Council, the 51% Staker activation threshold would be changed to 75% and at least 75% of the Stakers would be required to activate the new Rollup Contract which fixed vulnerabilities (higher threshold to decrease likelihood of malicious Staker behaviour during this sensitive period). If 75% of the stake has manually moved from implementation A (old Rollup Contract) to B (new Rollup Contract), implementation B will become canonical.
- Upon implementation of the solution by the Stakers:
- the Security Council would prepare a public report, explaining the rationale for triggering a pause and the solution implemented. The transparency of the individuals on the Security Council would incentivise good behaviour.
- The 75% activation threshold would revert to 51%.

- the Security Council would prepare a public report, explaining the rationale for triggering a pause and the solution implemented. The transparency of the individuals on the Security Council would incentivise good behaviour.
- The 75% activation threshold would revert to 51%.
- A new voting contract would likely need to be implemented (which would be unpausable) in theEmpire Stakes Back proposal that would designate a Security Council address on L1 capable of disabling the Rollup Contract functionality (ideally just the “real roll-up” and not any previous contracts that used ungoverned portals).
- Used only in the event of an unforeseen vulnerability, the Security Council has one and only one ability: to disable a select set of functions regarding the functionality of the Rollup Contract (scope of pause functionality to be discussed,

but assumption is that all functions could be paused other than the function to replace the Security Council / ability for Stakers to upgrade the network). The Security Council would not be able to unpause an action.

- Once a pause occurs as a result of any critical vulnerability:
- the Security Council would notify the community that a critical bug has been identified and emergency action has been taken to pause the Rollup Contract and that it and the Stakers are working on a fix which would be finalised asap, noting a report would be published explaining the reason behind the pause action following implementation.
- the Security Council would work with the Stakers to implement a solution in a timely manner.
- the normal 750/1000 blocks for a new rollup is ignored and anybody can propose a new rollup implementation.

- the Security Council would notify the community that a critical bug has been identified and emergency action has been taken to pause the Rollup Contract and that it and the Stakers are working on a fix which would be finalised asap, noting a report would be published explaining the reason behind the pause action following implementation.
- the Security Council would work with the Stakers to implement a solution in a timely manner.
- the normal 750/1000 blocks for a new rollup is ignored and anybody can propose a new rollup implementation.

- Upon initiation of any pause functionality by the Security Council, the 51% Staker activation threshold would be changed to 75% and at least 75% of the Stakers would be required to activate the new Rollup Contract which fixed vulnerabilities (higher threshold to decrease likelihood of malicious Staker behaviour during this sensitive period). If 75% of the stake has manually moved from implementation A (old Rollup Contract) to B (new Rollup Contract), implementation B will become canonical.
- Upon implementation of the solution by the Stakers:
- the Security Council would prepare a public report, explaining the rationale for triggering a pause and the solution implemented. The transparency of the individuals on the Security Council would incentivise good behaviour.
- The 75% activation threshold would revert to 51%.

- the Security Council would prepare a public report, explaining the rationale for triggering a pause and the solution implemented. The transparency of the individuals on the Security Council would incentivise good behaviour.
- The 75% activation threshold would revert to 51%.

- When?
- The Security Council would be able to pause the Rollup Contract at any time.
- The Stakers, working with the Security Council, could upgrade to resolve any vulnerabilities immediately, without a 30 day window.

- The Security Council would be able to pause the Rollup Contract at any time.
- The Stakers, working with the Security Council, could upgrade to resolve any vulnerabilities immediately, without a 30 day window.

- For How Long?
- The Security Council multi-sig will automatically fall away after 12 months, unless an AZIP proposal is passed to upgrade the network to extend the period and/or alter the Security Council (for example, change individuals, etc).

- The Security Council multi-sig will automatically fall away after 12 months, unless an AZIP proposal is passed to upgrade the network to extend the period and/or alter the Security Council (for example, change individuals, etc).

- Who?
- The genesis Stakers (i.e. the initial Stakers participating in the Aztec network at mainnet) would designate a Security Council address on L1 and select and approve an independent and transparent council of 8 technical experts, which would operate the address held by the mult-sig.
- 6 out of 8 Security Council members would be required to operate the multi-sig, spread over all time-zones to ensure effective response time. Regular fire drills would be conducted by the community/Foundation to ensure Security Council members are operational and can react quickly.
- Bugs reported through the Foundation bug bounty program (closed channels) would be accessible by the Security Council members who could act on them quickly.
- The Security Council members could be changed (for example because they were not sufficiently reactive to a fire

drill), or the Security Council could be removed in its entirety, by AZIP proposals / Stakers at any time.

- The genesis Stakers (i.e. the initial Stakers participating in the Aztec network at mainnet) would designate a Security Council address on L1 and select and approve an independent and transparent council of 8 technical experts, which would operate the address held by the mult-sig.
- 6 out of 8 Security Council members would be required to operate the multi-sig, spread over all time-zones to ensure effective response time. Regular fire drills would be conducted by the community/Foundation to ensure Security Council members are operational and can react quickly.
- Bugs reported through the Foundation bug bounty program (closed channels) would be accessible by the Security Council members who could act on them quickly.
- The Security Council members could be changed (for example because they were not sufficiently reactive to a fire drill), or the Security Council could be removed in its entirety, by AZIP proposals / Stakers at any time.
- The upgrade mechanism follows the Empire Stakes Back proposal, which requires Staker consensus, subject to the following modification(s):
- What?

In addition to Staker governance, a temporary Security Council would be responsible for an emergency multi-sig which would only be able to pause the Rollup Contract, in case of any suspected or actual unforeseen vulnerabilities.

- How?

(high-level, would require further technical / analysis to determine feasibility).

- A new voting contract would likely need to be implemented (which would be unpausable) in theEmpire Stakes Back proposal that would designate a Security Council address on L1 capable of disabling the Rollup Contract functionality (ideally just the “real roll-up” and not any previous contracts that used ungoverned portals).
- Used only in the event of an unforeseen vulnerability, the Security Council has one and only one ability: to disable a select set of functions regarding the functionality of the Rollup Contract (scope of pause functionality to be discussed, but assumption is that all functions could be paused other than the function to replace the Security Council / ability for Stakers to upgrade the network). The Security Council would not be able to unpause an action.
- Once a pause occurs as a result of any critical vulnerability:
- the Security Council would notify the community that a critical bug has been identified and emergency action has been taken to pause the Rollup Contract and that it and the Stakers are working on a fix which would be finalised asap, noting a report would be published explaining the reason behind the pause action following implementation.
- the Security Council would work with the Stakers to implement a solution in a timely manner.
- the normal 750/1000 blocks for a new rollup is ignored and anybody can propose a new rollup implementation.

- the Security Council would notify the community that a critical bug has been identified and emergency action has been taken to pause the Rollup Contract and that it and the Stakers are working on a fix which would be finalised asap, noting a report would be published explaining the reason behind the pause action following implementation.
- the Security Council would work with the Stakers to implement a solution in a timely manner.
- the normal 750/1000 blocks for a new rollup is ignored and anybody can propose a new rollup implementation.

- Upon initiation of any pause functionality by the Security Council, the 51% Staker activation threshold would be changed to 75% and at least 75% of the Stakers would be required to activate the new Rollup Contract which fixed vulnerabilities (higher threshold to decrease likelihood of malicious Staker behaviour during this sensitive period). If 75% of the stake has manually moved from implementation A (old Rollup Contract) to B (new Rollup Contract), implementation B will become canonical.
- Upon implementation of the solution by the Stakers:
- the Security Council would prepare a public report, explaining the rationale for triggering a pause and the solution implemented. The transparency of the individuals on the Security Council would incentivise good behaviour.
- The 75% activation threshold would revert to 51%.

- the Security Council would prepare a public report, explaining the rationale for triggering a pause and the solution implemented. The transparency of the individuals on the Security Council would incentivise good behaviour.
- The 75% activation threshold would revert to 51%.

- A new voting contract would likely need to be implemented (which would be unpausable) in theEmpire Stakes Back proposal that would designate a Security Council address on L1 capable of disabling the Rollup Contract functionality (ideally just the “real roll-up” and not any previous contracts that used ungoverned portals).
- Used only in the event of an unforeseen vulnerability, the Security Council has one and only one ability: to disable a select set of functions regarding the functionality of the Rollup Contract (scope of pause functionality to be discussed, but assumption is that all functions could be paused other than the function to replace the Security Council / ability for Stakers to upgrade the network). The Security Council would not be able to unpause an action.
- Once a pause occurs as a result of any critical vulnerability:
- the Security Council would notify the community that a critical bug has been identified and emergency action has been taken to pause the Rollup Contract and that it and the Stakers are working on a fix which would be finalised asap, noting a report would be published explaining the reason behind the pause action following implementation.
- the Security Council would work with the Stakers to implement a solution in a timely manner.
- the normal 750/1000 blocks for a new rollup is ignored and anybody can propose a new rollup implementation.

- the Security Council would notify the community that a critical bug has been identified and emergency action has been taken to pause the Rollup Contract and that it and the Stakers are working on a fix which would be finalised asap, noting a report would be published explaining the reason behind the pause action following implementation.
- the Security Council would work with the Stakers to implement a solution in a timely manner.
- the normal 750/1000 blocks for a new rollup is ignored and anybody can propose a new rollup implementation.

- Upon initiation of any pause functionality by the Security Council, the 51% Staker activation threshold would be changed to 75% and at least 75% of the Stakers would be required to activate the new Rollup Contract which fixed vulnerabilities (higher threshold to decrease likelihood of malicious Staker behaviour during this sensitive period). If 75% of the stake has manually moved from implementation A (old Rollup Contract) to B (new Rollup Contract), implementation B will become canonical.
- Upon implementation of the solution by the Stakers:
- the Security Council would prepare a public report, explaining the rationale for triggering a pause and the solution implemented. The transparency of the individuals on the Security Council would incentivise good behaviour.
- The 75% activation threshold would revert to 51%.

- the Security Council would prepare a public report, explaining the rationale for triggering a pause and the solution implemented. The transparency of the individuals on the Security Council would incentivise good behaviour.
- The 75% activation threshold would revert to 51%.

- When?
- The Security Council would be able to pause the Rollup Contract at any time.
- The Stakers, working with the Security Council, could upgrade to resolve any vulnerabilities immediately, without a 30 day window.

- The Security Council would be able to pause the Rollup Contract at any time.
- The Stakers, working with the Security Council, could upgrade to resolve any vulnerabilities immediately, without a 30 day window.

- For How Long?
- The Security Council multi-sig will automatically fall away after 12 months, unless an AZIP proposal is passed to upgrade the network to extend the period and/or alter the Security Council (for example, change individuals, etc).

- The Security Council multi-sig will automatically fall away after 12 months, unless an AZIP proposal is passed to upgrade the network to extend the period and/or alter the Security Council (for example, change individuals, etc).

- Who?
- The genesis Stakers (i.e. the initial Stakers participating in the Aztec network at mainnet) would designate a Security Council address on L1 and select and approve an independent and transparent council of 8 technical experts, which would operate the address held by the mult-sig.
- 6 out of 8 Security Council members would be required to operate the multi-sig, spread over all time-zones to ensure

effective response time. Regular fire drills would be conducted by the community/Foundation to ensure Security Council members are operational and can react quickly.

- Bugs reported through the Foundation bug bounty program (closed channels) would be accessible by the Security Council members who could act on them quickly.

- The Security Council members could be changed (for example because they were not sufficiently reactive to a fire drill), or the Security Council could be removed in its entirety, by AZIP proposals / Stakers at any time.

- The genesis Stakers (i.e. the initial Stakers participating in the Aztec network at mainnet) would designate a Security Council address on L1 and select and approve an independent and transparent council of 8 technical experts, which would operate the address held by the mult-sig.

- 6 out of 8 Security Council members would be required to operate the multi-sig, spread over all time-zones to ensure effective response time. Regular fire drills would be conducted by the community/Foundation to ensure Security Council members are operational and can react quickly.

- Bugs reported through the Foundation bug bounty program (closed channels) would be accessible by the Security Council members who could act on them quickly.

- The Security Council members could be changed (for example because they were not sufficiently reactive to a fire drill), or the Security Council could be removed in its entirety, by AZIP proposals / Stakers at any time.

- What?

In addition to Staker governance, a temporary Security Council would be responsible for an emergency multi-sig which would only be able to pause the Rollup Contract, in case of any suspected or actual unforeseen vulnerabilities.

- How?

(high-level, would require further technical / analysis to determine feasibility).

- A new voting contract would likely need to be implemented (which would be unpausable) in theEmpire Stakes Back proposal that would designate a Security Council address on L1 capable of disabling the Rollup Contract functionality (ideally just the “real roll-up” and not any previous contracts that used ungoverned portals).

- Used only in the event of an unforeseen vulnerability, the Security Council has one and only one ability: to disable a select set of functions regarding the functionality of the Rollup Contract (scope of pause functionality to be discussed, but assumption is that all functions could be paused other than the function to replace the Security Council / ability for Stakers to upgrade the network). The Security Council would not be able to unpause an action.

- Once a pause occurs as a result of any critical vulnerability:

- the Security Council would notify the community that a critical bug has been identified and emergency action has been taken to pause the Rollup Contract and that it and the Stakers are working on a fix which would be finalised asap, noting a report would be published explaining the reason behind the pause action following implementation.

- the Security Council would work with the Stakers to implement a solution in a timely manner.

- the normal 750/1000 blocks for a new rollup is ignored and anybody can propose a new rollup implementation.

- the Security Council would notify the community that a critical bug has been identified and emergency action has been taken to pause the Rollup Contract and that it and the Stakers are working on a fix which would be finalised asap, noting a report would be published explaining the reason behind the pause action following implementation.

- the Security Council would work with the Stakers to implement a solution in a timely manner.

- the normal 750/1000 blocks for a new rollup is ignored and anybody can propose a new rollup implementation.

- Upon initiation of any pause functionality by the Security Council, the 51% Staker activation threshold would be changed to 75% and at least 75% of the Stakers would be required to activate the new Rollup Contract which fixed vulnerabilities (higher threshold to decrease likelihood of malicious Staker behaviour during this sensitive period). If 75% of the stake has manually moved from implementation A (old Rollup Contract) to B (new Rollup Contract), implementation B will become canonical.

- Upon implementation of the solution by the Stakers:

- the Security Council would prepare a public report, explaining the rationale for triggering a pause and the solution implemented. The transparency of the individuals on the Security Council would incentivise good behaviour.

- The 75% activation threshold would revert to 51%.

- the Security Council would prepare a public report, explaining the rationale for triggering a pause and the solution implemented. The transparency of the individuals on the Security Council would incentivise good behaviour.

- The 75% activation threshold would revert to 51%.

- A new voting contract would likely need to be implemented (which would be unpausable) in theEmpire Stakes Back proposal that would designate a Security Council address on L1 capable of disabling the Rollup Contract functionality (ideally just the “real roll-up” and not any previous contracts that used ungoverned portals).

- Used only in the event of an unforeseen vulnerability, the Security Council has one and only one ability: to disable a select set of functions regarding the functionality of the Rollup Contract (scope of pause functionality to be discussed, but assumption is that all functions could be paused other than the function to replace the Security Council / ability for Stakers to upgrade the network). The Security Council would not be able to unpause an action.

- Once a pause occurs as a result of any critical vulnerability:

- the Security Council would notify the community that a critical bug has been identified and emergency action has been taken to pause the Rollup Contract and that it and the Stakers are working on a fix which would be finalised asap, noting a report would be published explaining the reason behind the pause action following implementation.

- the Security Council would work with the Stakers to implement a solution in a timely manner.

- the normal 750/1000 blocks for a new rollup is ignored and anybody can propose a new rollup implementation.

- the Security Council would notify the community that a critical bug has been identified and emergency action has been taken to pause the Rollup Contract and that it and the Stakers are working on a fix which would be finalised asap, noting a report would be published explaining the reason behind the pause action following implementation.

- the Security Council would work with the Stakers to implement a solution in a timely manner.

- the normal 750/1000 blocks for a new rollup is ignored and anybody can propose a new rollup implementation.

- Upon initiation of any pause functionality by the Security Council, the 51% Staker activation threshold would be changed to 75% and at least 75% of the Stakers would be required to activate the new Rollup Contract which fixed vulnerabilities (higher threshold to decrease likelihood of malicious Staker behaviour during this sensitive period). If 75% of the stake has manually moved from implementation A (old Rollup Contract) to B (new Rollup Contract), implementation B will become canonical.

- Upon implementation of the solution by the Stakers:

- the Security Council would prepare a public report, explaining the rationale for triggering a pause and the solution implemented. The transparency of the individuals on the Security Council would incentivise good behaviour.

- The 75% activation threshold would revert to 51%.

- the Security Council would prepare a public report, explaining the rationale for triggering a pause and the solution implemented. The transparency of the individuals on the Security Council would incentivise good behaviour.

- The 75% activation threshold would revert to 51%.

- When?

- The Security Council would be able to pause the Rollup Contract at any time.

- The Stakers, working with the Security Council, could upgrade to resolve any vulnerabilities immediately, without a 30 day window.

- The Security Council would be able to pause the Rollup Contract at any time.

- The Stakers, working with the Security Council, could upgrade to resolve any vulnerabilities immediately, without a 30 day window.

- For How Long?

- The Security Council multi-sig will automatically fall away after 12 months, unless an AZIP proposal is passed to upgrade the network to extend the period and/or alter the Security Council (for example, change individuals, etc).

- The Security Council multi-sig will automatically fall away after 12 months, unless an AZIP proposal is passed to upgrade the network to extend the period and/or alter the Security Council (for example, change individuals, etc).

- Who?

- The genesis Stakers (i.e. the initial Stakers participating in the Aztec network at mainnet) would designate a Security

Council address on L1 and select and approve an independent and transparent council of 8 technical experts, which would operate the address held by the mult-sig.

- 6 out of 8 Security Council members would be required to operate the multi-sig, spread over all time-zones to ensure effective response time. Regular fire drills would be conducted by the community/Foundation to ensure Security Council members are operational and can react quickly.
- Bugs reported through the Foundation bug bounty program (closed channels) would be accessible by the Security Council members who could act on them quickly.
- The Security Council members could be changed (for example because they were not sufficiently reactive to a fire drill), or the Security Council could be removed in its entirety, by AZIP proposals / Stakers at any time.
- The genesis Stakers (i.e. the initial Stakers participating in the Aztec network at mainnet) would designate a Security Council address on L1 and select and approve an independent and transparent council of 8 technical experts, which would operate the address held by the mult-sig.

- 6 out of 8 Security Council members would be required to operate the multi-sig, spread over all time-zones to ensure effective response time. Regular fire drills would be conducted by the community/Foundation to ensure Security Council members are operational and can react quickly.
- Bugs reported through the Foundation bug bounty program (closed channels) would be accessible by the Security Council members who could act on them quickly.
- The Security Council members could be changed (for example because they were not sufficiently reactive to a fire drill), or the Security Council could be removed in its entirety, by AZIP proposals / Stakers at any time.

- Pros
- The Security Council would be able to quickly respond to network vulnerabilities and pause the Rollup Contract quickly, to mitigate any critical vulnerabilities / risks.
- Limited risk of consequential multi-sig user misuse or censorship / legal risk - Security Council can only pause (and not upgrade the network) - Stakers could upgrade the network (remove the Security Council with an upgrade).
- The names of the 8 members of the Security Council would be transparent (and not anonymous) given pause only functionality, adding trust to the network (as opposed to using an anonymous multi-sig (such as Optimism)).
- Increased 75% (from 51%) Rollup Contract activation threshold during pause period would limit (but not eliminate) risk of malicious behaviour by Stakers.
- The selection of the technical set of Security Council members would be partly done by the genesis Stakers (and it may include a minority set of Aztec Labs technical experts) and the broader community as a whole, not by Aztec Labs, the Foundation or any single entity to ensure the Security Council is characterized as being on the "Decentralized" spectrum of a16z's Decentralization Factors for Tokenized Consensus Protocols (Layer 1s and Layer 2s):

[

1600×456 246 KB

](https://europe1.discourse-cdn.com/business20/uploads/aztec/original/1X/e0bacbd4e1f80b5d745e13bf4c6d13bc373525d6.png)

- The Security Council would be able to quickly respond to network vulnerabilities and pause the Rollup Contract quickly, to mitigate any critical vulnerabilities / risks.
- Limited risk of consequential multi-sig user misuse or censorship / legal risk - Security Council can only pause (and not upgrade the network) - Stakers could upgrade the network (remove the Security Council with an upgrade).
- The names of the 8 members of the Security Council would be transparent (and not anonymous) given pause only functionality, adding trust to the network (as opposed to using an anonymous multi-sig (such as Optimism)).
- Increased 75% (from 51%) Rollup Contract activation threshold during pause period would limit (but not eliminate) risk of malicious behaviour by Stakers.
- The selection of the technical set of Security Council members would be partly done by the genesis Stakers (and it may include a minority set of Aztec Labs technical experts) and the broader community as a whole, not by Aztec Labs, the Foundation or any single entity to ensure the Security Council is characterized as being on the "Decentralized" spectrum of a16z's Decentralization Factors for Tokenized Consensus Protocols (Layer 1s and Layer 2s):

[

1600×456 246 KB

](https://europe1.discourse-cdn.com/business20/uploads/aztec/original/1X/e0bacbd4e1f80b5d745e13bf4c6d13bc373525d6.png)

- Cons
- In a pause situation initiated by the Security Council, given Stakers could upgrade the network without any timelock, a harmful collusion of Stakers (over 75% for activation) could lead to a total loss of funds for users, without the ability to save themselves (which would exist if there was an exit window).
- Social consensus of the non-governance proposal ensures higher levels of censorship resistance (including judicial order resistance).
- Multi-sig could be attacked or the multi-sig holders could coordinate to pausing the network, which would diminish trust in the network and create centralisation optics.
- An attacker could time the date when the multi-sig falls away and act then.

[

920×940 715 KB

](https://europe1.discourse-cdn.com/business20/uploads/aztec/original/1X/e723262f5958df578c552d123d5c7fb1e1021d82.png)

- In a pause situation initiated by the Security Council, given Stakers could upgrade the network without any timelock, a harmful collusion of Stakers (over 75% for activation) could lead to a total loss of funds for users, without the ability to save themselves (which would exist if there was an exit window).
- Social consensus of the non-governance proposal ensures higher levels of censorship resistance (including judicial order resistance).
- Multi-sig could be attacked or the multi-sig holders could coordinate to pausing the network, which would diminish trust in the network and create centralisation optics.
- An attacker could time the date when the multi-sig falls away and act then.

[

920×940 715 KB

](https://europe1.discourse-cdn.com/business20/uploads/aztec/original/1X/e723262f5958df578c552d123d5c7fb1e1021d82.png)

- Questions and Other Concerns
- Who should be a member of the Security Council and how can we ensure a quick reaction to vulnerabilities (covering all time zones), who is trustworthy and who will act in the best interest of the network and not just the Stakers?
- Does a pause-only Security Council provide sufficient comfort to prevent bugs / vulnerabilities from being exploited?
- What exact pause functions should the Security Council have?
- How do we limit the potential for Security Council members to identify Stakers?
- Would anonymising the Security Council (which would further limit judicial order risk) outweigh the benefits of a transparent Security Council (which provides comfort that Security Council members are accountable)?
- Is 12 months a sufficiently long enough time for the Security Council to exist or is it too short? Are there any other ways to look at this?
- Are there any additional (conceptual) modifications that could be made to this proposal which would alleviate the key risk of having Stakers collude in a pause situation which could lead to a total loss of funds for users, without any ability to exit? Do we have to rely on the benevolence of Stakers at this point?
- Is the increase of the activation threshold (once Rollup Contract is paused by the Security Council) from 51% to 75% too high and would cause the Rollup to be stuck in a paused state?
- Are there any technical challenges that would not be capable of being overcome to implement this?

[^1]:

Note this concept proposal and table focuses only on judicial order risk (a particularly pertinent risk given recent developments (see footnote below)) and does not cover other risks, including other legal risks, such as sanctions and securities law risks.

[^2]:

See Oasis Judicial Order and Nomad Bridge Class Action; multi-sigs carry significant “legal” / judicial order risk. For example, Oasis received an order from the High Court of England and Wales to take all necessary steps that would result in the retrieval of certain assets involved with a specific wallet address. The specific legal risk here is the ability of a court to force security council members to take a specific action as directed by the court; halt the network or return certain funds to person X.

[^3]:

However, see Compound Pause Guardian multi-sig.