Ariadne Liveness

This document analyzes expected behaviour of the Ariadne v2 selection algorithm on Cardano mainnet.

Goals

This report serves the following goals:

1. To provide data for Ariadne v2 users to select appropriate values for Ariadne parameters,
2. To understand typical properties of committees selected by Ariadne v2,

in realistic conditions, with main concern being safety and liveness of the GRANDPA finality gadget, which requires at least 67% of voting power to be honest to progress safely.

Methodology

Results presented in this document were produced through a number of simulations using real Cardano mainnet SPO data. Each simulation run an Ariadne selection and computed the following data:

1. Number of distinct members of committee (`distinct_members`)
2. Maximum number of committee seats allocated to a single member (`max_single_member_seats`)
3. Number of top stake members that can go offline before the committee stops finalizing blocks (`safe_offline_members`)
4. Total stake of top members that need to go offline before the committee stops finalizing blocks (`top_safe_offline_stake` and `botom_safe_offline_stake`)

The simulations were parametrized by the following:

- SPO stake data (all mainnet SPOs, or top 500)
- `R` component of the D-Param (30, 300, 3000)
- number of registered SPOs (`registered_candidates`)

and run 1000 times for each combination.

Each simulation did the following steps:

1. Randomly selected `registered_candidates` of SPOs out of all SPO stakes to simulate different populations of registered SPOs
2. Run Ariadne v2 selection against that population
3. Computed metrics for the selected committee

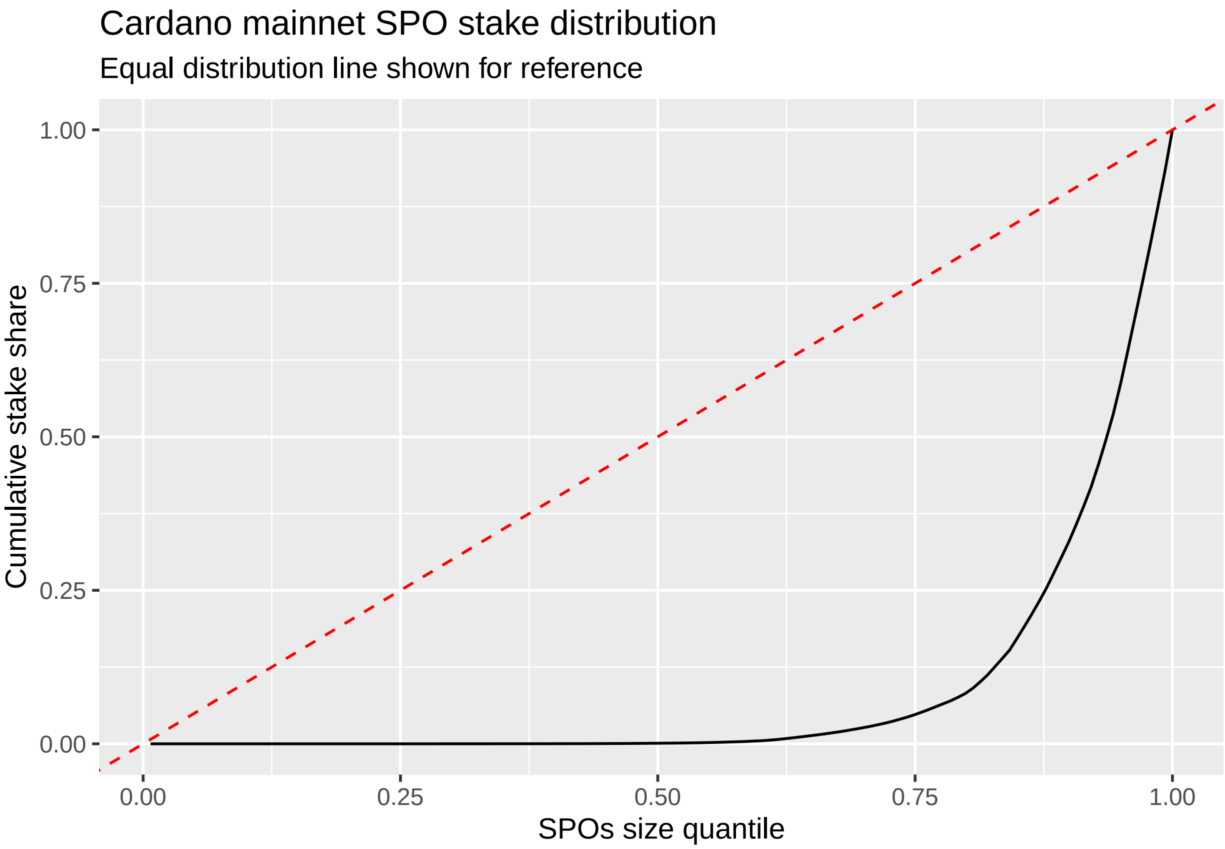
Data The simulations used for this document were run using Cardano SPO stake data obtained on May 22 2025.

Results can be found in the `data/ariadne-simulation-<timestamp>.csv` files.

The summary of the dataset used for this report can be seen below:

```
##  ariadne_version          R                 P           registered_candidates
##  Length:5404        Min.   :  30.0   Min.   : 0.000   Min.   :  20.0
##  Class :character   1st Qu.: 100.0   1st Qu.: 0.000   1st Qu.: 200.0
##  Mode  :character   Median : 500.0   Median :10.000   Median : 500.0
##                     Mean   : 823.7   Mean   : 5.065   Mean   : 795.8
##                     3rd Qu.:1000.0   3rd Qu.:10.000   3rd Qu.:1000.0
##                      Max.   :3000.0   Max.   :10.000   Max.   :2771.0  
##  total_registered_stake registered_file    permissioned_file 
##  Min.   :9.323e+12      Length:5404        Length:5404       
##  1st Qu.:1.462e+15      Class :character   Class :character  
##  Median :7.722e+15      Mode  :character   Mode  :character  
##  Mean   :8.924e+15                                           
##  3rd Qu.:1.624e+16                                           
##  Max.   :2.208e+16                                           
##  total_committee_stake distinct_members max_single_member_seats
##  Min.   :9.276e+12     Min.   :  3.0    Min.   :   1.00        
##  1st Qu.:1.184e+15     1st Qu.: 28.0    1st Qu.:   4.00        
##  Median :3.631e+15     Median : 89.0    Median :   8.00        
##  Mean   :5.709e+15     Mean   :158.9    Mean   :  60.65        
##  3rd Qu.:7.974e+15     3rd Qu.:233.0    3rd Qu.:  28.00        
##  Max.   :2.122e+16     Max.   :761.0    Max.   :2677.00        
##  safe_offline_members top_safe_offline_stake botom_safe_offline_stake
##  Min.   :  0.00       Min.   :0.000e+00      Min.   :7.734e+11       
##  1st Qu.:  6.00       1st Qu.:2.936e+14      1st Qu.:3.718e+14       
##  Median : 16.00       Median :9.028e+14      Median :1.233e+15       
##  Mean   : 26.26       Mean   :1.635e+15      Mean   :2.043e+15       
##  3rd Qu.: 37.00       3rd Qu.:2.428e+15      3rd Qu.:2.797e+15       
##  Max.   :105.00       Max.   :7.297e+15      Max.   :7.885e+15       
##  committee_to_registered_stake
##  Min.   :0.04751              
##  1st Qu.:0.64940              
##  Median :0.95199              
##  Mean   :0.77742              
##  3rd Qu.:0.99488              
##  Max.   :1.00000              
```

Stake distribution There are 2771 Cardano SPO in the data collected. Cardano mainnet stake distribution exhibits very high skew which can be seen by plotting cumulative stake against SPO pool size:



The vast majority of stake is controlled by top 20% with bottom 60% controlling virtually no stake at all, corresponding to a Gini coefficient of 0.8319587. For comparison, Gini coefficient of top:

- 20% is 0.3200561
- 10% is 0.1583383
- 1% is 0.045872

It can be seen that SPOs from the top 20% (= 27.8 SPOs) will control most of block production of any Partner Chain they register for.

To account for that, the Ariadne v2 selection was simulated using two data sets:

- All SPO list
- List of top 500 SPOs

Results

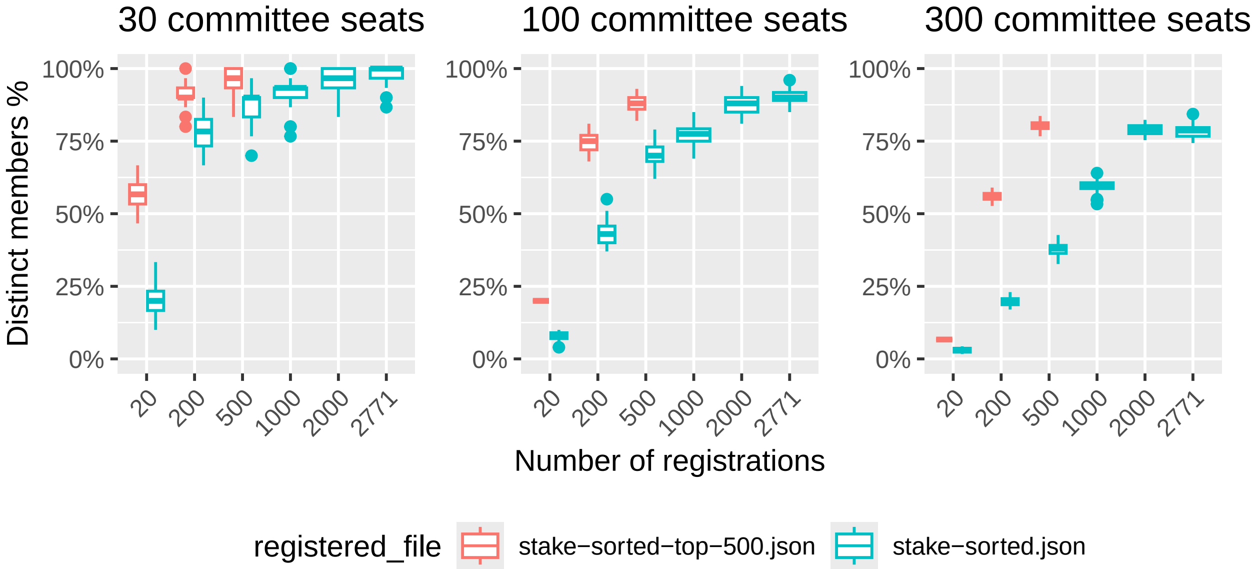
Fully decentralized case

This section talks about committees that are composed only of registered candidates.

Seat assignment

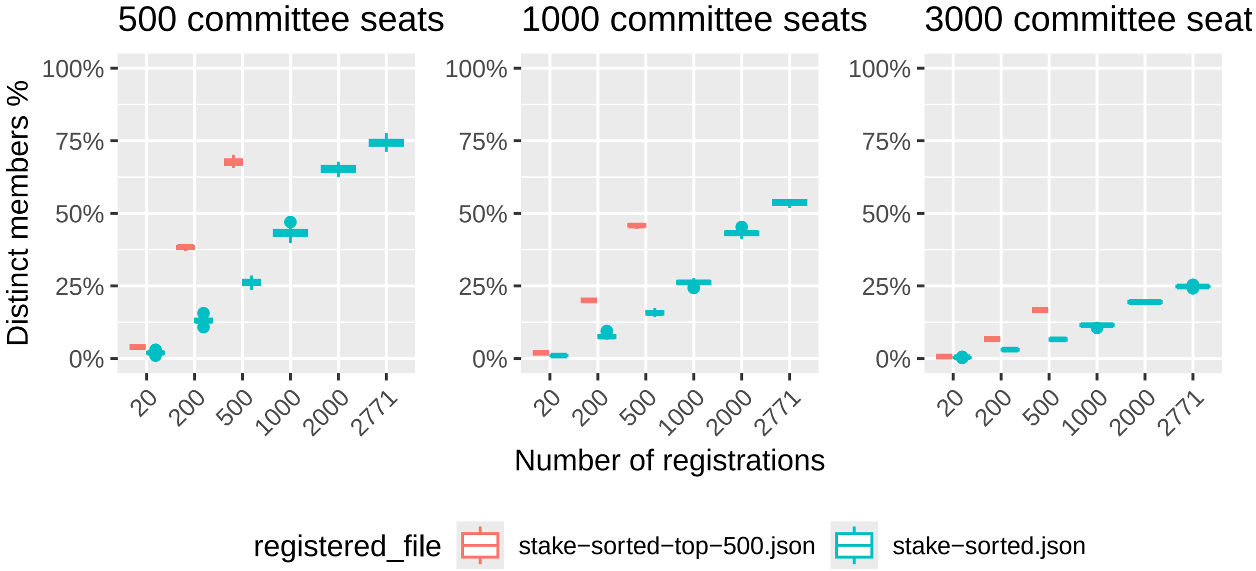
In a one-member-one-seat committee, 33% of members can be dishonest before it can no longer safely finalize blocks any more. However, in Ariadne multiple seats can be assigned to the same member, boosting their voting power. This means the actual number of dishonest members a committee can tolerate is lower than the upper bound of 33%. Therefore, it is beneficial to understand the actual distribution of seats in real committees.

The following charts show the real number of unique committee members as percentage of committee seats number for committee sizes smaller than the SPO population:

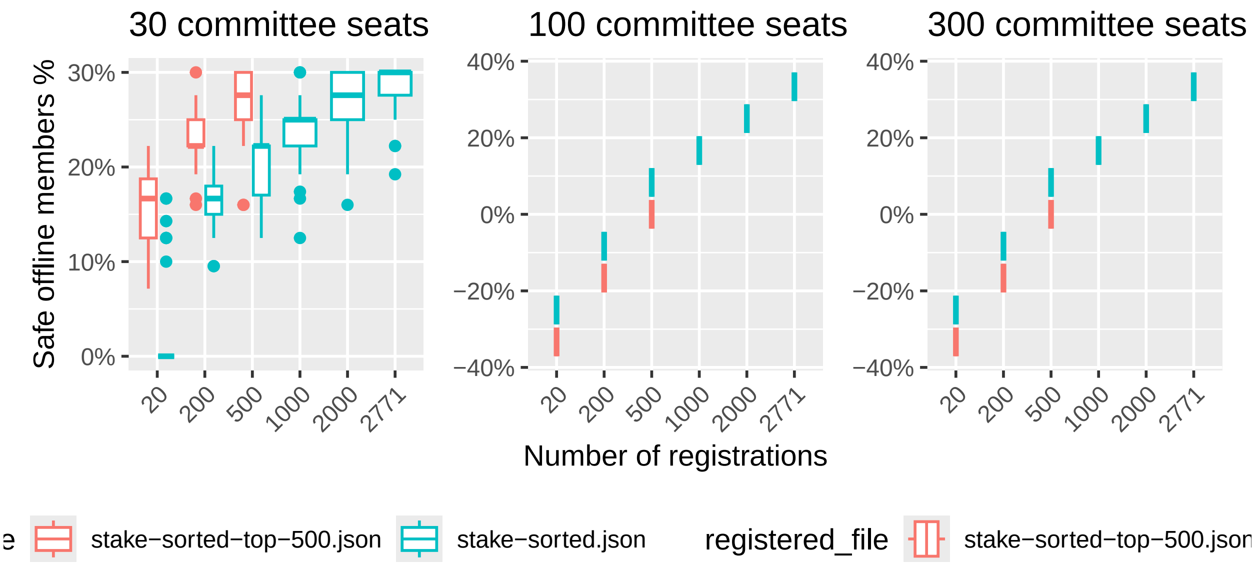


In the charts both full SPO data and top 500 SPO simulations approach a common upper bound on distinct member percentage as the registered candidate pool better reflects the underlying SPO population, which suggests that the resulting committees are dominated by the top 500 SPOs. The upper bound is mostly reached as the registered candidate pool grows to be an order of magnitude bigger than the committee size.

Plotting data for bigger committee sizes shows that they tend to have smaller distinct member percantage, indicating that there is a diminishing return on increasing the committee size, as bigger stake candidates get more chances to be assigned another slot:



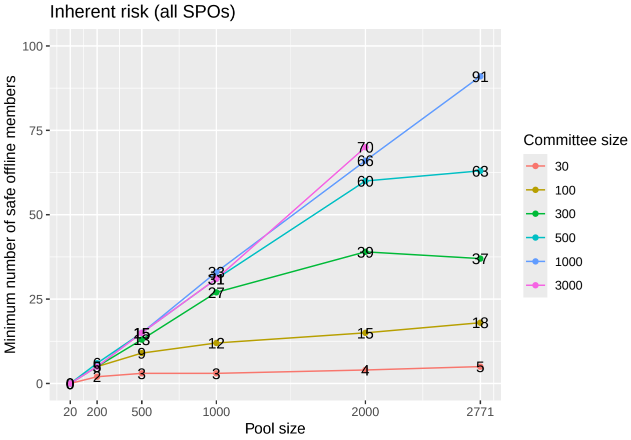
The number of unique committee members affects fault tolerance of the whole committee. If no member is assigned more than one seat, full 33% of malicious members can be tolerated, with this value shrinking as individual members get more seats. This can be observed by plotting the percentage of malicious committee members tolerated against candidate numbers:

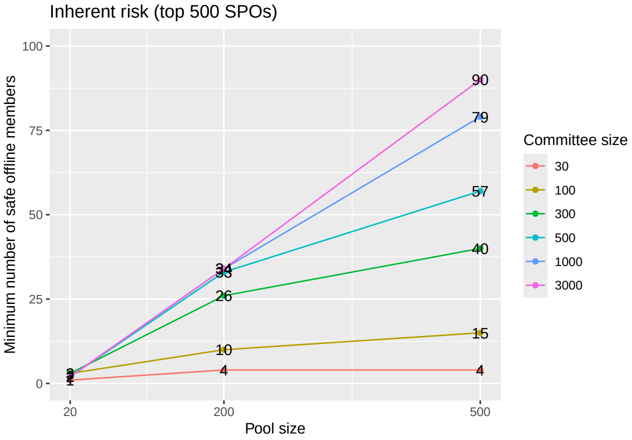


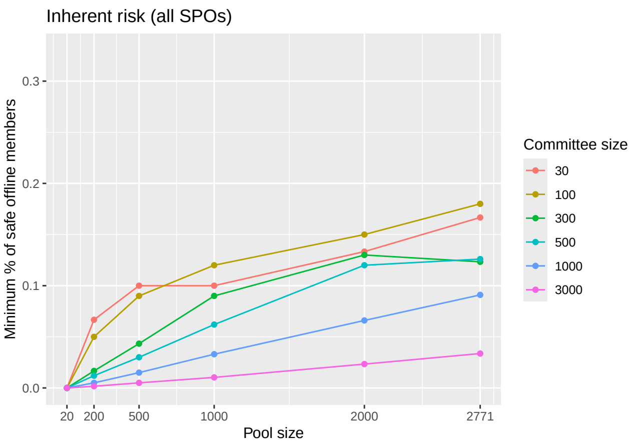
Similarly to the ratio of unique members, this ratio decreases as the committee size increases, even as the absolute underlying value grows, indicating a diminishing return in using bigger committees.

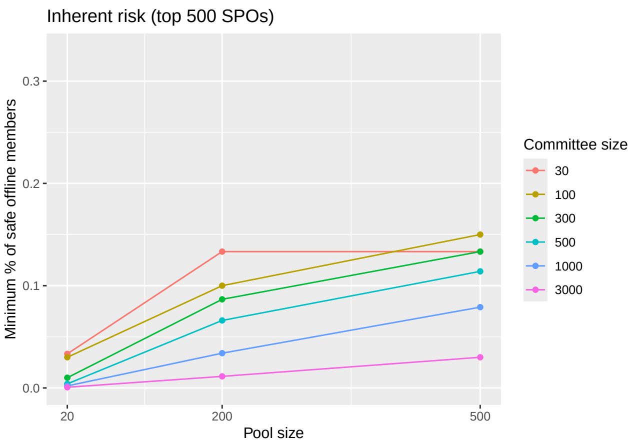
Inherent risk

Midnight finality risk document measures the "inherent risk" by the number of individual committee members (taking into account multiple seat assignments) that can go offline before the committee is no longer able to finalize blocks. The minimum number and percentage of safe offline members for each set of parameters can be visualised as follows:







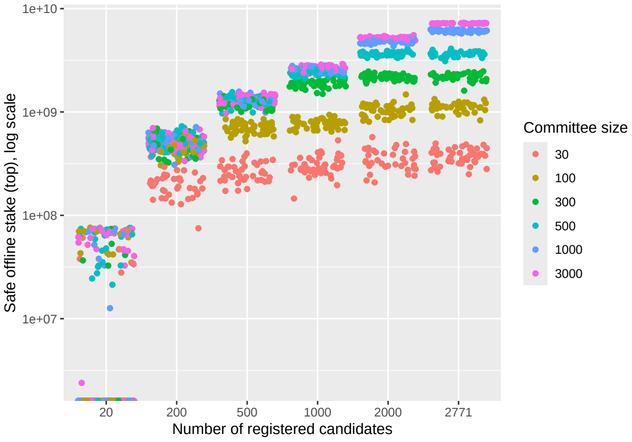


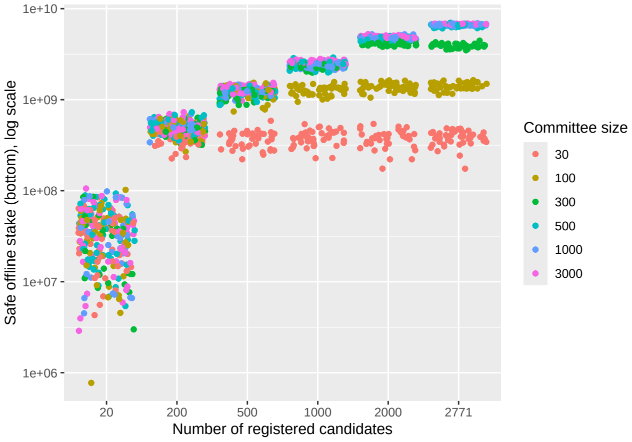
As expected, bigger committees gain more resilience when measured in absolute numbers of safe offline members. However, plotting the same data as percentage again shows that there is a diminishing return in relative terms from increasing committee size.

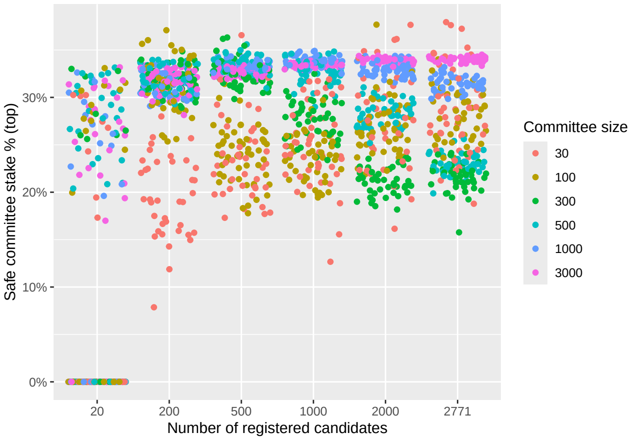
Cost of attack

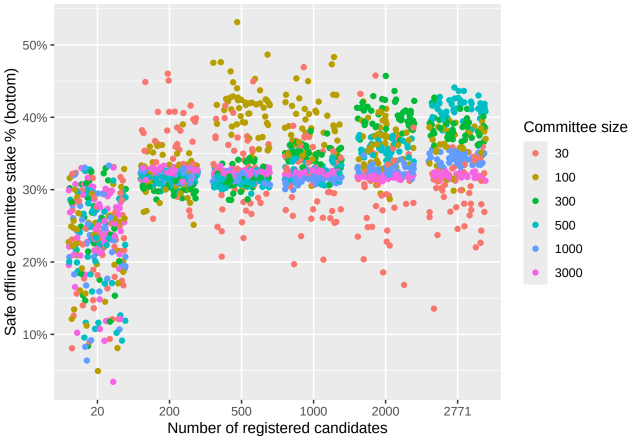
In addition to the minimum number of offline nodes that can be withstood by the committee, it is also important to understand what amount of ADA stake is behind the nodes that would need to go down to affect consensus. For that aim, the data set contains two metrics: - `top_safe_offline_stake`: total stake of top stake committee members that can safely go offline. this metric corresponds to a scenario where the least amount of physical nodes is affected in a successful attack - `bottom_safe_offline_stake`: total stake of lowest stake committee members that can go offlilne. this metric corresponds to a scenario where smallest players are affected, with the assumption, that lower stake means lower security or reliability.

Absolute and relative values of this stake are visualised below:



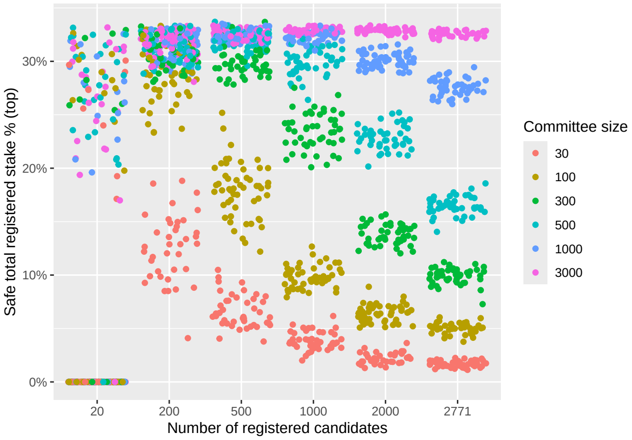


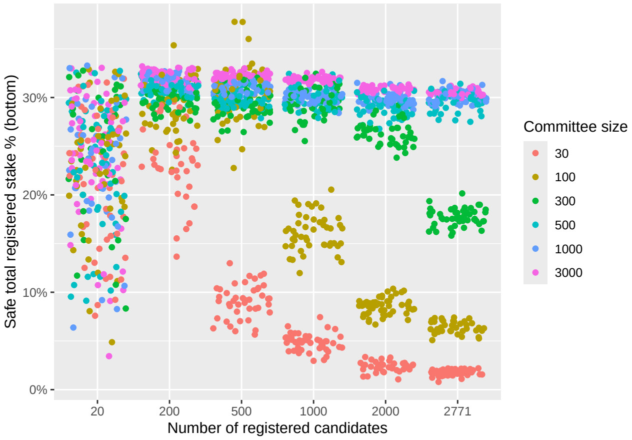




The plots show that the "safe stake" tends to converge on 33% when the committee is close to or higher than the number of candidates, which is expected as the committee closer approximates the candidate stake distribution.

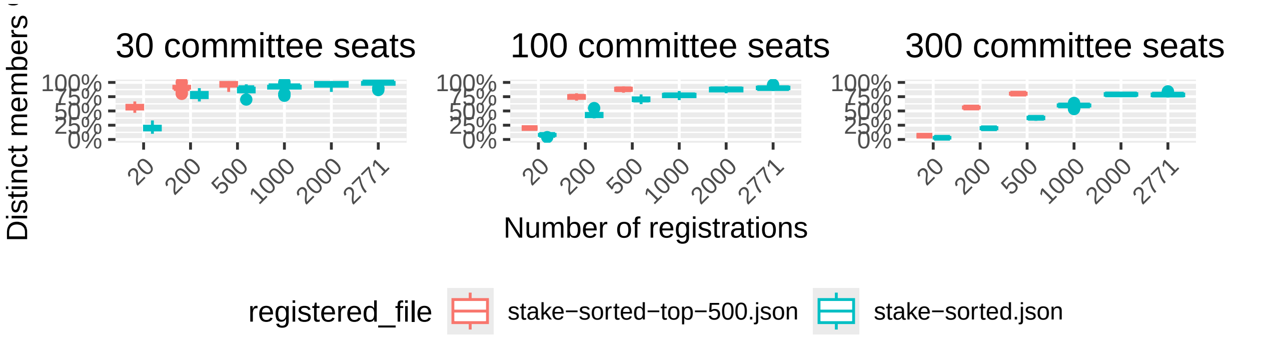
Plotting the ratio between the "safe stake" and total registered stake reinforces this observation:





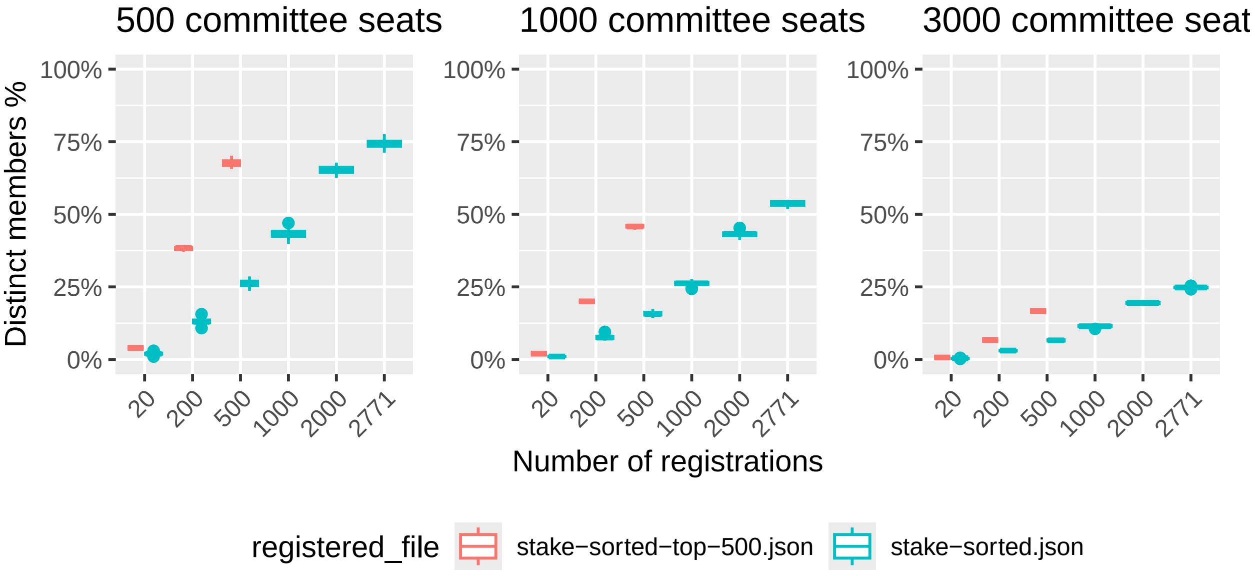
A cautious observation can be made that a committee that is 1/3 still typically requires around 34% of stake to be controlled by attacker to be affected. This suggests that a committee size should be kept above that number.

We can define "safe stake" as a minimum of "bottom" and "top safe stake" and plot its value as percentage of total registered stake:

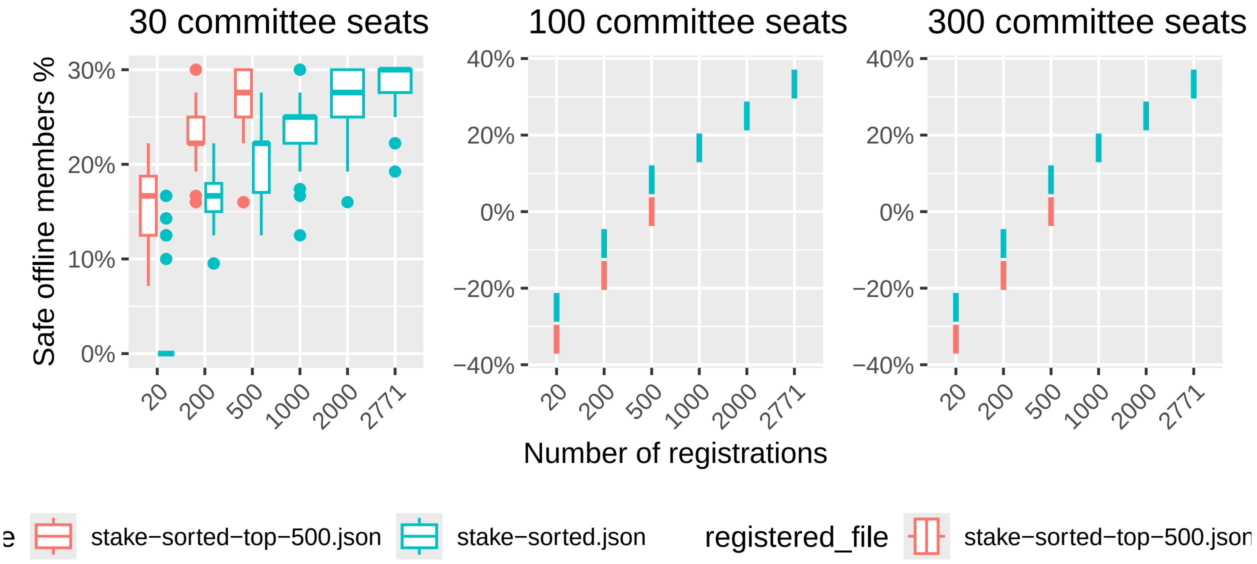


In the charts both full SPO data and top 500 SPO simulations approach a common upper bound on distinct member percentage as the registered candidate pool better reflects the underlying SPO population, which suggests that the resulting committees are dominated by the top 500 SPOs. The upper bound is mostly reached as the registered candidate pool grows to be an order of magnitude bigger than the committee size.

Plotting data for bigger committee sizes shows that they tend to have smaller distinct member percantage, indicating that there is a diminishing return on increasing the committee size, as bigger stake candidates get more chances to be assigned another slot:



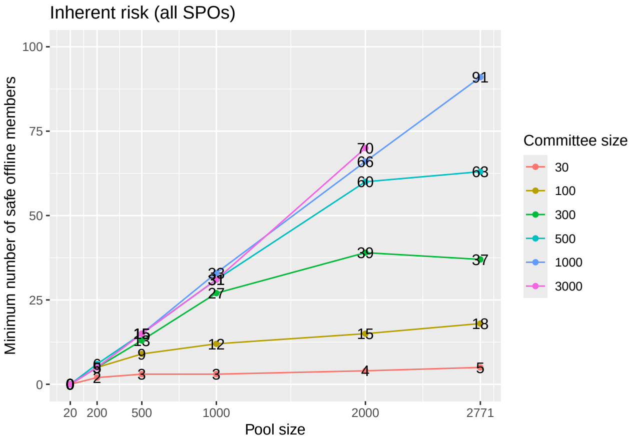
The number of unique committee members affects fault tolerance of the whole committee. If no member is assigned more than one seat, full 33% of malicious members can be tolerated, with this value shrinking as individual members get more seats. This can be observed by plotting the percentage of malicious committee members tolerated against candidate numbers:

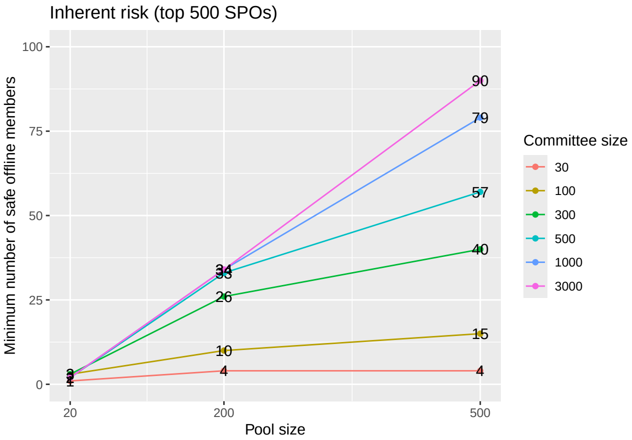


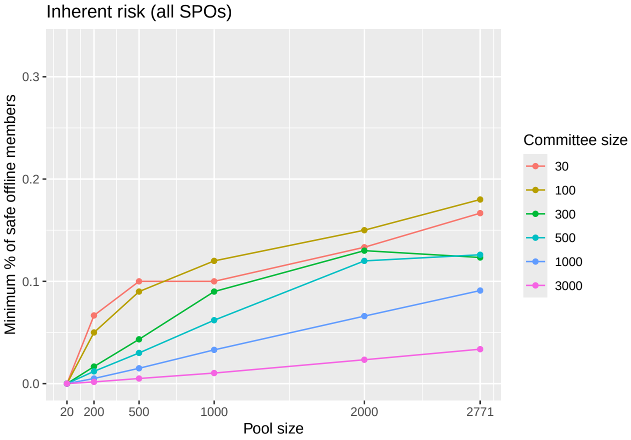
Similarly to the ratio of unique members, this ratio decreases as the committee size increases, even as the absolute underlying value grows, indicating a diminishing return in using bigger committees.

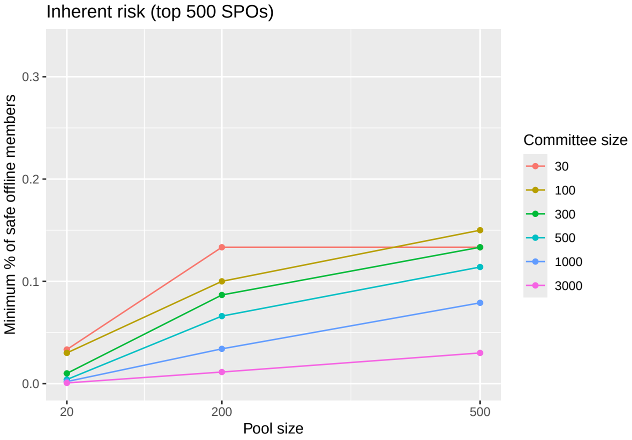
Inherent risk

Midnight finality risk document measures the “inherent risk” by the number of individual committee members (taking into account multiple seat assignments) that can go offline before the committee is no longer able to finalize blocks. The minimum number and percentage of safe offline members for each set of parameters can be visualised as follows:


Inherent risk (all SPOs)


Inherent risk (top 500 SPOs)


Inherent risk (all SPOs)

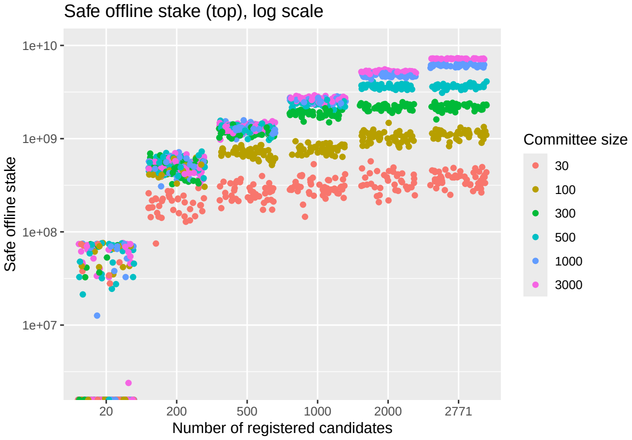

Inherent risk (top 500 SPOs)

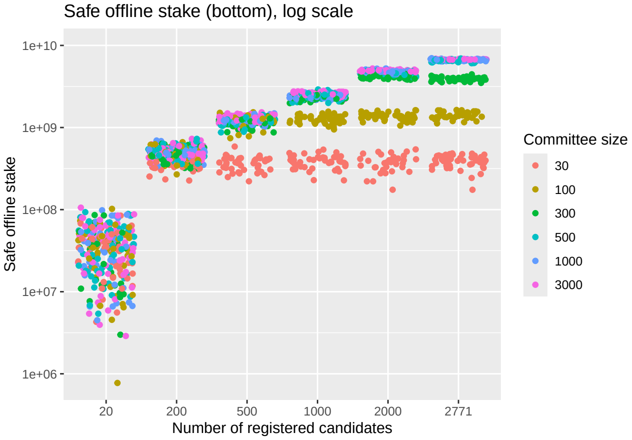
As expected, bigger committees gain more resilience when measured in absolute numbers of safe offline members. However, plotting the same data as percentage again shows that there is a diminishing return in relative terms from increasing committee size.

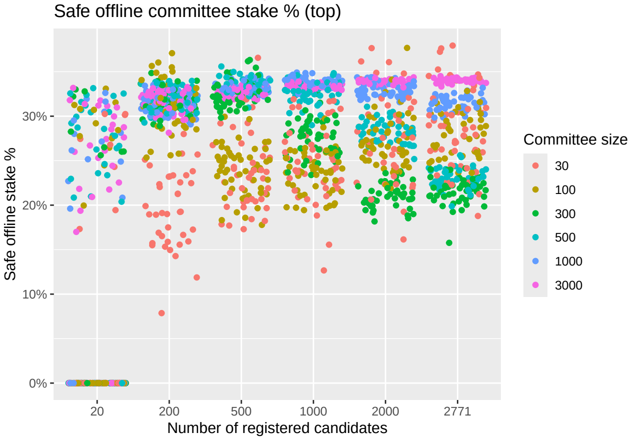
Cost of attack

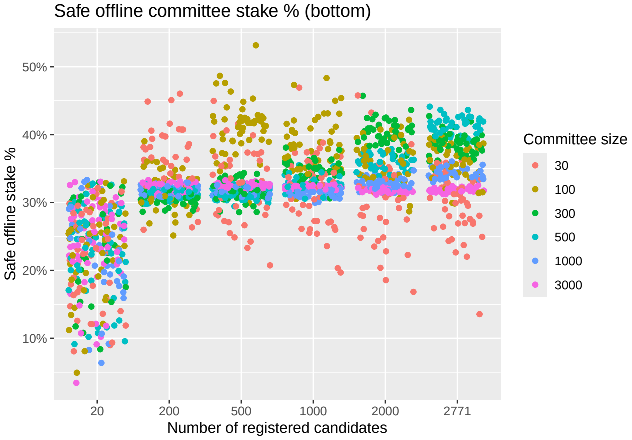
In addition to the minimum number of offline nodes that can be withstood by the committee, it is also important to understand what amount of ADA stake is behind the nodes that would need to go down to affect consensus. For that aim, the data set contains two metrics: - `top_safe_offline_stake`: total stake of top stake committee members that can safely go offline. this metric corresponds to a scenario where the least amount of physical nodes is affected in a successful attack - `bottom_safe_offline_stake`: total stake of lowest stake committee members that can go offlilne. this metric corresponds to a scenario where smallest players are affected, with the assumption, that lower stake means lower security or reliability.

Absolute and relative values of this stake are visualised below:


Safe offline stake (top), log scale

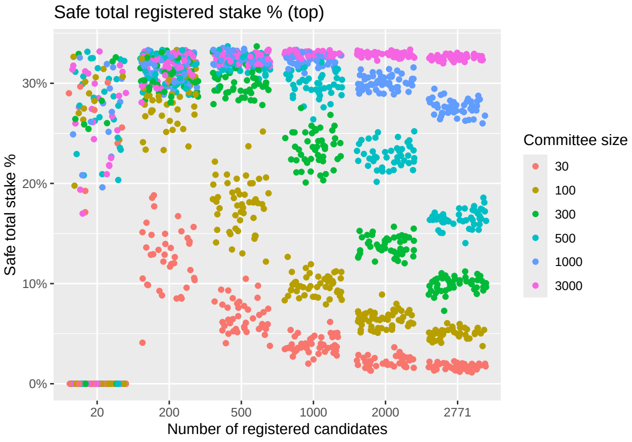

Safe offline stake (bottom), log scale

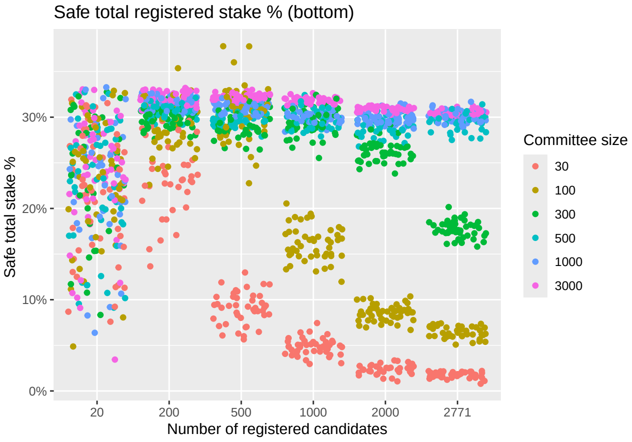

Safe offline committee stake % (top)


Safe offline committee stake % (bottom)

The plots show that the "safe stake" tends to converge on 33% when the committee is close to or higher than the number of candidates, which is expected as the committee closer approximates the candidate stake distribution.

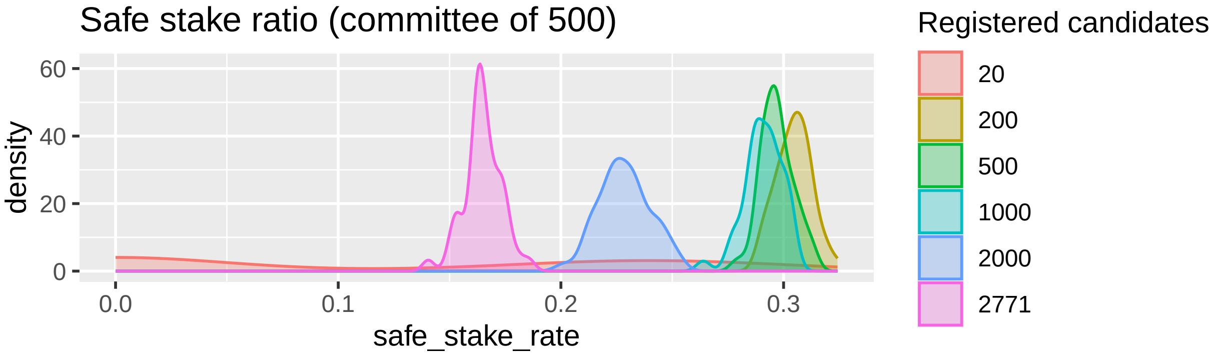
Plotting the ratio between the "safe stake" and total registered stake reinforces this observation:

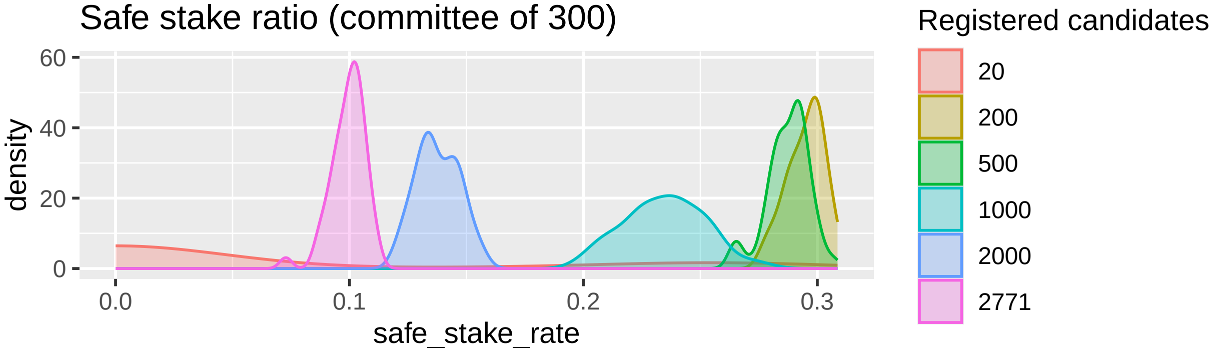

Safe total registered stake % (top)

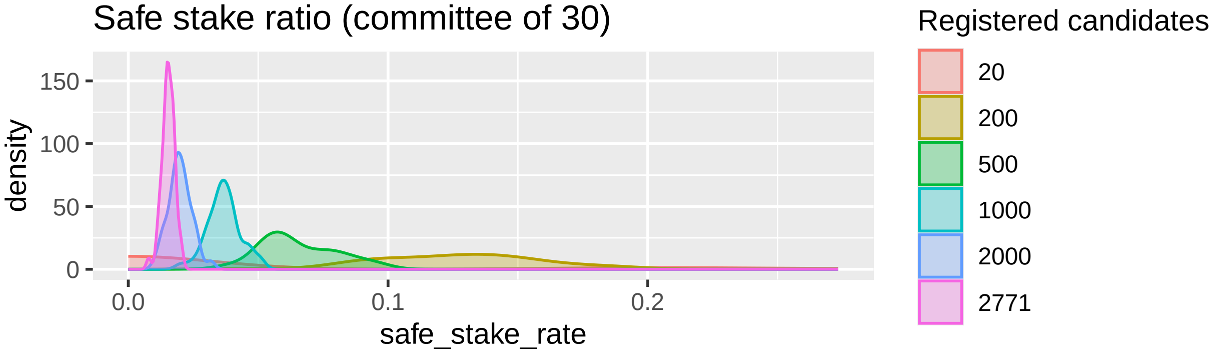

Safe total registered stake % (bottom)

A cautious observation can be made that a committee that is 1/3 still typically requires around 34% of stake to be controlled by attacker to be affected. This suggests that a committee size should be kept above that number.

We can define "safe stake" as a minimum of "bottom" and "top safe stake" and plot its value as percentage of total registered stake:


Safe stake ratio (committee of 500)
density
60
40
20
0
0.0
0.1
0.2
0.3
safe_stake_rate
Registered candidates
20
200
500
1000
2000
2771


Safe stake ratio (committee of 300)
density
60
40
20
0
0.0
0.1
0.2
0.3
safe_stake_rate
Registered candidates
20
200
500
1000
2000
2771


Safe stake ratio (committee of 30)
density
150
100
50
0
0.0
0.1
0.2
safe_stake_rate
Registered candidates
20
200
500
1000
2000
2771