In contexts where commitee sizes are sufficiently large, it could make sense to useAlgorand-style privately selected committees, in order to improve lookahead privacy to improve DoS resistance and resistance against other kinds of adaptive adversary attacks.

Algorand-style private selection works as follows. Suppose that each validator V_i

has a private preimage C_{V_i}

(a la RANDAO), and there is a common randomness source R

; for any given proposal P

, we derive a randomness R_P

(eg. $R_P = H(R, C_P)$)

, where C_P

is the proposer's

preimage). If there are in total N

validators and we want a committee of size M

, then anyone can make a signature by revealing C_{V_i}

and showing that $C_{V_i} \le 2^{256} * \frac{M}{N}$

. On average, M

of the N

validators will be able to do so for any given proposal, with standard deviation $\sqrt{M}$

and so at least $M - 3\sqrt{M}$

~99.85% of the time (and at most $M + 3\sqrt{M}$

99.85% of the time).

Suppose an attacker has fraction p

of proposers, and the committee threshold is $\frac{2}{3} * M$

; we can try to estimate the probability that a fraudulent proposal will get through for various values of p

and M

with publicly selected committees (which are guaranteed to have size exactly M

) and privately selected committees (using Poisson distributions, so assuming N

approaching infinity, values for $N = 20000$

are very close to the limit at $N \rightarrow \infty$

):

- $M = 200, p = \frac{1}{4}$

: public selection safety failure $6.25 * 10^{-35}$

, private selection $1.89 * 10^{-22}$

- $M = 100, p = \frac{1}{4}$

, public selection safety failure $1.21 * 10^{-18}$

, private selection $2.75 * 10^{-12}$

- $M = 200, p = \frac{1}{3}$

: public selection safety failure $1.07 * 10^{-21}$

, private selection $5.64 * 10^{-13}$

- $M = 100, p = \frac{1}{3}$

, public selection safety failure $6.45 * 10^{-12}$

, private selection $1.90 * 10^{-7}$

- $M = 200, p = \frac{1}{2}$

: public selection safety failure $1.77 * 10^{-6}$

, private selection $9.35 * 10^{-4}$

- $M = 100, p = \frac{1}{2}$

: public selection safety failure $4.36 * 10^{-4}$

, private selection $1.24 * 10^{-2}$

In summary, private selection unfortunately does have the weakness that it nearly doubles required safe committee sizes.