@JustinDrake @vbuterin

An election is called. Individuals can either vote by signing 0 or vote by signing 1, and may vote for both options.

Question: can we aggregate their votes so someone can verify the result quickly? Answer: yes, depending on how close the election is.

An aggregator for votes in one class (0 or 1 not both) creates a merkle tree storing the votes, with the additional condition that a path to leaf now represents a unique public address. At the leaf of a tree, the aggregator includes the signature for the corresponding public address (signing the correct number) as well as an id number up to the tally of votes being claimed N

.

The aggregator broadcasts the number N

along with the root of the merkle tree.

Now to verify the merkle tree does contain 70% of the claimed votes, a verifier picks 40 random numbers and requests the merkle paths to the leaves for all of them (with sibling nodes along the path to guarantee uniqueness of the address - represented in binary). Verifier accepts if all paths are formed correctly. The probability a tree with fewer than 70% of the purported votes gets past this test is $0.7^{40} = 6e^{-7}$

.

This protocol can be made non-interactive using the fiat-shamir heuristic and runs constant time in the number of votes, but is not constant in the difference between the two votes.

Now, suppose we have have verified a tally tree for 0 and a tally tree for 1, with the votes for 0 coming out higher than 1. The question is how do we decide whether to accept the outcome of the two tallies. Note, in a real election there may be multiple aggregators tallying the result. We accept the tally for 0 as the highest tally to pass the knowledge proof described above, and similarly for 1.

Denote the claimed and actual votes for 0 and 1 as c_0,c_1

and v_0,v_1 respectively

Let m

be the number of Merkle paths requested and t

be an acceptance threshold value say 0.00001.

Wlg assume $c_0>c_1$

.

To decide in favour of 0, we require that:

$\mathrm{P[v_0|c_0<c_1]} \leq t$

This is equivalent to:

$\mathrm{P[v_0|c_0<c_1]} = \mathrm{P[\frac{v_0}{c_0}<\frac{c_1}{c_0}]} =(\frac{c_1}{c_0})^{m} \leq t$

Hence:

$m \log (\frac{c_1}{c_0}) \leq \log t$

Dividing by $\log (\frac{c_1}{c_0})$

which is negative, we get:

$m\geq \frac{\log t }{\log \frac{c_1}{ c_0}}$

So we see that m

, the size of the proof, is inversely related to the logarithm of the ratio of the votes for either 1 or 0. So, short for most votes, if the result isn't too close, infinitely long for drawn votes. Good for situations where if a decision can't be made, one can wait for more votes to pile in on either side.