(It’s just a concept level idea. I hope this idea can be helpful to someone. Happy to get some feedback!)

tl;dr

: “One person, one vote” system that an address with more than a certain amount of token can vote, which detects fake identities using anomaly detection with a peer review system based on transaction history likeAdvogato trust metric.

To make a decision about an issue related to the protocol, we need to quantify the opinions of community. “One person, one vote” could be one of the best way to capture the opinions in the community. But we have to deal with the Sybil attack when we use this system.

As coin voting is Sybil-resistant, we might use a similar concept with a low level minimum balance(like 5 ETH or something) to get the voting right.

And in order to discriminate sockpuppet addresses, we could do some anomaly detection with the transaction history like Advogato or PageRank. For example, if an address received a transaction from a credible address, the address could be considered as not a fake identity(this is just an intuitive example. the real implementation might involve more sophisticated logic). We can do it with from hand-crafted rules to deep learning. The logic may not be able to discriminate sockpuppets perfectly, but this could be better than just one address one vote system.

To avoid oracle problems related to the anomaly detection logic(like an attacker exploits the logic which is open to public), we might use a logic pool which has a number of logics. We can aggregate the results of the logics and exclude outliers (e.g. cut head and tail). If a logic gives outliers too frequently, we can punish the author of the logic. Also we may use the confidence value of the anomaly detection result as a weight for each address, so that we can give the weight for each vote to calculate the final result.