Abstract: Decentralized Autonomous Organizations (DAOs) use smart contracts to foster communities working toward common goals. Existing definitions of decentralization, however-the 'D' in DAO-fall short of capturing key properties characteristic of diverse and equitable participation. We propose a new metric called Voting-Bloc Entropy (VBE, pronounced "vibe") that formalizes a broad notion of decentralization in voting on DAO proposals. VBE measures the similarity of participants' utility functions across a set of proposals. We use VBE to prove a number of results about the decentralizing effects of vote delegation, proposal bundling, bribery, and quadratic voting. Our results lead to practical suggestions for enhancing DAO decentralization. One of our results highlights the risk of systemic bribery with increasing DAO decentralization. To show that this threat is realistic, we present the first practical realization of a Dark DAO, a proposed mechanism for privacy-preserving corruption of identity systems, including those used in DAO voting. Our Dark-DAO prototype uses trusted execution environments (TEEs) in the Oasis Sapphire blockchain for attacks on Ethereum DAOs. It demonstrates that Dark DAOs constitute a realistic future concern for DAO governance.

arXiv.org

DAO Decentralization: Voting-Bloc Entropy, Bribery, and Dark DAOs

Decentralized Autonomous Organizations (DAOs) use smart contracts to foster communities working toward common goals. Existing definitions of decentralization, however-the 'D' in DAO-fall short of capturing key properties characteristic of diverse and...