DAOs Must Confront Dark DAOs — Or Fall Under Their Shadow

IC3

Follow

--

Listen

Share

Vote-buying in DAOs can be as easy as liquid staking and can be hidden from public view. To highlight this emerging risk, we've built a demo system.

by James Austgen (Cornell, IC3), Andrés Fábrega (Cornell, IC3), Sarah Allen (Flashbots, IC3), Kushal Babel (Cornell, IC3), Mahimna Kelkar (Cornell, IC3), and Ari Juels (Cornell, IC3)

Introduction

Decentralized Autonomous Organizations (DAOs) are increasingly popular, and already managing manybillions of dollars in treasuries. Their decentralized governance is a transformative new way of organizing communities. But as they grow, DAOs will face a new and potent threat to their decentralization: Dark DAOs

.

A Dark DAO is a private smart contract that targets a legitimate DAO, attacking its voting integrity by enabling vote-buying among its users. First considered in 2018, Dark DAOs haven't yet appeared in the wild — but only because DAOs arenot very decentralized today. As DAOs continue on a path to higher decentralization, Dark DAOs will inevitably surface.

Vote-buying may be illegal in political elections, but in DAOs it's probably legal. It'slegal in shareholder voting and there's even a marketplace to facilitate it. Vote-buying in DAOs would follow the trend in Web3 of monetizing everything from people's friends to maximal-extractable value (MEV).

More importantly, on the technical side, our new research shows that Dark DAOs are entirely practical. We've evenbuilt a fully functional prototype Dark DAO.

How a Dark DAO works

Consider T-DAO, a hypothetical Ethereum DAO. T-DAO is holding a referendum on whether to dissolve its large treasury and pay it out to token holders. Mallory, a T-DAO whale, wants the community to vote "Yes."

Mallory can launch a Dark DAO smart contract to buy votes from T-DAO users — offering, e.g., 0.001 ETH per token. To claim this money, a T-DAO voter like Alice deposits her tokens in the custody of the Dark DAO. The Dark DAO lets Mallory use Alice's tokens for the T-DAO vote and pays Alice for this one-time use. Since the Dark DAO is a smart contract, the whole process is automated, trustless, and scalable.

We've also prototyped a Dark DAO "Lite" that offers less privacy, but only requires Alice to acquire a new type of ERC-20 token (called "DD tokens") to participate. Dark DAO participation can be as easy as buying tokens on Uniswap, similar in spirit to liquid staking. In fact, our Dark DAO "Lite" can be extended to tokenize any

asset held by a single encumbered private key, breaking down the oft-held assumption that blockchain addresses are controlled by individuals or single entities. For example, this could enable derivatives for time-locked assets — e.g., escrowed tokens — held by an encumbered key to be tradable immediately, with assurance that the asset can be redeemed in the future. Our demo video shows how the tokenization process works.

The "dark" part

Of course, if a Dark DAO smart contract like Mallory's appeared on Ethereum, everyone would know. Given enough Dark-DAO activity, T-DAO members might manage somehow to cancel the referendum.

This is where the "dark" part of a Dark DAO comes in. Privacy-preserving blockchains — backed by technologies such as [trusted hardware

](https://www.intel.com/content/www/us/en/security/confidential-computing.html) — make it possible to implement a Dark DAO as a private

smart contract. Our prototype Dark DAO operates on Ethereum, but its back end uses a privacy chain called theOasis Sapphire ParaTime. The result is a truly "black box" Dark DAO that conceals vote-buying activity even from its creator.

To be clear, Dark DAOs — and private smart contracts more generally — can also serve many beneficial purposes. For instance, the ConstitutionDAO recently raised money from over 17,000 participants to bid on a copy of the U.S. Constitution at auction. This money, however, was publicly visible on Ethereum — a possible factor in their failure to win. Dark DAO tools could have concealed the ConstitutionDAO's fundraising. Use cases like this are good, but by stimulating privacy-tool development, also add to the inevitability of Dark DAOs.

A call to action

In the short term, the risk of Dark DAOs is small. That's why we chose to release our prototype. Our aim is to illuminate a looming danger while there's still time. But the DAO community needs to start working now

on ways to prevent or combat Dark DAOs.

There are technical countermeasures to Dark DAOs — at least in theory. Tools such as "complete knowledge" can prevent use of trusted hardware by DAO participants. But they're not ready for prime time. The DAO community needs to explore and advance such tools, develop new ones, and work together toward practical technologies to combat Dark DAOs.

Conclusion

As DAOs mature and become increasingly decentralized, Dark DAOs are certain to arise. Those who overlook the risk do so at the eventual peril of decentralization. The collective future of the DAO community has benefitted from the power of smart contracts. Its future now hinges on how well prepared it is to cope with that same technology being co-opted for Dark DAOs.

Editor: Bria Han (IC3, jh2584@cornell.edu)