Attacks on DAOs

Rainer Feichtinger, Robin Fritsch, Lioba Heimbach, Yann Vonlanthen and Roger Wattenhofer

Decentralized Autonomous Organizations (DAOs) are popular organizational structures that facilitate the trustless management of projects, by running atop a blockchain. In DAOs, governance is typically controlled by the holders of a designated governance token. Those who own these tokens can thus determine the course of the DAO. Today, DAOs govern many of the most used decentralized applications on blockchains and are estimated to hold and control in excess of $30B in their treasuries. Consequently, they hold significant power and a central position in the blockchain ecosystem.

"The DAO" on Ethereum in 2016 was the first attempt at creating a DAO on a blockchain. However, an infamous hack of The DAO stole $50M worth of ETH before the protocol even became operational. The event was so severe that it led to a controversial hard fork of the Ethereum blockchain. The original (unforked) blockchain still operates today as Ethereum Classic.

The DAO hack highlights the significant threat attacks on DAOs present not only to the DAOs themselves but also to the broader ecosystem. Additionally, given that DAOs are still in their early days and the ongoing evolution of their design frameworks, DAOs are particularly vulnerable to various novel attack vectors.

In our preliminary work, we analyze past real incidents and attacks on DAOs, study potential attacks that have been theorized, and describe additional possible attacks. We categorize these attacks on DAOs into four categories: (i) bribing and coalition (BC) attacks (ii) token acquisition (TA) attacks, (iii) computer-human interaction (CHI) attacks, and (iv) code and protocol vulnerability (CP) attacks.

We examine 23 past real incidents and attacks across four blockchains and indicate the attack vectors utilized. Our preliminary work finds that these attacks exploited vectors from all four categories fairly evenly. Moreover, we find that attack vectors that take advantage of human and economic aspects involved in governance represent a majority of past incidents, but are generally not analyzed in audits which heavily skew toward code and protocol vulnerability attacks.

Guided by our categorization of historical precedence, we introduce seven risk factors for DAOs and empirically analyze how susceptible a set of 24 DAOs is to them. Finally, we collect and discuss mitigations and safeguards that DAOs can implement.

We intend to use our improved understanding of DAO vulnerabilities to guide the development of more robust governance frameworks. Firstly, we want to understand which mitigations can readily be applied and which DAOs already do so. Secondly, through a more thorough analysis of the different voting mechanisms, we want to explore trade-offs in terms of decision efficiency versus vulnerability to attacks. Indeed,

while many DAOs follow a similar pattern, different ecosystems have adopted different implementations, comprising both on- and off-chain systems.

Our goal is to provide the necessary information and tools to facilitate design decisions for communities who might want to create new DAOs, allowing them to leverage knowledge gained from previous experiences and mistakes.