Double-Spend Counterattacks: Threat of Retaliation in Proof-of-Work Systems

Daniel J. Moroz, School of Engineering and Applied Sciences, Harvard University
Daniel J. Aronoff, Department of Economics, MIT
Neha Narula, MIT Media Lab
David C. Parkes, School of Engineering and Applied Sciences, Harvard University

Proof-of-Work mining is intended to provide blockchains with robustness against double-spend attacks. However, an economic analysis that follows from Budish (2018), considering free entry conditions together with the ability to rent sufficient hashrate to conduct an attack, suggests that the resulting block rewards can make the attack cheap. We formalize a defense to double-spend attacks, this defense having been proposed before but largely dismissed. We show that when the victim can counterattack in the same way as the attacker, this leads to a variation on the classic *War of Attrition* model from game theory. We show that, under mild assumptions, the threat of this kind of counterattack induces a subgame perfect equilibrium in which no attack occurs in the first place.

Latest version here

The authors would like to thank James P. Lovejoy, Eric Budish, Jacob Leshno, Mark Nesbitt, Jonathan Zittrain, James Mickens, Yiling Chen, Tadge Dryja, Nic Carter, and David Vorick for helpful discussions. This work is supported by two generous gifts to the Center for Research on Computation and Society at Harvard University, funders of the MIT Digital Currency Initiative, and NSF grant NSF CCF-15-09178. Daniel J. Moroz was supported in part by the Ethereum Foundation.