MEV-Freedom, in DeFi and Beyond

Massimo Bartoletti
University of Cagliari, Italy

Abstract

Maximal Extractable Value (MEV) refers to a class of recent attacks on public blockchains, where adversaries with the power to reorder, drop or insert transactions in a block can "extract" value from user transactions in the mempool. Empirical research has shown that mainstream DeFi protocols, like e.g. Automated Market Makers and Lending Pools, are massively targeted by MEV attacks. This has detrimental effects on their users, on transaction fees, and on the congestion of blockchain networks. Despite the growing knowledge on MEV attacks on blockchain protocols, an exact definition is still missing. Indeed, formally defining these attacks is an essential prerequisite to the design of provably secure, MEV-free blockchain protocols. In this talk, we propose a formal definition of MEV, based on a general, abstract model of blockchains and smart contracts. We then introduce MEV-freedom, a property enjoyed by contracts resistant to MEV attacks. We validate this notion by rigorously proving that Automated Market Makers and Lending Pools are not MEV-free. We finally discuss how to design MEV-free contracts.

2012 ACM Subject Classification Security and privacy → Formal methods and theory of security

Keywords and phrases Blockchain, Smart Contracts, Formal Security Notion

Digital Object Identifier 10.4230/OASIcs.FMBC.2022.1

Category Invited Talk

Bio

Massimo Bartoletti is Associate Professor at the Department of Mathematics and Computer Science of the University of Cagliari. His research activity concerns the development of tools and techniques for the specification, analysis and verification of software, with a special emphasis on security. Massimo Bartoletti is founder of the laboratory "BlockchainUnica" (`http://blockchain.unica.it`), one of the largest academic research group on blockchain technologies in Italy, director of the node of the Cyber Security National Lab for the University of Cagliari, and core member of the CINI working group on Blockchain. The laboratory is currently investigating several aspects of blockchain technologies, among which custom Domain-Specific Languages for smart contracts. He is principal investigator of several R&D projects on blockchain technologies, and member of the scientific board of several workshops on blockchain technologies. He is also the organisation chair of the first International School on Algorand Smart Contracts, funded by a grant of the Algorand Foundation.