Complete Citation

Eskandari, S., Moosavi, S., & Clark, J. (2020). Sok: Transparent dishonesty: front-running attacks on blockchain. In *Financial Cryptography and Data Security: FC 2019 International Workshops, VOTING and WTSC, St. Kitts, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers 23* (pp. 170-189). Springer International Publishing.

URL

https://arxiv.org/pdf/1902.05164.pdf

Key Words

Front-running, Security, Blockchain, Decentralized App(DApp), Initial Coin Offering(ICO), Ethereum

General Subject

The general subject of this paper is front-running attacks on blockchain applications, with a focus on decentralized applications (DApps) deployed on the Ethereum blockchain.

Specific Subject

The specific subject of this paper is front-running attacks on decentralized applications (DApps) deployed on the Ethereum blockchain. The paper provides a categorization of front-running attacks and proposed solutions, as well as case studies of specific DApps and an initial coin offering (ICO) that have been affected by front-running. It also provides a detailed analysis of front-running attacks and proposed solutions for preventing from front-running attacks.

Hypothesis

There are no explicit hypotheses stated in this paper. However, it considered front-running as a course of action where an entity benefits from prior access to privileged market information about upcoming transactions and trades.

Methodology

In this paper, the top 25 decentralized applications (DApps) deployed on Ethereum blockchain are analyzed for different instances of front-running attacks. Also it provided a detailed analysis of Status.im initial coin offering (ICO) and has shown evidences of miner's abnormal behaver indicative of front-running. Based on these analysis, front-running attacks are classified in different categories and some possible solutions are provided for preventing and mitigation of these attacks.

Results

The case studies presented in the paper illustrate the high impact of front-running attacks on top most used DApps and an initial coin offering (ICO).

Overall, the paper highlights the need for more research to develop effective mitigation strategies for front-running attacks on DApps and ICOs.

Summary of Key Points

The paper focuses on front-running attacks on decentralized applications (DApps) deployed on the Ethereum blockchain.

Front-running is a type of attack where a malicious actor exploits their knowledge of pending transactions to gain an advantage over other users.

The paper provides a categorization of front-running attacks. This categorization distinguishes three cases: displacement attack, insertion attack and suppression attacks. In all three cases the attacker (Mallory) tries to invoke her own function before the victim's (Alice) function. In displacement attack, it is not important for Mallory that Alice's function call runs or not after her function. But in insertion attack, Mallory needs Alice's function to run after her function to get any profits. In suppression attack the only target of Mallory is to delay Alice's transactions.

The paper presents case studies of specific DApps and an initial coin offering (ICO) that have been affected by front-running attacks, including decentralized exchanges, crypto-collectibles, gambling services, and decentralized name services.

The paper provides three categories of solutions for front-running: transaction sequencing, confidentiality and design practices.

The paper notes that more research is needed to develop effective mitigation strategies for front-running attacks on DApps and ICOs.

Important Figures

Fig. 3: The percentage of Ethereum blocks mined between block 3903900 and 3908029, this is the time frame in which Status.im ICO was running. This percentage roughly shows the hashing power ratio each miner had at that time.

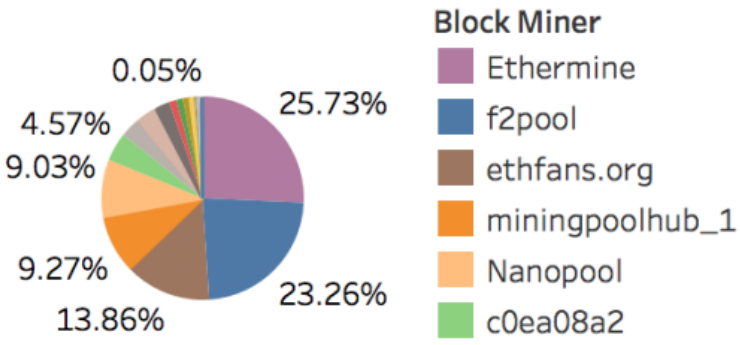
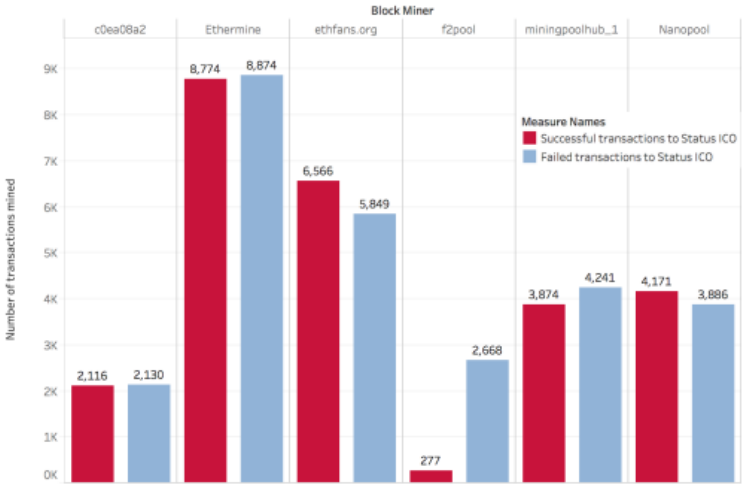


Fig. 4: This chart shows the miners behaviour on the time frame that Status.im ICO was running. It is clear that the number of successful transactions mined by F2Pool do not follow the random homogeneous pattern of the rest of the network.



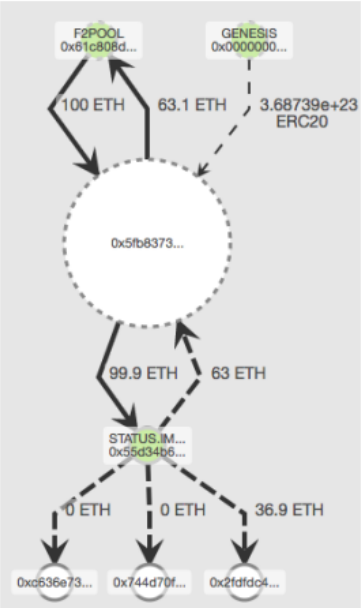


Fig. 5: Prior to *Status.im* ICO *F2Pool* deposited 100 Ether in multiple new Ethereum addresses. On the time of the ICO, transactions sent from these addresses to *Status* ICO smart contract were prioritized in their mining pool, resulting in purchasing *ERC20* tokens. This method was used to overcome the dynamic ceiling algorithm of the ICO smart contract. Later on they sent the refunded Ether back to their own address.[15]

Related Works

1. "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges" by Philip Daian et al. This paper explores front-running attacks on decentralized exchanges (DEXs) and proposes a new type of attack called "sandwich attacks" that exploit the mechanics of DEXs.
2. "Smart Contract Security: A Survey" by Nicola Atzei et al. This survey paper provides an overview of security issues related to smart contracts, including front-running attacks and other types of vulnerabilities that can be exploited by malicious actors. The paper also discusses potential mitigation strategies for these vulnerabilities.
3. Nowadays, smart contract auditing is one of the hottest topics in the domain of DApps. Many companies put their developed smart contracts and DApps into different contests and competitions so that people compete with each other to find different types of vulnerabilities in their smart contracts including front-running attacks. These kinds of competitions usually have a very high amount of reward for the contestants.

Presentation URL

https://drive.google.com/file/d/1HSS56rJG6xteSjdlv1Cx5_m4NtEyOPpN/view?usp=drive_link