Cyprus University of Technology
Department of Electrical Engineering and Computer Engineering and Informatics

Bachelor Thesis

Detecting, Analyzing and Understanding Zero-Transfer Attacks in the Ethereum Ecosystem

Leonidas Kotidis

Limassol, May 2025

CYPRUS UNIVERSITY OF TECHNOLOGY

Faculty of Engineering and Technology

Department of Electrical Engineering, Computer Engineering, and Informatics

Bachelor Thesis

Detecting, Analyzing and Understanding Zero-Transfer Attacks in the Ethereum Ecosystem

Leonidas Kotidis

Advisor: Panagiotis Ilia

Limassol, May 2025

Copyrights

The approval of the dissertation by the Department of Electrical Engineering, Computer Engineering, and Informaticsdoes not necessarily imply the approval by the Department of the views of the writer.

Acknowledgements

I would like to express my sincere gratitude to my thesis supervisor, Mr. Panagiotis Ilia, for his continuous guidance, support, and invaluable feedback throughout the development of this work. His expertise and knowledge have been crucial in shaping this project from start to finish.

I would also like to thank my parents for their patience, encouragement, understanding, and financial support throughout my university journey. Their unwavering support has been the foundation of my success.

ABSTRACT

This thesis looks into **zero-transfer attacks** on the **Ethereum blockchain** which is a type of scam where attackers trick users into sending money to the wrong wallet by sending fake, zero-value transactions. While the general idea of these attacks is known, its not widespread and there hasn't been much large-scale research to show how often they happen or how to detect them effectively.

To fix that, we built a **Python framework** using **Selenium** to collect wallet data directly from **Etherscan**. We scraped over 18,000 real user wallet histories and filtered out exchanges or non-wallet addresses. Then we parsed every transaction to pull info like wallet addresses, timestamps, amounts, and transaction IDs. We designed two versions of a detection method, one relaxed and one strict. The relaxed version flagged more possible attacks, but had more false positives. The strict version added checks for both the first and last four characters of the wallet address and only flagged transactions under $2 to improve accuracy.

On the strict version in total, 3.96% of wallets had been targeted, and over 11,600 attacks were detected. Of these, 1,205 were successful, though most only led to small losses. The results show that while these attacks don't bring big profits most of the time, they rely on volume. Attackers hope that eventually, someone makes a big mistake. Overall, the detection method worked well and can be a solid base for building tools to help users stay safe.