Τεχνολογικό Πανεπιστήμιο Κύπρου

Τμήμα Ηλεκτρολόγων Μηχανικών
και Μηχανικών Ηλεκτρονικών
Υπολογιστών και Πληροφορικής

Πτυχιακή εργασία

Ανίχνευση sandwich attacks στο Ethereum μέσω ανάλυσης on-chain δεδομένων

Κωνσταντίνος Ιωάννου

Λεμεσός, Ιούνιος 2025

Τεχνολογικό
Πανεπιστήμιο
Κύπρου

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΗΜΠ 412 -Διπλωματική Εργασία Ακαδημαϊκό έτος 2024-2025

Όνομα Φοιτητή / ΑΦΤ : Κωνσταντίνος Ιωάννου

Βαθμός: 6.5

Τίτλος: Ανάλυση sandwich attacks στο Ethereum μέσω ανάλυσης on-chain δεδομένων

Επιβλέπων Καθηγητής:

Παναγιώτης Ηλία		3/6/2025
Όνομα	Υπογραφή	Ημερ.

Εξεταστής 1:

Ανδρέας Λαβαστός		3/6/2025
Όνομα	Υπογραφή	Ημερ.

Εξεταστής 2:

Χρίστος Λοΐζου		3/6/2025
Όνομα	Υπογραφή	Ημερ.

ΤΕΧΝΟΛΟΓΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πτυχιακή εργασία

Ανίχνευση sandwich attacks στο Ethereum μέσω ανάλυσης on-chain δεδομένων

Κωνσταντίνος Ιωάννου

Επιβλέπων Καθηγητής

Δρ. Παναγιώτης Ηλία

Λεμεσός, Ιούνιος 2025

Πνευματικά δικαιώματα

Η έγκριση της πτυχιακής εργασίας από το Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογιών Πληροφορικής του Τεχνολογικού Πανεπιστημίου Κύπρου δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του/της συγγραφέα εκ μέρους του Τμήματος.

Ευχαριστίες

Με την ολοκλήρωση της παρούσας πτυχιακής εργασίας, αισθάνομαι την ανάγκη να εκφράσω τις βαθιές μου ευχαριστίες και την ειλικρινή μου εκτίμηση προς όλους εκείνους που συνέβαλαν με τον τρόπο τους στην επιτυχή ολοκλήρωση αυτής της προσπάθειας. Πρώτα απ' όλα, θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου, Δρ. Παναγιώτη Ηλία, για την πολύτιμη καθοδήγηση, τη συνεχή υποστήριξη, τις χρήσιμες συμβουλές και τις καίριες παρατηρήσεις του καθ' όλη τη διάρκεια της εκπόνησης της εργασίας. Η καθοδήγησή του αποτέλεσε βασικό πυλώνα για την επιστημονική και ερευνητική μου πορεία σε αυτό το εγχείρημα, και τον ευχαριστώ θερμά για τον χρόνο και την αφοσίωση που αφιέρωσε.

Επιπλέον, θα ήθελα να εκφράσω την ευγνωμοσύνη μου προς την οικογένειά μου για την αμέριστη στήριξη, την υπομονή, την ενθάρρυνση και την πίστη τους στις δυνατότητές μου καθ' όλη τη διάρκεια των σπουδών μου και ειδικότερα κατά την περίοδο συγγραφής της πτυχιακής εργασίας. Η στήριξή τους αποτέλεσε για μένα πηγή δύναμης και έμπνευσης.

Τέλος, ένα μεγάλο ευχαριστώ στους φίλους μου, οι οποίοι στάθηκαν δίπλα μου με κατανόηση και συμπαράσταση, συμβάλλοντας ουσιαστικά στη διατήρηση της ψυχικής μου ισορροπίας και ενθαρρύνοντάς με να συνεχίσω την προσπάθειά μου ακόμα και στις πιο απαιτητικές στιγμές.

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία επικεντρώνεται στην ανίχνευση και ανάλυση sandwich attacks στο οικοσύστημα του Ethereum, με έμφαση στις συναλλαγές που πραγματοποιούνται μέσω αποκεντρωμένων ανταλλακτηρίων (DEX) όπως το Uniswap [1]. Τα sandwich attacks αποτελούν μια κακόβουλη στρατηγική όπου ένας επιτιθέμενος παρεμβάλλει συναλλαγές πριν και μετά από μια συναλλαγή θύματος, εκμεταλλευόμενος τη διακύμανση της τιμής προς όφελός του [2].

Η εργασία εστιάζει στην ανάπτυξη ενός μηχανισμού ανίχνευσης τέτοιων επιθέσεων βάσει πραγματικών on-chain δεδομένων. Για την επίτευξη του στόχου, αξιοποιήθηκε η γλώσσα προγραμματισμού Python και εφαρμόστηκε μια προσέγγιση βασισμένη σε δεδομένα συναλλαγών εξαγόμενα από το Etherscan.

Το εργαλείο αναλύει τις συναλλαγές μέσω αρχείων .csv, πραγματοποιώντας φιλτράρισμα και χρονική ταξινόμηση. Έπειτα, εφαρμόζει έναν αλγόριθμο "κινούμενου παραθύρου", εντοπίζοντας ύποπτα μοτίβα τύπου BUY–BUY–SELL και SELL–SELL–BUY, τα οποία συνδέονται με επιθέσεις sandwich. Ανιχνεύονται περιπτώσεις όπου ο ίδιος λογαριασμός αλληλεπιδρά δύο φορές με το ίδιο pool, πριν και μετά τη συναλλαγή ενός τρίτου χρήστη, υποδεικνύοντας ενδεχόμενη εκμετάλλευση της τιμής. Οι επιτιθέμενοι που εντοπίζονται καταγράφονται σε δομημένο αρχείο τύπου JSON μαζί με τις σχετικές συναλλαγές και χρονικές πληροφορίες. Η προσέγγιση αυτή παρέχει ευελιξία και ακρίβεια, ενώ η χρήση τοπικών δεδομένων εξαλείφει τους τεχνικούς περιορισμούς των API.

Κατά την εφαρμογή του εργαλείου εντοπίστηκαν πολυάριθμες περιπτώσεις sandwich attacks, με μεγαλύτερη συχνότητα σε tokens με αυξημένη δραστηριότητα και όγκο συναλλαγών. Το μοτίβο SELL–SELL–BUY εμφανίστηκε συχνότερα σε σχέση με το BUY–BUY–SELL, ενώ η πλειονότητα των επιθέσεων εκδηλώθηκε με ελάχιστη χρονική απόσταση μεταξύ των επιμέρους συναλλαγών (0–2 δευτερόλεπτα). Επιπλέον, παρατηρήθηκαν επαναλαμβανόμενες διευθύνσεις επιτιθέμενων, γεγονός που υποδηλώνει τη δράση αυτοματοποιημένων bots με συστηματική στρατηγική.

Μέσω της επεξεργασίας των δεδομένων, το σύστημα εντοπίζει μοτίβα που υποδηλώνουν την ύπαρξη sandwich attacks και καταγράφει τους επιτιθέμενους σε αρχείο JSON. Αν και δεν υλοποιείται διαδικασία καταγγελίας, η παραγόμενη πληροφορία μπορεί δυνητικά να αξιοποιηθεί για τεκμηριωμένη υποβολή καταγγελιών σε αρμόδιους φορείς ή για

περαιτέρω ερευνητική αξιοποίηση με στόχο την ενίσχυση της ασφάλειας στο οικοσύστημα του DeFi [3].

Λέξεις-κλειδιά: Ethereum, Sandwich Attack, DeFi, Etherscan API, Dexscreener, Python, Ανίχνευση Επιθέσεων

ABSTRACT

This thesis focuses on the detection and analysis of sandwich attacks in the Ethereum ecosystem, with an emphasis on transactions executed through decentralized exchanges (DEXs) such as Uniswap [1]. Sandwich attacks are a malicious strategy in which an attacker inserts transactions before and after a victim's transaction, exploiting price fluctuations for personal gain [2].

The goal of the project is to develop a detection mechanism based on real on-chain data. To achieve this, the Python programming language was utilized, and the approach was based on transaction data exported from Etherscan.

The tool processes transactions via .csv files, performing filtering and chronological sorting. It then applies a sliding window algorithm to detect suspicious patterns such as BUY–BUY–SELL and SELL–SELL–BUY, which are associated with sandwich attacks. The tool identifies cases where the same address interacts with the same liquidity pool before and after a victim's transaction, suggesting potential price manipulation. Identified attackers are logged in a structured JSON file along with the relevant transactions and timestamps. This approach ensures both flexibility and accuracy, while avoiding the technical limitations of live API usage.

During testing, numerous sandwich attacks were detected, primarily in tokens with high transaction volume and activity. The SELL–SELL–BUY pattern was observed more frequently than BUY–BUY–SELL, with most attacks occurring within 0–2 seconds between steps. Furthermore, several repeated attacker addresses were identified, indicating the presence of bots executing systematic strategies.

Through this analysis, the system detects patterns indicative of sandwich attacks and records the attackers in a JSON file. While it does not implement an automated reporting mechanism, the generated data can potentially support the submission of formal complaints to regulatory entities or be used for further research aimed at strengthening security in the DeFi ecosystem [3].

Keywords: Ethereum, Sandwich Attack, DeFi, Etherscan API, Dexscreener, Python, Attack Detection