

**ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ**



**CÔNG TRÌNH DỰ THI
HỘI NGHỊ SINH VIÊN NGHIÊN CỨU KHOA HỌC
NĂM HỌC 2022-2023**

**PHÁT HIỆN TẤN CÔNG TRONG CÁC GIAO DỊCH
BLOCKCHAIN SỬ DỤNG HỌC MÁY**

Bùi Đức Mạnh - QH-2019-I/ĐA-CLC

Cán bộ hướng dẫn: TS. Trần Thị Thúy Quỳnh

HÀ NỘI - 2023

LỜI CẢM ƠN

*Tôi xin chân thành cảm ơn TS. Trần Thị Thúy Quỳnh, người đã dẫn dắt, định hướng cho tôi trong những nghiên cứu về **Phát hiện tấn công trong các giao dịch blockchain sử dụng học máy**. Tôi cũng xin cảm ơn các thầy, cô Khoa Điện tử - Viễn thông và các thầy cô phản biện đã cho nhiều góp ý giúp tôi khắc phục những điểm còn hạn chế trong nghiên cứu khoa học.*

Tôi cũng xin cảm ơn ...

Hà Nội, ngày ... tháng ... năm 2023

Sinh viên

Bùi Đức Mạnh

LỜI CAM ĐOAN

Tôi xin cam đoan **Phát hiện tấn công trong các giao dịch blockchain sử dụng học máy** là công trình nghiên cứu thực sự của tôi, được thực hiện dựa trên cơ sở lý thuyết, kiến thức chuyên ngành dưới sự hướng dẫn khoa học của TS. Trần Thị Thúy Quỳnh.

Tôi xin cam đoan những công việc trong nghiên cứu khoa học thực hiện chưa từng được các tác giả khác đề xuất. Với sự hiểu biết của mình, tôi chắc chắn các số liệu, kết quả trong nghiên cứu khoa học là trung thực và chưa được công bố ở đâu và trong bất cứ công trình nào trừ công trình của tác giả và tài liệu tham khảo.

Nếu có gì sai trái, tôi xin hoàn toàn chịu trách nhiệm.

Hà Nội, ngày ... tháng ... năm 2023

Sinh viên

Bùi Đức Mạnh

MỤC LỤC

Lời cảm ơn	
Lời cam đoan	
Mục lục	i
Tóm tắt	ii
Danh mục hình vẽ	iii
Danh mục bảng biểu	iv
Mở đầu	1
CHƯƠNG 1. TỔNG QUAN VỀ PHÁT HIỆN TẤN CÔNG TRONG CÁC GIAO DỊCH BLOCKCHAIN	2
CHƯƠNG 2. PHÁT HIỆN TẤN CÔNG TRONG MẠNG ETHEREUM SỬ DỤNG HỌC MÁY	3
CHƯƠNG 3. KẾT QUẢ MÔ PHỎNG VÀ ĐÁNH GIÁ	4
KẾT LUẬN VÀ HƯỚNG NGHIÊN CỨU TIẾP THEO	5
PHỤ LỤC	6
TÀI LIỆU THAM KHẢO	7

TÓM TẮT

Tóm tắt: Nghiên cứu này tập trung vào việc phân tích, phân loại và phát hiện các kiểu tấn công có khả năng xảy ra tại lớp ứng dụng của mạng Blockchain. Để tăng tính ứng dụng của nghiên cứu, nhóm lựa chọn hệ thống truy xuất nguồn gốc thực phẩm nông nghiệp trên nền tảng Blockchain để thực nghiệm và đánh giá các loại tấn công có thể xảy ra đối với một mạng Blockchain trong lĩnh vực nông nghiệp. Để tạo dữ liệu cho mô hình học, một mô hình mạng riêng tư Ethereum 2.0 đã được triển khai. Trong đó, dữ liệu của các giao dịch ở trạng thái thông thường được tạo bởi hệ thống truy xuất nguồn gốc mà nhóm đưa vào. Dữ liệu tấn công được tạo bởi các cuộc tấn công đã từng xảy ra gây thiệt hại lớn và được đánh giá là có khả năng gây hại đến hệ thống nông nghiệp trên nền tảng Blockchain. Với bộ dữ liệu thu thập được, nhóm đề xuất mô hình học máy sử dụng mạng neuron đa tầng với đầu vào rời rạc (SMLP) để có thể phân loại và phát hiện tấn công với phương pháp tiền xử lý dữ liệu áp dụng xử lý ngôn ngữ tự nhiên (NLP). Đồng thời, nhóm cũng sử dụng các mô hình phân loại cổ điển như SVM hay mô hình Ensemble để có thể tiến hành so sánh hiệu suất với phương pháp đề xuất và kết quả thu được cho thấy phương pháp đề xuất cho ra hiệu suất tốt hơn so với các mô hình truyền thống, lên đến 99% trong việc phân loại các tấn công. Kết quả này chỉ ra tính khả quan của mô hình cho việc áp dụng vào các mạng Blockchain thực tế

Từ khóa: Bảo mật, Phát hiện tấn công, Blockchain, Hợp đồng thông minh, Giao dịch, Học máy.

DANH MỤC HÌNH VẼ

DANH MỤC BẢNG BIỂU

MỞ ĐẦU

Lý do chọn đề tài

Phương pháp nghiên cứu

Nội dung nghiên cứu

Đóng góp của đề tài

Bố cục của báo cáo nghiên cứu khoa học

Nội dung chính của nghiên cứu khoa học được trình bày như sau:

- Mở đầu:
- Chương 1:
- Chương 2:
- Chương 3:
- Kết luận và hướng nghiên cứu tiếp theo:

CHƯƠNG 1
TỔNG QUAN VỀ PHÁT HIỆN TẤN CÔNG TRONG CÁC GIAO DỊCH
BLOCKCHAIN

[1]

CHƯƠNG 2

PHÁT HIỆN TẤN CÔNG TRONG MẠNG ETHEREUM SỬ DỤNG HỌC
MÁY

CHƯƠNG 3

KẾT QUẢ MÔ PHỎNG VÀ ĐÁNH GIÁ

KẾT LUẬN VÀ HƯỚNG NGHIÊN CỨU TIẾP THEO

PHỤ LỤC

TÀI LIỆU THAM KHẢO

- [1] X. Yang, M. Li, H. Yu, M. Wang, D. Xu, and C. Sun, “A trusted blockchain-based traceability system for fruit and vegetable agricultural products,” *IEEE Access*, vol. 9, pp. 36282–36293, Mar. 2021.