IMPLEMENTASI *DEEP LEARNING* SEBAGAI UPAYA MENDETEKSI TINDAK PENIPUAN TOKEN KRIPTO PADA JARINGAN ETHEREUM

SKRIPSI

DIMAS ARYA PAMUNGKAS
20120040004

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK, KOMPUTER DAN DESAIN

SUKABUMI

JULI 2023

IMPLEMENTASI *DEEP LEARNING* SEBAGAI UPAYA MENDETEKSI TINDAK PENIPUAN TOKEN KRIPTO PADA JARINGAN ETHEREUM

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat Dalam Menempuh Gelar Sarjana Teknik Informatika

DIMAS ARYA PAMUNGKAS
20190040004

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK, KOMPUTER DAN DESAIN

SUKABUMI

JULI 2023

PERNYATAAN PENULIS

JUDUL	:	IMPLEMENTASI *DEEP LEARNING* SEBAGAI UPAYA MENDETEKSI TINDAK PENIPUAN TOKEN KRIPTO PADA JARINGAN ETHEREUM
NAMA	:	DIMAS ARYA PAMUNGKAS
NIM	:	20190040004

"Saya menyatakan dan bertanggung jawab dengan sebenarnya bahwa Skripsi ini adalah hasil karya saya sendiri kecuali cuplikan dan ringkasan yang masing-masing telah saya jelaskan sumbernya. Jika pada waktu selanjutnya ada pihak lain yang mengklaim bahwa Skripsi ini sebagai karyanya, yang disertai dengan bukti-bukti yang cukup maka saya bersedia untuk dibatalkan gelar Sarjana Komputer saya beserta segala hak dan kewajiban yang melekat pada gelar tersebut"

Sukabumi, 13 Juli 2023

Dimas Arya Pamungkas
Penulis

PERSETUJUAN SKRIPSI

JUDUL	:	IMPLEMENTASI *DEEP LEARNING* SEBAGAI UPAYA MENDETEKSI TINDAK PENIPUAN TOKEN KRIPTO PADA JARINGAN ETHEREUM
NAMA	:	DIMAS ARYA PAMUNGKAS
NIM	:	20190040004

Skripsi ini telah diperiksa dan disetujui

Sukabumi, 13 Juli 2023

Ketua Program Studi,	Pembimbing,
Anggun Fergina, M.Kom	Ivana Lucia Kharisma, M.Kom
NIDN. 0407029301	NIDN. 0429038002

PENGESAHAN SKRIPSI

JUDUL : IMPLEMENTASI *DEEP LEARNING* SEBAGAI UPAYA MENDETEKSI TINDAK PENIPUAN TOKEN KRIPTO PADA JARINGAN ETHEREUM
NAMA : DIMAS ARYA PAMUNGKAS
NIM : 20190040004

Skripsi ini telah diujikan dan dipertahankan di depan Dewan Penguji pada Sidang Skripsi tanggal 13 Juli 2023 Menurut pandangan kami, Skripsi ini memadai dari segi kualitas untuk tujuan penganugerahan gelar Sarjana Komputer (S.Kom)

Sukabumi, 13 Juli 2023

Pembimbing I

Ivana Lucia Kharisma, M.Kom
NIDN : 0429038002

Pembimbing II

Dwi Sartika Simatupang, S.T., M.TI
NIDN : 0428058906

Ketua Dewan Penguji

Somantri, ST, M.Kom
NIDN : 0419128801

Ketua Program Studi Teknik Informatika

Anggun Fergina, M.Kom
NIDN : 040729301

Dekan Fakultas Teknik Komputer dan Desain

Ir. Paikun, S.T., M.T., IPM., Asean Eng.
NIDN : 0402037401

Betapa besarnya cinta dan kasihmu yang telah kau berikan
kepadaku sejak aku masih di dalam kandunganmu ibu.
Dan terima kasih ayah hingga saat ini aku sudah beranjak dewasa
engkau masih menjadi orang yang selalu ada buatku.
Terima kasih untuk semuanya ibu dan ayah.
Semoga Allah selalu memberikan cahaya kepadamu.

ABSCTRACT

With the increasing popularity of blockchain technology and the use of crypto tokens, the problem of financial security in blockchain transaction networks have become more serious. There have been many cases of fraud in blockchain technology, especially on the Ethereum network. To overcome this problem, this research designs and builds a system that can detect fraudulent acts on ERC-20 tokens on the Ethereum network. The method used in this study is the Deep Neural Networks (DNN) algorithm to detect objects from scam tokens. The results of the performance evaluation show that the model created is capable of detecting fraud very well with a very high level of accuracy, which is above 99%. In testing the app, 100 new tokens were randomly purchased and resold without issue, indicating that the app can distinguish between scam tokens and non-scam tokens.

Keywords : Blockchain, Scam, Ethereum, Crypto Token, Deep Neural Networks

ABSTRAK

Dengan semakin populernya teknologi *blockchain* dan penggunaan token kripto, masalah keamanan finansial dalam jaringan transaksi *blockchain* menjadi semakin serius. Banyak terjadi kasus penipuan dalam teknologi *blockchain* terutama pada jaringan Ethereum. Untuk mengatasi masalah tersebut, penelitian ini merancang dan membangun sistem yang dapat mendeteksi tindak penipuan pada token ERC-20 di jaringan Ethereum. Metode yang digunakan dalam penelitian ini adalah algoritma *Deep Neural Networks* (DNN) untuk mendeteksi objek dari token *scam*. Hasil evaluasi performa menunjukkan bahwa model yang dibuat mampu dengan sangat baik dalam mendeteksi penipuan dengan tingkat akurasi yang sangat tinggi, yaitu di atas 99%. Dalam pengujian aplikasi, 100 token baru secara *random* dibeli dan dapat dijual kembali tanpa masalah, hal ini menunjukkan bahwa aplikasi dapat membedakan antara token *scam* dan token yang bukan *scam*.

Kata kunci : *Blockchain*, *Scam*, Ethereum, Token Kripto, *Deep Neural Networks*

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT, atas rahmat serta karunia-Nya sehingga penulis akhirnya dapat menyelesaikan skripsi yang berjudul "IMPLEMENTASI *DEEP LEARNING* SEBAGAI UPAYA MENDETEKSI TINDAK PENIPUAN TOKEN KRIPTO PADA JARINGAN ETHEREUM" dengan lancar. Tujuan penulisan skripsi ini yaitu untuk memenuhi salah satu syarat mencapai gelar Sarjana di program studi Teknik Informatika Universitas Nusa Putra. Penyusunan skripsi ini tentunya tidak akan berjalan dengan baik tanpa adanya dukungan dan bimbingan dari berbagai pihak. Sehubungan dengan itu penulis menyampaikan penghargaan dan ucapan terima kasih yang sebesar-besarnya kepada :

1. Rektor Universitas Nusa Putra Sukabumi Bapak Dr. Kurniawan, ST., M. Si., MM dan seterusnya.
2. Wakil Rektor I Bidang Akademik Universitas Nusa Putra Sukabumi Bapak Anggi Pradifta Junfithrana, S.Pd., M.T dan seterusnya.
3. Kepala Program Studi Teknik Informatika Universitas Nusa Putra Sukabumi Ibu Anggun Fergina, M.Kom.
4. Dosen Pembimbing I Universitas Nusa Putra Sukabumi Ibu Ivana Lucia Kharisma, M.Kom yang telah menyediakan waktu, tenaga dan pikiran untuk membimbing dan mengarahkan penulis dalam menyusun skripsi ini.
5. Dosen Pembimbing II Universitas Nusa Putra Sukabumi Ibu Dwi Sartika Simatupang, ST. MTI yang telah membimbing penulis dengan memberikan yang terbaik demi kelancaran penulis dalam menyusun skripsi ini.
6. Dosen Penguji Bapak Somantri, S.T, M.Kom atas masukan, koreksi dan bimbingan yang diberikan.
7. Para Dosen Program Studi Teknik Informatika Universitas Nusa Putra Sukabumi yang senantiasa telah memberikan banyak ilmu pengetahuan yang sangat bermanfaat bagi penulis.
8. Orang tua dan keluarga yang telah mendidik dan merawat penulis selama ini dan tidak dapat terbalaskan oleh apa pun dan senantiasa memberikan dukungan, semangat, material dan moral sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan lancar.

9. Rekan-rekan mahasiswa Universitas Nusa Putra terutama TI19C yang telah menemani dan berjuang bersama demi tercapainya cita-cita dan tujuan kita.
10. Nira Aktaviana yang telah berjuang bersama. Selalu memberikan semangat serta mendoakan, dan berusaha memberikan yang terbaik dalam segala hal.

Penulis menyadari bahwa skripsi ini masih jauh dari kesempurnaan, oleh karena itu kritik dan saran yang membangun dari berbagai pihak sangat penulis harapkan demi kebaikan penulis. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu. Aamiin Ya Rabbal 'Alamin.

DAFTAR ISI

Halaman

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan dalam bidang teknologi dan komunikasi memberikan banyak dampak positif bagi manusia, namun juga tidak terlepas dari dampak negatif termasuk kasus penipuan. Banyak modus yang dilakukan oleh penipu untuk melancarkan aksinya tersebut. Menurut istilah yang secara umum, penipuan sendiri yaitu suatu tindakan yang sengaja dilakukan dengan tujuan untuk memperoleh keuntungan finansial dengan cara membohongi orang lain, yang dilakukan secara pribadi atau oleh beberapa pihak. Penipuan dalam transaksi *cryptocurrency* menjadi sebuah masalah serius yang perlu ditangani.

Dalam beberapa tahun terakhir penggunaan *blockchain* sendiri telah meningkat, banyak orang melakukan investasi terhadap Bitcoin karena dipercaya sebagai aset yang aman karena harganya terus melonjak. Bitcoin sendiri merupakan salah satu jenis *cryptocurrency* (mata uang digital) yang paling dikenal, namun terlepas dari *cryptocurrency* yang dikenal aman tersebut, tidak sedikit developer dalam sistem *blockchain* yang melakukan tindak kejahatan berupa penipuan untuk meraup keuntungan. Menurut laporan Lembaga Perlindungan Konsumen AS (FTC), pada periode Januari 2021 sampai Maret 2022 lebih dari 46.000 orang melaporkan kehilangan lebih dari $1 miliar dalam bentuk mata uang kripto akibat penipuan.[1] Selain Bitcoin, ada banyak *cryptocurrency* yang dibangun dengan protokolnya masing-masing, salah satunya adalah Ethereum yang dijadikan objek dalam penelitian ini.

Ethereum memiliki kapitalisasi pasar kedua setelah Bitcoin dengan teknologi sistem *blockchain* yang diciptakan oleh *programmer* bernama Vitalik Buterin pada tahun 2014 dan mempunyai mata uang sendiri yaitu Ether (ETH). Ethereum memungkinkan siapa saja untuk membuat *smart contract* yang dapat berinteraksi dengan penggunanya. *Smart contract* merupakan sebuah program otomatis yang ada di dalam sistem *blockchain.*[2]

Pada penelitian ini, penulis melakukan analisis, perancangan, pembuatan dan penelitian terkait deteksi penipuan *cryptocurrency* pada jaringan Ethereum dengan

menerapkan implementasi *deep learning* yang algoritmanya terinspirasi dari otak manusia (biasa disebut *neural networks*). Metode *Deep Neural Networks* digunakan karena beberapa penelitian telah berhasil dalam melakukan klasifikasi dan memberikan hasil yang baik.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah pada penelitian ini di antaranya :

1. Bagaimana membangun suatu sistem yang dapat mendeteksi tindak penipuan token kripto?
2. Bagaimana metode *deep learning* dapat mendeteksi tindak penipuan token kripto?
3. Bagaimana memastikan bahwa sistem yang dibangun memiliki mekanisme yang cukup baik untuk mencegah penipuan token kripto?

1.3 Batasan Masalah

Beberapa batasan masalah dalam penelitian ini adalah sebagai berikut :

1. Fokus penelitian ini ada pada proses *swapping* token (menukar satu token kripto dengan token lainnya) dengan tipe token ERC-20.
2. Algoritma *deep learning* yang digunakan yaitu DNN (*Deep Neural Networks*).
3. Aplikasi yang dirancang menggunakan bahasa pemrograman golang, solidity, dan web3.js.
4. Aplikasi ini di *deploy* pada server VPS (*Virtual Private Server*) hanya untuk penelitian, dikarenakan keterbatasan biaya pada sewa server.

1.4 Tujuan Penelitian

Adapun beberapa tujuan penelitian, sebagai berikut :

1. Membangun suatu sistem deteksi token kripto untuk mengatasi penipuan dalam melakukan pembelian / penjualan pada jaringan Ethereum.
2. Menerapkan metode *deep learning* pada sistem *blockchain* Ethereum untuk dapat mencegah aksi penipuan *cryptocurrency*

3. Memastikan bahwa sistem yang dirancang memiliki mekanisme yang andal untuk mencegah aksi penipuan.

1.5 Manfaat Penelitian

Berdasarkan rumusan masalah dan tujuan penelitian, maka dihasilkan beberapa manfaat penelitian, sebagai berikut:

1. Meningkatkan keamanan pengguna individu saat melakukan transaksi *cryptocurrency*.
2. Meningkatkan performa dan efisiensi dalam implementasi *deep learning* untuk mendeteksi penipuan *cryptocurrency*.
3. Menciptakan aplikasi yang efektif untuk mendeteksi penipuan *cryptocurrency* dalam jaringan *blockchain* Ethereum.

1.6 Sistematika Penulisan

Sistematika pembahasan dalam penelitian ini terdiri atas 5 bab, yaitu:

BAB I PENDAHULUAN

Berisi alasan memilih judul penelitian berupa latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika pembahasan.

BAB II TINJAUAN PUSTAKA

Berisi teori sebagai dasar untuk menganalisis pokok-pokok masalah dalam penelitian berupa telaah teori, hasil penelitian terdahulu, perumusan hipotesis, dan model penelitian.

BAB III METODOLOGI PENELITIAN

Pada bagian bab ini nantinya dijelaskan bagaimana penulis akan menjawab dari rumusan masalah pada Bab I

BAB IV HASIL DAN PEMBAHASAN

Pada bagian bab ini nantinya dijelaskan mengenai hasil dari perancangan sistem yang telah diimplementasikan, data yang diperoleh dari sistem ini akan dianalisis dan dilakukan perbandingan dengan alat ukur manual.

BAB V KESIMPULAN

Bab ini merupakan bagian akhir dari penyusunan skripsi yang berisi kesimpulan, keterbatasan penelitian dan saran

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian "IMPLEMENTASI *DEEP LEARNING* SEBAGAI UPAYA MENDETEKSI TINDAK PENIPUAN TOKEN KRIPTO PADA JARINGAN ETHEREUM" kesimpulan yang dapat diambil adalah sebagai berikut:

1. Implementasi *deep learning* dalam mendeteksi tindak penipuan token kripto pada jaringan Ethereum mendapatkan hasil yang sangat baik. Hasil evaluasi performa menunjukkan bahwa model yang dibuat mampu dengan sangat baik dalam mendeteksi penipuan dengan tingkat akurasi yang sangat tinggi, yaitu di atas 99%.
2. *Deep learning* dengan metode *deep neural network* berhasil diterapkan pada sistem *blockchain* dalam upaya mencegah aksi penipuan *cryptocurrency*. Pendekatan ini menunjukkan potensi untuk meningkatkan keamanan dalam ekosistem kripto.
3. Dalam penelitian ini, mekanisme yang dirancang telah diuji dan dievaluasi. Penelitian ini memiliki fokus pada memastikan bahwa sistem yang dikembangkan memiliki mekanisme yang andal untuk mencegah aksi penipuan. Evaluasi performa dilakukan menggunakan tiga skenario pengujian dengan pembagian *dataset* menjadi tiga rasio data latih dan data uji. Rasio yang digunakan adalah 90%:10%, 80%:20%, dan 70%:30%. *Callback* EarlyStopping digunakan dalam proses pelatihan model untuk mencegah *overfitting*. *Callback* ini menghentikan proses pelatihan jika terjadi penurunan yang signifikan dengan data *loss* pada data validasi. Hal ini membantu dalam memperoleh model terbaik. Performa model yang dihasilkan dari penelitian ini dapat dievaluasi berdasarkan metrik yang relevan, seperti *accuracy*, *precision*, *recall*, dan *F1-score*. Penelitian ini tidak memberikan informasi rinci mengenai performa model yang diperoleh.

5.2 Saran

1. Mengoptimalkan performa model: Penelitian dapat menggali lebih lanjut tentang berbagai arsitektur dan algoritma *deep learning* yang paling efektif

untuk mendeteksi penipuan pada jaringan *blockchain* Ethereum. Upaya untuk meningkatkan performa model dapat dilakukan dengan melakukan penyesuaian pada struktur model, fungsi aktivasi, atau parameter pelatihan.

2. Pengujian lebih lanjut dengan *dataset* yang lebih besar: Penelitian dapat memperluas pengujian dengan menggunakan *dataset* yang lebih besar dan lebih beragam untuk memastikan keandalan sistem dalam mendeteksi penipuan. Hal ini akan membantu dalam menguji generalisasi model terhadap berbagai skenario dan pola penipuan.
3. Integrasi dengan sistem keamanan lainnya: Sistem deteksi penipuan yang dikembangkan dalam penelitian ini dapat diintegrasikan dengan sistem keamanan lainnya dalam ekosistem kripto, seperti analisis risiko, verifikasi identitas, atau sistem reputasi. Hal ini akan membantu dalam menciptakan lapisan keamanan yang lebih kuat dan menyeluruh dalam mencegah penipuan.

DAFTAR PUSTAKA

[1] Emma Fletcher, "Reports show scammers cashing in on crypto craze," *www.ftc.gov*, 3 Juli 2022. www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze (diakses 28 Februari 2023).

[2] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, hlm. 1–32, 2014.

[3] M. F. Rochmatullah, "SMART CONTRACT DENGAN ETHEREUM SEBAGAI DASAR LELANG (STUDI KASUS DI AMERIKA SERIKAT)," Politeknik Keuangan Negara STAN, 2022.

[4] M. R. Behera, S. Upadhyay, dan S. Shetty, "Federated Learning using Smart Contracts on Blockchains, based on Reward Driven Approach," Jul 2021, [Daring]. Tersedia pada: http://arxiv.org/abs/2107.10243

[5] A. K. Shrestha, J. Vassileva, dan R. Deters, "A Blockchain Platform for User Data Sharing Ensuring User Control and Incentives," *Frontiers in Blockchain*, vol. 3, Okt 2020, doi: 10.3389/fbloc.2020.497985.

[6] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, dan J. Wan, "Smart Contract-Based Access Control for the Internet of Things," Feb 2018, [Daring]. Tersedia pada: http://arxiv.org/abs/1802.04410

[7] Y. Hu, M. Liyanage, A. Mansoor, K. Thilakarathna, G. Jourjon, dan A. Seneviratne, "Blockchain-based Smart Contracts - Applications and Challenges," Sep 2018, [Daring]. Tersedia pada: http://arxiv.org/abs/1810.04699

[8] J. Feist, G. Grieco, dan A. Groce, "Slither: A Static Analysis Framework For Smart Contracts," Agu 2019, doi: 10.1109/WETSEB.2019.00008.

[9] F. Vogelsteller dan V. Buterin, "Token Standard ERC-20," 15 November 2015. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md (diakses 14 Juni 2023).

[10] D. A. Badawi, "Sistem Verifikasi Dokumen Hasil Investigasi Forensik Digital Berbasis Teknologi Blockchain." Universitas Islam Indonesia, 2019.

[11] F. Chollet, *Deep Learning with Python* . Manning, 2017.

[12] R. M. Cichy dan D. Kaiser, "Deep Neural Networks as Scientific Models," *Trends in Cognitive Sciences*, vol. 23, no. 4. Elsevier Ltd, hlm. 305–317, 1 April 2019. doi: 10.1016/j.tics.2019.01.009.

[13] K. J. Bergen, P. A. Johnson, M. V. de Hoop, dan G. C. Beroza, "Machine learning for data-driven discovery in solid Earth geoscience," *Science (1979)*, vol. 363, no. 6433, Mar 2019, doi: 10.1126/science.aau0323.

[14] A. Mattew dan M. Anno Suwarno, "Rancang Bangun Aplikasi Donasi Terdesentralisasi Berbasis Blockchain," *ikraith-informatika*, vol. 7, no. 2, Nov 2022, doi: 10.37817/ikraith-informatika.v7i2.2247.

[15] "Run a node | ethereum.org." https://ethereum.org/en/run-a-node/ (diakses 16 Juni 2023).

[16] D. Guo, J. Dong, dan K. Wang, "Graph structure and statistical properties of Ethereum transaction relationships," *Inf Sci (N Y)*, vol. 492, hlm. 58–71, Agu 2019, doi: 10.1016/j.ins.2019.04.013.

[17] Yugesh Verma, "A Complete Guide to Categorical Data Encoding." https://analyticsindiamag.com/a-complete-guide-to-categorical-data-encoding/ (diakses 10 Juni 2023).

[18] I. Weber, Q. Lu, A. B. Tran, A. Deshmukh, M. Gorski, dan M. Strazds, "A Platform Architecture for Multi-Tenant Blockchain-Based Systems," dalam *2019 IEEE International Conference on Software Architecture (ICSA)*, IEEE, Mar 2019, hlm. 101–110. doi: 10.1109/ICSA.2019.00019.

[19] M. Bispham, S. Creese, W. H. Dutton, P. Esteve-Gonzalez, dan M. Goldsmith, "Cybersecurity in Working from Home: An Exploratory Study," *SSRN Electronic Journal*, Agu 2021, doi: 10.2139/ssrn.3897380.