

**DETEKSI ANOMALI TRANSAKSI BITCOIN
MENGUNAKAN METODE KMEANS DAN
KMEDOIDS**

Skripsi

**Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer**



OLEH :

RAHMAT JUNIANSYAH

09011382025150

**JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA**

2025

LEMBAR PENGESAHAN

DETEKSI ANOMALI TRANSAKSI BITCOIN MENGUNAKAN METODE KMEANS DAN KMEDOIDS

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Program Studi Sistem Komputer
Jenjang S1

Oleh

RAHMAT JUNIANSYAH
09011382025150

Palembang, Desember 2024
Pembimbing II

Pembimbing I

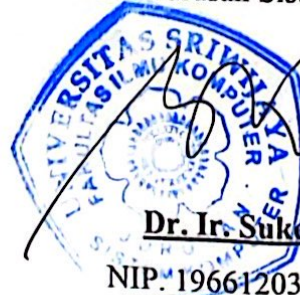


Prof. Ir. Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002



Nurul Afifah, M.Kom.
NIP. 199211102023212049

Mengetahui, 2/1/25
Ketua Jurusan Sistem Komputer



Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

AUTHENTICATION PAGE

**ANOMALY DETECTION IN BITCOIN TRANSACTIONS
USING KMEANS AND KMEDOIDS METHODS**

SKRIPSI

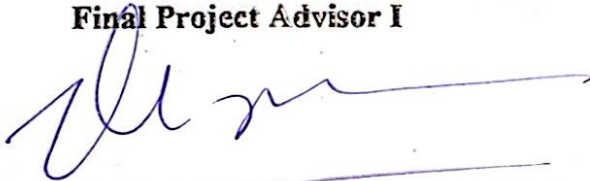
**Submitted To Complete One Of The Requirements For Obtaining A
Bachelor's Degree in Computer Science**

By:

RAHMAT JUNIANSYAH

Palembang, 20 January 2025

Final Project Advisor I



Prof. Ir. Deris Stiawan, M.T., Ph.D
NIP. 197806172006041002

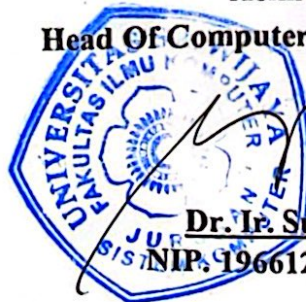
Final Project Advisor II



Nurul Afifah, M.Kom
NIP. 199211102023212049

Acknowledge. 20/1/25

Head Of Computer Science Departement



Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

LEMBAR PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Senin

Tanggal : 30 Desember 2024


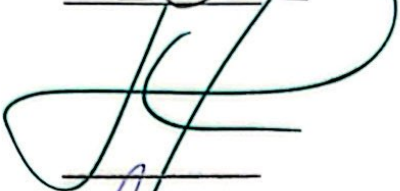
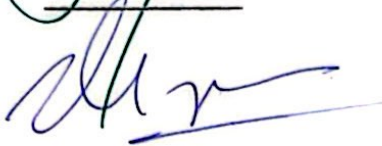

Tim Penguji :

1. Ketua : Ahmad Heryanto, S.Kom., M.T.


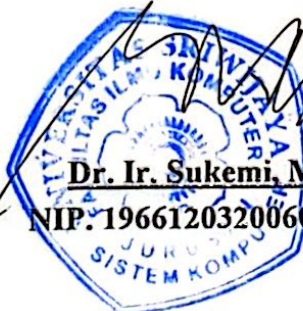
2. Penguji : Huda Ubaya, M.T.

3. Pembimbing I : Prof. Ir. Deris Stiawan, M.T., Ph.D.

4. Pembimbing II : Nurul Afifah, M.Kom

A. 




Mengetahui, *20/12/24*
Ketua Jurusan Sistem Komputer



Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Rahmat Juniansyah

NIM : 09011382025150

Judul : Deteksi Anomali Transaksi Bitcoin Menggunakan Metode Kmeans dan Kmedoids

Hasil Pengecekan Software *iThenticate* Turnitin : 3%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil pengjiplakan atau plagiat. Apabila ditemukan unsur pengjiplakan atau plagiat dalam laporan tugas akhir ini, maka saya menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.



Palembang, 20 Januari 2025

Yang Menyatakan



Rahmat Juniansyah
NIM. 09011382025150

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh,

Puji dan syukur penulis ucapkan atas kehadiran Allah SWT. Yang telah melimpahkan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan penyusunan tugas akhir dengan judul **“Deteksi Anomali Transaksi Bitcoin Menggunakan Metode KMeans dan KMedoids”**

Pada penyusunan tugas akhir ini tidak terlepas dari peran berbagai pihak yang telah memberikan dukungan doa, semangat, motivasi dan bimbingan pada penulis. Oleh karena itu, pada kesempatan ini penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Allah SWT. yang telah memberikan nikmat Kesehatan dan Kesempatan kepada penulis dalam penyusunan tugas akhir ini.
2. Kedua orang tua yang telah banyak memberikan do'a dan dukungan serta semangat.
3. Kakak-kakak dan Adik-adik yang selalu memberikan dukungan dan do'a.
4. Bapak Prof. Dr. Erwin, S.Si., M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
6. Bapak Prof. Deris Stiawan, M.T., Ph.D., IPU., ASEAN-Eng., CPENT selaku Dosen Pembimbing pertama Tugas Akhir Penulis yang telah meluangkan waktu untuk membimbing dan memberikan motivasi selama pengerjaan Tugas Akhir.
7. Ibu Nurul Afifah, M.Kom. selaku Dosen Pembimbing kedua Tugas Akhir yang telah meluangkan waktunya serta senantiasa memberikan kritik dan saran yang membangun sehingga penulisan Tugas Akhir ini dapat berjalan dengan lancar.
8. Bapak SUTARNO, S.T.,M,T. selaku Dosen Pembimbing Akademik.
9. Mba Sari Anhar selaku admin yang telah membantu dalam proses administrasi Tugas Akhir Penulis.
10. Teman-teman terdekat yang selalu memberikan dukungan dan semangat.
11. Teman-teman seperjuangan Jurusan Sistem Komputer Unggulan 2020.

12. Seluruh pihak yang tidak dapat penulis sebutkan satu per satu, yang telah memberikan semangat serta doa.
13. Almamater

Penulis menyadari bahwa laporan ini masih jauh dari kesempurnaan, oleh karena itu penulis dengan senang hati menerima kritik dan saran serta masukkan dari pembaca agar lebih baik lagi dikemudian hari. Penulis berharap semoga laporan ini dapat bermanfaat bagi kita semua khususnya bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya. Semoga ini bisa menjadi bagian dari kontribusi dalam meningkatkan kualitas pembelajaran dan penelitian. Demikian yang dapat penulis sampaikan.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Palembang, Januari 2025

Penulis,

Rahmat Juniansyah

NIM. 09011382025150

DETEKSI ANOMALI TRANSAKSI BITCOIN MENGUNAKAN METODE KMEANS DAN KMEDOIDS

Rahmat Juniansyah (09011382025150)

Jurusan sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email: rahmatjuniansyah1906@gmail.com

ABSTRAK

Bitcoin merupakan salah satu mata uang digital yang populer dan sering digunakan dalam transaksi online. Namun, transaksi Bitcoin tidak terlepas dari kemungkinan terjadinya anomali, yang dapat menjadi indikasi aktivitas mencurigakan seperti penipuan atau tindakan ilegal lainnya. Deteksi anomali ini menjadi langkah penting untuk meningkatkan keamanan dan keandalan jaringan Bitcoin. Penelitian ini bertujuan untuk mengidentifikasi anomali pada transaksi Bitcoin dengan menggunakan metode *clustering KMeans* dan *KMedoids*. Dataset yang digunakan mencakup transaksi harian Bitcoin dari tahun 2009 hingga 2024, yang diperoleh dari *BigQuery*. Proses *preprocessing* dilakukan, termasuk normalisasi menggunakan *Standard Scaler*, sebelum algoritma *clustering* diterapkan. Hasil penelitian menunjukkan bahwa metode *KMeans* menghasilkan *silhouette score* sebesar 0,96, sedangkan metode *KMedoids* mencapai nilai sebesar 0,98. Analisis lebih lanjut mengungkapkan bahwa *KMedoids* lebih andal dalam menangani data dengan outlier dibandingkan *KMeans*, meskipun membutuhkan waktu komputasi yang lebih lama.

Kata Kunci: *KMeans, KMedoids, Bitcoin, Anomali, Clustering*

ANOMALY DETECTION IN BITCOIN TRANSACTIONS USING KMEANS AND KMEDOIDS METHODS

Rahmat Juniansyah (09011382025150)

*Department of Computer Systems, Faculty of Computer Science, Sriwijaya
University*

Email: rahmatjuniansyah1906@gmail.com

ABSTRACT

Bitcoin is one of the most popular digital currencies widely used in online transactions. However, Bitcoin transactions are prone to anomalies, which may indicate suspicious activities such as fraud or other illegal actions. Detecting these anomalies is essential to enhance the security and reliability of the Bitcoin network. This study aims to identify anomalies in Bitcoin transactions using the KMeans and KMedoids clustering methods. The dataset consists of daily Bitcoin transactions from 2009 to 2024, sourced from BigQuery. The data preprocessing includes normalization using the Standard Scaler before applying the clustering algorithms. The results show that the KMeans method achieved a silhouette score of 0.96, while the KMedoids method scored 0.98. Further analysis revealed that KMedoids is more reliable in handling data with outliers compared to KMeans, despite requiring longer computation times.

Keywords: *KMeans, KMedoids, Bitcoin, Anomaly, Clustering*

DAFTAR ISI

LEMBAR PENGESAHAN.....	ii
KATA PENGANTAR.....	vi
DAFTAR ISI.....	x
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xiv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	4
1.3 Tujuan	4
1.4 Manfaat	4
1.5 Batasan Masalah	5
1.6 Metodologi Penelitian	5
1.7 Sistematika Penulisan	6
BAB II TINJAUAN PUSTAKA.....	7
2.1 Penelitian Terkait.....	7
2.2 Bitcoin.....	10
2.2.1 Konsensus Bitcoin	11
2.2.2 Bitcoin Mining.....	12
2.2.3 Transaksi Bitcoin	14
2.2.4 Supply dan Halving Bitcoin.....	15
2.3 Teknologi Dibalik Bitcoin	18
2.3.1 Jenis-jenis Blockchain	18
2.3.2 Keamanan dalam Teknologi Blockchain	20
2.4 Dataset	26
2.5 Metode	27
2.5.1 Metode KMeans.....	27

2.5.2 Metode KMedoids	28
2.6 Anomaly Score	28
2.7 Evaluasi Kinerja Model	30
BAB III METODOLOGI PENELITIAN	32
3.1 Kerangka Kerja Penelitian	32
3.2 Spesifikasi Perangkat Keras dan Perangkat Lunak.....	33
3.2.1 Perangkat Keras	34
3.2.2 Perangkat Lunak	34
3.3 Dataset	34
3.4 Pre-Processing.....	37
3.4.1 Pembuatan Fitur Label.....	37
3.4.2 Cleaning Data.....	39
3.4.3 Normalisasi Data.....	39
3.5 Model Machine Learning.....	40
3.5.1 KMeans.....	40
3.5.2 KMedoids.....	43
BAB IV HASIL DAN PEMBAHASAN	46
4.1 Pendahuluan	46
4.2 Pre-processing Data	46
4.2.1 Pembuatan Fitur “Label”	46
4.2.2 Type Casting	49
4.2.3 Data Cleaning	50
4.2.4 Exploratory Data Analysis (EDA).....	51
4.2.5 Normalisasi	54
4.3 Implementasi Model Kmeans	55
4.3.1 Menentukan Cluster Optimal.....	55

4.3.2 Hasil Clustering	57
4.3.3 Hasil dan Evaluasi	60
4.4 Implementasi Model Kmedoids	67
4.4.1 Menentukan Cluster Optimal	67
4.4.2 Hasil Clustering	69
4.4.3 Hasil dan Evaluasi	72
BAB V KESIMPULAN DAN SARAN	81
5.1 Kesimpulan	81
5.2 Saran	82
DAFTAR PUSTAKA	83

DAFTAR TABEL

Tabel 2. 1 Penelitian Terkait.....	7
Tabel 2. 2 Bitcoin Halving.....	16
Tabel 3. 1 Spesifikasi Perangkat Keras	34
Tabel 3. 2 Spesifikasi Perangkat Lunak	34
Tabel 3. 3 Rincian Fitur Dataset	35
Tabel 4. 1 Distribusi hasil pelabelan.....	49
Tabel 4. 2 Nilai Variansi Setiap Fitur	53
Tabel 4. 3 Hasil Perhitungan Nilai Inertia	56
Tabel 4. 4 Tabel Cluster Centroid (KMeans)	58
Tabel 4. 5 Beberapa Indeks data anomali Kmeans	62
Tabel 4. 6 Statistik jarak K-Means	63
Tabel 4. 7 Silhouette Score KMeans	64
Tabel 4. 8 Hasil Perhitungan Nilai Cost	68
Tabel 4. 9 Tabel pusat cluster (medoids).....	70
Tabel 4. 10 Beberapa Indeks data anomali Kmedoids.....	75
Tabel 4. 11 Statistik jarak K-Medoids	76
Tabel 4. 12 Silhouette Score KMedoids	77
Tabel 4. 13 Perbandingan silhoutte score	80

DAFTAR GAMBAR

Gambar 2. 1 Bitcoin [1]	11
Gambar 2. 2 Proof-of-Work [15].....	12
Gambar 2. 3 Solo Mining [19].....	13
Gambar 2. 4 Pool Mining [20].....	14
Gambar 2. 5 Transaksi Bitcoin [2].....	15
Gambar 2. 6 Jenis-jenis blockchain [24].....	19
Gambar 3. 1 Kerangka Kerja Penelitian	32
Gambar 3. 2 Flowchart Pre-Processing	37
Gambar 3. 3 Flowchart Pembuatan Fitur Label.....	38
Gambar 3. 4 Flowchart Model KMeans	42
Gambar 3. 5 Flowchart Model KMedoids	45
Gambar 4. 1 Grafik transaksi bitcoin pertahun	46
Gambar 4. 2 Dataset Sebelum Pelabelan	48
Gambar 4. 3 Grafik Hasil Pembuatan Label.....	48
Gambar 4. 4 Sebelum Type Casting	49
Gambar 4. 5 Setelah Type Casting	50
Gambar 4. 6 Data Cleaning.....	51
Gambar 4. 7 Deskriptif Data.....	51
Gambar 4. 8 Grafik Exploratory Data Analysis.....	52
Gambar 4. 9 Data Sebelum Normalisasi	54
Gambar 4. 10 Data Setelah Normalisasi	54
Gambar 4. 11 Grafik Elbow Kmeans.....	55
Gambar 4. 12 Hasil Clustering Kmeans	57
Gambar 4. 13 Hasil Clustering Kmeans 3D	59
Gambar 4. 14 Visualisasi Hasil Deteksi Kmeans	60
Gambar 4. 15 Plot silhouette.....	65
Gambar 4. 16 Silhoutte Score Elbow KMeans	66
Gambar 4. 17 Plot silhouette.....	67
Gambar 4. 18 Hasil Clustering Kmedoids	69
Gambar 4. 19 Hasil Clustering Kmedoids 3D	71
Gambar 4. 20 Visualisasi Hasil Deteksi Kmedoids	72

Gambar 4. 21 Plot silhouette.....	78
Gambar 4. 22 Silhouette Score Elbow KMedoids	79

BAB I

PENDAHULUAN

1.1 Latar Belakang

Bitcoin pertama kali ditemukan oleh Satoshi Nakamoto pada tahun 2008 yang memperkenalkan konsep transaksi mata uang digital yang beroperasi dalam system peer to peer tanpa memerlukan otoritas Pusat [1]. Bitcoin dirancang sebagai mata uang tanpa otoritas pusat, yang berarti tidak ada satu entitas pun yang mengontrol jaringan secara keseluruhan. Hal ini memberikan keamanan terhadap serangan dan upaya manipulasi, karena itu transaksi bitcoin dikumpulkan dalam blok, dan setiap blok dihubungkan dengan blok sebelumnya yang akan membentuk rantai blok atau yang disebut blockchain [2]. Bitcoin beroperasi dengan teknologi blockchain, yang memastikan bahwa semua transaksi yang dilakukan dicatat dalam buku besar publik yang transparan, aman, dan tidak dapat diubah.

Blockchain menarik banyak perhatian dalam beberapa tahun terakhir dan digunakan secara luas hampir disemua industri, termasuk sektor layanan kesehatan, cryptocurrency, kecerdasan buatan, sektor pemerintahan dan lain-lain [3]. Sebelum kemunculan blockchain sistem transaksi digital sering kali memerlukan pihak ketiga sebagai otoritas pusat untuk verifikasi dan penyelesaian transaksi. Hal ini dapat menimbulkan berbagai masalah termasuk biaya transaksi yang tinggi, resiko penipuan dan potensi manipulasi data. Blockchain muncul sebagai solusi untuk mengatasi tantangan ini dengan menyediakan mekanisme verifikasi yang terdistribusi dan otomatis. Struktur data blockchain menyimpan informasi dalam bentuk blok-blok yang terhubung secara berurutan, setiap blok berisi serangkaian transaksi dan merujuk pada blok sebelumnya melalui kode hash, membentuk rantai yang tidak dapat diubah.

Perkembangan pesat cryptocurrency khususnya pada bitcoin dimana tidak adanya peraturan di pasar bitcoin, terdapat kemungkinan terjadinya perilaku ilegal dalam transaksi. Situasi ini memunculkan pertanyaan mengenai apakah aktivitas ilegal dapat terjadi dalam transaksi bitcoin yang berlangsung dalam sistem blockchain [4]. Dalam transaksi Bitcoin, terdapat aturan tertentu untuk menentukan

validitas suatu transaksi, dimana transaksi dianggap tidak valid jika nilai outputnya melebihi total inputnya. Total input mencakup biaya transaksi. Transaksi yang tidak valid inilah yang akan menjadi target untuk mendeteksi anomali dalam transaksi bitcoin.

Penelitian sebelumnya telah berhasil mengeksplorasi fenomena perilaku ilegal yang terjadi di platform-platform bitcoin. Penelitian yang dilakukan oleh Iwan syarif, Adam Prugel-Bennett dan Gary Wills membahas keunggulan masing-masing algoritma seperti Kmeans, Kmeans yang ditingkatkan, Kmedoids, EM Clustering dan deteksi outlier berbasis jarak dalam mendeteksi anomali, dimana berdasarkan penelitian tersebut dari masing masing algoritma deteksi outlier berbasis jarak yang lebih unggul dengan akurasi sebesar 80% dengan tingkat positif false diatas 20% [5]. Pada penelitian Alexandru-Tudor membahas tentang deteksi anomali jaringan blockchain dengan menganalisis data transaksi bitcoin pada tahun 2011 hasil anomali terdeteksi dengan algoritma Local outlier Factor sebesar 68,234 dan algoritma Isolation Forest mendeteksi anomali sebanyak 68,141 [6]. Pada penelitian yang dilakukan oleh Priyanshi Singh dan teman-teman berhasil mendeteksi pola anomali transaksi bitcoin dengan membandingkan beberapa algoritma untuk menentukan algoritma mana yang paling efektif dalam mendeteksi anomali, penelitian ini menggunakan tiga algoritma utama untuk mendeteksi anomali yaitu Kmeans untuk mengelompokkan data berdasarkan kesamaan, Isolation Forest yang dirancang untuk menangani ketidakseimbangan kelas yang signifikan dan Support Vektor Machine(SVM) untuk memisahkan kelas data, hasil dari penelitian ini menunjukkan perbandingan kinerja dari ketiga algoritma yang diuji Dimana algoritma Support Vektor Machine menunjukkan akurasi tertinggi (98.2%) serta recall yang baik(91%) lalu algoritma Isolation Forest menunjukkan akurasi (96.82%) dengan recall yang lebih rendah (61.3%) dan Kmeans memiliki akurasi terendah (75%) dan menunjukkan hasil yang kurang memuaskan dalam hal presisi dan F1 Score [7]. Pada penelitian yang dilakukan oleh Jun Inoue dan kawan-kawan mendeteksi anomali dengan membandingkan dua metode unsupervised learning Deep Neural Network dan One Class SVM dengan hasil menunjukkan bahwa algoritma DNN berhasil mendeteksi dengan tingkat positif palsu lebih sedikit dibandingkan dengan One Class-SVM [8]. Pada penelitian yang dilakukan

oleh Omer shafiq berhasil mendeteksi anomali pada blockchain dengan menggunakan berbagai algoritma unsupervised learning seperti Isolation Forest, Histogram-based Outlier Score(HBOS), Cluster-Based Local Outlier Factor(CBLOF), Principal Component Analysis (PCA), Kmeans, Deep Autoencoders dan Ensemble Classification, dimana berdasarkan hasil dari evaluasi setiap metode didapatkan metode yang paling unggul dalam mendeteksi anomali adalah Isolation Forest dengan akurasi tertinggi yang menunjukkan stabilitas yang lebih baik dibandingkan dengan metode Unsupervised Learning yang lainnya [9]. Pada penelitian lain yang dilakukan Kingsly Leung dan Christopher Leckie yang membahas tentang deteksi anomali pada jaringan menggunakan metode unsupervised yang berbasis clustering dimana metode cluster yang ditingkatkan berhasil mendeteksi dengan nilai akurasi tertinggi dibandingkan dengan metode clustering lainnya [10]. Pada penelitian yang dilakukan oleh Thai T. Pham dan Steven Lee berhasil mendeteksi anomali pada jaringan bitcoin menggunakan tiga metode unsupervised Kmeans, Mahalanobis distance dan unsupervised SVM menunjukkan kesamaan dalam mendeteksi anomali dengan hasil deteksi yang cukup efektif [11]. Pada penelitian lain yang juga dilakukan Thai T. Pham dan Steven Lee mendeteksi anomali pada jaringan transaksi bitcoin menggunakan metode Kmeans dan Local Outlier Factor, penelitian ini menunjukkan bahwa ada anomali yang jelas terdeteksi dalam jaringan bitcoin yang menunjukkan bahwa beberapa pengguna lain terlibat dalam aktivitas ilegal pada jaringan bitcoin [12]. Pada penelitian yang dilakukan Hae-Sang Park dan rekan-rekannya membandingkan algoritma clustering Kmeans dengan Kmedoids dimana dari kedua algoritma tersebut menunjukkan algoritma Kmedoids lebih unggul dengan akurasi 92% dari pada Algoritma Kmeans dengan akurasi sebesar 88.7% [13]. Pada penelitian lain yang membahas perbandingan antara algoritma clustering kmeans dan Kmedoids dimana disimpulkan bahwa algoritma Kmedoids merupakan metode yang efektif untuk pengelompokan data, terutama dalam situasi di mana data memiliki outlier [14].

Berdasarkan beberapa ulasan di atas, penulis mengusulkan penelitian dengan judul "**Deteksi Anomali Transaksi Bitcoin Menggunakan Metode Kmeans dan**

Kmedoids”Tujuan dari penelitian ini adalah untuk menganalisis perbandingan kedua algoritma tersebut dalam mendeteksi anomali.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka rumusan masalah yang akan dibahas pada penelitian ini adalah:

1. Bagaimana proses ekstraksi data pada dataset Transaksi Bitcoin ?
2. Bagaimana algoritma KMeans dan KMedoids dapat digunakan untuk mendeteksi anomali pada transaksi Bitcoin?
3. Bagaimana cara kerja dan efektivitas masing-masing algoritma KMeans dan KMedoids dalam mendeteksi anomali pada transaksi bitcoin?

1.3 Tujuan

Berdasarkan penulisan latar belakang dan rumusan masalah yang telah ditulis sebelumnya, Tujuan yang ingin dicapai dalam penulisan Tugas Akhir ini adalah sebagai berikut:

1. Menerapkan algoritma KMeans dan KMedoids untuk mendeteksi anomali pada transaksi bitcoin serta mengevaluasi cara kerja dan efektivitas masing-masing algoritma.
2. Melakukan clustering dan mengukur jarak masing-masing titik data ke pusat cluster untuk mendeteksi anomali pada data transaksi Bitcoin.
3. Membandingkan hasil deteksi anomali yang dihasilkan oleh algoritma KMeans dan KMedoids untuk menentukan algoritma yang lebih optimal dalam mendeteksi anomali pada transaksi bitcoin.

1.4 Manfaat

Berikut beberapa manfaat dari penelitian yang akan dilakukan oleh penulis, diantaranya:

1. Mendeteksi anomali pada transaksi bitcoin untuk meningkatkan keamanan jaringan dan mengurangi potensi tindak kejahatan serta aktivitas ilegal.
2. Menerapkan algoritma Kmeans dan Kmedoids dalam mendeteksi anomali pada transaksi bitcoin, untuk mengidentifikasi metode clustering yang paling efektif.

3. Memberikan pemahaman yang lebih mendalam tentang metode clustering serta keunggulan masing-masing metode.

1.5 Batasan Masalah

Batasan Masalah pada Tugas Akhir ini adalah sebagai berikut :

1. Penelitian ini hanya berfokus pada deteksi anomali.
2. Faktor eksternal yang dapat mempengaruhi anomali pada transaksi bitcoin tidak dipertimbangkan dalam penelitian ini.
3. Menggunakan dataset *bigquery-public-data.crypto_bitcoin* yang tersedia di Google Cloud dan di kueri menggunakan SQL.
4. Penelitian ini hanya membandingkan metode clustering Kmeans dan Kmedoids dalam mendeteksi anomali.

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penulisan Tugas Akhir ini akan melalui beberapa tahapan, yaitu:

1. Tahap Pertama (Studi Pustaka/Studi Literatur)
Tahap ini dilakukan setelah masalah yang didapatkan telah sesuai untuk dijadikan sebagai penelitian, membaca artikel, jurnal atau makalah yang berhubungan dengan tugas akhir
2. Tahap Kedua (Perancangan Sistem)
Pada tahap ini bagaimana membangun dan menerapkan metode untuk tugas akhir, apa saja yang digunakan dalam penelitian, seperti software yang digunakan dan bagaimana proses penerapan metode pada tugas akhir
3. Tahap Ketiga (Testing)
Tahap ini merupakan tahap testing berdasarkan metodologi penelitian sebelumnya sehingga didapatkan hasil uji yang sesuai dengan algoritma
4. Tahap Keempat (Analisa)
tahap ini yaitu menganalisa data hasil pengujian dengan diterapkan pendekatan tertentu, sehingga mendapatkan hasil yang objektif
5. Tahap Kelima (Kesimpulan dan Saran)

Tahapan ini adalah tahap terakhir, yaitu membuat kesimpulan dari permasalahan, studi Pustaka, metodologi penelitian serta hasil dari Analisa testing, dan beberapa saran untuk dijadikan penelitian selanjutnya

1.7 Sistematika Penulisan

Adapun sistematika penulisan dari Tugas akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab pertama akan membahas landasan topik penelitian yang meliputi Latar Belakang, Rumusan Masalah, Tujuan dan Manfaat, selain itu termasuk juga Metodologi Penelitian dan Sistematika Penulisan

BAB II TINJAUAN PUSTAKA

Bab kedua berisi mengenai dasar teori dari kerangka teori, kerangka pikir penelitian, dimana pada bab ini akan membahas tentang Blockchain, Bitcoin. Isolation Forest dan hal-hal yang berhubungan dengan penelitian.

BAB III METODOLOGI PENELITIAN

Bab ketiga membahas secara sistematis mengenai proses tahapan apa saja yang dilakukan dalam penelitian, mencari pola deteksi dan menganalisa data untuk dilakukan deteksi.

BAB IV HASIL DAN ANALISIS

Bab ini menjelaskan hasil dari deteksi anomali dan evaluasi dari setiap percobaan yang dilakukan penulis.

BAB V KESIMPULAN DAN SARAN

Bab kelima berisi kesimpulan dan saran dari hasil dan analisa dari penelitian yang telah dilakukan.

DAFTAR PUSTAKA

- [1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008, [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [2] N. Atzei, M. Bartoletti, S. Lande, and R. Zunino, "A Formal Model of Bitcoin Transactions," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10957 LNCS, pp. 541–560, 2018, doi: 10.1007/978-3-662-58387-6_29.
- [3] A. Hafid, A. S. Hafid, and M. Samih, "Scaling Blockchains: A Comprehensive Survey," *IEEE Access*, vol. 8, pp. 125244–125262, 2020, doi: 10.1109/ACCESS.2020.3007251.
- [4] Y. Y. Hsieh, J. P. Vergne, P. Anderson, K. Lakhani, and M. Reitzig, "Bitcoin and the rise of decentralized autonomous organizations," *Journal of Organization Design*, vol. 7, no. 1, pp. 1–16, 2018, doi: 10.1186/s41469-018-0038-1.
- [5] I. Syarif, A. Prugel-Bennett, and G. Wills, "Unsupervised Clustering Approach for Network Anomaly Detection," 2012.
- [6] A.-T. Nechiti, "Anomaly Detection in Blockchain Networks," *Twente Student Conference on IT 39*, vol. 1, no. 1, pp. 1–10, 2023.
- [7] P. Singh, D. Agrawal, and S. Pandey, "Anomaly detection and analysis in blockchain systems," *Res Sq*, pp. 1–21, 2023, [Online]. Available: <https://doi.org/10.21203/rs.3.rs-2414745/v1>
- [8] J. Inoue, Y. Yamagata, Y. Chen, C. M. Poskitt, and J. Sun, "Anomaly detection for a water treatment system using unsupervised machine learning," *IEEE International Conference on Data Mining Workshops, ICDMW*, vol. 2017-Novem, pp. 1058–1065, 2017, doi: 10.1109/ICDMW.2017.149.
- [9] Omer Shafiq, "Anomaly Detection In Blockchain".
- [10] K. Leung and C. Leckie, "Unsupervised Anomaly Detection in Network Intrusion Detection Using Clusters."

- [11] T. Pham and S. Lee, “Anomaly Detection in Bitcoin Network Using Unsupervised Learning Methods,” 2016, [Online]. Available: <http://arxiv.org/abs/1611.03941>
- [12] T. Pham and S. Lee, “Anomaly Detection in the Bitcoin System - A Network Perspective,” 2016, [Online]. Available: <http://arxiv.org/abs/1611.03942>
- [13] H. S. Park, J. S. Lee, and C. H. Jun, “A k-means-like algorithm for k-medoids clustering and its performance,” *36th International Conference on Computers and Industrial Engineering, ICC and IE 2006*, pp. 1222–1231, 2006.
- [14] A. Batra, “Analysis and Approach: K-Means and K-Medoids Data Mining Algorithms,” *5th IEEE International Conference on Advanced Computing & Communication Technologies [ICACCT-2011]*, no. 274, pp. 274–279, 2011.
- [15] J. Yusoff, Z. Mohamad, and M. Anuar, “A Review : Consensus Algorithms on Blockchain,” no. Figure 1, pp. 37–50, 2022, doi: 10.4236/jcc.2022.109003.
- [16] R. Auer, “Beyond the Doomsday Economics of ‘Proof-of-Work’ in Cryptocurrencies,” *Federal Reserve Bank of Dallas, Globalization Institute Working Papers*, vol. 2019, no. 355, 2019, doi: 10.24149/gwp355.
- [17] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, “Blockchain smart contracts: Applications, challenges, and future trends,” *Peer Peer Netw Appl*, vol. 14, no. 5, pp. 2901–2925, 2021, doi: 10.1007/s12083-021-01127-0.
- [18] H. A. Aljasim, “Cryptocurrencies as protected investments under bilateral investment treaties,” 2021.
- [19] L. Shi, T. Wang, J. Li, S. Zhang, and S. Guo, “Pooling is not Favorable: Decentralize Mining Power of PoW Blockchain Using Age-of-Work,” *IEEE Transactions on Cloud Computing*, vol. 11, no. 3, pp. 2756–2769, 2023, doi: 10.1109/TCC.2022.3226496.
- [20] B. Li, Q. Lu, W. Jiang, T. Jung, and Y. Shi, “A collaboration strategy in the mining pool for proof-of-neural-architecture consensus,” *Blockchain*:

- Research and Applications*, vol. 3, no. 4, p. 100089, 2022, doi: 10.1016/j.bkra.2022.100089.
- [21] A. Singla, M. Singla, and M. Gupta, “Unpacking the Impact of Bitcoin Halving on the Crypto Market: Benefits and Limitations,” *Scientific Journal of Metaverse and Blockchain Technologies*, vol. 1, no. 1, pp. 43–50, 2023, doi: 10.36676/sjmbt.v1i1.06.
- [22] F. Sullivan and M. Di Pierro, “SECTION TITLE COMPUTING PRESCRIPTIONS What Is the Blockchain?,” *Comput Sci Eng*, vol. 19, no. October, 2017, [Online]. Available: www.computer.org/cise
- [23] Y. Zou, T. Meng, P. Zhang, W. Zhang, and H. Li, “Focus on blockchain: A comprehensive survey on academic and application,” *IEEE Access*, vol. 8, pp. 187182–187201, 2020, doi: 10.1109/ACCESS.2020.3030491.
- [24] P. K. Paul, “Blockchain Technology and its Types—A Short Review,” *International Journal of Applied Science and Engineering*, vol. 9, no. 2, pp. 189–200, 2021, doi: 10.30954/2322-0465.2.2021.7.
- [25] M. Jirgensons and J. Kapenieks, “Blockchain and the Future of Digital Learning Credential Assessment and Management,” *Journal of Teacher Education for Sustainability*, vol. 20, no. 1, pp. 145–156, 2018, doi: 10.2478/jtes-2018-0009.
- [26] S. Aggarwal and N. Kumar, *Attacks on blockchain*☆, 1st ed., vol. 121. Elsevier Inc., 2021. doi: 10.1016/bs.adcom.2020.08.020.
- [27] H. Abijono, P. Santoso, and N. L. Anggreini, “Algoritma Supervised Learning Dan Unsupervised Learning Dalam Pengolahan Data,” *Jurnal Teknologi Terapan: G-Tech*, vol. 4, no. 2, pp. 315–318, 2021, doi: 10.33379/gtech.v4i2.635.
- [28] N. Wakhidah, “Clustering Menggunakan K-Means Algorithm (K-Means Algorithm Clustering),” *Fakultas Teknologi informasi*, vol. 21, no. 1, pp. 70–80, 2014.
- [29] D. Xu and Y. Tian, “A Comprehensive Survey of Clustering Algorithms,” *Annals of Data Science*, vol. 2, no. 2, pp. 165–193, Jun. 2015, doi: 10.1007/s40745-015-0040-1.