

**DETEKSI TRANSAKSI ANOMALI PADA BLOCKCHAIN  
DENGAN MENGGUNAKAN METODE *DEEP BELIEF*  
*NETWORK* (DBN)**

**TUGAS AKHIR**

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



**Oleh :**

**Galih Bayu Permana**

**09011381924126**

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

**2023**

**LEMBAR PENGESAHAN**

**DETEKSI TRANSAKSI ANOMALI PADA BLOCKCHAIN  
DENGAN MENGGUNAKAN METODE *DEEF BELIEF NETWORK (DBN)***

**TUGAS AKHIR**

Diajukan Untuk Melengkapi Salah Satu Syarat  
Memperoleh Gelar Sarjana Komputer

Oleh

**Galih Bayu Permana**

**09011381924126**

Palembang, November 2023

Pembimbing I,



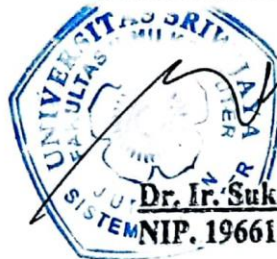
**Prof. Deris Stiawan, M.T., Ph.D.**  
NIP. 197806172006041002

Pembimbing II,



**Huda Ubaya, M.T.**  
NIP. 198106162012121003

Mengetahui, 21/11/23  
Ketua Jurusan Sistem Komputer



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

## HALAMAN PERSETUJUAN

Telah diuji dan lulus pada

Hari : Rabu

Tanggal : 4 Oktober 2023

Tim Penguji

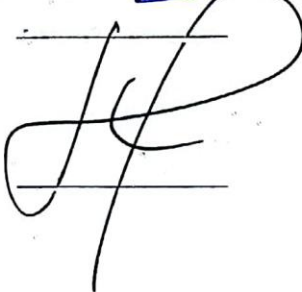
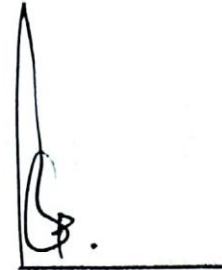
1. Ketua : Sutarno, S.T., M.T.

2. Sekretaris : Nurul Afifah, M.Kom.

3. Penguji : Ahmad Heryanto, M.T.

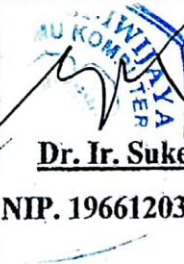
4. Pembimbing I : Prof. Deris Stiawan, M.T., Ph.D.

5. Pembimbing II : Huda Ubaya, M.T.



Mengetahui, 21/10/23

Ketua Jurusan Sistem Komputer



Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

## HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Galih Bayu Permana

NIM : 09011381924126

Judul : Deteksi transaksi anomali pada *blockchain* dengan menggunakan metode *Deep Belief Network (DBN)*

Hasil Pengecekan Plagiat/Turnitin: 4%

Menyatakan bahwa laporan tugas akhir ini adalah hasil karya saya sendiri dan tidak mengandung unsur penjiplakan atau plagiat. Saya sepenuhnya menyadari bahwa jika terbukti adanya penjiplakan atau plagiat dalam laporan tugas akhir ini, saya siap menerima sanksi akademik dari Universitas Sriwijaya. Pernyataan ini saya buat dengan kesadaran penuh dan tanpa adanya paksaan dari pihak manapun.



Palembang, November 2023



**Galih Bayu Permana**

**NIM. 09011381924102**

## KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh,

Puji dan syukur penulis panjatkan kepada Allah SWT yang telah melimpahkan rahmat dan karunianya yang sangat besar dan tidak berhenti, sehingga penulis dapat menyelesaikan Tugas Akhir ini yang berjudul “**Deteksi Transaksi Anomali Pada *Blockchain* Dengan Menggunakan metode *Deep Belief Network (DBN)*”**. Shalawat serta salam tak lupa kita curahkan kepada junjungan kita Nabi Muhammad SAW beserta keluarga, sahabat dan para pengikutnya yang insyaallah istiqomah hingga akhir zaman.

Selesainya penyusunan Tugas Akhir ini tidak terlepas dari peran semua pihak atas ide, bimbingan, dan saran serta bantuannya dalam menyelesaikan penulisan Tugas Akhir ini, antara lain :

1. Allah SWT yang telah memberikan berkah serta nikmat kesehatan dan kesempatan kepada penulis sehingga dapat menyelesaikan Tugas Akhir ini.
2. Kepada kedua orang tua saya yang tercinta yang telah berjasa dalam membesarkan dan mendidik saya dengan penuh kasih sayang, serta tidak henti – hentinya untuk memberikan motivasi dan dukungan baik secara moril, material maupun spiritual selama ini.
3. Bapak Prof. Dr. Erwin, S.Si., M.Si. yang merupakan Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T., selaku ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Prof. Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing 1 Tugas Akhir.
6. Bapak Huda Ubaya, M.T. selaku Dosen Pembimbing 2 Tugas Akhir.
7. Bapak Rossi Passarella, S.T., M.Eng. selaku Dosen Pembimbing Akademik Jurusan Sistem Komputer.
8. Mbak Sari selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas administrasi selama perkuliahan.

9. Bapak, Ibu dosen jurusan Sistem Komputer yang telah memberikan ilmu dan pengalamannya kepada saya.
10. Seluruh pihak yang tergabung dalam comnets terutama Wahyu, Imam, Faisal, dan Udin yang menjadi bagian dalam grup blockchain.
11. Teman – teman seperjuangan Jurusan Sistem Komputer Angkatan 2019, yang selalu memberikan dukungan kepada penulis.
12. Teman – teman saya yang terdapat pada Grup BACOD Mobile, Wake Up, Boys!, Botak, dan juga Fourth Reich yang selalu memberikan dukungan kepada penulis.
13. Jurusan Komputer.
14. Alamamater.

Penulis menyadari bahwa dalam penyusunan laporan ini masih sangat jauh dari kata sempurna. Oleh karena itu penulis mengharapkan kritik dan saran yang membangun untuk penulis, semoga Tugas Akhir ini dapat bermanfaat dan berguna bagi siapa saja yang membacanya.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Palembang, November 2023

Penulis,

**Galih Bayu Permana**

**NIM. 09011381924126**

**DETEKSI TRANSAKSI ANOMALI PADA *BLOCKCHAIN* DENGAN  
MENGUNAKAN METODE *DEEP BELIEF NETWORK (DBN)***

**GALIH BAYU PERMANA (09011381924126)**

Jurusan Sistem Komputer, Fakultas Ilmu Komputer

Universitas Sriwijaya

Email : [galihbp9@gmail.com](mailto:galihbp9@gmail.com)

**ABSTRAK**

Dalam beberapa tahun terakhir, *blockchain* telah banyak digunakan di berbagai bidang seperti *cryptocurrency*, layanan keuangan, dan manajemen risiko. *Cryptocurrency* telah menarik perhatian yang signifikan dari investor, regulator dan media sejak *Bitcoin* pertama kali diusulkan oleh Nakamoto. Penelitian ini menggunakan *Deep Belief Network (DBN)* untuk mendeteksi pola transaksi yang tidak normal (anomali) dalam dataset. Dataset diperoleh dengan mengekstrak data dari tahun 2011 hingga 2013 dan diseimbangkan dengan teknik oversampling dan undersampling. Model terbaik mencapai akurasi 83,05%. Melalui validasi k-fold, model menunjukkan konsistensi yang baik, dengan akurasi rata-rata 82,88%. Hasil ini menunjukkan bahwa model ini konsisten dan dapat diandalkan untuk tugas deteksi yang diberikan.

**Kata Kunci** : Blockchain, Deteksi Anomali, *Deep Belief Network*

**Pembimbing I,**

**Pembimbing II,**

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

**Huda Ubaya, M.T.**  
NIP. 198106162012121003

**Mengetahui,**  
**Ketua Jurusan Sistem Komputer**

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

***ANOMALOUS TRANSACTION DETECTION ON BLOCKCHAIN USING  
DEEP BELIEF NETWORK (DBN)***

**GALIH BAYU PERMANA (09011381924126)**

*Computer Engineering Department, Computer Science Faculty*

*Sriwijaya University*

*Email : [galihbp9@gmail.com](mailto:galihbp9@gmail.com)*

**ABSTRACT**

*In recent years, blockchain technology has found widespread applications across various domains, including cryptocurrency, financial services, and risk management. Cryptocurrency, in particular, has garnered significant attention from investors, regulators, and the media ever since Bitcoin was first proposed by Nakamoto. This research utilizes a Deep Belief Network (DBN) to detect patterns of abnormal transactions (anomaly) in a dataset. The dataset was generated by extracting data spanning from 2011 to 2013 and balanced using oversampling and undersampling techniques. The best-performing model achieved an accuracy of 83.05%. Through k-fold validation, the model exhibited good consistency, with an average accuracy of 82.88%. These results indicate that the model maintains consistency and can be relied upon for the given detection task.*

**Keywords** : *Anomaly Detection, Blockchain, Deep Belief Network*

**Supervisor I,**

**Supervisor II,**

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

**Huda Ubaya, M.T.**  
**NIP. 198106162012121003**

**Acknowledged,  
Head of Computer Systems Department**

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



## DAFTAR ISI

<b>HALAMAN JUDUL</b> .....	<b>i</b>
<b>LEMBAR PENGESAHAN</b> .....	<b>ii</b>
<b>HALAMAN PERSETUJUAN</b> .....	<b>iii</b>
<b>KATA PENGANTAR</b> .....	<b>v</b>
<b>ABSTRAK</b> .....	<b>vii</b>
<b>ABSTRACT</b> .....	<b>viii</b>
<b>DAFTAR ISI</b> .....	<b>ix</b>
<b>DAFTAR GAMBAR</b> .....	<b>xii</b>
<b>DAFTAR TABEL</b> .....	<b>xiii</b>
<b>BAB I PENDAHULUAN</b> .....	<b>1</b>
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	3
1.3 Batasan Masalah.....	3
1.4 Tujuan .....	3
1.5 Manfaat .....	4
1.6 Metodologi Penelitian .....	4
1.7 Sistematika Penulisan.....	5
<b>BAB II TINJAUAN PUSTAKA</b> .....	<b>6</b>
2.1 Pendahuluan .....	6
2.2 Penelitian Terkait .....	6
2.3 <i>Blockchain</i> .....	8
2.4 Dataset.....	9
2.5 <i>Robust Scaler</i> .....	10
2.6 <i>Deep Learning</i> .....	11
2.7 <i>Oversampling</i> .....	12
2.7.1 <i>Borderline SMOTE</i> .....	12
2.7.2 <i>ADASYN (Adaptive Synthetic Sampling)</i> .....	12
2.7.3 <i>Random Oversampling</i> .....	13
2.8 <i>Undersampling</i> .....	13
2.8.1 <i>Random Undersampling</i> .....	14
2.8.2 <i>NearMiss Undersampling</i> .....	14
2.8.3 <i>RUSBoost (RandomUndersampling Bossting)</i> .....	14
2.9 Klasifikasi <i>DBN</i> .....	14

2.10	<i>Confusion matrix</i> .....	16
<b>BAB III METODOLOGI PENELITIAN.....</b>		<b>18</b>
3.1.	Pendahuluan .....	18
3.2.	Kerangka Kerja Penelitian.....	18
3.3.	Perancangan Sistem.....	19
3.4.	Lingkungan <i>Hardware</i> dan <i>Software</i> .....	20
3.5.	<i>Data Understanding</i> .....	21
3.5.1.	<i>Data Cleaning</i> .....	21
3.5.2.	<i>Visualisasi Data</i> .....	21
3.6.	<i>Exploratory Data Analysis</i> .....	22
3.7.	<i>Preprocessing</i> .....	22
3.7.1.	<i>Seleksi Fitur</i> .....	22
3.7.2.	<i>Data Encoding</i> .....	22
3.7.3.	<i>Data Balancing</i> .....	23
3.7.4.	<i>Normalisasi RobustScaler</i> .....	24
3.7.5.	<i>Split Dataset</i> .....	25
3.8.	<i>Model DBN</i> .....	26
3.9.	Evaluasi Model DBN .....	29
3.10.	Validasi Model .....	29
<b>BAB IV HASIL DAN PEMBAHASAN.....</b>		<b>31</b>
4.1.	Pendahuluan .....	31
4.2.	<i>Data Understanding</i> .....	31
4.3.	<i>Exploratory Data Analysis</i> .....	33
4.4.	<i>Preprocessing</i> .....	34
4.4.1.	<i>Selection Feature</i> .....	34
4.4.2.	<i>Hasil Label Encoding</i> .....	35
4.4.3.	<i>Data Balancing</i> .....	35
4.4.4.	<i>Normalisasi</i> .....	39
4.4.5.	<i>Split Dataset</i> .....	39
4.5.	<i>Training Model</i> .....	41
4.6.	Evaluasi Model.....	41
4.6.1.	<i>BSMOTE</i> .....	42
4.6.2.	<i>Random Oversampling</i> .....	44
4.6.3.	<i>ADASYN</i> .....	46
4.6.4.	<i>Random Undersampling</i> .....	48
4.6.5.	<i>RUSBOOST</i> .....	50

4.6.6. <i>Nearmiss Undersampling</i> .....	52
4.7. Perbandingan Matrik .....	54
4.8. Validasi Model Terbaik .....	56
<b>BAB V KESIMPULAN DAN SARAN</b> .....	<b>57</b>
5.1. Kesimpulan .....	57
5.2. Saran .....	57
<b>DAFTAR PUSTAKA</b> .....	<b>58</b>
<b>LAMPIRAN</b> .....	<b>61</b>

## DAFTAR GAMBAR

<b>Gambar 2.1</b> <i>Keywords Analysis</i> .....	8
<b>Gambar 2.2</b> <i>Blockchain Connection Structure</i> .....	9
<b>Gambar 2.3</b> <i>Deep Learning</i> .....	11
<b>Gambar 2.4</b> <i>Deep Belief Network</i> .....	15
<b>Gambar 3.1</b> <i>Kerangka Kerja Penelitian</i> .....	19
<b>Gambar 3.2</b> <i>Rancangan Sistem</i> .....	20
<b>Gambar 3.3</b> <i>Flowchart Data Balancing</i> .....	24
<b>Gambar 3.4</b> <i>Flowchart Normalisasi</i> .....	25
<b>Gambar 3.5</b> <i>Flowchart Algoritma DBN</i> .....	27
<b>Gambar 4.1</b> <i>Fitur Data Kelas 0</i> .....	31
<b>Gambar 4.2</b> <i>Fitur Data Kelas 1</i> .....	31
<b>Gambar 4.3</b> <i>Jumlah Fitur Dengan Data Kosong</i> .....	32
<b>Gambar 4.4</b> <i>Jumlah Data Duplikat</i> .....	32
<b>Gambar 4.5</b> <i>Distribusi Data Kelas Normal dan Anomali</i> .....	33
<b>Gambar 4.6</b> <i>Hasil EDA pada Dataset</i> .....	34
<b>Gambar 4.7</b> <i>Hasil Feature Selection Dataset</i> .....	35
<b>Gambar 4.8</b> <i>Tipe Data Hasil Label Encoding</i> .....	35
<b>Gambar 4.9</b> <i>Distribusi Data Setelah Oversampling</i> .....	37
<b>Gambar 4.10</b> <i>Distribusi Data Setelah Undersampling</i> .....	38
<b>Gambar 4.11</b> <i>Hasil Normalisasi</i> .....	39
<b>Gambar 4.12</b> <i>Proses Training Model</i> .....	41
<b>Gambar 4.13</b> <i>Confusion Matrix data BSMOTE</i> .....	42
<b>Gambar 4.14</b> <i>Confusion Matrix data Random Oversampling</i> .....	44
<b>Gambar 4.15</b> <i>Confusion Matrix data Adasyn</i> .....	46
<b>Gambar 4.16</b> <i>Confusion Matrix data Random Undersampling</i> .....	48
<b>Gambar 4.17</b> <i>Confusion Matrix data RUSBOOST</i> .....	50
<b>Gambar 4.18</b> <i>Confusion Matrix data Nearmiss Undersampling</i> .....	52
<b>Gambar 4.19</b> <i>Perbandingan Akurasi Pada Setiap Model</i> .....	55

## DAFTAR TABEL

<b>Tabel 2.1</b> Jurnal Referensi.....	7
<b>Tabel 3.1</b> Spesifikasi <i>Hardware</i> .....	21
<b>Tabel 3.2</b> Spesifikasi <i>Software</i> .....	21
<b>Tabel 4.1</b> Jumlah Data Sebelum Dilakukan <i>Data Balancing</i> .....	35
<b>Tabel 4.2</b> Jumlah Data setelah <i>Oversampling</i> .....	36
<b>Tabel 4.3</b> Jumlah Data Setelah <i>Undersampling</i> .....	38
<b>Tabel 4.6</b> Metrik Validasi Model <i>DBN</i> data <i>BSMOTE</i> .....	43
<b>Tabel 4.7</b> Metrik Validasi Model <i>DBN</i> data <i>Random Oversampling</i> .....	45
<b>Tabel 4.8</b> Metrik Validasi Model <i>DBN</i> data <i>Adasyn</i> .....	47
<b>Tabel 4.9</b> Metrik Validasi Model <i>DBN</i> data <i>Random Undersampling</i> .....	49
<b>Tabel 4.10</b> Metrik Validasi Model <i>DBN</i> data <i>RUSBOOST</i> .....	51
<b>Tabel 4.11</b> Metrik Validasi Model <i>DBN</i> data <i>Nearmiss Undersampling</i> .....	53
<b>Tabel 4.12</b> Perbandingan Model.....	54
<b>Tabel 4.13</b> Hasil Validasi Terbaik .....	56

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Dalam beberapa tahun terakhir, *blockchain* telah banyak digunakan di berbagai bidang seperti *cryptocurrency*, layanan keuangan, dan manajemen risiko. *Cryptocurrency* telah menarik perhatian yang signifikan dari investor, regulator dan media sejak *Bitcoin* pertama kali diusulkan oleh Nakamoto. *Cryptocurrency* adalah sistem kas elektronik *peer-to-peer* yang memungkinkan pembayaran online dikirim langsung dari satu pihak ke pihak lain tanpa melalui lembaga keuangan. Pada [1] dijelaskan bahwa tidak seperti sebagian besar aset keuangan lain yang tersedia, mereka tidak memiliki hubungan dengan otoritas yang lebih tinggi, tidak memiliki representasi fisik, dan dapat dibagi tanpa batas.

*Blockchain* adalah rantai blok yang dapat menyimpan berbagai informasi (*hash*) dengan *digital signature* dalam jaringan terdesentralisasi dan terdistribusi sehingga membuat transaksi menjadi lebih aman. *Blockchain* adalah bentuk penyimpanan basis data yang terdesentralisasi, andal, dan sulit digunakan untuk tujuan penipuan. *Bitcoin*, di sisi lain, adalah bentuk digital mata uang yang menggunakan buku besar publik *Blockchain* untuk membuatnya transaksi antar jaringan *peer-to-peer*. Dalam jurnal [2] menyebutkan bahwa *bitcoin* hanyalah salah satunya aplikasi keuangan yang menggunakan teknologi Blockchain, ada juga yang lain seperti smart contract dan hyperledger.

*Bitcoin* adalah mata uang kripto yang mendapat perhatian besar karena inovasinya fitur, kesederhanaan, transparansi, dan popularitasnya yang semakin meningkat. Sejak dulu diuraikan dalam makalah oleh Nakamoto (2008) dan online pada tahun 2009, harga *Bitcoin* telah meningkat lebih dari 5000% hingga Juli 2016 [3]. *Bitcoin* [4] adalah versi uang elektronik murni *peer-to-peer* akan memungkinkan pembayaran online untuk dikirim langsung dari satu pihak ke pihak lain tanpa melalui lembaga keuangan.

Pada penelitian [5] menyebutkan bahwa telah ditemukan aktivitas ilegal dalam perdagangan *bitcoin*, kira-kira seperempat dari semuanya pengguna (26%) dan hampir setengah dari transaksi *bitcoin* (46%) terkait dengan kegiatan ilegal. Selanjutnya kurang lebih seperlima (23%) dari jumlah keseluruhan nilai dolar dari transaksi dan sekitar setengah dari kepemilikan *bitcoin* (49%) dari waktu ke waktu diperkirakan merupakan aktivitas ilegal. Dalam penelitian [6] membahas mengenai deteksi transaksi anomali pada *blockchain*, Data transaksi tersebut disinkronkan dari internet menggunakan *bitcoin client software* lalu diekstraksi dan kemudian dianalisa untuk menemukan apabila ada transaksi yang anomali menggunakan teknik *unsupervised machine learning*. Dengan berbagai algoritma seperti *isolation forest*, *histogram - based outlier score (HBOS)*, *cluster - based local outlier factor (CBLOF)*, *principal component analysis (PCA)*, *K - means*, *deep autoencoders*, dan *ensemble classification*. Dari berbagai metode tersebut didapatkan hasil akurasi yaitu (96.99%, 87.12%, 84.89%, 88.18%, 86.52%, 98.84%, 94.89%).

Pada penelitian [7] membahas mengenai deteksi jumlah transaksi yang abnormal pada pasar *cryptocurrency* yaitu Binance, Kucoin, Huobi, Kraken dan Coinbase. Data transaksi tersebut didapatkan melalui *etherscans* kemudian dilakukan analisa menggunakan metode *deep learning LSTM*. Dalam penelitian [8] melakukan penelitian mengenai prediksi transaksi mata uang virtual *cryptocurrency blockchain* menggunakan metode *LSTM* dan *DBN*. Setelah dilakukan analisa dan perbandingan antara metode *LSTM* dan *DBN*, dapat disimpulkan bahwa menggunakan metode *DBN* yang paling cocok untuk memprediksi pasar *cryptocurrency blockchain*.

*Deep Belief Network (DBN)* [9] ditemukan sebagai solusi untuk masalah yang dihadapi saat menggunakan training jaringan saraf tradisional di jaringan berlapis dalam, seperti pembelajaran lambat, macet di mini lokal karena pemilihan parameter yang buruk, dan membutuhkan dataset yang banyak untuk melakukan training.

Berdasarkan pada ulasan diatas maka penulis mengusulkan untuk melakukan penelitian yang berjudul “*Deteksi Transaksi Anomali Pada Blockchain Dengan Menggunakan Metode Deep Belief Network (DBN)*”.

## 1.2 Rumusan Masalah

Adapun rumusan masalah dari penelitian ini, yakni :

1. Bagaimana proses dalam mempersiapkan data untuk Deteksi Transaksi Anomali?
2. Bagaimana cara melakukan validasi terhadap data yang tidak seimbang (imbalance data) agar mendapatkan sampel training dan testing yang tepat?
3. Bagaimana cara yang dapat dilakukan untuk mengatasi data yang tidak seimbang (imbalance data) agar mencapai kinerja optimal?

## 1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah :

1. Dataset yang digunakan pada penelitian ini berupa *Bitcoin Network Transactional Metadata 2011 – 2013*.
2. Menggunakan algoritma *Deep Belief Network (DBN)* untuk deteksi anomaly yang terdiri dari 3 *hidden layer*, fungsi aktivasi *ReLU* serta *sigmoid*, *optimizer adam*, dengan *loss function MSE* dan *metrics binary accuracy*.

## 1.4 Tujuan

Berdasarkan perumusan masalah yang telah ditentukan, maka dibentuk juga tujuan dari penelitian ini, yaitu antara lain :

1. Mengetahui perbedaan data transaksi normal dengan data transaksi anomali pada dataset yang digunakan.
2. Mendeteksi transaksi anomali pada blockchain dengan menggunakan metode *DBN*.
3. Menggunakan teknik oversampling dan undersampling pada dataset untuk proses klasifikasi Deteksi Transaksi Anomali.



## 1.5 Manfaat

Adapun manfaat dari penelitian ini yaitu :

1. Dapat membedakan data transaksi normal dengan data transaksi anomali pada dataset transaksi bitcoin.
2. Dapat mendeteksi data transaksi normal dengan data transaksi anomali pada blockchain dengan menggunakan *DBN*.
3. Teknik oversampling dan undersampling membuat dataset baru untuk mengatasi imbalance dataset.

## 1.6 Metodologi Penelitian

Metodologi yang dilakukan pada penelitian ini yaitu mencari, dan mengumpulkan referensi yang terdapat pada buku, jurnal, tesis serta sumber – sumber yang terpercaya mengenai “*Deteksi Transaksi Anomali Pada Blockchain Dengan Menggunakan Metode Deep Belief Network (DBN)* dan referensi lainnya”

### 1. Metode Konsultasi

Pada metode ini melukan konsultasi secara langsung dan atau tidak langsung kepada semua pihak narasumber yang memiliki pengetahuan serta wawasan yang baik dalam mengatasi permasalahan yang ditemui pada penelitian ini.

### 2. Metode Pengujian Data

Metode ini dilakukan dengan cara membuat suatu perancangan pemodelan pada dataset yang sudah didapatkan dengan deep learning untuk mendapatkan hasil yang diinginkan.

### 3. Metode Analisa

Pada metode ini dilakukan Analisa terhadap sistem yang telah dibuat untuk melihat Batasan – Batasan kinerja sistem tersebut, dapat menghasilkan nilai akurasi yang baik atau sebaliknya.

### 4. Metode Kesimpulan dan Saran

Pada tahap ini penulis menarik kesimpulan dari seluruh kegiatan penelitian Deteksi Transaksi Anomali Pada Blockchain Dengan Menggunakan Metode *Deep Belief Network* (DBN), serta memberikan saran untuk penelitian selanjutnya.

### **1.7 Sistematika Penulisan**

Adapun sistematika dalam penulisan Tugas Akhir ini sebagai berikut :

#### **BAB I PENDAHULUAN**

Bab I berisikan latar belakang, tujuan, manfaat, perumusan masalah, batasan masalah, metodologi penelitian dan sistematika penulisan yang digunakan dalam penulisan tugas akhir ini.

#### **BAB II TINJAUAN PUSTAKA**

BAB II memiliki isi bacaan literature untuk mendukung serta menjadi referensi penelitian yang berisi teori dan metode Deep Belief Network.

#### **BAB III METODOLOGI PENELITIAN**

BAB III ini akan menjelaskan proses – proses dalam melakukan penelitian, menjelaskan kerangka kerja, proses pembentukan sistem, langkah kerja dan metodologi penelitian.

#### **BAB IV HASIL DAN ANALISA**

BAB IV akan menjelaskan hasil dari penelitian yang dilakukan, serta melakukan analisis dari Deteksi Transaksi Anomali Pada Blockchain Dengan Menggunakan Metode Deep Belief Network (DBN).

#### **BAB V KESIMPULAN DAN SARAN**

BAB V berisi mengenai kesimpulan dari bab – bab sebelumnya dan juga akan menyertakan saran agar penelitian ini dapat dikembangkan lagi kedepannya.

## DAFTAR PUSTAKA

- [1] S. Corbet, B. Lucey, A. Urquhart, and L. Yarovaya, “Cryptocurrencies as a financial asset: A systematic analysis,” *Int. Rev. Financ. Anal.*, vol. 62, pp. 182–199, 2019, doi: 10.1016/j.irfa.2018.09.003.
- [2] P. Tasatanattakool and C. Techapanupreeda, “Blockchain: Challenges and applications,” *Int. Conf. Inf. Netw.*, vol. 2018-Janua, pp. 473–475, 2018, doi: 10.1109/ICOIN.2018.8343163.
- [3] A. Urquhart, “The inefficiency of Bitcoin,” *Econ. Lett.*, vol. 148, pp. 80–82, 2016, doi: 10.1016/j.econlet.2016.09.019.
- [4] I. O. Adam and M. Dzang Alhassan, “Bridging the global digital divide through digital inclusion: the role of ICT access and ICT use,” *Transform. Gov. People, Process Policy*, vol. 15, no. 4, pp. 580–596, 2020, doi: 10.1108/TG-06-2020-0114.
- [5] S. Foley, J. R. Karlsen, and T. J. Putnins, “Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?,” *Rev. Financ. Stud.*, vol. 32, no. 5, pp. 1798–1853, 2019, doi: 10.1093/rfs/hhz015.
- [6] Omer Shafiq, “Anomaly Detection inBlockchain,” no. December, 2019.
- [7] Z. Gu, D. Lin, and J. Wu, “On-chain analysis-based detection of abnormal transaction amount on cryptocurrency exchanges,” *Phys. A Stat. Mech. its Appl.*, vol. 604, p. 127799, 2022, doi: 10.1016/j.physa.2022.127799.
- [8] X. Li, Q. Liu, and Y. Wu, “Prediction on blockchain virtual currency transaction under long short-term memory model and deep belief network,” *Appl. Soft Comput.*, vol. 116, no. December 2021, p. 108349, 2022, doi: 10.1016/j.asoc.2021.108349.
- [9] K. K. Al-jabery, T. Obafemi-Ajayi, G. R. Olbricht, and D. C. Wunsch II, “Selected approaches to supervised learning,” *Comput. Learn. Approaches to Data Anal. Biomed. Appl.*, pp. 101–123, 2020, doi: 10.1016/b978-0-12-

814482-4.00004-8.

- [10] T. Ashfaq *et al.*, “A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism,” *Sensors*, vol. 22, no. 19, pp. 1–20, 2022, doi: 10.3390/s22197162.
- [11] M. Rwibasira and S. R., “ADOBSVM: Anomaly detection on block chain using support vector machine,” *Meas. Sensors*, vol. 24, no. October, p. 100503, 2022, doi: 10.1016/j.measen.2022.100503.
- [12] P. Nerurkar, S. Bhirud, D. Patel, R. Ludinard, Y. Busnel, and S. Kumari, “Supervised learning model for identifying illegal activities in Bitcoin,” *Appl. Intell.*, vol. 51, no. 6, pp. 3824–3843, 2021, doi: 10.1007/s10489-020-02048-w.
- [13] P. Monamo, V. Marivate, and B. Twala, “Unsupervised learning for robust Bitcoin fraud detection,” *2016 Inf. Secur. South Africa - Proc. 2016 ISSA Conf.*, pp. 129–134, 2016, doi: 10.1109/ISSA.2016.7802939.
- [14] J. H. Park and J. H. Park, “Blockchain security in cloud computing: Use cases, challenges, and solutions,” *Symmetry (Basel)*, vol. 9, no. 8, pp. 1–13, 2017, doi: 10.3390/sym9080164.
- [15] Y. Jadhav and A. B. Farimani, “Dominant motion identification of multi-particle system using deep learning from video,” *2018 Fourth Int. Conf. Comput. Commun. Control Autom.*, pp. 1–6, 2021, [Online]. Available: <http://arxiv.org/abs/2104.12722>.
- [16] H. Shamsudin, U. K. Yusof, A. Jayalakshmi, and M. N. Akmal Khalid, “Combining oversampling and undersampling techniques for imbalanced classification: A comparative study using credit card fraudulent transaction dataset,” *IEEE Int. Conf. Control Autom. ICCA*, vol. 2020-Octob, pp. 803–808, 2020, doi: 10.1109/ICCA51439.2020.9264517.
- [17] E. AT, A. M, A.-M. F, and S. M, “Classification of Imbalance Data using Tomek Link (T-Link) Combined with Random Under-sampling (RUS) as a Data Reduction Method,” *Glob. J. Technol. Optim.*, vol. 01, no. S1, 2016,

doi: 10.4172/2229-8711.s1111.

- [18] N. M. Mqadi, N. Naicker, and T. Adeliyi, “Solving Misclassification of the Credit Card Imbalance Problem Using near Miss,” *Math. Probl. Eng.*, vol. 2021, 2021, doi: 10.1155/2021/7194728.
- [19] F. S. Abdullah *et al.*, “Recent Advances on Soft Computing and Data Mining,” vol. 549, 2017, doi: 10.1007/978-3-319-51281-5.
- [20] R. Dubey, J. Zhou, Y. Wang, P. M. Thompson, and J. Ye, “Analysis of sampling techniques for imbalanced data: An n=648 ADNI study,” *Neuroimage*, vol. 87, pp. 220–241, 2014, doi: 10.1016/j.neuroimage.2013.10.005.
- [21] H. Han, W.-Y. Wang, and B.-H. Mao, “Borderline-SMOTE: A New Over-Sampling Method in Imbalanced Data Sets Learning,” 2005.
- [22] H. He, Y. Bai, E. A. Garcia, and S. Li, “ADASYN: Adaptive synthetic sampling approach for imbalanced learning,” *Proc. Int. Jt. Conf. Neural Networks*, no. July 2008, pp. 1322–1328, 2008, doi: 10.1109/IJCNN.2008.4633969.
- [23] S. Kotsiantis, D. Kanellopoulos, and P. Pintelas, “Handling imbalanced datasets : A review,” *Science (80-. )*, vol. 30, no. 1, pp. 25–36, 2006, [Online]. Available: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.96.9248&rep=rep1&type=pdf>.
- [24] R. Vohra, K. Goel, and J. K. Sahoo, “Modeling temporal dependencies in data using a DBN-LSTM,” *Proc. 2015 IEEE Int. Conf. Data Sci. Adv. Anal. DSAA 2015*, no. 3, pp. 0–3, 2015, doi: 10.1109/DSAA.2015.7344820.
- [25] G. E. Hinton, “Nccd.Pdf,” vol. 1800, pp. 1771–1800, 2002.
- [26] T. R. Shultz and S. E. Fahlman, *Encyclopedia of Machine Learning and Data Mining*. 2017.