DETEKSI ANOMALI TRANSAKSI BITCOIN DENGAN METODE *ISOLATION FOREST*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

AGERA ANISKA

09011282025070

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN

DETEKSI ANOMALI TRANSAKSI BITCOIN DENGAN METODE *ISOLATION FOREST*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Program Studi Sistem Komputer
Jenjang S1

Oleh:
AGERA ANISKA
09011282025070

Palembang, 12 Juni 2024

Pembimbing I

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

Pembimbing II

Nurul Afifah, M.Kom.
NIP. 199211102023212049

Mengetahui,
Ketua Jurusan Sistem Komputer

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

AUTHENTICATION PAGE

ANOMALY DETECTION OF BITCOIN TRANSACTIONS USING ISOLATION FOREST METHOD

THESIS

One of the requirements for obtaining a Bachelor's Degree in Computer Science

Dept. of Computer System
Bachelor's Degree

By:
AGERA ANISKA
09011282025070

Palembang, 12 Juni 2024

Final Project Advisor I

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

Final Project Advisor II

Nurul Afifah, M.Kom.
NIP. 199211102023212049

Acknowledge,
Head of Computer Systems Departement

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Rabu
Tanggal : 22 Mei 2024

Tim Penguji :

1. Ketua : **Kemahyanto Exaudi, M.T.**
2. Sekretaris : **Abdurahman, S.Kom., M.Han.**
3. Penguji : **Huda Ubaya, M.T.**
4. Pembimbing I : Prof. Deris Stiawan, M.T., Ph.D.
5. Pembimbing II : Nurul Afifah, M.Kom.

Mengetahui, 12/6/24
Ketua Jurusan Sistem Komputer

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

HALAMAN PERNYATAAN

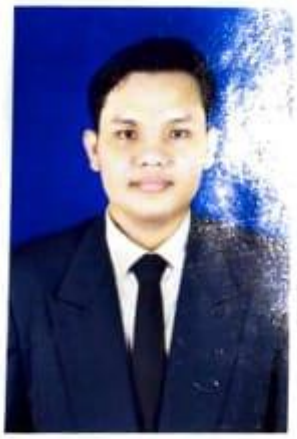
Yang bertandatangan di bawah ini :

Nama	:	Agera Aniska
NIM	:	09011282025070
Program Studi	:	Sistem Komputer
Judul Skripsi	:	Deteksi Anomali Transaksi Bitcoin Dengan Metode Isolation Forest

Hasil Pengecekan Software iThenticate/Turnitin : 6%

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

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



Indralaya, Juni 2024

Agera Aniska

NIM. 09011282025070

KATA PENGANTAR

Assalamualaikum Wr.Wb.

Puji dan syukur serta ucapan Alhamdulillah saya panjatkan kepada Allah SWT. atas Rida dan Rahmat-Nya, Penulis dapat menyelesaikan penyusunan skripsi ini. Adapun judul skripsi yang penulis ajukan adalah "**Deteksi Anomali Transaksi Bitcoin Dengan Metode *Isolation Forest***"

Penulis menyadari bahwa banyak pihak yang telah memberikan dukungan dan membantu selama penulisan tugas akhir ini, oleh karena itu penulis ingin mengucapkan terima kasih kepada beberapa pihak atas ide serta sarannya dan mendoakan semoga Allah memberikan balasan terbaik dan mengucapkan terima kasih kepada yang terhormat :

1. Almarhumah Ibu, sosok yang selalu memberikan dukungan tak terbatas sepanjang perjalanan penulisan skripsi ini, meskipun sayangnya tidak sempat menyaksikan penyelesaiannya.
2. Ayah, Adik dan keluarga yang telah banyak memberikan doa dan dukungan serta semangat.
3. Bapak Prof. Dr. Erwin, S.Si., M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
5. Bapak Prof. Deris Stiawan, M.T., Ph.D., IPU., ASEAN Eng., selaku Dosen Pembimbing pertama, telah meluangkan waktu untuk membimbing, memberikan saran, dan memberikan motivasi kepada penulis dalam menyelesaikan tugas akhir ini.
6. Ibu Nurul Afifah, M.Kom., selaku Dosen Pembimbing kedua, senantiasa memberikan kritik dan saran yang membangun sehingga penulisan tugas akhir ini dapat berjalan lancar tanpa adanya kendala.
7. Bapak Abdurahman, S. KOM., M. HAN. selaku Dosen Pembimbing Akademik.
8. Admin dan Staf akademik Jurusan Sistem Komputer dan Fakultas Ilmu Komputer yang telah membantu mengurus berkas-berkas yang diperlukan.

9. Teman-teman kelas SK Reg. B 2020.
10. Dan semua pihak yang tidak dapat disebutkan satu persatu.
11. Almamater.

Akhir kata, penulis ingin mengakhiri dengan penuh penghormatan, dengan kesadaran akan keterbatasan yang ada. Harapannya adalah agar Tugas Akhir ini dapat memberikan manfaat bagi kita semua, terutama bagi para mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya, baik secara langsung maupun tidak langsung. Semoga ini bisa menjadi kontribusi berharga dalam meningkatkan kualitas pembelajaran dan penelitian.

Wassalamualaikum Wr. Wb.

Indralaya, Juni 2024

Penulis,

Agera Aniska

Nim. 09011282025070

DETEKSI ANOMALI TRANSAKSI BITCOIN DENGAN METODE ISOLATION FOREST

Agera Aniska (09011282025070)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : agraaniska@gmail.com

ABSTRAK

Bitcoin, diperkenalkan pada 2008 oleh Satoshi Nakamoto, adalah mata uang digital pertama yang menggunakan blockchain untuk transaksi aman. Meskipun populer, tantangan dalam mendeteksi transaksi ilegal atau mencurigakan muncul karena kurangnya regulasi dan anonimitas. Penelitian ini menggunakan algoritma Isolation Forest untuk mengidentifikasi transaksi Bitcoin yang tidak sah. Hasilnya menunjukkan tingkat akurasi, presisi, recall, dan F1-score yang konsisten, meskipun ada kecenderungan mengklasifikasikan transaksi normal sebagai anomali. Evaluasi model menunjukkan kinerja terbaik dengan pembagian data train 30% dan testing 70%, dengan akurasi 96.56%, precision 98.25%, recall 98.35%, dan F1-score 98.24%. Isolation Forest efektif dalam mendeteksi transaksi mencurigakan, namun tantangan tetap ada dalam membedakan transaksi normal dan anomali.

Kata Kunci : Bitcoin, Isolation Forest, Deteksi Anomali, Blockchain.

ANOMALY DETECTION OF BITCOIN TRANSACTIONS USING ISOLATION FOREST METHOD

Agera Aniska (09011282025070)
Department of Computer Systems, Faculty of Computer Science, Sriwijaya University
Email : agraaniska@gmail.com

ABSTACT

Bitcoin, introduced in 2008 by Satoshi Nakamoto, is the first digital currency to use blockchain for secure transactions. Despite its popularity, challenges in detecting illegal or suspicious transactions arise due to lack of regulation and anonymity. This research employs the Isolation Forest algorithm to identify fraudulent Bitcoin transactions. Isolation Forest was chosen for its superiority in detecting anomalies in large and heterogeneous datasets, with the ability to handle high-dimensional and large-scale problems. The method was tested on a dataset of Bitcoin transactions from a specific period, which was then divided into training and testing data. Evaluation results show consistent levels of accuracy, precision, recall, and F1-score, albeit with a tendency to classify normal transactions as anomalies. Model evaluation indicates the best performance with a training data split of 30% and testing data split of 70%, yielding an accuracy of 96.56%, precision of 98.25%, recall of 98.35%, and F1-score of 98.24%. The findings of this study make a significant contribution to the development of fraud detection systems for digital currencies, particularly in addressing security and anomaly issues commonly associated with Bitcoin transactions.

Keywords : Bitcoin, Isolation Forest, Anomaly Detection, Blockchain.

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada tahun 2008, sekelompok orang atau individu yang menyebut dirinya sebagai “Satoshi Nakamoto” memperkenalkan bitcoin sebagai mata uang peer-to-peer untuk pertama kalinya, tujuannya adalah untuk membuat uang digital yang dapat ditransfer langsung tanpa melalui pihak ketiga[1], [2]. Bitcoin menjadi pilihan utama karena dengan keunggulan utamanya adalah terdesentralisasi, dengan teknologi dibaliknya, bitcoin memungkinkan transaksi untuk dilakukan dengan cara yang komprehensif dan terjamin keamanannya[3]. Teknologi dibalik bitcoin adalah Blockchain[2], [4]. Blockchain adalah sebuah buku besar terbuka dan terdistribusi yang mencatat transaksi dengan cara efisien, diverifikasi dan permanen[1], [5].

Struktur sistem Bitcoin didesain sedemikian rupa sehingga kompleksitas dalam menghitung checksum seiring dengan pertumbuhan kapasitas komputasi global[6]. Di dalam jaringan Bitcoin, entitas yang disebut node bertanggung jawab untuk menyimpan transaksi ke dalam blockchain. Setiap transaksi dicatat dalam satu blok, dan sistem blockchain diperpanjang untuk menghasilkan blok-blok baru. Mekanisme pembentukan blok baru ini dikenal sebagai penambangan atau "Mining," dan individu yang melaksanakan tugas ini disebut penambang atau "miner". Demi mencapai efektivitas dalam kegiatan penambangan, para penambang harus menemukan solusi yang dikenal sebagai proof-of-work (PoW)[7].

Dalam beberapa tahun belakangan ini, keberadaan bitcoin terus berkembang dengan pesat, dengan tidak adanya peraturan di pasar bitcoin, beberapa perilaku ilegal dapat terjadi kapan saja dalam transaksi. Hal ini dapat menimbulkan pertanyaan mengenai apakah terdapat perilaku ilegal dalam transaksi bitcoin dalam sistem blockchain[8]. Dalam jaringan Bitcoin, sebagian transaksi dilakukan melalui node yang bersifat anonim, sehingga mengakibatkan kesulitan dalam membedakan

transaksi yang biasa dengan transaksi yang mencurigakan[9]. Kehadiran anonimitas pada node menambah kompleksitas dalam pengawasan transaksi. Dengan kata lain, Blockchain sebagai infrastruktur tidak mampu secara efektif membedakan kedua jenis transaksi tersebut. Hal ini menimbulkan tantangan tersendiri bagi pihak-pihak yang berkepentingan dalam memonitor dan memastikan integritas serta keamanan transaksi dalam jaringan Bitcoin.[10]. Selain itu, dalam transaksi bitcoin ada aturan tertentu mengenai valid atau tidaknya sebuah transaksi, sebuah transaksi yang tidak valid merupakan transaksi dengan nilai total output lebih besar dari total input[11]. Total input sudah termasuk fee atau biaya transaksi [1]. Transaksi yang tidak valid ini akan dijadikan target untuk mendeteksi anomali pada transaksi bitcoin.

Penelitian sebelumnya telah menginvestigasi fenomena perilaku ilegal yang terjadi di platform-platform bitcoin, mencakup perbedaan karakteristik antar platform, praktik manipulasi harga, dan upaya pencucian uang, fokus penelitiannya juga termasuk pengembangan metode deteksi yang akurat untuk mengidentifikasi perilaku anomali tersebut[8]. Penelitian selanjutnya yang dilakukan oleh S. Gard mengulas penggunaan teknik machine learning yang relevan dalam mendeteksi anomali pada big data, dengan memberikan wawasan tentang langkah-langkah dan strategi yang efektif dalam proses deteksi tersebut[9]. Selanjutnya, penelitian oleh Pham T dan Lee S berhasil mendeteksi dua (2) dari 30 kasus pencurian menggunakan pendekatan unsupervised learning[12]. Pada penelitian terbaru, Swapna Siddamsetti dan Dr. Muktevi Srivenkatesh membahas pola anomali yang muncul dalam jaringan bitcoin dengan menggunakan pendekatan unsupervised learning isolation forest, dengan hasil accuracy 70% pada data training dan 80% pada testing, selain itu, untuk ROC AUC penelitian ini mendapatkan skor 87% pada training dan 90% pada testing[13]. Referensi terbaru yang relevan adalah penelitian yang dilakukan oleh Priyanshi Singh dan rekan-rekannya, yang membandingkan efektivitas metode K-Means, Isolation Forest, dan Support Vector Machine (SVM) dalam mendeteksi anomali pada sistem blockchain. Dimana hasil terbaik merupakan algoritma Support Vector Machine (SVM) dengan tingkat akurasi 98% dan untuk isolation forest tingkat akurasi sebesar 96%. Studi ini memberikan wawasan yang berharga dalam pemilihan algoritma yang tepat untuk deteksi

anomali dalam konteks sistem blockchain[14]. Pada penelitian deteksi dan klasifikasi anomali secara real time menggunakan isolation forest, k-means dan LoOp, hasil yang mereka dapatkan adalah mengklasifikasikan anomali data menjadi tiga kategori: bad data, peristiwa (events), dan kesalahan PDC dengan recall 96 – 99% dan precision 93 – 97%[15]. Pada penelitian yang membahas tentang perbandingan algoritma isolation forest dan local outlier factor, LOF sedikit lebih unggul dari isolation forest, isolation forest memiliki rentang accuracy dari 68 – 98% dan LOF memiliki rentang 63 - 99%[16]. Selain melakukan penelitian berdasarkan transaksi, Xiong Yang dan timnya pernah membahas deteksi anomali pada jaringan menggunakan metode yang serupa dengan penelitian yang penulis buat, yaitu isolation forest. Hasil penelitian mereka menunjukkan bahwa model yang dikembangkan mencapai nilai F1-score sebesar 0.6 atau 60%, dengan tingkat akurasi mencapai 96%[17]. Di sisi lain, dalam konteks deteksi penipuan pada cryptocurrency, Eran Kaufman dan rekannya telah melakukan penelitian serupa. Namun, dalam penelitian mereka, metode isolation forest menunjukkan kinerja yang lebih rendah dari tiga metode lain yang diuji. Hal ini disebabkan karena lebih banyak mendeteksi titik data normal daripada data penipuan[18]. Pada penelitian sebelumnya yang dilakukan oleh Joana Lorenz dan timnya, mereka membahas tentang eksperimen mendeteksi pencucian uang pada bitcoin menggunakan metode unsupervised learning seperti isolation forest dan Active Learning. Hasil penelitian ini menunjukkan bahwa unsupervised learning memiliki kinerja yang tidak sesuai dengan harapan, dengan tingkat akurasi pada evaluasi dengan label sebesar 23% hingga 83%[19].

Berdasarkan beberapa ulasan di atas, penulis mengusulkan penelitian dengan judul **"Deteksi Anomali Transaksi Bitcoin Dengan Metode Isolation Forest"**. Tujuan dari penelitian ini adalah untuk mengidentifikasi transaksi Bitcoin yang tidak sah atau mencurigakan yang tersimpan dalam blockchain. Penulis akan menggunakan metode Unsupervised Learning dengan algoritma Isolation Forest untuk menemukan transaksi-transaksi ini sebagai anomali. Selain itu, penulis juga akan mengevaluasi seberapa efektif algoritma ini dalam mendeteksi transaksi-transaksi yang tidak sah atau mencurigakan, yang pada dasarnya merupakan transaksi yang tidak valid tetapi tetap tercatat dalam blockchain.

1.2 Rumusan Masalah

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

1. Bagaimana cara mengidentifikasi transaksi Bitcoin yang tidak biasa atau anomali?.
2. Bagaimana algoritma Isolation Forest dapat diterapkan untuk mendeteksi anomali pada transaksi Bitcoin?.
3. Bagaimana kinerja algoritma Isolation Forest dalam mendeteksi anomali pada transaksi Bitcoin?.

1.3 Tujuan

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

1. Mengidentifikasi transaksi Bitcoin yang tidak biasa atau anomali.
2. Menerapkan algoritma Isolation Forest untuk mendeteksi anomali dalam transaksi Bitcoin.
3. Mengelompokkan transaksi bitcoin menjadi dua kelompok, yaitu transaksi normal dan transaksi anomali
4. Mengevaluasi kinerja Isolation Forest dalam mendeteksi anomali pada transaksi bitcoin.

1.4 Manfaat

Berikut beberapa manfaat dari penelitian yang akan penulis lakukan, diantara-Nya sebagai berikut :

1. Mengidentifikasi transaksi Bitcoin yang tidak biasa atau anomali guna meningkatkan keamanan jaringan Bitcoin dan mengurangi risiko penipuan atau aktivitas ilegal.
2. Menerapkan algoritma Isolation Forest untuk mendeteksi anomali dalam transaksi Bitcoin, memungkinkan pengembangan teknik deteksi yang lebih canggih dan efisien untuk mengatasi transaksi yang mencurigakan.

3. Memberikan pemahaman yang lebih baik tentang keandalan dan efektivitas algoritma isolation forest dalam mendeteksi anomali pada transaksi Bitcoin, serta potensi pengembangan lebih lanjut.

1.5 Batasan Masalah

Batasan Masalah pada Tugas Akhir ini adalah sebagai berikut :

1. Hanya berfokus pada deteksi anomali.
2. Anomali hanya berfokus pada data transaksi yang tidak valid.
3. Tidak mempertimbangkan faktor eksternal yang mempengaruhi anomali dalam transaksi bitcoin.
4. Menggunakan dataset *bigquery-public-data.crypto_bitcoin* yang tersedia di Google Cloud dan di kueri menggunakan SQL.
5. Metode deteksi anomali menggunakan Isolation Forest yang merupakan unsupervised learning.

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 menganalisis 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, dimanah pada bab ini akan membahas tentang Blockain, 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 menganalisis 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] Z. Zheng, H. Dai, and J. Wu, *Blockchain Intelligence*, no. January. 2021. doi: 10.1007/978-981-16-0127-9.

[3] A. K. Kibet, D. Gebresenbet Bayyou, R. Esquivel, D. G. Bayyou, and R. A. Esquivel, "Blockchain: It'S Structure, Principles, Applications and Foreseen Issues," *J Emerg Technol Innov Res*, vol. 6, no. April, p. 13, 2019, [Online]. Available: https://www.researchgate.net/publication/332858253_Blockchain_It's_Structure_Principles_Applications_And_Foreseen_Issues

[4] M. van Rijmenam and P. Ryan, "What is the Blockchain?," *Blockchain*, no. October, pp. 12–39, 2018, doi: 10.4324/9780429457715-2.

[5] K. R. Lakhani, "The Truth About Blockchain," no. February, 2017.

[6] M. Thum, "The economic cost of bitcoin mining," *CESifo Forum*, vol. 19, no. 1, pp. 43–45, 2018.

[7] Y. Kwon, H. Kim, J. Shin, and Y. Kim, "Bitcoin vs. Bitcoin cash: Coexistence or downfall of bitcoin cash?," *Proc IEEE Symp Secur Priv*, vol. 2019-May, pp. 935–951, 2019, doi: 10.1109/SP.2019.00075.

[8] F. Bin Shi, X. Q. Sun, J. H. Gao, L. Xu, H. W. Shen, and X. Q. Cheng, "Anomaly detection in Bitcoin market via price return analysis," *PLoS One*, vol. 14, no. 6, pp. 1–11, 2019, doi: 10.1371/journal.pone.0218341.

[9] S. Garg, "Anomaly Detection and Analysis in Big Data," pp. 1–21, 2018.

[10] S. Morishima, "Scalable anomaly detection in blockchain using graphics processing unit," *Computers and Electrical Engineering*, vol. 92, no. March, p. 107087, 2021, doi: 10.1016/j.compeleceng.2021.107087.

[11] N. Atzei, M. Bartoletti, S. Lande, and R. Zunino, "A formal model of Bitcoin transactions." [Online]. Available: https://github.com/bitcoin/bitcoin.

[12] T. T. Pham and S. Lee, "Anomaly Detection in Bitcoin Network Using Unsupervised Learning Methods." [Online]. Available: https://bitcoin.

[13] S. Siddamsetti and M. Srivenkatesh, “International Journal of Intelligent Systems And Applications In Engineering Deep Blockchain Approach for Anomaly Detection in the Bitcoin Network.” [Online]. Available: www.ijisae.org

[14] P. Singh, D. Agrawal, and S. Pandey, “Anomaly detection and analysis in blockchain systems,” 2023, doi: 10.21203/rs.3.rs-2414745/v1.

[15] E. Khaledian, S. Pandey, P. Kundu, and A. K. Srivastava, “Real-Time Synchrophasor Data Anomaly Detection and Classification Using Isolation Forest, KMeans, and LoOP,” *IEEE Trans Smart Grid*, vol. 12, no. 3, pp. 2378–2388, May 2021, doi: 10.1109/TSG.2020.3046602.

[16] Z. Cheng, C. Zou, and J. Dong, “Outlier detection using isolation forest and local outlier,” in *Proceedings of the 2019 Research in Adaptive and Convergent Systems, RACS 2019*, Association for Computing Machinery, Inc, Sep. 2019, pp. 161–168. doi: 10.1145/3338840.3355641.

[17] X. Yang, Y. Chen, X. Qian, T. Li, and X. Lv, “BCEAD: A Blockchain-Empowered Ensemble Anomaly Detection for Wireless Sensor Network via Isolation Forest,” *Security and Communication Networks*, vol. 2021, 2021, doi: 10.1155/2021/9430132.

[18] E. Kaufman and A. Iaremenko, “Anomaly Detection for Fraud in Cryptocurrency Time Series,” Jul. 2022, [Online]. Available: http://arxiv.org/abs/2207.11466

[19] T. Balch and Association for Computing Machinery, *The First ACM International Conference on AI in Finance (ICAIF 2020) : New York, New York, October 15 - 16, 2020*.

[20] I. Alqassem, I. Rahwan, and D. Svetinovic, “The Anti-Social System Properties: Bitcoin Network Data Analysis,” *IEEE Trans Syst Man Cybern Syst*, vol. 50, no. 1, pp. 21–31, Jan. 2020, doi: 10.1109/TSMC.2018.2883678.

[21] R. Grinberg, “Bitcoin: An Innovative Alternative Digital Currency,” 2011. [Online]. Available: http://bitcoinwatch.com/

[22] Q. Wang, J. Huang, S. Wang, Y. Chen, P. Zhang, and L. He, “A Comparative Study of Blockchain Consensus Algorithms,” in *Journal of Physics:*

Conference Series, Institute of Physics Publishing, Jan. 2020. doi: 10.1088/1742-6596/1437/1/012007.

[23] 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, Sep. 2021, doi: 10.1007/s12083-021-01127-0.

[24] H. Ali Aljasim Supervisor and P. Steffen Hindelang, "Department of Law Spring Term 2021 Cryptocurrencies as protected investments under bilateral investment treaties Is there a BIT of coin Protection?"

[25] R. Auer, "Beyond the doomsday economics of 'proof-of-work' in cryptocurrencies," 2019. [Online]. Available: www.bis.org

[26] J. Becker, D. Breuker, T. Heide, J. Holler, H. P. Rauer, and R. Böhme, "Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency", doi: 10.1007/978-3-642-39498-0__7.

[27] L. Shi, T. Wang, J. Li, and S. Zhang, "Pooling is not Favorable: Decentralize Mining Power of PoW Blockchain Using Age-of-Work," Apr. 2021, [Online]. Available: http://arxiv.org/abs/2104.01918

[28] L. William Cong Zhiguo He Jiasun Li *et al.*, "Nber Working Paper Series Decentralized Mining In Centralized Pools Decentralized Mining in Centralized Pools," 2019. [Online]. Available: http://www.nber.org/papers/w25592

[29] 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, Dec. 2022, doi: 10.1016/j.bcra.2022.100089.

[30] L. W. Cong, Z. He, and J. Li, "Decentralized Mining in Centralized Pools," *Review of Financial Studies*, vol. 34, no. 3, pp. 1191–1235, Mar. 2021, doi: 10.1093/rfs/hhaa040.

[31] 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.

[32] J. Taskinsoy, "Bitcoinmania: A Ticking Time Bomb Waiting to Explode ∗." [Online]. Available: https://ssrn.com/abstract=3861836

[33] F. Sullivan and M. Di Pierro, "Section Title Computing Prescriptions What Is the Blockchain?" [Online]. Available: www.computer.org/cise

[34] Z. Gu, D. Lin, and J. Wu, "On-chain analysis-based detection of abnormal transaction amount on cryptocurrency exchanges," *Physica A: Statistical Mechanics and its Applications*, vol. 604, Oct. 2022, doi: 10.1016/j.physa.2022.127799.

[35] 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. Institute of Electrical and Electronics Engineers Inc., pp. 187182–187201, 2020. doi: 10.1109/ACCESS.2020.3030491.

[36] Y. Ma, Y. Sun, Y. Lei, N. Qin, and J. Lu, "A survey of blockchain technology on security, privacy, and trust in crowdsourcing services," *World Wide Web*, vol. 23, no. 1, pp. 393–419, Jan. 2020, doi: 10.1007/s11280-019-00735-4.

[37] P. K. Aithal, P. S. Saavedra, and R. Ghosh, "Blockchain Technology and its Types-A Short Review," 2021.

[38] 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, Jun. 2018, doi: 10.2478/jtes-2018-0009.

[39] V. Nur, S. Ginting, and K. Tesselhof, "How Does Starbucks Implement The Blockchain System In Supply Chain Management To Maintain Its Product Quality?," *Diponegoro Journal Of Accounting*, vol. 12, no. 4, pp. 1–15, [Online]. Available: http://ejournal-s1.undip.ac.id/index.php/accounting

[40] S. Aggarwal and N. Kumar, "Attacks on blockchain☆," in *Advances in Computers*, vol. 121, Academic Press Inc., 2021, pp. 399–410. doi: 10.1016/bs.adcom.2020.08.020.

[41] Anitan and Vijayalakshmim, "Blockchain Security Attack: A Brief Survey."

[42] M. I. Mehar *et al.*, “Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack.” [Online]. Available: https://ssrn.com/abstract=3014782Electroniccopyavailableat:https://ssrn.com/abstract=3014782

[43] M. J. Jeyasheela Rakkini and K. Geetha, “Detection of Bitcoin Miners by Clustering Crypto Address with Google BigQuery Open Dataset,” in *Soft Computing: Theories and Applications*, R. Kumar, C. W. Ahn, T. K. Sharma, O. P. Verma, and A. Agarwal, Eds., Singapore: Springer Nature Singapore, 2022, pp. 25–32.

[44] M. Gregoriadis, R. Muth, and M. Florian, “Analysis of Arbitrary Content on Blockchain-Based Systems using BigQuery,” in *WWW 2022 - Companion Proceedings of the Web Conference 2022*, Association for Computing Machinery, Inc, Apr. 2022, pp. 478–487. doi: 10.1145/3487553.3524628.

[45] P. Santoso, H. Abijono, and N. L. Anggreini, “Algoritma Supervised Learning Dan Unsupervised Learning Dalam Pengolahan Data,” *Unira Malang* |, vol. 4, no. 2, 2021.

[46] W. Wu, “Unsupervised Learning,” 2022.

[47] F. T. Liu, K. M. Ting, and Z. H. Zhou, “Isolation forest,” in *Proceedings - IEEE International Conference on Data Mining, ICDM*, 2008, pp. 413–422. doi: 10.1109/ICDM.2008.17.

[48] M. Said Elsayed, N. A. Le-Khac, S. Dev, and A. D. Jurcut, “Network Anomaly Detection Using LSTM Based Autoencoder,” in *Q2SWinet 2020 - Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, Association for Computing Machinery, Inc, Nov. 2020, pp. 37–45. doi: 10.1145/3416013.3426457.

[49] D. Krstinić, M. Braović, L. Šerić, and D. Božić-Štulić, “Multi-label Classifier Performance Evaluation with Confusion Matrix,” Academy and Industry Research Collaboration Center (AIRCC), Jun. 2020, pp. 01–14. doi: 10.5121/csit.2020.100801.