JUTIS (Jurnal Teknik Informatika Unis)
Vol. 13 No. 2 Bulan November 2025 **p-ISSN: 2252-5351**
Program Studi Teknik Informatika – Fakultas Teknik **e-ISSN: 2656-0860**
Universitas Islam Syekh-Yusuf Tangerang

Deteksi Anomali dan Serangan pada Jaringan Blockchain Menggunakan *Machine Learning* di MATLAB

Rendi Prasetya[1*]
[1]Teknik Informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Indraprasta PGRI, Jl. Raya Tengah No.80 Kel. Gedong Pasar Rebo Jakarta Timur, 13760

*prasetyarendi@gmail.com[1]

Abstrak
Jaringan blockchain, yang mendasari cryptocurrency serta aplikasi terdesentralisasi, sangat rentan terhadap berbagai jenis anomali dan serangan, termasuk serangan 51%, serangan sybil, dan aktivitas bot yang manipulatif. Insiden-insiden ini dapat merusak integritas data, mengganggu konsensus, dan menyebabkan kerugian finansial yang besar (Werbach, 2018). Oleh karena itu, deteksi dini perilaku anomali dalam jaringan blockchain sangat krusial (Ahmed dkk., 2016). Penelitian ini mengusulkan sebuah proses pengidentifikasian anomali dan potensi serangan dalam jaringan blockchain dengan memanfaatkan algoritma machine learning (ML) yang dikembangkan menggunakan MATLAB. Pendekatan ini mencakup pengumpulan data on-chain dan metrik jaringan dari API penjelajah blockchain publik, seperti CoinGecko (CoinGecko API Documentation), diikuti oleh pra-pemrosesan dan ekstraksi fitur untuk menghasilkan indikator relevan terkait perilaku penambang, seperti harga Bitcoin dan volume perdagangan. Penelitian ini menggunakan algoritma unsupervised machine learning, yaitu isolation forest dan One-Class SVM, dengan memanfaatkan MATLAB Statistics and Machine Learning Toolbox. Hasilnya divisualisasikan melalui fasilitas plot MATLAB, yang akan menunjukkan anomali yang terdeteksi dan kemudian membandingkan kinerja dari kedua algoritma tersebut. Dari hasil simulasi yang dilakukan isolation forest berhasil mendeteksi lonjakan signifikan dalam harga dan volume sebagai anomali, sementara One-Class SVM, pada pengaturan yang digunakan, tidak dapat secara visual mengidentifikasi anomali dalam dataset yang digunakan, hal ini mengindikasikan perlunya penyesuaian kembali model dan parameter yang digunakan. Penelitian ini membuktikan bahwa MATLAB dapat digunakan sebagai alat yang sangat efektif untuk analisis data blockchain, dan memungkinkan estimasi awal terhadap terjadinya ancaman keamanan dan kesehatan pada jaringan secara keseluruhan.

Kata kunci: *blockchain, deteksi anomali, , isolation forest, machine learning, one-class svm.*

A. Pendahuluan

Blockchain diperkenalkan oleh Satoshi Nakamoto sebagai sistem uang elektronik *peer-to-peer* yang terdesentralisasi, dikenal sebagai Bitcoin. Blockchain telah mengubah berbagai industri dengan menyediakan sistem penyimpanan dan pertukaran transaksi yang aman, transparan, dan terdesentralisasi (Nakamoto, 2008). Konsep *distributed ledger technology* (DLT) yang diigunakan pada blockcain ini telah diterapkan dalam berbagai hal selain pada mata uang kripto seperti: Bitcoin dan Ethereum.

Menurut Swan (2015), "*Blockchain is a new technology layer that can become the fifth disruptive computing paradigm after mainframes, PCs, the Internet, and mobile/social networking*". Ia menjelaskan bahwa teknologi ini berkembang melalui tiga fase: Blockchain

1.0 (mata uang digital), Blockchain 2.0 (*smart contracts* dan aplikasi keuangan), dan Blockchain 3.0 (aplikasi non-keuangan seperti identitas, voting, dan kesehatan). Ia juga menekankan peran blockchain dalam mentransformasi sistem informasi dan nilai, dengan potensi untuk menciptakan model organisasi tahan sensor dan layanan publik yang lebih efisien. Namun, ia juga mencatat bahwa adopsi teknologi dan penerapan bisnis masih menjadi tantangan utama yang perlu diatasi agar manfaatnya bisa terealisasi secara luas.

Blockchain bukan hanya sekadar teknologi di balik mata uang digital, tetapi merupakan protokol revolusioner yang memungkinkan transaksi yang aman, transparan, dan tahan manipulasi. Terdapat tujuh prinsip desain blockchain—seperti *networked integrity*, *distributed power*, dan *inclusion*—yang diyakini dapat mengubah cara dunia menyimpan dan mentransfer nilai, serta mendisrupsi peran perantara seperti bank dan platform digital. Blockchain juga berpotensi dalam memperkuat hak individu, meningkatkan efisiensi bisnis, dan menciptakan sistem ekonomi yang lebih inklusif dan adil (Tapscott & Tapscott, 2016).

Kekuatan utama blockchain terletak pada sifatnya yang tidak dapat dipalsukan dan dapat diverifikasi, yang dihasilkan melalui skema konsensus dan teknik kriptografi yang canggih. Setiap blok dalam jaringan mencakup hash dari blok sebelumnya, timestamp, dan data transaksi, semua hal tersebut membentuk rantai yang aman dan terverifikasi (Zheng dkk., 2017). Blockchain memungkinkan terciptanya lingkungan digital yang aman dan transparan, di mana pengguna dapat berinteraksi tanpa perlu mengenal atau mempercayai satu sama lain secara langsung. Arsitektur ini menggeser paradigma tradisional yang bergantung pada perantara dan otoritas terpusat, menuju model desentralisasi yang berbasis konsensus dan kriptografi. Hal ini yang menjadi dasar kepercayaan tercipta karena tidak adanya otoritas pusat tunggal yang dapat memanipulasi data (Vujicic, 2018).

Akan tetapi, meskipun inovatif, jaringan blockchain tidak sepenuhnya kebal terhadap berbagai anomali dan serangan yang dapat mengancam penggunaannya, keamanan, dan juga fungsionalitas. Ancaman seperti serangan 51% (di mana satu entitas menguasai mayoritas kekuatan komputasi untuk mengubah riwayat transaksi dan melakukan pengeluaran ganda) (Gervais dkk., 2016), serangan sybil (menggunakan identitas palsu untuk mengontrol jaringan dan mengganggu konsensus), serta perilaku bot dan spam yang merusak dengan membanjiri jaringan dengan transaksi murah, hal ini tentunya dapat menyebabkan kerugian finansial yang besar, hilangnya kepercayaan pengguna, dan juga menghambat adopsi lebih lanjut. Selain itu, Ethereum yang memungkinkan eksekusi kontrak pintar secara otomatis dan transparan, masih terdapat celah keamanan yang dapat dimanfaatkan oleh pihak jahat. Untuk mengatasi hal ini, mereka mengembangkan *Oyente*, sebuah alat eksekusi simbolik yang mampu mendeteksi kerentanan dalam kode kontrak pintar. Dari 19.366 kontrak Ethereum yang dianalisis, Oyente menandai 8.833 di antaranya sebagai rentan, termasuk kontrak TheDAO yang menyebabkan kerugian sebesar 60 juta dolar AS (Luu dkk., 2016). Menurut Atzei dkk. (2017) terdapat beberapa taksonomi kerentanan keamanan dalam *smart contracts* Ethereum, yang mencakup kesalahan pemrograman umum seperti *reentrancy*, *timestamp*

dependence, dan *unhandled exceptions*. Terdapat banyak serangan nyata termasuk pencurian dana jutaan dolar berasal dari kesenjangan antara semantik bahasa *solidity* dan intuisi pengembang. Selain itu, dokumentasi yang tersebar dan kurangnya alat analisis formal turut memperparah risiko keamanan.

Oleh karena itu, deteksi dan pencegahan ancaman tersebut menjadi perhatian utama bagi pengembang dan operator jaringan blockchain. Deteksi anomali adalah bidang yang luas yang bertujuan untuk mengidentifikasi pola yang menyimpang dari perilaku yang diharapkan. Dalam konteks keamanan siber, deteksi anomali memegang peranan penting dalam menemukan intrusi, malware, dan aktivitas mencurigakan lainnya. Ahmed dkk. (2016) menyediakan tinjauan menyeluruh tentang teknik-teknik deteksi anomali dalam sistem deteksi intrusi jaringan. Literatur ini menjadi dasar teoretis untuk penerapan deteksi anomali pada data blockchain. Fawcett (2006) juga memberikan pengantar yang relevan mengenai analisis *receiver operating characteristic* (ROC), yang sering digunakan untuk mengevaluasi efektivitas deteksi anomali. Kebanyakan metode yang ada untuk mendeteksi anomali bersifat berbasis aturan atau menggunakan ambang batas tetap, seperti menandai transaksi yang melebihi nilai tertentu sebagai mencurigakan. Namun, pendekatan ini tidak efektif dalam konteks blockchain karena sifat data yang dinamis dan besar. Karakteristik jaringan dapat berubah seiring waktu, seperti peningkatan volume transaksi dalam pasar bullish atau kemajuan teknologi penambangan yang meningkatkan tingkat hash, sementara strategi serangan baru terus muncul, sehingga diperlukan mekanisme pertahanan yang lebih adaptif dan cerdas.

Dalam konteks ini, algoritma *machine learning* (ML) menawarkan peluang besar untuk menganalisis data kompleks dan mendeteksi pola anomali (Chandola dkk., 2009). Algoritma *machine learning* yang canggih memungkinkan sistem untuk belajar dari data historis dengan membangun model perilaku "normal" dan kemudian mengidentifikasi aktivitas yang menyimpang dari model tersebut sebagai anomali, bahkan jika pola anomali itu sendiri belum pernah terlihat sebelumnya (*anomaly zero-day*). Penggunaan *machine learning* dalam deteksi anomali semakin meningkat, terutama karena kemampuannya dalam mengelola volume data yang besar dan mengidentifikasi pola kompleks yang tidak dapat ditangkap oleh aturan statis (Hastie dkk., 2009a).

Meskipun banyak penelitian telah dilakukan mengenai *machine learning* untuk keamanan siber secara umum (seperti deteksi intrusi jaringan, malware), penerapannya untuk mendeteksi anomali dalam data blockchain on-chain, khususnya dengan menggunakan lingkungan komputasi seperti MATLAB, masih terbatas. Beberapa penelitian menggunakan Python untuk menganalisis data blockchain (Fan dkk., 2020). MATLAB memiliki keunggulan dalam kemampuan komputasi numerik yang kuat, alat machine learning yang komprehensif (misalnya, Statistics and Machine Learning Toolbox), serta kemampuan visualisasi data yang menarik. Lingkungan terintegrasi ini menyediakan kemudahan untuk eksperimen cepat, pemodelan, dan analisis data yang kompleks seperti data blockchain.

Berdasarkan permasalahan tersebut, tujuan dari penelitian ini adalah untuk

mengusulkan model kerangka deteksi anomali dan serangan dalam jaringan blockchain menggunakan MATLAB dengan pendekatan *machine learning*. Melalui kombinasi pengumpulan data dari API penjelajah blockchain publik (pada penelitian ini digunakan CoinGecko), pra-pemrosesan data, rekayasa fitur yang mendalam, dan penerapan model *unsupervised machine learning*. Penelitian ini bertujuan untuk berkontribusi terhadap pengembangan ruang blockchain yang aman dan keandalan ekosistem blockchain.

B. Metode Penelitian

Penelitian ini bertujuan untuk mengusulkan dan menguji kerangka kerja berbasis *machine learning* untuk dapat melakukan deteksi terhadap anomali yang terdapat dalam jaringan blockchain. Metode yang dilakukan pada penelitian terdiri dari beberapa langkah utama, yaitu: Akuisisi Data, Prapemrosesan Data, Rekayasa Fitur, Pemilihan & Pelatihan Model *machine learning*, dan Evaluasi & Visualisasi Hasil.

1. Akuisisi data blockchain

   Tahap ini melibatkan pengumpulan data transaksi blockchain yang relevan serta ukuran jaringan dari sumber publik.

   - Pemilihan sumber data: Pada penelitian ini digunakan data API dari penjelajah blockchain terkemuka untuk mengumpulkan data. Untuk Bitcoin, data historis harga dan volume perdagangan, yang dianggap sebagai indikator aktivitas relevan dan dapat menandakan anomali dalam dinamika ekonomi jaringan. Data ini akan diambil dari API CoinGecko (*CoinGecko API Documentation*). API ini dipilih karena kemudahan akses terhadap data historis tanpa memerlukan kunci API untuk penggunaan dasar dan karena stabilitas endpoint yang telah terbukti.
   - Pengumpulan data: Data diperoleh melalui fungsi *webread* pada MATLAB, yang dapat mengirim permintaan HTTP GET dan menguraikan respons secara otomatis dalam format JSON. Data historis harga dan volume perdagangan harian dikumpulkan selama periode waktu yang panjang (yaitu, 1 tahun). *Timestamp* CoinGecko dalam milisdetik akan dikonversi ke detik dan diubah ke tipe data *datetime* di MATLAB.
   - Pengambilan data historis: Data historis dari *epoch* besar, seperti setiap hari, dapat diekstraksi untuk menangkap pola waktu normal dan, jika ada, data ini akan mencatat peristiwa abnormal seperti volatilitas pasar atau volume perdagangan.

2. Prapemrosesan data

   Data mentah yang diperoleh dari API tersebut tidak selalu cocok untuk *machine learning*, sering kali memerlukan tingkat pemrosesan dan manipulasi.

   - Ekstraksi dan Strukturisasi Data: Respons JSON diekstraksi ke dalam struktur data yang sesuai untuk MATLAB. Informasi disusun menjadi objek tabel yang didukung dalam Tipe Data MATLAB. Kami mengonversi timestamp Unix ke tipe data datetime MATLAB untuk memfasilitasi analisis deret waktu.
   - Pembersihan Data: Proses ini mencakup penanganan nilai yang hilang (misalnya, menghapus baris yang tidak lengkap akibat ketidakcocokan timestamp dalam join luar dengan rmmissing), konversi tipe data (misalnya, mengonversi harga dan

volume ke format numerik), serta penanganan anomali awal yang mungkin disebabkan oleh data atau format yang tidak konsisten.

3. Rekayasa Fitur

   Rekayasa fitur merupakan langkah penting untuk menghasilkan fitur baru dan informatif dari data mentah, guna memudahkan model *machine learning* dalam mendeteksi anomali dengan lebih efektif (Hastie dkk., 2009b)

   - Fitur Berbasis Pasar: Mencakup harga harian Bitcoin (*PriceUSD*) dan volume perdagangan harian (*TotalVolumeUSD*). Varians yang sangat tinggi dari kedua variabel ini merupakan karakteristik dari anomali dalam aktivitas pasar dan kesehatan jaringan.
   - Skala Fitur: Normalisasi *Z-score* diterapkan untuk menskalakan fitur numerik agar tidak ada fitur yang mendominasi bobot dalam pelatihan model hanya karena memiliki nilai yang lebih tinggi. Normalisasi ini penting untuk algoritma berbasis jarak seperti *One-Class SVM*.

4. Pemilihan dan pelatihan model *machine learning*

   Pada fase ini, algoritma untuk deteksi anomali yang telah ditentukan (*isolation forest dan one-class SVM*) akan dilatih dengan data yang telah dipersiapkan pada proses sebelumnya.

   - Pada penelitian digunakan pendekatan *unsupervised*, yaitu: i*solation forest* dan OCSVM (dari *Statistics and Machine Learning Toolbox* pada MATLAB) melalui fungsi *iforest()* dan *fitcsvm()* dengan opsi *OneClass*.
   - Pelatihan Model: Kedua model akan dilakukan proses pelatihan data yang telah dinormalisasi. Parameter *OutlierFraction* (dalam kasus OCSVM) digunakan untuk memperkirakan persentase anomali yang diharapkan dalam data.

     Catatan: Parameter *NumTrees* dihapus dalam kode sumber *iforest* untuk menjaga kompatibilitas dengan berbagai versi MATLAB, sehingga fungsi ini menggunakan jumlah pohon default dari *iforest*.

5. Evaluasi kinerja dan visualisasi

   Pada tahap ini, model yang telah dibuat akan dievaluasi dan divisualisasikan untuk mendeteksi anomali yang kemungkinan terjadi pada data yang digunakan.

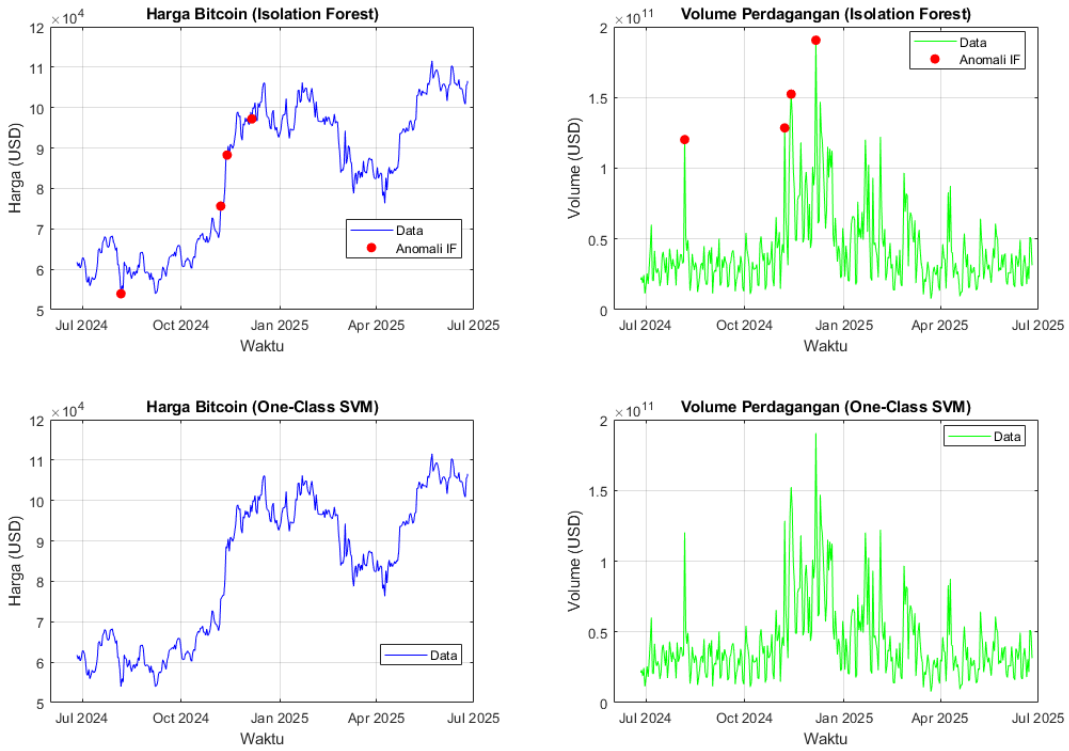
   - Ukuran evaluasi: Dalam konteks deteksi anomali *unsupervised*, evaluasi model dilakukan melalui skor anomali yang dihasilkan. Titik data yang dianggap outlier memiliki skor anomali melebihi ambang batas tertentu (ditentukan oleh persentil skor dan fraksi kontaminasi/outlier yang sudah ditentukan).
   - Visualisasi anomali: MATLAB digunakan untuk memvisualisasikan anomali dengan:
     a. Deret Waktu: Grafik yang menunjukkan tren harga dan volume dari waktu ke waktu. Anomali yang diidentifikasi oleh masing-masing model akan ditandai dengan warna yang berbeda (merah untuk *isolation forest*, magenta untuk OCSVM) dan disajikan dalam satu grafik agar dapat membandingkan secara langsung hasil dari kedua algoritma tersebut.

p-ISSN: 2252-5351
e-ISSN: 2656-0860

b. Plot Perbandingan: Untuk menunjukkan perbandingan antara *isolation forest* dan *One-Class SVM* dengan *PricesUSD* dan *TotalVolumeUSD*, empat subplot digunakan untuk menyampaikan perbandingan secara keseluruhan.

C. Hasil dan Pembahasan

Melalui proses pengumpulan data, pra-pemrosesan, rekayasa fitur, pelatihan model, dan evaluasi, sistem deteksi anomali yang dibuat pada penelitian berhasil mengidentifikasi beberapa pola yang mencolok dari operasi reguler jaringan blockchain berdasarkan entitas harga dan volume perdagangan pada mata uang kripto GeckoCoin (dapat dilihat pada Gambar 1).

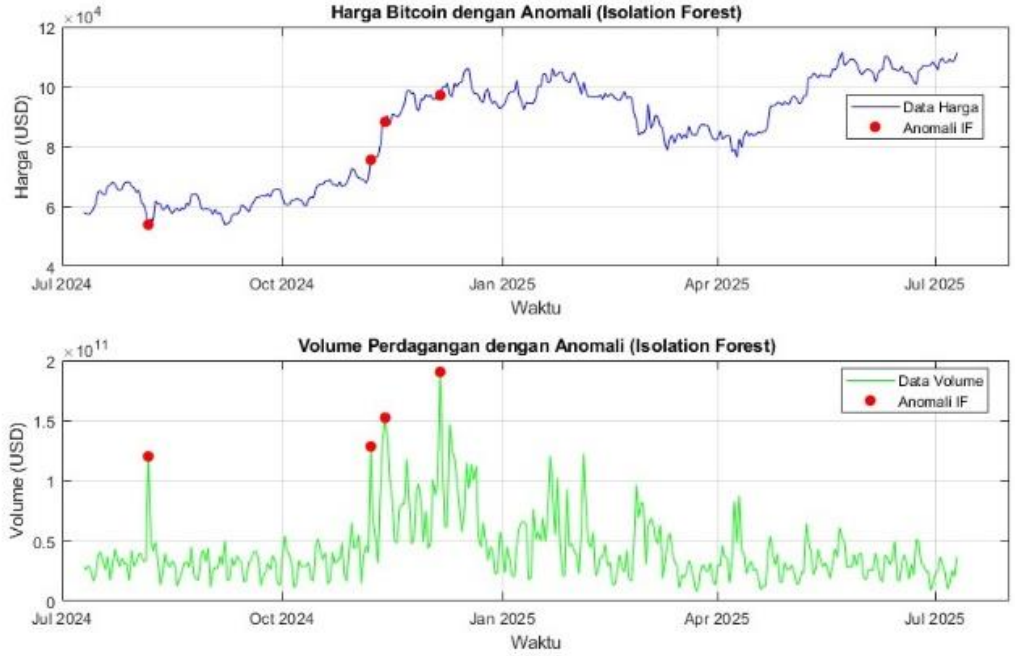


Gambar 1. Perbandingan Deteksi Anomali Bitcoin: *Isolation forest* dan *One-Class SVM* (Data Harga & Volume)

1. Hasil deteksi anomali

1.1. Deteksi anomali dengan *isolation forest*

Dalam grafik harga Bitcoin (Gambar 2), model *isolation forest* berhasil mengidentifikasi adanya anomali, yang ditandai dengan lingkaran merah. Anomali ini muncul dalam periode dengan fluktuasi besar dalam harga Bitcoin. Sebagai contoh, sekelompok anomali terdeteksi sekitar akhir 2024 dan awal 2025, saat terjadi lonjakan harga pasar yang signifikan, hal ini menunjukkan kemampuan dari algoritma *isolation forest* dalam mengidentifikasi outlier yang "terisolasi" dari pola harga normal.



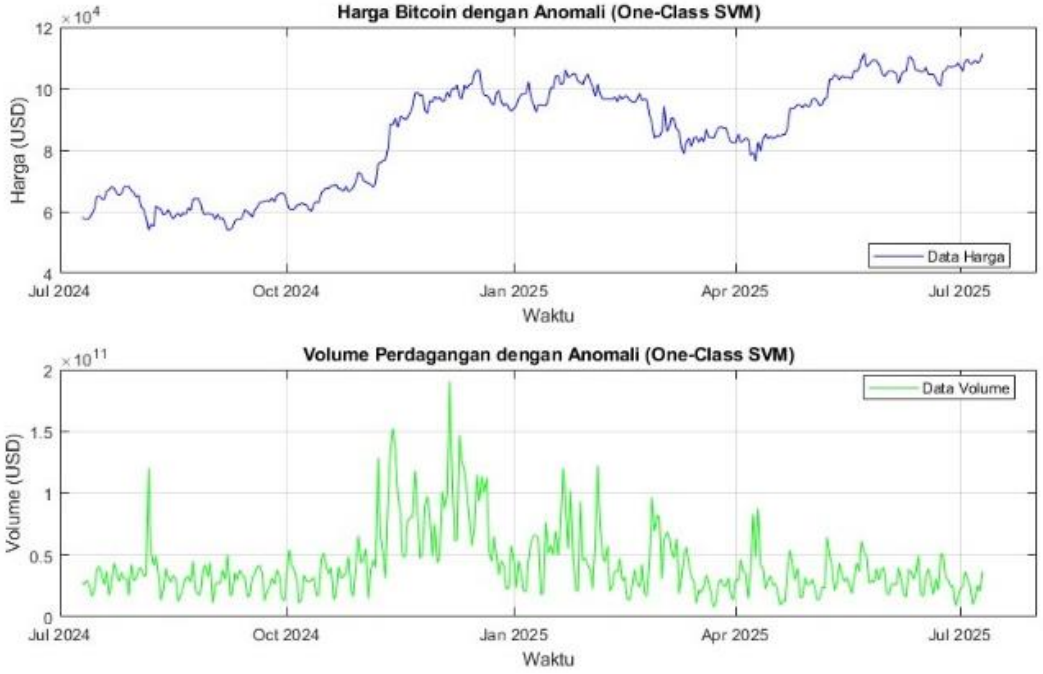
Gambar 2. Deteksi anomali bitcoin menggunakan *isolation forest*

Dalam grafik harga Bitcoin (Gambar 2), model *isolation forest* berhasil mengidentifikasi adanya anomali, yang ditandai dengan lingkaran merah. Anomali ini muncul dalam periode dengan fluktuasi besar dalam harga Bitcoin. Sebagai contoh, sekelompok anomali terdeteksi sekitar akhir 2024 dan awal 2025, saat terjadi lonjakan harga pasar yang signifikan, hal ini menunjukkan kemampuan dari algoritma *isolation forest* dalam mengidentifikasi outlier yang "terisolasi" dari pola harga normal.

Dalam grafik volume perdagangan pun, *isolation forest* menangkap beberapa anomali yang ditandai dengan lingkaran merah. Anomali ini sesuai dengan puncak volume perdagangan yang sangat tinggi melebihi rata-rata harian. Lonjakan volume yang tinggi ini dapat mengindikasikan adanya ketidaknormalan yang terjadi pada pasar, seperti akumulasi atau distribusi massal yang berpotensi mengubah arah harga.

1.2. Deteksi anomali dengan *one-class SVM* (OCSVM)

Dalam grafik harga Bitcoin (Gambar 3), tidak ada titik anomali yang terdeteksi menggunakan *One-Class SVM* (tidak ada lingkaran magenta). Ini menunjukkan bahwa, berdasarkan pengaturan saat ini, tidak ada titik yang diklasifikasikan sebagai anomali untuk fitur harga. Begitu pula dalam grafik volume perdagangan, tidak ada titik anomali yang terdeteksi oleh *One-Class SVM*, dengan grafik yang terlihat hanya menampilkan "Data." Hal ini menunjukkan bahwa OCSVM tidak dapat mendeteksi anomali pada fitur volume dengan pengaturan saat ini.



Gambar 3. Deteksi anomali bitcoin menggunakan *One-Class SVM*

Visualisasi ini menunjukkan karakteristik yang berbeda antara *isolation forest* dan *One-Class SVM* dalam mendeteksi anomali pada dataset yang sama. *Isolation forest* lebih efektif dalam mendeteksi outlier yang secara topologis "terisolasi" dari data normal. Algoritma ini bekerja dengan membangun pohon keputusan dari data dengan partisi acak, di mana outlier biasanya memerlukan jalur partisi yang lebih pendek untuk dipisahkan dari mayoritas data. Ini membuatnya lebih responsif terhadap lonjakan atau penurunan yang tajam, seperti fluktuasi harga dan volume.

Sebaliknya, *One-Class SVM* berusaha menemukan *hyperplane optimal* yang memisahkan sebagian besar data normal dari titik asal (titik nol) dalam ruang fitur, atau dengan kata lain mendekati batas di mana data "normal" berada. Semua titik di luar batas ini dianggap sebagai anomali. Ketidakmampuan OCSVM untuk mendeteksi anomali dalam plot menunjukkan beberapa kemungkinan:

- Parameter *OutlierFraction*: Nilai *OutlierFraction* yang ditetapkan mungkin terlalu rendah untuk dataset ini. Distribusi skor anomali OCSVM mungkin tidak cukup terpisah untuk mendefinisikan ambang batas yang dapat mengidentifikasi titik-titik yang terlihat jelas sebagai outlier. Meskipun model ini dirancang untuk mendeteksi 1% anomali, jika data "normal" memiliki varians tinggi atau jika model tidak menemukan pemisahan yang jelas, model ini mungkin tidak cukup agresif dalam menilai titik-titik sebagai anomali berdasarkan ambang batas yang ditetapkan secara otomatis.
- Parameter *KernelScale* dan *KernelFunction*: Parameter kernel RBF berusaha menentukan skala yang sesuai secara otomatis, namun hal ini dapat menghasilkan batas keputusan yang terlalu "longgar," sehingga mencakup sebagian besar titik sebagai normal. Penyetelan manual *KernelScale* mungkin diperlukan untuk meningkatkan sensitivitas OCSVM.

- Sifat anomali: Dataset ini mungkin memiliki jenis anomali yang lebih mudah ditemukan oleh pendekatan "isolasi" dibandingkan dengan pendekatan "batas," terutama jika data "normal" juga memiliki penyebaran yang besar.

Dari hasil yang didapatkan pada penelitian ini menunjukkan bahwa MATLAB dapat berfungsi sebagai platform yang berpotensi untuk membangun deteksi anomali berbasis *machine learning* dalam konteks blockchain menggunakan metrik data pasar yang tersedia secara publik. Nilai utama dari penelitian ini adalah menunjukkan kerangka kerja yang dapat diskalakan untuk menangani data transaksi keuangan yang dinamis dalam blockchain.

Perluasan yang disarankan untuk penelitian lebih lanjut mencakup eksplorasi ketergantungan temporal yang lebih kompleks dalam deret waktu melalui integrasi model pembelajaran mendalam dengan *MATLAB®'s Deep Learning Toolbox*. Pembangunan platform deteksi waktu nyata dengan aliran data juga akan menjadi langkah maju yang signifikan. Selain itu, pendekatan pembelajaran transfer yang lebih canggih, atau penggabungan prediksi dari model anomali yang berbeda, dapat meningkatkan akurasi. Terakhir, integrasi dengan penyedia data on-chain yang lebih mendalam untuk mengakses data yang lebih rinci seperti aktivitas alamat, pergerakan paus, dan perilaku penambang dapat memberikan prospek untuk deteksi anomali yang lebih tepat dan relevan terkait keamanan jaringan inti.

D. Kesimpulan

Penelitian ini telah menunjukkan adanya mekanisme yang efisien untuk mendeteksi sebuah anomali terkait data historis Bitcoin melalui aplikasi yang berbasis *machine learning* menggunakan MATLAB. Dengan menggunakan informasi dari API CoinGecko, pada penelitian ini dikembangkan profil perilaku pasar 'normal' dan menganggap anomali sebagai sesuatu yang berbeda secara signifikan dari profil ini.

Metodologi sistematis, yang mencakup pengumpulan data yang akurat, pra-pemrosesan (termasuk normalisasi fitur), hingga penggunaan model *unsupervised machine learning* (*isolation forest* dan *One-Class SVM*) terbukti sebagai faktor kunci. Kedua algoritma ini, ketika diterapkan dapat menunjukkan kemampuan yang kuat dalam mengidentifikasi penyimpangan dari norma tanpa memerlukan data anomali berlabel, yang sangat penting dalam konteks pasar kripto yang dinamis.

Dari hasil penelitian, kami menyimpulkan bahwa *isolation forest* efektif dalam mendeteksi pergerakan harga dan volume yang signifikan sebagai anomali. Sebaliknya, *one-class SVM* dengan pengaturan yang ada saat ini secara visual tidak dapat mengidentifikasi anomali dalam dataset ini, hal ini menunjukkan kebutuhan untuk melakukan penyesuaian parameter yang lebih hati-hati. Ini juga menegaskan bahwa tidak ada solusi tunggal yang cocok untuk semua, dan perbandingan kinerja antar model adalah aspek krusial dalam membangun sistem deteksi yang efektif.

Meskipun penelitian ini dibatasi oleh ketersediaan data on-chain yang granular di

sumber publik dan penyesuaian parameter model, hasilnya sekali lagi menunjukkan kekuatan dan fleksibilitas MATLAB sebagai platform analitik untuk data blockchain. Nilai utama dari penelitian ini adalah menyajikan metodologi yang realistis untuk memantau kesehatan dan integritas pasar blockchain, serta membuka jalan untuk desain sistem keamanan dan pemantauan pasar yang lebih proaktif dan adaptif di masa mendatang.

Daftar Pustaka

Ahmed, M., Naser Mahmood, A., & Hu, J. (2016). A survey of network anomaly detection techniques. Dalam *Journal of Network and Computer Applications* (Vol. 60, hlm. 19–31). Academic Press. https://doi.org/10.1016/j.jnca.2015.11.016

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A Survey of Attacks on Ethereum Smart Contracts (SoK). Dalam M. Maffei & M. Ryan (Ed.), *Principles of Security and Trust* (hlm. 164–186). Springer Berlin Heidelberg.

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Comput. Surv.*, *41*(3). https://doi.org/10.1145/1541880.1541882

Fan, J., Cai, Y., Li, G., Xu, Z., & Gao, D. (2020). Blockchain Transaction Analysis for Anomaly Detection. *Proceedings of the 2020 5th International Conference on Computing and Communications (ICCC)*, 381–385. https://doi.org/10.1109/ICCC51575.2020.9345036

Fawcett, T. (2006). An introduction to ROC analysis. *Pattern Recognition Letters*, *27*(8), 861–874. https://doi.org/https://doi.org/10.1016/j.patrec.2005.10.010

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the Security and Performance of Proof of Work Blockchains. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 3–16. https://doi.org/10.1145/2976749.2978341

Hastie, T., Tibshirani, R., & Friedman, J. (2009a). *The Elements of Statistical Learning: Data Mining, Inference, and Prediction* (2nd ed.). Springer.

Hastie, T., Tibshirani, R., & Friedman, J. (2009b). *The Elements of Statistical Learning: Data Mining, Inference, and Prediction, Second Edition*. Springer New York. https://books.google.co.id/books?id=tVIjmNS3Ob8C

Luu, L., Chu, D.-H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making Smart Contracts Smarter. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 254–269. https://doi.org/10.1145/2976749.2978309

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. www.bitcoin.org

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media, Incorporated. https://books.google.co.id/books?id=RHJmBgAAQBAJ

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Penguin Publishing Group.

https://books.google.co.id/books?id=NqBiCgAAQBAJ

Vujicic, D. (2018). The blockchain and new architecture of trust. *Strategic Solutions*, *2*(1), 1–13.

Werbach, K. (2018). *The Blockchain and the New Architecture of Trust*. The MIT Press. https://doi.org/10.7551/mitpress/11449.001.0001

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85