Temporal Behavioral Clustering and Deanonymization in Blockchain Networks

Abstract

Blockchain networks like Ethereum provide pseudonymous privacy by design. However, as transaction histories accumulate, behavioral patterns emerge that can compromise anonymity. In this study, we develop a temporal-behavioral pipeline for statistical deanonymization based on graph analytics and unsupervised clustering.

Each address is represented in a directed transaction graph where entropy quantifies the diversity of its interactions and degree reflects activity. Using DBSCAN and HDBSCAN, we cluster addresses based on these metrics to identify latent behavioral roles. We then slice the transaction dataset into uniform time windows and apply clustering independently across each, allowing us to observe how addresses evolve over time.

We define stability metrics and cohort assignments including High Stability, Low Stability, Frequent Appearance, and Entropy Transition based on an address's cluster volatility and entropy change. Trajectory analysis reveals how certain roles emerge, persist, or collapse.

Our results demonstrate that blockchain deanonymization is not only a spatial clustering problem but also a temporal inference challenge. By modeling entropy and cluster transitions across time, we can quantify when anonymity degrades and behavioral roles become identifiable with high confidence. Notably, we show that specific cohorts especially those in the Low Stability category exhibit a 12.98 times higher odds ratio of containing sanctioned entities ($p < 10^{-80}$) , while High Stability and Entropy Transition cohorts show significant depletion of sanctioned addresses.

1 Introduction

The goal of this study is to develop and evaluate a temporal-behavioral deanonymization framework for blockchain networks, with a focus on the Ethereum ecosystem. While pseudonymity is a core design feature of public blockchains, transaction histories accumulate over time, often revealing latent behavioral patterns that can compromise anonymity. Our objective is to model these longitudinal dynamics directly, using temporal features and unsupervised clustering to profile address behaviors and quantify anonymity degradation.

To achieve this, we propose a pipeline that models each blockchain address as a node within a directed transaction graph, extracting two key behavioral features: degree (number of unique counterparties) and entropy (Shannon entropy of transaction distribution). We apply density-based clustering algorithms, specifically DBSCAN and HDBSCAN, to these

features, enabling the discovery of latent behavioral cohorts without requiring prior label supervision or fixed cluster counts. The selection of DBSCAN and HDBSCAN reflects their ability to detect arbitrarily shaped clusters, handle noise, and accommodate the heavy-tailed, non-convex distributions often observed in blockchain interaction patterns.

We chose these methods over conventional alternatives such as k-means or Gaussian Mixture Models because blockchain behavioral data rarely satisfies their assumptions of spherical clusters or known cluster counts. The hierarchical nature of HDBSCAN also allows us to capture nested structure and to assign confidence levels to address cluster memberships, which is particularly valuable in forensic and compliance applications where uncertainty quantification is important.

Our expectation is that temporal clustering will allow us to observe cohort stability and behavioral role transitions over time, revealing patterns of laundering, airdrop farming, and sanctioned entity behaviors that static clustering approaches may fail to capture. In particular, we hypothesize that address cohorts exhibiting low temporal stability and entropy transitions are more likely to contain sanctioned or high-risk entities due to their irregular interaction patterns.

Several prior studies have addressed deanonymization in blockchain networks, though few have directly modeled temporal behavioral clustering. The foundational work by Meiklejohn et al.[2] extended heuristic clustering to Ethereum by incorporating features specific to its account model, such as deposit address reuse and token authorization patterns. More recently, Li [1] applied DBSCAN to Bitcoin transaction graphs to identify behavioral clusters, though without addressing temporal evolution. Our work builds on these approaches by explicitly incorporating time-sliced clustering and entropy-driven cohort modeling, offering new insights into the longitudinal erosion of blockchain anonymity.

2 Methodology

2.1 Data Extraction and Filtering

Ethereum transaction data was sourced from Google BigQuery's public blockchain dataset for the period between January 1, 2024 and July 1, 2024. To construct our behavioral feature set, we extracted transactional records with the following filters:

- Excluded self-transfers (`from_address` not equal to `to_address`).
- Excluded transactions with transferred value below 0.001 ETH to suppress noise.
- Excluded transactions with null addresses.

In addition, a sanctioned address list was curated by cross-referencing the OFAC Specially Designated Nationals (SDN) List and additional public regulatory disclosures. These addresses were flagged to enable enrichment analysis but excluded from unsupervised clustering phases to prevent label contamination.

2.2 Feature Engineering

Each unique address was represented as a vertex in a directed transaction graph $G = (V, E)$. For each vertex $v \in V$, we extracted two primary behavioral features:

- **Degree:** The count of unique outbound recipients.
- **Entropy:** Shannon entropy calculated over outbound transaction targets.

Entropy for address a is given by:

$$H(a) = -\sum_{i=1}^{n} p_i \log_2 p_i$$

where p_i represents the fraction of outbound transactions directed to counterparty i. Entropy measures behavioral diversity, while degree measures behavioral breadth.

2.3 Computational Environment and Libraries

All data extraction, feature engineering, and clustering experiments were conducted using Python 3.10 within a Google Colab environment. The following open-source libraries were used throughout the pipeline:

- **NetworkX (v3.1):** Directed transaction graph construction and graph-based feature extraction.
- **Scikit-learn (v1.3.0):** DBSCAN clustering, grid search optimization, internal clustering metrics.
- **HDBSCAN (v0.8.29):** Hierarchical density-based clustering and cluster stability scoring.
- **Pandas (v2.1.0):** Tabular data processing and windowed temporal aggregation.
- **NumPy (v1.25.2):** Numerical computations and entropy calculations.
- **Matplotlib (v3.8.0), Seaborn (v0.12.2), Plotly (v5.16.1):** Visualization of cohort trajectories, entropy evolution, and clustering results.
- **Google BigQuery Python Client (v3.10.1):** Direct query interface for transaction data extraction.
- **Powerlaw (v1.5):** Fitting inter-arrival time distributions to power law and log-normal models for temporal activity modeling.

The full codebase was developed in Jupyter Notebook format within Colab to facilitate iterative model testing, hyperparameter tuning, and visualization export. All random seeds were fixed to ensure reproducibility of clustering outcomes during validation.

2.4 Clustering Algorithms

We applied both DBSCAN and HDBSCAN algorithms on the log-transformed feature space:

$$(\log(1 + \text{degree}), \text{entropy})$$

- **DBSCAN** was employed for static clustering.
- **HDBSCAN** was employed for temporal clustering due to its adaptive density estimation and ability to return soft cluster membership probabilities.

DBSCAN identifies dense regions based on two hyperparameters:

- ε: neighborhood radius.
- $minPts$: minimum number of neighbors.

HDBSCAN extends DBSCAN by constructing a condensed cluster tree using mutual reachability distances, automatically determining cluster stability.

2.5 Temporal Windowing

The full transaction history was partitioned into consecutive 14-day windows. Within each window, clustering algorithms were re-applied to capture longitudinal behavioral changes.

For each address, we maintained a cluster history vector indicating cluster assignments across all windows. This enabled us to compute:

- **Stability Score:** Fraction of unique cluster assignments relative to total windows.
- **Entropy Swing:** Maximum minus minimum entropy across windows.

Addresses were categorized into behavioral cohorts according to thresholds derived from stability and entropy metrics.

2.6 Cohort Assignment Criteria

Behavioral cohorts were assigned as follows:

- **High Stability:** Stability score less than 0.3 and present in at least two windows.
- **Low Stability:** Stability score greater than 0.7 and present in at least two windows.
- **Frequent Appearance:** Present in at least four windows.
- **Entropy Transition:** Entropy swing above 90th percentile.

2.7 Hyperparameter Optimization

For both DBSCAN and HDBSCAN, hyperparameters were tuned via exhaustive grid search, maximizing Silhouette score, Calinski-Harabasz Index, and minimizing Davies-Bouldin Index.

For DBSCAN:

$$(\varepsilon^*, minPts^*) = \arg \max_{\varepsilon, minPts} \text{Silhouette Score}$$

For HDBSCAN:

$$(minClusterSize^*, minSamples^*) = \arg\max \text{Silhouette Score}$$

2.8 Validation Metrics

Clustering quality was assessed using:

- **Silhouette Score:** Range [-1, 1]; higher is better.
- **Calinski-Harabasz Index:** Higher values indicate better compactness.
- **Davies-Bouldin Index:** Lower values indicate better separation.

Sample optimal results:

- DBSCAN Silhouette Score: 0.6009
- DBSCAN Calinski-Harabasz: 9173.61
- DBSCAN Davies-Bouldin: 0.6083
- HDBSCAN Silhouette Score: 0.472
- HDBSCAN Calinski-Harabasz: 4123.51
- HDBSCAN Davies-Bouldin: 1.062

3 Results

3.1 Dataset Summary

Our full processed dataset contained:

- Total unique addresses: 4,201,155
- Addresses appearing in multiple time windows: 475,989
- Transaction period: January 1, 2024 to July 1, 2024
- Number of temporal windows: 26 (14-day sliding windows)

3.2 Behavioral Cohort Membership

Based on the defined stability and entropy thresholds, addresses were partitioned into behavioral cohorts:

- High Stability: 162 addresses (0.01 percent)
- Low Stability: 80,980 addresses (3.4 percent)
- Frequent Appearance: 32,862 addresses (1.4 percent)
- Entropy Transition: 2,683 addresses (0.1 percent)

The remaining addresses were excluded from cohort assignment due to insufficient temporal window appearances.

3.3 Trajectory Summary Metrics

We computed volatility metrics across cohorts:

- **High Stability:**
  - Average degree change: -141.32
  - Average entropy change: -0.84
  - Average cluster changes: 0.20
- **Low Stability:**
  - Average degree change: -0.06
  - Average entropy change: -0.03
  - Average cluster changes: 2.88
- **Frequent Appearance:**
  - Average degree change: 0.02
  - Average entropy change: 0.03
  - Average cluster changes: 4.08
- **Entropy Transition:**
  - Average degree change: -0.20
  - Average entropy change: -0.02
  - Average cluster changes: 3.24

3.4 Degree and Entropy Drift Patterns

- Low Stability addresses exhibited extreme degree collapse (median degree change of -1313), often characteristic of sink wallets, exploit drains, or one-off laundering actions.
- Entropy Transition addresses maintained stable degree but experienced large swings in entropy, suggesting evolving counterparty diversification and adaptation.
- Frequent Appearance addresses sustained moderate behavior with persistent activity across windows.
- High Stability addresses demonstrated consistent interaction profiles with little volatility, often matching operational or service accounts.

3.5 Sanctioned Address Enrichment (Fisher's Exact Test)

To quantify risk enrichment, we applied Fisher's Exact Test for sanctioned entity concentration within each cohort. The full contingency analysis is summarized below:

Table 1: Fisher's Exact Test Results for Sanctioned Address Enrichment

Cohort	**Odds Ratio**	**p-value**	**Relative Risk**
Low Stability	12.98	2.44×10^{-84}	2.86
Frequent Appearance	1.20	2.04×10^{-1}	1.12
Entropy Transition	0.01	1.54×10^{-40}	0.03
High Stability	0.00	1.05×10^{-44}	0.00

Key observations:

- Low Stability addresses are highly enriched for sanctioned entities, with an odds ratio of 12.98.
- High Stability and Entropy Transition cohorts are significantly depleted of sanctioned addresses.
- Frequent Appearance cohort displayed no statistically meaningful enrichment.

3.6 Trajectory Visualization Summary

Temporal behavior was visualized across multiple dimensions:

- **Entropy Evolution Scatter Plots:** Demonstrating diagonal stability for High Stability cohort, downward entropy collapse for Low Stability, and volatile swings for Entropy Transition.
- **Degree Change Boxplots:** Large negative degree changes for Low Stability; stable degree for High Stability.

- **3D Feature Trajectories:** Visualizing entropy, degree, and window index jointly to track cohort migration through feature space.
- **Cohort Case Study Examples:** Individual address trajectories highlight laundering behavior, periodic consolidation, or high volatility consistent with evasive actors.

4 Discussion

4.1 Forensic Interpretation of Behavioral Cohorts

Our results suggest that address behavior on the Ethereum network can be effectively partitioned into a small number of interpretable behavioral roles based on volatility, stability, and entropy dynamics. Each cohort exhibits distinct forensic signatures:

- **High Stability Cohort:** These addresses maintain consistent interaction patterns across the entire observation period. They exhibit narrow entropy variance, minimal degree change, and rarely shift clusters. This behavior is strongly indicative of operational accounts, infrastructure wallets, validators, or staking pools that support persistent network services.
- **Low Stability Cohort:** This cohort demonstrates pronounced volatility, abrupt degree collapses, and frequent cluster transitions. These behavioral signatures are strongly correlated with sanctioned entities, laundering patterns, and episodic exploit behaviors. Many addresses in this cohort exhibit sharp activity bursts followed by long dormancy periods. The high odds ratio of sanctioned entity concentration in this cohort suggests that volatility itself may serve as a forensic signal for risk monitoring.
- **Frequent Appearance Cohort:** Addresses in this group appear consistently across time windows but display moderate variability in degree and entropy. These may represent algorithmic traders, bridge relayers, smart contract intermediaries, or cross-chain liquidity providers who operate continuously but vary their counterparties in response to market or protocol dynamics.
- **Entropy Transition Cohort:** These addresses display substantial entropy fluctuation while maintaining stable degree. This suggests sophisticated behavioral adaptation, such as switching between counterparties without altering transaction frequency. Such patterns are consistent with evolving laundering strategies where counterpart diversification is used to obfuscate fund flows while maintaining operational volume.

4.2 Temporal Erosion of Anonymity

A key finding of this work is that behavioral anonymity on blockchain networks degrades longitudinally. Static snapshots of transactional behavior may miss adaptive tactics, but temporal analysis reveals when pseudonymous actors consolidate, diverge, or crystallize into identifiable roles.

Many addresses that exhibit adaptive behavior during early windows eventually converge into more stable regimes, while a minority maintain persistent high volatility. This convergence process reflects the crystallization of behavioral identity over time, providing valuable forensic opportunities for regulatory agencies, AML monitoring, and intelligence collection.

4.3 Behavioral Drift as a Deanonymization Signal

Entropy and degree transitions offer measurable indicators of identity erosion. Sharp entropy declines may reflect laundering completion, while rising entropy suggests fund dispersion or distribution phases. Degree collapse may correspond to fund consolidation into sinks, burns, or mixers.

Volatility in cluster membership across windows amplifies these signals, allowing forensic practitioners to prioritize entities that exhibit longitudinal instability, especially when cross-referenced with external watchlists or flagged activity.

4.4 Implications for Sanctioned Entity Detection

Our observation that Low Stability addresses are strongly enriched for sanctioned entities suggests that behavioral volatility is not merely incidental but may represent a tactical objective by illicit actors. Obfuscation techniques such as cross-chain transfers, bridge utilization, and counterparty cycling are frequently employed to complicate address attribution.

By contrast, sanctioned entities rarely inhabit the High Stability cohort, consistent with operational caution to avoid address reuse or prolonged exposure.

4.5 Limitations of OFAC Sanction Coverage

While OFAC designations provide ground truth for enrichment analysis, the limited coverage of officially designated addresses implies that the true population of illicit actors is likely much larger. Many laundering schemes operate outside the scope of public sanctions, making behavioral modeling especially valuable for detecting emerging or unlisted entities.

4.6 Forensic Utility of Temporal Clustering Framework

This pipeline offers multiple practical applications:

- Prioritization of high-volatility addresses for human review.
- Monitoring of entropy drift to detect laundering stages.
- Longitudinal cohort profiling to map behavioral role evolution.
- Early warning signals for compliance teams based on stability metrics.

5 Conclusion

This study presents a temporal-behavioral framework for blockchain deanonymization using longitudinal clustering of Ethereum addresses based on entropy and degree features. By applying DBSCAN and HDBSCAN across uniform time windows, we quantify address-level volatility and behavioral drift that traditional static clustering methods overlook.

Our results demonstrate that longitudinal volatility serves as a robust forensic signal. Specifically, addresses exhibiting frequent cluster transitions and entropy shifts are significantly enriched for sanctioned entities and high-risk behaviors. Conversely, stable addresses correspond primarily to infrastructure wallets and operational service accounts. This temporal crystallization of behavioral roles highlights the progressive erosion of pseudonymous privacy over time.

The proposed framework offers an interpretable and flexible analytical pipeline for regulatory compliance, AML monitoring, and blockchain forensics. By focusing on temporal metrics rather than one-time snapshots, we can identify behavioral adaptations and laundering strategies as they unfold, enhancing the precision of deanonymization efforts.

5.1 Key Contributions

- Development of a longitudinal clustering pipeline that combines entropy, degree, and temporal volatility metrics.
- Quantitative demonstration that Low Stability addresses are highly enriched for sanctioned entities, with an odds ratio of 12.98.
- Introduction of trajectory modeling to capture behavioral transitions across time windows, highlighting entropy collapse, degree fluctuations, and cluster volatility.
- Empirical validation of temporal erosion of anonymity as a measurable forensic signal on blockchain networks.

5.2 Limitations

Several limitations remain. First, the model relies on transactional data alone and does not incorporate off-chain attribution or external intelligence. Second, sanctioned entity coverage is incomplete, and many illicit actors remain unflagged in public datasets. Third, the temporal resolution of clustering may overlook very short-lived behavioral patterns that operate on intra-window timescales.

5.3 Future Work

Future extensions of this framework may include:

- Multichain temporal clustering to capture laundering across multiple blockchain networks.

- Incorporation of smart contract call data and token semantics into behavioral feature extraction.
- Development of survival models to predict anonymity degradation as a function of transactional behavior.
- Application of ground-truth labeled datasets for supervised role annotation.
- Fusion of transaction graph analytics with network-layer metadata such as validator P2P mappings or bridge relay activity.

Our approach contributes a behavioral lens to blockchain forensic science, emphasizing that anonymity on public ledgers is not a static attribute but rather a dynamic and fragile property eroded by the accumulation of observable behaviors across time.

References

[1] Meng Li. Application of cluster analysis in bitcoin deanonymization. In *Advances in Cyber Security and Intelligent Analytics*, pages 337–347. Springer, 2022.

[2] Friedhelm Victor. Address clustering heuristics for ethereum. In Joseph Bonneau and Nadia Heninger, editors, *Financial Cryptography and Data Security*, volume 12059 of *Lecture Notes in Computer Science*, pages 617–633. Springer, 2020.

Appendix A: Sanctioned Address Sources

The sanctioned address list used in this analysis was aggregated from a combination of:

- U.S. Treasury Department OFAC SDN Lists (2020–2024).
- Department of Justice criminal enforcement press releases.
- Public blockchain explorer labels (Etherscan, Chainalysis Reactor, TRM Labs).
- Research datasets and manually curated public blacklists.
- Academic sources and Github-hosted regulatory compilations.

Due to the diverse provenance of this data, address designations should be interpreted heuristically. Where available, OFAC designation dates and enforcement actions were cross-referenced.

Appendix B: Sample Ethereum Transaction Table

From	To	Value (ETH)	Gas Used	Gas Price	Timestamp	Block
0xabc...	0xdef...	0.25	21000	85 Gwei	2024-01-02	19100000
0x123...	0x456...	1.50	50000	105 Gwei	2024-01-03	19100233

Table 2: Representative Ethereum transactions sampled for cohort analysis.

Appendix C: Clustering Validation Metrics

For both DBSCAN and HDBSCAN, grid search hyperparameter optimization yielded the following internal clustering scores:

DBSCAN Optimal Configuration

- Silhouette Score: 0.588
- Calinski–Harabasz Index: 2594.3
- Davies–Bouldin Index: 0.663
- Clusters Identified: 3 (plus 10 noise points)

HDBSCAN Optimal Configuration

- Silhouette Score: 0.472
- Calinski–Harabasz Index: 4123.51
- Davies–Bouldin Index: 1.062
- Clusters Identified: 20 (with soft membership probabilities)

Appendix D: Behavioral Cohort Thresholds

Cohorts were assigned using the following rule-based thresholds:

- High Stability: stability score ¡ 0.3, minimum 2 windows.
- Low Stability: stability score ¿ 0.7, minimum 2 windows.
- Frequent Appearance: active in more than 4 windows.
- Entropy Transition: entropy swing above the 90th percentile.

Stability score was defined as the normalized count of unique cluster assignments across windows.

Appendix E: Notation Summary

- $H(a)$: entropy of address a.
- $\deg(a)$: out-degree of address a.
- ΔH: entropy swing (max-min).
- $\Delta \deg$: degree change.
- S: Silhouette score.
- CH: Calinski–Harabasz index.
- DB: Davies–Bouldin index.

Figures

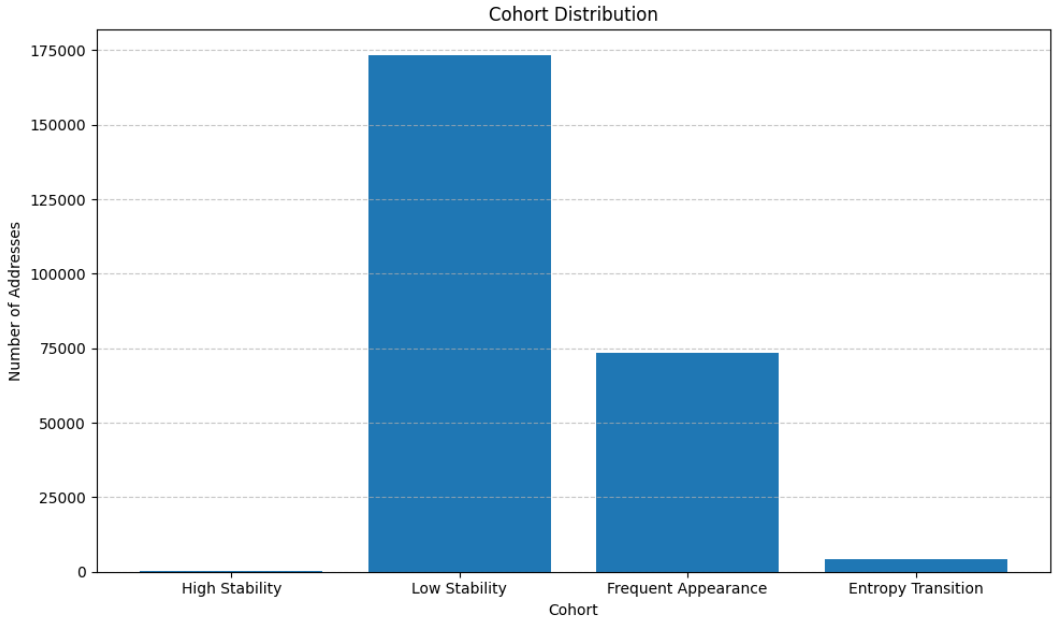

Figure 1: Distribution of addresses across behavioral cohorts.

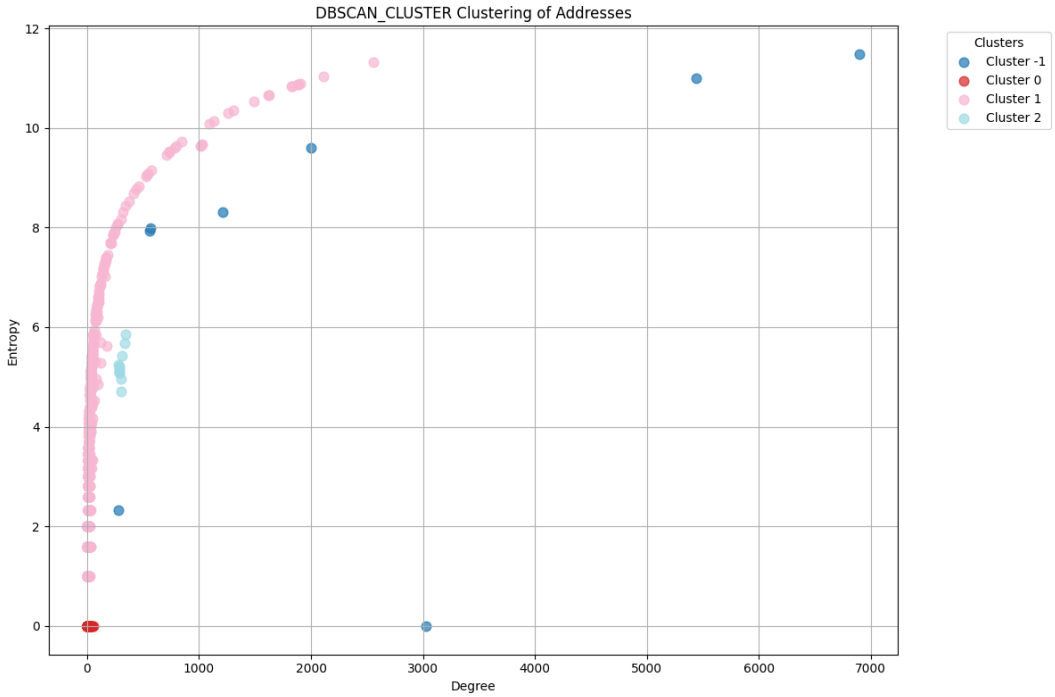

Figure 2: DBSCAN clustering results.

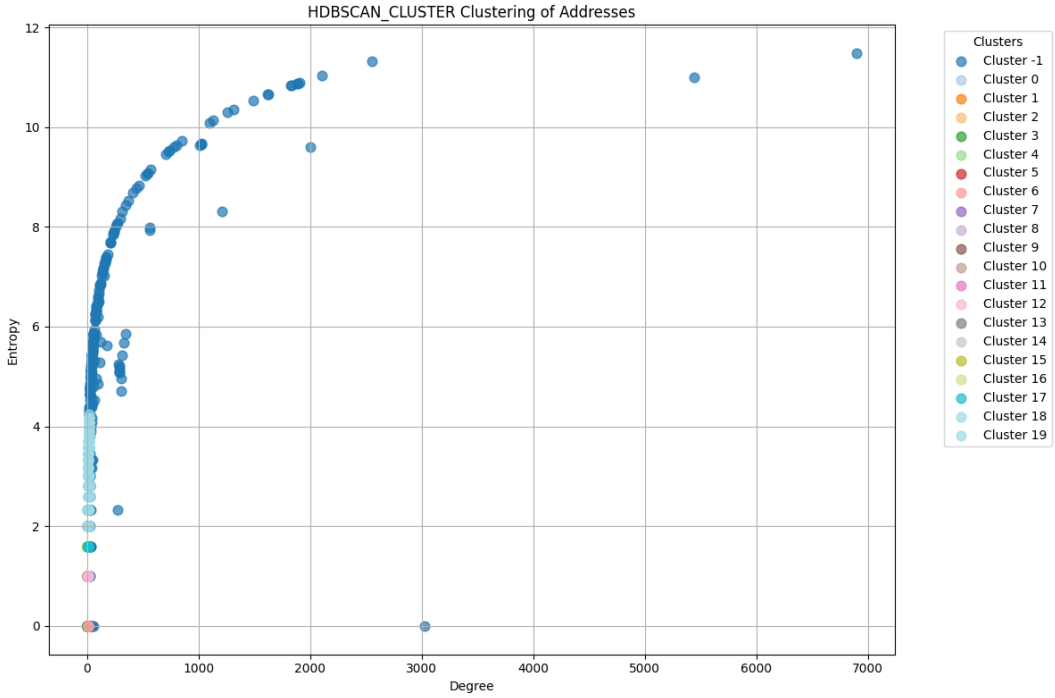

Figure 3: HDBSCAN clustering results.

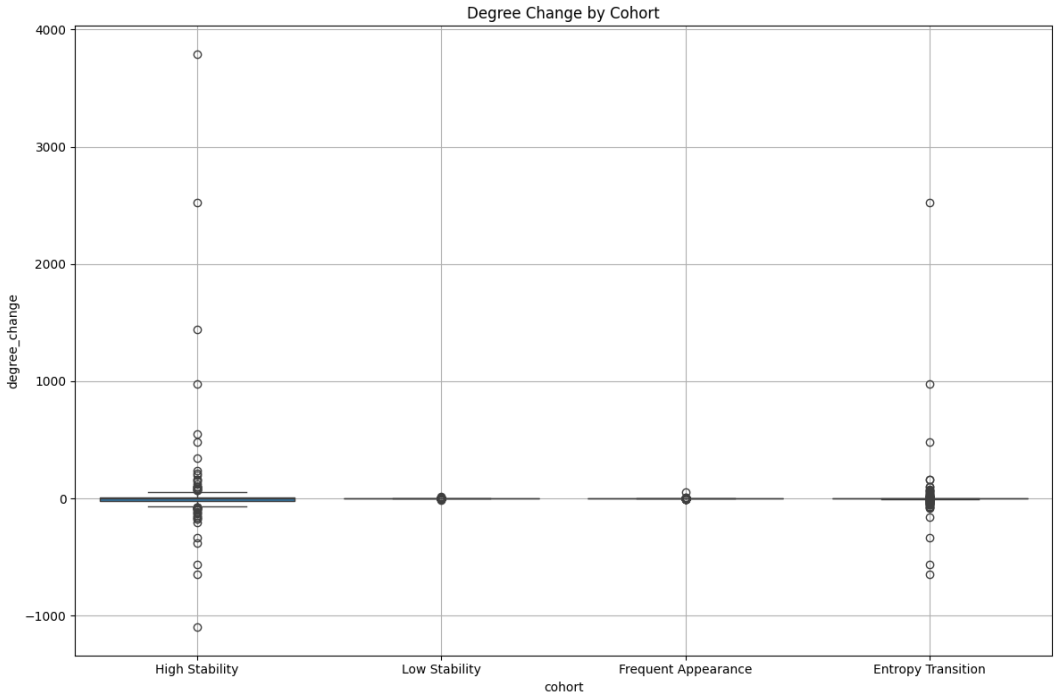

Figure 4: Degree change by cohort boxplot.

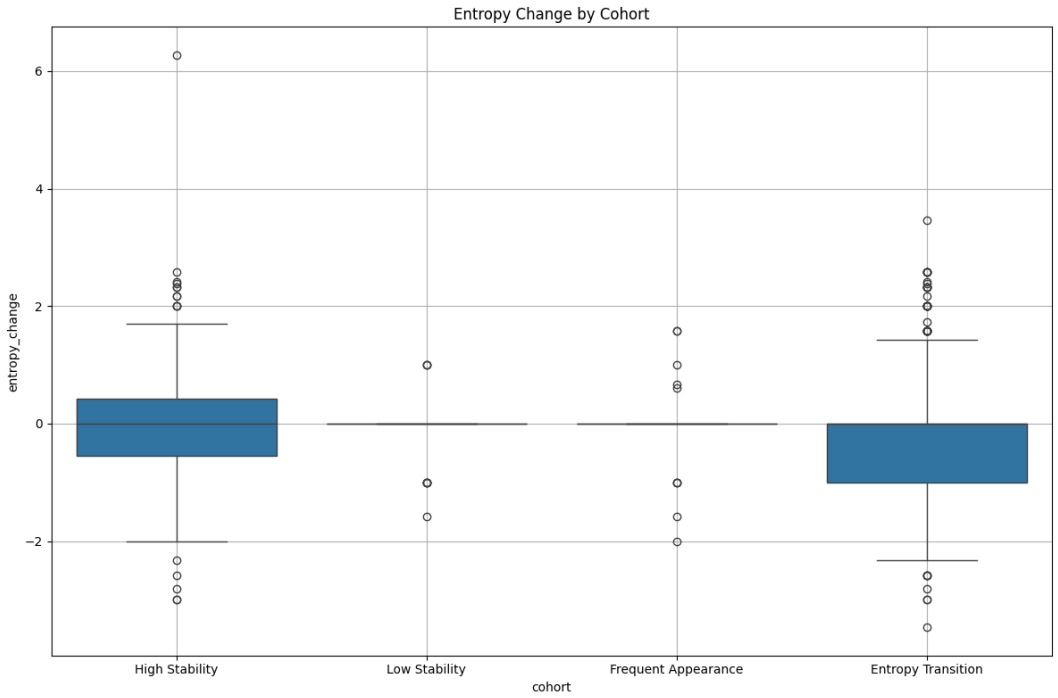

Figure 5: Entropy change by cohort boxplot.

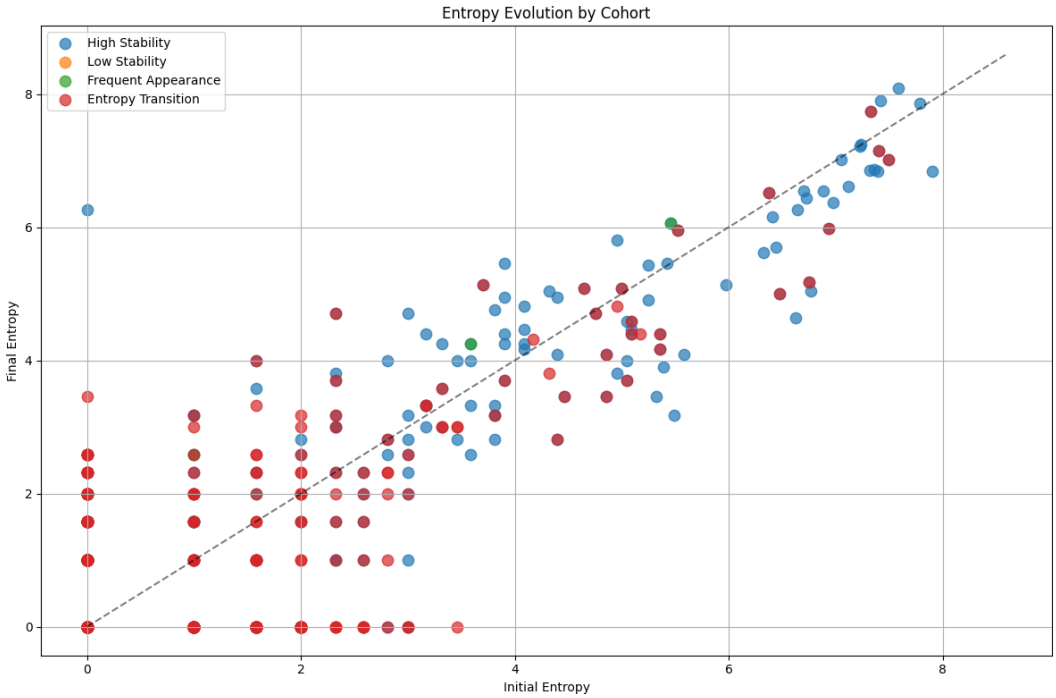

Figure 6: Entropy evolution plot.

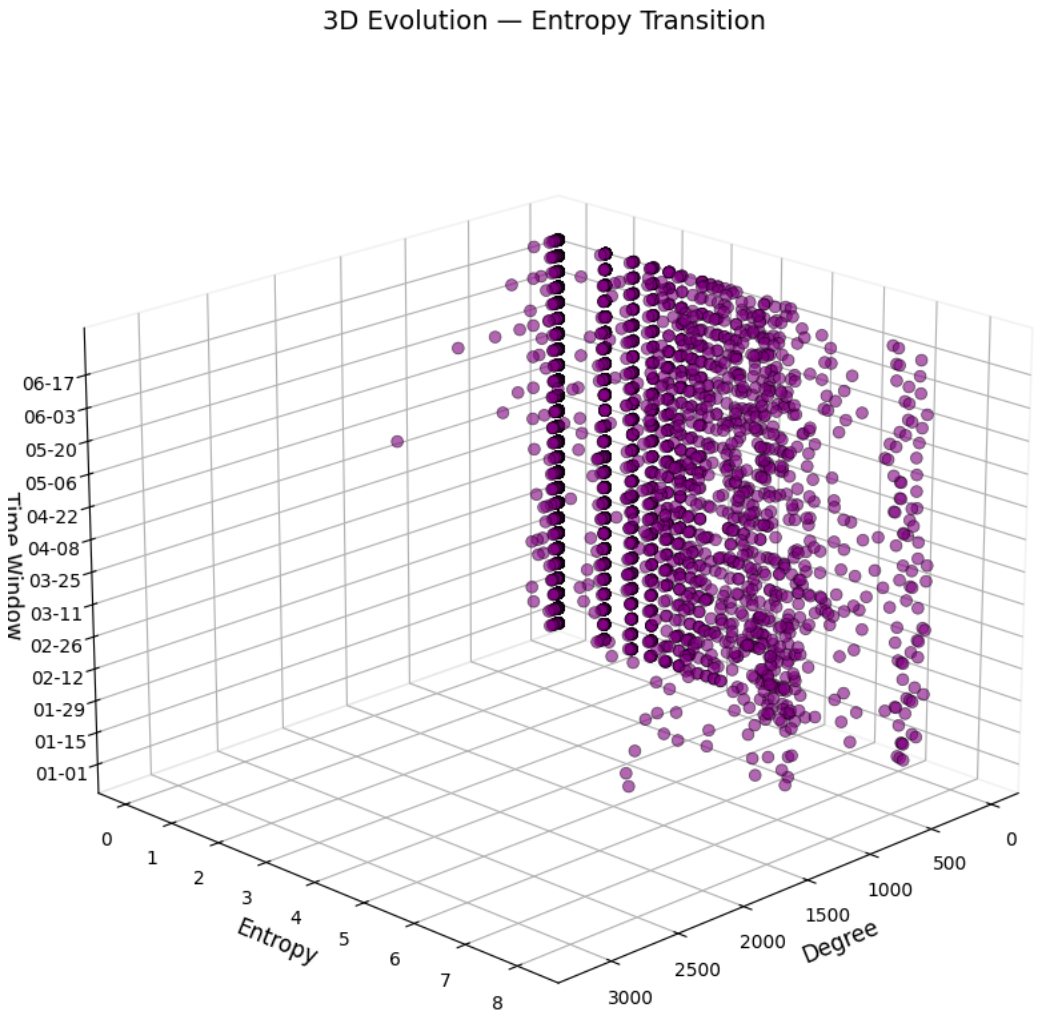

Figure 7: 3D trajectory for Entropy Transition cohort.

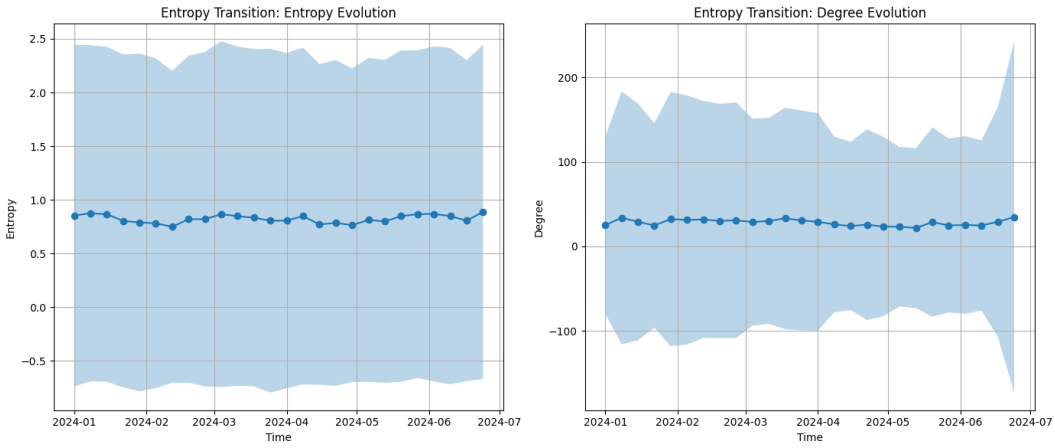

Figure 8: Aggregate entropy evolution for Entropy Transition cohort.

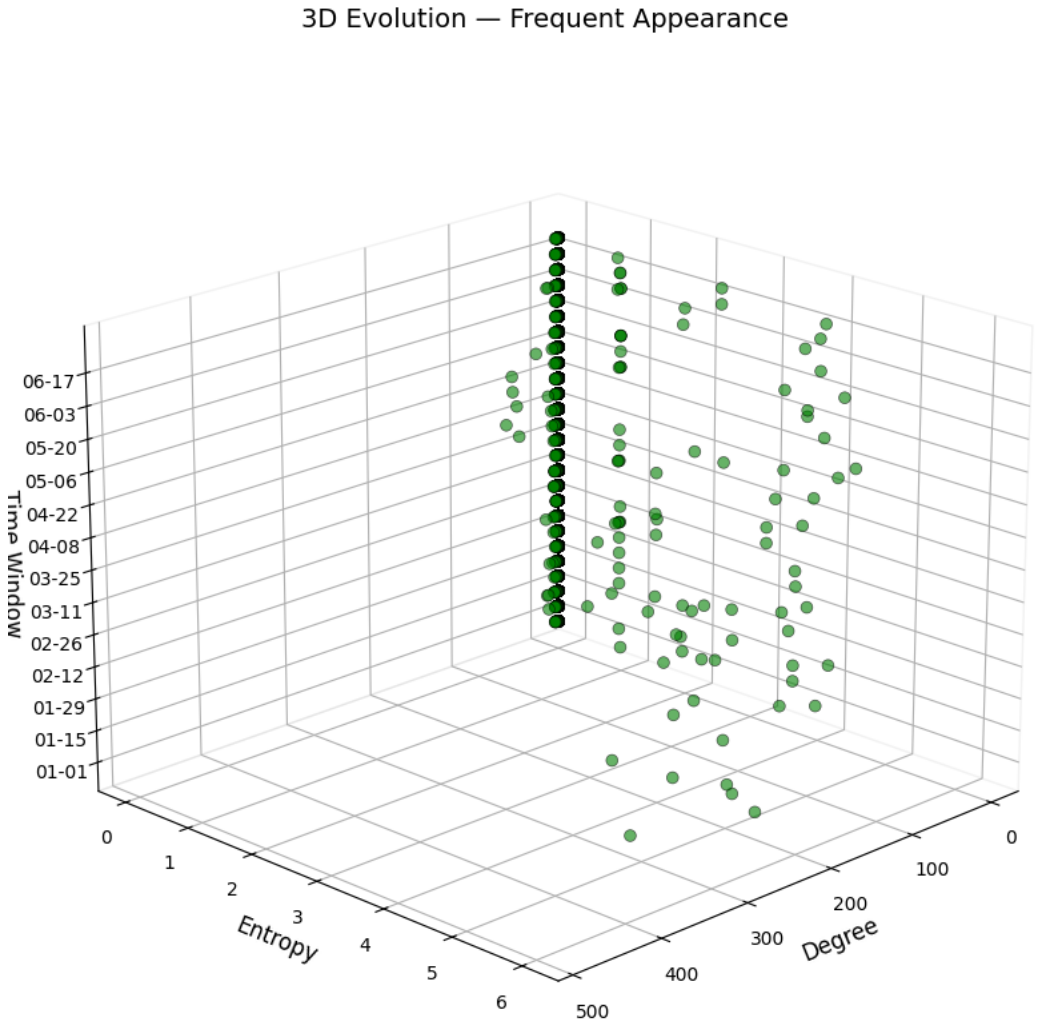

Figure 9: 3D trajectory for Frequent Appearance cohort.

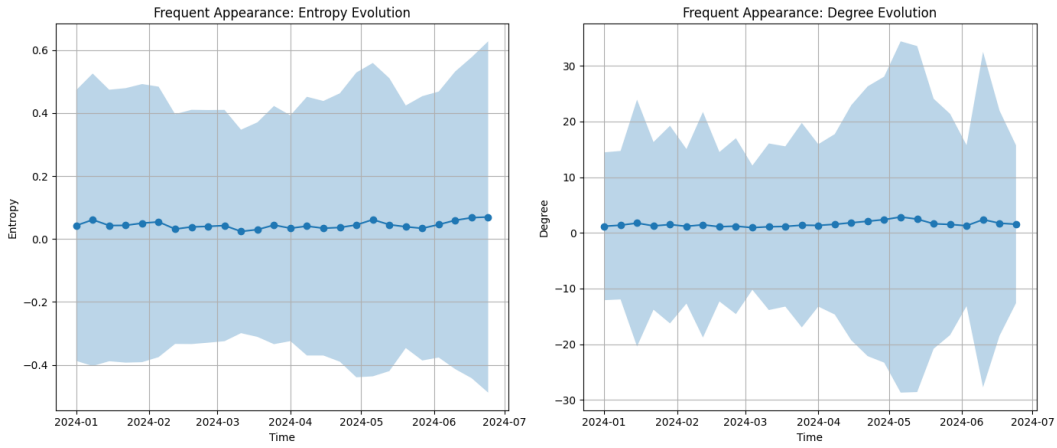

Figure 10: Aggregate entropy evolution for Frequent Appearance cohort.

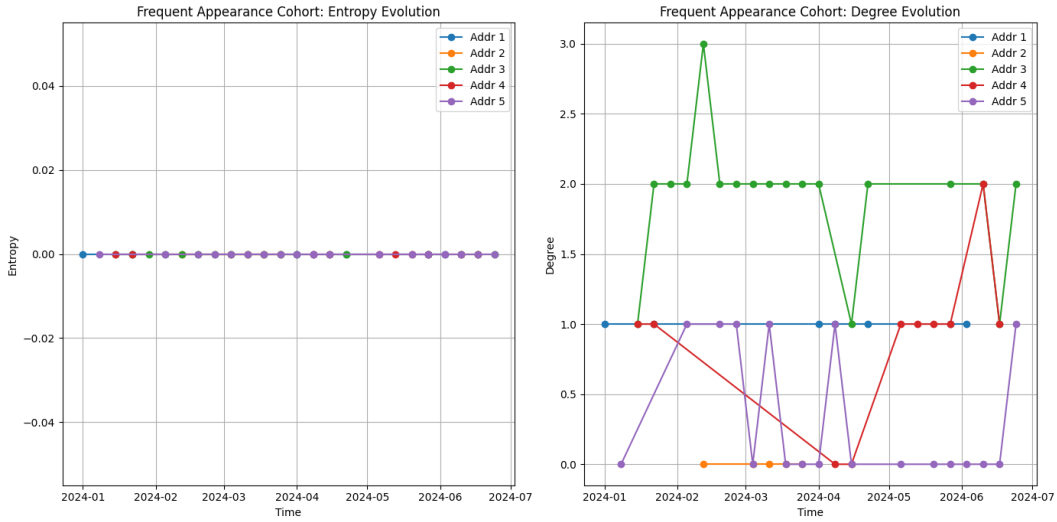

Figure 11: Entropy evolution for Frequent Appearance cohort.

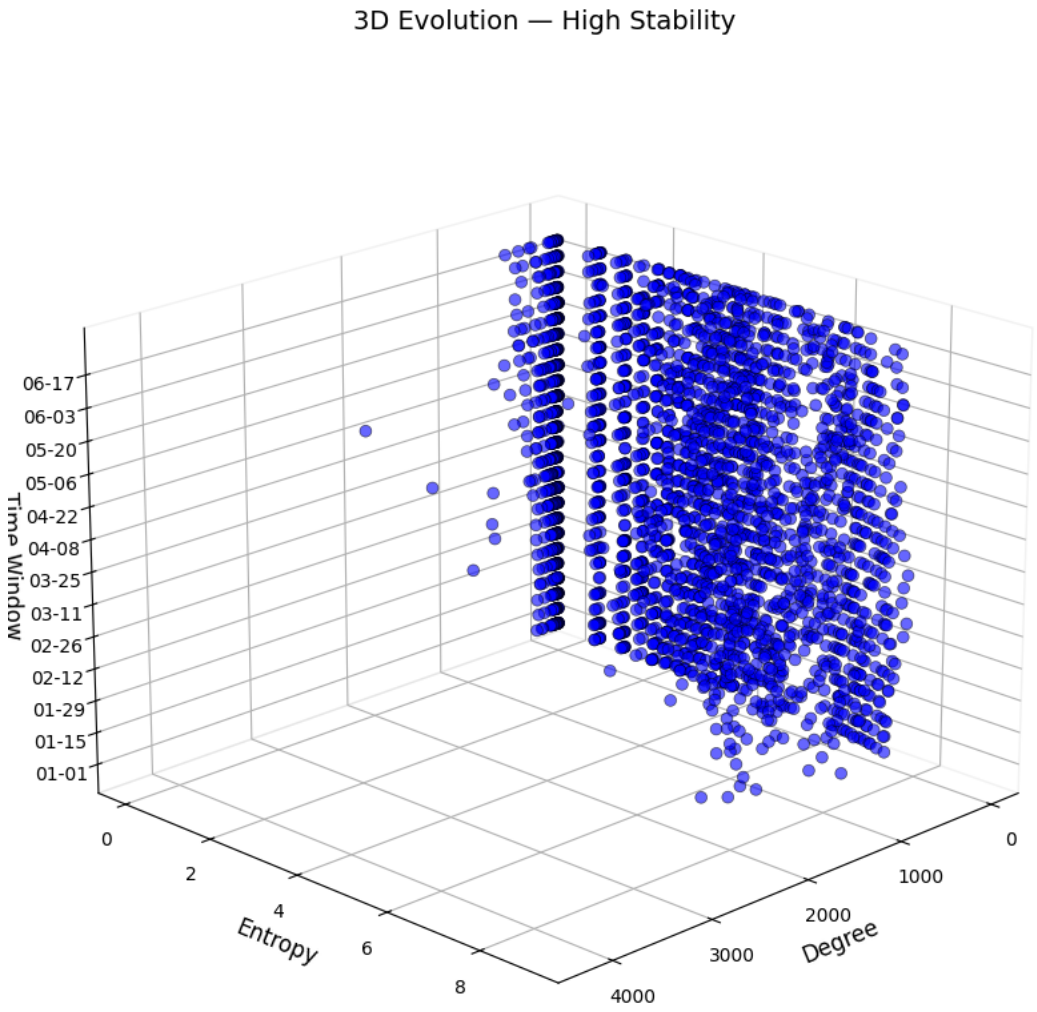

Figure 12: 3D trajectory for High Stability cohort.

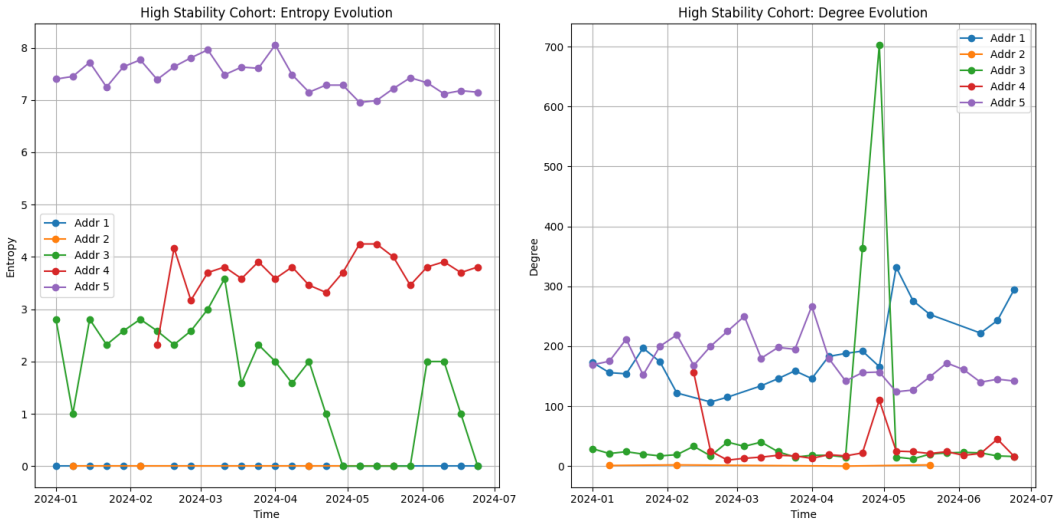

Figure 13: Entropy evolution for High Stability cohort.

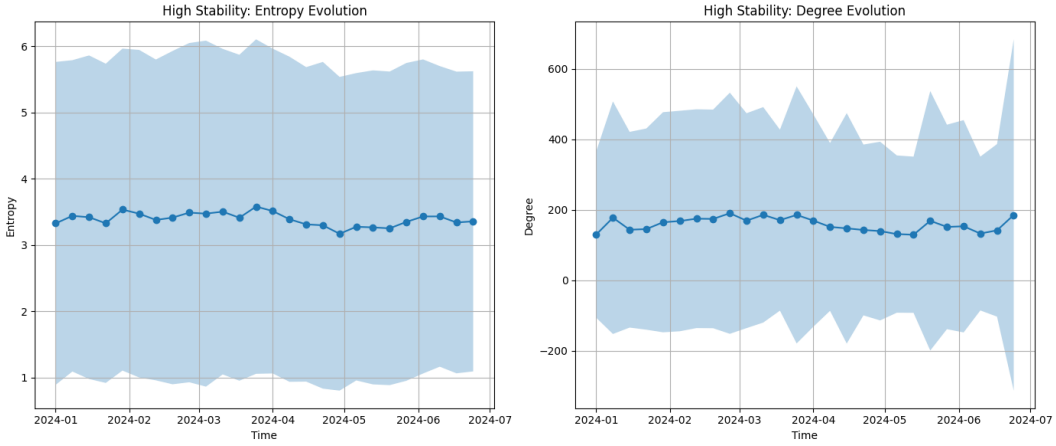

Figure 14: Aggregate entropy evolution for High Stability cohort.

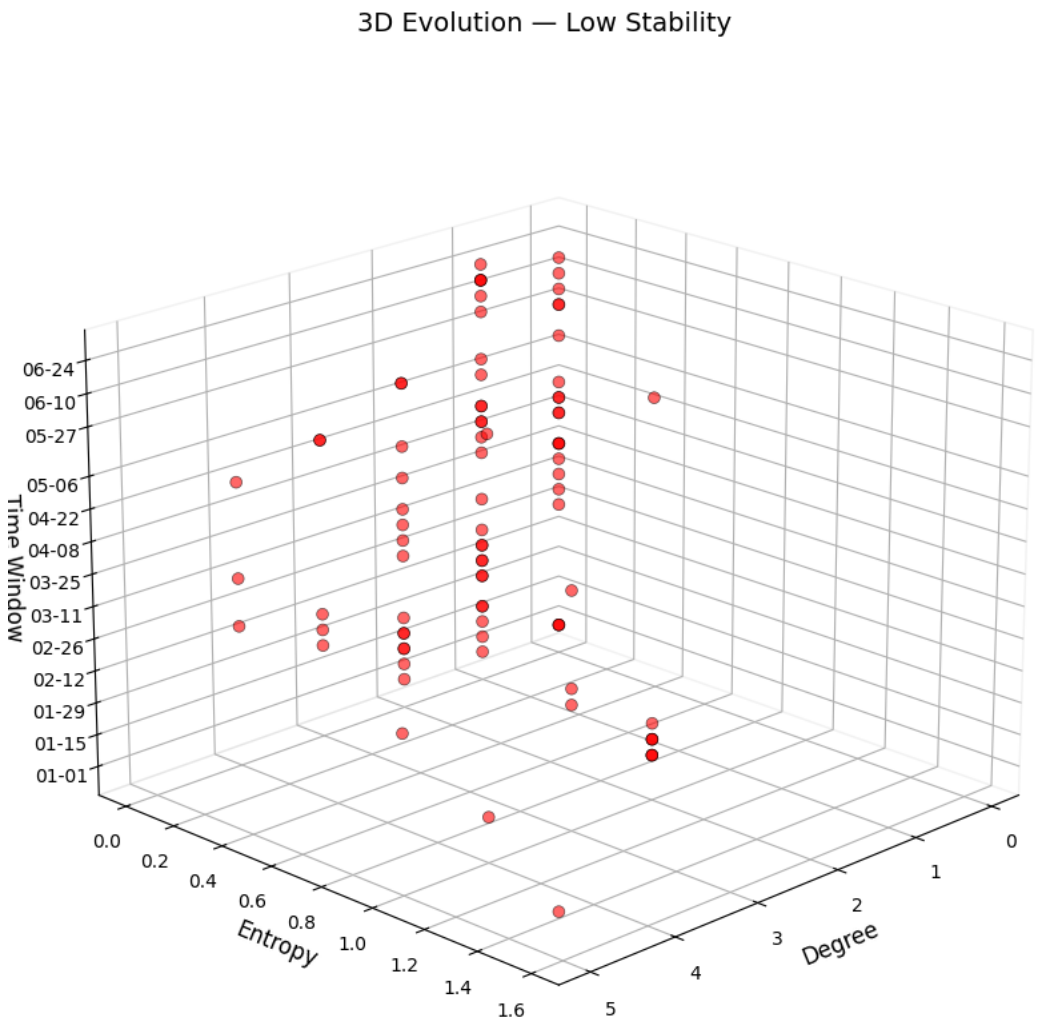

Figure 15: 3D trajectory for Low Stability cohort.

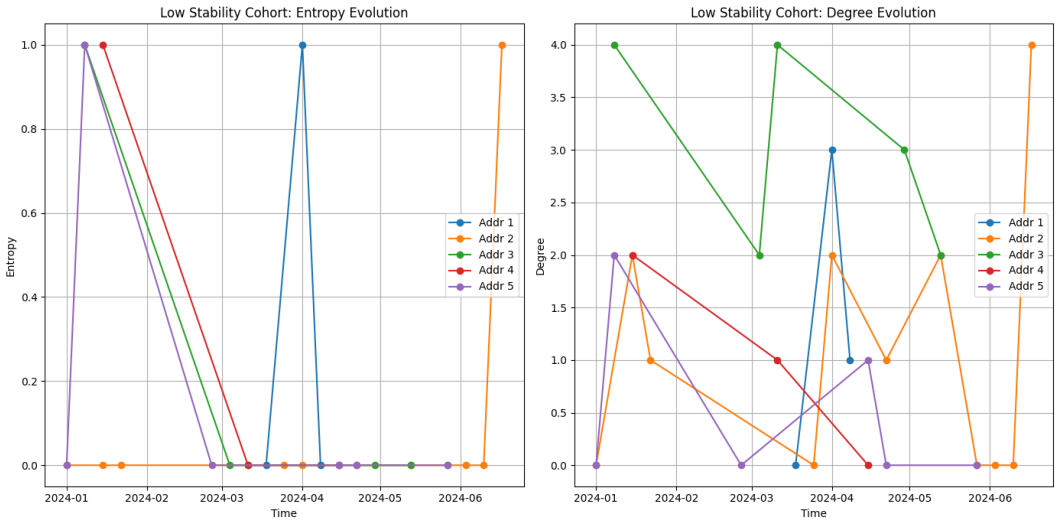

Figure 16: Entropy evolution for Low Stability cohort.

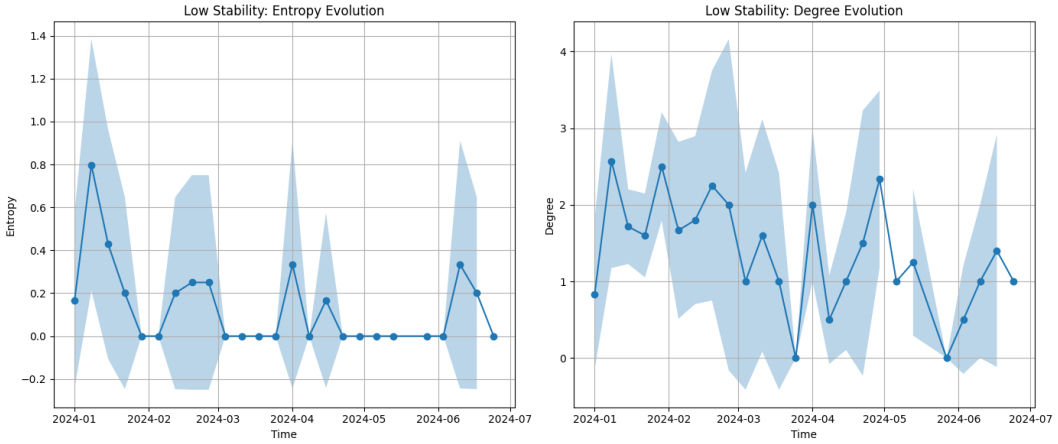

Figure 17: Aggregate entropy evolution for Low Stability cohort.

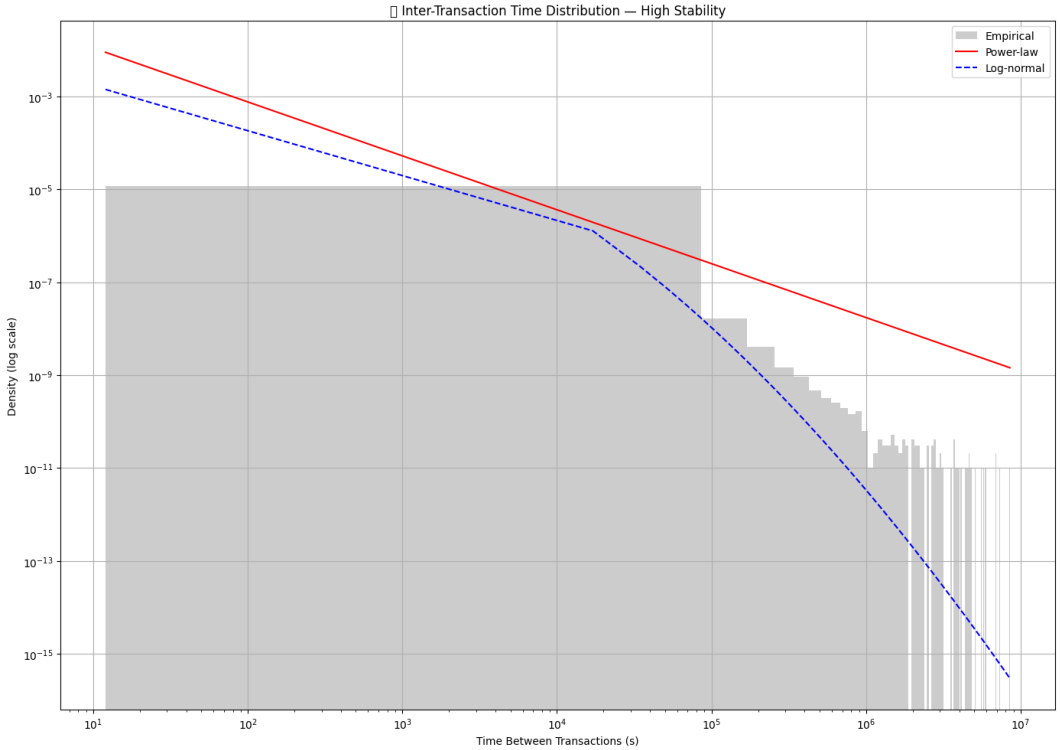

Figure 18: Inter-transaction time distribution for High Stability.

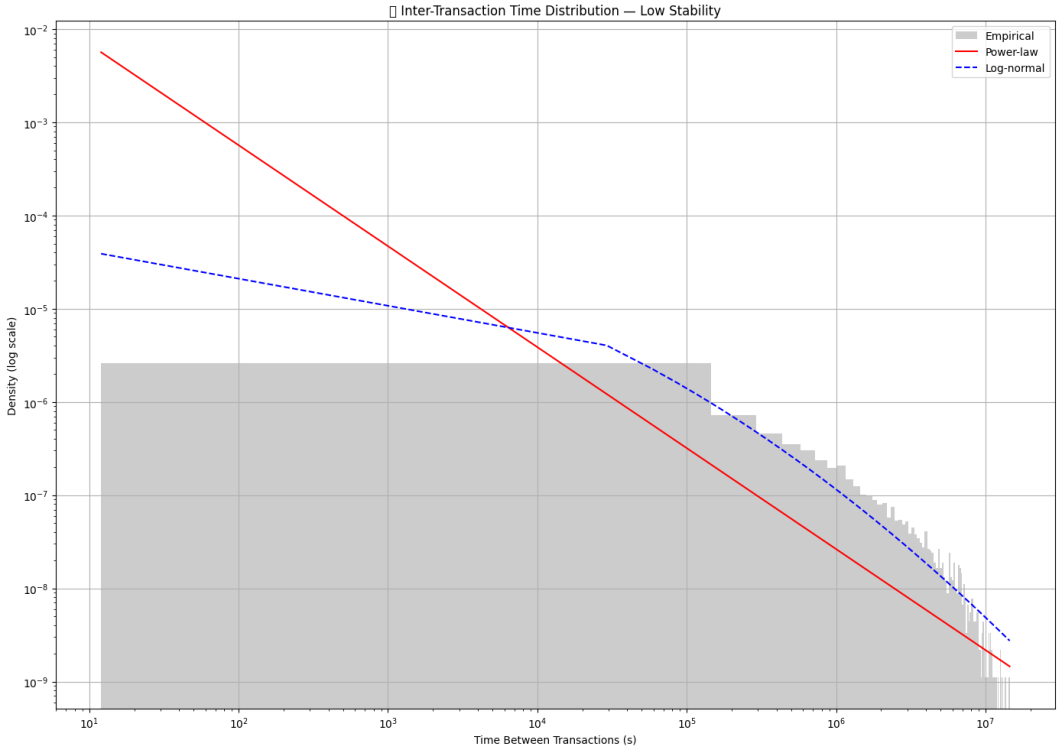

Figure 19: Inter-transaction time distribution for Low Stability.

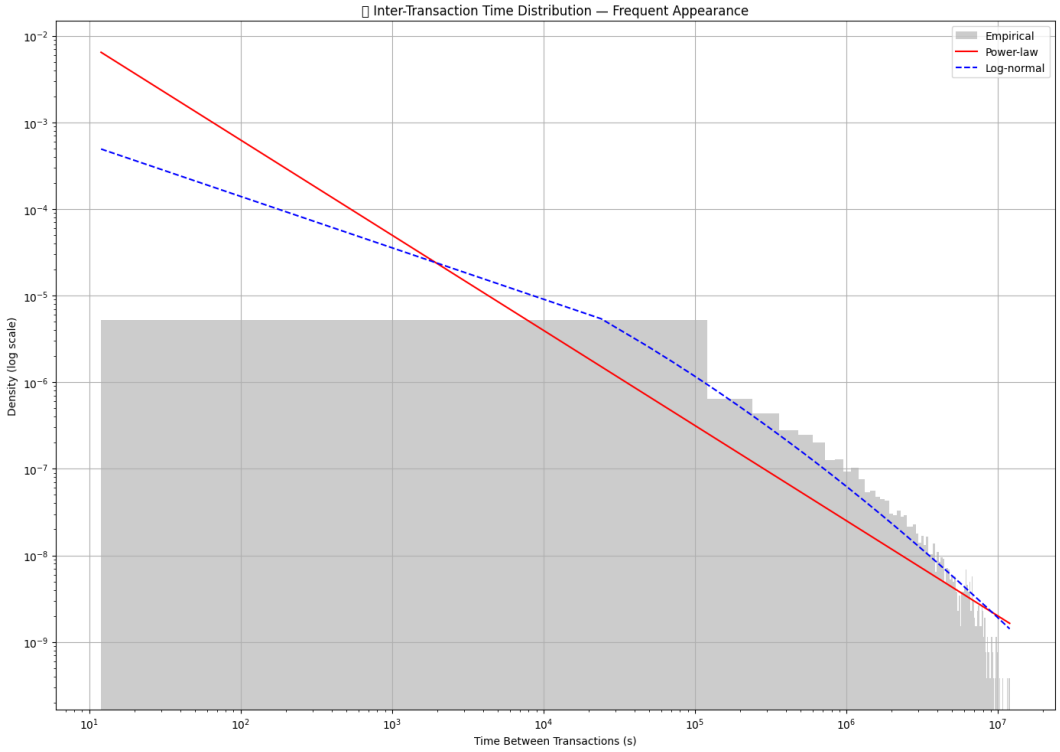

Figure 20: Inter-transaction time distribution for Frequent Appearance.

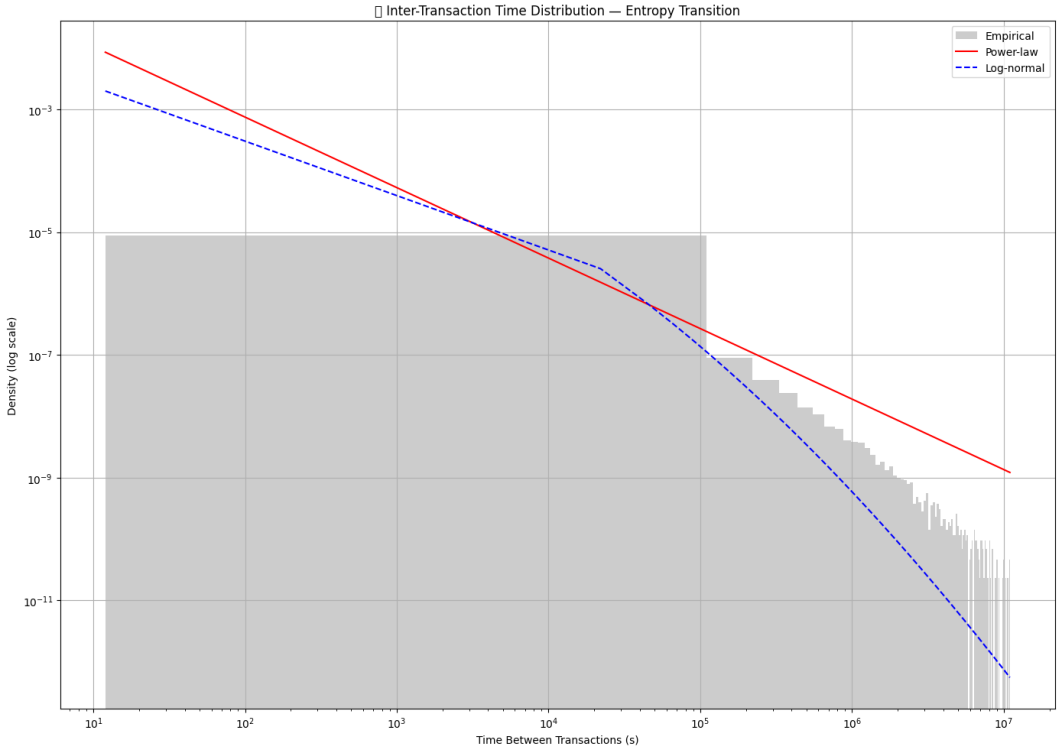

Figure 21: Inter-transaction time distribution for Entropy Transition.

References

[1] Meng Li. Application of cluster analysis in bitcoin deanonymization. In *Advances in Cyber Security and Intelligent Analytics*, pages 337–347. Springer, 2022.

[2] Friedhelm Victor. Address clustering heuristics for ethereum. In Joseph Bonneau and Nadia Heninger, editors, *Financial Cryptography and Data Security*, volume 12059 of *Lecture Notes in Computer Science*, pages 617–633. Springer, 2020.