UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

EVALUATING THE IMPACT OF EXTERNAL FACTORS ON THE STABILITY OF THE ETHEREUM NETWORK

A THESIS

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

Degree of

MASTER OF SCIENCE

By

TRISTAN BONY
Norman, Oklahoma
2024

Downloaded from SHAREOK. Persistent Handle URL: https://hdl.handle.net/11244/341281

EVALUATING THE IMPACT OF EXTERNAL FACTORS ON THE STABILITY OF THE ETHEREUM NETWORK

A THESIS APPROVED FOR THE
SCHOOL OF COMPUTER SCIENCE

BY THE COMMITTEE CONSISTING OF

Dr. Anindya Maiti (Chair)

Dr. Richard Veras

Dr. Shangqing Zhao

© Copyright by TRISTAN BONY 2024
All Rights Reserved.

Acknowledgments

First of all, I would like to thank Dr. Maiti who agreed to guide me during my research, as well as the two other members of my committee, Dr. Veras and Dr. Zhao, who were very responsive to my solicitations. Thanks also to Scott Seidenberger, a PhD student, for his invaluable help over the past few months.

I would also like to thank all the people who encouraged me during this period, such as my family, Dr. Badré and my close friends.

Table of Contents

chapterAcknowledgmentsiv

List Of Tables **vii**

List Of Figures **viii**

Abstract **ix**

1 Introduction **1**
1.1 Background and Motivation 1
1.2 Research Objectives 1

2 Literature Review **4**
2.1 Ethereum PoS Consensus 4
2.2 External Factors in Network Performance 5
2.2.1 Cybersecurity in Ethereum 5
2.2.2 Geomagnetic Activity and Network Systems 5
2.2.3 Media Impact on Blockchain Networks 6
2.3 Research Gap 6

3 Comparison of Ethereum Network with Non-Ethereum Hosts **7**
3.1 Data Collection 7
3.1.1 Ethereum Node Monitoring 7
3.1.2 Honeypot Implementation 8
3.2 Analysis Methodology 8
3.2.1 Attack Statistics 8
3.2.2 Port Activity Analysis 9
3.2.3 CVE Exploitation Patterns 9
3.2.4 Honeypot Interaction Analysis 9
3.3 Results 10

4 External Factors Impact Analysis **15**
4.1 Cyberattack Impact Analysis 15
4.1.1 Data and Methodology 15
4.1.2 Performance Analysis 16
4.2 Geomagnetic Activity Impact 18
4.2.1 Data and Methodology 18
4.2.2 Geomagnetic Disturbance Effects 18

4.3 Effects of News 19
4.3.1 Media Sentiment Methodology 19
4.3.2 Network Performance Correlation 20

5 Summary and Conclusions **22**
5.1 Discussion 22
5.1.1 Synthesis of Findings 22
5.1.2 Implications for Network Security 22
5.1.3 Limitations 23
5.1.4 Future Research Directions 23
5.2 Conclusion 24
5.2.1 Summary of Contributions 24
5.2.2 Key Findings 24

Reference List **27**
chapterAppendix27
1 Appendix A 27

List Of Tables

3.1 CVE detection patterns 13
3.2 Honeypot detection patterns 14

4.1 DTW values of each region 16
4.2 Causality test between attacks and attestations per region 17
4.3 Causality test between attestations of regions 17
4.4 Causality test against geomagnetic data 19
4.5 Causality test against geomagnetic data 21

List Of Figures

3.1 Cumulative attacks over 1 month 10
3.2 Attack statistics per region and group 11
3.3 Primary ports exhibiting anomalous activity 12
3.4 Secondary ports exhibiting anomalous activity (excluding 3 primary targets) 12
3.5 Attack patterns on Ethereum-specific ports 13

4.1 Least and most similar attacks vs attestations 16
4.2 Geomagnetic Activity against Attestation in EU 19
4.3 Attestation vs News Sentiment in NA 21

A.1 Attestation causality between regions 27

Abstract

This thesis investigates the resilience of the Ethereum peer-to-peer network against various external factors through empirical analysis. While previous researches have studied different aspects of the then proof-of-work (PoW) blockchain or the impact of external factors on other communication systems, the impact on the proof-of-stake (PoS) Ethereum blockchain remains unexplored. Our study examines three potential influence vectors: cyber threats, geomagnetic activity, and media coverage.

Through a comprehensive analysis of head attestations from Ethereum nodes, complemented by honeypot data, geomagnetic measurements, and news sentiment analysis, we compare security patterns between Ethereum and non-Ethereum hosts. Our methodology employs Dynamic Time Warping and Granger Causality Test to detect correlations and anomalies.

The results reveal that while Ethereum nodes face similar attack volumes as non-Ethereum hosts, they exhibit distinct patterns in targeted ports and CVEs exploitation attempts. There are also some differences between regions. Notably, our analysis found no significant correlation between the network performance and any of the examined external factors. While this suggests stability in the network's operation during normal conditions, further research over longer periods and during major events would be needed to make broader conclusions about the network's resilience.

This research contributes to the understanding of PoS blockchain network resilience and is a starting point for further research into the particularities of the Ethereum network against adversaries.

Chapter 1

Introduction

1.1 Background and Motivation

The Ethereum network stands as one of the most influential blockchain platforms in the decentralized ecosystem, ranking second on CoinGecko in terms of market cap, facilitating smart contracts and decentralized applications that power numerous financial and technological innovations. Its recent transition from Proof of Work (PoW) to Proof of Stake (PoS) in late 2022, marked a significant evolution in blockchain technology, reducing energy consumption significantly while maintaining network security and decentralization, as well as preparing the work for more scalability. This transition on such an important blockchain brings new challenges and behavior that need to be studied to verify the resilience of the network. That is the reason we decided to check how various external factors could impact this consensus.

1.2 Research Objectives

While extensive research has examined blockchain networks' internal dynamics and protocol-specific behaviors, the impact of external factors on network performance remains insufficiently explored, particularly in the context of Ethereum's post-PoS environment. The network's reliability and performance could potentially be influenced by various external factors, including targeted cyberattacks, environmental conditions,

and broader market dynamics. However, there is a notable lack of empirical evidence quantifying these potential relationships. This research addresses this knowledge gap by conducting a comprehensive analysis of the Ethereum network's behavior under different external conditions, focusing specifically on cyberattack activities, geomagnetic disturbances, and media influence.

This study aims to evaluate the resilience of the Ethereum network through empirical analysis of four key hypotheses:

1. Threats Differentiation: Ethereum nodes may experience distinct security threat patterns compared to non-Ethereum hosts, reflecting their unique role in the blockchain ecosystem.

2. Cyberattack Impact: Network performance metrics might show measurable variations during periods of increased cyberattack activity, potentially revealing vulnerabilities or resilience mechanisms.

3. Geomagnetic Influence: Earth geomagnetic activity could affect network performance through their impact on global communications infrastructure.

4. Media Impact: Significant news events and media coverage might influence network behavior through changes in user activity and validator participation.

The research employs a comprehensive data collection and analysis approach spanning one to two months of network activity. The methodology encompasses:

1. Network Performance Monitoring: Collection and analysis of head attestations from Ethereum nodes across five geographical regions to measure network health and performance.

2. Security Analysis: Deployment of honeypot systems to compare attack patterns between Ethereum and non-Ethereum hosts.

3. Environmental Data: Integration of geomagnetic activity data from NOAA to assess potential correlations with network performance.

4. Media Analysis: Tracking of news from the New York Times to evaluate media impact.

The analytical framework utilizes advanced statistical methods including:

- Dynamic Time Warping (DTW) for pattern comparison.
- Granger Causality Test for relationship analysis.

This thesis is organized into multiple chapters to reflect the progression over the different hypotheses:

- Literature Review: Examines existing research on blockchain network resilience, external factor impacts, and relevant analytical methods.
- Security pattern comparison between Ethereum and non-Ethereum hosts.
- Impact analysis of cyberattack activities.
- Correlation assessment with geomagnetic activity.
- Evaluation of news and media influence.

Chapter 2

Literature Review

2.1 Ethereum PoS Consensus

The Ethereum network's transition to Proof of Stake (PoS) marked a significant evolution in blockchain architecture. Vitalik Buterin, a co-founder of Ethereum, established the initial vision for Ethereum's consensus mechanism in 2014, but it took nearly a decade before it became ready for deployment. This method relies heavily on validator participation to attest new blocks as they come, with financial penalties if they appear to behave maliciously. Buterin et al. (2020)

Head attestations, represent validators' votes on the current state of the blockchain. It has been demonstrated how these attestations serve as key indicators of network health and consensus participation and how they can be used to penalize validators. Understanding validator behavior patterns has emerged as a critical area of study, with papers showing how it is possible to organize some sort of attacks penalizing nodes strictly respecting the consensus. Zhang et al. (2023)

2.2 External Factors in Network Performance

2.2.1 Cybersecurity in Ethereum

Previous research on the Ethereum network has primarily focused on three main areas. First, studies examining network topology and node distribution, such as Masoud et al. (2024), have revealed significant geographical disparities, with regions like the Middle East and North Africa (MENA) being underrepresented. Similar geographical imbalances were observed in earlier studies conducted during Ethereum's Proof-of-Work era Kim et al. (2018), which consistently showed the United States leading in node count.

The second major research focus has been on smart contract security Chen et al. (2020a); Kushwaha et al. (2022); Chen et al. (2020b). These studies have identified various vulnerabilities in smart contract implementations, including scenarios where attacks could be executed with lower stake requirements than theoretically predicted. Importantly, these security concerns stem from smart contract code vulnerabilities rather than underlying network infrastructure issues.

2.2.2 Geomagnetic Activity and Network Systems

While research directly linking geomagnetic activity to blockchain network performance remains limited, foundational work exists in related areas. Work for analyzing geomagnetic impacts on traditional network infrastructure have been done numerous time, mentioning their possibly devastating impact on satellites, and sometime on Earth grounds Boteler (2003).

2.2.3 Media Impact on Blockchain Networks

The relationship between media coverage and finance outcome have been studied for a long time, and blockchains are often related with trading cryptocurrencies. But, if there are researchers who tried to find statistical evidence to forecast the market ENGLE and NG (1993), more recent approaches based on natural language processing try to achieve similar results by analyzing a sentiment with tools like Hugging Face Transformers Wolf et al. (2020).

2.3 Research Gap

The blockchain technology is still young and have niche usage, resulting in fewer papers being published but it is still growing fast. Current literature reveals several gaps that this thesis try to address, such as the lack of analyses of Ethereum PoS network layer's data, or how the blockchain would react to several external factors, with a comparison with non-Ethereum hosts. It will also be interesting to see how the decentralized aspect of blockchains plays a part in the network stability.

Chapter 3

Comparison of Ethereum Network with Non-Ethereum Hosts

Before conducting a comparative analysis of external factors affecting the Ethereum network, it is essential to understand how attack patterns on blockchain nodes differ from those on conventional Internet servers.

3.1 Data Collection

3.1.1 Ethereum Node Monitoring

To gather comprehensive data, we deployed Ethereum nodes across five distinct geographical regions: North America (NA), Europe (EU), Middle East (ME), Asia Pacific (AP), and South America (SA). Additionally, we established a control group of non-Ethereum servers in these same regions. A complete Ethereum node implementation requires two clients: a Consensus Client and an Execution Client, each connecting to different network peers. We selected Nethermind and Lighthouse clients for their extensive analytical capabilities, which support future research endeavors. This research was conducted in collaboration with PhD candidate Scott Seidenberger, contributing to his doctoral dissertation.

For a two-month period, we collected various metrics from the Ethereum nodes, focusing primarily on head attestation percentages while gathering additional data for

future research. Head attestation percentage serves as a crucial indicator of network stability, as it measures the consistency with which validators can agree upon and attest to the latest block state — low percentages potentially indicating network or validator malfunctions.

3.1.2 Honeypot Implementation

To comprehensively analyze attack patterns, we augmented both Ethereum and non-Ethereum hosts with honeypots across all regions. These honeypots were designed to capture both the quantity and nature of attack incidents. For this study, we defined an attack as any unauthorized connection or connection attempt, ranging from benign port scans to actual exploit attempts.

3.2 Analysis Methodology

3.2.1 Attack Statistics

All attack data was consolidated into a single CSV file, with measurements taken at 30-minute intervals. Each data point is associated with an IP address corresponding to a specific region and group, enabling detailed comparative analysis. During the data extraction process from the database, null values were encountered and subsequently converted to zero for compatibility with analytical libraries and algorithms. While this conversion may introduce minor statistical variations, the impact on overall analysis remains limited.

Our initial analysis focused on calculating the cumulative attack frequency for both groups by aggregating values per IP address over a one-month period for each region.

To provide deeper insight into the attack distribution, we conducted box plot analyses to highlight statistical variations between groups.

3.2.2 Port Activity Analysis

Following the global attack analysis, we conducted a granular examination of port targeting patterns, comparing Ethereum nodes with non-Ethereum hosts. The data, organized by region, required careful differentiation between experimental and control groups. After parsing the data into Pandas DataFrames, we generated heat maps highlighting port utilization patterns. While comprehensive analysis of least-utilized ports could reveal specific attack patterns, such investigation fell outside the current scope. However, we specifically analyzed ports utilized by Ethereum protocols and clients to assess their vulnerability relative to commonly targeted ports.

3.2.3 CVE Exploitation Patterns

To broaden our analysis, we examined Common Vulnerabilities and Exposures (CVE) patterns across both study groups. Our analysis focused on identifying and tracking both the top 10 most exploited CVEs and the 10 least common CVEs, examining their occurrence patterns throughout the month-long observation period. We actually ended up not using the least 10 because of the numerous outputs and lacks of interesting information.

3.2.4 Honeypot Interaction Analysis

Finally, we analyzed honeypot service detection patterns to understand the nature and frequency of intrusion attempts across different deployment scenarios, again identifying the most frequent ones.

3.3 Results

Our analysis yielded several significant findings regarding attack patterns and system vulnerabilities.

The cumulative attack analysis revealed that while both control and experimental groups experienced similar attack patterns, the Ethereum node in NA received approximately half the number of attacks compared to the non-Ethereum host during the observation period (Figure 3.1).

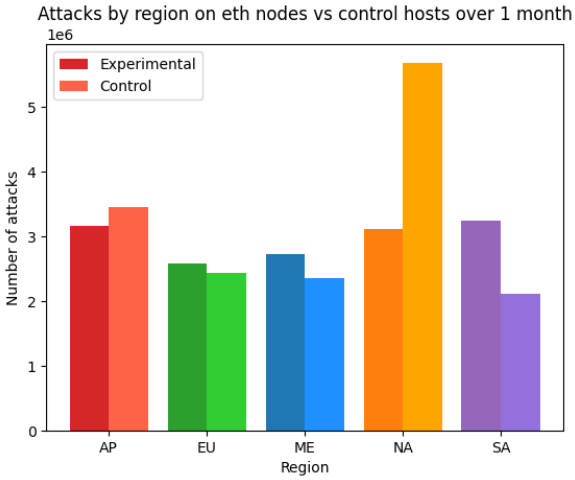


Figure 3.1: Cumulative attacks over 1 month

The box plot analysis (Figure 3.2), with zero values — due to their bias — and outliers removed for clarity, revealed significant variance across all hosts, with the control group showing higher variability. Notably, while the EU region displayed the lowest median attack rate, the Ethereum node in this region experienced the highest peak attack rate — approximately 1.5 times greater than any other host's maximum.

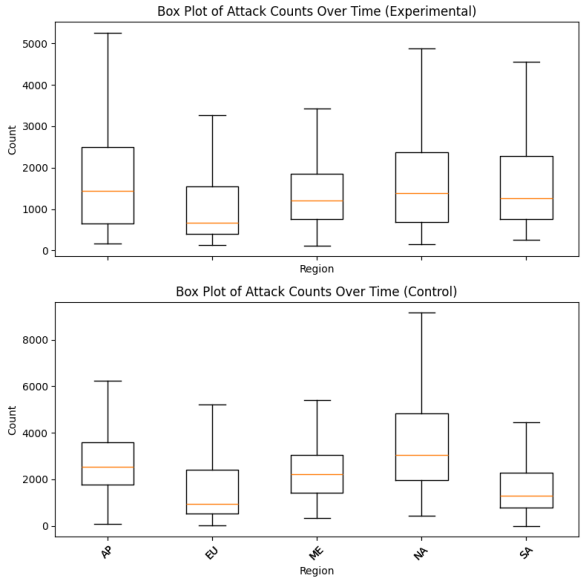


Figure 3.2: Attack statistics per region and group

Port analysis (Figure 3.3) revealed three predominantly targeted ports across both groups:

- Port 53: DNS (Domain Name Service) protocol (blocked in EU).
- Port 123: NTP (Network Time Protocol).
- Port 445: Primarily used for Microsoft file-sharing services.

While the first two ports are common on any system, and known to have had security flaws, the significant activity on port 445 was unexpected. Attack intensity varied notably between groups and regions, suggesting targeted rather than random attack patterns. After excluding these primary targets, secondary analysis revealed additional patterns (Figure 3.4), including:

- Port 1433 (ME region): Targeted exclusively in the control group, typically associated with Microsoft SQL Server deployments default TCP access.

- Port 5900 (EU region): Used for VNC (Virtual Network Computing) remote GUI access.
- Port 64333: Identified as a misconfiguration anomaly.

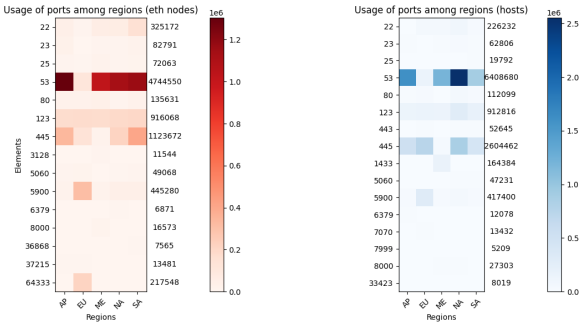


Figure 3.3: Primary ports exhibiting anomalous activity

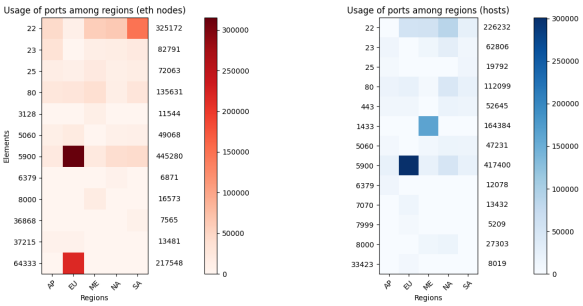


Figure 3.4: Secondary ports exhibiting anomalous activity (excluding 3 primary targets)

Analysis of Ethereum-specific ports (Figure 3.5) revealed targeted attacks on ports 8545, 8546, and 30303, with significantly higher activity on Ethereum nodes compared to non-Ethereum hosts. Port 9000 showed elevated activity across both groups, potentially due to its use in legacy gaming applications. However, these Ethereum-specific ports experienced lower overall attack volumes compared to the primary targeted ports.

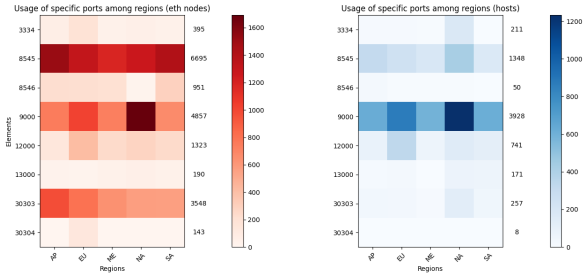


Figure 3.5: Attack patterns on Ethereum-specific ports

CVE analysis identified several significant exploitation patterns (Table 3.1). The control group predominantly experienced attempts targeting RealVNC authentication bypass vulnerabilities, while the experimental group showed potential Microsoft tool buffer overflow exploits, though further analysis is needed to confirm the latter. Notable patterns included CVE-1999-0675 (DDoS attacks) concentrated in ME and NA regions of the control group, and CVE-2020-11899 (Treck TCP/IP stack vulnerability) exclusively targeting NA region Ethereum nodes.

Attack timing patterns showed similar distributions across regions, but with varying intensities. Control group attacks in NA and EU regions were up to five times more intense than in other regions, reaching 6,000 attacks per 30-minute interval. The experimental group showed 20% higher intensity, with smaller regions experiencing similar maximum attack rates.

CVE	**Ethereum node**	**Non-Ethereum host**	**Regions**
CVE-2006-2369	YES	YES	All
CVE-2003-0903	YES	NO	All
CVE-1999-0675	NO	YES	ME, NA
CVE-2020-11899	YES	NO	NA

Table 3.1: CVE detection patterns

Honeypot analysis revealed comparable maximum and average detection rates across both groups, though temporal patterns varied significantly both between and within groups. Regional variations in honeypot effectiveness were observed, with Heralding showing increased activity in EU for credential collection, while Ddospot showed reduced DDoS detection in the same region. Average detection rates remained below 10,000 incidents per honeypot across all regions.

Honeypot	**Ethereum node**	**Non-Ethereum host**	**Regions**
Honeytrap	YES	YES	All
Cowrie	YES	YES	All
Dionaea	YES	YES	All
Ddospot	YES	YES	All, reduced in EU
Heralding	YES	YES	EU

Table 3.2: Honeypot detection patterns

Chapter 4

External Factors Impact Analysis

After observing variations between the control and experimental groups — sometimes small ones —, we investigated how external factors affect the Ethereum network's performance.

4.1 Cyberattack Impact Analysis

4.1.1 Data and Methodology

For this analysis, we compared previously observed total attacks against Ethereum head attestation values from our nodes. The primary challenge was aligning timestamps between datasets, as attack data was recorded in 30-minute intervals over one month, while attestation data used one-hour intervals over two months. To address this, we performed multiple operations using Pandas to resample the data and applied an Exponential Moving Average (EMA). We then normalized both datasets to a 0-1 scale and applied $1-x$ to the attestations to align directionally with attack data. After filtering to retain only the overlapping time period, we applied Dynamic Time Warping (DTW) to measure similarity between attacks and attestations.

We then investigated regional inter-dependencies using Granger Causality Tests to determine if one time series could predict another. This analysis was applied both between attack data and regional attestations, and between attestations across regions,

particularly examining if major regions (NA and EU) influenced smaller ones (AP, ME, and SA).

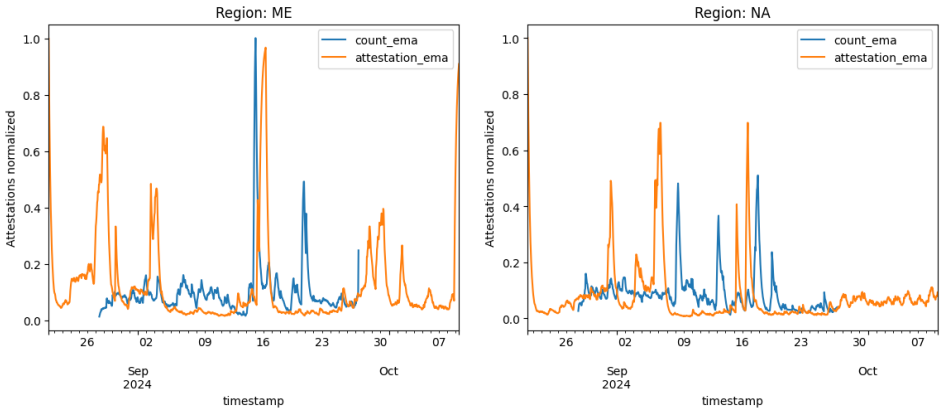
We also considered incorporating metrics from Rated Labs, a PoS blockchain analytics company, but their daily granularity proved insufficient for meaningful comparison.

4.1.2 Performance Analysis

Region	AP	EU	ME	NA	SA
DTW	1.52	2.97	3.22	1.20	2.95

Table 4.1: DTW values of each region

The DTW results in Table 4.1 reveal that ME demonstrated the least similarity between attacks and attestations (DTW = 3.22), while NA showed the strongest similarity (DTW = 1.20). These contrasting patterns are visualized in Figure 4.1.



(a) Least similar resemblance in ME (b) Most similar resemblance in NA

Figure 4.1: Least and most similar attacks vs attestations

The Granger Causality Test results are presented in Table 4.2. Notably, no regions achieved statistical significance (p-value below 0.05), as all p-values exceeded 0.6 across

both one-hour and two-hour horizons. This suggests that network performance in these regions is either resilient to attacks or influenced by multiple factors beyond cyberattacks within the studied time frame.

Region	AP	EU	ME	NA	SA
p (+1h)	0.6517	0.9727	0.6679	0.7053	0.9750
p (+2h)	0.8752	0.8884	0.9102	0.6942	0.8974

Table 4.2: Causality test between attacks and attestations per region

The inter-regional attestation analysis results are shown in Table 4.3. The EU region demonstrated consistent zeros, while NA showed minimal causality, suggesting limitations in the testing methodology, particularly given the lack of visible causality in Figure A.1.

Region	**p-value 1h**					**p-value 2h**				
	AP	EU	ME	NA	SA	AP	EU	ME	NA	SA
EU	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
NA	0.0240	0.0637	0.7481	0.0000	0.0065	0.0000	0.0000	0.0000	0.0000	0.0054

Table 4.3: Causality test between attestations of regions

4.2 Geomagnetic Activity Impact

4.2.1 Data and Methodology

For this hypothesis, we analyzed potential correlations between geomagnetic activity and network performance using data from the National Oceanic and Atmospheric Administration (NOAA). Our analysis focused on the Planetary-K (K_p) index, which provides quasi-logarithmic 3-hour intervals of mean-standardized geomagnetic activity relative to quiet-day measurements from 13 observatories, with values ranging from 0-9, low to high. While NOAA also provides the Planetary-A (A_p) index, measuring average daily amplitude of geomagnetic activity in nanotesla, based on linearized K values, we selected K_p for its superior temporal granularity.

Our methodology involved converting NOAA's text data to JSON format for efficient processing, standardizing all timestamps to UTC (as opposed to the America/Chicago timezone used in attestation and attack data), normalizing to a 0-1 scale, and resampling attestations to match the 3-hour intervals of geomagnetic data, as well as smoothing the data with EMA with a span of 12. This prepared dataset, quite similar to the previous test, then underwent Granger Causality testing to have an identical test method on all hypotheses.

4.2.2 Geomagnetic Disturbance Effects

Table 4.4 presents the causality test results. Most notably, the EU region approached statistical significance with a p-value of 0.0768 within the 3-hour window, while all other regions and time frames showed p-values well above the 0.05 significance threshold. Figure 4.2 provides a visual comparison for the EU region, though it's important to

note that the statistical analysis only considered the overlapping time period between both series.

Region	AP	EU	ME	NA	SA
p (+3h)	0.1519	0.0768	0.3376	0.3558	0.3127
p (+6h)	0.4649	0.3225	0.7568	0.1438	0.2639

Table 4.4: Causality test against geomagnetic data

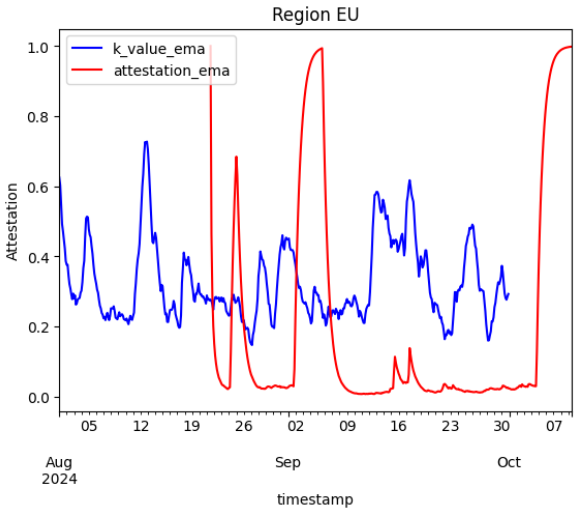


Figure 4.2: Geomagnetic Activity against Attestation in EU

4.3 Effects of News

4.3.1 Media Sentiment Methodology

To assess the final hypothesis about news impact on network performance, we analyzed New York Times articles due to their comprehensive API access to their archive — such as headlines, abstracts, sections, publishing dates, and many more metadata — and global influence, covering worldwide topics.

We filtered for relevant sections (politics, climate, economy, and science related topics), excluding lifestyle and arts coverage among others. The sentiment analysis employed Hugging Face Transformers, which assigned POSITIVE or NEGATIVE labels with associated confidence scores bounded between 0 and +1, to each texts. For the analysis, we considered POSITIVE to be +1, and NEGATIVE as -1, and we weighted them by their confidence levels to obtain values between -1 and +1. Similarly, we also used TextBlob, an alternative sentiment analyzer which only returns a sentiment polarity between -1 and +1. We then calculated an average of the values from the headline, abstract and lead paragraph of each article with both tools. The two methods follow a similar global pattern, but have different sentiment values locally, so taking the average of the output of each of them would reduce each other's bias. With the decrease in the number of articles, we didn't have enough ones to left to have a small window of analysis, so we then aggregated into 12-hour intervals and normalized to a 0-1 scale for consistency with our previous analyses and align attestations directionally with attacks again, before applying the EMA with a span of 6.

Complementary research about the impacts of cloud providers malfunctions on the network was started by analyzing the status page of the most used ones (AWS, Hetzner, OVH), but initial results didn't show any impact. Moreover, no major problems happened during our test period, so it's unlikely we would have seen anything else.

4.3.2 Network Performance Correlation

The causality test results in Table 4.5 show no significant correlation between news sentiment and network stability, with all p-values exceeding the 0.05 significance threshold across both 12-hour and 24-hour windows. Figure 4.3 provides a visual representation of attestations versus news sentiment in the NA region, supporting our statistical findings.

Region	AP	EU	ME	NA	SA
p (+12h)	0.9072	0.7667	0.4824	0.3353	0.9627
p (+1d)	0.3248	0.7938	0.7057	0.4442	0.6967

Table 4.5: Causality test against geomagnetic data

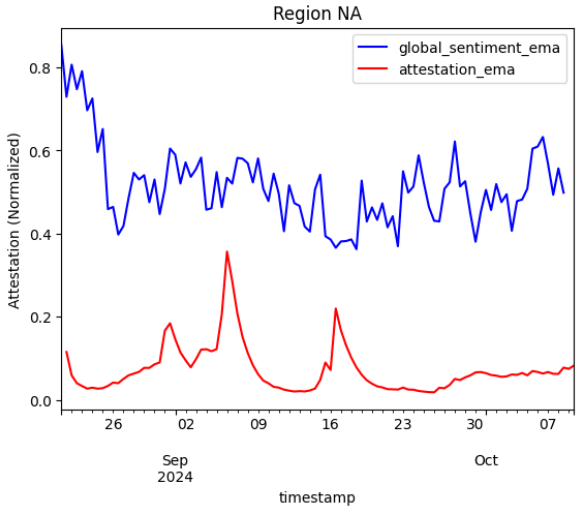


Figure 4.3: Attestation vs News Sentiment in NA

Chapter 5

Summary and Conclusions

5.1 Discussion

5.1.1 Synthesis of Findings

This research investigated the relationship between external factors and Ethereum network performance through the analysis of two months of head attestations data across five geographical regions. The comprehensive analysis, employing Dynamic Time Warping (DTW), and Granger Causality Testing, revealed no significant correlations between external factors (cyberattacks, geomagnetic activity, and news events) and network performance. However, the study uncovered distinct patterns in security threats between Ethereum nodes and non-Ethereum control group, suggesting differentiated attack vectors and security considerations for blockchain versus traditional infrastructure.

5.1.2 Implications for Network Security

The absence of significant correlations with external factors demonstrates the Ethereum network's resilience, which has important implications for blockchain security architecture:

- The decentralized nature of the network appears to effectively mitigate the impact of localized external disruptions.

- The distinct security threat patterns between Ethereum and non-Ethereum hosts suggest the need for specialized security approaches for blockchain infrastructure.
- Current security models focusing on external factor mitigation may need reevaluation and resource reallocation.

5.1.3 Limitations

Several limitations should be considered when interpreting these findings:

- Temporal Scope: The data collection period may not capture long-term patterns or seasonal variations. 3 months were planned, but only 1 to 2 (depending on the data) were a available in time for this thesis.
- Geographical Coverage: While spanning five regions provides a comprehensive overview of all of them, it may be beneficial to consider a more granular level of analysis to gain further insights, the majority of nodes being situated in the USA and the EU.
- Data Granularity: Having the more granularity for all of the data could help capture more aspect of the behaviors.

5.1.4 Future Research Directions

This study opens several promising avenues for future research:

- Longitudinal Studies: Extended temporal analysis to capture annual patterns and long-term trends.
- Expanded Factor Analysis: A more in-depth investigation of some external factors such as news to look for specific topic, or restrain the analysis to news of some regions, or looking at potential cyber kill chain.

- Detailed analysis: An advanced research for all these hypotheses, there could be impacts, but limited at specific moments, and not for the whole period.

5.2 Conclusion

5.2.1 Summary of Contributions

This research makes several contributions to the field:

1. Establishes a methodological framework for analyzing blockchain network performance in relation to external factors.
2. Provides a multi-regional analysis of external factor impacts on Ethereum network performance.
3. Identifies distinct security threat patterns between Ethereum and non-Ethereum hosts.

5.2.2 Key Findings

The primary findings of this research include:

1. There are no more attacks on Ethereum nodes than on other servers.
2. Distinct security threat patterns between Ethereum and non-Ethereum hosts.
3. Regional variations in attack patterns, though without significant impact on network performance.
4. No significant correlations between external factors (cyberattacks, geomagnetic activity, news events) and Ethereum network performance

This research demonstrates that while the Ethereum network shows remarkable resilience to external factors, understanding and addressing the distinct security challenges faced by blockchain infrastructure remains crucial for its continued evolution and adoption.

Reference List

Boteler, D. H., 2003: Geomagnetic hazards to conducting networks. *Natural Hazards*, **28 (2)**, 537–561, https://doi.org/10.1023/A:1022902713136.

Buterin, V., D. Reijsbergen, S. Leonardos, and G. Piliouras, 2020: Incentives in ethereum's hybrid casper protocol. *International Journal of Network Management*, **30 (5)**, e2098, https://doi.org/https://doi.org/10.1002/nem.2098, URL https://onlinelibrary.wiley.com/doi/abs/10.1002/nem.2098, e2098 nem.2098, https://onlinelibrary.wiley.com/doi/pdf/10.1002/nem.2098.

Chen, H., M. Pendleton, L. Njilla, and S. Xu, 2020a: A survey on ethereum systems security: Vulnerabilities, attacks, and defenses. *ACM Comput. Surv.*, **53 (3)**, https://doi.org/10.1145/3391195, URL https://doi.org/10.1145/3391195.

Chen, T., Z. Li, Y. Zhu, J. Chen, X. Luo, J. C.-S. Lui, X. Lin, and X. Zhang, 2020b: Understanding ethereum via graph analysis. *ACM Trans. Internet Technol.*, **20 (2)**, https://doi.org/10.1145/3381036, URL https://doi.org/10.1145/3381036.

ENGLE, R. F., and V. K. NG, 1993: Measuring and testing the impact of news on volatility. *The Journal of Finance*, **48 (5)**, 1749–1778, https://doi.org/https://doi.org/10.1111/j.1540-6261.1993.tb05127.x, URL https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1540-6261.1993.tb05127.x, https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1540-6261.1993.tb05127.x.

Kim, S. K., Z. Ma, S. Murali, J. Mason, A. Miller, and M. Bailey, 2018: Measuring ethereum network peers. *Proceedings of the Internet Measurement Conference 2018*, Association for Computing Machinery, New York, NY, USA, 91–104, IMC '18, https://doi.org/10.1145/3278532.3278542, URL https://doi.org/10.1145/3278532.3278542.

Kushwaha, S. S., S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, 2022: Ethereum smart contract analysis tools: A systematic review. *IEEE Access*, **10**, 57 037–57 062, https://doi.org/10.1109/ACCESS.2022.3169902.

Masoud, M. Z., Y. Jaradat, A. Manasrah, M. Ali, K. Suwais, and S. Almanasra, 2024: Ameasurement study of the ethereum underlying p2p network. *Computers, Materials & Continua*, **78 (1)**.

Wolf, T., and Coauthors, 2020: Huggingface's transformers: State-of-the-art natural language processing. URL https://arxiv.org/abs/1910.03771, 1910.03771.

Zhang, M., R. Li, and S. Duan, 2023: Max attestation matters: Making honest parties lose their incentives in ethereum PoS. URL https://eprint.iacr.org/2023/1622, Cryptology ePrint Archive, Paper 2023/1622.

1 Appendix A

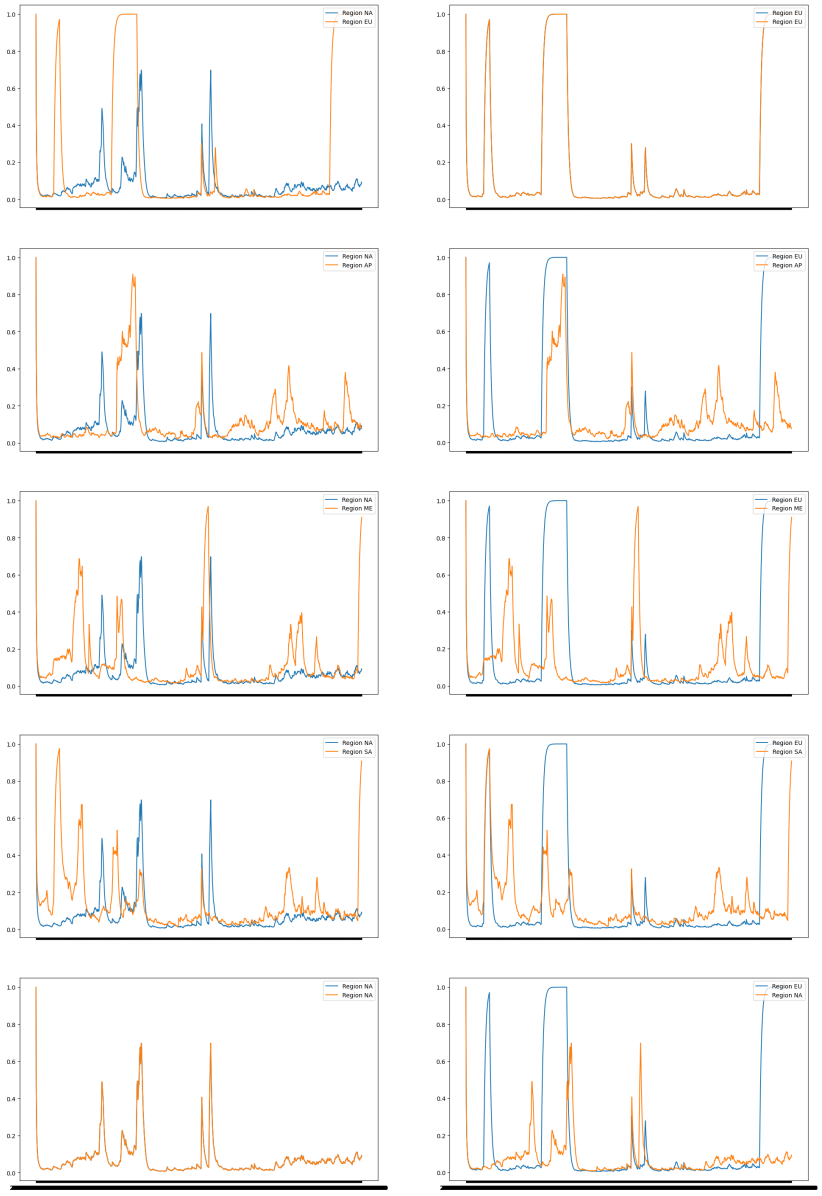


Figure A.1: Attestation causality between regions

On the left, NA vs EU, AP, ME, SA, NA in this order. On the right, EU vs EU, AP, ME, SA, NA.