Economics of the Helium Network: User Demand and Network Traffic

Kristijan Hornung
School of Cybersecurity
Old Dominion University
1113A Monarch Hall, 4607 Hampton Blvd.,
Norfolk, VA 23529
kristijan.hornung1@gmail.com

***Abstract*— Wireless network systems operating with blockchain technology provide application programming interface (API) utilities for fetching useful information about data traffic on the network. Helium Network is a distributed protocol used to share internet connectivity, whose Blockchain API contains data about transactions, users, hotspots, and other features of the network. In this research, Blockchain API was accessed with Python language, and the retrieved data was organized using various libraries (NumPy, Matplotlib, etc.) to plot graphs that depict economic trends of the network over the last several months to a year for some statistics and comparisons. Part of the attention was focused on HNT (Helium Network Token andvirtual currency) rewards for participating hotspots, which provides a means to measure network demand. The results are mostly in the form of list rankings and linear graphs. They show among other things that currently, Helium network is not as much utilized for its data transfer oriented functions as it is centered around coverage validation and transaction witnessing.**

Keywords—IoT devices, Decentralized Wireless Network (DWN), Global navigation satellite system (GNSS), Blockchain technology, Digital transactions, Application Programming Interface (API), Hypertext Transfer Protocol (HTTP) requests, Hotspot, Network User, Network Miner, Helium Network Token (HNT), Consensus Protocol, Consensus Group, Proof-of-Coverage (PoC), Python.

I. Introduction

The term Internet of Things dates to more than 22 years ago, when it was first used by the Auto-ID Labs at Massachusetts Institute of Technology (MIT) as part of the study of networked radio-frequency identification technology. The present definition by the International Telecommunication Union describes IoT as a "global infrastructure" providing services by interconnecting devices "based on, existing and evolving, interoperable information and communication technologies" [5]. IoT (Internet of Things) devices comprise all the hardware that connects to the Internet and exchanges data by means of communication networks. Such devices usually require sensors to be able to connect to the Internet. Originally, IoT was envisioned as a system of devices with radio-frequency sensors connected to the Internet, which would be used in a corporate supply chain for tracking products without the need for human overlook [6]. One such network designed for IoT devices is the Helium Network, a decentralized wireless network (DWN) to which devices all over the globe can connect wirelessly and self-geolocate, without any assistance from GNSS satellites for positioning and navigation [1]. DWNs have no central authority that verifies and manages transactions. Transaction integrity, security preservation, and cryptocurrency supply in DWNs are all based on a system of decentralized control [2]. Helium runs on a digital ledger of transactions called the Blockchain, with a native token (cryptocurrency) abbreviated as "HNT" [1]. In a taxonomy of blockchain systems, Helium ledger falls into a category of public blockchains. This means that all transactions on the network are visible to the public, and that all nodes (coverage providers) can become members of the consensus process [3]. Consensus process on the Helium network is achieved with the high-throughput and censor-resistant Consensus Protocol, which is based on a Consensus Group of miners elected in each epoch validating and forming transactions received by other Miners into blocks and adding them to the Blockchain [1]. Miners (coverage providers) earn HNT for their services, while users (consumers) pay them in HNT for connecting to the Internet. The Blockchain facilitates network decentralization and competition among miners to provide coverage, thus eliminating any corporation's monopoly over Internet industry [1]. Helium Blockchain database (the transaction ledger) is digitally accessible by means of the Blockchain API, a programming interface that can be utilized with simple HTTP requests (which are used to access resources/data on Internet servers). A method of using HTTP requests is a way to access information about all the previous transactions that occurred on the Helium network. It also provides information about other aspects of Helium like network statistics, organization, and the native token (currency) fluctuations. This led us to conclude that the Blockchain API can be used to study Helium network's dynamics, as well as its economic supply and demand. An objective of this research work was to make use of the Helium Blockchain API interface to fetch data about specific types of digital transactions, which would later help us analyze the demand side of the network. The programming environment chosen for this project was Anaconda, an open-source distribution of the Python and R languages. Python was selected as the most suitable language, and several different libraries and modules were employed to facilitate data collection. Python programs first had to establish connection with the Blockchain API with the help of HTTP requests, which was made possible thanks to the Requests library. The data extracted from the Blockchain database was then processed and stored in data structures appropriate for further analysis. Once the data was collected and saved on a local machine, it was represented either in numerical form tables, or visually in the form of linear graphs. For this, we used Matplotlib library in Python. The demand for the Helium network's coverage was analyzed by observing two relevant variables: HNT rewards hotspots for various services, and overall data traffic on the network. Analysis of Miner HNT rewards showed that most hotspots in all areas of study derived most of their token earnings from participating in the proof of coverage process with other hotspots' coverage. Furthermore, very low data traffic was observed in most areas, while serious disproportionalities existed between total data transfer rates when comparing certain cities. These findings hint at generally lower-than-expected user demand, and small levels of network prevalence in towns, cities, and their respective urban/metro areas. Further research of Helium Network's presence in other regions of the United States and/or other countries could be useful for a more elaborate analysis of Helium's economics.

This research was hosted by Old Dominion University and was sponsored by NSF (National Science Foundation).

II. Helium network structure

Listed below are the key components and principles governing the Helium Network:

- **Proof-of-Coverage:** a procedure for Miners to prove they are providing wireless coverage within their designated coverage area [1].

- **Helium Consensus Protocol:** a protocol that creates trustless and public, high-throughput, and censor-resistant system; a byzantine fault tolerant protocol which enables achieving consensus on transaction veracity throughout the network [1].

- **WHIP:** open, long-range, wireless, and low-power network protocol that can be used on inexpensive, commodity hardware. Any such hardware compatible with WHIP can communicate over large geographical areas and connect to the Helium network. WHIP is based on resilient public key cryptographical rules, with device data being encrypted to maintain security [1].

- **Proof-of-Location:** a system for finding the geolocation of a device connecting to the Helium network through WHIP. It does not need resource costly satellite compatible hardware to operate. By submitting Proofs-of-Location, devices publicly establish their geolocation and add it to the Blockchain [1].

- **Blockchain:** a decentralized, immutable, and foolproof public ledger containing record of all past transactions exchanged on the network. Blockchain is a database distributed over all network participants, which effectively removes any need for a central authority with respect to verifying transactions between two or more parties. It relies heavily on strong cryptography, using public and private keys to ensure a tamper-proof system for transaction and data exchange on the network. Once added to the end of the Blockchain, a transaction cannot be changed or disputed by any party, which means that the ledger is practically irreversible. Consensus strategies are employed to verify integrity of financial or data transactions on the network [4].

III. The Idea of a Decentralized Wireless Network (DWN)

A decentralized wireless network like Helium provides wireless access to the Internet to all devices capable of connecting to it. All participants in the Helium network must comply with the WHIP protocol in order to become part of the DWN. The physical foundation of Helium is composed of multiple independent internet connected Hotspots which provide coverage. Routers on the network pay Miners (Hotspot owners) to send data to or receive it providing internet connectivity to clients. Miners are in return paid in native tokens (HNT) for providing coverage and transferring user data. HNT is a completely digital token that is decentralized, and its exchange is based on cryptography, much like Bitcoin. As such, HNT is considered to be a cryptocurrency. All the transactions on the DWN are recorded in a decentralized digital ledger called the Blockchain, which is in its essence very similar to the blockchain technology used by networks like Bitcoin and Ethereum [1] [2].

IV. Participants in the Helium network

Helium network is comprised of three types of participants: devices, miners, and routers. Together they exchange transactions and transmit data across the network. Each participant has their respective role in the network, as described in the classification below [1].

A. Devices

Consumers on the Helium network are owners of devices with radio transceivers compatible with the Helium network's wireless protocol. These devices send and receive data from the network, for which they pay Miners in the HNT cryptocurrency. All data sent from devices is stored in the Blockchain [1].

B. Miners

Miners are users who are owners of hotspots. Hotspots are physical devices (hardware) which provide Internet coverage over broad geographical areas. They transfer data between the user's WHIP-compatible devices and their respective routers on the Internet. In addition, they regularly submit Proofs-of-Coverage, which are components of an electronic protocol for proving and verifying network coverage service in a hotspot's operational range. When joining the network, miners need to purchase a WHIP-compatible hotspot and stake an initial token deposit. Each miner is then assigned a score, which grows as they continuously provide coverage and transfer data or diminishes as blocks pass on the blockchain without them submitting valid Proofs-of-Coverage. Each epoch, a group of best scoring miners is selected for a Consensus group, which mine and add new blocks to the blockchain, thereby receiving HNT rewards. Miner's chance of being elected to a Consensus group depends on their overall score [1].

C. Routers

Routers are solely organizations that acquire data credits by burning HNT, which they sell to Users as a subscription. Routers are also an integral part of a Proof-of-Locations, because by receiving from Miners the data they fetch from Devices, Routers can geolocate Devices without the need for GNSS satellite positioning. Devices choose to which Routers they want their data to be sent. Upon receiving Device data, Routers must inform Hotspots that their Miners should be paid for data transfer service [1].

V. Methodology

A. Software and Tools

Data collection and representation phases of this research were all carried out on a machine with Intel Core i7-6700HQ CPU (2.60 GHz), Intel HD Graphics 530 GPU, 16 GB of RAM memory, and Windows 10 OS.

Several software applications were used for this research. The programming language chosen as most suitable for this specific kind of data analysis was Python.All of the applications were written in a generalized manner so that they could be easily applied and used in any location for analysis. Python is a high level, scripting and interpreted programming language suitable for data science. It was run on an environment distribution called Jupyter Notebook. Jupyter is a web-based open-source interactive computing environment developed for work in various programming languages. In this research, it was used for file organization and running Python code. All project files with code and data were maintained on a public GitHub repository. GitHub is an Internet software development platform for storing files and team working on coding projects. Python libraries and modules used in the research are the following:

- NumPy: with tools for array manipulation.
- Matplotlib: for data visualization in the form of linear graphs.
- Requests: for HTTP access.
- JSON: a syntax for more readable storing of data.
- Time: for working with time parameters.
- Datetime: with tools for using time and date parameters.
- Pickle: for converting output objects into byte streams, which are then stored into files.

B. Algorithm used for data collection and representation process:

Four programs in Python were written to obtain all the data required for network demand analysis. The library used for communicating with the Blockchain API was Requests library. Original fetched results were in dictionary (key value pair) format. JSON syntax was used for making the request output more readable by applications. Since the desired data was very large in memory size, the Blockchain would return a cursor code, which had to be used iteratively to get further batches of data for each HTTP request. Once full data outputs were obtained, programs searched for specific information within data dictionaries and stored it in proper data structures (lists, dictionaries, etc.) Upon getting all the necessary numerical and/or textual data, algorithms would use Matplotlib library to plot the results over specified time intervals for each hotspot address or area under study. In each program execution, geographical latitude and longitude information had to be provided, to specify the area being analyzed; along with the perimeter distance around the chosen geographical point. In addition, desired time intervals for time series graphing were selected in each program run. The visual data had to be represented more succinctly, so the Pickle module was employedto serialize and store the large data structures and read in to plot the mean data of all the hotspots and cities/metro areas in a given perimeter within the same graph.

Algorithm: Connecting to and extracting data from the Blockchain API

1. Select the latitude (lat) and longitude (lon) of the geographical point under study (to find all hotspots in the area), along with starting and terminating point in time for the data to be fetched.

2. Connect to the API via an HTTP request with following parameters: selected lat and lon, and desired perimeter (distance d) around the point; d = 32187 m was mostly used.

3. Iterate over a loop using consecutive Cursors by inserting them as parameters into an HTTP request (to fetch the full output).

4. Convert output received containing hotspot addresses into a JSON dictionary.

5. Extract from the output all hotspot addresses into a new dictionary, with addresses saved as keys (dictionary).

6. In a new loop, iteratively send new HTTP requests to the Blockchain API with all hotspot addresses from the saved dictionary; possibly multiple times for each hotspot using Cursors.

7. Extract the desired data (HNT earnings, number of data packets transferred, etc.) from the output and save it as a list in each dictionary key (hotspot address).

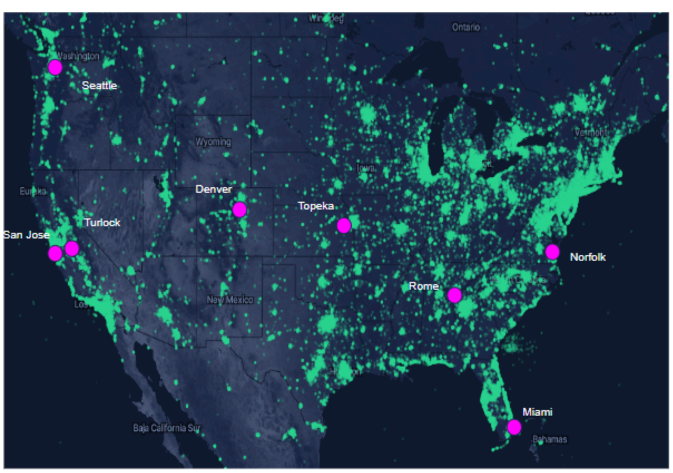
8. Process the numerical data in each list for each address.

9. Plot the results for each area of study either for each individual hotspot address, or as mean cumulative value for top x HNT earning/data transferring hotspots; x = 50 was mostly used.

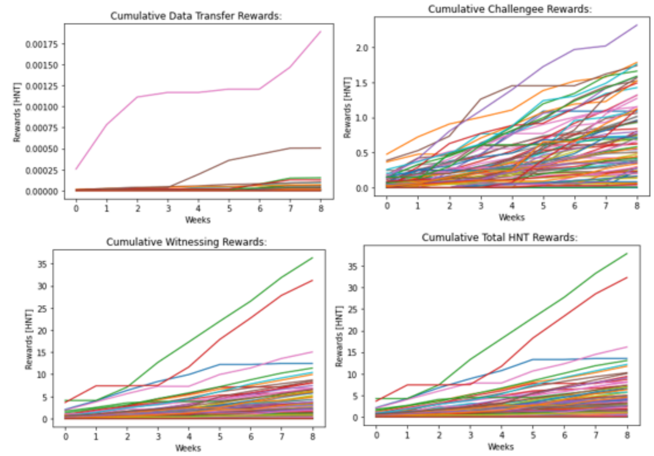
VI. Results

The first object of study about the demand side of the Helium Network's economics were HNT rewards. The goal was to determine how many hotspots in selected regions earn HNT tokens for each type of service provided: PoC Challengee (for proof of providing coverage), PoC Challenger (for Validator nodes who submit a PoC receipt to the Blockchain), Witnessing (for hotspots which witness other hotspots proving their coverage), Consensus (for Validators who form a Consensus Group and mine blocks), Security (for any holders of security tokens), Data Transfer (for hotspots which route data packets on the network from devices), and total HNT rewards for all services. This survey was conducted for a total of seven cities and towns: 1. Topeka, Kansas, 2. Norfolk, Virginia, 3. Denver, Colorado, 4. Miami, Florida, 5. Seattle, Washington, 6. Rome, Georgia, 7. Turlock, California). The results were plotted for each hotspot address in each region and converted to cumulative values over a period of around nine weeks (from 5/25 to 7/27, 2022). Note: Cumulative HNT rewards for Challenger, Consensus, and Securities roles were equal to zero (flat line graph) for all hotspots in all locations studied. Each colored line graph in the plots below represents one hotspot providing some type of service and thus making HNT (depending on the plot context).

FIGURE I. Approximate locations of cities surveyed for the study. Light green areas represent hotspot distribution throughout the contiguous United States. More prominently colored areas signify larger hotspot density, and therefore better network coverage.

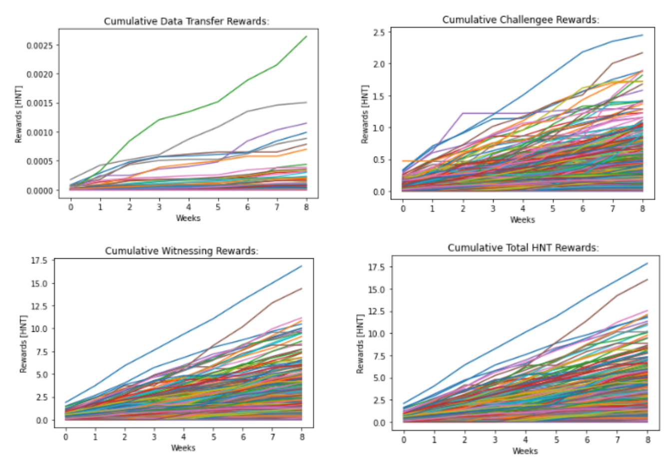


GRAPH SET I. Cumulative HNT rewards for all hotspots in 20-mile radius from the center of Topeka, KS.



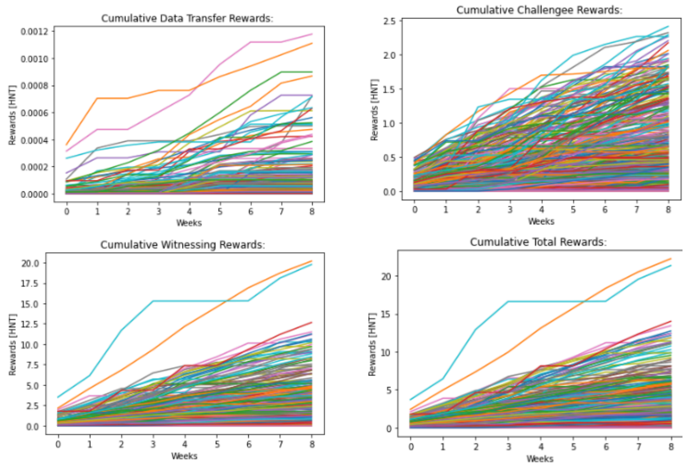
In Topeka, KS, there are two hotspots responsible for more data transfer than most other coverage providers in the city (visible as a pink and a brown line with clearly larger HNT rewards than all other linear graphs on the Cumulative Data Transfer Rewards plot, which show very low HNT rewards (< 0.00025). Another pair of hotspots did most witnessing, seen on the Cumulative Witnessing Rewards plot as a green and a red line, each earning over 30 HNT from witnessing. All other hotspots earned less than 20 HNT from witnessing.

GRAPH SET II. Cumulative HNT rewards for all hotspots in 20-mile radius from the center of Norfolk, VA.



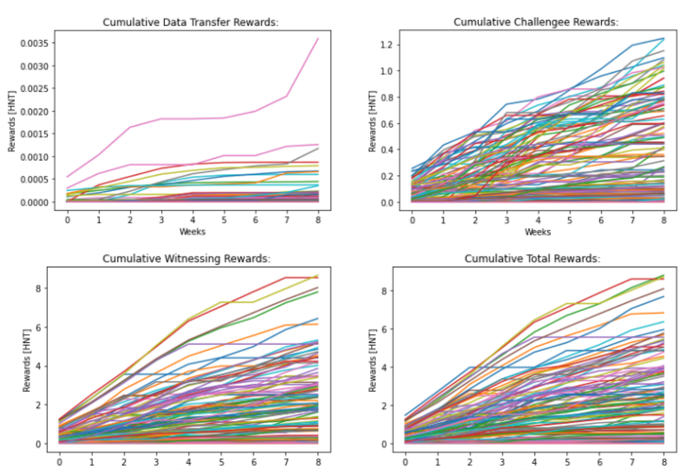
Data transfer in Norfolk, VA is dominated by seven hotspots, with one hotspot standing out with over 0.0025 HNT earned over the nine-week period (green line graph in Cumulative Data Transfer Rewards plot). Witnessing activity is much more distributed over hotspots, as most of them earned up to 10 HNT, and only several made more than 10 HNT in nine weeks.

GRAPH SET III. Cumulative HNT rewards for all hotspots in 20-mile radius from the center of Denver, CO.



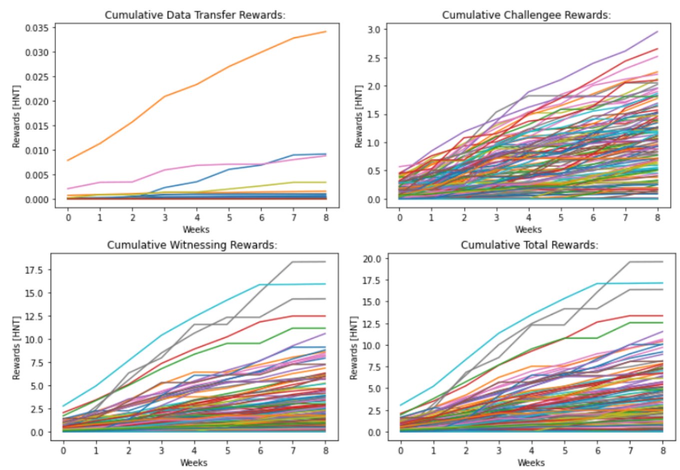
As for Denver, CO, hotspot data transfer activity is much better distributed than in Topeka, KS and Norfolk, VA, since many more colored lines with similar HNT earnings are visible in the Cumulative Data Transfer Rewards plot. However, average HNT earnings from data transfer are still very low for a city as large as Denver (almost 3 million residents in metro area, compared to slightly over 200 000 in Topeka metro area and around 1.7 million in Norfolk metro area). All hotspots in Denver made less than 0.002 HNT by transferring data, as did almost all hotspots in Topeka and Norfolk. This is inconsistent with city size, because Denver is significantly more populated than both Topeka and Norfolk, and should therefore have higher network data traffic. Since Denver and Norfolk are much bigger than Topeka, they have more densely situated linear graphs in Cumulative Witnessing Rewards plots, suggesting more active hotspots overall.

GRAPH SET IV. Cumulative HNT rewards for all hotspots in 20-mile radius from the center of Miami, FL.



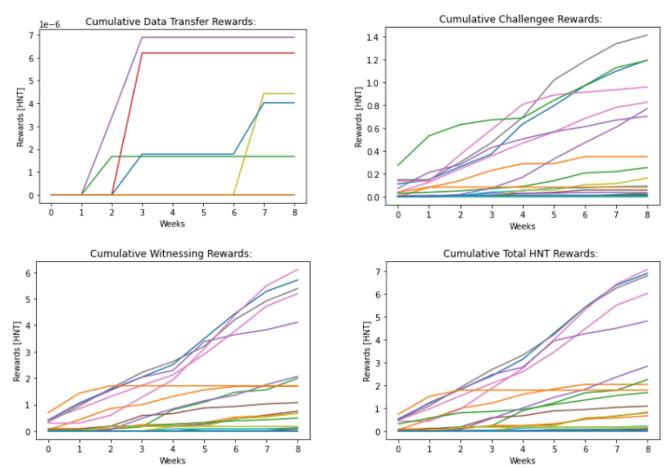
As seen above, most hotspots in Miami, FL made less than 0.0015 HNT from data transfer, similar to hotspots in Norfolk and Denver. But Miami is a large city with more than 6 million people in the metro area, implying that its data traffic should be much larger than in Norfolk and Denver, as more users would be connected to the network assuming that the network is widely utilized. Also surprising is the Cumulative Witnessing Rewards plot, which shows that no hotspots earned more than 9 HNT from witnessing. More HNT was made by witnessing in Norfolk and Denver, even though they are smaller cities than Miami. Large network with many users would require proportional witnessing activity.

GRAPH SET V. Cumulative HNT rewards for all hotspots in 20-mile radius from the center of Seattle, WA.



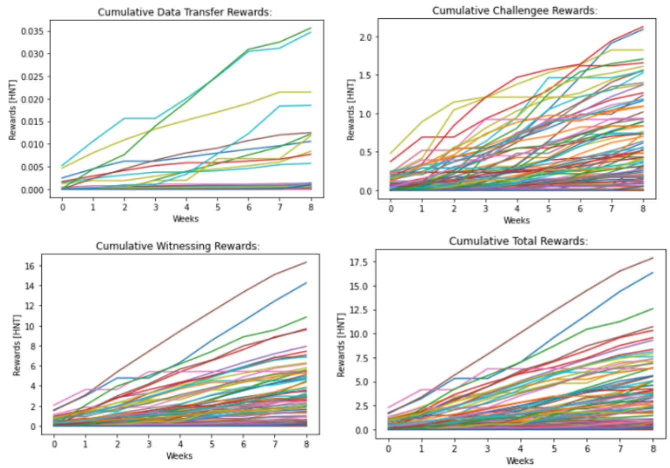
Cumulative data transfer in Seattle, WA seems to be as undistributed over hotspots as in Topeka, KS, judging by only a few linear graphs in the plot with noticeable HNT rewards. However, three hotspots earned more than 0.005 HNT by transferring data, which outperforms data transfer in Topeka, Norfolk, and Miami. Witnessing activity plot is similar to Denver's and Norfolk's respective plots, with most hotspots earning up to 10 HNT by witnessing.

GRAPH SET VI. Cumulative HNT rewards for all hotspots in 20-mile radius from the center of Rome, GA.



Given that Rome, GA is a small city with slightly below 40 000 residents, its data transfer and witnessing activity are accordingly low compared to all other areas studied. We see this phenomenon in the number of colored lines in the plots above. All graphs for Rome are very sparsely situated compared to plots for other cities, and total data transfer rewards are very low (in a 10^{-6} range). This difference in values of HNT rewards logically fits the size of the city, because Rome is much less populated than most other cities observed.

GRAPH SET VII. Cumulative HNT rewards for all hotspots in 20-mile radius from the center of Turlock, CA.



Hotspots in Turlock, CA exhibit larger HNT earnings from data transfer than those in all other cities except for Seattle, WA. We can see almost a dozen line graphs going above 0.005 HNT earnings on the Cumulative Data Transfer Rewards plot. Interestingly, even in Seattle only three hotspots exceed this much HNT made by transferring data. Average witnessing activity seems to correspond to that in other major cities like Norfolk, Denver, and Seattle, with some hotspots having made more than 10 HNT from witnessing. This is unusual due to the size of Turlock (little over 70 000 residents), because Norfolk, Denver, and Seattle are much larger cities. This suggests that Helium network is probably being more utilized in Turlock than in other cities surveyed, despite the fact that Turlock does not have as many active hotspots as some other cities like Seattle and Denver.

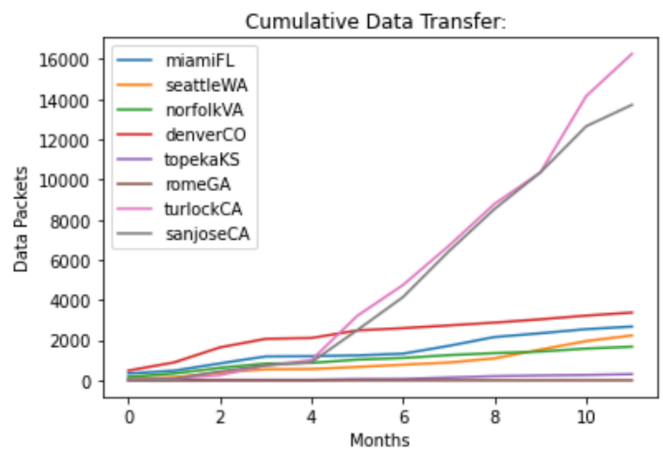
Next, a rank list of hotspots was created for six locations based on the total HNT earnings. This gave us insight into what portion of hotspots participate in the network through mining, as well as approximately how much HNT top-performing hotspots make. The data comes from a one-month period from 6/23 to 7/23, 2022. Results are organized in the table below.

TABLE I. Ratio of active hotspots in six locations, and range of total HNT earnings for top 10 mining hotspots.

	Denver, CO	Miami, FL	Seattle, WA	Turlock, CA	Topeka, KS	Rome, GA
Ratio and percentage of hotspots earning HNT from mining	291 out of 364 (80%)	99 out of 131 (76%)	107 out of 144 (74%)	81 out of 110 (74%)	81 out of 104 (78%)	19 out of 52 (37%)
Range of total earnings by top 10 hotspots [HNT]	5.91 to 11.17	2.82 to 3.47	4.60 to 13.35	3.93 to 8.63	5.21 to 20.32	0.67 to 4.12

Furthermore, to better asses the network data transfer rates from devices to hotspots, and therefore the demand for Helium, we created a graph showing mean cumulative data transfer for 50 top-performing hotspots in eight locations of study over the last year (from August 2021 to August 2022, more precisely around 360 days). Data transfer was measured in the number of data packets sent from devices (1 data packet = 24 bytes). Note: San Jose, California was added as another location in this survey.

GRAPH I. One year mean cumulative data transfer for top 50 hotspots in eight areas of study.



Finally, now that we collected data which shed light on HNT rewards and data transfer scores for hotspots in selected areas, we proceeded to making a table that compares percentages of hotspots transmitting data over the network to percentages of hotspots performing all other services (proving coverage and earning Challengee rewards or witnessing other hotspots' coverage and earning Witnessing rewards).

TABLE II. Percentages of hotspots transferring data compared to percentages of hotspots providing other services (PoC Challengee or PoC Witnessing) in seven locations (data for a period from 5/25 to 7/27, 2022).

	Denver, CO	Miami, FL	Norfolk, VA	Topeka, KS	Turlock, CA	Rome, GA	Seattle, WA
Data Transfer	257/365 (70%)	64/137 (47%)	126/487 (26%)	49/104 (47%)	73/111 (66%)	5/52 (10%)	66/144 (46%)
PoC	310/365 (85%)	110/137 (80%)	363/487 (75%)	81/104 (78%)	84/111 (76%)	19/52 (37%)	109/144 (76%)

VII. Discussion

Similarity between Witnessing and Total HNT rewards (in line shape and y-axis values) suggests that majority of hotspots derive most of their earnings from witnessing transactions as part of PoC challenges. Data Transfer accounts for low earnings across all studied areas (judging by the y-axis values). Very few miners provide significant Data Transfer service compared to performing Challengee or Witnessing roles (based on the density of linear graphs for each). Most hotspots perform Challengee roles, while only a small fraction transfers data across the network. This means that most hotspots make HNT from solely providing coverage and/or witnessing other hotspots providing coverage (as part of PoC protocol). From this we observe low network traffic, and low user demand. Around 70-80% of hotspots perform mining in all locations (except for Rome, GA), while other hotspots are inactive or have only recently been added to the network. Cumulative data traffic graph (GRAPH I.) for eight locations examined suggests an interesting discrepancy between city/town size by population and mean data traffic over the course of one year. Noteworthy is a comparison between Turlock, CA (population: 72 740 in 2020) and San Jose, CA (population: over 2 million residents in metro area; center of the Silicon Valley), because we can observe higher average data traffic in Turlock than San Jose, which is quite unexpected. Less populated locations like Turlock, CA should naturally have less consumers in the wireless network with less data being exchanged than would be the case in more densely populated areas and major cities like San Jose, CA. This is a significant demand inconsistency. Lastly, TABLE II. hints at the correctness of the previous findings about data traffic rewards as compared to PoC rewards to hotspots. It shows how in every location studied, more hotspots provide PoC services than data transfer service. In some areas this ratio is higher than 2 : 1.

VIII. Conclusion

The work presented in this paper shows that Helium Network demand is not yet fully established in cities and towns where we examined hotspot activity. Its data traffic is low compared to any other wireless alternatives such as Wi-Fi or cellular networks, since it was only measured in thousands or hundreds of data packets in the locations we sampled.The incentives of the Helium network seem to have been established early to encourage new miners to actively participate in consensus. By doing this, the network is able to establish before the demand arrives. Since most hotspots make majority of their cryptocurrency earnings from simply providing coverage and/or witnessing coverage of other hotspots, we can conclude that Helium is not at this point in time a widespread Internet network capable of serving large communities of Internet consumers. Therefore, Helium is at present not a significant competitor to other wireless network solutions, but that does not say anything about its future prevalence as an Internet access network. Its decentralized and secure publicly visible blockchain with complex and yet effective cryptography in the background might bring this network much more popularity and user demand in the future.
All Python code and the data used for this research is available in a public repository on GitHub at: https://github.com/kristijanH1998/REU-Summer-Internship.
Further research can be conducted based off this work. For example, it would be insightful to take a deeper look into HNT fluctuation and data traffic over longer time periods for a more methodical economic analysis. Such work could be useful for other students and scholars interested in studying decentralized IoT networks and virtual currencies. With the Blockchain being an open public ledger (meaning that vast and detailed data about the network is available through the access to the Blockchain API), there exists a revolutionary opportunity for researchers (data scientists, cybersecurity specialists, professors etc.) to study economics of decentralized wireless networks. Further research similar to this will be interesting to observe over time if demand for the Helium network increases, identifying the environmental factors that attribute to a miners success will be extremely desired.

IX. Acknowledgment

This research experience was sponsored by the National Science Foundation and hosted by The Old Dominion University. Special thanks to the mentor Dr. Sachin Shetty. Special thanks to the program directors, Dr. Chunsheng Xin and Dr. Khan Iftekharuddin, for the opportunity to participate in the research program. Special thanks to the graduate student and Lead Project Scientist Mr. Peter Foytik, who guided me throughout this research.

X. References

[1] Haleem, A., Allen, A., Thompson, A., Nijdam, M., & Garg, R. (2018, November 14). *Helium - A Decentralized Wireless Network*. Helium Whitepaper. Retrieved from http://whitepaper.helium.com/

[2] Halaburda, H., & Gandal, N. (2016, June 27). *Competition in the Cryptocurrency Market*. SSRN. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2506463

[3] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*. ResearchGate. Retrieved from https://www.researchgate.net/profile/Hong-Ning-Dai/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends/links/59d71faa458515db19c915a1/An-Overview-of-Blockchain-Technology-Architecture-Consensus-and-Future-Trends.pdf

[4] Puthal, D., Malik, N. S., Mohanty, S. P., Kougianos, E., & Yang, C. (2018, March). *The Blockchain as a Decentralized Security Framework [Future Directions]*. ResearchGate. Retrieved from https://www.researchgate.net/publication/323491592_T

he_Blockchain_as_a_Decentralized_Security_Framework_Future_Directions

[5] Wortmann, F., & Flüchter, K. (2015, March 27). *Internet of Things*. ResearchGate. Retrieved from https://www.researchgate.net/profile/Felix-Wortmann/publication/276439592_Internet_of_Things/links/561e5c8c08aecade1acc0b54/Internet-of-Things.pdf?origin=publication_detail

[6] Rose, K., Eldridge, S., & Chapin, L. (2015, October). *The Internet of Things: An Overview*. Internet Society. Retrieved from https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf

[7] Foytik, P., & Hornung, K. (Eds.). (n.d.). *KRISTIJANH1998/reu-summer-internship*. GitHub. Retrieved October 18, 2022, from https://github.com/kristijanH1998/REU-Summer-Internship.git