ODC DATA EXPLORATORY HACKATHON REPORT

Data Source

The datasets used for this data exploratory analysis was that provided by the Open Data Community (ODC) and sourced from Ocean protocol a decentralized data exchange platform. These datasets are collections of two grants donation rounds which are the **Fantom** and **UNICEF** grants. These datasets contain transaction that occurred in the Fantom contribution from the 12th of December to the 1st of January and the UNICEF contribution from the 9th of December to the 21st. Alright, enough of the introductory story let's get into the data.

Tools Used
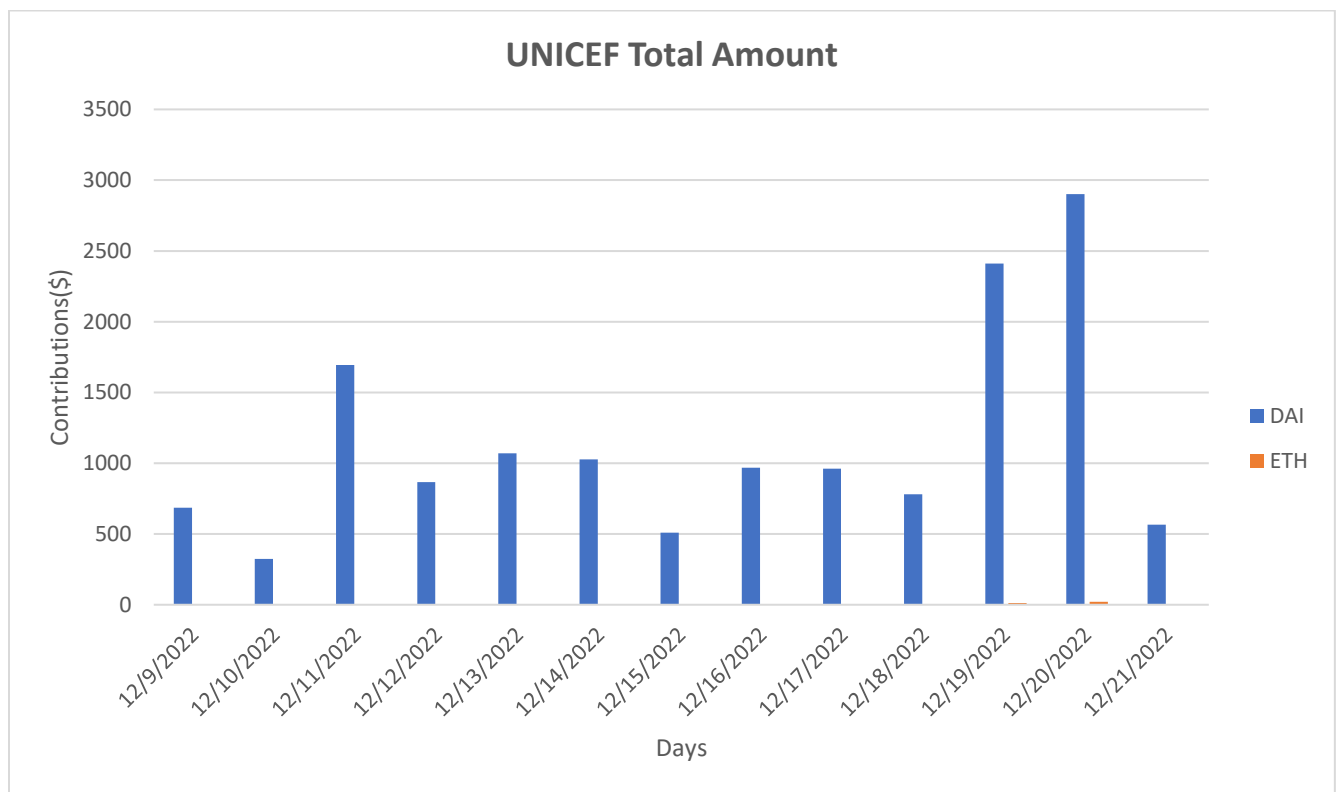
- Power BI
- Microsoft Excel

UNICEF Contribution

Fig 1

The chart above shows the total contributions made by each contributor in the donation round. A total of $14,830 was donated by 64,130 contributors including both sybils and genuine donors. A maximum of $500 was donated with a mean value of $0.23104. A descriptive analysis also showed a mode of $0.0001 indicating a high likelihood of sybil activities.
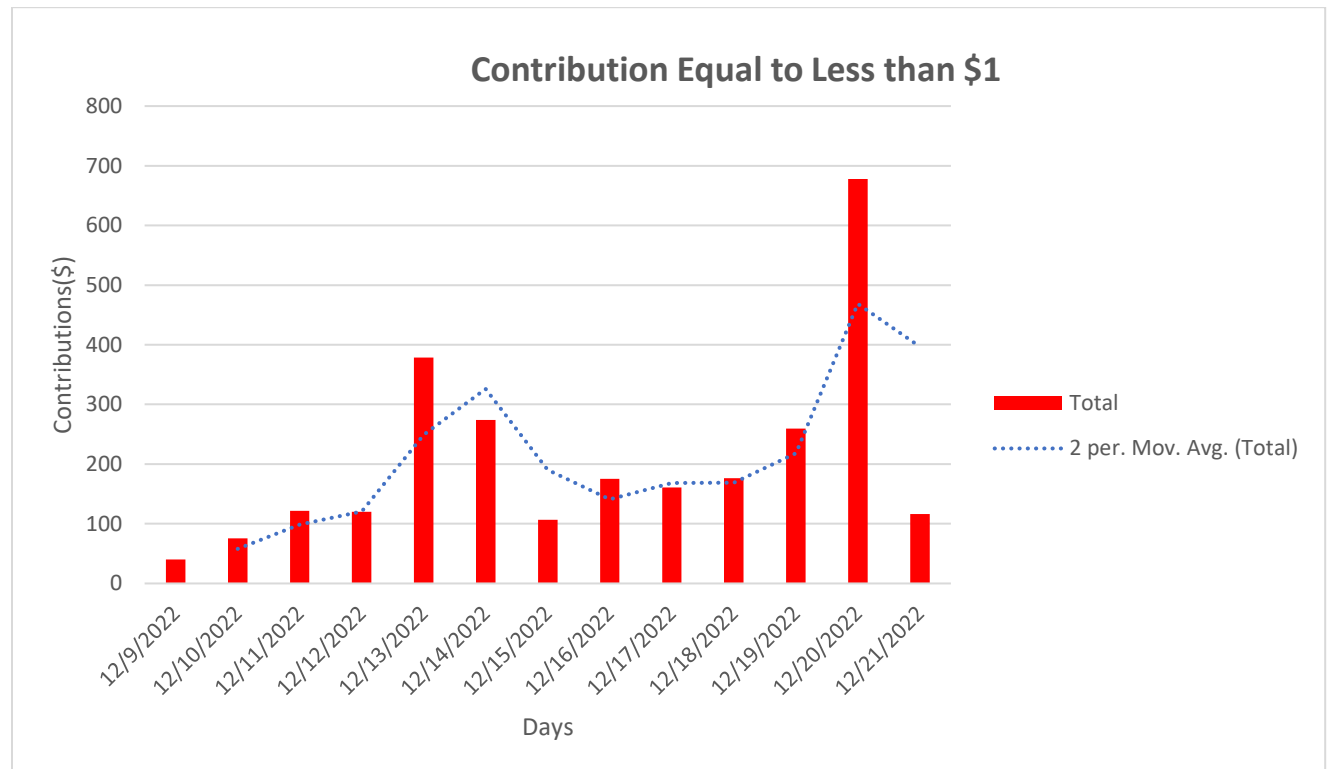

Fig 2

I filtered out addresses that contributed more than $1. This was because more 95% of sybil attackers contribute less than a dollar because of the nature of their attack. The chart above shows the distribution of contributions equal to or less than $1 for the UNICEF contribution round. A total of **$2,682** was contributed for this with **$2,620** worth of Dai token and **$62** worth of Eth token. From the chart above we can see that a high fluctuation in the trend shows that there was a massive number of activities in this chart indicating a large number of donations made from $1 and below. Fig 3 below also shows a distribution of each token per day.

From Fig 2 above we can deduce that the highest contribution was made on the 12th day of the contribution and also the lowest contribution was recorded on the opening day. Using the trend line to analyze the charts, similar patterns can be noticed between the total contributions made in Fig 2 and to the Dai token in Fig 3. This similarity in patterns by both charts concludes that the Dai token was the domineering token in terms of donations made.
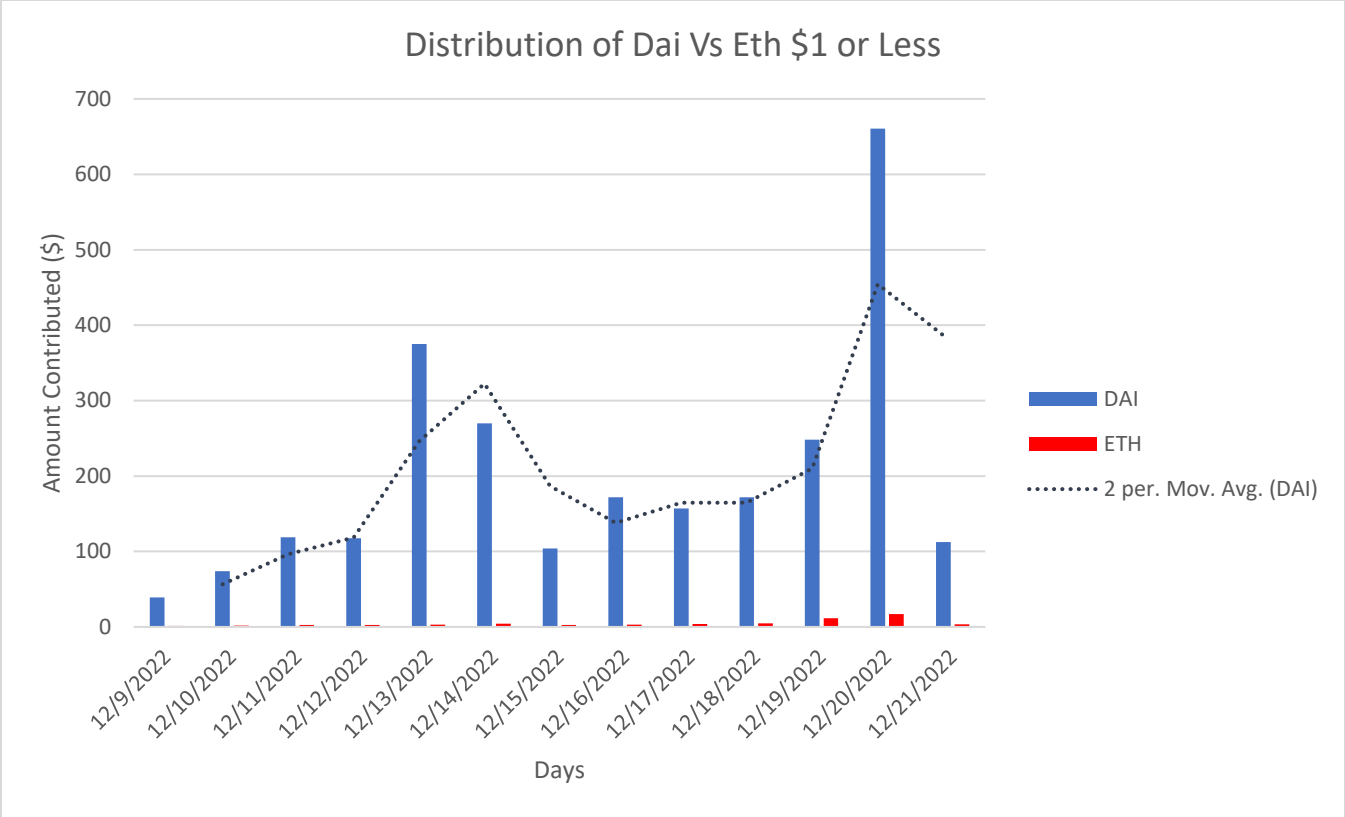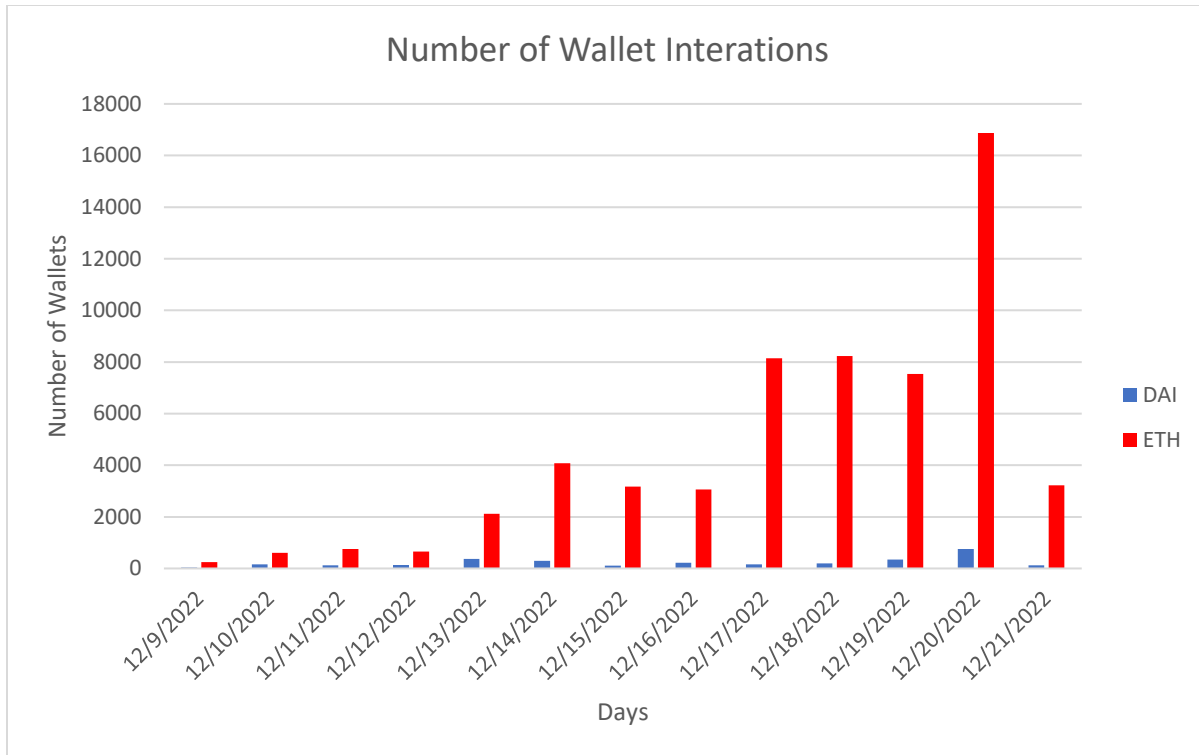
Fig 3

Fig 4

The chart above shows a distribution of the wallet interactions for the contribution. We can deduce that contrary to the amount of donation made the wallet interaction by Ethereum token donors supersedes that of Dai. A total of **61,742** contributions of $1 and below was deduced and 3047 of them were by Dai contributors while a whopping **58,695** of them were from Eth contributors. Further statistics sum up amount per contributor for Dai token to be **$0.86** and **$0.001** for Eth.

To uncover more trends and patterns I created a chart for the wallet interactions and amount contributed combined together.
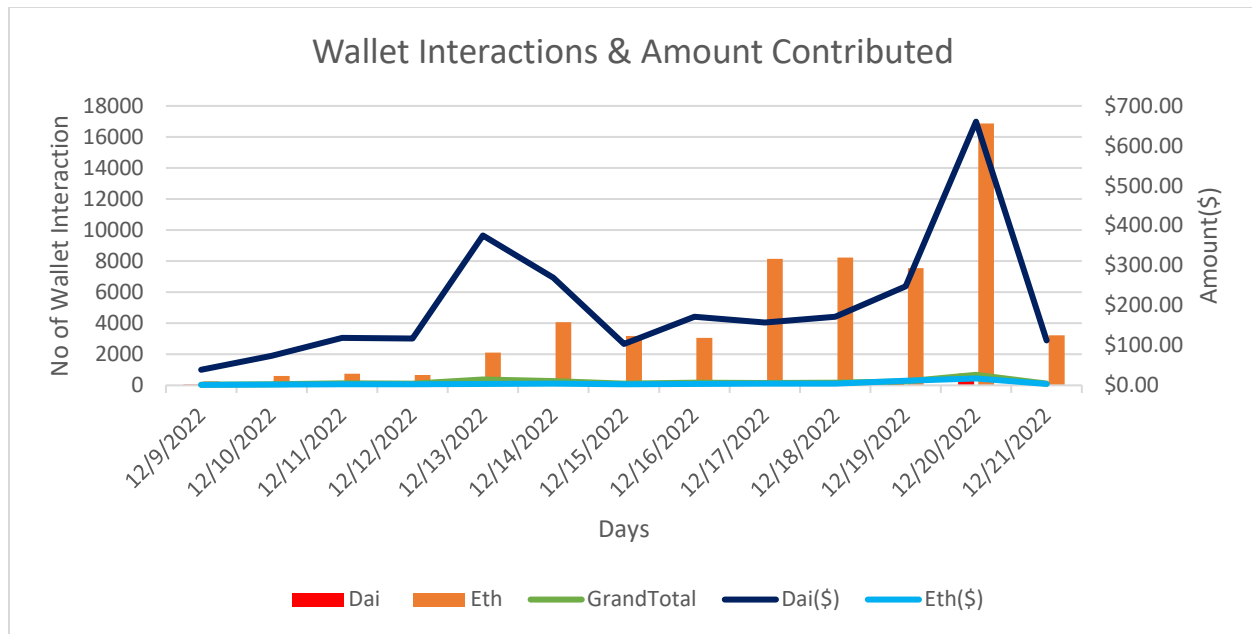
Fig 5

The ratio of amount per contributor for the Eth token was a high indication of a probable sybil attack. Also from Fig 5, we can analyze an almost uniform rate of activity in the amount of contribution made by Eth donors with the sky-blue line. This suggests that the sybil attack was always taking place in the donation with very little increase in the amount donated day by day.

A statistical description analysis was carried out to determine the most reoccurring donation or mode value of the donation made equal to or less than $1 and the result was **$0.0001.** To further analyze this result, I filtered down the value of the amount donated to only **$0.0001** the following conclusions were drawn from my analysis.

Initial Conclusions

- A total of **10,984** sybils suspect were discovered.
- A total of **$1.0984** of contribution was donated by these sybils.
- Ethereum was the only token used for this attack.
- This attack happened each day of the grant.
- Each donations made were to four destination wallets address only.

Note!!!

Below is a link to the dataset containing the sybils data. (Click to download)

https://market.oceanprotocol.com/asset/did:op:8b133e8d3d2b37e94e25485e7c98503e50546 1b9095e78af6960666b5cdd4cf6
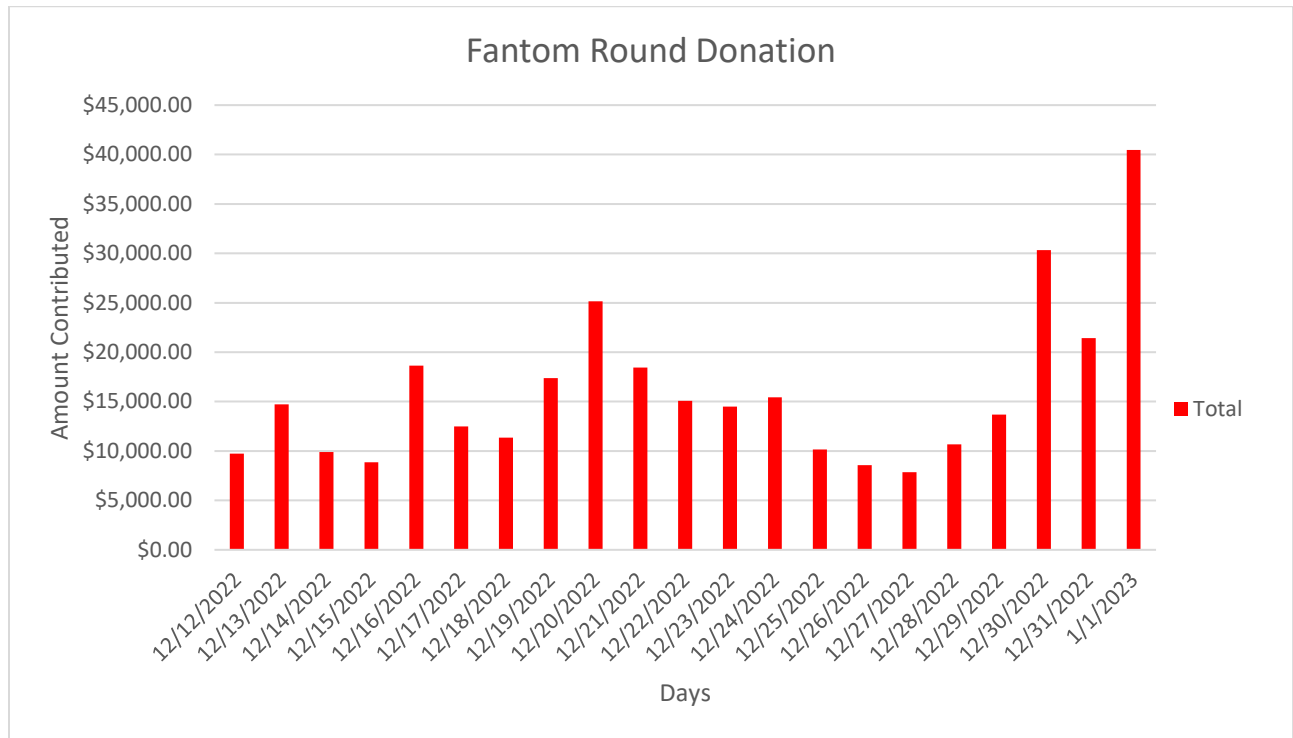
Fantom Round

Fig 6

The chart above gives an overview of the Fantom contribution round. The Fantom contribution round lasted for 21 days and recorded a sum total of **$334,863** donations. A total of **139,337** donors participated in this round (sybils included). An initial statistic description reveals $1 as the mode, also the distribution had a mean value of $2.40.   Fig 7 shows a distribution of the fantom round by tokens.
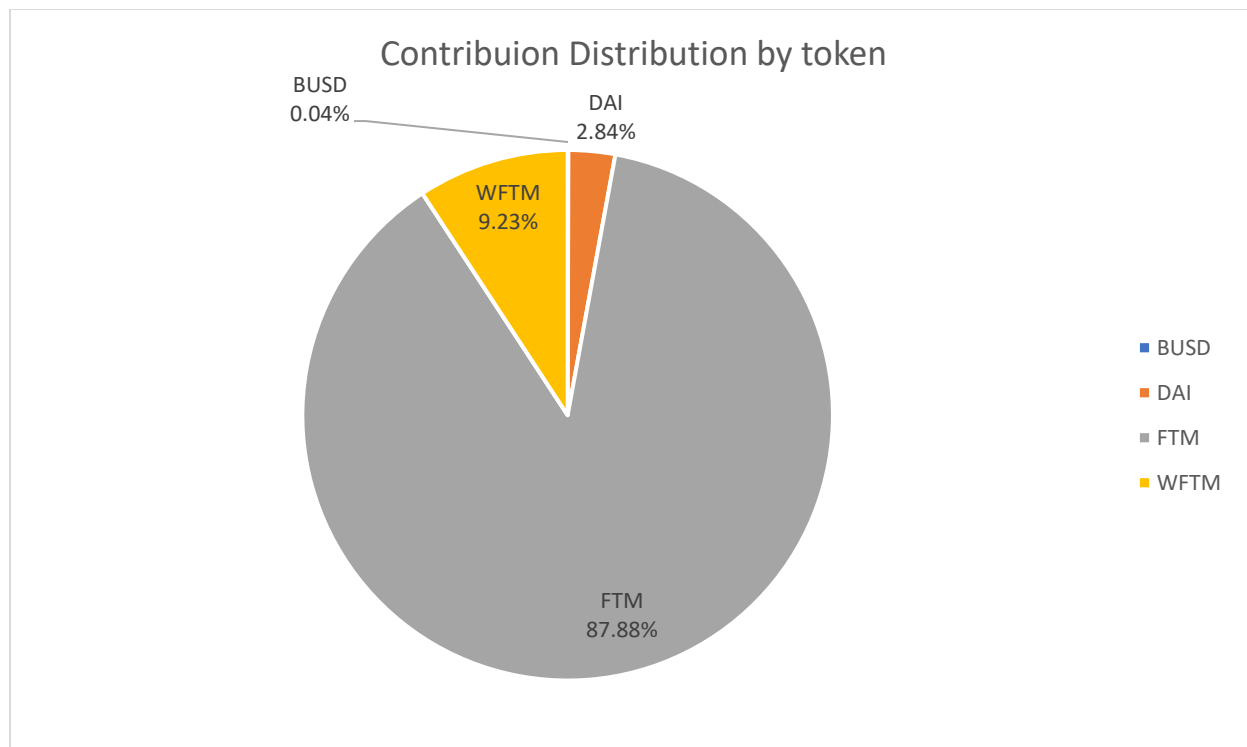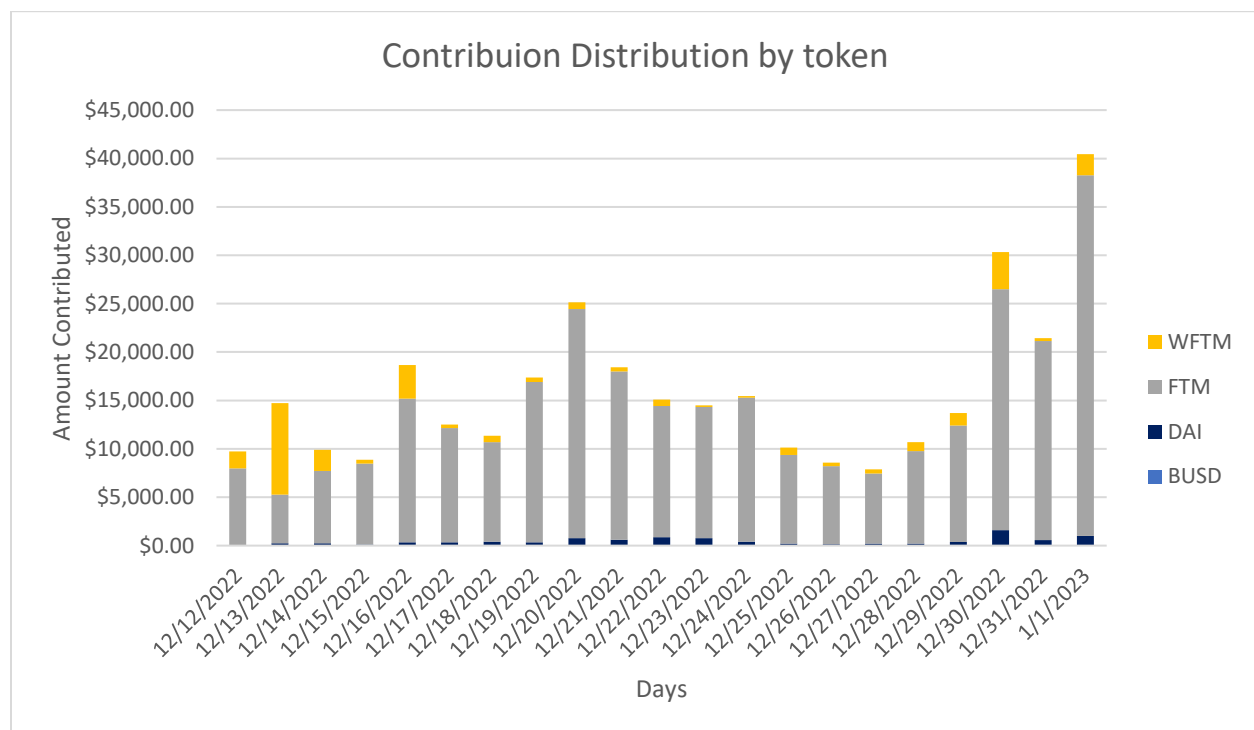
Fig 7

Fig 8

Fig 7&8 shows different distribution of the tokens contributed. Fig 7 is a pie chart that shows the total distribution of the tokens donated throughout the fantom round while Fig 8 shows the distribution by days.

From the charts above we deduce that the order of token used were in this order;

FTM → WFTM → DAI → BUSD

Unlike the UNICEF round the Fantom round had a fairer share of tokens across each of them.

Fantom Wallet Analysis

A chart was plotted for the wallet interaction that occurred during the donation round.
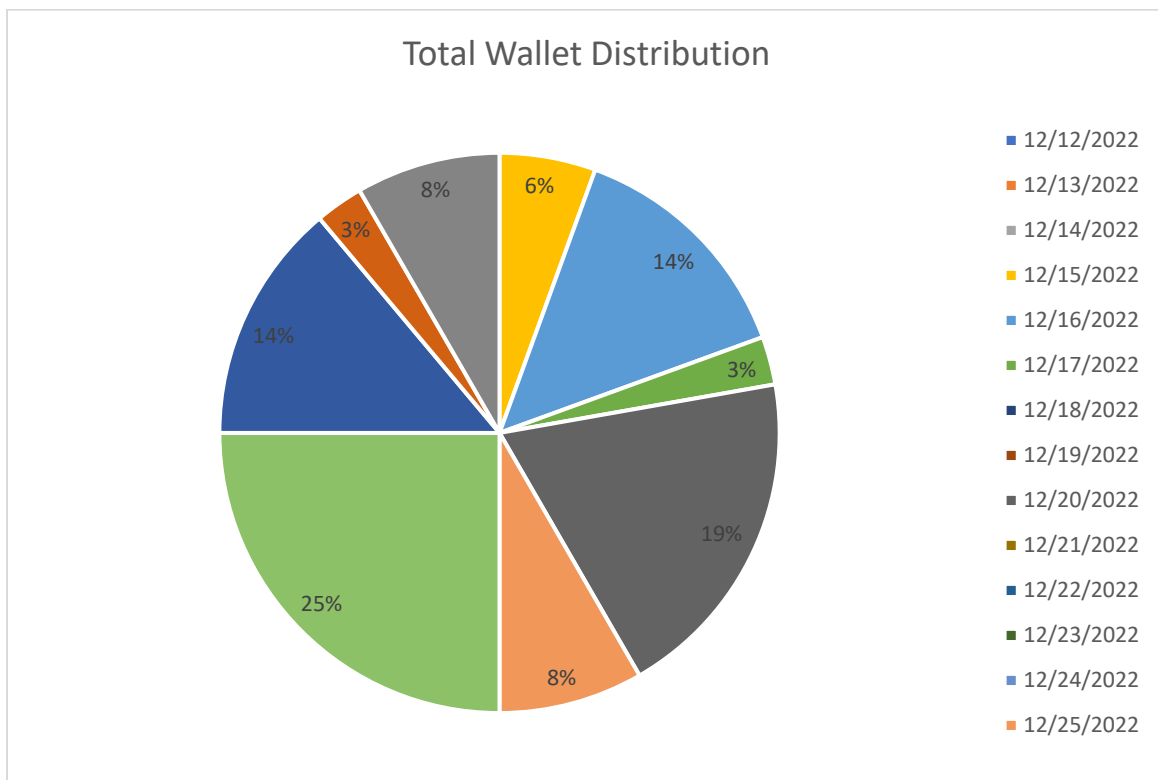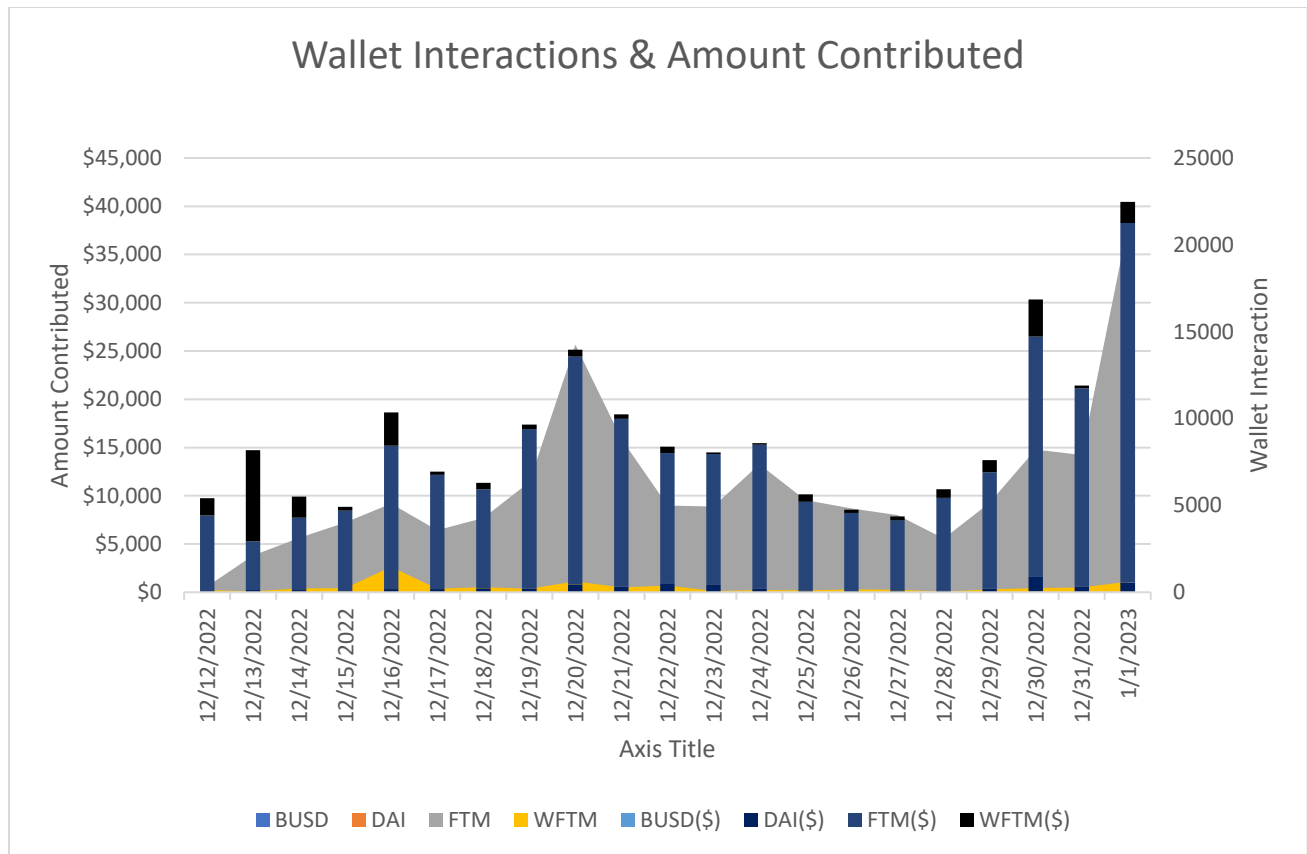

Fig 9

Fig 10

From the chart above we can see the distribution of the wallets used FTM was the dominant with 129,275 wallet interaction, WFTM was the next with 30,906 wallet interaction, DAI was the next with 3,943 wallet interaction, and lastly BUSD with a total of 36 wallet interactions.

To further analyze our wallet and total token deposited, I performed a **Value : Wallet (VTW)** computation to give us more insights on the cash flow.

$$Where = \frac{Total\ Sum}{Total\ No\ of\ Wallets}$$

BUSD→$3.92

DAI→$2.42

FTM→$2.28

WFTM→$5.08

I started my analysis with the token with the lowest VTW ratio i.e **FTM** token.

I started my analysis by filtering the token to FTM only and also filtering the amount contributed to less than or equal to $1.

After which, I filtered out these features I selected address that their cumulative contributions amounted to $100 or greater. Below is a table of the addresses.

ADDRESSES	AMOUNT ($)
0X0302F3434DBDEE9D3FAF680CBA8A2BAE6B34A83C	100
0X0308794CBD50174BE3401E08E352960B2E39B9D0	100
0X04DD23A3B1A1C1FE257F890B37466ADFF7240F80	800
0X0CAC11A7D29AB8C87D8FEDB9CC736146F4FE8E84	320
0X0FB3A55FFD9890A005DF5818039056B257AC0FE4	141
0X0F81B03E208A3FE457E864E50BD4A16281112095	203
0X114F0BBF1318AC34BE7D75658C98AE5684809887	230
0X13192B1056ED57EAA06BB7E49D70964A668E8604	100
0X151CB1A5D7A8C491D9586BCC019B1E654D9583E3	200
0X159943C9328C89F362B81F04D71AD44FC8A9D2FF	261
0X15C14F5A12A906832C131454DD3125542AAD569B	260
0X16679B41823DFA10A92BC822CC4F52C9D7EF2DF0	100
0X16956E96F71DBDAD8A1B334EAB7F14BFE004C37C	100
0X1697DB5839E8F997B61A57D723B498D9D1003301	207
0X16EC5EE1CC431CA95DE00B6C88D21D0B4D3FC2A6	100
0X289DEE1BE9F996B9ADEF2C45D59442E8DFBAE5DD	365
0X2932C3E41F92A3E4F5F36A81E346397DE8620502	100
0X32F93150E14FD67B5313DFC1AAD82873EF09FA0E	200
0X33606226E70B96CF2A07E85401A70661ADC3D019	100

Conclusions

- Compared to the UNICEF round the Fantom round had more sybils behavioral pattern compared to the UNICEF round. From my analysis I concluded that the Fantom round had more sybil attackers compared to the UNICEF round which had just a few attacks that occurred in a large frequency.
- Due to the large size of the Fantom dataset and high numbers of attackers I could not fish out 100% of the attackers because of time constraints. But I would be happy to do so if the Open Data Community request for it.
- A behavioral pattern detected from the attackers in the UNICEF round was splitting of a low amount of token into very minute values and using a ton of different addresses to attack.
- Another behavioral pattern detected from the attackers in the Fantom round was that sybils were able to use the same address to vote/ attack multiple times.