Anomaly detection

By team: Black Cap

- Tarek Chaalan
- Imad Mehmood
- Andleeb
- Robert Dzudzar
- Neda AfzaliSeresht
- Khai Fahmi Zaki
- Asif Rasool

HACK MAKERS

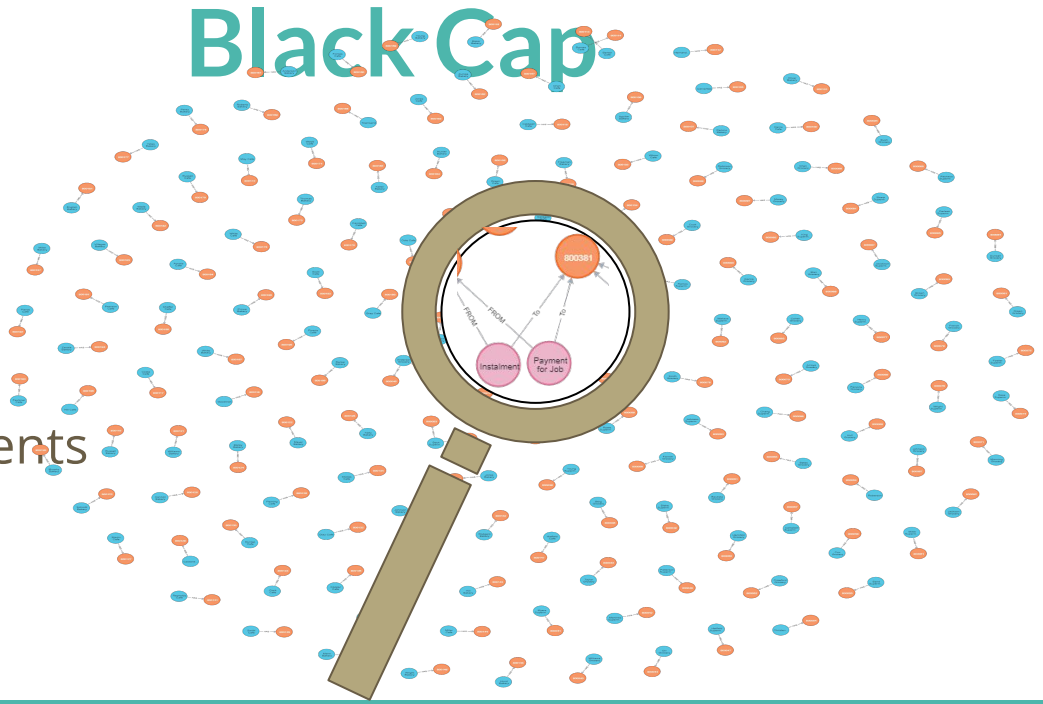
Overview

- Data & Problem
- Technologies Used
- Data Model
- Found Anomalies
- Insights
- Solutions
- Future Steps
- References & Acknowledgements

Anomaly detection

By team:

Black Cap



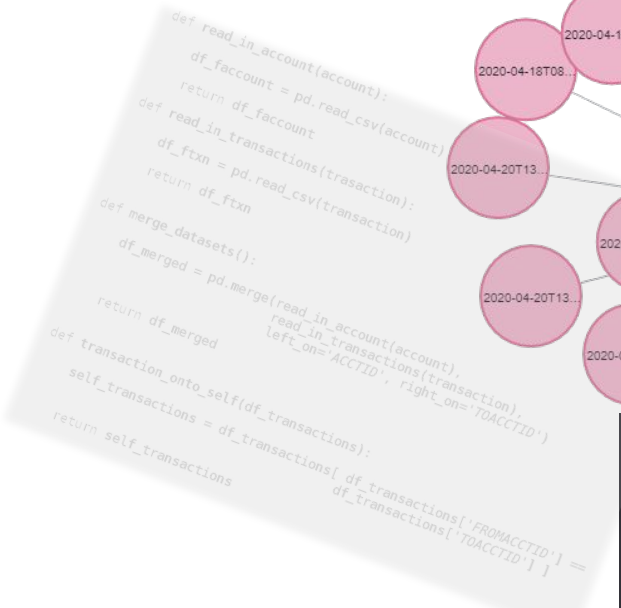
Data & Problem

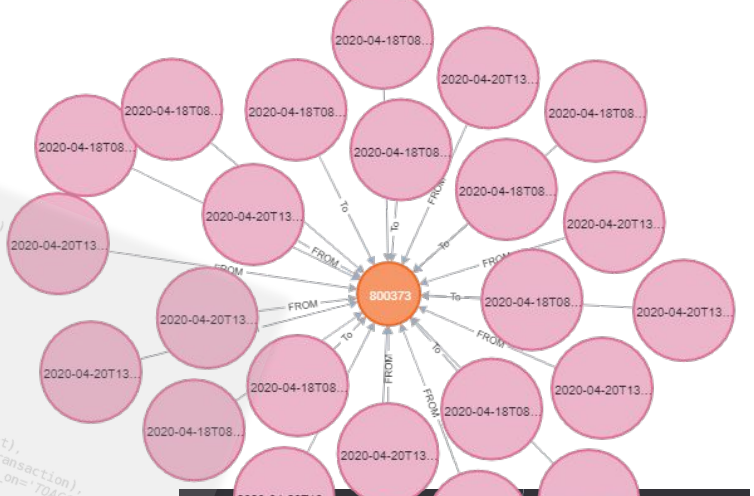
- Charlies Crash Repairs (CCR) business
  - Crash and mechanical repairs
  - Their expected turnover is **$2.1M**, while they operate with a turnover of **$14.3M**
    - Where is the additional **$12.2M** coming from?
- **Find anomalies in the transaction history and account information**

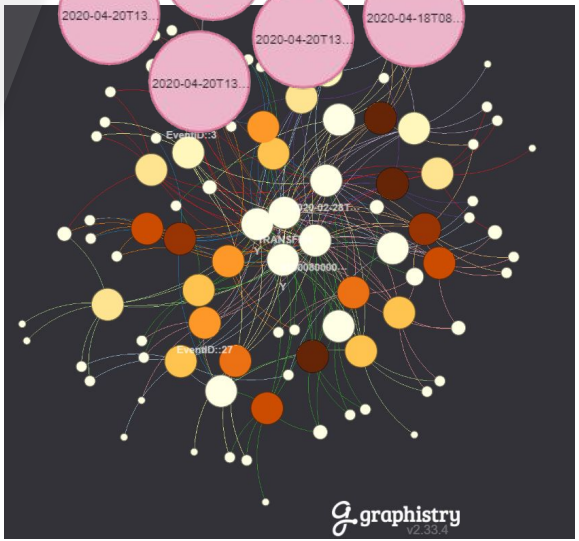
HACK MAKERS

Tools Used

- Python
- NEO4J
- Graphistry
- Tableau
- DataDog

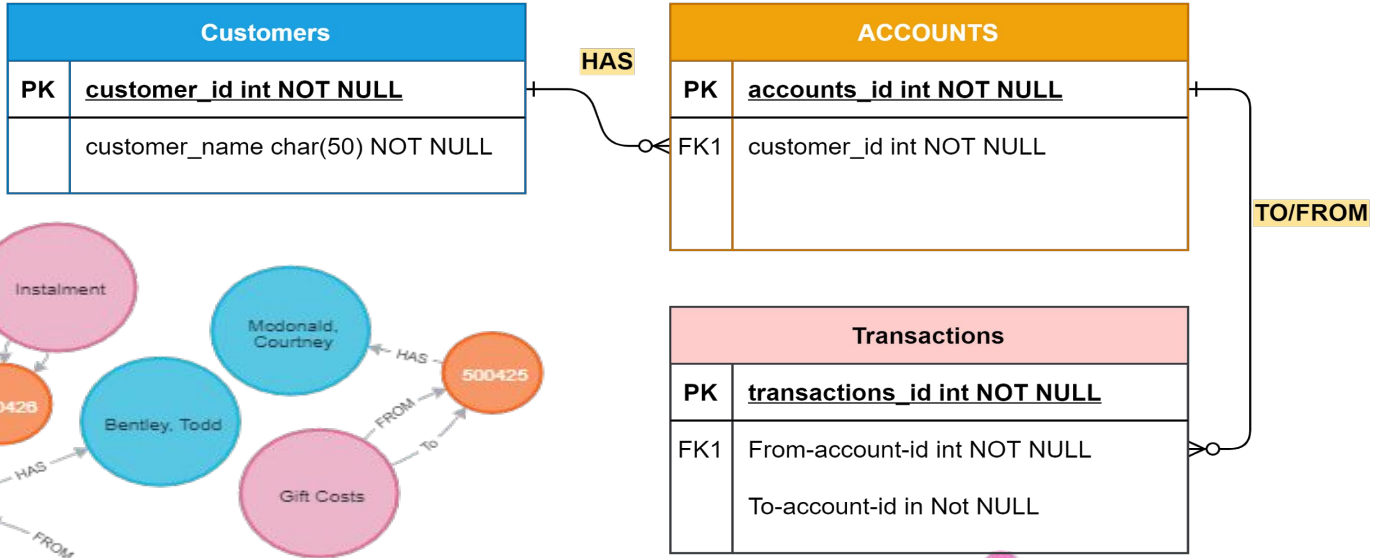






DataModel

Field in Data												
	ACCTID	ACCTTYPE	ACCTNAM	FIRSTNAM	SURNAME	DOB	ACCTCREA	ACCTRISK	ADDRESS	ADDRESS_	ADDRESS_	CATEGORY
	TXN_ID	TXTYPE	AMOUNT	FROMACC	TOACCTID	TXDA	REFERENC	ISFRAUD	ISFLAGGED			



HACK MAKERS

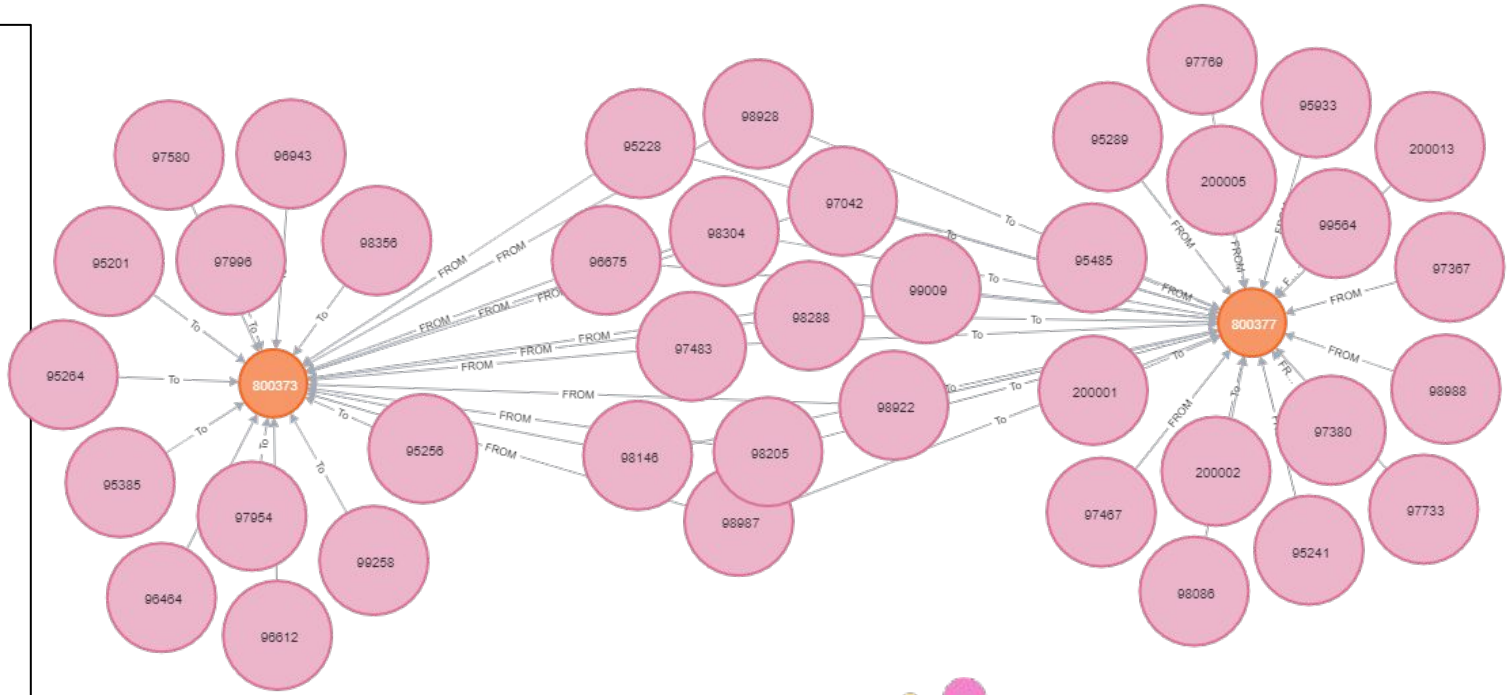
Scenarios

- Large transactions with > 90K
- Self-Self transactions
- Circular transactions
- Unusual amount spent on Meals
- Two accounts per person

HACK MAKERS

Found Anomaly: Large transactions

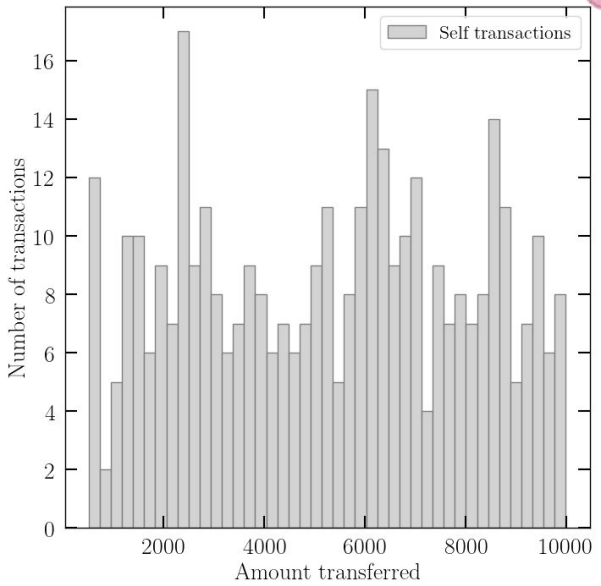
> 90K
Transactions FROM/TO suspicious accounts with transfer amounts

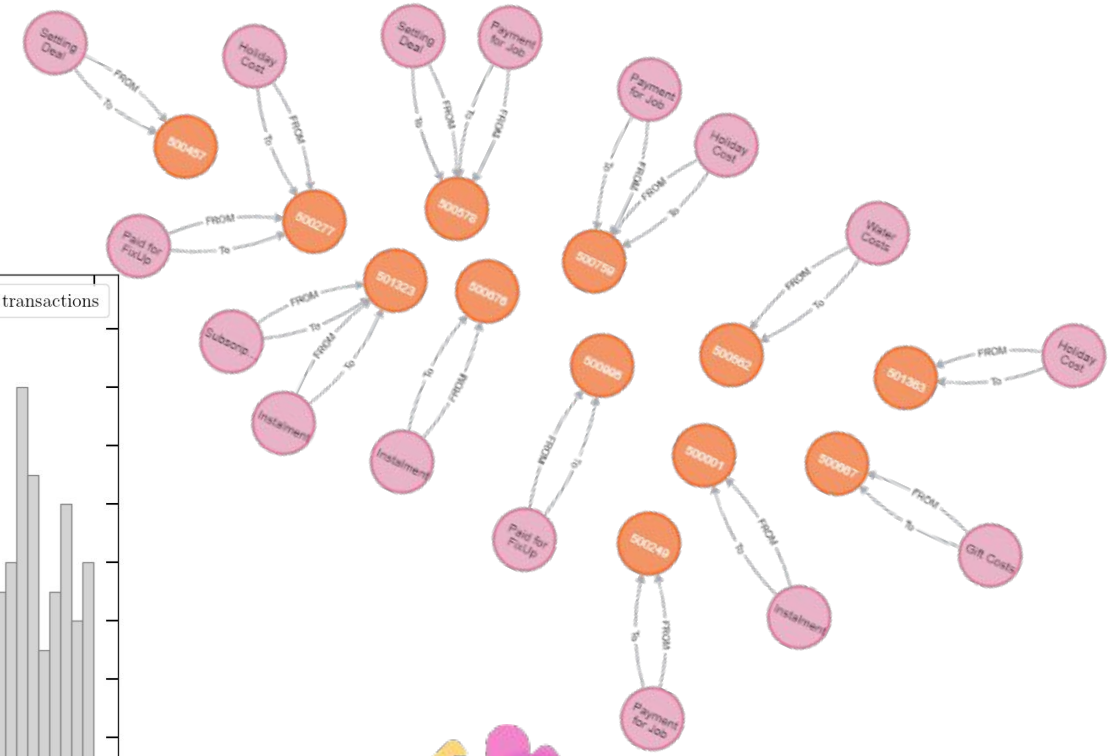


HACK MAKERS

Found Anomaly: Self-Self transactions

- With **maximum up to ~ $10K**
  (Possibly to avoid Threshold transaction reports)

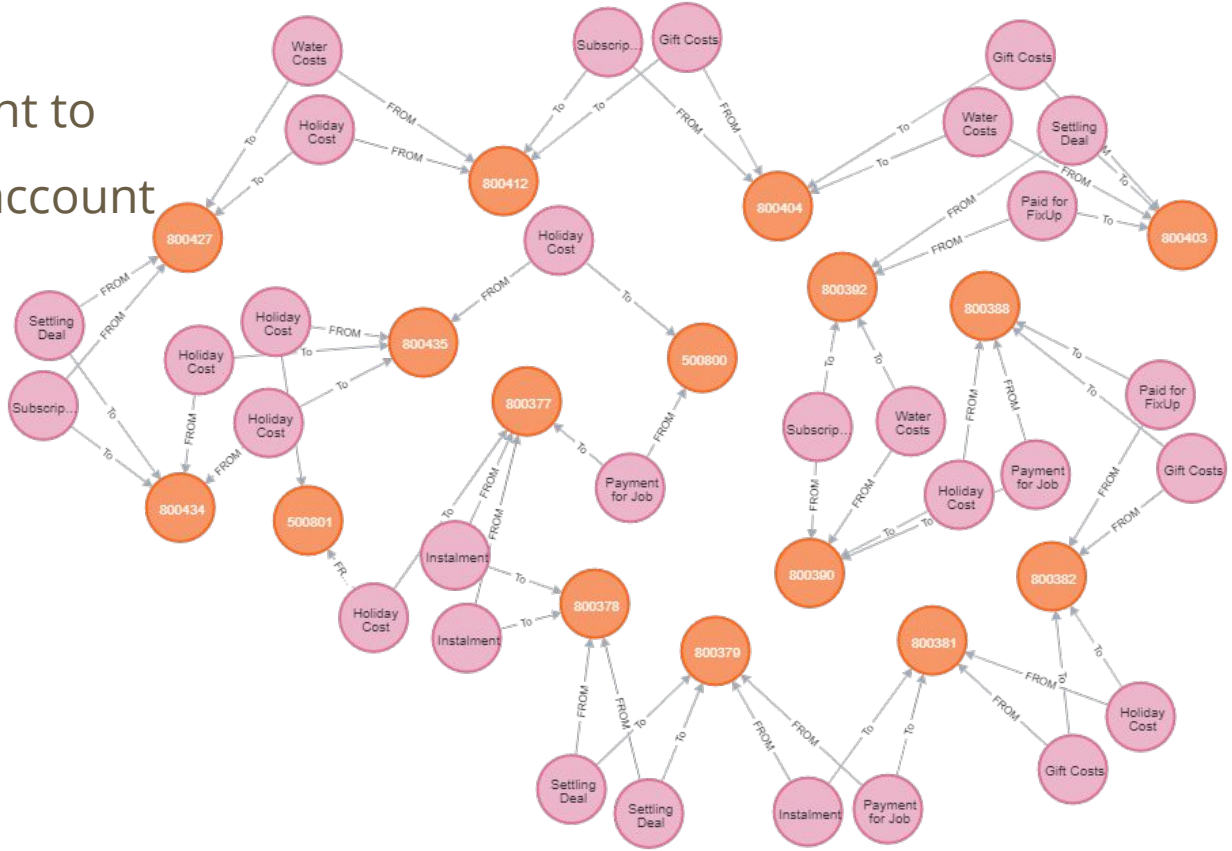




HACK MAKERS

Found Anomaly: Circular transactions

- From account to account to account to account to account
- **Within the same day!**



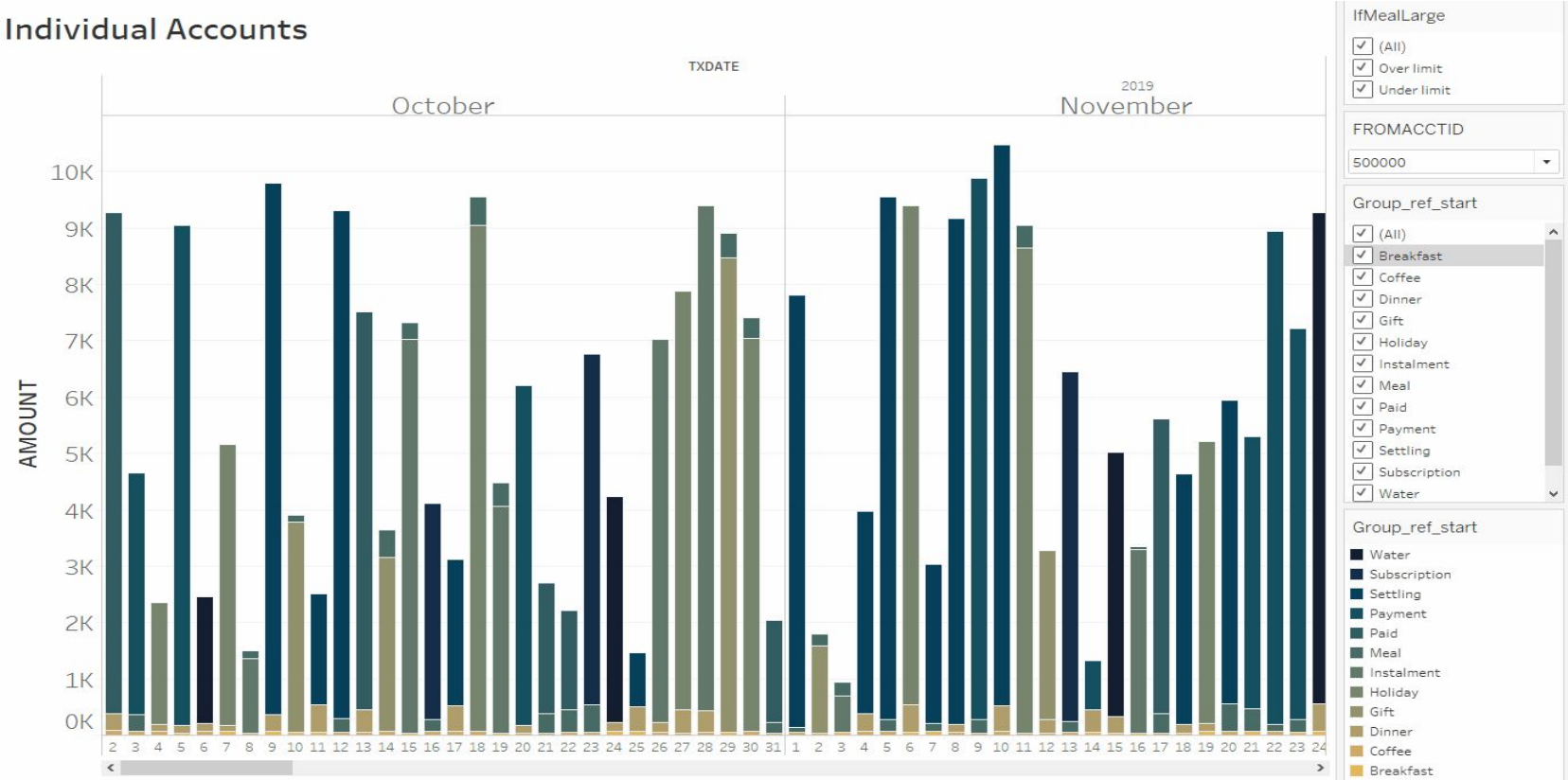
Solutions

- **We detect and interactively visualise Anomalies**
- Tools built:
  - **NEO4J & Graphistry** - To visualise Networks between accounts
  - **Tableau** - To interactively explore nuances of each account
  - **Coding scripts (Jupyter Notebook)** - To explore the datasets

Our developed tools can be used to inspect accounts

HACK MAKERS

Example: Our developed tools can be used to inspect accounts



Future Steps

- Create a web-app that will connect our
  - **Networks**
  - **Jupyter Notes**
  - **Tableau Dashboards**

- Function of the Web-app is to
  - **Automatically flag accounts**
  - **Provide Stakeholders a tool to inspect accounts timely & interactively**

- Using machine learning approach to detect anomalies
  - **This requires the appropriate labelled dataset**
  - **Dataset can be developed by crowdsourcing current anomalies**

HACK MAKERS

References & Acknowledgements

- **We used datasets that were provided by Organisers:**
  - **faccount.txt -** Contains Account information (https://objectstorage.ap-sydney-1.oraclecloud.com/n/sdc90vkxb5rj/b/data/o/anomaly-detection%2Ffaccount.txt)
  - **ftxn2.txt -** Contains transaction information (https://objectstorage.ap-sydney-1.oraclecloud.com/n/sdc90vkxb5rj/b/data/o/anomaly-detection%2Fftxn2.txt)

- **We are acknowledging support from the Mentors**
  - **Riyaz Ahamed**
  - **Jigna Thacker**

Thank you #DigitalDefence Hack organisers!

HACK MAKERS