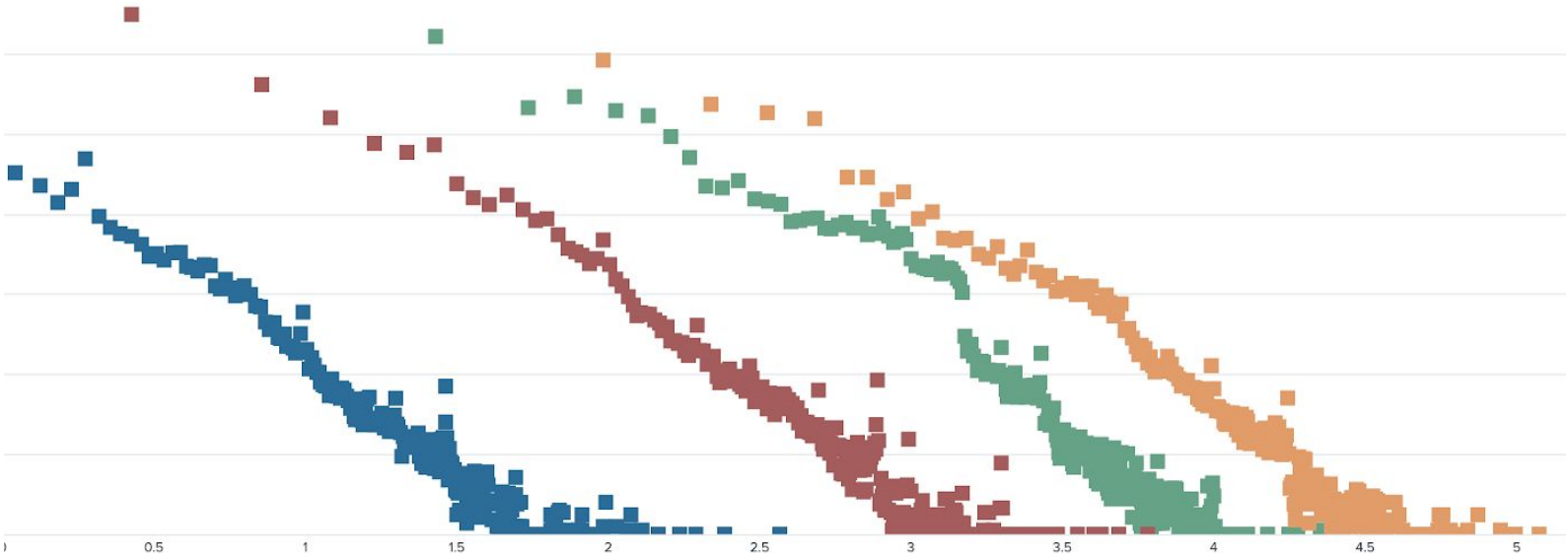
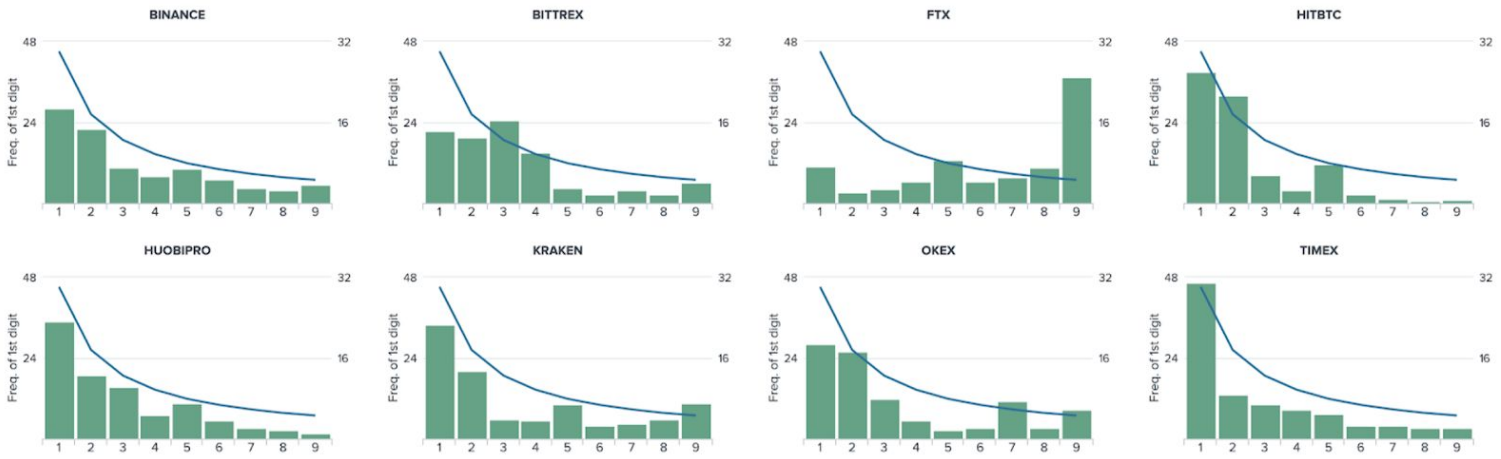
Crypto Market Anomalies
November 2020



Anomalous trades on FTX

FTX demonstrates a noticeable leading digit spike, possibly indicating non-standard trading activity on the exchange. Recent order distribution sizes for COMP (Compound) deviate from other markets and contradict Benford's law.



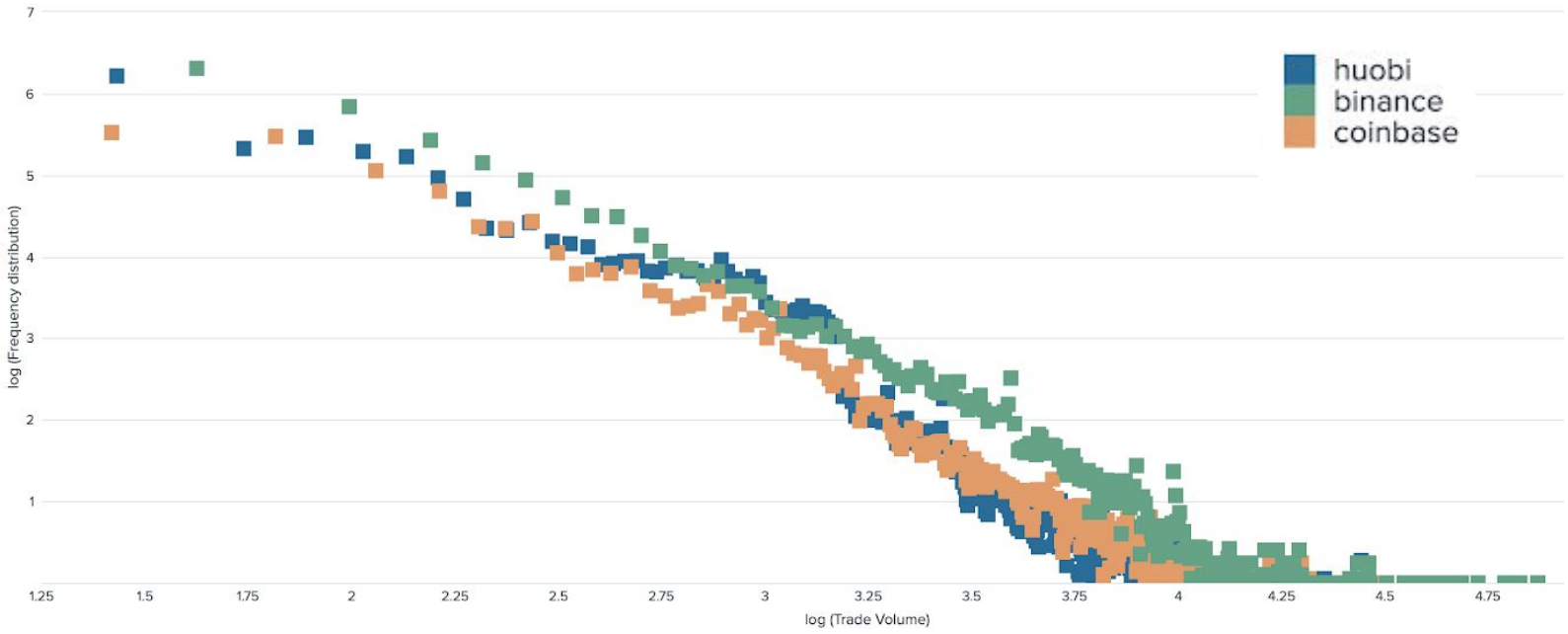
Gsfrvfodz!ejtusjcvujpo!pg!mfbejoh!ejhjut/!Tqpu!nbsl fu!DPNQ!upl fo!pse fs!tj{ fz Opw!9.21-!3131!) 611-111!fwfou!vt fe/zz*

Application of Benford’s Law to Fraud Detection

The ACFE published an article for how to discern naturally occurring statistical deviations from fraud using Nigrini’s tests. Evidence based on Benford's law has been used in federal and state criminal and regulatory cases.

LINK Trading Volumes Deviations on Huobi

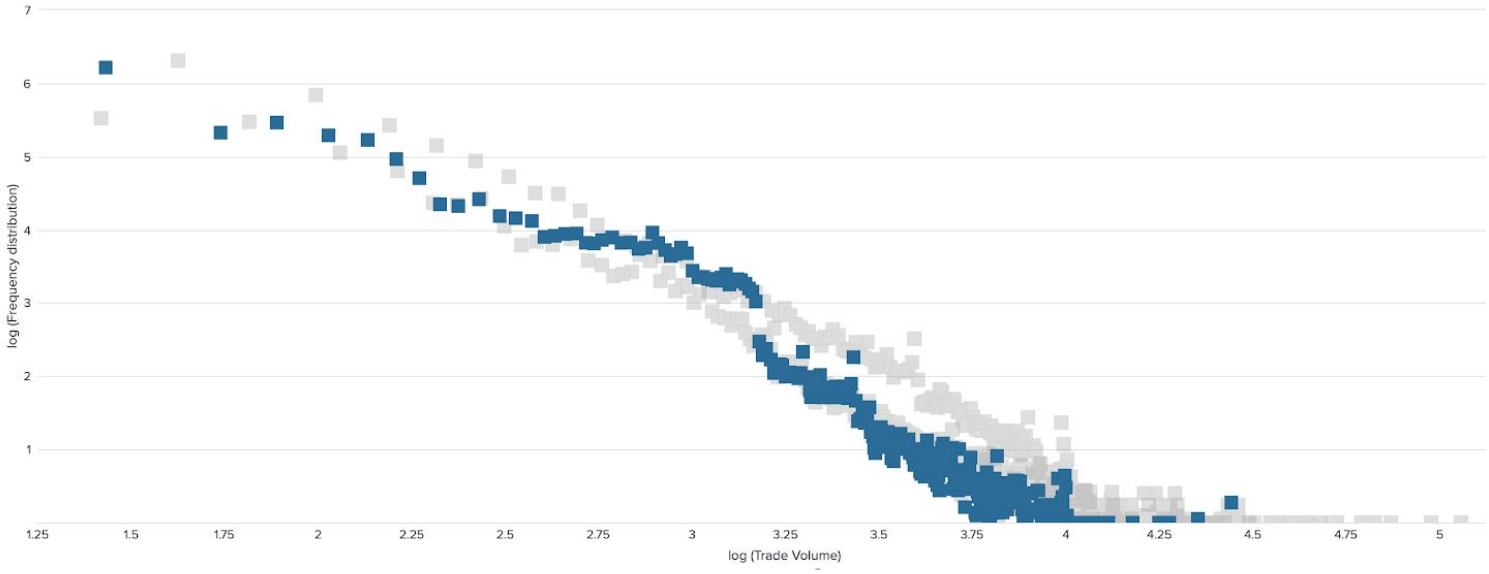
Typically, frequency distributions for logged trade volumes have an near linear relationship with a negative slope, and a long tail (at the high end of trade size). As an example, in comparing LINK trading activity, the distribution on Huobi stands out when compared to other high-liquidity exchanges.

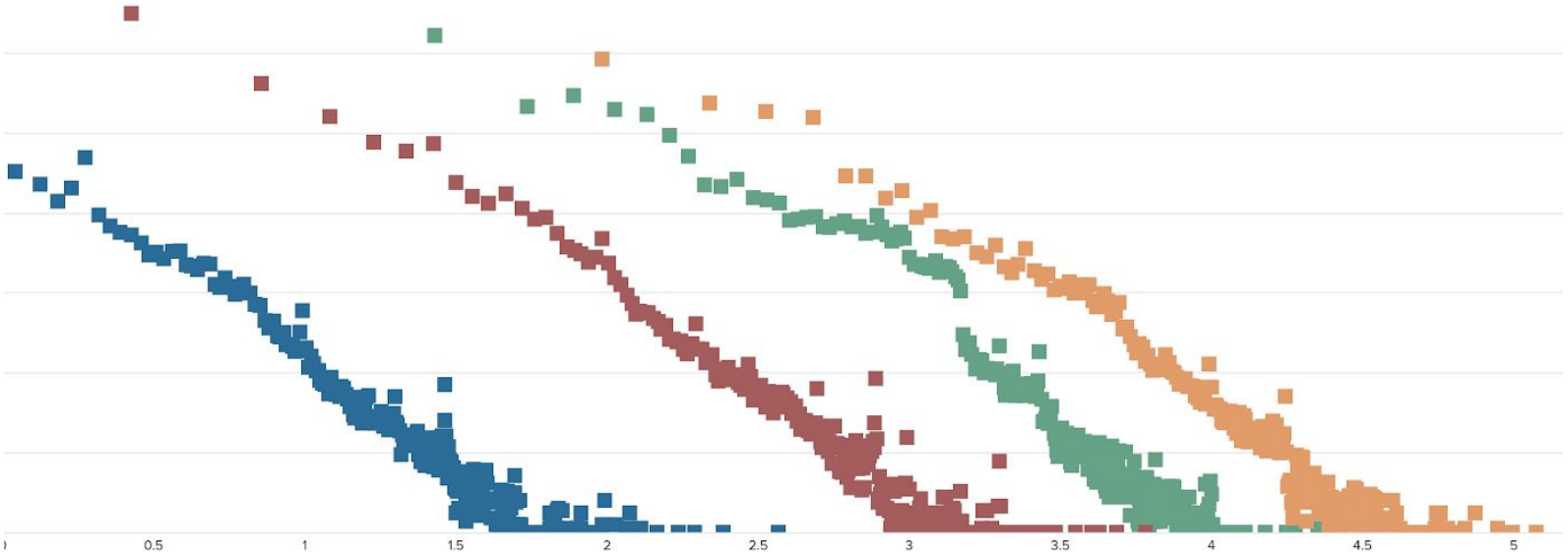


Gsfrvfodz!ejtusjcvujpo!pg!usbejoh!wpmvnft!pg!MJOL!upIfo!po!Dpjocbtf-!Cjobodf-!Ivpcjz fydiboh f!Pdu!21!p!Opw!21-!3131/!Tpvsdf;!DUfsnjobmEebub!jo!Tqmvolz

Exchanges or token creators can use trading algorithms that increase trading volumes to create an impression of a more active market. Many of the more simplistic and standardized methods of anomaly detection, such as aggregate raw trade-size distribution analysis, can be rendered ineffectual by more sophisticated wash trading schemes. Significant deviations from the theoretical power-law distribution in published trade volumes may be a reason for closer inspection.

z

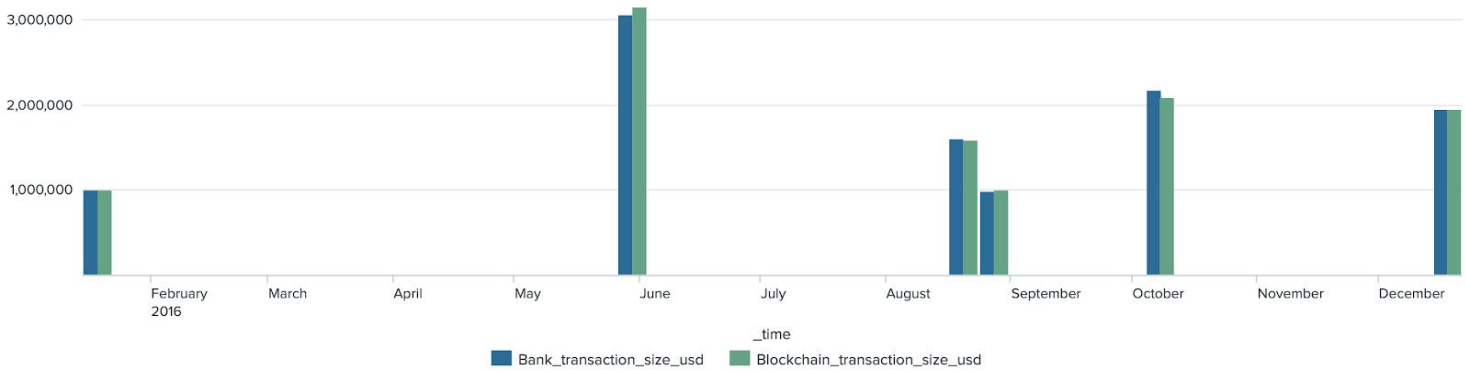




Gsfrvfodz!ejtusjcvujpo!pg!usbejoh!wpmvnft!pg!MJOL-!CUD-!FUI-!FPT!!upl fot!po! I vpcjz
fydiboh f!Pdu!21!p!Opw!21-!3131/!Tpvsdf;!5Ufsnjobm&ebub!jo!Tqmvol

Crypto in the FinCEN Leak

Our investigations team went through the FinCEN leak and found a few suspiciously similar transactions on Bitcoin blockchain. By looking at the transaction sizes and timestamps, NTerminal matches senders (originator banks) and receivers (beneficiary banks) mentioned in Suspicious Activity Reports (SARs) to specific blockchain addresses and business entities:



*Cmpdldibjozboezgmbhhfezcbolzusbotbdujpozwpmvnfz)VTE*ztusfbntzpwfsmbqqfezjozuifz dpnnpo!ujnf!qfsjpe-!Kbo! l !Efd-!3127/!Tpvsdf;!DUfsnjobmFebub!jo!Tqmvolz*

More cases with corroborating evidence, indicating that the flagged participants are likely using Bitcoin, can be found in the recent Inca Investigation Team post. The results highlight the importance of publicly available data and systems capable of correlating large datasets when performing fraud analysis.