

**NTerminal**

Digital Asset Data and Analysis

CRYPTO MARKET MANIPULATION

EXAMPLE NTERMINAL INVESTIGATION USING SPLUNK

[INCA DIGITAL](#)











Reliable and accurate data is crucial for understanding any market. While financial signals and metrics associated with an asset modify the decision making of traders, regulators, and financial institutions, crypto finance data still lack credibility. Volumes are widely assumed to be inflated or outright fabricated, project fundamentals (such as the identity of the founders, location of operation, affiliated organizations, or claims made in the white paper) are often difficult to obtain or verify, public sources of knowledge (such as news outlets and public data providers) commonly contradict one-another, and social media platforms are filled with scammers and bots.

Muddling through the noise to find signals requires more than time series analysis on Excel spreadsheets. Market participants need a tool that [combines and analyzes disparate data sets](#) real-time. This case example investigation combines disparate data and various methodologies of statistical analysis to highlight the capabilities of NTerminal on Splunk. Further analysis and statistical testing should be done before acting on any implications or conclusions from these results.



It is widely accepted that there are inflated trading volumes reported within the crypto-financial space ([Bitwise Presentation](#), [BitMEX Research](#)). Looking at the popular website CoinMarketCap (CMC), one will see 24h trading volumes for top assets that are larger than their entire reported market capitalizations. Many of the trading venues that this volume is supposedly coming from have suspiciously low community engagement (such as website visits, social media presence, or media mentions) and publicly available information.

Clearly the self-reported nature of CMC-type data sites do not lend to an accurate representation of true crypto-market behavior. Projects and exchanges benefit in equal parts from exaggerated or fabricated trading activity, which acts as free advertising (whether or not they are even remotely involved in the circulating of the inflated data).

Cryptocurrencies ▾				Exchanges ▾	Watchlist	USD ▾	← Previous 100	Next 100 →	View All
#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)		
144	 XMax	\$19,039,206	\$0.001062	\$215,721,186	17,931,338,566 XMX *	1.79%			***
146	 Lambda	\$18,723,219	\$0.026896	\$45,010,055	696,125,410 LAMB *	-0.14%			***
102	 Grin	\$33,086,987	\$1.04	\$27,649,147	31,842,660 GRIN	-2.07%			***
106	 Beam	\$31,654,975	\$0.592087	\$24,421,614	53,463,360 BEAM	2.04%			***
105	 TomoChain	\$31,815,145	\$0.458049	\$20,274,139	69,458,000 TOMO	0.45%			***

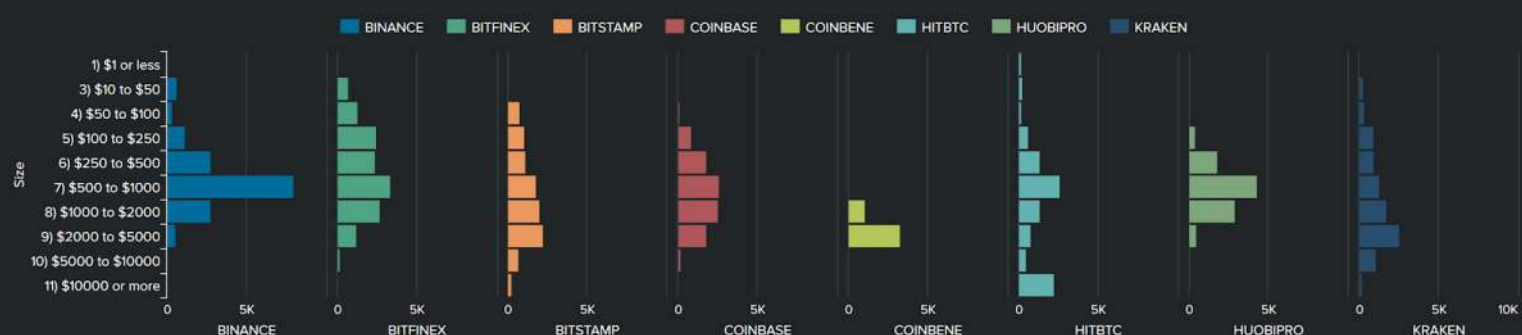
Jan 20, 2020 | screenshot from [CoinMarketCap](#)

Without even considering the number of scam projects, malicious wallet software, lending platforms, fake exchanges, or phishing schemes, **the crypto-financial environment is fraught with misinformation and misaligned incentives.** Common industry practices like exchange-listing fees for assets or the existence of zero-fee trading accounts, coupled with a lightly regulated market, create an environment ripe for manipulation. Many well-funded projects have been suspected of paying groups to actively pump trading volumes of their asset on public exchanges through wash trading. This [CoinDesk interview](#) with Alexey Andryunin, co-founder of Gotbit, who was hired to inflate trade volumes, clearly demonstrates the systemic issues in crypto with data fabrication.

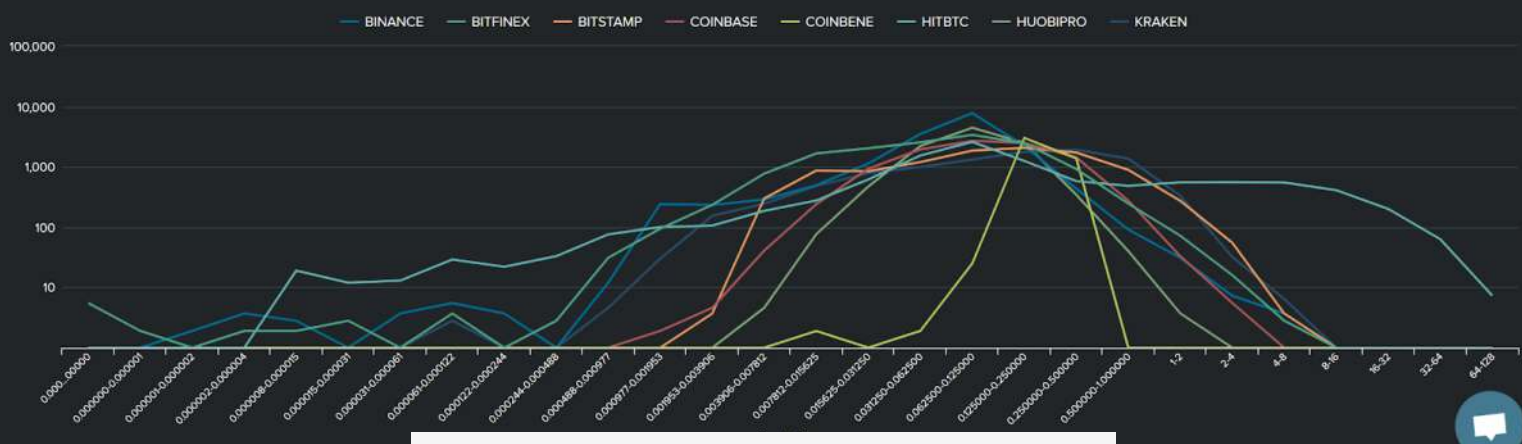
A few case examples of anomalous market activity are below. By combining data types using NTerminal data in Splunk Enterprise, **we can identify abnormal market patterns and investigate relationships between various entities in the digital asset ecosystem.**

In cryptography, the **root of many problems come from random number generators**. Their implementations **are often pseudorandom** and do not properly guarantee the level of security required by the protocol. Cryptography isn't the only industry that implements imperfect random number generators. Wash trading schemes employ various techniques of obfuscating their activity, including the use of pseudorandom sizes and timings for posting bids/asks. By observing a few prominent crypto exchanges' reported trade volumes, we can look for statistically abnormal patterns. I will start by looking at the recent sizes of trades for BTC on some of the "top" exchanges (by internet presence and reported volume).

Trade Size (Averaged)



Trade Size Analysis (Averaged)

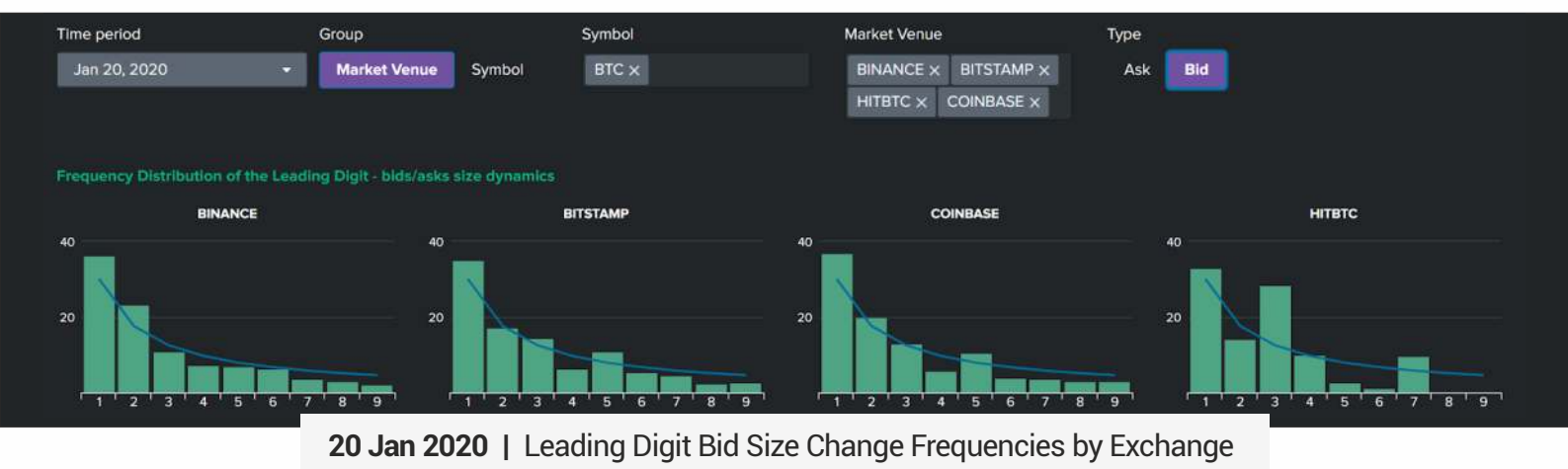
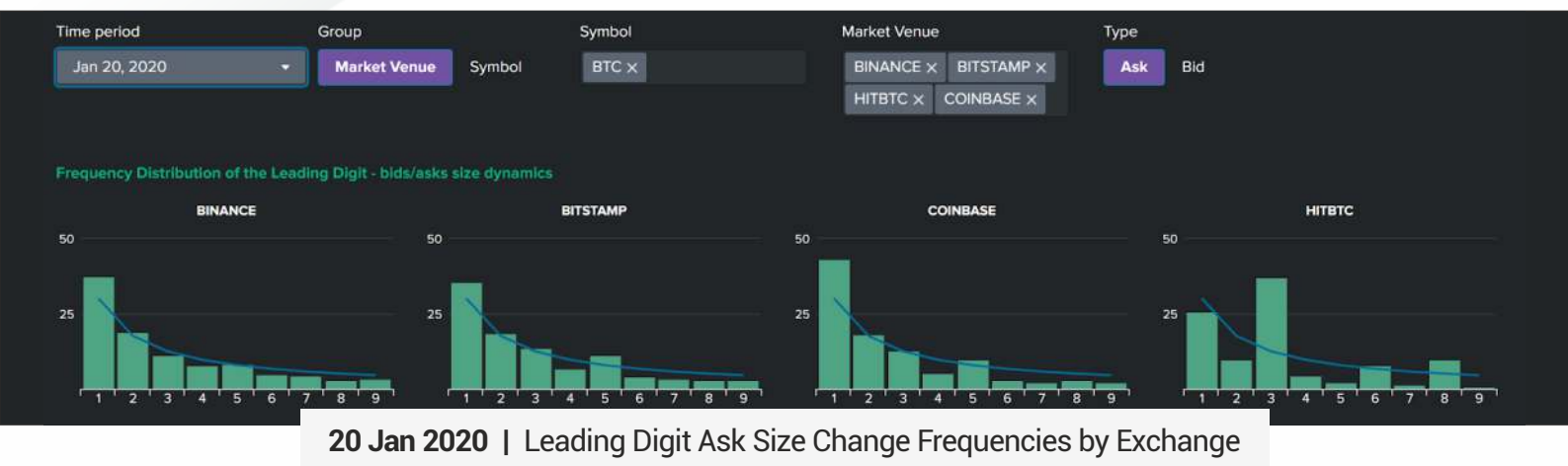


20 Jan 2020; -7d | BTC Trade Size Distributions

The differences in trade distributions can be explained by a variety of factors including exchange policies (such as maker/taker fees and platform trading tiers), different user demographics, fiat or stablecoin options available, trading API availability, and deposit + withdrawal fees/incentives. While the above factors suggest that trading activity should not be identical across market venues, analyzing trade data via multiple methodologies can certainly direct our attention to abnormalities worthy of further investigation.

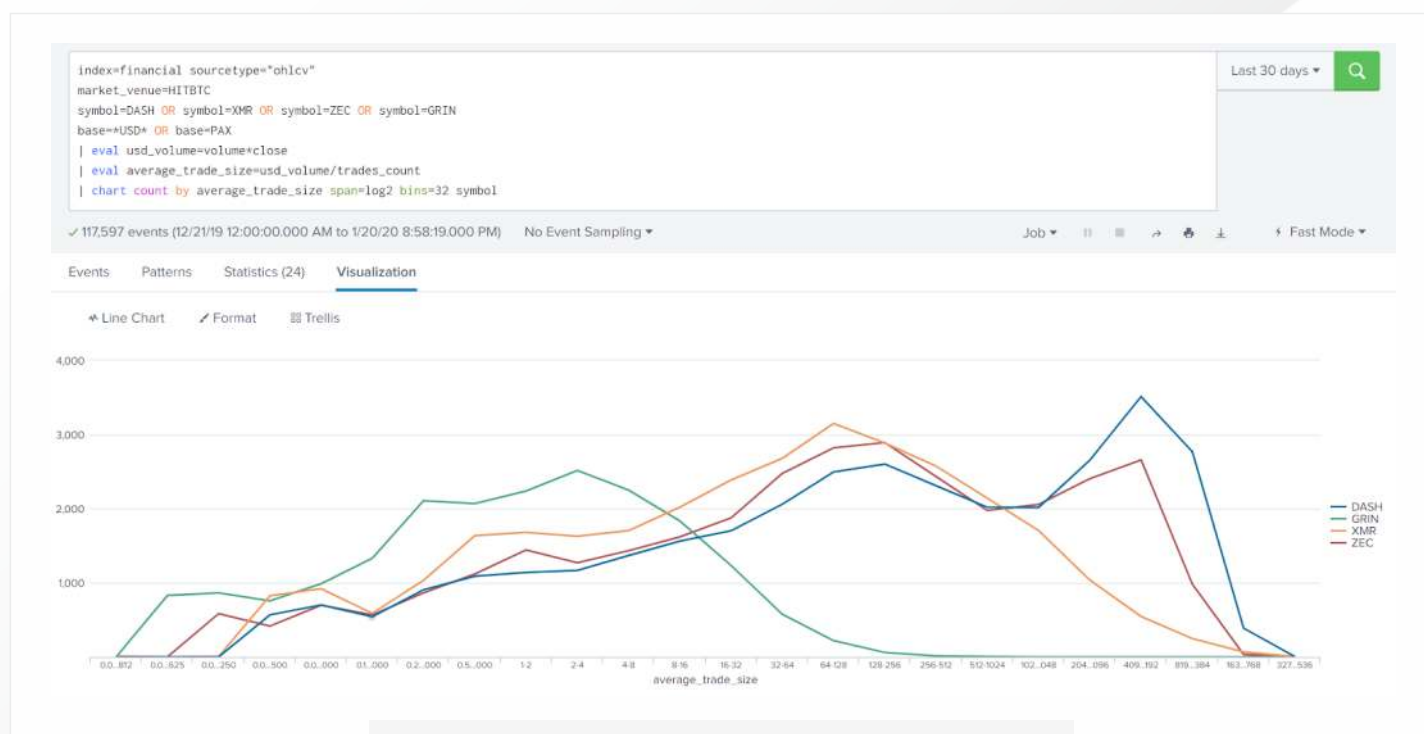


From the selected exchanges, CoinBene and HitBTC have visibly distinct patterns from the other market venues. I chose HitBTC as an example to look for further statistical discrepancies; the purpose of this article is not to specifically point a finger at HitBTC. I hope to simply demonstrate how we can go from recognizing strange financial data to conducting deeper analysis with Nterminal.



The [ACFE](#) published an [article](#) for how to discern naturally occurring statistical deviations from fraud. [Benford's Law](#) is an **observation of numerical data sets that states that leading significant digits do not occur in an even distribution** (~11% for leading digits 1-9). By plotting bids and asks against Benford's Law, we see that HitBTC has many more leading 3's than the other platforms report. The ACFE guide for the First Digit Test states that "fraud examiners are concerned with the over-usage of digits, because fraudsters, when inventing numbers, tend to overuse certain digit patterns. The digits that occur fewer times than Benford Law predicted (1, 5, 7, 8, and 9) result primarily from the over usage of 3."

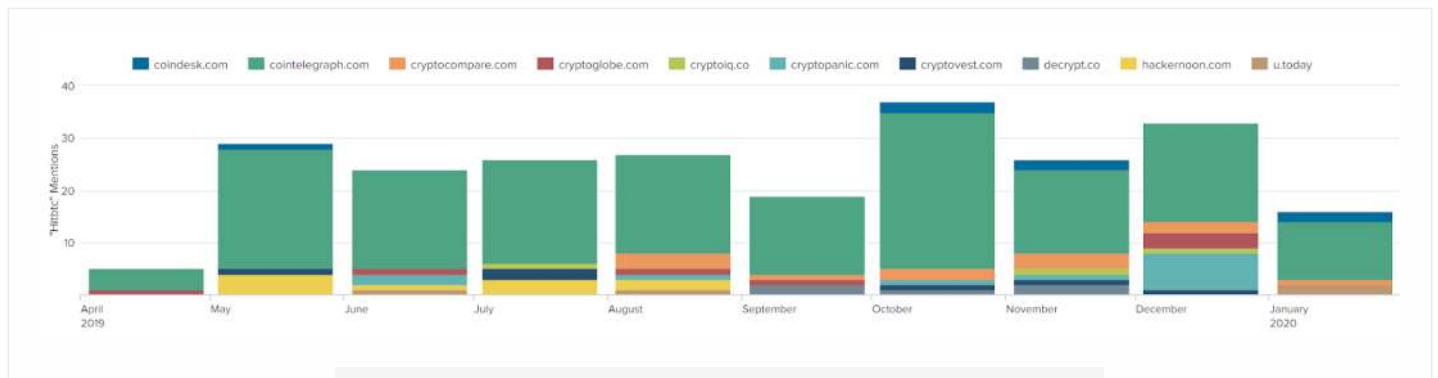
There are additional anomalous patterns with altcoin trading on HitBTC, in the following search we compare privacy coins. Not all altcoins seem to be traded in the same manner on HitBTC. Some are apparently traded in small chunks under \$1, while others are traded more frequently in large sums.



20 Jan 2020; -30d | HitBTC Trade Size Distribution

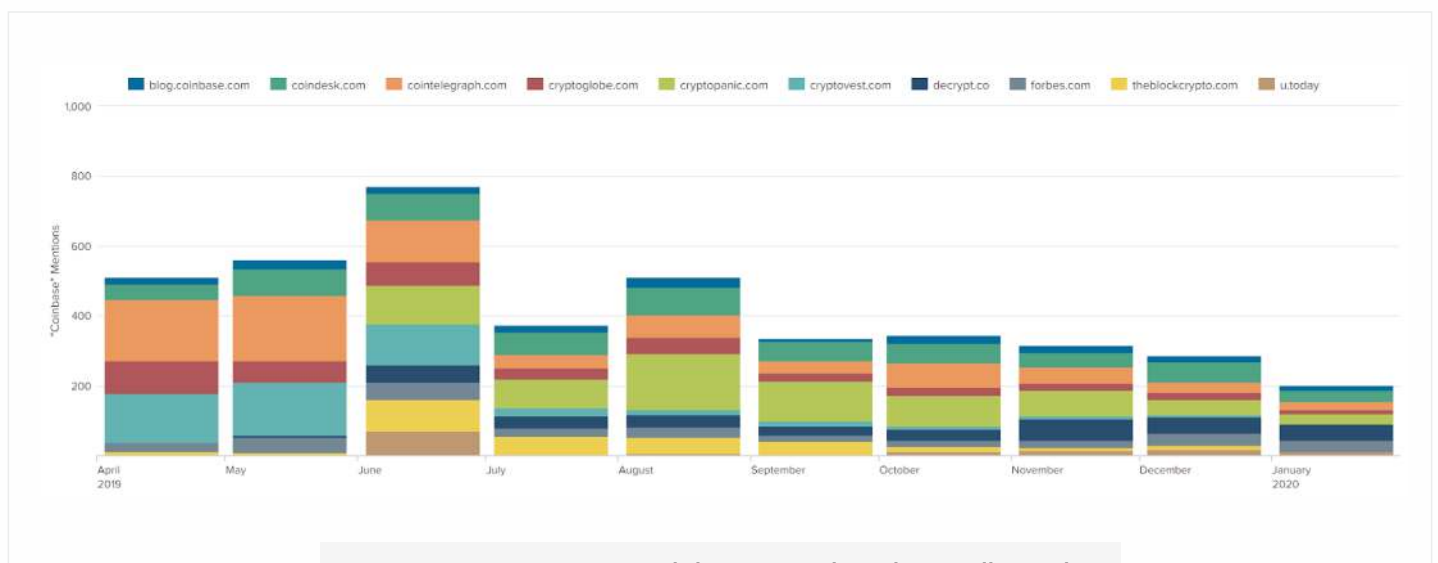
Looking at financial data alone can only be so effective, however. And while these deviations on HitBTC might be reason enough to look more closely at the exchange, there are many potential explanations that would not implicate the exchange itself in any wrong-doing. Many times, exchanges might not be conducting any wash trading themselves, but instead might knowingly or unknowingly facilitate wash trading on their platform through low/no fee accounts.

We can leverage **more than just market data analytics** on NTerminal. Using NTerminal's natural language processing (NLP) module, **we can put together a broader narrative**. First, we will query events from crypto media outlets for mentions of HitBTC over the past 9 months. Here notice a correlation between HitBTC mentions and Cointelegraph.



20 Jan 2020; -9mon | HitBTC Mentions by Media Outlet

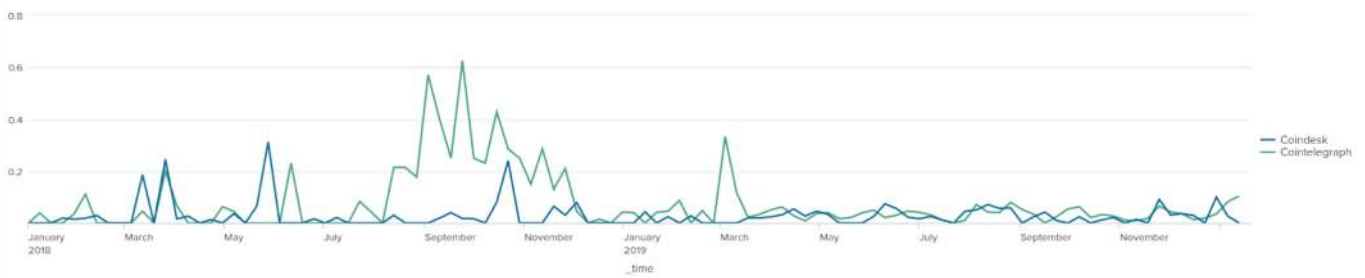
Looking at mentions of other exchanges, however, we do not see the same volume of mentions coming from CoinTelegraph. Compared to Coinbase, for example, HitBTC seems to get much more centralized press.



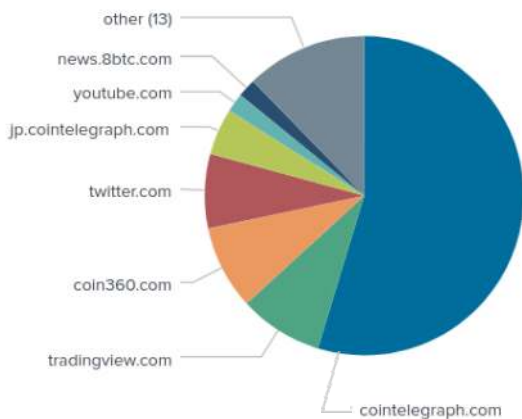
20 Jan 2020; -9mon | Coinbase Mentions by Media Outlet

Next we will look closer at the data surrounding CoinTelegraph to better understand why there might be such a large amount of content surrounding HitBTC from them. Simply looking at the number of mentions of various coins, we found abnormal spikes of chatter about Monero on Cointelegraph by looking into the ratio of Monero to Bitcoin mentions compared to other media outlets.

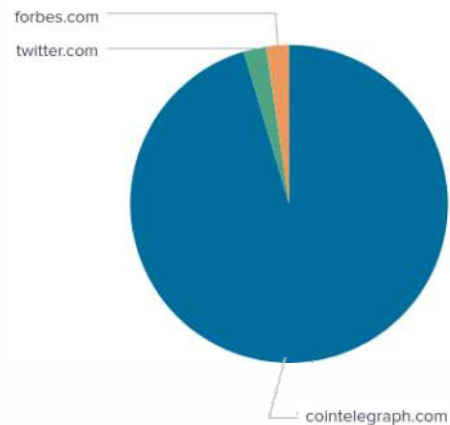




There is also an interesting correlation between references used by CoinTelegraph journalists and a [lesser-known](#) entity, coin360.com, a crypto market data provider. An analysis of their website, press releases, and reading common crypto blog sites show that they may be associated with Monero, [Changelly](#), [MinerGate](#), [ByteCoin](#), [Freewallet](#), and [HitBTC](#). This also seems to be corroborated by their former journalist, Ian DeMartino.



Outgoing Links from Cointelegraph (-6mon)



Mentions of coin360 (-6mon)

After looking up if any other resources are referencing coin360.com, we can see a two-way connection between CoinTelegraph and coin360.

In this article, we use NTerminal as an investigative tool to correlate and analyze data across the digital asset ecosystem. We use financial data reported by exchanges to identify anomalous distributions, and then investigate entity relationships using natural language data. We started by simply monitoring recent trading activity for any unique patterns. **By following additional surrounding anomalies from HitBTC on NTerminal, we noticed strange connections to otherwise seemingly distinct organizations.** This example investigation is by no means comprehensive, but may provide sufficient grounds to look closer at this exchange's activity and their associated organizations. There may well be large and coordinated manipulation efforts that have yet to be discovered - tools like NTerminal and Splunk allow analysts to find patterns to help them identify such efforts.

SOURCES

- Association of Certified Fraud Examiners. "Using Benford's Law To Detect Fraud." ACFE, www.acfe.com/uploadedFiles/Shared_Content/Products/Self-Study_CPE/UsingBenfordsLaw_2018_final_extract.pdf.
- BitMEX. (2018, November 12). Detailed Report Into The Cryptocurrency Exchange Industry (From CryptoCompare). BitMEX Blog | The official blog of BitMEX, the Bitcoin Mercantile Exchange. <https://blog.bitmex.com/crypto-currency-exchange-review-from-cryptocompare/>
- Bitwise Asset Management. "Presentation to the U.S. Securities and Exchange Commission." SEC.gov, 19 Mar. 2019, www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5164833-183434.pdf.
- Cong, Lin and Li, Xi and Tang, Ke and Yang, Yang, Crypto Wash Trading (December 30, 2019). Available at SSRN: <https://ssrn.com/abstract=3530220> or <http://dx.doi.org/10.2139/ssrn.3530220>
- Nigrini, Mark J. Benford's Law: Applications for forensic accounting, auditing, and fraud detection. Vol. 586. John Wiley & Sons, 2012.
- Who owns and runs Cointelegraph? MadBitcoins Live with Ian DeMartino https://www.reddit.com/r/Monero/comments/3g1x60/who_owns_and_runs_cointelegraph_madbitcoins_live/

