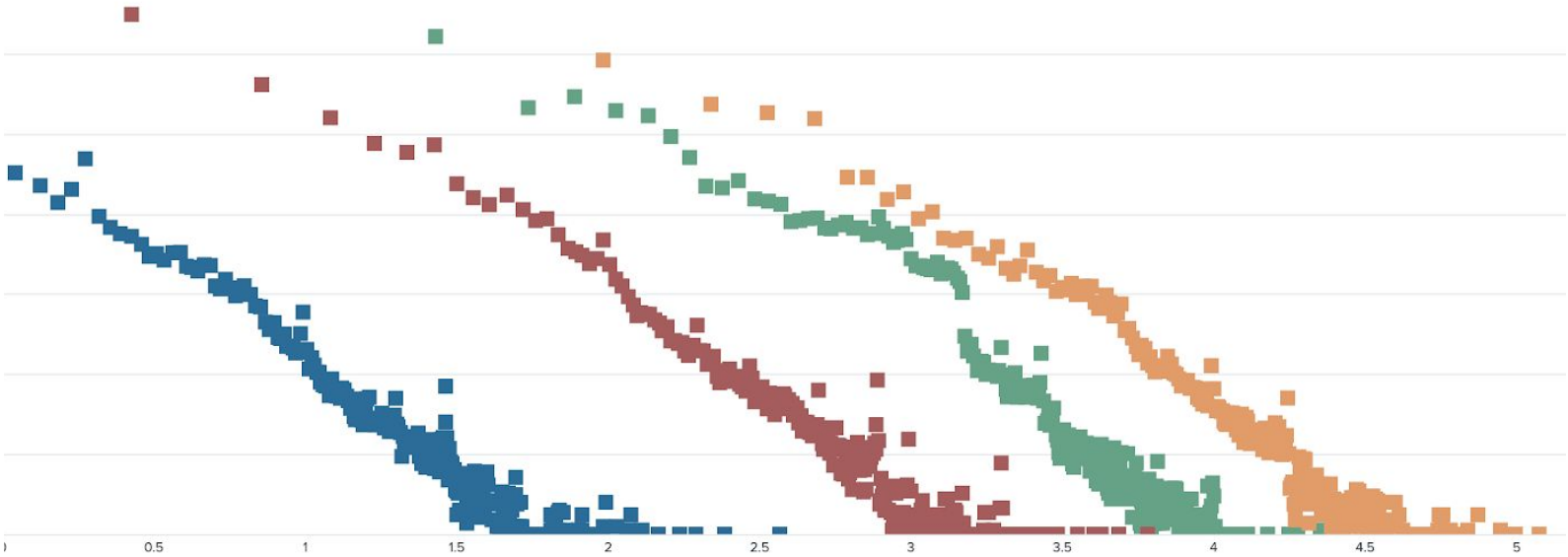
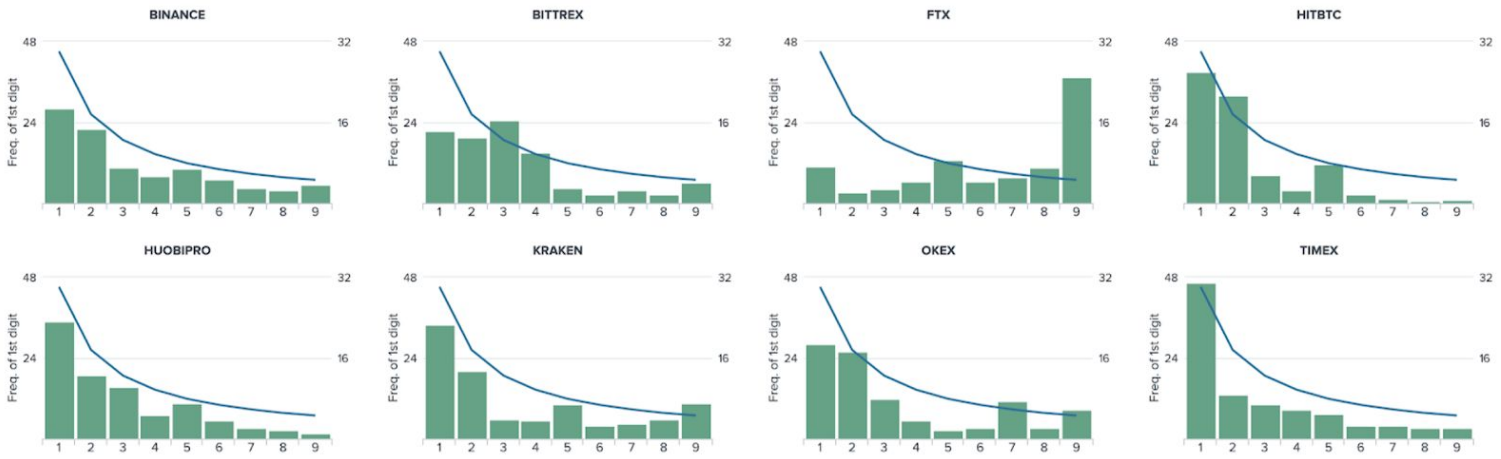
Crypto Market Anomalies
November 2020



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.



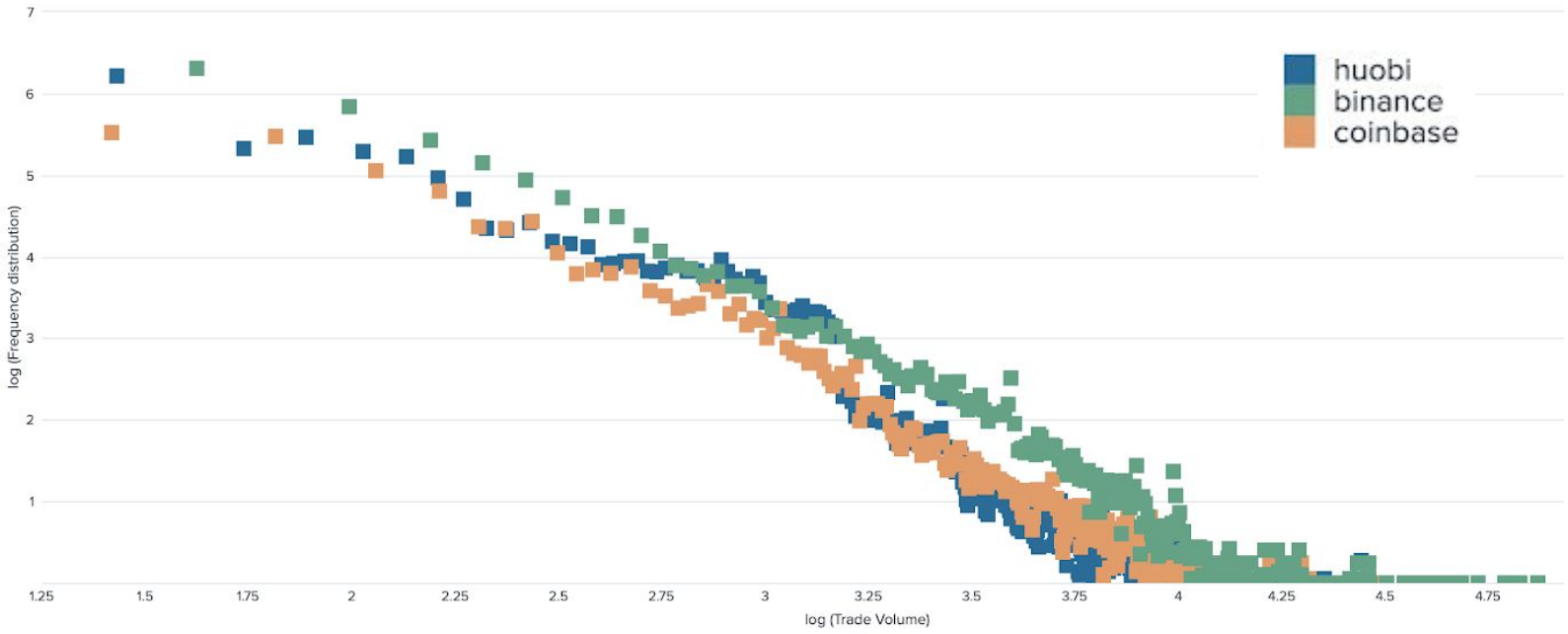
Frequency distribution of leading digits. Spot market COMP token order size Nov 8-10, 2020 (~500,000 events used).

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.

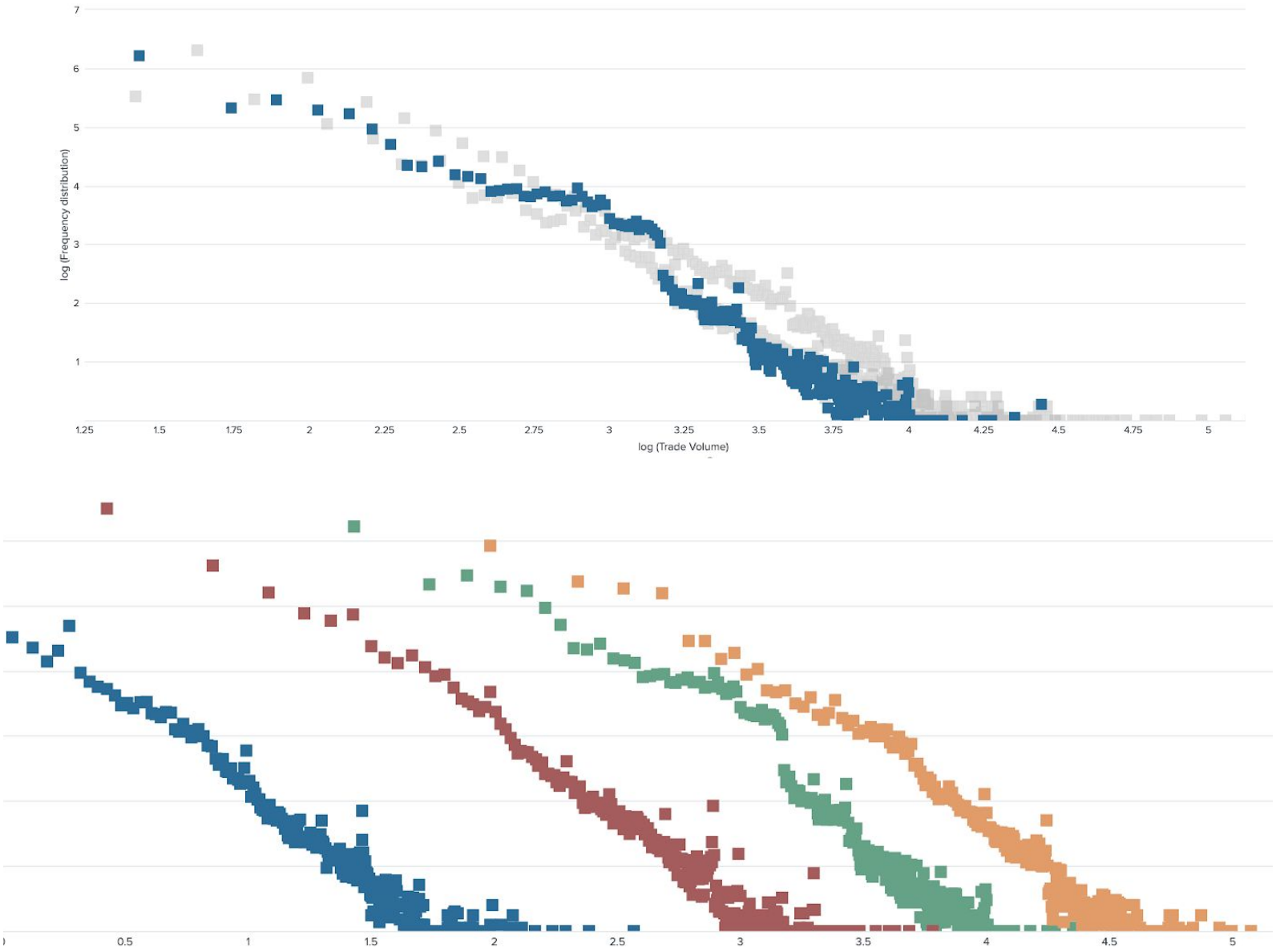
LINK Trading Volumes Deviations on Huobi

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.



Frequency distribution of trading volumes of LINK token on Coinbase, Binance, Huobi exchange Oct 10 – Nov 10, 2020. Source: NTerminal data in Splunk

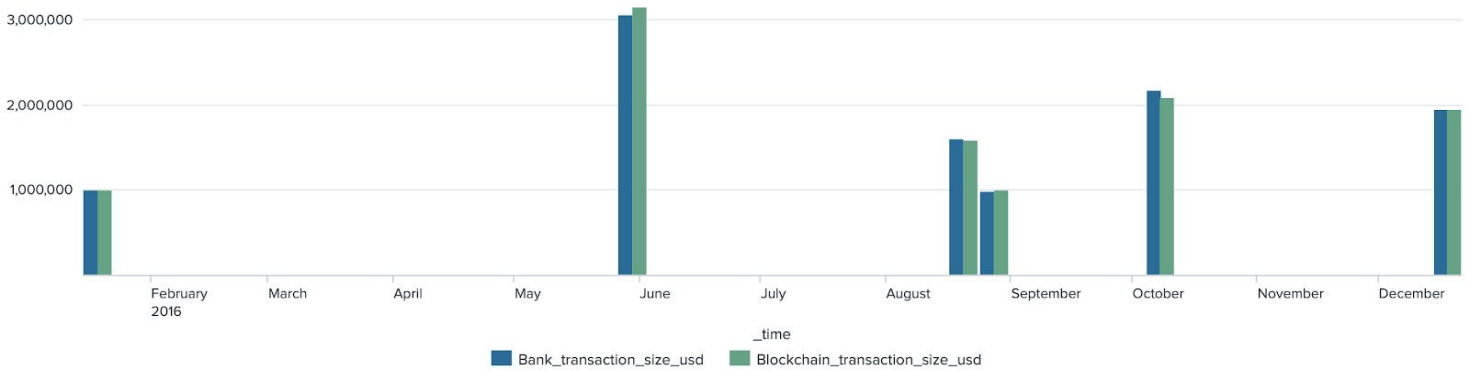
Exchanges or token creators can use trading algorithms that increase trading volumes to create an impression of a more active market. Many of the more simplistic and standardized methods of anomaly detection, such as aggregate raw trade-size distribution analysis, can be rendered ineffectual by more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



Frequency distribution of trading volumes of LINK, BTC, ETH, EOS tokens on Huobi exchange Oct 10 – Nov 10, 2020. Source: NTerminal data in Splunk

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:

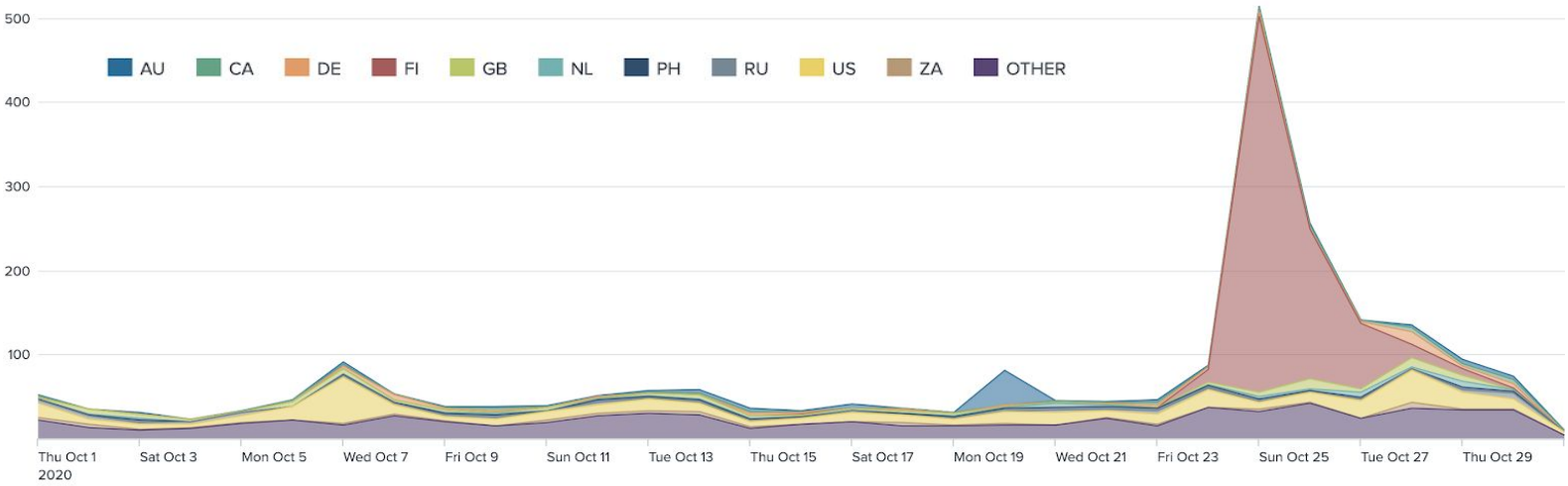


Blockchain and flagged bank transaction volume (USD) streams overlapped in the common time period, Jan — Dec, 2016. Source: NTerminal data in Splunk

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.

October Spike in Crypto Scam Activity - Finland

Traditionally, the United States and Russia lead in reported crypto scam activity. However, there was a recent spike in scams targeting Finland.



The number of reported abuse cases by country. Source: bitcoinabuse.com, tracks bitcoin addresses used by ransomware, blackmailers, fraudsters. Source: NTerminal data in Splunk

Such a spike may be explained by the recent data leak of 50,000 patients of Finnish mental health services provider Vastaamo. The data breach was discovered after many patients received messages threatening to publish personal data unless a bitcoin ransom is paid. Vastaamo admitted to losing their patients' data 2 weeks ago. This resulted in thousands of fraud reports submitted to bitcoinabuse.com and at least 6 ransom transactions totaling 0.467 BTC paid to the scammers.

Many of these reports are associated with a coordinated effort. Ransom attacks were conducted via the email “no-reply@smileup.site” which threatened to release patient records, therapy notes, and personal data. Blackmailer(s) sent Finnish emails demanding a payment of “200 euros during the first 24 hours or 500 euros during 48 hours in order to destroy our data.”

13FgAQMt87THtuVRp12R9bmXJaV7ThCGwA 13FzvVBSdFzMMDMnNMAqdj1W6HLotG51ME 13Ji22o7XK1ErVWRZNFb9dX3Y6zLzQ2rX3 13MZvfgUp3SaGzh37ufwNcubzjGaZVdzmX 13Xshh6Jo1Xt97X4KcZS9bikuGT8CP
13b7gkrwGz15L9XZ2G7ghBpvizZQFKPQkc 13d1nC8eF1iWiXtz7XBSe9FMTwz4prWp2h 13dPXr5SYNYhxZEeYs585kmDdvdRqRze5A 13dz3HnUsbV4yHTXGkt6JUJptjhB67rY2Y 13kMm3HMELtbeWiaP3WG47UWDsX9RxV
13qE7bSQDUA1wqPJ5Nqhc8LqBZAH5keG82 13vYFf4pJqyfs2CEGijsjiM6RuR72jx3Yo 13vyGJf6g8npGG6c9Jqpd1s1MxHoyjaeEM 141BHpyzSFRjb1wPQ23NZSMHmmuBKq58pD 147a98KrzpMFUHpsu8eifnuTFEBQJRR
147oMCyfPzUtk7TXaf5n9ZAMtfGLF9VEV8 148bZFgjTkqssnGrRVF3pxUgdtiEA5Lexm 14CLq5qRkp8CC7uEyfkqSdnTQ8xhrY2MQx 14EynaP32uNtfjYRzV96SEHpizTegv2mfE 14Gu8jpb4wECgjAPNtasTXjjtfFtQf
14H1rkiTwaTNRdytEvRfA7cFATEXgs9TDf 14KYuY4rNH2G9PRqLhNJiX5aMeNb7Syfcf 14LrgvGmx8qSBH7TWJFRF1dmqgHjZxkXsW 14NELRiP4zTYxnse6fUnBN84eQtu5yFMGD 14PQh1vt8QBgjd5uMqdqUMUM76AzZQ
14S7GHbjoaNuR3rWhLmAxNVBKt5DezvG3q 14Ud6tq9JZjX7yxev8p55sYo7jHSxdh9Ni 14V23dzi5RRf1yMpYh98vzazhkJzM4gfHQ 14WUyyigiF7Z4zbTToPVw3JZnP4cVqDJoe 14b62xYgrUCceKqi5RD1bpR6intp9uM
14bjpKY1PRz2MqYHP1AqjxRYhFsgKMAPBL 14bm6H9pQ7cSX9MR4HqzAhRg9svX6i96TA 14gDKBsJFJsX4DoGsAATAGQyWt64VwAbBb 14gbGSGqCb3bvy86FtUDJuC3CwAYbCV8zy 14hYPYtNtr2pTCoRJEfPJWGYnb92TJy
14jJEnwcvg8mp96wAi9KuW3pbSQ93WgTmH 14jQogSpouxdw73x1bzxks4ufi8zLTAXW3 14k7QRMHQRfzVVpTSRstqSPiLcLJqrepNM 14kQTp4tKY4WxE2TBCeKVDJ9yzfbJ2rFP7 14tJTSDg3HFfEfWrY4j8RMfSq5KQAB
14u6WJLeaPNnGB1xgbeJHW1cKaeYtHWvsL 14vSCf3AzMVq9SxSdZEw1YCDMVChiBeaq5 14wGpV4HTcFrq6tpQ9DzgrpsUJM7kDvh59 14wM4TH8F5WkSYeY9ttukoatjcuvFfbx4Q 14zJcRuLE2RZuQ79AyAB28uRFPxKMyD
14zNk37zyZrTfPkCCwuyjkeGtPcZ3arsN8 153E5K8MCbuXSXNScHhzCKaeFn3UVCJd7m 154zNduJePQxdPsdosCevzua6MuLBP3Vn1 157wa22fAd7GSp5cu8NA6jQTmCcQEQodYE 157xk5nTq4GfNr133w1LXRgY8y5CQTC