ISSN 1611-1699 / eISSN 2029-4433

VILNIUS TECH Vilnius Gediminas Technical University

JOURNAL of BUSINESS ECONOMICS & MANAGEMENT

2026
Volume 27
Issue 4
Pages 801–821

https://doi.org/10.3846/jbem.2026.27877

ANOMALIES IN CRYPTOCURRENCIES TRADING VOLUMES USING BENFORD'S LAW

Marian Pompiliu CRISTESCU[1], Raluca Andreea NERIȘANU[1]✉, Simona-Vasilica OPREA[2], Adela BÂRA[2], Dumitru Alexandru MARA[1], Lia Cornelia CULDA[1]

[1]*Department of Finance and Accounting, University Lucian Blaga of Sibiu, Sibiu, Romania*
[2]*Economic Informatics and Cybernetics Department, The Bucharest University of Economic Studies, Bucharest, Romania*

Article History:
- received 14 November 2025
- accepted 15 June 2026

Abstract. (1) Background: This research evaluates the efficacy of an expanded suite of Benford's Law analyses—integrating highly sensitive Kolmogorov-Smirnov (KS) and Anderson-Darling (AD) tests—across diverse cryptocurrencies and temporal scales. By examining both legitimate digital assets and a documented Ponzi scheme, the study identifies robust statistical methodologies for detecting manipulated trading-volume data in de-centralized markets; (2) Methods: The analytical framework assesses the conformity of first- and second-digit distributions with theoretical Benford expectations. The methodology employs a multi-test battery including Pearson Chi-square, Mean Absolute Deviation (MAD), Anderson-Darling, Kolmogorov-Smirnov, Kuiper and Cramér-von Mises tests to ensure sensitivity to both central and tail-end distributional anomalies; (3) Results: Empirical findings demonstrate that Dogecoin, Litecoin, and Luckycoin exhibit significant conformity with Benford's distribution across the KS and AD metrics. Conversely, Bitconnect demonstrates systemic nonconformity across all applied statis-tical tests; (4) Conclusions: While Benford's Law is an effective initial diagnostic, it is not a standalone solution for cryptocurrency fraud detection. Among the methods tested, the Anderson-Darling (A-D) and Kolmogorov-Smirnov (K-S) tests exhibited the highest sensitivity, providing a robust framework for identifying sophisticated data manipulation.

Keywords: Benford's law, cryptocurrency, trading volume, fraudulent activity, anomaly detection, manipulated dataset.

JEL Classification: G15, G17.

✉Corresponding author. E-mail: *raluca.andreea.nerisanu@gmail.com*

Notations

Abbreviations

A-D – Anderson-Darling (test);
BCC – Bitconnect (cryptocurrency);
Chi-square – Chi-squared (statistical test);
DOGE – Dogecoin (cryptocurrency);
FOMO – Fear Of Missing Out;
HDG – Hierarchical, Density-based and Grid-based (Clustering Algorithm);
ICO – Initial Coin Offering;
JEL – Journal of Economic Literature (classification codes);

K-S – Kolmogorov-Smirnov (test);
LITE – Litecoin (cryptocurrency);
LUCKY – Luckycoin (cryptocurrency);
MAD – Mean Absolute Deviation;
ML – Machine Learning;
SVM – Support Vector Machine;
CvM – Cramér-von Mises.

1. Introduction

Following the observation that logarithmic tables for smaller integers (1 and 2) exhibited significantly more wear than those for higher digits (8 and 9), physicist Frank Benford initiated a comprehensive study into the frequency distribution of leading digits across various numerical sequences (Benford, 1938). This investigation spanned a diverse empirical spectrum, including data from newspaper front pages, street addresses, and molecular weights (Benford, 1938). It is important to note, however, that Benford's original research did not encompass all possible numerical series (Benford, 1938); furthermore, Simon Newcomb had previously documented the distribution of first digits as early as 1881 (Mir & Ausloos, 2018; Newcomb, 1881). Subsequently, Badal-Valero et al. (2018) proposed a sophisticated methodology integrating Benford's Law distribution testing with machine learning algorithms to detect money laundering activities. The distribution of leading digits in datasets derived from natural and socio-economic phenomena—such as river drainage areas, stock market indices, census data, chemical heat capacities, and random figures from the press—is described by Benford's Law (Arshadi & Jahangir, 2014). Initially established through empirical observation, it has been confirmed that this statistical regularity applies not only to experimental data but also to mathematical sequences (such as the Fibonacci sequence and n!) and specific probability distributions, as documented in (Sarkar, 1973; Wlodarski, 1971).

Cryptocurrencies, as digital financial assets, have fundamentally disrupted the traditional financial landscape, posing substantial challenges to established institutional frameworks (Giudici et al., 2020). The regulatory environment governing their operation remains a critical global concern, with national policies ranging from active support to total prohibition or restrictive measures. Often characterized as virtual financial instruments synonymous with the millennial generation, cryptocurrencies offer the distinct advantage of investor anonymity (Ivan & Bădele, 2021). However, these assets are subject to concerns regarding market efficiency, stability, and inherent risks. The anonymity afforded to investors can potentially facilitate illicit activities, such as tax evasion, money laundering, and the financing of terrorism within financial markets (Nica et al., 2017).

The primary objective of the research presented in this paper is to evaluate the suitability of Benford's Law conformity tests in identifying anomalous behavior within cryptocurrency transactions. We aim to expand the application of Benford's Law from established domains—such as physics, astronomy, geophysics, chemistry, engineering, mathematics (Sambridge et al., 2010), environmental science (Stoerk, 2016), economics (Michalski & Stoltz, 2013; Nye & Moul, 2007), tourism (Cerqueti & Provenzano, 2023; Chemin & Mbiekop, 2015; Jawabreh et al., 2018; Matakovic, 2021; Neves et al., 2021), and finance (Ausloos et al., 2016; Clippe & Ausloos, 2012)—to the field of cryptocurrencies.

By considering the properties of datasets expected to conform to the Benford distribution, alongside the potential errors associated with anomaly detection, this study tests cryptocurrency trading volumes for irregularities to detect fraudulent activities, such as Ponzi schemes. Consequently, four datasets are analyzed for conformity: Litecoin (LITE), Luckycoin (LUCKY), and Dogecoin (DOGE)—representing assets with no recorded fraudulent activity during the analyzed period—and Bitconnect (BCC), representing assets associated with malicious activities. Initially, the tests were applied to datasets with no suspected data violations or public suspicion of anomalies (Litecoin, Dogecoin, and Luckycoin). These results were then compared against datasets from entities retracted due to verified violations to determine the test's efficacy in detecting known fraud (Bitconnect).

The primary contributions of this research include: (a) Comprehensive Multi-Coin and Multi-Period Analysis: The study spans seven years for Litecoin and Dogecoin, two years for Luckycoin, and includes the early Bitconnect era; (b) First- and Second-Digit Analysis: While most Benford-based studies focus exclusively on the first digit, this research evaluates both the first and second digits against expected frequencies, providing a higher level of granularity for anomaly detection; (c) Implementation of Advanced Goodness-of-Fit Tests: Moving beyond standard Chi-square and Mean Absolute Deviation (MAD) metrics, this study employs Anderson–Darling (AD), Kolmogorov–Smirnov (KS), Kuiper and Cramer-von-Mises (CvM) tests, demonstrating their superior sensitivity in flagging deviations in daily trading volumes.

The paper is organized into five sections. The first section provides the introduction, theoretical background on cryptocurrency fraud, and the application of Benford's Law in anomaly detection. The second section reviews the relevant literature, while the third section details the methodology. The fourth section presents the input data and the results of the conformity tests, followed by the conclusion in the final section.

2. Literature review

Cryptocurrency's technological evolution has facilitated sophisticated investor fraud, a paradigm comprehensively organized by Baum (2018). Prominent manifestations include Ponzi schemes reliant on nascent capital (Zuckoff, 2006; Bartoletti et al., 2020; Feng et al., 2024), fabricated Initial Coin Offerings (ICOs), and "pump-and-dump" market manipulations driven by hyperbolic prognostications (Martineau, 2018). These deceptive ecosystems, exacerbating an average daily systemic loss of 9.1 million (Shobhit, 2018), often culminate in misappropriated "exit schemes." A quintessential failure is the Bitconnect Ponzi, which plummeted 80% upon its 2018 collapse (Buntinx, 2018).

Fraudulent ICOs routinely exploit the psychological phenomenon of "Fear Of Missing Out" (FOMO). For instance, Plexcoin manipulated investors by promising unfeasible returns of 1.354% (Levine, 2017), while GIZA and LoopX executed abrupt exit plans that caused substantial capital flight from Bitcoin and Ethereum (Kharpal, 2018; Osborne, 2018).

While fake ICOs are identifiable via regulatory filings and technical whitepapers, extended Ponzi schemes manifest primarily as anomalous secondary market trading volumes. Consequently, this study applies Benford's Law to analyze volumetric nonconformity between Ponzi-associated and legitimate cryptocurrencies during the 2017–2018 period.

Systemic cryptocurrency fraud is driven by regulatory opacity, anonymity, low entry barriers, and technical complexity (Carol & Douglas, 2020), exemplified by counterfeit Ethereum Erc20 tokens (Gao et al., 2021). Detection increasingly relies on machine learning methodologies (Kamišalić et al., 2021; Vičič & Tošić, 2022), such as identifying illegitimate Ethereum accounts (Farrugia et al., 2020), utilizing random forest clustering for anomalous wallet behavior (Baek et al., 2019), and deploying Support Vector Machines (SVMs) for Bitcoin network irregularities (Sayadi et al., 2019).

Broadly, anomaly detection targets behavioral outliers (Prasad et al., 2009) via supervised (Goernitz et al., 2013), semi-supervised (Tsai & Yen, 2007), and unsupervised (Goldstein & Uchida, 2016) methodological architectures.

Benford's Law (Benford, 1938) provides robust forensic analysis for detecting accounting fraud (Kolar & Horvat, 2026), cryptocurrency behavior (Grigorescu & Amza, 2025), natural datasets (Coderre, 1999), COVID-19 trends (Kolias, 2022), scientometrics (Slosar, 2026; Bertin & Lafouge, 2025), manufactured interviews (Bredl et al., 2012) or even driver's deviations within a normal behavior (Kauko, 2024). Integrating this law with numerical analysis highlights statistical anomalies indiscernible through conventional means (Drake & Nigrini, 2000; Holz, 2014). Figure 1 provides a structured mind map synthesizing these foundational applications, crypto-fraud typologies, and computational detection strategies.

The existing literature identifies several inherent complications that may arise when implementing Benford's Law within the auditing process. A primary concern is the risk of a Type I error—a false-positive outcome wherein the researcher incorrectly rejects a null hypothesis that is, in fact, true for the underlying population (Cleary & Thibodeau, 2005). For instance, empirical evidence suggests that price distributions in eBay auctions do not conform to Benford's Law (Giles, 2007).

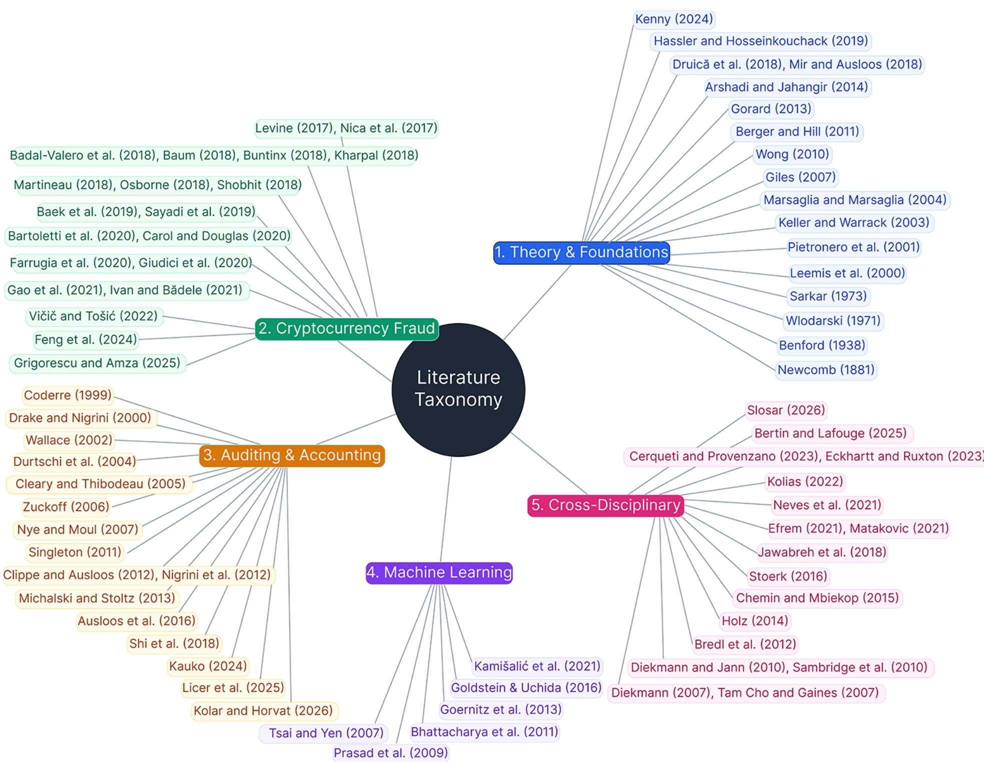

Figure 1. Structured mind map of previous works on specific areas

The rejection of the null hypothesis in this context implies that the observed numerical data deviates from the expected Benford distribution. According to Cleary and Thibodeau (2005), such non-conformity can be attributed to at least four distinct factors: (a) Statistical Variance: The dataset inherently follows Benford's Law, yet this specific sample set exhibits a deviation due to random chance (Type I error); (b) Structural Constraints: The data fails to fulfill the necessary assumption of spanning multiple orders of magnitude (Leemis et al., 2000); (c) Operational Regularities: There is a legitimate, non-fraudulent explanation for the overrepresentation of specific leading digits, such as standardized recurring transactions (e.g., fixed payments or refunds); (d) Actual Irregularities: Certain entries are indeed fraudulent, representing a valid alternative hypothesis.

In many practical scenarios, it remains a factual reality that such deviations may occur even in the absence of fraudulent activity.

3. Methodology

The Newcomb-Benford Law, also referred to as the First-Digit Law, is a statistical observation regarding the frequency distribution of leading digits in many real-life sets of numerical data (Newcomb, 1881; Vičič & Tošić, 2022). According to Benford's Law, the probability of the first significant digit occurring is governed by the following logarithmic function (1) (Cleary & Thibodeau, 2005):

$$P\left(d_1 = m_1\right) = \log_{10}\left(\frac{m_1+1}{m_1}\right), \; d1 \in \{1, 2, 3, \ldots, 9\}, \tag{1}$$

where $P(d)$ is a proportional quantity to the space between d and $d + 1$ on a logarithmic scale (Vičič & Tošić, 2022). Furthermore, the law extends to the second significant digit (d2), where the distribution follows Eq. (2) (Durtschi et al., 2004):

$$P\left(d_2 = m_2\right) = \sum_{m_1=1}^{9} \log\left(1+\frac{1}{m_1 m_2}\right), \; d_2 \in \{0, 1, 2, 3, \ldots, 9\}. \tag{2}$$

The following probabilities, associated with each digit are exposed in Table 1.

Table 1. Benford law distribution

Digit	Benford probability first digit	Benford probability second digit
0		12.00%
1	30.10%	11.40%
2	17.60%	10.90%
3	12.50%	10.40%
4	9.70%	10.00%
5	7.90%	9.70%
6	6.70%	9.30%
7	5.80%	9.00%
8	5.10%	8.80%
9	4.60%	8.50%

Prior research indicates that while the first digits of fabricated data often exhibit a pattern of monotonic decline, the second, third, and fourth digits typically deviate more significantly from Benford's Law (Diekmann, 2007). Consequently, this study evaluates both the first and second significant digits. Our alternative hypothesis posits that anomalous activities associated with fraudulent cryptocurrency reporting can be identified through their nonconformity with the Benford distribution. To test this hypothesis, we initially employ the Pearson Chi-squared Goodness-of-Fit test (Keller & Warrack, 2003), defined in Eq. (3):

$$\chi^2 = \Sigma\ ((O_i - E_i)^2/E_i, \tag{3}$$

where O_i and E_i represent the observed and expected frequencies, respectively. If the resulting p-value is below the predetermined threshold for Type I error (typically $\alpha = 0.05$), the null hypothesis of conformity is rejected. It has been noted that "digit-by-digit" evaluations may yield false positives more frequently than general tests (Cleary & Thibodeau, 2005). Therefore, a systematic procedure is adopted: first, performing both test-by-test and digit-by-digit examinations, and second, applying these analyses to both the first and the first two digits for large datasets (Cleary & Thibodeau, 2005).

In addition to the Chi-square test, we utilize the Mean Absolute Deviation (MAD) (Gorard, 2013), which is considered a more robust instrument for large-scale data analysis (Vičič & Tošić, 2022). However, even MAD estimates should be interpreted with caution as sample sizes increase (Druică et al., 2018). According to Nigrini (2012), MAD is the most effective metric for this purpose, utilizing the following thresholds for conformity: close conformity (0.000–0.006), acceptable conformity (0.006–0.012), marginally acceptable (0.012–0.015), and nonconformity (>0.015). MAD is calculated as follows (Efrem, 2021), in Eq. (4):

$$MAD = \frac{\sum_{i=1}^{k} \left| P_{obs} - P_{\exp} \right|}{k}, \tag{4}$$

where k represents the number of bins, in this case 9 for the first digit and 10 for the second digit.

To ensure analytical rigor, we further implement several nonparametric tests. The Cramér-von Mises (CvM) test (Hassler & Hosseinkouchack, 2019), which can be computed in relation to the Chi-square value, is expressed as follows from Eq. (5):

$$C = \sqrt{\frac{X^2}{n \times d_f}}, \tag{5}$$

where n is the number of observations, X^2 is the Pearson Chi-square and d_f are the degrees of freedom considered for the analyzed case.

Another nonparametric test used the equality of a continuous, one-dimension, probability distribution test is Kolmogorov-Smirnov, and can be estimated by comparing the value obtained with Eq. (6) with its critical value:

$$K - S = \max_x \left| S_n(x) - F_n(x) \right|, \tag{6}$$

where the S_n function is the cumulative distribution function of expected and F_n function is the cumulative distribution function of observed variables.

The Anderson-Darling test, also a nonparametric distribution test can be used to test the conformity with the Benford distribution, as follows in Eq. (7):

$$A - D = \frac{n}{2}\sum_{x=1}^{n-1} \frac{\left(E_x + E_{x+1}\right) \times (S_{nobserved}\left(x\right) - S_{nexp\,ected}\left(x\right))^2}{S_{nexp\,ected}\left(x\right) \times \left(1 - S_{nexp\,ected}\left(x\right)\right)}, \tag{7}$$

where the E_x is the expected value (Benford distribution probability) and S_n function is the cumulative distribution function of expected and observed variables.

In Hassler and Hosseinkouchack (2019), Monte-Carlo simulations were used to test the power of X_2, Cramer-von Mises, and Kuiper's variant of the Kolmogorov-Smirnov test, concluding that Cramer-von Mises and Kuiper's variant of the Kolmogorov-Smirnov test are underpowered in comparison to the simple X_2-test with one degree of freedom (Eckhartt & Ruxton, 2023). In Wong (2010), it is stated that, in the absence of the variance ratio and X2 with one degree of freedom, the Cramer-von Mises or Anderson-Darling tests can provide the greatest power to detect some types of deviation.

We will adopt the Kuiper's test in order to calculate the sum of the maximum deviations above and below the Benford's Law curve. This rotationally invariant approach is particularly advantageous for high-frequency volatility analysis because it provides equal statistical weight to all segments of the distribution. In financial forensics, anomalies often cluster at the extreme frequencies of digits 1 and 9, which the standard KS test may under-report. The Kuiper's test is shown in Eq. (8):

$$V = D^{+} + D^{-}, \tag{8}$$

where V is Kuiper's statistic, D^+ is the maximum deviations above, and D^- is the maximum deviations below the Benford's Law curve.

To further validate the distributional integrity datasets, this study utilizes the Cramer-von Mises (CvM) goodness-of-fit test. Unlike the Kolmogorov-Smirnov test, which identifies only the maximum local deviation, the CvM test is an integrated metric that calculates the sum of the squared differences between the empirical distribution function, and the theoretical Benford's Law cumulative distribution. This characteristic makes the CvM test exceptionally useful for financial forensic analysis; mainly because it can detect subtle, systemic biases that may not produce a single large spike but collectively indicate data smoothing or rounding. The statistic is formally defined by the Eq. (9):

$$W^2 = n\int_{-\infty}^{\infty} \left[S_n\left(x\right) - F\left(x\right)\right]^2 dF\left(x\right), \tag{9}$$

where W^2 is the Cramer-von Mises (CvM) statistic, $S_n(x)$ is the empirical distribution function, and $F(x)$ is the theoretical Benford's Law cumulative distribution.

To ensure a robust detection of market anomalies, this methodology shifts the analytical focus from average returns to the dispersion of data, specifically targeting market volatility. While price returns can aggregate and mask structural irregularities, the variance of those returns provides a transparent view of the market's movement. We apply the Mean Absolute Deviation (MAD) test to Absolute Returns as a direct proxy for volatility. By evaluating the conformity of this dispersion to Benford's Law, the MAD test serves as a high-sensitivity diagnostic tool, isolating non-conformities in the market's risk structure and providing a rigorous baseline for detecting data engineering in the dataset.

Data consisted of daily volumes of transactions for Litecoin, Dogecoin, Luckycoin and Bitconnect in three periods: 2017–2024 (Litecoin and Dogecoin), 2022–2024 (Luckycoin) and 2017–2018 (Bitconnect), obtained from Yahoo Finance (yahoo.finance.com).

4. Results

4.1. Input data

The bibliometric analysis facilitates the visualization of conceptual relationships among the most frequent keywords derived from 649 records indexed in the Web of Science Core Collection, retrieved using the search string "Benford's law." The entire corpus of results was included in this bibliometric assessment. As illustrated in Figure 2, "fraud" and "financial statements" emerge as primary thematic clusters frequently associated with Benford's Law in the extant literature. Furthermore, the analysis reveals significant interdisciplinary connections to terms such as "galaxies," "distributions," and "anisotropy," reflecting the law's application within the physical sciences.

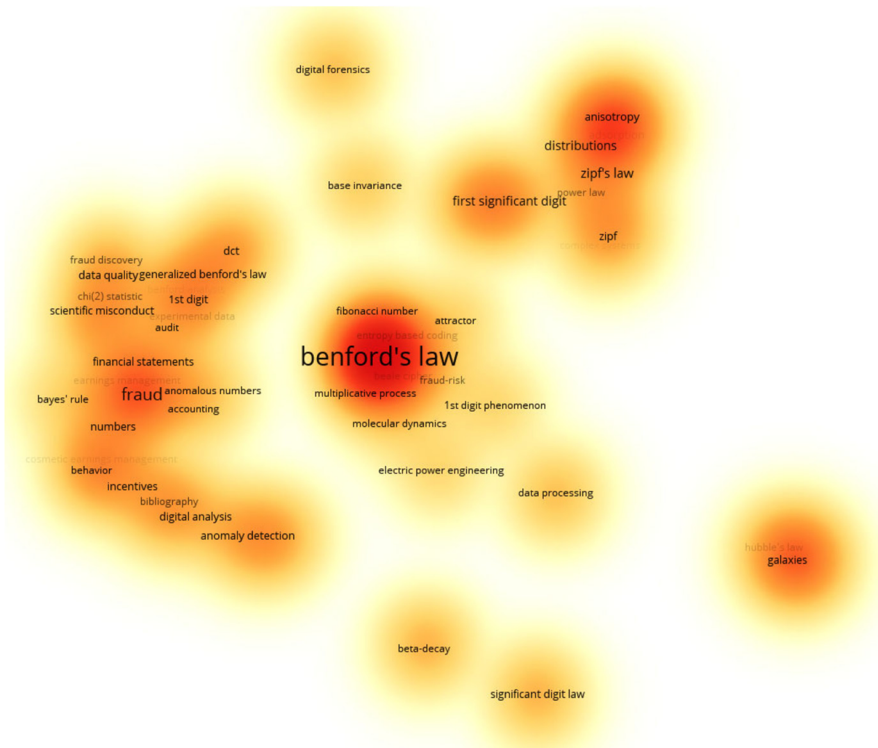

Figure 2. Density visualization of the Benford's law research article keywords, indexed in Web of Science, date created: 30.03.2024

To rigorously evaluate whether a dataset conforms to the Benford distribution, the selected data must satisfy a specific set of structural properties documented in the literature. As originally proposed in Singleton (2011) and subsequently cited in Vičič and Tošić (2022), datasets characterized by multiple geographic locations and a diverse range of value distributions are expected to exhibit first-digit frequencies congruent with Benford's Law.

For instance, "assigned" data—such as movie ratings or academic grades—represent unsuitable candidates for Benford analysis due to their constrained scales and lack of natural variance. Conversely, national population statistics serve as a prototypical example of suitable data, as they satisfy the requirements for both spatial dispersion and varied numerical distributions. Similarly, the daily trading volume of cryptocurrencies aligns with these criteria; the cryptocurrency market functions as a global, decentralized exchange environment with minimal systemic restrictions. Consequently, daily transaction volumes represent a comprehensive aggregation of global market activity. Such data is classified as "measured" rather than "assigned," further validating its eligibility for Benford's Law conformity testing.

The suitability of the selected datasets for Benford's Law analysis is supported by several statistical properties. Firstly, as illustrated in the distribution graphs for the four analyzed cryptocurrencies (Figure 3), the data exhibits a pronounced right-skewed (positively skewed) profile. Secondly, the daily transaction volumes adhere to the requirement of having no predefined functional maximum or minimum limits, with the exception of the natural lower bound of zero.

Regarding sample size constraints, the literature suggests that Benford's Law remains applicable for datasets containing a minimum of 50 to 100 observations (Kenny, 2024). Conversely, Wong (2010) indicates that in datasets exceeding 3,000 observations, the rejection rate of the null hypothesis increases significantly, potentially flagging distributions that deviate only marginally from the theoretical norm (Eckhartt & Ruxton, 2023). Our empirical datasets comprise a maximum of 2,328 observations (daily trading volumes), thereby aligning with these established boundaries and ensuring the statistical power of the tests remains appropriate.

Furthermore, Eckhartt and Ruxton (2023) posit that for a dataset to conform to Benford's Law, it must span multiple orders of magnitude. While physical attributes such as human height or weight typically oscillate within only two orders of magnitude, the daily transaction volumes of cryptocurrencies in this study span up to 11 orders of magnitude, significantly exceeding the minimum threshold. Additionally, Eckhartt and Ruxton (2023) note that conformity is often associated with datasets where the mean exceeds the median. This is further supported by Wallace (2002), who argues that if the mean of a numerical set is greater than its median and the skewness is positive, the dataset is highly probable to follow a Benford distribution (Berger & Hill, 2011).

The descriptive statistics for the four analyzed cases are detailed in Table 2. As evidenced by the data, the mean consistently exceeds the median across all observations, satisfying a key prerequisite for Benford's Law conformity. Furthermore, it is posited that datasets conforming to the Benford distribution are predominantly quantitative rather than qualitative; accordingly, the daily trading volumes of cryptocurrencies are classified herein as quantitative variables.

Should a dataset fail to meet these fundamental properties, it is unlikely to comply with Benford's Law. For instance, "assigned" numbers (such as check or order numbers) and those influenced by human psychological thresholds or institutional constraints (such as consumer pricing or ATM withdrawal limits) typically do not obey the distribution (Durtschi et al., 2004). In the context of forensic auditing, fraudulent activity often manifests as irregular numerical patterns, which serve as "red flags" necessitating a more exhaustive investigation (Bhattacharya et al., 2011).

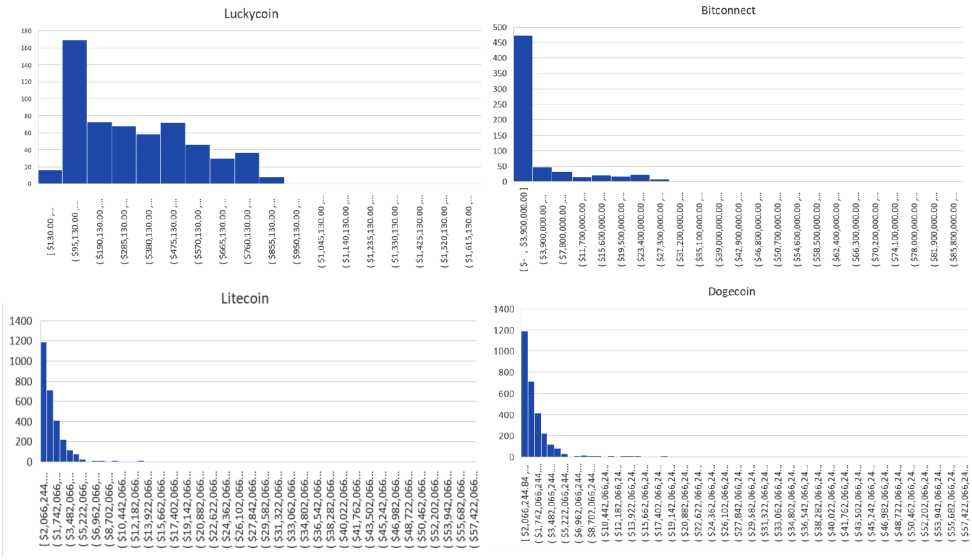

Figure 3. Histograms of analyzed coins

In testing for conformity to Benford's Law, the theoretical probability of the digit 1 occurring is 30.103%. Statistical significance is determined by the Z-statistic, where a value of 1.96 corresponds to a p-value of 0.05 (95% confidence level), and a Z-statistic of 1.64 corresponds to a p-value of 0.10 (90% confidence level). Significant deviations from expected values are identified when observations fall within the tails of the distribution (Durtschi et al., 2004).

Table 2. Descriptive statistics of Dogecoin, Luckycoin, Litecoin and Bitconnect

	DOGECOIN	LUCKYCOIN	LITECOIN	BITCONNECT
Mean	943,170,946	383,903	2,000,790,744	2,166,637
Standard Error	65,274,265	9,439	47,514,643	181,865
Median	188,892,121	349,329	987,349,424	5
Standard Deviation	3,149,440,991	227,512	2,292,550,757	6,906,076
Kurtosis	154.85	0.88	7.38	38.88
Skewness	10.41	0.86	2.35	5.23
Range	69,409,248,965	1,639,056	17,873,477,585	89,600,000
Minimum	1,431,720	130	120,785,909	0'
Maximum	69,410,680,685	1,639,186	17,994,263,494	89,600,000
Sum	2,195,701,962,381	223,047,380	4,657,840,852,167	3,124,291,071
Count	2,328	581	2,328	1,442
Confidence Level (95.0%)	128,001,786	18,538	93,175,453	356,748

4.2. Law distributions and conformity tests

Figures 4 through 7 illustrate the empirical distribution of the first two leading digits for the total daily transaction volumes of Dogecoin, Litecoin, Luckycoin, and Bitconnect. The analysis encompasses a seven-year longitudinal period from 2017 to 2024. In these visualizations, the observed distributions of the first and second digits of cryptocurrency trading volumes are represented in blue, while the theoretical Benford distributions for the corresponding digits are indicated in orange.

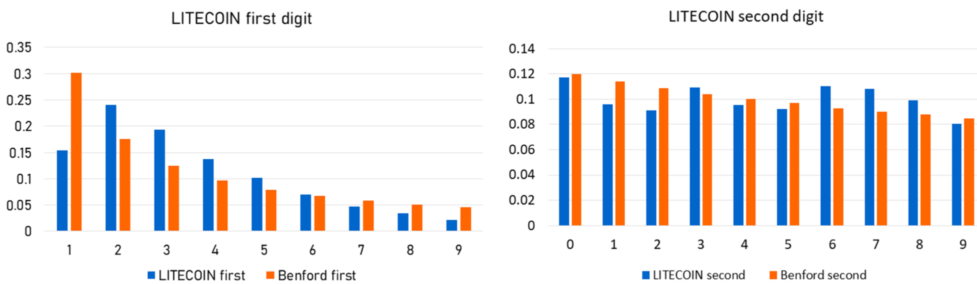

Figure 4. Bar graphs of Litecoin and Benford's law distribution for the first and second digit

Figure 4 present the distribution of the first two leading digits of the daily total volume transitioned with the Litecoin cryptocurrency. It can be observed nonconformity of the first two digits distributions to the Benford distribution.

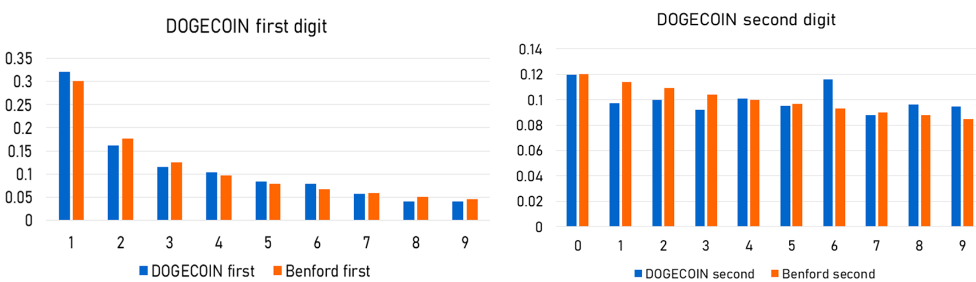

Figure 5. Bar graphs of Dogecoin and Benford's law distribution for the first and second digit

In Figure 5, it can be observed that the first digit of the daily transaction volume of Dogecoin has an acceptable level of conforming to Benford law distribution. In addition, the second digit distribution has a slight conformity value to the Benford law distribution.

Figures 6 and 7 illustrate the distribution of the first two leading digits for the daily trading volumes of Luckycoin and Bitconnect, respectively. Preliminary visual inspection reveals a lack of conformity between the empirical first- and second-digit distributions and the theoretical Benford distribution in the case of Luckycoin. Similarly, for Bitconnect, a marked nonconformity is observed specifically within the second-digit distribution.

The degree of alignment between the empirical data and Benford's Law was rigorously evaluated using a battery of statistical tests, including the Pearson Chi-square, Mean Absolute Deviation (MAD), Kolmogorov-Smirnov (K-S), Anderson-Darling (A-D), Kuiper, and Cramér-von Mises tests.

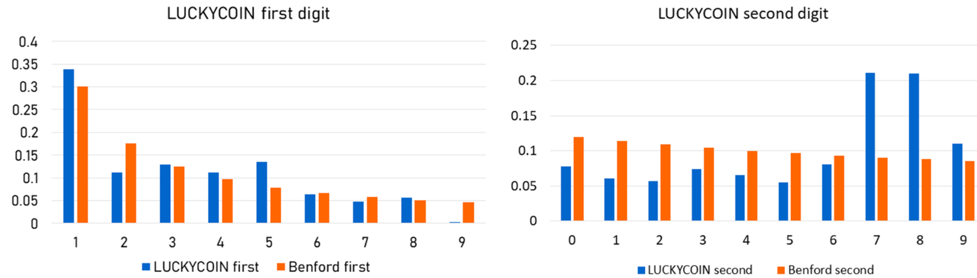

Figure 6. Bar graphs of Luckycoin and Benford's law distributions for the first and second digit

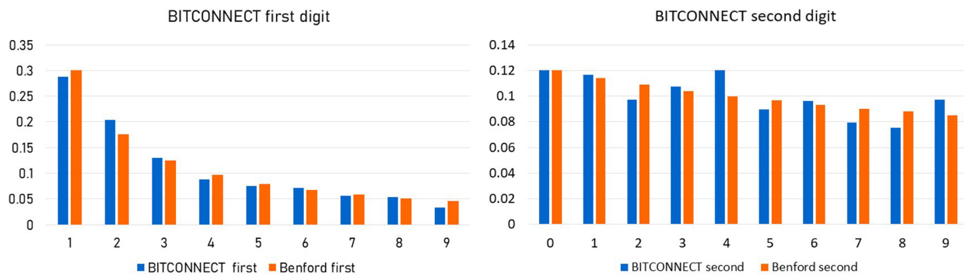

Figure 7. Bar graphs of Bitconnect and Benford's law distributions for the first and second digit

The results, as detailed in Table 4, provide a complex overview of distributional conformity. Regarding the Pearson Chi-square test, the obtained statistics do not provide sufficient evidence to support the null hypothesis of significant deviation for all assets; consequently, the test fails to clearly distinguish between non-fraudulent and fraudulent cryptocurrencies based solely on the first two digits of daily trading volumes. This limitation underscores the necessity for more sophisticated methodologies to evaluate distributional conformity effectively.

The MAD values were evaluated against the interpretative thresholds established by [54]: close conformity (0.000), acceptable conformity (0.006), marginally acceptable conformity (0.012), and nonconformity (>0.015). The adjusted MAD results confirm that the first and second digits of Dogecoin align with the Benford distribution. In contrast, the daily transaction volumes for Luckycoin, Litecoin, and Bitconnect exhibit degrees of nonconformity. Specifically, among all analyzed variables, only the Dogecoin first-digit distribution strictly conforms to the Benford model, while its second-digit distribution demonstrates "close conformity."

To further scrutinize these findings, the Kolmogorov-Smirnov (K-S) and Anderson-Darling (A-D) tests were applied. The K-S statistics for Dogecoin, Luckycoin, Litecoin, and Bitconnect were compared against their respective critical values. A statistically significant result—indicating nonconformity—occurs when the K-S statistic exceeds the critical threshold. While Dogecoin, Luckycoin, and Litecoin exhibit distributions largely in conformity with Benford's Law, the Bitconnect first- and second-digit distributions demonstrate significant deviations. These K-S results support the alternative hypothesis, suggesting that anomalous activity in daily trading volumes results in a measurable nonconformity with the Benford distribution.

Finally, the Anderson-Darling (A-D) procedure was employed to provide a more sensitive measure of distributional tail deviations. Statistical significance is achieved when the A-D value exceeds the critical threshold of 2.492 (corresponding to a 0.05 significance level for n >

100 (Marsaglia & Marsaglia, 2004)). The analysis reveals that the second digit of Dogecoin, along with both digits of Luckycoin and Litecoin, yield A-D values exceeding this critical limit. Conversely, the first digit of Dogecoin and both digits of Bitconnect produce A-D statistics below the threshold. These findings provide further empirical evidence for our alternative hypothesis: that anomalous behaviors associated with fraudulent cryptocurrency reporting can be identified through systematic nonconformity with Benford's Law.

The Kuiper test statistic represents the maximum spread between the empirical cumulative distribution function. Based on the results shown on Table 3, Bitconnect shows a relatively balanced deviation between the first and second digits. In fraud detection, a consistent deviation across both positions can sometimes be more indicative of systematic manipulation than a deviation in only one. Both Dogecoin and Litecoin show higher Kuiper statistics in the first digit compared to Bitconnect, but significantly lower statistics in the second digit. This suggests that while their first-digit distributions might be noisier, their second-digit distributions adhere more closely to Benford's Law than Bitconnect's.

Also, the Cramér-von Mises results are exposed in Table 3. Results for Bitconnect show very low and balanced divergence across both the first and second digits. This indicates that Bitconnect's volume distribution is remarkably consistent with the theoretical Benford expectation, in contrast with the 2016–2018 Ponzi history. Dogecoin shows the highest divergence in the first digit (W^2 = 0.013671), while Litecoin shows the lowest divergence in the second digit (W^2 = 0.000255). While Dogecoin exhibits higher divergence in the first digit, the extremely low second-digit statistic for Litecoin is a strong indicator of high-quality data conformity in that specific position.

Table 3. Chi-square, MAD, K-S, A-D, Kuiper and Cramer-von-Mises tests of the first two digits distributions of the Dogecoin, Luckycoin, Litecoin and Bitconnect daily transactional volume, analyzed in conformity to the Benford law distribution

	Chi-square	p-value	α-Bonferroni corrected	MAD	MAD conformity	K-S	K-S critical value	A-D	Kuiper	Cramer-von Mises
DOGE_ (Digit 1)	28.30	0.001	0.0055	0.0094	Acceptable conformity	0.029	0.024	1.8064	0.0795	0.0137
DOGE_ Digit 2)	24.31	0.004	0.0050	0.0083	Close conformity	0.061	0.024	22.5510	0.0159	0.0061
LUCKY_ (Digit 1)	245.06	0.000	0.0055	0.0265	Nonconformity	0.048	0.047	4.0000	0.0753	0.6686
LUCKY_ Digit 2)	28.33	0.001	0.0050	0.0536	Nonconformity	0.252	0.047	53.6330	0.2903	21.9792
LITE_ (Digit 1)	63.13	0.000	0.0055	0.0443	Nonconformity	0.147	0.024	76.9825	0.0760	0.0062
LITE_ (Digit 2)	244.36	0.000	0.0050	0.0104	Nonconformity	0.062	0.024	20.2233	0.0104	0.0003
BCC_ (Digit 1)	307.22	0.000	0.0055	0.1111	Nonconformity	0.019	0.034	0.6677	0.0439	0.0013
BCC_ Digit 2)	271.56	0.000	0.0050	0.3805	Nonconformity	0.015	0.034	0.2693	0.0411	0.0015

In Figure 8, the Empirical Cumulative Distribution Function (ECDF) plots reveal distinct patterns of non-conformity across the sampled cryptocurrencies, particularly when comparing Litecoin and Luckycoin. In the Litecoin distribution, the observed ECDF (blue line) sits significantly below the theoretical Benford curve (red dashed line) at the start of the scale (Digits 1–2). This indicates a right-skewed anomaly where lower significant digits appear less frequently than naturally expected, that suggests a market dominated by larger, institutional-scale transactions. Conversely, the Luckycoin distribution shows that the observed line sits above the Benford curve, specifically between Digits 5 and 8. This represents an over-concentration of mid-range value. Unlike the natural logarithmic decay of Benford's Law, the volumes in Luckycoin appear to be clustered around specific sub-ranges, potentially indicating automated wash trading or liquidity injection designed to maintain a consistent volume profile. Dogecoin serves as control variables, showing a closer trend to the Benford curve. Their relative conformity suggests that their transaction volumes follow a more organic, power-law distribution typical of decentralized, multi-participant markets.

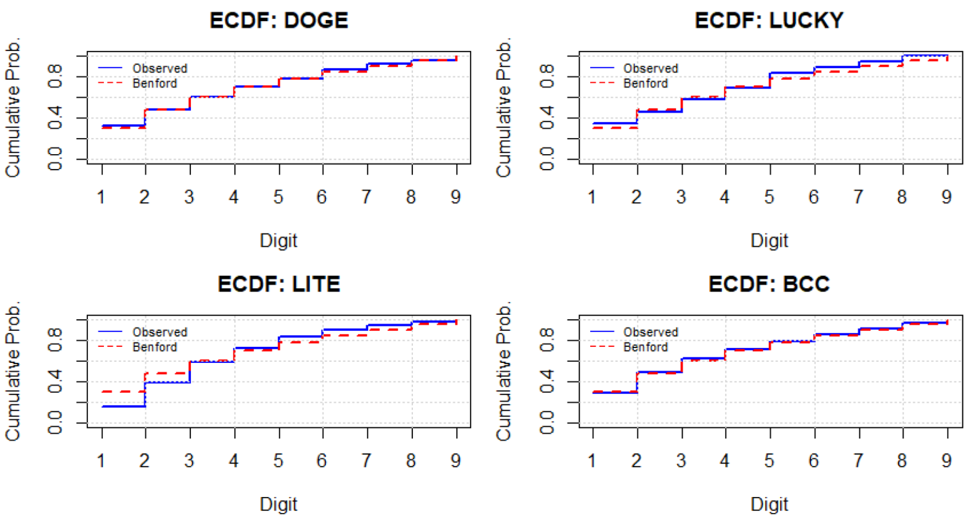

Figure 8. The empirical cumulative distribution function of Dogecoin, Luckycoin, Litecoin and Bitconnect's second digit of the daily transactional volumes

4.3. Volatility analysis

Beyond first-order returns, we examine the structural integrity of market risk through the lens of volume volatility. By applying Benford's Law to absolute returns as a proxy for dispersion, we isolate anomalies, revealing patterns of artificial smoothing that traditional volume metrics fail to capture.

The results from Table 4 reveal a consistent degradation in conformity when moving from the first to the second digit across all cryptocurrencies. While digit 1 distributions generally show "Acceptable" or "Marginal" conformity, digit 2 distributions across Dogecoin, Luckycoin, Litecoin and Bitconnect are universally classified as "Nonconformity". This suggests that while the macro-scale of volume dispersion (digit 1) follows natural logarithmic expectations, the micro-scale (digit 2) exhibits significant structural distortion. Notably, Luckycoin exhibits the strongest adherence to Benford's Law in its first-order volatility (digit 1), with an "Acceptable conformity" rating, a low Chi-square of 6.36, and the lowest MAD (0.00876) in the set. However, the transition to digit 2 shows a sharp increase in the K-S statistic (0.11968), exceeding its critical value of 0.047. Litecoin demonstrates a similar "Acceptable" status for digit 1 but shows the highest Chi-square value for digit 2 (413.35), indicating extreme variance in its second-digit distribution compared to theoretical expectations. Dogecoin shows "Marginal conformity" at the first digit, while Bitconnect maintains "Acceptable" status. Both, however, fail the K-S test at the second digit, with Bitconnect reaching a K-S value of 0.13239 against a 0.047 threshold. The widespread non-conformity in the second digit of volatility indicates that the "noise" or micro-fluctuations in transaction volumes are not occurring organically. High Kuiper and Cramér-von Mises values, particularly in Litecoin and Dogecoin, suggest that volatility profiles may be influenced by automated trading systems or liquidity injections designed to maintain specific volume profiles, thereby "smoothing" the natural dispersion of market risk.

Table 4. Chi-square, MAD, K-S, A-D, Kuiper and Cramer-von-Mises tests of the first two digits distributions of the Dogecoin, Luckycoin, Litecoin and Bitconnect volume absolute returns, analyzed in conformity to the Benford law distribution

	Chi-square	p-value	MAD	MAD conformity	K-S	K-S critical value	A-D	Watson*	Kuiper
DOGE_volatility (Digit 1)	48.01	0.0241	0.0130	Marginal conformity	0.0506	0.024	0.0238	0.3449	0.0390
DOGE_volatility (Digit 2)	384.19	0.3141	0.0239	Nonconformity	0.1196	0.024	0.0238	0.2909	0.1197
LUCKY_volatility (Digit 1)	6.36	0.6099	0.0088	Acceptable conformity	0.0254	0.047	0.0067	0.0908	0.0387
LUCKY_volatility (Digit 2)	83.32	0.1704	0.0243	Nonconformity	0.1196	0.047	0.0067	0.0953	0.1197
LITE_volatility (Digit 1)	21.69	0.0892	0.0083	Acceptable conformity	0.0373	0.024	–0.0181	0.2947	0.0280
LITE_volatility (Digit 2)	413.35	0.0494	0.0245	Nonconformity	0.1196	0.024	–0.0181	0.3270	0.1197
BCC_volatility (Digit 1)	8.75	0.0931	0.0119	Acceptable conformity	0.0295	0.034	–0.0025	0.2170	0.0510
BCC_volatility (Digit 2)	96.39	0.0710	0.0268	Nonconformity	0.1323	0.034	–0.0025	0.2132	0.0861

Note: *We employ Watson's U2 statistic, a rotation-invariant modification of the Cramer-von Mises test, to assess goodness-of-fit.

5. Discussions

Litecoin was inaugurated in 2011, reaching a peak daily trading volume of 17.9 billion dollars; Dogecoin, launched in 2013, recorded a maximum daily volume of 69.4 billion dollars, while Luckycoin, introduced in 2022, reached a total traded volume of 1.6 million dollars. Litecoin, Luckycoin, and Dogecoin were selected for this longitudinal analysis due to the absence of fraudulent reports or illicit activities. Conversely, Bitconnect—originally launched in 2016 and identified as a major Ponzi scheme until its 2018 cessation and subsequent pecuniary collapse—was selected as a representative case of documented fraudulent activity.

The fundamental motivation behind the research we present in this article is to test the suitability of a well-established method for identifying anomalous behavior in cryptocurrency transactions using Benford's Law compliance testing. Data includes daily trading volumes for Litecoin, Dogecoin, Luckycoin and Bitconnect over three time periods: 2017–2024 (Litecoin and Dogecoin), 2022–2024 (Luckycoin) and 2017–2018 (Bitconnect). When testing compliance with Benford law, we applied the Chi-square test, the MAD test, the Kolmogorov-Smirnov, Anderson-Darling, Kuiper and Cramér-von Mises tests. The tested hypothesis presumes that the anomalous cryptocurrency activity, related to unnormal volume trading, can be identified using conformity with the Benford distribution.

The results of the chi2 and MAD tests partially corroborate our alternative hypothesis—that anomalous cryptocurrency trading volumes can be identified through nonconformity with Benford's Law. These metrics indicated nonconformity for Luckycoin, Litecoin, and Bitconnect, while Dogecoin exhibited acceptable conformity. These findings diverge from prior results in Vičič and Tošić (2022), where Dogecoin was found to be nonconformant. As previously established, deviations from Benford's Law may stem from four distinct factors, including the risk of a Type I error (false-positive nonconformity).

To enhance the accuracy of our inferences, we extended the analysis to include the Kolmogorov-Smirnov and Anderson-Darling tests, which yielded results that strongly support our hypothesis. Specifically, both the K-S and A-D tests indicate that the daily trading volumes of cryptocurrencies without reported spurious activity (Doge, Lucky, and Lite) conform to Benford's Law, whereas the daily volume of Bitconnect demonstrates significant nonconformity. These methods validate the utility of Benford-based distribution testing in detecting anomalous market activity.

In the case of Litecoin, the digit 2 emerges as the most frequent leading digit, resulting in statistical nonconformity. During two critical intervals—December 2017 and the second quarter of 2021—Litecoin experienced substantial price surges, surpassing the 250 USD threshold and peaking at approximately 410 USD before a sharp correction. Such high-volatility price fluctuations inevitably induce atypical transaction volumes, thereby constraining conformity to the Benford distribution. Furthermore, Litecoin's volume was influenced by its accessibility on Coinbase; as investors sought alternatives to Bitcoin or Ethereum, Litecoin became a primary entry point.

Regarding Luckycoin, a more recent asset, the distribution is led by the digit 1, followed by 5. This pattern is attributed to a significant contraction in daily transactional volume starting in August 2023, during which average volumes declined from 500,000 USD to 100,000 USD. This spontaneous shift in volume affected the distributional alignment, likely resulting in a Type I error (false positive) within the chi2 and MAD tests. As noted in Diekmann and Jann (2010), many studies encounter such results, as the mathematical hypothesis of a Benford distribution does not always perfectly coincide with the absence of data manipulation.

The discussion of Bitconnect's results in Table 4 reveals a paradox: while it was a known fraud, its first-digit volatility shows "Acceptable conformity" with a Chi-square of only 8.75. Similar results regarding inconsistent Chi-square were found in Licer et al. (2025) where the accounting anomalies and divergence from Benford were found to have an inconsistent relationship. This suggests that Ponzi schemes often maintain a veneer of macro-organic growth to lure investors. However, the first anomaly indicator appears in the second-digit analysis, where Bitconnect shows a massive K-S statistic of 0.13239—nearly triple its critical threshold—and an extreme MAD of 0.3805. This indicates that while the digit 1 was managed to look like a successful asset, the micro-scale price movements (digit 2) were completely synthetic. When comparing this to Luckycoin, which also shows non-conformity in the second digit and clustering in the ECDF between digits 5–8, a clear parallel emerges. The clustering seen in the Luckycoin ECDF resembles the managed volatility of Bitconnect, where price discovery is replaced by programmatic price-setting to prevent the appearance of a market crash.

Comparing the "Nonconformity" labels for the second digits of Luckycoin and Litecoin against the known-fraud baseline of Bitconnect suggests that these assets share a common structural pathology: the elimination of natural market noise. From a policy perspective, the Bitconnect precedent proves that traditional volume metrics are insufficient for fraud detection, as BCC's first-digit conformity could have been used to argue for its legitimacy, although the Kolmogorov-Smirnov and Anderson-Darling test provide optimistic evidence. Consequently, regulatory frameworks should adopt a "Bitconnect-Standard" for volatility testing; if an emerging asset exhibits the same second-digit breakdown and ECDF clustering seen in known Ponzi schemes, it should trigger immediate anomaly alerts status for liquidity audits. This transition from reactive to proactive forensic oversight is essential for protecting retail participants from assets that mimic the synthetic stability of the Bitconnect era.

To address these limitations, future research should develop hybrid models combining Benford's Law with machine learning to reduce false positives (Badal-Valero et al., 2018). Incorporating random forest or support vector machines can effectively detect illicit accounts, counterfeit tokens, and data anomalies (Baek et al., 2019; Kamišalić et al., 2021; Sayadi et al., 2019). As Shi et al. (2018) noted, "complementary accounting techniques tests should be considered before deciding whether some data is faked or erroneous." These include trend analyses alongside semi-supervised (Goernitz et al., 2013) or unsupervised methods like the HDG-Clustering Algorithm (Tsai & Yen, 2007).

Second, expanding the sample to other manipulative activities (e.g., pump-and-dump, wash trading, spoofing) could reveal distinctive statistical signatures. Longitudinal studies tracking conformity throughout a cryptocurrency's lifecycle could identify early temporal patterns preceding fraud.

Third, researchers should test Benford's or Zipf's laws on anomalous Bitcoin and Ethereum activities (Baek et al., 2019; Gao et al., 2021; Sayadi et al., 2019). Applying Benford's Law to daily transactions helps isolate suspicious operational days. Since "first-digit laws are not universally applicable... other tools are necessary for particular applications" (Tam Cho & Gaines, 2007), alternative methods are required to pinpoint fraud sources, though Benford's Law remains a reliable anomaly indicator (Rauch et al., 2011). Finally, future work can evaluate Zipf's law on daily transaction volumes and examine cross-law correlations (Ausloos et al., 2016; Pietronero et al., 2001).

6. Conclusions

Our research carries several critical implications for regulatory bodies, market participants, and forensic accountants, primarily by highlighting the limitations of traditional Benford's Law conformity testing. While the first-digit analysis of Bitconnect (BCC) showed "Acceptable conformity," its status as a confirmed Ponzi scheme proves that basic Benford tests can be easily bypassed by sophisticated bad actors. Consequently, this study establishes that Benford's Law is not a standalone solution for fraud detection but rather a preliminary diagnostic that must be supplemented by more rigorous, high-dimensional forensic tools.

The "Nonconformity" labels for the second digits of Luckycoin and Litecoin, when measured against the Bitconnect baseline, suggest a common structural pathology: the systematic elimination of natural market noise. However, the "Acceptable" results for LUCKY's first digit—despite known volume drops—warn of Type I errors (false positives), where natural market shocks mimic the fingerprints of manipulation. Therefore, regulatory frameworks must move beyond simple digit-frequency counts. We propose a "Multi-Layered Forensic Protocol" where Benford analysis serves only as an initial "anomaly alert." If a second-digit breakdown or ECDF clustering is detected, it should trigger immediate, mandatory liquidity audits and order-book depth analysis.

The study also highlights that Traditional Ponzi schemes have adapted to cryptocurrency environment, leveraging technological complexity and market opacity to attract unsuspecting investors. For investors and oversight bodies, this research proves that traditional volume metrics and basic Benford tests are insufficient for modern cryptocurrency markets. The transition from reactive oversight to proactive defense requires a "Bitconnect-Standard" that integrates K-S and A-D tests not as final proof, but as indicators of "synthetic stability". Ultimately, protecting retail participants requires a more sophisticated toolkit that can distinguish between organic price discovery, institutional scaling in Litecoin, and the deceptive, programmed profiles that defined the Bitconnect era.

However, several limitations must be remembered. First, while Benford's Law deviation signals potential anomalies, it cannot definitively prove fraudulent activity. False positives may occur due to legitimate market dynamics, as potentially demonstrated by inconsistent Chi-square and MAD results for Litecoin and Luckycoin. The occurrence of Type I errors remains significant concern when applying Benford's Law in practical contexts, necessitating cautious interpretation of results. Second, our analysis focused exclusively on daily trading volumes, while cryptocurrency markets operate continuously and involve multiple transaction types beyond simple trading volumes, including market orders, limit orders, and off-exchange transactions. Third, market volatility and legitimate price surges (as observed with Litecoin during December 2017 and April/May 2021) can generate trading volume patterns that deviate from Benford's distribution without indicating fraud. This underscores importance of contextualizing statistical anomalies within broader market trends and fundamental developments before drawing conclusions about potential manipulation.

References

Arshadi, L., & Jahangir, A. H. (2014). Benford's law behavior of internet traffic. *Journal of Network and Computer Applications*, *40*, 194–205. https://doi.org/10.1016/j.jnca.2013.09.007

Ausloos, M., Castellano, R., & Cerqueti, R. (2016). Regularities and discrepancies of credit default swaps: A data science approach through Benford's law. *Chaos*, *Solitons* & *Fractals*, *90*, 8–17. https://doi.org/10.1016/j.chaos.2016.03.002

Badal-Valero, E., Alvarez-Jareño, A. Ignasi, & Pavía, J. M. (2018). Combining Benford's Law and machine learning to detect money laundering. An actual Spanish court case. *Forensic Science International*, *282*, 24–34. https://doi.org/10.1016/j.forsciint.2017.11.008

Baek, H., Oh, J., Kim, C. Y., & Lee, K. (2019). A model for detecting cryptocurrency transactions with discernible purpose. In *2019 Eleventh International Conference on Ubiquitous and Future Networks* (*ICUFN*) (pp. 713–717). IEEE. https://doi.org/10.1109/ICUFN.2019.8806126

Bartoletti, M., Carta, S., Cimoli, T., & Saia, R. (2020). Dissecting Ponzi schemes on Ethereum: Identification, analysis, and impact. *Future Generation Computer Systems*, *102*, 259–277. https://doi.org/10.1016/J.FUTURE.2019.08.014

Baum, S. C. (2018). *Cryptocurrency fraud*: *A look into the frontier of fraud* [Honors College Theses]. Georgia Southern University.

Benford, F. (1938). The law of anomalous numbers. *Proceedings of the American Philosophical Society*, *78*(4), 551–572.

Berger, A., & Hill, T. P. (2011). A basic theory of Benford's law. *Probability Surveys*, *8*, 1–126. https://doi.org/10.1214/11-PS175

Bertin, M., & Lafouge, T. (2025). Categorization of scientometric data in a Benfordian context. *Quantitative Science Studies*, *6*, 524–545. https://doi.org/10.1162/qss_a_00361

Bhattacharya, S., Xu, D., & Kumar, K. (2011). An ANN-based auditor decision support system using Benford's law. *Decision Support Systems*, *50*, 576–584. https://doi.org/10.1016/j.dss.2010.08.011

Bredl, S., Winker, P., & Kötschau, K. (2012). A statistical approach to detect interviewer falsification of survey data. *Survey Methodology*, *38*, 1–10.

Buntinx, J. (2018). The BitConnect Ponzi scheme has finally collapsed as exit scam becomes evident. *NewsBTC*.

Carol, A., & Douglas, C. (2020). *Corruption and fraud in financial markets*: *Malpractice*, *misconduct and manipulation*. John Wiley & Sons.

Cerqueti, R., & Provenzano, D. (2023). Benford's Law for economic data reliability: The case of tourism flows in Sicily. *Chaos*, *Solitons* & *Fractals*, *173*, Article 113635. https://doi.org/10.1016/j.chaos.2023.113635

Chemin, M., & Mbiekop, F. (2015). Addressing child sex tourism: The Indian case. *European Journal of Political Economy*, *38*, 169–180. https://doi.org/10.1016/j.ejpoleco.2015.02.005

Cleary, R., & Thibodeau, J. C. (2005). Applying digital analysis using Benford's Law to detect fraud: The dangers of type I errors. *Auditing*, *24*, 77–81. https://doi.org/10.2308/aud.2005.24.1.77

Clippe, P., & Ausloos, M. (2012). Benford's law and Theil transform of financial data. *Physica A*: *Statistical Mechanics and its Applications*, *391*, 6556–6567. https://doi.org/10.1016/j.physa.2012.07.063

Coderre, D. (1999). Computer-assisted techniques for fraud detection. *CPA Journal*, *69*(8), 57–59.

Diekmann, A. (2007). Not the first digit! Using Benford's Law to detect fraudulent scientific data. *Journal of Applied Statistics*, *34*, 321–329. https://doi.org/10.1080/02664760601004940

Diekmann, A., & Jann, B. (2010). Benford's law and fraud detection: Facts and legends. *German Economic Review*, *11*, 397–401. https://doi.org/10.1111/j.1468-0475.2010.00510.x

Drake, P. D., & Nigrini, M. J. (2000). Computer assisted analytical procedures using Benford's Law. *Journal of Accounting Education*, *18*, 127–146. https://doi.org/10.1016/S0748-5751(00)00008-7

Druică, E., Oancea, B., & Vâlsan, C. (2018). Benford's law and the limits of digit analysis. *International Journal of Accounting Information Systems*, *31*, 75–82. https://doi.org/10.1016/j.accinf.2018.09.004

Durtschi, C., Hillison, W., & Pacini, C. (2004). The effective use of Benford's law to assist in detecting fraud in accounting data. *Journal of Forensic Accounting*, *5*, 17–43.

Eckhartt, G. M., & Ruxton, G. D. (2023). Investigating and preventing scientific misconduct using Benford's Law. *Research Integrity and Peer Review*, *8*, 1–10. https://doi.org/10.1186/s41073-022-00126-w

Efrem, N. (2021). *Benford's law applied to sale prices on the Swedish housing market* [Thesis]. Stockholms Universitet.

Farrugia, S., Ellul, J., & Azzopardi, G. (2020). Detection of illicit accounts over the Ethereum blockchain. *Expert Systems with Applications*, *150*, Article 113318. https://doi.org/10.1016/j.eswa.2020.113318

Feng, X., Shi, Q., Li, X., Liu, H., & Wang, L. (2024). IDPonzi: An interpretable detection model for identifying smart Ponzi schemes. *Engineering Applications of Artificial Intelligence*, *136*, Article 108868. https://doi.org/10.1016/j.engappai.2024.108868

Gao, B., Wang, H., Xia, P., Wu, S., Zhou, Y., Luo, X., & Tyson, G. (2021). Tracking counterfeit cryptocurrency end-to-end. *ACM SIGMETRICS Performance Evaluation Review*, *49*(1), 33–34. https://doi.org/10.1145/3543516.3456282

Giles, D. E. (2007). Benford's law and naturally occurring prices in certain eBay auctions. *Applied Economics Letters*, *14*, 157–161. https://doi.org/10.1080/13504850500425667

Giudici, G., Milne, A., & Vinogradov, D. (2020). Cryptocurrencies: Market analysis and perspectives. *Journal of Industrial and Business Economics*, *47*, 1–18. https://doi.org/10.1007/s40812-019-00138-6

Goernitz, N., Kloft, M., Rieck, K., & Brefeld, U. (2013). Toward supervised anomaly detection. *Journal of Artificial Intelligence Research*, *46*, 235–262. https://doi.org/10.1613/jair.3623

Goldstein, M., & Uchida, S. (2016). A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. *PLoS ONE*, *11*, Article e0152173. https://doi.org/10.1371/journal.pone.0152173

Grigorescu, P.-C., & Amza, A. (2025). Cryptocurrency trading pairs and Benford's law: Investigating market irregularities. *Proceedings of the International Conference on Business Excellence*, *19*, 506–513. https://doi.org/10.2478/picbe-2025-0041

Hassler, U., & Hosseinkouchack, M. (2019). Testing the Newcomb-Benford Law: Experimental evidence. *Applied Economics Letters*, *26*, 1762–1769. https://doi.org/10.1080/13504851.2019.1597248

Holz, C. A. (2014). The quality of China's GDP statistics. *China Economic Review*, *30*, 309–338. https://doi.org/10.1016/j.chieco.2014.06.009

Ivan, L., & Bădele, C. S. (2021). Cryptocurrencies–The modality of payment of the future. Risks and vulnerabilities. *The Journal Contemporary Economy*, *6*(4), 130–141.

Jawabreh, O., Bader, A., Saleh, M., & Alrabie, A. M. A. (2018). Fraud inference investigation within tourism sector in Jordan. *Journal of Economic & Management Perspectives*, *12*, 5–20.

Kamišalić, A., Kramberger, R., & Fister, I. (2021). Synergy of blockchain technology and data mining techniques for anomaly detection. *Applied Sciences*, *11*, Article 7987. https://doi.org/10.3390/app11177987

Kauko, K. (2024). How to detect what drives deviations from Benford's law? An application to bank deposit data. *Empirical Economics*, *67*, 1045–1061. https://doi.org/10.1007/s00181-024-02576-1

Keller, G., & Warrack, B. (2003). *Statistics for management and economics*. Thomson/Brooks/Cole.

Kenny, D. A. (2024). *Measuring model fit*. http://davidakenny.net/cm/fit.htm

Kharpal, A. (2018, March 9). Mysterious cryptocurrency scammers ran off with more than $2 million after ditching their investors. *CNBC*. http://www.cnbc.com/2018/03/09/cryptocurrency-scammers-of-giza-make-off-with-2-million-after-ico.html

Kolar, I., & Horvat, R. (2026). Benford's Law as an investigative tool: Application to the financial statements of Slovenian micro and small enterprises and sole proprietors. *Revija za kriminalistiko in kriminologijo*, *77*.

Kolias, P. (2022). Applying Benford's law to COVID-19 data: The case of the European Union. *Journal of Public Health*, *44*, e221–e226. https://doi.org/10.1093/pubmed/fdac005

Leemis, L. M., Schmeiser, B. W., & Evans, D. L. (2000). Survival distributions satisfying Benford's Law. *The American Statistician*, *54*(4), 236–241. https://doi.org/10.2307/2685773

Levine, M. (2017). SEC halts a silly Initial Coin Offering. *Bloomberg*. https://www.bloomberg.com/opinion/articles/2017-12-05/sec-halts-a-silly-initial-coin-offering

Licer, A., Cano-rodríguez, M., & Nú, M. (2025). Divergence from Benford's law fails to measure financial statement accuracy. *International Journal of Accounting Information Systems*, *56*, Article 100745. https://doi.org/10.1016/j.accinf.2025.100745

Marsaglia, G., & Marsaglia, J. (2004). Evaluating the Anderson-Darling distribution. *Journal of Statistical Software*, *9*(2), 1–5. https://doi.org/10.18637/jss.v009.i02

Martineau, P. (2018, January 23). Inside the group chats where people pump and dump cryptocurrency. *Future*. https://theoutline.com/post/3074/inside-the-group-chats-where-people-pump-and-dump-cryptocurrency

Matakovic, H. (2021). Tourism data in Croatia assessed by Benford's Law. *Journal of Public Administration, Finance and Law*, *19*, 166–184. https://doi.org/10.47743/jopafl-2021-19-13

Michalski, T., & Stoltz, G. (2013). Do countries falsify economic data strategically? Some evidence that they might. *The Review of Economics and Statistics*, *95*(2), 591–616. https://doi.org/10.1162/REST_a_00274

Mir, T. A., & Ausloos, M. (2018). Benford's law: A "sleeping beauty" sleeping in the dirty pages of logarithmic tables. *Journal of the Association for Information Science and Technology*, *69*, 349–358. https://doi.org/10.1002/asi.23845

Neves, G. A., Nunes, C. S., & Fernandes, P. O. (2021). *Application of Benford's Law to the tourism demand: The case of the Island of Sal, Cape Verde*. Springer International Publishing. https://doi.org/10.1007/978-3-030-91885-9_43

Newcomb, S. (1881). Note on the frequency of use of the different digits in natural numbers. *American Journal of Mathematics*, *4*(1), 39–40. https://doi.org/10.2307/2369148

Nica, O., Piotrowska, K., & Schenk-Hoppé, K. R. (2017). *Cryptocurrencies*: *Economic benefits and risks*. SSRN. https://doi.org/10.2139/ssrn.3059856

Nigrini, M. J., Wells, J. T., Almeida, C. S. de, et al. (2012). *Benford's Law*: *Applications for forensic accounting*, *auditing*, *and fraud detection*. Wiley. https://doi.org/10.1002/9781119203094

Nye, J., & Moul, C. (2007). The political economy of numbers: On the application of Benford's Law to international macroeconomic statistics. *The BE Journal of Macroeconomics*, *7*(1). https://doi.org/10.2202/1935-1690.1449

Osborne, C. (2018, February 13). LoopX pulls exit scam, walks away with $4.5m in investor cryptocurrency. *ZDnet*. https://www.zdnet.com/article/loopx-pulls-exit-scam-walks-away-with-4-5m-in-investor-funds/

Pietronero, L., Tosatti, E., Tosatti, V., & Vespignani, A. (2001). Explaining the uneven distribution of numbers in nature: The laws of Benford and Zipf. *Physica A*: *Statistical Mechanics and its Applications*, *293*(1-2), 297–304. https://doi.org/10.1016/S0378-4371(00)00633-6

Prasad, N. R., Almanza-Garcia, S., & Lu, T. T. (2009). Anomaly detection: A survey. *Computers*, *Materials*, *& Continua*, *14*, 1–22. https://doi.org/10.3970/cmc.2009.014.001

Sambridge, M., Tkalčić, H., & Jackson, A. (2010). Benford's law in the natural sciences. *Geophysical Research Letters*, *37*(22), L22301. https://doi.org/10.1029/2010GL044830

Sarkar, B. P. (1973). An observation on the significant digits of the binomial coefficients and factorials. *Sankhyā*: *The Indian Journal of Statistics*, *Series B*, *35*, 363–364.

Sayadi, S., Ben Rejeb, S., & Choukair, Z. (2019). Anomaly detection model over blockchain electronic transactions. In *2019 15th International Wireless Communications* & *Mobile Computing Conference* (*IWCMC*) (pp. 895–900). IEEE. https://doi.org/10.1109/IWCMC.2019.8766765

Shi, J., Ausloos, M., & Zhu, T. (2018). Benford's law first significant digit and distribution distances for testing the reliability of financial reports in developing countries. *Physica A*: *Statistical Mechanics and its Applications*, *492*, 878–888. https://doi.org/10.1016/j.physa.2017.11.017

Shobhit, S. (2018). $9 Million lost each day in cryptocurrency scams. *Investopedia*. https://www.investopedia.com/news/beware-9m-are-lost-each-day-crypto-scams/

Singleton, T. W. (2011). IT audit basics: Understanding and applying Benford's Law. *Isaca Journal*, *3*.

Slosar, D. J. (2026). Analysis of Benford's Law conformity with Web of Science citations of documents. *Acta Informatica Pragensia*, *15*, 22–35. https://doi.org/10.18267/j.aip.281

Stoerk, T. (2016). Statistical corruption in Beijing's air quality data has likely ended in 2012. *Atmospheric Environment*, *127*, 365–371. https://doi.org/10.1016/j.atmosenv.2015.12.055

Gorard, S. (2013). Revisiting a 90-Year-Old debate: The advantages of the mean deviation. *British Journal of Educational Studies*, *53*, 417–430. https://doi.org/10.1111/j.1467-8527.2005.00304.x

Tam Cho, W. K., & Gaines, B. J. (2007). Breaking the (Benford) Law: Statistical fraud detection in campaign finance. *The American Statistician*, *61*(3), 218–223. https://doi.org/10.1198/000313007X223496

Tsai, C.-F., & Yen, C.-C. (2007). Unsupervised anomaly detection using HDG-Clustering algorithm. in M. Ishikawa, K. Doya, H. Miyamoto, & T. Yamakawa (Eds.), *Lecture notes in computer science*: *Vol. 4985*. *Neural information processing*. *ICONIP 2007* (pp. 356–365). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-69162-4_37

Vičič, J., & Tošić, A. (2022). Application of Benford's Law on cryptocurrencies. *Journal of Theoretical and Applied Electronic Commerce Research*, *17*, 313–326. https://doi.org/10.3390/jtaer17010016

Wallace, W. A. (2002). Assessing the quality of data used for benchmarking and decision-making. *The Journal of Government Financial Management*, *51*(3), 16–22.

Wlodarski, J. (1971). Fibonacci an Luca numbers tend to obey Benford's Law. *The Fibonacci Quarterly*, *9*, 87–88. https://doi.org/10.1080/00150517.1971.12431041

Wong, S. C. Y. (2010). *Testing Benford's Law with the first two significant digits* [MSc Thesis, University of Victoria].

Zuckoff, M. (2006). *Ponzi's scheme*: *The true story of a financial legend*. Random House Incorporated.