

To the Moon: A History of Bitcoin Price Manipulation

Timothy F. Peterson, CFA, CAIA*

“How easy it is to make people believe a lie, and how hard it is to undo that work again!”
—Mark Twain, *Autobiography*, Volume 2

Bitcoin’s coming of age in 2017 sparked worldwide interest in the first successful digital currency. The increase of new and uninformed investors into the marketplace has been accompanied by an increase in the number of scams, frauds, and stories of retail investors who lose their money to shady ventures.

This article strives to educate and inform current and potential bitcoin investors as to the most common bitcoin price manipulation techniques and how they can be identified. Benford’s law serves as the methodology for this endeavor. Data is sourced from coinmetrics.io (prices, transactions, and active addresses) and glassnode.com (non-zero balance addresses) and is freely available to download. Anecdotal evidence of bitcoin price manipulation has been carefully selected from sources that have credibility. The principal aim is to raise the level of awareness such that future illicit behavior is more easily identified and mitigated, either through market forces or regulatory oversight.

Objectives

There are three objectives in producing this research:

1. Educate investors, academics, regulators, and journalists about the nature of bitcoin’s price history to dispel the prevalent belief that bitcoin is primarily driven by speculative mania. This document serves as a narrative record of three highly suspect periods in bitcoin’s price history. We do not delve into the fundamentals of why bitcoin has value here.¹ However it is important to state that bitcoin is neither a Ponzi scheme nor greater fool investment. Refutations of Ponzi scheme and greater fool attacks, along with discussions on why bitcoin has value, can be found at Grinberg (2011), Velde (2013), Alabi (2017), Putnam *et al.* (2018), Peterson (2018), and Andolfatto *et al.* (2019).
2. Draw attention to the consequences of a flawed price record:
 - a. Prospective investors struggle to value bitcoin, but some valuation models have emerged. However, any valuation model that relies on the full price history of bitcoin is flawed, especially given the severity of the effects of manipulation on that price history. These periods of manipulation must be recognized and addressed in any viable model.
 - b. Bitcoin’s reported volatility is artificially high. Large upswings contain elements of speculative mania but were triggered by fraud. Severe crashes are not indicative of investors fleeing bitcoin but are instead corrections to sustainable levels of buyer-seller equilibrium. Absent manipulation, bitcoin’s volatility would be lower and therefore its price would be higher.
 - c. The risk associated with the lack of regulation is heavily underestimated.
3. Motivate market participants to recognize manipulation and, where possible, correct with market intervention (e.g., shorting) or regulatory intervention. An educated, vigilant market is healthy and efficient.

¹ Given the title, the author wishes to state the intention behind this research. This research is not meant to disparage bitcoin or its users. The author explicitly opposes any effort to use or characterize this research in a way that would hinder or prohibit bitcoin’s use, growth, or development for lawful purposes. Bitcoin has several economic uses that the author believes have merit to at least a subset of the global economy.

Price Manipulation: A Primer

There are dozens of asset price manipulation techniques. While these have undoubtedly been used in the cryptocurrency market, they have been used in the equity and commodity futures markets for centuries. This review will help familiarize the reader with some of the common practices.

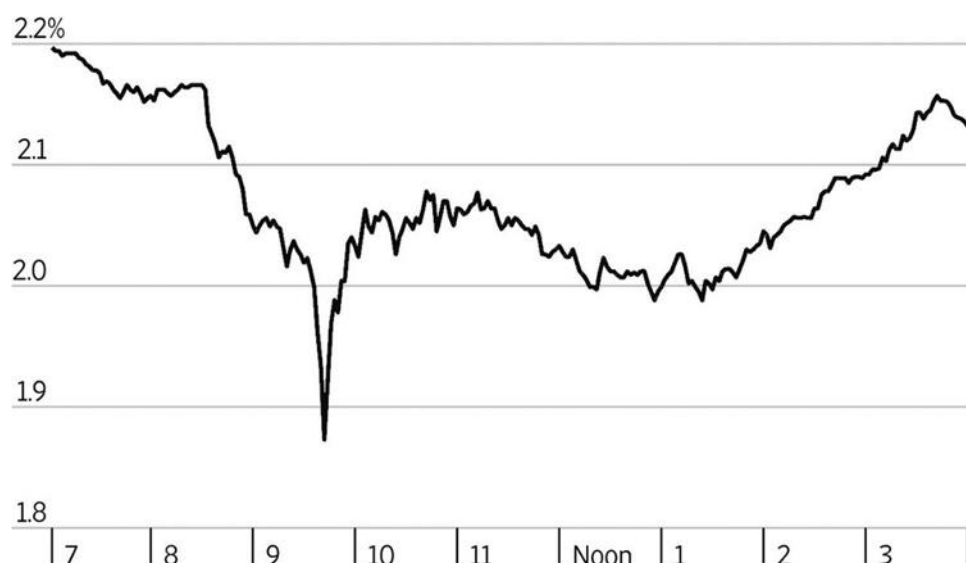
Spoofing: Posting large numbers of limit orders—orders with a specified execution price that is away from current market price—on one side of the order book to make other market participants believe that there is pressure to sell or to buy the asset. There is typically no intention to trade on the part of the spoofer. The orders create the illusion that the demand (or supply, as the case may be) of the asset in question exceeds that which exists. Unwitting market participants then act on the false information, driving the price up or down. Example: Mangan (2018) and Robinson (2020) detail JPMorgan’s manipulation of the silver futures market from 2010 through 2011 (Figure 1) using spoofing.

Figure 1: Effect of JPMorgan’s Alleged Spoofing on the Silver to Gold Ratio



Wash Trading: A single actor sells and repurchases the same or substantially the same security for the purpose of generating activity and increasing the price. An “actor” may involve multiple accounts or affiliate entities, but the transaction itself has no economic value. With a wash trade, the effect of the sale and purchase are offsetting (hence “washed” out) but the price record of the transaction remains a part of the public record. Thus, it is typically the case that the result of a wash trade is misleading information about market price. Example: Zero Hedge (2015) showed how wash trading played a role in the exceptionally large decline in yields on October 15, 2014 (Figure 2).

Figure 2: Crash in 10-year Treasury Note Yields on October 15, 2014



Painting the Tape: Painting the tape attempts to indirectly influence price by manipulating volume. The “tape” references the historical record (ticker tape) of price and volume in the traded asset. The actor engages in computerized or high-frequency transactions among accounts intended for that purpose, or among accounts of co-conspirators. In other cases, the reported volume itself may simply be false.² Large volume skews volume-weighted technical metrics and induces traders to act (usually buy) on that information. Example: In a brazen example, a Moscow State University student built a small business specifically to manipulate volumes of newly issued cryptocurrencies. This business allowed the new coins to meet minimum volume requirements for listing on exchanges, giving the opportunity for greater distribution to an unsuspecting marketplace. The firm, Gotbit, charged \$15,000 for its services and advertised openly, even telling investigative journalists “The business is not entirely ethical,” (Baydakova, 2019).

In a subsequent section, the application of these techniques to bitcoin are discussed in more detail, as studied in Monamo *et al.* (2016), Gandal *et al.* (2018), Chen *et al.* (2019), Hougan *et al.* (2019), and Griffin *et al.* (2020).

Data and Methodology

Data is sourced from coinmetrics.io (prices, transactions, and active addresses) and glassnode.com (non-zero balance addresses). It consists solely of date and associated daily closing price for bitcoin.

Benford’s Law

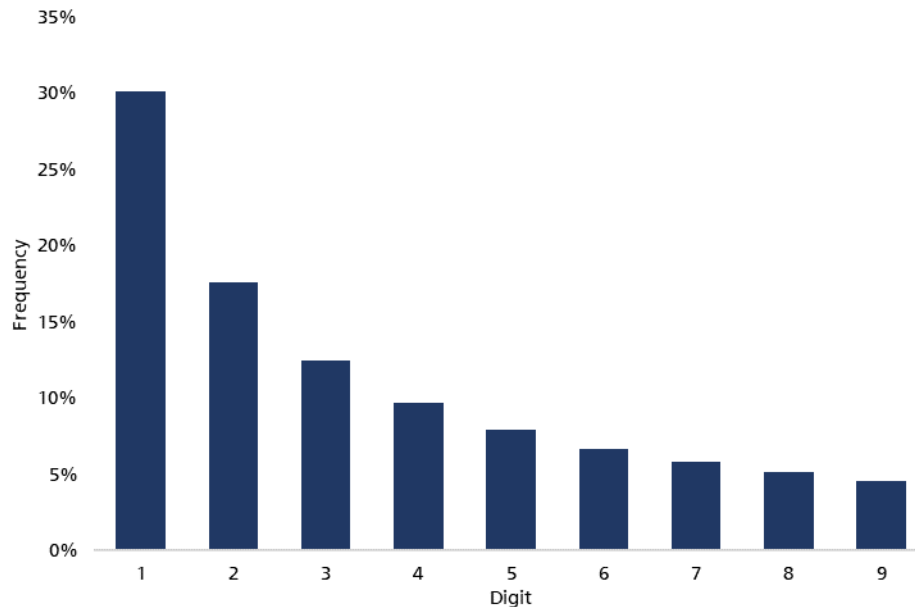
Benford’s law is an observation about the frequency distribution of leading digits in many real-life sets of numerical data. The law states that in many naturally occurring collections of numbers, the leading significant digit is likely to be small (Benford, 1938). Specifically, the number 1 appears as the leading significant digit about 30% of the time, while 9 appears as the leading significant digit less than 5% of the time. Benford’s law also makes predictions about the distribution of second digits, third digits, digit combinations, and so on.

A Benford distribution resembles a Pareto distribution (Figure 3). Deviations from this distribution indicate an anomaly, and typically that anomaly is caused by some type of fraud. Application of Benford’s law to fraud detection dates to at least Varian (1972) as a test of validity of scientific data. It has been used to assess reported earnings (Carslaw, 1988; Thomas 1989), tax compliance (Nigrini, 1996), and auditing (Durtschi *et al.*, 2004). Grammatikos *et al.* (2020) lists several advantages to Benford’s law in a study that related to distressed institutions manipulating data to conceal financial

² Painting the tape is common in bitcoin and is apparent by the evidence of specific price formations. Cryptocurrency traders call these patterns “Barts” because the chart looks like the silhouette of Bart Simpson’s head. Leverage and liquidity play a role as well (Gheorghe, 2019).

difficulties. As demonstrated, this context is directly applicable to the behavior of cryptocurrency exchanges that have been hacked.

Figure 3: Benford Distribution for the First Digit



Benford analysis has limitations. The dataset must be large in order to establish statistical significance. The generation of the numerical dataset cannot be constructed, that is, it must be unrestricted by maximums or minimums and not the result of assignment. For example, certain psychological price fixings (\$1.99) will not obey Benford's law. However, numbers that result from mathematical algorithms (e.g., $\text{quantity} \times \text{price}$) will generally obey Benford's law, as long as the distribution span orders of magnitude (1, 10, 100). Values within an order of magnitude are less likely to adhere to the law; however, a second digit test may overcome this limitation.

Quantitative Approach

The methodology employs the first-, second-, and third-digit tests set out in Benford (1938), Durtschi *et al.* (2004), and Stambaugh *et al.* (2012). For bitcoin prices less than \$1.00 leading zeros after the decimal are ignored.

The bitcoin price history dataset was evaluated against the limitations and requirements necessary to apply Benford's law. We forego presentation of the results of this evaluation for brevity's sake; suffice it to say that bitcoin's daily price history spans ten years and has many orders of magnitude.

To ensure there is statistical significance in our distribution results, we require that each bin (0 through 9) in our histogram be populated with at least eight observations. If this condition is not met for the first-digit test, we rely on the second-digit test. If this condition is not met for the second-digit test, we rely on the third-digit test.

A key reason for this approach is that there could be extended periods where the first digit may only be comprised of one or two unique numbers. For example, the S&P 500 started with a "1" or a "2" from 2009 to 2019. First-digit Benford analysis over this time period would be meaningless.

An analysis was conducted for the entire period of daily closing prices from July 2010 through May 2020. Analyses for calendar years 2011–2019 also was conducted (excluding the 2010 and 2020 partial years as having too few observations). Because Benford analysis requires large datasets, it is difficult to narrow down anomalies to a granularity of less than one year.

Empirical Results

Table 1 shows results for those tests where there was a 90% or greater probability of anomalous pricing. Periods where there was less than 90% probability of anomalous pricing are shown with a dash (–). All annual periods were subjected to at least one test.

Position test indicates whether the first-digit, second-digit, or third-digit test was used.

Digit is the digit 0 through 9 where the high z-score was detected.

n_d is the number of observations in the bin where an anomalous result was detected (but not the number of anomalous events). n_d / N gives the observed distribution, whereas the expected distribution is governed by Benford's law.

N is the total number of observations in the test.

z is the z-score for the test.

Conf. is the assumed normal distribution confidence level that an anomalous event occurred during the tested period.

Table 1: Z-Score and Confidence of Anomalous Pricing in Bitcoin

Year	Position test	Digit	n_d	N	z	Conf.
All	1	1	713	3618	6.94	100.0%
All	1	2	503	3618	2.34	99.0%
All	1	6	494	3618	4.44	100.0%
All	1	8	289	3618	1.69	95.5%
2011	2	–	–	–	–	–
2012	2	–	–	–	–	–
2013	2	3	70	365	1.62	94.7%
2014	2	–	–	–	–	–
2015	3	–	–	–	–	–
2016	2	–	–	–	–	–
2017	2	1	136	365	1.64	94.9%
2018	2	–	–	–	–	–
2019	2	1	81	365	2.07	98.2%

Mania vs. Manipulation

A typical reaction to bitcoin's volatile price history is to assign speculative mania as the cause. It could be the case that episodes of frantic and naïve buying are responsible for bitcoin's price appreciation in the periods identified above; we do not doubt it. However, buying a bitcoin leaves a detailed transaction record on bitcoin's immutable blockchain ledger. There is an undisturbed and high-quality record of addresses, amounts, dates, and transaction frequencies. If speculative buying and panic selling are responsible for bitcoin's volatility, we should see corresponding increases in the data recorded on the blockchain.

Daily ratios of price to three fundamental metrics of network size and activity were examined: active addresses, non-zero balance addresses, and transaction counts. These are graphed at Figures 2a, 2b, and 2c. The Iglewicz-Hoaglin (1993) modified z-score was used to identify outliers ($z > 3.5$) with greater than 95% confidence.

Figure 2a: Bitcoin Price to Unique Active Addresses (Detrended), and Corresponding Modified z-score

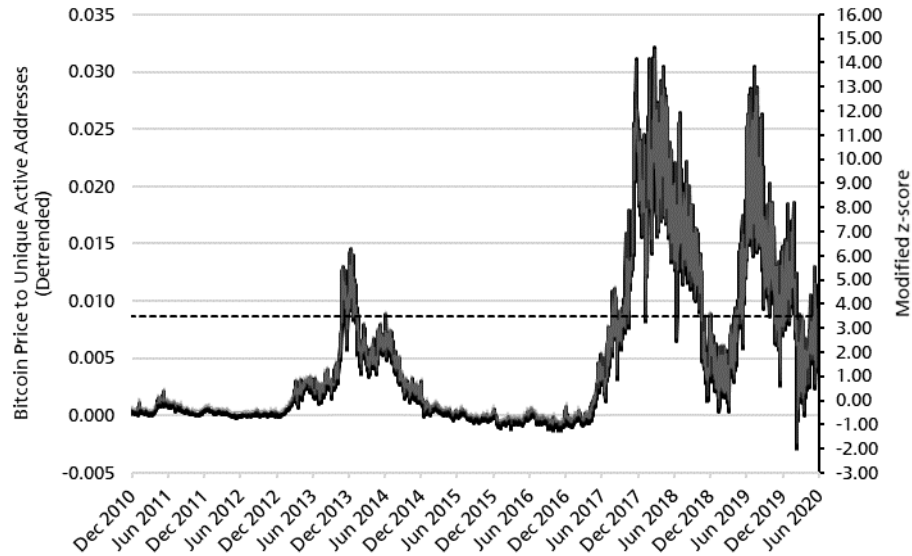


Figure 2b: Bitcoin Price to Non-Zero Balance Addresses (Detrended), and Corresponding Modified z-score

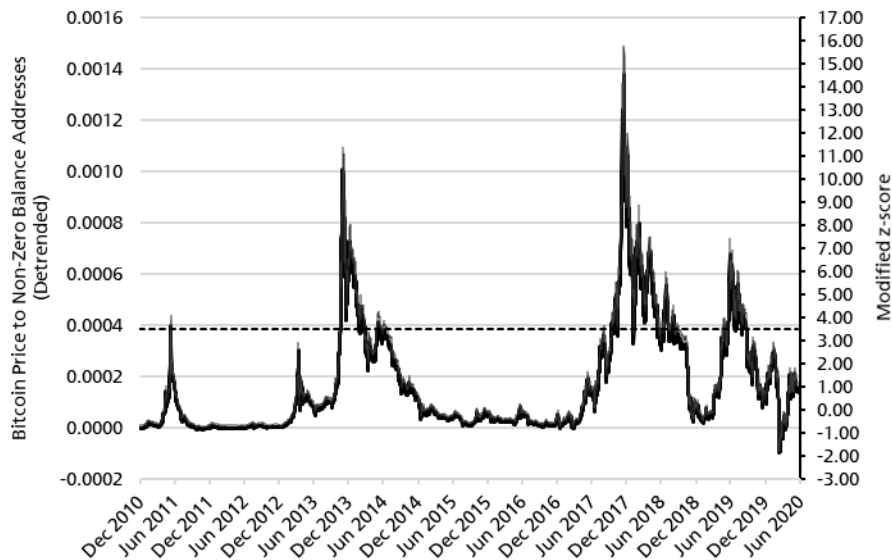
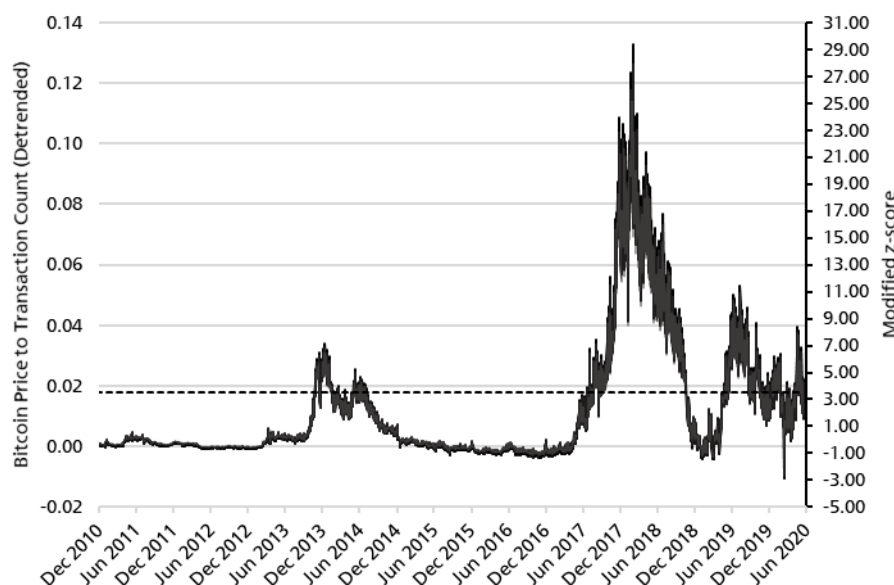


Figure 2c: Bitcoin Price to Transaction Count (Detrended), and Corresponding Modified z-score



Because these ratios measure price-to-user activity, the deviation represents changes in price that cannot be attributed to user activity in general. In other words, whatever speculative mania was present is accounted for with the use of these ratios. What remains is price deviation that is not explained by user activity at large: for a ratio above $z = 3.5$, there is a 95%+ probability that the cause is fraud and manipulation.

Impact on Volatility and Value

Price manipulation causes economic harm beyond the losses incurred by investors, and that damage is not hypothetical. Volatility is a key component of price formation, because investors must discount future values commensurate with the range of possible outcomes.

A cursory review examined bitcoin volatility when anomalous price periods are excluded. Using the data from Figures 2a-2c, the anomalous periods are identified as

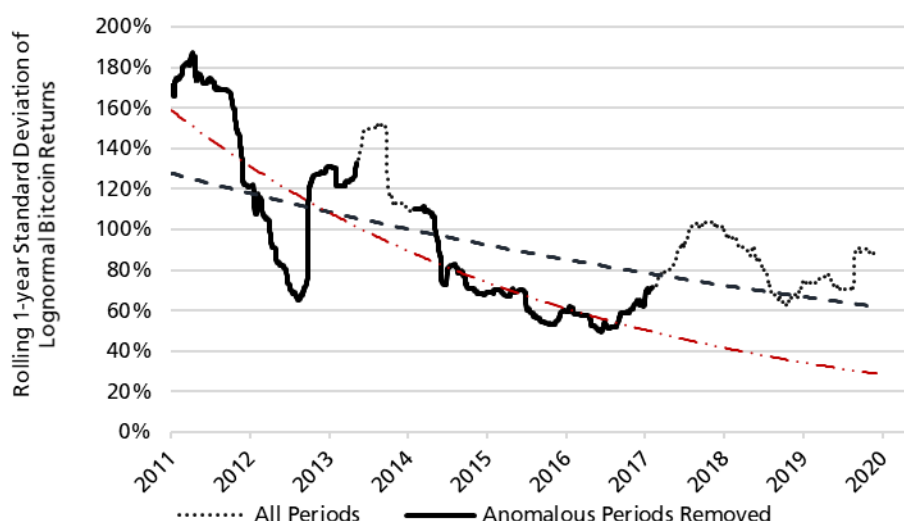
- 23 November 2013–16 February 2014;
- 20 August 2017–19 November 2018; and
- 16 May 2019–24 February 2020.

If we remove the above periods plus an additional 180 days, we can then plot a comparison of trailing standard deviation of lognormal daily returns.

Excluding the anomalous periods, which are believed to be caused by artificially manipulated prices, one can estimate that bitcoin's annualized daily volatility would be approximately 50% of what the historical price record indicates. This percentage implies bitcoin's discount rate has been artificially higher as well, reducing the present value (and presumably price) of bitcoin.

In theory at least, substantial mitigation of bitcoin price manipulation would increase bitcoin's value by about 40%, based on a naïve Capital Asset Pricing Model. As of June 2020, this fact means the estimated market capitalization of bitcoin has been reduced by approximately \$100 billion. Put another way, the expectation of future volatility reduces the present value of bitcoin's market capitalization by \$100 billion. But those expectations are incorporating future instances of price manipulation, which is not a farfetched assumption.

Figure 3: Bitcoin Trailing Annualized Standard Deviation of Returns



It could be that a single actor, or a few actors, could transact in large quantities in such a way as to influence price. In such cases we would expect to see large price movements with little change to address or transaction counts. As we discuss in the next section, this expectation is almost certainly the case for each of the suspect periods.

Past Suspected Bitcoin Price Manipulations

Possibly, Benford analysis can result in a false positive, meaning not all datasets indicated as non-conforming will be fraudulent. However, to those familiar with prior research on bitcoin price manipulation, the aforementioned results are not entirely surprising.

To provide context, we examine some events surrounding bitcoin in 2013, 2017, and 2019. In some cases, the explanation makes it obvious that fraudulent price manipulation occurred. In others, it is less provable, but still convincing.

2013 and Mt. Gox

In early 2014, a cryptocurrency exchange located in Japan—Mt. Gox—suspended operations, filed for bankruptcy protection, and immediately began liquidation proceedings. It disclosed to customers that approximately 850,000 bitcoins were missing and likely stolen, an amount valued at more than \$450 million. At the time, Mt. Gox handled about 70% of all global bitcoin transactions. In April 2015, Tokyo security company WizSec provided evidence that “most or all of the missing bitcoins were stolen straight out of the Mt. Gox hot cryptocurrency wallet over time, beginning in late 2011,” (Nilsson, 2015).

A contemporaneous public blog written by several anonymous Mt. Gox traders documented suspicious activity (Anonymous, 2014) regarding Mt. Gox trading. The bloggers identified two suspicious actors, dubbed “Willy” and “Markus”.

Subsequently Gandal *et al.* (2018) examined a leaked data dump of 18 million matching buy and sell bitcoin transactions which spanned April 2011 to November 2013. Their findings are summarized as follows:

- Markus was active from 14 February 2013 until 27 September 2013. His account was fraudulently credited and, because transactions were duplicated, no legitimate Mt. Gox customer received the currency Markus supposedly paid to acquire these bitcoins. On 33 of the 225 days that the account was active, Markus acquired 335,898 bitcoins (worth around \$76 million).
- Willy was a collection of 49 separate accounts that each rapidly bought exactly 2.5 million USD in sequential order and never sold the acquired bitcoin. Willy became active on 27 September 2013, hours after Markus became permanently inactive. Willy traded on 50 of the 65 days before the data cutoff. Willy acquired 268,132 bitcoins, nominally for around \$112 million.

- On the 82 days that bots were active on Mt. Gox, bitcoin's price rose 79% of the time. On days without such activity, bitcoin's price rose 55% of the time.
 - When Markus was active, the average daily return ranged from +1.9% to +2.9% over four exchanges. On other days, the average return was slightly negative on all four exchanges.
 - Similarly, when Willy was active, that the average daily return ranged from +4.8 to +5.0% on four exchanges. On other days, the average return was slightly negative on all four exchanges.

At trial in Japan, the former Mt. Gox CEO Mark Karpeles confirmed that the exchange itself operated the “Willy” accounts and that the trades were issued automatically (Suberg, 2017).

Using a fundamental metric of network size, Peterson (2018) independently confirmed Gandal's findings using price deviation from fundamental value.

2017 and Tether/Bitfinex

By 2017 it was apparent that anyone could issue a cryptocurrency token. A few realized that one token could be used to bid up the price of another. For example, one way to manipulate bitcoin's price is to issue a relatively worthless new token, and use that token, say Token X, to purchase bitcoin. The problem is that it will take many X tokens to buy enough bitcoin to impact price. Issuing more Token X only devalues Token X further, making it even more difficult to buy bitcoin. However, if Token X were pegged to a fiat currency like the dollar, Token X would not lose value in the short term.

The purported scheme is that investors use dollars to buy stablecoin Token X, meaning Token X is “backed” by dollars 1:1. Essentially a digital dollar, Token X is then used to buy bitcoin. Token X has credibility because it is denominated in the world reserve currency and is in effect a collateralized digital security.

If Exchange X and Token X are affiliated, then Exchange X can issue IOUs to purchase Token X. Token X is then used on Exchange X to bid up the price of bitcoin. Bitcoin is later sold at an inflated price for dollars, which is deposited into Token X's account to retire the IOU, giving the appearance, *ex post facto*, that Token X was backed by dollars all along. These dollars appear as reserves backing Token X, but they are not liabilities of Token X as one would expect, they are fraudulently obtained equity.

Difficulties and Allegations Involving Bitfinex and Tether

Anonymous blogger Bitfinex'd (2017) alleged this scam was the scheme perpetrated by Tether and Bitfinex in response to a hack and theft of bitcoins on the Bitfinex exchange. His allegation is that tether tokens (USD₣) are issued to purchase bitcoin, which are then sold on the open market for dollars. The dollars are diverted to Tether's account to back USD₣ after the fact.³

In 2016, almost 120,000 bitcoin worth around \$78 million had been stolen from Hong Kong-based Bitfinex, one of the most popular cryptocurrency exchanges. Rather than accept the loss, Bitfinex seized 36% of all customer assets, and granted a “token of credit.” This token was a new cryptocurrency it created for the specific purpose of serving as an IOU until assets could be recovered. These tokens could be exchanged for equity in the parent company iFinex or sold on the open market to a willing buyer. Bitfinex encouraged its customers to sell these tokens on the open market.

Shortly thereafter, several other developments unfolded. Cermak (2019) provides a more thorough history but the salient points are summarized here for convenience.

- Bitfinex struggled to maintain its banking relationships. Wells Fargo ceased wire transfers in April 2017, and that same month Bitfinex's Taiwanese banking relationship was terminated (Tether, 2018a). Though Tether was formed in 2014, its connection to Bitfinex was undisclosed and not known until Tether joined a lawsuit against Wells Fargo.
- In August 2017, Bitfinex announced it would no longer service “verification (of asset) requests for U.S. individuals,” citing “ongoing difficulties in providing USD deposit and withdrawals for U.S.

³ For clarity, we refer to the tether token as USD₣ or tether (lowercase) and the issuing company as Tether.

individuals.” In the same announcement, Bitfinex gave its intention to quit the U.S. marketplace within 90 days (Bitfinex, 2017).

- Tether was unable to complete an audit of its reserves backing USD₯ token. In September 2017, Tether announced it had hired Friedman LLP for an historical balance sheet audit. However, by January 2018, Tether announced it had severed its relationship with Friedman, and no audit was ever completed. In June 2018, Tether released a letter from the Law Firm of Freeh, Spokin & Sullivan LLP (FSS) expressing that “FSS is confident that Tether’s unencumbered assets exceed the balance of fully backed USD tether...” (Anonymous, 2018). However, this letter contains several anomalies and deviations from traditional accounting attestations:
 - The letter is marked “Attorney-Client Communication / Work Product — Privileged & Confidential.” Among other things, this disclosure prohibits a prosecutor from taking legal action should any representations in the letter be deemed false or misleading;
 - The letter notes a named partner of FSS as an advisory board member of one of Tether’s banks. This listing is a universal and fundamental violation of independence not tolerated in traditional auditing;
 - The letter explicitly states that “FSS procedures performed are not for the purpose of providing assurance...” Thus, the work product is not intended as an attestation of any kind;
 - The findings cover balances as of June 1, 2018 only, whereas the alleged misconduct occurred throughout 2017; and
 - The letter is undated, unsigned, and contains no address or contact information.

In November 2017, Tether was hacked, netting the hacker approximately \$31 million worth of USD₯. The company responded with a temporary hard fork in an attempt to recover the lost funds, in other words, a variation of the approach Bitfinex used when it was hacked in 2016.

The U.S. Commodity Futures Trading Commission subpoenaed Tether on 6 December 2017. However, this investigation was not publicized until 30 January 2018 (Price *et al.*, 2018). Between 6 December 2017 and 30 January 2018, Tether printed approximately 1.5 billion USD₯. About half of that issuance occurred in the two weeks leading up to January 30th, even though user activity in USD₯ was on a shallow decline. This situation seems inconsistent with the notion that tethers are printed on demand to purchase bitcoin and other cryptocurrencies. After January 2018, USD₯ production ground to a halt (Coin Metrics, 2020).

Over the course of this period, Tether updated its website regarding the reserves backing the USD₯ token:

April 2017: Our reserve holdings are published daily and subject to frequent professional audits. All tethers in circulation always match our reserves (Tether, 2017a).

November 2017: All tethers are pegged at one-to-one with matching fiat currency (e.g., 1 USD₯ = 1 USD) and are backed 100% by actual assets in our reserve account (Tether, 2017b).

March 2018: Tether is a token backed by actual fiat currency assets, including USD, Euros and soon, Japanese Yen. One Tether equals one underlying unit of the currency backing it, e.g., the U.S. Dollar, and is backed 100% by actual assets in the Tether platform’s reserve account (Tether, 2018b).

March 2019: Tether tokens are 100% backed by Tether’s Reserves...If you cause to be issued EURT 100.00, Tether holds reserves valued at €100.00 to back those tether tokens. The composition of the reserves used to back tether tokens is within the sole control and at the sole and absolute discretion of Tether. Tether tokens are backed by Tether’s reserves, including fiat, but tether tokens are not fiat themselves (Tether, 2019).

June 2020: Every tether is always 100% backed by our reserves, which include traditional currency and cash equivalents and, from time to time, may include other assets and receivables from loans made by Tether to third parties, which may include affiliated entities (collectively, “reserves”). Every tether also is 1-to-1 pegged to the dollar, so 1 USD₯ is always valued by Tether at 1 USD (Tether, 2020).

The latest change is notable because it admits that tether tokens are backed by loans from an affiliate, and that the backing reserves are valued internally; this admission was precisely the original allegation made by the cryptocurrency community in 2017. However, by December 2018, Bloomberg had reported it had seen bank statements indicating adequate backing of Tether (Leising, 2018).

The early allegations from 2017 were apparently enough that the U.S. Department of Justice opened a criminal investigation into the matter (Robinson *et al.*, 2018). The status of that investigation is currently unknown.

In April 2019, Tether's general counsel said in an affidavit that its stablecoins are only 74% backed by cash reserves, and it knowingly did not disclose this information to its customers (Wan, 2019).

In a civil suit filed June 2020 (US District Court, 2020), plaintiffs alleged, among other things:

Defendants have executed a sophisticated scheme to fraudulently inflate the price of cryptocommodities, a class of crypto assets that includes bitcoin. Defendants' scheme was wildly effective, causing the price of these cryptocommodities to spike far above their legitimate value in the largest bubble in human history, and ultimately resulting in billions of dollars of damage to innocent cryptocommodity purchasers.

These purchases were made with Defendants' own fraudulently issued crypto asset called "tether" or "USD£"...Tether, the company that created USD£, represented to the market that every USD£ in circulation was backed by a U.S. dollar in Tether's bank account...That was a lie. In reality, Tether issued billions of USD£ to itself with no U.S. dollar backing...Tether hid that fact by "selling" newly issued USD£ to Bitfinex, a crypto exchange that was secretly owned and operated by the same individuals who owned and operated Tether.

Tether issued a vehement denial of the allegations. The suit is pending.

Crypto Capital

Bitfinex suffered a \$850 million loss of access to user funds which were reportedly seized by authorities in four different countries after bank accounts held by its payment processor, Crypto Capital, were frozen in August 2018. In April 2019, the State of New York (2019) sued Bitfinex and Tether "to expose ongoing fraud being carried out" by the two firms. New York claims Bitfinex and Tether were engaging in a cover-up to hide the apparent loss of \$850 million of co-mingled client and corporate funds related to Crypto Capital.

In summary, the lawsuit claimed:

- Bitfinex partnered with Panama-based payment processor Crypto Capital to handle customer withdrawals after struggling to find a reputable bank to work with. Bitfinex commingled client funds through Panama-based payment processor Crypto Capital, meaning the firm mixed funds held on behalf of clients with its own capital.
- In October 2018, Bitfinex began to struggle with client withdrawal requests. Per the NY State Attorney General, this problem was due to the loss or theft of ~\$851 million in funds by Crypto Capital.

Bitfinex responded saying the "court filings were written in bad faith and are riddled with false assertions." Bitfinex claimed the tokens were not lost "but have been, in fact, seized and safeguarded."

In 2021, the suit was settled with Bitfinex paying a \$18.5 million fine and no admission of wrongdoing. Tether and Bitfinex agreed to cease trading activity with New Yorkers and submit quarterly transparency reports. Post settlement, New York Attorney General (NYAG) Letitia James' office said it found that Tether sometimes held no reserves to back its cryptocurrency's dollar peg. The NYAG claimed from mid-2017, the company had no access to banking and misled clients about liquidity issues.⁴ However, Tether posted a message on its website stating, "Contrary to online speculation, after two

⁴ The NYAG statement read, in part, "Bitfinex and Tether recklessly and unlawfully covered-up massive financial losses to keep their scheme going and protect their bottom lines. Tether's claims that its virtual currency was fully backed by U.S. dollars at all times was a

and half years there was no finding that Tether ever issued tethers without backing, or to manipulate crypto prices,” (Browne, 2021).

Manipulation on the Bitfinex Exchange

Griffin *et al.* (2020) asserted that one large player on Bitfinex used USD₯ to purchase large amounts of bitcoin when bitcoin prices were falling and that such purchases followed the printing of USD₯. Such price supporting activities are successful, as Bitcoin prices rise following the periods of intervention.

Critics, including Tether, point out that investors would naturally buy bitcoin when prices were falling, and that at least some buyers would use USD₯ to make the purchase.

Our analysis shows rather convincingly that this situation was not the case. The natural purchase of bitcoin, be it from USD₯ or some other currency, would not manifest substantial deviations in expected price as characterized by Benford’s law. If many buyers bid up bitcoin’s price in a speculative mania (via USD₯ or otherwise), then the metrics recorded on the bitcoin blockchain would bear that out with increased addresses and transaction counts. A transaction-based explanation for bitcoin’s price rise in 2017 is not borne out when price is compared to fundamental statistics of network activity, as we have shown in Figures 2a-2c.

Benford analysis is unable to ascertain the specific cause of fraud or price manipulation, let alone identify perpetrators. Our analysis of 2017 prices cannot confirm specific allegations of fraud, it can only confirm that the price behavior of bitcoin in 2017 was unnatural, with fraudulent manipulation being the most likely explanation.

2019 and PlusToken/Bitfinex II

A report by Bitwise (Hougan *et al.*, 2019) indicated that the practice of painting the tape is widespread throughout cryptocurrency exchanges. Its principle conclusion was that 95% of bitcoin-related exchange volume is fake, with volumes at different price levels being completely manufactured and posted on exchange websites. This volume is known to be false because it is not recorded on the bitcoin blockchain.

The Trade Size Distribution Histograms in the Bitwise study shows a remarkable array of patterns not found in nature. A veritable kaleidoscope of fictitious activity, these histograms show steadily increasing volumes at increasing prices; intentionally repeated patterns; large ranges of prices where no trading occurs at all; and completely consistent and equal trading volumes at all price levels. Da Vinci himself could not have painted the tape better.

PlusToken Ponzi

There are also allegations that a Ponzi scheme known as PlusToken may be responsible for bitcoin’s price run in Summer of 2019. PlusToken was a classic Ponzi scheme that lured unsuspecting victims to invest with promises of high returns and low investments (Harper, 2020).

From January 1–June 30, 2019, bitcoin gained 212% to nearly \$13,000. Shortly thereafter, bitcoin’s price declined until December of that year where it traded around \$7,000. Some operators of the scheme left a note “Sorry we have run” in June 2019 and were arrested by Chinese authorities on June 29th. This period (and into July) corresponds with bitcoin’s price peak for 2019.

Presumably, the scheme involves

1. Selling a worthless token PlusToken to naïve investors for fiat currency;
2. Purchasing bitcoin with PlusToken and bidding up the price; then
3. Selling bitcoin at an inflated price for fiat currency.

If that is in fact the scheme, then this situation appears to be an attempt at money laundering as well as price manipulation.

On July 30th, China’s Ministry of Public Security announced it had arrested all 27 major suspects of the scheme; victims were defrauded of an estimated \$3 billion (Khatri, 2020).

lie. These companies obscured the true risk investors faced and were operated by unlicensed and unregulated individuals and entities dealing in the darkest corners of the financial system.”

Bitfinex II

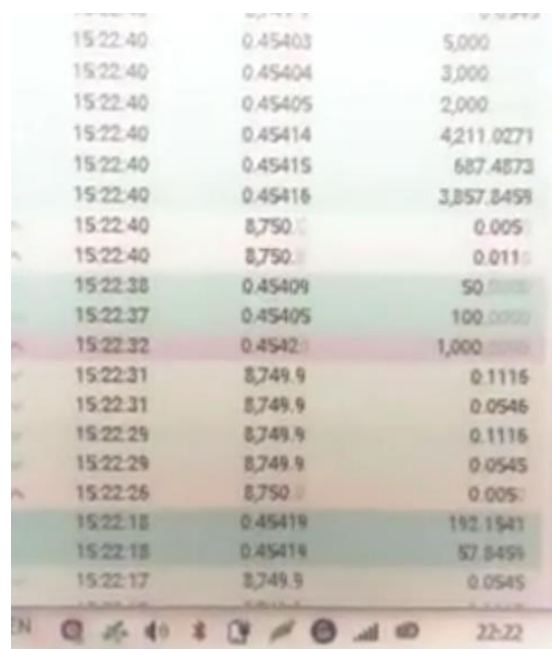
In 2019, a video was posted to YouTube (Anonymous, 2019) purportedly showing—in real time—fraudulent trades being posted to the website at www.bitfinex.com. The video was recorded circa May 29, 2019 and runs 4 minutes 52 seconds.

A screenshot of the video is shown at Figure 4. A transcript is provided also. Using data in the transcription we see that—in 33 seconds—19,656.3535 bitcoin were traded at an average price of \$0.4544. Just 0.4078 bitcoin were traded at the market price of \$8,749.91. The fraudulent trades quickly disappeared from the website, but the trade amounts were included in volume totals. With the market value applied to the falsified trades, the reported volume in that 33-second span was \$172 million rather than about \$4,000. Those figures apply only to the trades in screenshot shown below. This volume manipulation continued throughout the duration of the video.

Further, because these \$0.45 falsified trades occurred on the website and not the blockchain, they either (a) represented trades submitted to Bitfinex and not executed, or (b) software was running on the Bitfinex website that generated the falsified trades, similar to what occurred at Mt. Gox in 2013.

Benford analysis cannot validate any such specifics, only that prices in 2019 are suspected of being manipulated. The PlusToken scheme, along with anecdotal (Gotbit) and forensic evidence of falsified trades and volumes, however, appear to support the hypothesis of price manipulation and not speculative mania.

Figure 4: Bitcoin Trades on the Bitfinex Exchange in 2019 and Transcription



Time	Price	BTC
15:22:40	0.45403	5,000
15:22:40	0.45404	3,000
15:22:40	0.45405	2,000
15:22:40	0.45414	4,211.0271
15:22:40	0.45415	687.4873
15:22:40	0.45416	3,357.8458
15:22:40	8,750.0000	0.005
15:22:40	8,750.0000	0.011
15:22:38	0.45409	50
15:22:37	0.45405	100
15:22:32	0.4542	1,000
15:22:31	8,749.9	0.1116
15:22:31	8,749.9	0.0546
15:22:29	8,749.9	0.1116
15:22:29	8,749.9	0.0545
15:22:26	8,750.0	0.005
15:22:18	0.45419	192.1541
15:22:18	0.45419	57.8459
15:22:17	8,749.9	0.0545

Time	Price	BTC
15:22:40	0.45403	5,000.0000
15:22:40	0.45404	3,000.0000
15:22:40	0.45405	2,000.0000
15:22:40	0.45414	4,211.0271
15:22:40	0.45415	687.4873
15:22:40	0.45416	3,357.8400
15:22:40	8,750.0000	0.0050
15:22:40	8,750.0000	0.0110
15:22:38	0.49490	50.0000
15:22:37	0.49405	100.0000
15:22:32	0.45420	1,000.0000
15:22:31	8,749.9000	0.1116
15:22:31	8,749.9000	0.0546
15:22:29	8,749.9000	0.1116
15:22:29	8,749.9000	0.0545
15:22:26	8,750.0000	0.0050
15:22:18	0.45419	192.1541
15:22:18	0.45419	57.8450
15:22:17	8,749.9000	0.0545

Conclusions

Unmolested prices have been shown to exhibit an expected, natural distribution characterized by Benford's law. Benford's law has been used to identify and investigate financial anomalies and fraud for nearly 30 years. We believe this article is the first application of Benford's law to bitcoin.

Allegations of impropriety regarding bitcoin, especially with respect to cryptocurrency exchanges, are not new. What is unique with this research is that a commonly accepted and independent methodology supports, indirectly at least, previous allegations evidence of price manipulation.

Benford analysis confirmed anomalies in bitcoin prices for 2013, 2017, and 2019. One can say with near 100% confidence that bitcoin's price has been fraudulently manipulated at some point in its lifespan since 2010. One can say with 95%

confidence that bitcoin was manipulated in 2013; 95% confidence that bitcoin was manipulated in 2018; and 98% confidence that bitcoin was manipulated in 2019.

Based on prior research on bitcoin fraud, these manipulative spikes also conform to a distinct behavioral pattern:

1. Spark. Bitcoin is acquired through misappropriation, that often takes the form of a security breach and theft of bitcoin from an exchange.
2. Smoke. Suspicious activity is almost always reported first by the cryptocurrency enthusiasts who post their research on the internet. These amateur sleuths have far more time, resources, and subject matter knowledge than regulators. In at least one case and possible a second, it appears that manipulation was used to recover losses incurred from the theft.
3. Fire. Bitcoin price appreciates at a rate that exceeds the rate of growth in fundamental metrics like address and transaction counts. This excess is indicative of one or few actors manipulating price. The price soars, and interest follows. This situation is evident in searches for “bitcoin” as reported by Google Trends (e.g., Figure 5).
4. Collapse. The timing of each major decline coincides with cessation of suspected fraudulent activity (Figure 6).

Figure 5: Google Trends “bitcoin” for 2015–2018

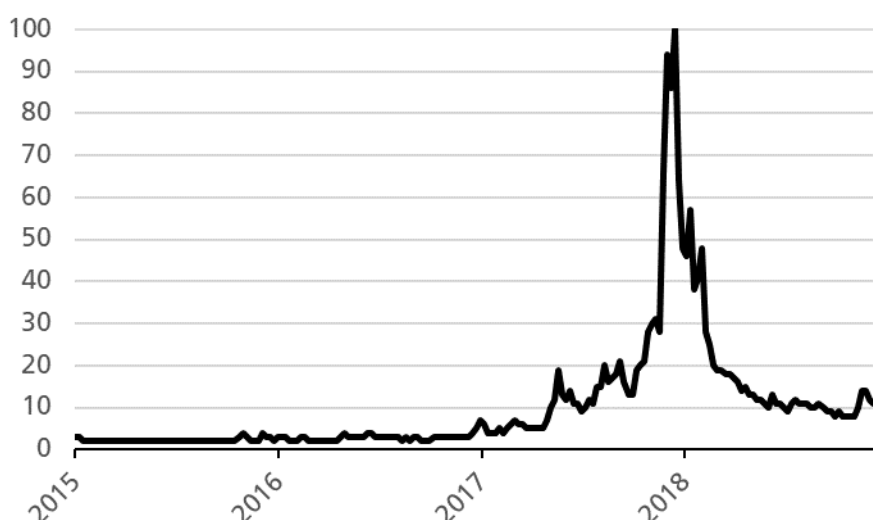
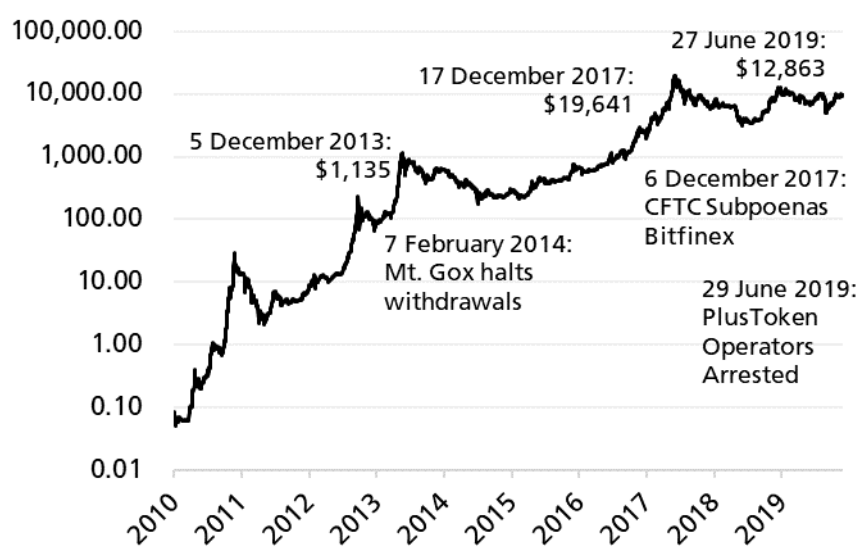


Figure 6: Timing of Bitcoin Price Peaks and Cessation of Suspicious Activity



Impact on Bitcoin Valuation Models

The implications for bitcoin valuation are profound. First and foremost, it means that technical price analysis of bitcoin over the suspect periods is likely meaningless; bitcoin's price did not reflect equally motivated buyers and sellers, and therefore bitcoin's price cannot be indicative of market psychology.

Another conclusion of this research is that even fundamental analysis of bitcoin is problematic. Fundamental analysis typically relies on historical relationships between price and some other metric to ascertain if an asset is overvalued or undervalued. When price has been manipulated, any such comparisons are then skewed, and would likely have a detrimental impact on both the assessment of current value and forecasts of future price.

Thirdly, as we mentioned earlier, increased volatility in bitcoin prices increases the required discount rate and reduces value.

Moving Forward

Most bitcoin holders are retail investors. This investor class is least likely to be aware of price manipulation as a likely cause of exceptional short-term performance. Even seasoned investors are often unwilling to accept that they have at times been duped. Overconfidence bias means that a trader views himself as smart rather than lucky. To accept that you have been fooled means you were wrong not only about your investment choice, but about yourself and your abilities. This admission is more than most people can handle. Anecdotally, we have found that those who have not owned bitcoin are accepting of such findings and those who do own bitcoin engage in various attempts at rationalization to reject them; hence the meaning behind the Mark Twain quote at the beginning of this article. The bright spot is that those that have either held or accumulated bitcoin over time have probably done well, and wisely so.

We can expect cryptocurrency frauds and manipulations to continue into the foreseeable future. There is a perception, perhaps warranted, that bitcoin competes with government fiat currency. Governments, therefore, have no incentive to foster bitcoin adoption by setting up a legal framework to protect its use and users at the expense of their own economic interests. The current approach taken by most governments is to be cautiously permissive while issuing a heavy dose of *caveat emptor* warnings.

Yet even from a practical standpoint, enforcement of bitcoin and cryptocurrency exchanges is difficult at best. Many intentionally choose to operate in multiple jurisdictions with no regulatory oversight and weak consumer protection laws. The operations themselves span multiple countries and transact in multiple currencies through affiliates. They sometimes use cryptocurrencies, perhaps of their own design, that are difficult to trace. The resources necessary for effective regulation, and the associated costs, quickly start to exceed the benefits.

Bitcoin is an apolitical token, an "inanimate" digital object that polarizes like the 1s and 0s it is comprised of. Bitcoin is still largely identified with illicit activity in the eyes of many. Education and awareness are therefore crucial if it is to continue

to grow. If investors, regulators, and journalists are armed with the knowledge of how to spot these schemes, then they can better combat against them.

References

- Alabi, Ken. (2017). Digital blockchain networks appear to be following Metcalfe's Law. *Electronic Commerce Research and Applications*, 24, July–August, 23–29.
- Andolfatto, David, and A. Spewak. (2019). Whither the Price of Bitcoin? *Economic Synopses*, No. 1.
- Anonymous. (2014, May 26). Proof of massive fraudulent trading activity at Mt. Gox, and how it has affected the price of bitcoin. *The Willy Report*, willyreport.wordpress.com/2014/05/25/the-willy-report-proof-of-massive-fraudulent-trading-activity-at-mt-gox-and-how-it-has-affected-the-price-of-bitcoin/.
- —. (2018, June 15) Letter from Freeh, Sporkin & Sullivan LLP re: Tether reserves as of June 1, 2018. <https://tether.to/wp-content/uploads/2018/06/FSS1JUN18-Account-Snapshot-Statement-final-15JUN18.pdf>.
- —. (2019, July 3). Thousands of bitcoins being traded on Bitfinex for 45 cents each. *Bitfinexed*, www.youtube.com/watch?v=PkT0ZzKiL_M.
- Baydakova, Anna. (2019, July 23). For \$15K, he'll fake your exchange volume – You'll get on CoinMarketCap. *CoinDesk*, CoinDesk, www.coindesk.com/for-15k-hell-fake-your-exchange-volume-youll-get-on-coinmarketcap.
- Benford, Frank. (1938). The Law of Anomalous Numbers. *Proceedings of the American Philosophical Society*, 78, 4, 551–572.
- Bitfinex. (2017, August 12). Service changes for U.S. customers (Amended as of August 12, 2017). *Bitfinex*, www.bitfinex.com/posts/216/review.
- Bitfinex'd. (2018, February 13). Bitfinex never 'repaid' their tokens, Bitfinex started a ponzi scheme. *Medium*, medium.com/@bitfinexed/bitfinex-never-repaid-their-tokens-bitfinex-started-a-ponzi-scheme-86a9291add29.
- Browne, Ryan. (2021, February 23). "Cryptocurrency Firms Tether and Bitfinex Agree to Pay \$18.5 Million Fine to End New York Probe." *CNBC*, www.cnn.com/2021/02/23/tether-bitfinex-reach-settlement-with-new-york-attorney-general.html.
- Carslaw, C.A.P.N. (1988). Anomalies in Income Numbers: Evidence of Goal Oriented Behavior. *The Accounting Review*, 63, 2, 321–327.
- Chen, Weili, J. Wu, *et al.* (2019). Market manipulation of bitcoin: Evidence from mining the Mt. Gox transaction network. *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*.
- Cermak, Larry. (2019, May 3). A chronological history of Tether. *The Block*, finance.yahoo.com/news/chronological-history-tether-144445744.html.
- Community network data. *Coin Metrics*, coinmetrics.io/community-network-data/#comm-files.
- Durtschi, Cindy, W. Hillison, and C. Pacini. (2004). The Effective Use of Benford's Law to Assist in Detecting Fraud in Accounting Data. *Journal of Forensic Accounting*, 5, 17–34.
- Gandal, Neil, J. Hamrick, *et al.* (2018). Price Manipulation in the Bitcoin Ecosystem. *Journal of Monetary Economics*, 95, 86–96.
- Gheorghe, Florian. (2019, June 13). What causes the infamous bitcoin Bart pattern? *BeInCrypto*, beincrypto.com/what-causes-the-infamous-bitcoin-bart-pattern/.
- Grammatikos, Theoharry, and N. Papanikolaou. (2016, November). Applying Benford's Law to detect accounting data manipulation in the banking industry. Luxembourg School of Finance Working Paper Series.
- Griffin, John, and A. Shams. (2020). Is Bitcoin Really Untethered? *The Journal of Finance*, 75, 4, 2020, 1913–1964.
- Grinberg, Reuben. (2011). Bitcoin: An Innovative Alternative Digital Currency. *Hastings Science & Technology Law Journal*, 4, 1, 159–208.
- Harper, Colin. (2020, March 17). How PlusToken got 1 percent of the bitcoin supply. *Bitcoin Magazine*, bitcoinmagazine.com/articles/how-the-plustoken-scam-absconded-with-over-1-percent-of-the-bitcoin-supply.

- Hougan, Matthew, H. Kim, and M. Lerner. (2019). Economic and non-economic trading in bitcoin: Exploring the real spot market for the world's first digital commodity. *Bitwise Asset Management*.
<https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5574233-185408.pdf>.
- Iglewicz, Boris, and D. Hoaglin. (1993). *How to detect and handle outliers*. ASQC Quality Press.
- Imbert, Fred. (2017, September 12). JPMorgan CEO Jamie Dimon says bitcoin is a 'fraud' that will eventually blow up. *CNBC*, www.cnbc.com/2017/09/12/jpmorgan-ceo-jamie-dimon-raises-flag-on-trading-revenue-sees-20-percent-fall-for-the-third-quarter.html.
- Khatari, Yogita. (2020, July 30). Chinese authorities have arrested all 27 major suspects of PlusToken ponzi scheme – report. *The Block*, <https://www.theblockcrypto.com/linked/73412/china-arrested-suspects-of-plustoken-ponzi-scheme>.
- Leising, Matthew. (2018, December 18). Crypto-mystery clues suggest tether has the billions it promised. *Bloomberg.com*, www.bloomberg.com/news/articles/2018-12-18/crypto-mystery-clues-suggest-tether-has-the-billions-it-promised.
- Mangan, Dan. (2018, November 13). How ex-JP Morgan silver trader's guilty plea could boost manipulation claim against bank. *CNBC*, www.cnbc.com/2018/11/12/ex-jp-morgan-silver-traders-guilty-plea-could-boost-manipulation-suit.html.
- Monamo, Patrick, V. Marivate, and B. Twala. (2016). Unsupervised Learning for Robust Bitcoin Fraud Detection. *2016 Information Security for South Africa (ISSA)*.
- Nigrini, M. J. (1996). Taxpayer Compliance Application of Benford's Law. *Journal of the American Taxation Association*, 18, 1, 72–92.
- Nilsson, Kim. (2015, April 15). The missing Mt. Gox bitcoins. *WizSec*, blog.wizsec.jp/2015/04/the-missing-mtgox-bitcoins.html.
- Peterson, Timothy. (2018). Metcalfe's Law as a Model for Bitcoin's Value. *Alternative Investment Analyst Review*, 7, 2, 9–18.
- Price, Michelle and A. Irrera. (2018, January 30). U.S. regulator subpoenas cryptocurrency platforms Bitfinex and Tether: Source. *Thomson Reuters*, www.reuters.com/article/us-usa-cftc-subpoena-idUSKBN1FJ2ZK.
- Putnam, Bluford and E. Norland. (2018). An in-depth look at the economics of bitcoin. *CME Group*, <https://www.cmegroup.com/education/featured-reports/an-in-depth-look-at-the-economics-of-bitcoin.html>.
- Robinson, Matt, and T. Schoenberg. (2018, November 20). Bitcoin price manipulated by tether? justice department probing. *Bloomberg.com*, www.bloomberg.com/news/articles/2018-11-20/bitcoin-rigging-criminal-probe-is-said-to-focus-on-tie-to-tether.
- —. (2020, September 29). JPMorgan admits spoofing by 15 traders, two desks in record deal. *Bloomberg.com*, www.bloomberg.com/news/articles/2020-09-29/jpmorgan-pays-920-million-admits-misconduct-in-spoofing-probe.
- Stambaugh, Clyde, M. Tipgos, *et al.* (2012). Using Benford Analysis to Detect Fraud. *Internal Auditing*, 27, 3, 21–29.
- Suberg, William. (2017, July 11). Mt. Gox trial update: Karpeles admits 'Willy bot' existence. *Cointelegraph*, cointelegraph.com/news/mt-gox-trial-update-karpeles-admits-willy-bot-existence.
- Supreme Court of the State of New York. (2019, April 25). *James v iFinex et al.* New York County Clerk Index #450545/2019, iapps.courts.state.ny.us/fbem/DocumentDisplayServlet?documentId=vIexA1b0spKOnK_PLUS_ZUGTJ3A==&system=prod.
- Tether. (2017, April 29). Tether announcement. <https://tether.to/announcement/> retrieved from <http://archive.is/uLzlT>.
- —. (2017, November 20). FAQs, <http://archive.is/ONMSv#selection-1153.0-1153.149>.

- —. (2018, January 28). Announcement, <https://tether.to/announcement/> retrieved from <https://archive.is/UQUAw>.
- —. (2018, March 19). About us, <http://archive.is/zNKru#selection-635.0-635.270>.
- —. (2019, March 24). Legal, <http://archive.is/yw7nb>.
- —. (2020, June 20). Tether – Stable digital cash on the blockchain. <https://tether.to>.
- Thomas, Jacob. (1989). Unusual Patterns in Reported Earnings. *The Accounting Review*, 64, 4, 773–787.
- Twain, Mark. (1924). *Mark Twain autobiography*. Harper et Brothers Publ.
- US District Court for the Southern District of New York. (2020, June 3). *Faubus et al v Tether Holdings Limited et al*. Case #1:2020cv00211, <https://www.courtlistener.com/recap/gov.uscourts.nysd.524076/gov.uscourts.nysd.524076.110.0.pdf>.
- Varian, Hal. (1972). Benford's Law. *The American Statistician*, 26, 65–66.
- Velde, Francois. (2013). Bitcoin: A primer. *Chicago Fed Letter*, 317, <https://www.chicagofed.org/publications/chicago-fed-letter/2013/december-317>.
- Wan, Celia. (2019, April 30). Bitfinex reveals stablecoin is only 74% backed by cash, says it's 'simultaneously addressing' requests from NYAG, DOJ and CFTC. *The Block*, www.theblockcrypto.com/daily/21536/bitfinex-reveals-stablecoin-is-only-74-backed-by-cash-says-its-simultaneously-addressing-requests-from-nyag-doj-and-cftc.
- Zero Hedge. (2015, July 13). How high frequency traders broke, and manipulated, the treasury market on October 15, 2014. *Zero Hedge*, www.zerohedge.com/news/2015-07-13/how-high-frequency-traders-broke-treasury-market-october-15-2014-step-step-guide.