Received: Added at production | Revised: Added at production | Accepted: Added at production

DOI: xxx/xxxx

RESEARCH ARTICLE SUBMITTED TO JOURNAL OF FINANCIAL RESEARCH

# Breaking the Stablecoin Buck: The Attenuating Impact of Security Breach Shocks at Cryptocurrency Exchanges

**Andrew Morin**[1] | **Tyler Moore**[1] | **Eric Olson**[2]

[1]School of Cyber Studies, The University of Tulsa, Tulsa, OK, USA

[2]Collins College of Business, The University of Tulsa, Tulsa, OK, USA

**Correspondence**
Andrew Morin.
Email: andrewdmorin@gmail.com

## Abstract

Cryptocurrency markets rely on stablecoins maintaining their peg to fiat currencies like the US Dollar. Customers trade between these stablecoins and their counterparts on exchanges which operate like banks without consumer protections to mitigate run risk. We investigate whether exchange breaches break the peg of Tether, the leading stablecoin. Using an event study, we find that shocks are associated with a break in Tether's peg but return quickly to its par value. By contrast, we find no effect on the price of Bitcoin. We also observe diminishing effects over time, consistent with a maturing market and Lo's adaptive market hypothesis.

**JEL Classification:**
G23, O33, G01

## 1 | INTRODUCTION

Since Bitcoin's introduction, cryptocurrency exchanges have been dogged by unwelcome security breaches, high-profile vulnerability exposures (Böhme et al., 2020), denial-of-service attacks (Vasek, Thornton, & Moore, 2014) and outright scams (Bartoletti, Lande, Loddo, Pompianu, & Serusi, 2021; Siu, Hutchings, Vasek, & Moore, 2022). From the perspective of cryptocurrency users, the most worrying security event occurs when cryptocurrency exchanges are breached and customer funds are stolen. Regrettably, such events are extremely common. Mt. Gox, one of the first cryptocurrency exchanges, suffered multiple security lapses and ultimately collapsed due to unauthorized insider trading.

As cryptocurrencies grow in popularity, thefts at exchanges have continued to proliferate, with criminals regularly absconding with tens of millions of dollars in each heist. What is the impact of persistent security shocks on the functioning of a cryptocurrency ecosystem? Despite repeated warnings that breaches could trigger an "extinction event," trading activity within cryptocurrency markets has consistently grown. This development raises the question: what underpins this remarkable resilience?

This paper provides empirical evidence demonstrating the impact of security events on cryptocurrency exchanges. We demonstrate that the effects of security shocks are real but diminish over time. Specifically, the paper focuses on how security shocks impact Tether (USDT), the largest U.S. dollar (USD) denominated stablecoin. With a market capitalization of $155 billion (CoinMarketCap, 2021), Tether serves as the reserve currency of the cryptocurrency ecosystem. Tether operates similar to a money market mutual fund in traditional finance. Tether's price is officially pegged at $1, but all cryptocurrency exchanges allow the price to float. During times of stress, the price and volatility fluctuates in response to market pressures.

The impact of significant shock events on stablecoins is particularly relevant today, as the Senate recently passed the GENIUS Act (Sen. Hagerty, 2025), which lays out the regulatory framework for fiat-backed stablecoins. As these stablecoins increase in number and popularity, the run risk and contagion effects across decentralized and traditional financial markets is a serious concern. For example, regulatory-compliant stablecoins may decrease the perceived risk of holding them, while in reality, they remain uninsured, and lack a clear distinction from even riskier cryptocurrencies such as algorithmic stablecoins. This work

  

investigates how the current leader in stablecoins, Tether, reacts to shock events, offering a glimpse into the future landscape of stablecoins.

Using an event study, we measure the impact of 44 security breaches (in which money was stolen) on cryptocurrency exchanges over the 2017–2025 time period. We find a negative effect on Tether's USD peg in the days immediately following a breach. The impact attenuates over time, but does result in a cumulative abnormal return of -0.5% over the subsequent 21 day time-period. The dynamics in Tether's price is consistent with the adaptive market hypothesis (AMH) (Lo, 2004), in which survival is the primary objective of market participants. Additionally, we examine the price dynamics of Bitcoin around the dates of our security breaches. Surprisingly, we find no statistically significant impact of breaches on the dynamics of the USD/Bitcoin price. The findings indicate that cryptocurrency markets are becoming *more* resilient to security shocks, not less. This is surprising, given that the magnitude of funds stolen in breaches has steadily risen (Tsihitas, 2019). Our findings suggest that as market participants' understanding of the cryptocurrency ecosystem matures, arbitrage opportunities actively shrink over time leading to a more robust market.

## 2 | RELATED WORK

The frequency and scale of cryptocurrency-related crimes has motivated numerous studies investigating how these events impact cryptocurrency exchanges. Mt. Gox, one of the first major centralized cryptocurrency exchanges, is often the focus of these studies. Feder et al. (Feder, Gandal, Hamrick, & Moore, 2017) found that DDoS and other security shocks significantly affected the trading activity at Mt. Gox, resulting in fewer larger trades. Gandal et al (Gandal, Hamrick, Moore, & Oberman, 2018) analyzed suspicious trading activity at the exchange, and found that a single actor was able to manipulate the price of bitcoin, pushing it from $150 to $1000 within just a few months. However, since the collapse of Mt. Gox in early 2014, thousands of new exchanges have emerged. Many of these exchanges have fallen victim to similar manipulations and hacks. Researchers have studied these new exchanges and found that security shocks and breaches are strongly correlated with exchange closure (Moore & Christin, 2013), (Moore, Christin, & Szurdi, 2018), (Oosthoek & Doerr, 2020).

In addition to exchanges, the effects of security shocks and periods of high volatility on individual cryptocurrencies have also been studied. Corbet et al. (Corbet, Larkin, Lucey, Meegan, & Yarovaya, 2020) investigate the relationship between Federal Open Market Committee announcements and cryptocurrency prices, revealing varying reactions based on the underlying structure of the currencies. Antonakakis et al. (Antonakakis, Chatziantoniou, & Gabauer, 2019) find that periods of high volatility within the cryptocurrency markets, potentially resulting from security incidents, leads to an increase in connectedness between cryptocurrency price return movements. Similarly, Ferreira et al. (Ferreira & Pereira, 2019) found a statistically significant contagion effect in which shocks to bitcoin had contemporaneous effects on other cryptocurrencies, and Wajidi et al. (Wajdi, Nadia, & Ines, 2020) find significant, bidirectional return volatility spillover between many of the largest cryptocurrencies. Additionally, some research has looked at the relationship between security shocks and cryptocurrency price behavior ((Chen, Chang, & Yang, 2023) (Li, Zhou, & Cavusoglu, 2025)). However, these works often focus on highly regulated markets such as the Chicago Mercantile Exchange, or US-based cryptocurrency exchanges which are designed to withstand such volatility. Meanwhile, the majority of cryptocurrency trading happens beyond the reach of such regulatory bodies at exchanges with intentionally complex organizational structure, and often headquartered in countries with lax regulations. For our work, we focus on all major centralized exchanges. These findings, as well as the previous findings on exchange shocks, reveal a notable sensitivity of the cryptocurrency ecosystem to cyber security events.

Stablecoins, due to their peg to non-cryptocurrency assets, are largely omitted in security breach studies. Instead, stablecoins, specifically Tether, are often the focus of general price stability research. Numerous studies have looked at the relative volatility of Tether (Hoang & Baur, 2024) (Hairudin & Mohamad, 2024) (Grobys & Huynh, 2022), how traditional market mechanics such as arbitrage influence Tether's peg (Lyons & Viswanath-Natraj, 2023) (Shao & Rajapaksa, 2025), and even the relationship between stablecoin issuance and non-stablecoin cryptocurrency prices (Wei, 2018). Furthermore, Tether has found itself as the subject of negative media headlines (*Bitfinex's Biggest Critic Is Back on Twitter*, 2018), often related to the questionable existence of funds supporting the digital tokens. Griffin and Shams (Griffin & Shams, 2020) reveal evidence supporting the possibility that Tether is not fully backed by reserves and identify instances where Tether is used to purchase large amounts of bitcoin leading to suspicious market behaviors. The uncertainty of Tether's reserves were also studied by Chohan (Chohan, 2019), who points out the run-risk faced by Tether and other stablecoins if they are not truly fully backed. The dubious nature of these reserves ultimately resulted in a lawsuit brought by the New York Attorney General's office (Browne, 2021).

A notable exception to the existing literature is how stablecoins respond to security shock events. Such events may trigger a flight-to-safety response from cryptocurrency market participants as they seek a portfolio better insulated from market volatility (Anadu et al., 2023), or perhaps these stablecoins become increasingly volatile like their non-fiat pegged counterparts. Our work seeks to answer these questions and better understand how stablecoins respond to security shock events.

# 3 | THE TETHER PEG

Stablecoins are a type of cryptocurrency designed to offer a less volatile, more liquid asset for market participants. This is achieved by stripping away the speculative traits of a cryptocurrency and pegging the price to a predictable value. The leading method for achieving this stability is through a direct swap from fiat currencies (e.g. USD or Euros) to a cryptocurrency which can be later redeemed for the original amount. According to Coinmarketcap.com there are currently 233 stablecoins with a collective market capitalization of over $230 billion (CoinMarketCap, 2021). Of these, $210 billion are isolated to the top two stablecoins: Tether and USD Coin, both of which are "fiat-pegged" stablecoins as described above. Tether itself captures more than half the total market share at $155 billion. Both of these stablecoins, not coincidentally, are closely tied to two of the top exchanges: Bitfinex and Coinbase.[1] Despite being created by the operators of these exchanges, stablecoins themselves can be traded on any exchange that choose to list them.

For this work, we choose to focus solely on Tether for two primary reasons. First, Tether's market dominance – specifically market capitalization, daily trade volume, and listed markets – has resulted in its use as a reserve currency for decentralized markets. Second, Tether was one of the first stablecoins, and pre-dates the second oldest fiat-pegged stablecoins by four years. This allows us to evaluate security shocks over the longest possible time window.

## 3.1 | The role of Tether

In theory, acquiring Tether is a simple process: an individual sets up an account on tether.to, deposits USD, and receives Tether in return. On their website, Tether claims that "Tether tokens hold their value at 1:1 to the underlying assets," and that the underlying assets include cash reserves, precious metals, and commercial paper.[2] Tether maintains its peg because users can redeem their Tether tokens on the tether.to website at a rate of 1 USDT to 1 USD. However, this redemption process only occurs at the Tether website; yet, tens of billions of dollars worth of Tether transactions occur on exchanges daily. While Tether Limited (the stablecoin issuer) is willing to redeem USDT for USD at a 1:1 ratio, the average cryptocurrency market participant is far more likely to encounter Tether on an exchange where the price is dictated by market forces.[3] For example, a trader can sell USDT for USD on Bitfinex at a rate close to, but rarely, exactly 1 USD. This is because the Tether being sold is not being redeemed from the reserves held at Tether Limited; instead, it is being traded between users on the exchange at a market-clearing price. The large number of trade pairs involving Tether, and its nearly universal adoption among exchanges, keeps the price close to its $1 peg. This price stability is reinforced by a built-in arbitrage mechanism (Lyons & Viswanath-Natraj, 2023). When Tether trades below $1 on exchanges, arbitrageurs can purchase discounted USDT and redeem it at Tether.to for par value, profiting from the spread. This buying pressure pushes the exchange price back toward $1. Conversely, when Tether trades above $1, arbitrageurs can deposit USD at Tether.to, receive newly minted USDT, and sell it on exchanges at a premium. This mechanism ensures that deviations from the peg are self-correcting, provided sufficient arbitrage capital is available and redemption channels remain open.

Importantly, this arbitrage mechanism distinguishes Tether from assets like Bitcoin. Bitcoin has no "par value" toward which market forces can push the price; there is no issuer willing to exchange Bitcoin for a fixed amount of USD. Consequently, while both Tether and Bitcoin may be affected by the same underlying shock—such as news of an exchange breach—we would expect systematically different price responses. For Tether, selling pressure causes temporary discounts that arbitrageurs then correct. For Bitcoin, there is no analogous mean-reverting mechanism, and price effects (if any) depend entirely on shifts in market sentiment rather than arbitrage dynamics.

[1] The largest cryptocurrency exchange, Binance, also issued a stablecoin between 2019 and 2024. This stablecoin, Binance USD, was the third largest stablecoin before becoming the focus of an SEC investigation and subsequently collapsing.

[2] Analysis by (Griffin & Shams, 2020) has shown that this is likely untrue, that Tether is only partially backed, and that Tether can be used to manipulate Bitcoin prices.

[3] Tether requires a minimum redemption amount of $100,000, pricing out most retail traders.

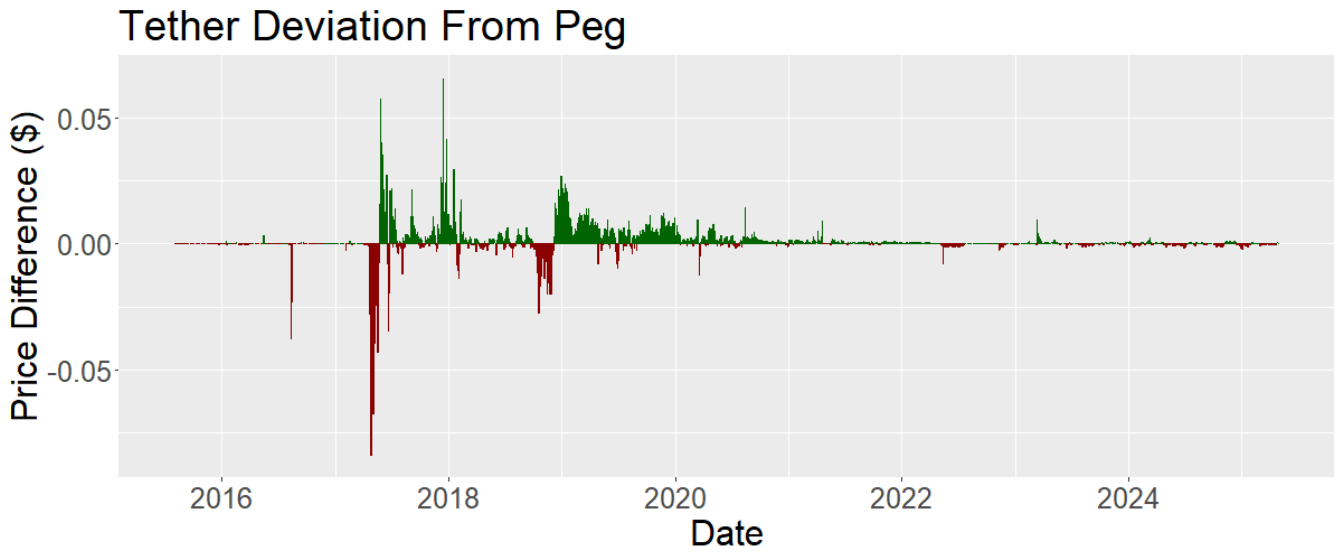


**FIGURE 1** Tether deviations from $1 peg over time.

Because stablecoins increase liquidity, exchanges incentivize their use by having different withdrawal fees and contribution limits for fiat currencies. Bitfinex, for example, charges 0.1% on any USD withdrawal, with a minimum of $60 (Bitfinex, 2021); FTX, before failing, charged a flat $75 fee to withdraw USD (FTX, 2021). In contrast, both exchanges have substantially lower fees for withdrawals using Tether. Kraken, a California-based exchange regularly in the top 10 cryptocurrency exchanges by volume, restricts users with the lowest verification level to just $9,000 in withdrawals per month. However, these users could instead withdraw $5,000 worth of cryptocurrencies, including stablecoins, every day with no monthly limit (Kraken, 2021). Furthermore, cryptocurrency derivatives, such as perpetual futures contracts, are often priced in stablecoins which necessitate the need to hold stablecoins. Each of the top six derivative exchanges offer Tether-settled perpetual futures contracts, which are significantly more popular than the cryptocurrency settled versions.

Despite the widespread use, stablecoins are much riskier than many traders likely realize. Capital controls are usually stated in the Terms of Service agreements. For example, consider the statements within the Tether Terms of Service agreement:

> *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 Tethers Reserves, including Fiat, but Tether Tokens are not Fiat themselves..... In order to cause Tether Tokens to be issued or redeemed directly by Tether, you must be a verified customer of Tether. No exceptions will be made to this provision. The right to have Tether Tokens redeemed or issued is a contractual right personal to you. Tether reserves the right to delay the redemption or withdrawal of Tether Tokens if such delay is necessitated by the illiquidity or unavailability or loss of any Reserves held by Tether to back the Tether Tokens, and Tether reserves the right to redeem Tether Tokens by in-kind redemptions of securities and other assets held in the Reserves. Tether makes no representations or warranties about whether Tether Tokens that may be traded on the Site may be traded on the Site at any point in the future, if at all.*

Note that Tether reserves the right to delay the redemption or withdrawal of Tether token for (1) illiquidity, (2) unavailability, or (3) loss of reserves. Moreover, note that if a user purchased a Tether token on a 3rd-party exchange (as is common), the customer would have to be a verified customer of Tether before exchanging the Tether for USD.

Because of the direct connection between the value of Tether and the underlying assets backing the tokens, one risk to the stability of Tether is a panic-induced run. Thus, while it is far from certain that most market participants understand the Tether Terms of Service, the fact that Tether articulates the controls likely reduces the risk of a panic-run redemption. In other words, as noted in (Brown, Trautmann, & Vlahu, 2016), the fact that Tether declares the strict rules of withdrawal in the Terms of Service likely impacts the beliefs of how likely customers think there is to be a run on Tether, which in turn reduces the risk of a run. If a customer holds Tether but is unable to redeem Tether for USD at Tether.to, they may be willing to sell the Tether below par value on an exchange. In this example, the buyer of Tether may be an institutional trader capable of redeeming Tether directly from Tether.to, or they could simply be a more risk-tolerant retail trader. As Figure 1 shows, this behavior is common (although diminishing in magnitude over time) with Tether frequently traded at prices above and below the peg.

The trading of Tether at prices other than the pegged value could be explained, at least in part, by security breaches of cryptocurrency exchanges. When a cryptocurrency exchange suffers a breach, particularly when money is stolen, it is common for

news of the incident to quickly propagate through the cryptocurrency community. Forums, social media accounts, and specialist news sites regularly report on such events, with some of the more significant breaches catching the attention of mainstream news media outlets. These breaches are newsworthy, not only because money is lost at that particular exchange, but also because they make salient the risks of a similar incident taking place elsewhere in the decentralized financial markets. In fact, many of the more popular markets are anything but decentralized. The reliance on centralized ledgers, partnerships between exchanges (*Crypto Exchanges Huobi, Poloniex to Form 'Strategic Partnership'*, 2023), merging of large service providers (*Crypto Exchange Kraken Agrees to Buy Futures Platform NinjaTrader for $1.5B*, 2025), and deals between competitors (*Binance Partners With Circle to Push USDC Stablecoin Adoption Across the Globe*, 2024) have resulting in a cryptocurrency market with numerous, often hard to discern, connections across exchanges.

Consequently, we anticipate that some users at all exchanges, not just those at the affected exchange, could be alarmed by such a breach and elect to pull money out of the exchange. Users may rationally fear that the funds they have stored in a hosted wallet on an exchange are no longer safe and wish to "cash out" of their stablecoins. As a result, we hypothesize that traders may be willing to buy/sell Tether at prices other than the pegged value during periods of high uncertainty – namely, following security shock events. Formally, the first hypothesis we investigate is **H1: Security shock events trigger a short term flight-to-safety response resulting in a deviation from the peg.**

## 3.2 | The maturity of Tether

Existing research (Hoang & Baur, 2024) (Hairudin & Mohamad, 2024) (Grobys & Huynh, 2022), market capitalization data[4], and visualizations such as Figure 1 have shown that Tether continues to grow in popularity while reducing its price volatility. It is reasonable then to expect that as the Tether market matures, the magnitude and frequency of deviations may be affected. This relationship between the maturity of markets and their participants over time is described in the Adaptive Market Hypothesis (AMH) proposed by Lo (Lo, 2004), where the primary objective of market participants is survival. Specifically, Lo makes the case that prices will reflect "as much information as dictated by the combination of environmental conditions and the number and nature of species in the ecology." These *species* are described as "distinct groups of market participants each behaving in a common manner." Because of the niche role Tether plays in the cryptocurrency ecosystem, the users of Tether fit this definition well. Furthermore, the AMH posits that the efficiency of a market can change based on the amount of participating species and the available resources, both of which have changed significantly for Tether since its inception.

Lo describes four practical implications of the AMH which we believe are testable. First, the relationship between risk and reward will not be constant across time as the market infrastructure evolves, the regulatory environment changes, the psychology of market participants adapt, and the type of market participants change. Tether has experienced substantial changes in the infrastructure of their market. From its initial release on the Bitcoin blockchain in October 2014 until early 2017, Tether failed to surpass $10 million market capitalization. During 2017, Tether released a second contract on the Ethereum blockchain, which coincided with a dramatic increase in the number of cryptocurrency exchanges. By the end of 2017 Tethers market cap was over $1 billion. Currently, Tether is consistently the most traded cryptocurrency. Moreover, in 2021 regulators set their sights on the risks that stablecoins pose to the traditional payment system. As such, increased regulatory oversight likely impacts the risk/reward tradeoff for market participants. In cases in which the infrastructure of the market undergoes substantial changes and the regulatory environment is uncertain, the AMH suggests that the market participants will adapt, and the risk/return tradeoff of holding/using Tether will change. Second, the AMH posits that arbitrage opportunities will exist and fluctuate depending upon the type and number of market participants as well as the ecology of the system. Third, trading strategies will be profitable depending upon the type and number of a particular type of "species" in the market. Finally, Lo argues that within the AMH, survival is the only objective that matters. In our case, implications (1) (3) are easily tested using basic time series regressions in Section 5, and the fourth implication will be investigated using event studies in Section 6. Thus, the second hypothesis we investigate is **H2: The impact of security shock events on the Tether price will diminish over time as the market matures and efficiency increases.**

[4] According to Coinmarketcap.com, Tether's market capitalization has increased 37% in the last year alone, from $112 billion in July 2024, to $154 billion in June 2025.

# 4 | SECURITY SHOCK EVENTS AND MARKET DATA

Security breaches at centralized cryptocurrency exchanges present a unique risk to market participants. These exchanges, in an effort to reduce transaction times and costs, serve as custodians of user funds. That is, users must deposit their funds to the exchange before conducting trades which occur beyond the scope of the blockchain. As a result, these funds are not protected by blockchain security mechanisms, nor are the funds easily accessible during periods of uncertainty. While many of the largest cryptocurrency breaches have taken place at fully decentralized financial platforms such as blockchain bridges (*The aftermath of Axie Infinitys $650M Ronin Bridge hack*, 2022),(Faife, 2022), the impact is isolated to users and funds who interacted with specific smart contracts. In contrast, a breach at a centralized exchange could affect all users on the exchange while users are unable to verify the security of their deposits. Due to this unique risk, we define shock events within this study as centralized cryptocurrency exchange breaches where user funds have been stolen.

## 4.1 | Shock events

For an event to qualify as a security shock event, we use the following criteria. First, it must meet the National Institute of Standards and Technology definition of a data breach: "An incident that involves sensitive, protected, or confidential information being copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so." Second, the breached exchange must host cryptocurrency exchange pairs for spot and/or derivative trading. This excludes thefts from non-custodial wallets and individual customer accounts. Finally, money must be stolen from the exchange itself; as such, this criteria excludes cases where breaches are detected before money is stolen, or where confidential information is accessed without a loss of customer funds.

The initial phase of gathering data on security shock events involved consolidating existing event datasets from (Moore et al., 2018; Oosthoek & Doerr, 2020; Vasek, 2019; Passeri, 2023). In order to find additional exchange breaches not captured by prior efforts, we manually reviewed all cryptocurrency events in (Passeri, 2023) and constructed a set of keywords used in a restricted date range web searches. Plausible reports were manually inspected and compared against the criteria outlined above. Once a potential event was identified, we searched for corroboration of the event from an official source. Only corroborated breaches were added to our dataset, which included all but one of the new events, yielding an additional 51 events for a total of 76.

The timeline for the breaches is shown in Figure 2, where the breaches are weighted by the amount of money stolen on a logarithmic scale. The date of each shock corresponds to the earliest corroborated public report. Note that pricing data on Tether began after February 25, 2015. Four of our security breaches occurred prior to this date and are indicated by the dashed lines in the figure. Prior to 2017, Tether's market capitalization failed to surpass $10 million and the daily trading volume rarely exceeded $1 million. However, by the end of 2017 the market capitalization surpassed $1 billion with a daily trading volume exceeding $2 billion. To put this into perspective, by the end of 2016, Bitcoin had a market capitalization over $15 billion and a daily trade volume in the tens to hundreds of millions. This period of relatively low volume and market capitalization is extremely volatile and susceptible to large deviations. Furthermore, different sources report significantly different prices at certain points between February and June of 2015, making prices unreliable. For example, Coinmarketcap.com (CoinMarketCap, 2021) reports prices as high as $1.21 in February 2015, while a similar aggregate website Coingecko.com (Coingecko, 2025) reports prices as low as $0.57 weeks later. Experiments performed while including this period skewed the results, over-estimating the efficiency of Tether over time. While our findings are the same with and without this data, we chose to omit this early period to avoid distorting our results with unreliable data. As such, the data used for this work includes Tether data starting in January of 2017, which is denoted by the dashed green line in Figure 2. Finally, we omit any shock events which overlap with previous events such that the estimation window for a later event may include a previous event, contaminating the expected returns. These steps leave 44 security shock events for our analysis. The full list of events used can be seen in Table A1.

## 4.2 | Market data

The breaches studied in this work occur at 62 unique exchanges, many of which are no longer operating. This makes it impossible to collect historical Tether price data from every impacted exchange. However, the hypotheses we aim to test in this work can be investigated using aggregate prices collected across the majority of exchanges. Coinmarketcap.com collects such data

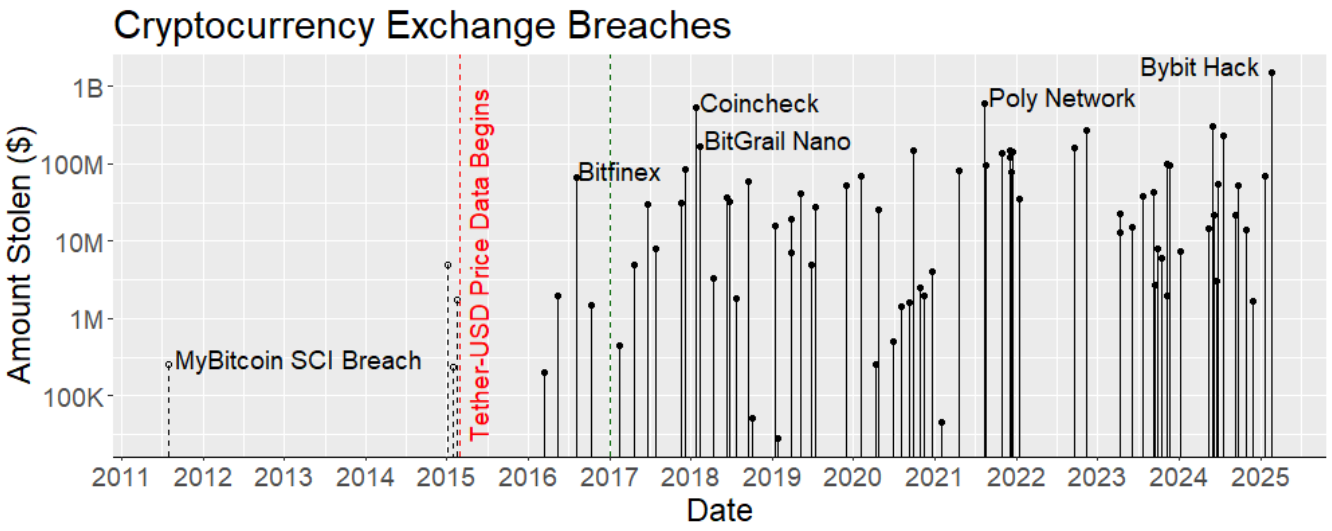


**FIGURE 2** Timeline of exchange breaches and the release of Tether. The amount of money stolen is shown in log-scale on the vertical axis.

from more than 800 exchanges, and for more than 17 million individual cryptocurrencies. The prices reported by Coinmarketcap.com are calculated based on the law of large numbers. Due to the large number of exchanges providing prices, the "real" price of a cryptocurrency is expected to be the average of all reports. Coinmarketcap.com does state that they omit outliers from the calculation, as well as exchange prices where the "price does not seem indicative of a free market price; for example, when an exchange disables withdrawals or deposits, or regulatory conditions make it impossible for anyone else outside of a certain geographical region to buy coins" (Coinmarketcap, 2025). A benefit of using such data when investigating flight-to-safety responses is the inherent capture of market-wide behavior. Due to the unavailability of historical data to all breached exchanges and the benefits of using aggregate data, we choose to collect historical data from Coinmarketcap.com for this work. We gathered data for Tether between February 25, 2015 and May 1, 2025 at the five minute granularity, which includes the average price, total volume, and peak market capitalization for each five-minute bin.

One drawback of using aggregate data is the inability to pinpoint individual trade pair behavior at exchanges. Specifically, the price of Tether is reported by most aggregate sites in fiat currencies such as USD, while only a fraction of overall trading volume is direct trading between Tether and USD. This means Tether/Bitcoin, Tether/Ether, and many other trade pairs are converted into a Tether/USD price. If the price of Tether were to deviate from the peg, the question then becomes whether this is truly a change in the Tether/USD price? Should we find that the aggregate price of Tether does deviate following a shock, individual trade pairs can be used to evaluate which prices are moving in a second set of event studies. For these studies, we use five minute price data from the Binance exchange (Binance, 2025). We collect price data on six trade pairs: Bitcoin/Tether, Ether/Tether, Bitcoin/Ether, XRP/Bitcoin, XRP/Ether, and XRP/Tether. This data ranges from August 2017 until May 2025.

## 5 | GENERAL TETHER BEHAVIOR

The hypotheses presented in this work are focused on how Tether reacts to significant shock events. A meaningful investigation of these hypotheses requires a clear understanding of *normal* Tether behavior. In this section we will define the general behavior of Tether, with a focus on the persistence of deviations from the $1 peg over time.

### 5.1 | Persistence of peg deviation

We use three metrics to investigate the persistence of deviations from Tether's peg: price, deviation, and returns. The price is reported directly from the aggregate data source, and the deviation is the difference between the reported price and the purported peg of $1. For the returns we use the first difference of the natural logarithms. That is,

**Panel A:** Daily Tether Returns

$$r_t = \alpha_0 + \alpha_1 r_{t-1} + \epsilon_t$$

| | Coefficient | Std. Error | T-statistic | P-value |
|---|---|---|---|---|
| $a_0$ | 0.00 | 0.00 | 0.00 | 0.99 |
| $a_1$ | –0.04* | 0.02 | –2.54 | 0.01 |
| $R^2$: 0.002 | | *DW*: 2.0 | | Obs: 3039 |

**Panel B:** Daily Tether Deviations from its $1 peg

$$deviation_t = c_0 + c_1 deviation_{t-1} + \tau_t$$

| | Coefficient | Std. Error | T-statistic | P-value |
|---|---|---|---|---|
| $c_0$ | 0.00 | 0.00 | 1.35 | 0.18 |
| $c_1$ | 0.93*** | 0.01 | 135.7 | 0.00 |
| $R^2$: 0.86 | | *DW*: 1.87 | | Obs: 3040 |

**TABLE 1** Time-series regressions on Tether returns and deviations. The sample covers daily observations from January 2017 through May 2025. Returns are computed as the first difference of natural logarithms of Tether prices. Deviations are defined as the difference between the reported price and the $1 peg. *DW* denotes the Durbin-Watson statistic. $^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$.

$$r_t = \ln(p_t) - \ln(p_{t-1}) \tag{1}$$

where $r_t$ is the daily rate of return, $p_t$ is the price of Tether at the end of day $t$, and $p_{t-1}$ is the price of Tether at the end of day $t-1$. We subsequently estimate one time-series regression for each of these three metrics. First, we estimate the returns using:

$$r_t = \alpha_0 + \alpha_1 r_{t-1} + \epsilon_t \tag{2}$$

where $\alpha_0$ measures the average return (which in our case should be 0) and $\alpha_1$ is the estimated first-order serial correlation coefficient. We estimate the deviation of Tether from $1 using:

$$deviation_t = c_0 + c_1 deviation_{t-1} + \tau_t \tag{3}$$

where $deviation_t$ is $1 minus the end of day $t$ price. The coefficients $\alpha_1$ and $c_1$ are identical to the formal definition of serial correlation for Tether returns, prices, and deviations, respectively.

After estimating the equations (2) - (3), which can be seen in Table 1, we find that the deviation behavior is particularly interesting (Panel B). These deviations are quite persistent (0.93) and statistically significant at the 99% level.

## 5.2 | Deviation behavior over time

While the estimations show statistically significant and persistent deviations from the peg, they are taking into account the entire dataset at once. To identify how this behavior has changed over time we modify equations (2) - (3) to examine a 200-day rolling window. That is, we estimate,

$$r_{wt} = \alpha_{0w} + \alpha_{1w} r_{t-1} + \epsilon_{tw} \tag{4}$$

$$deviation_{wt} = c_{0w} + c_{1w} deviation_{t-1} + \tau_{tw} \tag{5}$$

where $\alpha_{1w}$ and $c_{1w}$ capture the first order autocorrelation for each 200-day rolling window $w$. Figure 3 plots the autocorrelation and R-Square statistics for Tether deviations. Most surprising is the variation in the first order autocorrelation. Earlier periods, as well as more recent periods, correlate to higher autocorrelation, where deviations from the peg seem to persist, while periods between 2019 and 2023 have lower autocorrelation. Although deviations persist in more recent periods, we know from Figure 1 that the magnitude of these persistent deviations is decreasing. There are many possible explanations for why deviations are decreasing in magnitude over time, such as an overall decrease in volatility. However, these rolling regressions make it clear

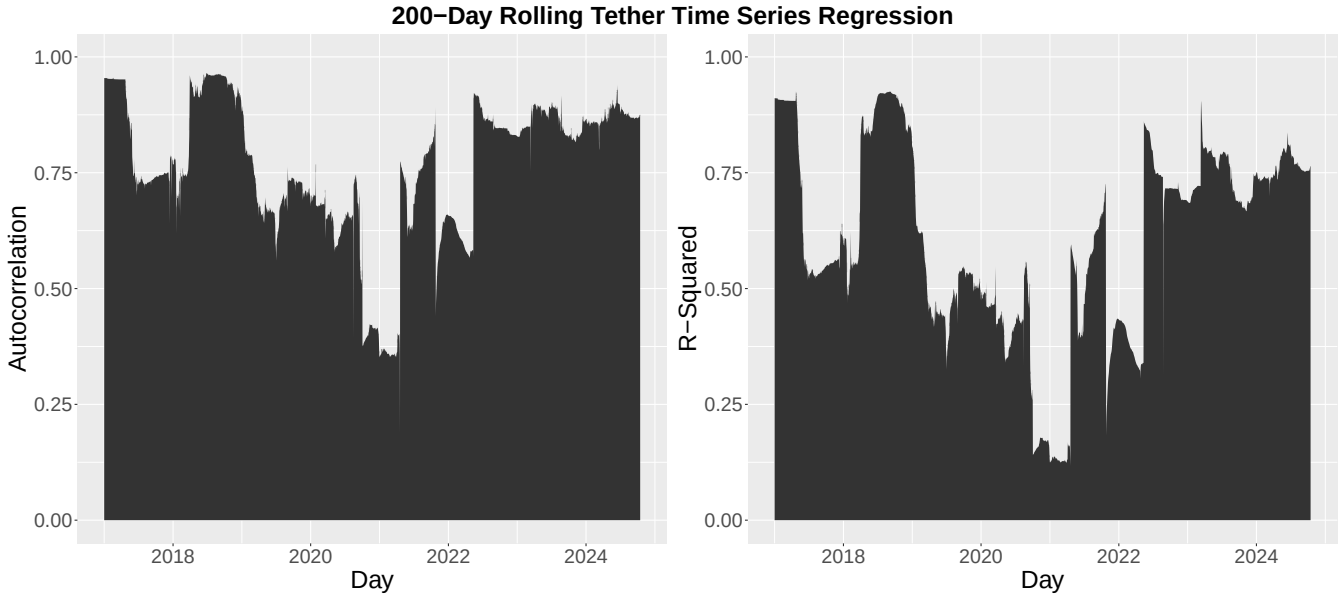


**FIGURE 3** Autocorrelation and R-Square Statistics from 200 day rolling regressions from on Tether Deviations from $1.

that the persistence of the deviations (whether they are small or large in magnitude) indicates an overall lack of efficiency in eliminating price deviations.

| Daily Tether Prices $p_{wt} = b_{0w} + b_{1w}p_{t-1} + \gamma_{tw}$ | | | | |
|---|---|---|---|---|
| **Coefficient** | **Average** | **Std. Error** | **Min** | **Max** |
| $b_0$ | 0.24 | 0.003 | -0.64 | 0.82 |
| $b_1$ | 0.76 | 0.003 | 0.18 | 1.64 |
| $r^2$ | 0.61 | 0.004 | 0.12 | 0.93 |

**TABLE 2** Rolling window time-series regressions of Tether prices. Each row reports summary statistics across all 200-day rolling windows estimated over the January 2017 through May 2025 sample period. The dependent variable is the daily Tether price, regressed on its first lag. $r^2$ denotes the coefficient of determination for each rolling window. $^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$.

In addition to the variation in the first order autocorrelation coefficient, the range of the $r^2$ statistics is quite large. Table 2 shows summary statistics for the rolling 200 day regression for Tether's prices. Note that the $r^2$ from the first order time-series regression ranges from 0.12 to 0.93, and that on average, an AR(1) regression explains more than 60% of the variation in Tether prices, which is quite large. We believe, in a highly efficient market, market participants should arbitrage away any of Tether's deviation from it's $1 peg, which implies that the first order autocorrelation, $c_{1w} = 0$. We find these results in Table 2 and the variation of the first order autocorrelation coefficient in Figure 3 at odds with this prediction. The full summary statistics for price, returns, and deviations from the $1 peg can be seen in Table B2 in B.

## 6 | TETHER SHOCK RESPONSE

Our findings related to the stability and persistence of Tether peg deviations is in line with the existing literature (Hoang & Baur, 2024) (Hairudin & Mohamad, 2024) (Grobys & Huynh, 2022). Namely, the peg is not perfectly stable and deviations do occur, with a decreasing magnitude over time. What has not yet been investigated is how this stability stands up to extreme pressure, such as a security breach. Our first hypothesis suggests that such an event could trigger a flight-to-safety response and a peg

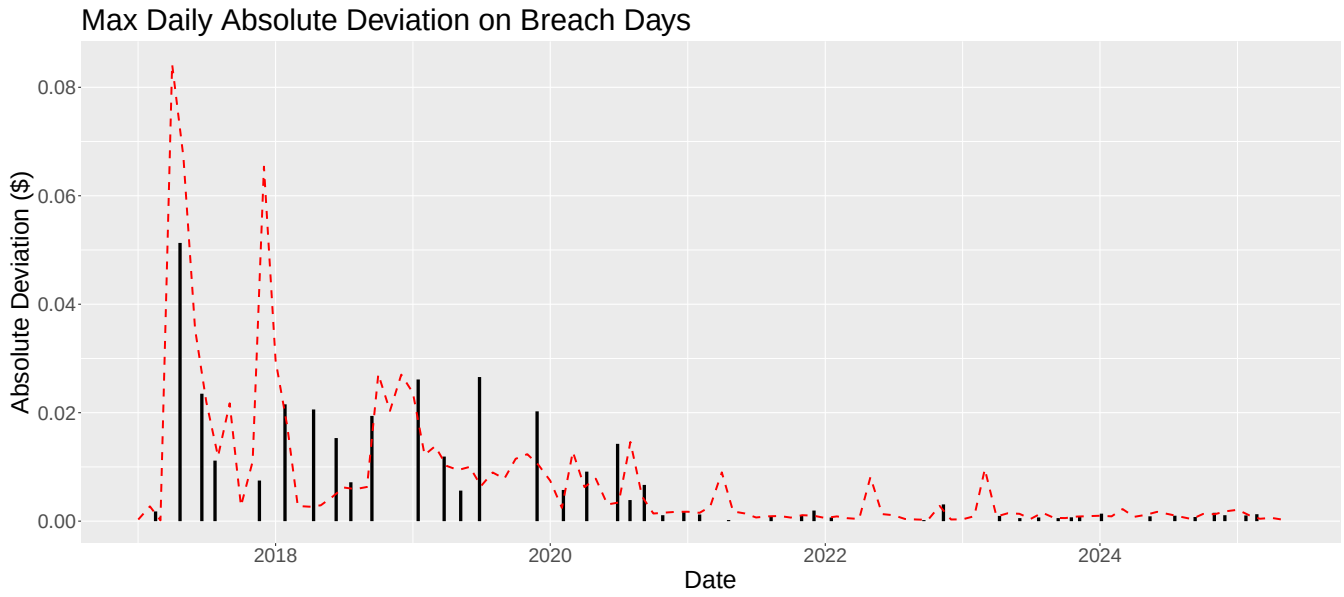


**FIGURE 4** Maximum deviation from $1 peg on each day experiencing a breach event. The two costliest breaches (Poly Network and Bybit) occur in August 2021, and February 2025.

deviation may occur. Figure 4 visualizes the maximum absolute Tether price deviation on breach days (with monthly median deviation denoted by the dashed red line), which reveals large deviations of up to five cents in the earlier periods, and decreasing in magnitude over time. It is noteworthy that early 2021, when major deviations largely disappear, closely aligns with several important events for Tether. These include the first asset audits[5], a settlement with the New York Attorney General (Stempel, 2021), and a ruling from the Commodity Futures Trading Commission (Prentice & Prentice, 2021). To better understand how these deviations relate to breaches themselves, we utilize two different methodologies: an event study analysis of abnormal returns which takes into account all of these breaches together, and a survivability analysis focused on returns, prices, and deviations over time, investigating the apparent diminishing effect seen over time. The event studies will allow us to answer our first hypothesis, where a significant deviation from the peg in the periods following a breach are indicative of a flight-to-safety from market participants. The survivability analysis captures changes to the maturity over time, and allows us to investigate our second hypothesis related to a diminishing effect of breaches on the peg.

## 6.1 | Event study of breaches

Event studies are used to empirically test for statistically significant deviations in a time series. This is achieved by first estimating the normal return of an asset, followed by measuring the abnormal returns, or the difference between this and the actual observed values, around significant events. While relatively large deviations are expected around these events as new information propagates, an efficient market should see these abnormal returns quickly revert to normal. Event studies can be performed on long- and short-term time frames, however short-term event studies offer "[t]he cleanest evidence on market-efficiency." (Fama, 1991) As such, we find the granular price data and precise event times associated with cryptocurrency data to be an optimal use case for the event study methodology.

For our event study, we follow the process outlined by (MacKinlay, 1997), and shown in Equation 6, which is to calculate abnormal return, $AR$, as the difference between actual returns, $R$, and expected returns, $E(R)$.

$$AR = R - E(R) \tag{6}$$

To follow the process outlined by MacKinlay et al. directly, our next step would be to calculate $R$ as simply the closing price of the asset each day. However, cryptocurrencies are far more volatile than the majority of financial assets, and during our

[5] Tether reserve reports can be found here: https://tether.to/en/transparency/?tab=reports

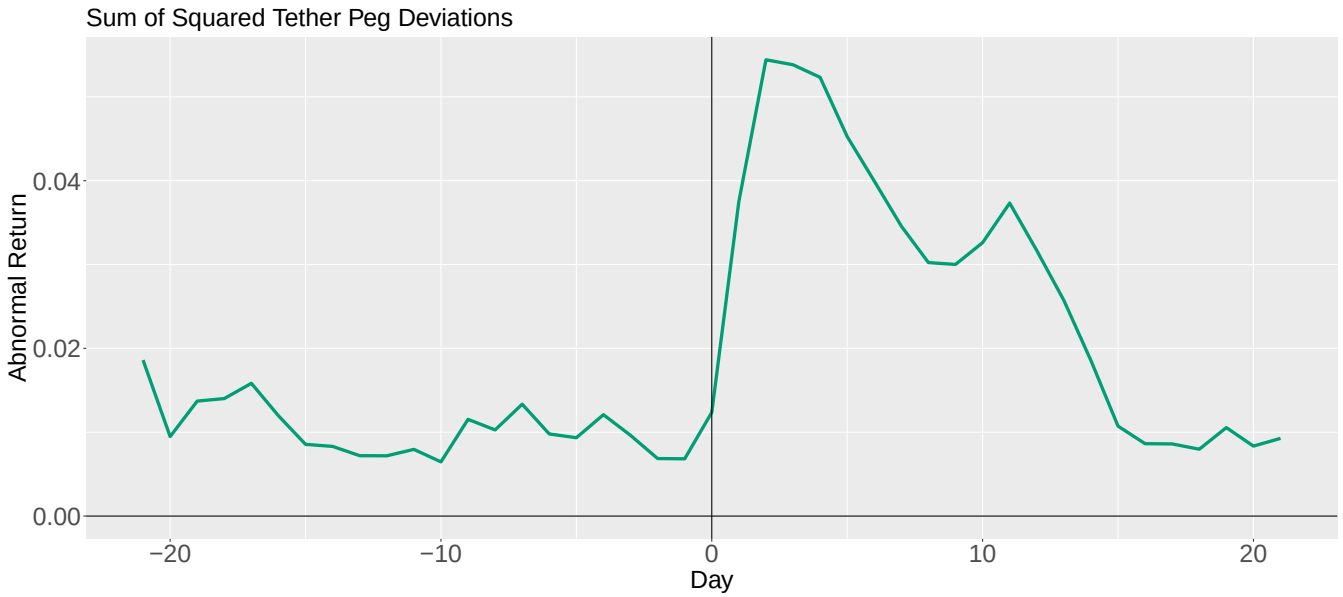


**FIGURE 5** Event study plot of the Tether(USDT)/USD peg. A t-test of the pre- and post-event windows is statistically significant (p = 0.00007).

initial exploration of the data we noticed that daily granularity data failed to fully detail the wide swings in the price between "closing" times. What's more, cryptocurrency markets never truly close, and therefore the "closing" price is simply the final data point for the granularity and timezone chosen. To account for these inconsistent and relative prices, we utilized hourly pricing data which were converted into two daily measures: sum of squared differences, and average daily return. For the sum of squared differences approach, we calculate the total daily difference between the stablecoin and its peg value. Because the price may be either higher or lower than \$1, we first square any difference and subsequently sum the squared difference for a given day. This process is shown in Equation 7, where $R_t$ is the actual squared difference for a given day, $t$, and $S$ and $P$ are the stablecoin price and peg price respectively, at hour, $i$, of the day.

$$R_t = \sum_{i=1}^{24} (S_i - P_i)^2 \tag{7}$$

The second way we calculate actual returns is by finding the return of the average daily price. This is detailed in Equation 8, where $\overline{S}_t$ is the average daily stablecoin price on day, $t$.

$$R_t = \frac{\overline{S}_t - \overline{S}_{t-1}}{\overline{S}_{t-1}} \times 100 \tag{8}$$

Next, we need to identify an expected return, $E(R)$, for our time series data. While the cryptocurrency markets lack reliable indices, stablecoins offer a uniquely reliable expected behavior. For returns calculated using sum of squared differences (Equation 7), the expected return, or total deviations from the peg, is simply zero. When computing the average daily returns (Equation 8), the expected return a stable asset is the return of the previous day, and therefore $E(R)_t$ is once again zero. This zero expected return benchmark distinguishes our event study from traditional applications that require a market model to estimate abnormal returns. For most financial assets, expected returns are non-zero and time-varying, necessitating the use of an index or factor model. However, Tether is explicitly designed to maintain a constant \$1 price, implying an expected return of exactly zero by construction. Any non-zero return therefore represents a deviation from the intended peg which is what we seek to measure. Using an alternative benchmark such as Bitcoin returns or a cryptocurrency index would conflate Tether's idiosyncratic peg dynamics with broader market movements and obscure the peg breaks that are our focus.

The first event study we perform is on the hourly squared differences of Tether around security breach events on exchanges using Equation 7. We use a window size of 21 days before and after the event, for a total of 43 days including the event day itself. The results of this event study can be seen in Figure 5. From these results it can be observed that, prior to breaches, the price consistently has minor volatility around its peg. However, immediately following exchange breaches, this volatility increases dramatically by a factor of 5. The volatility eventually returns to normal levels around 20 days post event.

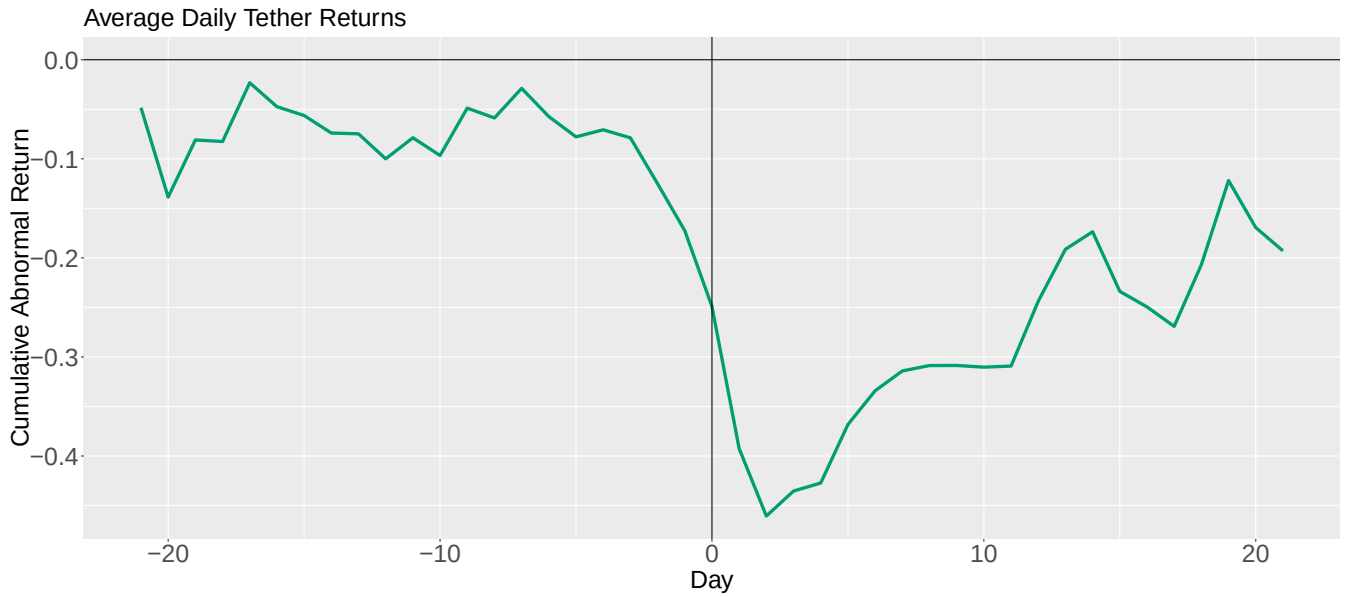


**FIGURE 6** Event study plot of the Tether daily returns. The event window starts 21 days before the event, and extend 21 days after. A t-test of the pre- and post-event windows is statistically significant (p = 0.0000000007).

The abnormal returns in Figure 5 are calculated as the sum of squares, and does not show which direction the price moves relative to the peg. Therefore, we perform a second event study using Equation 8, which allows us to observe the direction of abnormal returns. We can see the cumulative abnormal returns of this event study in Figure 6, where it becomes apparent that this volatility is the result of the Tether peg breaking into a discounted rate. That is, the price of Tether drops below $1 and oscillates between extended periods of positive and negative returns, slowly returning to pre-event volatility around 3 weeks post-event. Note that the cumulative effect seen in Figure 6 is approximately -0.5%. While each of these breach events are localized to individual exchanges, this break from the USD peg is realized in the entire aggregate price and implies that an exchange-level breach event can induce a universal break from the 1:1 peg.

$$R = \beta_0 + \sum_{i=1}^{5} \beta_i L_i + \beta_6 D + \epsilon \tag{9}$$

To quantify the impact a breach has on the Tether peg, we create a linear model, shown in Equation 9, where the Tether returns, R, are the response variable and five lags, L, of the Tether returns and a dummy variable, D, are the explanatory variables. The dummy variable holds the value of one for any day within the breach window, and zero every other day. The breach window is defined as any day with a recorded breach, plus or minus some number of days to account for delays between the breach occurring and news outlet reporting on it. In Table 3 we can see the coefficients and their significance from three different breach window sizes. For each of the breach windows we see a statistically significant negative coefficient for the breach window, representing a decrease in Tether returns between 0.05% and 0.08% during a breach.

It might seem counter-intuitive that a user would sell their Tether at a discount, since they could instead redeem their stablecoins at the issuer for a higher rate. However, there are costs incurred by moving and redeeming stablecoins at the issuer. As noted above, at a minimum one must first be a verified user from `Tether.to` before one can redeem the tokens for USD. Moreover, most exchanges charge users a fee for withdrawing cryptocurrency. Once a user has paid this fee and withdrawn their stablecoin, they must deposit it onto the their stablecoin issuer account, again incurring blockchain fees. For Tether specifically, the user then must pay a one time fee of $150 to verify their account "... to ensure that only those who are serious about establishing an account apply." Finally, the user can then redeem their Tether for USD, incurring a fee of $1,000 or 0.1% per transaction, whichever is greater, and with a required minimum redemption of $100,000.

For comparison, we perform an event study on bitcoin returns using the same 43 day window, and use a 21-day estimation period leading up to this window to calculate an average return as the index[6]. The results of this event study can be seen in

[6] While Tether is expected to have a constant value, and therefore a return of 0%, bitcoin has experienced an overall positive trend since its inception.

| | +/- 0 Days | +/- 1 Day | +/- 2 Days |
|---|---|---|---|
| Intercept | 0.002 | 0.005 | 0.007 |
| | (0.005) | (0.005) | (0.005) |
| Lag1 | 0.04* | 0.04* | 0.03 |
| | (0.02) | (0.02) | (0.02) |
| Lag2 | –0.05** | –0.05** | –0.05** |
| | (0.02) | (0.02) | (0.02) |
| Lag3 | –0.07*** | –0.07*** | –0.07*** |
| | (0.02) | (0.02) | (0.02) |
| Lag4 | –0.03 | –0.03 | –0.03 |
| | (0.02) | (0.02) | (0.02) |
| Lag5 | –0.01 | –0.01 | –0.01 |
| | (0.02) | (0.02) | (0.02) |
| BreachWindow | –0.08* | –0.09*** | –0.08*** |
| | (0.04) | (0.02) | (0.02) |
| $R^2$ | 0.01 | 0.01 | 0.02 |
| Adj. $R^2$ | 0.01 | 0.01 | 0.01 |
| Num. obs. | 3030 | 3030 | 3030 |

$^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$

**TABLE 3** Lag and breach coefficients for 0, 1, and 2 day event windows. The dependent variable is daily Tether returns. Five lags of returns and a breach dummy variable are included as regressors (Equation 9). The breach dummy equals one for days within the specified window around a recorded breach, and zero otherwise. The sample covers January 2017 through May 2025 (3,030 daily observations). Standard errors are in parentheses. $^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$.

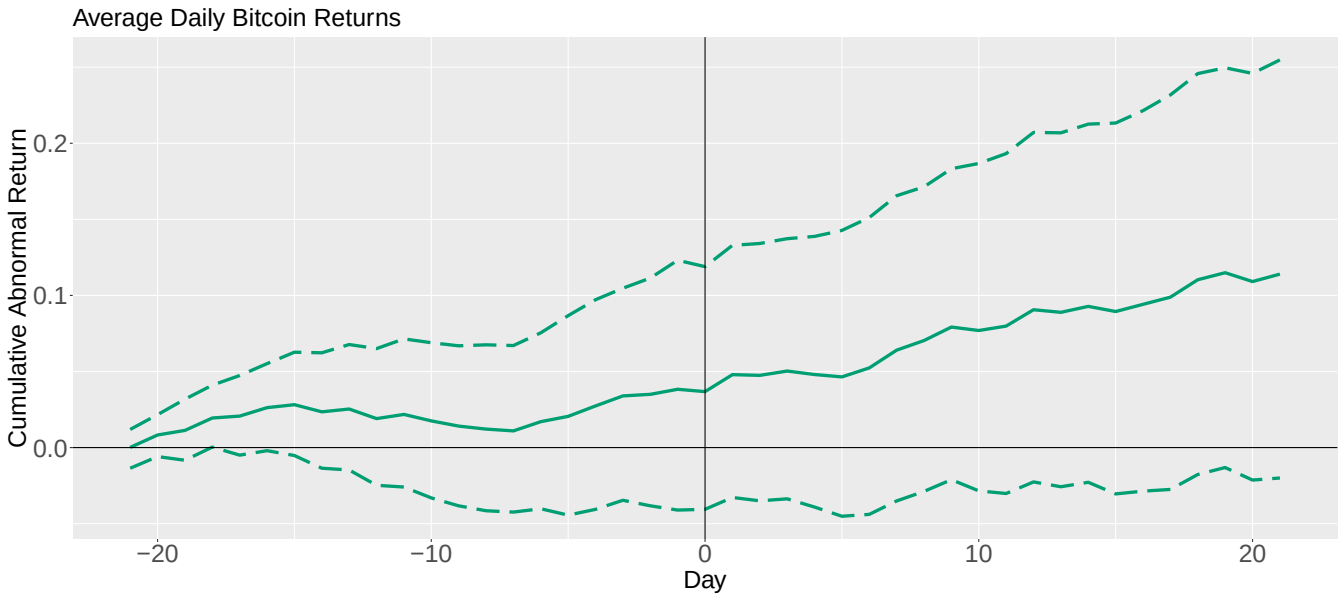


**FIGURE 7** Event study plot of the bitcoin daily returns. The event window is the same 21 day window before and after, however the expected value is based on a 21-day estimation window.

Figure 7. Where Tether experiences a sudden drop in cumulative returns, the response by bitcoin is indiscernible, hovering around zero for the entire event window.

One drawback of using aggregate data is the inability to isolate individual prices. While the aggregate Tether price we use in this work is the Tether/USD price, the majority of exchanges do not allow fiat currencies to be used directly, as this opens up the exchange to regulatory oversight and requires the exchange to follow strict "Know Your Customer" (KYC) and "Anti-Money Laundering" (AML) rules. As a result, the price of Tether as reported by aggregate websites is a mixture of fiat-permitting exchanges and converted prices from cryptocurrency pairs. Therefore, when an exchange which does not permit Tether/USD pairs reports a decrease in Tether returns, it could represent either (1) the price of Tether deviating from $1, or

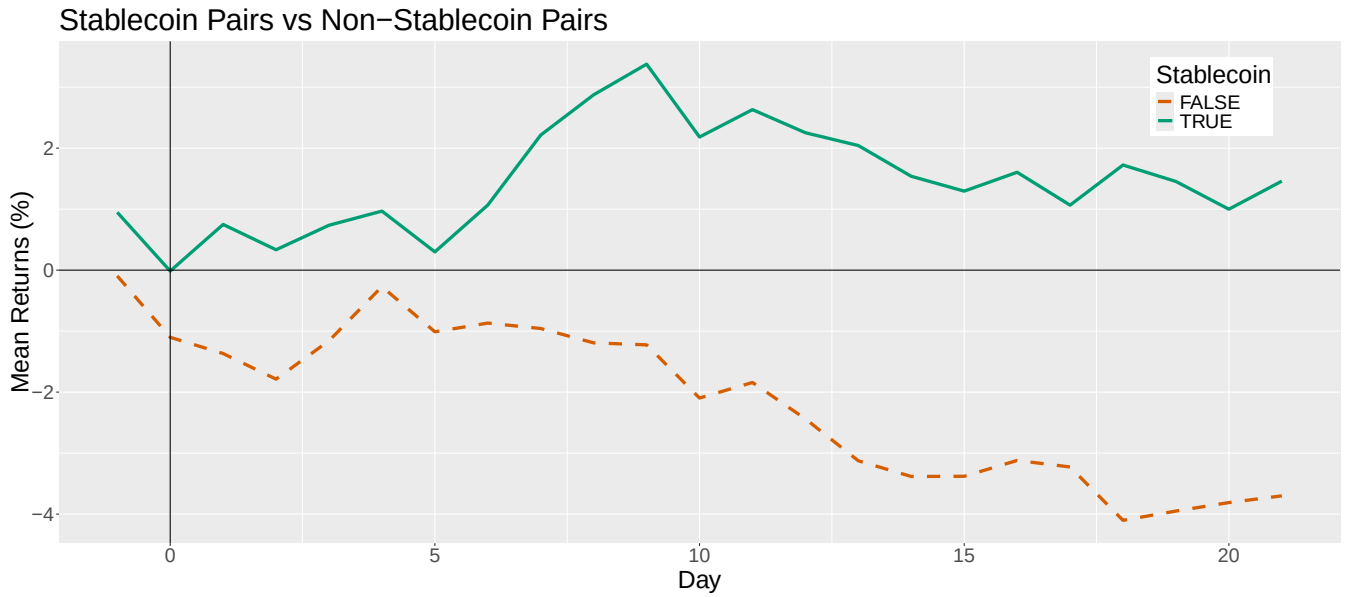


**FIGURE 8** Binance stablecoin (green solid) vs non-stablecoin (orange dashed) mean abnormal return following security shocks.

(2) the other, non-USD, asset changing in value. It is not unreasonable to assume a security breach may increase demand for popular cryptocurrencies such as Bitcoin or Ether, pushing those prices up while Tether remains stable.

To explore this possibility, we use five-minute data from a single exchange, Binance, to compare returns of stablecoin and non-stablecoin pairs surrounding these events. We use six trade pairs: Bitcoin/Tether, Ether/Tether, Bitcoin/Ether, XRP/Bitcoin, XRP/Ether, and XRP/Tether. Three of these pairs use Tether, while the other three are direct swaps between non-Tether cryptocurrencies. For each pair we conduct an event study using a 21-day estimation window of average returns to use as our expected returns. We then group the abnormal returns into stablecoin pairs and non-stablecoin pairs and calculate the average abnormal returns. The results of these event studies, which can be seen in Figure 8, reveal a noticeable difference in return behavior following breaches. Stablecoin pair returns increase more than 3% on average within the first 10 days, while non-stablecoin pairs trend downward for up to three weeks. The observed behavior can be explained by the value of Tether decreasing following a shock event, which aligns with our previous findings. Another explanation for this behavior is that non-stablecoin assets are simultaneously increasing in value at nearly identical rates following breaches. While existing research does reveal possible correlation between some of the most popular cryptocurrency returns (Blau, Griffith, & Whitby, 2020), (Katsiampa, 2019), rarely is the correlation coefficient one. For example, (Blau et al., 2020) find a statistically significant positive correlation between Ether and Bitcoin returns, yet the coefficient is 0.59, not 1. The same can be said for XRP (titled "Ripple" in the literature), with a coefficient of 0.46.

We believe these results offer strong evidence that our first hypothesis is true, and Tether does suffer a deviation from the peg due to a flight-to-safety response from market participants following periods of extreme uncertainty. However, up to this point we have seen strong evidence that the market is maturing and these deviations are lessening in magnitude over time. As such, we move on to our second hypothesis which investigates the applicability of the AMH to cryptocurrency markets.

## 6.2 | Survivability analysis

One implication of AMH states that "survivability" is the only thing that matters. To this end, we develop a unique proxy variable to gauge market reactions to "survivability shocks." Specifically, we argue that security breaches of a cryptocurrency exchanges in which market participants lose money are a particularly salient event. Because there is no FDIC or SPIC insurance, security breaches of cryptocurrency exchanges directly impact the extent to which a market participant survives. As such, a market that is in its infancy may "overreact" to security breaches on exchanges as market participants assess and update their survivability probability. From Figure 4 we observe an apparent decreasing trend in the impact of breaches on the deviation of

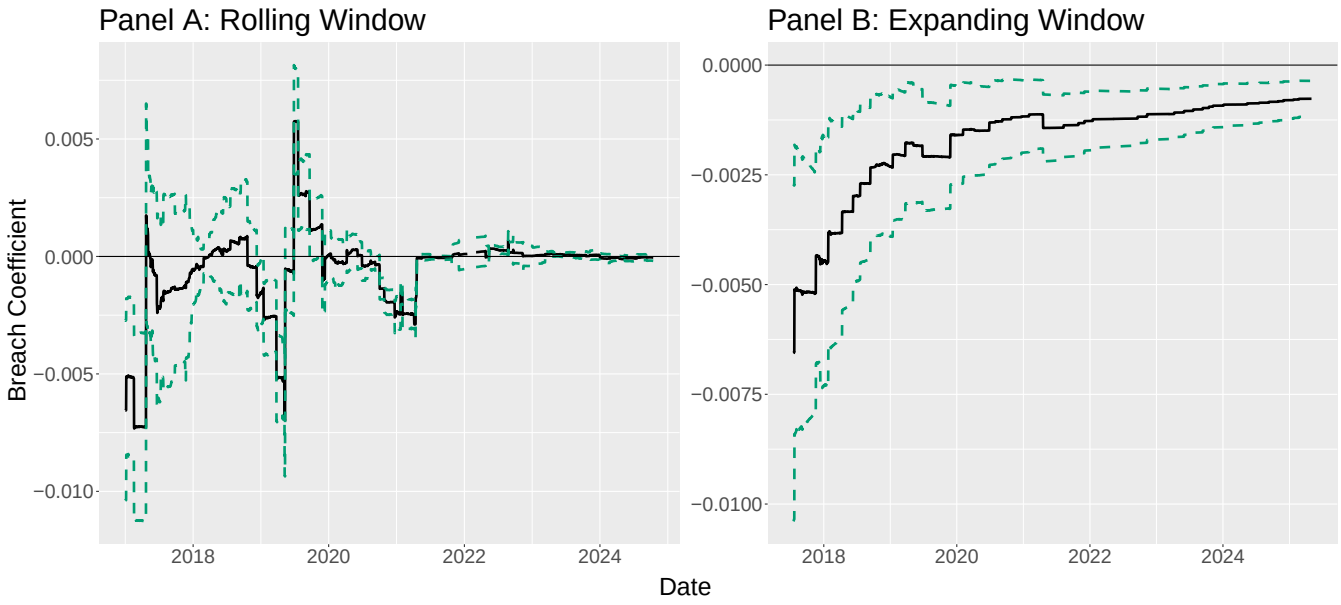


**FIGURE 9** Survivability shocks on Tether deviations from $1.

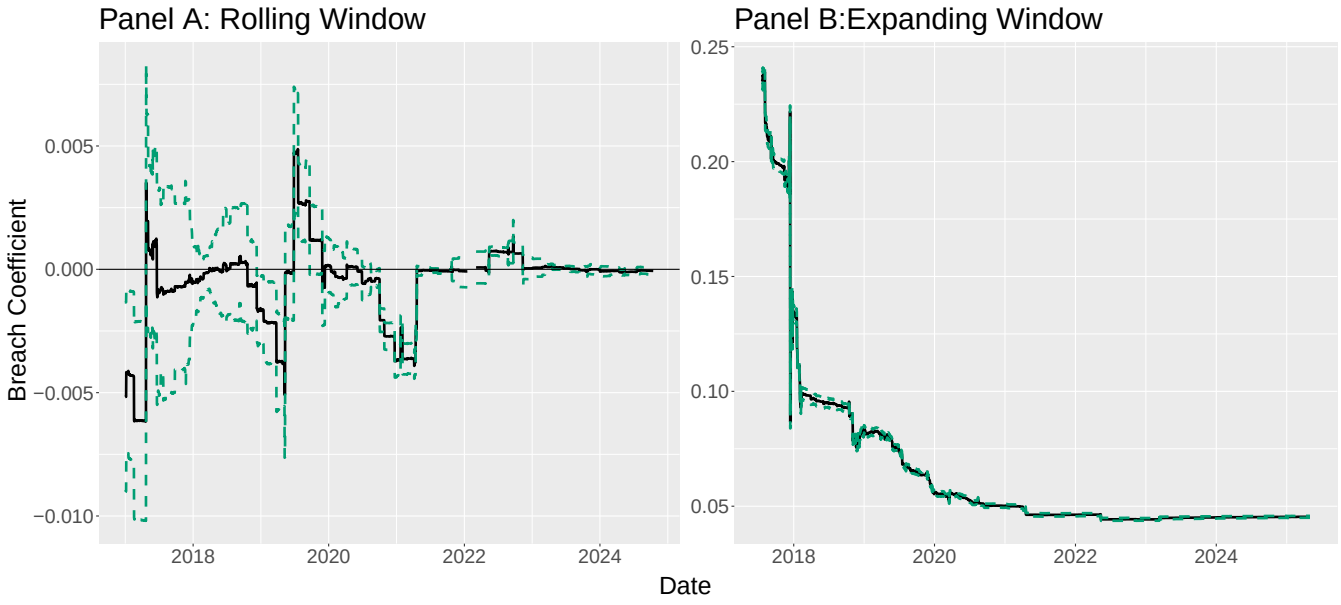


**FIGURE 10** Survivability shocks on Tether returns.

Tether's peg. While the event study confirms the destabilizing impact of these breaches, it could be the case that this impact has been diminishing over time. To this end, we perform a survivability analysis to identify this effect over time.

The time series regression defined in Equation 9 incorporates the breaches to estimate the Tether returns for our entire sample period. Since we are now interested in how a breach may influence returns differently over time, we re-estimate these time series regressions using the same rolling 200-day window technique from Section 5. That is, we estimate a new regression for every 200-day window across our dataset, and track the coefficient of the dummy variable related to breaches. Figure 9 shows the breach coefficient, and one standard deviation for the rolling window of peg deviations in Panel A. In the early rolling windows, the breach coefficient is relatively large, especially compared to the windows beginning in mid 2021. To better observe this pattern, we modify the 200-day rolling window to be an expanding window, that is, the breach coefficient on any day is the cumulative effect of breaches for every day preceding it. Panel B for Figure 9 displays the breach coefficient associated with

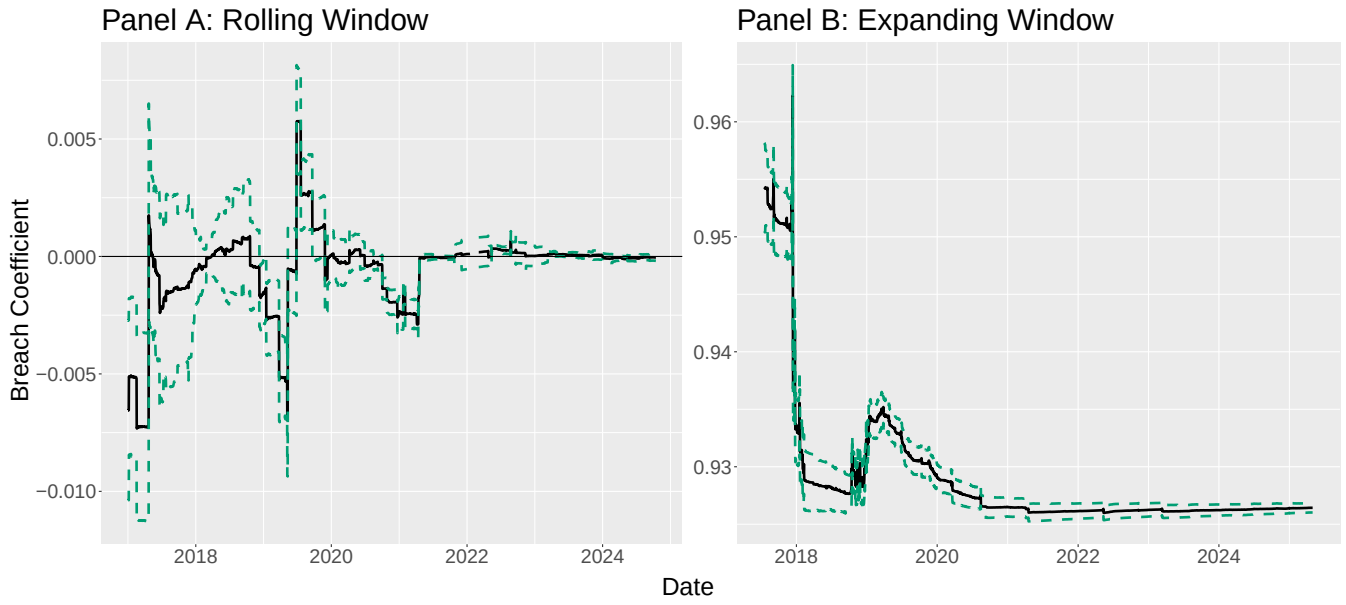


**FIGURE 11** Survivability shocks on Tether prices.

this expanding window for Tether price deviations. From this panel we see a converging behavior toward breaches having a zero coefficient over time.

Plots for the Tether price and returns can be seen in Figures 10 and 11, which show the same converging trend. These patterns show that "survivability shocks" (breaches) have an attenuating effect on Tether prices, Tether returns and Tether deviations. Specifically, a security breach at the beginning part of our sample from 2017 to early 2019 causes up to a half-cent (0.5%) deviation of Tether from its peg whereas that effect goes to zero by the beginning of 2021. We believe that these results are consistent with Los (2004) AMH, and confirm our second hypothesis. That is, in a market that is developing, the effect of survivability shocks will have an attenuating affect as (1) market participants learn and (2) more participants of different species enter the market. These findings map directly onto the four practical implications of Lo's (2004) AMH. First, the rolling autocorrelation of deviations (Figure 3) varies substantially over time (ranging from 0.18 to 1.64), confirming that the risk-reward relationship for arbitrageurs is not constant but evolves with market conditions. Second, our event study results demonstrate that breaches create transient arbitrage opportunities—buying discounted Tether—that have diminished over time as more arbitrageurs entered the market (Figures 9–11). Third, the attenuation of breach effects implies that trading strategies exploiting post-breach deviations would have been profitable in 2017–2019 but substantially less so in recent years, consistent with Lo's prediction that strategy profitability depends on the competitive environment. Fourth, and most directly, we frame security breaches as "survivability shocks" that threaten market participants' funds. In the early, immature market, these shocks caused panic and large deviations; as the ecosystem developed survival mechanisms—insurance funds, proof of reserves, regulatory settlements—the market's reaction became more muted, exactly as the AMH predicts for an adapting population.

## 7 | CONCLUSION

Recent turmoil in the traditional finance sector has resulted in a number of bank failures, including Silicon Valley Bank. The collapse of Silicon Valley Bank had a particularly significant impact on the cryptocurrency ecosystem due to the second most popular USD pegged stablecoin, USD Coin (USDC), using it for part of their reserves backing(Reuters, 2023). The issuer of USDC, Circle, touted transparency as one of the primary benefits of using USDC over other, more opaque stablecoin issuers. However, following the Silicon Valley Bank collapse, the USDC peg fell to 88 cents. During the same time, Tether began trading at a 2.5 cent premium, possibly resulting from an influx of USDC holders abandoning the suddenly volatile stablecoin. This desire to hold Tether, a much less transparent and at times proven to be partially unbacked(De, 2021), is somewhat surprising.

It is possible that this could be due to the widespread adoption and market capitalization of Tether (nearly three times that of USDC), or perhaps a perception of safety in the absence of apparent contagion risk due to opaque backing.

When detached from the greater cryptocurrency market, Tether is a deceptively simple construct. Tokens are issued on a 1:1 basis from fiat deposits held by the issuer, and the token holder can redeem those tokens at will, gaining back the fiat used to initially acquire the tokens. By definition, Tether should experience a constant rate of return of zero, and any deviation from its peg should be instantly arbitraged away. As we observe in this paper, this is not always the case. Several high-profile breach events at cryptocurrency exchanges result in acute shifts to Tethers returns and deviations. However, over time this effect appears to be diminishing.

We perform an event study of 44 exchange breaches showing sudden, short-lived deviations from the $1 peg. As cryptocurrency exchange users react to the perceived threat of losing their funds Tether is traded at a discounted rate for up to 21 days after a breach. The floating exchange rate eventually returns to its peg as users return to normal trading activity. As the market has matured, and more exchanges have adopted Tether as an integral part of their operations, this effect has diminished. We perform time-series regressions of Tether's price, returns, and deviations, and note a marginally significant effect of these breaches on prices and deviations, with a statistically significant effect on returns. By modifying these regressions to incorporate rolling and expanding windows, we observe an attenuating effect of breaches over time. Earlier exchange breaches inflicted large and persistent deviations. As the ecology changed and modifications were made, such as proof of reserves and "insurance funds", these shocks have had less of an impact. These behaviors lend themselves well to the expectations and implications from the AMH. That is, each of these ecologically modifying events guide the species, and overall market, towards a more survivable state. Our findings carry implications for the ongoing policy debate surrounding stablecoin regulation. The recently passed GENIUS Act establishes a regulatory framework for fiat-backed stablecoins, reflecting policymakers' concerns about run risk and potential contagion effects across decentralized and traditional financial markets. Our results suggest several considerations for this framework. First, the floating exchange rate mechanism employed by Tether appears to absorb shocks that might otherwise trigger destabilizing redemption runs. Unlike traditional money market funds that "break the buck" catastrophically when redemptions are suspended, Tether's market-determined price allows temporary discounts that arbitrageurs then correct. Second, regulatory interventions (including the 2021 New York Attorney General settlement, CFTC ruling, and subsequent reserve transparency requirements) coincided with a reduction in peg deviations and faster mean reversion following shocks. This suggests that transparency mandates and regulatory oversight can meaningfully improve stablecoin stability without requiring deposit insurance or lender-of-last-resort guarantees. Finally, policymakers should recognize that fiat-backed stablecoins like Tether operate fundamentally differently from algorithmic stablecoins, which lack reserve backing and have proven far more fragile. Regulatory frameworks that fail to distinguish between these categories risk either over-regulating relatively stable instruments or under-regulating genuinely risky ones.

## ACKNOWLEDGMENTS

We gratefully acknowledge support from the US National Science Foundation Award No. 1714291.

## References

*The aftermath of Axie Infinitys $650M Ronin Bridge hack.* (2022, April). Retrieved 2023-08-23, from https://cointelegraph.com/news/the-aftermath-of-axie-infinity-s-650m-ronin-bridge-hack

Anadu, K., Azar, P., Cipriani, M., Eisenbach, T. M., Huang, C., Landoni, M., … Wang, J. C. (2023, August). *Runs and Flights to Safety: Are Stablecoins the New Money Market Funds?* [SSRN Scholarly Paper]. Rochester, NY: Social Science Research Network. Retrieved 2025-06-12, from https://papers.ssrn.com/abstract=4594064

Antonakakis, N., Chatziantoniou, I., & Gabauer, D. (2019). *Cryptocurrency market contagion: Market uncertainty, market complexity, and dynamic portfolios | Elsevier Enhanced Reader.* doi: 10.1016/j.intfin.2019.02.003

Bartoletti, M., Lande, S., Loddo, A., Pompianu, L., & Serusi, S. (2021). Cryptocurrency scams: analysis and perspectives. *IEEE Access*, *9*, 148353–148373.

Binance. (2025). *Binance exchange.* https://www.binance.com.

*Binance Partners With Circle to Push USDC Stablecoin Adoption Across the Globe.* (2024, December). Retrieved 2025-06-14, from https://www.coindesk.com/business/2024/12/10/binance-partners-with-circle-to

-push-usdc-stablecoin-adoption-across-the-globe

Bitfinex. (2021). *Bitfinex withdrawal fees.* https://www.bitfinex.com/fees/#withdrawal-table.

*Bitfinex's Biggest Critic Is Back on Twitter.* (2018, February). Retrieved 2023-05-03, from https://www.coindesk.com/markets/2018/02/08/bitfinexs-biggest-critic-is-back-on-twitter/ Section: Markets.

Blau, B., Griffith, T., & Whitby, R. (2020, February). Comovement in the Cryptocurrency Market. *Economics Bulletin*, *40*(1), 1–9. Retrieved from https://digitalcommons.usu.edu/econ_facpubs/944

Böhme, R., Eckey, L., Moore, T., Narula, N., Ruffing, T., & Zohar, A. (2020). Responsible vulnerability disclosure in cryptocurrencies. *Communications of the ACM*, *63*(10), 62–71. Retrieved from https://tylermoore.utulsa.edu/cacm20cryptovuln.pdf

Brown, M., Trautmann, S. T., & Vlahu, R. (2016, April). Understanding Bank-Run Contagion. *Management Science*. Retrieved 2023-04-21, from https://pubsonline.informs.org/doi/abs/10.1287/mnsc.2015.2416 Publisher: INFORMS. doi: 10.1287/mnsc.2015.2416

Browne, R. (2021, February). *Cryptocurrency firms Tether and Bitfinex agree to pay $18.5 million fine to end New York probe.* Retrieved 2023-05-03, from https://www.cnbc.com/2021/02/23/tether-bitfinex-reach-settlement-with-new-york-attorney-general

Chen, Y.-L., Chang, Y. T., & Yang, J. J. (2023, None). Cryptocurrency hacking incidents and the price dynamics of bitcoin spot and futures. *Finance Research Letters*, *55*(PB), None. Retrieved from https://ideas.repec.org/a/eee/finlet/v55y2023ipbs1544612323003276.html doi: 10.1016/j.frl.2023.103955

Chohan, U. W. (2019). Are Stable Coins Stable? *SSRN Electronic Journal*. Retrieved 2023-05-03, from https://www.ssrn.com/abstract=3326823 doi: 10.2139/ssrn.3326823

Coingecko. (2025). *Coingecko tether.* https://www.coingecko.com/en/coins/tether.

CoinMarketCap. (2021). *Coinmarketcap stablecoins.* https://coinmarketcap.com/view/stablecoin/.

Coinmarketcap. (2025). *Coinmarketcap support.* https://support.coinmarketcap.com/hc/en-us/articles/360043395752-Price-Market-Pair-Cryptoasset.

Corbet, S., Larkin, C., Lucey, B., Meegan, A., & Yarovaya, L. (2020, February). Cryptocurrency reaction to FOMC Announcements: Evidence of heterogeneity based on blockchain stack position. *Journal of Financial Stability*, *46*, 100706. Retrieved 2025-06-12, from https://www.sciencedirect.com/science/article/pii/S1572308919306576 doi: 10.1016/j.jfs.2019.100706

*Crypto Exchange Kraken Agrees to Buy Futures Platform NinjaTrader for $1.5B.* (2025, March). Retrieved 2025-06-14, from https://www.coindesk.com/business/2025/03/20/kraken-buys-ninjatrader-for-usd1-5b-to-enter-u-s-crypto-futures-market

*Crypto Exchanges Huobi, Poloniex to Form 'Strategic Partnership'.* (2023, May). Retrieved 2025-06-14, from https://www.coindesk.com/business/2022/11/30/crypto-exchanges-huobi-poloniex-to-form-strategic-partnership

De, N. (2021, February). *NY AGs $850M Probe of Bitfinex, Tether Ends in an $18.5M Settlement.* Retrieved 2023-04-09, from https://www.coindesk.com/markets/2021/02/23/ny-ags-850m-probe-of-bitfinex-tether-ends-in-an-185m-settlement/ Section: Markets.

Faife, C. (2022, February). *Wormhole cryptocurrency platform hacked for $325 million after error on GitHub.* Retrieved 2023-08-23, from https://www.theverge.com/2022/2/3/22916111/wormhole-hack-github-error-325-million-theft-ethereum-solana

Fama, E. F. (1991). Efficient Capital Markets: II. *The Journal of Finance*, *46*(5), 1575–1617. Retrieved 2024-01-16, from https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1540-6261.1991.tb04636.x _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1540-6261.1991.tb04636.x. doi: 10.1111/j.1540-6261.1991.tb04636.x

Feder, A., Gandal, N., Hamrick, J. T., & Moore, T. (2017, June). The impact of DDoS and other security shocks on Bitcoin currency exchanges: evidence from Mt. Gox. *Journal of Cybersecurity*, *3*(2), 137–144. doi: 10.1093/cybsec/tyx012

Ferreira, P., & Pereira, E. (2019, September). Contagion Effect in Cryptocurrency Market. *Journal of Risk and Financial Management*, *12*(3), 115. Retrieved 2023-05-03, from https://www.mdpi.com/1911-8074/12/3/115 Number: 3 Publisher: Multidisciplinary Digital Publishing Institute. doi: 10.3390/jrfm12030115

FTX. (2021). *Ftx withdrawal fees.* https://help.ftx.com/hc/en-us/articles/360043023772-Depositing-Withdrawing-Fiat-.

Gandal, N., Hamrick, J., Moore, T., & Oberman, T. (2018, May). Price manipulation in the Bitcoin ecosystem. *Journal of Monetary Economics*, *95*, 86–96. doi: 10.1016/j.jmoneco.2017.12.004

Griffin, J. M., & Shams, A. (2020). Is Bitcoin Really Untethered? *The Journal of Finance*, *75*(4), 1913–1964. Retrieved 2023-04-21, from https://onlinelibrary.wiley.com/doi/abs/10.1111/jofi.12903 doi: 10.1111/jofi.12903

Grobys, K., & Huynh, T. L. D. (2022, June). When Tether says JUMP! Bitcoin asks How low?. *Finance Research Letters*, *47*, 102644. Retrieved 2025-06-12, from https://www.sciencedirect.com/science/article/pii/S1544612321005778 doi: 10.1016/j.frl.2021.102644

Hairudin, A., & Mohamad, A. (2024). The isotropy of cryptocurrency volatility. *International Journal of Finance & Economics*, *29*(3), 3779–3810. Retrieved 2025-06-12, from https://onlinelibrary.wiley.com/doi/abs/10.1002/ijfe.2857 _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/ijfe.2857. doi: 10.1002/ijfe.2857

Hoang, L. T., & Baur, D. G. (2024). How stable are stablecoins? *The European Journal of Finance*, *30*(16), 1984–2000. https://doi.org/10.1080/1351847X.2021.1949369. doi: 10.1080/1351847X.2021.1949369

Katsiampa, P. (2019, September). Volatility co-movement between Bitcoin and Ether. *Finance Research Letters*, *30*, 221–227. Retrieved 2025-06-20, from https://linkinghub.elsevier.com/retrieve/pii/S1544612318305580 doi: 10.1016/j.frl.2018.10.005

Kraken. (2021). *Kraken withdrawal limits.* https://support.kraken.com.

Li, Z., Zhou, M., & Cavusoglu, H. (2025). The Impact of Blockchain Security Breaches on Crypto Token Valuation.. Retrieved 2025-09-15, from https://hdl.handle.net/10125/109317 doi: 10.24251/HICSS.2025.473

Lo, A. W. (2004, October). *The Adaptive Markets Hypothesis: Market Efficiency from an Evolutionary Perspective* [SSRN Scholarly Paper]. Rochester, NY: Social Science Research Network. Retrieved 2025-06-15, from https://papers.ssrn.com/abstract=602222

Lyons, R. K., & Viswanath-Natraj, G. (2023, March). What keeps stablecoins stable? *Journal of International Money and Finance*, *131*, 102777. Retrieved 2025-06-11, from https://www.sciencedirect.com/science/article/pii/S0261560622001802 doi: 10.1016/j.jimonfin.2022.102777

MacKinlay, A. C. (1997). Event Studies in Economics and Finance. *Journal of Economic Literature*, *35*(1), 13–39. Retrieved 2023-04-21, from https://www.jstor.org/stable/2729691 Publisher: American Economic Association.

Moore, T., & Christin, N. (2013). Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. In *Financial Cryptography and Data Security* (Vol. 7859, pp. 25–33). Berlin, Heidelberg: Springer Berlin Heidelberg. Retrieved 2023-04-10, from http://link.springer.com/10.1007/978-3-642-39884-1_3 Series Title: Lecture Notes in Computer Science. doi: 10.1007/978-3-642-39884-1_3

Moore, T., Christin, N., & Szurdi, J. (2018, September). Revisiting the Risks of Bitcoin Currency Exchange Closure. *ACM Transactions on Internet Technology*, *18*(4), 50:1–50:18. Retrieved 2023-04-10, from https://dl.acm.org/doi/10.1145/3155808 doi: 10.1145/3155808

Oosthoek, K., & Doerr, C. (2020, May). From Hodl to Heist: Analysis of Cyber Security Threats to Bitcoin Exchanges. In *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 1–9). doi: 10.1109/ICBC48266.2020.9169412

Passeri, P. (2023). *Hackmageddon Database.* Retrieved from https://www.hackmageddon.com

Prentice, C., & Prentice, C. (2021, October). Crypto firms Tether, Bitfinex to pay $42.5 mln to settle U.S. CFTC charges. *Reuters*. Retrieved 2026-01-23, from https://www.reuters.com/technology/tether-bitfinex-agree-pay-425-mln-fines-settle-us-cftc-charges-2021-10-15/

Reuters. (2023, March). *Stablecoin USDC breaks dollar peg after revealing $3.3 billion Silicon Valley Bank exposure | CNN Business.* Retrieved 2023-05-05, from https://www.cnn.com/2023/03/11/business/stablecoin-circle-silicon-valley-bank/index.html

Sen. Hagerty, B. R.-T. (2025, February). *Text - S.394 - 119th Congress (2025-2026): GENIUS Act of 2025* [legislation]. Retrieved 2025-06-20, from https://www.congress.gov/bill/119th-congress/senate-bill/394/text Archive Location: 2025-02-04.

Shao, E., & Rajapaksa, D. (2025, February). *On the Relationship between Tether and Other Cryptocurrencies* [SSRN Scholarly Paper]. Rochester, NY: Social Science Research Network. Retrieved 2025-06-12, from https://papers.ssrn.com/abstract=4906933

Siu, G. A., Hutchings, A., Vasek, M., & Moore, T. (2022). invest in crypto!: An analysis of investment scam advertisements found in Bitcointalk. In *Proceedings of the apwg symposium on electronic crime research (ecrime).* IEEE.

Stempel, J. (2021, February). Bitfinex, Tether owner pays $18.5 mln fine to settle NYAG cryptocurrency cover-up charges. *Reuters*. Retrieved 2026-01-23, from https://www.reuters.com/world/americas/bitfinex-tether-owner-pays-185-mln-fine-settle-nyag-cryptocurrency-cover-up-2021-02-23/

Tsihitas, T. (2019, June). *The Biggest Cryptocurrency Heists of All Time.* Retrieved 2023-09-20, from comparitech.com/crypto/biggest-cryptocurrency-heists/

Vasek, M. (2019). *BitcoinTalk Security Events.* Retrieved from https://www.dropbox.com/s/7xw2lzov8hjrrcb/securityEvents.csv?dl=0

Vasek, M., Thornton, M., & Moore, T. (2014). Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem. In R. Böhme, M. Brenner, T. Moore, & M. Smith (Eds.), *Financial Cryptography and Data Security* (pp. 57–71). Berlin, Heidelberg: Springer. doi: 10.1007/978-3-662-44774-1_5

Wajdi, M., Nadia, B., & Ines, G. (2020). Asymmetric effect and dynamic relationships over the cryptocurrencies market. *Computers & Security*, *96*, 101860. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404820301322 doi: https://doi.org/10.1016/j.cose.2020.101860

Wei, W. C. (2018, October). The impact of Tether grants on Bitcoin. *Economics Letters*, *171*, 19–22. Retrieved 2025-06-12, from https://www.sciencedirect.com/science/article/pii/S0165176518302556 doi: 10.1016/j.econlet.2018.07.001

□

## APPENDIX

# A SECURITY SHOCK EVENTS

| Date | Source | Exchange | Date | Source | Exchange |
|---|---|---|---|---|---|
| 2017-02-16 | (Passeri, 2023) | zcoin | 2021-08-10 | New | polynetwork |
| 2017-04-22 | (Passeri, 2023) | yapizon | 2021-08-19 | New | liquid |
| 2017-06-19 | (Passeri, 2023) | bithumb | 2021-10-30 | New | bxh |
| 2017-07-24 | (Passeri, 2023) | veritaseum | 2021-12-02 | New | badger |
| 2017-11-19 | (Passeri, 2023) | Tether | 2021-12-04 | New | bitmart |
| 2017-12-06 | (Passeri, 2023) | nicehash | 2021-12-11 | New | ascendex |
| 2018-01-26 | (Passeri, 2023) | coincheck | 2021-12-13 | New | vulcanforged |
| 2018-02-10 | (Passeri, 2023) | bitgrail | 2022-01-17 | New | cryptodotcom |
| 2018-04-12 | (Passeri, 2023) | coinsecure | 2022-09-20 | New | wintermute |
| 2018-06-11 | (Passeri, 2023) | coinrail | 2022-11-11 | New | ftx |
| 2018-06-20 | (Passeri, 2023) | bithumb | 2023-04-09 | New | gdac |
| 2018-07-20 | (Passeri, 2023) | livecoin | 2023-04-14 | New | bitrue |
| 2018-09-14 | (Passeri, 2023) | zaif | 2023-06-02 | New | polynetwork |
| 2018-10-01 | (Oosthoek & Doerr, 2020) | maplechange | 2023-07-22 | New | coinspaid |
| 2019-01-15 | New | cryptopia | 2023-09-12 | New | coinex |
| 2019-01-26 | New | localbitcoins | 2023-09-14 | New | remitano |
| 2019-03-25 | (Vasek, 2019) | dragonex | 2023-09-25 | New | huobi |
| 2019-03-29 | New | bithumb | 2023-10-17 | New | coinsph |
| 2019-05-08 | (Vasek, 2019) | binance | 2023-11-08 | New | coinspot |
| 2019-06-27 | (Vasek, 2019) | bitrue | 2023-11-10 | New | poloniex |
| 2019-07-11 | (Oosthoek & Doerr, 2020) | bitpoint | 2023-11-22 | New | huobi/htx |
| 2019-11-27 | New | upbit | 2024-01-05 | New | coinspaid |
| 2020-02-05 | New | altsbit | 2024-05-13 | New | rain |
| 2020-04-07 | New | bisq | 2024-05-31 | New | dmm bitcoin |
| 2020-04-19 | New | dforce | 2024-06-06 | New | Lykke |
| 2020-06-28 | New | balancer | 2024-06-19 | New | kraken |
| 2020-07-31 | New | 2gether | 2024-06-22 | New | btcturk |
| 2020-09-07 | New | eterbase | 2024-07-18 | New | wazirx |
| 2020-09-26 | New | kucoin | 2024-09-10 | New | indodax |
| 2020-10-26 | New | harvest | 2024-09-20 | New | bingx |
| 2020-11-12 | New | akropolis | 2024-10-31 | New | m2 |
| 2020-12-21 | New | exmo | 2024-11-28 | New | xt |
| 2021-02-01 | New | cryptopia | 2025-01-23 | New | phemex |
| 2021-04-19 | New | easyfi | 2025-02-21 | New | bybit |

**TABLE** A1 List of all security shock events. Those shaded gray are included in the event studies, while the non-shaded were omitted to avoid overlapping estimation windows.

# B GENERAL TETHER BEHAVIOR

Panel A: Daily Tether Returns

$$r_{wt} = \alpha_{0w} + \alpha_{1w} r_{t-1} + \epsilon_{tw}$$

| Coefficient | Average | Std. Error | Min | Max |
|---|---|---|---|---|
| $a_0$ | 0.00 | 0.00 | -0.0003 | 0.0005 |
| $a_1$ | -0.06 | 0.004 | -0.72 | 1.41 |
| $r^2$ | 0.04 | 0.001 | 0.00 | 0.40 |

Panel B: Daily Tether Deviations from its $1 peg

$$deviation_{wt} = c_{0w} + c_{1w} deviation_{t-1} + \tau_{tw}$$

| Coefficient | Average | Std. Error | Min | Max |
|---|---|---|---|---|
| $c_0$ | 0.00 | 0.00 | -0.0003 | 0.002 |
| $c_1$ | 0.76 | 0.003 | 0.18 | 1.64 |
| $r^2$ | 0.61 | 0.004 | 0.012 | 0.93 |

**TABLE B2** Time-series regressions on Tether returns and deviations from $1

.

**TABLE** B3 Annual summary statistics for Tether prices, returns, and deviations from the $1 peg. The sample covers daily observations from January 2017 through May 2025. Prices are reported from Coinmarketcap.com. Returns are computed as the first difference of natural logarithms. Deviations are defined as the difference between the reported price and $1.

| | Price | | Return | | Deviation | |
|---|---|---|---|---|---|---|
| Year | Average | Median | Average | Median | Average | Median |
| 2017 | 1.0002 | 1.0001 | 0.0049 | –0.0000 | 0.0002 | 0.0001 |
| 2018 | 1.0002 | 1.0005 | 0.0028 | –0.0039 | 0.0002 | 0.0005 |
| 2019 | 1.0052 | 1.0045 | –0.0035 | –0.0083 | 0.0052 | 0.0045 |
| 2020 | 1.0012 | 1.0010 | –0.0012 | 0.0015 | 0.0012 | 0.0010 |
| 2021 | 1.0005 | 1.0004 | 0.0001 | –0.0000 | 0.0005 | 0.0004 |
| 2022 | 0.9999 | 1.0001 | –0.0002 | 0.0007 | –0.0001 | 0.0001 |
| 2023 | 1.0002 | 1.0002 | 0.0000 | –0.0002 | 0.0002 | 0.0002 |
| 2024 | 1.0000 | 1.0000 | –0.0004 | –0.0009 | –0.0000 | 0.0000 |
| 2025 | 0.9998 | 0.9999 | 0.0016 | –0.0012 | –0.0002 | –0.0001 |