Breaking the Stablecoin Buck: Measuring the Impact of Security Breach and Liquidation Shocks

Andrew Morin
School of Cyber Studies &
Tandy School of Computer Science
The University of Tulsa
Tulsa, Oklahoma 74104
Email: anm1198@utulsa.edu

Tyler Moore
School of Cyber Studies &
Tandy School of Computer Science
The University of Tulsa
Tulsa, Oklahoma 74104
Email: tyler-moore@utulsa.edu

Eric Olson
School of Cyber Studies &
School of Finance & Operations Management
The University of Tulsa
Tulsa, Oklahoma 74104
Email: eric-olson@utulsa.edu

Abstract—**Cryptocurrencies have exploded in popularity, due in no small part to the rising value of Bitcoin. Yet much of their success relies upon stablecoins maintaining a consistent value pegged to fiat currencies like the US dollar. Customers of cryptocurrency exchanges regularly trade between these stablecoins and their more volatile counterparts. These exchanges operate like banks and Money Market Mutual Funds (MMMFs), but without the regulatory oversight or consumer protections to mitigate run risk. This paper investigates whether two types of shocks – security breaches at exchanges and derivative liquidations prompted by price volatility – can break the peg of Tether, the leading stablecoin. Using an event study, we find that both types of shocks are associated with a break in the Tether's peg to the dollar but return relatively quickly to its par value. The cumulative effect of a security breach is approximately -0.5%. We conclude that by permitting the stablecoin price to float (rather than having the price fixed to $1 as in MMMFs), exchanges have mitigated some of the financial contagion risk associated with panic-runs thus far.**

Index Terms—**Cryptocurrency, Tether, Stablecoin, Liquidation, Breach**

I. Introduction

Stablecoins are cryptocurrencies that are designed to maintain their peg to a particular fiat currency, a basket of fiat currencies, or a digital asset. The three largest stablecoins by volume are Tether, Binance USD and USDC, which have partnerships with three of the largest exchanges: Bitfinex, Binance and Coinbase (respectively). Mechanically, stablecoins are similar in spirit to Money Market Mutual Funds (MMMFs). However, one important difference between MMMFs and stablecoins is the fact that MMMFs do not issue debt claims. Shares in MMMFs are actually equity shares that are pegged to $1 whereas stablecoins issue debt claims pegged at $1. Runs on MMMFs could easily be avoided simply by allowing the dollar price of the equity shares of MMMFs to flucatuate. Moreover, MMMFs cannot become insolvent because the shares owned are actually equity claims. Stablecoins, on the other hand, are debt claims that are backed by a particular set of assets. Issuers of stablecoins can become insolvent if the value of their assets that back the stablecoins fall below the total amount of issued stablecoins. For example, as of March 31, 2021, the stablecoin Tether was backed by the following reserves: 75% of the reserves are in cash, cash equivalents and commercial paper. 12.5% are in secured loans, approximately 10% are in corporate bonds and precious metals and 1.6% are in other investments including digital tokens [1].

The run risk that Governor Brainard references is straightforward. If holders of Tether chose to redeem their Tether for dollars, the institution would have to liquidate their holdings of financial assets in Figure 1 at market prices and exchange dollars for those seeking to redeem their Tether. The systemic risk that Governor Brainard is likely worried about is the financial contagion that may result from fire sales of the assets spelled out in Figure 1. In such a scenario, if a large volume of Tether or other stablecoins were suddenly redeemed and triggered a fire sale of reserve assets, there is significant potential for negative spillover effects on the traditional financial sector given that they hold many of the same assets.

[2] Note that panic-based runs can be caused by a variety of factors including (1) the fundamentals of the financial institution, (2) the fundamentals of other financial institutions, (3) shocks to a set of particular asset prices, and (4) security events. However, of first order importance to the run's severity are customers' *beliefs* about whether other customers plan to withdraw their funds. On this basis, stablecoins appear to be at high risk for panic withdrawals given the volatility of cryptocurrencies and the unregulated nature of the exchanges. Moreover, the damage to the overall economy that results from financial contagion has been well documented for both the Great Depression ([3], [4], [5], [6]) and the more recent Great Recession ([7], [8]).

The systemic risk associated with bank runs have prompted government or government-sponsored entities to offer insurance to protect financial market participants. For example, the Federal Deposit Insurance Corporate (FDIC) was established by Congress in 1933 to insure bank deposits at member banks. Moreover, given the rise in the shadow banking system, the

The academic literature is vast on this subject. Google Scholar reports over 14,300 academic papers on financial crises and bank runs. The list here was certainly not intended to be exhaustive.

Workshop on the Economics of Information Security (WEIS) 2022, Tulsa, Oklahoma, USA, June 21–22, 2022

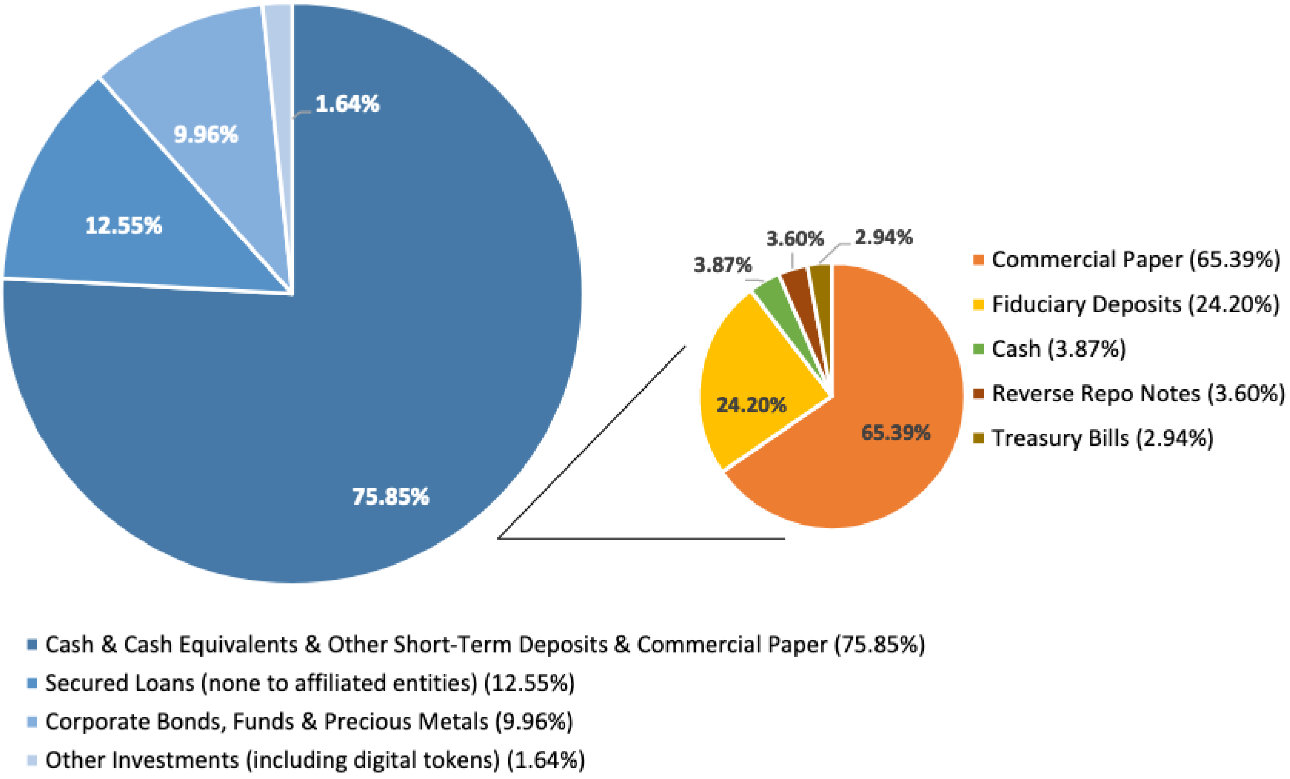


Fig. 1: Composition of Tether reserves [1].

Federal Reserve has acted extensively in its Lender of Last Resort (LoLR) function to mitigate run-risk for a range of financial institutions that experienced an unexpected surge of withdrawals. Moreover, the U.S. Treasury and Federal Reserve set up facilities to guarantee the liabilities of MMMFs to stop the redemptions in 2008 and 2020.

Cryptocurrencies and cryptocurrency exchanges, on the other hand, are not covered by any type of deposit or investor insurance. In fact, the Securities Investor Protection Corporation (SIPC) explicitly excludes fiat or cryptocurrency as an insured security. In most circumstances, customers deposit fiat or cryptocurrency into an account on the exchange but often the exchanges combine the deposits and invest the deposits in short term fiat-denominated assets (such as commercial paper, treasuries, etc.).

Many cryptocurrency traders prefer to use stablecoins rather than dollars because it allows them to (1) avoid US dollar regulations, and (2) avoid the ACH wire system which is substantially slower than transferring stablecoins between accounts. Moreover, nearly all of the derivative trading using cryptocurrencies is settled in a stablecoin rather than a fiat currency such as the dollar. As such, stablecoins like Tether have become the preferred currency choice for settlements of derivative contracts in the cryptocurrency ecosystem.

However, 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 Tether's 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. 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 [2], the fact that Tether articulates 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. For example, if a customer holds Tether but is not a registered user, they may be willing to sell the Tether below par value to another customer that is registered.

Our aim in this paper is twofold. First, we seek to examine how two types of shocks affect the Tether/USD stablecoin peg. In particular, we are interested in examining how (i) security breaches at cryptocurrency exchanges and (ii) Bitcoin price shocks affect the Tether/USD peg. To that end, as described in Section III, we have constructed a unique dataset of security breaches from multiple sources, as well a dataset on forced liquidations (essentially margin calls) of Bitcoin.

To preview our results, we find that security breaches and margin calls do in fact induce a break in the Tether/USD peg. However, the effect is short-lived and the price returns to parity rather quickly. For our events, we do not find any evidence that security events or large movements in the price of Bitcoin induce a run on stablecoins. Rather, we believe that because the USD price of Tether is freely floating on the exchanges rather than fixed at $1, arbitrageurs step in to stabilize the price. As such, while we certainly acknowledge the similarity in stablecoins to MMMFs (and the run risk referenced by Governor Brainard) in spirit, the structural feature of Tether that allows the price of Tether to fluctuate on different exchanges is a feature that likely reduces the risk of panic-induced withdrawals at the exchanges.

The rest of the paper proceeds as follows. Section II outlines the ecosystem while providing background on the structure of exchanges, wallets, stablecoins and derivatives; Section III describes our exchange security breach and liquidation datasets; Section IV describes our event study methodology and results, and Section V concludes.

II. The Cryptocurrency Ecosystem

We now describe the operation of the cryptocurrency ecosystem, with a particular emphasis on exchanges. We explain different ways cryptocurrency can be stored, what services and financial instruments exchanges provide, and the role of stablecoins in facilitating transactions and mitigating risks.

a) Cryptocurrency Exchanges: One of the primary benefits of cryptocurrencies, according to proponents, is decentralization. However, such decentralization exists more in theory than practice. The vast majority of consumers interact with cryptocurrencies via an "exchange," where coins can be bought and sold with fiat currency such as dollars or with one of the thousands of other cryptocurrencies. As such, most transactions involving the purchase or sale of a cryptocurrency never reaches the blockchain; instead, user accounts are debited and credited by the exchange itself, similar to a bank. Thus, the fact that most of the trade in cryptocurrencies occurs on exchanges suggests a higher degree of centralization than proponents admit. Furthermore, while hundreds of exchanges operate across the globe, trade is dominated by a handful of the largest ones. These exchanges operate in a largely unregulated environment compared to traditional financial institutions. In the United States, cryptocurrency exchanges must register as Money Services Businesses.

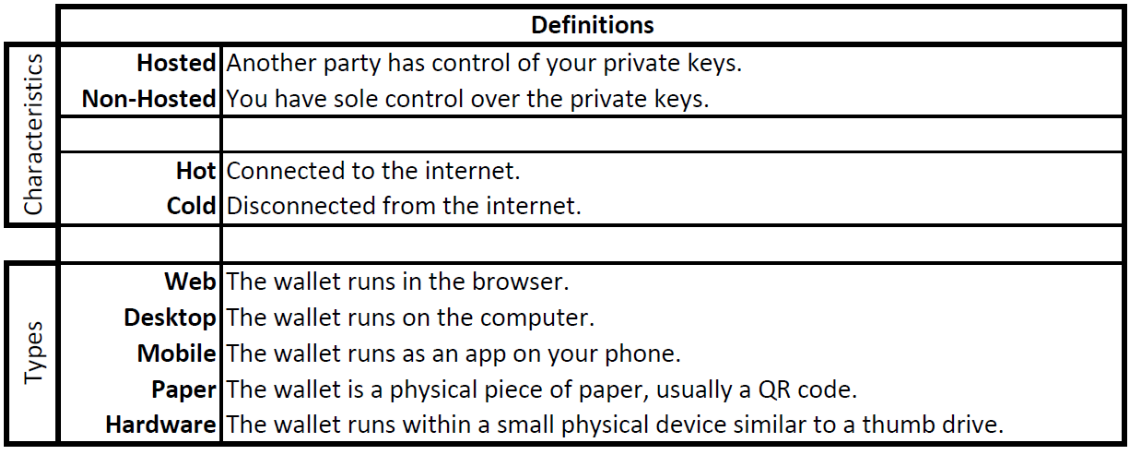
There are two general types of exchange: centralized and decentralized exchanges. The largest exchange, by trading volume, is Binance, which facilitates tens of billions of dollars worth of trading every day. A centralized exchange operates as a central authority managing the transactions between users. These users deposit their funds, either fiat or cryptocurrency, into an account they have created on the exchange website. When two customers' bid and ask orders match, the exchange updates the customer accounts internally, batching transactions across many users before posting to blockchains when required. In contrast, a decentralized exchange facilitates transactions between users without ever possessing the user funds. On decentralized blockchains, all transactions are posted to the blockchains, which is similar to the over-the-counter market for stocks and bonds.

While decentralized exchanges are growing in popularity, they remain dwarfed by their much larger centralized counterparts. As of August 10, 2021, the top 5 centralized exchanges had a combined daily trading volume of $140 billion, compared to just $3.3 billion for the top 5 decentralized exchanges. Why is centralization preferred? First, centralized exchanges are generally much more user friendly. Because the exchange handles all the custodial services for the user, including the management and security of those cryptocurrencies, there is a reduced time and learning investment required by the users. Second, centralized exchanges are inherently faster. While blockchains have increased their throughput in recent years, "off-chain" centralized servers continue to be much faster. Finally, decentralized exchanges do not accept fiat. Because of this, any user not already in possession of cryptocurrencies, must utilize a centralized exchange to participate in the crypto economy. Hence, for the remainder of this paper, when referring to exchanges we are in fact referring specifically to centralized exchanges.

Exchanges have long been a point of vulnerability in the cryptocurrency ecosystem. Prior research has shown that nearly half of these exchanges subsequently close, often without explanation and sometimes leaving customers without access to their deposits [10, 11]. Insider trading at the then-leading exchange Mt. Gox artificially inflated the Bitcoin price [12]. The exchange later failed, leaving many customers without access to the Bitcoin or fiat balances to which they were purportedly entitled. As we will explain below, funds are regularly stolen from exchanges. Because cryptocurrency payments are irreversible, a cybercriminal who can illicitly transfer funds from an exchange's wallet can profit handsomely.

b) Custody and Wallets: To better explain the run risk faced by these exchanges, we now explain where and how user funds are held. Cryptocurrency exchanges rely on wallets to

One notable exception occurred when the United Kingdom's Financial Conduct Authority effectively banished Binance, the largest digital currency exchange, from operating in the country. [9]



		Definitions
Characteristics	Hosted	Another party has control of your private keys.
	Non-Hosted	You have sole control over the private keys.
	Hot	Connected to the internet.
	Cold	Disconnected from the internet.
Types	Web	The wallet runs in the browser.
	Desktop	The wallet runs on the computer.
	Mobile	The wallet runs as an app on your phone.
	Paper	The wallet is a physical piece of paper, usually a QR code.
	Hardware	The wallet runs within a small physical device similar to a thumb drive.

Fig. 2: Cryptocurrency wallet definitions.

manage and safeguard user funds. Similar to how a physical wallet stores cash which itself is used to make purchases, a cryptocurrency wallet controls access to cryptocurrencies, rather than storing the cryptocurrency itself. A wallet operates by managing the public and private keys associated with one or more cryptocurrencies, which are essential for buying, selling and trading cryptocurrencies. A cryptocurrency wallet can take many forms, from web-based wallets running in the browser, to a piece of paper with a QR code on it. However, regardless of which format the wallet takes, it will be either hosted or non-hosted, and hot or cold. These characteristics are important for understanding the risks and accessibility of the cryptocurrency stored within them. Figure 2 details some of the common terms used with wallets.

The first distinction that must be made is between hosted and non-hosted wallets. A non-hosted wallet is a wallet in which the user has full access to both the public and private keys. The user is entirely responsible for the safekeeping of these private keys, and only the user can initiate transactions. The vast majority of exchanges, however, use hosted wallets. In the last column of Table I we see the top 10 exchanges by volume all employ hosted wallets. When a user interacts with a hosted wallet, the exchange will create public/private key pairs on his or her behalf. They will share the public key, often in a compressed alpha numeric format as well as a QR code. The private key however, will be kept secret by the exchange. Exchanges usually describe hosted wallets as being similar in spirit to consumer checking or saving accounts. When one conducts transactions (whether in fiat or cryptocurrency) on an exchange using hosted wallets, the exchange is responsible for keeping track of the individual account balances. For example, if one decides to purchase Bitcoin on an exchange, one is in actuality only buying the rights to that Bitcoin stored within the exchange. There is no adjustment to the actual Bitcoin blockchain, nor is there any activity involved in the wallets themselves. In such a case, the purchaser of the Bitcoin is trusting that the exchange has the Bitcoin, and that it is accurately keeping track of the transactions through an internal database. As such, hosted wallets are reasonably analogous to checking accounts at a bank (we will discuss these risks more below). The security of the funds in the hosted wallet are primarily the responsibility of the exchange.

In addition to the hosted vs non-hosted distinction, a wallet's online accessibility is also important. Any wallet accessible via the internet is a *hot wallet*. For an exchange using hosted wallets, a customer's initial deposit is placed in a hot wallet. This is because the wallet needs to interact with customers over the internet. The wallet needs to generate a key pair and QR code. However, a hot wallet is at greater risk of theft, and therefore many exchanges will quickly move the cryptocurrencies out of hot wallets and into a cold wallet. Cold wallets are simply any wallet whose private keys are disconnected entirely from the internet. In the context of a cryptocurrency exchange using hosted wallets, most of the exchange cryptocurrency balance will be stored in cold wallets, which are not only disconnected from the internet, but also likely air-gapped, and difficult to physically gain access to. These cold wallets will be interacted with in far fewer transactions than the hot wallets, as they're only used to either offload excess crypto from hot wallets, or top up low balance hot wallets. Because these wallets are difficult to access, even for the exchange itself, the exchange can't keep the entire balance in cold wallets without risking liquidity issues. Ideally a small fraction of total funds will be stored in the less safe, more liquid hot wallets.

For individuals that opt for hosted wallets, the exchanges' Terms of Service agreement specifies how and what the exchange may do with the customers' deposits. Most exchanges engage in investing activities with customer funds that are in hosted wallets. For example, Coinbase details in their Terms of Service that "[Coinbase] invests those funds in liquid U.S. Treasuries or USD denominated money market funds" [13]. Bittrex goes further, stating "You will not be entitled to receive any interest or other fees on any fiat currency held in your Bittrex Account or any Tokens held in your Hosted Wallet,

Exchange	Fiat		Stablecoin			Derivatives	Hosted
	EUR	USD	Tether	BinanceUSD	USDCoin	Offered	Wallet
Binance	✓	✗	✓	✓	✓	✓	✓
Coinbase	✓	✓	✗	✗	✓	✗	✓
Huobi	✗	✗	✓	✗	✗	✓	✓
Kraken	✓	✓	✓	✗	✓	✓	✓
KuCoin	✗	✗	✓	✓	✓	✓	✓
Bitfinex	✓	✓	✓	✗	✗	✓	✓
Bithumb	✗	✗	✗	✗	✗	✗	✓
Gate.io	✗	✗	✓	✓	✗	✓	✓
Bitstamp	✓	✓	✗	✗	✓	✗	✓
Coinone	✗	✗	✓	✗	✓	✗	✓

TABLE I: Summary of fiat and stablecoins used by the top 10 exchanges.

even if Bittrex receives interest or other fees from any third parties” [14].

This makes it clear that at least some portion of user funds are likely not being stored in the original asset, as well as highlights the run risk these exchanges face. This behavior, without any of the reserve ratio requirements, without any clear lender of last resort, and without transparent details on what is happening with user funds, could put exchanges at risk of insolvency. It is impossible to know for sure given the lack of transparency and lack of regulation.

c) Financial Services: Cryptocurrency exchanges have innovated many new ways for customers to invest. The traditional service offered by exchanges is to facilitate trade between currencies, but an important distinction remains. Some exchanges enable customers to buy and sell fiat currencies and cryptocurrencies. However, many exchanges do not. Table I describes characteristics of the top 10 exchanges (as measured by trading volume). Only 4 of the top 10 exchanges allow USD trading, and 5 of 10 allow EUR trading. Why is that? Allowing such trades opens the door to greater regulatory oversight, both in terms of oversight of products and services offered as well as know-your-customer obligations. By not offering specific fiat options, they enjoy more freedom to experiment with other, sometimes risky, services.

Some of these riskier services include margin trading, futures, and swaps, collectively known as derivatives. Currently one of the most popular derivatives is known as a perpetual future. A perpetual future is similar to a classic futures contract, where a user can purchase a contract that will expire at some point in the future, and upon expiry, the contract buyer then purchases the asset. The primary difference between a classic future and a perpetual future, is the absence of an expiry date. Instead, these contracts implement a “Funding Rate”, which is a payment between opposite sides of the contract on a regular basis. The size and direction of these payments varies based on the deviation between the contract price and the underlying asset price. Additionally, these contracts can be opened using leverage, up to 125x for Bitcoin on the Binance Futures market. Perpetual futures can be open as long as a user desires, contingent upon their ability to keep their collateral above a limit called the maintenance margin. If a user is unable to maintain sufficient collateral, they risk being liquidated. This liquidation process varies by exchange, but in general the user will have their position closed, and the funds held in their margin account will be used to pay out the other side of the contract.

Over recent years the interest in these derivatives has exploded. Although the concepts themselves have been around for decades, the share of overall cryptocurrency market activity associated with them has skyrocketed since 2016 when BitMEX announced they would become the first cryptocurrency exchange to offer these perpetual futures [15]. Today, they account for tens of billions of dollars worth of trade volume every day across all exchanges.

d) Stablecoins: Cryptocurrencies such as Bitcoin and Ethereum employ floating exchange rates. While this has helped drive popularity through rising prices, it does create problems if the goal is to create a store of value. By contrast, stablecoins are designed to maintain a consistent value, which can be achieved through a variety of means (see [16] for a thorough discussion). CoinMarketCap tracks 66 stablecoins with a collective market capitalization of $115 billion [17], $103 billion of which belong to the top 3 stablecoins Tether, Binance USD and USDCoin. Tether itself captures more than half the total market share at $65 billion. These top 3 stablecoins, not coincidentally, are closely tied to three of the top exchanges, Bitfinex, Binance and Coinbase, respectively. Despite being created by the operators of these exchanges, the stablecoins themselves can be traded on any exchange that chooses to do so.

How do consumers acquire stablecoins? We use Tether as an illustrative example. In theory, an individual can set up an account on tether.to, deposit USD, and receive Tether in return. On their website, Tether claim that “Tether tokens hold their value at 1:1 to the underlying assets”, and that these underlying assets, among other things, include cash reserves, precious metals, and commercial paper. Analysis by [18] has shown that this is likely untrue, that Tether is only partially backed, and that Tether can be used to manipulate Bitcoin prices. Tether is able to maintain its peg because at any point a user can redeem their Tether 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 across cryptocurrrency exchanges every day. 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 peg is dictated by the market demand on the exchange itself. 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 this market demand high and, in turn, its peg close to 1 USD. This prompts a question: if the Tether peg is not entirely dependent on the reserves held at Tether Limited, could a localized shock event at an exchange cause this peg to break? We investigate that possibility empirically in later sections.

Why do customers like to trade stablecoins? Exchanges trading stablecoins experience greater liquidity, which in turn makes it easier to purchase the non-stable cryptocurrencies of interest. Stablecoins perform a role similar to money-market funds in brokerage accounts, offering a place for customers to park funds before or after the sale of a more volatile security. Moreover, the exchanges incentivize the use of stablecoins. They place substantial fees on withdrawals to fiat currencies, in addition to withdrawal and contribution limits. Bitfinex, for example, charges 0.1% on any USD withdrawal, with a minimum of $60 [19]. Another large exchange, FTX, charges a flat $75 fee to withdraw USD [20]. Both of these exchanges, in contrast, offer either no fees at all, or just the fees required from the underlying blockchain to withdraw Tether. Kraken, a California-based exchange regularly in the top 10 crypto 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 [21]. A final benefit is that most derivatives are priced in stablecoins, so such trading necessitates holding stablecoins. Each of the top six derivative exchanges offer Tether-settled futures contracts, which are usually far more popular than the cryptocurrency settled versions. At the time of writing, the largest derivative market, Binance Futures, reported a 24-hour trading volume in Bitcoin settled perpetual futures of 4 billion USD. This is dwarfed by the Tether-settled version, which reports 18.4 billion USD trading volume over the same period.

Why, then, do exchanges promote the use of stablecoins? First, they offer the benefits consumers value mentioned above, notably liquidity and offering a more stable store of value. But the reasons go deeper. Stablecoin issuers take cash deposits and then invest the deposits in a variety of interest-bearing assets. Tether, for example, invests at least some fraction of user deposits into treasury bills, corporate bonds, and "other investments" [1]. TrueUSD, another large stablecoin, details in their terms of service that all their tokens are "backed by an equivalent amount of dollar deposits, cash equivalents, short-term government treasuries, or liquid investments" [22].

Additionally, stablecoins offer some protections to mitigate run risk. Exchanges are widely known to be at risk of security breaches, and customers do not have the same regulatory protections against theft and fraud that banking customers have. Additionally, the price of cryptocurrencies is highly volatile. If customers lose confidence due to a breach at an exchange or a big drop in price, they may try to withdraw en masse. By offering the opportunity to temporarily eliminate volatility, spooked investors may stay put. Following a breach, some customers may choose to exit completely, converting stablecoins back to fiat. Since the exchange offers the stablecoin on a floating price, the exchanges have a built-in mechanism to accommodate such requests, by letting risk-averse customers sell at a discount to risk-seeking investors willing to stay put.

III. Shocks Affecting Stablecoins

We now investigate two scenarios in which we hypothesize a significant shock could break a stablecoin's peg.

a) H1: Security breaches trigger a flight to safety: Anytime an exchange is breached and money is stolen, the news makes waves in the cryptocurrency community. Specialist news sites regularly report on the event, and in some cases even tech and mainstream outlets write about it. 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 at other 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 user concern abates over time, we expect to see a reversion back towards the peg price.

b) H2: Large liquidations introduce a glut of stablecoins that are immediately converted: When cryptocurrency derivatives are liquidated, the winning side of these positions will receive a large influx of stablecoins. We anticipate that many such traders will seek to immediately realize these gains by converting into fiat. This should create a temporary decline in the stablecoin price. Once again, we expect this deviation from a peg should be short lived and self-correcting, as more risk-seeking traders acquire stablecoins at discount.

We use two datasets for our analysis. First, we have our market data which consists of hourly and daily cryptocurrency pair prices and volumes. Second, we have our shock data which includes exchange breaches and significant liquidation events.

A. Market Data

Cryptocurrency prices can vary slightly across exchanges. Since we are investigating shocks that affect stablecoin prices across many exchanges, we utilize prices obtained from [23], which aggregates prices across multiple exchanges. We gathered data on the top 3 stablecoins (USDT, USDC, BUSD). Nonetheless, we primarily focus on the USDT price because Tether is by far the most widely used stablecoin, both in terms of total transaction volume and the number of exchanges that trade it. Additionally, most derivatives are priced in USDT.

B. Security Breaches

In order to comprehensively identify historical security breaches at exchanges, we combine several existing datasets with our own new efforts [11, 24, 25, 26]. These studies cover different time periods and track different types of events, including DDoS attacks, service outages, individual account compromises, and service closures. They also do not focus exclusively on cryptocurrency exchanges.

We applied the following criteria for a shock to qualify as a breach and be included in our analysis. 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 target of the breach must be an exchange that hosts cryptocurrency exchange pairs for spot and/or derivative trading. This excludes thefts from wallets, as well as compromises of individual customer accounts. Finally, some amount of money must be stolen from the exchange itself in the process and be referenced in the reporting. This is designed to exclude cases such as when breaches are detected before money can be stolen, or situations where confidential information is accessed without a loss of funds.

To seek out additional exchange breaches that may not have been captured by prior efforts, we took the following steps. We began by manually reviewing all cryptocurrency events in [26] and the associated news reports. Informed by these articles, we constructed a set of keywords (e.g., “exchange hack”, “exchange breach”, “exchange vulnerability”) and then issued web searches using restricted date ranges that eventually covered the entire period of study. Any plausible report was 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 (e.g., the exchange’s official social media accounts). We were able to corroborate all but one of the security breaches. Only corroborated breaches were added. This process yielded an additional 16 events, for a total of 41 including the other sources.

The timeline for these breaches is shown in Figure 3, weighted by the amount of money stolen (on logarithmic scale). The date of the shock is assigned to be when the earliest public report is observed. Note that pricing data on Tether only began reporting on February 25, 2015. Hence, we exclude the four breaches that occurred before then from the event study. These are indicated by the dashed lines in the Figure.

1) Significant Liquidations: In addition to these exchange breach events, we also collected exchange liquidation data. Given the inherent volatility of cryptocurrencies, deviations between the underlying asset and the contract price is common. Paired with the amplifying effect leverage has on a users ability to maintain their margin account, liquidations are common in cryptocurrency derivative markets. Particularly volatile days can lead to massive liquidations of derivative positions.

The [27] website records daily long and short futures liquidations at six of the largest derivative exchanges. This is daily liquidation data for each exchange and ranges from July 3, 2020 to July 9, 2021. During this period, there were 50 days where total liquidation volume exceeded five standard deviations of the 30 day rolling average. The largest liquidation occurred on April 18, 2021 when the price of Bitcoin dropped from over $61,000 to under $55,000 in less than 24 hours. On this day futures liquidations across just a handful of the top derivative exchanges amounted to over 6 billion USD worth of short positions being liquidated.

For a given day to qualify as a significant liquidation event, the 24 hour liquidation volume for that day, on that exchange, needs to meet or exceed five standard deviations of the rolling average of the previous 30 days on that exchange. The six exchanges tracked were Binance, Bitfinex, ByBit, FTX, Huobi, and OKEx. Combined, these six exchanges have 50 significant liquidation events. 31 of these events are significant short liquidation days, and the remaining 19 are significant long liquidation days. FTX had the most significant liquidation events at 10, while both Deribit and BitMEX had zero. Figure 4 plots the long and short liquidations, weighted by the liquidation size.

IV. Analysis

We employ an event study methodology to measure the impact of exchange shocks on stablecoin prices over time. We follow the process outlined by [28], and shown in Equation 1, which is to calculate abnormal return, AR, as the difference between actual returns, R, and expected returns, $E(R)$.

$$AR = R - E(R) \tag{1}$$

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 initial exploration of the data we noticed that daily granularity data failed to fully detail the wide swings in the price between “closing” times. To correct for this, we utilized hourly pricing data. Because the events are still measured daily, we must convert the pricing data into a daily measure. Hence, we use two methods to calculate actual returns: 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 2, where R_t is the actual squared difference for a given day, t, S and P are the stablecoin price and peg price respectively, at hour, i, of the day.

As a robustness check, we also combined all liquidation amounts into an aggregate amount and then identified significant liquidations. The results were unchanged.

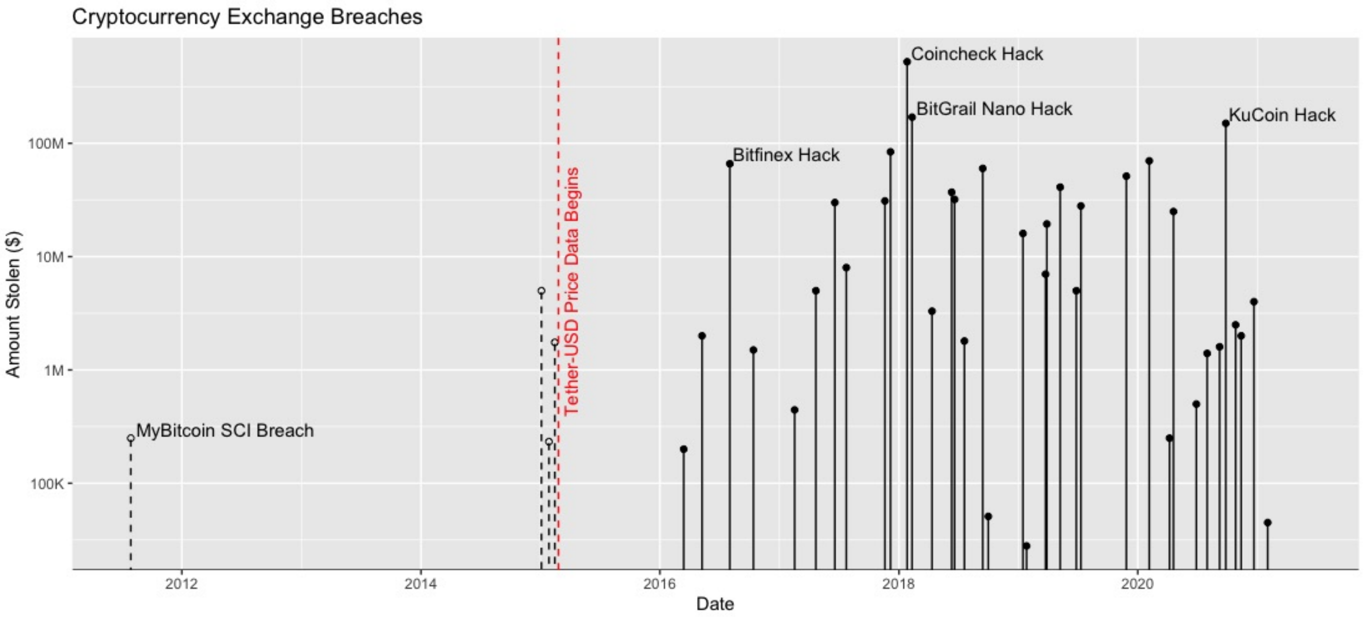


Fig. 3: Timeline of exchange breaches. The amount stolen is shown on the vertical axis (logarithmic scale).

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

The second way we calculate actual returns is by finding the return of the average daily price. This is detailed in Equation 3, where $\overline{S}_t$ is the average daily stablecoin price on day, t.

$$R_t = \frac{\overline{S}_t - \overline{S}_{t-1}}{\overline{S}_{t-1}} \times 100 \tag{3}$$

Next, we need to identify an expected return, $E(R)$, for our time series data. For returns calculated using Equation 2, the expected return is simply the value of the peg. For example, with a stablecoin pegged to 1 USD, we expect the sum of squared differences to be zero for a perfectly pegged stablecoin. When computing the returns using Equation 3, the expected return is the return of the previous day, and therefore $E(R)_t$ is simply 0.

A. Exchange Breach Event Study

The first event study we perform is on the hourly squared differences of Tether around security breach events on exchanges. As noted above, our hypothesis is to examine how breaches affect market confidence in Tether. These returns are calculated using Equation 2, and the window size we use is 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.

As we can see from Figure 5, 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. Because these returns are calculated as the sum of squares, it does not show which direction the price moves relative to the peg, and therefore we perform a second event study using Equation 3. We can see the results 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 USD and oscillates between extended periods of positive and negative returns, slowly returning to pre-event volatility and price levels around 3 weeks after an event. However, 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 U.S. Dollar 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.

To quantify the impact a breach has on the Tether peg, we create a linear model, shown in Equation 4, where the Tether returns, Y, 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 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 II we can see the coefficients and their significance from three different breach window sizes.

$$R = \beta_0 + \sum_{i=1}^{5} \beta_i L_i + \beta_6 D + \epsilon \tag{4}$$

The linear model estimates agree with our event study plots. We see a significant negative impact on Tether returns surrounding breach events.

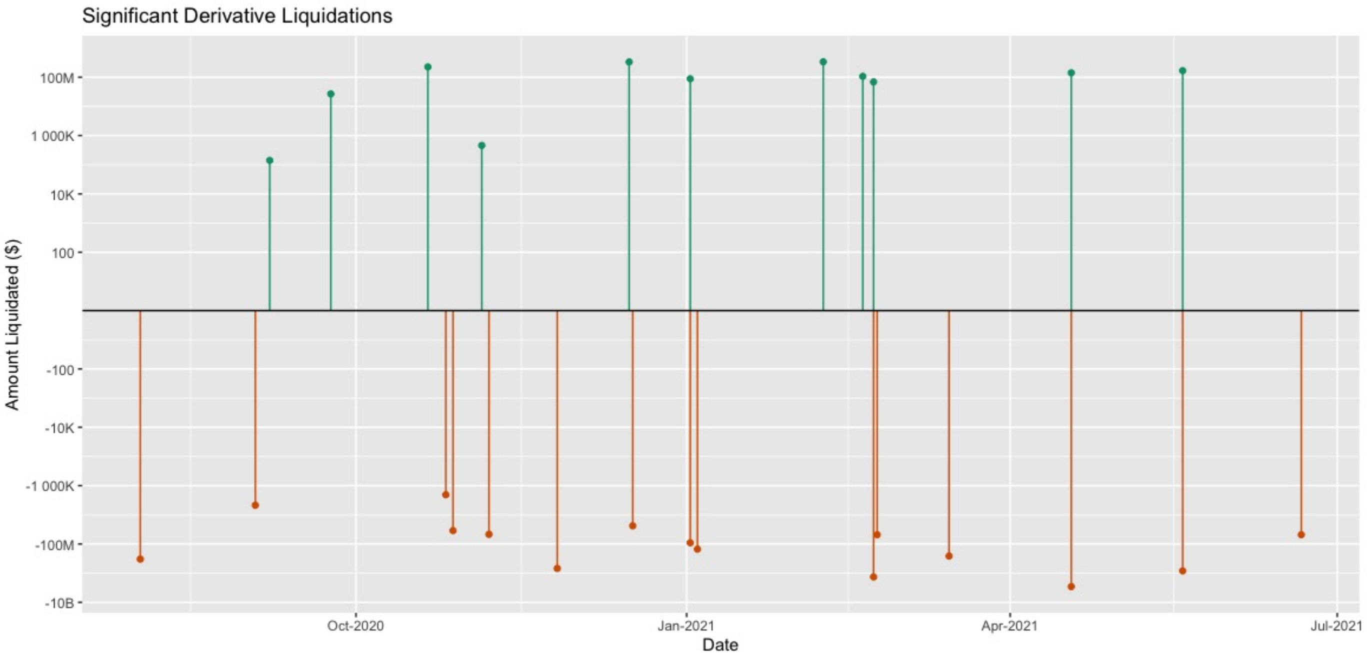


Fig. 4: Timeline of significant liquidations (5 Standard Deviations). Green/positive are long liquidation events, red/negative are short liquidation events.

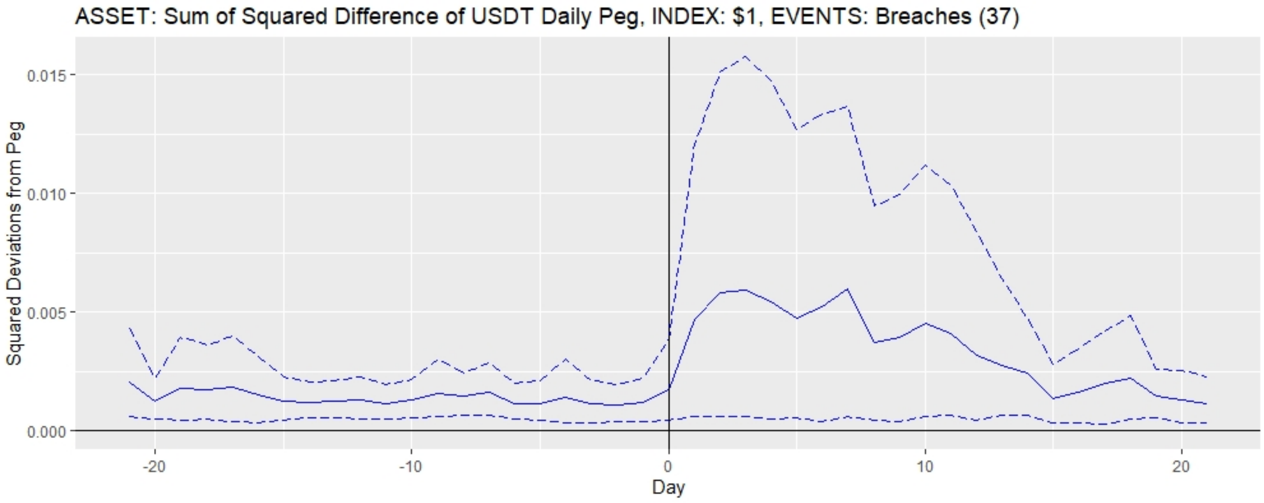


Fig. 5: Event study plot of the Tether(USDT)/USD peg. Events are breaches with any money lost, which amounts to 37 events in total. Dashed lines represent 95% confidence interval.

It might seem counterintuitive 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.

B. Liquidations

Our second hypothesis was related to the fact that Tether is the currency that most derivative contracts are denominated in. As such, we again use the event study methodology to identify the impact of the liquidation events on the Tether peg. Again,

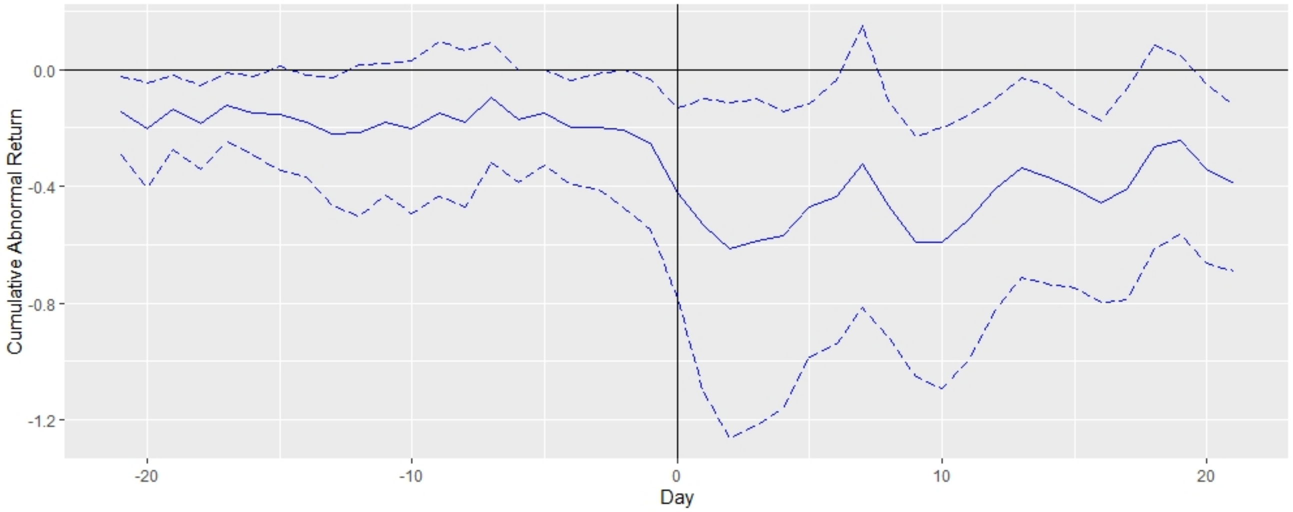


Fig. 6: Event study plot of the Tether(USDT) daily returns. Events are breaches with any money lost, which amounts to 37 events in total. The event window starts 21 days before the event, and extend 21 days after.

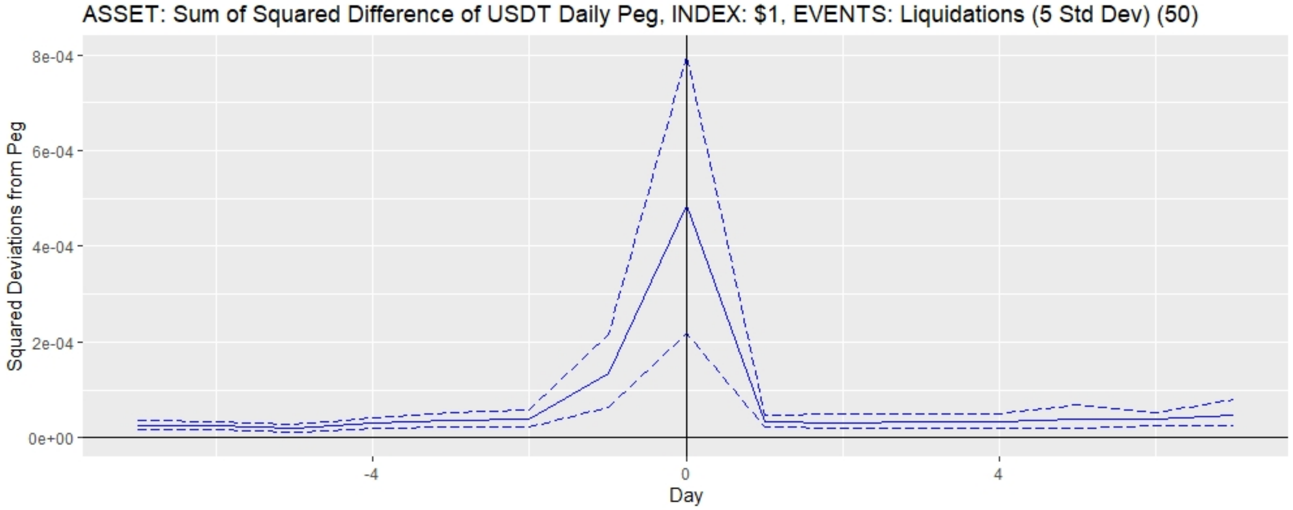


Fig. 7: Event study plot of the Tether(USDT)/USD peg. Events are days with liquidation volume beyond five standard deviations of the 30 day rolling average, which amounts to 50 events in total. The event window starts 7 days before the event, and extend 7 days after.

we start with Equation 2, and can see the results in Figure 7. Interestingly, we see a spike in volatility on the prior to the large liquidations, however, this spike lasts only a single day consistent with expectations from price theory. That is, liquidations cause a transitory supply/demand imbalance but arbitrageurs drive the price back to parity.

Finally, we perform an event study on the returns calculated from Equation 3 with the liquidation events. Figure 8 presents the cumulative results of the returns event study. It should be noted that the cumulative abnormal effect is only 0.0025%, which is quite small. It is interesting that Tether begins trading at a premium several days prior to the large event. The fact that the squared deviations in Figure 7 increase prior to large liquidation event dates combined with the results in Figure 8, suggest that liquidation events cause Tether to trade at a slight premium in volatile time periods. This is likely attributed to increased demand for Tether since derivative contracts are settled in Tether rather than U.S. dollars. This fact, combined with price behavior around liquidation events, suggests that Tether may have assumed a reserve status role in the cryptocurrency ecosystem.

V. Conclusions

We find that Tether's peg is vulnerable to both exchange breaches and significant liquidation events in the derivative market. When money is stolen from an exchange, it can undermine the confidence of traders elsewhere who could naturally worry that funds deposited at their own exchanges might be

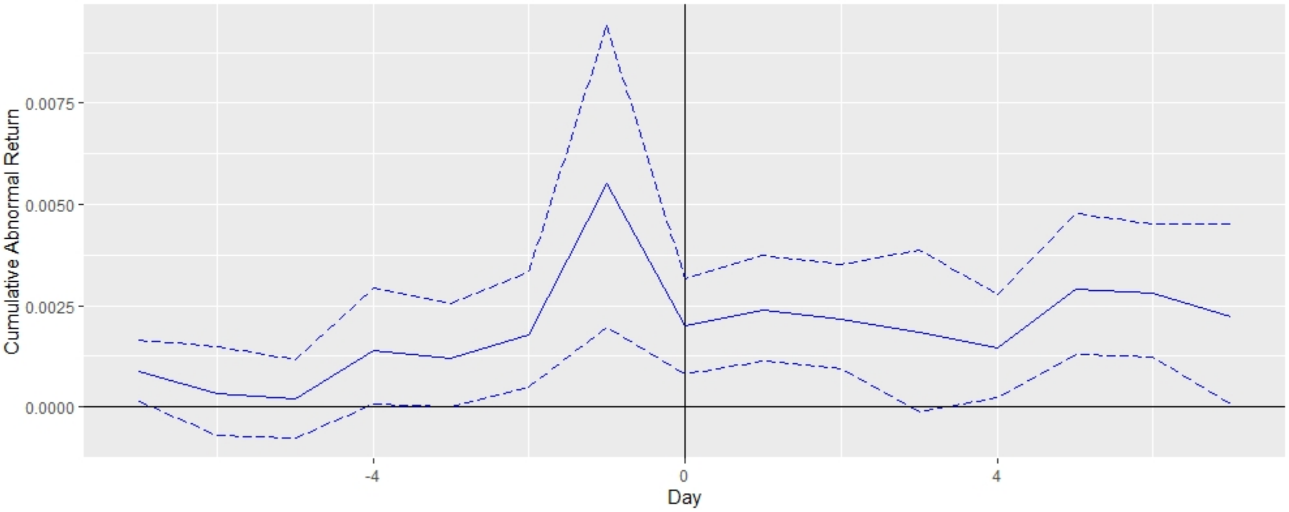


Fig. 8: Event study plot of the average daily Tether(USDT)/USD returns. Events are days with liquidation volume beyond five standard deviations of the 30 day rolling average, which amounts to 50 events in total. The event window starts 7 days before the event, and extend 7 days after.

	+/- 0 Days	+/- 1 Day	+/- 2 Days
(Intercept)	0.11^{***}	0.11^{***}	0.11^{***}
	(0.02)	(0.02)	(0.02)
Lag1	0.57^{***}	0.57^{***}	0.57^{***}
	(0.03)	(0.03)	(0.03)
Lag2	0.22^{***}	0.22^{***}	0.21^{***}
	(0.03)	(0.03)	(0.03)
Lag3	0.05	0.04	0.04
	(0.03)	(0.03)	(0.03)
Lag4	0.04	0.04	0.04
	(0.03)	(0.03)	(0.03)
Lag5	0.01	0.01	0.01
	(0.03)	(0.03)	(0.03)
BreachWindow	-0.00^{*}	-0.00^{**}	-0.00^{***}
	(0.00)	(0.00)	(0.00)
R^2	0.70	0.70	0.70
Adj. R^2	0.70	0.70	0.70
Num. obs.	1568	1568	1568

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

TABLE II: The first column is when only the day of the breach is included, the second includes one day before and after a breach, and the third column includes two days before and after a breach.

next. Using an event study investigating 37 such security shocks from 2015–2021, we have shown that Tether-USD price volatility rises rapidly following a breach. Moreover, the break from the peg persists for up to three weeks with the cumulative effect being approximately -0.5%.

In the days following a security breach at an exchange, we additionally observe that the price of Tether drops. This is consistent with our hypothesis that a breach at one exchange could trigger a broader flight to safety reaction by participants. We observed an oscillating pattern, where the price falls, then rises and falls repeatedly before the volatility disappears. Hence, by letting the stablecoin price float, the market appears to be naturally mitigating run panic-risk by adjusting prices so that risk-seeking traders can buy Tether at a discount the more risk-averse traders are willing to accept.

When Bitcoin prices fluctuate wildly, this has knock-on effects in derivatives trading, especially perpetual futures. Big price swings can trigger forced liquidations, where the "winning" side of the contract receives a payment from the losing side, usually in stablecoins. We presented a second event study examining the effect of 50 large liquidations from leading derivative-trading exchanges in 2020–2021. Here we observed a sharp increase in volatility in the Tether price on the day of the liquidation, which rapidly abates by the next day. However, the cumulative effect is quite small.

Nonetheless, the run risk at cryptocurrency exchanges persists. If market participants lose confidence in the assets backing Tether (i.e., Figure 1), then participants will likely dump Tether on the exchanges or attempt to redeem their tokens similar to traditional finance runs. Stablecoins have only recently started releasing auditing reports showing the assets that back each respective coin. Tether released their first report in May 2021. Future research could use event studies to examine the effect of the increased transparency on the price, as well as the volume, of stablecoins. Moreover, future research should examine the extent to which Tether (or other stablecoins) becomes the "reserve currency" for crypto traders.

This paper has shown how a series of relatively frequent incidents of moderate severity can break Tether's peg, ultimately exhibiting self-correcting behavior that forestalls a run. A true test of the system's resiliency, and to the financial system's susceptibility to cryptocurrency contagion, has not yet materialized. An event that prompted widespread and persistent withdrawals from exchanges and stablecoin issuers is a bigger test, one that we fear may eventually come to pass. Regulators would be wise to prepare for such an event before the day arrives.

Acknowledgements

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

References

[1] Tether.to, "Tether assets," *Tether.to*, May 2021. [Online]. Available: https://tether.to/wp-content/uploads/2021/05/tether-march-31-2021-reserves-breakdown.pdf

[2] M. Brown, S. T. Trautmann, and R. Vlahu, "Understanding Bank-Run Contagion," *Management Science*, vol. 63, no. 7, pp. 2272–2282, Jul. 2017, publisher: INFORMS. [Online]. Available: https://pubsonline.informs.org/doi/10.1287/mnsc.2015.2416

[3] A. Schwartz and M. Friedman, "A Monetary History of the United States 1867-1960," 1963.

[4] B. S. Bernanke, "Nonmonetary Effects of the Financial Crisis in Propagation of the Great Depression," *American Economic Review*, vol. 73, no. 3, pp. 257–276, June 1983.

[5] C. W. Calomiris and J. R. Mason, "Contagion and bank failures during the great depression: The june 1932 chicago banking panic," *The American Economic Review*, vol. 87, no. 5, pp. 863–883, 1997. [Online]. Available: http://www.jstor.org/stable/2951329

[6] D. W. Diamond and P. H. Dybvig, "Bank runs, deposit insurance, and liquidity," *Journal of Political Economy*, vol. 91, no. 3, pp. 401–419, 1983. [Online]. Available: http://www.jstor.org/stable/1837095

[7] H. S. Shin, "Securitisation and financial stability*," *The Economic Journal*, vol. 119, no. 536, pp. 309–332, 2009. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1468-0297.2008.02239.x

[8] V. Ivashina and D. Scharfstein, "Bank lending during the financial crisis of 2008," *Journal of Financial Economics*, vol. 97, no. 3, pp. 319–338, 2010. [Online]. Available: https://EconPapers.repec.org/RePEc:eee:jfinec:v:97:y:2010:i:3:p:319-338

[9] R. Browne, "Binance, the world's largest cryptocurrency exchange, gets banned by uk regulator," *CNBC*, Jun 2021.

[10] T. Moore and N. Christin, "Beware the middleman: Empirical analysis of Bitcoin-exchange risk," in *Financial Cryptography and Data Security*, ser. Lecture Notes in Computer Science, vol. 7859. Springer, April 2013, pp. 25–33. [Online]. Available: https://tylermoore.utulsa.edu/fc13.pdf

[11] T. Moore, N. Christin, and J. Szurdi, "Revisiting the risks of bitcoin currency exchange closure," *ACM Trans. Internet Technol.*, vol. 18, no. 4, Sep. 2018. [Online]. Available: https://doi.org/10.1145/3155808

[12] N. Gandal, J. Hamrick, T. Moore, and T. Obermann, "Price manipulation in the Bitcoin ecosystem," *Journal of Monetary Economics*, vol. 95, pp. 86–96, May 2018. [Online]. Available: https://tylermoore.utulsa.edu/jme17.pdf

[13] Coinbase, "Coinbase user agreement," 2021. [Online]. Available: https://web.archive.org/web/20210824021535/https://www.coinbase.com/legal/user_agreement/united_states

[14] Bittrex, "Bittrex user agreement," 2018. [Online]. Available: https://web.archive.org/web/20210710043437/https://bittrex.zendesk.com/hc/en-us/articles/360000560871

[15] K. Soska, J.-D. Dong, A. Khodaverdian, A. Zetlin-Jones, B. Routledge, and N. Christin, *Towards Understanding Cryptocurrency Derivatives:A Case Study of BitMEX*. New York, NY, USA: Association for Computing Machinery, 2021, p. 45–57. [Online]. Available: https://doi.org/10.1145/3442381.3450059

[16] J. Clark, D. Demirag, and S. Moosavi, "Demystifying stablecoins," *Commun. ACM*, vol. 63, no. 7, p. 40–46, Jun. 2020. [Online]. Available: https://doi.org/10.1145/3386275

[17] CoinMarketCap, "Coinmarketcap stablecoins," 2021. [Online]. Available: https://coinmarketcap.com/view/stablecoin/

[18] J. M. Griffin and A. Shams, "Is Bitcoin Really Untethered?" *The Journal of Finance*, vol. 75, no. 4, pp. 1913–1964, 2020, _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/jofi.12903. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/jofi.12903

[19] Bitfinex, "Bitfinex withdrawal fees," 2021. [Online]. Available: https://www.bitfinex.com/fees/#withdrawal-table

[20] FTX, "FTX withdrawal fees," 2021. [Online]. Available: https://help.ftx.com/hc/en-us/articles/360043023772-Depositing-Withdrawing-Fiat-

[21] Kraken, "Kraken withdrawal limits," 2021, https://support.kraken.com/hc/en-us/articles/360001449826-Deposit-and-withdrawal-limits-by-verification-level.

[22] TrueUSD, "TrueUSD assets," 2021. [Online]. Available: https://trueusd.com/terms-of-service

[23] CoinMarketCap, "Cryptocurrency market capitalizations," 2021. [Online]. Available: https://www.coinmarketcap.com

[24] K. Oosthoek and C. Doerr, "From hodl to heist: Analysis of cyber security threats to bitcoin exchanges," in *IEEE International Conference on Blockchain and Cryptocurrency*. IEEE, 2020, pp. 1–9.

[25] M. Vasek, "Bitcointalk security events," 2019, https://www.dropbox.com/s/7xw2lzov8hjrrcb/securityEvents.csv?dl=0.

[26] P. Passer, "Information security timelines and statistics," 2021, https://www.hackmageddon.com.

[27] Coinalyze, "Advanced cryptocurrency analytics platform," 2021. [Online]. Available: https://coinalyze.net/

[28] A. C. MacKinlay, "Event Studies in Economics and Finance," *Journal of Economic Literature*, vol. 35, no. 1, pp. 13–39, 1997, publisher: American Economic Association. [Online]. Available: https://www.jstor.org/stable/2729691