A flight-to-safety from bitcoin to stock markets: Evidence from cyber attacks

Yang Fang
University of Aberdeen, UK, AB24 3FX, r01yf17@abdn.ac.uk

Cathy Yi-Hsuan Chen
University of Glasgow, UK, G12 8QQ, CathyYi-Hsuan.Chen@glasgow.ac.uk

Chunxia Jiang
University of Aberdeen, UK, AB24 3FX, chunxia.jiang@abdn.ac.uk

We discover a novel flight-to-safety effect from cryptocurrency markets to stock markets. It occurs after a series of hacking attacks on crypto exchanges as greater uncertainty heightens investors' risk awareness and perception, which, in turn, induces herd-like behaviour in favor of safer stock markets over riskier cryptocurrency markets. We extensively examine this effect worldwide across 39 countries and confirm this novelty. This effect is amplified when investors' risk awareness is strengthened by frequent attacks. Intriguingly, the sentiment elicited from the attacks discussed on social media not only serves as a timely warning indicator for the forthcoming attack events, but also measures the flight-to-safety pressure after attack events. We conclude that the collapse of investors' confidence is the primary cause of such an effect. Through the lens of cyber attacks, we document how a shock in crypto markets is transmitted into stock markets through investors' flight-to-safety behavior.

Key words: Cyber-crime; Cryptocurrency; Flight-to-safety; Stock market; Social media

1. Introduction

In the past decade, bitcoin, the most popular cryptocurrency, has attracted enormous attention and instigated huge debate on its functions. This unregulated market operates 24/7, is characterised as an anonymity, and launches borderless transactions. The use of privacy-enhanced cryptocurrencies has been rising and has been marked by substantial proportion of illegal criminal activities (Foley et al. 2019). According to the IOCTA report 2020, hacking attacks have become more frequent over the past few years, partially stimulated by the growing adoption of cryptocurrencies.[1] Cryptocurrency users have become the targets of cybercriminals. In 2019, there were 10 publicly confirmed hacking attacks on crypto exchanges with stolen cryptocurrencies worth 244 million euro.

Early research strongly indicates that unsophisticated users approaching digital currencies perhaps are not primarily interested in an alternative transaction system but seek to participate in

[1] Internet Organised Crime Threat Assessment (IOCTA, 2020) can be found at `https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020`.

an alternative investment vehicle for new experience (Glaser et al. 2014). Cryptocurrency investors may not have the adequate financial literacy to engage in inherently complex, risky, and volatile financial instruments (Panos and Karkkainen 2019). Frequent hacking attacks on crypto exchanges may dampen investors' interest in cryptocurrency. Investors realize that they may not be well-equipped to make financial decisions within such a complex system and they will not be protected by central authorities or law enforcement. Consequently, they favor regulated asset markets, resulting in a 'flight-to-safety' effect from cryptocurrency markets to stock markets.

A flight-to-safety is considered as an episode of the co-occurrence of higher economic uncertainty, lower equity prices, and low real rates (Barsky 1986, Bekaert, Engstrom and Xing 2009). Investors' fear of redemption and increased effective risk aversion cause investment movements, i.e., from equity markets to bond markets, for liquidity and quality (Vayanos 2004). Such a phenomenon might be observed in bond markets or currency markets. In this study, a flight-to-safety phenomenon between cryptos and stocks is particularly portrayed and it is characterized by changing risk perception from an alternative investment vehicle, known as high-risk assets, to a conventional investment vehicle. Investors who are interested in cryptocurrencies are risk takers/speculators for higher returns.[2] Facing hacking attacks on crypto markets, these 'risk-loving' investors are more likely to consider unaffected stock markets for relative higher returns instead of other less riskier markets/investments (e.g., bonds or mutual funds). As such, the flight-to-safety effect is likely to take place from crypto markets to stock markets as (potential) cryptocurrency investors flee to the stock markets.

Baele et al. (2020) propose three criteria to signify a flight-to-safety from stock markets to bond markets and employ different models to measure the flight-to-safety.[3] Given the very nature of cryptocurrency markets and the resultant difficulty in tracing capital flows, it is impossible to identify a flight-to-safety between crypto markets and stock markets as in a conventional scenario. We attempt to address this challenge through the lens of cyber-attacks on crypto markets - how stock markets react to these attacks. Literature suggests that risk-averse investors are prevalent with the emergence of cyber-attacks (Caporale et al. 2020). As victims of cyber-attacks, investors' risk perception and awareness increased and they decided to seek a safe haven. A herd of investors flee from alternative assets under the threat of cyber-attacks and retreat to equity markets. Consequently, these two markets will move in opposite directions.

[2] Bitcoin is an investment vehicle of the highest risk worldwide. According to Yermack (2013), the volatility of bitcoin-dollar exchange rate was 142%, higher than the dynamic movement of the riskiest stock of a volatility of 100%. Widely traded stocks normally had volatility in the range of 20% to 30%, other fiat currency had volatility between 7% and 12%, and gold, an alternative investment for hedging risk, had a volatility of 22% in 2013 based on dollar-denominated exchange rate.

[3] The three criteria are (1) the bond and stock market have a large positive and negative return, respectively; (2) bond and stock returns are negatively correlations; and (3) a high equity market volatility.

In particular, this unconventional 'flight-to-safety' behavior is examined from three perspectives. First, we consider bearish sentiments and increased risk awareness as the causes that trigger the redemption and asset re-allocation between different asset classes. Investors are frustrated with their limited financial literacy in the crypto markets where they lack confidence. We examine whether stock markets react positively to the hacking events in crypto markets, given considerable capital flowing out of the crypto markets and into stock markets.[4] Second, we conjecture that this effect may become more prominent under consecutive attacks on crypto exchanges. These consecutive attacks substantially weaken the confidence of market participants and heighten their risk awareness. Therefore, we further examine whether consecutive attacks strengthen the flight-to-safety effect. Third, for the cryptocurrency community, social media is an ideal venue to exchange information, given the fact that crypto markets are neither as transparent nor as efficient as stock markets. Hackers tend to target crypto exchanges with vulnerable security by initiating small attacks before radically breaching these crypto exchanges (Gandal et al. 2018). Those investors whose crypto wallets have been stolen are inclined to spread attack alerts to their communities via social media platforms. We posit that in crypto markets, the founders of exchanges, cyber security experts, and targeted people who suffer from hacking losses can be seen as informed players since they are aware of attacks prior to an official announcement. By distilling social media sentiment in the crypto community, we examine whether the discussed attacks on social media can foresee the upcoming major attack event and whether social media sentiment is informative in terms of timing a flight-to-safety. As cryptocurrency markets are borderless with investors around the world, we examine the flight-to-safety effect in an international setting of 39 countries, including both developed countries and emerging economies.

Identifying the event date of a breach in crypto exchanges, more specifically the event time stamp confirmed by exchanges, is critical to this study. We manually collect information on hack events reported by the mainstream press (such as Reuters and The Guardian) or disclosed on blockchain forums or crypto exchange websites. Over the period January 2011 to February 2020, there were 76 attacks with an average stolen value of US$ 29.19 million per event. The likelihood of attacks relates to cryptocurrency market prices, evidenced by the crypto bubble period in 2018 (see Figure 1). It appears that exuberant cryptocurrency prices incentivize hackers stealing from individual wallets managed by the crypto exchanges. The attacks are also quite frequent in the early phase of exchanges' establishment because of inadequate security infrastructure. The disruptive breach suffered by the Mt. Gox exchange in 2014 is the most representative event, resulting in a total loss of US$ 460 million.

[4] Prospective cryptocurrency investors also pour capital back into stock markets.

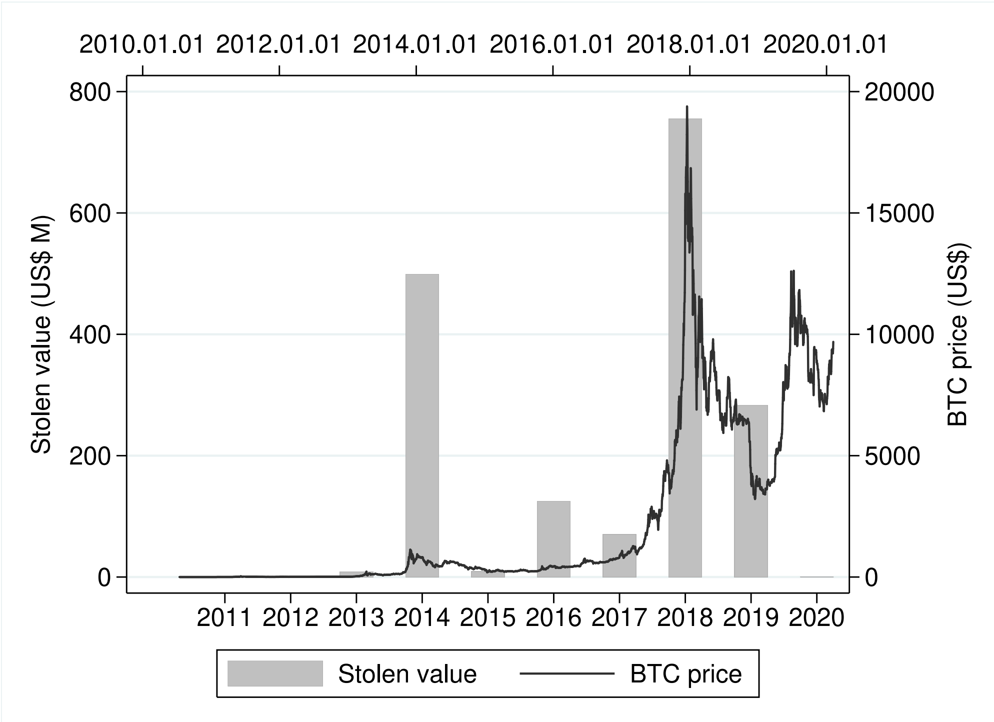

Figure 1 Stolen value versus bitcoin price.

This figure plots stolen value by hacking attacks in US dollar million (the left y-axis) and bitcoin (BTC) price in US dollar (the right y-axis) during the period 2011-2020.

We observe a counter-movement between bitcoin and stock markets, estimated from a time-series of the bitcoin exchange rate and worldwide stock index. We elaborate the flight-to-safety phenomenon during the hacking period of a pre- and post-event window. When hacking attacks are officially announced (the event date), the counter-movement between two markets becomes prominent: the expected bitcoin return, normalized by its risk, continues to fall, whereas the expected stock return with the same normalization rises. Under the threat of hacking attacks on crypto markets, stock markets turn out to be the safe haven for cryptocurrency investors - a role that will continue as long as threats present in crypto markets.

We find that social media sentiments, reflecting a collapse of confidence caused by attacks, alert the crypto community to the incoming cybercrime event. In other words, the sentiment indicator serves as an early indication of attack events. We further associate the sentiment distilled from messages on social media with stock market returns and confirm that the flight-to-safety pressure, measured by investor's sentiment, can explain stock market returns. A sharp decline in sentiment precedes a downward plunge in bitcoin returns and an upward soar in stock market returns. We, therefore, explain this novelty with (1) the collapse of investors' confidence expressed by social media sentiment; and (2) the increased risk perception that leads to a plunge in bitcoin returns and a shift in investors' interest from an alternative investment vehicle to a conventional investment vehicle.

This study contributes to the literature in three aspects. Firstly, we focus our interest on the novel flight-to-safety effect from alternative asset markets (crypto markets) to conventional financial venues such as stock markets, triggered by cyber attacks. Extant research shows that the flight-to-safety effect appears during market downturn or crisis periods. For instance, the 1997 Asian crisis, the 1998 Russian crisis, and the Enron crisis in 2011 are defined as flight-to-safety events (Baur and Lucey 2009). Adrian et al. (2019) find that the effect of managers transferring investment to relatively safe assets as a result of flight-to-safety is stronger during a volatile period, while Baele et al. (2020) systemically define, detect, and characterize flight-to-safety episodes between stock markets and bond markets. We provide evidence for a new paradigm of the flight-to-safety effect from the digital asset markets to the conventional asset markets.

Secondly, we contribute to the literature by revealing the link between crypto markets and conventional financial markets through the lens of cyber attacks. There has been debate about whether cryptocurrencies are separated from the conventional financial and economic assets (i.e., stock markets). Akyildirim et al. (2020) provide evidence for the contagion channels between stock markets and crypto markets that changes in corporate names to blockchain and crypto-related names affect their stock market performance. Liu and Tsyvinski (2018) find that cryptocurrency returns have no strong correlation with traditional asset classes. Klein et al. (2018) find no evidence supporting the role of bitcoin as safe haven or hedging function. Other researchers argue that bitcoin have the similar feature with gold (Dyhrberg 2016), can act as a hedge tool (Demir et al. 2018, Guesmi et al. 2019), and can be used as a diversifier with short-term investment horizons (Corbet et al. 2018). These studies attempt to establish a link between crypto markets and conventional financial markets by exploring the potential role of cryptocurrencies as an alternative investing or hedging vehicle. In this study, we investigate how a shock (cyber attack) in crypto markets is transmitted to stock markets.

Finally, this paper contributes to the literature on cryptocurrency markets from the perspective of cybercrime. Extensive academic attention has been paid to cryptocurrency, focusing on the factors that drive the dynamics of cryptocurrency price, such as the network effect of cryptocurrency adoption (e.g., Cong et al. 2020), the marginal cost of production (e.g., Cong, He and Li 2019, Sockin and Xiong 2020), the value of stable coins such as Tether (Griffin and Shams 2020), and the movements of traditional asset classes such as fiat money (e.g., Schilling and Uhlig 2019). Due to the featured decentralized system and a growing darknet market (Foley et al. 2019), cryptocurrency users have been targeted by cybercriminals. Existing research has documented a range of security threats, including forking, mining botnets, and private key issues (Biais et al. 2019, Spathoulas et al.

2019, Li et al. 2020). Sokolov (2018) finds that blockchain congestion and rising transaction fees are significantly caused by cyber ransomware. Cyber ransomware and attacks concurrently emerge when cryptocurrency prices jump up and mainstream adoption becomes prevalent. Caporale et al. (2020) examine how cryptocurrencies react to general cyber-attacks that target different sectors in the economy. In this paper, we focus on hacking attacks on crypto exchanges, which triggers investors' fear and risk perception. We provide a new perspective from investors' risk perception and resultant asset re-allocating behavior.

The remainder of the paper is organized as follows. Section 2 discusses economic theories that underpin our hypotheses for the flight-to-safety effect. Section 3 describes data and defines variables. Section 4 undertakes empirical analysis and interprets the results. Section 5 presents an extended analysis on the country-specific characteristics. Section 6 concludes.

2. Theoretical background and hypothesis

2.1. The risk of trading cryptocurrency on crypto exchanges

Interest in cryptocurrency has become unprecedented as it represents not only the emergence of a new form of currency but also a disruptive and innovative payment technology. However, investors bear the risks around each transaction as cybercriminals employ more holistic strategies. Unlike trading conventional financial assets (i.e., stocks or bonds) that are insured by regulators, trading cryptocurrency faces default risk as there is no assurance for investors who lose money due to unexpected hacking attacks. For instance, the Federal Deposit Insurance Corporation (FDIC) in the US can handle failing banks going into liquidation, paying off depositors in full, selling the bank's assets to another bank, and assisting the bank in restructuring under a new management team (Buser et al. 1981). However, in the cryptocurrency world, there are neither schemes supported by any authorities or third parties to recover the losses caused by cyber-attacks nor regulations for preventing the malfunction of crypto exchanges. Recently, Securities and Commission (2018) has called crypto exchanges "potentially unlawful online platforms" as none of the exchanges is registered with securities regulators.

Technically, from the cryptocurrency transaction perspective, because of the privacy-enhanced payment techniques, traders' identity in each transaction cannot be verified by records. In the event of exchanges being attacked by hackers, it is extremely difficult or sometimes impossible to trace the cash flow.[5] By contrast, in stock markets, stolen or transferred securities by illegal operations to other trading account(s) can be traced back since every single account is linked with a government authenticated identity. Thanks to the anonymity and the lack of a direct ownership

[5] Mainstream cryptocurrencies, such as bitcoin, support mixer/tumbler functions for privacy reasons, where bitcoin mixing uses a third-party service to break the connection between the source and destination of bitcoins.

identification with cryptocurrency, hackers find crypto exchanges extremely attractive. According to a report (Hackernoon 2019), many exchanges are poorly rated in terms of security.[6] Needless to say, exchanges have been struggling with frequent attacks and fail to prevent such events effectively.

2.2. What makes crypto exchanges so hackable?

A number of facts make crypto exchanges attractive to hackers, including the rapid increase in coins' value, the centralized business operation model, the hot wallet practice to store customers' cryptocurrency without secure protection, and the no-traceback of stolen coins. In this subsection, we elaborate these in detail.

First, bitcoin price has been soaring explosively since 2017 with a record high of US$ 64,550 in April 2021, which makes it rather attractive to hackers. From April 2017 to February 2020, there were 30 hacking attacks with a total stolen value of $1108 million. As shown in Figure 1, the stolen value is positively correlated with bitcoin price.[7] Meanwhile, crypto exchanges experienced intense attacks and suffered the worst losses in the crypto-bubble period of 2018, when the stolen value reached a historical high of $755 million. Following the burst of the bitcoin bubble in 2018, the stolen value shrank. Another exceptional period of consecutive hacking events occurred in 2014 when, as shown in Figure 1, the stolen value was surprisingly high despite the low price of bitcoin. The main reason for this surge was that Mt.Gox, the biggest crypto exchange, experienced severe hacking attacks with stolen bitcoins worth about $480 million and subsequently went into liquidation.

Second, crypto exchanges conduct daily business in a centralized-model. About 99% of crypto transactions are carried out through the centralized operation of crypto exchanges, which gives rise to a higher probability of cybercrime than in stock exchanges. Different from stock exchanges, crypto exchanges deal with trading and even hold cryptocurrency on behalf of investors: crypto exchanges take full control of bitcoin storage to ensure buying and selling orders in real-time. The

[6] There is no crypto exchange that can provide absolute security to its users, regardless of whether it is a top exchange with a team of highly paid IT professionals and programmers or a novice that is new to the market. The crypto exchange market faces fragile firewall to prevent cybercrime. Based on the report (Hackernoon 2019), exchange security has four aspects: user security; domain & registrar security; web security; and DoS protection. The evaluation survey on these four security aspects shows that none of the crypto exchanges has received an A+ rating and most of them have a B score. Nearly 30-40% of the exchanges are not protected from Clickjacking attacks and DoS attacks. This means that none of exchanges works with sufficient protection against cyber attacks, and as a result, a fairly large proportion of exchanges have experienced data leakage and assets losses.

[7] Based on Google Trends, interest in the topic "cryptocurrencies" peaked at the end of 2017 when "bitcoin" won the second-highest search volume in Global news. The search query "how to buy bitcoin" was also made the TOP-3 searching topic in 2017. Aligning with public attention, the overall value of the global cryptocurrency market exceeded $800 billion for the first time in January 2018. This figure is only slightly less than the capitalization of Apple at the same time. Therefore, it is not surprising to find that soaring numbers of cyber-attacks correspond with huge demand for cryptocurrencies. For instance, the number of account leaks by exchanges increased by 689% from the end of 2016 to 2017 (Group-IB 2018).

central storage of coins, akin to cash stored in banks, raises security concerns and makes crypto exchanges into sitting ducks for hackers (Russolillo and Jeong 2018). When a crypto exchange is under attack, a trader needs permission from the central authority to withdraw the fund. The approval process inevitably causes losses related to high price volatility, as in the case of the attack on Mt. Gox.

Third, crypto exchanges store the coins for their customers in hot wallets. A hot wallet means that a user's private key information is kept online and maintained by the exchange. This presents another potential risk of trading in crypto exchanges - a high probability of losing users' private key stored in their hot wallets. The private key is a unique identity of ownership and security credential.[8] Crypto exchanges that manage a pool of private keys expose themselves to a variety of attacks, which can lead to leaks of confidential information. From the users' perspective, losing a private key will be disastrous as they subsequently lose the connection to the blockchain ecosystem.

Finally, the structure of the Bitcoin system makes it impossible for crypto exchanges to trace back the stolen coins/funds. When hackers successfully steal coins from exchanges and transferred funds into their private wallets, millions of wallet addresses, created through blockchain, can be automatically created to store bitcoin (Foley et al. 2019). The stolen coins may have a mystery journey across multiple token addresses through blockchains. With cryptocurrencies, hackers manage to undermine law enforcement's ability to trace payments connected to criminal activities.

2.3. Hypotheses

In this section, we develop our hypotheses for flight-to-safety behaviour in the presence of cyber-attacks. We start by examining whether hacking attacks trigger a re-allocation of asset classes by down-weighting the risky one (cryptocurrency) in favor of the relatively safer one (stocks). We further study whether the flight-to-safety effect is more pronounced during a period of consecutive attacks to crypto markets. Moreover, we investigate the role of social media sentiment. The victims of cyber attacks, who are also social media users, post messages about the attacks on social media to alert the crypto community. Since these posts arrive prior to the outbreak of extensive attacks, social media sentiment serves as an early warning indicator for incoming attack events and therefore measures the flight-to-safety pressure.

Hypothesis 1: *Cyber attacks on crypto markets undermine existing and prospective cryptocurrency investors' confidence, increase their risk awareness, and trigger their fear, resulting in a flight-to-safety effect on stock markets.*

Cyber attacks on crypto exchanges have a reverse contagion effect on stock markets. Cybercrime systematically disrupts the function of crypto exchanges. The risk of leaking out private keys and

[8] A hot wallet is preferable to a cold wallet, considering the expense and speed of online selling, buying or trading orders (Gentilal et al. 2017).

losing coins leads to a rise in investors' risk perception. Investors, therefore, demand a higher risk premium and at the same time express their propensity for relatively safe assets, leading to counter-movements in these two markets. As asset management pricing theory suggested (Vayanos 2004), asset managers are subject to funding constraints, which, in turn, depends on the level of market volatility. We further investigate this effect between the decentralized asset class and the centralized asset class under regulation. When uncertainty and fear emerge under hacking attacks, the likelihood of withdrawal rises and a desire to hedge increases, leading to a decline in traders' risk appetite in favor of the assets with familiarity for better information acquisition (Massa and Simonov 2006). A rich body of literature confirms that "flight-to-safety" or "flights-to-quality" behaviour is a commonly observed phenomenon during a financial crisis (Adrian et al. 2019, Baur and Lucey 2009, Baele et al. 2020). In the context of cryptocurrency, such an effect is likely to be witnessed under the threat of cyber attacks. The resultant uncertainty, extreme volatility and declining sentiment give rise to flying to safer markets.

Hypothesis 2: *Consecutive hacking attacks strengthen a flight-to-safety effect.*

Consecutive attacks may deteriorate investors' confidence in crypto markets and elevate their risk perception. This conjecture is made following the lesson from a crisis where consecutive arrivals of negative news scare away the investors in stock markets. Examining attack events with different scale levels, we find that two particular years experienced a series of hacking events that exceed the average attack level. In 2014, 10 hacking events were reported, following the hacking event at Mt. Gox. During the 2018 crypto bubble period, 13 hacking activities were formally detected. When hacking becomes more prevalent and intense, investors are more likely to fear and escape/avoid such a threat. The relationship between hacking frequency and the strength of flight-to-safety behaviour enhances our understanding of the nature of fear.

Hypothesis 3: *The social media sentiment toward attacks serves as a timely warning indicator for incoming major attack announcements and induces flight-to-safety behaviour.*

Social media have significant predictive power for hacking attacks in crypto markets as messages convey information. It is worth noting that bitcoin users/traders are very often social media users (Duggan and Brenner 2013). They opt for information exchange on social media because crypto markets are less transparent compared to stock markets where companies are required to release corporate reports in compliance with regulations. According to Chen and Hafner (2019), social media information is highly relevant to future market performance and can be regarded as an instrument to predict price and market volatility. Markets tend to be more sensitive to bad events than good news (Medovikov 2016). We investigate whether social media, where users report and discuss an attack and related losses that happened to them before the outbreak of extensive attacks, may offer a warning indication so that the reflected sentiment from social media messages can help predict an upcoming attack.

With social media, the herding behavior is more likely to be witnessed (Linton et al. 2017), causing the spillover of fear across media users. Crypto markets generally consider the owners of exchanges, cybersecurity professionals, and the victims of wallet theft from exchanges to be informed investors since they are aware of hacking news before the general public. This group of players possess information advantage relating to the outbreak of attacks. Another group of players which normally are the majority of retail investors, are far behind the information and susceptible to unexpected shocks (attacks). When news of an attack arrives, overwhelming discussions on social media cause a herding effect and induce flight-to-safety behaviors.

3. Data, sample, and variables

We collect data on a series of hacking events mainly from Reuters, The Guardian, other mainstream press and crypto exchanges' websites that report hacking events and information leakage regarding investors' private keys. Our analysis starts in 2011 when cyber-attack were first recorded online and reported by mainstream press. We collect the daily market price of bitcoin and its bid-ask spread from Bitcoinity (Corbet et al. 2019), a platform that uses API to gather data directly from crypto exchanges, including Coinbase, Bitfinex, Bitstamp, Kraken, BitX, BTCE, CEX.IO, EXNO, Gemini, itBit, LakeBTC, Okcoin and among others. Over the period from January 2011 to November 2019, there were 76 hacking events. Due to the inferior information regarding some hacking events (i.e., the specific hacking date) and considering the amount of losses, we end up with 45 hacking attacks in our sample, as listed in Appendix A1. As for data on stock markets, aligning with the designated sample period for hacking events, we are left with 84,747 daily observations in 39 countries across 6 continents, of which 59% are developed economies and 41% are emerging economies.[9] Data on stock markets are collected from DataStream and relevant financial data are obtained from the World Bank's world development indicators (WDI) database.

The performance of crypto markets is measured in terms of bitcoin returns and bitcoin liquidity across crypto exchanges. The notations introduced for the bitcoin-related variable include $R_{j,t}^{BTC}$

[9] The countries/economies include Argentina, Australia, Austria, Belgium, Brazil, Canada, Chile, China, Colombia, Denmark, Egypt, Finland, France, Germany, Hungary, India, Indonesia, Ireland, Italy, Japan, Korea, Malaysia, Mexico, Netherlands, New Zealand, https://www.overleaf.com/project/5f88e793a4518500018d9991Norway, Philippines, Poland, Portugal, Russia, Singapore, South Africa, Spain, Sweden, Switzerland, Thailand, Turkey, UK and USA. One might argue that a natural empirical design would be to match crypto exchanges and stock markets by geographical location. However, this is not practical for two reasons. First, bitcoin trading volume of online exchanges is highly concentrated. According to Statista (`https://www.statista.com`), more than 85% of all global bitcoin trading in 2020 happened in the top ten countries (i.e., USA, Russia, Nigeria, China, and UK). Second, crypto exchanges are online platforms serving different countries. For example, Binance, headquartered in Shanghai (China), operates from over 40 countries and serves more than 180 countries across the world.

and $Spread_{j,t}$, defined as the daily changes in bitcoin price - $log(BTC\ price_{i,t}/BTC\ price_{i,t-1})$, and the daily bid-ask spread, from the j-th crypto exchange at date t, respectively. A smaller return implies worse bitcoin performance, while a larger spread indicates higher liquidity costs and risk. The stock market performance of country i at date t, $R_{i,t}$, is defined as the daily changes in stock market return - $log(stock_{i,t}/stock_{i,t-1})$.[10]

Our primary research interest is a three-day period - the announcement date and the following two trading days. We define three indicator variables for each date to better capture the dynamics of the impact - D_0, D_1, D_2, taking a value of 1 for the announcement date, the first, and the second trading day after the announcement date, respectively.

To measure social media sentiment of the cryptocurrency community, we are particularly interested in two leading social microblogging platforms - StockTwits and Reddit, where the crypto community members share and exchange information and opinions, especially from a financial investment perspective. In this study, we make use of a sentiment indicator constructed by Chen et al. (2019). The authors develop a novel lexicon tailored for the cryptocurrency-specific semantic distillation and construct a consolidated sentiment indicator on a daily basis.[11] They extensively retrieve the granular social media streams from StockTwits and Reddit during the period from January 2014 to December 2018. We denote $Stwits_t$ as the measure of investor sentiment in the StockTwist community, ranging from -1 (negative sentiment) to +1 (positive sentiment). The daily log changes in *Stwits* is $\Delta \ln(Stwits_t)$. Using the crypto-specific lexicon, we also quantify the sentiment from messages on the Reddit website. The daily log changes, $\Delta \ln(Reddit_t)$, is an alternative measure of sentiment movement.[12]

The heterogeneity across countries and over years may be partially responsible for the differences in stock market performance. Therefore, in addition to year and country fixed effects, we also control for country-specific characteristics. Following the literature, we include stock market development - *MKT*, defined as the ratio of stock market capitalization to GDP; credit market development - *CREDIT*, defined as the ratio of domestic credit to private sector over GDP; stock market volatility - *Volatility*, defined as the annual stock market standard deviation; annual changes in global equity market index - *SP*; *GDP growth*; *GDP percap* measured by the logarithmic GDP per capita (in

[10] When the closing index on date $t-1$ or t is unavailable, we treat the stock market return as missing. An alternative method is to use a different time horizon (i.e., weekly) to calculate the returns. However, we consider that longer intervals cannot fully capture market volatility and are likely to result in greater distortion.

[11] The crypto-specific lexicon can be downloaded from Cathy Y. Chen's website `https://sites.google.com/site/professorcathychen/resume`

[12] For StockTwits, the authors end up with 1,533,975 messages from 38,812 distinct users and related to 465 cryptocurrencies. As for Reddit, the message volume is 1,392,587 posted on the eight subreddits with the highest number of subscribers: "CryptoCurrency", "CryptoCurrencyTrading", "CryptoMarkets", "Bitcoin", "Bit-coinMarkets", "btc", "ethereum", and "ethtrader".

USD); monthly broad money growth - *M3*; *Inflation* proxied by GDP deflator; *Saving* as the ratio of saving over GDP, and *Popurban* as the proportion of urban population (Levine et al. 2000, Djankov et al. 2007, Hsu et al. 2014, Chen et al. 2017).

Table 1 Panel A reports descriptive statistics for our full sample. Daily changes in stock return ($R_{i,t}$) has a mean of 0.025% with a standard deviation of 1.2%, while bitcoin return ($R_{j,t}^{BTC}$) has a mean of 0.22% with a standard deviation of 3.8%. Bitcoin spread ($Spread_{j,t}$) has a mean of 64.3% with a standard deviation of 199%. A total of 1.2% of our sample have crypto exchanges making hacking attack announcements (D_0). The corresponding figures for the first trading day (D_1) and the second trading day (D_2) after the attack announcement date are both about 1.7%.[13] 7.8% of our sample have experienced multiple crypto-exchange attacks within one month (M). Global equity growth rate (SP) shows an increase in stock market growth, on average, by 2.48% per annum and its standard deviation of 21.27% indicates a wide gap across countries. Stock market development (MKT) and credit market development ($CREDIT$) have mean values of 78.53% and 101.91% with standard deviations of 57.8% and 50.7%, respectively. During the sample period, investor sentiment ($Stwits_t$)[14] on average is 0.21 and its changes ($\Delta \ln(Stwits_t)$) is negative (-0.2%), while the changes in the sentiment measure from Reddit ($\Delta \ln(Reddit_t)$) is positive (0.1%). Table 1 Panel B reports comparative statistics for a sub-sample with a pre- and post-event two-day window $(-2, +2)$.

[13] The reason for D_0, D_1, D_2 having different sample statistics is that when a hacking event is announced during weekend, there is no corresponding stock market return on the attack announcement date (D_0) and such observations are excluded from our sample.

[14] The standard for identifying investor sentiment from -1(totally negative) to +1(totally positive).

Table 1 Summary statistic.

	No.Obs	Mean	SD	Min	Max
Panel A: Full sample					
$R_{j,t}$	84,708	0.025	1.165	-13.9518	12.9684
$R^{BTC}_{j,t}$	21,328	0.22	3.766	-75.644	72.447
$Spread_{j,t}$	17,606	64.264	198.8	0.010	3333.15
ΔBTC	33,090	0.004	0.046	-0.415	0.606
D_0	84,747	0.012	0.109	0	1
D_1	84,747	0.017	0.131	0	1
D_2	84,747	0.017	0.131	0	1
M	84,747	0.078	0.268	0	1
Bubble	84,747	0.120	0.325	0	1
SP	84,747	2.479	21.274	-49.144	71.655
Volatility	71,175	18.34	5.525	7.500	41.230
MKT	84,747	78.53	57.750	6.274	352.156
CREDIT	84,747	101.91	50.731	13.668	256.200
GDP growth	81,989	0.660	1.191	-6.300	22.340
GDP percap	84,747	9.946	1.036	7.252	11.436
M3	82,790	0.594	1.274	-5.250	16.832
Inflation	84,747	3.581	5.786	-2.855	50.623
Saving	84,747	25.172	8.185	9.593	49.233
Popurban	84,747	74.325	15.513	31.280	100.000
Stwits_t	1,929	0.213	0.170	-0.255	0.587
$\Delta \ln(Stwits_t)$	41,964	-0.002	0.563	-5.256	4.345
$\Delta \ln(Reddit_t)$	44,499	0.001	0.218	-1.520	1.169
Panel B: Two-day window subsample (-2,+2)					
$R_{j,t}$	7,254	0.022	1.166	-11.028	7.238
SP	7,254	0.572	20.25	-49.144	71.655
Volatility	4,563	18.07	5.642	7.5	41.23
MKT	7,254	79.03	57.973	6.274	352.156
CREDIT	7,254	102.2	51.606	13.668	256.200
GDP growth	7,045	0.662	1.354	-6.3	22.34
GDP percap	7,254	9.968	1.029	7.252	11.436
M3	7,127	0.508	1.140	-4.820	9.742
inflation	7,254	3.691	6.453	-2.855	50.623
Saving	7,254	25.294	8.055	9.593	49.233
Popurban	7,254	74.622	15.400	31.28	100
$\Delta \ln(Stwits_t)$	4,056	-0.028	0.389	-1.520	1.022
$\Delta \ln(Reddit_t)$	4,212	-0.008	0.271	-1.520	0.682

This table reports summary statistics for the data set used in this study, covering the period 2011 to 2019. Panel A reports the summary statistics of the full sample, while Panel B reports those of a sub-sample with a pre- and post- two-day window period. $R_{i,t}$ measures daily changes in stock market index return at the country level, defined as $log(stock_{i,t}/stock_{i,t-1})$. $R^{BTC}_{j,t}$ measures the daily bitcoin return at the crypto exchange level, defined as $log(BTC\ price_{i,t}/BTC\ price_{i,t-1})$. $Spread_{j,t}$ denotes the daily bid-ask spread at the crypto exchange level. ΔBTC is the average daily change in bitcoin price across crypto exchanges. D_0, D_1, D_2 are indicator variables, taking a value of 1 for the attack announcement date, the first, and second trading day after the attack announcement date, respectively. M is a binary variable and takes a value of 1 if there is more than one hacking events announced within the same month and 0 otherwise. *Bubble* is a time dummy for bitcoin market bubble in 2018 and 0 otherwise. *SP* denotes the annual changes in global stock index. *Volatility* denotes the annual standard deviation of stock market. *MKT* denotes the ratio of listed companies' market capitalization over GDP. *CREDIT* denotes the ratio of domestic credit to private sectors over GDP. *GDP growth* denotes the quarterly GDP growth rate. *GDP percap* is the logarithmic GDP per capita (in USD). *M3* is the monthly broad money growth rate. *Inflation* is measured by GDP deflator. *Saving* denotes the ratio of saving over GDP. *Popurban* denotes the proportion of people living in urban areas. $Stwits_t$ is a measure of investor sentiment in the StockTwists community, ranging from -1 (negative sentiment) to +1 (positive) and $\Delta \ln(Stwits_t)$ denotes the daily changes in *Stwits* . $\Delta \ln(Reddit_t)$ denotes the daily changes in a sentiment measure from the Reddit website.

4. Empirical results

4.1. The flight-to-safety effect

Cybercrime undermines investors' confidence in crypto markets, inducing asset re-allocation to less risky investment such as stocks. We expect hacking attacks to have a negative impact on cryptocurrency markets but a positive impact on stock markets, thereby signifying a flight-to-safety effect. We first investigate how the announcements of attacking events affect crypto markets in terms of bitcoin returns and bitcoin liquidity, as shown in Eq.(1) and Eq.(2), respectively.

$$R_{j,t}^{BTC} = \alpha + \beta_0 D_0 + \beta_1 D_1 + \beta_2 D_2 + \beta_3 \Delta BTC_{t-1} + \gamma_j + \epsilon_t \tag{1}$$

$$Spread_{j,t} = \alpha + \beta_0 D_0 + \beta_1 D_1 + \beta_2 D_2 + \beta_3 \Delta BTC_{t-1} + \gamma_j + \epsilon_t \tag{2}$$

where the dependent variable $R_{j,t}^{BTC}$ in Eq.(1) and $Spread_{j,t}$ in Eq.(2) denotes the daily bitcoin return and the bid-ask spread of the j-th crypto exchange at date t, respectively.[15] D_0, D_1 and D_2 are dummy variables for dating hacking events. D_0 denotes the attack announcement date reported by the mainstream media, while D_1 and D_2 denote the first and second calendar day after the attack announcement, respectively. Note that D_0, D_1, D_2 are set according to calendar days which may slightly depart from the trading days defined in Section 3 and applied to Eq.(3), given that the crypto markets operate 24/7. ΔBTC_{t-1} is the lagged average daily changes in bitcoin price across bitcoin exchanges, γ_j is the crypto exchange fixed effect, and ϵ is an error term.

Estimation results from Eq.(1) and Eq.(2) are reported in Table 2 and all regressions control for bitcoin price fluctuations and the crypto exchange fixed effect.[16] Columns (1) to (3) show that the average contemporaneous estimate of β_0 on D_0 is significantly different from zero across a range of specifications, suggesting a decline in bitcoin returns with respect to hacking attack announcements. The effect is economically sizeable and statistically significant. On average, following attack announcements, the bitcoin returns attenuate by about 43% compared with those of no attack periods. This effect dies out rapidly as the coefficients on D_1 and D_2 are insignificant, suggesting that crypto markets react to hacking events instantly without any delay. Regarding the impact of hacking attacks on bitcoin liquidity, we follow Stange and Kaserer (2011) to bring liquidity costs into our regression analysis. Columns (4)-(6) present the estimation results from Eq.(2). Consistent with Chordia et al. (2001), we find that after hacking attack announcements, bitcoin liquidity becomes worse and liquidity risk emerges in the crypto markets. The attack announcement increase

[15] Bitcoin returns from exchanges lsuch as Bitfinex, Bitstamp, BitX, CEX.IO, Coinbase, EXMO, Gemini, itBit, Kraken, and Others; and bitcoin bid-ask spreads from exchanges such asBitfinex, Bitstamp, BTCE, CEX.IO, Coinbase, Gemini, ItBit, LakeBTC, Okcoin, and Others.

[16] As our key variables, D_0, D_1, D_2, are dummy variables, we cannot use the fixed effect estimator. Instead, we employ the OLS estimator while controlling for exchanges and year fixed effect.

the bid-ask spread by about 30 percentage points every day during the hacking attacks period (D_0 , D_1, D_2) and the effect is more statistically and economically significant at D_1. The overall evidence shows that hacking attacks on average are associated with a decrease in bitcoin return by 43% and a rise in liquidity costs amounts to an additional 30 percentage points in bid-ask spread.

Table 2 BTC markets towards hack events.

	(1)	(2)	(3)	(4)	(5)	(6)
Dependent variable:		$R_{j,t}^{BTC}$			$Spread_{j,t}$	
D_0	-0.427**	-0.429**	-0.428**	29.12*	29.63*	30.08*
	(-2.02)	(-2.03)	(-2.02)	(1.89)	(1.92)	(1.95)
D_1		-0.14	-0.139		31.23**	31.68**
		(-0.50)	(-0.49)		(1.96)	(1.99)
D_2			0.09			29.56*
			(0.40)			(1.76)
ΔBTC_{t-1}	22.48***	22.47***	22.47***	53.94	55.64	56.66
	(8.55)	(8.55)	(8.55)	(1.03)	(1.07)	(1.09)
Constant	0.151*	0.153**	0.152*	7.61***	7.08***	6.62***
	(1.94)	(1.96)	(1.94)	(15.12)	(12.45)	(10.57)
Exchange FE	Yes	Yes	Yes	Yes	Yes	Yes
Observations	21,326	21,326	21,326	13,822	13,822	13,822
R-squared	0.048	0.048	0.048	0.354	0.354	0.355

This table reports regression results for the impact of hacking attack announcements on crypto markets in terms of bitcoin return and bitcoin liquidity over the period 2011-2019. All coefficients are presented in percent. We consider heteroscedasticity and robust standard errors. $R_{j,t}^{BTC}$ measures the daily bitcoin return at the crypto exchange level, defined as $log(BTC\ price_{i,t}/BTC\ price_{i,t-1})$. $Spread_{j,t}$ denotes the daily bid-ask spread at the crypto exchange level. D_0, D_1, D_2 are indicator variables, taking a value of 1 for the attack announcement date, the first, and the second calendar day after the attack announcement date, respectively. ΔBTC_{t-1} is the lagged average daily change of bitcoin price across crypto exchanges. Exchange FE denotes the exchange fixed effect. T-statistics are reported in parentheses and ***, **, * signify the 1%, 5%, and 10% significance level, respectively.

As a response to security concerns, the declining confidence and rising uncertainty around crypto markets are likely to trigger and/or enhance flight-to-safety behaviors. To justify this conjecture, we treat hacking attacks in crypto markets as exogenous shocks to stock markets and examine how stock markets react to those shocks under a global investigation. Our baseline model is shown in Eq.(3), with control for heterogeneity across countries and over years.

$$R_{i,t} = \alpha + \beta_0 D_0 + \beta_1 D_1 + \beta_2 D_2 + \delta_i X_{i,t} + \gamma_i + \gamma_{year} + \epsilon_{i,t} \quad (3)$$

$R_{i,t}$ is daily changes in stock market return of the i-th country at date t.[17] We pay our attention to the dummy variables - D_0, D_1, D_2, dating hacking attacks for the announcement date, the

[17] The results remain robust when using dividend-adjusted returns.

first, and the second trading day after the announcement date, respectively. $X_{i,t}$ is a set of control variables in country i at date t; γ_i and γ_{year} are the country and year fixed effects, respectively; and $\epsilon_{i,t}$ is an error term.

Table 3 reports estimation results from our baseline model in Eq.(3). We account for heteroscedasticity robust standard errors in the panel. The coefficients on D_0 and D_1 are statistically significant with a positive sign as expected in all model specifications, while the coefficient on D_2 is insignificant. As shown in column (3), stock market returns increase by 15% on the announcement date, compared to those on the days without attack announcements. This effect continues with a further increase by 7% on the first trading day (D_1) after the attack announcement but vanishes on the second trading day (D_2).

Concerning the omitted variable problem that stock market performance may also be driven by time-varying country level heterogeneity (Levine et al. 2000, Djankov et al. 2007, Hsu et al. 2014, Chen et al. 2017), we introduce a set of control variables to our baseline model. We control for the characteristics of stock markets in terms of the global stock market index growth (*SP*) and stock market volatility (*Volatility*) in column (4) and cross-country variations in financial development (proxied by stock market capitalization *MKT* and credit to the private sector *CREDIT*) in column (5), and the results remain unchanged. In column (6), we further control for macroeconomic conditions (proxied by *GDP growth*, *GDP percap*, *M3*, *Inflation*, *Saving* and *Popurban*) along with the characteristics of stock market and financial development, our main results are robust. On average, hacking announcements are followed by an 11% increase in stock market return.

Although we have controlled for country-specific stock market characteristics and general macroeconomic conditions, our model may still face potential omitted variable problems. We carry out a battery of additional tests. First, literature has shown the connection between investment behavior and investors' religious backgrounds (e.g., Hilary and Hui 2009, Callen and Fang 2015). We include dummy variables ($Buddhism$, $Catholic$, $Muslim$, and $Protestant$) to control for countries religion. Secondly, cryptocurrencies are unregulated and anonymous, which makes them attractive to shadow economy participants. As such, we include the size of shadow economy as a country level control. Thirdly, recent studies suggest that culture and trust play an important role in stock market returns (Engelberg et al. 2012, Chang and Lin 2015, Liu 2019, Caporale and Kang 2020), especially during the COVID-19 period (Fernandez-Perez et al. 2021). We include cultural tightness to show that a country with a tight (loose) culture has strong (weak) social norms and low (high) tolerance for deviant behaviour (Gelfand et al. 2011, Eun et al. 2015), individualism that measures the extent to which people focus on their internal attributes and tend to differentiate themselves from others (Hofstede and Hofstede 1984, Eun et al. 2015), and a measure of trust behaviour with a higher value indicating a more trustworthy environment. Results and detailed variable definitions are reported in the Appendix - Table A2. With the inclusion of these additional controls, our main results hold.

To address the potential issue of inflated statistical power in our pooled regression setting, we cluster the standard errors by continent, income group and developed/developing country group, respectively, and our results hold with at least one of the coefficient on the post-event period (D_0, D_1, D_2) are positive and statistical significant. We also run regressions by income groups separately and our results hold for high and upper middle income country groups but not for the lower middle income country group. We further consider the geographical location and run regression by continents separately and our results hold except for Africa and South America.[18]

In short, we have found robust evidence for the flight-to-safety effect. Given the hacking attacks, we observe rising stock returns, along with declining bitcoin returns and liquidity across cryptocurrency exchanges for at least 2 trading days. This effect turns out to be worldwide, supporting our hypothesis (H1) that *Cyber attacks on crypto markets undermine existing and prospective cryptocurrency investors' confidence and simultaneously increase their risk awareness and trigger their fear, resulting in a flight-to-safety effect to stock markets.*

4.2. The impact of consecutive attacks

As shown in Figure 1, attacks arrive consecutively, resulting in huge losses in terms of the dollar value of stolen coins. Concerning that consecutive attacks may weaken the confidence in crypto markets and increase investors' risk perception, we test whether recurring attacks in crypto markets amplify the flight-to-safety effect. In this respect, we define a period as under consecutive attacks if there is more than one attack in the same month. In addition, we introduce an additional dummy variable, M, and its interaction terms with $D_j, j \in (0,2)$ to our baseline model in Eq.(3). We examine whether and how stock markets react differently during high-frequency attack episodes relative to low-frequency periods. The empirical specification is delineated in Eq.(4):

$$R_{i,t} = \alpha + \beta_j D_j + \theta M_t + \lambda_j D_j * M_t + \delta_i X_{i,t} + \gamma_i + \gamma_{year} + \epsilon_{i,t} \tag{4}$$

Estimation results are reported in Table 4. The coefficients on the interaction terms $D_j \times M$ (j=0,1,2) are of our particular interest to assess the impact of consecutive attacks on stock markets. As shown in columns (1)-(6), the point estimates of the effect of multiple attacks at the attack announcement date ($D_0 \times M$) is positively and statistically significant at the 1% or 5% level. This effect is insignificant on the following first trading day ($D_1 \times M$) but significant on the second trading day ($D_2 \times M$). As shown in column (6), after controlling for a set of country-specific factors,

[18] Results are not reported for the sake of brevity, but they are available from the authors on request.

Table 3 Flight to safety during hack attacks.

	(1)	(2)	(3)	(4)	(5)	(6)
Dependent variable:				$R_{i,t}$		
D_0	0.145***	0.147***	0.147***	0.113**	0.147***	0.117**
	(3.94)	(3.98)	(3.99)	(2.37)	(3.99)	(2.43)
D_1		0.064**	0.065**	0.116***	0.065**	0.106***
		(2.11)	(2.11)	(2.97)	(2.11)	(2.69)
D_2			0.006	0.041	0.006	0.057
			(0.18)	(1.06)	(0.18)	(1.44)
SP				0.003***		0.003***
				(9.14)		(8.67)
Volatility				-0.0001		0.0001
				(-0.05)		(0.07)
MKT					0.0004	-0.0004
					(1.26)	(-1.08)
CREDIT					-0.0002	0.0005
					(-0.40)	(0.73)
GDP growth						0.005
						(1.24)
GDP percap						-0.078
						(-0.56)
M3						-0.008**
						(-2.12)
Inflation						0.001
						(0.61)
Saving						0.001
						(0.32)
Popurban						0.004
						(0.43)
Constant	-0.103***	-0.104***	-0.104***	-0.030	-0.101***	0.250
	(-3.80)	(-3.82)	(-3.82)	(-0.43)	(-3.61)	(0.21)
Year FE	Yes	Yes	Yes	Yes	Yes	Yes
Country FE	Yes	Yes	Yes	Yes	Yes	Yes
Observations	84,708	84,708	84,708	71,136	84,708	67,990
R-squared	0.002	0.002	0.002	0.003	0.002	0.003

This table reports regression results for the flight-to-safety effect over the period 2011-2019. We consider heteroscedasticity and robust standard errors. The dependent variable $R_{i,t}$ measures daily changes in stock market index return at the country level, defined as $log(stock_{i,t}/stock_{i,t-1})$. D_0, D_1, D_2 are indicator variables, taking a value of 1 for the attack announcement date, the first, and the second trading day after the attack announcement date, respectively. *SP* denotes the annual changes in global stock index. *Volatility* denotes the annual standard deviation of stock market. *MKT* denotes the ratio of listed companies' market capitalization over GDP. *CREDIT* denotes the ratio of domestic credit to private sectors over GDP. *GDP growth* denotes quarterly GDP growth rate. *GDP percap* measured by the logarithmic GDP per capita (in USD). *M3* is the monthly broad money growth rate. *Inflation* denotes inflation measured by GDP deflator. *Saving* denotes as the ratio of saving over GDP. *Popurban* denotes the proportion of people living in urban areas. Country FE is the country fixed effect and Year FE is the year fixed effect. T-statistics of the test are reported in parentheses and ***, **, * signify the 1%, 5%, and 10% significance level, respectively.

stock market return on average is higher by 5.8% during a period of frequent attacks compared with that of those months with one or no cyber attacks on crypto markets, indicated by the positive and significant coefficient on M. Under a sequence of attacks, on average, the stock markets experience a rise in returns by 27% on the date of announcement ($D_0 \times M$), no extra gain on the following first trading day ($D_1 \times M$),[19] and a surge by 43.5% on the second trading day ($D_2 \times M$). When introducing interaction terms, the meaning of the coefficients on D_j (j=0,1,2) are not directly comparable to those in Table 3. We focus on the overall marginal effect of consecutive attacks and we find that stock market returns increase by 26% on D_0 and 33% on D_2 (insignificant on D_1). The overall impact of consecutive attacks on stock market return is stronger compared with those in Table 3.[20] Our results reveal investors' differential behaviour. With the initial attack, some risk sensitive investors react acutely on the announcement day, whereas others hesitate and take a "wait-and-see" action until their confidence eventually collapses after further attacks. The overall evidence supports Hypothesis 2 that *Consecutive attacks strengthen the flight-to-safety effect.*

4.3. The flight-to-safety effect: The role of social media

Social media have become prevalent platforms for sharing information, which is particularly true for the cryptocurrency community. Early study has found that messages written by bitcoin developers and investors are a rich source of information (Linton et al. 2017), and messages and discussions on social media affect the movement of bitcoin prices (Mai et al. 2015). The information on crypto markets is neither as abundant nor as efficient as that on stock markets, hence investors or traders are inclined to gather and exchange information via social media.

In this section, we advance our analysis by exploring the underlying pressure of the flight-to-safety. We consider a sentiment measure developed by Chen et al. (2019) based on social media messages from StockTwits, where players share information, express opinions and moods instantly. The smaller the sentiment value, the more pessimistic investors become. Figure 2 shows a boxplot of the changes of sentiment during a 3-day pre- and post-attack event window period (-3,+3). Prior to the event date, a number of pessimistic outliers emerge and the greatest dispersion is exhibited from $t-3$ to $t-2$, reflecting diverse opinions. The blue dots in the first two days are the maximum negative sentiment exceeding the estimation for 95% confidence level. The observed outliers are the extremely bearish sentiment expressed by the social media users who suffer from huge losses. The boxplots at $t-1$ and t display a left-skewed distribution, implying the predominance of bearish mood. Although the median changes slightly, the mean is implied to be much lower than the median given the asymmetric skewedness. We may draw a conclusion that social media sentiment conveys attack information prior to the official announcements.

[19] The stock return increases 12.7% at (D_1) regardless of the consecutive attack period or not.

[20] As the flight-to-safety effect tends to be short-term while it doesn't happen frequently, we define the consecutive attack period in same-month interval. Employing an alternative two-week rolling window to define the consecutive attack period, results are consistent (unreported results are available from the authors on request).

Table 4 Flight to safety during repeated attacks.

	(1)	(2)	(3)	(4)	(5)	(6)
Dependent variable:				$R_{i,t}$		
D_0	0.071	0.073	0.071	0.003	0.071	-0.003
	(1.46)	(1.50)	(1.46)	(0.05)	(1.46)	(-0.06)
M	0.008	0.010	-0.011	0.062**	-0.011	0.058**
	(0.49)	(0.60)	(-0.59)	(2.46)	(-0.59)	(2.28)
D_0 × M	0.171**	0.169**	0.189**	0.240**	0.189**	0.27***
	(2.26)	(2.23)	(2.49)	(2.38)	(2.49)	(2.65)
D_1		0.097**	0.094**	0.143***	0.094**	0.127***
		(2.56)	(2.51)	(2.99)	(2.51)	(2.64)
D_1 × M		-0.100	-0.079	-0.133	-0.079	-0.112
		(-1.51)	(-1.19)	(-1.55)	(-1.19)	(-1.29)
D_2			-0.093**	-0.126***	-0.093**	-0.106**
			(-2.48)	(-2.65)	(-2.48)	(-2.19)
D_2 × M			0.297***	0.450***	0.297***	0.435***
			(4.50)	(5.26)	(4.50)	(5.03)
SP				0.003***		0.003***
				(9.14)		(8.67)
Volatility				-0.0001		0.0001
				(-0.05)		(0.07)
MKT					0.0004	-0.0004
					(1.26)	(-1.08)
CREDIT					-0.0002	0.0005
					(-0.40)	(0.72)
GDP growth						0.005
						(1.14)
GDP percap						-0.077
						(-0.55)
M3						-0.008**
						(-2.11)
Inflation						0.001
						(0.61)
Saving						0.001
						(0.32)
Popurban						0.004
						(0.43)
Constant	-0.103***	-0.104***	-0.103***	-0.029	-0.100***	0.245
	(-3.79)	(-3.82)	(-3.79)	(-0.41)	(-3.58)	(0.21)
Year FE	Yes	Yes	Yes	Yes	Yes	Yes
Country FE	Yes	Yes	Yes	Yes	Yes	Yes
Observations	84,708	84,708	84,708	71,136	84,708	67,990
R-squared	0.002	0.002	0.002	0.003	0.002	0.003

This table reports regression results for the flight-to-safety effect under consecutive hacking attacks in crypto markets over the period 2011-2019. All coefficients are presented in terms of percent. We consider heteroscedasticity and robust standard errors.$R_{i,t}$ measures daily changes in stock market index return at the country level, defined as $log(stock_{i,t}/stock_{i,t-1})$. D_0, D_1, D_2 are indicator variables, taking a value of 1 for the attack announcement date, the first, and the second trading day after the attack announcement date, respectively. M is a binary variable and takes a value of 1 if there is more than one hacking events announced within the same month and 0 otherwise. *SP* denotes the annual changes in global stock index. *Volatility* denotes the annual standard deviation of stock market. *MKT* denotes the ratio of listed companies' market capitalization over GDP. *CREDIT* denotes the ratio of domestic credit to private sectors over GDP. *GDP growth* denotes quarterly GDP growth rate. *GDP percap* measured by the logarithmic GDP per capita (in USD). *M3* is the monthly broad money growth rate. *Inflation* denotes inflation measured by GDP deflator. *Saving* denotes as the ratio of saving over GDP. *Popurban* denotes the proportion of people living in urban areas. Country FE is the country fixed effect and Year FE is the year fixed effect. T-statistics are reported in parentheses and ***, **, * signify the 1%, 5%, and 10% significance level, respectively.

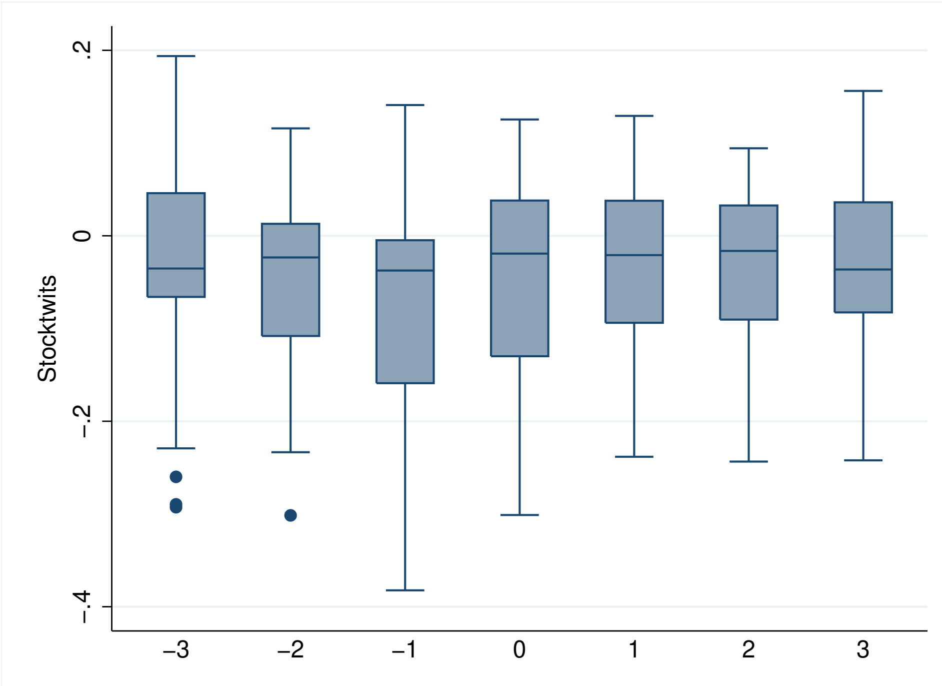

Figure 2 Sentiment variation around hacking event announcement.
This figure presents boxplot of the changes in sentiment during the hacking period with pre- and post-event 3-day window. The horizontal line in the boxes represents the median, while blue dots are the outliers.The sentiment is extracted from Stocktwits from 2014 to 2018.

To empirically test whether hacking events announcements can be predicted by the changes in investor sentiment, we construct panel data for each event and adopt a logistic model shown in Eq.(5), where $p_t = P(D_{0,t} = 1)$ indicates the probability of the occurrence of attacks. The sentiment indicator is the explanatory variable for such prediction in probability.

$$\log \frac{p_t}{1-p_t} = \alpha + \beta Sentiment_{t-j} + \epsilon_t \qquad j \in (1,3), \qquad Sentiment_t \in \{Stwits_t, \Delta \ln(Stwits_t), \Delta \ln(Reddit_t)\} \tag{5}$$

We employ a variety of sentiment measures from different social media channels, either at the level or in the log changes to ensure the robustness of our results. $Stwits_t$ is a sentiment measure from StockTwits, ranging from -1 to +1. $\Delta \ln(Stwits_t)$ is the daily log changes of $Stwits_t$ from *t-1* to t, and $\Delta \ln(Reddit_t)$ is applied to Reddit data. These two social media platforms potentially attract users with different interests (Chen et al. 2019). The discussions on StockTwits focus more on cryptocurrency speculation and investment, while the messages on Reddit are more about crypto technology and other general topics.

Columns (1) and (2) of Table 5 show the results from the full sample with the year and event fixed effect controlled. The estimate on $Stwits_{t-1}$ is statistically significant at the 1% level in most specifications, confirming our conjecture that social media sentiment is able to predict the probability of hacking news. As the number of cybercrimes rocketed during the crypto bubble period in 2018, we limit our attention to the year 2018 to further examine the predictive power of investor sentiment. The analysis focuses on changes in sentiment and results from $\Delta \ln(Stwits_{t-j})$ and $\Delta \ln(Reddit_{t-j})$, $j \in (1,3)$, are reported in columns (3)-(4) and columns (5)-(6), respectively. Those results consistently show a strong predictive power of sentiment in forecasting subsequent cybercrime announcements. We, therefore, confirm that discussions about hacking activities among social media users, have the predictive power for upcoming official cyber-attack announcements by crypto exchanges.[21]

To address the economic importance, we use the estimates in column (2) and document that a decrease by one standard deviation in sentiment at $t-1$, irrespective of the level of other regressors, increases the probability of observing attacks by $\frac{1}{1+\exp^{8\times 0.17}} = 20\%$. A fall in investor sentiment assigns a higher probability to the occurrence of attacks, which supports the literature in the context of the information content and predictability of social media messages (Chen and Hafner 2019, Nasekin and Chen 2020).

Given the discovered insights into investor sentiment during the hacking period (Figure 2), we pay particular attention to a sub-sample of the event period with a pre- and post-event two-day window (-2,+2) to mitigate the potential impact of noisy sentiment during the non-event period. We replace the hacking attack announcement indicators (D_j) $j \in (0,2)$ in Eq.(3) with the changes in sentiment ($\Delta \ln(Stwits_t)$ or $\Delta \ln(Reddit_t)$), as shown in Eq.(6). This allows us to directly examine how changes in sentiment related hacking events in crypto markets, as a measure of flight-to-safety pressure, affect stock market returns. Different from the lagged value of sentiment (sentiment prior to the event date) in Eq.(5) representing the sentiment from the informed investors, a contemporaneous change in sentiment at the event date captures a sentimental variation from the uninformed investors - a large group of people who have been unaware of fragmentary attacks and far behind the information.

$$R_{i,t} = \alpha + \beta_1 Sentiment_t + \delta_i X_{i,t} + \gamma_i + \gamma_{year} + \epsilon_{i,t}, \quad Sentiment_t \in \{\Delta \ln(Stwits_t), \Delta \ln(Reddit_t)\} \tag{6}$$

Estimation results from Eq.(6) are reported in Table 6. In column (1) and (2) , we observe a reverse movement between sentiment and stock returns, inferred by the negative sign of the

[21] The date of the cyber-attack precedes the official announcement date. It normally takes some time for crypto exchanges to discover the breach, conduct a security review, and fix the problems. A hacking announcement is submitted only when losses are beyond the exchange's capacity to cover it up. In Table 5, we provide evidence that social media users' negative sentiment may exert pressure on crypto exchanges to release the hacking news and can predict the official announcement of hacking events.

Table 5 **The likelihood of posting attacked news with sentiment change.**

	Full sample		Sub-period:year 2018			
	(1)	(2)	(3)	(4)	(5)	(6)
Dependent variable:	$P(D_{0,t}=1)$		$P(D_{0,t}=1)$			
$Stwits_{t-1}$	-6.489***	-8.025***				
	(-3.59)	(-4.00)				
$Stwits_{t-2}$		2.166				
		(1.19)				
$Stwits_{t-3}$		3.515*				
		(1.95)				
$\Delta\ln(Stwits_{t-1})$			-1.289***	-1.928***		
			(-3.19)	(-2.98)		
$\Delta\ln(Stwits_{t-2})$				-1.399*		
				(-1.68)		
$\Delta\ln(Stwits_{t-3})$				-0.818		
				(-1.41)		
$\Delta\ln(Reddit_{t-1})$					-1.789***	-2.089***
					(-3.30)	(-2.98)
$\Delta\ln(Reddit_{t-2})$						-0.046
						(-0.05)
$\Delta\ln(Reddit_{t-3})$						-0.802
						(-1.05)
Year FE	Yes	Yes	No	No	No	No
Event FE	Yes	Yes	Yes	Yes	Yes	Yes
Constant	-28.67	-32.695	-3.072***	-3.293***	-3.187***	-3.28***
	(-0.01)	(-0.00)	(-4.25)	(-3.98)	(-4.23)	(-4.05)
Pseudo R-square	0.085	0.112	0.053	0.062	0.063	0.068
Observations	985	918	440	418	440	418

This table reports regression results for the informativeness of investor sentiment in forecasting hacking event announcements, over the period of 2014–2018. We consider heteroscedasticity and robust standard errors. The dependent variable $P_t = P(D_{0,t}=1)$ indicates attack events announced at date t, and $D_{0,t}=0$ otherwise. We employ three measures of sentiment: (1) $Stwits_t$, distilled from StockTwits and in the range of -1 to +1; (2) $\Delta\ln(Swits_t)$, denotes the daily changes in $Stwits$; (3) $\Delta\ln(Reddit_t)$, denotes the daily changes in a sentiment measure from the Reddit website. Exchange FE is the exchange fixed effect. Year FE is the year fixed effect. T-statistics are reported in parentheses and ***, **, * signify the 1%, 5%, and 10% significance level, respectively.

coefficient on $\Delta\ln(Stwits_t)$ with the statistical significance at the 1% level. In the full specification after accounting for stock market characteristics, macro-economic factors, and country and year fixed effect, a 1% decrease in $\Delta\ln(Stwits)$ is associated with an increase in stock market return by 0.19% during the attacking period. The results from $\Delta\ln(Reddit)$ in the last three columns, in general, show a consistent picture.[22] All in all, we find that before the event being formally announced, social media sentiment serves as a warning indicator for hacking events. At the event episode, the sentiment is capable of capturing flight-to-safety pressure among a herd.

[22] In this small sample regression, we employ a range-based daily volatility Var_{RS}.

Table 6 Flight to safety under investor sentiment channel.

	(1)	(2)	(3)	(4)	(5)	(6)
Dependent variable:		$R_{i,t}$			$R_{i,t}$	
	Paenl A: $\Delta\ln(Stwits_t)$			Panel B: $\Delta\ln(Reddit_t)$		
Sentiment	-0.121***	-0.185***	-0.186***	-0.383***	-0.507***	-0.498***
	(-3.06)	(-3.46)	(-3.48)	(-7.03)	(-8.57)	(-8.43)
Var_{RS}		-10.377***	-10.304***		-10.685***	-10.615***
		(-10.29)	(-10.22)		(-10.37)	(-10.36)
SP		0.005*	0.005		0.004	0.005
		(1.69)	(1.61)		(1.60)	(1.56)
MKT			0.001			0.000
			(0.27)			(0.14)
CREDIT			0.001			0.001
			(0.29)			(0.25)
GDP growth			-0.056			-0.050
			(-0.99)			(-0.92)
GDP percap			2.271			1.439
			(1.14)			(0.78)
M3			0.046*			0.052**
			(1.88)			(2.15)
Inflation			0.022			0.024
			(0.64)			(0.72)
Saving			-0.021			-0.011
			(-0.74)			(-0.42)
Popurban			-0.119			-0.096
			(-1.34)			(-1.16)
Constant	0.302	0.231**	-14.082	0.258	0.194**	-7.204
	(1.40)	(2.47)	(-0.79)	(1.21)	(2.13)	(-0.44)
Year FE	Yes	Yes	Yes	Yes	Yes	Yes
Country FE	Yes	Yes	Yes	Yes	Yes	Yes
Observations	4,056	2,125	2,078	4,212	2,204	2,157
R-squared	0.013	0.071	0.075	0.021	0.087	0.090

This table reports regression results explaining the flight-to-safety effect in terms of investor sentiment. All coefficients are presented in terms of percent. We consider heteroscedasticity and robust standard errors. The sample is restricted to a sub-sample of a two-day pre- and post-event window (-2,+2) over the period 2014-2018. The dependent variable $R_{i,t}$ measures daily changes in stock market index return at the country level, defined as $log(stock_{i,t}/stock_{i,t-1})$. We use two measures of sentiment: $\Delta\ln(Swits_t)$, denotes the daily changes in *Stwits* and $\Delta\ln(Reddit_t)$ denotes the daily changes in a sentiment measure from the Reddit website. *SP* denotes the annual changes in global stock index. Var_{RS} denotes the daily ranged-based volatility of stock market across different countries (Rogers and Satchell 1991).*MKT* denotes the ratio of listed companies' market capitalization over GDP. *CREDIT* denotes the ratio of domestic credit to private sectors over GDP. *GDP growth* denotes quarterly GDP growth rate. *GDP percap* measured by the logarithmic GDP per capita (in USD). *M3* is the monthly broad money growth rate. *Inflation* denotes inflation measured by GDP deflator. *Saving* denotes as the ratio of saving over GDP. *Popurban* denotes the proportion of people living in urban areas. Country FE is the country fixed effect and Year FE is the year fixed effect. T-statistics are reported in parentheses and ***, **, * signify the 1%, 5%, and 10% significance level, respectively.

To inspect whether the flight-to-safety is concentrated on the bubble period, we undertake additional exploration by introducing *Bubble*, a time dummy for the bitcoin bubble in 2018. Investors who crowded into crypto markets during the bubble period for a speculative intention are susceptible to unexpected shocks. A certain proportion of investors lack financial and technological literacy and they are unlikely to make a wise financial decision. For instance, they may hold poorly diversified portfolios. Using microdata from 15 countries, Panos and Karkkainen (2019) find that financial literacy has a negative impact on the probability of owning cryptocurrency; in other words, those who are more financially literate are less likely to engage in highly volatile assets. They conclude that crypto markets are largely comprised of unsophisticated investors. During the bubble period, a skyrocketed cryptocurrency price attracts more unsophisticated investors than the usual time. When the bubble bursts following attacks by malicious hackers, we expect an unprecedented flight-to-safety pressure, which is examined in Eq.(7).

$$\begin{aligned} R_{i,t} = \alpha + \sum_{j=0}^{2} \theta_j D_j \times Sentiment_t \times Bubble + \sum_{j=0}^{2} \zeta_{jt} D_j \times Sentiment_t + \sum_{j=0}^{2} \eta_j D_j \times Bubble \\ + \sum_{j=0}^{2} \beta_j D_j + \rho Sentiment_t + \nu Bubble + \lambda Sentiment_t \times Bubble + \delta_i X_{i,t} + \gamma_i + \gamma_{year} + \epsilon_{i,t} \end{aligned} \tag{7}$$

where $j \in (0, 2)$, $Sentiment_t \in \{\Delta \ln(Stwits_t), \Delta \ln(Reddit_t)\}$.

Our main interest is on the triple interaction terms in Table 7, $D_j \times Bubble \times \Delta \ln(Stwits_t)$. In Panel A, the coefficient on the tripe interaction term is negative, statistically and economically significant, implying that the flight-to-safety pressure during the bubble period is more prominent than that of non-bubble period. In column (3), given a decline in sentiment by 1%, the difference in stock market reaction between the bubble period and non-bubble period is 0.35% on the date of the attacking announcement. This effect peaks at 1.08% on the first trading day after the announcement and slows down to a further 0.51% increase on the second trading day, showing a discernible economic significance in the bubble period. In Panel B, we employ an alternative sentiment measure of $\Delta \ln(Reddit_t)$ and we also find evidence for the flight-to-safety effect with a slightly different pattern - a much stronger effect on the event date and the second trading day after the hacking announcement. For 1% decline in sentiment, the stock market return is higher by 0.85% on the event date and 5.49% on the second trading day after the event announcement during the bubble period compared to those in non-bubble period. We attribute the different results to the diverse soft information on two social media platforms that the discussions on StockTwits are more about speculative opportunities while the messages on Reddit are more about crypto-related technology. To better gauge the timing of the flight-to-safety effect and constantly monitor the flight-to-safety pressure revealed in social media, we suggest future research to explore sentiment on StockTwits.[23]

[23] To address the potential mulcollinearity issue when the *Bubble* is a year dummy for 2018 along with year fixed effect, following Petersen (2009), we exclude the year fixed effect in the model with standard errors clustered by year, results are consistent.

In sum, the presence of a bubble attracts unsophisticated investors as well as greedy hackers. With intensive attacks by hackers, investors rectify their over-excitement and risk-attitudes toward digital assets. The collapse of confidence among a herd of existing and prospective investors, whilst a bubble bursts, is the major cause of this phenomenon. Our argument coincides with the flight-to-safety episodes interacting with VIX, a measure for market sentiment (Baele et al. 2020).

4.4. Robustness Tests

To enhance the robustness of results, we carry out two tests around the baseline model. The first robustness test is formulated in Eq.(8) where we focus on the stock return reactions during the event window period and lengthen the window further to test the duration of the flight-to-safety effect.

$$R_{i,t} = \alpha + \beta_0 D_\tau + \delta_i X_{i,t} + \gamma_i + \gamma_{year} + \epsilon_{i,t}, \quad t \in (-\tau, \tau) \tag{8}$$

$$D_\tau = \begin{cases} 1, & 0 \leq t \leq \tau \\ 0, & -\tau \leq t < 0 \end{cases}$$

Clearly, $\tau = 0$ indicates the event date. We pay our attention to an indicator variable - D_τ, splitting the observations in the window period into the pre- and post-event groups. $X_{i,t}$ are vectors of country-specific control variables in country i at date t; γ_i and γ_{year} are the country and year fixed effects, respectively; and $\epsilon_{i,t}$ is an error term. In Table 8, the coefficients on D_τ over a range of τ are overwhelmingly significant until a window of 30 trading days. The positive sign indicates the stock index returns during the post-event window are pumping up, compared to those in the pre-event period. By lengthening the window period, one observes that the flight-to-safety effect is persistent, lasting up to 30 trading days.

In the second robustness check, we conduct a firm-level data as a supplementary verification to the study on the country-level data. To ensure that the flight-to-safety is applied to the firm-level investigation, for the dependent variables in the baseline model we consider the log returns of the stocks that are the constituents of S&P 500 index.[24]

$$R_{f,t} = \alpha + \beta_j D_j + \theta X_t + \gamma_s + \gamma_{year} + \epsilon_{i,t} \quad j \in (0, 2) \tag{9}$$

where $R_{f,t}$ is the daily change of stock price of the f-th firm at date t. D_j is a set of dummy variables as usual. In order to control the fluctuation of economic uncertainty, we add a list of control

[24] For the purpose of robustness, we accentuate the US market for the reason that, bitcoin trading in the US market has occupied more than half of the trading volume worldwide (Patrick et al. 2019).

Table 7 Flight to safety during bubble period.

	(1)	(2)	(3)	(4)	(5)	(6)
Dependent variable:		$R_{i,t}$			$R_{i,t}$	
Sentiment	Paenl A: $\Delta\ln(Stwits_t)$			Panel B: $\Delta\ln(Reddit_t)$		
D_0 × Bubble × Sentiment$_t$	-0.308	-0.343*	-0.351*	-0.327	-0.835*	-0.853*
	(-1.57)	(-1.66)	(-1.69)	(-0.73)	(-1.65)	(-1.71)
D_1 × Bubble × Sentiment$_t$	-1.213***	-1.036***	-1.078***	0.447*	0.222	0.224
	(-5.00)	(-3.26)	(-3.34)	(1.76)	(0.69)	(0.69)
D_2 × Bubble × Sentiment$_t$	-0.251*	-0.511***	-0.508***	-5.131***	-5.676***	-5.490***
	(-1.84)	(-3.14)	(-3.17)	(-8.93)	(-8.43)	(-7.86)
D_0	-0.277***	-0.324***	-0.299***	-0.261***	-0.360***	-0.337***
	(-5.07)	(-5.08)	(-4.69)	(-3.32)	(-4.09)	(-3.82)
Sentiment$_t$	0.015	0.014	0.019	-0.005	-0.005	-0.006
	(1.42)	(1.05)	(1.37)	(-0.16)	(-0.10)	(-0.13)
D_0 × Sentiment$_t$	-0.056	-0.061	-0.060	-0.013	0.395	0.411
	(-0.48)	(-0.49)	(-0.47)	(-0.03)	(0.83)	(0.87)
D_0 × Bubble	0.473***	0.584***	0.560***	0.440***	0.603***	0.582***
	(5.91)	(6.51)	(6.24)	(4.45)	(5.57)	(5.36)
D_1	0.137***	0.164**	0.139**	0.174***	0.197***	0.175***
	(2.70)	(2.37)	(1.98)	(3.56)	(2.95)	(2.59)
D_1 × Sentiment$_t$	0.709***	0.459*	0.492*	-1.012***	-1.002***	-1.012***
	(3.81)	(1.83)	(1.92)	(-5.69)	(-4.26)	(-4.28)
D_1 × Bubble	-0.134*	-0.100	-0.071	-0.160**	-0.116	-0.090
	(-1.75)	(-1.03)	(-0.72)	(-2.12)	(-1.23)	(-0.94)
D_2	-0.092	-0.117	-0.103	-0.247***	-0.285***	-0.279***
	(-1.34)	(-1.25)	(-1.12)	(-4.00)	(-3.65)	(-3.51)
D_2 × Sentiment$_t$	0.106	0.167	0.166	5.060***	5.377***	5.195***
	(0.99)	(1.23)	(1.25)	(8.91)	(8.07)	(7.51)
D_2 × Bubble	0.021	0.093	0.089	0.161*	0.241**	0.244**
	(0.24)	(0.82)	(0.79)	(1.90)	(2.39)	(2.39)
Bubble	-0.177***	-0.191***	-0.243***	-0.083***	-0.081***	-0.095*
	(-7.70)	(-6.22)	(-4.53)	(-3.88)	(-2.79)	(-1.86)
Bubble × Sentiment$_t$	0.015	0.065	0.064	-0.076	0.000	0.002
	(0.40)	(1.39)	(1.37)	(-1.41)	(0.00)	(0.03)
Constant	0.111*	0.225***	-9.786	0.019	0.109***	-4.169
	(1.69)	(6.28)	(-1.59)	(0.31)	(3.19)	(-0.71)
Stock market controls	No	Yes	Yes	No	Yes	Yes
Country economics controls	No	No	Yes	No	No	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes
Country FE	Yes	Yes	Yes	Yes	Yes	Yes
Observations	41,964	21,770	21,075	44,499	23,071	22,340
R-squared	0.004	0.033	0.032	0.007	0.034	0.032

This table reports regression results for a stronger flight-to-safety effect driven by sentiment during the bitcoin bubble period. All coefficients are presented in terms of percent. The sample period is restricted to 2014 to 2018 due to sentiment data availability and we consider heteroscedasticity and robust standard errors. The dependent variable $R_{i,t}$ measures daily changes in stock market index return at the country level, defined as $log(stock_{i,t}/stock_{i,t-1})$. D_0, D_1, D_2 are indicator variables, taking a value of 1 for the attack announcement date, the first, and the second trading day after the attack announcement date, respectively. We use two measures of sentiment. $\Delta\ln(Stwits_t)$ denotes the daily changes in sentiment measure of StockTwits. $\Delta\ln(Reddit_t)$ denotes the daily changes in a sentiment measure from the Reddit website. *Bubble* is a dummy variable, taking a value of 1 for the year 2018, and 0 otherwise. Control variables in column (2) and (5) include SP - the annual changes in global stock return and Var_{RS} - a ranged-based daily volatility measure of stock market. Macro economic controls in column(3) and (6) include MKT denotes the ratio of listed companies' market capitalization over GDP; $CREDIT$ denotes the ratio of domestic credit to private sectors over GDP; *GDP growth* denotes quarterly GDP growth rate; *GDP percap* measured by the logarithmic GDP per capita (in USD); *M3* is the monthly broad money growth rate; *Inflation* denotes inflation measured by GDP deflator; *Saving* denotes as the ratio of saving over GDP; *Popurban* denotes the proportion of people living in urban areas. Country FE is the country fixed effect and Year FE is the year fixed effect. T-statistics are reported in parentheses and ***, **, * signify the 1%, 5%, and 10% significance level, respectively.

Table 8 Flight to safety under various window group.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Window:	(-1,+1)	(-2,+2)	(-3,+3)	(-6,+6)	(-10,+10)	(-15,+15)	(-30,+30)
D	0.198***	0.156***	0.214***	0.250***	0.236***	0.162***	0.036***
	(3.73)	(4.14)	(7.09)	(11.12)	(13.16)	(10.68)	(2.89)
SP	0.003	0.003*	0.003**	0.003***	0.002***	0.003***	0.003***
	(1.27)	(1.91)	(2.56)	(3.25)	(3.16)	(5.23)	(6.59)
Volatility	-0.002	0.008	0.007	0.008	0.003	0.001	0.001
	(-0.21)	(0.90)	(0.91)	(1.49)	(0.63)	(0.15)	(0.40)
MKT	0.001	-0.001	-0.002	-0.001	-0.000	-0.000	-0.000
	(0.27)	(-0.64)	(-1.21)	(-0.62)	(-0.35)	(-0.42)	(-0.85)
CREDIT	0.002	0.002	0.002	0.001	0.001	0.001	0.001
	(0.61)	(0.60)	(0.75)	(0.72)	(0.70)	(1.37)	(0.77)
GDP growth	-0.002	0.001	0.007	0.007	0.003	0.008	0.007
	(-0.08)	(0.04)	(0.45)	(0.72)	(0.42)	(1.06)	(1.09)
GDP percap	1.414	0.680	0.220	-0.243	0.084	0.051	-0.097
	(1.53)	(0.95)	(0.37)	(-0.57)	(0.25)	(0.18)	(-0.45)
M3	0.065**	0.009	0.007	0.001	-0.003	-0.010	-0.014**
	(2.52)	(0.44)	(0.45)	(0.06)	(-0.38)	(-1.25)	(-2.43)
Inflation	0.009	0.013	0.004	0.006	0.002	0.002	0.006
	(0.38)	(0.82)	(0.34)	(0.64)	(0.34)	(0.30)	(1.29)
Saving	-0.020	-0.017	-0.008	0.002	-0.002	0.002	0.003
	(-0.86)	(-1.03)	(-0.56)	(0.16)	(-0.31)	(0.24)	(0.64)
Popurban	-0.036	-0.006	0.021	0.003	0.012	0.016	0.009
	(-0.50)	(-0.10)	(0.48)	(0.10)	(0.47)	(0.81)	(0.60)
Constant	-9.425	-6.245	-4.255	1.607	-2.002	-1.970	-0.206
	(-1.05)	(-0.88)	(-0.75)	(0.41)	(-0.63)	(-0.77)	(-0.11)
Country FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	2,545	4,379	6,251	10,769	16,367	22,489	38,690
R-squared	0.044	0.019	0.020	0.022	0.015	0.010	0.003

This table reports results from robustness tests for the flight-to-safety effect, under different window period from 2011-2019. All coefficients are presented in terms of percent. We consider heteroscedasticity and robust standard errors. The dependent variable $R_{(-\imath,+\imath),i,t}$ is measured daily changes in stock market index return at the country level under different sub-sample, defined as $log(stock_{i,t}/stock_{i,t-1})$. *D* is an indicator variable, taking a value of 1 for the attack announcement date and after during the respective window days. *SP* denotes the annual changes in global stock index. *Volatility* denotes the annual standard deviation of stock market. *MKT* denotes the ratio of listed companies' market capitalization over GDP. *CREDIT* denotes the ratio of domestic credit to private sectors over GDP. *GDP growth* denotes quarterly GDP growth rate. *GDP percap* measured by the logarithmic GDP per capita (in USD). *M3* is the monthly broad money growth rate. *Inflation* denotes inflation measured by GDP deflator. *Saving* denotes as the ratio of saving over GDP. *Popurban* denotes the proportion of people living in urban areas. Country FE is the country fixed effect and Year FE is the year fixed effect. T-statistics are reported in parentheses and ***, **, * signify the 1%, 5%, and 10% significance level, respectively.

variables from the CBOE[25] and Board of Governors of the Federal Reserve System[26] respectively. ΔVIX_t, from the CBOE is the daily log difference of the daily VIX index. $\Delta INDPRO_t$ measures the monthly industrial production growth. ΔPDI is the change in personal dividend payment,

[25] https://www.cboe.com/tradable_products/vix/

[26] https://fred.stlouisfed.org

$\Delta NFDP_t$ denotes the change ratio for non-financial dividend paid. We expect the coefficients on D_j to be consistent with our preceding findings. We also control the sector and year fixed effects.

Regression results are reported in Table 9 with robust standard errors, the year and the sector fixed effects. Unsurprisingly, the evidence from the firm-level analysis is consistent with our main results. As it is shown in Panel A that all coefficients on D_0 and D_2 are statistically significant, the constituents of S&P 500 index appear to be the safe haven. In column (3), the firm-level stock returns, on average, increase sharply by 13.8% on the announcement date. After experiencing a moderate downward adjustment by 9.2% on the following trading day, the returns rebound by 3.9% at D_2. On average, the firm-level return gains of 1.9% change over the attacking period, from D_0 to D_2 denoted by the employed $D_{(0,2)}$, as shown in column (4). In sum, it appears that the economic impact of cyber hacking incidents is stronger in the US than the worldwide average of 11% in Table 3.

In Panel B, we carry out an additional test based on portfolio returns denoted as $R_{p,t}$, an equally-weighted portfolio across various industries at date t.[27] Results are generally consistent but weaker in terms of both economic and statistical significance.

[27] We collected 39 industries across SP 500. They are aerospace and defense, automobiles and parts, banks, beverages, chemicals, construction and materials, electricity, electronic and electrical equipment, financial services (sector), fixed-line telecommunications, food producers, food and drug retailers, forestry and paper, gas, water and multi utilities, general industrials, general retailers, health care equipment and services, household goods and home construction, industrial engineering, industrial metals and mining, industrial transportation, leisure goods, life insurance, media, mining, nonlife insurance, oil equipment and services, oil and gas producers, personal goods, pharmaceuticals and biotechnology, real estate investment trusts, real estate investment and services, software and computer services, support services, technology hardware and equipment, tobacco, travel and leisure, unclassified.

Table 9 Flight to safety under firm-level.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Dependent variable:		Paenl A: $R_{f,t}$				Paenl B: $R_{p,t}$		
D_0	0.139***	0.137***	0.138***		0.145**	0.144**	0.146**	
	(9.81)	(9.66)	(9.73)		(2.56)	(2.54)	(2.56)	
D_1		-0.093***	-0.092***			-0.049	-0.048	
		(-7.46)	(-7.38)			(-0.85)	(-0.83)	
D_2			0.039***				0.052	
			(3.18)				(1.08)	
$D_{(0,2)}$				0.019**				0.042
				(2.51)				(1.30)
ΔVIX	-10.076***	-10.074***	-10.073***	-10.076***	-9.588***	-9.587***	-9.586***	-9.588***
	(-377.42)	(-377.36)	(-377.26)	(-377.42)	(-100.73)	(-100.71)	(-100.65)	(-100.72)
$\Delta INDPRO$	-1.826***	-1.793***	-1.808***	-1.786***	-1.024	-1.006	-1.027	-1.008
	(-4.40)	(-4.33)	(-4.36)	(-4.31)	(-0.62)	(-0.61)	(-0.62)	(-0.61)
ΔPDI	-0.212***	-0.211***	-0.212***	-0.214***	-0.870***	-0.870***	-0.871***	-0.872***
	(-8.34)	(-8.34)	(-8.35)	(-8.43)	(-9.18)	(-9.18)	(-9.19)	(-9.21)
$\Delta NFDP$	0.081***	0.081***	0.081***	0.082***	-0.072***	-0.072***	-0.072***	-0.071***
	(13.03)	(13.03)	(13.03)	(13.24)	(-3.37)	(-3.37)	(-3.37)	(-3.32)
Constant	-0.006	-0.005	-0.005	-0.006	3.647***	3.648***	3.647***	3.647***
	(-0.79)	(-0.67)	(-0.71)	(-0.76)	(118.17)	(118.15)	(118.11)	(118.10)
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Sector FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	928,885	928,885	928,885	928,885	72,504	72,504	72,504	72,504
R-squared	0.196	0.196	0.196	0.196	0.716	0.716	0.716	0.716

This table reports results from robustness tests for the flight-to-safety effect, using USA firm level data from 2011-2019. All coefficients are presented in terms of percent. We consider heteroscedasticity and robust standard errors. The dependent variable $R_{f,t}$ is measured daily individual stock return at the USA firm-level, defined as $log((stock_{f,t} - stock_{f,t-1})/stock_{f,t-1})$. We also use alternative measure $R_{p,t}$ to define the return for equally weighted portfolio across 38 industries. D_0, D_1, D_2 are indicator variables, taking a value of 1 for the attack announcement date, the first, and the second trading day after the attack announcement date, respectively. An alternative measure $D_{(0,2)}$ presents the event period covering the episodes from announcement dates to the second trading days. ΔVIX_t is the daily change in VIX index. $\Delta INDPRO_t$ denotes the the monthly changes of Industrial Production index in US. ΔPDI_t is the quarterly changes of Personal dividend income. $NFDP_t$ denotes the quarterly change ratio of non-financial dividend paid. Sector FE is the sector fixed effect and Year FE is the year fixed effect. T-statistics are reported in parentheses and ***, **, * signify the 1%, 5%, and 10% significance level, respectively.

5. Extension study: The flight-to-safety and country specific characteristics

5.1. Evidence for short-run reversal of daily stock returns

We examine the short-run reversal of daily stock market returns, in terms of a reaction to attack events, at a 3-days interval (D_{-1}, D_{+1}). Firstly, 39 countries are ranked according to their stock returns at D_{-1}, the date before the hacking event announcement, and then they are further grouped into 10 deciles. In Table 10, we discover the disparate impacts caused by attacks on these 10 deciles. The summary statistics for the returns under each decile are reported, in a time span - D_{-1}, D_0, and D_1. At D_{-1}, and the mean value is -1.63% for decile 1 and 1.52% for decile 10, respectively.

A configuration at D_0 is 0.35% for decile 1 and 0.23% for decile 10, followed by 0.13% and -0.05% for decile 1 and 10, respectively, at D_1. A discernible return reversal across deciles is documented.

We perform the t-test and nonparametric equality-of-median test. The results show that the differences in means and medians between deciles 1 and 10 are statistically significant at D_{-1}, but insignificant on/after the attack announcement date (D_0, D_1). 60% (6 out of 10 deciles) of stock markets experience an increase in average returns at D_0 and D_1. The flight-to-safety effect appears to be stronger in countries with relatively poor performance on their respective stock markets. A possible explanation for this reversal is that investors who are not satisfied with the rewards from investing domestic stocks are inclined to invest in alternative assets hoping for higher rewards. These investors withdraw their investment from the stock markets in their respective countries and crowd into the crypto markets, while they soon flee from it under a threat of a cyber breach. As a result, the stock markets in these countries rebound in response to their flight-to-safety behavior. Panel B presents a similar analysis by grouping countries into quartiles, and our main findings hold.

5.2. The flight-to-safety effect: The role of country-specific characteristics

In this section, we investigate how the flight-to-safety effect varies according to a country's economic infrastructure. We particularly focus on five characteristics - *economic freedom, institutional infrastructure, financial development, technological development, and financial literacy*. Economic freedom measures the overall economic strengths based on 12 equally-weighted quantitative and qualitative components. We consider three representative components: (1) monetary freedom referring to the currency value of the country and monetary policy (the higher the rank, the more stable the currency price); (2) government integrity relating to corruption, i.e., bribery and graft (the lower the level of government integrity, the weaker the economic vitality and market growth); and (3) government spending (the higher the degree of government spending, the greater the risk of crowding out the private economy). Institutional infrastructure, mainly for creditor rights, measures the legal rights of creditors against defaulting debtors in different jurisdictions. Financial development has an immediate effect on the efficient allocation of capital via investment that follows the most productive uses of capital (Love and Zicchino 2006). Sizeable stock markets are associated with more liquidity, less volatility and more integration (Levine and Demirgüç-Kunt 1999). We employ stock market capitalization (MKT) as a measure of financial development. Considering the vast deployment of advanced technology into the crypto markets (i.e., blockchain), we particularly include technological development (patent) across the countries under investigation. Further, we consider financial literacy at country level, which has a direct effect on the proportion of unsophisticated investors. Van Rooij et al. (2011) documents that higher financial sophistication

Table 10 T-test,median test for three window day.

Panel A		D_{-1}			D_0			D_1		
Decile	Total ob	N	mean	median	N	mean	median	N	mean	median
1	510	190	-1.631%	-1.329%	130	0.353%	0.307%	190	0.128%	0.052%
2	510	190	-0.904%	-0.730%	130	0.108%	0.028%	190	0.137%	0.000%
3	510	190	-0.617%	-0.432%	130	0.225%	0.008%	190	0.249%	0.186%
4	408	152	-0.435%	-0.281%	104	0.183%	0.136%	152	0.043%	0.028%
5	510	190	-0.264%	-0.156%	130	0.095%	0.131%	190	0.093%	0.078%
6	510	190	-0.079%	-0.000003%	130	0.014%	0.014%	190	0.195%	0.135%
7	408	152	0.107%	0.093%	104	0.132%	0.104%	152	0.047%	0.061%
8	510	190	0.312%	0.340%	130	0.003%	0.000004%	190	0.092%	0.035%
9	510	190	0.654%	0.601%	130	0.090%	0.0000021%	190	-0.038%	-0.000001%
10	408	152	1.525%	1.335%	104	0.232%	0.0000007%	152	-0.051%	-0.000001%
(10)-(1)			-3.155%	2.665%		0.121%	-0.307%		0.179%	-0.052%
t-statisitc			-24.502			0.657			1.158	
chi2(1)				273.6			4.431			0.189
P value			0.000	0.000		0.512	0.035		0.248	0.663
Panel B		D_{-1}			D_0			D_1		
Quartile	Total ob	N	mean	median	N	mean	median	N	mean	median
1	1224	456	-1.170%	-0.948%	312	0.206%	0.172%	456	0.172%	0.070%
2	1224	456	-0.398%	-0.266%	312	0.181%	0.127%	456	0.095%	0.054%
3	1224	456	0.067%	0.093%	312	0.062%	0.046%	456	0.116%	0.080%
4	1122	418	0.924%	0.781%	286	0.113%	0.0000007%	418	-0.015%	0.000002%
(4)-(1)			-2.094%	1.728%		0.092%	-0.172%		0.187%	-0.070%
t-statisitc			-30.022			0.946			2.223	
chi2(1)				548.937			2.681			0.660
P value			0.000	0.000		0.345	0.102		0.026	0.416

This table presents evidence for the short-run reversal of daily stock market returns across countries during a one-day pre- and post-event window period. Panel A reports the average stock market return changes at trading days around the attack announcement date (D_{-1}, D_0, and D_1) in terms of deciles where deciles are determined by ranking stock market returns movement at date D_{-1} in an ascending order. Panel B reports similar results in terms of quartiles.

tends to be associated with higher propensity of engaging the investment with complexity, and hence higher participation. A more recent study by Panos and Karkkainen (2019) finds that the financially literate are also more likely to be aware, but not to own/invest in cryptocurrencies. We may expect that those countries with high financial literacy and consequently higher participation in the cryptocurrency investment are likely to witness a flight-to-safety effect.

We summarize the data source of these country characteristics. The economic freedom data is published by the Heritage Foundation.[28] We apply the Creditor Rights Index (Djankov et al. 2007) to classify the countries that are featured as high (low) creditor protection countries. MKT and Patent are obtained from the World Bank's World Development Indicators (WDI) database.[29]

[28] https://www.heritage.org/index/about

[29] https://data.worldbank.org

Financial literacy worldwide data is extracted from Standard & Poor's Ratings Services Global Financial Literacy Survey 2014.[30]

For each characteristic, we first rank the corresponding quantities at D_{-1} across countries in ascending order and partition them into 4 quartiles. We then calculate the average stock market return for each quartile at D_{-1}, D_0, D_1. To save space, Table 11 only reports the results from the lowest and highest quartiles, along with t-statistics for testing the mean difference between the highest and lowest quartiles. The average stock market return over date D_0 and date D_1 , denoted $D_{(0,1)}$, is reported in the last column.

In terms of country economic freedom (Panel A), stock markets in the fourth quartile generally react positively to hacking attacks with a return of 0.1427% and 0.1857% at D_0 and D_1, respectively. The three representative components of this characteristic show a similar picture. The mean difference between quartiles 1 and 4 at D_1 is statistically significant, except for government spending. The countries with higher economic freedom, monetary freedom and government integrity appear to manifest the flight-to-safety effect at D_1, while countries with low government spending react more acutely.

Panel B shows that countries with poor creditor rights react more instantly than countries with better creditor protection. It indicates that those investors concerning the deterioration of creditor rights are inclined to search for alternative investment venues. Nevertheless, after the hacking events, the countries featured with better creditor protection turn out to be a safe-haven. In Panel C, we find that countries with an underdeveloped financial sector exhibit an apparent flight-to-safety effect, which is consistent with literature that claims the impact of temporary shocks and the subsequent financial constraints tend to be larger in the countries with imperfection capital markets (Kiyotaki and Moore 1997, Levine and Demirgüç-Kunt 1999). We observe in Panel D that stock markets in the technologically underdeveloped countries (quartile 1) respond positively and strongly to the hacking events, which may be attributed to low technological literacy in that country. However, there lack significant variations with respect to the country's financial literacy as shown in Panel E. Overall, the evidence suggests that country-specific characteristics shed light on the extent and timing of the flight-to-safety effect.

[30] https://gflec.org/wp-content/uploads/2015/11/3313-Finlit$_{R}eport_{F}INAL-5.11.16.pdf?x47626$

Table 11 Flight to safety under country characteristics .

	Quartile	Observation	D_{-1}	D_0	D_1	$D_{(0,1)}$
Panel A: Economic freedom						
Overall score	1	918	-0.103%	0.162%	-0.025%	0.051%
	4	918	-0.113%	0.143%	0.186%	0.168%
	(4)-(1)		-0.01%	-0.02%	0.21%	0.117%
	t-statistic		-0.11	-0.20	2.31	1.74
Monetary freedom	1	918	-0.162%	0.131%	0.041%	0.078%
	4	909	-0.21%	0.128%	0.238%	0.193%
	(4)-(1)		-0.048%	-0.004%	0.197%	0.115%
	t-statistic		-0.52	-0.03	2.09	1.61
G_integrity	1	938	-0.124%	0.117%	0.006%	0.051%
	4	895	-0.19%	0.158%	0.216%	0.192%
	(4)-(1)		-0.066%	0.04%	0.21%	0.141%
	t-statistic		-0.72	0.41	2.19	2.04
G_spending	1	935	-0.207%	0.326%	0.12%	0.204%
	4	904	-0.158%	0.102%	0.04%	0.065%
	(4)-(1)		0.049%	-0.224%	-0.08%	-0.139%
	t-statistic		0.55	-2.19	-0.87	-2.02
Panel B: Institutional infrastructure						
Creditor rights	1	1530	-0.1%	0.238%	0.004%	0.099%
	4	306	-0.165%	-0.05%	0.255%	0.131%
	(4)-(1)		-0.064%	-0.287%	0.251%	0.032%
	t-statistic		-0.51	-2.05	2.05	0.35
Panel C: Financial development						
MKT	1	582	-0.113%	0.354%	0.16%	0.238%
	4	547	-0.306%	-0.004%	0.203%	0.12%
	(4)-(1)		-0.193%	-0.358%	0.044%	-0.117%
	t-statistic		-1.52	-2.23	0.34	-1.18
Panel D: Technological development						
Patent	1	704	-0.12%	0.282%	0.121%	0.186%
	4	640	-0.204%	-0.031%	0.094%	0.044%
	(4)-(1)		-0.083%	-0.313%	-0.027%	-0.141%
	t-statistic		-0.77	-2.38	-0.25	-1.69
Panel E: Literacy						
Financial literacy	1	1020	-0.081%	0.002	0.056%	0.092%
	4	1020	-0.119%	0.002	0.1777%	0.178%
	(4)-(1)		-0.037%	0.0003	0.122%	0.086%
	t-statistic		-0.44	0.33	1.37	1.29

This table shows how the flight-to-safety effect varies with country-specific characteristics. Stock markets are first ranked in an ascending order and partitioned into quartiles by the value of each country-specific characteristic at the day before hacking attack announcement date (D_{-1}). The average stock return movement at the day before, on and after the cyber attack announcement date (D_{-1}, D_0, D_1) of the highest and lowest quartiles are reported in terms of economic freedom and its three components (money freedom, government integrity, and government spending) in Panel A, institutional infrastructure in Panel B, financial development in Panel C, technological development in Panel D, and financial literacy in Panel E.

6. Conclusion

We uncover a novel flight-to-safety effect from alternative asset markets to stock markets in the context of cyber attacks on crypto exchanges. Such attacks raise investors' concerns about the uncertainty and risk of investing in cryptocurrencies and undermine their confidence in crypto markets. We find that the official announcements of hacking events instantly wipe out bitcoin returns by 43%, while pumping up bitcoin liquidity costs by 30 percentage points in terms of the bid-ask spread. The resultant market panic induces herd-like capital reallocation, which contributes to stock market returns by 27% on the date of announcement and 44% on the second trading day during a high-incident period. We also find that investor sentiment embedded in messages on social media platforms serves as an early warning indicator prior to the events and measures the flight-to-safety pressure during and after the events. Finally, the magnitude and timing of the flight-to-safety effect vary by country characteristics. Our results are robust regarding the firm-level investigation and the length of event window.

To the best of our knowledge, this is the first study examining the impact of cybercrime in crypto markets on the real economy. Crypto markets have been generally deemed to be closely related to underground unlawful activities (Foley et al. 2019) and are isolated from the real economy. We document a link between crypto markets and the real economy. The examination of transmitted shocks from unregulated crypto markets to regulated stock markets has significant policy implications. Stock markets might become more volatile in response to the exogenous shocks from alternative asset markets. More importantly, social media play a pivotal role in conveying soft information relating to crypto markets to investors. For the purpose of stock market stability, keeping a close eye on social media sentiment toward cryptocurrencies can aid the task of monitoring stock market fluctuation. Policymakers can utilize social media information to help safeguard the real economy. Since early 2021, crypto markets have gained increased attention from some principal players in the financial markets. For instance, in March J.P.Morgan and Morgan Stanley started to offer 'crypto exposure' products or offer clients access to bitcoin funds. It seems likely that the conventional financial markets and cryptocurrency markets will become more connected, providing a fascinating area for future research. more information available, future research may focus on each exchange/clustered groups, and perhaps trace fund flows.

7. Appendix

Table A1 The list of hacking events included in this study

Exchange name	News announcement date	Stolen value	Source of information	Event ID
Mtgox	2011.06.19	$35,200	Bitcoin Forum	1
Bitcoin7	2011.10.05	$25,000	Reuters	2
Bitcoinica	2012.03.02	$228,000	Reuters	3
Bitcoinica	2012.05.12	$87,000	Reuters	4
Bitfloor	2012.09.04	$250,000	Reuters	5
Vircurex	2013.05.10	$352,000	Reuters	6
Picostocks	2013.11.29	$5,979,134	Bitcoin Forum	7
Silk road2	2014.02.13	$3,624,866	Bitcoin forum	8
Huobi	2014.02.14	/	Published Paper	9
Mtgox	2014.02.24	$480,000,000	Reuters	10
Flexcoin	2014.03.02	$600,000	Bitcoin Forum	11
Poloniex	2014.03.04	$67,500	Reuters	12
Bitcurex	2014.03.14	/	Coindesk	13
Cryptorush	2014.03.25	$630,000	Bitcoin Forum	14
Mintpal	2014.07.13	$1,933,000	Reuters	15
Bter	2014.08.15	$1,650,000	Coindesk	16
Bitstamp	2015.01.04	$5,100,000	Reuters	17
796exchange	2015.01.18	$270,000	Reuters	18
Bter	2015.02.14	$1,750,000	Reuters	19
Cryptsy	2016.01.15	$4,150,000	Coindesk	20
Shapeshift	2016.04.09	$49,000,000	Reuters	21
Gatecoin	2016.05.16	$2,140,000	Reuters	22
Bitfinex	2016.08.03	$72,000,000	Reuters	23
Bitcurex	2016.10.13	$1,500,000	Reuters	24
Bithumb	2017.07.05	$31,600,000	BBC	25
Nicehash	2017.12.06	$65,082,863	Coindesk	26
Youbit	2017.12.19	/	Guardian	27
Coincheck	2018.01.26	$400,000,000	Guardian	28
Bitgrail	2018.02.10	$170,000,000	Twitter/Wiki	29
Coinsecure	2018.04.12	$3,233,603	Coindesk	30
Taylor	2018.05.22	$1,671,159	Bitcoinist	31
Bitcoin gold	2018.05.24	$18,000,000	Medium.Com	32
Coinrail	2018.06.10	$40,000,000	Wiki	33
Bithumb	2018.06.20	$31,000,000	Coindesk	34
Bancor	2018.07.10	$23,500,000	Coindesk	35
Zaif	2018.09.20	$60,000,000	Coindesk	36
Maplechange	2018.10.28	$5,000,000	Twitter	37
Pure bit	2018.11.09	$2,835,999	Nasdaq	38
Cryptopia	2019.01.13	$3,620,000	Coindesk	39
Coinmama	2019.02.15	/	Cointelegraph	40
Coinbin	2019.02.26	$26,000,000	Official Twitter	41
Dragonex	2019.03.24	/	Coindesk	42
Coinbene	2019.03.27	$118,600,000	Cointelegraph	43
Bithumb	2019.03.29	$6,200,000	Coindesk	44
Binance	2019.05.07	$40,000,000	Binance Webstie	45

Table A2 Flight to safety: Controlling for Religion, Shadow economy, and Culture.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Dependent variable:	$R_{i,t}$		$R_{i,t}$		$R_{i,t}$		$R_{i,t}$
	Religion		Shadow economy		Culture and Trust		Full
D_0	0.147***	0.117**	0.431***	0.442***	0.123**	0.118	0.513***
	(4.12)	(2.33)	(6.00)	(5.98)	(2.49)	(1.64)	(4.92)
D_1	0.065**	0.106**	0.022	0.021	0.057	0.109*	0.023
	(2.07)	(2.48)	(0.38)	(0.36)	(1.38)	(1.96)	(0.30)
D_2	0.006	0.057	0.136**	0.139**	0.047	0.076	0.171**
	(0.18)	(1.29)	(2.53)	(2.55)	(1.11)	(1.27)	(2.30)
Buddhist	0.000	0.027					-0.032
	(0.00)	(0.11)					(-0.03)
Catholic	-0.053	-0.120					-0.067
	(-0.99)	(-0.62)					(-0.07)
Muslim	-0.005	0.014					-0.123
	(-0.12)	(0.26)					(-0.11)
Protestant	0.017	0.073					-0.008
	(0.50)	(0.31)					(-0.01)
Shadowe			0.017**	0.005			0.007
			(2.02)	(0.55)			(0.44)
Idv					0.001	-0.001	0.002
					(0.41)	(-0.18)	(0.19)
Tight					-0.008	0.008	-0.002
					(-0.66)	(0.24)	(-0.03)
Trust					-0.002	-0.002	-0.001
					(-0.72)	(-0.24)	(-0.11)
Constant	-0.051	0.370	-0.473**	1.729	0.026	-0.815	-0.064
	(-1.64)	(0.29)	(-2.44)	(0.65)	(0.17)	(-0.38)	(-0.02)
Stock market controls	No	Yes	No	Yes	No	Yes	Yes
Country economics controls	No	Yes	No	Yes	No	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Country FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	84,708	67,990	50,817	48,734	45,612	37,263	26,843
R-squared	0.002	0.003	0.003	0.004	0.002	0.003	0.004

This table reports regression results for the flight-to-safety effect after controlling for the effect of religion, shadow economy and culture over the period 2011-2019. We consider heteroscedasticity and robust standard errors. The dependent variable $R_{i,t}$ measures daily changes in stock market index return at the country level, defined as $log(stock_{i,t}/stock_{i,t-1})$. D_0, D_1, D_2 are indicator variables, taking a value of 1 for the attack announcement date, the first, and the second trading day after the attack announcement date, respectively. *Buddhist*, *Catholic*,*Muslim*, and *Protestant* equals to 1 for countries if more than 50% of the residents are Buddhists, Catholics, Muslims, and Protestants, respectively, and 0 otherwise. The omitted control group is countries with all other religions, including Hindu, Athiest, and Orthodox. *Shadowe* measures the ratio of shadow economy over GDP (Medina and Schneider 2018). *Idv* denotes the country-specific individualism-collectivism score from the Hofstede (2001)'s data set. *Tight* denotes the country-specific tightness score extracted from Gelfand et al. (2011)'s data set. *Trust* denotes the country-specific score for general trust in other people, collected from World Values Survey (WVS). Stock market controls include global stock index growth (SP) and stock market volatility, while country economics controls consist of stock market capitalization, credit to private sector, GDP growth, GDP per capita, broad money growth, savings rate and the proportion of people living in urban areas. Country FE is the country fixed effect and Year FE is the year fixed effect. T-statistics of the test are reported in parentheses and ***, **, * signify the 1%, 5%, and 10% significance level, respectively.

References

Adrian, T., Crump, R.K., Vogt, E., 2019. Nonlinearity and flight-to-safety in the risk-return trade-off for stocks and bonds. The Journal of Finance 74, 1931–1973.

Akyildirim, E., Corbet, S., Sensoy, A., Yarovaya, L., 2020. The impact of blockchain related name changes on corporate performance. Journal of Corporate Finance 65, 101759.

Baele, L., Bekaert, G., Inghelbrecht, K., Wei, M., 2020. Flights to Safety. The Review of Financial Studies doi:10.1093/rfs/hhz055.

Barsky, R.B., 1986. Why don't the prices of stocks and bonds move together? Technical Report. National Bureau of Economic Research.

Baur, D.G., Lucey, B.M., 2009. Flights and contagion—an empirical analysis of stock–bond correlations. Journal of Financial stability 5, 339–352.

Bekaert, G., Engstrom, E., Xing, Y., 2009. Risk, uncertainty, and asset prices. Journal of Financial Economics 91, 59–82.

Biais, B., Bisiere, C., Bouvard, M., Casamatta, C., 2019. The blockchain folk theorem. The Review of Financial Studies 32, 1662–1715.

Buser, S.A., Chen, A.H., Kane, E.J., 1981. Federal deposit insurance, regulatory policy, and optimal bank capital. The journal of Finance 36, 51–60.

Callen, J.L., Fang, X., 2015. Religion and stock price crash risk. Journal of Financial and Quantitative Analysis , 169–195.

Caporale, G.M., Kang, W.Y., 2020. Bitcoin Price Co-Movements and Culture. CESifo Working Paper No. 8076.

Caporale, G.M., Kang, W.Y., Spagnolo, F., Spagnolo, N., 2020. Cyber-attacks and cryptocurrencies. Economics and Finance Working Paper Series No. 2003, Brunel University .

Chang, C.H., Lin, S.J., 2015. The effects of national culture and behavioral pitfalls on investors' decision-making: Herding behavior in international stock markets. International Review of Economics & Finance 37, 380–392.

Chen, C.Y.H., Despres, R., Guo, L., Renault, T., 2019. What makes cryptocurrencies special? investor sentiment and return predictability during the bubble. Investor Sentiment and Return Predictability During the Bubble (June 3, 2019) .

Chen, C.Y.H., Hafner, C.M., 2019. Sentiment-induced bubbles in the cryptocurrency market. Journal of Risk and Financial Management 12, 53.

Chen, D., Guan, Y., Zhang, T., Zhao, G., 2017. Political connection of financial intermediaries: Evidence from China's IPO market. Journal of Banking and Finance doi:10.1016/j.jbankfin.2016.11.023.

Chordia, T., Roll, R., Subrahmanyam, A., 2001. Market liquidity and trading activity. The journal of finance 56, 501–530.

Cong, L.W., He, Z., Li, J., 2019. Decentralized mining in centralized pools. The Review of Financial Studies .

Cong, L.W., Li, Y., Wang, N., 2020. Tokenomics: Dynamic adoption and valuation. Technical Report. National Bureau of Economic Research.

Corbet, S., Lucey, B., Urquhart, A., Yarovaya, L., 2019. Cryptocurrencies as a financial asset: A systematic analysis. International Review of Financial Analysis 62, 182–199. doi:10.1016/j.irfa.2018.09.003.

Corbet, S., Meegan, A., Larkin, C., Lucey, B., Yarovaya, L., 2018. Exploring the dynamic relationships between cryptocurrencies and other financial assets. Economics Letters 165, 28–34.

Demir, E., Gozgor, G., Lau, C.K.M., Vigne, S.A., 2018. Does economic policy uncertainty predict the bitcoin returns? an empirical investigation. Finance Research Letters 26, 145–149.

Djankov, S., McLiesh, C., Shleifer, A., 2007. Private credit in 129 countries. Journal of financial Economics 84, 299–329.

Duggan, M., Brenner, J., 2013. The demographics of social media users, 2012. volume 14. Pew Research Center's Internet & American Life Project Washington, DC.

Dyhrberg, A.H., 2016. Bitcoin, gold and the dollar–a garch volatility analysis. Finance Research Letters 16, 85–92.

Engelberg, J., Gao, P., Parsons, C.A., 2012. Friends with money. Journal of Financial Economics doi:10.1016/j.jfineco.2011.08.003.

Eun, C.S., Wang, L., Xiao, S.C., 2015. Culture and r2. Journal of Financial Economics 115, 283–303.

Fernandez-Perez, A., Gilbert, A., Indriawan, I., Nguyen, N.H., 2021. Covid-19 pandemic and stock market response: A culture effect. Journal of Behavioral and Experimental Finance 29, 100454.

Foley, S., Karlsen, J.R., Putniņš, T.J., 2019. Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? The Review of Financial Studies 32, 1798–1853.

Gandal, N., Hamrick, J., Moore, T., Oberman, T., 2018. Price manipulation in the bitcoin ecosystem. Journal of Monetary Economics 95, 86–96.

Gelfand, M.J., Raver, J.L., Nishii, L., Leslie, L.M., Lun, J., Lim, B.C., Duan, L., Almaliach, A., Ang, S., Arnadottir, J., et al., 2011. Differences between tight and loose cultures: A 33-nation study. science 332, 1100–1104.

Gentilal, M., Martins, P., Sousa, L., 2017. TrustZone-backed bitcoin wallet, in: ACM International Conference Proceeding Series. doi:10.1145/3031836.3031841.

Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M.C., Siering, M., 2014. Bitcoin-asset or currency? revealing users' hidden intentions .

Griffin, J.M., Shams, A., 2020. Is bitcoin really untethered? The Journal of Finance 75, 1913–1964.

Group-IB, 2018. 2018 Cryptocurrency Exchanges User Accounts Leaks Analysis. Technical Report.

Guesmi, K., Saadi, S., Abid, I., Ftiti, Z., 2019. Portfolio diversification with virtual currency: Evidence from bitcoin. International Review of Financial Analysis 63, 431–437.

Hackernoon, 2019. Security problems of Crypto Exchanges. URL: https://hackernoon.com/security-problems-of-crypto-exchanges-d5e2f595fb79.

Hilary, G., Hui, K.W., 2009. Does religion matter in corporate decision making in america? Journal of financial economics 93, 455–473.

Hofstede, G., 2001. Culture's consequences: Comparing values, behaviors, institutions and organizations across nations. Sage publications.

Hofstede, G., Hofstede, G.H., 1984. Culture's consequences: International differences in work-related values. volume 5. sage.

Hsu, P.H., Tian, X., Xu, Y., 2014. Financial development and innovation: Cross-country evidence. Journal of Financial Economics doi:10.1016/j.jfineco.2013.12.002.

Kiyotaki, N., Moore, J., 1997. Credit cycles. Journal of political economy 105, 211–248.

Klein, T., Thu, H.P., Walther, T., 2018. Bitcoin is not the new gold–a comparison of volatility, correlation, and portfolio performance. International Review of Financial Analysis 59, 105–116.

Levine, R., Demirgüç-Kunt, A., 1999. Stock market development and financial intermediaries: stylized facts. The World Bank.

Levine, R., Loayza, N., Beck, T., 2000. Financial intermediation and growth: Causality and causes. Journal of monetary Economics 46, 31–77.

Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q., 2020. A survey on the security of blockchain systems. Future Generation Computer Systems 107, 841–853.

Linton, M., Teo, E.G.S., Bommes, E., Chen, C., Härdle, W.K., 2017. Dynamic topic modelling for cryptocurrency community forums, in: Applied Quantitative Finance. Springer, pp. 355–372.

Liu, W.h., 2019. National culture effects on stock market volatility level. Empirical Economics 57, 1229–1253.

Liu, Y., Tsyvinski, A., 2018. Risks and returns of cryptocurrency. Technical Report. National Bureau of Economic Research.

Love, I., Zicchino, L., 2006. Financial development and dynamic investment behavior: Evidence from panel var. The Quarterly Review of Economics and Finance 46, 190–210.

Mai, F., Bai, Q., Shan, Z., Wang, X., Chiang, R.H., 2015. The impacts of social media on bitcoin performance, in: 2015 International Conference on Information Systems: Exploring the Information Frontier, ICIS 2015.

Massa, M., Simonov, A., 2006. Hedging, familiarity and portfolio choice. The Review of Financial Studies 19, 633–685.

Medina, L., Schneider, F., 2018. Shadow economies around the world: what did we learn over the last 20 years? .

Medovikov, I., 2016. When does the stock market listen to economic news? New evidence from copulas and news wires. Journal of Banking & Finance 65, 27–40. URL: http://www.sciencedirect.com/science/article/pii/S0378426616000145, doi:https://doi.org/10.1016/j.jbankfin.2016.01.004.

Nasekin, S., Chen, C.Y.H., 2020. Deep learning-based cryptocurrency sentiment construction. Digital Finance , 1–29.

Panos, G.A., Karkkainen, T., 2019. Financial literacy and attitudes to cryptocurrencies. Available at SSRN 3482083 .

Patrick, B., Marie, L., Ally, J., 2019. How many active crypto traders are there across the globe? Technical Report. URL: https://www.chappuishalder.com/wp-content/uploads/2019/06/Publication_Crypto-traders-06-2019.pdf.

Petersen, M.A., 2009. Estimating standard errors in finance panel data sets: Comparing approaches. The Review of financial studies 22, 435–480.

Rogers, L.C.G., Satchell, S.E., 1991. Estimating variance from high, low and closing prices. The Annals of Applied Probability , 504–512.

Russolillo, S., Jeong, E.Y., 2018. Cryptocurrency exchanges are getting hacked because it's easy. Wall Street Journal (July 18, 2018), https://www. wsj. com/articles/whycryptocurrency-exchange-hacks-keep-happening-1531656000 .

Schilling, L., Uhlig, H., 2019. Some simple bitcoin economics. Journal of Monetary Economics 106, 16–26.

Securities, U., Commission, E., 2018. Statement on potentially unlawful online platforms for trading digital assets. Public Statement 7.

Sockin, M., Xiong, W., 2020. A model of cryptocurrencies. Technical Report. National Bureau of Economic Research.

Sokolov, K., 2018. Ransomware activity and blockchain congestion. Available at SSRN 3175986 .

Spathoulas, G., Giachoudis, N., Damiris, G.P., Theodoridis, G., 2019. Collaborative blockchain-based detection of distributed denial of service attacks based on internet of things botnets. Future Internet 11, 226.

Stange, S., Kaserer, C., 2011. The impact of liquidity risk: a fresh look. International Review of Finance 11, 269–301.

Van Rooij, M., Lusardi, A., Alessie, R., 2011. Financial literacy and stock market participation. Journal of Financial Economics 101, 449–472.

Vayanos, D., 2004. Flight to quality, flight to liquidity, and the pricing of risk. Technical Report. National bureau of economic research.

Yermack, D., 2013. Is Bitcoin a Real Currency? SSRN Electronic Journal doi:10.2139/ssrn.2361599.