Quantitative Finance

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rquf20

When the blockchain does not block: on hackings and uncertainty in the cryptocurrency market

Klaus Grobys

To cite this article: Klaus Grobys (2021): When the blockchain does not block: on hackings and uncertainty in the cryptocurrency market, Quantitative Finance, DOI: 10.1080/14697688.2020.1849779

To link to this article: https://doi.org/10.1080/14697688.2020.1849779

Published online: 05 Feb 2021.

Quantitative Finance, 2021
https://doi.org/10.1080/14697688.2020.1849779

When the blockchain does not block: on hackings and uncertainty in the cryptocurrency market

KLAUS GROBYS*[†][‡]

[†]School of Accounting and Finance, University of Vaasa, P.O. Box 700, Vaasa FI-65101, Finland
[‡]Innovation and Entrepreneurship InnoLab, University of Vaasa, Wolffintie 34, Vaasa FI-65200, Finland

(*Received 23 January 2020; accepted 6 November 2020; published online 5 February 2021*)

A total of 1.1 million bitcoins were stolen in the 2013–2017 period. Noting that the average price for a Bitcoin in 2018 was $7572 the corresponding monetary equivalent of losses is $8.9 billion highlighting the societal impact of this criminal activity. Investigating the response of the uncertainty of Bitcoin returns when hacking incidents occur, the results of this study point toward two different responses. After experiencing a contemporaneous effect at day $t = 0$, the volatility increases significantly again at day $t + 5$. Hacking incidents that occur in the Bitcoin market also affect the uncertainty in the Ethereum market with a time delay of five days. Notably, neither Bitcoin nor Ethereum appear to exhibit asymmetric responses to negative innovations.

Keywords: Bitcoin; Contagion; Cryptocurrency; Cyberattack; Ethereum; Hacking; Volatility

JEL Classification: C22, G12, G13, G14, O10

1. Introduction

In a recent paper, Foley *et al.* (2019, p. 1798) highlight that ‘cryptocurrencies have grown rapidly in price, popularity, and mainstream adoption’. As of December 2019, there are more than 4900 cryptocurrencies in the market with a market capitalization of more than $197 billion.[†] The largest, Bitcoin, dominates the new digital financial market with a market capitalization of more than $131 billion corresponding to 67% of the overall market capitalization. In this regard, Easily *et al.* (2019) emphasize about 35 million wallets are held worldwide and 100 000 companies accept payment in bitcoin. Moreover, Hileman and Rausch (2017) find that more than 10 million users now hold a material amount of bitcoin as a (speculative) financial asset.

In his *Forbes* article from October 2019, Ilker Koksal argues that ‘blockchain technology has evolved greatly since the introduction of Bitcoin in 2008, the first decentralized peer-to-peer electronic cash system’. Koksal summarizes four advantages that blockchain technology offers; greater transparency, increased efficiency, better security, and improved traceability.[‡] Unfortunately, these advantages come at a cost, as there are also some new risks that users may face: Specifically, Kethineni and Cao (2020) document that cryptocurrencies became the currency of choice for many drug dealers and extortionists because of the opportunities to hide behind the presumed privacy and anonymity. Foley *et al.*’s (2019) study supports Kethineni and Cao (2020) in finding that about one-quarter of all users and close to one-half of Bitcoin transactions are associated with illegal activity. Maume (2020) examines Initial Coin Offerings (ICO) and concludes that the potential lack of regulation and enforcement is particularly tempting for scammers and other miscreants.

Referring to a recent study of Grobys and Sapkota (2020), Simon Moore’s *Forbes* article of May 2019 discusses credit risk in cryptocurrency markets, as the above-mentioned study’s findings indicate that the vast majority of cryptocurrencies eventually end up in default.[§] Finally, on both the blockchain and exchange levels, cryptocurrencies are vulnerable to cyberattacks. In this regard, Hileman and Rausch (2017, p. 39) document that ‘73% of exchanges control customers’ private keys, making them a potentially attractive “honeypot” for hackers as these exchanges have possession of user funds denominated in cryptocurrency’. In an attempt to avoid hacking incidents (referred to here as *hackings)*, about 90% of the

*Corresponding author. Email: klaus.grobys@uwasa.fi, kgrobys@uva.fi

[†] Source: coinmarketcap.com (accessed on December 13, 2019).

[‡] See https://www.forbes.com/sites/ilkerkoksal/2019/10/23/the-benefits-of-applying-blockchain-technology-in-any-industry/#62a64cd249a5.

[§] See https://www.forbes.com/sites/simonmoore/2019/05/28/how-to-tell-if-your-cryptocurrency-will-go-bust/?fbclid = IwAR162IFlZdEfNaj0YGCJTFzSZjsnf0h_Ntci6zzXoRJ4e_-kFjvuoLy2VYQ#7cec6f833364.

exchanges use some type of cold storage system where they keep their keys offline. Notably, the number of Bitcoin wallets has increased more than four times from 8.2 million in 2013 to 35 million in 2016.

The purpose of this study is to explore the effects of cyberattacks in the form of preceding hackings on the subsequent uncertainty in the Bitcoin market. In the 2013–2017 period, 29 hackings occurred in the Bitcoin market, as documented in Biais *et al.* (2019, Table 3). Given an average price for Bitcoin of $7572 in the calendar year 2018, and given that 1.1 million coins were stolen in the 2013–2017 period, the corresponding monetary equivalent of the losses is $8.9 billion which suggests that the societal impact of these thefts is considerable.[†]

For comparison, the ‘Annual Fraud Statistics’ released by *The Nilson Report* documents that credit card fraud losses worldwide reached $27.85 billion in 2018.[‡] Notably, the United States—taken alone—accounted for $9.47 billion in credit card fraud losses in 2018. However, these numbers are difficult to compare with fraud in cryptocurreny markets because first (*i*) the user base for credit cards is considerably larger (e.g. taking VISA card as an example for one out of many different credit cards, more than 1.1 billion people used VISA cards worldwide at the end of 2018, whereas about 35 million people had Bitcoin wallets at the same point in time),[§] second (*ii*) the frequency of fraud is likely to be much higher but the average amount of stolen monetary equivalent per fraud is likely to be considerably lower (e.g. the average amount of monetary equivalent per hacking in the Bitcoin market is $21 million in the 2013–2017 period), third (*iii*) it is much more likely that users are insured by the credit card company (while Bitcoin users typically do not have such an insurance), and fourth (*iv*), it is much more likely that the police have some chances to successfully tracing back the criminal activity (which seems to be virtually impossible in cyberspace). Overall, the frequency of fraud in cryptocurrency markets is considerably lower compared to credit card markets but it appears to be that each incident is considerably larger, and hence, more consequential in terms of lost monetary equivalent. As a result, fraud in new virtual currency markets is difficult—if not impossible—to compare with fraud in a traditional payment industry such as the credit card industry.

To investigate the effects of cyberattacks in the form of earlier hackings on the subsequent uncertainty in the Bitcoin market, this study employs modified EGARCH models that account for dummy variables up to five days after hacking incidents occurred. Since volatility clustering appears to be a stylized fact of financial markets, the chosen model is also able to capture potential asymmetries in the volatility process of Bitcoin returns. Moreover, this study extends the analysis of volatility effects to another important cryptocurrency market, that of Ethereum. Even if the purpose of Ethererum is very different from Bitcoin, cryptocurrencies typically exhibit a high level of co-movement (Borri 2019).[¶] The question arises whether hackings spillover to other cryptocurrencies such as Ethereum. Ethereum has a market capitalization of about $16 billion as of December 2019, making it the second largest cryptocurrency traded.[‖] Finally, to check the robustness of the findings, this study performs a scientific replication as called for by Hou *et al.* (2020).

This study adds to a growing literature exploring Bitcoin and digital currencies. A recent stream of literature investigates aspects of the Bitcoin ecosystem particularly as they relate to finance and the financial markets (see Böhme *et al.* 2015, Harvey 2016, Malinova and Park 2016, Aune *et al.* 2017, Raskin and Yermack 2017, Howell *et al.* 2020, Makarov and Schoar 2020). Another recent stream of literature analyzes microstructure issues related to Bitcoin. In this regard, Huberman *et al.* (2017) investigate a congestion queuing game that includes miners and fees, whereas Easily *et al.* (2019) develop a game-theory model to explain the factors leading to the emergence of transaction fees. While these two papers share similarities, Huberman *et al.*’s (2017) concern is that equilibrium fees could be too low for the blockchain to be viable, whereas Easily *et al.* (2019) have the opposite concern, that is, the waiting times and equilibrium fees could be so high as to discourage user participation. Moreover, their model examines the evolution of these mining rewards and transaction fees in equilibrium, while Huberman *et al.*’s (2017) study focuses only on the long-term steady state where mining rewards have disappeared and the price effects of Bitcoin are assumed to be irrelevant. Another recent study addressing microstructure issues in the Bitcoin market is that of Foley *et al.* (2019), who propose a model to identify illegal activities in Bitcoin. Their findings indicate that about one-quarter of all users (26%) and close to one-half of Bitcoin transactions (46%) are associated with illegal activity. Moreover, approximately one-fifth (23%) of the total dollar value of transactions and approximately one-half of Bitcoin holdings (49%) over time are associated with illegal activity. The current research was inspired by this stream of recent research and seeks to shed light on another dark side of activities in cryptocurrency markets—the impact of illegal hackings.

A surprising result of this study obtained using fat-tailed *t*-distributed innovation processes to model the EGARCH models is that Bitcoin return volatility does not respond to hackings with an subsequent increase in uncertainty between time $t+1$ and $t+4$. However, there is evidence for a delayed response in volatility. Specifically, Bitcoin return volatility increases substantially at time $t+5$. This result remains robust even after controlling for the immediate volatility response at time $t=0$. The delayed response of Bitcoin return volatility points towards inefficiency in the Bitcoin market as shocks need time to be fully priced-in (Beneki *et al.* 2019). While earlier literature documented co-movements of cryptocurrency returns (Borri 2019), a novel finding of the current

[†] From Table 1 it becomes evident that if one took the price of Bitcoin as a basis for the calculation at the point in time when the virtual currency was stolen, 1.1 million coins would correspond to $608.4 million.

[‡] See https://www.prnewswire.com/news-releases/payment-card-fraud-losses-reach-27-85-billion-300963232.html.

[§] See https://www.statista.com/statistics/618115/number-of-visa-credit-cards-worldwide-by-region/ and https://news.bitcoin.com/the-number-of-cryptocurrency-wallets-is-growing-exponentially/.

[¶] While Bitcoin is created for the sole purpose of payment transfers, the Ethereum platform allows for embedding smart contracts.

[‖] Source: coinmarketcap.com (accessed on December 13, 2019).

research is that hackings in the Bitcoin market also affect other cryptocurrency markets. Our evidence suggests that there is a contagion effect in volatility associated with hacking incidents. In this study, the focus was kept on the two largest cryptocurrency markets in terms of market capitalizations; Bitcoin and Ethereum. As evidenced in the Bitcoin market, the volatility in the Ethereum market increases dramatically with a time delay at time $t + 5$. Surprisingly, there is no evidence for a contemporaneous response in Ethereum's volatility. However, the delayed volatility increase for Ethereum returns is virtually the same as for Bitcoin returns in terms of its economic magnitude. A scientific replication, as asked for in Hou *et al*. (2020), strongly supports the key findings. Another interesting result is that neither Bitcoin returns nor Ethereum returns appear to exhibit asymmetries in their volatility processes even though it is a stylized fact of traditional financial markets that the volatility responds stronger to negative innovations.

2. Literature review

The literature on cryptocurrencies has lately sparked considerable attention. In a recent study, Ammous (2018) analyzes the monetary characteristics of five cryptocurrencies to assess whether they can perform the functions of money. While the author draws the conclusion that most cryptocurrencies are unlikely to fulfill monetary functions, Bitcoin appears to have the potential to serve as a store of value, due to its predetermined and limited supply growth (which is credibly backed by the network's distributed protocol) and Bitcoin's credible demonstration of authorities' incapability of altering the supply schedule.[†]

Even if the original idea for inventing virtual currencies has been to disrupt existing payment systems—and perhaps even the overall monetary system—there is a wide strand of literature emerging that considers cryptocurrencies as new digital asset class. In this regard, Fang *et al*. (2020) conduct a survey covering 118 research papers on various aspects of cryptocurrency trading. The authors argue that cryptocurrencies are the first pure digital assets that are included in managed investment portfolios. In this regard, a recent rapport from Price Waterhouse Cooper documents that the total Assets under Management (AuM) of crypto hedge funds globally increased to over \$2 billion in 2019 from \$1 billion the previous year, whereas the average AuM increased from \$21.9 million to \$44 million.[‡] Moreover, Fang *et al*.'s (2020) findings indicate that cryptocurrencies have a separate nature of its own and their behavior as an asset is not yet fully understood. In another survey on the predictability of the pricing behavior of cryptocurrencies, Kyriazis (2019a) concludes that the majority of academic studies provides evidence for inefficiency of cryptocurrencies, and hence, argues that speculation is feasible via trading.[§]

Another strand of emerging literature explores the volatility in cryptocurrency markets. For instance, Katsiampa (2017) compares various GARCH-type models and assesses the optimal conditional heteroskedasticity model with regards to goodness-of-fit to Bitcoin price data. Even if Katsiampa's (2017) findings indicate that the Auto-Regressive-Component GARCH (ARCGARCH) is optimal in the sample from July 18, 2010 to October 1, 2016, various other studies favor the Exponential GARCH (EGARCH) model due to its statistical properties (Bouoiyour and Selmi 2015, 2016). Other recent studies focus on volatility transmissions. In this regard, Beneki *et al.* (2019) employ a multivariate BEKK-GARCH methodology in association with impulse response analysis to explore whether volatility spillovers and hedging abilities exist between Bitcoin and Ethereum. Surprisingly, their findings indicate a volatility transmission from Ethereum to Bitcoin, which peaks in less than 10 days and fades out after more than two weeks, whereas the reverse impact appears to be significantly weaker. The authors argue that the delayed response of Bitcoin return volatility to a volatility shock of Ethereum returns points towards inefficiency in the Bitcoin market because shocks need time to be fully priced-in. Taking a more practical point of view, the authors highlight that their finding leaves space for profit-making and provides opportunities for speculation in the Bitcoin market as it may help traders to construct profitable strategies on derivative markets.

Moreover, Katsiampa (2019) uses a bivariate Diagonal BEKK model to explore the volatility dynamics of Bitcoin and Ether. While the two cryptocurrencies' volatilities appear to be responsive to major news, the author finds strong statistical evidence for interconnectedness of the two cryptocurrencies. Notably, Katsiampa's (2019) empirical findings also indicate that Ether can be an effective hedge against Bitcoin which could be of importance for investment management.

Furthermore, Katsiampa *et al*. (2019) employ three pairwise bivariate BEKK models to explore the conditional volatility dynamics along with interlinkages and conditional correlations between three pairs of cryptocurrencies—which are (*i*) Bitcoin-Ether, (*ii*) Bitcoin-Litecoin, and (*iii*) Ether-Litecoin. Confirming earlier studies, Katsiampa *et al.*'s (2019) findings indicate that a cryptocurrency's own current conditional variance is mostly affected by its own past shocks and volatility. Interestingly, the bi-directional shock transmission effects between Bitcoin and Ether as well as between Bitcoin and Litecoin, and uni-directional shock spillover from Ether to Litecoin. They also identified bi-directional volatility spillover effects between all the three pairs of cryptocurrencies. The authors conclude that their results provide strong evidence supporting the progress of cryptocurrency market integration and further support earlier studies' findings on interdependencies within the cryptocurrency market (Beneki *et al*. 2019, Katsiampa 2019).

While the current study follows Bouoiyour and Selmi (2016) by adopting EGARCH-type model specifications, it is also related to the literature on volatility transmission (Beneki *et al*. 2019, Katsiampa 2019, Katsiampa *et al*. 2019). While earlier studies focus mainly on revealing volatility interdependencies, the current research steps on new grounds as it

[†] A more detailed review of Bitcoin's design principles and properties is provided in Böhme *et al.* (2015).

[‡] See https://www.pwc.com/gx/en/financial-services/pdf/pwc-elwood-annual-crypto-hedge-fund-report-may-2020.pdf.

[§] Other recent cryptocurrency-related surveys are provided Kyriazis (2019b) and Corbet *et al.* (2019).

is the first study that (*i*) explores potential effects of hacking incidents on the Bitcoin market, and (*ii*) investigates whether these attacks would also affect Ethereum—which is the second largest cryptocurrency market in terms of market capitalization.

3. Data

Data for Bitcoin and Ethereum were downloaded from coinmarketcap.com. For the main analysis of this study, data for Bitcoin covers a sample from April 28, 2013 to December 31, 2017, whereas data for Ethereum covers the period from April 7, 2015 to December 31, 2017. Data on hacking incidents were retrieved from Table 3 in Biais *et al.* (2019), who report hackings from June 13, 2011 until December 6, 2017. For a scientific replication, additional data for Bitcoin covering the period January 1, 2011 until April 27, 2013 and January 1, 2017 until December 31, 2018 were downloaded from investing.com. Additional data on hackings for the 2018 period were borrowed from Table 3 in Grobys and Sapkota (2019). Table 1 reports the hackings that occurred in April 28, 2013 to December 31, 2017 period which are of primary interest in this study. Descriptive statistics for the log-returns of Bitcoin and Ethereum are reported in Table 2.

4. Methodology

4.1. *Exploring the one-day lagged volatility response to hackings in the Bitcoin market*

I start the analysis by estimating a modified version of Nelson's (1991) EGARCH model, where the mean equation is

Table 2. Descriptive statistics of Bitcoin and Ethereum.

	BTC	ETH
Mean	0.27	0.64
Median	0.20	– 0.05
Maximum	35.75	41.23
Minimum	– 26.62	– 130.21
Std.Dev.	4.40	8.52
Skewness	– 0.14	– 3.72
Kurtosis	11.90	67.55
Jarque-Bera	5640.10	154 281.40
Probability	0.00	0.00
Observations	1708	877

Notes: This table reports the descriptive statistics of log-returns for Bitcoin (BTC) and Ethereum (ETH). The sample period is from April 28, 2013 to December 31, 2017 for BTC and April 7, 2015 to December 31, 2017 for Ethereum.

Table 1. Hacking incidents in the Bitcoin market.

Date	BTC	Price	Loss in USD	Incident
2013-05-10	1454	117.20	170 408.8	Vircurex hack
2013-06-10	1300	106.35	138 255	PicoStocks hack
2013-10-02	29 655	114.13	3 384 525.15	FBI seizes Silk Road funds
2013-10-25	144 336	186.69	26 946 087.84	FBI seizes Silk Road funds
2013-10-26	22 000	177.32	3 901 040	GBL scam
2013-11-07	4100	296.41	1 215 281	Inputs.io hack
2013-11-12	484	360.33	174 399.72	Bitcash.cz hack
2013-11-29	5896	1131.97	6 674 095.12	PicoStocks hack
2013-11-29	5400	1131.97	6 112 638	Sheep Marketplace closes
2014-02-13	4400	605.24	2 663 056	Silk Road 2 hacked
2014-02-25	744 408	538.71	401 020 033.7	MtGox collapse
2014-03-04	896	666.78	597 434.88	Flexcoin hack
2014-03-04	97	666.78	64 677.66	Poloniex hack
2014-03-25	950	583.92	554 724	CryptoRush hacked
2014-10-14	3894	400.87	1 560 987.78	Mintpal hack
2015-01-05	18 886	274.47	5 183 640.42	Bitstamp hack
2015-01-28	1000	233.91	233 910	796 Exchange hack
2015-02-15	7170	234.82	1 683 659.4	BTER hack
2015-02-17	3000	243.61	730 830	KipCoin hack
2015-05-22	1581	240.35	379 993.35	Bit?niex hack
2015-09-15	5000	230.30	1 151 500	Bitpay?shing scam
2016-01-15	11 325	364.33	4 126 037.25	Cryptsy hack
2016-04-07	315	422.74	133 163.1	ShapeShift hack
2016-04-13	154	423.73	65 254.42	ShapeShift hack
2016-05-14	250	455.67	113 917.5	Gatecoin hack
2016-08-02	119 756	547.47	65 562 817.32	Bit?nex hack
2016-10-13	2300	636.79	1 464 617	Bitcurex hack
2017-04-22	3816	1231.71	4 700 205.36	Yapizon hack
2017-12-06	4736	14 291.50	67 684 544	NiceHash hacked

Notes: This table reports hacking incidents in the Bitcoin market during the 2013–2017 period. The data for hackings were retrieved from Table 3 in Biais *et al.* (2019) and matched with price data retrieved from coinmarketap.com.

given by,

$$r_{BTC,t} = \mu_{BTC} + \rho_{BTC} r_{BTC,t-1} + \epsilon_{BTC,t}, \text{ with} \quad (1)$$

$$\epsilon_{BTC,t} = \zeta_{BTC,t} \sigma_{BTC,t} \quad (2)$$

where $r_{BTC,t} = \ln\left(\frac{BTC_t}{BTC_{t-1}}\right)$ and BTC_t denotes the price of Bitcoin at time t, μ_{BTC} denotes the intercept term of the mean equation, ρ_{BTC} is the parameter measuring first-order autocorrelation and $\epsilon_{BTC,t}$ is the residual term at time t and $\zeta_{BTC,t}$ with $\zeta_{BTC,t}|\mathbf{\Omega}_{t-1} \sim N(0,1)$ is assumed to be the innovation process. For this EGARCH model, the equation for the conditional variance is given by,

$$\ln(\sigma^2_{BTC,t}) = \omega_{BTC} + \alpha_{BTC}\left|\frac{\epsilon_{BTC,t-1}}{\sigma_{BTC,t-1}}\right| + \beta_{BTC}\ln(\sigma^2_{BTC,t-1}) + \gamma_{BTC}\frac{\epsilon_{BTC,t-1}}{\sigma_{BTC,t-1}} + \delta_{BTC} d_{BTC,t} \quad (3)$$

where $\sigma^2_{BTC,t}$ is the conditional variance at time t, and the parameter vector $\boldsymbol{\theta}_{BTC} = (\omega_{BTC}, \alpha_{BTC}, \beta_{BTC}, \gamma_{BTC}, \delta_{BTC})$ is to be estimated using maximum-likelihood estimation. The variable $d_{BTC,t}$ is binary and defined as $d_{BTC,t} = 1$ if a hacking occurred at time $t-1$ and $d_{BTC,t} = 0$ otherwise. The EGARCH model has the advantage that the variance will be positive even if some parameters in the parameter vector $\boldsymbol{\theta}_{BTC}$ were negative. At the same time, this model allows for modeling asymmetries. Specifically, if $\gamma_{BTC} < 0$, positive shocks generate less volatility than negative shocks (bad news). Furthermore, if $\delta_{BTC} > 0$ a hacking in the Bitcoin market generates on average a higher level of volatility on day $t+1$ (the immediate day after the hacking occurred).

Using a sample period from April 28, 2013 until December 31, 2017, we observe from Panel A of Table 3 three main results. First, Bitcoin returns do not exhibit first-order autocorrelation as the estimated parameter for ρ_{BTC} is statistically not different from zero. Second, negative news do not appear to have a higher impact on the volatility than good news because the estimated parameter for γ_{BTC} is statistically not different from zero. This is indeed a surprising result as it appears to be a stylized fact for traditional financial markets that bad news have a greater impact on volatility than good news.

In this regard, Baur and Dimpfl (2018), who employ Glosten *et al.*'s (1993) Threshold GARCH (TGARCH) model for exploring asymmetric volatility responses for a set of 20 cryptocurrencies, find that for virtually all coefficients measuring asymmetries in volatility responses the coefficient is negative. Their result implies that negative shocks increase the volatility by less than positive shocks which is in stark contrast to the positive coefficient generally reported in stock markets. However, using an EGARCH model specification, the current research does not find any evidence for asymmetries in Bitcoin's volatility process in the presence of bad

Table 3. EGARCH model estimates for Bitcoin returns using different innovation processes.

Panel A. Estimates based on standard normal distributed innovations					
Mean equation parameters	μ_{BTC}	ρ_{BTC}			
Estimates	0.21***	0.02			
	(2.86)	(0.93)			
Variance equation parameters	ω_{BTC}	α_{BTC}	β_{BTC}	γ_{BTC}	δ_{BTC}
Estimates	– 0.09***	0.31***	0.95***	– 0.01	0.18***
	(– 7.26)	(17.31)	(210.08)	(– 0.89)	(3.63)
Panel B. Estimates based on t-distributed innovations					
Mean equation parameters	μ_{BTC}	ρ_{BTC}			
Estimates	0.18***	– 0.02			
	(3.10)	(– 0.65)			
Variance equation parameters	ω_{BTC}	α_{BTC}	β_{BTC}	γ_{BTC}	δ_{BTC}
Estimates	– 0.48***	0.33***	0.97***	0.03*	– 0.07
	(– 8.64)	(12.61)	(147.67)	(1.68)	(– 0.47)

This table reports the estimates for the EGARCH model where the mean equation is given by,

$$r_{BTC,t} = \mu_{BTC} + \rho_{BTC} r_{BTC,t-1} + \epsilon_{BTC,t}, \text{ with}$$

$$\epsilon_{BTC,t} = \zeta_{BTC,t}\sigma_{BTC,t},$$

where $r_{BTC,t} = ln\left(\frac{BTC_t}{BTC_{t-1}}\right)$ and BTC_t denotes the price of Bitcoin at time t, μ_{BTC} denotes the intercept term of the mean equation, ρ_{BTC} is the parameter measuring first-order autocorrelation and $\epsilon_{BTC,t}$ is the residual term at time t. The equation for the variance is given by,

$$\ln(\sigma^2_{BTC,t}) = \omega_{BTC} + \alpha_{BTC}\left|\frac{\epsilon_{BTC,t-1}}{\sigma_{BTC,t-1}}\right| + \beta_{BTC}\ln(\sigma^2_{BTC,t-1}) + \gamma_{BTC}\frac{\epsilon_{BTC,t-1}}{\sigma_{BTC,t-1}} + \delta_{BTC} d_{BTC,t},$$

where $\sigma^2_{BTC,t}$ is the conditional variance at time t, and the parameter vector $\boldsymbol{\theta}_{BTC} = (\omega_{BTC}, \alpha_{BTC}, \beta_{BTC}, \gamma_{BTC}, \delta_{BTC})$ is estimated using maximum-likelihood estimation. In this model, the variable $d_{BTC,t}$ is binary and defined as $d_{BTC,t} = 1$ if a hacking occurred at time $t-1$ and $d_{BTC,t} = 0$ otherwise. In Panel A, the assumption is made that the innovation process $\zeta_{BTC,t}$ is normally distributed, that is, $\zeta_{BTC,t}|\mathbf{\Omega}_{t-1} \sim N(0,1)$, whereas in Panel B it is assumed that the innovation process follows a fat-tailed t-distribution, that is, $\zeta_{BTC,t}|\mathbf{\Omega}_{t-1} \sim t(v)$ where v denotes the degrees of freedom. The sample period is from April 28, 2013 to December 31, 2017. The corresponding t-statistics are given in parentheses.

***Statistically significant on a 1% level.

*Statistically significant on a 10% level.

news. A potential explanation for this discrepancy could be the application of different model types. Future research is encouraged to elaborate more on this issue.

Next, the estimated parameter for δ_{BTC} is positive, which prima facie indicates that hackings result in higher levels of return volatility on the day after the hacking occurred. The t-statistic of 3.63 suggests statistical significance on any level. It should be noted, however, that the assumption of this model is that $\zeta_{BTC,t}|\mathbf{\Omega}_{t-1} \sim N(0,1)$ which does not account for excess kurtosis, which is observed in cryptocurrency markets too (see Table 2). In this regard, Taleb (2020) points out that the consequences of using wrong model assumptions in statistical inferences are severe—especially in the presence of fat-tailed distributions. While the current research follows Bouoiyour and Selmi (2016) in employing EGARCH-type models, it next addresses Taleb's (2020) critique concerning unjustified usage of the normal distribution by employing a fat-tailed t-distribution for modeling the innovation process of the (modified) EGARCH models.

Therefore, I re-estimated the model of equations (1)–(3) using a t-distribution for modeling the excess kurtosis of the innovation process, $\zeta_{BTC,t}|\mathbf{\Omega}_{t-1} \sim t(v)$ where v denotes the degrees of freedom. Unlike the normal distribution, employing t-distributions for EGARCH model specifications allows to model fat-tails in the innovation process.† Since the excess kurtosis of a t-distribution is dependent on the degrees of freedom and given by $6/(v-4)$, I use $v = 12$ as a default value for the degrees of freedom and successively estimate the corresponding values of the log-likelihood functions for the model given by equations (1)–(3) provided $v \in \{\mathbb{N}|v > 4\}$. The values of the log-likelihood functions are reported in Table A1 (see Appendix). From Table A1, we observe that the values for the log-likelihood functions linearly increase as the degrees of freedom decrease. Hence, $v = 5$ is used for modeling a heavily fat-tailed innovation process. The results reported in Panel B of Table 3 suggest that hackings do not affect the uncertainty in the Bitcoin market at time $t+1$ as the parameter estimate for δ_{BTC} is statistically not different from zero.‡ As a consequence, accounting for fat-tails in the innovation process, the analyses that follows uses only heavily fat-tailed t-distributed innovation processes with $v = 5$.

4.2. *Delayed volatility response to hackings in the Bitcoin market*

Next, to explore whether Bitcoin returns exhibit any delayed response due to potential market frictions, I account for five binary variables measuring the volatility responses up to five days after the hacking in the Bitcoin market occurred. The variance equation in (3) is replaced by

$$\log(\sigma^2_{BTC,t}) = \omega_{BTC} + \alpha_{BTC}\left|\frac{\epsilon_{BTC,t-1}}{\sigma_{BTC,t-1}}\right| + \beta_{BTC}\log(\sigma^2_{BTC,t-1}) + \gamma_{BTC}\frac{\epsilon_{BTC,t-1}}{\sigma_{BTC,t-1}} + \sum_{i=1}^{K}\delta_{BTC,i}d_{BTC,i,t} \quad (4)$$

In this model, the variable $d_{BTC,i,t}$ is binary and defined as $d_{BTC,i,t} = 1$ if a hacking occurred at time $t-i$ and $d_{BTC,i,t} = 0$ otherwise. Assuming that $\zeta_{BTC,t}|\mathbf{\Omega}_{t-1} \sim t(v)$ where $v = 5$ denotes the degrees of freedom, and given that $K = 5$, the parameter vector $\boldsymbol{\theta}_{BTC} = (\omega_{BTC}, \alpha_{BTC}, \beta_{BTC}, \gamma_{BTC}, \delta_{BTC,1}, \ldots, \delta_{BTC,5})$ is estimated using maximum-likelihood estimation. The results are reported in Table 4 and illustrate that the volatility does not appear to be affected until the fifth day after the hacking occurred because the parameter estimates for $\delta_{BTC,1}$, $\delta_{BTC,2}$, $\delta_{BTC,3}$, and $\delta_{BTC,4}$ are statistically not different from zero, whereas $\hat{\delta}_{BTC,5} = 0.99$ with a t-statistic of 2.54, suggesting that Bitcoin return volatility substantially increases at time $t+5$. An increase in volatility due to hackings is not a surprising finding; the surprising finding here is that the response appears to be considerably delayed. Furthermore, to substantiate the apparent absence of second moment effects until time $t+5$, I implemented a joint test of the hypothesis

$$H_0: \ \delta_{BTC,1} = \delta_{BTC,2} = \delta_{BTC,3} = \delta_{BTC,4} = 0$$

versus

$$H_1: \text{at least one } \delta_{BTC,i} \neq 0 \text{ for } i = \{1,2,3,4\}$$

where the corresponding test statistic is under the null hypothesis asymptotically distributed as $\chi^2(4)$. The estimated test statistic corresponding to $\hat{\lambda} = 6.80$ (p-value 0.15) indicates that H_0 cannot be rejected on a 5% significance level, implying that the uncertainty is unaffected within the time window $t+1$ and $t+4$. The empirical fact that the volatility of Bitcoin returns increases on the fifth day after the hacking occurred suggests a delayed response to hacking incidents. The delayed response of Bitcoin return volatility points towards inefficiency in the Bitcoin market because shocks need time to be fully priced-in (Beneki *et al.* 2019). A question that may arise is first whether other cryptocurrencies respond to hackings in the Bitcoin market, and second if the potential response is similar (i.e. delayed) as we observed here.

4.3. *Volatility response of Ethereum to hackings in the Bitcoin market*

Due to the appropriate features of the EGARCH model—as discussed earlier—I modeled the mean equation for the

† Note that the innovation process $\zeta_{BTC,t}$ of the econometric model defined by equations (1)–(3) exhibits a kurtosis of 11.80.

‡ Note that the convergence of the maximum likelihood function is achieved after 39 iterations. Moreover, to investigate whether Bitcoin return volatility is stationary, the conditional variance of the estimated EGARCH model specification as given by equations (1)–(3) is retrieved and the Augmented Dickey Fuller (ADF) test implemented. Under the null hypothesis, Bitcoin return volatility is an integrated stochastic process, whereas under the alternative hypothesis, Bitcoin return volatility is stationary. Using a maximum lag-order of 24 and the Schwarz Criterion for selecting the optimal lag-length and using an intercept term in the test statistic, the corresponding ADF test statistic (accounting for 6 lags) is estimated at -6.82 suggesting stationarity at a 1% significance level (the critical value for the 1% significance level is –3.43). Using the Akaike Info Criterion as a robustness check and using again a maximum lag-order of 24 and an intercept term in the test statistic, the corresponding ADF test statistic (accounting for 19 lags) is estimated at –4.77 suggesting again stationarity at a 1% significance level. Since the null hypothesis is clearly rejected, Bitcoin return volatility is assumed to be stationary.

Table 4. Modified EGARCH model estimates for Bitcoin.

Mean equation parameters	μ_{BTC}	ρ_{BTC}							
Estimates	0.17***	– 0.02							
	(3.09)	(– 0.75)							
Variance equation parameters	ω_{BTC}	α_{BTC}	β_{BTC}	γ_{BTC}	$\delta_{BTC,1}$	$\delta_{BTC,2}$	$\delta_{BTC,3}$	$\delta_{BTC,4}$	$\delta_{BTC,5}$
Estimates	– 0.47***	0.32***	0.97***	0.03*	0.29	– 0.30	– 0.47	– 0.46	0.99**
	(– 8.57)	(12.34)	(153.01)	(1.79)	(0.83)	(– 0.70)	(– 0.94)	(– 0.82)	(2.54)

This table reports the estimates for the EGARCH model where the mean equation is given by,

$$r_{BTC,t} = \mu_{BTC} + \rho_{BTC} r_{BTC,t-1} + \epsilon_{BTC,t}, \text{ with}$$
$$\epsilon_{BTC,t} = \zeta_{BTC,t}\sigma_{BTC,t},$$

where $r_{BTC,t} = ln\left(\frac{BTC_t}{BTC_{t-1}}\right)$ and BTC_t denotes the price of Bitcoin at time t, μ_{BTC} denotes the intercept term of the mean equation, ρ_{BTC} is the parameter measuring first-order autocorrelation and $\epsilon_{BTC,t}$ is the residual term at time t. The equation for the variance is given by,

$$\ln(\sigma^2_{BTC,t}) = \omega_{BTC} + \alpha_{BTC}\left|\frac{\epsilon_{BTC,t-1}}{\sigma_{BTC,t-1}}\right| + \beta_{BTC}\ln(\sigma^2_{BTC,t-1}) + \gamma_{BTC}\frac{\epsilon_{BTC,t-1}}{\sigma_{BTC,t-1}} + \sum_{i=1}^{K}\delta_{BTC,i}d_{BTC,i,t},$$

where $\sigma^2_{BTC,t}$ is the conditional variance at time t, and the parameter vector $\boldsymbol{\theta}_{BTC} = (\omega_{BTC}, \alpha_{BTC}, \beta_{BTC}, \gamma_{BTC}, \delta_{BTC,1}, \ldots, \delta_{BTC,5})$ is estimated using maximum-likelihood estimation. In this model, the variable $d_{BTC,i,t}$ is binary and defined as $d_{BTC,i,t} = 1$ if a hacking occurred at time $t - i$ and $d_{BTC,i,t} = 0$ otherwise. In this model, the assumption is made that the innovation process $\zeta_{BTC,t}$ follows a fat-tailed t-distribution, that is, $\zeta_{BTC,t}|\boldsymbol{\Omega}_{t-1} \sim t(v)$ where v denotes the degrees of freedom. The sample period is from April 28, 2013 to December 31, 2017. The corresponding t-statistics are given in parentheses.
***Statistically significant on a 1% level.
**Statistically significant on a 5% level.
*Statistically significant on a 1% level.

logarithmic returns of Ethereum as

$$r_{ETH,t} = \mu_{ETH} + \rho_{ETH} r_{ETH,t-1} + \epsilon_{ETH,t}, \text{with} \quad (4)$$
$$\epsilon_{ETH,t} = \zeta_{ETH,t}\sigma_{ETH,t} \quad (5)$$

where $r_{ETH,t} = \ln\left(\frac{ETH_t}{ETH_{t-1}}\right)$ and ETH_t denotes the price of Ethereum at time t, μ_{ETH} denotes the intercept term of the mean equation, ρ_{ETH} is the parameter measuring first-order autocorrelation, $\epsilon_{ETH,t}$ is the residual term at time t and $\zeta_{ETH,t}$ is the innovation process. Then, the equation for the conditional variance is given by

$$\ln(\sigma^2_{ETH,t}) = \omega_{ETH} + \alpha_{ETH}\left|\frac{\epsilon_{ETH,t-1}}{\sigma_{ETH,t-1}}\right| + \beta_{ETH}\ln(\sigma^2_{ETH,t-1})$$
$$+ \gamma_{ETH}\frac{\epsilon_{ETH,t-1}}{\sigma_{ETH,t-1}} + \sum_{i=1}^{K}\delta_{ETH,i}d_{BTC,i,t} \quad (6)$$

where $\sigma^2_{ETH,t}$ is the conditional variance of Ethereum returns at time t. Again, I use fat-tailed innovations and assume $\zeta_{ETH,t}|\boldsymbol{\Omega}_{t-1} \sim t(v)$ where v denotes the degrees of freedom. To determine the optimal degrees of freedom, I again use the log-likelihood functions for the model given by equations (4)–(6), provided $v \in \{\mathbb{N}|v > 4\}$. The values of the log-likelihood functions are reported in Table A2 (see Appendix). From Table A2, we observe that the values for the log-likelihood functions linearly increase as the degrees of freedom decrease which is the same pattern that we observed for Bitcoin. Hence, $v = 5$ is also used for modeling Ethereum's heavily fat-tailed innovation process. Using $v = 5$ and $K = 5$, the parameter vector $\boldsymbol{\theta}_{ETH} = (\omega_{ETH}, \alpha_{ETH}, \beta_{ETH}, \gamma_{ETH}, \delta_{ETH,1}, \ldots, \delta_{ETH,5})$ is estimated using maximum-likelihood estimation. In this model, the variable $d_{BTC,t}$ is binary and defined as in section 4.2. It is important to note that this binary variable is associated with hackings in the Bitcoin market, whereas the point estimates for $\delta_{ETH,1}, \ldots, \delta_{ETH,5}$ measure the (delayed) volatility response in the Ethereum market.

Table 5 reports the corresponding parameter estimates. Unlike Bitcoin, the parameter estimates suggest that the intercept of the mean equation of Ethereum log-returns is statistically not different from zero. Moreover, neither cryptocurrency exhibits first-order autocorrelation (the estimated parameter for ρ_{ETH} is statististically not different from zero, which also holds for the estimated parameter for ρ_{BTC}). Interestingly, the null hypothesis $\gamma_{ETH} = 0$ cannot be rejected (p-value 0.72) indicating that the volatility of the Ethereum market does not exhibit an asymmetric response to negative innovations either. Another commonality between the volatility processes of Bitcoin returns and Ethereum returns is that both do not respond to hackings in the Bitcoin market on day $t + 1$. Interestingly, the t-statistics for the point estimates for $\delta_{ETH,1}$, $\delta_{ETH,2}$, $\delta_{ETH,3}$, $\delta_{ETH,4}$, and $\delta_{ETH,5}$ do not reach statistical significance when considering single variable tests. However, the point estimate $\hat{\delta}_{ETH,5} = 0.97$ exhibits a t-statistic of 1.59 which is considerably higher than for $\hat{\delta}_{ETH,1}$, $\hat{\delta}_{ETH,2}$, $\hat{\delta}_{ETH,3}$, or $\hat{\delta}_{ETH,4}$.

Next, I test the joint hypothesis

$$H_0: \ \delta_{ETH,1} = \delta_{ETH,2} = \delta_{ETH,3} = \delta_{ETH,4} = \delta_{ETH,5} = 0$$

versus

$$H_1: \text{at least one } \delta_{ETH,i} \neq 0 \text{ for } i = \{1, 2, 3, 4, 5\}.$$

Table 5. Modified EGARCH model estimates for Ethereum.

Mean equation parameters	μ_{ETH}	ρ_{ETH}							
Estimates	0.12	0.01							
	(0.73)	(0.23)							
Variance equation parameters	ω_{ETH}	α_{ETH}	β_{ETH}	γ_{ETH}	$\delta_{ETH,1}$	$\delta_{ETH,2}$	$\delta_{ETH,3}$	$\delta_{ETH,4}$	$\delta_{ETH,5}$
Estimates	− 0.86	0.48***	0.91***	− 0.01	− 0.77	0.85	− 0.80	0.60	0.97
	(− 6.78)	(7.94)	(47.90)	(− 0.36)	(− 1.11)	(1.17)	(− 1.21)	(0.71)	(1.59)

This table reports the estimates for the EGARCH model where the mean equation is given by,

$$r_{ETH,t} = \mu_{ETH} + \rho_{ETH} r_{ETH,t} + \epsilon_{ETH,t}, \text{ with}$$

$$\epsilon_{ETH,t} = \zeta_{ETH,t}\sigma_{ETH,t},$$

where $r_{ETH,t} = \ln\left(\frac{ETH_t}{ETH_{t-1}}\right)$ and ETH_t denotes the price of Ethereum at time t, μ_{ETH} denotes the intercept term of the mean equation, ρ_{ETH} is the parameter measuring first-order autocorrelation and $\epsilon_{ETH,t}$ is the residual term at time t. The variance equation is given by

$$\ln(\sigma^2_{ETH,t}) = \omega_{ETH} + \alpha_{ETH}\left|\frac{\epsilon_{ETH,t-1}}{\sigma_{ETH,t-1}}\right| + \beta_{ETH}\ln(\sigma^2_{ETH,t-1}) + \gamma_{ETH}\frac{\epsilon_{ETH,t-1}}{\sigma_{ETH,t-1}} + \sum_{i=1}^{K}\delta_{ETH,i}d_{BTC,i,t},$$

where $\sigma^2_{ETH,t}$ is the conditional variance at time t, and the parameter vector $\boldsymbol{\theta}_{ETH} = (\omega_{ETH}, \alpha_{ETH}, \beta_{ETH}, \gamma_{ETH}, \delta_{ETH,1}, \ldots, \delta_{ETH,5})$ is estimated using maximum-likelihood estimation. In this model, the variable $d_{ETH,i,t}$ is binary and defined as $d_{ETH,i,t} = 1$ if a hacking occurred in the Bitcoin market at time $t - i$ and $d_{ETH,i,t} = 0$ otherwise. In this model, the assumption is made that the innovation process $\zeta_{ETH,t}$ follows a fat-tailed t-distribution, that is, $\zeta_{ETH,t}|\boldsymbol{\Omega}_{t-1} \sim t(v)$ where v denotes the degrees of freedom. The sample period is from April 7, 2015 to December 31, 2017. The corresponding t-statistics are given in parentheses.
***Statistically significant on a 1% level.
**Statistically significant on a 5% level.

The test statistic is under the null hypothesis asymptotically distributed as $\chi^2(5)$. The estimated test statistic corresponding to $\hat{\lambda} = 11.02$ (p-value of 0.05) indicates that H_0 can be marginally rejected on a 5% significance level. This result suggests that the volatility process of Ethereum responds to hackings in the Bitcoin market between $t + 1$ and $t + 5$, provided a hacking occurred at $t = 0$. The question arises whether the uncertainty is unaffected within the time window $t + 1$ and $t + 4$ as we observed for the Bitcoin market. To test this issue, I implement a joint test of the following hypothesis,

$$H_0 : \delta_{ETH,1} = \delta_{ETH,2} = \delta_{ETH,3} = \delta_{ETH,4} = 0$$

versus

$$H_1 : \text{at least one } \delta_{ETH,i} \neq 0 \text{ for } i = \{1, 2, 3, 4\},$$

where the corresponding test statistic is under the null hypothesis asymptotically distributed as $\chi^2(4)$. The estimated test statistic corresponding to $\hat{\lambda} = 2.79$ (p-value of 0.59) indicates that H_0 cannot be rejected at a common 5% significance level. This result strongly supports the empirical finding that it is on day $t + 5$ (after a hacking in the Bitcoin market occurred) when the volatility process of Ethereum significantly increases. Next, to assess the impact on the uncertainty in the Ethereum market in more detail, I estimate the restricted model given by equations (4)–(5) in association with the conditional variance equation given by

$$\ln(\sigma^2_{ETH,t}) = \omega_{ETH} + \alpha_{ETH}\left|\frac{\epsilon_{ETH,t-1}}{\sigma_{ETH,t-1}}\right| + \beta_{ETH}\ln(\sigma^2_{ETH,t-1}) + \gamma_{ETH}\frac{\epsilon_{ETH,t-1}}{\sigma_{ETH,t-1}} + \delta_{ETH,5}d_{BTC,5,t} \quad (7)$$

Using again $v = 5$, the parameter vector $\boldsymbol{\theta}_{ETH} = (\omega_{ETH}, \alpha_{ETH}, \beta_{ETH}, \gamma_{ETH}, \delta_{ETH,5})$ is estimated using maximum-likelihood estimation. In this model, the variable $d_{BTC,5,t}$ is binary and defined as in section 4.2. The results are reported in Table 6. From Table 6, we observe that the restricted model's point estimate corresponding to $\hat{\delta}_{ETH,5} = 1.03$ with a t-statistic of 2.79 is statistical significant on any level. This result implies that Ethereum's volatility exhibits the same delayed response to Bitcoin hackings as we observed for the Bitcoin market.

4.4. Additional robustness checks

Hou *et al*. (2020), who investigate 452 asset pricing anomalies, find that most anomalies do not meet currently acceptable standards for empirical finance research. The authors emphasize that 'the crux is that unlike natural sciences, economics, finance and accounting are mostly observational in nature. As such, it is critical to evaluate the reliability of published results against "similar, but not identical", specifications' (Hou *et al*. 2020, p. 2022). According to Hamermesh (2007), a scientific replication first requires a different or at least expanded sample and second a similar but not identical model. To perform a scientific replication of this study, I download additional data covering the sample period January 1, 2011 to April 27, 2013 from investing.com and retrieve data covering the period January 1, 2018 to December 31, 2018 from coinmarketcap.com. These data are added to the previous sample covering the period April 28, 2013 to December 31, 2017. In Table A3 in Appendix, it can be seen that in this expanded time period, 21 more hackings occurred. Using this expanded sample, I implement the following EGARCH model,

$$r_{BTC,t} = \mu_{BTC} + \epsilon_{BTC,t}, \text{ with} \quad (8)$$

Table 6. Restricted EGARCH model estimates for Ethereum.

Mean equation parameters	μ_{ETH}	ρ_{ETH}			
Estimates	0.12	0.01			
	(0.80)	(0.20)			
Variance equation parameters	ω_{ETH}	α_{ETH}	β_{ETH}	γ_{ETH}	$\delta_{ETH,5}$
Estimates	– 0.83***	0.46***	0.92***	– 0.01	1.03***
	(– 6.74)	(7.85)	(49.88)	(– 0.18)	(2.79)

This table reports the estimates for the EGARCH model where the mean equation is given by,

$$r_{ETH,t} = \mu_{ETH} + \rho_{ETH} r_{ETH,t} + \epsilon_{ETH,t}, \text{ with}$$
$$\epsilon_{ETH,t} = \zeta_{ETH,t}\sigma_{ETH,t}$$

where $r_{ETH,t} = ln\left(\frac{ETH_t}{ETH_{t-1}}\right)$ and ETH_t denotes the price of Ethereum at time t, μ_{ETH} denotes the intercept term of the mean equation, ρ_{ETH} is the parameter measuring first-order autocorrelation and $\epsilon_{ETH,t}$ is the residual term at time t. The variance equation is given by

$$\ln(\sigma^2_{ETH,t}) = \omega_{ETH} + \alpha_{ETH}\left|\frac{\epsilon_{ETH,t-1}}{\sigma_{ETH,t-1}}\right| + \beta_{ETH}\ln(\sigma^2_{ETH,t-1}) + \gamma_{ETH}\frac{\epsilon_{ETH,t-1}}{\sigma_{ETH,t-1}} + \delta_{ETH,5}d_{BTC,5,t}$$

where $\sigma^2_{ETH,t}$ is the conditional variance at time t, and the parameter vector $\boldsymbol{\theta}_{ETH} = (\omega_{ETH}, \alpha_{ETH}, \beta_{ETH}, \gamma_{ETH}, \delta_{ETH})$ is estimated using maximum-likelihood estimation. In this model, the variable $d_{ETH,5,t}$ is binary and defined as $d_{ETH,5,t} = 1$ if a hacking occurred in the Bitcoin market at time $t - 5$ and $d_{ETH,i,t} = 0$ otherwise. In this model, the assumption is made that the innovation process $\zeta_{ETH,t}$ follows a fat-tailed t-distribution, that is, $\zeta_{ETH,t}|\boldsymbol{\Omega}_{t-1} \sim t(v)$ where v denotes the degrees of freedom. The sample period is from April 7, 2015 to December 31, 2017. The corresponding t-statistics are given in parentheses.
*** Statistically significant on a 1% level.

Table 7. Modified EGARCH model estimates for Bitcoin using an extended period.

Mean equation parameters	μ_{BTC}							
Estimates	0.00***							
	(4.34)							
Variance equation parameters	ω_{BTC}	α_{BTC}	β_{BTC}	$\delta_{BTC,1}$	$\delta_{BTC,2}$	$\delta_{BTC,3}$	$\delta_{BTC,4}$	$\delta_{BTC,5}$
Estimates	– 0.39	0.29***	0.97***	0.24	– 0.38	– 0.11	– 0.65*	0.76***
	(– 12.98)	(21.02)	(269.26)	(0.97)	(– 1.21)	(– 0.33)	(– 1.87)	(3.02)

This table reports the estimates for the EGARCH model where the mean equation is given by,

$$r_{BTC,t} = \mu_{BTC} + \epsilon_{BTC,t}, \text{ with}$$
$$\epsilon_{BTC,t} = \zeta_{BTC,t}\sigma_{BTC,t}$$

where $r_{BTC,t} = ln\left(\frac{BTC_t}{BTC_{t-1}}\right)$ and BTC_t denotes the price of Bitcoin at time t, μ_{BTC} denotes the intercept term of the mean equation and $\epsilon_{BTC,t}$ is the residual term at time t. The equation for the variance is given by,

$$ln(\sigma^2_{BTC,t}) = \omega_{BTC} + \alpha_{BTC}\left|\frac{\epsilon_{BTC,t-1}}{\sigma_{BTC,t-1}}\right| + \beta_{BTC}ln(\sigma^2_{BTC,t-1}) + \sum_{i=1}^{K}\delta_{BTC,i}d_{BTC,i,t}$$

where $\sigma^2_{BTC,t}$ is the conditional variance at time t, and the parameter vector $\boldsymbol{\theta}_{BTC} = (\omega_{BTC}, \alpha_{BTC}, \beta_{BTC}, \delta_{BTC,1}, \ldots, \delta_{BTC,5})$ is estimated using maximum-likelihood estimation. In this model, the variable $d_{BTC,i,t}$ is binary and defined as $d_{BTC,i,t} = 1$ if a hacking occurred at time $t - i$ and $d_{BTC,i,t} = 0$ otherwise. In this model, the assumption is made that the innovation process $\zeta_{BTC,t}$ follows a fat-tailed t-distribution, that is, $\zeta_{BTC,t}|\boldsymbol{\Omega}_{t-1} \sim t(v)$ where v denotes the degrees of freedom. The sample period is from January 1, 2011 to December 31, 2018. The corresponding t-statistics are given in parentheses.
***Statistically significant on a 1% level.
*Statistically significant on a 10% level.

$$\epsilon_{BTC,t} = \zeta_{BTC,t}\sigma_{BTC,t} \tag{9}$$

$$\log(\sigma^2_{BTC,t}) = \omega_{BTC} + \alpha_{BTC}\left|\frac{\epsilon_{BTC,t-1}}{\sigma_{BTC,t-1}}\right| + \beta_{BTC}\ln(\sigma^2_{BTC,t-1}) + \sum_{i=1}^{K}\delta_{BTC,i}d_{BTC,i,t} \tag{10}$$

Since the result in the previous section revealed that Bitcoin log-returns do not exhibit first-order autocorrelation and because it is found that the volatility process does not exhibit asymmetries, the model in equations (8)–(10) does not account for parametrization of those variables. Since the model given by equations (8)–(10) is similar but not identical to the model given by equations (1)–(3), or equations (1), (2) and (4), respectively, and because the sample period is different, this replication meets the requirements of a scientific replication as called for in Hou *et al.* (2020).

Table 8. Modified EGARCH model estimates for Bitcoin accounting for contemporaneous volatility responses.

Mean equation parameters	μ_{BTC}	ρ_{BTC}								
Estimates	0.17***	– 0.02								
	(3.10)	(– 0.75)								
Variance equation parameters	ω_{BTC}	α_{BTC}	β_{BTC}	γ_{BTC}	$\delta_{BTC,0}$	$\delta_{BTC,1}$	$\delta_{BTC,2}$	$\delta_{BTC,3}$	$\delta_{BTC,4}$	$\delta_{BTC,5}$
Estimates	– 0.47***	0.32***	0.97***	0.02	1.30***	– 0.69*	– 0.42	– 0.43	– 0.43	0.97**
	(– 8.57)	(12.24)	(154.03)	(1.47)	(5.14)	(– 1.88)	(– 1.03)	(– 0.85)	(– 0.77)	(2.46)

This table reports the estimates for the EGARCH model where the mean equation is given by,

$$r_{BTC,t} = \mu_{BTC} + \rho_{BTC} r_{BTC,t-1} + \epsilon_{BTC,t}, \text{ with}$$
$$\epsilon_{BTC,t} = \zeta_{BTC,t}\sigma_{BTC,t}$$

where $r_{BTC,t} = ln\left(\frac{BTC_t}{BTC_{t-1}}\right)$ and BTC_t denotes the price of Bitcoin at time t, μ_{BTC} denotes the intercept term of the mean equation, ρ_{BTC} is the parameter measuring first-order autocorrelation and $\epsilon_{BTC,t}$ is the residual term at time t. The equation for the variance is given by,

$$\ln(\sigma^2_{BTC,t}) = \omega_{BTC} + \alpha_{BTC}\left|\frac{\epsilon_{BTC,t-1}}{\sigma_{BTC,t-1}}\right| + \beta_{BTC}\ln(\sigma^2_{BTC,t-1}) + \gamma_{BTC}\frac{\epsilon_{BTC,t-1}}{\sigma_{BTC,t-1}} + \delta_{BTC,0}d_{BTC,0,t} + \sum_{i=1}^{K}\delta_{BTC,i}d_{BTC,i,t}$$

where $\sigma^2_{BTC,t}$ is the conditional variance at time t, and the parameter vector $\boldsymbol{\theta}_{BTC} = (\omega_{BTC}, \alpha_{BTC}, \beta_{BTC}, \gamma_{BTC}, \delta_{BTC,0}, \ldots, \delta_{BTC,5})$ is estimated using maximum-likelihood estimation. In this model, the variable $d_{BTC,i,t}$ is binary and defined as $d_{BTC,i,t} = 1$ if a hacking occurred at time $t - i$ and $d_{BTC,i,t} = 0$ otherwise. Moreover, the variable $d_{BTC,0,t}$ measure the contemporaneous respond and is binary and defined as $d_{BTC,i,t} = 1$ if a hacking occurred at time t and $d_{BTC,0,t} = 0$ otherwise. Furthermore, the assumption is made that the innovation process $\zeta_{BTC,t}$ follows a fat-tailed t-distribution, that is, $\zeta_{BTC,t}|\boldsymbol{\Omega}_{t-1} \sim t(v)$ where v denotes the degrees of freedom. The sample period is from April 28, 2013 to December 31, 2017. The corresponding t-statistics are given in parentheses.
*** Statistically significant on a 1% level.
** Statistically significant on a 5% level.
* Statistically significant on a 1% level.

Using this model, I again make the more conservative assumption that $\zeta_{BTC,t}|\boldsymbol{\Omega}_{t-1} \sim t(v)$ where v denotes the degrees of freedom. Using $v = 5$ and the expanded sample period from January 1, 2011 to December 31, 2018, Table 7 reports the corresponding estimates. The results reported in Table 7 strongly support two earlier findings; that is, first, the volatility of Bitcoin returns does not respond during the first couple of days after a hacking occurred. Second, on day $t + 5$ the volatility significantly increases. However, it is noteworthy that the results of this robustness check should be interpreted with caution: In the earlier period (January 1, 2011 to April 27, 2013), 28.30% of the days had zero log-return entries, which might have an impact on the accuracy of the estimation procedure. Nevertheless, the key finding of a delayed volatility response to hackings is strongly supported by this scientific replication.

While this study explores the effects of hacking incidents on the uncertainty in the Bitcoin market in a Granger-sense, and hence, explores responses in Bitcoin's volatility to preceding hacking incidents, the question arises if the effects are robust after controlling for the contemporaneous volatility response to hacking incidents. To address this issue, I re-estimate the model given by equations (1), (2), and (4), by employing the model of equations (1) and (2) in association with variance equation (11), given by

$$\ln(\sigma^2_{BTC,t}) = \omega_{BTC} + \alpha_{BTC}\left|\frac{\epsilon_{BTC,t-1}}{\sigma_{BTC,t-1}}\right| + \beta_{BTC}\ln(\sigma^2_{BTC,t-1}) + \gamma_{BTC}\frac{\epsilon_{BTC,t-1}}{\sigma_{BTC,t-1}} + \delta_{BTC,0}d_{BTC,0,t} + \sum_{i=1}^{K}\delta_{BTC,i}d_{BTC,i,t} \qquad (11)$$

where $\sigma^2_{BTC,t}$ is the conditional variance at time t, $d_{BTC,0,t}$ measures the contemporaneous response and is binary and defined as $d_{BTC,i,t} = 1$ if a hacking occurred at time t and $d_{BTC,0,t} = 0$ otherwise. All other variables are defined as in section 4.2. The parameter vector $\boldsymbol{\theta}_{BTC} = (\omega_{BTC}, \alpha_{BTC}, \beta_{BTC}, \gamma_{BTC}, \delta_{BTC,0}, \ldots, \delta_{BTC,5})$ is estimated using maximum-likelihood estimation. Again, the assumption is made that the innovation process $\zeta_{BTC,t}$ follows a fat-tailed t-distribution, that is, $\zeta_{BTC,t}|\boldsymbol{\Omega}_{t-1} \sim t(v)$ where v denotes the degrees of freedom. Choosing $v = 5$ to account for a heavily fat-tailed innovation process and using the sample from April 28, 2013 to December 31, 2017, the point estimates and corresponding t-statistics of this model are reported in Table 8. The results reported in Table 8 strongly support two earlier findings: First, the volatility of Bitcoin returns does not respond during the first couple of days after a hacking occurred. Second, on day $t + 5$ the volatility significantly increases. Moreover, Table 8 reveals a strong contemporaneous respond because the point estimator for $\delta_{BTC,0}$ which measures the volatility response at time $t = 0$ is $\hat{\delta}_{BTC,0} = 1.30$ and with a t-statistic of 5.14 statistically significant on any level.†

† Unreported results show that Ethereum does not exhibit any contemporaneous response when the Bitcoin market is subject to hacking incidents. The results are available upon request from the author.

Next, to substantiate the results documented in this study, in Table 9 the descriptive statistics are reported for the realized volatility of Bitcoin on the day of the attack, immediately after the incident occurred, and during the rest of the sample period. To estimate realized Bitcoin volatility, I calculate the realized annualized daily volatilities in line with Rogers and Satchell (1991) as

$$\sigma_{BTC,t} = \sqrt{T}\sqrt{\begin{aligned}&\left(\ln\left(\frac{HIGH_t^{BTC}}{CLOSE_t^{BTC}}\right)\cdot\ln\left(\frac{HIGH_t^{BTC}}{OPEN_t^{BTC}}\right)\right.\\&\left.+\ln\left(\frac{LOW_t^{BTC}}{CLOSE_t^{BTC}}\right)\cdot\ln\left(\frac{LOW_t^{BTC}}{OPEN_t^{BTC}}\right)\right)\end{aligned}} \tag{12}$$

where $HIGH_t^{BTC}$, LOW_t^{BTC}, $OPEN_t^{BTC}$, and $CLOSE_t^{BTC}$ denote the highest, lowest, opening, and closing price for Bitcoin on day t, $\sigma_{BTC,t}$ denotes Bitcoin's corresponding realized volatility and $T = 365$ because Bitcoin is traded 24/7. In Table 9, $\sigma_{BTC}^{t=0}$ measures the realized annualized daily volatility of Bitcoin on the day of the hacking incident, whereas $\sigma_{BTC}^{t=1}$ measures the realized annualized daily volatility of Bitcoin on the day after the hacking incident occurred (e.g. day $t+1$), whereas σ_{BTC}^{ALL} measures the realized annualized daily volatility of Bitcoin on all other days over the sample excluding the days $t = 0$ and $t+1$. The sample period is from April 28, 2013 to December 31, 2017. From Table 9, we observe that the average of $\sigma_{BTC}^{t=0}$ is more than twice as the average of σ_{BTC}^{ALL}, whereas the median of $\sigma_{BTC}^{t=0}$ is 1.84 times higher than the median of σ_{BTC}^{ALL}. This result supports the finding of a strong contemporaneous volatility effect to hacking incidents, whereas there is no such evidence for the subsequent day $\sigma_{BTC}^{t=1}$.

Finally, one could wonder whether the autoregressive structure for the volatility process given by the model in equations (1), (2), and (4), is correctly specified. Higher order autoregressive structures for the volatility process are useful if there is any evidence for remaining ARCH-effects. To investigate this issue, I regress the squared estimated innovation process denoted as $\hat{\zeta}_{BTC,t}^2$ on five lags given by,

$$\begin{aligned}\hat{\zeta}_{BTC,t}^2 &= \vartheta_0 + \vartheta_1\hat{\zeta}_{BTC,t-1}^2 + \vartheta_2\hat{\zeta}_{BTC,t-2}^2 + \vartheta_3\hat{\zeta}_{BTC,t-3}^2\\&\quad + \vartheta_4\hat{\zeta}_{BTC,t-4}^2 + \vartheta_5\hat{\zeta}_{BTC,t-5}^2 + e_t\end{aligned}$$

where $\vartheta_1, \vartheta_2, \ldots, \vartheta_5$ denote the parameters associated with the estimated lagged squared innovations, ϑ_0 denotes the regression intercept, and e_t is assumed to be a stationary stochastic process, distributed as $e_t \sim (0, \sigma_e^2)$. The ARCH-LM test statistic λ is given by $\lambda = TR^2$, where R^2 denotes the R-squared of the auxiliary regression as defined above and T defines the number of sample observations. Accounting for a lag-order of five, the test statistic is under the null hypothesis asymptotically distributed as $\chi^2(5)$. Furthermore, under the null hypothesis, it is assumed that there are no remaining ARCH-effects, whereas under the alternative hypothesis it is assumed that there are remaining ARCH-effects pointing towards a higher autoregressive structure for the volatility process. Since the estimated test statistic is $\hat{\lambda} = 2.50$, the null hypothesis cannot be rejected (p-value is 0.78) implying that there are no remaining ARCH-effects in the volatility process and the econometric model is correctly specified.†

Table 9. Realized Bitcoin volatility.

Metric	$\sigma_{BTC}^{t=0}$	$\sigma_{BTC}^{t=1}$	σ_{BTC}^{ALL}
Mean	1.12	0.67	0.53
Std.Dev	1.11	0.62	0.55
Maximum	4.76	3.16	7.40
Median	0.70	0.58	0.38
Minimum	0.06	0.06	0.02
Skewness	1.76	2.67	3.91
Kurtosis	3.61	9.95	26.99

This table reports the realized annualized daily volatilities of Bitcoin using the Rogers and Satchell (1991) estimator,

$$\sigma_{BTC,t} = \sqrt{T}\sqrt{\begin{aligned}&\left(\ln\left(\frac{HIGH_t^{BTC}}{CLOSE_t^{BTC}}\right)\cdot\ln\left(\frac{HIGH_t^{BTC}}{OPEN_t^{BTC}}\right)\right.\\&\left.+\ln\left(\frac{LOW_t^{BTC}}{CLOSE_t^{BTC}}\right)\cdot\ln\left(\frac{LOW_t^{BTC}}{OPEN_t^{BTC}}\right)\right)\end{aligned}}$$

where $HIGH_t^{BTC}$, LOW_t^{BTC}, $OPEN_t^{BTC}$, and $CLOSE_t^{BTC}$ denote the highest, lowest, opening, and closing price for Bitcoin on day t, $\sigma_{BTC,t}$ denotes Bitcoin's corresponding realized annualized daily volatility and $T = 365$. The realized volatility denoted as $\sigma_{BTC}^{t=0}$ measures the realized annualized daily volatility of Bitcoin on the day of the hacking incident, whereas $\sigma_{BTC}^{t=1}$ measures the realized annualized daily volatility of Bitcoin on the day after the hacking incident occurred, that is, $t+1$, and σ_{BTC}^{ALL} measures the realized annualized daily volatility of Bitcoin on all other days over the sample excluding both the days when hacking incidents occurred and the subsequent days after hacking incidents occurred. The sample period is from April 28, 2013 to December 31, 2017.

5. Conclusion

In contrast to stock exchanges, which facilitate trading but do not actually hold securities on behalf of clients, cryptocurrency exchanges typically charge fees for trading and store virtual currencies for their clients, which makes cryptocurrency exchanges vulnerable. This study investigated how hacking incidents in the Bitcoin market affect the uncertainty in this market. The findings indicate that the volatility increases significantly. More specifically, this study finds two effects—a contemporaneous effect and a delayed effect. While the contemporaneous effect could be driven by a substantial increase in uncertainty generated at the exchange that was subject to the hacking incident, a possible explanation for the delayed effect could be that hackings are more likely to occur at small exchanges that perhaps have lower security standards than larger exchanges. Information diffusion then occurs more slowly. Furthermore, exchanges trade multiple cryptocurrencies and if an exchange was hacked, thieves could steal both Bitcoin and Ethereum, which could be a possible explanation for volatility spillovers found in

† As an additional robustness check, I implement the test for remaining ARCH-effects using a lag-order of 10. The results remain unchanged. (The results are available from the author upon request.)

the current study. Another possible explanation for this phenomenon could be that thieves are using one cryptocurrency to cash out on their theft of the other, thus shifting the demand for cryptocurrencies from the one that was hacked to the other. The empirical finding might also have some practical implications. For instance, option strategies such as straddles benefit from increased volatility. A delayed volatility response offers an opportunity for making profits using the derivative markets, which could be a potential area for future research. This study also found a type of contagion in volatility effects. While earlier research suggested that cryptocurrencies comove in their first moments, this study finds second moment spillover effects in the presence of hacking incidents. Future studies could explore whether hacking incidents that occur in smaller cryptocurrency markets exhibit similar spillover effects. Finally, the aim of this study was to draw market-wide conclusions. However, Bitcoin is traded on multiple exchanges but the attacks are always limited to one exchange. It could be interesting to investigate how Bitcoin volatility behaves at the respective exchange after hacking incidents occurred. Since this issue is outside of the current study's scope, it is left for future research.

Acknowledgements

The author would like to thank Niranjan Sapkota and Maarten van Oordt for useful and encouraging comments. He is also greatly appreciative of the insightful comments and helpful suggestions provided by the participants of the 3rd Cryptocurrency Research Conference in September 2020 (ICMA Centre, University of Reading). Finally, he would like to thank two anonymous reviewers for valuable comments.

Disclosure statement

No potential conflict of interest was reported by the author.

References

Ammous, S., Can cryptocurrencies fulfill the functions of money? *Q Rev. Econ. Finance*, 2018, **70**, 38–51.

Aune, R., Krellenstein, A., O'Hara, M. and Slama, O., Footprints on a blockchain: Trading and information leakage in distributed ledgers. *J. Trading*, 2017, **12**(2), 5–13.

Baur, D. G. and Dimpfl, T., Asymmetric volatility in cryptocurrencies. *Econ. Lett.*, 2018, **173**, 148–151.

Beneki, C., Koulis, A., Kyriazis, N. A. and Papadamou, S., Investigating volatility transmission and hedging properties between Bitcoin and Ethereum. *Res. Int. Bus. Finance*, 2019, **48**, 219–227.

Biais, B., Bisiere, C., Bouvard, M., Casamatta, C. and Menkveld, A., Equilibrium Bitcoin pricing, 2019 Meeting Papers 360, Society for Economic Dynamics, 2019.

Böhme, R., Christin, N., Edelman, B. and Moore, T., Bitcoin: Economics, technology, and governance. *J. Econ. Perspect.*, 2015, **29**, 213–238.

Borri, N., Conditional tail-risk in cryptocurrency markets. *J. Empir. Finance*, 2019, **50**, 1–19.

Bouoiyour, J. and Selmi, R., Bitcoin price: Is it really that new round of volatility can be on way? Munich Pers. RePEc Arch., 6558, 2015.

Bouoiyour, J. and Selmi, R., Bitcoin: A beginning of a new phase? *Econ. Bull.*, 2016, **36**(3), 1430–1440.

Corbet, S., Lucey, B., Urquhart, A. and Yarovaya, L., Cryptocurrencies as a financial asset: A systematic analysis. *Int. Rev. Financ. Anal.*, 2019, **62**, 182–199.

Easily, D., O'Hara, M. and Basu, S., From mining to markets: The evolution of Bitcoin transaction. *J. Financ. Econ.*, 2019, **134**, 91–109.

Fang, F., Ventre, C., Basios, M., Kong, H., Kanthan, L., Martinez-Rego, D., Wu, F. and Li, L., Cryptocurrency trading: A comprehensive survey. arXiv preprint arXiv:2003.11352, 2020.

Foley, S., Karlsen, J. R. and Putniņš, T. J., Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies? *Rev. Financ. Stud.*, 2019, **32**(5), 1798–1853.

Glosten, L. R., Jagannathan, R. and Runkle, D. E., On the relation between the expected value and the volatility of the nominal excess return on stocks. *J. Finance*, 1993, **48**(5), 1779–1801.

Grobys, K. and Sapkota, N., Contagion of uncertainty: Transmission of risk from the cryptocurrency market to the foreign exchange market. Proceedings of the 28th European Financial Management Association (EFMA) Conference, Island of St. Miguel, 2019.

Grobys, K. and Sapkota, N., Predicting cryptocurrency defaults. *Appl. Econ.*, 2020, **52**(46), 5060–5076.

Hamermesh, D. S., Viewpoint: Replication in economics. *Can. J. Econ.*, 2007, **40**, 15–33.

Harvey, C. R., Cryptofinance. Social Science Research Network, 2016. Available online at: http://ssrn.com/abstract = 2438299.

Hileman, G. and Rausch, M., *Global Cryptocurrency Benchmarking Study*, 2017 (Cambridge University, Cambridge Center for Alternative Finance: Cambridge).

Hou, K., Xue, C. and Zhang, L., Replicating anomalies. *Rev. Financ. Stud.*, 2020, **33**(5), 2019–2133.

Howell, S. T., Niessner, M. and Yermack, D., Initial coin offerings: Financing growth with cryptocurrency token sales. *Rev. Financ. Stud.*, 2020, **33**(9), 3925–3974.

Huberman, G., Leshno, J. D. and Moallemi, C., Monopoly without a monopolist: An economic analysis of the Bitcoin payment system. Unpublished Working Paper. Columbia Business School, New York, 2017.

Katsiampa, P., Volatility estimation for Bitcoin: A comparison of GARCH models. *Econ. Lett.*, 2017, **158**, 3–6.

Katsiampa, P., Volatility co-movement between Bitcoin and Ether. *Financ. Res. Lett.*, 2019, **30**, 221–227.

Katsiampa, P., Corbet, S. and Lucey, B., Volatility spillover effects in leading cryptocurrencies: A BEKK-MGARCH analysis. *Financ. Res. Lett.*, 2019, **29**, 68–74.

Kethineni, S. and Cao, Y., The rise in popularity of cryptocurrency and associated criminal activity. *Int. Crim. Justice. Rev.*, 2020, **30**(3), 325–344.

Kyriazis, N. A., A survey on efficiency and profitable trading opportunities in cryptocurrency markets. *J. Risk Financ. Manag.*, 2019a, **12**(2), 67.

Kyriazis, N. A., A survey on empirical findings about spillovers in cryptocurrency markets. *J. Risk Financ. Manag.*, 2019b, **12**(4), 170.

Makarov, I. and Schoar, A., Trading and arbitrage in cryptocurrency markets. *J. Financ. Econ.*, 2020, **135**(2), 293–319.

Malinova, K. and Park, A., Market design with blockchain technology. Social Science Research Network, 2016. Available online at: https://papers.ssrn.com/sol3/Delivery.cfm?abstractid = 2785626.

Maume, P., Initial coin offerings and EU prospectus disclosure. *Eur. Bus. Law Rev.*, 2020, **31**(2), 185–208.

Nelson, D. B., Conditional heteroskedasticity in asset returns: A new approach. *Econometrica*, 1991, **59**(2), 347–370.

Raskin, M. and Yermack, D., Corporate governance and blockchains. *Rev. Financ.*, 2017, **21**, 7–31.

Rogers, L. and Satchell, S., Estimating variance from high, low and closing prices. *Ann. Appl. Probab.*, 1991, **1**, 504–512.

Taleb, N. N., *Statistical Consequences of Fat Tails: Real World Preasymptotics, Epistemology, and Applications*, 2020 (STEM Academic Press). arXiv:2001.10488 [stat.OT]

Appendix

Table A1 reports the values of the log-likelihood function for the EGARCH model where the mean equation is given by,

$$r_{BTC,t} = \mu_{BTC} + \rho_{BTC} r_{BTC,t-1} + \epsilon_{BTC,t}, \text{with}$$
$$\epsilon_{BTC,t} = \zeta_{BTC,t}\sigma_{BTC,t}$$

where $r_{BTC,t} = \ln\left(\frac{BTC_t}{BTC_{t-1}}\right)$ and BTC_t denotes the price of Bitcoin at time t, μ_{BTC} denotes the intercept term of the mean equation, ρ_{BTC} is the parameter measuring first-order autocorrelation and $\epsilon_{BTC,t}$ is the residual term at time t. The equation for the variance is given by,

$$\ln(\sigma^2_{BTC,t}) = \omega_{BTC} + \alpha_{BTC}\left|\frac{\epsilon_{BTC,t-1}}{\sigma_{BTC,t-1}}\right| + \beta_{BTC}\ln(\sigma^2_{BTC,t-1}) + \gamma_{BTC}\frac{\epsilon_{BTC,t-1}}{\sigma_{BTC,t-1}} + \delta_{BTC} d_{BTC,t}$$

where $\sigma^2_{BTC,t}$ is the conditional variance at time t, and the parameter vector $\boldsymbol{\theta}_{BTC} = (\omega_{BTC}, \alpha_{BTC}, \beta_{BTC}, \gamma_{BTC}, \delta_{BTC})$ is estimated using maximum-likelihood estimation. In this model, the variable $d_{BTC,i,t}$ is binary and defined as $d_{BTC,i,t} = 1$ if a hacking occurred at time $t - i$ and $d_{BTC,i,t} = 0$ otherwise. In this model, the assumption is made that the innovation process $\zeta_{BTC,t}$ follows a fat-tailed t-distribution, that is, $\zeta_{BTC,t}|\boldsymbol{\Omega}_{t-1} \sim t(v)$ where $v \in \{\mathbb{N}|v > 4\}$ denotes the degrees of freedom. The sample period is from April 28, 2013 to December 31, 2017.

Table A1. Values for Bitcoin's log-likelihood functions.

Degrees of freedom ***v***	Log-likelihood
5	3459.74
6	3445.12
7	3432.04
8	3420.48
9	3410.25
10	3401.17
11	3393.06
12	3385.79

Table A2 reports the values of the log-likelihood function for the EGARCH model where the mean equation is given by,

$$r_{ETH,t} = \mu_{ETH} + \rho_{ETH} r_{ETH,t-1} + \epsilon_{ETH,t}, \text{ with}$$
$$\epsilon_{ETH,t} = \zeta_{ETH,t}\sigma_{ETH,t}$$

where $r_{ETH,t} = \ln\left(\frac{ETH_t}{ETH_{t-1}}\right)$ and ETH_t denotes the price of Ethereum at time t, μ_{ETH} denotes the intercept term of the mean equation, ρ_{ETH} is the parameter measuring first-order autocorrelation and $\epsilon_{ETH,t}$ is the residual term at time t. The variance equation is given by

$$ln(\sigma^2_{ETH,t}) = \omega_{ETH} + \alpha_{ETH}\left|\frac{\epsilon_{ETH,t-1}}{\sigma_{ETH,t-1}}\right| + \beta_{ETH} ln(\sigma^2_{ETH,t-1}) + \gamma_{ETH}\frac{\epsilon_{ETH,t-1}}{\sigma_{ETH,t-1}} + \sum_{i=1}^{K}\delta_{ETH,i} d_{BTC,i,t}$$

where $\sigma^2_{ETH,t}$ is the conditional variance at time t, and the parameter vector $\boldsymbol{\theta}_{ETH} = (\omega_{ETH}, \alpha_{ETH}, \beta_{ETH}, \gamma_{ETH}, \delta_{ETH})$ is estimated using maximum-likelihood estimation. In this model, the variable $d_{ETH,i,t}$ is binary and defined as $d_{ETH,i,t} = 1$ if a hacking occurred in the Bitcoin market at time $t - i$ and $d_{ETH,i,t} = 0$ otherwise. In this model, the assumption is made that the innovation process $\zeta_{ETH,t}$ follows a fat-tailed t-distribution, that is, $\zeta_{BTC,t}|\boldsymbol{\Omega}_{t-1} \sim t(v)$ where $v \in \{\mathbb{N}|v > 4\}$ denotes the degrees of freedom. The sample period is from April 7, 2015 to December 31, 2017.

Table A2. Values for Ethereum's log–likelihood functions.

Degrees of freedom ***v***	Log-likelihood
5	1251.88
6	1248.73
7	1245.68
8	1242.88
9	1240.35
10	1238.08
11	1236.03
12	1234.18

Table A3 reports hacking incidents in the Bitcoin market in 2011, 2012 and 2018. The data for hackings were retrieved from Table 3 in *Biais et al.* (*2019*) and Table 3 in Grobys and Sapkota (2019) and matched with price data retrieved from coinmarketap.com and investing.com.

Table A3. Additional hacking incidents in the Bitcoin market in the extended sample.

Date	BTC	BTC Price	Loss in USD given time t	Incident
2011-06-13	25 000	19.8	495 000	User Allinvain hacked
2011-06-19	2000	17.5	35 000	MtGox theft
2011-06-25	4019	17.5	70 332.5	MyBitcoin theft
2011-07-26	17 000	17.5	297 500	Bitomat loss
2011-07-29	78 739	13.5	1 062 976.5	MyBitcoin theft
2011-10-06	5000	4.7	23 500	Bitcoin7 hack
2011-10-28	2609	3.2	8348.8	MtGox loss
2012-03-01	46 653	4.9	228 599.7	Linode hacks
2012-04-13	3171	4.9	15 537.9	Betcoin hack
2012-04-27	20 000	5.1	102 000	Tony76 Silk Road scam
2012-05-11	18 547	5	92 735	Bitcoinica hack
2012-07-04	1853	5.3	9820.9	MtGox hack
2012-07-13	40 000	5.9	236 000	Bitcoinica theft
2012-07-17	180 819	6.2	1 121 077.8	BST Ponzi scheme
2012-07-31	4500	6.7	30 150	BTC-e hack
2012-09-04	24 086	10.4	250 494.4	Bitfloor theft
2012-09-28	9222	12.4	114 352.8	User Cdecker hacked
2012-10-17	3500	11.8	41 300	Trojan horse
2012-12-21	18 787	13.5	253 624.5	Bitmarket.eu hack
2018-04-09	438	6770.73	2 965 579.74	Coin Secure hack
2018-09-14	5966	6512.71	38 854 827.86	Zaif hack