SAGE Open
July-September 2021: 1–8
© The Author(s) 2021
DOI: 10.1177/21582440211029911
journals.sagepub.com/home/sgo
SAGE

Herding on Fundamental/ Nonfundamental Information During the COVID-19 Outbreak and Cyber-Attacks: Evidence From the Cryptocurrency Market

Imran Yousaf[1], Shoaib Ali[1], Elie Bouri[2], and Anupam Dutta[3]

Abstract

We provide an empirical analysis of herding behavior in cryptocurrency markets during COVID-19 and periods of cyber-attacks, differentiating between fundamental and nonfundamental herding. The results show that herding behavior is driven by fundamental information during the full sample period and the cyber-attack days. However, herding is not prevalent during the COVID-19 outbreak, either when reacting to fundamental or nonfundamental information. This finding suggests heterogeneity in the behaviors of participants in the cryptocurrency markets during the COVID-19 period.

Keywords

cryptocurrency markets, herding behavior, COVID-19 outbreak, cyber-attacks, fundamental/nonfundamental information

Introduction

It is often argued that herding behavior among investors challenges the efficient market hypothesis and can explain some of behavioral anomalies in the financial markets. Herding can be classified into two categories (Bikhchandani & Sharma, 2000). First, "spurious herding" is the tendency of investors to behave similarly to the same set of fundamental information. When fundamental information is easily available and processable, investors herd by buying or selling specific assets until the market price becomes equal to its fundamental value (Alhaj-Yaseen & Rao, 2019). This type of herding stabilizes the asset market, because it is fundamental information based. Second, "intentional herding" is the inclination of investors to suppress their own private information (or fundamental information) and intentionally copy others. This type of herding increases volatility, drives prices away from the fundamental value (Dang & Lin, 2016), and leads to instability in financial markets. Therefore, spurious (intentional) herding leads to market efficiency (inefficiency).

Although herding is well documented in conventional assets such as stocks (Chang et al., 2000; Christie & Huang, 1995), bonds (Galariotis et al., 2016), and commodities (Kumar et al., 2021), it is relatively understudied in the cryptocurrency markets that have emerged over the past years as a new digital asset, attracting a great deal of attention from researchers, investors, and policymakers. The emergence and attractiveness of the cryptocurrency markets are mostly supported by (a) the speculative nature of cryptocurrencies and their detachment from the global financial system, (b) the decline in public trust toward the central banking system after the global financial crisis (Weber, 2016), (c) the fourth industrial revolution and use of smart technologies, and (d) the acceptance of Bitcoin and many other cryptocurrencies as digital means of payment (https://www.businessinsider.com/top-cryptocurrencies). Cryptocurrency markets are immature, highly subject to psychological and sociological factors, and often criticized as risky and inefficient (Bouri et al., 2019). Their market participants are mostly young individuals, with a low level of education, an "animal" spirit, large cultural differences, and their information is irregular. Furthermore, the cryptocurrency markets have weak regulatory frameworks and weak information disclosure, and there is a lack of fundamental models to evaluate the price of a

[1]Air University, Islamabad, Pakistan
[2]Lebanese American University, Beirut, Lebanon
[3]University of Vaasa, Finland

Corresponding Author:
Elie Bouri, School of Business, Lebanese American University, Beirut, Chouran POBO 13-5053, Lebanon.
Email: elie.elbouri@lau.edu.lb

cryptocurrency (Gerritsen et al., 2020). These malfunctions can push crypto-traders to ignore their own opinions and herd toward the market consensus, leading to abnormal volatility. Previous studies examine herding in the cryptocurrency markets during bullish and bearish days (Ballis & Drakos, 2019; Bouri et al., 2019; da Gama Silva et al., 2019; Stavroyiannis & Babalos, 2019; Vidal-Tomás et al., 2019) and high and low trading volume days (Haryanto et al., 2020; Kallinterakis & Wang, 2019). Notably, the scarce evidence on herding points to the tendency of herding in cryptocurrencies when uncertainty is high (Bouri et al., 2019). However, no study has so far examined whether specific informational events related to the unprecedented COVID-19 outbreak and cyber-attacks induce herding behavior and whether herding in the cryptocurrency markets is driven by fundamental or nonfundamental information. This study addresses this literature gap.

The COVID-19 outbreak has adversely affected stock market indices and raised economic policy uncertainty and implied volatility indices to extremely high levels. It has shaped global economic activity and the financial markets (The China Manufacturing Purchasing Manager's Index [PMI] declined by 33% in February 2020. U.S. equity indices declined by more than 30% during the period February 19, 2020 to March 23, 2020. Crude oil prices declined by more than 60% during the period January 1, 2020 to March 23, 2020. During the same period, Bitcoin price declined by 19%, including the cryptocurrency markets (e.g., Shahzad et al., 2021). Given the assumption that investors are fully informed, behave rationally, and make investment decisions after considering public information, crisis events such as COVID-19 have the power to induce uncertainty and noise in markets that disturb the decision processes of investors leading to irrational behavior. Herding intensity increases during market stress (Christie & Huang, 1995). Several studies have detected herding in various stock markets during crisis periods (Chiang & Zheng, 2010; Yousaf et al., 2018) as well as in commodity markets (Babalos & Stavroyiannis, 2015; Kumar et al., 2021). However, the existing literature remains salient regarding the herding behavior in the cryptocurrency markets around the COVID-19 outbreak.

As for cyber-attacks, they represent a major challenge in the cryptocurrency markets that rely on the internet and blockchain technology. Previous evidence exists for the frequent occurrence of cyber-attacks and their ability to destabilize the cryptocurrency markets (Caporale et al., 2020; Ciaian et al., 2016; Moore & Christin, 2013). Negative events related to cyber-attacks on Bitcoin/cryptocurrency exchanges reduce Bitcoin/cryptocurrency attractiveness for investors (Ciaian et al., 2016). The occurrence of cyber-attacks in the cryptocurrency markets generally drive crypto-traders to engage in sell-offs as a way to conform to the market consensus. Corbet et al. (2020) find that cyber-attacks not only increase the volatility of the cryptocurrency involved but also increase the correlation with other currencies. However, it is not clear whether cyber-attacks can shape herding in the cryptocurrency markets.

Cryptocurrencies do not have an underlying physical/monetary form as conventional assets such as equities. Various methods have been employed for valuation, such as the cost of production model for determining the fair value of Bitcoin (e.g., Hayes, 2017), aggregate blockchain characteristics (e.g., Bhambhwani et al., 2019), and the concept of utility (García-Monleón et al., 2020). This suggests the need for examining whether herding is driven by fundamental or nonfundamental information, which remains understudied.

This article contributes to the academic literature on four fronts. First, it contributes to the growing body of literature on the effects of the COVID-19 pandemic on financial markets (Bouri et al., 2021; Chowdhury et al., 2021) and cryptocurrency markets (Corbet et al., 2020; Shahzad et al., 2021; Yousaf & Ali, 2020) by extending the studies on herding in cryptocurrencies to the effect of the COVID-19 outbreak which represents an unprecedented crisis period. Second, it contributes to the literature on the effects of cyber-attacks on the cryptocurrency markets that are continuously facing the challenge of cybersecurity (e.g., Corbet et al., 2020). Caporale et al. (2020) point to the necessity to extend our limited understanding of the impact of cyber-crime to avoid potential disruption to cryptocurrency markets. Third, it nicely extends the growing literature on herding behaviors in cryptocurrencies by exploring whether herding is driven by fundamental or nonfundamental information (e.g., Bouri et al., 2019; Vidal-Tomás et al., 2019), especially given recent on the use of valuation models to evaluate the price of cryptocurrencies (Bhambhwani et al., 2019; García-Monleón et al., 2020; Hayes, 2017). Fourth, it accounts for the three-factors (market, size, and reversal factor) of the cryptocurrency model of Shen et al. (2019), which adequately capture important fundamental information that may affect cryptocurrency investor decisions at a market level.

Data and Methodology

Data

This study employs daily data on 75 cryptocurrencies that represent more than 82% (as of January 1, 2020) of the market capitalization of all cryptocurrencies (www.coinmarketcap.com). The full sample period is from 01/03/2015 to 19/03/2020, yielding 1,845 daily observations and covering the recent COVID-19 outbreak period that spans 01/01/2020 to 19/03/2020. Many recent studies (e.g., Shahzad et al., 2021; Yousaf & Ali, 2020) use approximately similar data segments to define the COVID-19 period while studying the financial markets and cryptocurrency markets. In Table 1, we have provided a list of the 32 largest cryptocurrency hacking events between 01/03/2015 and 19/03/2020. This list consists of different types of cyber-attack events that affected either the wallets of cryptocurrency investors, the cryptocurrency

Table 1. List of Major Cyber-Attacks in Cryptocurrency Markets.

Sr. #	Date	Amount of cryptocurrency theft ($ Million)	Exchange/ Market	Detail	Source
1	09/05/2016	2.14	Gatecoin	Gatecoin lost as much as 185,000 ethers and 250 Bitcoins, an amount worth roughly $2.14 m at press time	https://www.coindesk.com/gatecoin-2-million-bitcoin-ether-security-breach
2	01/08/2016	65	Bitfinex	In the second largest Bitcoin hack ever made after Mt. Gox. 119,756 Bitcoins were stolen	https://www.bloomberg.com/news/articles/2016-08-03/bitcoin-plunges-after-hackers-breach-h-k-exchange-steal-coins
3	13/10/2016	1.5	Bitcurex	Bitcurex's cold wallet revealed that someone had transferred 2,300 Bitcoin out of the trading platform's account	https://news.bitcoin.com/bitcurex-forced-million-theft/
4	22/04/2017	73	Yapizon	Yapizon (new name Youbit), reportedly lost 4,000 Bitcoins now worth $73m (£55m) to cyberthieves	https://www.bbc.com/news/technology-42409815
5	17/07/2017	7	CoinDash	"Hacker Steals $7 Million Worth of Ethereum from CoinDash Platform"	https://www.bloomberg.com/news/articles/2017-07-17/coindash-says-hacker-stole-7-million-at-initial-coin-offering
6	07/11/2017	280	Ethereum	A user playing with the Parity multisig wallet library contract triggered its kill function, effectively freezing the funds	https://www.cnbc.com/2017/11/08/accidental-bug-may-have-frozen-280-worth-of-ether-on-parity-wallet.html
7	21/11/2017	30	Tether	Tether stated that $30,950,010 USDT was sent to an unauthorized Bitcoin address	https://www.coindesk.com/tether-claims-30-million-stable-token-stolen-attacker
8	06/12/2017	67	NiceHash	Service breach and hack at NiceHash	https://www.cnbc.com/2017/12/07/bitcoin-stolen-in-hack-on-nicehash-cryptocurrency-mining-marketplace.html
9	18/12/2017	N/A	Youbit	Youbit, filed for bankruptcy after losing 17% of its crypto holdings in the cyber-attack	https://www.bbc.com/news/technology-42409815
10	26/01/2018	500	Coincheck	Hackers broke into a Coincheck Inc. and made off with nearly $500 million in digital tokens	https://fortune.com/2018/01/31/coincheck-hack-how/
11	31/01/2018	1	BeeToken	Cryptocurrency startup BeeToken was hacked while the attackers targeted its Initial Coin Offering (ICO) with phishing attacks	https://www.coindesk.com/bee-token-phishing-scam
12	04/02/2018	1.8	Ethereum	Potential Seele ICO investors were scammed out of nearly $2 million by impersonators posing as administrators	https://cointelegraph.com/news/scammers-steal-over-18-mln-by-posing-as-admins-of-steele-ico
13	08/02/2018	195	BitGrail	Italian exchange BitGrail was hacked in early February, with team members suggesting that $195 million in the token nano was stolen	https://fortune.com/2018/02/11/bitgrail-cryptocurrency-claims-hack/
14	15/02/2018	50	Bitcoin	A large scam netted $50 million in cryptocurrency	https://www.coindesk.com/cisco-50-million-bitcoin-phishing-scam-mimicked-blockchain-web-wallet
15	02/03/2018	50	Bitcoin	BTC Global was a scam launched in September 2017 by 'famous' trader Steven Twain	https://www.coindesk.com/south-african-investor-makes-off-50m-in-crypto-scam
16	05/04/2018	300	Bitcoin	Amit Bhardwaj was found to be the kingpin behind India's biggest cryptocurrency scam of GainBitcoin	https://finance.yahoo.com/news/founder-150-indian-bitcoin-ponzi-090953390.html
17	09/04/2018	650	ICO	Occurring in Vietnam, the largest alleged scam connected to an ICO was pulled off by two blockchain firms, Ifan, and Pincoin	https://cointelegraph.com/news/vietnam-pincoin-ifan-icos-exposed-as-scams-that-allegedly-stole-660-million

(continued)

Table 1. (continued)

Sr. #	Date	Amount of cryptocurrency theft ($ Million)	Exchange/ Market	Detail	Source
18	19/04/2018	20	Bitcoin	Two men started a scheme in 2015 and subsequently built a multilevel company by promising investors high returns through investing in Bitcoin	https://www.coindesk.com/bitcoin-pyramid-scheme-amassed-20-million-in-south-korea
19	18/05/2018	18	Bitcoin Gold	An unidentified hacker performed several "double spend" attacks on the infrastructure of the Bitcoin Gold cryptocurrency	https://fortune.com/2018/05/29/bitcoin-gold-hack/
20	10/06/2018	40	Coinrail	Cyber intrusion causing a loss of about 30% of the coins traded on the exchange	https://www.theguardian.com/technology/2018/jun/11/bitcoin-price-cryptocurrency-hacked-south-korea-coincheck
21	20/06/2018	32	Bithumb	One of the biggest cryptocurrency exchanges in South Korean, Bithumb was hacked in June 2018	https://www.bloomberg.com/news/articles/2018-06-20/cryptocurrencies-fall-as-korean-exchange-says-coins-were-stolen
22	09/07/2018	23.5	Bancor	Bancor lost some $23.5 million of cryptocurrency tokens belonging to its users following a hack	https://techcrunch.com/2018/07/10/bancor-loses-23-5m/
23	14/09/2018	62.5	Zaif	Zaif, lost approximately $62.5 million in the Bitcoin (BTC), Monacoin (MONA), and Bitcoin cash (BCH) cryptocurrencies	https://finance.yahoo.com/news/hacked-crypto-exchange-zaif-resuming-120518736.html
24	28/10/2018	5	MapleChange	Maple change reported over $5 million in losses—virtually all its funds	https://www.forbes.com/sites/rogerhuang/2018/10/29/maplechange-hack-is-a-reminder-to-get-your-cryptocurrencies-off-exchanges/#15ed99497df5
25	13/01/2019	16	Cryptopia	According to the calculations of the analytical company Elementus, they lost $16 million in Ethereum (ETH) and ERC-20 tokens	https://www.coindesk.com/new-zealand-crypto-exchange-cryptopia-goes-offline-citing-major-hack
26	25/03/2019	100	Coinbene	"Over $100 Million Missing: CoinBene Claims Maintenance, a Month of Questions Point Toward a Hack"	https://cointelegraph.com/news/over-100-million-missing-coinbene-claims-maintenance-a-month-of-questions-point-toward-a-hack
27	29/03/2019	19	Bithumb	More than 3 million EOS tokens (about $ 13 million) and 20 million Ripple tokens (about $ 6 million) were withdrawn from the exchange's hot wallet	https://www.coindesk.com/crypto-exchange-bithumb-hacked-for-13-million-in-suspected-insider-job
28	07/05/2019	40.5	Binance	One of the hot wallets was hacked, from which 7,000 Bitcoins were withdrawn in one transaction	https://www.telegraph.co.uk/technology/2019/05/08/bitcoin-safety-spotlight-hackers-steal-30-million-digital-currency/
29	28/06/2019	4.2	Bitrue	The Singaporean trade Bitrue suffered a robbery of about $5 million. The attackers accessed 90 client accounts	https://finance.yahoo.com/news/4-2-million-stolen-bitrue-192956062.html
30	06/06/2019	10	GateHub	More than $10 Million in Ripple was stolen by unknown thieves from GateHub	https://finance.yahoo.com/news/report-nearly-10-million-xrp-200800454.html
31	11/07/2019	32	BitPoint	Unknown attackers stole 3.5 billion yen (about $ 32 million) in cryptocurrencies Bitcoin, Bitcoin Cash, Litecoin, Ripple, and Ethereum	https://www.bloomberg.com/news/articles/2019-07-12/japan-s-bitpoint-loses-32m-in-lastest-crypto-exchange-hack
32	27/11/2019	49	Upbit	342,000 ETH was sent from Upbit's Ethereum hot wallet to an anonymous wallet address	https://www.wsj.com/articles/nearly-50-million-of-ether-swiped-from-south-korean-cryptocurrency-exchange-11574918838

exchange, or the blockchain supporting a specific cryptocurrency. We have used the mainstream news sources of cryptocurrency market to identify these cyber-attack events, like Bloomberg, BBC, Forbes, Fortune, Yahoo Finance, Wall street Journal, and Coin desk. We have also used those cyber-attack events which are used by the Corbet et al. (2020). The risk-free rate is defined as the U.S. 3-month T-bill rate, for which the data are taken from the U.S. Department of the Treasury (https://www.treasury.gov/resource-center/data-chart-center/interest-rates/Pages/default.aspx). The empirical analysis is performed with daily log return of cryptocurrency series. Unreported results show that all cryptocurrency returns exhibit a high standard deviation value and a departure from the normal distribution, which points to tail events. Furthermore, all return series are stationary.

Spurious vs. Intentional Herding During COVID-19 and Hacking Days

Our base model follows Chang et al. (2000) who argue that the nonlinear relationship between the dispersion of individual asset returns and market returns is interpreted as evidence of herding behavior. Dispersion is measured through the cross-sectional absolute deviations (CSAD) as follows:

$$CSAD_t = \frac{\sum_{i=1}^{N} \left| R_{it} - R_{mt} \right|}{N}. \tag{1}$$

In the framework of our study, i denotes the cryptocurrency, t denotes the time period, and N represents the number of cryptocurrencies. R_{it} indicates the returns of each cryptocurrency i at time t, R_{mt} denotes the market returns (i.e., cross-sectional average returns of N cryptocurrencies) at time t. Lower values of CSADs suggest that investors discard their private information and copy their peers. Chang et al. (2000) propose the following model to estimate herding:

$$CSAD_t = \alpha + \beta_1 \left| R_{mt} \right| + \beta_2 \left(R_{mt} \right)^2 + e_t. \tag{2}$$

The rational asset pricing model suggests that β_1 should be positive and β_2 should be 0. However, Chang et al.'s (2000) model indicates the existence of herding in the market if β_2 is negatively significant. Hence, the negative and nonlinear association between the CSAD and the market returns points to the presence of herding behavior by showing that individual cryptocurrency returns are clustered around the market return.

Following Galariotis et al. (2015), we split the total CSAD into two parts, (a) CSAD due to common fundamental factors and (b) CSAD due to nonfundamental information. To estimate CSAD fundamental and CSAD nonfundamental, we first calculate the three-factors (excess market returns, small minus big, and reversal factor) of the cryptocurrency model, suggested by the Shen et al. (2019), to adequately capture the important fundamental information that may affect cryptocurrency investor decisions on a market level. We then estimate a regression of the total *CSAD* as follows:

$$CSAD_t = \beta_0 + \beta_1 \left(R_{m,t} - Rf_t \right) + \beta_2 SMB_t + \beta_3 DMU_t + \varepsilon_t, \tag{3}$$

where $R_{m,t} - Rf_t$ denotes the excess market returns, *SMB* is the small minus big return factor, and *DMU* is the reversal factor. Following Galariotis et al. (2015), the CSAD based on nonfundamental information is given by:

$$CSAD_{NonFundamental,t} = \varepsilon_t, \tag{4}$$

However, the CSAD based on fundamental information can be written as:

$$CSAD_{Fundamental,t} = CSAD_t - CSAD_{NonFundamental,t}. \tag{5}$$

Then, the fundamental and nonfundamental information-based herding is estimated through the following equations:

$$CSAD_{Fundamental,t} = \alpha + \beta_1 \left| R_{mt} \right| + \beta_2 (R_{mt})^2 + e_t, \tag{6}$$

$$CSAD_{NonFundamental,t} = \alpha + \beta_1 \left| R_{mt} \right| + \beta_2 (R_{mt})^2 + e_t. \tag{7}$$

In Equation 6, if β_2 is negatively significant then there is spurious herding. In Equation 7, if β_2 is negatively significant then there is intentional herding.

To estimate whether herding is spurious or intentional in the cryptocurrency markets during the COVID-19 outbreak, the following regressions are used:

$$CSAD_t = \alpha + \beta_1 \left| R_{mt} \right| + \beta_2 \left(R_{mt} \right)^2 + \beta_3 \left(R_{mt} \right)^2 * DM_t^{COVID} + e_t, \tag{8}$$

$$CSAD_{FUN,t} = \alpha + \beta_1 \left| R_{mt} \right| + \beta_2 \left(R_{mt} \right)^2 + \beta_3 \left(R_{mt} \right)^2 * DM_t^{COVID} + e_t, \tag{9}$$

$$CSAD_{NON_{FUN},t} = \alpha + \beta_1 \left| R_{mt} \right| + \beta_2 \left(R_{mt} \right)^2 + \beta_3 \left(R_{mt} \right)^2 * DM_t^{COVID} + e_t. \tag{10}$$

For COVID-19, DM_t is a dummy variable that takes the value of 1 during the COVID-19 period (01/01/2020 to 19/03/2020) and 0 otherwise.

To examine whether herding is spurious or intentional during cyber-attack days in cryptocurrency markets, the following regressions are used:

$$CSAD_t = \alpha + \beta_1 \left| R_{mt} \right| + \beta_2 \left(R_{mt} \right)^2 + \beta_3 \left(R_{mt} \right)^2 * DM_t^{Cyber} + e_t, \tag{11}$$

Table 2. Results of Fundamental and Nonfundamental Herding—Full Sample Period.

	Total CSAD			Fundamental driven CSAD			Nonfundamental driven CSAD		
	$CSAD_t = \alpha + \beta_1 \lvert R_{mt} \rvert + \beta_2 (R_{mt})^2 + e_t$			$CSAD_{FUN,t} = \alpha + \beta_1 \lvert R_{mt} \rvert + \beta_2 (R_{mt})^2 + e_t$			$CSAD_{Non-FUN,t} = \alpha + \beta_1 \lvert R_{mt} \rvert + \beta_2 (R_{mt})^2 + e_t$		
	β0	β1	β2	β0	β1	β2	β0	β1	β2
Coefficients	0.133	0.872	**−1.900**	0.155	0.062	**−1.049**	−0.022	0.810	−0.851
P value	0.000	0.000	**0.002**	0.000	0.004	**0.000**	0.000	0.000	0.159

Note. If β_3 is negatively significant, then there is significant herding. Significant values of β_3 at the 1% level of significance are given in Bold. CSAD = cross-sectional absolute deviations.

Table 3. Results of Fundamental and Nonfundamental Herding During COVID-19.

	Total CSAD				Fundamental driven CSAD				Nonfundamental driven CSAD			
	$CSAD_t = \alpha + \beta_1 \lvert R_{mt} \rvert + \beta_2 (R_{mt})^2 + \beta_3 (R_{mt})^2 * DM_t^{COVID} + e_t$				$CSAD_{FUN,t} = \alpha + \beta_1 \lvert R_{mt} \rvert + \beta_2 (R_{mt})^2 + \beta_3 (R_{mt})^2 * DM_t^{COVID} + e_t$				$CSAD_{NON_{FUN},t} = \alpha + \beta_1 \lvert R_{mt} \rvert + \beta_2 (R_{mt})^2 + \beta_3 (R_{mt})^2 * DM_t^{COVID} + e_t$			
	β0	β1	β2	β3	β0	β1	β2	β3	β0	β1	β2	β3
Coefficients	0.132	0.969	−2.975	0.961	0.153	0.174	−2.286	1.106	−0.022	0.796	−0.689	−0.145
P value	0.000	0.000	0.043	0.418	0.000	0.000	0.000	0.000	0.000	0.000	0.629	0.900

Note. DM_t^{COVID} is a dummy variable equal to 1 during the period of COVID-19 (01/01/2020 to 19/03/2020) and zero otherwise. If β_3 is negatively significant, then there is significant herding during the COVID-19 period. CSAD = cross-sectional absolute deviations.

$$CSAD_{FUN,t} = \alpha + \beta_1 \lvert R_{mt} \rvert + \beta_2 (R_{mt})^2 + \beta_3 (R_{mt})^2 * DM_t^{Cyber} + e_t, \quad (12)$$

$$CSAD_{NON_{FUN},t} = \alpha + \beta_1 \lvert R_{mt} \rvert + \beta_2 (R_{mt})^2 + \beta_3 (R_{mt})^2 * DM_t^{Cyber} + e_t. \quad (13)$$

For hacking events, DM_t is a dummy variable equal to 1 on a day when a cyber-attack event occurs (see Table 1) and 0 otherwise.

Empirical Findings

The results for fundamental and nonfundamental herding are reported in Tables 2 to 4. Table 2 reveals that the β_2 coefficient (−1.900) is negative and significant in the total CSAD-based equation, indicating the existence of herding in the cryptocurrency markets for the full sample period. These findings are similar to results of da Gama Silva et al. (2019) and Ballis and Drakos (2019), which provides evidence of herding in the cryptocurrency markets. The β_2 coefficient (−1.049) is also negative and significant in the fundamental driven CSAD equation, showing the presence of spurious (i.e., fundamental information based) herding. This finding adds to previous studies (e.g., Bouri et al., 2019) by arguing that herding is due to fundamentals. Table 3 shows the results of herding during the COVID-19 period. The coefficient of β_3 is positive in both total and fundamental CSAD-based regressions, whereas it is negative but insignificant in nonfundamental CSAD-based regression. These results indicate no evidence of total, spurious, or intentional herding during the COVID-19 period, suggesting heterogeneity in the behaviors of participants in the cryptocurrency markets during the COVID-19 period. This finding is quite different from previous evidence of herding in the cryptocurrency markets during market turmoil periods (e.g., Bouri et al., 2019), suggesting that not all crisis periods are alike when it comes to herding. Table 4 indicates that the β_3 coefficient (−0.861) is negative and significant, providing evidence of spurious herding during the days of cyber-attacks in the cryptocurrency markets (i.e., investors behave similarly in response to fundamental information during cyber-attack days). This finding implies that cyber-attack events matter to investors and contain information that affects investor behavior and their future preferences (Caporale et al., 2020; Corbet et al., 2020). This is a particularity of cryptocurrency markets that lack fundamentals and are shaped by security issues and technological development related to blockchain technology (Corbet et al., 2020). It adds to previous studies arguing that herding is affected by sentiment factors due to the shortage of a fundamental basis (Philippas et al., 2020).

Our results emphasize the importance of the sample periods used in this analysis. The cryptocurrency markets exhibit significant (fundamental) herding during cyber-attacks but do not show any evidence of herding behaviors due to the

Table 4. Results of Fundamental and Nonfundamental Herding During Cyber Security Attacks.

	Total CSAD				Fundamental driven CSAD				Nonfundamental driven CSAD			
	$CSAD_t = \alpha + \beta_1\lvert R_{mt}\rvert + \beta_2\left(R_{mt}\right)^2 + \beta_3\left(R_{mt}\right)^2 * DM_t^{Cyber} + e_t$				$CSAD_{FUN,t} = \alpha + \beta_1\lvert R_{mt}\rvert + \beta_2\left(R_{mt}\right)^2 + \beta_3\left(R_{mt}\right)^2 * DM_t^{Cyber} + e_t$				$CSAD_{NONFUN,t} = \alpha + \beta_1\lvert R_{mt}\rvert + \beta_2\left(R_{mt}\right)^2 + \beta_3\left(R_{mt}\right)^2 * DM_t^{Cyber} + e_t$			
	β0	β1	β2	β3	β0	β1	β2	β3	β0	β1	β2	β3
Coefficients	0.133	0.877	−1.900	−0.458	0.155	0.071	−1.049	**−0.861**	−0.022	0.806	−0.851	0.403
P value	0.000	0.000	0.002	0.781	0.000	0.001	0.000	**0.091**	0.000	0.000	0.159	0.802

Note. DM_t^{Cyber} is a dummy variable equals to 1 on the days when cyber-attack events occur (see Table 1), and zero otherwise. If β_3 is negatively significant, then there is significant herding during Cyber security attack days. Significant values of β_3 at the 10% level of significance are given in Bold. CSAD = cross-sectional absolute deviations.

COVID-19 pandemic. This concords with previous studies showing that herding increases with the level of uncertainty, which in our case is related to cyber-attacks, but not to COVID-19. The latter seems to represent an exogenous factor to the behavior of crypto-traders, suggesting the irrelevance of informative signals derived from COVID-19 on herding whereas informative signals derived from technological factors such as cyber-attacks matter to herding. This finding can also be explained in light of the literature showing the detachment of cryptocurrencies from the global financial system and their hedging ability. Accordingly, our results indicate that participants in the cryptocurrency markets during COVID-19 do not feel the panic of uncertainty seen during cyber-attacks, probably because COVID-19 does not induce enough uncertainty to make investors mimic the actions of others, implying a lack of consensus on how crypto-traders interpret this unprecedented pandemic event in the era of cryptocurrencies. In contrast, crypto-traders have the learning from previous cyber-attacks, which makes them use their cognitive learning and long memories to herd toward the consensus.

Conclusion

The related literature is unclear about whether herding behavior in cryptocurrencies is significant during specific informational events related to COVID-19 and to cyber-attacks. In this article, we provide an empirical analysis of herding behavior in the cryptocurrency markets while decomposing deviations into deviations due to fundamental and deviations due to nonfundamental information. Results show significant fundamental herding during the full sample period and the cyber-attack days, which leads to efficiency (Bikhchandani & Sharma, 2000) in the cryptocurrency markets. Therefore, investors behave similarly in response to fundamental information during cyber-attack days, suggesting that cyber-attack events matter to investors and contain information that affects investor behavior and their future preferences. This evidence is not surprising given that the cryptocurrency markets are shaped by security issues and technological development related to blockchain technology. However, further analysis shows no evidence of significant fundamental or nonfundamental herding behavior during the COVID-19 outbreak, suggesting that investors behave heterogeneously in cryptocurrency markets during this unprecedented pandemic period. It seems that crypto-traders believe that the cryptocurrency markets, which are detached from the global financial system, will be relatively unaffected by the COVID-19 uncertainty. Accordingly, crypto-traders exhibit heterogenous behavior regarding whether they should cash out or remain invested, which has led to insignificant herding.

Our results matter to portfolio managers and have implications that involve both theory and empirical study. Theoretical herding models could benefit from our new evidence that crypto-traders spuriously copy each other's actions during cyber-attacks, whereas the COVID-19 outbreak does not provide significant information to induce herding. These findings deserve further investigation in the spirit of Philippas et al. (2020). As argued by Bikhchandani and Sharma (2000), the lack of nonfundamental herding does not jeopardize the fragility of markets. Therefore, crypto-traders can herd for various reasons, independent of global uncertainty. This seems to be a feature of cryptocurrency markets, which requires future studies on equity markets. Further studies can consider how COVID-19 and cyber-attacks have shaped the dynamics of return and volatility across cryptocurrencies. This can be done using high-frequency data.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Elie Bouri https://orcid.org/0000-0003-2628-5027

Availability of Data and Materials

Data will be available from the authors upon request.

References

Alhaj-Yaseen, Y. S., & Rao, X. (2019). Does asymmetric information drive herding? An empirical analysis. *Journal of Behavioral Finance*, *20*(4), 451–470.

Babalos, V., & Stavroyiannis, S. (2015). Herding, anti-herding behaviour in metal commodities futures: A novel portfolio-based approach. *Applied Economics*, *47*(46), 4952–4966.

Ballis, A., & Drakos, K. (2019). Testing for herding in the cryptocurrency market. *Finance Research Letters*, *33*, 101210.

Bhambhwani, S., Delikouras, S., & Korniotis, G. M. (2019). *Do fundamentals drive cryptocurrency prices?* (SSRN 3342842). https://wpcarey.asu.edu/sites/default/files/george_korniotis_seminar_paper_november_8_2019.pdf

Bikhchandani, S., & Sharma, S. (2000). Herd behavior in financial markets. *IMF Staff Papers*, *47*(3), 279–310.

Bouri, E., Cepni, B., Gabauer, D., & Gupta, R. (2021). Return connectedness across asset classes around the COVID-19 outbreak. *International Review of Financial Analysis*, *73*, 101646.

Bouri, E., Gupta, R., & Roubaud, D. (2019). Herding behaviour in cryptocurrencies. *Finance Research Letters*, *29*, 216–221.

Caporale, G. M., Kang, W. Y., Spagnolo, F., & Spagnolo, N. (2020). Non-linearities, cyber attacks and cryptocurrencies. *Finance Research Letters*, *32*, 101297.

Chang, E. C., Cheng, J. W., & Khorana, A. (2000). An examination of herd behavior in equity markets: An international perspective. *Journal of Banking & Finance*, *24*(10), 1651–1679.

Chiang, T. C., & Zheng, D. (2010). An empirical analysis of herd behavior in global stock markets. *Journal of Banking & Finance*, *34*(8), 1911–1921.

Chowdhury, E. K., Khan, I. I., & Dhar, B. K. (2021). Catastrophic impact of Covid-19 on the global stock markets and economic activities. *Business and Society Review*. Advance online publication. https://doi.org/10.1111/basr.12219

Christie, W. G., & Huang, R. D. (1995). Following the pied piper: Do individual returns herd around the market? *Financial Analysts Journal*, *51*(4), 31–37.

Ciaian, P., Rajcaniova, M., & Kancs, D. A. (2016). The economics of Bitcoin price formation. *Applied Economics*, *48*(19), 1799–1815.

Corbet, S., Cumming, D. J., Lucey, B. M., Peat, M., & Vigne, S. A. (2020). The destabilising effects of cryptocurrency cybercriminality. *Economics Letters*, *191*, 108741.

da Gama Silva, P. V. J., Klotzle, M. C., Pinto, A. C. F., & Gomes, L. L. (2019). Herding behavior and contagion in the cryptocurrency market. *Journal of Behavioral and Experimental Finance*, *22*, 41–50.

Dang, H. V., & Lin, M. (2016). Herd mentality in the stock market: On the role of idiosyncratic participants with heterogeneous information. *International Review of Financial Analysis*, *48*, 247–260.

Galariotis, E. C., Krokida, S. I., & Spyrou, S. I. (2016). Bond market investor herding: Evidence from the European financial crisis. *International Review of Financial Analysis*, *48*, 367–375.

Galariotis, E. C., Rong, W., & Spyrou, S. I. (2015). Herding on fundamental information: A comparative study. *Journal of Banking & Finance*, *50*, 589–598.

García-Monleón, F., Danvila-del-Valle, I., & Lara, F. J. (2020). Intrinsic value in crypto currencies. *Technological Forecasting and Social Change*, *162*, 120393.

Gerritsen, D. F., Bouri, E., Ramezanifar, E., & Roubaud, D. (2020). The profitability of technical trading rules in the Bitcoin market. *Finance Research Letters*, *34*, 101263.

Haryanto, S., Subroto, A., & Ulpah, M. (2020). Disposition effect and herding behavior in the cryptocurrency market. *Journal of Industrial and Business Economics*, *47*, 115–132.

Hayes, A. S. (2017). Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing Bitcoin. *Telematics and Informatics*, *34*(7), 1308–1321.

Kallinterakis, V., & Wang, Y. (2019). Do investors herd in cryptocurrencies–and why? *Research in International Business and Finance*, *50*, 240–245.

Kumar, A., Badhani, K. N., Bouri, E., & Saeed, T. (2021). Herding behavior in the commodity markets of the Asia-Pacific region. *Finance Research Letters*, *41*, 101813. https://doi.org/10.1016/j.frl.2020.101813

Moore, T., & Christin, N. (2013). Beware the middleman: Empirical analysis of Bitcoin-exchange risk. *Financial Cryptography and Data Security*, *7859*, 25–33.

Philippas, D., Philippas, N., Tziogkidis, P., & Rjiba, H. (2020). Signal-herding in cryptocurrencies. *Journal of International Financial Markets, Institutions & Money*, *65*, 101191. https://doi.org/10.1016/j.intfin.2020.101191

Shahzad, S. J. H., Bouri, E., Kang, S. H., & Saeed, T. (2021). Regime specific spillover across cryptocurrencies and the role of COVID-19. *Financial Innovation*, *7*(1), 1–24.

Shen, D., Urquhart, A., & Wang, P. (2019). A three-factor pricing model for cryptocurrencies. *Finance Research Letters*, *34*, 101248.

Stavroyiannis, S., & Babalos, V. (2019). Herding behavior in cryptocurrencies revisited: Novel evidence from a TVP model. *Journal of Behavioral and Experimental Finance*, *22*, 57–63.

Vidal-Tomás, D., Ibáñez, A. M., & Farinós, J. E. (2019). Herding in the cryptocurrency market: CSSD and CSAD approaches. *Finance Research Letters*, *30*, 181–186.

Weber, B. (2016). Bitcoin and the legitimacy crisis of money. *Cambridge Journal of Economics*, *40*(1), 17–41.

Yousaf, I., & Ali, S. (2020). Discovering interlinkages between major cryptocurrencies using high-frequency data: New evidence from COVID-19 pandemic. *Financial Innovation*, *6*, 45. https://doi.org/10.1186/s40854-020-00213-1

Yousaf, I., Ali, S., & Shah, S. Z. A. (2018). Herding behavior in Ramadan and financial crises: The case of the Pakistani stock market. *Financial Innovation*, *4*(1), 16.