ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/354995772

Cryptocurrency Market Manipulation: A Systematic Literature Review

Conference Paper · December 2021

CITATIONS
18

READS
8,611

3 authors:

Felix Eigelshoven
Universität Potsdam
6 PUBLICATIONS **42** CITATIONS
SEE PROFILE

André Ullrich
Weizenbaum Institute for the Networked Society
93 PUBLICATIONS **932** CITATIONS
SEE PROFILE

Douglas A Parry
Stellenbosch University
63 PUBLICATIONS **953** CITATIONS
SEE PROFILE

All content following this page was uploaded by Felix Eigelshoven on 25 October 2021.

The user has requested enhancement of the downloaded file.

Cryptocurrency Market Manipulation: A Systematic Literature Review

Completed Research

Felix Eigelshoven
University of Potsdam
Potsdam, Germany
feigelshoven@lswi.de

André Ullrich
University of Potsdam
Potsdam, Germany
aullrich@lswi.de

Douglas Parry
Stellenbosch University
Stellenbosch, South Africa
dougaparry@sun.ac.za

Abstract

Cryptocurrencies, a new class of digital asset predominantly based on blockchain technologies, have gained immense popularity in recent years. Despite of advantages over traditional monetary systems such as lower transaction cost, increased transactional security, or transparency, cryptocurrencies are not free of disadvantages. The increase in popularity has also led to an increase in market manipulation in these markets. While there has been some attempt to identify and classify various cryptocurrency market manipulation schemes, there is a distinct need for a holistic description and classification of current cryptocurrency market manipulation schemes. Therefore, based on a systematic literature review, this paper provides an overview of cryptocurrency market manipulation methods using a concept-centric approach, a characterization of these methods, and identifies market vulnerabilities.

Keywords: Cryptocurrencies, market manipulation, regulation, systematic literature review

Introduction

Cryptocurrencies, a new class of digital asset predominantly based on blockchain technologies, have gained immense popularity in recent years. Most recently, this attention has been reflected in the investments of large institutional investors and companies, such as Tesla, and the recent IPO of the biggest cryptocurrency exchange, Coinbase (Philipps and Graves 2021). Together with blockchain technology, cryptocurrencies represent one of the most promising fintech innovations of the last decade. Due to their capacity to support financial transaction-making, disintermediation and enable new service models these technologies hold the potential to permanently change market mechanisms and financial services (Gomber et al. 2018).

Although many of the fundamental concepts of cryptocurrencies, such as the proof of work system of *Hashcash*, were introduced in the early 1990s (Back 2002), a key event that singularly advanced the development of cryptocurrencies was the introduction of Bitcoin in 2008 by the pseudonymous Satoshi Nakamoto (2008). Thirteen years on, in April 2021, there were over 9,000 different cryptocurrencies at a total market capitalization of over USD 1.7 trillion (CoinMarketCap 2021). Following the work of Chohan (2017a), cryptocurrencies can be understood as "a digital asset that is constructed to function as a medium of exchange, premised on the technology of cryptography, to secure the transactional flow, as well as to control the creation of additional units of the currency". Due to their decentralized nature, cryptocurrencies do not require a central third party to confirm individual transactions, as is the case with traditional transactions in *fiat* currency. Decentralization is made possible by so-called consensus algorithms. These

Preprint Version

provide different sets of rules that allow network peers to reach a common agreement about the state of the network. For cryptocurrencies, such consensus may also pertain to the status of a transaction or the balance of a user (Viriyasitavat and Hoonsopon 2019).

The decentralized and peer-to-peer structure of cryptocurrencies offer various advantages and opportunities over traditional monetary systems. Some of the advantages are lower transaction costs, increased transactional security and privacy, transaction transparency, and higher transaction efficiency (Rejeb et al. 2021). However, cryptocurrencies are not free of disadvantages and especially decentralization can be considered a double-edged sword. The absence of a central third party to manage the cryptocurrency can make it difficult to regulate the currency and protect it from price or market manipulation. Market manipulation in this case refers to a series of practices to influence pricing in markets through unfair measures in order to make unjustified profits (Lin 2017). In the case of Bitcoin, it remains unclear to what extent the price is affected by market manipulations. For example, Gandal et al. (2018) assumed that the price spike from USD 150 to USD 1000 in 2013 arose from artificial trading by bots, initiated by the owners of the popular Mt. Gox exchange. Griffin and Shams (2019) argued that the price rally to USD 20,000 in 2017 was affected by large-scale market manipulation by just one single entity. Market manipulation is one of the greatest threats to the well-being of financial markets. It distorts prices and hinders the efficient allocation of resources (Putniņš 2012), which in the long run can discourage investors from entering the market. There has been some attempt to identify and classify various cryptocurrency market manipulation schemes (Twomey and Mann 2020). However, given the increasing prominence of cryptocurrencies and the ongoing prevalence of market manipulation (McIntosh 2020), there is a distinct need for holistic description and classification of current cryptocurrency market manipulation schemes based on current scientific knowledge. Due to the complexity of the cryptocurrency ecosystem and the continuous development of blockchain technologies, most studies (Cong et al. 2020; Li et al. 2018; Sobol 2020) have focused on an isolated analysis of a single manipulation method. Thus, this paper aims to answer the following research questions:

RQ1: Which cryptocurrency market manipulation techniques exist and what elements characterize these schemes?

In the context of the 2007 financial crisis, the Dodd-Frank Act (United States 2010) demonstrated that regulation was an adequate tool to improve market efficiency and restore investor confidence in markets. However, regulation inevitably leads to centralization. This dynamic violates the fundamental idea of the blockchain, and it remains unclear to what extent cryptocurrency markets should be regulated. To reduce the risk of overregulation, it is essential to understand how market manipulation manifests within the cryptocurrency market and which market vulnerabilities influence the success of those manipulation methods. Given the above context, this paper aims to answer the second question:

RQ2: Which market vulnerabilities influence the success of manipulation within cryptocurrency markets?

By addressing these research questions and the gap in literature, this paper contributes to the body of knowledge on cryptocurrencies in the following ways. First, a holistic classification of cryptocurrency market manipulation techniques is provided in the form of a concept matrix. This comprehensive classification of market manipulation techniques is beneficial for both practice and research as it provides an understanding of the underlying market dynamics. Second, identification of market vulnerabilities allows for the sustainable development of regulatory approaches and reduces the risk of overregulating the market. Finally, the study provides future research opportunities.

This paper is set out as follows. The second section provides the theoretical background of blockchain technologies, cryptocurrencies, and their markets. The third section describes the methodology of the systematic literature review and final literature basket. The fourth section presents a synthesis of the results in the form of a concept-centric matrix and classifies the market manipulation schemes identified. The fifth section discusses the results regarding market vulnerabilities and provides directions for future research. The final section provides an overall conclusion and discusses the limitations of the paper.

Preprint Version

Background

Cryptocurrencies are classified as a subset of virtual currencies. They are defined as a digital representation of value, issued by a private developer instead of a central bank, credit institute or e-money institute. In some circumstances, they can be used as an alternative form of money (European-Central-Bank 2015). Most cryptocurrencies are based on the blockchain, which is a distributed and decentralized ledger where data is aggregated in the form of blocks (Nakamoto 2009). Unlike previous attempts at digital currencies (e.g., e-gold), cryptocurrencies do not require a central authority to process and settle transactions. Instead, transactions are verified within a decentralized network though cryptographic techniques; the transaction data are then stored immutably on a distributed ledger (Gandal et al. 2018). Cryptocurrencies can be transferred between addresses that are managed, in the form of wallets. Each wallet owner possesses a private and a public key. To send a transaction the owner needs the address of the target wallet, which can be derived from its public key. Additionally, a valid transaction has to be signed by the private key of the sender (Victor and Weintraud 2021). As with other virtual currencies, cryptocurrencies run the risk of money being spent twice – which is called the "double spending problem". This can be attributed primarily to their digital nature and the associated ease of reproducibility (Chohan 2017b). Until the rise of Bitcoin and the Proof of Work consensus in early 2009, solving this problem always required a central party, which created a dependency. Among cryptocurrencies, a distinction can be made between coins and tokens. Coins are standalone crypto assets that are native to their own primary blockchain and do not require another blockchain-based platform for their execution. For example, *Ether* can be classified as a coin that operates on the Ethereum blockchain. Cryptocurrency tokens, by contrast, can be described as a digital fungible asset derived from another primary blockchain (Ledger 2019). An example here are *ERC20* tokens. ERC20 describes a standard for the implementation of tokens via smart contracts on the Ethereum platform (Vogelsteller and Buterin 2020). The two main forms of cryptographic tokens are utility and security tokens (Liu and Wang 2019). Utility tokens are usually developed to serve a specific purpose within a blockchain application or platform; they are most commonly used as a payment for purchases within blockchain platforms. Security tokens, by contrast, function similarly to traditional securities and are the blockchain counterpart to a classic share.

Cryptocurrency Exchanges and Market Dynamics

Cryptocurrency exchanges play a central role in cryptocurrency markets because they provide liquidity and facilitate price discovery (Cong et al. 2020). Because of the growing exposure of Bitcoin and other new Altcoins (alternative cryptocurrencies to Bitcoin), at the time of writing at least 368 exchanges allow for the trading of cryptocurrencies (CoinMarketCap 2021). Like stock markets, cryptocurrency exchanges have two main order types: limit orders and market orders. A limit order specifies a certain price that the user wishes to trade for. A market order is executed against the current best bid or ask price. A market order consumes liquidity in the market, whereas a limit order increases the supply of available shares and therefore provides liquidity (Parlour and Seppi 2008).

Cryptocurrency exchanges can be classified as centralized or decentralized. Centralized exchanges (CEX) keep the assets of a user in the collective wallet of the exchange and are generally owned by a central organization – such as Coinbase or Binance. To trade on a CEX, the user must send their funds to an exchange-owned wallet, which is specifically created for that user. Within CEXs, all trading happens outside of the blockchain and is executed by the exchange (Victor and Weintraud 2021). Multiple exchange frauds and thefts, and especially the shutdown of the Mt. Gox exchange in 2013, have shown that storing cryptocurrencies directly on exchange wallets carries a significant risk of loss for the user (Xia et al. 2020). A decentralized exchange (DEX) use smart contracts or other forms of peer-to-peer networks to execute exchange functionality and enable non-custodial cryptocurrency trading (Victor and Weintraud 2021). DEXs are implemented in two ways. Within a DEX that is based on a limit order book (e.g., EtherDelta), users trade with each other by placing buy and sell orders into the order book. The order books of a DEX can be managed on-chain as well as off-chain, although the actual settlement typically takes place on-chain. Within a DEX based on an automated market maker (e.g., PancakeSwap), users do not directly trade with each other but rather with a liquidity pool. The price of a coin or token is calculated using an exchange-specific pricing mechanism (Victor and Weintraud 2021). Because users do not send their funds to an exchange wallet, the DEX approach reduces the risk of theft via exchange hacking (Lin 2019). On the downside, DEXs carry a greater risk of market manipulation because there is no supervision and users do not have to verify themselves via a know your customer (KYC) process (Victor and Weintraud 2021).

In comparison to conventional financial assets, cryptocurrencies have experienced more price fluctuations and they face greater volatility and fluctuating liquidity. Recent studies have indicated that the price discovery process is affected not only by macroeconomic fundamentals such as supply and demand, or the

Preprint Version

intrinsic value of the underlying asset, but also by unconventional factors. These include news about national bans and regulations, exchange hacks (Lyócsa et al. 2020), and current hash rates (Bouoiyour and Selmi 2017). Furthermore, cryptocurrency markets have attracted many uninformed investors, who largely dominate those markets (Dyhrberg et al. 2018). Uninformed investors usually rely on noise and amplify the volatility of markets by participating in pump-and-dump schemes, herding effects and by buying assets based on the fear of missing out (Baur and Dimpfl 2018).

Market Manipulation

Market manipulation refers to trading strategies that are designed to reduce the economic efficiency of the market. They achieve this by reducing the liquidity of the market for risk transfer. In addition, they undermine the accuracy of price discovery by making prices less accurate as signals of efficient resource allocation (Kyle and Viswanathan 2008). Benefiting from insider information in trades, for example, reduces price efficiency and market liquidity because of information asymmetry.

The decentralized nature of cryptocurrencies and weak regulation of the blockchain ecosystem render cryptocurrency markets vulnerable to different kinds of fraud, scams, and market manipulation. Several papers have examined how cryptocurrencies have been affected by various scams and forms of fraud. Vasek and Moore (2015), for instance, provided the first empirical analysis of Bitcoin-based scams and an investigation of the advertisement of Ponzi schemes on bitclontalk.com (2019). Bartoletti et al. (2018) developed a model for predicting Ponzi schemes that involve cryptocurrencies. The researchers applied data-mining techniques to develop a classifier that effectively identifies Bitcoin addresses related to Ponzi schemes. The popularity and exposure of cryptocurrencies have prompted many studies on the applicability of specific market manipulation schemes to cryptocurrency markets. Researchers have investigated the effects of, among others, pump-and-dump schemes (Chen et al. 2019b; Hamrick et al. 2021; Mansourifar et al. 2020; Xu and Livshits 2019), wash trading (Aloosh and li 2019; Cong et al. 2020; Pennec et al. 2021), suspicious bot activity within the exchange of Mt. Gox (Gandal et al. 2018), and frontrunning (Bernhardt and Taub 2008; Daian et al. 2020) as forms of cryptocurrency market manipulation. Other forms of manipulation harness specific characteristics of the actual cryptocurrencies.

Methodology

This study follows the guidelines of Webster and Watson (2002) and vom Brocke et al. (2009) for conducting a systematic literature review (SLR) in the field of information systems. The SLR methodology consists of three sequential phases: *identification, screening* and *analysis*. The review focused on the identification of research outcomes, theories and applications by examining a representative sample of the literature of information systems, computer science and finance. By following a conceptual approach in its organization, the SLR integrates and systematizes past literature and identifies central issues from a neutral perspective. The results of the review are relevant for both specialist and general scholars of the field as well as practitioners who are interested in cryptocurrencies but lack extensive technical knowledge.

Identification Phase

A *keyword-centric* approach was adopted to gain comprehensive coverage of the existing blockchain and cryptocurrency literature. The following broad search string was developed:

((cryptocurrenc OR bitcoin OR blockchain OR altcoin OR "distributed ledger") AND ((price OR "order Book" OR market OR exchange OR coin OR volume) AND (manipulation OR fraud OR corruption)))*

The *selection of keywords* was based on an initial brief screening of important blockchain and cryptocurrency literature. The selection was then iteratively refined during the identification and search phase (Rowley and Slack 2004). By applying Boolean operators, the search string combines a wide variety of terminology commonly used in the field of cryptocurrencies (part one) with different pricing (part two) and manipulations terms (part three). Furthermore, multiple synonyms were included to ensure a robust search. To achieve representative coverage of relevant literature, a hybrid approach for the sources of the SLR was applied. This strategy covered both specific outlets and academic databases of multiple broad publication outlets; hence, it ensured the inclusion of relevant sources that may not be indexed by academic

Preprint version

databases. Because many academic databases only partially overlap in the scope and depth of the content covered, several such databases were used for the search (Bramer et al. 2017).

The *final database selection* included seven academic databases, based on the database screening conducted by Pearce (2018). The IEEE and ACM databases were included because of the in-depth focus on technological research topics. The EBSCOhost (Business Source Premier) and Emerald Insight databases were included because of their economic and social science focus; and Web of Science and Scopus were included because of their breadth of coverage of various research domains. Finally, the AIS database was included as it cover (among others) five of the leading conferences in information systems (IS).Because major contributions are likely to be published in the leading journals (Webster and Watson 2002), specific top-ranked outlets were also added to the basket of literature to search. Based on the JOURQUAL3 ranking (2015) for the research domain of IS and Finance, all outlets in the ranking categories A+ and A were included. To ensure adequate coverage of blockchain research, the study included six leading blockchain and cryptography outlets as well. Furthermore, three leading journals specializing in technical trends were added to the literature basket. The final basket of literature included 29 outlets and seven databases.

Search and Screening Phase

The second phase consisted of screening the identified literature by applying the search string to the selected outlets and databases. As the databases differ in their formats and indexing, minor adjustments were made to the specific search strings when necessary. The search was conducted between December 2020 and January 2021. Figure 1 illustrates the flow of the literature screening process. The initial keyword search, based on the predefined search terms and outlets, yielded 3,603 hits. After the removal of results not qualified as academic publications (e.g., editors' comments, editorials, book reviews, student theses, news) and duplicates, 2331 distinct hits remained. Subsequently, to check whether a hit fit the research scope, an initial screening of the title, abstract and keywords defined by the author or database was conducted. A total of 173 hits were identified that were eligible for a full text screening based on the four inclusive criteria described below.

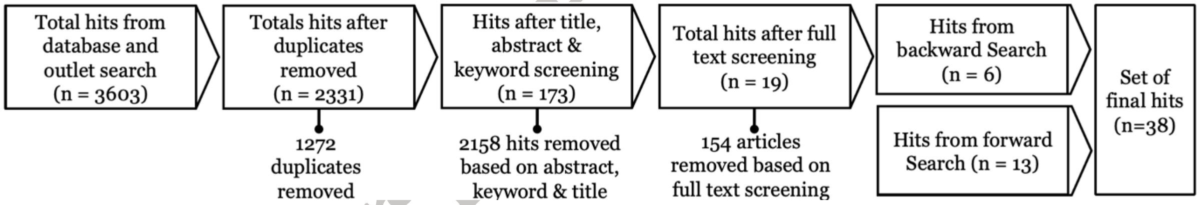
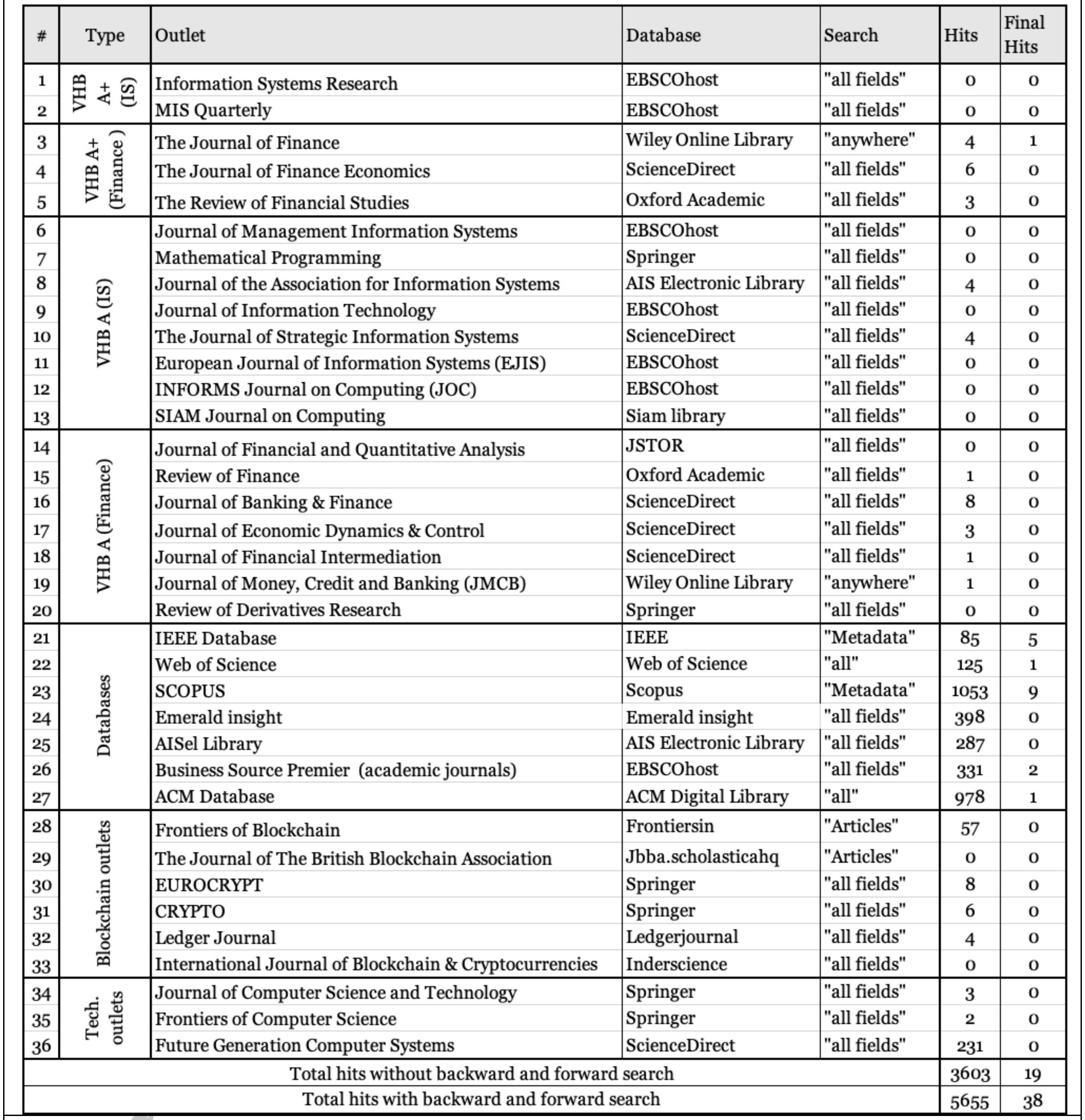

Total hits from database and outlet search (n = 3603)
Totals hits after duplicates removed (n = 2331)
1272 duplicates removed
Hits after title, abstract & keyword screening (n = 173)
2158 hits removed based on abstract, keyword & title
Total hits after full text screening (n = 19)
154 articles removed based on full text screening
Hits from backward Search (n = 6)
Hits from forward Search (n = 13)
Set of final hits (n=38)

Figure 1. Flow of the search process

First, eligible publications were required to focus in depth on the topic of price and/or market manipulation in cryptocurrencies. Second, they had to be original research contributions; third, they must be written in English. Finally, publications without a full list of references were excluded. No limitations were applied regarding the publication period. If a publication met all four criteria, it was accepted as a final hit and added to the dataset for further analysis.

To ensure a comprehensive screening of the field, a forward and backward search via Google Scholar was performed. The selection of additional final hits via this search was based on the same eligibility process and criteria as used for the keyword search. Frequent occurrences of pivotal concepts, citations and cross-references during the forward and backward search indicated that the review had reached a sufficient level of saturation (Boell and Cecez-Kecmanovic 2014; Leedy 2019). The final literature basket is summarized in Figure 2.

Preprint Version



#	Type	Outlet	Database	Search	Hits	Final Hits
1	VHB A+ (IS)	Information Systems Research	EBSCOhost	"all fields"	0	0
2		MIS Quarterly	EBSCOhost	"all fields"	0	0
3	VHB A+ (Finance)	The Journal of Finance	Wiley Online Library	"anywhere"	4	1
4		The Journal of Finance Economics	ScienceDirect	"all fields"	6	0
5		The Review of Financial Studies	Oxford Academic	"all fields"	3	0
6	VHB A (IS)	Journal of Management Information Systems	EBSCOhost	"all fields"	0	0
7		Mathematical Programming	Springer	"all fields"	0	0
8		Journal of the Association for Information Systems	AIS Electronic Library	"all fields"	4	0
9		Journal of Information Technology	EBSCOhost	"all fields"	0	0
10		The Journal of Strategic Information Systems	ScienceDirect	"all fields"	4	0
11		European Journal of Information Systems (EJIS)	EBSCOhost	"all fields"	0	0
12		INFORMS Journal on Computing (JOC)	EBSCOhost	"all fields"	0	0
13		SIAM Journal on Computing	Siam library	"all fields"	0	0
14	VHB A (Finance)	Journal of Financial and Quantitative Analysis	JSTOR	"all fields"	0	0
15		Review of Finance	Oxford Academic	"all fields"	1	0
16		Journal of Banking & Finance	ScienceDirect	"all fields"	8	0
17		Journal of Economic Dynamics & Control	ScienceDirect	"all fields"	3	0
18		Journal of Financial Intermediation	ScienceDirect	"all fields"	1	0
19		Journal of Money, Credit and Banking (JMCB)	Wiley Online Library	"anywhere"	1	0
20		Review of Derivatives Research	Springer	"all fields"	0	0
21	Databases	IEEE Database	IEEE	"Metadata"	85	5
22		Web of Science	Web of Science	"all"	125	1
23		SCOPUS	Scopus	"Metadata"	1053	9
24		Emerald insight	Emerald insight	"all fields"	398	0
25		AISel Library	AIS Electronic Library	"all fields"	287	0
26		Business Source Premier (academic journals)	EBSCOhost	"all fields"	331	2
27		ACM Database	ACM Digital Library	"all"	978	1
28	Blockchain outlets	Frontiers of Blockchain	Frontiersin	"Articles"	57	0
29		The Journal of The British Blockchain Association	Jbba.scholasticahq	"Articles"	0	0
30		EUROCRYPT	Springer	"all fields"	8	0
31		CRYPTO	Springer	"all fields"	6	0
32		Ledger Journal	Ledgerjournal	"all fields"	4	0
33		International Journal of Blockchain & Cryptocurrencies	Inderscience	"all fields"	0	0
34	Tech. outlets	Journal of Computer Science and Technology	Springer	"all fields"	3	0
35		Frontiers of Computer Science	Springer	"all fields"	2	0
36		Future Generation Computer Systems	ScienceDirect	"all fields"	231	0
Total hits without backward and forward search					3603	19
Total hits with backward and forward search					5655	38

Figure 2. Summary of the final literature basket

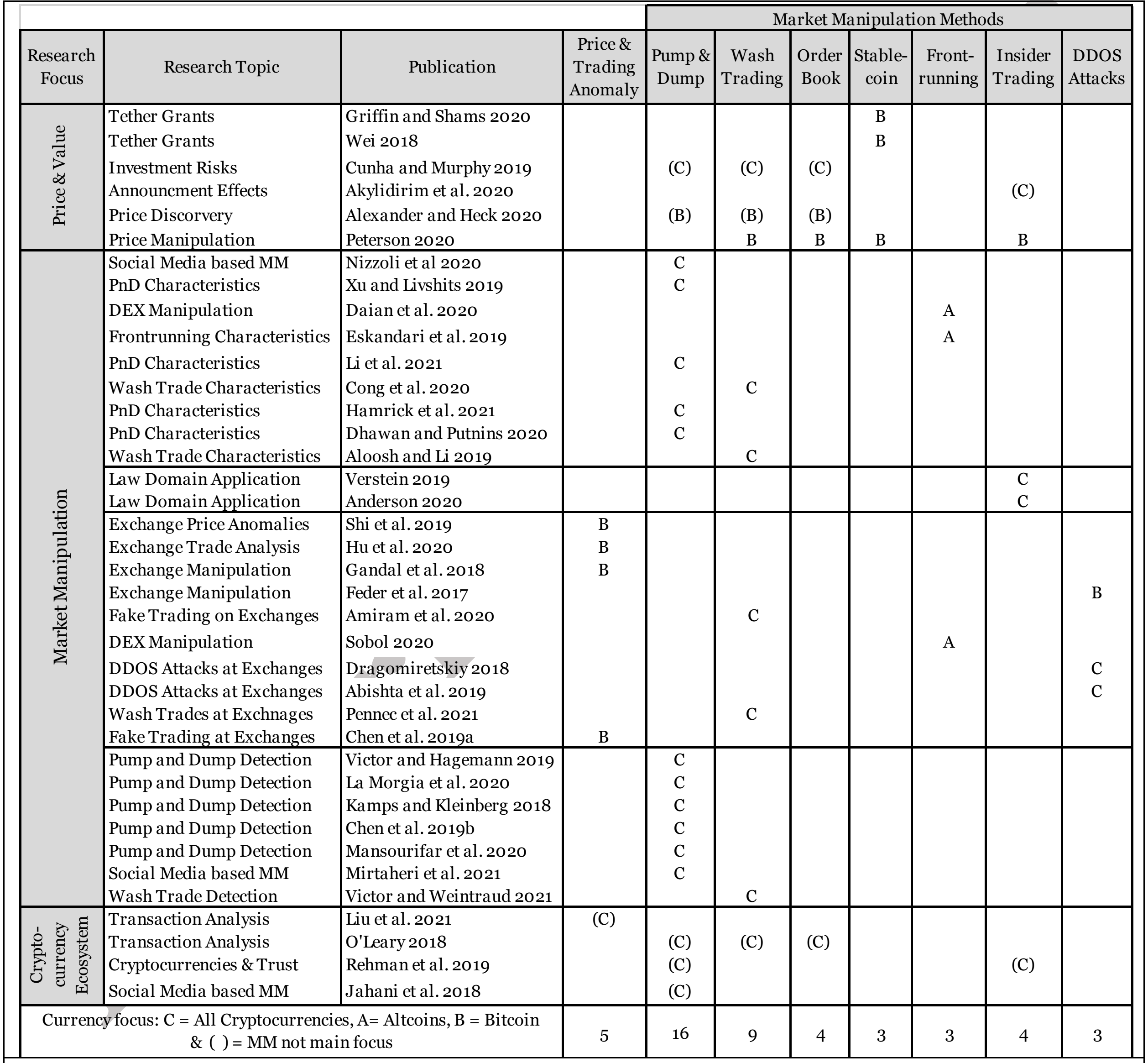
PI

Analysis Phase

Based on the 3,603 initial hits from the keyword search, 19 final hits were extracted from the literature basket. Moreover, during the screening of the 898 references and 1,154 citations, 19 additional final hits were found. Overall, the SLR led to 38 unique final hits. The final hits were then analyzed from a concept-centric perspective to extract the distinctive methods of market manipulation in cryptocurrency markets. The concept matrix covers the underlying market manipulation schemes, the research perspective and the investigated cryptocurrency or ecosystem of each identified publication. The process of analysis was iterative. The particular manipulation artifact characteristics, market vulnerabilities and potential countermeasures of each publication were extracted, analyzed and subsequently merged into distinctive classes of cryptocurrency market manipulation schemes, and market weaknesses. The approach followed the suggested coding strategies of Forman and Damschroder (2007) regarding qualitative content analysis.

Results

Figure 3 synthesizes the publications in a concept-centric matrix according to two dimensions. The market manipulation methods appear on the horizontal axis, and the research focus, and research topic of each publication appears on the vertical axis. Within the matrix, B indicates a focus on Bitcoin; A indicates a focus on altcoins, and C indicates a general emphasis on all cryptocurrencies. Brackets around letters indicate that the main focus of the paper is not on market manipulation.



				Market Manipulation Methods						
Research Focus	Research Topic	Publication	Price & Trading Anomaly	Pump & Dump	Wash Trading	Order Book	Stable-coin	Front-running	Insider Trading	DDOS Attacks
Price & Value	Tether Grants	Griffin and Shams 2020					B			
	Tether Grants	Wei 2018					B			
	Investment Risks	Cunha and Murphy 2019		(C)	(C)	(C)				
	Announcment Effects	Akylidirim et al. 2020							(C)	
	Price Discovery	Alexander and Heck 2020		(B)	(B)	(B)				
	Price Manipulation	Peterson 2020			B	B	B		B	
Market Manipulation	Social Media based MM	Nizzoli et al 2020		C						
	PnD Characteristics	Xu and Livshits 2019		C						
	DEX Manipulation	Daian et al. 2020						A		
	Frontrunning Characteristics	Eskandari et al. 2019						A		
	PnD Characteristics	Li et al. 2021		C						
	Wash Trade Characteristics	Cong et al. 2020			C					
	PnD Characteristics	Hamrick et al. 2021		C						
	PnD Characteristics	Dhawan and Putnins 2020		C						
	Wash Trade Characteristics	Aloosh and Li 2019			C					
	Law Domain Application	Verstein 2019							C	
	Law Domain Application	Anderson 2020							C	
	Exchange Price Anomalies	Shi et al. 2019	B							
	Exchange Trade Analysis	Hu et al. 2020	B							
	Exchange Manipulation	Gandal et al. 2018	B							
	Exchange Manipulation	Feder et al. 2017								B
	Fake Trading on Exchanges	Amiram et al. 2020			C					
	DEX Manipulation	Sobol 2020						A		
	DDOS Attacks at Exchanges	Dragomiretskiy 2018								C
	DDOS Attacks at Exchanges	Abishta et al. 2019								C
	Wash Trades at Exchnages	Pennec et al. 2021			C					
	Fake Trading at Exchanges	Chen et al. 2019a	B							
	Pump and Dump Detection	Victor and Hagemann 2019		C						
	Pump and Dump Detection	La Morgia et al. 2020		C						
	Pump and Dump Detection	Kamps and Kleinberg 2018		C						
	Pump and Dump Detection	Chen et al. 2019b		C						
	Pump and Dump Detection	Mansourifar et al. 2020		C						
	Social Media based MM	Mirtaheri et al. 2021		C						
	Wash Trade Detection	Victor and Weintraud 2021			C					
Crypto-currency Ecosystem	Transaction Analysis	Liu et al. 2021	(C)							
	Transaction Analysis	O'Leary 2018		(C)	(C)	(C)				
	Cryptocurrencies & Trust	Rehman et al. 2019		(C)					(C)	
	Social Media based MM	Jahani et al. 2018		(C)						
Currency focus: C = All Cryptocurrencies, A= Altcoins, B = Bitcoin & ( ) = MM not main focus			5	16	9	4	3	3	4	3

Figure 3. Concept matrix of the manipulation methods within cryptocurrency markets

The analysis of the literature resulted in the identification of seven main market manipulation methods within cryptocurrency markets. Furthermore, five publications were identified that investigated price manipulation but could not directly be assigned to a specific market manipulation method. These publications are listed in the *Price and Trade Anomaly* column of Figure 3. They included, for example, an analysis of suspicious trading behavior via bots on the Mt. Gox exchange (Gandal et al. 2018) or the investigation of anomalies in Bitcoin price returns (Shi et al. 2019).

In addition to the seven manipulation methods, three distinct research foci are evident in the concept matrix. Articles in the first category concern cryptocurrency price dynamics and how market valuations are affected by market manipulation schemes. For example, Alexander and Heck (2020) investigated the effects of unregulated markets on cryptocurrency price dynamics. Publications in the second category focus on market manipulation methods and can be divided in four subcategories. The first subcategory concerns the general prevalence and analysis of specific manipulation characteristics. Publications in the second subcategory deal with topics of a legal nature. For example, Verstein et al. (2019) investigated whether insider trading laws apply to cryptocurrencies. Publications in the third subcategory focus on market manipulation methods, with an emphasis on the impact on, and role of, cryptocurrency exchanges. Publications in the fourth subcategory investigate different methods and technologies for detecting and identifying market manipulation methods in cryptocurrencies. The last of the three main categories focuses on the cryptocurrency ecosystem and how market manipulation affects it. The subsequent adoption of cryptocurrencies is also studied.

Methods of Market Manipulation in Cryptocurrency Markets

Within the analyzed literature, pump-and-dump schemes have received the most research attention, with 17 publications reporting on this form of manipulation. In contrast, manipulation via stablecoins has received much less attention, with only three publications reporting on this type of manipulation. In the section that follows, research on each of these methods and their functionality is briefly summarized. Table 1 lists the key characteristics of the seven market manipulation methods identified, classified by the overall manipulation type according to the scheme of Allen and Gale (1992). Furthermore, the study summarizes differences within the market manipulation methods to traditional financial markets.

	Pump & dump	Wash trading	Order book	Front-running	Insider trading	DDoS attacks	Stable-coins
Type	Information	Trade	Trade	Trade	Trade	N/A	N/A
Difference to trad. Financial Markets	Orga-nization, Implemen-tation	Anonymity within Exchanges and Order Books	Anonymity within Exchanges and Order Books	Exploitation of Blockchain Infra-structure	Usually target Coin-listings and Announce-ments	Similar to trad. Financial Markets	N/A to trad. Markets
Target Domain	CEX & DEX ICO	CEX & DEX	CEX & DEX	DEX ICO	CEX & DEX	CEX & DEX	CEX & DEX
Effect/ Goal	Price Distortion	Volume Inflation	Volume Inflation	Market Advantages	Market Advantages	Exchange Exploits	Price Distortion
Manipula-tion Focus	Low Market cap Coins	Order Books	Un-regulated Exchanges	Un-confirmed Transactions	Un-regulated-Exchanges	Technical exploits	Un-regulated Exchanges
Bot-Activity	Yes	Yes	Yes	Yes	Yes	Yes	N/A
Observed Types / Attacks	Sustained Pumps Short-Term PnDs	Self-Trades Wash trades	N/A	Displacemen t Attack Insertion Attack Suppression Attack	Exchange Insider Blockchain Insider	DDOS DOS	N/A

Table 1. Summary of market manipulation methods

Pump-and-dump schemes (PnD) are a market manipulation strategy in which the price of a previously acquired asset is artificially inflated and followed by sell-off to other investors (Kamps and Kleinberg 2018).

Preprint Version

By promoting and spreading misleading information, the operator of the PnD scheme tries to convince other investors to buy the promoted assets and therefore boosts the price; this is the “pump” aspect. As other investors start to believe the rumor, the operator of the scheme starts to sell the inflated asset, leaving the investors at a loss; this is the “dump” aspect.

Market manipulation via PnD schemes is a well-known phenomenon. It was mainly observed within microcap or so-called “penny” stocks (Aggarwal and Wu 2006; Leuz et al. 2017). Although PnD schemes based on real-time misinformation have been observed within cryptocurrency markets, cf. McAfee Twitter Hack (Shome 2017), a different variation has been established. In contrast to traditional financial markets, cryptocurrencies PnD schemes are mainly achieved and organized via so-called pump groups, whose sole goal consists of driving up the price of a coin through coordinated buys. These schemes have been almost exclusively organized via social media and platforms like Twitter, Reddit, Telegram and Discord. Telegram in particular is preferred by PnD groups due to the high level of anonymity within the app (Mirtaheri et al. 2021). Pump groups are organized with a distinct hierarchy and usually consist of three main actors: the *pump organizer, pump participants* and *pump target exchanges* (Xu and Livshits 2019). The pump organizer announces the next target and communicates various buy signals to the members. High-ranking members benefit from early information, such as target exchange, target coin or target pump price, and therefore have the opportunity to buy at a relatively low price and dump with a profit. Apart from the purchase of coins and tokens by the members of the pump group, organizers of PnD schemes speculate that other investors will be attracted by the sudden price increase and also invest in the coin. The promotion of cryptocurrency PnD is strongly affected by botnets operating on Twitter and Discord. Nizzoli et al. (2020) reported that pump-and-dump channels were mainly endorsed by star structure Twitter botnets. Within their dataset, they identified that 15 Twitter accounts were responsible for 75.4% of all invitation links. Compared to traditional markets, pump-and-dump schemes in cryptocurrency markets are rather short-lived. Martineau (2018) reported on two events that reached their peaks within 5–10 minutes, whereas a pump in traditional markets usually occurs over several days or weeks (Kamps and Kleinberg 2018). Furthermore, multiple studies have indicated that pump-and-dump groups usually target less popular coins with relatively low market caps and low coin circulation (La Morgia et al. 2020; Victor and Weintraud 2021). In addition, because of arbitrage bots, it is possible that the price pump of a coin spills over to another exchange (La Morgia et al. 2020). According to a report of the Wall Street Journal (Shifflet 2018), which investigated the trading activities of pump-and-dump groups over a period of 6 months, $825 million in trading volume was linked to cryptocurrency PnD schemes.

Wash trading describes a manipulation technique wherein an entity creates artificial trading volume by executing trades against itself (Pennec et al. 2021). For example, a trader places a sell order on an exchange and buys the same sell order, which results in a false impression of liquidity (Cunha and Murphy 2019). In comparison to traditional financial markets, wash trading is made possible due to the anonymity within exchanges, especially within DEXs. Cong et al. (2020) examined Benford’s law, a statistical benchmark to detect fraud in macroeconomics; based on this law, 70% of the volume traded on non-regulated exchanges was highly suspicious and probably fake. Pennec et al. (2021) analyzed token balances, web traffic, and exchange volume and found similar magnitudes of suspicious trading volume. Gandal et al. (2018) indicated that trading volume before the collapse of the Mt. Gox exchange was highly manipulated by two trading bots. Similar activities could be observed on DEXs. Victor and Weintraud (2021) identified that on the decentralized exchanges IDEX and EtherDelta, more the 30% of all traded tokens had been subject to wash trading activities. Furthermore, they identified that a small group of accounts were responsible for a wash trading volume of $159 million.

Two types of **manipulation based on order books** were noted in the cryptocurrency literature, namely o*rder spoofing* and q*uote stuffing*. *Both* types are already known from the traditional markets and are generally regarded as illegal. Spoofing describes a form of order book manipulation in which a trader places buy or sell orders into the order book, but without the intention of actually executing them (Cartea et al. 2019). To drive the market in a certain direction, a trader places a huge number of orders on one side of the order book, implying buy/sell pressure. Typically, bots and algorithms are used to manipulate the perception of supply and demand for a certain coin, in the favor of the spoof trader (O'Leary 2018). In the case of cryptocurrencies, multiple reports indicate that the rise in the price of Bitcoin in 2017 was the result of a large-scale spoofing of the market, orchestrated by a single entity dubbed “Spoofy” (Bitfinex’ed 2017; O'Leary 2018). Examination of the order book of the exchange Bitfinex revealed that one entity repeatedly placed large buy orders (upward of $2 million), with those orders having a lifetime of around 5–10 seconds

Preprint Version

(Bitfinex'ed 2017). Quote stuffing is a manipulation technique known from high frequency trading, in which order congestion is generated by placing a vast number of orders into the order book, followed by immediate cancellation of those orders (Dalko and Wang 2020). Quote stuffing creates a false mid-price, which is the average of the current best bid and the ask price; it can create false signals regarding rising or falling prices (Twomey and Mann 2020). Similar to spoofing, the same report claimed that quote stuffing occurred on Bitfinex (Bitfinex'ed 2017). In comparison to traditional financial markets, both methods benefit in their implementation from the anonymity within most cryptocurrency exchanges due to missing know your customer processes and regulations.

Frontrunning is based on the problem of information asymmetry, with agents in the market having different information at different times (Sobol 2020). This method describes how an entity can benefit from early access to market information, such as an upcoming trade or transaction, because of a privileged position such as being a broker (Bernhardt and Taub 2008). An example in traditional financial markets would be a stockbroker who "front-runs" their own client by ordering stocks for themselves before executing the client's order for the same stock. In cryptocurrency markets, the frontrunning problem manifests mainly in Ethereum-based decentralized applications (Eskandari et al. 2019). It is made possible by the transaction transparency of the blockchain and the smart contract design. Within the Ethereum blockchain, the user pays a small sum in the form of *gas* – which is a pseudo currency representing the computational steps of a confirmation – to a miner for confirming a transaction. As miners tend to maximize profits, every market actor who monitors unconfirmed transactions (e.g. by running a full node) can potentially front-run unconfirmed transactions by sending an adaptive transaction with a higher amount of *gas* (Daian et al. 2020). The DEXs based on limit order books (Eskandari et al. 2019) or automated marked making mechanisms (Sobol 2020) are especially prone to frontrunning. Furthermore, increased frontrunning activity was observed in the 2017 initial coin offering boom, as many users wanted to invest early in blockchain companies with limited token supplies. Eskandari et al. (2019) analyzed the ICO of *Status.Im* and found evidence of abnormal mining behavior of mining pools, indicating potential token front-runs.

Insider trading refers to the abusive usage of insider information that might predict future transactions for trading strategies; this issue can be observed in all financial markets (Anderson 2020; Verstein 2019). Regarding cryptocurrencies, dishonest market participants benefit from the fact that blockchain technologies provide substantial autonomy and that cryptocurrency markets and many exchanges are widely unregulated (Rehman et al. 2020).In comparison to traditional financial markets, insider trading in cryptocurrencies mainly occurs in the context of coin listings of exchanges and can result in sudden price movements, such as the price spike of Bitcoin Cash before its listing on Coinbase (Rehman et al. 2020; Wilmoth 2017). Exchange employees can profit from insider knowledge of future coin listings or delisting's on exchanges. This gives them the opportunity to open trading positions early (Rehman et al. 2020).

A **distributed denial-of-service (DDoS)** attack refers to an attempt to disable the service provided by a website or network by repeatedly sending a high volume of service requests. Compared to simple denial-of-service attacks, DDoS attacks are carried out by several different sources, usually by a remotely controlled botnet (Mirkovic and Reiher 2004). A DDoS attack leads to serious performance loss in crypto exchanges, and in a worst-case scenario to a temporary unavailability of the exchange. In combination with different order setups on a cryptocurrency exchange, DDoS attacks can be used as a lucrative market manipulation instrument (Feder et al. 2017). For example, in combination with a sell order, the initiated denial-of-service can be exploited to freeze trading within an exchange and utilize the existing volume to depress the price of a targeted cryptocurrency. This enables accumulating a large number of coins at a lower price. In the past, multiple cryptocurrency exchanges, such as Bitfinex or OKEx, have been the target of DDoS attacks (O'Neal 2020). Feder et al. (2017) investigated the impact of DDoS attacks on cryptocurrency exchanges and found that the number of large trades on the Mt. Gox exchange fell sharply after each one. Abhishta et al. (2019) reached similar conclusions. In 17 reviewed cases, DDoS attacks lead to significant decrease in volume. However, the negative impact on the traded volume usually recovered within a day.

Stablecoins are cryptocurrencies whose price is controlled by an active or automatic monetary policy. The aim is price stability in relation to a national currency, a basket of currencies or other assets (Mita et al. 2019). Tether, for example, is a stablecoin that is anchored to the value of one U.S. dollar (Tether ltd. 2021). Stablecoins – and especially Tether – play an important role in cryptocurrency exchanges. They allow dollar-like transactions and pricing of cryptocurrencies, in USD, without having to set up USD bank accounts, which most exchanges struggle with (Griffin and Shams 2020; Wei 2018). In the past, multiple

Preprint Version

reports – such as the anonymous Tether Report (2018) – have claimed that Tether grants are related to the inflation of the Bitcoin price. Furthermore, while Tether Ltd. claims that every Tether coin is backed by a reserve, multiple reports express skepticism about such reserves. Recent research indicates suspicious trading behavior in the context of stablecoins, which might play an important role regarding the manipulation of cryptocurrency markets. Griffin and Shams (2020) identified that one entity directly associated with the exchange Bitfinex was involved in suspicious Tether trades. Based on the mapping of the Bitcoin and Tether blockchain and in-depth algorithmic analysis, they found that vast amounts of Tether were used to buy Bitcoin when the Bitcoin value was falling; this was followed by new Tether grants. However, Wei (2018) found not statistical evidence that the so-called "printing" of Tether directly affected Bitcoin returns positively. Rather, Wei identified short-term increases in Bitcoin and Tether volumes. Wei's findings were confirmed by Griffin and Shams (2020), who found that during the 2017 Bitcoin rally, negative Bitcoin returns preceded new Tether grants.

Discussion

To avoid overregulation, it is important to understand why markets are subject to manipulation. This section discusses the identified market manipulation methods in light of possible market vulnerabilities and how those vulnerabilities influence the success of each method. All identified publications were published in 2017 or later. Furthermore, only one hit (out of 38) was assigned to outlets rated as A+ and A, which indicates that the research field is still in an early or emerging phase. Figure 4 illustrates the temporal distribution of the literature basket.

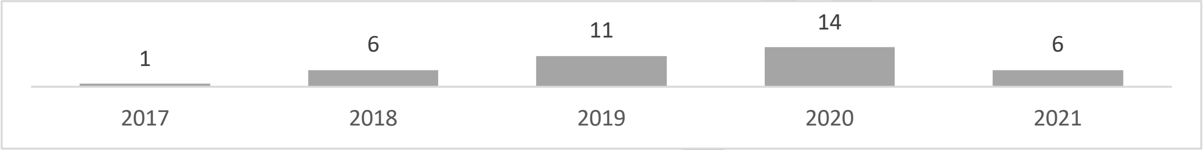


Figure 4. Publications by year

Among the publications, a trend was observed with regard to research on pump-and-dump schemes and the role of social media. Considerably less research has been conducted on the other manipulation methods. For example, only three papers were identified that investigated manipulation attempts via stablecoins. There are several explanations for this discrepancy. First, the possibility of acquiring suitable data varies greatly among the different manipulation methods. For example, publicly available candlestick data can be used in combination with social media data to identify pump and dumps retrospectively (Mirtaheri et al. 2021). By contrast, for wash trading, detailed information about individual trades and parties are required. Since central exchanges usually perform trades off-chain and clients are protected for privacy reasons, such data are not easily available. Second, considering the cryptocurrency focus of the individual publications, it was evident that most research has focused on the broad perspective of cryptocurrencies or in detail on Bitcoin. Few studies have examined specific altcoins.

The analysis of the 38 studies and the seven identified market manipulation methods led to the identification of six potential market vulnerabilities. These vulnerabilities could have a significant impact on the success of market manipulation methods within cryptocurrencies. The work of Twomey and Mann (2020) was used as the basis for identifying market weaknesses and vulnerabilities, supplemented by the results from the analyzed papers. Table 2 summarizes the market vulnerabilities identified and how they affect the success of a specific market manipulation method.

As Table 2 illustrates, the occurrence of market manipulation within cryptocurrency markets cannot be attributed to only one weakness or vulnerability. Instead, there is an interplay of various market components, regulations, and technological conditions. The success of a manipulative method is linked to several factors; these include differences in exchange standards and sophistication, anonymity across the cryptocurrency ecosystem, absence of market regulation, low market barriers, inexperienced investors, exploitation of social media, and design vulnerabilities and exploits in the blockchain ecosystem and consensus protocols. Cryptocurrency exchanges, in particular, are the focus of manipulation. The absence of standards as well as the variance in functionality and maturity of the individual exchanges positively

Preprint Version

influence the success of all seven manipulation methods. In contrast to traditional exchanges, cryptocurrency exchanges do not require a license; depending on the country, there might be no regulations regarding their establishment and operation. These features can result in technical vulnerabilities, which can lead to exploitation points for DDoS attacks (Twomey and Mann 2020).

Market Manipulation Methods	Market Vulnerabilities					
	Exchange Standards & Sophistication	Anonymity	Market Regulation	Market Barriers & Inexperienced Investors	Social Media	Blockchain Design & Ecosystem
Pump & Dump	✓	✓	✓	✓	✓	
Wash Trading	✓	✓	✓	✓		
Frontrunning	✓	✓	✓	✓		✓
Order Book	✓	✓	✓	✓		
Insider Trading	✓	✓	✓	✓		
DDOS	✓	✓	✓			
Stablecoin	✓	✓	✓			✓

Table 2. Market vulnerabilities on market manipulation methods

In addition to being the target of manipulation techniques, cryptocurrency exchanges can play a more active role in market manipulation. Multiple studies have indicated that exchanges have been actively involved in wash trades and the artificial inflation of volume (Aloosh and li 2019; Gandal et al. 2018). As high volume attracts new potential traders, exchanges benefit in the short run from wash trades (Amiram et al. 2020). The identification of previous wash trades with zero fees points to the potential involvement of exchanges in this form of manipulation (Aloosh and li 2019; Victor and Weintraud 2021). Current research has not identified a clear role played by exchanges in pump-and-dump schemes and wash trades; however, during pump and dumps, exchanges do profit from higher transaction fees due to the higher trading volume (Xu and Livshits 2019). For example, the exchange *Yobit* was actively involved in promoting and participating in pump and dumps on its own exchange (Canellis 2018).

In addition to these effects, there remains a large difference in terms of user anonymity among different exchanges. As the OAG Report (2018) indicates, KYC processes between exchanges vary widely, with some exchanges not requiring any form of government ID or address. The lack of KYC processes makes it difficult to identify the entity behind suspicious accounts and permanently ban them from exchanges. Furthermore, this allows for the misuse of insider information by insiders within exchanges or blockchain companies (Sam 2019). In the case of DEXs, KYC processes are usually completely absent. A wallet address and a smart contract that links to the DEX is usually sufficient to transact. In addition to wash trades that are realized with several wallets, it is possible to observe so-called self-trades. Here, the trader fills their own orders (Victor and Weintraud 2021).

Despite the apparent role of exchanges in market manipulation, it is too simplistic to argue that exchanges are the root cause of all cryptocurrency market manipulation. A study by Mirtaheri et al. (2021) shows that social media play an important role in the organization and execution of cryptocurrency market manipulation. Inexperienced traders are persuaded via social media platforms to invest in a coin or join a pump-and-dump group, with the promise of quick profits. Through fear of missing out on profits, investors often neglect to conduct their own due diligence (Kamps and Kleinberg 2018). In addition, within cryptocurrency markets, any person – regardless of their experience – can sign up to an exchange for free. In this context, inexperienced users are relatively likely to fall for manipulations in the order book; they may believe in faked volumes or in buy and sell walls created by order spoofing (Twomey and Mann 2020). Manipulations can also be traced back to the actual vulnerabilities in the blockchain technologies and the consensus protocols. Daian et al. (2020) identified concrete differences in the consensus security layer

Preprint Version

model for simple payments and for smart contracts. For example, the concept of the gas option and higher fees for priority transactions within the Ethereum blockchain can be exploited to front-run other transactions.

Research Agenda

The literature from the fields of computer science, finance and business informatics provide first promising results. However, considering the publication period of the literature basket, it becomes clear that the research field is still at an early stage. Based on the analyzed literature basket, three main challenges can be identified: too narrow scope, variance in data quality and missing implications & solutions. Most of the identified papers within the literature basket concentrate on a single cryptocurrency or the isolated analyzation of a market manipulation method. A too narrow research scope can lead to a lack of study comparability. Furthermore, a too narrow scope can lead to neglecting the bigger picture and less implications for the whole market. Second, the publications studied showed wide differences in the quality of the data and the sophistication of the research design. This is mainly due to the fact that exchange data is relatively difficult to obtain and usually expensive. Finally, within the literature basket, it was identified that while market manipulations methods are analyzed in-depth, a lot of papers miss possible solutions to the underlying problems. This can lead to the risk that only the phenomenon itself is studied, but not the underlying issue or causing factors. Table 3 summarizes the identified challenges and issues. Furthermore, based on the identified challenges, research recommendations for future research directions are provided.

Main Challenges	Issues	Research Recommendations
Scope	Narrow focus on the effect of specific market manipulation methods/ specific cryptocurrencies	In-depth comparison of market manipulation methods with traditional financial markets and cryptocurrency markets Investigation of the impact of different market manipulation methods on the cryptocurrency market Cross-sectional analysis of existing regulations and exchange sophistication
Data Quality	Multiple studies rely on the same leaked data set of Mt. Gox	Collection of different data from multiple currencies and exchanges Reduction of paywalls and improvement of data accessibility for academic research
	Great variation of data richness and quality	
Implications & Solutions	Only a few papers list implications and address sustainable solutions for the manipulation methods	Analysis of existing countermeasures and regulations within traditional financial markets and to what extent they are applicable to cryptocurrency markets Investigation of flaws and exploits within consensus algorithms and the Blockchain infrastructure, especially within the *gas* wars of Ethereum Vulnerability analysis of decentralized exchanges

Table 3. Main challenges, issues and recommendations based on the literature basket

Preprint Version

Conclusion

This paper provides a comprehensive overview of the academic literature on cryptocurrency market manipulations. The SLR revealed seven market manipulation methods in cryptocurrency markets and three areas of focus for research. Furthermore, the SLR indicated six drivers of the success of market manipulation schemes. The review also indicated that six of the seven identified manipulation methods are already known from traditional markets. Furthermore, this study demonstrates that exchanges play a central role in market manipulation due to the lack of regulation and standardized KYC procedures. Based on the identified market vulnerabilities, this paper offers a starting point for developing regulation approaches based on the scientific literature.

Although the review was systematic, and a comprehensive design was adopted for analyzing the literature, this work has certain limitations. First, the inclusion of multiple databases, conferences, and specific outlets relevant to blockchain and cryptocurrency was aimed at achieving a representative sample; however, the basket of literature was not exhaustive and potentially missed important works. Second, the selection of final hits and the extraction of the results was not entirely objective. Although the selection was based on a well-defined procedure and specific inclusion criteria, an element of subjectivity remained. Third, a key limitation of the review relates to the quality and relevance of the literature. Academic investigations inevitably lag behind market operations. Hence, it is possible that several earlier – but potentially ongoing – market manipulation techniques have not yet received academic attention. If that is the case, they would not be included in this synthesis.

Preprint Version

References

Abhishta, A., Joosten, R., Dragomiretskiy, S., and Nieuwenhuis, L. 2019. "Impact of Successful Ddos Attacks on a Major Crypto-Currency Exchange," *27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing 2019*, Pavia, Italy: IEEE, pp. 379-384.

Aggarwal, R., and Wu, G. 2006. "Stock Market Manipulations," *The Journal of Business* (79:4), pp. 1915-1954.

Akyildirim, E., Corbet, S., Cumming, D., Lucey, B., and Sensoy, A. 2020. "Riding the Wave of Crypto-Exuberance: The Potential Misusage of Corporate Blockchain Announcements," *Technological Forecasting and Social Change* (159).

Alexander, C., and Heck, D. F. 2020. "Price Discovery in Bitcoin: The Impact of Unregulated Markets," *Journal of Financial Stability* (50).

Allen, F., and Gale, D. 1992. "Stock-Price Manipulation," *Review of Financial Studies* (5:3), pp. 503-529.

Aloosh, A., and li, J. 2019. "Direct Evidence of Bitcoin Wash Trading*," *SSRN Electronic Journal* (doi: 10.2139/ssrn.3362153).

Amiram, D., Lyandres, E., and Rabetti, D. 2020. "Competition and Product Quality: Fake Trading on Crypto Exchanges," *SSRN Electronic Journal* (doi: 10.2139/ssrn.3745617).

Anderson, J. P. 2020. "Insider Trading and Cryptoassets: The Waters Just Got Muddier," *SSRN Electronic Journal* (doi: 10.2139/ssrn.3674018).

Anonymous. 2018. "The Tether Report " Retrieved 04.04.2021, from http://www.tetherreport.com

Back, A. 2002. "Hashcash - a Denial of Service Counter-Measure."

Bartoletti, M., Pes, B., and Serusi, S. 2018. "Data Mining for Detecting Bitcoin Ponzi Schemes," *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, Zurich, Switzerland: IEEE, pp. 75-84.

Baur, D., and Dimpfl, T. 2018. "Asymmetric Volatility in Cryptocurrencies," *Economics Letters* (173), pp. 148-151.

Bernhardt, D., and Taub, B. 2008. "Front-Running Dynamics," *Journal of Economic Theory* (138:1), pp. 288-296.

Bitfinex'ed. 2017. "Meet 'Spoofy'. How a Single Entity Dominates the Price of Bitcoin." Retrieved 02.04.2020, from https://tinyurl.com/f95hwt6x

Boell, S., and Cecez-Kecmanovic, D. 2014. "A Hermeneutic Approach for Conducting Literature Reviews and Literature Searches," *Communications of the Association for information Systems* (34), p. 12.

Bouoiyour, J., and Selmi, R. 2017. "The Bitcoin Price Formation: Beyond the Fundamental Sources," in: *ArXiv: 1707.01284*.

Bramer, W. M., Rethlefsen, M. L., Kleijnen, J., and Franco, O. H. 2017. "Optimal Database Combinations for Literature Searches in Systematic Reviews: A Prospective Exploratory Study," *Systematic Reviews* (6:1), p. 245.

Canellis, D. 2018. "Cryptocurrency Exchange Orchestrates Shameless 'Pump & Dump' Scheme." Retrieved 09.04.2021, from https://thenextweb.com/news/cryptocurrency-exchange-pump-dump

Cartea, A., Jaimungal, S., and Wang, Y. 2019. "Spoofing and Price Manipulation in Order Driven Markets," *Applied Mathematical Finance* (27:1-2), pp. 67-98.

Chen, W., Wu, J., Zheng, Z., Chen, C., and Zhou, Y. 2019a. "Market Manipulation of Bitcoin: Evidence from Mining the Mt. Gox Transaction Network," *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*, Paris, France: IEEE, pp. 964-972.

Chen, W., Xu, Y., Zheng, Z., Zhou, Y., Yang, E. J., and Bian, J. 2019b. "Detecting "Pump & Dump Schemes" on Cryptocurrency Market Using an Improved Apriori Algorithm," *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*, SF, CA, USA: IEEE, pp. 293-2935.

Chohan, U. W. 2017a. "Cryptocurrencies: A Brief Thematic Review," *SSRN Electronic Journal* (doi: 10.2139/ssrn.3024330).

Chohan, U. W. 2017b. "The Double Spending Problem and Cryptocurrencies," *SSRN Electronic Journal* (doi: 10.2139/ssrn.3090174).

CoinMarketCap. 2021. "Prices by Market Cap." Retrieved 20.04.2021, from https://coinmarketcap.com

Cong, L., Li, X., Tang, K., and Yang, Y. 2020. "Crypto Wash Trading," *SSRN Electronic Journal* (doi: 10.2139/ssrn.3530220).

Cunha, J., and Murphy, C. 2019. "Are Cryptocurrencies a Good Investment?," *The Journal of Investing* (28:3), pp. 45-56.

Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., and Juels, A. 2020. "Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability," *2020 IEEE Symposium on Security and Privacy (SP)*, Virtual IEEE, pp. 910-927.

Dalko, V., and Wang, M. H. 2020. "High-Frequency Trading: Order-Based Innovation or Manipulation?," *Journal of Banking Regulation* (21), pp. 289-298.

Dhawan, A., and Putnins, T. J. 2020. "A New Wolf in Town? Pump-and-Dump Manipulation in Cryptocurrency Markets," *SSRN Electronic Journal* (doi: 10.2139/ssrn.3670714).

Dragomiretskiy, S. 2018. "The Influence of Ddos Attacks on Cryptocurrency Exchanges." Retrieved 04.04.2021, from http://essay.utwente.nl/76402/1/Dragomiretskiy_BA_BMS.pdf

Dyhrberg, A. H., Foley, S. M., and Svec, J. 2018. "How Investible Is Bitcoin? Analyzing the Liquidity and Transaction Costs of Bitcoin Markets," *Economics Letters* (171), pp. 140-143.

Eskandari, S., Moosavi, S., and Clark, J. 2019. "Sok: Transparent Dishonesty: Front-Running Attacks on Blockchain," *Financial Cryptography and Data Security,* A. Bracciali, J. Clark, F. Pintore, P.B. Rønne and M. Sala (eds.), Kota Kinabalu, Malaysia: Springer International Publishing, pp. 170-189.

European-Central-Bank. 2015. "Virtual Currency Schemes – a Further Analysis." *Eurosystem* Retrieved 01.04.2021, from https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

Feder, A., Gandal, N., Hamrick, J., and Moore, T. 2017. "The Impact of Ddos and Other Security Shocks on Bitcoin Currency Exchanges: Evidence from Mt. Gox," *Journal of Cybersecuroty* (3:2), pp. 137-144.

Felix, T., and von Eije, H. 2018. "Underpricing in the Cryptocurrency World: Evidence from Initial Coin Offerings," *Managerial Finance* (45:4), pp. 563-578.

Forman, J., and L., D. 2007. "Qualitative Content Analysis," in *Empirical Methods for Bioethics : A Primer* L. Jacoby and L. Siminoff (eds.). Bingley, England: Emeral Group Publishing limited, pp. 39-62.

Gandal, N., Hamrick, J. T., Moore, T., and Oberman, T. 2018. "Price Manipulation in the Bitcoin Ecosystem," *Journal of Monetary Economics* (95), pp. 86-96.

Gomber, P., Kauffman, R., Parker, C., and Weber, B. 2018. "On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services," *Journal of Management Information Systems* (35:1), pp. 220 - 265.

Griffin, J. M., and Shams, A. 2020. "Is Bitcoin Really Untethered?," *The Journal of Finance* (75:4), pp. 1913-1964.

Hamrick, J., Rouhi, F., Mukherjee, A., Feder, A., Gandal, N., Moore, T., and Vasek, M. 2021. "An Examination of the Cryptocurrency Pump and Dump Ecosystem," *Information Processing & Management* (58:4).

Hu, B., Hwang, J. H., Jain, C., and Washam, J. 2020. "Bitcoin Price Manipulation: Evidence from Intraday Orders and Trades," *Applied Economics Letters* (Routledge), pp. 1-5.

Jahani, E., Krafft, P. M., Suhara, Y., Moro, E., and Pentland, A. S. 2018. "Scamcoins, S*** Posters, and the Search for the Next Bitcoin," *Proceedings of the ACM on Human-Computer Interaction* (2:CSCW), pp. 1-28.

Kamps, J., and Kleinberg, B. 2018. "To the Moon: Defining and Detecting Cryptocurrency Pump-and-Dumps," *Crime Science* (7:1).

Kyle, A., and Viswanathan, S. 2008. "How to Define Illegal Price Manipulation," *The American Economic Review* (98:2), pp. 274-279.

Preprint Version

La Morgia, M., Mei, A., Sassi, F., and Stefa, J. 2020. "Pump and Dumps in the Bitcoin Era: Real Time Detection of Cryptocurrency Market Manipulations," *2020 29th International Conference on Computer Communications and Networks (ICCCN)*, Honolulu, HI, USA, pp. 1-9.

Ledger. 2019. "What Is the Difference between Coins and Tokens?" Retrieved 06.04.2021, from https://www.ledger.com/academy/crypto/what-is-the-difference-between-coins-and-tokens

Leedy, P. D. 2019. *Practical Research: Planning and Design*, (12 ed.). NJ, USA: Pearson Education.

Leuz, C., Meyer, S., Muhn, M., Soltes, E. F., and Hackethal, A. 2017. "Who Falls Prey to the Wolf of Wall Street? Investor Participation in Market Manipulation," *SSRN Electronic Journal* (doi: 10.2139/ssrn.3289931).

Li, T., Shin, D., and Wang, B. 2018. "Cryptocurrency Pump-and-Dump Schemes," *SSRN Electronic Journal* (doi: 10.2139/ssrn.3267041).

Lin, T. 2017. "The New Market Manipulation," *Emory Law Journal* (66), p. 1253.

Liu, C., and Wang, H. 2019. "Crypto Tokens and Token Offerings: An Introduction," in *Cryptofinance and Mechanisms of Exchange,* S. Goutte, K. Guesmi and S. Saadi (eds.). MA,USA: Springer, pp. 125-144.

Liu, X., Jiang, X., Liu, S., and Tse, C. 2021. "Knowledge Discovery in Cryptocurrency Transactions: A Survey," *IEEE Access* (9), pp. 37229-37254.

Lyócsa, S., Molnár, P., Plíhal, T., and Širanováf, M. 2020. "Impact of Macroeconomic News, Regulation and Hacking Exchange Markets on the Volatility of Bitcoin," *Journal of Economic Dynamics and Control* (119).

Mansourifar, H., Chen, L., and Shi, W. 2020. "Hybrid Cryptocurrency Pump and Dump Detection," in: *ArXiv:2003.06551*.

McIntosh, R. 2020. "Crypto Market Manipulation Is Still Alive and Well, Says Orbs' Ilan Sterk." Retrieved 06.04.2021, from https://t1p.de/v8zm

Mirkovic, J., and Reiher, P. 2004. "A Taxonomy of Ddos Attack and Ddos Defense Mechanisms," *Computer Communication Review* (34:2), pp. 39-53.

Mirtaheri, M., Abu-El-Haija, S., Morstatter, F., Steeg, G. V., and Galstyan, A. 2021. "Identifying and Analyzing Cryptocurrency Manipulations in Social Media," *IEEE Transactions on Computational Social Systems* (8:3), pp. 607-617.

Mita, M., Ito, K., Ohsawa, S., and Tanaka, H. 2019. "What Is Stablecoin?: A Survey on Price Stabilization Mechanisms for Decentralized Payment Systems," *2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI)*, Toyama, Japan: IEEE, pp. 60-66.

Nakamoto, S. 2009. "Bitcoin : A Peer-to-Peer Electronic Cash System," in: *Decentralized Business Review*.

Nizzoli, L., Tardelli, S., Avvenuti, M., Cresci, S., Tesconi, M., and Ferrara, E. 2020. "Charting the Landscape of Online Cryptocurrency Manipulation," *IEEE Access* (8), pp. 113230-113245.

O'Leary, D. 2018. "Open Information Enterprise Transactions: Business Intelligence and Wash and Spoof Transactions in Blockchain and Social Commerce," *Int. J. Intell. Syst. Account. Financ. Manage.* (25:3), pp. 148-158.

O'Neal, S. 2020. "Ddos Attacks on Okex and Bitfinex Were Sophisticated, Possibly Related." Retrieved 20.04.2021, from https://tinyurl.com/nka2bhmj

Parlour, C. A., and Seppi, D. J. 2008. "Limit Order Markets: A Survey," in *Handbook of Financial Intermediation and Banking,* A.V. Thakor and A.W.A. Boot (eds.). CA, USA: Elsevier, pp. 63-96.

Pearce, J. M. 2018. "How to Perform a Literature Review with Free and Open Source Software," *Practical Assessment, Research, and Evaluation* (23:1).

Pennec, G. L., Fiedler, I., and Ante, L. 2021. "Wash Trading at Cryptocurrency Exchanges," *Finance Research Letters*), p. 101982.

Peterson, T. 2020. "To the Moon: A History of Bitcoin Price Manipulation," *Journal of Forensic and Investigative Accounting* (13).

Philipps, D., and Graves, S. 2021. "The 9 Public Companies with the Biggest Bitcoin Portfolios." Retrieved 20.04.2021, from https://decrypt.co/47061/public-companies-biggest-bitcoin-portfolios

Putniņš, T. J. 2012. "Market Manipulation: A Survey," *Journal of Economic Surveys* (26:5), pp. 952-967.

Rehman, M. H. U., Salah, K., Damiani, E., and Svetinovic, D. 2020. "Trust in Blockchain Cryptocurrency Ecosystem," *IEEE Transactions on Engineering Management* (67:4), pp. 1196-1212.

Rejeb, A., Rejeb, K., and Keogh, J. G. 2021. "Cryptocurrencies in Modern Finance: A Literature Review," *Etikonomi* (20:1), pp. 93-118.

Rowley, J., and Slack, F. 2004. "Conducting a Literature Review," *Management Research News* (27:6), pp. 31-39.

Preprint Version

Sam, S. 2019. "Insider Trading in Cryptocurrency." Retrieved 04.04.2021, from https://tinyurl.com/9ba5buvc

Shi, F. B., Sun, X. Q., Gao, J. H., Xu, L., Shen, H. W., and Cheng, X. Q. 2019. "Anomaly Detection in Bitcoin Market Via Price Return Analysis," *PLoS One* (14:6), p. e0218341.

Shifflet, S. 2018. "Some Traders Are Talking up Cryptocurrencies, Then Dumping Them, Costing Others Millions." Retrieved 05.04.2021, from https://tinyurl.com/kys7jdfk

Shome, A. 2017. "John Mcafee Twitter Handle Hack Results in Pump and Dump of Multiple Coins." Retrieved 02.02.2021, from https://tinyurl.com/s5a28fnj

Sobol, A. 2020. "Frontrunning on Automated Decentralized Exchange in Proof of Stake Environment," *IACR Cryptol. ePrint Arch.* (2020), p. 1206.

Tether ltd. 2021. "About Tether." Retrieved 03.03.2021, from https://tether.to/faqs/

Twomey, D., and Mann, A. 2020. "Fraud and Manipulation within Cryptocurrency Markets," in *Corruption and Fraud in Financial Markets: Malpractice, Misconduct and Manipulation,* C. Alexander and D. Cumming (eds.). New Jersey: John Wiley & Sons, p. 214.

Underwood, B. D. 2018. "Virtual Markets Integrity Initiative." Retrieved 20.04.2021, from https://virtualmarkets.ag.ny.gov

United States. 2010. "Dodd-Frank Wall Street Reform and Consumer Protection Act." Retrieved 20.04.2021, from https://tinyurl.com/fp2j4cdy

Vasek, M., and Moore, T. 2015. "There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams," *International Conference on Financial Cryptography and Data Security,* R. Böhme and T. Okamoto (eds.), Berlin, Heidelberg: Springer, pp. 44-61.

Vasek, M., and Moore, T. 2019. "Analyzing the Bitcoin Ponzi Scheme Ecosystem," *International Conference on Financial Cryptography and Data Security,* A. Zohar, I. Eyal, V. Teague, J. Clark, A. Bracciali, F. Pintore and M. Sala (eds.), Berlin, Heidelberg: Springer, pp. 101-112.

Verstein, A. 2019. "Crypto Assets and Insider Trading Law S Domain," *Iowa Law Review* (105:1).

VHB. 2015. "Vhb-Jourqual3." Retrieved 01.01.2021, from https://t1p.de/xzei

Victor, F., and Hagemann, T. 2019. "Cryptocurrency Pump and Dump Schemes: Quantification and Detection," *2019 International Conference on Data Mining Workshops (ICDMW)*, Beijing, China: IEEE, pp. 244-251.

Victor, F., and Weintraud, A. M. 2021. "Detecting and Quantifying Wash Trading on Decentralized Cryptocurrency Exchanges," in: *ArXiv:2102.070001*.

Viriyasitavat, W., and Hoonsopon, D. 2019. "Blockchain Characteristics and Consensus in Modern Business Processes," *Journal of Industrial Information Integration* (13), pp. 32-39.

Vogelsteller, F., and Buterin, V. 2020. "“Eip-20: Erc-20 Token Standard," Ethereum Improvement Proposals, No. 20." Retrieved 20.04.2021, from https://eips.ethereum.org/EIPS/eip-20

vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., and Cleven, A. 2009. "Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process," *ECIS 2009 Proceedings*, Verona, Italy: AIS.

Webster, J., and Watson, R. T. 2002. "Analysing the Past to Prepare for the Future: Writing a Literature Review a Roadmap for Release 2.0," *Journal of Decision Systems* (29:3), pp. 129-147.

Wei, W. 2018. "The Impact of Tether Grants on Bitcoin," *Economics Letters* (171), pp. 19-22.

Wilmoth, J. 2017. "Think Coinbase Employees Engaged in Insider Trading? Deal with It." Retrieved 20.04.2021, from https://tinyurl.com/khmnu6y

Xia, P., Wang, H., Zhang, B., Ji, R., Gao, B., Wu, L., Luo, X., and Xu, G. 2020. "Characterizing Cryptocurrency Exchange Scams," *Computers & Security* (98).

Xu, J., and Livshits, B. 2019. "The Anatomy of a Cryptocurrency Pump-and-Dump Scheme," *Proceedings of the 28th USENIX Security Symposium*, Santa Clara, CA, USA: USENIX Assoc., pp. 1609-1625.

Preprint version

View publication stats