A Taxonomy of Violations in Digital Asset Markets

Benjamin Clapham
Goethe University Frankfurt, clapham@wiwi.uni-frankfurt.de

Jenny Jakobs
University of Augsburg, jenny.jakobs@uni-a.de

Julian Schmidt
Goethe University Frankfurt, julian.schmidt@wiwi.uni-frankfurt.de

Peter Gomber
Goethe University Frankfurt, Gomber@wiwi.uni-frankfurt.de

Jan Muntermann
University of Augsburg, jan.muntermann@uni-a.de

A Taxonomy of Violations in Digital Asset Markets

Completed Research Paper

Benjamin Clapham
Goethe University Frankfurt
Frankfurt, Germany
clapham@wiwi.uni-frankfurt.de

Jenny Jakobs
University of Augsburg
Augsburg, Germany
jenny.jakobs@uni-a.de

Julian Schmidt
Goethe University Frankfurt
Frankfurt, Germany
julian.schmidt@wiwi.uni-frankfurt.de

Peter Gomber
Goethe University Frankfurt
Frankfurt, Germany
gomber@wiwi.uni-frankfurt.de

Jan Muntermann
University of Augsburg
Augsburg, Germany
jan.muntermann@uni-a.de

Abstract

Numerous frauds, market manipulations and other violations have recently shaken investor confidence in digital asset markets and digital assets themselves. Yet, investor confidence and market integrity are key requirements for the continued success of crypto and other digital assets. In order to facilitate the integrity of digital asset markets and avoid integrity incidents in the future, a systematic overview of violations and their main characteristics is needed to develop appropriate countermeasures. Therefore, we develop a taxonomy of violations in digital asset markets and evaluate the taxonomy based on real-world cases. Our results show that many types of market manipulation in traditional financial markets can also be observed in digital asset markets. However, there are new and additional violations in digital asset markets. We also find that many violations depend on specific capabilities of the violator, certain trading conditions, and asset-specific characteristics.

Keywords: Digital asset markets, cryptocurrencies, blockchain, market manipulation, fraud

Introduction

The global financial crisis and the resulting loss of investor confidence in traditional financial markets and intermediaries gave rise to blockchain technologies, which provide a trustless environment in which all transactions are stored in distributed ledgers that are immutable, transparent, secure, and integer. This technology, known as distributed ledger technology (DLT), has since become one of the most important innovations, reshaping industries like healthcare, law, security and finance (Guo and Yu 2022; Lin and Liao 2017). In finance, DLT has enabled the emergence of digital assets such as cryptocurrencies, security tokens, utility tokens and non-fungible tokens (NFTs). These assets are traded on digital asset markets (DAMs), which function as counterparts to traditional stock exchanges. Initially, digital assets primarily attracted

retail investors, but institutional investors have begun to offer digital asset products to their clients and include these assets into their portfolios for diversification (Huang et al. 2022).

However, the promise of blockchain and DLT to increase transparency and security in financial markets has also raised security concerns. These concerns include wallet hacks, denial-of-service attacks, exploited smart contracts resulting from code vulnerabilities, among others, which negatively impact the digital world (Guo and Yu 2022). Consequently, trading activities on DAMs are negatively affected, making them prone to violations such as market manipulation, scams, and other fraudulent activities to the detriment of investors' assets and the integrity of these platforms. Notably, these violations affect not only the vast number of small platforms, where up to 70% of the transaction volume has been found to be artificial trades without actual change in ownership (Cong et al. 2022), but also large, established markets such as Binance, the world's largest DAM. In June 2023, the U.S. Securities and Exchange Commission charged Binance and its founder with 13 different securities law violations (Mondo Visione 2023). Similarly, hacks and thefts represent a major threat for DAMs with investors suffering losses of 513 million U.S. dollars in 2020, an increase of 38.4% from the previous year (TradingPlatforms 2022). A prominent example is the FTX Trading Ltd. scandal, which caused a billion-dollar damage to cryptocurrency investors, generated widespread public attention and caused confidence losses for both institutional and retail investors in DAMs (Reuters 2022). However, investor confidence and market integrity are key requirements for the continued success and development of DAMs and the digital assets they trade.

Against this background, a systematic overview of violations in DAMs is needed, benefiting investors, intermediaries, market operators, as well as regulators. It serves as a basis for developing appropriate countermeasures to prevent future violations and to restore trust in DAMs. As DAMs are relatively new, a classification approach would also help regulators to (re)evaluate initiatives such as the European Union's Markets in Crypto-Assets (MiCA) regulation (European Commission 2020), set to take effect in 2024. This regulation transfers issues from traditional financial markets but does not consider DAM-specific challenges, such as the low liquidity environment in which many digital assets are traded (La Morgia et al. 2023). Therefore, a systematic overview is essential to identify the unique vulnerabilities of DAMs. While a comprehensive taxonomy of potential market manipulations already exists for traditional financial markets (Siering et al. 2017), none exists for DAMs. We are the first to develop a taxonomy to classify DAM violations following Nickerson et al. (2013) and Kundisch et al. (2022). This taxonomy organizes and structures incidents based on their specific dimensions and characteristics, providing new insights into the nature of violations in DAMs. Stakeholders can use it as a toolbox to identify, differentiate and respond to violations in these markets based on their specific characteristics.

Our taxonomy serves to deepen the understanding of violations in DAMs, adds to a scarce research stream and serves as a foundation for further empirical research in this area. Additionally, it helps investors to assess risks when trading in DAMs and support market operators in designing DAMs. It also assists regulatory authorities in protecting investors more effectively against violations and researchers in developing systems to detect DAM incidents. Thereby, it finally helps to hold violators accountable.

The remainder of the paper is organized as follows. The second section describes the research context of our study and presents related literature. The third section describes our methodology for developing a taxonomy of violations in DAMs. Section four elaborates on our data set and discusses the identified violations. We develop the taxonomy of violations in DAMs in section five and evaluate it in section six. The final section discusses the implications and limitations of the paper and provides an overall conclusion.

Research Background

Digital Asset Markets and Violations in These Markets

Digital assets, also known as crypto assets, have emerged as a new form of digital representation of value that can be stored and transferred electronically (European Commission 2020). These assets include both fungible tokens, such as cryptocurrencies, which are interchangeable with one another, and non-fungible tokens (NFTs), which represent unique digital assets, such as digital art, and are not interchangeable (Chohan 2021).

DAMs are platforms where buyers and sellers of digital assets can be brought together, resulting in a contract between the two parties (European Commission 2020). These markets are either trading platforms

provided by a market operator such as Binance, i.e., centralized exchanges (CEXs), or decentralized exchanges (DEXs) such as Uniswap. They offer important liquidity and price discovery functions for digital assets. However, DAMs are also associated with several unique risks and challenges, such as security vulnerabilities, market manipulation or regulatory uncertainty, which can lead to violations such as fraud, hacking, scams, and manipulation of asset prices and trading volumes. These violations harm the integrity of DAMs and, thus, investors' trust in these markets. Market integrity exists when the asset pricing process is fair and transparent (G7 Working Group on Stablecoins 2019). Maintaining integrity is crucial for a market to realize its potential, to support the development and growth of the assets traded in that market, and to enable investment decisions to be made in a safe environment. In our research context, violations in DAMs refer to any actions or events that potentially violate the integrity of these markets, i.e., the principles of reliability and trust. These principles include the existence of reliable and informative prices, the protection of investor funds from unauthorized third-party access, and the functioning of the underlying infrastructure. Further, prices must represent a realistic picture of the actual existing supply and demand (Austin 2017). Consequently, violations damage investors' trust and confidence in DAMs.

Related Literature

Research on market manipulation and fraud in traditional financial markets dates back more than 20 years and is quite extensive (Allen and Gale 1992; Hart 1977; Putniņš 2012). With the emergence of digital assets and DAMs, traditional market manipulation strategies have evolved and been transferred to these new markets (Dupuis et al. 2023).

While the literature on market manipulation and other violations in DAMs is still less extensive than the literature covering traditional financial markets, it is steadily growing. There are several studies on violation methods in DAMs, which can be summarized in different categories (Eigelshoven et al. 2021; Scharfman 2023). First, the category of **market manipulation** includes fraudulent activities aiming at manipulating asset prices or trading activity. One very prevalent market manipulation scheme in DAMs is pump-and-dump where the price of an asset is artificially inflated and then sold to generate a profit (La Morgia et al. 2023). Cryptocurrency manipulators openly announce their intention to pump-and-dump certain coins on social media or messaging apps thereby attracting investors despite expected negative returns (La Morgia et al. 2023; Li et al. 2018). Another common market manipulation scheme is wash trading, where the volume of a coin is artificially inflated by transactions without any actual change of ownership. Cong et al. (2022) even find that wash trades account for more than 70% of reported volume on some exchanges. Due to their specific nature, new manipulation strategies have evolved that are unique to DAMs. For example, Daian et al. (2020) study miner extractable value, a market-exploiting behavior common on DEXs. Second, there are also a variety of **insider trading** schemes which aim at exploiting information asymmetries in digital assets. Insider trading is a threat to the integrity of DAMs yet Félez-Viñas et al. (2022) find evidence of insider trading in up to a quarter of cryptocurrency exchange listings. This also happens in NFT markets where insider buying activity has been found to be a predictor of NFT returns (Oh 2023). Third, **investment fraud** occurs in DAMs, e.g., in the form of a Ponzi scheme, a "classic" fraud that has migrated from traditional financial markets (Dupuis et al. 2023). Vasek and Moore (2019), for instance, study the success factors of Bitcoin-based Ponzi schemes in a Bitcoin forum and find that the scammer's reputation and the amount of interaction with victims affect the success rate of a scam. Fraudulent activity can also occur through the manipulation of financial statements or whitepapers, which we refer to as **accounting fraud.** As Dupuis et al. (2023) point out, the digital age has brought new challenges with respect to the falsification of financial statements and the ability of regulators to deal with such misleading disclosures.

Furthermore, a significant number of DAMs or brokers lack **regulatory approval**. Evidence from a recent study by Cong et al. (2022) indicates that wash trading occurs on approximately 50% to 80% of unregulated exchanges, while it is notably absent from regulated exchanges. Additionally, the study highlights that the reported trading volumes on unregulated exchanges are subject to substantial inflation. These findings demonstrate the efficacy of regulatory measures in curbing wash trading and improving the accuracy of trading volume reporting. **Scams** are prevalent in the digital asset space and include rug pulls or the misappropriation of clients' assets. A recent case involves the misappropriation of clients' funds carried out by FTX Trading Ltd., resulting in the collapse of this DAM. Notably, this event marks the largest collapse of a DAM to date (Bouri et al. 2023; Vidal-Tomás et al. 2023). Vidal-Tomás et al. (2023) show that this collapse can be attributed to a decline in the value of FTX's native token, which triggered a shortage of available credit. In an attempt to hide their deteriorating financial situation, FTX engaged in various forms of fraud,

including a large-scale misuse of user funds. Finally, due to their digital nature, **cyber attacks** are a common threat in DAMs, such as flash loan attacks. A flash loan is a smart contract-based loan that is borrowed and repaid within a single transaction block. Qin et al. (2021) explain how flash loans can be exploited for attacks and describe two major existing attacks.

Understanding violations in DAMs is important for information systems research, as evidenced by several studies (Daian et al. 2020; La Morgia et al. 2023; Xia et al. 2021). However, the effective identification and mitigation of such violations require the establishment of a systematic classification, which can be achieved through the development of a taxonomy. Several taxonomies have been developed in related domains, including a taxonomy of FinTech types (Imerman and Fabozzi 2020), FinTech business models (Beinke et al. 2018; Eickhoff et al. 2017) and digital markets in general (Blaschke et al. 2019). Researchers have also worked on taxonomies in the field of digital assets. Lausen (2019) develops a taxonomy of digital assets, while Fridgen et al. (2018) construct a taxonomy of initial coin offerings (ICOs). Similarly, Ziegler and Welpe (2022) contribute a taxonomy of decentralized autonomous organizations. Furthermore, a taxonomy of market manipulations exists for traditional financial markets, which segments market manipulation techniques into eight dimensions and classifies traditional market manipulation techniques (Siering et al. 2017). However, despite these existing efforts, there remains a gap in the literature regarding a comprehensive categorization of violations within DAMs. To bridge this gap, our study aims to introduce and evaluate a taxonomy of violations within these markets.

Methodology

To develop a comprehensive taxonomy of violations in DAMs, we adopt the well-established methodology proposed by Nickerson et al. (2013) and Kundisch et al. (2022). The first step of this methodology is to specify the observed phenomenon, the target user group, and the intended purpose of the taxonomy (Kundisch et al. 2022; Nickerson et al. 2013). In this regard, our taxonomy is intended to be used by market participants (investors and intermediaries), DAM operators, researchers, and regulators to provide them with a toolbox to differentiate violations based on their specific characteristics. Our goal is to help stakeholders to identify vulnerabilities in terms of incidents that may be exploited in DAMs. The next step in developing the taxonomy is to determine the meta-characteristic, the ending conditions, and the evaluation goals. The meta-characteristic serves as the starting point for defining all other dimensions that describe violations in DAMs (Nickerson et al. 2013). In our case, the meta-characteristic is to identify the characteristics that differentiate violations in DAMs. We assess the taxonomy based on our evaluation goal of better identifying, classifying, analyzing, and clustering violations compared to other classification schemes or without any taxonomy.

Creating a taxonomy requires an iterative approach. The process is complete when the ending conditions are met. We adopt the subjective and objective ending conditions proposed by Nickerson et al. (2013) for the taxonomy-building phase. Subjective conditions determine whether a taxonomy is applicable, and these conditions are satisfied when the taxonomy is (1) concise, (2) robust, (3) comprehensive, (4) extensible, and (5) explanatory. Objective ending conditions are satisfied when the taxonomy meets all necessary criteria, including (1) examining a representative sample of objects, (2) avoiding merging or splitting an object in the last iteration, (3) having at least one object that can be classified under every dimension, (4) avoiding adding new characteristics or dimensions in the last iteration, (5) avoiding merging or splitting a dimension or characteristic in the last iteration, (6) having no duplicate dimensions, (7) having no duplicated characteristics within a dimension, and (8) avoiding the duplication of cells (Nickerson et al. 2013).

Using a structured approach to develop a taxonomy not only increases the reproducibility of the results and the consistency of the classification of concepts but also reduces ambiguity and the potential for confusion. To build the taxonomy, we follow a multi-step process involving several iterations, which can be either conceptual-to-empirical or empirical-to-conceptual approaches. After each iteration, the characteristics and dimensions are reviewed and revised, and the process continues until the ending conditions are met (Kundisch et al. 2022). In the empirical-to-conceptual approach, the first step involves identifying a set of objects to be classified, followed by the identification of common characteristics. The conceptual-to-empirical approach is a deductive process that begins by conceptualizing dimensions without first examining objects (Nickerson et al. 2013).

Data Set and Violations in Digital Asset Markets

In order to build a comprehensive sample of objects, which serves as a basis for the subsequent taxonomy development process, we create a data set of real-world violations that occurred in DAMs using news articles from the digital asset news portal Coindesk. We identify the representative sample of violations in DAMs using a keyword-based search that uses search terms related to events that negatively affect market integrity. The relevant integrity incidents were found by searching for the keywords "fraud", "hack", "scam", "market manipulation", "violation" and "incident" and by applying the "markets" filter on coindesk.com (Coindesk 2023). The keywords reflect standard types of integrity incidents known from traditional financial markets (e.g., Putniņš 2012) as well as cyber-attacks and scams that hit DAMs in the past (e.g., Scharfman 2023). The "markets" filter ensures that we only obtain news about integrity incidents that are related to DAMs. We collected the data in March 2023 and included articles from January 2020 until December 2022, resulting in a data set of 1,645 news articles. Thereby, the time span includes important developments such as the COVID-19 pandemic, which boosted crypto trading volumes, as well as the all-time highs in cryptocurrency prices with the subsequent "crypto winter" to capture today's relevant violations on DAMs (Corbet et al. 2020; Gorton and Zhang 2023).

From this data set, two researchers identified 75 relevant integrity incidents in DAMs by reviewing the identified news articles independently. Furthermore, they aggregated the real-world cases according to the type of violation (e.g., specific Ponzi schemes are aggregated to the violation "Ponzi scheme"). For the identification of relevant incidents, the researchers used the definition of integrity relevant violations introduced in the background section and discussed cases where they deviated together with a third researcher until they came to a consensus. Some cases in our data set involve multiple types of violations simultaneously. To ensure proper categorization, we assigned these cases to the primary or more severe violation. For example, the case of John McAfee and his business partner involved both an unlawful celebrity ICO promotion and a pump-and-dump scheme. However, we categorized this case as an unlawful celebrity ICO promotion because the monetary damage from this violation was approximately five times higher than that of the pump-and-dump scheme (De 2023). As a final robustness check, we validated all identified incidents by cross-checking them with Cointelegraph as additional source and used a web search for 9 cases that were not reported on Cointelegraph.

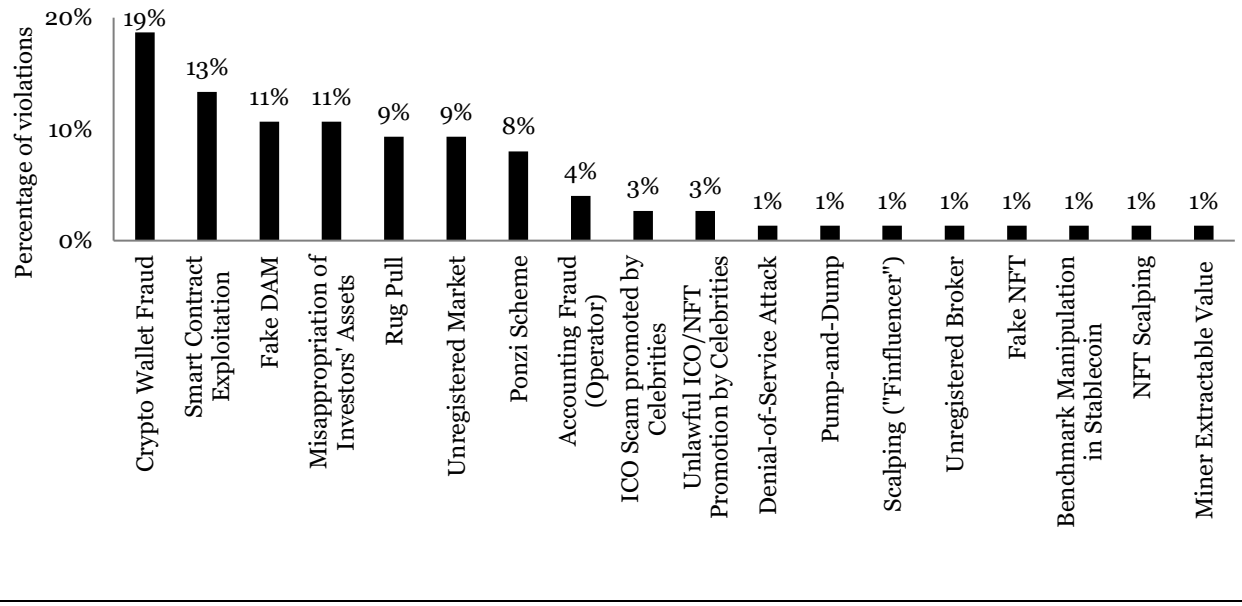

Figure 1. Identified Real-World Violations in DAMs

Figure 1 shows the frequency of the different violations in DAMs that we identified in our data set. Analyzing our cases, about one third are crypto-wallet fraud and smart contract exploitation, both of which are types of cyber attacks. The categories of fake DAM and misappropriation of clients' assets each account for more

than 10% of the cases in our data set, while the remaining cases are less common in our sample. A brief definition of all identified DAM violations is provided in Panel A of Table 1. To improve readability and provide a clearer overview, we have grouped all identified violations into the categories identified in the literature review, i.e., accounting fraud, investment fraud, insider trading, cyber attacks, lack of regulatory approval, scams, and market manipulation.

Panel A		
Violation	Cate-gory	Definition
Accounting Fraud (Operator)	AF	The operator of a DAM manipulating, e.g., the balance sheet by improper accounting thereby misrepresenting the financial health of the company.
Benchmark Manipulation in Stablecoins	IF	Manipulation of the price of a stablecoin's underlying in order to profit from related changes in the stablecoin's price.
Ponzi Scheme	IF	An asset manager consecutively raising external funds and paying returns to investors from new capital raised from new investors, thereby faking returns.
Denial-of-Service Attack	CA	Cyber attack jamming a DAM's business and services (e.g., to profit from information arbitrage opportunities based on knowledge of the timing of the attack or for political motives).
Crypto Wallet Fraud	CA	Cyber attack targeting a DAM's IT infrastructure to steal money or assets from the investors' wallets, possibly by exploiting bugs in the code.
Smart Contract Exploitation	CA	Cyber attack exploiting smart contracts in the digital asset environment, e.g., a flash loan attack.
Unregistered Broker	RA	Broker failing to register with relevant regulatory authorities and depriving its customers of the protections associated with registration, including SEC inspections and examinations and the requirement to establish policies and procedures to safeguard customer information.
Unregistered DAM	RA	DAM failing to register with relevant regulatory authorities and depriving its customers of the protections associated with registration, including SEC inspections and examinations and the requirement to establish policies and procedures to safeguard customer information.
Fake DAM	S	Scammers establishing a website similar to an established DAM to attract investors, charging high fees, and then disappearing with investors' money.
Fake NFTs	S	Scammers forging NFTs by creating copycat collections, sometimes stealing the original art and cloning entire projects to mimic the real, valuable ones.
Rug Pull	S	Scammers establishing a fake project on their own, issuing a fake-coin, without the intention to invest investors' money in the project.
Misappropriation of Investors' Assets	S	Scammers operating a DAM, attracting investors, and misusing (and potentially disappearing with) the money and assets of investors that are hold by the DAM.
ICO Scam Promoted by Celebrities	S	Celebrities recommending to invest in a fraudulent ICO without disclosing the payment they received for promoting this investment.
Pump-and-Dump/Short-and-Distort	MM	Scammers entering a long/short position in a digital asset, disseminating wrong positive/negative information about the asset or the company behind the token and selling/buying (back) the asset after its inflation/decline, thereby making substantial profits.
Miner Extractable Value	MM	Miners placing their transactions right before those of other network participants to profit from arbitrage opportunities before others or to profit from price changes by front-running transactions of other participants.
Scalping ("Finfluencer")	MM	Non-professional investment advisors (active in social media) purchasing a digital asset before recommending it to third parties without disclosing their position and profiting from the rise in the price following the recommendation.
Unlawful ICO/NFT Promotion by Celebrities	MM	Celebrities recommending investing in an ICO to artificially inflate the price without disclosing the payment they received for promoting this investment.
NFT Scalping (Bots)	MM	Violators using bots to buy all available tokens from a specific NFT collection at the moment they go on sale in order to sell them for inflated prices.

Table 1. Definitions of Violations in DAMs

Panel B		
Violation	Cate-gory	Definition
Accounting Fraud (Issuer)	AF	Issuer of a digital asset deliberately manipulating, e.g., the whitepaper or company financials, by making false statements thereby misrepresenting the prospects of the asset and/or crypto project.
Non-disclosure of Insider Information	IT	Willful misrepresentation of a digital asset (market) by non-disclosure of relevant information.
Insider Trading	IT	Investment decisions based on relevant non-public information (e.g., token issuers using their private information to profit from digital assets' price changes).
Spoofing/Layering/ Advancing the Bid/ Reducing the Ask	MM	Placing order(s) on one side of the order book and/or submitting increasing/decreasing bids/asks for the same asset on the other side of the market without the intention of the additional order(s) being executed to move the market price in the direction of the first order(s) thereby creating a false impression of supply and demand. Once the initial order(s) is/are executed, the investor cancels all other orders and profits from the price reversal.
Quote Stuffing	MM	High-frequency traders placing and immediately cancelling a large number of orders to flood the trading system with excessive messages. Quote stuffing can create information arbitrage opportunities due to increased data latencies for other market participants.
Front-Running	MM	Brokers or market makers using their private information about incoming order flow by buying or selling a digital asset in advance of other parties' large trades, thereby profiting from the price movement that follows the large trades.
Cornering/Squeezing	MM	Cornering the market of a digital asset by obtaining large quantities of the asset, thereby gaining a price-controlling market position due to the shortage of supply. Third parties are then forced to buy the digital asset at inflated prices (squeezing).
Wash Trading	MM	Entering into arrangements for the sale or purchase of a digital asset where there is no change in beneficial interests or market risk or where the transfer of beneficial interest or market risk is only between parties who are acting in concert or collusion.
Improper Matched Orders	MM	Transactions in which colluding investors enter matching buy and sell orders simultaneously with the same price and quantity to feign an active market to lure other investors into buying the digital asset, thereby causing a price increase.
Painting the Tape	MM	Engaging in a series of publicly reported transactions to give the impression of trading activity and price movements. As for matched orders, the objective is to attract other investors buying the digital asset leading to a higher price. However, collusion of several investors is not a necessary characteristic of painting the tape.
Capping/Pegging	MM	Manipulating the price of a digital asset underlying a digital option shortly before the option's expiration date to prevent a rise/decline in the price of the digital asset so that the previously written call/put option will expire worthless, thereby protecting the option premium initially received.
Churning	MM	Brokers engaging in excessive buying and selling of digital assets in clients' accounts to create higher commissions against the clients' interests.
Scalping (Investment Adviser)	MM	Professional investment advisors purchasing a digital asset before recommending it to their clients without disclosing their position and profiting from the rise in the price following the recommendation.
Pinging	MM	Submission of small marketable orders without an intention to trade to detect large hidden orders (abusive liquidity detection) to benefit from that information.
Ramping	MM	Entering buy orders at successively increasing prices to mislead other investors to perceive an active interest in a digital asset.
AF = Accounting Fraud, IF = Investment Fraud, IT = Insider Trading, CA = Cyber Attack, RA = Lack of Regulatory Approval, S = Scam, MM = Market Manipulation		

Table 1. Continued

Developing a Taxonomy of Violations in Digital Asset Markets

To develop our taxonomy of violations in DAMs, we follow the iterative procedure proposed by Nickerson et al. (2013), which includes conceptual-to-empirical and empirical-to-conceptual iterations.

Iteration 1:

In the first iteration, we choose the conceptual-to-empirical approach because the taxonomy of market manipulations in traditional financial markets by Siering et al. (2017) provides in-depth knowledge about violations, much of which can be transferred to DAMs. Thereby, two important steps are necessary: (1) For each manipulation technique identified by Siering et al. (2017), we need to check whether such an integrity incident is also possible in DAMs. (2) We need to evaluate which dimensions and characteristics of their taxonomy can be used for the taxonomy of violations in DAMs.

With respect to (1), the manipulation technique "Marking the Close", which describes the manipulation of the closing price of a security, is not relevant in DAMs because these markets typically operate 24/7. Moreover, benchmark manipulations with and without official fixing in traditional financial markets (e.g., interest rate fixing) are not directly applicable to DAMs. However, stablecoins, i.e., tokens whose value is tied to an underlying asset or currency, are vulnerable to manipulations that aim at artificially changing the value of the stablecoin's underlying asset. Therefore, we transform the manipulation techniques related to benchmark manipulation into "benchmark manipulation in stablecoins", which we also identified in our sample of real-world cases (see Panel A of Table 1). Since digital assets on CEXs such as Binance, Coinbase, or Kraken are traded in standard limit order books (LOBs), basically all violations from traditional financial markets are also possible in DAMs. Therefore, we also include all other incidents from Siering et al. (2017) in the taxonomy for violations in DAMs. Panel B of Table 1 provides the list of violations known from traditional financial markets that can be transferred to DAMs, which we have not yet identified in our sample of real violations in DAMs.

Concerning the transferable dimensions (2), we can transfer four relevant dimensions (i)-(iv). First of all, an important property describing violations is who commits them. Therefore, the dimension (i) of the taxonomy is the "*violator*" with the characteristics "*issuer*", "*investor*", and "*intermediary*". Depending on the violation, different market participants are involved in each case of the violations that occurs in both traditional financial markets and in DAMs. Moreover, we adopt the dimension (ii) "*means*" of the violation that describes how the violator conducts an integrity incident. Thereby, we also refer to the seminal work by Allen and Gale (1992) who introduced this important distinction. As proposed by Siering et al. (2017), the characteristics "*action-based*", "*information-based*", "*trade-based*", and "*order-based*" are also suitable in the context of violations in DAMs. Thereby, action-based violations describe incidents where the manipulator actively does something, such as setting up a Ponzi scheme. Information-based violations are those where the violator provides false or misleading information to other market participants. Trade-based violations are those where prices or volumes are manipulated based on executed trades while order-based incidents are those where order submissions and cancellations are used to artificially increase demand or supply of an asset. Furthermore, we transfer the dimension (iii) violation "*target*" along with its characteristics "*fundamentals*", "*price*", "*volume*", "*bid/ask*", "*latency*", and "*commissions*" to the domain of violations in DAMs. Since many DAMs operate standard open LOBs just as stock exchanges do, these characteristics are directly transferable. The three characteristics bid/ask, price, and volume relate to standard data describing the market situation in digital and traditional asset markets. Fundamentals in this context refer to the manipulation of a token issuer's financial statements, while the generation of unsubstantiated commissions may be a goal of intermediaries. Latency is the target of violations such as "quote stuffing", which aims at slowing down exchange systems by flooding the servers with a large number of order submissions and cancellations. Finally, we adopt the dimension (iv) "*direct economic advantage*" with its characteristics "*yes*" and "*no*". This dimension helps to identify and distinguish many violations because some of them represent, at first sight, economically irrational behavior. The violator does not profit from her initial action but only from later changes in, for example, asset prices.

$$\begin{aligned} T_1 = \{&Violator\ [Issuer, Investor, Intermediary];\\ &Means\ [Action\ Based, Information\ Based, Trade\ Based, Order\ Based];\\ &Target\ [\ Fundamentals, Price, Volume, Bid/Ask, Latency, Commissions];\\ &Direct\ Economic\ Advantage\ [Yes, No]\} \end{aligned} \tag{1}$$

After the first iteration, we arrive at the taxonomy T_1 provided in Equation (1). At this point, neither the objective nor the subjective ending conditions are met since we have added new objects, dimensions, and characteristics. The taxonomy is not yet comprehensive and explanatory for violations in DAMs because it is solely based on violations known from traditional financial markets that can be transferred to DAMs.

Iteration 2:

For the second iteration, we rely on the empirical-to-conceptual approach. Based on the comprehensive search for violations in DAMs, we can enrich our list of objects. Specifically, we add violations that are completely new in DAMs and revise existing ones based on the real-world data. For example, the violations of "scalping" and "accounting fraud" need to be further defined in DAMs and split up according to who causes these incidents. For example, the FTX scandal has shown that not only issuers but also market operators can commit accounting fraud in DAMs to attract business (in traditional financial markets, issuers and exchange operators are separate institutions and market operators do not profit from changes in asset prices). Also, scalping in DAMs is more often committed by non-professional investment advisers being active on social media (so-called "Finfluencers") and not primarily by professional investment advisers as in traditional financial markets. Besides splitting objects of the taxonomy, some of the violations also need to be merged due to their similarity (Nickerson et al. 2013). "Pump-and-dump" and its counterpart "short-and-distort" essentially describe the same manipulation technique. The only difference is that the violator takes either a long or a short position in the manipulated asset in advance and consequently manipulates the price either up or down. Also, the two objects cannot be differentiated with the taxonomy developed in Iteration 1. Therefore, we merge them into a single object following Nickerson et al. (2013). For the same reason, we merge the manipulations aimed at artificially inflating or altering the supply and demand in LOBs (i.e., "advancing the bid", "reducing the ask", "spoofing", "layering") into a single object.

Besides changes to the list of objects, we also use this iteration to check whether the taxonomy after Iteration 1 (T_1) is appropriate for the entire set of objects (i.e., violations in DAMs) or whether certain dimensions or characteristics need to be revised or added in order to correctly reflect the DAM-specific violations. Based on our sample of real-world violations in DAMs, it becomes clear that many violations caused by scams are directly aimed at misusing or stealing investors' assets. Therefore, we add the corresponding characteristic "*investors' assets*" to the dimension "*manipulation target*". Moreover, we need to add the characteristics "*market operator*" and "*third party*" to the dimension "*violator*" since many violations related to the misuse of clients' assets are committed by the market operator. Similarly, third-party hackers attack a DAM's IT infrastructure to steal investors' assets. Moreover, we also need to add the characteristic "*multiple*" to the "*violator*" dimension because wash trading, a very common violation in DAMs (e.g., Cong et al. 2022), can be committed by multiple parties. Wash trades can be used by market operators to boost volumes on their trading platform to make it more visible compared to other markets, by token issuers to amplify investor interest in their asset, or by investors to attract further purchases of a token in which they have invested. The other two dimensions "*means*" and "*direct economic advantage*" remain unchanged, as we can assign all violations in our sample to the characteristics in a comprehensible and mutually exclusive way, which leads to the following taxonomy T_2 after the second iteration:

$$\begin{aligned} T_2 = \{&Violator\ [Market\ Operator, Issuer, Investor, Third\ Party, Intermediary, Multiple];\\ &Means\ [Action\ Based, Information\ Based, Trade\ Based, Order\ Based];\\ &Target\ [Investors' Assets, Fundamentals, Price, Volume, Bid/Ask, Latency, Commissions];\\ &Direct\ Economic\ Advantage\ [Yes, No]\} \end{aligned} \tag{2}$$

Because we have added further objects in this iteration and revised the characteristics of two dimensions, we need to perform another iteration in the taxonomy development process.

Iteration 3:

As we can extract more DAM-specific information from our collection of violations, we again choose the empirical-to-conceptual approach for the third iteration. Because we have already used all the identified real-world cases in the last iteration, no new objects can be added in this iteration. Instead, we take all objects from our data set and search for new dimensions that help to characterize and distinguish violations

in DAMs. The collected cases clearly show that several violations depend critically on specific capabilities or preconditions, either of the violator herself or of the trading environment of the asset or the market on which the asset is traded. Therefore, the following dimensions are added to the taxonomy. First, we add the dimension (v) "*specific capabilities of the violator*", which describes whether a violation can only be committed if the violator possesses specific capabilities. We identify the following characteristics that describe these specific capabilities: "*dominance (asset/market)*", "*IT infrastructure*", "*dominance (IT)*", "*collusion with other parties*", and "*no*" specific capabilities. Our collection of violations shows that cyber attack-related violations, such as denial-of-service attacks or market manipulations such as quote stuffing (reducing the speed of a trading system by flooding it with order messages), can only be carried out if the violator has the necessary computing power and IT infrastructure. Furthermore, certain violations demand economic dominance of the violator within the digital asset or its corresponding market. For example, cornering a digital asset is only feasible if the violator holds a majority of the asset to push prices up by artificially creating a shortage of supply. Similarly, manipulating the price of a stablecoin's benchmark is only possible if the violator has enough economic power relative to the liquidity of the benchmark to be able to manipulate its price. However, the violator's dominance may also be related to the IT infrastructure in the digital asset space. For example, the common violation "miner extractable value" is only possible if the violator, in her role as a miner, has enough computing power relative to other network participants to be able to mine blocks with a high degree of certainty to profit from this technique. In addition, the violation "improper matched orders" requires that violators collude with other market participants in advance to facilitate this violation. Finally, most violations do not require any specific capabilities of the violator and can potentially be committed by any market participant.

Second, we include the dimension (vi) whether other market- or event-related "*specific preconditions*" are necessary for certain violations. We identify the following characteristics that describe these necessary preconditions: "*specific event*", "*LOB environment*", "*custody of client keys*", "*only DEX*", and "*no*" specific preconditions. A closer analysis of our sample of violations reveals that many of them can only be executed at specific times or upon specific events. For example, accounting fraud by issuers or market operators can only appear when quarterly or annual financial statements are released. Similarly, violations related to ICOs crucially depend on the event of the initial offering and are not feasible for tokens that already trade in the secondary market. In addition, front-running can only occur when an intermediary receives a customer order that needs to be executed. Furthermore, many violations aim at manipulating supply and demand or quoted prices in the LOB of the assets traded. Consequently, violations such as "layering" or "spoofing" can only occur in DAMs that operate open LOBs but not in other trading systems where investors can only buy and sell at pre-defined quotes. Moreover, violations that aim at misusing or stealing investors' assets from DAMs can only occur if the custody of client keys is in the hand of the market operator. If all assets are stored in private wallets, a fake market operator could not misuse or steal them. Similarly, a cyber attack on assets requires that the DAMs store the private keys of the assets. In contrast, other violations can only be performed in the case of DEXs. The technique miner extractable value is only possible if a digital asset is traded on a DEX, as no blocks are mined to the underlying blockchain in case of trades on CEXs where assets are only transferred within the exchange system. Again, most violations do not require any specific preconditions and are feasible in all circumstances. Equation (3) shows the taxonomy T_3 resulting from the third iteration.

$$
\begin{aligned}
&T_3 = \{Violator\ [Market\ Operator, Issuer, Investor, Intermediary, Third\ Party, Multiple];\\
&Means\ [Action\ Based, Information\ Based, Trade\ Based, Order\ Based];\\
&Target\ [Investors' Assets, Fundamentals, Price, Volume, Bid/Ask, Latency, Commissions];\\
&Direct\ Economic\ Advantage\ [Yes, No];\\
&Specific\ Capabilities\ of\ the\ Violator\ [\ Dominance\ (Asset/Market), IT\ Infrastructure,\\
&Dominance\ (IT), Collusion\ With\ Other\ Parties, No];\\
&Specific\ Preconditions\ [Specific\ Event, LOB\ Environment, Custody\ of\ Client\ Keys,\\
&Only\ DEX, No]\}
\end{aligned}
\tag{3}
$$

Although we did not add any new objects in this iteration, we need to perform another iteration in the taxonomy development process because we added two new dimensions, and the taxonomy still needs to be improved to make it robust and explanatory.

Iteration 4:

For this iteration, we rely on the empirical-to-conceptual approach because we can extract further relevant properties of violations based on our representative sample. No new objects are added, and we take all objects from our data set again and look for new dimensions that help to further characterize and distinguish violations in DAMs. Based on the collection of incidents, we find that many violations are more likely to occur when the asset is less liquid or when an asset is traded in an illiquid market. This is particularly true for wash sales, which aim at creating the impression of an active market or an actively traded asset in order to attract more investors. It is also true for the benchmark manipulation of stablecoins, which is easier to conduct with less capital if the benchmark is a rather illiquid asset. In contrast, a highly liquid benchmark, such as the U.S. dollar, can hardly be manipulated by a single investor. Consequently, we add the dimension (vii) "*low liquidity advantageous*" with its characteristics "*yes*" and "*no*". While this dimension does not represent a necessary condition such as those that we developed in iteration 3, the level of liquidity significantly influences the likelihood of specific violations in an asset or market. Therefore, this dimension is highly relevant for investors, market operators, and regulators who want to assess and distinguish the risk of violations in a particular digital asset or DAM. Furthermore, our collection of violations shows that the fungibility of a digital asset has a significant impact on the types of potential violations. Non-fungible tokens stand out as being significantly different from fungible tokens, such as utility tokens, payment tokens and asset tokens, which are highly similar in their susceptibility to various violations. Therefore, we add the dimension (viii) "*asset fungibility*" with its characteristics "*fungible tokens (FT)*", "*non-fungible tokens (NFT)*", and "*all tokens (All)*". While some violations are possible in all types of digital assets, e.g., violations that aim at stealing or misusing investors' assets, others are only possible in fungible tokens or non-fungible tokens. For example, the violation "NFT scalping", where manipulators may intentionally raise NFT prices by using bots to buy all the NFTs in a particular collection that are being sold on the market, is therefore not possible for fungible tokens. In contrast, accounting fraud by either coin issuers or market operators only applies to fungible tokens. Finally, violations such as "crypto wallet fraud" where cyber attackers steal investors' assets can occur in all coins and tokens. Equation (4) shows the taxonomy T_4 at the end of this iteration.

$$
\begin{aligned}
&T_4 = \{Violator\ [Market\ Operator, Issuer, Investor, Third\ Party, Intermediary, Multiple];\\
&Means\ [Action\ Based, Information\ Based, Trade\ Based, Order\ Based];\\
&Target\ [Investors' Assets, Fundamentals, Price, Volume, Bid/Ask, Latency, Commissions];\\
&Direct\ Economic\ Advantage\ [Yes, No];\\
&Specific\ Capabilities\ of\ the\ Violator\ [Dominance\ (Asset/Market), IT\ Infrastructure,\\
&Dominance\ (IT), Collusion\ With\ Other\ Parties, No];\\
&Specific\ Preconditions\ [Specific\ Event, LOB\ Environment, Custody\ of\ Client\ Keys,\\
&Only\ DEX, No];\\
&Low\ Liquidity\ Advantageous\ [Yes, No];\\
&Asset\ Fungibility\ [FT, NFT, All]\}
\end{aligned}
\tag{4}
$$

While the taxonomy after this iteration is explanatory and comprehensive, we need to perform another iteration because the objective ending conditions are not yet met since we added two new dimensions in this iteration.

Iteration 5:

At this point, no further information can be extracted from the sample to help to characterizing and distinguishing between different violations. Therefore, the eight dimensions developed so far, and the corresponding characteristics do not need to be modified further. Moreover, there are no objects left in the representative sample of violations that could be added in this iteration. Therefore, T_4 represents the final taxonomy and is shown together with all violations being classified according to the dimensions and characteristics in Table 2. We find that at least one object is classified under every characteristic of each dimension and that each cell, i.e., the combination of characteristics, is unique and not repeated. Consequently, the taxonomy now satisfies all objective ending conditions (Nickerson et al. 2013). Our developed taxonomy also satisfies all subjective ending conditions according to Nickerson et al. (2013). The first subjective ending criterion is the conciseness, which is met when the taxonomy contains a reasonable number of dimensions. A concise taxonomy should contain seven dimensions plus or minus two to be

meaningful, but be brief enough for people to remember it in short-term memory (Miller 1956). Our taxonomy meets this criterion as it contains eight dimensions and a maximum of seven characteristics per dimension. The taxonomy is robust in that it allows differentiation among violations with the developed dimensions and characteristics, and it is comprehensive since all violations derived from our representative sample of incidents could be assigned. With the identified dimensions and characteristics, the taxonomy is explanatory because it provides the key properties of violations that help relevant stakeholders to identify and distinguish them. Finally, the taxonomy is extensible because new dimensions and characteristics can be easily added if new violations emerge, e.g., due to technological advances or innovations in digital assets and DAMs.

Evaluation of the Taxonomy

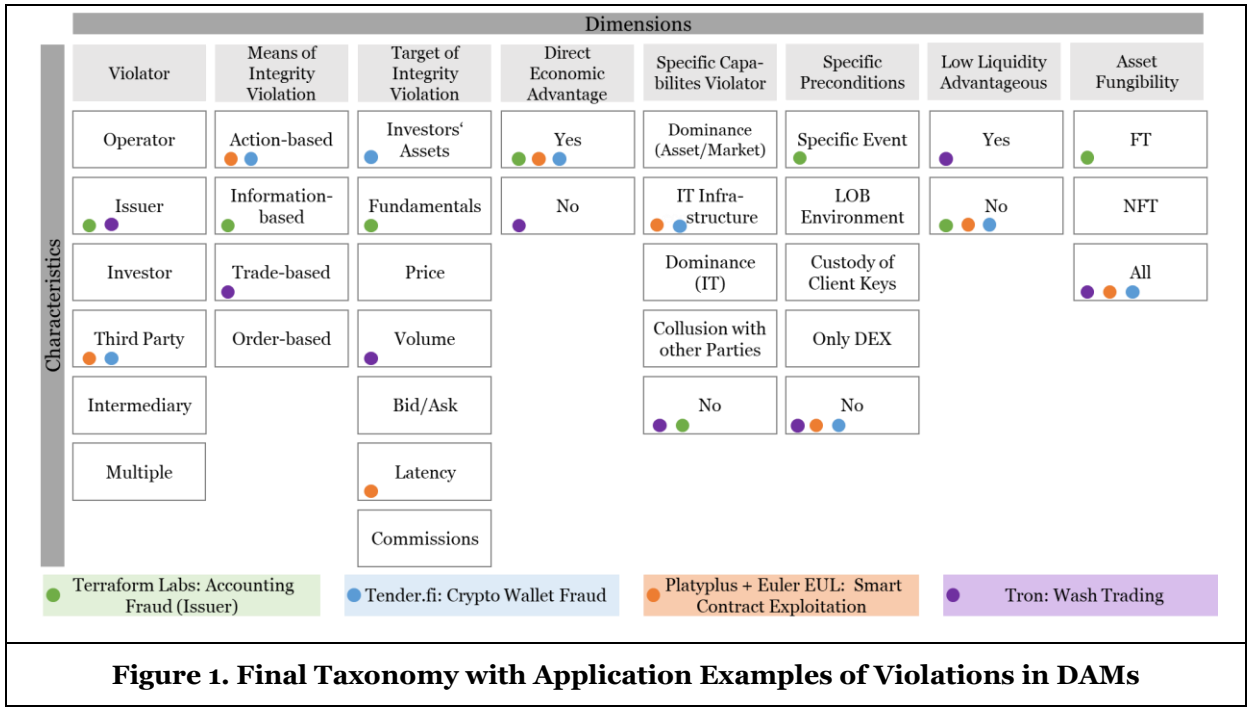

Figure 1. Final Taxonomy with Application Examples of Violations in DAMs

To evaluate the effectiveness of our taxonomy, we employ an ex-post evaluation approach as suggested by Kundisch et al. (2022) and Nickerson et al. (2013). In this process, we apply the taxonomy to recent real-world DAM incidents to demonstrate practicality and usefulness. We identify the incidents from Coinbase using the same methodology as described for the taxonomy building process, but with a timeframe from January 2023 to March 2023. Our analysis reveals five real-world DAM incidents involving Terraform Labs, Euler EUL, Platypus, Tender.fi, and Tron, which include cases of issuer accounting fraud, crypto wallet fraud, smart contract exploitation and wash trading (Coindesk 2023). Our results show that the real-world cases match the theoretical incidents in their dimensions and characteristics. With respect to the real-world wash trading incident (Tron), it is noteworthy that the violator here is the token issuer, deviating from the proposed taxonomy's *"violator"* classification. However, wash trading can also be carried out by investors or market operators, which justifies the use of the "*multiple*" characteristic in the taxonomy. Expanding on the Tron case, we aim to provide a more detailed application of the taxonomy. In March 2023, the SEC announced charges against the founder of the digital asset TRX for wash-trading TRX among other charges (SEC 2022). This violation falls under the "trade-based" category as it aimed to artificially boost TRX's value through over half a million wash trades between two DAMs owned by the same entity (SEC 2022). The goal presumably was to manipulate trading volumes and thus the perception of the asset's popularity and demand. This manipulation provides no direct economic gains for the violator, and it does not require any specific capabilities or conditions. However, a low liquidity environment is advantageous, as inflating the volume of a more actively traded asset is more challenging. Importantly, this type of violation occurs across both fungible and non-fungible tokens, demonstrating the versatility of our taxonomy in classifying real-world cases.

Category	Violation	Violator						Means of Violation				Target of Violation						
		Operator	Issuer	Investor	Third Party	Intermediary	Multiple	Action-based	Information-based	Trade-based	Order-based	Investors' Assets	Fundamentals	Price	Volume	Bid/Ask	Latency	Commissions
AF	Accounting Fraud (Operator)	X							X				X					
	Accounting Fraud (Issuer)		X						X				X					
IF	Benchmark Manipulation in Stablecoins			X						X				X				
	Ponzi Scheme					X		X						X				
IT	Non-Disclosure of Insider Information		X						X					X				
	Insider Trading		X							X				X				
CA	Denial-of-Service Attack				X			X									X	
	Crypto Wallet Fraud				X			X				X						
	Smart Contract Exploitation				X			X				X						
RA	Unregistered Broker					X		X										X
	Unregistered DAM	X						X										X
Scam	Fake DAM				X			X				X						
	Fake NFTs		X					X				X						
	Rug Pull		X					X				X						
	Misappropriation of Investors' Assets	X						X				X						
	ICO Scam Promoted by Celebrities				X				X			X						
Market Manipulation	Pump-and-Dump/Short-and-Distort			X					X					X				
	Spoofing/Layering/Advancing the Bid/Reducing the Ask			X							X					X		
	Quote Stuffing			X							X						X	
	Front-Running					X				X				X				
	Miner Extractable Value					X				X				X				
	Cornering/Squeezing			X						X				X				
	Wash Trading						X			X					X			
	Improper Matched Orders			X						X					X			
	Painting the Tape			X						X					X			
	Capping/Pegging			X						X				X				
	Churning					X				X								X
	Scalping (Investment Adviser)					X			X					X				
	Scalping ("Finfluencer")			X					X					X				
	Unlawful ICO/NFT Promotion by Celebrities				X				X					X				
	NFT Scalping (Bots)			X						X				X				
	Pinging			X							X				X			
	Ramping			X							X			X				

Table 2. Taxonomy of Violations in Digital Asset Markets

Category	Violation	Direct Economic Advantage		Specific Capabilities of the Violator Necessary					Specific Preconditions Necessary					Low Liquidity Advantageous		Asset Fungibility		
		Yes	No	Dominance (asset /market)	IT Infra-structure	Domi-nance (IT)	Collusion W. Other parties	No	Specific Event	LOB Environ-ment	Custody of Client Keys	Only DEX	No	Yes	No	FT	NFT	All
AF	Accounting Fraud (Operator)	X						X	X						X			X
	Accounting Fraud (Issuer)	X						X	X						X	X		
IF	Benchmark Manipulation in Stablecoins	X		X									X	X		X		
	Ponzi Scheme	X						X					X		X	X		
IT	Non-Disclosure of Insider Information	X						X					X		X			X
	Insider Trading	X						X					X		X			X
CA	Denial-of-Service Attack		X		X								X		X			X
	Crypto Wallet Fraud	X			X						X				X			X
	Smart Contract Exploitation	X			X								X		X			X
RA	Unregistered Broker	X						X					X		X			X
	Unregistered DAM	X						X					X		X			X
Scam	Fake DAM		X					X			X				X			X
	Fake NFTs		X					X					X		X		X	
	Rug Pull	X						X					X		X			X
	Misappropriation of Investors' Assets	X						X			X				X			X
	ICO Scam Promoted by Celebrities	X		X					X						X			X
Market Manipulation	Pump-and-Dump/Short-and-Distort		X					X					X	X				X
	Spoofing/Layering/Advancing the Bid/Reducing the Ask		X					X		X					X	X		
	Quote Stuffing		X		X					X					X	X		
	Front-Running	X						X	X					X		X		
	Miner Extractable Value	X				X						X		X		X		
	Cornering/Squeezing		X	X									X	X		X		
	Wash Trading		X					X					X	X				X
	Improper Matched Orders		X				X						X	X		X		
	Painting the Tape		X					X					X	X		X		
	Capping/Pegging		X					X	X					X		X		
	Churning	X						X					X		X	X		
	Scalping (Investment Adviser)	X						X					X	X				X
	Scalping ("Finfluencer")	X						X					X	X				X
	Unlawful ICO/NFT Promotion by Celebrities	X		X					X					X				X
	NFT Scalping (Bots)		X		X				X					X			X	
	Pinging		X					X		X					X	X		
	Ramping		X		X					X				X		X		

Table 2. Continued

Discussion and Conclusion

Since the existence of financial markets, dishonest and fraudulent market players have exploited others through manipulative and deceptive practices. The emergence of DAMs has led to additional violations of market integrity that have become common in recent years, such as those committed by coin issuers, hackers, and even market operators. However, there is currently no comprehensive and consistent taxonomy of these violations. This prevents effective fraud detection and limits the awareness of potential threats among DAM stakeholders. To address this gap, we employ an iterative taxonomy-building approach. We thereby analyze real-world DAM violations from 2020-2022, along with cases previously discussed in the literature (Siering et al. 2017). Through this process, we develop eight dimensions that facilitate the differentiation of fraudulent activities and highlight the essential information stakeholders should consider when identifying potential threats in DAMs.

By analyzing the distribution of the classification of violations in our taxonomy, we find that investors are the primary perpetrators of most violations in DAMs. However, most violations that are unique to DAMs are committed by issuers. Therefore, participants trading in these markets must pay particular attention to the issuers of the coins they trade. While operators are responsible for only a few types of violations, they have played a significant role in cases such as the FTX scandal, where their actions have had serious consequences. The means used to commit the violations are mainly action- or trade-based. Therefore, market operators as well as supervisory authorities should closely monitor the activities of market participants in terms of trading patterns. The taxonomy shows that the most common target of violations is the asset price, especially for violations that have already occurred in traditional financial markets. Furthermore, most violations directly benefit the violator in terms of economic advantage. Therefore, being able to identify the violators and their accounts is critical to potentially access, freeze, and reclaim their funds to prevent these cases from occurring in the first place. The taxonomy shows that most cases do not require specific capabilities of the violator. For DAM-specific cases like crypto wallet fraud or traditional cases like quote stuffing, however, an IT infrastructure is needed. Moreover, the lack of specific preconditions in most cases makes it difficult to develop countermeasures and take preventive steps in advance. The taxonomy indicates that less-liquid DAMs and digital assets are more vulnerable to violations, including pump-and-dump schemes. Investors should be cautious in these cases, as the consequences can be more severe than in traditional, more liquid assets such as stocks.

Based on a set of recently reported incidents in an out-of-sample period, we successfully evaluate the taxonomy and show how to classify new cases of violations. However, our taxonomy-building process also comes with limitations. The explanatory nature of the taxonomy could be increased by performing a cluster analysis on selected DAMs. While it is possible that some violations are not covered, the taxonomy aligns with the literature requirements and its robustness and extensibility serve to cover additional violations in the future. When comparing our taxonomy with existing classification schemes of financial market violations, we find that our taxonomy of violations in DAMs shares some aspects with Siering et al.'s (2017) taxonomy. However, it also includes new dimensions (e.g., network and IT-related capabilities of the violator) and characteristics (e.g., new violators such as the market operator), which are only applicable to violations in DAMs. Thereby, our taxonomy covers the DAM-related violations identified by Eigelshoven et al. (2021) and Scharfman (2023).

Our taxonomy contributes to the regulatory discussion and research on digital assets in multiple ways: First, the evidence of several studies shows the importance of understanding DAM violations for information systems research (Daian et al. 2020; La Morgia et al. 2023; Xia et al. 2021). An effective identification and mitigation of such violations is possible through the development of a taxonomy. By proposing a taxonomy of DAM violations, we are the first to develop such a systematic classification system, thereby contributing to a scarce research stream. The taxonomy serves to deepen the understanding of violations in DAMs by clearly separating different types of violations by eight dimensions. It can serve as a basis for researchers to develop information systems to detect DAM violations. Furthermore, the taxonomy also helps investors in assessing trading risks. Additionally, market operators can use the taxonomy as a decision support tool to assess which combination of characteristics is more prone to violations. Regulators benefit by gaining insights into DAM-specific challenges, which can enhance investor protection and improve the accountability of violators. In doing so, the proposed taxonomy assists in evaluating regulatory initiatives, such as MiCA, which does not address DAM-specific issues and instead largely replicates violations observed in traditional financial markets. This taxonomy can thus form the basis for future research in this

area. One potential research direction is the development of integrity measures that can quantify violations. A second area of future research is the design and implementation of decision support systems that can assist in the early detection of harmful trends in DAMs. Researchers could conduct a qualitative analysis of the violations identified in our study to assess their severity and assign weights to each case. Additionally, mapping the characteristics of violations to the characteristics of DAMs provides insights into which markets, such as CEXs or DEXs, are more vulnerable to certain types of violations. In this regard, future research may develop a taxonomy of DAMs that systematically identifies their key characteristics.

Acknowledgements

We acknowledge financial support from the Frankfurt Institute for Risk Management and Regulation.

References

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

Austin, J. 2017. "What Exactly is Market Integrity? An Analysis of One of the Core Objectives of Securities Regulation," *William and Mary Business Law Review* (8:2), pp. 2015-2240.

Beinke, J. H., Nguyen, D., and Teuteberg, F. 2018. "Towards a Business Model Taxonomy of Startups in the Finance Sector using Blockchain," in *Proceedings of the 39th International Conference on Information Systems (ICIS),* San Francisco, CA, USA.

Blaschke, M., Haki, K., Aier, S., and Winter, R. 2019. "Taxonomy of Digital Platforms: A Platform Architecture Perspective," in *Proceedings of the 14th International Conference on Wirtschaftsinformatik (WI),* Siegen, Germany.

Bouri, E., Kamal, E., and Kinateder, H. 2023. "FTX Collapse and Systemic Risk Spillovers from FTX Token to Major Cryptocurrencies," *Finance Research Letters* (56), p. 104099.

Chohan, U. W. 2021. "Non-Fungible Tokens: Blockchains, Scarcity, and Value," *Working Paper*.

Coindesk. 2023. "Coindesk," available at https://www.coindesk.com/.

Cong, L. W., Li, X., Tang, K., and Yang, Y. 2022. "Crypto Wash Trading," *NBER Working Paper*.

Corbet, S., Hou, Y. G., Hu, Y., Larkin, C., and Oxley, L. 2020. "Any Port in a Storm: Cryptocurrency Safe-Havens during the COVID-19 Pandemic," *Economics Letters* (194), p. 109377.

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," in *2020 IEEE Symposium on Security and Privacy,* San Francisco, CA, USA, pp. 910-927.

De, N. 2023. "John McAfee Indicted by DOJ on Money Laundering, Fraud Charges for Boosting ICOs," available at https://www.coindesk.com/markets/2021/03/05/john-mcafee-indicted-by-doj-on-money-laundering-fraud-charges-for-boosting-icos/.

Dupuis, D., Smith, D., and Gleason, K. 2023. "Old Frauds with a New Sauce: Digital Assets and Space Transition," *Journal of Financial Crime* (30:1), pp. 205-220.

Eickhoff, M., Muntermann, J., and Weinrich, T. 2017. "What Do Fintechs Actually Do? A Taxonomy of Fintech Business Models," in *Proceedings of the 38th International Conference on Information Systems (ICIS),* Seoul, South Korea.

Eigelshoven, F., Ullrich, A., and Parry, D. 2021. "Cryptocurrency Market Manipulation: A Systematic Literature Review," in *Proceedings of the 42nd International Conference on Information Systems (ICIS),* Austin, TX, USA.

European Commission. 2020. "Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA)," available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593.

Félez-Viñas, E., Johnson, L., and Putnins, T. J. 2022. "Insider Trading in Cryptocurrency Markets," *Working Paper*.

Fridgen, G., Regner, F., Schweizer, A., and Urbach, N. 2018. "Don't Slip on the ICO – A Taxonomy for a Blockchain-enabled Form of Crowdfunding," in *Proceedings of the 26th European Conference on Information Systems (ECIS),* Portsmouth, UK.

G7 Working Group on Stablecoins. 2019. "Investigating the Impact of Global Stablecoins," available at https://www.bis.org/cpmi/publ/d187.pdf.

Gorton, G. B., and Zhang, J. 2023. "Bank Runs During Crypto Winter," *Working Paper*.

Guo, H., and Yu, X. 2022. "A Survey on Blockchain Technology and its Security," *Blockchain: Research and Applications* (3:2), p. 100067.

Hart, O. D. 1977. "On the Profitability of Speculation," *The Quarterly Journal of Economics* (91:4), pp. 579-597.

Huang, X., Lin, J., and Wang, P. 2022. "Are Institutional Investors Marching into the Crypto Market?" *Economics Letters* (220), p. 110856.

Imerman, M. B., and Fabozzi, F. J. 2020. "Cashing in on Innovation: A Taxonomy of FinTech," *Journal of Asset Management* (21:3), pp. 167-177.

Kundisch, D., Muntermann, J., Oberländer, A. M., Rau, D., Röglinger, M., Schoormann, T., and Szopinski, D. 2022. "An Update for Taxonomy Designers: Methodological Guidance from Information Systems Research," *Business & Information Systems Engineering* (64:4), pp. 421-439.

La Morgia, M., Mei, A., Sassi, F., and Stefa, J. 2023. "The Doge of Wall Street: Analysis and Detection of Pump and Dump Cryptocurrency Manipulations," *ACM Transactions on Internet Technology* (23:1), pp. 1-28.

Lausen, J. 2019. "Regulating Initial Coin Offerings? A Taxonomy of Crypto-Assets," in *Proceedings of the 27th European Conference on Information Systems (ECIS),* Stockholm & Uppsala, Sweden.

Li, T., Shin, D., and Wang, B. 2018. "Cryptocurrency Pump-and-Dump Schemes," *Working Paper*.

Lin, I.-C., and Liao, T.-C. 2017. "A Survey of Blockchain Security Issues and Challenges," *International Journal of Network Security* (19:5), pp. 653-659.

Miller, G. A. 1956. "The Magical Number Seven, Plus or Minus Two: Some Limits on our Capacity for Processing Information," *Psychological Review* (63:2), pp. 81-97.

Mondo Visione. 2023. "SEC Files 13 Charges Against Binance Entities And Founder Changpeng Zhao," available at https://mondovisione.com/media-and-resources/news/sec-files-13-charges-against-binance-entities-and-founder-changpeng-zhao-charg?disablemobileredirect=true.

Nickerson, R. C., Varshney, U., and Muntermann, J. 2013. "A Method for Taxonomy Development and its Application in Information Systems," *European Journal of Information Systems* (22:3), pp. 336-359.

Oh, S. 2023. "Market Manipulation in NFT Markets," *Working Paper*.

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

Qin, K., Zhou, L., Livshits, B., and Gervais, A. 2021. "Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit," in *Financial Cryptography and Data Security*, N. Borisov and C. Diaz (eds.), Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 3-32.

Reuters. 2022. "Exclusive: At Least $1 Billion of Client Funds Missing at Failed Crypto Firm FTX," available at https://www.reuters.com/markets/currencies/exclusive-least-1-billion-client-funds-missing-failed-crypto-firm-ftx-sources-2022-11-12/.

Scharfman, J. A. 2023. *The Cryptocurrency and Digital Asset Fraud Casebook*, Cham: Springer International Publishing.

SEC. 2022. "SEC Charges Crypto Entrepreneur Justin Sun and His Companies for Fraud and Other Securities Law Violations," available at https://www.sec.gov/news/press-release/2023-59.

Siering, M., Clapham, B., Engel, O., and Gomber, P. 2017. "A Taxonomy of Financial Market Manipulations: Establishing Trust and Market Integrity in the Financialized Economy through Automated Fraud Detection," *Journal of Information Technology* (32:3), pp. 251-269.

TradingPlatforms. 2022. "Cryptocurrency Theft Global Value Rise 38% with $513 Million Stolen in 2020," available at https://tradingplatforms.com/uk/blog-uk/2021/03/02/cryptocurrency-theft-global-value-rise-38-with-513-million-stolen-in-2020/.

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

Vidal-Tomás, D., Briola, A., and Aste, T. 2023. "FTX's Downfall and Binance's Consolidation: The Fragility of Centralised Digital Finance," *Physica A: Statistical Mechanics and its Applications* (625), p. 129044.

Xia, P., Wang, H., Gao, B., Su, W., Yu, Z., Luo, X., Zhang, C., Xiao, X., and Xu, G. 2021. "Trade or Trick?" *Proceedings of the ACM on Measurement and Analysis of Computing Systems* (5:3), pp. 1-26.

Ziegler, C., and Welpe, I. M. 2022. "A Taxonomy of Decentralized Autonomous Organizations," in *Proceedings of the 43rd International Conference on Information Systems (ICIS),* Copenhagen, Denmark.