Risk analyses of the crypto-market: A literature review

Jean-Guillaume Dumas, Sonia Jimenez-Garces, Florentina Șoiman

Risk analyses of the crypto-market: A literature review[1]

Jean-Guillaume Dumas[a], Sonia Jimenez-Garces[b], Florentina Șoiman[a,b]

[Firstname.Lastname]@univ-grenoble-alpes.fr

[a] *Univ. Grenoble Alpes, UMR CNRS 5224, LJK, 38000 Grenoble, France*
[b] *Univ. Grenoble Alpes, Grenoble INP, CERAG, 38000 Grenoble France*

Abstract

This paper studies the literature on the vulnerabilities and risks of the crypto-market. Since their creation, crypto-assets have experienced remarkable market growth and performance, solidifying their position as an indispensable instrument within financial markets. The existing literature has often addressed the crypto-market risks independently based on their nature. Consequently, in this paper, we aim to provide a holistic analysis of the various risks that exist in the crypto-market. Notably, we focus on the financial and technological types of risk and emphasize their influence on price stability. Furthermore, to complete this study, we propose a conceptual metric to determine the likelihood of technological vulnerabilities triggering financial risks. Our contributions are twofold. First, we perform a cross-disciplinary literature review addressing financial and technological crypto-market risks together. Secondly, we show that these risks can become a trigger one for another.

Keywords: **Asset pricing, Risk assessment, Financial risks, Attacks, Bitcoin.**
JEL Codes: G10, G15, G19

[1] A former version of this paper was named "Blockchain technology and cryptomarket: vulnerabilities and risk assessment". This paper has been presented at the 12th International Multi-Conference on Complexity, Informatics and Cybernetics (IMCIC 2021) in Orlando, USA, and at Workshop Blockchains & Cryptomonnaies 2021 in Grenoble, France.

1. Introduction

Crypto-assets have gained the reputation of being the best-performing asset class, which is primarily due to their high volatility. While looking at the performance of various financial asset classes over the past decade (2011-2021), it becomes evident that crypto-assets secured their first place with an impressive annualized gain of 230.6%. The next best performers were the Nasdaq 100, yielding a return on investment (ROI) of 20%, and US Large Caps, with an ROI of 14% (Sriram, 2021). The remarkable growth of the crypto-market coincided perfectly with the longest bull market period in history, the 2010s, therefore establishing itself as an indispensable instrument in financial markets (Messamore, 2019; Sinclair, 2019). Simultaneously, we have witnessed the widespread adoption of Blockchain technology across various sectors of the economy, with a growing number of organizations expressing their enthusiasm and a keen interest in adopting it (Collomb and Sok, 2017). Furthermore, institutional investors like Grayscale and Blackrock are showing a growing interest in crypto-assets, highlighting their emergence as an intriguing investment asset class (Xu et al., 2022). Therefore we mention the need for research to address the challenges faced by market participants in the crypto-market and provide them with valuable insights and information.

In the crypto-market, while there's considerable potential, it has attracted attention primarily due to its vulnerabilities. The market's high volatility and frequent cyber-attacks are key drivers of concern. Numerous studies have explored these risks, some proposing solutions (Bonneau et al., 2015; Stewart et al., 2018; Ma et al., 2018; Goffard, 2019; Morganti et al., 2019; Drljevic et al., 2019; Patel, 2020), while others aim to raise awareness (Saad et al., 2019; Canh et al., 2019; Lemieux, 2016; Gazali et al., 2018; Lu, 2019). However, these studies often address risks in isolation, categorizing them by type, like technological or regulatory.

In the contemporary financial landscape, the growing reliance on advanced technology has given rise to cyber-risk as a systemic concern within financial markets (Bouveret, 2018). Researchers such as Bouveret (2018) and Hacibedel and Perez-Saiz (2023) discuss the high reliance on complex technologies and analyse the exposure to cyber-risks that comes with it. Furthermore, Corbet et al. (2020) conducted a study that demonstrated how 17 cyberattacks that occurred between 2017 and 2018 had a notable impact on the volatility among the top 8 crypto-assets. Similarly, Grobys (2021) explored the consequences of 29 cyber-attacks on Bitcoin shedding light on their effects on BTC and ETH returns. Caporale et al. (2021) conducted an extensive analysis revealing that a staggering 4693 cyber-attacks, spanning from 2015 to 2020 and targeting not only the crypto-market but also other sectors, triggered spillover and contagion effects among the top three crypto-assets. As it can be observed, there is a growing literature addressing the relationship between technological and financial risks. Our paper takes a systematic approach by delving into some of the key technological risks within the crypto-market. It also investigates their interconnectedness with financial risks. Notably, our study distinguishes itself from existing research by conducting a comprehensive analysis of various risk types, differentiating them based on their inherent characteristics, asset classification (e.g., cryptocurrency or token), technology classification (e.g., POW or POS), exposure factors, and resulting impact. This in-depth exploration allows us to discern which crypto-assets may be more susceptible to specific risks, identify the technological risk factors that instigate financial risks, and assess the magnitude of their influence.

This paper is a systematic literature review (SLR). Such reviews involve the systematic acquisition, organization, and evaluation of existing literature through structured procedures, such as for example content analyses (Donthu et al., 2021). In conducting this research, we use various types of information from both academic [2] and non-academic [3] publications. The selection of papers was performed by first taking into account the subject, crypto-market, and risk; afterward, we underwent a careful examination and selected only the publications that aligned with our research topic. In our search, we have used many keywords such as: crypto*, cryptocurrency, bitcoin, Blockchain, asset-pricing, financial, technological, risk, cyber-attack,

[2] Academic journals, academic theses.
[3] Websites, official reports issued by research or governmental organizations, magazines, etc.

vulnerability, literacy, and others. These keywords have been used in various ways, such as searches with two keywords or with a combination of two or more (i.e., search with 'crypto*'+'cyber-attack'+'price'). More details about SLR methodology and the data used are presented in Section 3.

The objective of this research is to review the existing literature on crypto-related risks and provide a comprehensive and cross-disciplinary risk analysis. Notably, we focus on the financial and technological types of risk and highlight their influence on price stability. Complementary to the risk analysis, we performed an assessment of the triggering elements behind the surveyed risks. The contributions derived from the literature review demonstrate that these risks can be interconnected, irrespective of their nature. Additionally, we follow the example of Benoit et al. (2017)'s literature review and perform a short data analysis which is displayed in the B attached to this paper; here, we show that bitcoin's price instability (financial risk) can be triggered by attacks targeting the crypto-market (technological vulnerability). This result is in line with our literature review conclusions.

This paper is organized as follows. Section 2 presents the theoretical background for this study. Section 3 introduces the research methodology and data. Section 4 comprises the risk analysis and the assessment of triggering elements. Section 5 discusses the results and concludes.

2. Theoretical background

2.1. Risk-return relationship

The valuation of assets is one of the most studied issues in finance. While searching for ways to determine the (theoretical) fair value of an asset, academicians proposed several models to price securities. Among the most well-known and widely used pricing models, we have the Capital Asset Pricing Model (CAPM) (Markowitz, 1952; Lintner, 1965; Mossin, 1966; Treynor, 1961; Sharpe, 1964; Black et al., 1972), Arbitrage Pricing Theory (APT) (Ross, 1976) and Fama-French multi-factor models (Fama and French, 1992; Carhart, 1997; Fama and French, 2015). In order to accurately price financial assets, these frameworks consider the risks incurred by holding a security and price it accordingly. A higher risk means a higher probability of significant positive (or negative) change in the expected return (Tobin, 1958), which means that investors may obtain a profit on their investment only by taking risk (Markowitz, 1952).

Extensive research has been conducted on cryptocurrencies, which are considered a distinct asset class from traditional securities (Bouri et al., 2017; Corbet et al., 2019; Jiang et al., 2022). A great share of studies examines the correlation between cryptocurrency prices and their underlying fundamental value (Biais et al., 2020; Athey et al., 2016; Zimmerman, 2020; Cong et al., 2021; Liu and Tsyvinski, 2021). While some works have suggested that bitcoin lacks a fundamental value and is purely speculative (Cheah and Fry, 2015; Kallinterakis and Wang, 2019), others argue that cryptocurrencies, as a whole, possess a fundamental value, albeit one that is challenging to ascertain (Dowd, 2014; Beigman et al., 2021).

Cryptocurrencies, a unique asset class by nature, present challenges in terms of pricing (Dyhrberg, 2016b; Corbet et al., 2019; Liu et al., 2022). Various methods have been employed to price cryptocurrencies, with the most common ones being the CAPM and multifactor models like Fama-French and Carhart. Studies have shown that multifactor models outperform the CAPM in predicting cryptocurrency returns due to their consideration of multiple systematic risk factors (Ciaian et al., 2016; Shen et al., 2020; Jia et al., 2022; Liu et al., 2022). Similar to traditional pricing frameworks for the stock market, the pricing of cryptocurrencies also accounts for non-diversifiable risk. The underlying assumption is that despite their independence from economic variables, cryptocurrency returns are influenced by systematic risks like traditional financial assets (Koutmos, 2020). However, it is important to note that cryptocurrency prices demonstrate limited correlation with factors related to stock markets and macroeconomic variables (Ciaian et al., 2016; Liu and Tsyvinski, 2021), and therefore, an appropriate pricing framework for cryptocurrencies should incorporate crypto-specific factors.

2.2. Investors' attitude towards risk

In addition to financial theory explaining how prices often deviate from their fair value, the behavioral theory points out that investors' behavior can influence the stock price (Williams, 1938; Blanchard and Watson, 1982). The study conducted by Bachelier (1900) was one of the earliest investigations into the behavior of security prices, characterizing it as random. Subsequently, Fama (1965a,b) built upon similar assumptions of randomness in stock price fluctuations and developed the Efficient Market Hypothesis (EMH). Fama argued that in an efficient market, security prices reflect all relevant information and thus provide a reliable estimate of intrinsic value. Furthermore, Fama highlighted the important role played by the investors (market participants) in the stability of price: *"In an uncertain world, the intrinsic value of a security can never be determined exactly. Thus, there is always room for disagreement among market participants concerning just what the intrinsic value of an individual security is, and such disagreement will give rise to discrepancies between actual prices and intrinsic values. In an efficient market, however, the actions of the many competing participants should cause the actual price of a security to wander randomly about its intrinsic value."* (p.76 Fama (1965b)).

Empirical evidence from several studies indicates that individuals with a higher propensity for risk are more likely to invest in stocks compared to those who are less risk-oriented (Clark-Murphy and Soutar, 2004; Wood and Zaichkowsky, 2004; Keller and Siegrist, 2006). The stock market offers potential opportunities for financial gains, but despite this, many individuals choose not to invest in stocks and instead allocate their funds to savings or real estate investments. According to the Prospect Theory model of risky decision-making developed by Kahneman and Tversky (1979) and Tversky and Kahneman (1992), this behavior is explained by the fact that most individuals exhibit risk aversion when there is a possibility of making gains. The perceived uncertainty surrounding future stock market developments contributes to the evaluation of potential gains as too uncertain, thus deterring many individuals from participating in stock market investments (Keller and Siegrist, 2006).

The behavior of investors in the crypto-market can be partially explained by Prospect Theory. Crypto investors often exhibit a tendency to follow the actions of others, driven by social proof and fear of missing out (Giudici et al., 2020). This herding behavior can lead to price momentum and increased market volatility as investors flock to popular trends or narratives (Bouri et al., 2019; King and Koutmos, 2021; Gazali et al., 2018). This behavior is driven by the loss aversion aspect of Prospect Theory, where individuals place more weight on losses than gains Kahneman and Tversky (1979). Gazali et al. (2018) examined the link between human behavior and the inclination to invest in the cryptocurrency market. Their findings revealed that several factors significantly influenced individuals' intention to invest or participate in the crypto-market. These factors included attitudes towards the crypto-market, social norms (where decisions were influenced by prevailing trends and a mentality such as *'if I lose, at least I am not alone'*), risk tolerance, and perceived benefits associated with the use of cryptocurrencies (Gazali et al., 2018).

2.3. Literature about the crypto-market risks

Over time, crypto-assets' popularity has grown significantly, making them increasingly attractive as investment assets for investors. Given the high volatility associated with such assets, investing in crypto-assets requires significant risk tolerance. Therefore, it is crucial for investors in the crypto-market to understand the factors influencing crypto-assets returns and the risks they should consider.

The emergence of Blockchain technology and the integration of crypto-assets into financial markets represent significant ongoing challenges for both academics and practitioners. Although Blockchain technology has garnered attention for its immense potential and innovative solutions, it has primarily gained fame due to its vulnerabilities. The high volatility of crypto-assets returns and the prevalence of cyber-attacks targeting the technology have emerged as significant factors driving the popularity of crypto-market. Among the existing research literature, several studies have addressed the crypto-market risks. Some to find solutions to the technological vulnerabilities (Bonneau et al., 2015; Stewart et al., 2018; Ma et al., 2018; Goffard, 2019; Chen et al., 2020; Drljevic et al., 2019; Patel, 2020), while others just to increase general awareness (Saad et al., 2019; Canh et al., 2019; Lemieux, 2016; Gazali et al., 2018; Lu, 2019). Within the

realm of financial research, the predominant focus regarding the crypto-market risks lies in the context of price modeling. Several research papers confirmed that crypto-assets exhibit a lack of correlation with traditional assets such as equities, currencies, and commodities markets. Furthermore, they also demonstrate indirect independence from global macroeconomic factors (Dyhrberg, 2016b; Bouri et al., 2017; Das and Kannadhasan, 2018). In their research, Wang et al. (2021) discovered that volatility, liquidity, and attention factors are highly relevant for predicting the returns of cryptocurrencies. Other risk factors capable of successfully predicting crypto-assets returns are momentum, market risk, size, and the network effect (Koutmos, 2018; Biais et al., 2019, 2020; Sockin and Xiong, 2023; Liu et al., 2020; Cong et al., 2021; Momtaz, 2021; Routledge and Zetlin-Jones, 2021; Pagnotta, 2022; Liu et al., 2022).

We contribute to the above-mentioned research on crypto-market risks by performing a literature review on this topic. Systematic literature reviews (SLRs) are commonly regarded as the most suitable approach for narrow or specialized research domains (Donthu et al., 2021). Given the relatively narrow focus of our study, we considered SLR as the most appropriate methodology for conducting the literature review. In this work, we will focus exclusively on crypto-assets' risks and choose to limit our review to the fields of finance and computer science. These two areas are selected based on three factors: (1) Crypto-assets are virtual assets relying on Blockchain technology; because of their technological nature, research on crypto-assets often covers their technological characteristics (e.g., mining difficulty). (2) While most of the research on crypto-assets comes from the field of finance, some of the main risks from the crypto-market are of a technological nature and therefore covered by computer science specialists. (3) From our knowledge, there are no systematic reviews of the financial and technological risks analyzed together. This systematic review aims to analyze and consolidate the body of knowledge from the two fields.

3. Methodology and Data

3.1. Systematic review methodology

This paper represents a systematic literature review (SLR) of the crypto-market risks. As a research methodology, a systematic review encompasses the methodical gathering, arrangement, and assessment of pre-existing literature via structured processes (e.g., content analyses), often carried out manually by scholars (Snyder, 2019; Donthu et al., 2021). At their most fundamental level, review papers encompass rigorous assessments of preexisting literature. These assessments may contain quantitative effects estimation as seen in meta-analyses, or may include qualitative analysis, as often observed in systematic reviews. Initially used in the field of medical sciences, Tranfield et al. (2003) proposed SLR methodology for its use in management-related literature reviews. A compelling rationale for this proposition is that systematic reviews possess the capability to synthesize research in a systematic, transparent, and reproducible manner. As a result, they provide practitioners and policymakers with a solid groundwork upon which to make well-informed decisions and undertake appropriate actions (Snyder, 2019). Compared to other disciplines like medicine and policy-oriented areas of social sciences, systematic reviews in the field of management are scarcer. This is mostly due to the prioritization of empirical contributions over reviews and syntheses, which has led to a field that is characterized by a large volume of fragmented and sometimes contested research (Briner and Denyer, 2012).

Since Blockchain's invention, the crypto-market has witnessed a rapid acceleration in research production, resulting in an increasingly fragmented and transdisciplinary body of knowledge. With its main application in finance, Blockchain technology revolutionizes several other fields, such as computer science, supply chain, health, etc. Consequently, when we look at Blockchain's existing research, this topic is covered by most of its domains of innovation, with dominance from the finance and computer science/engineering fields (Martínez et al., 2022). Our study reviews the multidisciplinary literature on crypto-related risks and provides a comprehensive risk analysis.

3.2. Data

The work includes the following electronic databases: Google Scholar, Web of Science (WoS), IEEE Xplore, Springer SpringerLink, Elsevier ScienceDirect, Online library Wiley, MDPI, Taylor & Francis,

Google search and other non-academic sources[4] (yield through Google searches).

The search for relevant papers was performed using several keywords, as defined below. The keywords were constructed based on the research domain (finance and computer science) and the defined research topic (cryptocurrencies risks). When a precise search was not possible because of the lack of an advanced search filter (e.g., Google Scholar), we included only the first 100 most relevant results.

The keywords used in our search are: crypto*, cryptocurrency, bitcoin, cryptoasset, Blockchain, risk, price, asset-pricing, financial, technological, cyber-attack, vulnerability, microstructure, investment, responsible, and literacy. These keywords have been used in various combinations, as shown in Table 1.

Table 1: **Keywords used in the search for relevant literature**

Nr.	Combinations of keywords
1	*(Blockchain) AND (asset-pricing)*
2	*(Blockchain) AND (cyber-attack)*
3	*(Blockchain) AND (financial) AND (risk)*
4	*(Blockchain) AND (literacy)*
5	*(Blockchain) AND (risk)*
6	*(Blockchain) AND (vulnerability)*
7	*(bitcoin) AND (financial) AND (risk)*
8	*(bitcoin) AND (technological) AND (risk)*
9	*(crypto*) AND (vulnerability)*
10	*(crypto*) AND (cyber-attack)*
11	*(crypto*) AND (microstructure)*
12	*(crypto*) AND (financial) AND (risk)*
13	*(crypto*) AND (technological) AND (risk)*
14	*(crypto*) AND (responsible) AND (investment)*
15	*(cryptoasset) AND (price)*
16	*(cryptocurrency) AND (risk)*
17	*(cryptocurrency) AND (literacy)*

3.2.1. Selection of papers

The selection of relevant papers for this work was divided into four phases:
Phase 1: The initial search was for papers and publications that appeared between 2009 and 2023.
Phase 2: We assessed and selected the papers based on their relevance to our research topic, cryptocurrencies-related risks, by analyzing the title and abstract.
Phase 3: All the duplicates have been removed.
Phase 4: The remaining results underwent a careful examination. We selected only the publications that aligned with our research topic as closely as possible. Several results were excluded at this stage due to their lack of specificity and real contribution.

In the initial manual screening, which was primarily based on titles and abstracts, we identified 1837 potentially relevant results (phase 2). After a thorough selection process, encompassing multiple phases, we ultimately included in our literature review 70 pertinent publications (phase 4). The selected papers are presented in the tables from Section A.

[4] hub.packtpub.com, www2.deloitte.com, money.cnn.com, Litecoinpool.org, Magoo.github.io, underscore.vc, www.buybitcoinworldwide.com, Crypto51.app, CryptoSlate.com, cointelegraph.com, FOXBusiness.com, AMF report (www.amf-france.org), Bitcoin.com, Blockchain.com, 99bitcoins.com, IMF report (www.imf.org).

4. Risks analysis and assessment

In this section, we perform a theoretical risk assessment of the crypto-market. The goals of this assessment are:

- To understand the vulnerabilities of the crypto-market and their possible consequences and impact;
- To offer a broad view of possible financial and technological risks for the investors from this market.

Before delving into our comprehensive analysis of the crypto-market risks, a preliminary step involved quantitative analysis of our 70 papers. This initial assessment relied on content analysis and co-citation data. Our primary objectives in conducting these preliminary evaluations were twofold: firstly, to discern the principal areas of interest within the included studies through keyword analysis, and secondly, to understand how these papers are referenced within the literature.

To synthesise the key research directions on our topic of study, Figures 1, 2 and 3 offer insights into the prevalent keywords, risks, and co-citation patterns within the selected literature collection. In Figure 1, we observe the most extensively studied risks, with volatility, market risk, illiquidity, regulatory risks, and cyber-attacks emerging prominently. These findings underscore the necessity for interdisciplinary research, given that the crypto-world is susceptible to various types of risks originating from diverse domains. Our keyword analysis, as illustrated in Figure 2, affirms the existence of multidisciplinary risks inherent in crypto-market research. Conversely, the co-citation map depicted in Figure 3 reveals a clustering of papers according to their respective domains. This highlights the prevalent trend in crypto-market research, where the majority of studies remain within their disciplinary area and may not comprehensively address the full spectrum of crypto-related risks. These important findings derived from our quantitative analysis reinforce our motivation to consolidate the body of knowledge from diverse fields and conduct a comprehensive multidisciplinary literature review on crypto-related risks.

Figure 1: **Content analysis**
Most common risks words come out from our selected 70 papers. The data has been obtained through text screening. The graph has been generated with www.wordclouds.com

In this risk assessment, we are going to investigate several technological and financial risks, and emphasise their impact on the crypto-assets price. Through our selection of technological risks, we try to cover different levels of exposure/vulnerability that crypto-assets inherited from Blockchain technology: consensus-level attacks, network-level attacks, cryptographic key threats, and smart contract threats. While the list is not exhaustive, we address the most common issues encountered by the investors and

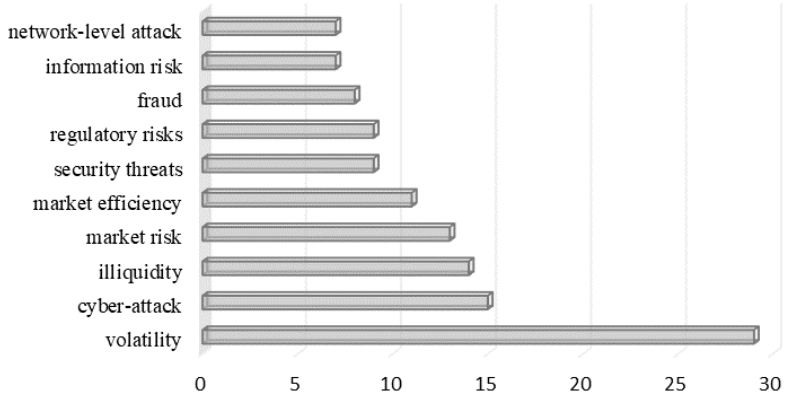

Figure 2: **Keywords analysis**
This graph shows the top 10 most common keywords and their frequency.

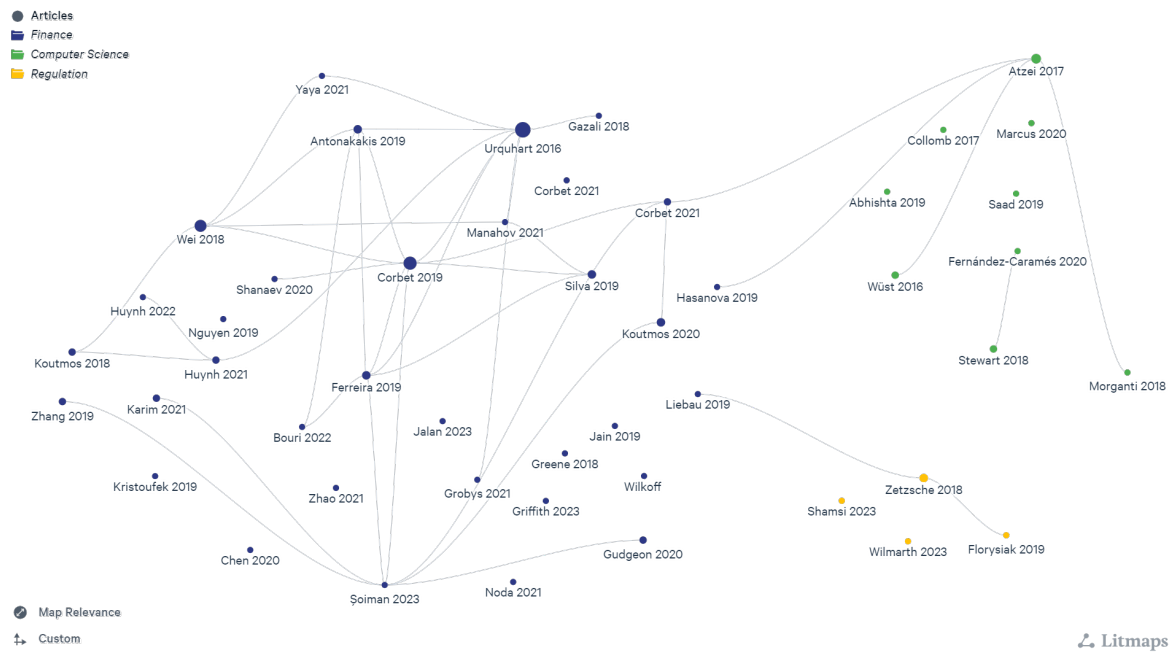

Figure 3: **Citation analysis**
Here we show the co-citation map among our selected papers, clustered by research field. The research field has been determined based on Journal name or paper topic. The graph was generated using Litmaps, which imposed restrictions, allowing only (49) academic sources to be included.

users from this market. Our focus on financial risks in this study primarily revolves around market microstructure and the factors influencing crypto-asset prices. From a crypto trader's standpoint, some of the most significant risks in the crypto-market include market risk, liquidity risk, and information asymmetry risk (Bouri et al., 2022). Examining our analysis from Figures 1, 2, and 3, it becomes evident that these risks have been addressed in the existing literature, albeit with limited multidisciplinary consideration. Motivated by these key findings, our analysis will delve into these financial risks and explore whether the technological vulnerabilities of the crypto-market can potentially trigger them.

4.1. Technological risks

To initiate our risk analysis, we begin by examining the technological risks prevalent in the crypto-market. These risks are organized based on their nature, namely consensus-level attacks, network-level attacks, cryptographic key attacks, and smart contract attacks. While there are numerous types of attacks not covered in this study, our aim is to encompass the most significant ones by considering their likelihood,

the potential exposure of the crypto-market to such incidents, and the resulting financial impact.

4.1.1. Consensus-level attacks

Consensus algorithms in Blockchain technology are code-based protocols designed to facilitate agreement processes within a network. These algorithms came as a solution to the "Byzantine General Problem", which concerns the failure to reach consensus due to faulty actors (Zhang et al., 2019). The most popular and widespread consensus algorithms in the crypto-market are the Proof of Work (PoW), Proof of Stake (PoS), and the Practical Byzantine Fault Tolerance (PBFT) protocols (see Table 2).

Table 2: **Comparison of most notable consensus mechanisms used in the Blockchain applications**

Proprieties	**PoW**	**PoS**	**PBFT**
Blockchain type	*Permissionless*	*Permissionless*	*Permissioned*
Fault Tolerance	*<50%(of computing power)*	*<50%(of stake)*	*<33%(of faulty nodes)*

The most noteworthy attacks at the consensus level, are:

Nothing at stake attack: This type of attack is associated with the Proof-of-Stake (PoS) protocol, where owners with low stakes attempt to devalue the crypto-asset. In the PoS system, control within the network is determined based on a user's wealth, often in combination with other factors such as coin age-based selection or random factors. Any PoS-based Blockchain can be susceptible to this type of attack, particularly during the initial stages when there are no significant imbalances in users' wealth and low-stake owners stand to lose relatively little (Morganti et al., 2019).

The majority attack, also known as a >50% attack: occurs when the consensus protocol of a blockchain is compromised, leading to a monopolistic system. This type of attack is considered a security issue due to its potential implications. Additionally, based on the target type, it can be divided into two variants: "the >50% (or 51%) computational power attack" [5] and "The 51% stake attack" [6] (Tuwiner, 2021; Blockchain.com, 2020).

Bitcoin has never experienced a successful majority attack. However, we cannot say the same about other coins: Feathercoin (June 2013), Bitcoin Gold (May 2018), Vertcoin (December 2018), Ethereum Classic (January 2019), and Bitcoin Cash (May 2019) (Beigel, 2019). The size of the Blockchain network influences the difficulty of executing an attack. Table 3 shows how expensive it is to perform a majority attack. These costs are computed taking into account the expenses incurred in the mining process, such as the electricity costs, or the network hash rate & the Nicehash cost expressed in BTC/per hour, which represents the necessary rented PC power. These values can change every minute, as the BTC price has a strong influence (Crypto51.app, 2023).

4.1.2. Network-level attack

Network-level attacks are widely considered difficult and expensive to perform (Koshik, 2019); however, they should never be regarded as impossible.

DDoS (Distributed Denial of Service: refers to an attack on the host, aiming to disrupt the normal operation process. For example, if a (host) Blockchain system is under attack, it can become unresponsive and unavailable. The system is usually compromised by being fed with misleading information or large

[5] An attack on the PoW protocol, involving the possession of more than 50% of the total mining power to manipulate and corrupt the network.

[6] An attack targeting the PoS protocol; it involves acquiring more than 50% of the total circulating supply of coins within the same network, with the aim of gaining monopolistic power and manipulating the system for personal profit. This type of attack is conceptually similar to a computational power attack, which targets the Proof-of-Work (PoW) protocol.

Table 3: **PoW 51% theoretical attack cost for the top 7 crypto-assets.**

System	Hash rate [7]	1 h attack estimated Cost
Bitcoin	*370,112 PH/s*	*$1,134,847*
Litecoin	*687 TH/s*	*$70,900*
EthereumClassic	*124 TH/s*	*$11,855)*
B. Cash	*1,413 PH/s*	*$4,332)*
Conflux	*9 TH/s*	*$2,105*
B. SV	*502 PH/s)*	*$1,539*
Zcash	*7 GH/s)*	*$3,414*

Values computed as per May 2023
Source: derived from Crypto51.app (2023)

amounts of data (Zhang et al., 2019). DDoS attacks can have a notable impact within the crypto-market, as they can target Blockchains [8], exchange and trading platforms, and even mining pools (Abhishta et al., 2019; Litecoinpool.org, 2020). These attacks are closely linked to the rise in value and popularity of crypto-assets (Crothers, 2021).

Some other notable examples of network-level attacks, worth mentioning are the Sybil attack[9] and the Eclipse attack[10]. From our knowledge, there is no Sybil or Eclipse attack successfully performed on the Blockchain technology, in practice, but researchers have made theoretical demonstrations for the Eclipse attacks on both PoW (Ether and Bitcoin) (Heilman et al., 2015; Marcus et al., 2010; Wüst and Gervais, 2016) and PoS networks (Zhang et al., 2019). Usually, the network-level attacks are planned so they can precede other assaults (Morganti et al., 2019).

4.1.3. Cryptographic key attacks

In Blockchain technology, cryptographic keys serve as a crucial component that grants users access to their funds through crypto wallets and play a critical role in facilitating transactional processes. In other words, anyone handling the keys can access the users' accounts and freely manage their funds. These keys are stored in crypto wallets; therefore, depending on the version of crypto wallet used (software, hardware, cloud, brain[11] or paper), the keys are more or less kept safely (hardware & paper - most secure, software, brain & cloudless secure). Having such a variety of key storage options gives attackers ideas to approach the wallets in different ways.

Wallet attack: These attacks are primarily driven by factors such as system hacking, software vulnerabilities, malware, or user error. Usually, the objective of a Wallet attack is to obtain or steal the private key, which allows the attacker to manipulate the system, execute unauthorized transactions, and transfer coins into the thief's wallet using the victim's private key. Among various types of crypto attacks, wallet attacks are not only prevalent but also highly detrimental, posing significant risks to users' funds and security [12]. This statement is also supported by the Blockchain Graveyard organization, as according to their thorough analysis of the incidents associated with Blockchain, more than half relate to wallet attacks (Magoo.github.io, 2023).

[8] The difficulty to execute an attack is influenced by the size of the Blockchain network. Private Blockchains are considered more exposed compared to public ones, as they usually grow around just 100 nodes. The adversary needs to control only 33% of the network to perform an attack, which is easier to achieve in small Blockchains (Saad et al., 2019).

[9] A user creates multiple identities and uses them to gain dominance and manipulate the Blockchain system.

[10] Similar to a Sybil attack, Eclipse misleads its victims such as they will see and believe a different truth than the rest of the network.

[11] A type of wallet that allows users to generate a key using a password. In terms of security, it is considered a weak option.

[12] In 2018, Coincheck's wallets were hacked and lost $530 million worth of NEM. This incident surpasses even the losses of the Mt. Gox case, being classified as the most significant theft in the crypto history (Shane, 2018).

Some other notable examples of attacks at this level are the Random number generator attack[13] and Quantum attacks[14].

4.1.4. Smart contract attacks

Smart contract attacks mainly refer to the manipulation of external data entered in the Blockchain through oracle technology and misleading the execution of the smart contract. The trigger represents information related to external events, which affects the contract's conditions. As such information is usually manually introduced, the execution of the system can be easily misled. Blockchain is an open-source technology, giving access to its full code. This is an opportunity for intruders, who may take advantage of this feature and exploit it with malevolent intentions. Concurrently, if the programming language used in the smart contract has weaknesses, this might also create an opportunity for hackers to initiate a successful attack (Hasanova et al., 2019; Atzei et al., 2017).

Re-entrancy attack, as a variant, refers to a malfunction in the smart contract protocol. During the attack, the hacker sends multiple requests to the system, for example, invoking the call function continuously until the gas supply ends. Overwhelmed by the avalanche of orders, the system will perform inaccurately (Hasanova et al., 2019).

A summary of all technological risks discussed in this section is presented in Table 4.

4.2. Financial risks

In this section, we examine various financial risks and evaluate the factors that contribute to their occurrence. Additionally, we introduce a conceptual metric aimed at highlighting the probability of technological risks transitioning into financial risks. The selection of financial risks is primarily centered around the market microstructure and the factors influencing the prices of crypto-assets. From the perspective of a crypto trader, among the most prominent risks in the crypto-market are the market risk, liquidity risk, and information asymmetry risk (Bouri et al., 2022).

Determining the likelihood: To gauge the likelihood of technological risks transitioning into financial risks, it is crucial to consider both the severity effect, such as financial losses and investment costs incurred, and the probability of occurrence of the triggering elements. By evaluating these factors, one can establish a clearer understanding of the potential transformation of technological risks into financial risks. Measurement plays an essential role in management. Up to this point, we have different tools to measure financial risks; however, things are not as simple when talking about the triggering elements. According to Kaplan and Norton (1992), if we cannot measure something, then we cannot properly manage it. Therefore, in this part of the assessment, we propose ways to measure the probability of technological vulnerabilities triggering financial risk.

4.2.1. Total market risk

This is the financial risk arising from high movement in market prices. The most used measure for appraising the total market risk of an asset is the volatility of its market returns. Following the traditional financial theory, the total market risk can be decomposed into the systematic risk and the specific one. If the crypto-market is vulnerable to a risk threatening the whole market, this could be a systematic risk. On the other hand, if we consider risks targeting a specific crypto-asset or type of Blockchain, then this

[13] Targets the weak security of the cryptographic keys, which is possible due to insufficient randomness used in their generation process and which makes them easy to predict; despite the common knowledge that the cryptographic keys are difficult to break, a combination of weak hashing algorithms and skilled hackers have led to such kind of incidents.

[14] In the context of Blockchain, attacks performed with quantum computers (QC) can break the cryptographic keys, corrupt the hashing functions and forge digital signatures. These attacks can have serious implications for the Blockchain network, implying theft of the users' funds, crypto wallets corruption, dominance over the network, and even possible recreation of the entire Blockchain. It is maybe a matter of time until we will have a QC powerful enough able to break the Blockchain technology (Fernandez-Carames and Fraga-Lamas, 2020; Stewart et al., 2018).

Table 4: **Summary of technological risks**

	Risk	*Consequences*	*Exposure*
Consensus-level attack	**Nothing at stake attack**	*Manipulates the system by entering invalid data* *Monopolized consensus process*	*Blockchains using PoS (over 400 cryptocurrencies) source: (CryptoSlate.com, 2022)*
	Majority attack	*Manipulates the system* *Monopolized consensus process* *Enters invalid data in the system* *Forks the Blockchain* *Performs other attacks (Eclipse, double spending, DoS)*	*Blockchains using PoW consensus (over 500 cryptocurrencies);* *Mining pools*
Network-level attack	**DDoS attack**	*Manipulates the system by entering invalid or big flow of data* *Disrupts the normal operation process* *Knocks out part of or the whole network*	*All Blockchains (small ones most exposed)* *Mining pools* *Exchange platforms*
	Sybil attack	*Manipulates the system* *Monopolized consensus process* *Enters invalid data in the system*	*Permissionless Blockchains*
	Eclipse attack	*Manipulates the system* *Monopolized consensus process* *Enters invalid data in the system*	*Permissionless Blockchains*
Cryptographic key threats	**Wallet attack**	*Steals the cryptographic keys* *Takes the control of the afferent funds* *Deters the security and trust of the users*	*All Blockchains*
	Random number generator attack	*Corrupts the cryptographic keys & crypto wallets*	*All Blockchains*
	Quantum attacks	*Corrupts the cryptographic keys & crypto wallets* *Forges hashing functions & digital signatures* *Rewrites Blockchain and manipulation of the network*	*All Blockchains*
Smart contract threats	**Reentrancy attack**	*Manipulates the network & spends unlimited*	*Blockchains supporting smart contracts (over 50 cryptocurrencies) Source:(CryptoSlate.com, 2022)*
	Smart contract attack	*Misleads the technology's application*	*Blockchains supporting smart contracts (over 50 cryptocurrencies) Source: (CryptoSlate.com, 2022)*

could be an example of specific risk [15].
From the previous list, if we take into consideration the (technological) risks' exposure and their potential impact, it becomes evident that several attacks have the capability to trigger financial risks. For instance, the majority attacks (exposure: almost half of the total crypto-market, plus the mining pools), Sybil and Eclipse attacks (target: Permissionless Blockchains - the most common and significant representatives of this market), DDoS attack, wallet attack, random number generator attack, and quantum attacks (target: all types of Blockchain) can be considered potential triggers for systematic risk. At the same time, if affecting just one type of Blockchain, one crypto-asset, or a few casualties, such as a mining pool/exchange platform, the same technological risk can trigger a specific one.

The influence of regulatory and cybersecurity-related events on crypto-assets prices is widely acknowledged (Corbet et al., 2019; Shanaev et al., 2020). Subsequently, such events influence the investors' behavior, impacting the crypto-market's volatility (Griffith and Clancey-Shang, 2023). It was also proved that crypto-assets suffer from contagion effects (herding behavior)(da Gama Silva et al., 2019). Shiller (2015) suggests that price explosivity in markets occurs due to psychological contagion, where news of price increases (decreases) spreads rapidly, leading to increased investor enthusiasm (panic). Bitcoin, and Ether have proven their strong influence over the price evolution of the whole crypto-market. In 2017, when bitcoin prices skyrocketed and crashed, the rest of the crypto-assets followed a similar trend (Antonakakis et al., 2019; Pereira and Ferreira, 2019). Karim et al. (2022) find important risk spillovers between cryptocurrencies and decentralized finance (DeFi) tokens and a strong disconnection with non-fungible tokens (NFTs). Şoiman et al. (2023) reveal that while the main driver for DeFi tokens returns is the cryptocurrency market, there is, in fact, a bidirectional causality relationship between BTC and DeFi prices. The strong power of influence among crypto-assets and the herding behavior present in this market may trigger systematic risk. Here, we have the perfect example of how an independent event, initially affecting one cryptocurrency (specific risk), can eventually transform into a systematic risk [16], impacting the whole market (Jain et al., 2019). It is well known that systematic risk can be triggered by various factors such as socio-political, economic, and any other market-related events. In the crypto-market, we can see that on top of the already existing factors, we also have technological vulnerabilities as a possible trigger. Under the hypothesis of traditional financial theory, the specific risk is diversifiable and is not priced by the market. On the opposite, investors require a risk premium, and, thus, higher returns for compensating the systematic risk they incur. Finally, in line with the findings of Koutmos (2020), we affirm that despite its distinctive technological nature and inherent vulnerabilities, the crypto-market, akin to the traditional financial market, remains susceptible to the similar financial risks, namely systematic and specific risks.

Likelihood: Cyber-attacks (technological risks) are considered one of the primary triggers for market risks in the crypto-market. According to the Blockchain-Graveyard, a database of crypto attacks, the most frequent and damaging are the ones on the wallet (about half of the total incidents), followed by code breaches and protocol issues (Magoo.github.io, 2023). In a cyclical manner, favorable financial conditions in the crypto-market can serve as motivation for attackers to carry out more cyber-attacks (Crothers, 2021). This implies that certain financial risks, such as volatility, can potentially act as triggers for cyber-attacks when prices are high. Given the prevalence of attacks in the crypto-market and the significant financial losses they often entail, we assert that the likelihood of technological risks triggering financial ones is high. Simultaneously, considering the persistently high volatility inherent in the crypto-market, we believe that there is a high likelihood that this financial risk will continue to attract hackers, thus serving as a trigger for technological risks such as attacks.

[15] Specific risk concerns isolated cases (one crypto-asset or a specific group, usually not dominating the market) and has fewer casualties than a systematic risk, which affects a large part of the market or the whole.

[16] This was possible through investors' behavior, which tend to associate bitcoin's image with the one of the whole market.

4.2.2. Information asymmetry risk

Information asymmetry risk refers to the imbalance of information spread among the market players. As per the Efficient Market Hypothesis (EMH) proposed by Fama (1965a,b), market efficiency is achieved when prices accurately incorporate all relevant information. Consequently, if the EMH was applicable to the crypto-market, it would imply that forecasting the price dynamics of crypto-assets is inherently unpredictable. Conceptually, Blockchain technology's decentralized and open-source nature makes it a valuable tool for reducing information asymmetry, ensuring complete transparency, and fostering trust. Over time, the crypto-market has witnessed a rise in the number of Blockchain-based assets (cryptocurrencies, ICO tokens, DeFi tokens, NFTs, etc.), resulting in increased complexity and posing greater challenges for investors. Furthermore, Bouri et al. (2022) show that acquiring a deep understanding of the functioning and structure of the crypto-market is essential to help traders identify potentially profitable crypto-assets.

During their early stages, Initial Coin Offerings (ICOs) played a significant role in addressing transparency and information asymmetry issues in the crypto-market. The complexity of ICOs' white paper [17], investors' lack of training and insufficient regulation led to various manipulation cases and financial losses on the investors' side. According to the existing literature (Pawczuk et al., 2019; Gazali et al., 2018; Underscore VC, 2018), most investors in this market lack the required capabilities to interpret the market's signals. The discrepancy between the traditional market and crypto-market pushes investors and users toward questionable sources of information, such as social media (Shahzad et al., 2022). Simultaneously, it has been observed that crypto investors tend to prioritize information based on easily interpretable criteria rather than focusing on factors such as quality and credibility (Florysiak and Schandlbauer, 2019). Shahzad et al. (2022) reveal that new investors in the crypto-market tend to rely more on public information rather than private information, which leads to the emergence of herding behavior.

In contrast to IPO prospectuses, Florysiak and Schandlbauer (2019) highlight that the information presented in ICO white papers is less standardized (due to inadequate regulation) and more challenging to comprehend due to the introduction of novel technological concepts and business models. Consequently, investors and professionals in the market often overlook this information. Additionally, the authors discuss that expert ratings of ICOs are uncorrelated with the content of the white paper, indicating that these ratings may not accurately reflect the project's quality or technological merits (Florysiak and Schandlbauer, 2019). As a result, it becomes more challenging to integrate accurate information into the market ecosystem. This phenomenon could potentially explain the persistent inefficiency of the crypto-market, despite the abundance of available information (Rui Chen and Chen, 2020; Gazali et al., 2018).

Likelihood: Among the most important factors responsible for information risk in the crypto-market, we have the lack of available information (e.g., missing white/yellow papers or inconsistent data in these documents), technological complexity, and the lack of technical knowledge of investors and users. The existence of a relatively weak regulatory framework creates opportunities for malicious actors to exploit the situation. One example of this is the issuance[18] of low-quality crypto-assets through ICOs or forks, accompanied by minimal or incomplete information (white papers) about these new crypto-assets. This deceptive practice can mislead market participants, enticing them to invest in or purchase questionable crypto-assets. A similar story is behind most fraudulent crypto-assets such as ICO tokens, forks, DeFi tokens, or NFTs (Al Shamsi et al., 2023; Corbet, 2021).

The buzz around the crypto world is also responsible for attracting more enthusiasts to this market. We believe that the investors present in this market are pretty various, such as institutional investors, retail investors, and crypto-enthusiasts. This fact is relevant as, for example, an institutional investor such as Blackrock might have access to more information and support in understanding crypto-market

[17] The white paper is a document describing the technology used and functioning of the ICO platform. It aims to convince the public that the new crypto-assets represent a good investment opportunity, mainly thanks to Blockchain innovation.

[18] In the crypto-market, anyone can be an entrepreneur and launch Blockchain-based businesses, without any pre-existing legal authorizations. Because of this, often, we do not know the identity of who is behind the Blockchain.

complexities. Afterward, depending on the proportion of retail investors and crypto-enthusiasts present in this market, this can lead to inefficient price discovery. An important body of literature tackles the informational inefficiency of the crypto-market (Urquhart, 2016; Kristoufek, 2019; Huynh, 2021; Gudgeon et al., 2020; Grobys and Huynh, 2021; Corbet et al., 2023), while some other papers reveal the presence of a time-varying efficiency (Chu et al., 2019; Noda, 2021; Yaya et al., 2021; Huynh, 2022). Taking into account the large number of crypto scams mainly due to Blockchain illiteracy and the resulting high financial losses suffered by the crypto investors, (Zetzsche et al., 2019; Liebau and Schueffel, 2019), we state that the likelihood of this risk is high.

4.2.3. Liquidity risk

A market is said to be liquid if an agent can rapidly make significant trades without creating an important change in the price (with a small market impact). Put differently, in a liquid market transactions will likely not change the price, but new information will be smoothly incorporated. On the other hand, an illiquid market, often associated with market inefficiency, tends to exhibit significant price volatility thereby increasing the likelihood of unfair pricing. Other possible consequences of illiquidity are a lower number of investors and reduced opportunities for transactions or trading. Liquidity risk can be categorized into three distinct classes: asset liquidity, exchange liquidity, and market liquidity. Asset liquidity pertains to the availability and interaction between sellers and buyers on the platform, more precisely, the availability of an asset on exchanges. Exchange liquidity relates to the interaction between market makers and takers, involving the supply of assets and orders. Market liquidity encompasses both asset liquidity and exchange liquidity (Crowell, 2020). Corbet et al. (2019) suggest that instances of illiquidity in the crypto-market often arise as a response to cyber-attacks or regulatory issues, being an indicator of investors' attitude toward risk. Jalan and Matkovskyy (2023) show that illiquidity in the crypto-market mimics the systemic risk pattern. Koutmos (2018) reveals that the most common factors explaining liquidity in the crypto-market are the price, trading volume, capitalization, fees, hash value (for PoW crypto-assets), and the size of the network.

It is important to mention the fact that liquidity is different from one crypto-asset to another (the well-established ones are more liquid) (Wei, 2018; Koutmos, 2020), as well as from one exchange platform to another. Despite the many benefits associated with liquidity, illiquid environments can also present some advantages, especially for the traders on this market, which can benefit from arbitrage opportunities and purchases at discounts (Crowell, 2020).

Likelihood: An important factor driving market liquidity for crypto-assets is the supply risk. Some examples of important supply risk triggers are the loss of cryptographic keys (without which there is no possibility to access the afferent funds), cyber-attacks[19], unclaimed rewards (Coinmetrics.com, 2019), the programmed limited supply coins and algorithmic stablecoins. Certain crypto-assets have a limited supply. For example, crypto-assets such as Bitcoin, Ripple, IOTA, Litecoin, and many others have a pre-established limited supply, while coins like Ethereum, Zcash, Monero, and others have no such limits. Following Rational Expectation Equilibrium theory (Lucas and Sargent, 1981), the higher the supply uncertainty, the less informative crypto-assets prices will be. In this case, market prices are less efficient, and liquidity risk could thus lead to an information risk (Collomb and Sok, 2017). A notable example of an algorithmic stablecoin issue resulting in market illiquidity is the case of the LUNA (Terra) DeFi platform. Terra is a Blockchain protocol and payment platform that specializes in facilitating the creation and utilization of algorithmic stablecoins, notably the UST (TerraUSD) stablecoin. The stability of UST was established through algorithms that interconnected its value with Luna. At the beginning of May 2022, a panic among the crypto traders lead to a huge sell-off of UST, resulting in additional minting of Luna and a subsequent increase in its circulating supply (Forbes.com, 2022). As a result of these events, the peg between UST and Luna eventually broke, thereby confirming the initial doubts expressed by experts regarding the

[19] After certain attacks (e.g., DAO Ethereum Classic 2016), the coins remained blocked in the intruder's account who is trying to avoid the public eye.

algorithm's ability to sustain stability between the two tokens. The meltdown of Luna had a significant and far-reaching impact on the overall cryptocurrency market, resulting in a loss of nearly $45 billion in market capitalization in just several days (Wilmarth, 2023; Forbes.com, 2022). Before its collapse, UST was recognized as the largest algorithmic stablecoin in the market.

Liquidity is an important characteristic of the market, influencing the investment costs and implicitly the desirability to trade. The crypto-market suffers from illiquidity, especially during extreme price movement periods (Manahov, 2021; Wilkoff and Yildiz, 2023). Examining this risk from the perspective of a limited supply asset such as bitcoin, it becomes apparent that liquidity risk is indeed significant. Nguyen et al. (2019) show that despite its high market capitalization, bitcoin can be vulnerable to competition from other crypto-assets, as investors tend to diversify their portfolios and compensate for their decrease in bitcoin holdings with altcoins. On the other hand, when considering the crypto-market as a whole, we assert that the likelihood of technological vulnerabilities triggering liquidity risk is moderate[20].

A summary of all financial risks discussed above is presented in Table 5.

Table 5: **Summary of financial risks**

Risk	Trigger	Influence / Consequences	Likelihood
Total market risk	*Cyber-attacks* *Technological risks* *Regulatory mismatches* *Human behavior* *Reputation*	• *Large loses for investors.* • *Sometimes volatility (financial risk) resulting in increased prices can trigger attacks (technological vulnerability)* • *Crypto assets trade with a risk premium relative to the risk investors may incur*	High
Information asymmetry risk	*Lack of available information (e.g., white/yellow papers, inconsistent data)* *Lack of knowledge/ understanding* *Reputation*	• *Financial losses for uninformed investors.* • *Assets trade at prices far from their fundamental value*	High
Liquidity risk	*Algorithmic limitations* *Supply risk*	• *Less investors* • *Less efficient market*	Moderate

5. Conclusion

In this paper, we perform a literature review of the crypto-market risks with a focus on the technological and financial types. We investigated several types of technological risks, while trying to cover different levels of exposure/vulnerability that crypto-assets inherited from Blockchain technology, such as consensus-level attacks, network-level attacks, cryptographic key threats, and smart contract threats. The selection of financial risks was primarily centered around the market microstructure and the factors influencing the prices of crypto-assets. From the perspective of a crypto trader, among the most prominent risks in the crypto-market we have the market risk, liquidity risk, and information asymmetry risk (Bouri et al., 2022). We, therefore, have addressed these financial risks in our analysis and investigated if the technological vulnerabilities of the crypto-market can trigger them.

[20]The rationale behind this conclusion is that, as mentioned before, the liquidity in this market is different from one crypto-asset to another, the well-established ones being most liquid (Koutmos, 2020; Wei, 2018), as well as from one exchange platform to another. That being said, traders who want to invest in smaller-cap crypto-assets, which are numerous in the market, might face liquidity challenges.

With our work, we first show that financial and technological risks can be related and that during specific market conditions, they can become a trigger one for another. Secondly, we offer a way to determine the likelihood of triggering financial risks through technological vulnerabilities. Here, we also emphasize the role played by financial behavior and Blockchain literacy in the stability of the crypto-market. Furthermore, to complete this study, we perform a short data analysis, demonstrating that bitcoin's performance can be disrupted by technological vulnerabilities characteristic of this market. This evidence reveals the implication of cybersecurity risks and poor regulation in the crypto-market stability. The empirical demonstration and its results are shown in the B attached to this paper. Our results support the general discussion from the literature review.

The implications of our findings are significant for regulators involved in the crypto-market, highlighting the need for increased efforts in regulating this sector. In line with (La Porta et al., 2002)'s statement *"legal protection of investors is an important determinant of the development of financial markets. Where laws are protective of outside investors and well-enforced, investors are willing to finance firms, and financial markets are both broader and more valuable."*, we believe that technological vulnerabilities could perhaps be perceived as less harmful if the investors from the crypto-market were better protected. This reveals the fact that the development and stability of this market depend not only on technological innovation but also on the legal system that supports it. Lastly, our research holds relevance for both researchers and (potential) investors who have an interest in the crypto-market. Despite its numerous intriguing features and innovative advantages, the crypto-market primarily gains recognition due to the exceptionally volatile prices of crypto-assets (Yi et al., 2018; Dyhrberg, 2016a; Baur and Dimpfl, 2021). Our findings bring new evidence that could help to better understand this market. At the same time, we think that supporting Blockchain literacy among investors would greatly improve the performance and reputation of the crypto-market as a whole.

Finally, we conclude this work with some research directions in an attempt to bridge a part of the existent literature gaps:

1. As a decentralized system by design, Blockchain technology is not managed by any central authority but by its own algorithm, *the code is law*. This leaves the duty of legal and international regulatory supervision in the hands of specialists from governments and industries. After more than 10 years since the launch of the crypto-market, we have the DLT Pilot (officially implemented in March 2023) regulatory framework addressing the use of DLT in the issuance, trading, and settlement of financial instruments. Another important work under development is the Markets in Crypto-Assets (MiCA) EU framework aiming to create legal certainty and one harmonized crypto-market. Considering that some of the vulnerabilities examined in this literature review could have been mitigated with appropriate regulations, we believe that further exploration of this topic is necessary, particularly through cross-disciplinary research.
2. There is a growing emphasis on the ethical dimension within the realm of finance. This is exemplified by the emergence of concepts such as socially responsible investing (SRI) or 'ethical investing.' That being said, ethical investors base their investment decisions on their moral convictions and want their assets to have a positive impact on our planet, society, and people (Keller and Siegrist, 2006). Frequently regarded as a concern for environmental sustainability, crypto-assets that utilize the Proof-of-Work (PoW) algorithm consume significant amounts of energy in order to provide enhanced security measures. In an effort to balance its potential upside against its inherent risks, environmental, social and governance (ESG) ratings have been created for crypto-assets [21]. While we are still far from a green crypto-market, we think this issue could be alleviated with a joint effort from specialists in computer science, regulation, and finance field. Consequently, we state that this subject needs further attention from both professionals and researchers interested in the crypto-market.
3. Despite the growing number of empirical papers about the crypto-market, we still lack theory development in this field. With our study, we show that using the existing finance theories is insufficient

[21] See https://www.greencryptoresearch.com/.

if the technological characteristics of this market are not taken into consideration. Therefore, there is a need for more cross-disciplinary research that will take into account the important functions and implications of crypto-assets and their underlying technology (finance, regulation, cybersecurity, management, etc.).

6. CRediT authorship contribution statement

Florentina Șoiman: Conceptualization, Methodology, Writing, Data extraction, and Analysis.

Jean-Guillaume Dumas: Supervision, Reviewing, and Editing.

Sonia Jimenez-Garces: Supervision, Reviewing, and Editing.

A. Appendix - Literature data

The comprehensive compilation of all risk-related papers utilized in this literature review focused on the crypto-market.

Citations	Publication Title	Year	Publication source / Journal
Abhishta et al. (2019)	Impact of Successful DDoS Attacks on a Major Crypto-Currency Exchange	2019	Proc. - 27th Euromicro Int. Conf. Parallel, Distrib. Network-Based Process. PDP 2019
Al Shamsi et al. (2023)	Space transition and the vulnerabilities of the NFT market to financial crime	2023	Journal of Financial Crime
Antonakakis et al. (2019)	Cryptocurrency market contagion: Market uncertainty, market complexity, and dynamic portfolios	2019	J. Int. Financ. Mark. Institutions Money
Atzei et al. (2017)	A survey of attacks on Ethereum smart contracts (SoK)	2017	Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)
Beigel (2019)	51% Attack Explained Simply	2019	https://99bitcoins.com
Bitcoin.com (2020)	Onchain Data Shows Rising Bitcoin Whale Index Surpassing 4-Year High	2020	Bitcoin.com
Blockchain.com (2020)	Bitcoin Hashrate distribution among mining farms	2020	Blockchain.com
Bouri et al. (2022)	Microstructure noise and idiosyncratic volatility anomalies in cryptocurrencies	2022	Annals of Operations Research
Bouveret (2018)	Cyber risk for the financial sector: A framework for quantitative assessment	2018	IMF report
Chu et al. (2019)	The adaptive market hypothesis in the high frequency cryptocurrency market	2019	Int. Rev. Financ. Anal.
CoinGuides.org (2020)	HashPower Calculator - Convert Hash to kH/s to MH/s to GH/s to TH/s to PH/s	2020	CoinGuides.org
Coinmetrics.com (2019)	Coin Metrics' State of the Network: Issue 26 - Coin Metrics' State of the Network	2019	Coinmetrics.com
Collomb and Sok (2017)	Blockchain et autre registres distribues: quel avenir pour les marches financiers?	2016	AMF report
Corbet et al. (2019)	Cryptocurrencies as a financial asset: A systematic analysis	2019	Int. Rev. Financ. Anal.
Corbet (2021)	Understanding cryptocurrency fraud: The challenges and headwinds to regulate digital currencies	2021	Handbooks in Alternative Investments
Corbet et al. (2023)	Are DeFi tokens a separate asset class from conventional cryptocurrencies?	2023	Annals of Operations Research
Crothers (2021)	As Bitcoin price surged, it fueled rise in cyberattacks, researchers say	2021	FOXBusiness
Crowell (2020)	Crypto Exchange Liquidity, Explained	2020	https://cointelegraph.com
Crypto51.app (2023)	Theoretical cost of a 51% Attack for Different Cryptocurrencies	2020	Crypto51.app
CryptoSlate.com (2022)	Token Cryptocurrencies	2020	CryptoSlate.com
da Gama Silva et al. (2019)	Herding behavior and contagion in the cryptocurrency market	2019	J. Behav. Exp. Financ.
Fernandez-Carames and Fraga-Lamas (2020)	Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks	2020	IEEE Access
Florysiak and Schandlbauer (2019)	The information content of ICO White Papers	2018	SSRN
Forbes.com (2022)	What Really Happened To LUNA Crypto?	2022	Forbes.com
Gazali et al. (2018)	Exploring the intention to invest in cryptocurrency: The case of bitcoin	2018	Proc. - Int. Conf. Inf. Commun. Technol. Muslim World 2018, ICT4M 2018
Greene and McDowall (2018)	Liquidity Or Leakage Plumbing Problems With Cryptocurrencies	2018	Cardano Foundation report
Griffith and Clancey-Shang (2023)	Cryptocurrency regulation and market quality	2023	Journal of International Financial Markets, Institutions and Money
Grobys and Huynh (2021)	When Tether Says "JUMP!" Bitcoin Asks "How Low?"	2022	Finance Research Letters
Gudgeon et al. (2020)	DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency	2020	2020 Crypto Val. Conf. Blockchain Technol. CVCBT 2020
Hacibedel and Perez-Saiz (2023)	Assessing Macrofinancial Risks from Crypto Assets	2023	IMF report
Hasanova et al. (2019)	A survey on blockchain cybersecurity vulnerabilities and possible countermeasures	2019	Int. J. Netw. Manag.
Heilman et al. (2015)	Eclipse Attacks on Bitcoin's Peer-to-Peer Network	2015	SEC'15 Proc. 24th USENIX Conf. Secur. Symp.
Huynh (2021)	Does bitcoin react to Trump's tweets?	2021	Journal of Behavioral and Experimental Finance
Huynh (2022)	When Elon Musk changes his tone, does bitcoin adjust its tune?	2022	Computational Economics
Iwamura et al. (2019)	Can we stabilize the price of a cryptocurrency? Understanding the design of bitcoin and its potential to compete with central bank money	2019	Hitotsubashi J. Econ.

Citations	Publication Title	Year	Publication source / Journal
Jain et al. (2019)	Insights from bitcoin trading	2019	Financ. Manag.
Jalan and Matkovskyy (2023)	Systemic risks in the cryptocurrency market: Evidence from the FTX collapse	2023	Finance Research Letters
Karim et al. (2022)	Examining the Interrelatedness of NFT's, DeFi Tokens and Cryptocurrencies	2022	Financ. Res. Lett.
Koshik (2019)	What Blockchain developers learn from Eclipse Attacks in bitcoin network	2019	https://hub.packtpub.com
Koutmos (2018)	Liquidity uncertainty and Bitcoin's market microstructure	2018	Econ. Lett.
Koutmos (2020)	Market risk and Bitcoin returns	2020	Ann. Oper. Res.
Kristoufek (2019)	Is the Bitcoin price dynamics economically reasonable? Evidence from fundamental laws	2019	Phys. A Stat. Mech. its Appl.
Liebau and Schueffel (2019)	Crypto-Currencies and ICOs: Are They Scams? An Empirical Study	2019	SSRN
Litecoinpool.org (2020)	Hash Rate Distribution — litecoinpool.org	2020	Litecoinpool.org
Magoo.github.io (2023)	Blockchain Graveyard	2020	Magoo.github.io
Manahov (2021)	Cryptocurrency liquidity during extreme price movements: is there a problem with virtual money?	2020	Quant. Financ.
Marcus et al. (2010)	Low-resource eclipse attacks on Ethereum's peer-to-peer network	2018	Cryptol. Rep.
Morganti et al. (2019)	Risk Assessment of Blockchain Technology	2019	Proc. - 8th Latin-American Symp. Dependable Comput. LADC 2018
Nguyen et al. (2019)	Bitcoin return: Impacts from the introduction of new altcoins	2019	Res. Int. Bus. Financ.
Noda (2021)	On the Evolution of Cryptocurrency Market Efficiency	2021	Appl. Econ. Lett.
Pawczuk et al. (2019)	Deloitte's 2019 Global Blockchain Survey	2019	https://www2.deloitte.com
Pereira and Ferreira (2019)	Contagion Effect in Cryptocurrency Market	2019	J. Risk Financ. Manag.
Rui Chen and Chen (2020)	A 2020 perspective on "Information asymmetry in initial coin offerings (ICOs) Investigating the effects of multiple channel signals"	2020	Electron. Commer. Res. Appl.
Saad et al. (2019)	Exploring the attack surface of blockchain: A systematic overview	2019	IEEE Commun. Surv. Tutorials
Shahzad et al. (2022)	Price explosiveness in cryptocurrencies and Elon Musk's tweets	2022	Finance Research Letters
Shanaev et al. (2020)	Taming the blockchain beast? Regulatory implications for the cryptocurrency Market	2020	Res. Int. Bus. Financ.
Shane (2018)	Coincheck: $530M cryptocurrency heist may be biggest ever	2018	https://money.cnn.com/
Şoiman et al. (2023)	What drives DeFi market returns?	2023	Journal of International Financial Markets, Institutions and Money
Stewart et al. (2018)	Committing to quantum resistance: A slow defense for Bitcoin against a fast quantum computing attack	2018	R. Soc. Open Sci.
Tuwiner (2021)	Bitcoin Mining Pools	2021	www.buybitcoinworldwide.com
Underscore VC (2018)	Future of Blockchain Survey and Results	2018	https://underscore.vc
Urquhart (2016)	The inefficiency of Bitcoin	2016	Econ. Lett.
Wei (2018)	Liquidity and market efficiency in cryptocurrencies	2018	Econ. Lett.
Wilkoff and Yildiz (2023)	The behavior and determinants of illiquidity in the non-fungible tokens (NFTs) market	2023	Global Finance Journal
Wilmarth (2023)	We Must Protect Investors and Our Banking System from the Crypto Industry	2023	GWU Legal Studies Research Paper
Wüst and Gervais (2016)	Ethereum Eclipse Attacks	2016	ETH Zurich Research Collection
Yaya et al. (2021)	Market efficiency and volatility persistence of cryptocurrency during pre- and post-crash periods of Bitcoin Evidence based on fractional integratio	2021	Int. J. Financ. Econ.
Zetzsche et al. (2019)	The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators	2019	Harvard Int. Law J.
Zhang et al. (2019)	Cryptocurrency, confirmatory bias and news readability – evidence from the largest Chinese cryptocurrency exchange	2019	Account. Financ.
Zhao and Zhang (2021)	Financial literacy or investment experience: which is more influential in cryptocurrency investment?	2021	Int. J. Bank Mark.

B. Appendix - Empirical demonstration

To complete the literature review, we assess if bitcoin's volatility is affected by events targeting the crypto-market. Some preliminary work on this problem has already been done by Corbet et al. (2020); Caporale et al. (2021); Grobys (2021). Corbet et al. (2020) proved that (17) hackings that took place between 2017 and 2018 had affected the volatility and cross-correlation for the top 8 crypto-assets, while Grobys (2021) showed how the (29) cyber-attacks performed on bitcoin during the 2013–2017 period affected BTC and ETH returns. Caporale et al. (2021) demonstrated how (4693) cyber-attacks targeting not only the crypto-market and happening between 2015 to 2020 created spillovers and contagion effects among the top three crypto-assets.

In our analysis, we are using a sample of (53) events, which cover both the early times of bitcoin (2011-2013) as well as the hype period in 2018. Corbet et al. (2019) showed that among many factors, news related to cyber-attacks have an important impact on the price movement of crypto-assets. As of January 2022, the amounts lost during our events (2011-2018) correspond to a 39 billion Eur (945,066 BTC) monetary equivalent. Given the extent of the losses incurred, it would be interesting to investigate if they impact the market. Therefore, in addition to what was already shown, more specifically, that cyber-attacks events impact the price of crypto-assets, we want to take it a little further and see if the market is sensitive to the amounts lost.

This data analysis is an illustration meant to complement our previously performed literature review. In accordance with the literature and with the aim to answer our research question: *'Can financial risks be triggered by technological vulnerabilities*[22] *of Blockchain technology?'*, we establish the following research hypotheses:

H1:Bitcoin's volatility is positively linked to the number of events targeting the crypto-market.
H2: Bitcoin's volatility is positively linked to the amounts lost due to these events targeting the crypto-market.

Similar to Corbet et al. (2020); Aliu et al. (2020); Akyildirim et al. (2020) and others, we retrieved the bitcoin prices from the Thomson Reuters Eikon database, while the list of events targeting bitcoin has been taken from Biais et al. (2020). In total, our dataset comprises 53 events (see table 6), and the historical price data spans from August 2011 to September 2021.

In order to verify whether technological events have an influence on the risk of crypto-assets, we investigate the relationship between bitcoin's volatility and the attacks on bitcoin. We check for the relationship between the volatility and the number of events, as well as the relationship between volatility and the amounts (in terms of bitcoin) lost as a consequence of these events.

In the following section, we are going to compute volatility using the standard deviation method. Our choice is justified by the scope of this analysis: to demonstrate that there is a relationship between bitcoin's volatility and our events. It is important to mention that for all our computations, our variables have been aggregated on a monthly basis. Table 7 displays the descriptive statistics of all variables used.

The rationale behind choosing these events as proof of technological vulnerability is the following: most of them are attacks that show the vulnerability of this technology. Some events may represent the consequence of malevolent actions (e.g., FBI seizes dark-net operations) that were accomplished thanks to the distinctive characteristics of this technology and which eventually represent one of the vulnerabilities/drawbacks of the crypto-market. By distinctive characteristics of this market, we mean:

[22] 83% of the events considered represent attacks, while the rest of 13% are malevolent actions that were possible thanks to Blockchain's unique features; more details are provided in the next part.

- Crypto-assets are built on open-source software code, which means that they exist and operate just in the online environment. As a consequence of their virtual nature, crypto-assets are often the target of cyber-attacks, which try to exploit any possible vulnerability of this technology.
- Crypto-assets' users need cryptographic keys in order to access their funds or to place transactions. These keys can easily become the source of attacks when they are not kept safely or if the (key) code is easy to break.
- The identity protection (anonymity) offered by Blockchain technology attracted many enthusiasts; however, this feature makes it almost impossible to catch hackers /thieves.
- The insufficient regulation and incertitude around the crypto-asset world made them the perfect tool to transact in black markets; these markets are also the few places accepting crypto-assets as payment.
- The complicated nature of this technology and Blockchain illiteracy. The lack of proper understanding of how the crypto-world works was exploited in many forms, to trick the users and steal their coins. An example would be the many scams performed by early crypto-exchange platforms, such as Mt Gox.
- Blockchain's transactions are immutable, implying that in case of a cyber-attack, it is impossible to reverse (fraudulent) transactions in an attempt to recuperate the stolen funds. This feature, together with the anonymity, may incite malevolent actors to execute their plans.

For our data analysis, we compute the monthly standard deviation of bitcoin's returns as:

$$\sigma = \sqrt{\frac{(R_i - \mu)^2}{n}} \tag{1}$$

Where R is the bitcoin's returns, μ is the average return, and n is the number of days of the window considered.

Accordingly, with our hypotheses, we perform two correlation tests using the Pearson test and Spearman's rank correlation. We want to measure the relationship degree between volatility and the number of events, as well as the relationship between volatility and the amounts lost during these events. Pearson, also known as a parametric correlation test, is one of the most common methods to assess the degree of relationship between two linearly related variables (Pearson, 1932). Spearman rho (a non-parametric test) measures the degree of association between two variables (Spearman, 1904). Both tests confirmed that bitcoin's volatility is correlated (uncorrelated) with the number of events (the amounts lost during these events). The results are in the bellow table 8.

Furthermore, we want to check the relationship between bitcoin's volatility and the amounts lost and number of events together. In order to make this check, we perform the following linear regression:

$$\sigma_t = \alpha + \beta_1 * EVENT_{number} + \beta_2 * EVENT_{amount} + \epsilon_t \tag{2}$$

Where $EVENT_{number}$ is the variable representing the monthly volume of events targeting bitcoin, and $EVENT_{amount}$ is the monthly amounts lost, in bitcoins, due to these events.

Our regression checks if there is a relationship between the monthly volatility of bitcoin and the monthly number of events with their respective losses. For the number of events, we obtain a β_1 of 0.193 with a p-value equal to 0.026. Meanwhile, for the losses incurred during these events, we obtain a β_2 of -7.589e-8 and a p-value equal to 0.832. Therefore, we conclude that our sample data provided enough evidence to show a relationship between the monthly volatility of bitcoin and the number of events targeting it. Concurrently, the results prove that there is no relationship between bitcoin volatility values and the amounts lost due to events. Detailed results are shown in Table 9.

Our analysis shows that the volatility of bitcoin is not influenced by the financial losses incurred but rather by the number of attacks or other malevolent events targeting this market. This result, while in

line with the existing literature (Corbet et al., 2020; Caporale et al., 2021; Grobys, 2021; An et al., 2021), proves that participants from the crypto-market are more sensitive to the number of cyber-attacks than to the magnitude of financial losses. A way to justify this would be to analyze the discrepancy between the users' expectations versus reality. Blockchain technology was created to offer a more secure and transparent alternative to the existing payment tools. However, that does not make it immune to cyber-attacks, nor an absolutely secure tool. On the same idea, An et al. (2021) has confirmed that cyber risks are negatively associated with crypto-assets' success, damaging their reputation and investors' trust.

To explore the possibility that individuals may revise their beliefs in response to an increase in the number of cyberattacks, we formulated a hypothesis. To examine bitcoin's reaction to cyberattack events, we conducted tests incorporating the squared terms of these events. In order to make this check, we perform the following linear regressions:

$$\sigma_t = \alpha + \beta_1 * EVENT_{number} + \beta_2 * EVENT^2_{number} + \epsilon_t \tag{3}$$

$$\sigma_t = \alpha + \beta_1 * EVENT_{amount} + \beta_2 * EVENT^2_{amount} + \epsilon_t \tag{4}$$

Our results are reported in Tables 10 and 11 and show that there is no quadratic relationship between monthly BTC volatility and the number of events or losses incurred.

In our literature review, we investigated several types of technological and financial risks and showed that these risks can be related and that during specific market conditions, they can become a trigger one for another. In this empirical demonstration, we show that bitcoin's price instability (financial risk) can be triggered by attacks targeting the crypto-market (technological vulnerability). The findings derived from the empirical demonstration align with the conclusions drawn from the literature review.

References

Abhishta, A., Joosten, R., Dragomiretskiy, S., Nieuwenhuis, L.J., 2019. Impact of Successful DDoS Attacks on a Major Crypto-Currency Exchange. Proc. - 27th Euromicro Int. Conf. Parallel, Distrib. Network-Based Process. PDP 2019 , 379–384doi:10.1109/EMPDP.2019.8671642.

Akyildirim, E., Corbet, S., Katsiampa, P., Kellard, N., Sensoy, A., 2020. The development of Bitcoin futures: Exploring the interactions between cryptocurrency derivatives. Financ. Res. Lett. 34, 101234. doi:10.1016/J.FRL.2019.07.007.

Al Shamsi, M., Smith, D., Gleason, K., 2023. Space transition and the vulnerabilities of the nft market to financial crime. Journal of Financial Crime .

Aliu, F., Nuhiu, A., Krasniqi, B.A., Jusufi, G., 2020. Modeling the optimal diversification opportunities: the case of crypto portfolios and equity portfolios. Stud. Econ. Financ. 38, 50–66. doi:10.1108/SEF-07-2020-0282.

An, J., Duan, T., Hou, W., Liu, X., 2021. Cyber risks and initial coin offerings: Evidence from the world. Financ. Res. Lett. 41, 101858. doi:10.1016/J.FRL.2020.101858.

Antonakakis, N., Chatziantoniou, I., Gabauer, D., 2019. Cryptocurrency market contagion: Market uncertainty, market complexity, and dynamic portfolios. J. Int. Financ. Mark. Institutions Money 61, 37–51. doi:10.1016/j.intfin.2019.02.003.

Athey, S., Parashkevov, I., Sarukkai, V., Xia, J., 2016. Bitcoin Pricing, Adoption, and Usage: Theory and Evidence.

Atzei, N., Bartoletti, M., Cimoli, T., 2017. A survey of attacks on Ethereum smart contracts (SoK). Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics) 10204 LNCS, 164–186. doi:10.1007/978-3-662-54455-6_8.

Bachelier, L., 1900. Théorie de la spéculation. Ann. Sci. l' École Norm. Supérieure 17, 21–86.

Baur, D.G., Dimpfl, T., 2021. The volatility of Bitcoin and its role as a medium of exchange and a store of value. Empir. Econ. 61, 2663–2683. doi:10.1007/S00181-020-01990-5/FIGURES/9.

Beigel, O., 2019. 51% Attack Explained Simply. URL: https://99bitcoins.com/51-percent-attack/.

Beigman, E., Brennan, G., Hsieh, S.F., Sannella, A.J., 2021. Dynamic Principal Market Determination: Fair Value Measurement of Cryptocurrency:. J. Accounting, Audit. Financ. doi:10.1177/0148558X211004134.

Benoit, S., Colliard, J.E., Hurlin, C., Pérignon, C., 2017. Where the Risks Lie: A Survey on Systemic Risk. Rev. Financ. 21, 109–152. doi:10.1093/ROF/RFW026.

Biais, B., Bisière, C., Bouvard, M., Casamatta, C., 2019. The Blockchain Folk Theorem. Rev. Financ. Stud. doi:10.1093/rfs/hhy095.

Biais, B., Bisiere, C., Bouvard, M., Casamatta, C., Menkveld, A.J., 2020. Equilibrium Bitcoin Pricing. J. Finance doi:10.2139/ssrn.3261063.

Bitcoin.com, 2020. Onchain Data Shows Rising Bitcoin Whale Index Surpassing 4-Year High . URL: https://news.bitcoin.com/onchain-data-shows-rising-bitcoin-whale-index-surpassing-4-year-high/.

Black, F., Jensen, M.C., Scholes, M., 1972. The Capital Asset Pricing Model: Some Empirical Tests. Stud. Theory Cap. Mark. .

Blanchard, O.J., Watson, M.W., 1982. Bubbles, Rational Expectations and Financial Markets.

Blockchain.com, 2020. Bitcoin Hashrate distribution among mining farms . URL: https://www.blockchain.com/charts/pools.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., Felten, E.W., 2015. SoK: Research perspectives and challenges for bitcoin and cryptocurrencies. Proc. - IEEE Symp. Secur. Priv. 2015-July, 104–121. doi:10.1109/SP.2015.14.

Bouri, E., Gupta, R., Roubaud, D., 2019. Herding behaviour in cryptocurrencies. Financ. Res. Lett. 29, 216–221. doi:10.1016/j.frl.2018.07.008.

Bouri, E., Kristoufek, L., Ahmad, T., Shahzad, S.J.H., 2022. Microstructure noise and idiosyncratic volatility anomalies in cryptocurrencies. Annals of Operations Research , 1–27doi:10.1007/s10479-022-04568-9.

Bouri, E., Molnár, P., Azzi, G., Roubaud, D., Hagfors, L.I., 2017. On the hedge and safe haven properties of Bitcoin: Is it really more than a diversifier? Financ. Res. Lett. 20, 192–198. doi:10.1016/J.FRL.2016.09.025.

Bouveret, A., 2018. Cyber risk for the financial sector: A framework for quantitative assessment. International Monetary Fund, Technical report.

Briner, R.B., Denyer, D., 2012. Systematic review and evidence synthesis as a practice and scholarship tool .

Canh, N.P., Wongchoti, U., Thanh, S.D., Thong, N.T., 2019. Systematic risk in cryptocurrency market: Evidence from DCC-MGARCH model. Financ. Res. Lett. 29, 90–100. doi:10.1016/j.frl.2019.03.011.

Caporale, G.M., Kang, W.Y.Y., Spagnolo, F., Spagnolo, N., 2021. Cyber-attacks, spillovers and contagion in the cryptocurrency markets. J. Int. Financ. Mark. Institutions Money 74, 101298. doi:10.1016/J.INTFIN.2021.101298.

Carhart, M.M., 1997. On persistence in mutual fund performance. J. Finance 52, 57–82. doi:10.1111/j.1540-6261.1997.tb03808.x.

Cheah, E.T., Fry, J., 2015. Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin. Econ. Lett. 130, 32–36. doi:10.1016/j.econlet.2015.02.029.

Chen, C., Chen, X., Yu, J., Wu, W., Wu, D., 2020. Impact of Temporary Fork on the Evolution of Mining Pools in Blockchain Networks: An Evolutionary Game Analysis. IEEE Trans. Netw. Sci. Eng. doi:10.1109/TNSE.2020.3038943.

Chu, J., Zhang, Y., Chan, S., 2019. The adaptive market hypothesis in the high frequency cryptocurrency market. Int. Rev. Financ. Anal. 64, 221–231. doi:10.1016/j.irfa.2019.05.008.

Ciaian, P., Rajcaniova, M., Kancs, D., 2016. The economics of BitCoin price formation. Appl. Econ. 48, 1799–1815. doi:10.1080/00036846.2015.1109038.

Clark-Murphy, M., Soutar, G.N., 2004. What individual investors value: Some australian evidence. Journal of Economic Psychology 25, 539–555.

CoinGuides.org, 2020. HashPower Calculator - Convert Hash to kH/s to MH/s to GH/s to TH/s to PH/s. URL: https://coinguides.org/hashpower-converter-calculator/.

Coinmetrics.com, 2019. Coin Metrics' State of the Network: Issue 26 - Coin Metrics' State of the Network. URL: https://coinmetrics.substack.com/p/coin-metrics-state-of-the-network-d2e.

Collomb, A., Sok, K., 2017. Blockchain et autre registres distribues: quel avenir pour les marches financiers? Technical Report 1. Intitut Louis Bachelier. Paris.

Cong, L.W., Li, Y., Wang, N., 2021. Tokenomics: Dynamic Adoption and Valuation. Rev. Financ. Stud. 34, 1105–1155. doi:10.1093/rfs/hhaa089.

Corbet, S., 2021. Understanding cryptocurrency fraud: The challenges and headwinds to regulate digital currencies. volume 2. Walter de Gruyter GmbH & Co KG.

Corbet, S., Cumming, D.J., Lucey, B.M., Peat, M., Vigne, S.A., 2020. The destabilising effects of cryptocurrency cybercriminality. Econ. Lett. 191, 108741. doi:10.1016/J.ECONLET.2019.108741.

Corbet, S., Goodell, J.W., Gunay, S., Kaskaloglu, K., 2023. Are defi tokens a separate asset class from conventional cryptocurrencies? Annals of Operations Research 322, 609–630.

Corbet, S., Lucey, B., Urquhart, A., Yarovaya, L., 2019. Cryptocurrencies as a financial asset: A systematic analysis. Int. Rev. Financ. Anal. doi:10.1016/j.irfa.2018.09.003.

Crothers, B., 2021. As Bitcoin price surged, it fueled rise in cyberattacks, researchers say. FOXBusiness .

Crowell, B., 2020. Crypto Exchange Liquidity, Explained. URL: https://cointelegraph.com/explained/crypto-exchange-liquidity-and-why-it-matters-explained.

Crypto51.app, 2023. Theoretical cost of a 51% Attack for Different Cryptocurrencies. URL: https://www.crypto51.app/.

CryptoSlate.com, 2022. Token Cryptocurrencies . URL: https://cryptoslate.com/cryptos/tokens/.

da Gama Silva, P.V.J., Klotzle, M.C., Pinto, A.C.F., Gomes, L.L., 2019. Herding behavior and contagion in the cryptocurrency market. J. Behav. Exp. Financ. 22, 41–50. doi:10.1016/J.JBEF.2019.01.006.

Das, D., Kannadhasan, M., 2018. Do global factors impact bitcoin prices?: evidence from wavelet approach. J. Econ. Res. 23, 227–264.

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., Lim, W.M., 2021. How to conduct a bibliometric analysis: An overview and guidelines. Journal of Business Research 133, 285–296.

Dowd, K., 2014. New Private Monies: A Bit-Part Player?

Drljevic, N., Aranda, D.A., Stantchev, V., 2019. Perspectives on risks and standards that affect the requirements engineering of blockchain technology. Comput. Stand. Interfaces 69, 103409. doi:10.1016/j.csi.2019.103409.

Dyhrberg, A.H., 2016a. Bitcoin, gold and the dollar – A GARCH volatility analysis. Financ. Res. Lett. 16, 85–92. doi:10.1016/J.FRL.2015.10.008.

Dyhrberg, A.H., 2016b. Hedging capabilities of bitcoin. Is it the virtual gold? Financ. Res. Lett. 16, 139–144. doi:10.1016/J.FRL.2015.10.025.

Fama, E., 1965a. Random Walks in Stock Market Prices. Financ. Anal. J. 21, 55–59.

Fama, E., 1965b. The Behavior of Stock-Market Prices. J. Bus. 38, 34–105.

Fama, E.F., French, K.R., 1992. The Cross-Section of Expected Stock Returns. J. Finance 47, 427–465. doi:10.2307/2329112.

Fama, E.F., French, K.R., 2015. A five-factor asset pricing model. J. financ. econ. 116, 1–22. doi:10.1016/J.JFINECO.2014.10.010.

Fernandez-Carames, T.M., Fraga-Lamas, P., 2020. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. IEEE Access 8, 21091–21116. doi:10.1109/ACCESS.2020.2968985.

Florysiak, D., Schandlbauer, A., 2019. The information content of ico white papers.

Forbes.com, 2022. What Really Happened To LUNA Crypto? URL: https://www.forbes.com/sites/qai/2022/09/20/what-really-happened-to-luna-crypto/?sh=30e7cc3e4ff1.

Gazali, H.M., Ismail, C.M.H.B.C., Amboala, T., 2018. Exploring the intention to invest in cryptocurrency: The case of bitcoin. Proc. - Int. Conf. Inf. Commun. Technol. Muslim World 2018, ICT4M 2018 , 64–68doi:10.1109/ICT4M.2018.00021.

Giudici, G., Milne, A., Vinogradov, D., 2020. Cryptocurrencies: market analysis and perspectives. Journal of Industrial and Business Economics 47, 1–18.

Goffard, P.O., 2019. Fraud risk assessment within blockchain transactions. Adv. Appl. Probab. 51, 443–467. doi:10.1017/apr.2019.18.

Greene, R., McDowall, B., 2018. Liquidity Or Leakage Plumbing Problems With Cryptocurrencies. Technical Report. Cardano Foundation & Long Finance.

Griffith, T., Clancey-Shang, D., 2023. Cryptocurrency regulation and market quality. Journal of International Financial Markets, Institutions and Money 84, 101744.

Grobys, K., 2021. When the blockchain does not block: on hackings and uncertainty in the cryptocurrency market. Quant. Financ. 21, 1267–1279. doi:10.1080/14697688.2020.1849779.

Grobys, K., Huynh, T.L.D., 2021. When tether says "jump!" bitcoin asks "how low?". Finance Research Letters 47, 102644.

Gudgeon, L., Perez, D., Harz, D., Livshits, B., Gervais, A., 2020. DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency, in: 2020 Crypto Val. Conf. Blockchain Technol. CVCBT 2020, Institute of Electrical and Electronics Engineers Inc.. pp. 1–15. doi:10.1109/CVCBT50464.2020.00005, arXiv:2002.08099.

Hacibedel, B., Perez-Saiz, H., 2023. Assessing Macrofinancial Risks from Crypto Assets. Technical Report. Technical report, International Monetary Fund.

Hasanova, H., jun Baek, U., gon Shin, M., Cho, K., Kim, M.S., 2019. A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. Int. J. Netw. Manag. 29, 1–36. doi:10.1002/nem.2060.

Heilman, E., Kendler, A., Zohar, A., Goldberg, S., 2015. Eclipse Attacks on Bitcoin's Peer-to-Peer Network, in: SEC'15 Proc. 24th USENIX Conf. Secur. Symp., pp. 129–144.

Huynh, T.L.D., 2021. Does bitcoin react to trump's tweets? Journal of Behavioral and Experimental Finance 31, 100546.

Huynh, T.L.D., 2022. When elon musk changes his tone, does bitcoin adjust its tune? Computational Economics , 1–23.

Iwamura, M., Kitamura, Y., Matsumoto, T., Saito, K., 2019. Can we stabilize the price of a cryptocurrency? Understanding the design of bitcoin and its potential to compete with central bank money. Hitotsubashi J. Econ. 60, 41–60.

Jain, P.K., McInish, T.H., Miller, J.L., 2019. Insights from bitcoin trading. Financ. Manag. 48, 1031–1048. doi:10.1111/fima.12299.

Jalan, A., Matkovskyy, R., 2023. Systemic risks in the cryptocurrency market: Evidence from the ftx collapse. Finance Research Letters 53, 103670.

Jia, B., Goodell, J.W., Shen, D., 2022. Momentum or reversal: Which is the appropriate third factor for cryptocurrencies? Financ. Res. Lett. 45, 102139. doi:10.1016/J.FRL.2021.102139.

Jiang, S., Li, Y., Wang, S., Zhao, L., 2022. Blockchain competition: The tradeoff between platform stability and efficiency. Eur. J. Oper. Res. 296, 1084–1097. doi:10.1016/J.EJOR.2021.05.031.

Kahneman, D., Tversky, A., 1979. Prospect theory: An analysis of decision under risk. Econometrica 47, 363–391.

Kallinterakis, V., Wang, Y., 2019. Do investors herd in cryptocurrencies – and why? Res. Int. Bus. Financ. 50, 240–245. doi:10.1016/J.RIBAF.2019.05.005.

Kaplan, R.S., Norton, D.P., 1992. The Balanced Scorecard—Measures that Drive Performance. Harv. Bus. Rev. URL: https://hbr.org/1992/01/the-balanced-scorecard-measures-that-drive-performance-2.

Karim, S., Lucey, B.M., Naeem, M.A., Uddin, G.S., 2022. Examining the Interrelatedness of NFT's, DeFi Tokens and Cryptocurrencies. Financ. Res. Lett. , 102696doi:10.1016/j.frl.2022.102696.

Keller, C., Siegrist, M., 2006. Investing in stocks: The influence of financial risk attitude and values-related money and stock market attitudes. Journal of Economic Psychology 27, 285–303.

King, T., Koutmos, D., 2021. Herding and feedback trading in cryptocurrency markets. Annals of Operations Research 300, 79–96.

Koshik, R., 2019. What Blockchain developers learn from Eclipse Attacks in bitcoin network. URL: https://hub.packtpub.com/what-can-blockchain-developers-learn-from-eclipse-attacks-in-a-bitcoin-network-koshik-raj/.

Koutmos, D., 2018. Liquidity uncertainty and Bitcoin's market microstructure. Econ. Lett. 172, 97–101. doi:10.1016/j.econlet.2018.08.041.

Koutmos, D., 2020. Market risk and Bitcoin returns. Ann. Oper. Res. 294, 453–477. doi:10.1007/S10479-019-03255-6/TABLES/6.

Kristoufek, L., 2019. Is the Bitcoin price dynamics economically reasonable? Evidence from fundamental laws. Phys. A Stat. Mech. its Appl. 536, 120873. doi:10.1016/j.physa.2019.04.109.

La Porta, R., Lopez-De-Silanes, F., Shleifer, A., Vishny, R., 2002. Investor Protection and Corporate Valuation. J. Finance 57, 1147–1170. doi:10.1111/1540-6261.00457.

Lemieux, V.L., 2016. Trusting records: is Blockchain technology the answer? Rec. Manag. J. 26, 110–139. doi:10.1108/RMJ-12-2015-0042.

Liebau, D., Schueffel, P., 2019. Crypto-Currencies and ICOs: Are They Scams? An Empirical Study. doi:10.2139/ssrn.3320884.

Lintner, J., 1965. The valuation of Risk assets and the Selection of Risky investments in Stock portfolios and Capital Budgets. Rev. Econ. Stat. 47, 13–37.

Litecoinpool.org, 2020. Hash Rate Distribution — litecoinpool.org. URL: https://www.litecoinpool.org/pools.

Liu, W., Liang, X., Cui, G., 2020. Common risk factors in the returns on cryptocurrencies. Econ. Model. 86, 299–305.

Liu, Y., Tsyvinski, A., 2021. Risks and Returns of Cryptocurrency. Rev. Financ. Stud. 34, 2689–2727.

Liu, Y., Tsyvinski, A., Wu, X., 2022. Common Risk Factors in Cryptocurrency. J. Finance 77.

Lu, Y., 2019. The blockchain: State-of-the-art and research challenges. J. Ind. Inf. Integr. 15, 80–90. doi:10.1016/j.jii.2019.04.002.

Lucas, R.E., Sargent, T.J., 1981. Rational expectations and econometric practice. volume 2. U of Minnesota Press.

Ma, S., Hao, W., Dai, H.N., Cheng, S., Yi, R., Wang, T., 2018. A blockchain-based risk and information system control framework. Proc. - IEEE 16th Int. Conf. Dependable, Auton. Secur. Comput. , 114–120doi:10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00031.

Magoo.github.io, 2023. Blockchain Graveyard. URL: https://magoo.github.io/Blockchain-Graveyard/.

Manahov, V., 2021. Cryptocurrency liquidity during extreme price movements: is there a problem with virtual money? Quant. Financ. 21, 341–360. doi:10.1080/14697688.2020.1788718.

Marcus, Y., Heilman, E., Goldberg, S., 2010. Low-resource eclipse attacks on Ethereum's peer-to-peer network. Cryptol. Rep. 236.

Markowitz, H., 1952. Portfolio Selection. J. Finance 7, 77–91.

Martínez, J.M.G., Carracedo, P., Comas, D.G., Siemens, C.H., 2022. An analysis of the blockchain and covid-19 research landscape using a bibliometric study. Sustainable Technology and Entrepreneurship 1, 100006.

Messamore, W.E., 2019. 3 Best Performing Securities by Asset Class in the Last Decade. URL: https://www.ccn.com/3-best-performing-securities-by-asset-class-decade/.

Momtaz, P.P., 2021. The Pricing and Performance of Cryptocurrency. Eur. J. Financ. 27, 367–380. doi:10.1080/1351847X.2019.1647259.

Morganti, G., Schiavone, E., Bondavalli, A., 2019. Risk Assessment of Blockchain Technology. Proc. - 8th Latin-American Symp. Dependable Comput. LADC 2018 , 87–96doi:10.1109/LADC.2018.00019.

Mossin, J., 1966. Equilibrium in a Capital Asset Market. Econometrica 34, 768. doi:10.2307/1910098.

Nguyen, T.V.H., Nguyen, B.T., Nguyen, T.C., Nguyen, Q.Q., 2019. Bitcoin return: Impacts from the introduction of new altcoins. Res. Int. Bus. Financ. 48, 420–425. doi:10.1016/j.ribaf.2019.02.001.

Noda, A., 2021. On the Evolution of Cryptocurrency Market Efficiency. Appl. Econ. Lett. 28. doi:10.1080/13504851.2020.1758617, arXiv:1904.09403.

Pagnotta, E.S., 2022. Decentralizing Money: Bitcoin Prices and Blockchain Security. Rev. Financ. Stud. 35, 866–907. doi:10.1093/RFS/HHAA149.

Patel, D., 2020. Blockchain Technology towards the Mitigation of Distributed Denial of Service Attacks. Int. J. Recent Technol. Eng. 8, 961–965. doi:10.35940/ijrte.f7420.038620.

Pawczuk, L., Massey, R., Holdowsky J., 2019. Deloitte's 2019 Global Blockchain Survey. URL: https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf.

Pearson, E.S., 1932. The Test of Significance for the Correlation Coefficient: Some Further Results. J. Am. Stat. Assoc. 27, 424. doi:10.2307/2278641.

Pereira, É.D., Ferreira, P., 2019. Contagion Effect in Cryptocurrency Market. J. Risk Financ. Manag. 12, 115. doi:10.3390/jrfm12030115.

Ross, S.A., 1976. The Arbitrage Theory of Capital Asset Pricing. J. Econ. Theory 13, 341–360.

Routledge, B., Zetlin-Jones, A., 2021. Currency stability using blockchain technology. J. Econ. Dyn. Control , 104155doi:10.1016/J.JEDC.2021.104155.

Rui Chen, R., Chen, K., 2020. A 2020 perspective on "Information asymmetry in initial coin offerings (ICOs): Investigating the effects of multiple channel signals". Electron. Commer. Res. Appl. 40, 100936. doi:10.1016/j.elerap.2020.100936.

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D.H., Mohaisen, A., 2019. Exploring the attack surface of blockchain: A systematic overview. IEEE Commun. Surv. Tutorials 99, 1–30. arXiv:1904.03487.

Shahzad, S.J.H., Anas, M., Bouri, E., 2022. Price explosiveness in cryptocurrencies and elon musk's tweets. Finance Research Letters 47, 102695.

Shanaev, S., Sharma, S., Ghimire, B., Shuraeva, A., 2020. Taming the blockchain beast? Regulatory implications for the cryptocurrency Market. Res. Int. Bus. Financ. 51, 101080. doi:10.1016/j.ribaf.2019.101080.

Shane, D., 2018. Coincheck: $530M cryptocurrency heist may be biggest ever. URL: https://money.cnn.com/2018/01/29/technology/coincheck-cryptocurrency-exchange-hack-japan/index.html.

Sharpe, W.F., 1964. Capital asset prices: a theory of market equilibrium under conditions of risk. J. Finance 19, 425–442. doi:10.1111/J.1540-6261.1964.TB02865.X.

Shen, D., Urquhart, A., Wang, P., 2020. A three-factor pricing model for cryptocurrencies. Financ. Res. Lett. 34, 101248. doi:10.1016/J.FRL.2019.07.021.

Shiller, R.J., 2015. Irrational exuberance, in: Irrational exuberance. Princeton university press.

Sinclair, S., 2019. Cryptocurrencies Are Still the World's Best Performing Asset Class This Year. URL: https://uk.finance.yahoo.com/news/cryptocurrency-still-world-best-performing-020000891.html?guccounter=1.

Snyder, H., 2019. Literature review as a research methodology: An overview and guidelines. J. Bus. Res. 104, 333–339. doi:10.1016/j.jbusres.2019.07.039.

Sockin, M., Xiong, W., 2023. A model of cryptocurrencies. Management Science doi:10.3386/W26816.

Şoiman, F., Dumas, J.G., Jimenez-Garces, S., 2023. What drives defi market returns? Journal of International Financial Markets, Institutions and Money , 101786.

Spearman, C., 1904. The Proof and Measurement of Association between Two Things. Am. J. Psychol. 15, 72. doi:10.2307/1412159.

Sriram, S., 2021. Bitcoin Becomes Best Performing Asset Of The Decade, Returning Ten Times More Than Nasdaq 100. URL: https://www.yahoo.com/video/bitcoin-becomes-best-performing-asset-132208120.html.

Stewart, I., Ilie, D., Zamyatin, A., Werner, S., Torshizi, M.F., Knottenbelt, W.J., 2018. Committing to quantum resistance: A slow defence for Bitcoin against a fast quantum computing attack. R. Soc. Open Sci. 5. doi:10.1098/rsos.180410.

Tobin, J., 1958. Liquidity preference as behavior towards risk. Rev. Econ. Stud. 25, 65–86. doi:10.2307/2296205/2/25-2-65.PDF.GIF.

Tranfield, D., Denyer, D., Smart, P., 2003. Towards a methodology for developing evidence-informed management knowledge by means of systematic review. British journal of management 14, 207–222.

Treynor, J.L., 1961. Market Value, Time, and Risk. SSRN Electron. J. doi:10.2139/SSRN.2600356.

Tuwiner, J., 2021. Bitcoin Mining Pools. URL: https://www.buybitcoinworldwide.com/mining/pools/.

Tversky, A., Kahneman, D., 1992. Advances in prospect theory: Cumulative representation of uncertainty. Journal of Risk and uncertainty 5, 297–323.

Underscore VC, 2018. Future of Blockchain Survey & Results. URL: https://underscore.vc/blog/future-of-blockchain-survey-results/.

Urquhart, A., 2016. The inefficiency of Bitcoin. Econ. Lett. 148, 80–82. doi:10.1016/j.econlet.2016.09.019.

Wang, G., Zhang, S., Yu, T., Ning, Y., 2021. A systematic overview of blockchain research. J. Syst. Sci. Inf. 9, 205–238. doi:10.21078/JSSI-2021-205-34/ASSET/GRAPHIC/J_JSSI-2021-205-34_FIG_012.JPG.

Wei, W.C., 2018. Liquidity and market efficiency in cryptocurrencies. Econ. Lett. 168, 21–24. doi:10.1016/j.econlet.2018.04.003.

Wilkoff, S., Yildiz, S., 2023. The behavior and determinants of illiquidity in the non-fungible tokens (nfts) market. Global Finance Journal 55, 100782.

Williams, J.B., 1938. The theory of investment value. Business & ed., Fraser Publishing Company.

Wilmarth, A.E., 2023. We must protect investors and our banking system from the crypto industry. GWU Legal Studies Research Paper .

Wood, R., Zaichkowsky, J.L., 2004. Attitudes and trading behavior of stock market investors: A segmentation approach. The Journal of Behavioral Finance 5, 170–179.

Wüst, K.., Gervais, A., 2016. Ethereum Eclipse Attacks. Technical Report. doi:10.3929/ethz-a-010724205.

Xu, A.T., Xu, J., Lommers, K., 2022. DeFi vs TradFi: Valuation Using Multiples and Discounted Cash Flows. URL: https://docs.tokenterminal.com/, arXiv:2210.16846v1.

Yaya, O.O.S., Ogbonna, A.E., Mudida, R., Abu, N., 2021. Market efficiency and volatility persistence of cryptocurrency during pre- and post-crash periods of Bitcoin: Evidence based on fractional integration. Int. J. Financ. Econ. 26, 1318–1335. doi:10.1002/ijfe.1851.

Yi, S., Xu, Z., Wang, G.J., 2018. Volatility connectedness in the cryptocurrency market: Is Bitcoin a dominant cryptocurrency? Int. Rev. Financ. Anal. 60, 98–114. doi:10.1016/J.IRFA.2018.08.012.

Zetzsche, D.A., Buckley, R.P., Arner, D.W., Fohr, L., 2019. the ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators. Harvard Int. Law J. 60, 267.

Zhang, S., Zhou, X., Pan, H., Jia, J., 2019. Cryptocurrency, confirmatory bias and news readability – evidence from the largest Chinese cryptocurrency exchange. Account. Financ. 58, 1445–1468. doi:10.1111/acfi.12454.

Zhao, H., Zhang, L., 2021. Financial literacy or investment experience: which is more influential in cryptocurrency investment? Int. J. Bank Mark. 39, 1208–1226. doi:10.1108/IJBM-11-2020-0552/FULL/XML.

Zimmerman, P., 2020. Blockchain Structure and Cryptocurrency Prices. doi:10.2139/ssrn.3538334.

Table 6: **Hacks, thefts and losses events related to Bitcoin**
Source: (Biais et al., 2020)

Date	Amount loss (BTC)	Description
6/13/2011	25,000	Early user Allinvain was hacked
6/19/2011	2,000	MtGox theft - compromised account
6/25/2011	4,019	*MyBitcoin theft - wallet keys hacked*
7/26/2011	17,000	*Bitomat loss - Wallet access lost*
7/29/2011	78,739	*MyBitcoin theft - wallet website hacked*
10/6/2011	5,000	*Bitcoin7 hack*
10/28/2011	2,609	*MtGox loss due to hacking*
3/1/2012	46,653	*Linode hacks*
4/13/2012	3,171	*Betcoin hack*
4/27/2012	20,000	*Tony76 Silk Road scam*
5/11/2012	18,547	*Bitcoinica hack*
7/4/2012	1,853	*MtGox hack*
7/13/2012	40,000	*Bitcoinica theft - due to server hack*
7/17/2012	180,819	*BST Ponzi scheme*
7/31/2012	4,500	*BTC-e hack*
9/4/2012	24,086	*Bitfloor theft - wallet keys hacked*
9/28/2012	9,222	*User Cdecker hacked*
10/17/2012	3,500	*Trojan horse*
12/21/2012	18,787	*Bitmarket.eu hack*
5/10/2013	1,454	*Vircurex hack*
6/10/2013	1,300	*PicoStocks hack*
10/2/2013	29,655	*FBI seizes Silk Road funds*
10/25/2013	144,336	*FBI seizes Silk Road funds*
10/26/2013	22,000	*GBL scam*
11/7/2013	4,100	*Inputs.io hack*
11/12/2013	484	*Bitcash.cz hack*
11/29/2013	5,400	*Sheep Marketplace hacked & closes*
11/29/2013	5,896	*PicoStocks hack*
2/13/2014	4,400	*Silk Road 2 hacked*
2/25/2014	744,408	*MtGox collapse due to hacks losses*
3/4/2014	896	*Flexcoin hack*
3/4/2014	97	*Poloniex hack*
3/25/2014	950	*CryptoRush hacked*
10/14/2014	3,894	*Mintpal hack*
1/5/2015	18,886	*Bitstamp hack*
1/28/2015	1,000	*796Exchange hack*
2/15/2015	7,170	*BTER hack*
2/17/2015	3,000	*KipCoin hack*
5/22/2015	1,581	*Bitfiniex hack*
9/15/2015	5,000	*BitPay phishing scam - hacker takes over the CEO's accounts*
1/15/2016	11,325	*Cryptsy hack*
4/7/2016	315	*ShapeShift hack*
4/13/2016	154	*ShapeShift hack*
5/14/2016	250	*Gatecoin hack*
8/2/2016	119,756	*Bitfinex hack*
10/13/2016	2,300	*Bitcurex hack*
4/22/2017	3,816	*Yapizon hack*
7/12/2017	1,942	*AlphaBay (darknet) admins assets sized by FBI*
7/20/2017	1,200	*Hansa (darknet) funds seized by Dutch police*
12/6/2017	4,736	*NiceHash hacked*
6/20/2018	2,016	*Bithumb hacked*
9/20/2018	5,966	*Zaif hacked*
10/28/2018	8	*MapleChange hack / scam*

Table 7: Descriptive Statistics of all variables

	volatility	event losses	number of events
Median	0.254	4736.000	1.000
Mean	0.341	46743.630	1.407
Std. Deviation	0.271	146592.481	0.636
Skewness	2.306	4.591	1.343
Kurtosis	6.909	22.177	0.832
Minimum	0.089	8.000	1.000
Maximum	1.359	748808.000	3.000

The table summarizes the descriptive statistics of all variables for the sample period.

Table 8: **Correlation tests for *volatility versus the number of events and the amounts lost during these events***

Test	**p-value**	**Correlation estimates**	**Variable**
Pearson	0.02156	0.4402268	*number of events*
Spearman	0.03387	0.4095827	*number of events*
Pearson	0.6606	0.08853083	*amounts lost*
Spearman	0.3888	0.4095827	*amounts lost*

By looking at the p-values (0.02 & 0.03) resulting from our tests for correlation with the number of events, we observe that the results obtained are less than the significance level alpha = 0.05. Meaning that the monthly volatility of bitcoin and the number of events targeting it are correlated. At the same time, the high p-values (0.6 & 0.3) that surpass the significance level alpha of 0.05, prove that there is no correlation between bitcoin's volatility and the amounts lost due to events.

Table 9: **Linear regression 1**
Summary of the OLS regression used to identify the relationship between monthly volatility and the number of events targeting bitcoin together with the losses incurred. Computations performed with R studio.

Dep. Variable:	Volatility	**Df Model:**	2
Model:	OLS	**R-squared:**	0.195
Method:	Least Squares	**Adj. R-squared:**	0.128
Date:	14 October 2021	**F-statistic:**	2.913
No. of Observations:	27	**Prob. (F-statistic):**	0.074
Df Residuals:	24	**Residual standard error:**	0.253

Coefficients:

Model		**Estimate**	**Std. Error**	**t**	**p-value**
H_1	$EVENT_{number}$	0.193	0.081	2.364	0.026*
H_2	$EVENT_{amount}$	-7.589e-8	3.534e-7	-0.215	0.832

*With a **p-value** of 0.026*, a result that is significant and less than the significance level alpha: 0.05, we can conclude that there is a relationship between the monthly volatility and the number of events targeting bitcoin. At the same time, with a **p-value** of 0.832, a result that is higher than the significance level alpha: 0.05, we conclude that there is no relationship between the monthly volatility of bitcoin and the amounts lost during the events targeting it.*

Table 10: **Linear regression 2**
Summary of the OLS regression used to identify the existence of a quadratic relationship between monthly BTC volatility and the number of events. Computations performed with R studio.

	Estimate	Std. Error	t value	Pr(>|t|)
(Intercept)	-0.2799	0.3752	-0.75	0.4629
number	0.6641	0.4811	1.38	0.1802
number_2	-0.1322	0.1317	-1.00	0.3258

*We obtained **p-values** of 0.1802 & 0.3258, a result that is higher than the significance level alpha, 0.05; therefore, we conclude that there is no quadratic relationship between the monthly BTC volatility and the number of events.*

Table 11: **Linear regression 3**
Summary of the OLS regression used to identify the existence of a quadratic relationship between monthly BTC volatility and the amounts lost during the events. Computations performed with R studio.

	Estimate	Std. Error	t value	Pr(>|t|)
(Intercept)	0.3221	0.0615	5.23	0.0000
amount	0.0000	0.0000	0.57	0.5724
amount_2	-0.0000	0.0000	-0.49	0.6307

*We obtained **p-values** of 0.5724 & 0.6307, a result that is higher than the significance level alpha, 0.05; therefore, we conclude that there is no quadratic relationship between the monthly BTC volatility and the amounts lost.*