Blockchain technology and the crypto-market: A literature survey

Jean-Guillaume Dumas[1], Sonia Jimenez-Garces[2], and Florentina Șoiman[1,2]

[1]Univ. Grenoble Alpes, CNRS, LJK, F-38040 Grenoble, France
[2]Univ. Grenoble Alpes, Grenoble INP, CERAG, 38000 Grenoble France
[Firstname.Lastname]@univ-grenoble-alpes.fr

October 11, 2021

Abstract

This paper provides a literature survey on the vulnerabilities and risks of Blockchain technology and the crypto-market. Since their creation, the crypto-market and Blockchain technology are still very much challenged and far from the mainstream adoption. We thus here propose a detailed literature survey focusing on the relationship between technological characteristics and financial risks. Furthermore, to complete this study, we propose ways to determine the likelihood of technological vulnerabilities triggering financial risks. Additionally, we find a significant relationship between Blockchain attacks and cryptocurrency volatility, hence illustrating the relationship between technological vulnerabilities and financial risk. While we take into consideration the existent literature on the vulnerabilities and risks associated with the crypto-market, we cannot ignore the limited work with respect to crypto-fundamentals. Alleviating this gap will require more theoretical models and empirical research that encompass the technological characteristics of this market. Our results are twofold. First, we show an identified continuity between the technological risks and financial ones. Secondly, we find that price stability is disturbed by technological vulnerabilities.

Keywords: Blockchain, Risk assessment, Financial risks, Attacks, Literature survey
JEL Codes: G10, G15, G19

1 Introduction

Everyone has heard about the enormous potential of the Blockchain technology and the fact that it might revolutionize business models and reinvent the contemporary firms and economies. At the same time, we know that it is still far from keeping all its promises and before that happens, Blockchain has to first overcome its technological, organizational and social barriers (Iansiti & Lakhani, 2017; Charles, 2019). As professor Karim Beddiar said, "The Internet has democratized the information, the Blockchain will democratize the transaction" [1], however, there is still a lot of work left for research before that happens and a lot of experience to gain before the technology will mature (Charles, 2019). This global distributed, open and transparent database, which stores and transfers information of any kind (money, art, science, titles, votes, etc.) has the potential to create new foundations for the economy and business sector. Blockchain might be a complex technology, but the concept behind it is very simple (Tapscott & Tapscott, 2016; Iansiti & Lakhani, 2017).

Inspired from the existing systems and technologies, the solutions promised by Blockchain seem to be far beyond what we have already seen. Little by little, Blockchain is taking over many sectors of the economy and a growing number of organizations are declaring their enthusiasm and interest in using it (Collomb & Sok, 2016).Given the spread of Blockchain-based solutions across various industries and the growing interest in using it, there is an urgent need for researchers and market participants to gain understanding of what it means to be part of the crypto-market.

As previously mentioned, Blockchain needs to overcome a series of challenges, before becoming a mainstream technology (Wachsman, 2019). According to Iansiti & Lakhani (2017),there are two dimensions affecting the way technology evolves. The first dimension represents novelty, referring to the degree of originality and uniqueness in comparison with the existing systems. This dimension implies as well the difficulty in seeing the use and innovation of technology. The second dimension refers to complexity, implying the extent to which this technology touches various fields, regardless the market or area of expertise (Iansiti & Lakhani, 2017; Notheisen & Weinhardt, 2019). The same idea is sustained by the results obtained in the surveys conducted by Deloitte and Underscore companies. While assessing the Blockchain adoption, they found out that some of the main barriers are: the technological complexity, regulatory issues, lack of in-house skills and understanding, security threats and the uncertain profitability (Pawczuk et al., 2019; Underscore VC, 2018). In 2018, Gazali et al. (2018) explored the relationship between human conduct and the intention to invest in the crypto-market. Consequently, they found out that the attitude towards the crypto-market, the social norms [2], the risk tolerance and the perceived benefits coming from using this technology, represent some of the main factors influencing the interested parties to invest or be part of the crypto-market.

Regardless the big potential and great innovative solutions brought by Blockchain, this technology gained most of its fame thanks to its vulnerabilities. The cryptocurrencies' volatility and the numerous cyber-attacks suffered by this technology, represent the main driving factors towards the Blockchain's popularity. Among the existing research literature, several studies have addressed the crypto-market risks. Some with the aim to find solutions to these vulnerabilities (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 just to increase general awareness (Saad et al., 2019; Canh et al., 2019; Lemieux, 2016; Gazali et al., 2018; Lu, 2019).

Consequently, following the review of the existing literature, we claim that there is a need for further research on risks and vulnerabilities of the crypto-market. Compared to previous papers, where risks were usually treated based on their nature (i.e. economic, political, regulatory, etc.),

[1] Own translation from original: " Internet a démocratisé l'information, la Blockchain va démocratiser la transaction" (Charles, 2019)

[2] decisions are made based on the actual trends and influenced by a mentality such like: "if I lose, at least I am not alone")

we intend to provide a parallel analysis of both the financial and technological risks. We show that these risks, regardless their nature, have many characteristics in common. Moreover, we offer ways to determine the likelihood that technological risks could transform into financial ones and provide a short empirical demonstration.

This study is a literature-based research. Compared to other areas, finance is mostly dominated by quantitative type of analysis. However, we believe that a new field of research like the crypto-market, would greatly benefit from such a powerful scrutinizing tool that explores the existing papers and informs the reader about the current state of knowledge. In conducting this research, we have used various types of information, from both academic [3] and non-academic [4] literature. The selection of papers was done by taking into account the topic of investigation, while the afterwards information has been grouped by the types of risk. In our search we have used a big variety of keywords such as: crypto, Blockchain, financial risk, technological risk, attack, financial behavior, Blockchain literacy, etc. With this literature survey, we will answer to the following research question: 'Can financial risks be triggered by technological vulnerabilities of Blockchain technology?'.

With the aim to enlighten our research problem, the objective of this survey is to provide a two-dimension risk analysis (technological and financial) completed by an assessment of triggering elements (the likelihood). Furthermore, following the example of Benoit et al. (2017) literature survey, we are going to complete this study with a short data analysis. In line with the statements made in the literature review, we show that bitcoin's price instability (financial risk) can be triggered by the attacks targeting the crypto-market (technological vulnerability).

This paper is organized as follows. Section 2 presents the assessment of technological and financial risks; Section 3 proposes a brief empirical illustration. Section 4 discusses the results and concludes.

2 Blockchain risks 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 Blockchain and their possible consequences and impact;
- To offer a broad view to Blockchain stakeholders on possible financial and technological risks.

According to Leemoon (2017), crypto-market's challenges can be divided into four main areas:

1. Technological issues
2. Financial issues
3. Policy and legal issues
4. Political issues

While all four types of risks are indisputably affecting the crypto-market development and slowing its acceptance, we consider that the first two could represent a starting point and a reliable support in designing a better legal framework. At the same time, we believe that all these together could eventually alleviate some of the political issues. That being said, in this study, we tackle the first two categories, leaving the last two for future research. We make a parallel analysis between the technological and financial risks. At this point, we, for instance, intend to help users and investors find the answer to possible questions, such as: "Is this investment / technology safe? What are the risks and vulnerabilities I may encounter?". To the best of our knowledge, this is the first study trying to assess both financial and technological risks in parallel.

[3] Academic journals, academic theses

[4] Websites, official reports issued by research or governmental organizations, magazines, etc.

The complexity of this technology, inherited by nature, represents a challenge for users, investors and any other participants from this market (Salmela, 2019). Highly secure at first sight, Blockchain is not exempt of risks, but is rather an imperfect innovation leaving generous room for many improvements (Iwamura et al., 2019). According to Swan (2017) Blockchain technology is the only one which has the potential to change or, better said, to revolutionize the way businesses and financial markets work.

According to the latest surveys performed with regards to the factors slowing down the Blockchain's adoption, the main barriers are: the scalability issues, insufficient regulation, unproven or the debatable value of technology, security threats, lack of in-house skills and uncertain rate of return (Underscore VC, 2018; Pawczuk et al., 2019). As we can observe, most of the mentioned obstacles are either technological or finance related. These findings encourage us to perform a risk assessment and support the necessity of prioritizing the first two categories of risks, namely the financial and technological ones.

2.1 Technological risks

We here systemize the crypto-market threats in accordance with their nature, namely, consensus level attack, network level attack, cryptographic key attacks and smart contract attacks. There are many types of attacks which are not discussed in this study. However, we tried to cover the most important ones, by taking into account the likelihood, the exposure of the crypto-market to such incidents and the impact they might have.

Consensus algorithms for Blockchain technology represent a code-based protocol, aiming to facilitate reaching agreement processes within a network. These algorithms came as a solution to the "Byzantine General Problem", which concerns the failure of reaching consensus due to faulty actors (Zhang et al., 2019). The most popular and widespread consensus algorithms in the Blockchain technology, are the Proof of Work (PoW), Proof of Stake (PoS) and the Practical Byzantine Fault Tolerance (PBFT) protocols (see Table 1).

Table 1: **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: on the PoS protocol, where low stake owners try to decrease the value of cryptocurrency. Indeed, the control inside the system is given based on the user's wealth, potentially combined with other factors (coin age-based selection or random factors). Any PoS Blockchain can be exposed to this type of attack, especially in their beginnings, when there are no real imbalances among the users' wealth and low stake owners will not lose much (Morganti et al., 2019).

The majority attack (>50% attack): means that the consensus protocol is compromised, functioning as a monopolistic system. Taking into account its possible implications, the majority attack is considered also a security issue. Moreover, considering the target type, it can be split in two variants: "the >50% (or 51%) computational power attack" [5] and "The 51% stake attack" [6] (Tuwiner, 2021; Blockchain.com, 2020).

[5] an attack on the PoW protocol, implying the possession of more than 50% of the total mining power, with the purpose to manipulate and corrupt the network

[6] An attack targeting the PoS protocol; it implies the possession of more than 50% of the total circulating supply of coins (within the same network) with the purpose to gain monopoly power and mislead the system for profit purposes. It is conceptually similar to computational power attack.

Bitcoin has never experienced a successful majority attack. However, we cannot say the same about altcoins: Feathercoin (June 2013), Bitcoin Gold (May 2018), Vertcoin (December 2018), Ethereum Classic (January 2019) and Bitcoin Cash (May 2019) (Beigel, 2019). The difficulty to execute an attack is very much influenced by the size of the Blockchain network. Table 2 shows how expensive is to perform a majority attack, depending on the cryptocurrency. These costs are computed taking into account the expenses incurred in the mining process, namely the network hash rate & the Nicehash cost in BTC /per hour (rented PC power). These values can change every minute, as the cryptos' prices have a big influence (Crypto51.app, 2020).

Table 2: **PoW 51% attack cost for the top 7 cryptocurrencies.**

System	Hash rate [7]	1 h attack estimated Cost
Bitcoin	*114,915 PH/s*	*$716,072*
Ethereum	*253 TH/s*	*$418,438*
Litecoin	*227 TH/s*	*$29,287)*
B. Cash	*1,374 PH/s*	*$8,560)*
Zcash	*8 GH/s*	*$8,710*
B. SV	*1,109 PH/s)*	*$6,912*
Dash	*7 PH/s)*	*$3,246*

Values computed as per 10th February 2021
Source: derived from Crypto51.app (2020)

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. If for example, the (host) Blockchain system is under attack, it can become unresponsive, unavailable. The system is compromised by being feed with misleading information or big 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 highly associated with the increase in value and popularity of the cryptocurrencies (Crothers, 2021).

Some other notable examples of network level attacks, worth to mention if we take into account the exposure and powerful impact they could have, 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; Packtpub, 2019; Marcus et al., 2018; Wüst & 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).

Cryptographic key attacks. In Blockchain technology, cryptographic keys give access to funds (through crypto wallets) and play a critical role in transactional processes. In other words, anyone handling the cryptographic keys can access the wallet account and freely manage the associated funds. These keys are stored in crypto wallets. According to the version of crypto wallet used (software, hardware, cloud, brain[11] or paper), the keys are more or less safe (hardware & paper - most secure, software, brain & cloud – less secure). Having such a variety of key storage options

[8] The difficulty to execute an attack is very much influenced by the size of Blockchain network. Private Blockchains are considered more exposed compared to the 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] It's a type of wallet which gives the user the option to generate a key using a password (a word, number, combination of bot, etc.). This type of wallet and keys are considered weak in terms of security.

gives attackers ideas to approach the wallets in different ways.

Wallet attack: The main causes behind wallet attacks are system hacking, software vulnerabilities, malwares or incorrect usage from the users' side. The objective is to obtain (steal) the private key, with which the attacker can mislead the system, perform un-authorized transactions and steal coins (send them into the thief's wallet using the victim's private key). Compared to any other types of crypto attacks, the ones targeting the wallets are among the most common and harmful incidents [12]. This statement is also supported by the Blockchain Graveyard organization, as according to their thorough analysis on the incidents associated to Blockchain, more than half relate to wallet attacks (Magoo.github.io, 2020).

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

Smart contract attacks mainly refer to the manipulation of external data entered in the Blockchain (through oracle technology), misleading the execution of the smart contract. The trigger represents information related to external events, which affects the contract's conditions. The information is manually introduced, reason why, 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 the perfect opportunity for any hacker 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 is sending multiple requests to the system, as 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 above will be presented in Table 3.

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

[13] targets the weak security of the cryptographic keys, due to insufficient randomness used in their generation process, making them easy to predict (Independent Security Evaluators, 2019); in spite of the common knowledge that the cryptographic keys are difficult to break, apparently, a combination of weak hashing algorithms and skilled hackers have led to such kind of incidents.

[14] performed with the quantum computers (QC); In the context of Blockchain, they 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 & Fraga-Lamas, 2020; Stewart et al., 2018).

Table 3: **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[15]) source:(CryptoSlate.com, 2020)*
	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);* *Blockchains using PoS (over 400 cryptocurrencies) source:(CryptoSlate.com, 2020)* *Mining pools[16]*
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, 2020)*
	Smart contract attack	*Misleads the technology's application*	*Blockchains supporting smart contracts (over 50 cryptocurrencies) Source:(CryptoSlate.com, 2020)*

2.2 Financial risks

In this section, we give example of several financial risks that can be triggered by technological risks. After detailing how this phenomenon happens and in what kind of circumstances, we propose a conceptual metric, with the purpose to emphasize the likelihood that these technological risks may transform into financial ones.

Determining the likelihood: The likelihood that the technological risks may transform into financial risks, can be established by taking into account the severity [17] effect and probability of occurrence of triggering elements. Here, we will also introduce the concepts financial behavior, responsible investment and Blockchain literacy, as possible tools for assessing risk. Measurement plays an important 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 & Norton (1992),if we can't measure something, then we can't properly manage it. Therefore, in this part of the assessment, we propose ways to measure the probability that technological vulnerabilities may trigger financial risk.

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 threating 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 could be an example of specific risk [18].

From the above list, by taking into consideration the risks' exposure and their consequential power, we can easily identify several attacks, which may trigger financial risks. For instance, majority attacks (almost half of the total crypto-market is exposed to this risk, plus the mining pools), Sybil and Eclipse attacks (targeting Permissionless Blockchains- the most common and big representatives of this market-), DDoS attack, wallet attack, random number generator attack and quantum attacks (targeting all types of Blockchains) can be considered potential triggers for systematic risk [19]. At the same time, if affecting just one type of Blockchain, one cryptocurrency or few casualties such as a mining pool/exchange platform, the same technological can trigger a specific risk.

It is well known that the crypto-assets' price is influenced by regulatory and cybersecurity related events (Corbet et al., 2019). Subsequently, such events influence the investors' behavior, which is eventually impacting crypto-market's volatility. It was also proved that cryptocurrencies suffer from contagion effects (herding behavior)(da Gama Silva et al., 2019). Bitcoin, Ether or any other strong and well-known currency have proved their influence over the evolution of the whole cryptocurrency market. In 2017, when Bitcoin prices skyrocketed and crashed, the rest of the cryptocurrencies followed a similar trend (Antonakakis et al., 2019; Pereira & Ferreira, 2019). The strong power of influence and the herding behavior present in the crypto-market, represent a trigger for systematic risk. Here, we have the perfect example of how an independent event, initially affecting one currency (specific risk), can eventually transform in a systematic risk [20], impacting the whole market (P. K. 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 have also the technological vulnerabilities as a possible trigger. Under the hypothesis of traditional financial theory, specific risk is diversifiable and

[17] Financial loses and investment cost incurred.

[18] 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 big part of the market or the whole.

[19] risks inherent to the entire market or market segment, reflecting not just the impact of economic, geo-political and financial factors but also the technological vulnerabilities.

[20] this was possible through investor's behavior, which tend to associate Bitcoin's image with the one of the whole market.

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.

Likelihood: The main triggers for market risks are the cyber-attacks and technological risks. According to Blockchain-Graveyard database of crypto attacks, the most frequent and damaging are the ones on cryptographic keys (about half of the total incidents), followed by application vulnerabilities (security breaches) and protocol issues (Magoo.github.io, 2020). As a vicious circle, good financial conditions in the crypto-market can motivate intruders to perform more attacks (Crothers, 2021). Eventually, depending on the amplitude of damaged caused, technological risks might transpose into different financial risks. Since attacks are pretty common in the crypto-market and usually imply important financial losses, we state that the likelihood as high.

Information risk risk refers to the imbalance of information spread among the market players. Conceptually speaking, thanks to its features, Blockchain technology represents itself a useful tool in reducing information asymmetry, assuring transparency and trust. However, along the evolution of the crypto-market, these innovations became more complex, challenging investors and users to acknowledge the potential. The novelty and technological nature of the crypto-market may get stakeholders into trouble, as some do not understand it. At the same time, the lack of knowledge and specific skills, sometimes completed by the insufficient information supplied to the public, increases the uncertainty and restrain towards the whole market.

Compared to any other Blockchain application, initial Coin Offerings (ICO) impose most of the problems regarding the transparency and information asymmetry. The complexity of ICOs' white paper [21], investors' lack of training and the insufficient regulation, led to manipulation and financial losses for investors. According to the existing literature, most investors in this market, lack the required capabilities to interpret the market's signals. The discrepancy between traditional market and crypto-market, pushes investors and users towards questionable sources of information such as social media. Here, the selection is based rather on the 'easy-to-interpret' criteria than quality and credibility. At the same time, the general opinion surrounding the crypto-market seems to influence the players (investors and users), which might take decisions rather based on the social trends (led by a herd mentality [22].) than rationally. This could explain the inefficiency of the crypto-market, despite the quantity of information available (Rui Chen & 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. white / yellow papers, inconsistent data) and insufficient knowledge or understanding for investors and users. Due to the poor regulatory framework, intruders found an opportunity to become rich overnight. They issue low quality crypto-assets, about which there is little information available (incomplete white papers or inconsistent data), and use them to trick the other market players. This risk is behind most of the fraudulent coins or low-quality ICO projects. Reputation might attract more enthusiasts in this market; therefore, we believe that the investors interested in cryptos are pretty various. Here, we introduce the Blockchain literacy (ability to understand the Blockchain related knowledge and make informed and effective decisions (van Rooij et al., 2011))and financial behavior (how individuals gather and interpret information, eventually reflecting in decisional processes (De Bondt et al., 2008)), concepts, as important factors in the way the market evolves. Market signals can be complex, including both information and noise (**?**). Less mysterious than at the beginning, however, still significantly complicated, the Blockchain world might pose some problems in understanding. Blockchain illiteracy leads to irrational behavior, which eventually reflects in inefficient markets. Taking into account the big number

[21] a document describing the technology used in the Blockchain project (ICO). It has the purpose to convince the public that the new crypto-asset offers a good investment opportunity.

[22] a "If I am losing, at least I am not losing alone' mentality – investors might believe that following trends or the majority provides some security and makes losses easier to tolerate (Gazali et al., 2018)

of crypto scams and the important financial losses incurred (especially during the Bitcoin bubble 2017-2018 (Zetzsche et al., 2019; Liebau & Schueffel, 2019)), we state that the likelihood for this risk is high.

Liquidity risk. A market is said to be liquid if an agent can make rapidly some significant trades without creating an important change in the price (small market impact). In other words, in a liquid market, transactions will likely not create a change in the price, but new information will be smoothly incorporated. On the other hand, an illiquid market (most of the time linked to inefficient market), will reflect a large volatility in prices (hence a higher probability of an unfair price), a lower number of investors and lower chances to transact/trade.

Liquidity risk, can be split into three categories: assets liquidity (refers to the interaction between sellers and buyers on the platform and the asset availability on exchanges), exchange liquidity (refers to the interaction between makers and takers concerning the assets' and the orders' supply) and market liquidity (encompasses the first two) (Crowell, 2020). The most debated factors explaining liquidity in the crypto-market are the price, trading volume, capitalization, fees, hash value (for PoW cryptocurrencies) and the size of the network. Contrary to traditional assets, in the crypto-market, high returns are negatively correlated with liquidity, while a rise in trading volume, market capitalization and volatility are associated with lower liquidity uncertainty (Koutmos, 2018). At the same time, liquidity risk is highly correlated with the events concerning cyber-attacks or regulatory issues, as a response to human behavior and investors' attitude towards this market (Corbet et al., 2019). A liquid market will be stable, showing less volatility and a bigger range of orders to pick from. A stable market in a liquid environment is resistant to possible manipulation, such as whales or group orders, placed with the intention to exploit the price benefits. It is important to mention the fact that liquidity is different from one cryptocurrency to another (the most popular ones are more liquid) as well as from one exchange platform to another. In spite of the many benefits associated with liquidity, illiquid environments can also present some advantages, especially for the traders for this market, which can benefit from new arbitrage opportunities and purchases at discounts (Crowell, 2020).

Likelihood: Analyzed from the cryptocurrencies' (crypto-assets that claim to be 'money') perspective, this risk would translate into an impossibility to be transformed in cash. That being said, one of the principal roles of money (being a medium of exchange) has just failed (Greene & McDowall, 2018). There are many triggers behind crypto-assets illiquidity, among which: token supply algorithm, investors' behavior, available supply, asset usage, fees, exchange platforms failure, etc. As liquidity risk is already well-known in the financial markets (is one of the indicators for market efficiency), we already know tools to measure it (trading volumes, book depth and the bid-ask spread, different liquidity ratios, etc.) (M. Jain & Singla, 2018). Similar to traditional securities, crypto-market suffers from illiquidity during extreme price movement period of times (Manahov, 2020). A proof of market efficiency, represents the difficulty to manipulate prices. In the crypto-market, specifically concerning bitcoin, it has been observed a significant hoarding behavior. The number of bitcoin whales increasing to the impressive number of more than 2 thousand addresses [23] (Bitcoin.com, 2020). Beside the fact that hoarding implies a significant movement in prices (buy/sell big amounts of crypto-assets), it has important supply implications as in the end, there are little assets available to trade (Manahov, 2020). Asset usage plays an important role within this market, as the more people believe the assets has value, the more desirability to trade it. The asset usage perception is increasing along with the acceptance and development of crypto-market. Liquidity is an important characteristic of the market, influencing the investment costs and implicitly the desirability to trade. If we look at this risk from the Bitcoin perspective, we could easily state that

[23] Owning between 1,000 to 10,000 BTC.

liquidity risk is very high. At the same time, by capturing the big picture of the crypto-market, where we have over 2000 crypto-assets available, we state that the likelihood is medium.

Supply risk refers to the reserve available of crypto-assets. Some of 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[24], unclaimed rewards (Coinmetrics.com, 2019), reputation and the programmed limit of supplies. Not all the cryptocurrencies have a maximum supply limit. For example, cryptocurrencies 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 models, the higher the supply uncertainty, the less informative crypto-assets prices will be. In this case, market prices are less efficient and supply risk could thus even lead to an information risk (Collomb & Sok, 2016). Compared to national currencies, cryptocurrencies (especially bitcoin) were conceived as being less sensitive to the market changes and inflation rate. However, with time we saw that Satoshi's 'perfect' innovation leaves room for further improvement.

Mainly associated with market inefficiency at users' and exchange platforms' cost, the supply risk is affecting the mining and transaction validation processes, as well. Miners are absolutely necessary in a PoW Blockchain performing both transaction validation and coin 'minting' functions. For successful work, they are rewarded by the system with an amount of newly created crypto coins. The reward offered by the system, represents a method to create new coins and to increase the available supply of cryptocurrencies. At the same time, rewards are programmed to decrease steadily, until the maximum supply will be reached (Eyal & Sirer, 2018). When this happens, the mining reward will be based only on transactions fees (CryptoLi.st, 2020).

Keeping in mind the above arguments, we state that the difficulty to create (mine) new cryptocurrency, the supply limits and the expenses incurred during this process, they all have a great impact on the supply imbalances and the final value of the assets.

Likelihood: Since market liquidity is driven by the total supply available for trade, we understand that it makes it an important characteristic for market efficiency as well. Among the most notable triggers for supply issues, we have: token supply algorithm, hoarding behavior, loss of keys, wallet attacks, etc. (Coinmetrics.com, 2019). If the supply limits are not a risk for all the crypto-assets, it represents a threat at market level, concerning the leader bitcoin. As initially programmed, bitcoin maximum supply is 21 million coins. The already issued coins attain the approximate number of 18 million, supposing that the limit will be reached sometime around 2140 (Ciaian et al., 2015). As we already discussed the negative sides of limited supply (illiquidity and market inefficiency), we will mention now the bright side of this risk. Similar to commodities such as precious metals and natural gas, crypto-assets with limited supply attain high preference (subsequently high value), being regarded as 'scare' assets. By just looking at the price and market share of bitcoin, we can obviously observe that the investor's choices show a specific preference for this coin. In this case, the financial behavior within this market is under the influence of 'scarcity gives value' idea (Verhallen, 1982). However, this idea of value can bring important investment costs, as investors putting their money into such assets, will consider asking for scarcity premiums on top of the existing ones for other risks (Haase & Zimmermann, 2013). By assessing the supply risk at crypto-market level, we state that the likelihood is medium.

Environmental risk. Known as an energy-gourmet, Blockchain technology represents one of the key players in the fight towards the green transition (Charles, 2019). This type of risk concerns specifically the PoW Blockchains, which through their design, require high computational power

[24] e.g. the coins may stay blocked in the intruder's account for a while, attempting to avoid the public eye.

and a lot of electricity, for functioning purposes. According to recent surveys, the bitcoin network is responsible for using about 0.2% of the global electricity and emitting as much carbon dioxide emission as the country of Jordan (Irfan, 2019). Another important aspect to mention is the increasing number of ICOs, which require Ethereum Blockchain (PoW based) for their smart contract application. According to the current statistics, there are over three hundred thousand ether derived crypto-assets (both active and non-active[25] tokens) (CryptoSlate.com, 2020). We believe that the technological constraints regarding the electricity consumption should receive priority consideration; perhaps very soon, the success of ICO projects and the performance of businesses (using Blockchain technology), will be influenced by the environmental considerations. In the light of current environmental context, there were many attempts to reduce the costs and unnecessary pollution, although no significant progress was made so far (Lasla et al., 2020; Saleh, 2021; Bentov et al., 2016; Lepore et al., 2020). The emergence of mining pools, the use of renewable energy (74% of the used electricity is renewable) and lightning network, the emergence of platforms for renting mining power (e.g. Nicehash), first step towards a greener crypto world. Although, we know that there is a long road until we reach the point of zero-emission power (Irfan, 2019). A solution to stimulate a rapid transition to eco-friendly Blockchains, could be the implementation of a tax regime relative to the amount of energy consumed or to the units of carbon emitted per transaction. In this way, the crypto industry could become more aware of its environmental impact, contribute to the domestic economy and hopefully, make an effort to find the best alternative for both the ecosystem and business (Mecca, 2019; Goodkind et al., 2020). Simultaneously, with the increasing sensitivity of investors to social responsibility of their investment (Brown-Liburd & Zamora, 2015), the assets showing negative environmental externalities may be submitted to boycott from investors. The environmental risk thus translates into a financial risk.

Likelihood: We know that during specific economic conditions (pandemics, financial crisis, war, etc.) the stability of financial markets can be highly affected. At the same time, as we learn from the past events, such as the 2008 financial crisis or COVID pandemics, the most performant and least risky investments were the socially responsible ones (Lins et al., 2017; Singh et al., 2020; Palma-Ruiz et al., 2020). Well-informed market players have concerns regarding the enterprise risk management, financial performance and considerations for the surrounding environments (Ballou et al., 2006). As a strategy to decrease the risk exposure and make safer 'investment bets', investors pay careful attention at what kind of assets they put money in and make more socially responsible investments.

Once with the creation of crypto-derivatives and tokenized securities, we can consider that the first step towards a convergence between crypto world and traditional markets was done. Crypto derivatives can now be traded on both exchange platforms and OTC market (Deribit Insights, 2020). Brokers can switch from securities to crypto-assets, or trade both. Regarding investment preferences, it was noticed that during turbulent periods and for safety considerations, investors tend to choose financial markets in the favor of crypto-market (Matkovskyy & Jalan, 2019). Taking into account the investors preference for 'safety bets' and concerns about environmental and social implications, we believe that a more ecologically oriented Blockchain could significantly change the overall 'safety' perception. If this kind of risk doesn't have direct financial losses, it impacts the investment profitability, increasing the costs[26] for financing. As time passes, investors give more attention to the crypto-market, therefore we consider that for the moment the likelihood is Medium. At the same time, we would like to mention that there are big chances that the likelihood becomes high, if from technological point of view nothing changes.

A summary of all financial risks discussed above will be presented in Table 4.

[25] tokens from former ICOs.

[26] E.g. A company issuing ICO projects, can be directly affected by the investors' social considerations, which will reflect in the amount of funds raised or the price/value of their crypto-assets (lower)

Table 4: **Summary of financial risks**

Risk	Trigger	Influence / Consequences	Likelihood
Total market risk	*Cyber-attacks* *Technological risks* *Regulatory mismatches* *Human behavior* *Reputation*	• *Big loses for investors.* • *A sign that the market is not stable and mature* • *Crypto assets trade with a risk premium relative to the risk they may incur*	High
Information risk	*Lack of available information (e.g. white / yellow papers, inconsistent data)* *Lack of knowledge/ understanding* *Reputation*	• *Financial loses for uninformed investors.* • *Assets trade at prices far from their fundamental value*	High
Liquidity risk	*Regulatory mismatches* *Reputation*	• *Less investors* • *Less efficient market*	Medium
Supply risk	*Technological issue (supply limits)* *Cyber- attacks* *Loss of cryptographic keys*	• *Deflation, which can be a problem if crypto-assets will work as a method of payment* • *Less efficient market*	Medium
Environmental risk	*Technological issue (PoW)* *Reputation* *Lack of regulation*	• *Damage for the environment* • *Crypto assets trade with a risk premium relative to their environmental externalities*	Medium

3 Data analysis

In line with the literature review done in the previous sections, here we are going to provide an example of how financial risk is linked to technological vulnerabilities. More specifically, we are going to assess if bitcoin's volatility is affected by the events targeting the crypto-market. This data analysis is an illustration that complements the literature survey performed in this paper, without any intention to transform it in an empirical study. In accordance with the literature and with the aim to answer to our research question, we establish the following 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.
We retrieved bitcoin prices from Thomson Reuters Eikon database and the list of events targeting bitcoin has been taken from Biais et al. (2020). Many other researchers have used the same Eikon database, among which we mention: Corbet et al. (2020); Aliu et al. (2020); Akyildirim et al. (2020) etc. In total, our dataset comprises 53 events (see table 8), and the bitcoin's historical price starts from August 2011 to September 2021.

In order to verify whether technological events have an influence on the perceived risk of cryptocurrencies, 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 for the one between volatility and the amount (in term of bitcoin) lost in each event. Volatility is widely regarded as a signal for risk in finance. Hence, we are looking for a relationship between technological

events (attacks) and financial risk (volatility).

In the following section we are going to compute volatility using 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. The rationale behind choosing these events as a proof of technological vulnerability is the following: most of these events are attacks that were possible thanks to the characteristics of this market. By the characteristics of this market, we mean:

- Cryptocurrencies represent a virtual currency; they exist and operate just in the online environment. This makes them the target of cyberattacks that exploit any possible vulnerability of this technology.
- Cryptocurrencies' users need cryptographic keys in order to access their funds or to place transactions. These keys easily become the source of attacks, when they are not kept safely or the code is easy to break.
- The identity protection (anonymity) offered by the Blockchain technology attracted many enthusiasts, however, this feature makes it almost impossible to catch the hackers / thieves.
- The insufficient regulation and incertitude around cryptocurrency world made them the perfect tool for the black markets; these ones being also the few places accepting cryptocurrencies as a payment.
- Blockchain literacy is slowly increasing. Along the time, the lack of proper understanding about how this crypto world works, was exploited in many forms in order to trick the users and steal their coins. An example would be the many scams performed by crypto-exchange platforms.
- Blockchain is a decentralized technology and its transactions are immutable. That makes it impossible to reverse fraudulent transactions or recuperate the stolen funds. This characteristic together with the anonymity feature may incite malevolent actors to execute their plans.

We compute the monthly standard deviation of bitcoin's returns as:

$$\sigma = \sqrt{\frac{(R-\mu)^2}{n}}$$

Where, R are bitcoin returns, μ is the average return and n is the number of days of the window considered. Accordingly with our hypotheses, we perform the following linear regression:

$$\sigma = \alpha + \beta * EVENT_{number} + \epsilon$$

$$\sigma = \alpha + \beta * EVENT_{amount} + \epsilon$$

Where, $EVENT_{number}$ is 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.

The first regression checks if there is a relationship between the monthly volatility of bitcoin and the number of events per month. The results obtained are significant, with a p value of 0.0216. We therefore conclude that our sample data provided enough evidence to reject the null hypothesis; these results show that there is a relationship between the monthly volatility of bitcoin and the number of events targeting it. Detailed results are shown in appendix section, table 6.

In the second regression, we test if there is a relationship between the volatility level of bitcoin and the amount (in terms of bitcoin) lost as a result of these events. The amounts have been aggregated

on monthly basis. The result obtained (p value of 0.66) show that there is no relationship between the volatility and the amounts lost. Detailed results are shown in appendix section, table 7.

Furthermore, we measure the relationship degree between the volatility and the number of events, using Pearson test and Spearman's rank correlation. Pearson, also known as a parametric correlation test, is one of the most common methods used in assessing 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 with the number of events. The results can be seen in the bellow table 5.

Test	p-value	Correlation estimates	Interpretation
Pearson	0.02156	0.4402268	Moderate positive correlation
Spearman	0.03387	0.4095827	Moderate positive correlation

Table 5: **Correlation tests for *the volatility versus number of events***
The p-values resulted from the correlation tests are less than the significance level alpha = 0.05. We can conclude that the monthly volatility of bitcoin and the number of events targeting it, are moderately correlated with correlation coefficients of 0.44 and 0.40.

It is interesting to observe that according to our analysis, the volatility of bitcoin is not influenced by the financial losses inquired by the users of bitcoin, but rather by the number of attacks, scams or other negative events targeting this market. This result proves that the participants from the crypto-market are more sensitive to cybersecurity risks than financial ones. A way to justify this would be the discrepancy between the users' expectations versus reality. Blockchain technology was created with the purpose to offer a more secure and transparent alternative to the existing payment tools. However, that doesn't make it immune to cyberattacks and scams. At the same time, we argue that Blockchain illiteracy may have a big implication in how crypto-market players behave.

4 Conclusion

The crypto-market emerged in 2008, together with the first cryptocurrency created, bitcoin. Since then, Blockchain technology evolved, potentially disrupting many fields beyond finance. However, it is still in infancy compared to its promised future, the crypto-market has to overcome its many challenges. We believe that understanding and analyzing the crypto-market vulnerabilities, represents the first step in overcoming its challenges.

In this paper we perform a literature survey focusing the types of risks present in the crypto-market. Our focus is on the technological and financial risks of crypto-market and Blockchain technology. First, we show that these risks can be related and that during specific market conditions, they can become a trigger one for another. From our knowledge, this is the first study showing that financial risks can be triggered by the technological vulnerabilities of Blockchain. Second, 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, social responsibility and Blockchain literacy in the stability of crypto-market. Furthermore, to complete this study, we perform a short data analysis, demonstrating that cryptocurrencies' price stability can be disrupted by technological vulnerabilities characteristic to this market. More research is needed on this matter, however, with the little data available, we could show that the bitcoin's volatility level is influenced by the number of events targeting it. These evidences show the implication of cybersecurity risks and Blockchain illiteracy in the crypto-market players' behavior.

Our results support the general discussion from this literature survey, while at the same time answer to our initial research question: 'Can financial risks be triggered by technological vulnerabilities of Blockchain technology?'. The empirical illustration provided in this article cannot be fully considered as an empirical proof. This is mostly due to the size of our database. Broadly speaking,

information related to crypto-market is spread all over the internet, making it complicated when it comes to data collection and research. Up to this point in time, there is no official or centralized database with attacks performed in the crypto-market, but rather a collection of mini statistics. On account of this, our limitation is reducing the possibility to perform empirical studies and accurately assess certain risks.
Finally, we conclude this survey with some research directions, in an attempt to bridge a part of the existent literature gaps:

1. There is need for more research to increase the Blockchain literacy. In spite of the growing interest in the crypto-market, practitioners are still challenged to transfer the Blockchain concept to market-oriented applications. General confidence in this new technology is often shattered by the negative news, scams or attacks targeting this market. With their special features and exponential price changes, cryptocurrencies attract the attention of the large public, including investors, researchers, regulators or hackers. We believe that an increased knowledge and understanding about these innovative technologies will better serve the participants within the crypto-market in making informed decisions; last but not least, it will help this market to evolve towards achieving its full potential.

2. Despite the growing number of empirical papers about crypto-market, we still lack the theory development in this field. With our study, we show that using the existing finance theories is insufficient if the technological characteristics of this market are not taken into consideration. Blockchain technology is not just a new tool; it represents a new way of doing business, a new operational system. Therefore, there is a need of more cross-disciplinary research, that will take into account the important functions and implications of this technology (finance, regulation, cybersecurity, management, etc.).

3. In recent years, there has been a growing awareness of climate change and environmental issues. Knowing that PoW cryptocurrencies represent a threat for our planet health, this subject needs more attention from both practitioners and academics. Investors represent an important group of stakeholders in the crypto-market. Before selecting their preferred investable assets, investors pay now more attention to their options and generally adopt the ESG[27] evaluation criterion. With the ongoing pandemic and the continuous expansion of crypto-market, mainly based on PoW technology, we think that there is an urgent need of research addressing this challenge.

4. In the course of the past decade, Blockchain has evolved while proving its capacity to disrupt various business sectors. Starting with an already complicated technology, namely cryptocurrencies, Blockchain development achieved high levels of both performance and complexity. Innovations such as ICO or DeFi[28] projects are built on stacks of complicated technologies, with each layer carrying an important amount of (attack) risk. With that in mind, we argue that literature should address more the vulnerabilities and risks of this market; more specifically, the ones concerning other Blockchains then bitcoin. An assessment of the risks and vulnerabilities of the crypto-market as a whole, could prevent investors from unnecessary loses, diminish the number of low-quality products and increase performance and efficiency overall.

5. 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 the specialists from governments and industries.

[27] Environmental, Social, and Governance conscientiousness.
[28] Decentralized finance

The only real progress in this direction started just in the beginning of 2017 (Botos, 2017). Knowing that a big part of the vulnerabilities discussed in this survey would have not been possible if proper regulation was in place, we also consider this an area of further research.

Overall, we think this analysis will not only be useful to the existing participants but also to those considering to enter this market, them being practitioners or academics.

References

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

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

Aliu, F., Nuhiu, A., Krasniqi, B. A., & Jusufi, G. (2020, mar). Modeling the optimal diversification opportunities: the case of crypto portfolios and equity portfolios. *Stud. Econ. Financ.*, *38*(1), 50–66. doi: 10.1108/SEF-07-2020-0282

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

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*(July 2015), 164–186. doi: 10.1007/978-3-662-54455-6_8

Ballou, B., Heitger, D., & Landes, C. (2006). The Rise of Corporate Sustainability Reporting: A Rapidly-Growing Assurance Opportunity. *J. Account.*, *202*(6), 65–74. Retrieved from www.globalreporting.org

Beigel, O. (2019). *51% Attack Explained Simply.* Retrieved 2021-01-18, from https://99bitcoins.com/51-percent-attack/

Benoit, S., Colliard, J.-E., Hurlin, C., & Pérignon, C. (2017, mar). Where the Risks Lie: A Survey on Systemic Risk. *Rev. Financ.*, *21*(1), 109–152. Retrieved from https://academic.oup.com/rof/article/21/1/109/2670094 doi: 10.1093/ROF/RFW026

Bentov, I., Gabizon, A., & Mizrahi, A. (2016). Cryptocurrencies Without Proof of Work. *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, *9604 LNCS*, 142–157. Retrieved from https://link-springer-com.gaelnomade-2.grenet.fr/chapter/10.1007/978-3-662-53357-4{_}10 doi: 10.1007/978-3-662-53357-4_10

Biais, B., Bisiere, C., Bouvard, M., Casamatta, C., & Menkveld, A. J. (2020, nov). *Equilibrium Bitcoin Pricing.* Retrieved from https://papers.ssrn.com/abstract=3261063 doi: 10.2139/ssrn.3261063

Bitcoin.com. (2020). *Onchain Data Shows Rising Bitcoin Whale Index Surpassing 4-Year High .* Retrieved 2021-01-18, from https://news.bitcoin.com/onchain-data-shows-rising-bitcoin-whale-index-surpassing-4-year-high/

Blockchain.com. (2020). *Bitcoin Hashrate distribution among mining farms .* Retrieved 2021-01-18, from 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

Botos, H. M. (2017). Bitcoin Intelligence - Business Intelligence meets Crypto Currency. *Cent. Eur. Stud. Work. Pap.*.

Brown-Liburd, H., & Zamora, V. L. (2015, feb). The Role of Corporate Social Responsibility (CSR) Assurance in Investors' Judgments When Managerial Pay is Explicitly Tied to CSR Performance. *Audit. A J. Pract. Theory*, *34*(1), 75–96. doi: 10.2308/AJPT-50813

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*(March), 90–100. Retrieved from https://doi.org/10.1016/j.frl.2019.03.011 doi: 10.1016/j.frl.2019.03.011

Charles, M. (2019). *Technologie: Prometteuse, la blockchain est encore loin de tenir toutes ses promesses.* Retrieved 2021-01-18, from https://www.20minutes.fr/magazine/transition-energetique-mag/2582587-20190813-technologie-prometteuse-blockchain-encore-loin-tenir-toutes-promesses

Ciaian, P., Rajcaniova, M., & d'Artis Kancs. (2015, apr). The economics of BitCoin price formation. *Appl. Econ.*, *48*(19), 1799–1815. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/00036846.2015.1109038 doi: 10.1080/00036846.2015.1109038

CoinGuides.org. (2020). *HashPower Calculator - Convert Hash to kH/s to MH/s to GH/s to TH/s to PH/s.* Retrieved 2021-01-18, from https://coinguides.org/hashpower-converter-calculator/

Coinmetrics.com. (2019). *Coin Metrics' State of the Network: Issue 26 - Coin Metrics' State of the Network.* Retrieved 2021-01-18, from https://coinmetrics.substack.com/p/coin-metrics-state-of-the-network-d2e

Collomb, A., & Sok, K. (2016). *Blockchain et autre registres distribues: quel avenir pour les marches financiers?* (Vol. 15; Tech. Rep. No. 1). Paris: Intitut Louis Bachelier.

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

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, jul). As Bitcoin price surged, it fueled rise in cyberattacks, researchers say. *FOXBusiness*. Retrieved from https://www.foxbusiness.com/technology/bitcoin-price-surged-cyberattacks

Crowell, B. (2020). *Crypto Exchange Liquidity, Explained.* Retrieved 2021-01-18, from https://cointelegraph.com/explained/crypto-exchange-liquidity-and-why-it-matters-explained

Crypto51.app. (2020). *Cost of a 51% Attack for Different Cryptocurrencies.* Retrieved 2021-01-18, from https://www.crypto51.app/

CryptoLi.st. (2020). *Mineable Cryptocurrencies* . Retrieved 2021-01-18, from https://cryptoli.st/lists/mineable

CryptoSlate.com. (2020). *Token Cryptocurrencies* . Retrieved 2021-01-18, from https://cryptoslate.com/cryptos/tokens/

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

De Bondt, W., Muradoglu, G., Shefrin, H., & Staikouras, S. K. (2008). Behavioral Finance: Quo Vadis? *J. Appl. Financ.*, *18*(2).

Deribit Insights. (2020). *Exchange vs Over-the-Counter (OTC) Bitcoin Trading* . Retrieved 2021-01-18, from https://insights.deribit.com/market-research/exchange-vs-over-the-counter-otc-bitcoin-trading/

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. Retrieved from https://doi.org/10.1016/j.csi.2019.103409 doi: 10.1016/j.csi.2019.103409

Eyal, I., & Sirer, E. G. (2018). Majority Is Not Enough: Bitcoin mining is vulnerable. *Commun. ACM*, *61*(7), 95–102. doi: 10.1145/3212998

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

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*, 64–68. doi: 10.1109/ICT4M.2018.00021

Goffard, P. O. (2019). Fraud risk assessment within blockchain transactions. *Adv. Appl. Probab.*, *51*(2), 443–467. doi: 10.1017/apr.2019.18

Goodkind, A. L., Jones, B. A., & Berrens, R. P. (2020). Cryptodamages: Monetary value estimates of the air pollution and human health impacts of cryptocurrency mining. *Energy Res. Soc. Sci.*, *59*(August 2019), 101281. Retrieved from https://doi.org/10.1016/j.erss.2019.101281 doi: 10.1016/j.erss.2019.101281

Greene, R., & McDowall, B. (2018). *Liquidity Or Leakage-Plumbing Problems With Cryptocurrencies Liquidity Or Leakage Plumbing Problems With Cryptocurrencies Liquidity Or Leakage-Plumbing Problems With Cryptocurrencies* (Tech. Rep.). Cardano Foundation & Long Finance.

Haase, M., & Zimmermann, H. (2013, jun). Scarcity, Risk Premiums, and the Pricingof Commodity Futures: The Case of Crude Oil Contracts. *J. Altern. Investments*, *16*(1), 43–71. Retrieved from https://jai.pm-research.com/content/16/1/43https://jai.pm-research.com/content/16/1/43.abstract doi: 10.3905/JAI.2013.16.1.043

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*(2), 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).

Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harv. Bus. Rev.*, *2017*(January-February).

Irfan, U. (2019). *Bitcoin mining: a report finds the network mostly runs on renewables - Vox.* Retrieved 2021-01-18, from https://www.vox.com/2019/6/18/18642645/bitcoin-energy-price-renewable-china

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, M., & Singla, R. (2018, apr). Liquitity and its measures. *Int. J. Res. Anal. Rev.*, *5*(2). Retrieved from http://ijrar.com/

Jain, P. K., McInish, T. H., & Miller, J. L. (2019, dec). Insights from bitcoin trading. *Financ. Manag.*, *48*(4), 1031–1048. Retrieved from https://www. doi: 10.1111/fima.12299

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

Koshik, R. (2019). *What Blockchain developers learn from Eclipse Attacks in bitcoin network.* Retrieved 2021-01-18, from 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. Retrieved from https://doi.org/10.1016/j.econlet.2018.08.041 doi: 10.1016/j.econlet.2018.08.041

Lasla, N., Alsahan, L., Abdallah, M., & Younis, M. (2020). *Green-PoW: An Energy-Efficient Blockchain Proof-of-Work Consensus Algorithm.* Retrieved from https://mdsoar.org/handle/11603/20600

Leemoon, B. (2017). *Bitcoin Valuation Framework Pub Boom or Bust.* doi: 10.13140/RG.2.2.26771.99366

Lemieux, V. L. (2016). Trusting records: is Blockchain technology the answer? *Rec. Manag. J.*, *26*(2), 110–139. doi: 10.1108/RMJ-12-2015-0042

Lepore, C., Ceria, M., Visconti, A., Rao, U. P., Shah, K. A., & Zanolini, L. (2020, oct). A Survey on Blockchain Consensus with a Performance Comparison of PoW, PoS and Pure PoS. *Math.*, *8*(10), 1782. Retrieved from https://www.mdpi.com/2227-7390/8/10/1782/htmhttps://www.mdpi.com/2227-7390/8/10/1782 doi: 10.3390/MATH8101782

Liebau, D., & Schueffel, P. (2019). *Crypto-Currencies and ICOs: Are They Scams? An Empirical Study.* Retrieved from https://www.researchgate.net/publication/330922954 doi: 10.2139/ssrn.3320884

Lins, K. V., Servaes, H., & Tamayo, A. (2017). Social Capital, Trust, and Firm Performance: The Value of Corporate Social Responsibility during the Financial Crisis. *J. Finance*, *72*(4), 1785–1824. doi: 10.1111/jofi.12505

Litecoinpool.org. (2020). *Hash Rate Distribution — litecoinpool.org.* Retrieved 2021-01-18, from https://www.litecoinpool.org/pools

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

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. IEEE 16th Int. Conf. Pervasive Intell. Comput. IEEE 4th Int. Conf. Big Data Intell. Comput. IEEE 3*, 114–120. doi: 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00031

Magoo.github.io. (2020). *Blockchain Graveyard.* Retrieved 2021-01-18, from https://magoo.github.io/Blockchain-Graveyard/

Manahov, V. (2020, sep). Cryptocurrency liquidity during extreme price movements: is there a problem with virtual money? *Quant. Financ.*, *21*(2), 341–360. Retrieved from https://www-tandfonline-com.gaelnomade-2.grenet.fr/doi/abs/10.1080/14697688.2020.1788718 doi: 10.1080/14697688.2020.1788718

Marcus, Y., Heilman, E., & Goldberg, S. (2018, mar). Low-resource eclipse attacks on Ethereum's peer-to-peer network. *Cryptol. Rep.*, *236*. Retrieved from https://open.bu.edu/handle/2144/39208

Matkovskyy, R., & Jalan, A. (2019, dec). From financial markets to Bitcoin markets: A fresh look at the contagion effect. *Financ. Res. Lett.*, *31*, 93–97. doi: 10.1016/J.FRL.2019.04.007

Mecca, B. (2019). *How can we reduce Bitcoin pollution? — Yale Environment Review.* Retrieved 2021-01-18, from https://environment-review.yale.edu/how-can-we-reduce-bitcoin-pollution-0?fbclid=IwAR2c8Hm1lyh6PvSfQ{_}G8OBLMGVLS8xDykqyISe8l3amw4Xsx4wSFefsa9rQ

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

Notheisen, B., & Weinhardt, C. (2019, feb). *The blockchain, plums, and lemons: Information asymmetries & transparency in decentralized markets* (No. 130). Retrieved from https://publikationen.bibliothek.kit.edu/1000092486 doi: 10.5445/IR/1000092486

Packtpub. (2019). *What Blockchain developers learn from Eclipse Attacks in bitcoin network.* Retrieved 2021-10-05, from https://hub.packtpub.com/what-can-blockchain-developers-learn-from-eclipse-attacks-in-a-bitcoin-network-koshik-raj/

Palma-Ruiz, J. M., Castillo-Apraiz, J., & Gómez-Martínez, R. (2020, jul). Socially Responsible Investing as a Competitive Strategy for Trading Companies in Times of Upheaval Amid COVID-19: Evidence from Spain. *Int. J. Financ. Stud.*, *8*(3), 41. Retrieved from https://www.mdpi.com/2227-7072/8/3/41/htmhttps://www.mdpi.com/2227-7072/8/3/41 doi: 10.3390/IJFS8030041

Patel, D. (2020). Blockchain Technology towards the Mitigation of Distributed Denial of Service Attacks. *Int. J. Recent Technol. Eng.*, *8*(6), 961–965. doi: 10.35940/ijrte.f7420.038620

Pawczuk, L., Massey, R., & Holdowsky J. (2019). *Deloitte's 2019 Global Blockchain Survey* . Retrieved 2021-01-18, from https://www2.deloitte.com/content/dam/insights/us/articles/6608{_}2020-global-blockchain-survey/DI{_}CIR2020globalblockchainsurvey.pdf

Pearson, E. S. (1932, dec). The Test of Significance for the Correlation Coefficient: Some Further Results. *J. Am. Stat. Assoc.*, *27*(180), 424. doi: 10.2307/2278641

Pereira, É. D., & Ferreira, P. (2019, jul). Contagion Effect in Cryptocurrency Market. *J. Risk Financ. Manag.*, *12*(December 2017), 115. Retrieved from www.mdpi.com/journal/jrfm doi: 10.3390/jrfm12030115

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. Retrieved from https://doi.org/10.1016/j.elerap.2020.100936 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.

Saleh, F. (2021, feb). Blockchain without Waste: Proof-of-Stake. *Rev. Financ. Stud.*, *34*(3), 1156–1190. Retrieved from https://academic.oup.com/rfs/article/34/3/1156/5868423 doi: 10.1093/RFS/HHAA075

Salmela, S. (2019). *Micro-level legitimacy in new industry creation – the role of media in legitimacy construction* (Master thesis). Turku School of Economics.

Shane, D. (2018, jan). *Coincheck: $530M cryptocurrency heist may be biggest ever.* Retrieved 2021-10-05, from https://money.cnn.com/2018/01/29/technology/coincheck-cryptocurrency-exchange-hack-japan/index.html

Singh, A., Click, K., Parizi, R. M., Zhang, Q., Dehghantanha, A., & Choo, K. K. R. (2020). Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *J. Netw. Comput. Appl.*, *149*(July 2019), 102471. Retrieved from https://doi.org/10.1016/j.jnca.2019.102471 doi: 10.1016/j.jnca.2019.102471

Spearman, C. (1904, jan). The Proof and Measurement of Association between Two Things. *Am. J. Psychol.*, *15*(1), 72. doi: 10.2307/1412159

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*(6). doi: 10.1098/rsos.180410

Swan, M. (2017). Expectation on Blockchain : Blockchain Economics and Finance. *Front. Blockchain, Intell. Chijo (Intelplace), Cent. Glob. Commun. (GLOCOM), Int. Univ. Japan.*, *121*, 17–24.

Tapscott, D., & Tapscott, A. (2016). *The Impact of the Blockchain Goes Beyond Financial Services.* Retrieved from https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services

Tuwiner, J. (2021). *Bitcoin Mining Pools.* Retrieved 2021-04-10, from https://www.buybitcoinworldwide.com/mining/pools/

Underscore VC. (2018). *Future of Blockchain Survey & Results — Underscore VC.* Retrieved 2021-01-18, from https://underscore.vc/blog/future-of-blockchain-survey-results/

van Rooij, M., Lusardi, A., & Alessie, R. (2011, aug). Financial literacy and stock market participation. *J. financ. econ.*, *101*(2), 449–472. doi: 10.1016/J.JFINECO.2011.03.006

Verhallen, T. M. (1982, dec). Scarcity and consumer choice behavior. *J. Econ. Psychol.*, *2*(4), 299–322. doi: 10.1016/0167-4870(82)90034-4

Wachsman, M. (2019). *Research: Blockchain must overcome hurdles before becoming a mainstream technology.* Retrieved 2021-10-03, from https://www.zdnet.com/article/research-blockchain-must-overcome-hurdles-before-becoming-a-mainstream-technology/

Wüst, K. ., & Gervais, A. (2016). *Ethereum Eclipse Attacks* (Tech. Rep.). ETH Zurich Research Collection. Retrieved from https://doi.org/10.3929/ethz-a-010724205 doi: 10.3929/ethz-a-010724205

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*(2), 267. Retrieved from https://heinonline.org/HOL/Page?handle=hein.journals/hilj60{&}id=276{&}div={&}collection=

Zhang, S., Zhou, X., Pan, H., & Jia, J. (2019, mar). Cryptocurrency, confirmatory bias and news readability – evidence from the largest Chinese cryptocurrency exchange. *Account. Financ.*, *58*(5), 1445–1468. Retrieved from https://coinmarketcap.com/ doi: 10.1111/acfi.12454

A Appendix

Table 6: **Linear regression 1**
Summary of the OLS regression used to identify the relationship between monthly volatility and the number of events targeting bitcoin.

Dep. Variable:	Volatility	**Df Model:**	1
Model:	OLS	**R-squared:**	0.1938
Method:	Least Squares	**Adj. R-squared:**	0.1616
Date:	24 September 2021	**F-statistic:**	6.01
No. of Observations:	27	**Prob. (F-statistic):**	0.02156
Df Residuals:	25	**Residual standard error:**	0.2482

Coefficients:

Model		**Estimate**	**Std. Error**	**t**	**p-value**
H_1	(Intercept)	0.077	0.11783	0.657	0.517
	$EVENT_{number}$	0.18761	0.07653	2.451	0.0216*

*The **p-value** obtained from this regression is 0.0216*. This result is significant and is less than the significance level alpha: 0.05. We can therefore conclude that there is a relationship between the monthly volatility and the number of events targeting bitcoin.*

Table 7: **Linear regression 2**
Summary of the OLS regression used to identify the relationship between monthly volatility and the amounts lost (BTC).

Dep. Variable:	Volatility	**Df Model:**	1
Model:	OLS	**R-squared:**	0.007838
Method:	Least Squares	**Adj. R-squared:**	-0.03185
Date:	24 September 2021	**F-statistic:**	0.1975
No. of Observations:	27	**Prob. (F-statistic):**	0.661
Df Residuals:	25	**Residual standard error:**	0.2754

Coefficients:

Model		**Estimate**	**Std. Error**	**t**	**p-value**
H_1	(Intercept)	3.34E-01	5.57E-02	5.992	2.95e-06 ***
	$EVENT_{amount}$	1.64E-07	3.68E-07	0.444	0.661

*The **p-value** obtained from this regression is 0.661. This result is higher than the significance level alpha: 0.05. Therefore, we conclude that there is no relationship between the monthly volatility of bitcoin and the amounts lost during the events targeting bitcoin.*

Table 8: **Hacks, thefts and losses events related to Bitcoin**
Source: (Biais et al., 2020)

	Date	Amount.loss.(BTC)	Description
1	15138.00	25000.00	Early user Allinvain was hacked
2	15144.00	2000.00	MtGox theft - compromised account
3	15150.00	4019.00	MyBitcoin theft - wallet keys hacked
4	15181.00	17000.00	Bitomat loss - Wallet access lost
5	15184.00	78739.00	MyBitcoin theft - wallet website hacked
6	15253.00	5000.00	Bitcoin7 hack
7	15275.00	2609.00	MtGox loss due to hacking
8	15400.00	46653.00	Linode hacks
9	15443.00	3171.00	Betcoin hack
10	15457.00	20000.00	Tony76 Silk Road scam
11	15471.00	18547.00	Bitcoinica hack
12	15525.00	1853.00	MtGox hack
13	15534.00	40000.00	Bitcoinica theft - due to server hack
14	15538.00	180819.00	BST Ponzi scheme
15	15552.00	4500.00	BTC-e hack
16	15587.00	24086.00	Bitfloor theft - wallet keys hacked
17	15611.00	9222.00	User Cdecker hacked
18	15630.00	3500.00	Trojan horse
19	15695.00	18787.00	Bitmarket.eu hack
20	15835.00	1454.00	Vircurex hack
21	15866.00	1300.00	PicoStocks hack
22	15980.00	29655.00	FBI seizes Silk Road funds
23	16003.00	144336.00	FBI seizes Silk Road funds
24	16004.00	22000.00	GBL scam
25	16016.00	4100.00	Inputs.io hack
26	16021.00	484.00	Bitcash.cz hack
27	16038.00	5400.00	Sheep Marketplace hacked & closes
28	16038.00	5896.00	PicoStocks hack
29	16114.00	4400.00	Silk Road 2 hacked
30	16126.00	744408.00	MtGox collapse due to hacks losses
31	16133.00	896.00	Flexcoin hack
32	16133.00	97.00	Poloniex hack
33	16154.00	950.00	CryptoRush hacked
34	16357.00	3894.00	Mintpal hack
35	16440.00	18886.00	Bitstamp hack
36	16463.00	1000.00	796Exchange hack
37	16481.00	7170.00	BTER hack
38	16483.00	3000.00	KipCoin hack
39	16577.00	1581.00	Bitfiniex hack
40	16693.00	5000.00	BitPay phishing scam - hacker takes over the CEO's accounts and access
41	16815.00	11325.00	Cryptsy hack
42	16898.00	315.00	ShapeShift hack
43	16904.00	154.00	ShapeShift hack
44	16935.00	250.00	Gatecoin hack
45	17015.00	119756.00	Bitfinex hack
46	17087.00	2300.00	Bitcurex hack
47	17278.00	3816.00	Yapizon hack
48	17359.00	1942.00	AlphaBay admins assets sized by FBI
49	17367.00	1200.00	Hansas funds seized by Dutch police
50	17506.00	4736.00	NiceHash hacked
51	17702.00	2016.00	Bithumb hacked
52	17794.00	5966.00	Zaif hacked
53	17832.00	8.00	MapleChange hack / scam