Blockchain technology and crypto-assets market analysis: vulnerabilities and risk assessment

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

Blockchain technology and crypto-assets market analysis: vulnerabilities and risk assessment

Jean-Guillaume **DUMAS** [0000-0002-2591-172X]
CNRS, LJK, Université Grenoble Alpes
Grenoble, F-38040, France

Sonia **JIMENEZ-GARCES**
CERAG, Université Grenoble Alpes
Grenoble, F-38040, France

Florentina **ȘOIMAN** [0000-0002-2794-7726]
CNRS, CERAG, LJK, Université Grenoble Alpes
Grenoble, F-38040, France
{Firstname.Lastname}@univ-grenoble-alpes.fr

ABSTRACT

After ten years of continuous development and innovation, the cryptomarket and the Blockchain technology are still very much challenged and far from the mainstream adoption. We thus propose a risk assessment, as well as a market analysis of the Blockchain technology and the cryptomarket. This study is conceived as a two-level analysis. We first start with the micro-level analysis by performing a detailed risk assessment. Here, we take into consideration technological issues, such as such as consensus, network, cryptographic primitives, quantum and smart contract attacks, together with financial concerns such as market, information, liquidity, supply, reputation and environmental risks. Moreover, we propose ways to determine the probability that technological vulnerabilities can trigger financial risk. Here, we tackle concepts such as financial behavior, responsible investment and Blockchain literacy, as possible tools for assessing risk. Then, we complete this study with a macro-level analysis, which consists of the crypto-market appraisal performed with the Porter's five forces model. This market analysis is performed with respect to its stakeholders, such as the business process managers, investors, regulators, firms, developers, miners, hackers, exchange and trading platforms, etc. The results are relative to: 1. an identified continuity between the technological risks and financial ones; 2. a way to determine the likelihood of triggering financial risks through technical vulnerabilities; 3. a long-term profitability of the stakeholders' strategy / position within the market.

Keywords: Blockchain, Risk assessment, Financial risks, Technological characteristics, Stakeholders, Financial behavior, Blockchain literacy, Socially responsible investment

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 and social barriers (Lakhani & Iansiti, 2017; 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; Lakhani & Iansiti, 2017). Inspired from the existing systems, the solutions promised by Blockchain are more beyond what we currently use. 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 cryptomarket.

According to Lakhani and Iansiti (2017), there are two dimensions affecting the way technology evolves. The first dimension represents novelty, referring to the degree of originality, uniqueness and perceived use in comparison with the existing systems. The second dimension refers to complexity, implying the extent to which this technology touches various fields, regardless the market or specialty. The same idea is sustained by the findings obtained in recent research, where it was revealed that some of the main barriers in Blockchain adoption 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. explored the relationship between human conduct and the intention to invest in the cryptomarket. Consequently, they found out that the attitude towards the cryptomarket, the social norms1, the risk tolerance and the perceived benefits coming from using this technology, represent some of the main factors influencing interested parties to invest or to be part of the cryptomarket.

Among the existing research literature, several studies have addressed the cryptomarket 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., 2018; Drljevic, Aranda and Stantchev, 2019; Patel, 2020), while others just to increase general awareness (Saad et al., 2020; 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 cryptomarket. In the light of this fast-paced world and in order to overcome the challenges faced by this complex technology, we first identify and present its major risks. Compared to previous papers, where risks were usually treated based on their nature (i.e. economic, political, regulatory, etc.), 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 propose ways to determine the likelihood that technological risks could transform into financial ones. The stakeholders[2] of the crypto market have an important role in our analysis approach. We perform the second assessment, specifically the market analysis, with respect to them. We believe that stakeholders can be strongly influenced by the risks of this market, based on their role played and degree of involvement.

This study is a literature based research. Compared to other areas, finance is mostly dominated by quantitative analyses. However, we believe that a new field of research like cryptomarket, 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 and non-academic literature. The selection of papers and data was done by taking into account the topic of investigation. We have used a big variety of keywords such as: crypto, Blockchain, financial risk, technological risk, attack, financial behavior, Blockchain literacy, etc. The identified questions in leading this study, are: 'Can financial risks be triggered by technical vulnerabilities of Blockchain technology?', 'If yes, what is the likelihood that this happens?'.

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

[2] We consider as stakeholders of the crypto-market, the following players: the users of a Blockchain-based process, but also the inventors or developers, the miner or transactions' validators, the hackers, the investors, the exchange and trading platforms, the governments and regulators, the firms, etc. (see appendix 1)

The below figure aims to show the two-level analysis approach used in this research paper.

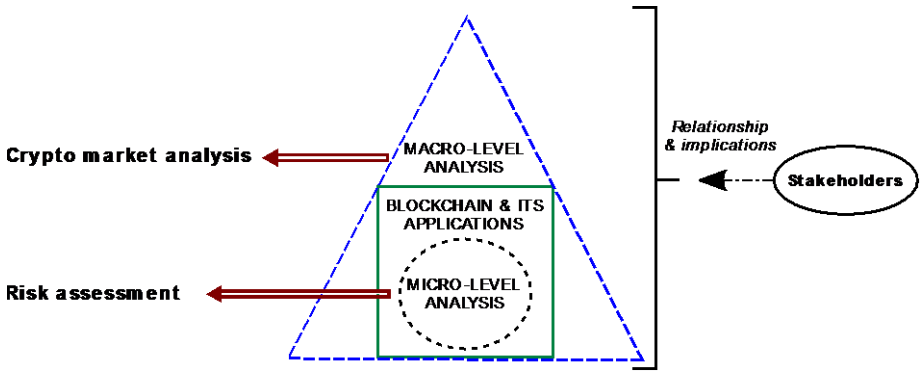

Fig. 1: Multilevel model of analysis (own representation to visualize the contribution of the study)

Fig. 1 illustrates the methodological approach used in this paper. The dashed lines represent the contribution made through this research. The central point of focus is the Blockchain and its applications, which, together, form the crypto market. Stakeholders are taken into consideration as well, highlighting their relationship and implications with the market. The macro-level analysis consists of a crypto-market study, while the micro-level analysis refers to the risk assessment.

The first objective of this paper is to contribute to the scientific literature in the field of management. With the aim to enlighten our research problem, the objective of this paper is to provide a two-dimension risk analysis (technological and financial) completed by an assessment of triggering elements (the likelihood). Furthermore, we show that the threats and vulnerabilities affecting the technology's evolution are very much linked to Blockchain literacy and stakeholders' behavior. At the same time, we highlight the shareholders' exposure and offer support in their decision-making processes. With our research we contribute to both dimensions affecting the technology's evolution (Lakhani and Iansiti, 2017), while also tackling some of the factors influencing stakeholders' behavior (Gazali et al., 2018).

This paper is organized as follows. We start with the introduction. Section 2 comprises a short presentation of the existing types of Blockchain, followed by the assessment of technological and financial risks. Section 3 presents the crypto market analysis, performed with the Porter's five forces methodology. Finally, we conclude in section 4.

2 BLOCKCHAIN RISKS ASSESSMENT

Before scrutinizing the threats and vulnerabilities of the crypto-market, it is important to understand the implications and applications of the Blockchain technology. Therefore, we will start by providing a brief introduction to the existing Blockchain networks

.

2.1 Types of Blockchain technology

As we know, Blockchain technology refers to chains of blocks underlying transactional information. Initially conceived as a permissionless ledger and open to wide public technology, nowadays Blockchain has been developed in different other versions.

Fig. 2 shows that there exist four types of Blockchain, each categorized based on their operation, user type, technical key features and last but not least, their innovative contributions to the existing markets

and businesses: **Public** (Permissionless & Open), **public & hybrid** (Permissioned & Open), **private** (Permissionless & Closed) and **private & hybrid** (Permissioned & Closed). The main key factors taken into account in differentiating Blockchains, are: the permission dimension (limitations concerning the miners' right to write and amend the ledger), the openness (limitations concerning the users' right to access and add data within the ledger), de/centralization dimension (concerning the type of governance) and, last but not least, the type of technology (public -anyone can access it and become part of the network or private - only restricted/predefined members have access and can be part of the network).

Powerful, however not immune to threats and vulnerabilities, some of these derived versions of the Blockchain represent just a step forward towards a better technology. As promising as the public version, but with a different operational approach, the private Blockchain are mostly addressed to firms and organisations, which need a full control over the technology network and personalized solutions to their existing challenges.

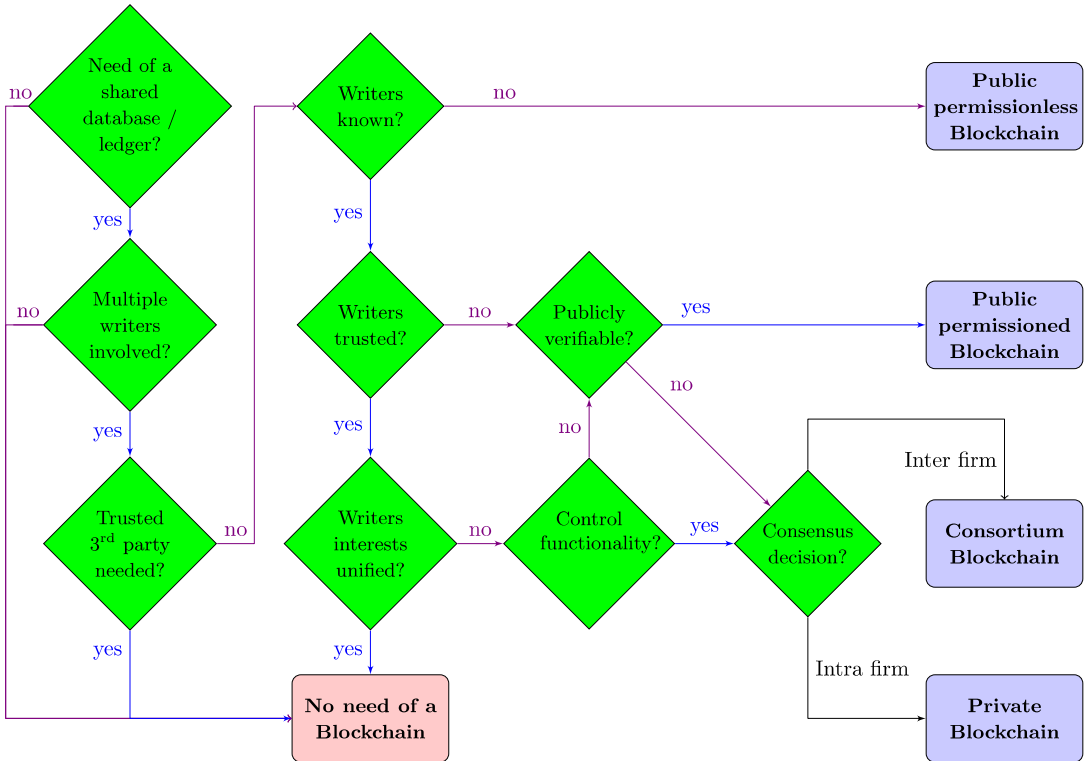

Fig. 2: Blockchain decision tree for business process management
Source: adapted after (Exterkate & Wagenaar, 2018)

2.2 Risks assessment

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

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

While all four types of risks are indisputably affecting the cryptomarket 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?''.

2.2.1 Technological risks

We systemize the cryptomarket threats in accordance with their nature. There are many types of attacks which are not discussed in this study. However, we tried to cover the most important ones.

We systemized 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 some 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.

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

Table 1. Comparison of most notable consensus mechanisms used in the Blockchain applications (own representation)

The most noteworthy **attacks at the consensus level**, are:
Nothing at stake attack: on the PoS algorithm, 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 have little to lose (Morganti, et al., 2018).
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[3]" and "the 51% stake attack[4]" (Tuwiner 2020, Blockchain.com 2020).

[3] an attack on the PoW algorithm, implying the possession of more than 50% of the total mining power, with the purpose to manipulate and corrupt the network
[4] An attack targeting the PoS algorithm; 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 table below presents the necessary computational power and implied financial expenses in order to perform a majority attack.

System	*Hash rate*[5]	*1 h attack estimated Cost*
Bitcoin	*112,458 PH/s*	*$560,359*
Ethereum	*171 TH/s*	*$111,891*
B. Cash	*1,766 PH/s*	*$9,919*
B. SV	*1,601 PH/s*	*$7,386*
Litecoin	*177 TH/s*	*$13,189*
Dash	*5 PH/s*	*$2,801*
Zcash	*5 GH/s*	*$10,575*

Table 2. PoW 51% attack cost for the top 7 cryptocurrencies. Values computed as per 24th April 2020 [6]
Source: derived from (Crypto51.app, 2020)

Network level attack are widely considered difficult and expensive to perform (Packt Hub, 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 cryptomarket, as they can target Blockchains[7], 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 (Williams, 2017).

Some other notable examples of network level attacks, worth to mention are the Sybil attack[8] and the Eclipse attack[9]. From our knowledge, there is no successful execution in practice of these attacks on the Blockchain technology, however, theoretical demonstrations prove that Eclipse attacks are possible on PoW (Ether and Bitcoin) (Heilman et al. 2015, Packt Hub 2019, Marcus et al. 2018, Wüst & Gervais 2016) and PoS networks (Zhang & Lee, 2019). Frequently, the network level attacks are planned so they can precede other assaults (Morganti, et al., 2018; Wüst & Gervais 2016; Zhang & Lee, 2019; Heilman et al. 2015).

Cryptographic key attacks. In Blockchain technology, the 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,

[5] The Hashing power is expressed in different units: TH = TeraHash; MH = MegaHash; KH = KiloHash; GH = GigaHash (CoinGuides.org, 2020).

[6] The values computed take into account the expenses incurred in the mining process, namely the network hash rate & the Nicehash cost per hour (rented PC power). These values can change every minute (Crypto51.app, 2020)

[7] 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. 2020).

[8] a user creates multiple identities and uses them to gain dominance and manipulate the Blockchain system

[9] 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

hardware, cloud, brain[10] 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 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[11]. This statement is also supported by statistical evidences, as Blockchain Graveyard organization show that more than half of the total Blockchain incidents, relate to wallet attacks (Magoo.github.io, 2020). Some other notable examples of attacks at this level, are: the *Random number generator attack* [12] and *Quantum attacks*[13].

Smart contract attacks: mainly refer to the manipulation of external data entered in the Blockchain misleading the execution of the smart contract. The trigger represents information related to external events, which affects the contract's conditions. This 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 represents 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, Bartoletti and Cimoli, 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 (Lee 2019, Hasanova et al. 2019).

A summary of all technological risks discussed above will be presented in Table 3.

2.2.2 Financial risks

In this section, we give example of several financial risks that can be triggered by technological vulnerabilities. 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: we take into account the severity effect[14] and the probability of occurrence of triggering elements (e.g. attacks, technological weaknesses, etc.). An official database on Blockchain attacks would be very useful, so we could determine the most likely probability

[10] 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.

[11] 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).

[12] 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.

[13] 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)

[14] Such as financial loses and the investment cost incurred

distribution from which financial risks have raised. In the absence of such data or any other relevant information that could help to establish a statistical measurement, we will limit ourselves to an abstract and more intuitive sense of likelihood, based on the vast literature reviewed. At this point, we will also introduce the concepts financial behavior, responsible investment and Blockchain literacy, as possible tools for assessing risk.

Total market risk. This is the financial risk arising from high movements in market prices. The most used measure for appraising the total market risk of an asset is the volatility of its market returns.

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 algorithm (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*

[15] The total number of cryptocurrencies is over 2500 (CryptoSlate.com, 2020)

[16]The total number of mining pools is not known, as there are many which keep their identity secret. Therefore, we cannot accurately assess the market exposure with this respect.

Smart contract threats	**Re-entrancy 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)*

Following the traditional financial theory, the total market risk can be decomposed into the systematic risk and the specific one. 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 cryptomarket 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[17]. For instance, majority attacks (almost half of the total cryptomarket 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[18]. 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 vulnerability 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, impacting eventually the cryptomarket's volatility. Bitcoin, Ether or any other strong and well-known coin have proved their influence over the evolution of the whole cryptomarket. In 2017, when Bitcoin prices skyrocketed and crashed, the rest of the cryptocurrencies followed a similar trend (Antonakakis et al. 2019, Ferreira & Pereira 2019). The strong power of influence and the herding behavior present in the cryptomarket, 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[19], impacting the whole market (Jain & Jain, 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 cryptomarket, 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 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 cryptomarket can motivate intruders to initiate more attacks (Williams, 2017). Eventually, depending on the amplitude of damage caused, technological risks might transpose into different financial risks. Since attacks are pretty common in the cryptomarket and usually imply important financial losses, we state that the likelihood as high.

[17] 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.

[18] 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.

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

Information 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 cryptomarket, these innovations became more complex, challenging investors and users to acknowledge the potential. The novelty and technical nature of the cryptomarket 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) expose most of the problems regarding the transparency and information asymmetry. The complexity of ICOs' white paper[20], 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 cryptomarket, pushes investors and users towards questionable sources of information such as social media. Here, the selection is based rather on the 'easy-interpretable' criteria than quality and integrity. At the same time, the general opinion surrounding the cryptomarket seems to influence the players (investors & users), who might take decisions rather based on social trends (led by a herd mentality[21]) than rationally. This could explain the inefficiency of the cryptomarket, 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 cryptomarket, we have the lack of available information (e.g. white / yellow papers, inconsistent news) and insufficient knowledge or understanding for investors and users. Thanks to the poor regulatory framework, intruders may find opportunities to become rich overnight. For example, issuing low quality crypto-assets about which, there is little information available (incomplete or missing white papers), and use them to trick the other market players. This risk hides behind most of the fraudulent coins or low-quality ICO projects. Reputation attracts more enthusiasts in this market, therefore, we believe that a diverse type of investors is interested in cryptos. Here, we introduce the Blockchain literacy (ability to understand the Blockchain related knowledge and make informed decisions) (Van Rooij et al., 2011) and financial behavior (how individuals collect and interpret the information, eventually reflects 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 (Rizzi, 2008). 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 of crypto scams and the important financial losses incurred (especially during the Bitcoin bubble 2017-2018 (Zetzsche et al., 2019, Liebau, et al., 2019)), we state that the likelihood for this risk is high.

Liquidity risk. 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 (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.

Contrary to traditional assets, in the cryptomarket, 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

[20] 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

[21] A "If I am losing, at least I am not losing alone' mentality – investors might believe that following the trends or what is the majority doing, gives them more security and makes losses easier to digest (Gazali et al., 2018).

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 volatile prices 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, such as new arbitrage opportunities and purchases at discounts (Crowell, 2020).

Likelihood: Analyzed from the cryptocurrencies' (crypto-assets that claim to be 'money') angle this risk would translate into an impossibility to be transformed in cash. That being said, one of the main duties of money (being a medium of exchange) has just failed (Greene and 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.) (Jain & Singla, 2020). Similar to traditional securities, cryptomarket 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 cryptomarket, 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[22] (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 less assets available to trade (Manahov, 2020). Asset usage plays an important role within this market, as the more people believe that crypto has value, the more desirability to trade it. The asset usage perception is increasing along with the acceptance and development of cryptomarket. 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's angle, we can easily see that liquidity risk is high. At the same time, by capturing the big picture of the cryptomarket, we state that the likelihood is medium.

Supply risk refers to the reserve available of crypto-assets. 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[23], unclaimed rewards (Coinmetrics.com, 2019), reputation and the programmed crypto supply. Not all the cryptocurrencies have a 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, Satoshi Nakamoto's innovation proved to be imperfect, leaving considerable room for further development.
Mainly associated with market inefficiency at users' (and exchange platforms') cost, the supply risk is affecting also the mining and transaction validation processes. Miners are absolutely necessary in a PoW Blockchain performing both transaction validation and coin 'minting' functions. Only for successful work, they are rewarded by the system with an amount of newly created crypto coins. This reward represents a method to create new coins and to increase the available supply of cryptocurrencies. With time, we observe that rewards are programmed to decrease steadily, until the

[22] Owning between 1,000 to 10,000 BTC
[23] e.g. the coins may stay blocked in the intruder's account for a while, attempting to avoid the public eye.

maximum supply is reached (Eyal & Sirer, 2018). When this happens, the mining reward will be the transactions fees (Cryptoli.st, n.d.).
By keeping in mind the above ideas, we state that the difficulty to create (mine) new cryptocurrencies, the supply limits and the expenses incurred during this process, have all a great impact on the supply imbalances and the final value of these assets.

Likelihood: As 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 limit is not a risk for all crypto-assets, it represents a threat at market level, especially concerning the coin leader. As initially programmed, bitcoin maximum supply is 21 million coins. Up to now, we have issued approximately 18 million, supposing that the limit will be reached around 2140 (Ciaian et al., 2015). As we have discussed the negative sides of limited supply (illiquidity and market inefficiency), we will present now, the positive side of this risk. Similar to commodities such as precious metals and natural gas, crypto-assets with limited supply attain high preference, being perceived as 'scare' assets. By just looking at the price and market share of bitcoin, we can easily observe that the investors' 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). From an investing position, this idea can bring important 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 cryptomarket level, we state that the likelihood is medium.

Environmental risk. Already 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 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 releasing as much carbon dioxide emission as the country of Jordan (Irfan, 2019). Another important aspect to mention is the increasing number of projects using Ethereum Blockchain (PoW) 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 [24]tokens) (CryptoSlate.com, 2020).

We believe that the technological constraints regarding the electricity consumption should receive priority consideration. For example, perhaps very soon, the success of ICO projects and the performance of businesses (using PoW Blockchain), 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; Bentov et al., 2016; Saleh, 2018; Lepore et al., 2020). The emergence of mining pool organizations, 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), and more generally the future development of environmentally friendly algorithms (e.g. PoS), represent a 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

[24] tokens from former ICOs

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 pandemic, the most performant and least risky investments were the socially responsible ones (Lins et al., 2017; Palma-Ruiz et al., 2020; Singh, 2020). Well-informed market players are preoccupied by 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 cryptomarket (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 impact the investment profitability, increasing the costs[25] for financing. As time passes, investors give more attention to the cryptomarket, therefore we consider that for the moment the likelihood is Medium. Concurrently, we believe that there are big chances so this 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.

3 MARKET ANALYSIS

In the following section, we will perform the crypto-market analysis using the Porter's five forces framework. This method is frequently used to analyze the business environment or existing competition within an industry. It is also a simple but effective tool in assessing the long-term profitability of your strategy / position within the market, taking into account various aspects (Porter, 1979).

As Porter (1979) said, while assessing the market, we should broad our view and look at the issue from a different perspective. We are planning to use the same approach, therefore the analysis will be performed at a macro level, meaning that we look at the crypto market as a whole, taking into consideration both the Blockchain technology and its applications (cryptocurrencies, tokens, smart contracts, etc.) At the same time, we take into account most of the stakeholders of this market, such as the users, developers, firms and investors and try to highlight the critical strengths and weaknesses from their perspective.

The market analysis is split according to the relevant parties concerned. Various stakeholders are named if the argument is relevant to them, while the general arguments will concern the whole market

[25] 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)

players. Every category of stakeholders considers both the existing (the ones already being part of the crypto market) and potential players (the ones considering joining).

The analysis will be performed following the below Fig. 3.

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 weaknesses (algorithmic supply limit)* *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 weaknesses (PoW)* *Reputation* *Lack of regulation*	• *Damage for the environment* • *Crypto assets trade with a risk premium relative to their environmental externalities*	*Medium*

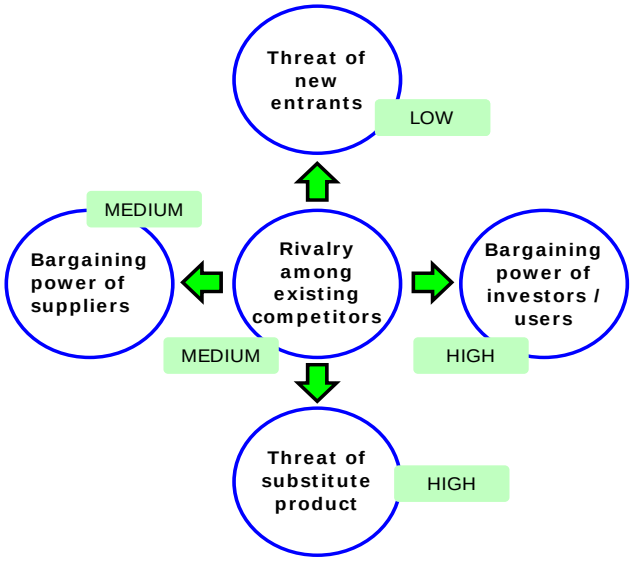

Fig. 3: Five forces framework for Blockchain adoption

Rivalry among existing competitors – Medium

Developers, users & investors: If we analyze the rivalry from this market, we can observe that the top crypto-assets are fighting to acquire more market share and notoriety, while the rest have little chances to achieve supremacy and are mainly struggling to survive in this continuously growing market. However, there are some exceptions, mainly represented by successfully forked [26]coins, which managed to gain market share and a place in the race for supremacy (e.g. Bitcoin Cash, Bitcoin SV, Litecoin, Ethereum, Zcash, Stellar, etc.). In spite of the exhaustive and still growing list of crypto-assets or the numerous frauds and attacks on the crypto market (Corbet et al., 2019), all of these are not intimidating any of the big players. Owning a big and relatively stable market share, makes them less concerned about rivalry, which leads to a deterred market competition.

General: Despite the fact that, at global level, the number of crypto-assets is now exceeding 2500, bitcoin continues to lead the market with a share usually larger than 60%, followed by Ether and Ripple (ECB crypto-assets Task Force, 2019). If we look at the market dominance, from a broader perspective, we can observe that market supremacy is achieved by the top cryptocurrencies. Just the first three currencies reach 80% dominance, then slowly increases up to 92% for the top 25 (Haig, 2019). It was proved that Bitcoin, is the one controlling the prices in the whole market (ESMA 2019), followed by Ether, which is influencing its derived [27]crypto-assets (Nadler & Guo, 2020). Out of 1600 active tokens, 1300 are derived from Ether (CryptoSlate.com, 2020), which represent almost half of the total number of crypto-assets.

In spite of the big number of assets within this market, the reason behind the relatively weak form of competition, represents the fact that investors narrow their focus on reputation and seniority. Trends and rumors influence the behavior of Blockchain's stakeholders, who can become the victims of

[26] theoretically they represent an improved version of one of the top coins

[27] Now, the existing Ether derived smart contracts (ERC-20 tokens) have reached the number of almost 250 thousand. These represent both active and non-active tokens (e.g. tokens from former ICOs).

informational risks[28]. Generally speaking, but especially in ambiguous scenarios, people feel 'safer' if they follow the social norms (Gazali et al., 2018). Social media and news attract many enthusiasts, which eventually might follow the trends blindly. Lead by a herd mentality 'if I am losing, at least I am not losing alone', they might think that a loss is easier to overcome if more people are involved. This statement proves that the crypto-market trends are very much influenced by its stakeholders' behavior (Gazali et al., 2018). The same idea is sustained by Kuo Chuen et al. (2017), who, through their study, proved that investors' sentiment represents a driving factor in creating high volatility episodes.

Threats of new entrants – Low

Developers & investors: It is very difficult to gain market share and credibility, as the industry is quasi-monopolistic/oligopolistic, shared just by some few big players (Haig, 2019). Reputation, seniority, opportunity and preeminence matter a lot in this industry, as investors seem to base their selection choices on that (Nadler & Guo, 2020). At the same time, taking into account controversies around this market, new crypto-assets might encounter difficulties in being accepted by exchanges & trading platforms, which play an essential role in the expansion of this market.

Users, investors, exchange and trading platforms & firms: A step further towards the adoption and development direction would be the acceptance of crypto-assets by retailers, exchanges and trading platforms. However, this is controversial and sometimes a challenge, even for the leaders from this market (Katz, 2017). At the same time, in the cases of non-acceptance from the exchange and trading platforms, the crypto-market might suffer from **illiquidity risk.** In an opposite scenario, platforms can be victims of **information risk** due to unexplored and mysterious new coins**,** which can lead to market manipulation and important financial losses.

General: We expect that, with the support of regulators, interested parties will have a greater chance to join the market and gain the world's trust more easily. The aim of regulation is to enhance compliancy, accountability, transparency and support a fairer competition in the crypto market (Collomb & Sok 2016, Corbet et al 2019).

Threat of substitute products – High

General: It is believed that the main market challenges and influencers represent the events related to regulatory changes and cybersecurity attacks (Corbet et al., 2019). These factors are lessening the general trust in Blockchain and slowing down the adoption of Blockchain technology and crypto-assets. At the same time, the complexity of this technology could be another reason why many people chose to remain loyal to traditional tools and national currencies (Pawczuk, Massey & Holdowsky, 2019).

As previously discussed, in the market seniority matters. Compared to the existing technologies and currencies, Blockchain and crypto-assets are new and less trusted. The control of government gives national currencies their value and legal tender status. At the same time, they are transformed in a commonly accepted mean of payment, used by everyone within their respective countries (Quest, 2018).

On the other hand, the Crypto market's value and expansion rely on its network size. In spite of its already proved big potential, Blockchain technology and crypto-assets are still fighting with their biggest enemy: public's trust. Not being backed by any government or central authority, however, still appealing thanks to their special features, crypto-assets are promising high levels of return for

[28] real information is not known and available to everyone, therefore as a consequence of the lack of knowledge, the players might not make decisions mindfully, but rather based on the current trends

investors, as no other tradable asset can offer (Corbet et al. 2019, Kuo Chuen et al., 2017). Such a benefit could serve well, especially during moments of turmoil, when countries with vulnerable economy might consider crypto-assets an interesting tool, less exposed to monetary risks (e.g. hyperinflation, an issue affecting the national currencies) (Gurguc, and Knottenbelt, 2018).
With years, technology has demonstrated its crucial role in evolution and business world, making it an indispensable tool for daily life. However, for the moment, these technological innovations are still 'threated' by their substitute products (national currencies, securities, existing technologies, etc.). I believe that it is just a matter of time, until people will learn more about these novel innovations and their special features. Once this happens, it will boost the trust in this technology and enhance the wide acceptance and development of crypto world.

Bargaining power of suppliers – Medium

General & especially developers: The main suppliers in this context are the inventors / developers who 'supply' the market with new technological innovations and the communities which maintain and prosper it. They all can have a significant control over the technology and its development. However, there are situations when developers' decision can be highly influenced or in conflict with other parties, as for instance the users. The best example of such an incident are the forks. When it is decided to make software changes, if the users cannot unanimously agree and make the necessary steps, this often leads to a split called fork. A fork means that the chain of blocks will split in two; one with a new (updated) software and the original one (using the old version of software). The new chain, creates a new technology and a new coin. This whole event has also as a consequence, the separation of the community of users. A pertinent example is the case of Ethereum and DAO attack. Following the attack, developers of Ether coin decided, that as a matter of security, the network rules and the software should be improved. This decision was not unanimously supported, leading to the creation of famous Ether fork (Massessi, 2019). Some users continued to use the old software of Ethereum Classic platform, while the adopters of the new software are using (the new) Ethereum. Because of mismatches principles between developers and part of the network, some Ether users have deserted definitively, while others followed the chain they trusted more leading to the creation of Ether (new coin) and Ether classic (original/old coin). Surprisingly, the new platform's community (Ethereum) grew more, surpassing the old one (Ethereum Classic) (Hays & Valek, 2018).
General & especially miners: Another important category of suppliers are the miners. In the case of Bitcoin technology or any other Blockchain using PoW consensus algorithm, miners play a crucial role. In other words, the Blockchain is maintained and developed with the support of the miners. Their role is to record valid transaction (if inputs are unspent) and add them in the Blockchain network through the new created blocks (Eyal & Sirer, 2018). Miners are absolutely necessary in a PoW Blockchain. The mining activity requires a considerable effort and implies significant costs[29], reason why miners prioritize transactions based on reward/compensation criteria. Miners are rewarded by the system with an amount of newly created crypto coins, just if their work was successful[30]. In addition to that, they collect also the transaction fees attached to the validated transactions. The reward offered by the system, represents a method to create new coins and at the same time, a way to increase the available supply of cryptocurrencies. This reward is distributed in a programmed, pre-established way,

[29] According to the figures from Appendix 1, we can observe that mining becomes expensive when the coin rate goes down below a certain level. Taking into account the volatility from this market, mining can easily become too pricey to go further. At the same time, miners who have invested in one type of mining device dedicated to one technology might not be willing to switch to another one (these machines are designed to work according to specific parameters adequate to the respective cryptocurrency architecture).
[30] Only the fastest miner is rewarded, while the rest, will mine on their expense.

such as the rate is slowly decreasing until the maximum supply of the respective cryptocurrency is reached (Eyal & Sirer, 2018).
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 limit. In the case where a mineable coin (e.g. Bitcoin) will reach its supply limit, the mining reward will be based only on transaction fees (Cryptoli.st, n.d.).

In order to keep the miners motivated in maintaining the Blockchain network and validate transactions, in spite of the big costs encountered, users contribute to their compensation by adding transaction fees. The higher the fee, the faster the transaction will be processed, which gives satisfaction to the user and a considerable power to the miners (Biais et al. 2019; Easley et al. 2019). However, it is important to mention that a successful coin, such as for example Bitcoin, tends to attract high transactional fees, making the coin less interesting and efficient (victim of its own success). In the end, the first goal of this technology was to replace the traditional payment tools and reduce overall costs. Therefore, increasing the transactional fees will never be a reasonable solution.

Bargaining power of investors/ users – High

General: Stories of crypto-billionaires and 'overnight gained wealth' opened the appetite of the big public and boosted the 'Bitcoin mania'. Investors interested in the Blockchain technology and crypto-assets can be large and influent. Since there exists a fairly large availability of products, coupled with low entry barriers, the user's bargaining power is high. The large variety of choices, gives the user the power to be selective and make the best choice possible (Pollock, 2018).

Investors & users: Whales[31] are frequently the actors who control the market and the crypto-assets' prices (Bloomberg.com, 2018; CoinDesk, 2020). It was proved that cryptocurrencies are correlated to each other, showing signs of contagion effect (Alfieri 2020; Kumar & Anandarao 2019). As a consequence, Bitcoin has the power to influence the whole crypto market, driving the prices up or down (ESMA, 2019). In other words, it is enough to manipulate the top coin, as for example through whales, such as if they decide to sell the whole market be affected and will react.

Miners (also users) can have a big influence on the crypto market. As depicted in the Appendix 2, mining can easily become a centralized activity, if we take into consideration the geographical localization of these mining farms and the hash rate distribution owned by the top ones. If any of these powerful companies decide to conspire, they can easily take over the control of the whole network. For example, in the case of bitcoin and Litecoin, a majority attack could be possible, if just the first 3 miners collude (owning together over 50% power). In the case of Ethereum, just the first two mining pools own more than 50% of the network power.
Developers: Software updates and any necessary technological changes for security and efficiency purposes, have to be accepted by users, prior to implementation. If this is not happening, as previously discussed, the community might split (the case of forks) (Massessi, 2019).
Investing firms & users: Poor regulation is a story with two faces, as in the case of ICOs for example. Firms might take advantage of gaps in current regulation and escape taxation or issue low quality / unlawful projects on the expense of investors (Momtaz, 2019). In this scenario, investors are the users,

[31] Owners (investors) of big amounts of crypto-assets

and are the ones affected. The latest initiatives regarding a new legislation and a better surveillance over this market, promise that the future will leverage even more power on the users' side, making it safer to invest in this market and increase the overall quality of these innovations.

4 CONCLUSIONS

The cryptomarket 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 cryptomarket has to overcome its many challenges. We believe that understanding and analyzing the cryptomarket vulnerabilities, represents the first step in overcoming its challenges.

Conceived as a two-level analysis, we started this research with a risk assessment, where we focus on the technological and financial risks of cryptomarket and Blockchain technology. We show that these risks are correlated 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 technical vulnerabilities of Blockchain. To perfect this assessment, we propose a way to determine the likelihood of triggering financial risks through technical vulnerabilities. Here, we also emphasize the role played by financial behavior, social responsibility and Blockchain literacy in the stability of cryptomarket. Furthermore, we complete this paper with a cryptomarket appraisal, performed with respect to its stakeholders, such as the business process managers, investors, regulators, firms, developers, exchange and trading platforms, etc. Here, we highlighted some of the challenges faced by different players and show the profitability of the stakeholders' strategy/position towards Blockchain adoption.

Limitations and future pathways for research:

Information related to cryptomarket 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 not centralized database about the attacks performed on the cryptomarket, but rather a collection of unrelated mini statistics. This represents one of the limitations of our study, reducing the possibility to perform empirical studies and accurately assess certain risks.

Another limitation represents the lack of data regarding Blockchain literacy and financial behavior within the cryptomarket. This could be also an interesting path for further research.

As a decentralized system by design, blockchain technology is not managed by any central authority but by its own algorithm (Hays & Valek, 2018). This leaves the duty of legal and regulatory supervision in the hands of the specialists from governments and industries (Xie et al., 2019). The only real progress in this direction started just in the beginning of 2017 (Botos, 2017). Therefore, 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 academics or practitioners. Indeed, an assessment of the risks and vulnerabilities of this market, could prevent investors from unnecessary loses, diminish the number of low-quality products and increase performance and efficiency overall.

REFERENCES

1. Abhishta, A., Joosten, R., Dragomiretskiy, S. & Nieuwenhuis, L. (2019) Impact of Successful DDoS Attacks on a Major Crypto-Currency Exchange. 2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP). [Online]. DOI: 10.1109/empdp.2019.8671642 [Accessed: 24 April 2020].
2. Alfieri, E., 2020. Cryptocurrencies and Market Efficiency. Ph.D. Thesis. UNIVERSITÉ GRENOBLE ALPES.
3. Americn Crypto Association (2020) Could Quantum Computing Be Used to Crack Cryptocurrency? - American Crypto Association [Online]. Available from https://www.americancryptoassociation.com/2020/04/04/quantum-computing-crack-crypto/ [Accessed: 22 May 2020]
4. Antonakakis, N., Chatziantoniou, I. & Gabauer, D. (2019) Cryptocurrency market contagion: Market uncertainty, market complexity, and dynamic portfolios. Journal of International Financial Markets, Institutions and Money. 61. pp. 37-51. [Online]. DOI: 10.1016/j.intfin.2019.02.003 [Accessed: 1 June 2020].
5. Atzei, N., Bartoletti, M. and Cimoli, T., 2017. A Survey of Attacks on Ethereum Smart Contracts (SoK). Lecture Notes in Computer Science, pp.164-186.
6. Ballou, B., Heitger, D. and Landes, C., (2006) The rise of corporate sustainability reporting: A rapidly growing assurance opportunity. Journal of Accountancy, 202(6), pp.65-74.
7. Beigel, O. (2019) 51% Attack Explained Simply + Real Life Example (2020 Updated) [Online]. Available from https://99bitcoins.com/51-percent-attack/ [Accessed: 20 April 2020].
8. Bentov, I., Gabizon, A. & Mizrahi, A. (2016) Cryptocurrencies Without Proof of Work. Financial Cryptography and Data Security. pp. 142-157. [Online]. DOI: 10.1007/978-3-662-53357-4_10 [Accessed: 24 October 2020].
9. Biais, B., Bisière, C., Bouvard, M. & Casamatta, C. (2019) The Blockchain Folk Theorem. The Review of Financial Studies. 32 (5). pp. 1662-1715. [Online]. DOI: 10.1093/rfs/hhy095.
10. Bitcoin.com (2020) Onchain Data Shows Rising Bitcoin Whale Index Surpassing 4-Year High | Bitcoin News [Online]. Available from https://news.bitcoin.com/onchain-data-shows-rising-bitcoin-whale-index-surpassing-4-year-high/ [Accessed: 27 October 2020]
11. Bitcointalk.org (2014) GHASH.IO IS NEARING 51% - LEAVE THE POOL [Online]. Available from https://bitcointalk.org/index.php?topic=406534.0 [Accessed: 20 April 2020]
12. Blockchain.com (2020) Bitcoin Hashrate distribution among mining farms [Online]. Available from https://www.blockchain.com/charts/pools [Accessed: 20 April 2020]
13. Bloomberg.com (2018) Bitcoin's Tokyo Whale Sold $400 Million and He's Not Done Yet [Online]. Available from https://www.bloomberg.com/news/articles/2018-03-07/bitcoin-s-tokyo-whale-sold-400-million-and-he-s-not-done-yet [Accessed: 21 March 2020]
14. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. & Felten, E. (2015) SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. IEEE Symposium on Security and Privacy. [Online]. DOI: 10.1109/SP.2015.14 [Accessed: 16 April 2020].
15. Botos, M. H. (2017) Bitcoin Intelligence – Business Intelligence meets Crypto Currency, CES Working Papers – Vol. IX, Issue 3, 488-501.
16. Brown-Liburd, H. & Zamora, V. (2015) The Role of Corporate Social Responsibility (CSR) Assurance in Investors' Judgments When Managerial Pay is Explicitly Tied to CSR Performance. AUDITING: A Journal of Practice & Theory. 34 (1). pp. 75-96. [Online]. DOI: 10.2308/ajpt-50813 [Accessed: 24 October 2020].

17. Buybitcoinworldwide.com (2020) 10 Best and Biggest Bitcoin Mining Pools 2020 (Comparison) [Online]. Available from https://www.buybitcoinworldwide.com/mining/pools/ [Accessed: 28 April 2020]
18. Canh, N., Wongchoti, U., Thanh, S. & Thong, N. (2019) Systematic risk in cryptocurrency market: Evidence from DCC-MGARCH model. Finance Research Letters. 29. pp. 90-100. [Online]. DOI: 10.1016/j.frl.2019.03.011.
19. Charles, M. (2019) Prometteuse, la blockchain est encore loin de tenir toutes ses promesses [Online]. Available from https://www.20minutes.fr/magazine/transition-energetique-mag/2582587-20190813-technologie-prometteuse-blockchain-encore-loin-tenir-toutes-promesses [Accessed: 12 April 2020].
20. Chen, Y. (2019) Decentralized Finance: Blockchain Technology and the Quest for an Open Financial System. SSRN Electronic Journal. [Online]. DOI: 10.2139/ssrn.3418557.
21. Ciaian, P., Rajcaniova, M. & Kancs, d. (2015) The economics of BitCoin price formation. Applied Economics. 48 (19). pp. 1799-1815. [Online]. DOI: 10.1080/00036846.2015.1109038 [Accessed: 27 October 2020].
22. CoinCentral (2020) The 3 Best Ethereum Mining Pool Options [Online]. Available from https://coincentral.com/best-ethereum-mining-pool/ [Accessed: 29 April 2020]
23. CoinDesk (2014) Ghash.io: We Will Never Launch a 51% Attack Against Bitcoin [Online]. Available from https://www.coindesk.com/ghash-io-never-launch-51-attack [Accessed: 20 April 2020].
24. CoinDesk (2020) Whale Watching: Exchange Data Contained Early Warning of Thursday's Bitcoin Dump - CoinDesk [Online]. Available from https://www.coindesk.com/whale-watching-exchange-data-contained-early-warning-of-thursdays-bitcoin-dump [Accessed: 21 March 2020]
25. CoinGuides.org (2020) HashPower Calculator - Convert Hash to kH/s to MH/s to GH/s to TH/s to PH/s [Online]. Available from https://coinguides.org/hashpower-converter-calculator/ [Accessed: 29 April 2020]
26. Coinmetrics.com (2019) Coin Metrics' State of the Network: Issue 26 [Online]. Available from https://coinmetrics.substack.com/p/coin-metrics-state-of-the-network-d2e [Accessed: 24 October 2020]
27. Cointelegraph (2019) 'Blockchain Bandit' Has Stolen 45
28. Collomb, A. & Sok, K. (2016) Blockchain and distributed ledger technologies (DLT): what impact on financial markets ?. AMF. Options & debates No.15 Paris: Institut Louis Bachelier.
29. Corbet, S., Lucey, B., Urquhart, A. and Yarovaya, L. (2019). Cryptocurrencies as a financial asset: A systematic analysis. International Review of Financial Analysis, 62, pp.182-199
30. Crowell, B. (2020) Crypto Exchange Liquidity, Explained [Online]. Available from https://cointelegraph.com/explained/crypto-exchange-liquidity-and-why-it-matters-explained [Accessed: 2 June 2020].
31. Crypto51.app (2020) Cost of a 51% Attack for Different Cryptocurrencies | Crypto51 [Online]. Available from https://www.crypto51.app/ [Accessed: 20 April 2020].
32. CryptoCompare (2020) Mining Calculator Bitcoin
33. CryptoSlate.com (2020) Token Cryptocurrencies [Online]. Available from https://cryptoslate.com/cryptos/tokens/page/17/ [Accessed: 1 April 2020]
34. Cryptoli.st (n.d.) Mineable Cryptocurrencies | CryptoList [Online]. Available from https://cryptoli.st/lists/mineable [Accessed: 19 April 2020]
35. De Bondt, W.F., Muradoglu, Y.G., Shefrin, H. and Staikouras, S.K. (2008), Behavioral finance: Quo vadis?. Journal of Applied Finance (Formerly Financial Practice and Education), 18(2).
36. Deribit Insights (2020) Exchange vs Over-the-Counter (OTC) Bitcoin Trading - Deribit Insights [Online]. Available from https://insights.deribit.com/market-research/exchange-vs-over-the-counter-otc-bitcoin-trading/ [Accessed: 26 October 2020]

37. Drljevic, N., Aranda, D. and Stantchev, V., 2019. Perspectives on risks and standards that affect the requirements engineering of blockchain technology. Computer Standards & Interfaces, 69, p.103409.
38. ECB Crypto-Assets Task Force (2019). Crypto-Assets: Implications for financial stability
39. ESMA (2019). Report on Trends
40. Easley, D., Hvidkjaer, S. & O'Hara, M. (2002) Is Information Risk a Determinant of Asset Returns? The Journal of Finance. 57 (5). pp. 2185-2221. [Online]. DOI: 10.1111/1540-6261.00493.
41. Easley, D., O'Hara, M. & Basu, S. (2019) From mining to markets: The evolution of bitcoin transaction fees. Journal of Financial Economics. 134 (1). pp. 91-109. [Online]. DOI: 10.1016/j.jfineco.2019.03.004 [Accessed: 23 March 2020].
42. En.wikipedia.org (2020) Bitfinex [Online]. Available from https://en.wikipedia.org/wiki/Bitfinex [Accessed: 24 April 2020]
43. Etherchain.org (2020) Top Miners over the last 24h - etherchain.org [Online]. Available from https://www.etherchain.org/charts/topMiners [Accessed: 28 April 2020]
44. Ethereum Community Forum (2016) Dwarfpool is now 50.5% [Online]. Available from https://forum.ethereum.org/discussion/5244/dwarfpool-is-now-50-5 [Accessed: 20 April 2020]
45. Exterkate & Wagenaar (2018) Blockchain Decision Tree — Steemit [Online]. Available from https://steemit.com/blockchain/@wagenaarm/blockchain-decision-tree [Accessed: 1 April 2020]
46. Eyal, I. & Sirer, E. (2018) Majority is not enough. Communications of the ACM. 61 (7). pp. 95-102. [Online]. DOI: 10.1145/3212998.
47. Ferreira, P. & Pereira, É. (2019) Contagion Effect in Cryptocurrency Market. Journal of Risk and Financial Management. 12 (3). p. 115. [Online]. DOI: 10.3390/jrfm12030115 [Accessed: 1 June 2020].
48. Gazali, H., Ismail, C. & Amboala, T. (2018) Exploring the Intention to Invest in Cryptocurrency: The Case of Bitcoin. International Conference on Information and Communication Technology for the Muslim World. [Online]. DOI: 10.1109/ICT4M.2018.00021 [Accessed: 16 April 2020].
49. GlobalPetrpPrices.com (2020) France electricity prices [Online]. Available from https://www.globalpetrolprices.com/France/electricity_prices/ [Accessed: 29 April 2020]
50. Goffard, P. (2019) Fraud risk assessment within blockchain transactions. Advances in Applied Probability. 51 (2). pp. 443-467. [Online]. DOI: 10.1017/apr.2019.18 [Accessed: 16 April 2020].
51. Goodkind, A., Jones, B. & Berrens, R. (2020) Cryptodamages: Monetary value estimates of the air pollution and human health impacts of cryptocurrency mining. Energy Research & Social Science. 59. p. 101281. [Online]. DOI: 10.1016/j.erss.2019.101281 [Accessed: 2 June 2020].
52. Greene, R. and McDowall, B., (2018). Liquidity or Leakage: Plumbing Problems with Cryptocurrencies. Plumbing Problems With Cryptocurrencies-Long Finance.
53. Gurguc, Z. and Knottenbelt, W. (2018). Cryptocurrencies: overcoming barriers to trust and adoption. eToro.
54. Haase, M. & Zimmermann, H. (2013) Scarcity, Risk Premiums, and the Pricingof Commodity Futures: The Case of Crude Oil Contracts. The Journal of Alternative Investments. 16 (1). pp. 43-71. [Online]. DOI: 10.3905/jai.2013.16.1.043 [Accessed: 27 October 2020].
55. Haig, S., (2019). A Different Look At Crypto Market And Top Assets, How Dominated Is It?. [online] Cointelegraph. Available at: <https://cointelegraph.com/news/a-different-look-at-crypto-market-and-top-assets-how-dominated-is-it>
56. Hasanova, H., Baek, U., Shin, M., Cho, K. & Kim, M. (2019) A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. International Journal of Network Management. 29 (2). p. e2060. [Online]. DOI: 10.1002/nem.2060.
57. Hays, D. & Valek, M. (2018) Smart Contracts. Liechtenstein's Blockchain Strategy. The "Network Effect" as Valuation Methodology. CryptoResearch.report Incrementum AG [Online]. Available from

https://cryptoresearch.report/wp-content/uploads/2018/10/Crypto-Research-Report-October_2018_EN.pdf [Accessed: 21 March 2020].
58. Heilman, E., Kendler, A., Zohar, A. & Goldberg, S. (2015) Eclipse Attacks on Bitcoin's Peer-to-Peer Network. 24th USENIX Security Symposium. [Accessed: 20 April 2020].
59. Holochain (2020) Holochain [Online]. Available from https://holochain.org/ [Accessed: 2 April 2020]
60. Indepedent Security Evaluators (2019) The Blockchain Bandit - Ethercombing: Finding Secrets in Popular Places [Online]. Available from https://www.ise.io/casestudies/ethercombing/ [Accessed: 2 May 2020]
61. Independent Security Evaluators (2019) The Blockchain Bandit - Ethercombing: Finding Secrets in Popular Places [Online]. Available from https://www.ise.io/casestudies/ethercombing/ [Accessed: 22 May 2020]
62. Irfan, U. (2019) Bitcoin is an energy hog. Where is all that electricity coming from? [Online]. Available from https://www.vox.com/2019/6/18/18642645/bitcoin-energy-price-renewable-china [Accessed: 2 June 2020].
63. Jain, A. & Jain, C. (2019) Blockchain hysteria: Adding "blockchain" to company's name. Economics Letters. 181. pp. 178-181. [Online]. DOI: 10.1016/j.econlet.2019.05.011 [Accessed: 1 June 2020].
64. Jain, M. & Singla, R. (2020) LIQUIDITY AND ITS MEASURES. International Journal of Research and Analytical Reviews. 5 (2). [Accessed: 27 October 2020].
65. Katz, L. (2017) Bitcoin Acceptance Among Retailers Is Low and Getting Lower [Online]. Available from https://www.bloomberg.com/news/articles/2017-07-12/bitcoin-acceptance-among-retailers-is-low-and-getting-lower [Accessed: 23 March 2020].
66. Koutmos, D. (2018) Liquidity uncertainty and Bitcoin's market microstructure. Economics Letters. 172. pp. 97-101. [Online]. DOI: 10.1016/j.econlet.2018.08.041 [Accessed: 2 June 2020].
67. Kumar, A. & Anandarao, S. (2019) Volatility spillover in crypto-currency markets: Some evidences from GARCH and wavelet analysis. Physica A: Statistical Mechanics and its Applications. 524. pp. 448-458. [Online]. DOI: 10.1016/j.physa.2019.04.154 [Accessed: 21 March 2020].
68. Lakhani, M. & Iansiti, K. (2017) The Truth About Blockchain. Harvard Business Review. (January-February). [Online]. Available from https://hbr.org/2017/01/the-truth-about-blockchain
69. Lasla, N., Alsahan, L., Abdallah, M., & Younis, M. (2020). Green-PoW: An Energy-Efficient Blockchain Proof-of-Work Consensus Algorithm. ArXiv, abs/2007.04086.
70. Lee, J. (2019) Systematic Approach to Analyzing Security and Vulnerabilities of Blockchain Systems. Working Paper CISL# 2019-05. Massachusetts Institute of Technology.
71. Lemieux, V. (2016) Trusting records: is Blockchain technology the answer?. Records Management Journal. 26 (2). pp. 110-139. [Online]. DOI: 10.1108/rmj-12-2015-0042.
72. Lepore, C., Ceria, M., Visconti, A., Rao, U., Shah, K. & Zanolini, L. (2020) A Survey on Blockchain Consensus with a Performance Comparison of PoW, PoS and Pure PoS. Mathematics. 8 (10). p. 1782. [Online]. DOI: 10.3390/math8101782 [Accessed: 24 October 2020].
73. Liebau, D. and Schueffel, P. (2019), Crypto-Currencies and ICOs: Are They Scams? An Empirical Study. An Empirical Study (January 23, 2019).
74. Lins, K., Servaes, H. & Tamayo, A. (2017) Social Capital, Trust, and Firm Performance: The Value of Corporate Social Responsibility during the Financial Crisis. The Journal of Finance. 72 (4). pp. 1785-1824. [Online]. DOI: 10.1111/jofi.12505 [Accessed: 26 October 2020].
75. Litecoinpool.org (2020) Hash Rate Distribution | litecoinpool.org [Online]. Available from https://www.litecoinpool.org/pools [Accessed: 28 April 2020]
76. Lu, Y., 2019. The blockchain: State-of-the-art and research challenges. Journal of Industrial Information Integration, 15, pp.80-90.

77. Ma, S., Wang, H., Dai, H., Cheng, S., Yi, R. & Wang, T. (2018) A Blockchain-based Risk and Information System Control Framework. IEEE 16th Int. Conf. on Dependable, Autonomic & Secure Comp., 16th Int. Conf. on Pervasive Intelligence & Comp., 4th Int. Conf. on Big Data Intelligence & Comp., and 3rd Cyber Sci. & Tech. Cong. [Online]. DOI: 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00031 [Accessed: 16 April 2020].
78. Magoo.gthub.io (2020) Blockchain Graveyard [Online]. Available from https://magoo.github.io/Blockchain-Graveyard/ [Accessed: 2 May 2020]
79. Manahov, V. (2020) Cryptocurrency liquidity during extreme price movements: is there a problem with virtual money?. Quantitative Finance. pp. 1-20. [Online]. DOI: 10.1080/14697688.2020.1788718 [Accessed: 27 October 2020].
80. Marcus, Y., Heilman, E. & Goldberg, S. (2018) Low-Resource Eclipse Attacks on Ethereum's Peer-to-Peer Network. IACR Cryptology ePrint Archive. [Accessed: 20 April 2020].
81. Massessi, D. (2019) Blockchain Governance In A Nutshell [Online]. Available from https://medium.com/coinmonks/blockchain-governance-in-a-nutshell-67903c0d2ea8 [Accessed: 24 March 2020].
82. Matkovskyy, R. & Jalan, A. (2019) From financial markets to Bitcoin markets: A fresh look at the contagion effect. Finance Research Letters. 31. pp. 93-97. [Online]. DOI: 10.1016/j.frl.2019.04.007 [Accessed: 26 October 2020].
83. Mecca, B. (2019) How can we reduce Bitcoin pollution? [Online]. Available from https://environment-review.yale.edu/how-can-we-reduce-bitcoin-pollution-0?fbclid=IwAR2c8Hm1lyh6PvSfQ_G8OBLMGVLS8xDykqyISe8l3amw4Xsx4wSFefsa9rQ [Accessed: 2 June 2020].
84. Momtaz, P. (2019) Token Sales and Initial Coin Offerings: Introduction. The Journal of Alternative Investments. 21 (4). pp. 7-12. [Online]. DOI: 10.3905/jai.2019.21.4.007.
85. Monet.network (2020) MONET: infrastructure for distributed mobile peer-to-peer applications [Online]. Available from https://monet.network/about.html [Accessed: 2 April 2020]
86. Morganti,, G., Schiavone, E. & Bondavalli, A. (2018) Risk Assessment of Blockchain Technology. IEEE Xplore. [Online]. DOI: 10.1109/LADC.2018.00019 [Accessed: 3 April 2020].
87. Nadler, P. & Guo, Y. (2020) The fair value of a token: How do markets price cryptocurrencies? Research in International Business and Finance. 52. p. 101108. [Online]. DOI: 10.1016/j.ribaf.2019.101108.
88. PWC (2019) Quantum computing. A technology of the future already present. The 5th revolution [Online]. Available from https://www.pwc.fr/fr/assets/files/pdf/2019/11/en-france-pwc-point-of-view-quantum-computing-2019.pdf [Accessed: 19 May 2020]
89. Packt Hub (2019) What Blockchain developers learn from Eclipse Attacks in bitcoin network [Online]. Available from https://hub.packtpub.com/what-can-blockchain-developers-learn-from-eclipse-attacks-in-a-bitcoin-network-koshik-raj/ [Accessed: 20 April 2020]
90. Palma-Ruiz, J., Castillo-Apraiz, J. & Gómez-Martínez, R. (2020) Socially Responsible Investing as a Competitive Strategy for Trading Companies in Times of Upheaval Amid COVID-19: Evidence from Spain. International Journal of Financial Studies. 8 (3). p. 41. [Online]. DOI: 10.3390/ijfs8030041 [Accessed: 26 October 2020].
91. Patel, D., 2020. Blockchain Technology towards the Mitigation of Distributed Denial of Service Attacks. International Journal of Recent Technology and Engineering, 8(6), pp.961-965.
92. Pawczuk, L., Massey, R. & Holdowsky, J. (2019) Deloitte's 2019 Global Blockchain Survey [Online]. Available from https://www2.deloitte.com/us/en/insights/topics/understanding-blockchain-potential/global-blockchain-survey.html [Accessed: 16 April 2020].

93. Pollock, D., (2018). Volatility: The Necessary Evil Of Cryptocurrency And How To Handle It. [online] Cointelegraph. Available at: <https://cointelegraph.com/news/volatility-the-necessary-evil-of-cryptocurrency-and-how-to-handle-it>
94. Porter, M. (1979) How Competitive Forces Shape Strategy. Harvard Business Review. 57 (2). pp. 137–145. [Accessed: 1 April 2020].
95. Quest, M. (2018). Cryptocurrency Master Bundle: Everything You Need to Know about Cryptocurrency and Bitcoin Trading, Mining, Investing, Ethereum, ICOs, and the Blockchain. CreateSpace Independent Publishing Platform.
96. Rizzi, J. V. (2008).Behavioral Biases of the Financial Crisis, Journal of Applied Finance,Vol.18, No. 2, pp. 84-96.
97. Rui Chen, R. & Chen, K. (2020) A 2020 perspective on "Information asymmetry in initial coin offerings (ICOs): Investigating the effects of multiple channel signals". Electronic Commerce Research and Applications. 40. p. 100936. [Online]. DOI: 10.1016/j.elerap.2020.100936 [Accessed: 2 June 2020].
98. Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D. & Mohaisen, D. (2020) Exploring the Attack Surface of Blockchain: A Comprehensive Survey. IEEE Communications Surveys & Tutorials. pp. 1-1. [Online]. DOI: 10.1109/comst.2020.2975999.
99. Saleh, F. (2018) Blockchain without Waste: Proof-of-Stake. The Review of Financial Studies. [Online]. DOI: 10.1093/rfs/hhaa075.
100. Stewart, I., Ilie, D., Zamyatin, A., Werner, S., Torshizi, M. & Knottenbelt, W. (2018) Committing to quantum resistance: a slow defence for Bitcoin against a fast quantum computing attack. Royal Society Open Science. 5 (6). p. 180410. [Online]. DOI: 10.1098/rsos.180410.
101. Tapscott, D. & Tapscott, A. (2016) The Impact of the Blockchain Goes Beyond Financial Services. Harvard Business Review. (May). [Online]. Available from https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services
102. Team L. (2018) How public and private keys work? What is a seed phrase? [Online]. Available from https://www.lykke.com/city/blog/2018-12-how-public-and-private-keys-work [Accessed: 2 May 2020]
103. Tuwiner, J. (2020) 5 Best Ethereum Mining Pools to Join 2020 (Comparison) [Online]. Available from https://www.buybitcoinworldwide.com/ethereum/mining-pools/ [Accessed: 20 April 2020].
104. Tuwiner, J. (2020) 9 Best Bitcoin & Cryptocurrency Exchange Reviews (2020) [Online]. Available from https://www.buybitcoinworldwide.com/exchanges/ [Accessed: 24 April 2020].
105. Underscore VC (2018) Future of Blockchain Survey & Results | Underscore VC [Online]. Available from https://underscore.vc/blog/future-of-blockchain-survey-results/ [Accessed: 16 April 2020]
106. Van Rooij, M., Lusardi, A. & Alessie, R. (2011) Financial literacy and stock market participation. Journal of Financial Economics. 101 (2). pp. 449-472. [Online]. DOI: 10.1016/j.jfineco.2011.03.006 [Accessed: 26 October 2020].
107. Verhallen, T. (1982) Scarcity and consumer choice behavior. Journal of Economic Psychology. 2 (4). pp. 299-322. [Online]. DOI: 10.1016/0167-4870(82)90034-4 [Accessed: 27 October 2020].
108. Wheretomine.io (2020) Ethereum Mining Pools (ETH) Ethash | WhereToMine [Online]. Available from https://wheretomine.io/coins/ethereum/ [Accessed: 29 April 2020]
109. Williams, O., 2017. Cyber Attacks On Bitcoin Exchanges Are Surging As The Cryptocurrency Soars In Value. [online] NS Tech. Available at: <https://tech.newstatesman.com/news/ddos-attacks-bitcoin-exchanges> [Accessed 20 April 2020].

110. Wüst, K. & Gervais, A. (2016) Ethereum Eclipse Attacks. ETH Zurich Research Collection. [Online]. DOI: doi.org/10.3929/ethz-a-010724205 [Accessed: 20 April 2020].
111. Wüst, K. & Gervais, A. (2018) Do you Need a Blockchain?. 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). [Online]. DOI: 10.1109/CVCBT.2018.00011 [Accessed: 18 April 2020].
112. Xie, J., Tang, H., Huang, T., Yu, F., Xie, R., Liu, J. & Liu, Y. (2019) A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. IEEE Communications Surveys & Tutorials. 21 (3). pp. 2794-2830. [Online]. DOI: 10.1109/comst.2019.2899617.
113. Zhang, R., Xue, R. & Liu, L. (2019) Security and Privacy on Blockchain. ACM Computing Surveys. 52 (3), 1-34. Available from: doi:10.1145/3316481
114. Zhang, S. & Lee, J. (2019) Eclipse-based Stake-Bleeding Attacks in PoS Blockchain Systems. Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure - BSCI '19. [Online]. DOI: 10.1145/3327960.3332391 [Accessed: 20 April 2020].
115. btc.com (2020) Pool Distribution [Online]. Available from https://btc.com/stats/pool [Accessed: 28 April 2020]
116. etherscan.io (2020) Token Tracker ERC-20 [Online]. Available from https://etherscan.io/tokens?p=20 [Accessed: 1 April 2020]

Appendixes

Appendix 1

Below table offers an overview of what costs and profits does the mining process imply. The final values are very much dependent on the cryptocurrency rate. That's happening because for every successful operation, the afferent miner is rewarded with a fixed amount of the mined cryptocurrencies (main reward) and some complementary benefits depending on the coin (e.g. transaction fees, gas & uncles rewards). The average price of electricity in the world, for the last quarter of 2019, was estimated to be 0.12 U.S. Dollar per kWh for businesses (GlobalPetrpPrices.com, 2020) and it was considered as a standard electricity price in performing these estimations. The Hashing power is expressed in different units: TH = TeraHash; MH = MegaHash; KH = KiloHash; GH = GigaHash (CoinGuides.org, 2020). Every coin requires different hash rates in conformity with the hashing algorithm used, while the difficulty of the mining process within a network is continuously adjusting according to the miners' performance. The estimated power cost is computed based on the Hashing power, the consumption and the costs per KWh. The estimated profit/loss per year is computed taking into account all the variables, including the coins' price (just fixed rewards are considered, without complementary ones).

Cryptocurrency	Price	Hashing power	Estimated Power consumption (w)	Estimated Cost / KWh ($)	Estimated Power cost / year	Estimated Profit / year
Bitcoin	*$ 8,340.08*	*40 TH/s*	*1500*	*0.12*	*$ 1,576.80*	*$ 322.61*
Ether	*$ 209.72*	*200 MH/s*	*140*	*0.12*	*$ 147.17*	*$ 880.28*
Ether Classic	*$ 6.599*	*500 MH/s*	*1000*	*0.12*	*$ 1,051.20*	*$ 1,715.15*
Monero	*$ 65.10*	*100 KH/s*	*1200*	*0.12*	*$ 1,261.44*	*$ 1,239.46*
Zcash	*$ 45.91*	*100 KH/s*	*1000*	*0.12*	*$ 1,051.20*	*$ 615.02*
Dash	*$ 84.34*	*200 GH/s*	*1110*	*0.12*	*$ 1,166.83*	*$ -137.02*
Litecoin	*$ 47.32*	*5 GH/s*	*1000*	*0.12*	*$ 1,051.20*	*$ 3,252.61*

Title: Crypto mining calculator. Values computed as per 29th April 2020 rates

Source: data extracted from (CryptoCompare, 2020)

Appendix 2

The below table shows the main mining pools. The '*country*' parameter refers to the main servers' location, as most of these mining pool have extended globally, having servers all over the world. Global refers to mining pools which don't have a mainland location, but rather many servers throughout the globe. Ethermine and ethpool (not in this top) operate from different websites but share in fact the same pool (CoinCentral, 2020). In this kind of situation, network supremacy could be acquired without even noticing.

	Bitcoin		**Ethereum**		**Litecoin**	
Rank	*Country*	*Pool*	*Country*	*Pool*	*Country*	*Pool*
1.	China	Poolin (18%)	China	Sparkpool (29%)	China	Poolin (23%)
2.	China	F2Pool (17%)	Global	Ethermine (22%)	China	F2Pool (14%)
3.	China	AntPool (16%)	China	F2Pool (8%)	UK	Litecoinpool (14%)
4.	China	BTC.com (11%)	Global	Nanopool (6%)	China	BTC.com (10%)
5.	China	ViaBTC (7%)	China	Zhizhu (5%)	China	ViaBTC (10%)

Title: Main mining pools by location, hash rate distribution (HRD %) and cryptocurrency. HRD as per 28th April 2020 values

Source: data extracted from (Litecoinpool.org 2020, Etherchain.org 2020, btc.com 2020, Buybitcoinworldwide.com 2020, wheretomine.io 2020)