UGA
Université
Grenoble Alpes

# THÈSE

Pour obtenir le grade de

## DOCTEUR DE L'UNIVERSITÉ GRENOBLE ALPES

Spécialité : Sciences de Gestion

Arrêté ministériel : 25 mai 2016

Présentée par


## Elise ALFIERI

Thèse dirigée par **Radu BURLACU**, Communauté Université Grenoble Alpes
et codirigée par **Geoffroy ENJOLRAS**, Communauté Université Grenoble Alpes

préparée au sein du **Laboratoire Centre d'Etudes et de Recherches appliquées à la gestion**
dans **l'École Doctorale Sciences de gestion**


# Cryptomonnaies et efficience des marchés

# Cryptocurrencies and market efficiency

Thèse soutenue publiquement le **22 novembre 2019**,
devant le jury composé de :

**Monsieur Radu BURLACU**
PROFESSEUR, UNIVERNIVERSITE GRENOBLE ALPES, Directeur de thèse
**Monsieur William KNOTTENBELT**
PROFESSEUR, IMPERIAL COLLEGE LONDON, Rapporteur
**Monsieur Jean-Francois GAJEWSKI**
PROFESSEUR, UNIVERSITE DE LYON , Rapporteur
**Madame Sonia JIMENEZ-GARCES**
PROFESSEUR, UNIVERSITE GRENOBLE ALPES, Président
**Monsieur Patrice FONTAINE**
DIRECTEUR DE RECHERCHE, CNRS, Examinateur
**Monsieur Geoffroy ENJOLRAS**
PROFESSEUR, UNIVERSITE GRENOBLE ALPES, Co-directeur de thèse

## ACKNOWLEDGEMENT

Loin de n'être qu'un parcours solitaire, la thèse est surtout un moment que l'on partage avec un grand nombre de personnes qui nous apportent leur soutien d'une façon ou d'une autre.

En premier lieu, je tiens à remercier vivement mes directeurs de thèses, Monsieur le Professeur Radu Burlacu et Monsieur le Professeur Geoffroy Enjolras. Je suis très reconnaissante de cet encadrement partagé, de leur implication dans mes recherches, dans mon travail de thèse et dans mes choix professionnels.

Je remercie Monsieur le Professeur Radu Burlacu de m'avoir initiée au monde académique depuis le master Finance, de l'autonomie et de la confiance qu'il m'a accordées dans mes différents projets et surtout dans le choix de cette thèse. J'ai un profond respect pour son expertise, sa rigueur et sa volonté. Je le remercie pour toute son implication dans mes années de thèse, sa grande disponibilité à mon égard, ses conseils et commentaires précieux et son soutien, parfois même dans des délais serrés, qui m'ont permis de mener à bien mon travail de thèse en trois années.

Je remercie Monsieur le Professeur Geoffroy Enjolras pour avoir accepté de faire partie de l'aventure de cette thèse autour de la thématique des cryptomonnaies. Un grand merci pour son dynamisme, son expertise, sa réactivité et son implication constante dans mes recherches. Ses conseils et remarques judicieuses, ainsi que le temps qu'il m'a accordé pour travailler ensemble sur ces thématiques de recherche, ont permis l'aboutissement de cette thèse.

J'adresse aussi mes remerciements aux professeurs qui ont accepté d'être présents à mon jury de thèse :

My sincere thanks to Professor William Knottenbelt for being « rapporteur » of my thesis. Thank you for your kind welcome and hospitality at the Center for Cryptocurrency Research and Engineering - Imperial College London during my visiting, for integrating me into your team and sharing projects together. Your expertise on my research topic has been and still is of great help to me.

Je tiens également à remercier Monsieur le Professeur Jean-François Gajewski pour son accueil au sein de l'Université Savoie-Mont Blanc en tant que tuteur pour mon service d'enseignement durant mes trois années de doctorat et pour avoir accepté d'évaluer mon travail de thèse en tant que rapporteur.

Je souhaiterais exprimer ma gratitude à Madame le Professeur Sonia Jimenez-Garcès pour avoir contribué à me donner envie de rejoindre le monde de la recherche et de l'enseignement. Je la remercie pour nos nombreuses discussions et ses encouragements depuis le tout début de ma thèse. C'est un honneur pour moi aujourd'hui de la compter dans mon jury.

Enfin, je remercie également Monsieur le Professeur Patrice Fontaine pour sa participation à mon jury. Je le remercie de m'avoir accueillie durant mon stage de fin de master au sein d'Eurofidai, de m'avoir permis de découvrir et de m'avoir formée aux bases de données financières. Cette compétence s'est révélée indispensable pour la réalisation de ma thèse.

Mes remerciements s'adressent également aux membres du laboratoire Centre d'Etudes et de Recherches Appliquées à la Gestion (CERAG) notamment les différents enseignants-chercheurs qui m'ont apporté leurs connaissances lors de présentations au sein de différents ateliers. Je remercie Monsieur le Professeur Ollivier Taramasco pour le temps qu'il m'a accordé et pour son expertise au sein de différentes séances de travail. Je remercie tout le personnel administratif en particulier Mesdames Florence Alberti et Coralie Lucatello qui nous permettent de réaliser notre travail dans les meilleures conditions possibles.

Ces années de thèse furent également l'occasion de dispenser des cours à l'IAE Savoie Mont Blanc et cette année à Grenoble IAE – campus de Valence en tant qu'ATER. Un grand merci à Monsieur Sébastien Geindre et à toute l'équipe administrative pour leur accueil chaleureux, leur compréhension et leur réactivité. Je remercie aussi Monsieur Philippe Madiès pour ses nombreuses discussions sur mon sujet de thèse et pour mon intégration au sein du campus de Valence.

J'adresse mes remerciements à l'Ecole Doctorale Sciences de Gestion (EDSG) de Grenoble, en particulier à Madame le Professeur Marie-Laure Gavard-Perret, directrice de l'EDSG, ainsi qu'à Madame Claire Escalon, gestionnaire de l'EDSG, pour leur soutien à de multiples reprises durant mon parcours de doctorat. Je remercie le conseil de l'EDSG pour la confiance qu'il m'a accordée dans l'attribution de mon financement de thèse.

Mes remerciements vont vers tous mes amis anciens ou actuels doctorants avec lesquels j'ai partagé des moments de joie, de travail et de doute parfois. Un grand merci à Barbara, Houda, Justine, Imène, Jingwen, Emma, Azadeh, Charlotte, Yann, Khalil, Chebli, Omar, Julien, Mathis, Hamza, Imad et tous les autres. J'ai une pensée spéciale pour Ahmad et Samarmar. Merci à Yann et Mohamad pour avoir pris le temps de relire mon travail.

Merci également à l'équipe d'Eurofidai durant mon stage et notamment aux repas du midi qui se sont poursuivis après.

Je remercie les responsables du master de cryptologie et sécurité informatique de Bordeaux, Monsieur Emmanuel Fleury et Monsieur le Professeur Gilles Zémor, qui m'ont permis d'améliorer mes bases en informatique et surtout qui m'ont fait découvrir mon sujet de thèse : les cryptomonnaies.

Je tiens à remercier également tous mes proches en dehors du monde académique, notamment mes amis, pour leur soutien, leurs conseils, les moments de pause qui m'ont permis de souffler et de me ressourcer pour réattaquer de plus belle.

Enfin, je tiens à remercier ma famille au sens large, très présente dans ma vie et particulièrement ma sœur et mes parents. Je les remercie pour tout l'amour, toute la confiance et toutes les valeurs qu'ils m'ont inculquées. Merci de nous avoir toujours soutenues, ma sœur et moi, dans tous nos choix quels qu'ils aient été et plus encore de nous avoir accompagnées dans nos découvertes personnelles et professionnelles. The Best Family.

**Elise Alfieri**

# Contents

**ACKNOWLEDGEMENT** . . . . . . . . . . . . . . . . . . . . . . . . . ii
**LIST OF FIGURES** . . . . . . . . . . . . . . . . . . . . . . . . . . viii
**LIST OF TABLES** . . . . . . . . . . . . . . . . . . . . . . . . . . x

**1 General Introduction** **1**
1.1 Overview . . . . . . . . . . . . . . . . . . . . . . . . . . 1
1.2 Research motivations . . . . . . . . . . . . . . . . . . . . . 8
1.3 Theoretical background and research questions . . . . . . . . . . 11
1.4 Contents of the dissertation . . . . . . . . . . . . . . . . . . 15
1.4.1 First research . . . . . . . . . . . . . . . . . . . . . . . 15
1.4.2 Second research . . . . . . . . . . . . . . . . . . . . . . 17
1.4.3 Third research . . . . . . . . . . . . . . . . . . . . . . . 18

**2 The blockchain, an innovative community tool serving organizations?** **27**
2.1 Introduction . . . . . . . . . . . . . . . . . . . . . . . . . 28
2.2 Blockchain as a community tool . . . . . . . . . . . . . . . . . 31
2.2.1 The starting point: Bitcoin's blockchain . . . . . . . . . . 31
2.2.2 Key dimensions . . . . . . . . . . . . . . . . . . . . . . 35
2.2.3 Features of blockchain communities . . . . . . . . . . . . 39
2.3 The potential impact of the blockchain on informational efficiency within organizations: A theoretical framework . . . . . . . . . . . 40
2.3.1 Issues faced by organizations . . . . . . . . . . . . . . . . 41
2.3.2 Solutions brought by blockchain . . . . . . . . . . . . . . 49
2.4 The appropriation process that leads to the extension of blockchain within organizations . . . . . . . . . . . . . . . . . . . . . . . 59
2.4.1 Appropriation process . . . . . . . . . . . . . . . . . . . 59
2.4.2 Blockchain evolution . . . . . . . . . . . . . . . . . . . . 63

2.4.3 Towards new institutions? . . . . . . . . . . . . . . . . . . 75
2.5 Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . 77

**3 On the nature and financial performance of Bitcoin 91**
3.1 Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . 92
3.2 About the nature of Bitcoin . . . . . . . . . . . . . . . . . . . 94
3.2.1 What is Bitcoin? . . . . . . . . . . . . . . . . . . . . . . 95
3.2.2 Is Bitcoin a currency ? . . . . . . . . . . . . . . . . . . . 96
3.2.3 Is Bitcoin "digital" gold or cash ? . . . . . . . . . . . . . . 97
3.2.4 Bitcoin as common stock . . . . . . . . . . . . . . . . . . 98
3.3 Performance models . . . . . . . . . . . . . . . . . . . . . . . 99
3.4 Results . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 103
3.4.1 Univariate results . . . . . . . . . . . . . . . . . . . . . . 103
3.4.2 Multivariate results . . . . . . . . . . . . . . . . . . . . . 110
3.5 Robustness checks . . . . . . . . . . . . . . . . . . . . . . . . 120
3.5.1 Regression specification . . . . . . . . . . . . . . . . . . . 120
3.5.2 Behavioral aspects . . . . . . . . . . . . . . . . . . . . . . 124
3.6 Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . 131

**4 Speculative bubbles and contagion effect in the cryptocurrency market 137**
4.1 Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . 138
4.2 Literature review . . . . . . . . . . . . . . . . . . . . . . . . 141
4.2.1 Speculative nature of the cryptocurrencies . . . . . . . . . 141
4.2.2 The financial bubble literature and methods for their detection . . . . . . . . . . . . . . . . . . . . . . . . . . 142
4.2.3 Cryptocurrencies and bubble aspects . . . . . . . . . . . . 145
4.3 Methodology . . . . . . . . . . . . . . . . . . . . . . . . . . 147
4.3.1 Multiple bubbles detection . . . . . . . . . . . . . . . . . 148
4.3.2 The main boom: 2017's peak/burst . . . . . . . . . . . . . 150
4.3.3 Data . . . . . . . . . . . . . . . . . . . . . . . . . . . . 161
4.4 Results . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 162
4.4.1 Univariate results . . . . . . . . . . . . . . . . . . . . . . 162
4.4.2 Multiple bubble detection - PSY results . . . . . . . . . . 166
4.4.3 The 2017 boom - LPPL results . . . . . . . . . . . . . . . 171

4.5 Robustness . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 185
4.5.1 Contagion analysis . . . . . . . . . . . . . . . . . . . . . . . 186
4.5.2 Cryptocurrencies' fundamental value model . . . . . . . . . 192
4.6 Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 193

**5 General Conclusion 205**
5.1 Main findings and contributions . . . . . . . . . . . . . . . . . . . . 205
5.2 Limits and further research . . . . . . . . . . . . . . . . . . . . . . 210

**6 Résumé en français 215**
**LIST OF TERMS AND ABBREVIATIONS** . . . . . . . . . . . . . . . . 241

# List of Figures


1.1 **Chronological timeline** . . . . . 2

1.2 **A taxonomy of money** . . . . . 3

1.3 **Different possible networks** . . . . . 4

1.4 **Cryptocurrency market dynamics** . . . . . 6

1.5 **Cryptocurrency market dominance** . . . . . 7

1.6 **Bitcoin price in USD** . . . . . 8

1.7 **Number of publications related to cryptocurrency by topic and by year** . . . . . 9

1.8 **Sub-research questions by study** . . . . . 13

2.1 **Research questions of the first study** . . . . . 29

2.2 **The stakeholders around the blockchain** . . . . . 32

2.3 **Forms of governance according to (Williamson, 1979)** . . . . . 43

2.4 **The blockchain Trilemma concept** . . . . . 55

2.5 **The two-level dimension mapping** . . . . . 64

2.6 **Top-10 cryptocurrencies** . . . . . 71

3.1 **Bitcoin market price** . . . . . 92

3.2 **Research questions of the second study** . . . . . 93

3.3 **Bitcoin return analysis - Histogram** . . . . . 105

3.4 **Bitcoin return analysis - QQplot** . . . . . 105

3.5 **Sharpe ratios** . . . . . 107

3.6 **Annual Sharpe ratio for Bitcoin** . . . . . 109

3.7 **Sharpe ratio: MSCI Indexes, Stocks Indexes and Bitcoin** . . . . . 109

3.8 **Sharpe ratio: Bonds, Commodities, Currencies and Bitcoin** . . . . . 110

4.1 **Research questions of the third study** . . . . . . . . . . . . . 140
4.2 **The top-4 cryptocurrencies prices in USD** . . . . . . . . . . . 146
4.3 **Hierarchical diamond lattice** . . . . . . . . . . . . . . . . . . . . 157
4.4 **Cryptocurrency returns - Histogram** . . . . . . . . . . . . . . 166
4.5 **Cryptocurrency returns - QQplot** . . . . . . . . . . . . . . . . 167
4.6 **LPPL fitting Bitcoin market prices** . . . . . . . . . . . . . . . . 178
4.7 **LPPL fitting Ether market prices** . . . . . . . . . . . . . . . . . 179
4.8 **LPPL fitting Litecoin market prices** . . . . . . . . . . . . . . . 180
4.9 **LPPL Ripple market prices** . . . . . . . . . . . . . . . . . . . . 181
4.10 **The top-4 cryptocurrencies returns** . . . . . . . . . . . . . . . . 187
4.11 **Autocorrelation of cryptocurrencies series** . . . . . . . . . . . 189
4.12 **Autocorrelation of cryptocurrencies series squares** . . . . . . 189
4.13 **The dynamic correlation coefficients** . . . . . . . . . . . . . . 192
4.14 **Predicted and actual market capitalization of Bitcoin** . . . . 193

# List of Tables


2.1 **Features** . . . . . . . . . . . . . . . . . . . . . . . . . . . 37

2.2 **Differences between contractual and cognitive approaches of the firm** . . . . . . . . . . . . . . . . . . . . . . . . . . . 47

2.3 **Strengths and weaknesses of the blockchain** . . . . . . . . . . 58

2.4 **Two-level dimension analysis of the blockchain** . . . . . . . . 65

2.5 **Top-10 cryptocurrencies** . . . . . . . . . . . . . . . . . . . . 70

3.1 **Descriptive statistics** . . . . . . . . . . . . . . . . . . . . . . 104

3.2 **Bitcoin return normality test** . . . . . . . . . . . . . . . . . . 104

3.3 **Correlation coefficients between Bitcoin and various asset classes** . . . . . . . . . . . . . . . . . . . . . . . . . . . . 106

3.4 **Sharpe ratios** . . . . . . . . . . . . . . . . . . . . . . . . . . 108

3.5 **Descriptive statistics of variables used in regressions** . . . . . 111

3.6 **Correlation matrix** . . . . . . . . . . . . . . . . . . . . . . . . 113

3.7 **Performance using the CAPM (Model 1), FF (Model 2) and extensions (Model 3)** . . . . . . . . . . . . . . . . . . . . . . 114

3.8 **Bitcoin's $\alpha$ based on Model 2 (Fama and French three-factor model)** . . . . . . . . . . . . . . . . . . . . . . . . . . . . 115

3.9 **Descriptive statistics of variables used in regressions for the Chinese market** . . . . . . . . . . . . . . . . . . . . . . . . . 117

3.10 **Correlation matrix on the Chinese market - Fama French Factors** . . . . . . . . . . . . . . . . . . . . . . . . . . . . 118

3.11 **Correlation matrix on the Chinese market - MSCI Factors** . 118

3.12 **Bitcoin's $\alpha$ on the Chinese market** . . . . . . . . . . . . . . . 119

3.13 **Collinearity: Test of independent variables** . . . . . . . . . . 120
3.14 **Residual analysis** . . . . . . . . . . . . . . . . . . . . . . . . . . 121
3.15 **Controlling for market sentiment in the CAPM (Model 1)** . . 128
3.16 **Controlling for market sentiment in the FF model (Model 2)** 129
3.17 **Controlling for market sentiment in the FF extended model (Model 3)** . . . . . . . . . . . . . . . . . . . . . . . . . . . . 130
4.1 **The actual peaks of the main boom in the cryptocurrency market** . . . . . . . . . . . . . . . . . . . . . . . . . . . . 161
4.2 **The windows samples for the LPPL model** . . . . . . . . . . . 162
4.3 **Descriptive statistics** . . . . . . . . . . . . . . . . . . . . . . . . 164
4.4 **Correlation matrices** . . . . . . . . . . . . . . . . . . . . . . . . 165
4.5 **Cryptocurrency returns normality tests** . . . . . . . . . . . . 166
4.6 **Multiple bubbles - Occurrence** . . . . . . . . . . . . . . . . . . 168
4.7 **Multiple bubbles - Bitcoin and Ether** . . . . . . . . . . . . . . 169
4.8 **Multiple bubbles - Litecoin and Ripple** . . . . . . . . . . . . . 170
4.9 **LPPL fitting model for Bitcoin prices** . . . . . . . . . . . . . 172
4.10 **LPPL fitting model for Ether prices** . . . . . . . . . . . . . . 173
4.11 **LPPL fitting model for Litecoin prices** . . . . . . . . . . . . . 174
4.12 **LPPL fitting model for Ripple prices** . . . . . . . . . . . . . . 175
4.13 **The bests fitting LPPL windows** . . . . . . . . . . . . . . . . . 177
4.14 **Numbers of significant results of LPPL - Expanding windows** 182
4.15 **Numbers of significant results of LPPL - Shrinking windows** 183
4.16 **Stationarity test of the fitting LPPL residuals** . . . . . . . . . 185
4.17 **Cryptocurrency returns and prices stationarity test** . . . . . 188
4.18 **Information related DCC-GARCH results** . . . . . . . . . . . 190
4.19 **DCC-GARCH results** . . . . . . . . . . . . . . . . . . . . . . . 191

## Chapter 1

# General Introduction

## 1.1 Overview

"I think the internet is going to be one of the major forces for reducing the role of government. The one thing that's missing but that will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B without A knowing B or B knowing A." claimed the Nobel Prize in economics, Professor Milton Friedman, 1999.

While cryptocurrencies[1] are a recent innovation that make multiple headlines, the underlying concept goes back several decades ago. As suggested by Friedman in 1999, the concept of "e-cash" was studied by several cryptographers (notably the cypherpunk movement[2]) during the same decade with the idea to create a new world and a novel way of exchanging through the Internet and cryptographic improvements[3]. eCash owned by DigiCash was the first digital currency company project using blind signatures innovations (Chaum, 1983), (Chaum, 1990) and the first attempt to solve the double-spending problem in computing sciences (e.g. the risk of spending twice the same coin or information[4]). However, this system was still linked to existing financial institutions and banks, and finally went bankrupt in 1998. After, there were several other attempts to improve the digital currency concept. For instance, "B-money" was

[1]All technical vocabulary is presented in the list of terms and abbreviations.

[2]A group of informal individuals who preach for proactive cryptography in order to ensure privacy and security.

[3]Several concepts used in the Bitcoin protocol are created during this period, for example: Timestamping (Haber and Stornetta, 1991), (Massias et al., 1999), the ECDSA elliptic curve (Vanstone, 1992), the Smart Contracts (Szabo, 1994), HashCash (Back, 1997), the creation of the peer-to-peer file sharing technology, Napster in 1999.

[4]See the list of terms and abbreviations.

at the origin of the Proof-of-Work and Proof-of-Stake concepts[5] (Dai, 1999). In 2004, the direct precursor of Ripples cryptocurrency, named “Ripplepay” was created by Ryan Fugger. The objective was to create a distributed monetary system for financial services where individuals can loan directly to each other without requiring a bank. The same year, Finney (2004) created the Reusable Proofs of Work (“RPOW”) that requires a reusable token through the Proof-of-Work mechanism. One year after, “Bit Gold”, a project similar to the Bitcoin system and based on computing performance (Proof-of-Work), works through the consensus mechanism in a distributed manner with the ledger concept (registry) (Szabo, 2005). However, this project was never implemented in practice and differs from Bitcoin in some points such as the purpose (a reserve currency based on metal (gold) properties for Bit Gold versus electronic cash for Bitcoin), different functions in the Proof-of-Work (a benchmark function for Bit Gold versus hash function for Bitcoin) and the supply rules (the Bit Gold value depends on the difficulty to create Bit Gold which varies over time versus in the Bitcoin system this difficulty is increasing over time due to the fixed supply of Bitcoin).

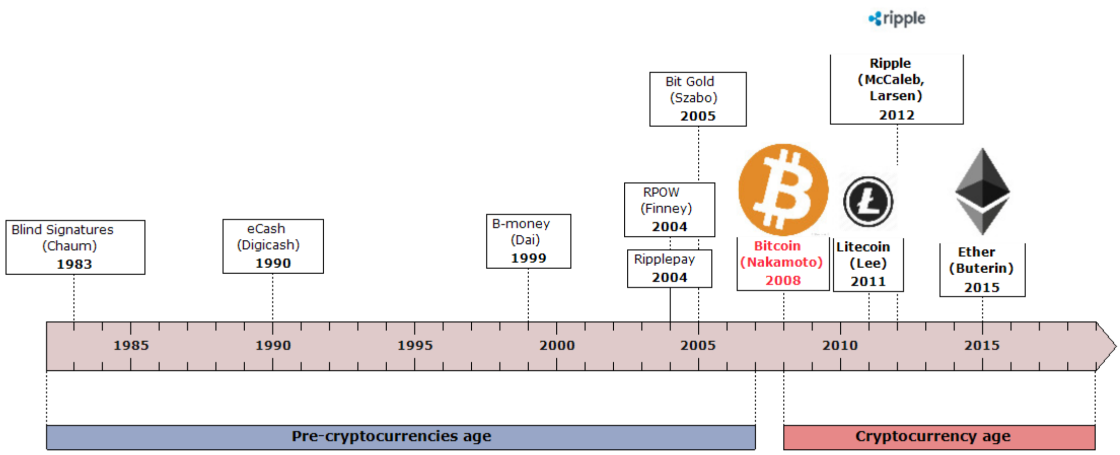


**Figure 1.1 Chronological timeline**
This figure illustrates the chronological timeline of the pre-cryptocurrency age and the cryptocurrency age and is annotated with the main events. Own work

[5] See the list of terms and abbreviations.

The main flaws in the previous attempts to create digital currencies was the double-spending problem, solved in a centralized manner through a designed third-party to ensure the coin transfer. The third-party is present to check for the transfer information, such as issue of identical information (or a coin) is sent (or spent) two times. Figure 1.1 - *Chronological timeline* summarizes the different innovations related to digital currencies.

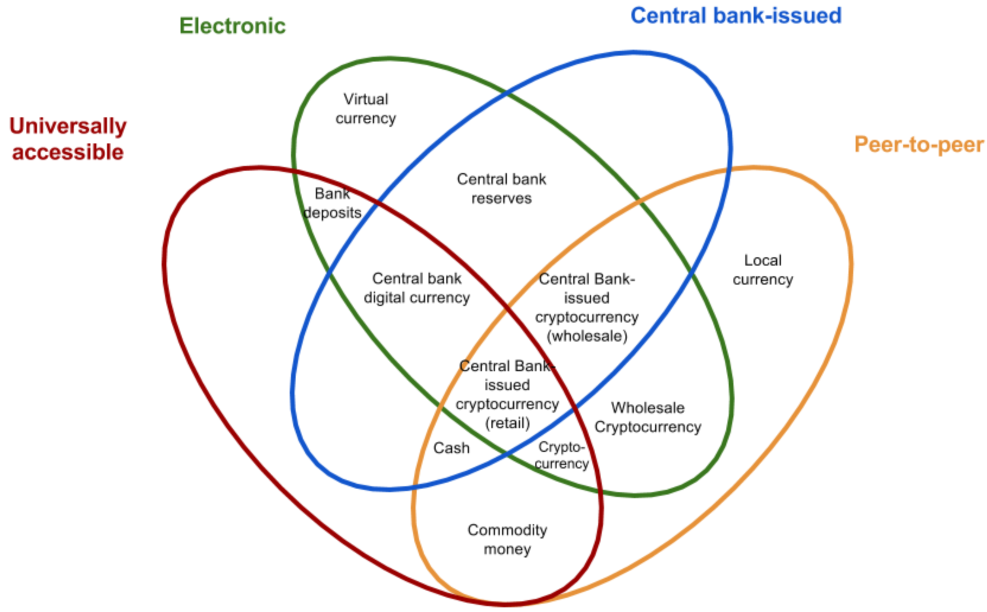


**Figure 1.2 A taxonomy of money**
This figure presents a taxonomy of money and is adapted from the Bank for International Settlements in 2017.

After the subprime crisis, in 2008, the trust in financial and monetary institutions is weakened. Whereupon, grouping all previous research findings together, Satoshi Nakamoto[6] establishes and implements the first existing cryptocurrency: the Bitcoin protocol (“bit” for the basic unit of information binary and “coin” for a piece of money).

As shown in Figure 1.2 - *A taxonomy of money*, the Bank for International Settlements defines a “cryptocurrency” as an electronic, peer-to-peer and universally accessible form of money that is not issued by a central bank. The solution of the double spending issue in a distributed network is found by grouping

[6]Satoshi Nakamoto is the pseudonymous of unknown creator of the Bitcoins.

together all previous findings in cryptography, which explains the success of Bitcoin. Exchanges are based on a consensus system implicating the responsibility of all users in a distributed network, (see Figure 1.3 - *Different possible networks*).

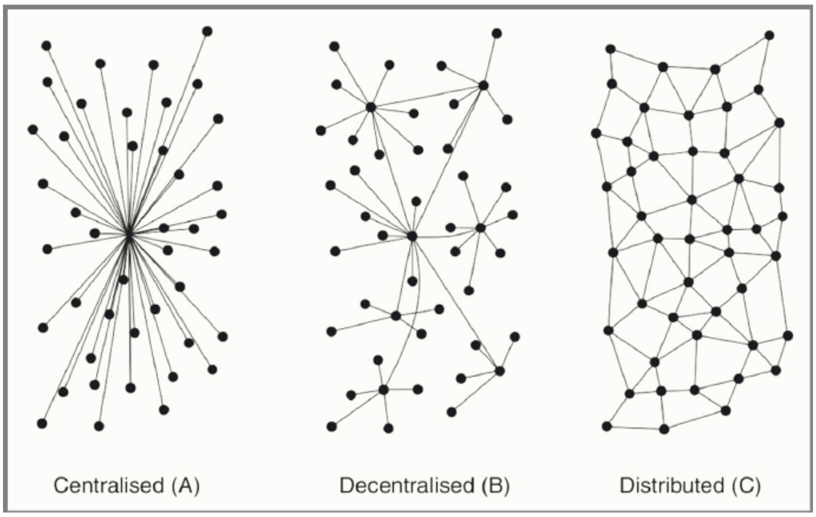


**Figure 1.3 Different possible networks**
This figure shows three different possible network configurations: the centralized one (A) where all the nodes converge to one center (server), the decentralized (B) where there exist several intermediaries and the distributed one (C) where there are no intermediaries at all and where all the nodes directly connected to each other. Source: (Baran, 1962).

The underlying ledger, the blockchain[7], is the public (initial) database which records all the transactions since its inception and ensures the proper functioning in a transparent way. The low exchange and transactions costs relatively to the traditional monetary systems, the privacy issues related to the investors' identity while the transactions are public, accessible, reliable and inviolable have the potential to attract many users and investors. The success of Bitcoin fosters many improvements related to this innovation. First, on technical aspects of the blockchain technology, many other applications than a single mean-of-payment system are put in place in different industries where there is a need to store, transfer and exchange data through a third-party such as financial industry, insurance, Internet of Things (IoT) and supply chain activities.

[7] See the list of terms and abbreviations.

Second, related to the cryptocurrency market, many different new cryptocurrencies are initiated since the creation of Bitcoin. Some are devoted to humanitarian support (FoldingCoin[8] (Ross et al., 2018)), micropayment (ReddCoin[9] (Ren, 2014)), anonymity and privacy (Monero[10] and Dash[11] (Duffield and Diaz, 2018)), intended for financial services (Ripple[12] (Schwartz et al., 2015)), or for commercial use (NEM[13](Nem, 2018)). Companies may also be willing to create their own cryptocurrencies in a customer loyalty purpose (Whoppercoin of Burger King) or grouped with different businesses to create a new way of exchanging (Facebook's Libra (Amsden et al., 2018) (Libra, 2019)).

Most of time, these new cryptocurrencies are a single improvement of Bitcoin. Ethereum[14] is a blockchain-based platform available to run different Smart Contracts and decentralized applications. Ether is its associated cryptocurrency used as means of payment for the platform service of Ethereum blockchain (Buterin, 2015). If Bitcoin is sometimes referred to as the "gold coin", [15] is the "silver" version, notably because it aims to facilitate the small transactions rapidly. The maximal number of units is fixed at 21 million for Bitcoin, 84 million for Litecoin but virtually infinite for Ether. In the same vein, the time between transactions amounts to 10 minutes for Bitcoin, 2.5 minutes for Litecoin, and seconds for Dash and Ripple.

More recently, cryptocurrency-based tokens are created to raise funds for various projects through an Initial Coin Offering process. An Initial Coin Offering (ICO) is a fundraising method in which specific tokens are issued and priced in cryptocurrencies at the launch of a project and for a limited period of time. After the project, the token holders can trade their tokens in a secondary market or sometimes use it in the project itself. The number of ICOs exceeds

[8] FoldingCoin is a health-based token which the purpose is to support diseases such as cancer and Alzheimer. https://foldingcoin.net/

[9] Reddcoin is focusing on social network tipping and micro-donation. https://reddcoin.com/

[10] Transaction sources and destinations are untraceable, the total of coins held by a user cannot be known due to stealth addresses. https://web.getmonero.org/

[11] Dash lets the possibility hide the transactions. https://www.dash.org/

[12] https://www.ripple.com/

[13] The NEM project offers the possibility to personalize the blockchain for many different purposes such as financial payments, creation of its own cryptocurrency, mobile payments, equity market, escrow services, liquid asset and Paypal adaptation. https://nem.io/xem/

[14] See the list of terms and abbreviations at Ether. https://www.ethereum.org/

[15] See the list of terms and abbreviations. https://Litecoin.org/

2,000 in 2018 for a total amount raised of $11.4 billion[16] [17]. This is why some improvements have been set up recently such as Security Token Offering (STO) which is simply an Initial Public Offering (IPO) in the cryptocurrency market with specific legal market rules or the Initial Exchange Offering (IEO) in which the project is audited by exchange platforms. Nowadays, more than the half of cryptocurrencies recorded on the Coinmarketcap website[18] are considered as tokens (1,422). Because the extensions of Bitcoin are numerous, in this thesis, we will focus our analysis, mainly on the blockchain technology and cryptocurrencies.

The success of cryptocurrencies since their creation (2008) can be illustrated by their market capitalization and the number of cryptocurrencies created, Figure 1.4 - *Cryptocurrency market dynamics*.

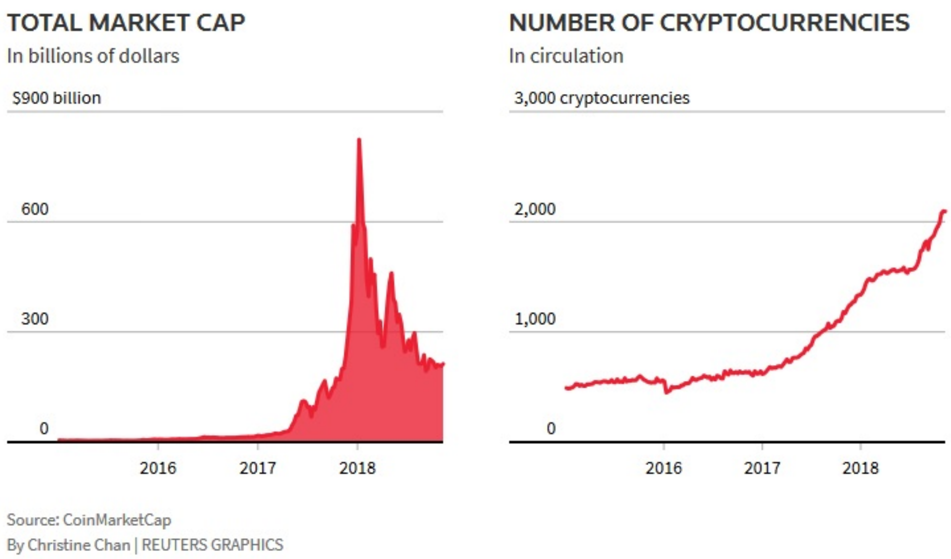


**Figure 1.4 Cryptocurrency market dynamics**
This figure shows the total market capitalization and the number of cryptocurrencies in the market. The sample is drawn from Reuters website using the data from the Coinmarketcap website and covers the period between 2014 and the end of 2018.

[16]https://cointelegraph.com/news/ico-market-2018-vs-2017-trends-capitalization-localization-industries-success-rate

[17]This number should be taken with a grain of salt because the process is unregulated, there exist multiple database concerning ICO data.

[18]https://coinmarketcap.com/

Bitcoin is created in 2008, less than 9 years after Friedman's premonitory statement, and 11 years later, the number of cryptocurrencies reached 2,449 on August 8th, 2019[19]. Figure 1.4 shows that, in 2016, the number of cryptocurrencies was stable around 500. An important expansion in the number of cryptocurrencies has occurred since 2017. The number of cryptocurrencies is not the only indicator of how huge and rapid the evolution of the cryptocurrency market is. The increase in market capitalization is more than 19,700% from 2013 ($ 1.6 billion) to July 2019 ($ 317 billion), reaching even a total amount of $ 830 billion on January 7th, 2018. Between 2013 and 2019, the market capitalization has increased on average every year by 141%. However, the market is largely dominated by the famous Bitcoin cryptocurrency which accounts for 61% of the market in July 2 2019, Figure 1.5 - *Cryptocurrency market dominance*.


**Figure 1.5 Cryptocurrency market dominance**

This figure shows the share of total market capitalization (dominance) over time of the following cryptocurrencies: Bitcoin, Ether, Bitcoin Cash, Litecoin, Ripple, Dash, NEM, Monero, IOTA, NEO and others. The sample is drawn from the Coinmarketcap website and covers the period between 2013 and mid-2019.

[19]https://coinmarketcap.com

Cryptocurrency's prices are also a proper indicator of their attractiveness. *Ceteris paribus*, the price is based on the supply and demand equilibrium implying that a higher price is due to an augmented demand. The price of Bitcoin is significantly volatile and impressive, Figure 1.6 - *Bitcoin prices in USD*, providing an annual risk-return profile of 269% of return for 116% of volatility since its creation until mid-July 2019. The other cryptocurrencies follow the same trends as Bitcoin but at a smaller scale.

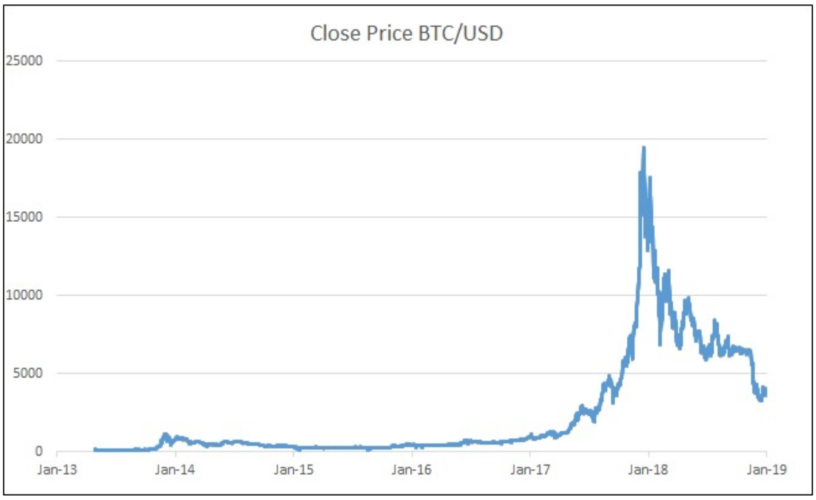


**Figure 1.6 Bitcoin price in USD**
This figure presents the price of Bitcoin expressed in dollars covering the period of June 2013 until July 2019. The sample comes from the Coinmarketcap website.

## 1.2 Research motivations

The research in cryptocurrencies has a multi-disciplinary nature. The main domain interested in this topic is technological sciences, with 556 publications (38%) over the period 2013-2018 in computer sciences, 308 (21%) in engineering and 181 (12%) in telecommunications. The economic and management sciences represent only 8% (114) of the entire sample of publications between 2013 and 2018, (Dabbagh et al., 2019). When years 2012 and 2019 are included, this proportion becomes slightly higher: 18% (279) (Merediz-Sola and Bariviera, 2019). Bibliometric studies show the increasing trend in research related to cryptocurrencies and blockchain regardless of the field, (Dabbagh et al., 2019) (Merediz-Sola and Bariviera, 2019). Since the beginning of this thesis

(2016), the number of publications, in all disciplines combined, has dramatically increased. For example, based on the Web of Science Core Collection[20], the publications specifically focusing on the Bitcoin subject has significantly increased (Dabbagh et al. (2019) find 176 Bitcoin-related publications in 2016 and 262 in 2018 whereas Merediz-Sola and Bariviera (2019) find 192 Bitcoin's publications in 2016 and 384 in 2018). The research on other related keywords such as "blockchain", "cryptocurrency", "ethereum" or "Smart Contracts" shows the same increasing trend (Dabbagh et al., 2019) (see Figure 1.7 - *Number of publications related to cryptocurrency by topic and by year*).

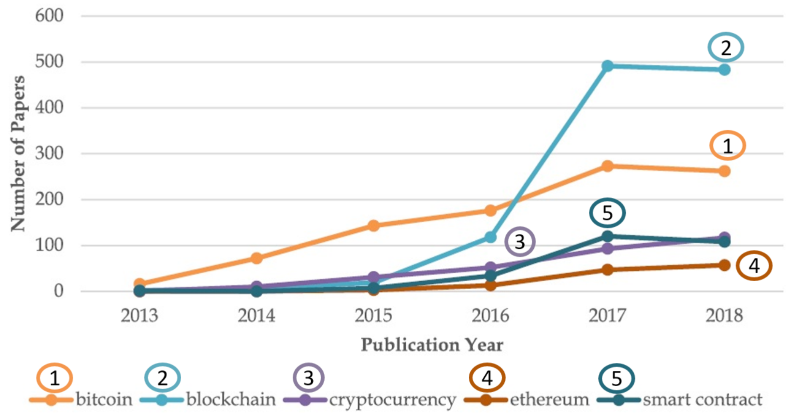


**Figure 1.7 Number of publications related to cryptocurrency by topic and by year**
This figure is adapted from the article of (Dabbagh et al., 2019). This is the first figure of their paper entitled "Yearly publication trends of different topics"[21].

At the beginning of the writing of this thesis (in 2016), there was a gap in social sciences compared to computing science literature. However, the subject is important for the economic and management fields because cryptocurrencies and their underlying technology (the blockchain) have significant implications regarding the dissemination of information between stakeholders. At the same time, they offer an additional way to create value for investors through cryptocurrency investments and the adoption of blockchain to business. Because this field of research is quite new, the relevance of this research topic depends on the cryptocurrency dynamics and its innovative projects related to the blockchain. After a trend favoring research in computing and technological sciences, social

[20] A citation indexing service owned by Clarivate Analytics.

sciences start to study this new phenomenon, particularly studies in economics and management. The topic is split in two main literature reviews, one focusing on blockchain technology and the second one on cryptocurrencies themselves.

In the blockchain literature, the cryptocurrency-based technology is considered as a disruptive innovation, source of a huge evolution in the management field. The blockchain technology has been a topic of interest these last years (with the largest number of publications: 483 between 2013 and 2018 (Dabbagh et al., 2019)). The literature emphasizes its potential for innovation in all industries, particularly the financial industry (Lamberti et al., 2017), and in a more general way, for organizations (Chapter 2). Some authors model the blockchain system using the game theory (Biais et al., 2017), (Shermin, 2017). The blockchain challenges existing organizations and through its characteristics has an impact on different costs as well as on the design of contracts (Chapter 2), such as (1) transaction costs (MacDonnell, 2014), (Kim, 2017), (Larios-Hernandez, 2017), (Pietrewicz, 2018); (2) agency costs (Collomb and Sok, 2016), (Tapscott and Tapscott, 2017); (3) incompleteness of contracts through the implementation of the so-called "Smart Contracts" (Szabo, 1997), (Cong and He, 2017) (Catalini and Gans, 2018).

Economists were the first in the field of social sciences to take an interest in cryptocurrencies. Bitcoin, considered as a currency, offers a new way to exchange and to buy products and services. The first studies focuses on the currency nature and properties of the cryptocurrency innovation, (Grant, 2014), (Kancs et al., 2015), (Lakosmki-Laguerre and Desmedt, 2015), (Baur et al., 2016), (Figuet, 2016). In a second phase, the financial science starts to have an interest in the topic by timidly testing its performance with simple measures (Brière et al., 2015), (Burniske and White, 2017). The creation of mutual funds, e.g. the Bitcoin Investment Trust and ARK Investment Management in 2015, as well as the decision of the Internal Revenue Service[22] to consider cryptocurrencies as a property, confirm the financial interest in terms of investments. One of the contributions of this thesis is to debate the nature of cryptocurrencies as well as to provide an insight of its financial performance with more relevant models based on informational concept such as the CAPM and Fama and French models (Fama and French, 1992), never considered previ-

[22]The Internal Revenue Service (IRS) is the US federal government agency of the Department of the Treasury that collects taxes and administrates the Internal Revenue Code.

ously in the literature to the best of our knowledge (Chapter 3, this study being published in the Journal of Risk Finance).

If we remain on the cryptocurrency market, which faces a very high volatility, the efficiency (Nadarajah and Chu, 2017), (Urquhart, 2017) and more precisely the speculative aspect of cryptocurrencies are quickly highlighted. Existing research focuses on potential bubble periods independently of each other; for example by studying the end of 2013 when Bitcoin price reached for the first time $1,000 (MacDonnell, 2014) (Cheah and Fry, 2015) (Fry and Cheah, 2016) or focusing on the end of 2017 when the price of Bitcoin exceeded $19,000 with contradictory results of bubble evidence (Corbet et al., 2017), (Fry, 2018), (Chaim and Laurini, 2019), (Wheatley et al., 2019). The first complete bubble detection analyses over a large period and including potential bubbles for different cryptocurrencies (not just Bitcoin) are very recent (Hafner, 2018), (Su et al., 2018), (Bouri et al., 2019), (Li et al., 2019), (Vogiazas and Alexiou, 2019), (Wheatley et al., 2019). By using two different detection models adapted from (Phillips and Shi, 2018) and (Johansen et al., 2000), we perform a global research of multiple bubbles detection with a focus on the 2017 peak for different cryptocurrencies, thus highlighting some correlation and even contagion effects in the cryptocurrency market (Chapter 4).

## 1.3 Theoretical background and research questions

The novelty, the attractiveness, the low transaction costs as well as the tremendous volatility of prices on the cryptocurrency market raise the question of the efficiency. Market efficiency represents "a market in which prices always fully reflect available information", (Fama, 1970). Fama explains in his seminal paper that the market is unbeatable if it is efficient ("Efficient Market Hypothesis"). This theory is based on several assumptions: (1) Investors are rational about financial decisions; (2) Information has to be freely available (information is not costly and the access to information is possible and easy for everyone), allowing investors to analyze it together instantly; (3) There are no transaction costs or taxes; (4) The market is liquid and no investor can influence the price by selling or buying orders involving an important number of assets (investor atomicity). Information is a key feature of the Efficient Market Hypothesis (EMH) because prices have to be reactive to new information. However, there are different types of information such as past, present, public and private information, implying different levels of efficiency. A strong efficiency means no one can beat the market regardless if the information utilized is past, present, public or private. An insider that takes a financial decision based on his own private information sends a fully revealing signal to the market because transactions are transparent to other investors. In the semi-strong efficiency form, the private information would allow him to beat the market, while public information is instantly integrated into prices. With weak efficiency, past information does not allow to beat the market, only private and public information could be used to beat the market.

In practice, there are frictions such as informational asymmetries and transaction costs which reduce the market's efficiency. The cryptocurrency market seems to be less affected by such frictions. The blockchain technology allows to reduce transaction costs and improves the information's transparency and its accessibility to economic agents, such as the stakeholders of a firm if the process is applied to businesses or investors on the cryptocurrency market. The blockchain technology as well as investments on the cryptocurrency market create value by reducing frictions related to information. To become more efficient, a market has to respect four features: (1) Availability of information; (2) Large number of investors with the ability to analyze the information; (3) Legal investor protections; (4) Liquid secondary market with low transaction costs (D'avolio et al., 2002). These authors study the impact of a new technology on the efficiency of stock markets and find that new technology democratizes this market by increasing the number of investors and reducing transactions costs (such as the costs of gathering and executing trades). They emphasize the legal aspect of investor protections. Lee et al. (2017) study the relationship between technology (Information and communications technology, ICT) and stock market capitalization. They find this relationship to be positive and more precisely that ICT allows participants to have better access to accurate information as well as to improve the country's economic factors. Information technologies improve efficiency of the stock market (Abadi et al., 2013) as well as in the real estate market (Kummerow and Lun, 2005) due to its long-run impact in organizations (businesses processes and industry structure).

Therefore, the research problems tackled by this thesis are centered around the notion of **efficiency of the cryptocurrency market considering that the underlying technology, the blockchain, plays a central role in this sense**. The sub-research questions are summarized in Figure 1.8 - *Sub-research questions by study*.

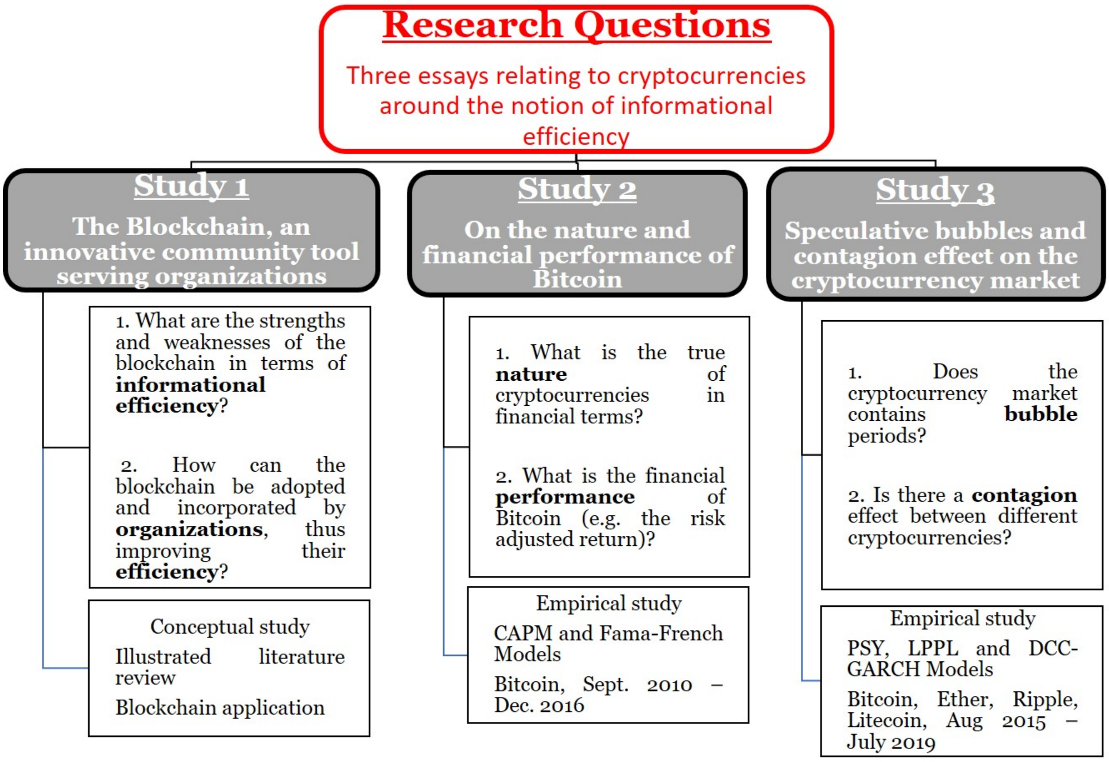


**Figure 1.8 Sub-research questions by study**
This figure presents the sub-research questions of the three studies of the dissertation around the central notion of efficiency.

Firstly, our analysis focuses on blockchain by considering that cryptocurrencies are an important application of this technology. Cryptocurrencies rely mainly on the information that is stored and transferred thanks to the blockchain. The blockchain technology allows to reduce frictions such as information asymmetries thanks to its transparency and to decentralization between all participants in the process. It also allows to reduce transactions costs thanks to its speed and simplicity in the validation process compared to the existing services. Existing services require a third-party that spends time, effort and money to correctly execute the transactions. The informational efficiency related to blockchain could be explained by the arbitrage between information acquisition costs and the extra-performance generated by this technology thanks to informational advantages, as analyzed in the theoretical framework related to the contractual perspectives of the organization theory (such as transaction cost, agency issues and property rights concerns). This disruptive technology can be considered as an adaptive management tool for existing and future businesses, aimed at improving their services in several industries for which information needs to be stored and exchanged. The first sub-questions to study is at a macro-level: *What is the general potential (strenghts and weaknesses) of the blockchain technology in terms of informational efficiency issues?* and *How can the blockchain developed in informal communities be adopted and incorporated by organizations, thus improving their efficiency?* To that aim, the case of cryptocurrencies will be the focus of our analysis.

Before starting to analyze the cryptocurrency market itself, it is necessary to understand what we are dealing with, namely, *what is the true nature of cryptocurrencies in financial terms?* Are they "currencies" as their name suggests? Are they rather a kind of "store of value" frequently described as an electronic gold? Are they similar to financial assets such as common stocks? After this discussion on the nature of cryptocurrencies we will base our analysis on the assumption that cryptocurrencies represent financial assets and more precisely they may be assimilated to common stocks. The arguments to support this hypothesis will be developed in this thesis. After analyzing the nature of the Bitcoin, we will analyze *the financial performance of cryptocurrencies (e.g. the risk-adjusted return), and more precisely that of the Bitcoin* by using a large database. Our objective is to analyze whether the Bitcoin over or under performs the common stock market. The theoretical frameworks used to test the financial performance coming from the Efficient Market Hypothesis are the CAPM and Fama and French Models (Fama and French, 1992). If the market is fully efficient, then the price integrates all the information and therefore, there is no possibility to beat the market and to earn money by investing in specific assets, such as Bitcoin.

The finding of a positive and persistent financial performance for Bitcoin leads us naturally to ask the question whether it is just a speculative bubble. This hypothesis is supported by the tremendous volatility of Bitcoin. The third main analysis is focused on *the speculative bubble aspect of cryptocurrencies*.

To that aim we choose theoretical models of bubble detection that do not require to determine the fundamental value such as multiple bubble model (Phillips and Shi, 2018) as well as single bubble detection and prediction model (Johansen et al., 2000). We apply these models to several cryptocurrencies that are correlated to each other, therefore the contagion effect between them has to be tested. Contagion is impacted by the information asymmetry level on the market, (Kodres and Pritsker, 2002).

## 1.4 Contents of the dissertation

Specifically, our research is developed through three studies in this thesis. First at the macro-level, we focus on the innovation provided by blockchain technology and its potential to improve efficiency for organizations and businesses. Second, we study the cryptocurrency market by raising the question of their nature in a financial perspective and testing their risk-adjusted returns. Third, we study their speculative bubble aspects and the contagion/correlation between cryptocurrencies inside this market. These three studies are briefly described below.

### 1.4.1 First research

The blockchain technology innovation is initially created for the development of a cryptocurrency application inside a special informal community. The idea is to create a new ecosystem decorrelated from existing financial institutions and formal businesses in which individuals exchange with each other directly through the blockchain technology. Rapidly, this technology demonstrates its potential to be adopted and integrated inside several services of existing formal organizations to improve information transfers (higher transparency, less intermediaries) and to create value. The first study aims to explain how the blockchain developed within informal communities has the potential to be adopted into organizations.

First, we provide a theoretical framework for the blockchain technology centered around the organization theory. The reasoning focuses on the basic contractual approach with transaction cost theory, agency theory, incomplete contract theory and property rights, as well as the capabilities-based approach with the cognitive approach. The blockchain fundamentally deals with information because it is a tool for storing data as well as exchanging data in a more transparent and distributed way implying several improvements in terms of informational efficiency. Blockchain enhances access to information for participants (especially users), decreasing transaction costs and agency costs thanks to transparency, rapidity and simplicity in a secured way. Opportunist behaviors are therefore controlled by the blockchain technology through the implementation of Smart Contracts that take into account as many future situations as possible. The validation process of transactions is distributed among participants (miners) through a consensus-based mechanism supporting the stakeholder perspective. All stakeholders are involved in the eco-system based on a technology which works with cryptographic principles. However, the blockchain is also source of other issues (such as operational risks or ethical questions) that present a subtle tradeoff to take into consideration, by balancing strengths and weaknesses.

Second, through an illustrated literature review, we provide a two-prong analysis regarding the blockchain technology characteristics and their evolution with a community focus. We focus on two main participants in the community blockchain: (1) users that can read the ledger and exchange information (a coin, in the case of Bitcoin) through the openness dimension; (2) miners that participate to the consensus mechanism to validate each transaction through the permission dimension. The respective access rights of both participants to the ledger can evolve according to the use of blockchain in a new organizational project depending on the project purposes (for example a project with sensitive and confidential data is not the same as a public project). We present four cases of possible blockchains based on both dimensions and more precisely we highlight that the blockchain evolution trend starts with public permissionless blockchain (cryptocurrency ones) to private permissioned blockchain (formal industries and for example the Libra project of Facebook). Blockchain could appear as a full-blown institution of governance connecting many organizations together. For instance, Facebook's Libra has the potential to gather all together organizations with different purposes such as payment services, e-commerce and sharing economy, cryptocurrencies business, investment funds and NGOs.

### 1.4.2 Second research

The question that arises from the first study is to determine the "true" nature of cryptocurrencies. This second reasearch has two aims. The first one is to provide a clear answer related to the nature of cryptocurrencies allowing to use specific models existing in the literature depending on the asset's nature. We show that Bitcoin shares similarities with currencies (payment systems that allow to exchange goods and services), with gold (some economic properties such as the monetary creation, the role of safe haven decorrelated from government), and with financial assets, more precisely common stocks. Bitcoin can be part of the intangible asset of the blockchain as well as the human capital of the community (experts in computing) to ensure the credibility of the system. The high risk-return profile is more similar to investments in common stock than other assets. This argument is supported empirically (Glaser et al., 2014), (Yermack, 2017), (Baur et al., 2016) and in practice by the US Internal Revenue Service (IRS) in 2014 as well as the Securities and Exchange Commission (SEC) in 2017. Since 2014 the IRS defines cryptocurrencies as part of the properties whereas the SEC in 2017 considers tokens-based cryptocurrencies as securities.

The second objective is to study empirically Bitcoin performance with more relevant measures than those already used in the literature. After arguing that cryptocurrencies look more like common stocks than currencies or gold, we choose to study the performance by measuring the risk-adjusted return ($\alpha$) by main regions based on the CAPM and the Fama-French 3-Factors models (Fama and French, 1992) as well as an extended model adding two others factors (gold and bonds). We use daily Bitcoin prices from September 2010 to December 2016 from the blockchain.info (now blockchain.com) website[23] as well as international global factors of the Kenneth R. French's website[24] for the World, Europe and Asia-Pacific regions. We extend the analysis by studying the performance also in China because the Chinese exchange cryptocurrency market covers 90% of Bitcoin transaction. We self-constructed the Chinese portfolios and the Fama-French factors and compared them to MSCI China factors related to the size and the value. Chinese data, gold, bond indices benchmarks (Gold bullion USD/troy ounce rate, and Pimco Invest Grade Corporate Bond

[23]https://blockchain.info

[24]http://mba.tuck.dartmouth.edu/pages/faculty/ken.french/

Exchange-Traded Fund, respectively) come from the Datastream database. Our findings show that integrating Bitcoin in a portfolio improves its diversification and provides a positive and significant risk-adjusted return regardless the regions. We also test for the robustness of our results with econometric methodologies that account for non-normality issues of with the regressions' errors and market sentiment variables. Controlling for such issues do not change qualitatively our results, thus further confirming our findings.

### 1.4.3 Third research

The high performance of Bitcoin measured in the second research questions the speculative bubble aspect of cryptocurrencies. First, we recall that the recent literature attempts to model a cryptocurrency fundamental value different from zero, implying that cryptocurrencies are not just only one bubble. However, bubbles can exist even if an asset possesses a fundamental value because by definition bubbles are characterized by prices deviating far from their fundamental value. It is very likely that the cryptocurrency market dynamics includes some periods of bubbles notably appearing in Bitcoin prices at the end of 2013 and at the end of 2017. The innovation aspects of cryptocurrencies, notably their technology (the blockchain), could emphasize a speculative reaction. Such reaction related to new products or technologies added to the "showmanship" of lead-users may explain the creation and development of a bubble (Chang et al., 2016). This phenomenon seems to be a reminiscence of the dotcom bubble in the early 2000.

The objective of the third study is also twofold. First, we analyze the cryptocurrency market on the period from 2013 to July 2019 using a recent multiple bubble detection model (Phillips and Shi, 2018). Second, we focus on the main peak/burst in the cryptocurrency market that happened at the end of 2017 using the Log Period Power Model (LPPL) model of (Johansen et al., 2000)[25]. The purpose of this research is to provide an entire analysis of the market dynamics in terms of bubbles detection on a long period of time as well as to focus on the main peak/burst that happened on the cryptocurrency market. We go further than in traditional bubble detection studies, in particular by highlighting a strong contagion effect between the different cryptocurrencies. The information

[25]Both models do not require the "true" fundamental value.

provided by the most dominant cryptocurrency (Bitcoin) seems to influence the dynamics of the others. This is why in the robustness section, we test the contagion of these four cryptocurrencies using the Dynamic Conditional Correlation (DCC)-GARCH Model (Engle and Sheppard, 2001). Another contribution is that our study is applied to the four main cryptocurrencies including Bitcoin but also Ether, Ripple and Litecoin, using their daily closing prices in USD from the coindesk[26] and the coinmarketcap websites. Our results show evidence of multiple bubbles on the cryptocurrency market using (Phillips and Shi, 2018) model and predict a crash for the end of 2017 using the LPPL model (Johansen et al., 2000), close to the reality. More precisely, the detection of bubbles suggests a dynamic correlation between cryptocurrencies (stronger in normal period and lower in bubble situation).

## References

Abadi, H. R. D., Faghani, F. and Tabatabaee, S. M. (2013). Impact of information technology development on stock marketdevelopment.empirical study in the world's leading capital markets, *International Journal of Academic Research in Accounting, Finance and Management Sciences* **3**(1): 382–390.

Amsden, Z., Arora, R., Bano, S., Baudet, M., Blackshear, S., Bothra, A., Cabrera, G., Catalini, C., Chalkias, K., Cheng, E., Ching, A., Chursin, A., Danezis, G., Giacomo, G. D., Dill, D. L., Ding, H., Doudchenko, N., Gao, V., Gao, Z., Garillot, F., Gorven, M., Hayes, P., Hou, J. M., Hu, Y., Hurley, K., Lewi, K., Li, C., Li, Z., Malkhi, D., Margulis, S., Maurer, B., Mohassel, P., de Naurois, L., Nikolaenko, V., Nowacki, T., Orlov, O., Perelman, D., Pott, A., Proctor, B., Qadeer, S., Rain, Russi, D., Schwab, B., Sezer, S., Sonnino, A., Venter, H., Wei, L., Wernerfelt, N., Williams, B., Wu, Q., Yan, X., Zakian, T. and Zhou, R. (2018). The libra blockchain, *White paper* .

Back, A. (1997). A partial hash collision based postage scheme.
**URL:** `http://www.hashcash.org/papers/announce.txt`

Baran, P. (1962). On distributed communications networks, *RAND Corporation* pp. 2626–1962.

[26]https://www.coindesk.com/

Baur, D. G., Hong, K. and Lee, A. D. (2016). Virtual currencies: Media of exchange or speculative asset?, *SWIF Institute Working Paper* (2014-007).

Biais, B., Bisière, C., Bouvard, M. and Casamatta, C. (2017). The blockchain folk theorem, *Working paper* **TSE-817**.

Bouri, E., Shahzad, S. J. H. and Roubaud, D. (2019). Co-explosivity in the cryptocurrency market, *Finance Research Letters* **29**: 178–183.

Brière, M., Oosterlinck, K. and Szafarz, A. (2015). Virtual currency, tangible return: Portfolio diversification with bitcoins, *Journal of Asset Management* **16**(6): 365–373.

Burniske, C. and White, A. (2017). Bitcoin: Ringing the bell for a new asset class, *Ark Invest Research* .

Buterin, V. (2015). A next-generation smart contract and decentralized application platform, *White Paper* .

Catalini, C. and Gans, J. (2018). Some simple economics of the blockchain, *NBER Working Paper* .

Chaim, P. and Laurini, M. (2019). Is bitcoin a bubble?, *Physica A: Statistical Mechanics and its Applications* **517**: 222–232.

Chang, V., Newman, R., Walters, R. and Wills, G. (2016). Review of economic bubbles, *International Journal of Information Management* **36**(4): 497–506.

Chaum, D. (1983). Blind signatures for untraceable payments, *Advances in Cryptology Proceedings of Crypto* **82**(3).

Chaum, D. (1990). Untraceable electronic cash, *in* S. Goldwasser (ed.), *Advances in Cryptology - CRYPO'88*, pp. 319–327.

Cheah, E.-T. and Fry, J. (2015). Speculative bubbles in bitcoin markets? An empirical investigation into the fundamental value of bitcoin, *Economics Letters* **130**: 32–36.

Collomb, A. and Sok, K. (2016). Blockchain and distributed ledger technologies (DLT): What impact on financial markets ?, *Opinions and debats* **15**.

Cong, L. W. and He, Z. (2017). Blockchain disruption and smart contracts, *SSRN Elec. Journal* .

Corbet, S., Lucey, B. and Yarovaya, L. (2017). Datestamping the bitoin and ethereum bubbles, *Finance Research Letter* .

Dabbagh, M., Sookhak, M. and Safa, N. S. (2019). The evolution of blockchain: A bibliometric study, *IEEE Access* **7**.

Dai, W. (1999). B-money.
**URL:** `http://www.weidai.com/bmoney.txt`

D'avolio, G., Gildor, E. and Shleifer, A. (2002). Technology, information production, and market efficiency, *Economic Policy for the Information Economy. Federal Reserve Bank of Kansas City* .

Duffield, E. and Diaz, D. (2018). Dash: A payments-focused cryptocurrency, *White Paper* .

Engle, R. F. and Sheppard, K. (2001). Theoretical and empirical properties of dynamic conditional correlation multivariate GARCH, *NBER Working Paper* **8554**.

Fama, E. (1970). Efficient capital markets: A review of theory and empirical work, *The Journal of Finance* **25**(2): 383–417.

Fama, E. and French, K. (1992). The cross-section of expected stock returns, *The Journal of Finance* **XLVII**(2): 427–465.

Figuet, J.-M. (2016). Bitcoin et blockchain : quelles opportunités ?, *Revue d'économie financière* **123**(3): 325–338.

Finney, H. (2004). Reusable proofs of work.
**URL:** `https://nakamotoinstitute.org/finney/rpow/index.html`

Fry, J. (2018). Booms, busts and heavy-tails: The story of bitcoin and cryptocurrency markets?, *Economics Letters* **171**: 225–229.

Fry, J. and Cheah, E.-T. (2016). Negative bubbles and shocks in cryptocurrency markets, *International Review of Financial Analysis* **47**: 342–352.

Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. C. and Siering, M. (2014). Bitcoin - Asset or Currency? Revealing users' hidden intentions, *Twenty Second European Conference on Information Systems*.

Grant, J. M. (2014). Is bitcoin money?: Implications for bitcoin derivatives regulation and security interest treatment of bitcoins under article 9 of the uniform commercial code, *New York University (NYU), School of Law* .

Haber, S. and Stornetta, W. (1991). How to time-stamp a digital document, *Journal of Cryptology* **3**(2): 99–111.

Hafner, C. (2018). Testing for bubbles in cryptocurrencies with time-varying volatility, *SSNR Elec. Journal* .

Johansen, A., Ledoit, O. and Sornette, D. (2000). Crashes as critical point, *International Journal of Theoretical and Applied Finance* **3**(2): 219–255.

Kancs, D., Ciaian, P. and Miroslava, R. (2015). The digital agenda of virtual currencies. Can bitcoin become a global currency?, *Publications Office of the European Union, JRC Technical report* .

Kim, T. (2017). On the transaction cost of bitcoin, *Finance Research Letters* **23**: 300–305.

Kodres, L. and Pritsker, M. (2002). A rational expectations model of financial contagion, *The Journal of Finance* **57**(2): 769–799.

Kummerow, M. and Lun, J. C. (2005). Information and communication technology in the real estate industry: Productivity, industry structure and market efficiency, *Telecommunications Policy* **29**: 179–190.

Lakosmki-Laguerre, O. and Desmedt, L. (2015). L'alternative monétaire bitcoin : une perspective institutionnaliste, *Revue de la régulation* **18**(2).

Lamberti, F., Gatteschi, V., Demartini, C., Pranteda, C. and Santamaria, V. (2017). Blockchain or not blockchain, that is the question of the insurance and other sectors, *IT Professional* **PP**(99).

Larios-Hernandez, G. J. (2017). Blockchain entrepreneurship opportunity in the practices of the unbanked, *Business Horizons* **60**(6): 865–874.

Lee, S., Alford, M., Cresson, J. and Garner, L. (2017). The effects of information communication technology on stock market capitalization: A panel data analysis, *Business and Economic Research* **7**(1): 261–272.

Li, Z.-Z., Tao, R., wei su, C. and Lobont, O.-R. (2019). Does bitcoin bubble burst?, *Quality & Quantity* (1).

Libra, A. (2019). An introduction to Libra, White Paper.
**URL:** *https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US.pdf*

MacDonnell, A. (2014). Popping the bitcoin bubble: An application of log-periodic power law modeling to digital currency, *Working Paper* .

Massias, H., Avila, X. S. and Quisquater, J.-J. (1999). Design of a secure timestamping service with minimal trust requirement, *The 20th Symposium on Information Theory in the Benelux* .

Merediz-Sola, I. and Bariviera, A. (2019). A bibliometric analysis of bitcoin scientific production, *Research in International Business and Finance* **50**: 294–305.

Nadarajah, S. and Chu, J. (2017). On the inefficiency of bitcoin, *Economics Letter* **150**: 6–9.

Nem (2018). NEM technical reference version 1.2.1, *White Paper* .

Phillips, P. and Shi, S. (2018). Real time monitoring of asset markets: Bubbles and crises, *Cowles Foundation Discussion Paper* (2152).

Pietrewicz, L. (2018). Token-based blockchain financing and governance: A transaction cost approach, *Working Paper* .

Ren, L. (2014). Proof of stake velocity: Building the social currency of the digital age, *White Paper* .

Ross, R., Molina, M. and Beard, B. (2018). Waste not, want not: Your computer could help cure cancer, *White Paper 4.0* .

Schwartz, D., Youngs, N. and Britto, A. (2015). The Ripple protocol consensus algorithm, *White Paper* .

Shermin, V. (2017). Disrupting governance with blockchains and smart contracts, *Strategic Change* **26**(5): 499–509.

Su, C.-W., Li, Z.-Z., Tao, R. and Si, D.-K. (2018). Testing for multiple bubbles in bitcoin markets: A generalized sup ADF test, *Japan and the World Economy* **46**: 56–63.

Szabo, N. (1994). Smart contracts.
**URL:** `http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html`

Szabo, N. (1997). The idea of smart contracts, *White Paper* .
**URL:** `http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html`

Szabo, N. (2005). Bit gold.
**URL:** `https://unenumerated.blogspot.com/2005/12/bit-gold.html`

Tapscott, D. and Tapscott, A. (2017). How blockchain will change organizations, *MIT Sloan Management Review* **58**(2): 10–13.

Urquhart, A. (2017). Price clustering in bitcoin, *Economics Letter* **159**: 145–148.

Vanstone, S. (1992). Responses to NIST's proposal communications of the ACM, **35**: 50–52.

Vogiazas, S. and Alexiou, C. (2019). Bitcoin: The road to hell is paved with good promises, *Economic Notes, Review of Banking, Finance and Monetary Economics* **48**(1).

Wheatley, S., Sornette, D., Huber, T., Reppen, M. and Gantner, R. (2019). Are bitcoin bubbles predictable? Combining a generalized Metcalfe's Law and the log-periodic power law singularity model, *Royal Society Open Science* **6**.

Yermack, D. (2017). Corporate governance and blockchains, *Review of Finance* **21**(1): 1–31.

## Chapter 2

# The blockchain, an innovative community tool serving organizations?

The potential of the blockchain technology goes beyond the original purpose of its creation within an informal virtual community, the Bitcoin. Indeed, large businesses are investing in this technology in order to improve their services. The purpose of this article is to explain how the blockchain developed in informal communities has the potential to be adopted and incorporated by organizations. The blockchain's advantages such as transparency, low cost, decentralization, and speed transform exchange processes. Therefore, the theoretical framework related to this technology used in this article is the organization theory, notably the contractual approaches with transaction costs theory, agency theory and incomplete contracts theory, as well as the cognitive approach of the firm. A two-level dimension analysis is used to present the possible uses of blockchain through case studies and emphasizes the current transition from an informal community project towards a technology adapted by formal existing organizations.

## 2.1 Introduction

"In the next two years, every FAANG—you know, Facebook, Apple, Netflix, Amazon—are probably going to have their own coins or projects and they're probably watching Libra closely to see how it fares." said Cameron and Tyler Winklevoss at 92$^{nd}$ Street, New York on July 9$^{th}$, 2019 concerning the launch of Facebook's cryptocurrency, named "Libra" (Amsden et al., 2018), (Libra, 2019). Bitcoin, the first cryptocurrency, is created on November 1$^{st}$, 2008. Within 11 years, the innovation brought by cryptocurrencies has been appropriated by one of the most powerful private companies in the world, until challenging existing financial and banking institutions. Bitcoin is a community-based payment system which uses a coin (cryptocurrency) that works globally without any trusted third-party such as central banks, commercial banks, financial institutions or governments (Nakamoto, 2008). The third-party is replaced by the blockchain technology that ensures the proper functioning of the system.

A blockchain is defined as "a distributed and immutable (write-once and read-only) record of digital events that is shared peer to peer between different parties (networked database systems)" (Tapscott and Tapscott, 2016). Blockchain can be represented as a large public, anonymous and unfalsifiable accounting book which contains the entire historical background of transactions (from its creation to its current state). The major idea is the following: security and viability are ensured by all participants which form a consensus. No middlemen exist, the system is fully distributed, that is, the data are stored on the nodes of the users themselves (i.e. no server is needed). The decision-making is delegated to all participants in a decentralized and public ledger.

The first participants of the technology are an informal virtual community sharing the same values regarding the decentralization governance in a monetary exchange system. Thanks to its advantages in terms of speed, transparency, decentralization and reduced costs, both academics and professionals re-use this technology for some other applications, mostly in finance (Yermack, 2017), (Figuet, 2016), (Lee, 2016). More generally, blockchain has the potential to be adopted in many domains where a third-party is required, e.g. votes, administration, management and contracts (Collomb and Sok, 2016). This variety of applications requires blockchain adaptations regarding the required degree of openness.

For a long time, existing organizations have captured innovations which come from outside communities but the novelty, is the appropriation of an innovation that comes from an IT community inside the organization process. The blockchain is considered as a disruptive technology with the potential to change the existing way of exchange between individuals. Given the growing recognition of the importance of blockchain, we attempt to explain how the blockchain developed within informal communities has the potential to be adopted and incorporated into organizations. Blockchain advantages brought by an informal community of experts (users, miners, developers, hackers) outside formal organizations may create value for these organizations. First, we focus our analysis on the general potential of the blockchain technology (strengths and weaknesses) related to informational efficiency issues. Second, we highlight the implications of the adoption of the blockchain by existing formal organizations. Figure 2.1 - *Research questions of the first study* presents these sub-research questions, their methodologies and main findings.

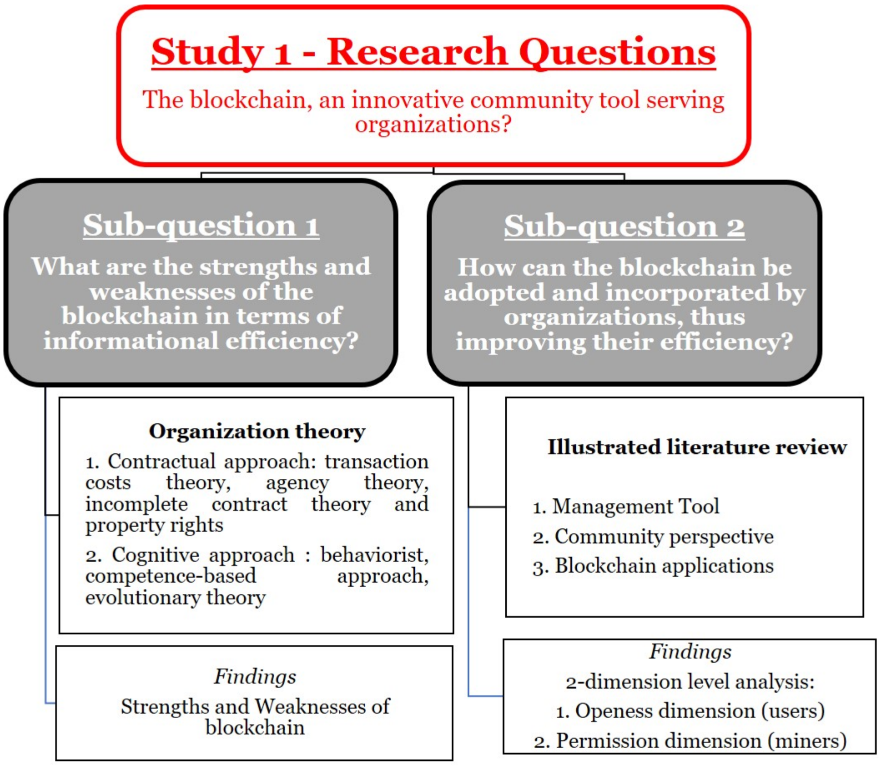


**Figure 2.1 Research questions of the first study**
This figure presents the sub-research questions of the first study.

In order to answer the first sub-question, we provide a theoretical framework for blockchain, based on the organization theory. The choice of this framework is motivated by the nature of blockchain technology which concerns the information (coins in the case of cryptocurrencies) that individuals exchange and share. This access to information raises the question of informational efficiency and the cost of acquiring information. A better access to accurate information improves the way of exchanging between economic agents. Information and communications technologies (ICT) seem to improve efficiency by their democratization aspect and the reduction of transaction costs (D'avolio et al., 2002). Individuals look for ways to exchange between each other by preventing themselves from unexpected events and opportunistic behaviors of their partners. These exchange relationships are studied in a contractual approach in the theory of organization which consider the transaction costs (Coase, 1937), (Williamson, 1975), (Williamson, 1979), (Williamson, 1981), (Williamson, 1985), agency costs (Berle and Means, 1932), (Alchian and Demsetz, 1972), (Jensen and Meckling, 1976), as well as the property right and incomplete contracts issues (Grossman and Hart, 1986), (Hart and Moore, 1988), (Hart and Moore, 1990). The contractual approach faces some limits (Foss and Klein, 2005) which lead other scholars to focus on the knowledge, capabilities and individual preferences of stakeholders within organizations (Penrose, 1959), (Nelson and Winter, 1982), (Chandler, 1992).

The second sub-question considers blockchain adoptions inside formal organizations through an illustrated literature review and a two-dimension analysis concerning the characteristics of participants in a blockchain community. The stakeholders' strong involvement is indeed one of the main particularities of blockchain. Compared to existing systems, there is no third-party to manage the system. Therefore, participants – users and miners - can play different roles in the system. Users[1] have the right to participate, read and download the ledger (e.g., the blockchain). They have a scrutiny right to the work of miners and they are fully part of the system. Miners[2] can write in the ledger in order to validate the transactions. In the Bitcoin blockchain, every user can be easily a miner and the ledger is totally open to users and to miners. Their respective accesses can

[1]Economic agents that exchange to each other, see list of terms and abbreviations.

[2]Participants who write in the ledger and validate transactions through the consensus mechanism, see list of terms and abbreviations.

be restricted for business applications (e.g. due to the management of confidential data). The two-dimension analysis is based on the openness dimension for the users and on the permission dimension for the miners.

Our article is structured as follows. The first part presents the concepts behind blockchain from a community perspective. The second part describes the general potential of the blockchain technology (strengths and weaknesses) in a theoretical framework based on the organization theory. In the third part, we analyze the appropriation process of the blockchain from an informal community towards the existing formal organizations. The fourth part concludes and discusses the possible theoretical, managerial and political implications.

## 2.2 Blockchain as a community tool

Blockchain is a secured storage and transmission technology (generally transparent) that works without the requirement of a third-party. Initially studied by computing and engineering sciences (see Chapter 1), blockchain nevertheless remains a technology dedicated to management issues. This technology aims to improve exchange between individuals and was born in a spirit of community. In this part we will present the blockchain technology from a community perspective, first by presenting the origin of the blockchain (the Bitcoin case), and second by showing and analyzing its different characteristics.

### 2.2.1 The starting point: Bitcoin's blockchain

In 2008, the traditional financial and monetary system faces troubles due to the Subprime crisis. Trust in these institutions and more generally on the monetary-based system is called into question. Most of the critics are related to the governments' decisions (by definition a fiat currency is promoted and linked to a government), the complexity and the opacity of the financial system that develops some services and products allowing to prone some manipulation behaviors. More generally, the centralization of the power in some hands increasing a social inertial effect[3] (Carroll and Bellotti, 2015).

The same year, an anonymous individual/entity called Satoshi Nakamoto (the lead user of the Bitcoin community) has the idea to create an international

[3]"Rich" people are more motivated to become richer because they have more access to regenerate money whereas "poor" people bear more risk to be marginalized.

secured payment system which could work without a third-party such as central or commercial banks, namely: Bitcoin. The main idea is to create an informal eco-system of exchange that works without intermediaries and in which the transactions are public and recorded in a ledger (blockchain). This ledger records all the history of transactions made in the network between participants. This entire ledger is distributed to all participants and each transaction is broadcasted to others, (Tschorsch and Scheuermann, 2016).

This ledger takes the form of a public and transparent database represented by blocks which record several transactions. Instead of central authorities that verify and validate the transactions, the Bitcoin community requires all participants of the community to agree on the validation of the transactions, thus reaching a consensus. As shown in Figure 2.2 - *The stakeholders around the blockchain*, there are several participants in the network. The users exchange information (a coin in the case of Bitcoin) to each other, the miners validate the transactions, the developers maintain the blockchain protocol, and the hackers try to find a breach within the system. Our analysis will mainly focus on the user and miner participants because they are directly linked to exchanges (developers and hackers are in charge of building or destroying the computer code, they do not participate in the exchanges via a blockchain).

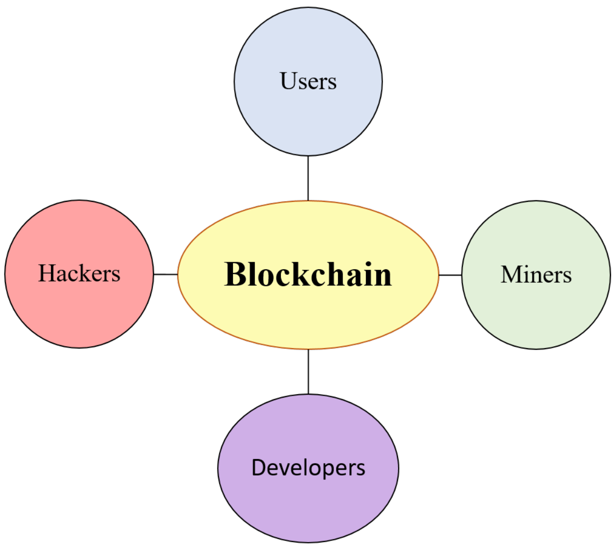


**Figure 2.2 The stakeholders around the blockchain**
This figure presents the stakeholders that gravitate around the blockchain technology. Own representation.

The first group of participants (users) performs transactions in the network, for example let's say Alice buys a computer from Bob. In this case, the amount of coins (Bitcoins) sent to Bob is not directly validated, thus the transaction is waiting for the consensus agreement of the community. The second group (miners) collects a set of pending transactions and create a new block of transactions by solving an algorithm based on efforts and that could be confirmed by the community of the network[4]. The system has to respect some properties, "secured ownership", "unfalsifiability" and "no double spending" to control for the opportunist behavior of a potential opponent, let's say Oscar.

In the first step, it is necessary to ensure the authentication of participants during a transaction, otherwise, Oscar would be able to send a transaction on the network to transfer money from Alice to his account. Nakamoto set up digital signatures based on asymmetric cryptography using public and private keys in a distributed network to comply with the authentication condition (Chaum, 1983). In the second step, it is necessary to ensure the monetary creation (mining process[5]) and to control for coins transfer between their successive owners. Otherwise, Oscar could create new coins by crediting his own account. Nakamoto (2008) creates a way to follow each coin using a Proof of Ownership[6]. Thanks to this chain, everyone can check the legality of a coin and track the owners. The monetary creation is based on a consensus: each new block must be agreed by all the participants and distributed in a fair way. As stated before, Bitcoin miners choose pending transactions and put them on their block locally. Each miner is in competition with other miners. All of them try to solve a mathematical problem in order to win Bitcoins. To respect fairness between participants, winning Bitcoins depends on the computation power: the higher the miners' computational power is, the more the miners have a chance to win (Proof-of-Work). Finally, the winner adds his block to the ledger and validates the transactions in his blocks. The solution and the new added block are easily verifiable by all the users in the network, (Tschorsch and Scheuermann, 2016), (Biais et al., 2017). The miner-winner obtains a reward for his effort (computational power and energy consumption) which is a number of Bitcoins (which decreases with time, as of January 2018 it is set at 12.5 Bitcoins) as an incentive to participate.

[4] See mining, Proof-of-Work and Proof-of-Work in the list of terms and abbreviation.

[5] See the list of terms and abbreviations.

[6] Proof of Ownership is a method within Blockchain to track the owners of a certain information over the time, see the list of terms and abbreviations.

Miners receive as well transactions fees chosen arbitrarily by the user when he performs a transaction. The Proof-of-Work is also a solution to limit the double-spending problem[7]. The third step consists to manage this problem otherwise Oscar could make one of these two transactions on his own account. The suggested solution is that the entire network checks for the transactions based on the majority (of the network) rule. The double-spending might be realized by a Fork[8]. To resolve the Fork issue, the rule is the following: the longest chain wins and the second one is canceled (Tschorsch and Scheuermann, 2016).

Finally, Bitcoin is an innovation based on the blockchain which allows to exchange money in a distributed manner, without any control by a special entity but under everyone's supervision. The added value of the system is that everyone can be a stakeholder (Shermin, 2017).

The first participants in the Bitcoin system can be considered as a particular community coming from the IT community including voluntary participants in a communication system aimed to share and exchange (coins in the case of Bitcoin). They shares values, interests, and practices: (1) Being autonomous and free in a monetary exchange process; (2) Redistributing the power of the government to every participant; (3) Reducing transactions costs resulting from intermediaries such as banks; through an innovative technology, the blockchain. This technology ensures the system's security using cryptography principles and provides collective consensus and effort sharing. We refer to this by "wisdom of the crowd", a concept which means the solution of some problems is more efficient using the crowd, i.e. the Bitcoin community, than by one individual or an entity such as the government, (Joffre and Trabelsi, 2018)). This community is led firstly by Satoshi Nakamoto as well as all other creators of new cryptocurrencies and opinion leaders who promote and spark discussions on forums.

Cryptocurrencies allow to resolve some problems caused by the current monetary system so they could play a role of integration of marginalized people (the only condition to be part of the Bitcoin exchange system is to have access to the Internet) (Kshetri, 2017), (Larios-Hernandez, 2017). The confidence in the system is shifted from the government to the technology (blockchain). The

[7]The double-spending problem arises when two different transactions are made with the same coin, see the list of terms and abbreviations.

[8]The splitting of a ledger in two ledgers. See the list of terms and abbreviations.

system is more transparent by making all the information accessible and public, and finally, the power is redistributed to all participants based on a decentralized peer-to-peer protocol secured by cryptographic principles (Angel and McCabe, 2015), (Carroll and Bellotti, 2015), (Dierksmeier and Seele, 2018).

Therefore, the blockchain technology come from a community grouping several participants in an informal manner. Its use is progressively spread widely through media coverage.

### 2.2.2 Key dimensions

The main innovation of Bitcoin and cryptocurrencies is the underlying technology, the blockchain, especially because it solves the double-spending problem and allows to store and make exchanges of information in a collaborative manner inside a community instead of being under the control of a third-party. Therefore, the information exchanges in the cryptocurrency system could be replaced by any other information that needs to be stored, tracked or exchanged. Based on this postulate, Ethereum, the second main blockchain suggests to offer another service in addition to the cryptocurrency system, which is the possibility to use the blockchain technology to execute special contracts called "Smart Contracts" (Szabo, 1997a), (Szabo, 1997b) (Szabo, 1998), (Buterin, 2015b), (Wright and DeFilippi, 2015), (Cong and He, 2017).

A smart contract is a software-based contract that runs automatically, i.e. without direct human intervention but based on conditions previously defined by humans[9]. It is a simple form of decentralization automation (Buterin, 2014) which allows to set up more efficiently, automatically and clearly the relationship between a fixed number of parties (Buterin, 2014), (Wright and DeFilippi, 2015).

The nature of the exchanged information through Smart Contracts sometimes requires more confidentiality and more control, especially when it deals with personal or sensitive data from businesses. Therefore, the most recent blockchains are taking into consideration these issues and adapt their restrictions to users and miners in different ways. In this part, we present the different

[9]Let us consider the following example: a donation. Alice decides to give her money to Bob when she becomes 70 years old. The condition is "Alice is 70 years old" previously defined by a human (Alice). The result is "Bob receives the savings from Alice". This agreement is put on a code, the smart contract linked to a blockchain. When Alice is 70 years old, the smart contract is automatically executed and Bob obtains the money.

dimensions that exist based on the power granted to the participants in the community, the users and the validators (the miners), and other features in order to characterize the blockchain that will be used in the results of the fourth part, 2.4.

#### 2.2.2.1 Permission and openness dimensions

The blockchain is created through a community, especially users and miners, that is initially granted total access rights to the system (in the Bitcoin one) beyond the control of formal existing firm communities. In order to be accepted inside the formal existing organizations community, the technology has to be flexible regarding the access rights granted to participants (e.g. users and miners). Therefore, we suggest to analyze the blockchain possibilities through a 2-level dimension.

The first one is the dimension related to the permission conferred to the miners, whilst the second concerns the openness of the ledger for its users. By definition, we assert that the miners have the possibility to write, commit and therefore validate the transactions of the system whereas the users can read or join the network by sending transactions or just reading the information inside the ledger, (Wust and Gervais, 2017).

The *Permission* dimension indicates there is a restriction on who can write and make changes to the ledger. There are two possibilities: a permissionless blockchain in which there is no restriction on validators (miners). Thus, anyone can participate to the consensus mechanism and validate the transactions and their identity is not necessarily known. By contrast, a permissioned blockchain implies that validators are known and need a permission to write in the ledger.

The *Openness* dimension indicates there is a restriction related to the access to the data in the ledger by users. In some firm projects, it is preferable to restrict the access to data reading for users as well as to participation to transactions in the system. After the validation of transactions by miners, the information is recorded in the ledger. In the public blockchain case, the information is public, so that anyone can have access to the data (download and read) and send transactions in the network. In the private blockchain case, the information is private so that access to the data is limited to predefined users (that can also send transactions according to their permission level).

**Table 2.1 Features**

This Table presents the different features which characterize the blockchain related to participants, management and governance and technical aspects.

| | Features | Explanation |
|---|---|---|
| *Participants* | | |
| (1) | users | Send, read and analyze the data. |
| (2) | miners | Validate the transactions. |
| *Management and Governance* | | |
| (3) | Anonymity | Participants' privacy. |
| (4) | Trust | Confidence in the validation process (miners). |
| (5) | Consensus | Consensus mechanisms (Proof-Of-Work (PoW), Proof-Of-Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), Federated Byzantine Agreement (FBA)). |
| (6) | Governance | Decision-making (decentralized, centralized). |
| (7) | Reward | Incentive based-tokens in the consensus mechanism. |
| *Technical* | | |
| (8) | Throughput | Transactions by period of time to be validated by the consensus (e.g., performance). |
| (9) | Scalability | Reach a higher Throughput when the number of users is growing (node-Scalability, performance-Scalability). |
| (10) | Immutability | Possibility to not change the history of the blockchain. |
| (11) | Finality | Number of validated blocks a user has to wait to be sure the block, in which his transaction is located, is validated. |

#### 2.2.2.2 Other features

According to the 2-level dimensions, there are several features which characterize the blockchain that might be different, Table 2.1 - *Features*.

In this part, we present the main required (individual, management and governance, and technical) variables associated with the blockchain concept. Some features are related to the participants. (1) Users are participants in the system who send transactions or read and analyze the data inside the ledger. The actions of users are both to read and send transactions. (2) Miners are participants in the system who validate transactions through the consensus mechanism. The actions of miners are to write, commit and validate.

Other features concern management and governance. (3) Anonymity relates to the privacy of participants (users or miners). (4) Trust relates to confidence in miners' behavior during the consensus mechanism. The more the miners are known and pre-selected, the higher the trust is. As mentioned before, the validation and verification of transactions need to be reached by a consensus (5) in the community. The consensus management is a concept described by (Wilkof, 1989) in which responsibilities are distributed, decisions are made collectively, without objections and interferences. In the blockchain system, there are several possibilities to implement a consensus mechanism. The two famous ways are the Proof-of-Work (PoW)[10], and the Proof-of-Stake (PoS) which is not based on the computational power but on the ownership of tokens into the technology (e.g. the number of coin held) in a deterministic manner. The more one invests in the blockchain, the more he has a chance of winning and getting the reward (Yermack, 2017), (Collomb and Sok, 2016), (Cong and He, 2017), (Lamberti et al., 2017). In the Practical Byzantine Fault Tolerance (PBFT), a block will be accepted if more than two thirds of all participants chose this block (Castro and Liskov, 1999). The Federated Byzantine Agreement (FBA) establishes the veracity through sorted and voted transactions. Governance (6) issues arise because the decision-making is either distributed or concentrated in the community. Notably, when the technology is appropriated inside a firm with an existing governance, the way an organization manages the technology and its characteristics within its own strategy is called "IT governance" (Wilkin and Chenhall,

[10]Previously defined, in which the effort is based on the computational power. See list of terms and abbreviations.

2010). Many blockchains require a reward (7) on the form of a token in order to provide stakeholders an incentive to be part of the consensus process.

The last group of features deals with technical aspects. (8) relates to the transactions by period of time to be validated by the consensus mechanism (performance). (9) Scalability is the fact to reach a higher Throughput (performance) when the number of users is growing. Vukolić (2015) presents two factors, the first one deals with the number of users that the network can support without losing performance (node-Scalability), whilst the second one is related to the transactions per second impacted by the latency between transactions and block size (performance Scalability). (10) Immutability is when no one can modify or alternate the history of transactions within a blockchain. (11) Finality is the number of validated blocks a user has to wait to be sure his transactions will be validated and added in a blockchain.

### 2.2.3 Features of blockchain communities

Our objective is to show how the blockchain is a tool for communities and how it enhances innovation for firms. In management sciences, the literature concerning the blockchain and the community concept is quite scant. If existing papers sometimes refer to the idea of building a community attracting early adopters or developers (Chen, 2018), most of them focus on the users of cryptocurrencies (especially the Bitcoin ones). As far as we know, the first article that analyzes Bitcoin users is Ron and Shamir (2018). These authors show that most of the Bitcoin wallets[11] remain inactive for a "huge number of tiny transactions which move only a small fraction of a single Bitcoin, but there are also hundreds of transactions which move more than 50,000 Bitcoins". Subsequently, following an online survey[12], other researchers find that age, time of initial use, geographic location, mining status, involvement in online discussions and political orientation are factors influencing Bitcoin wealth accumulation, optimism in the future, and user's attraction (Bohr and Bashir, 2014). Four potential groups of users in the community are also highlighted: computer programming enthusiasts, speculative investors (for profit), libertarians (political) and "criminals" (anonymity

[11] Secure storage solution (physical or digital) for cryptocurrencies. See the list of terms and abbreviations.

[12] https://spacedruiddotcom.wordpress.com/2013/03/04/the-demographics-of-Bitcoin-part-1-updated/

- illegal products) (Munksgaard and Demant, 2016). In the USA, between 2011 and 2013, only criminals and computer programmers are interested in using Bitcoin (Yelowitz and Wilson, 2015) whereas none of them are interested in using Bitcoin in Canada between 2015 and 2017 (Garg, 2019). More recently, Kang et al. (2019) find that most of the Bitcoin community users have an interest in its market price but the opinion leader[13] groups go further and are sensitive to other types of information such as technical information. Opinion leaders represent better the community than the majority of users even if they are more than the opinion leaders.

To conclude this part, blockchain comes from an informal and special community, different from the formal existing firm communities. In the blockchain community, all stakeholders are involved in the process with different level restrictions of access (for users or miners). The blockchain technology is therefore basically an innovative technology which has also an important impact for the firms' future in particular in their ways of storing and exchanging data as well as enhancing participation of the different stakeholders. The blockchain technology changes the organization of exchanges because it provides new access to information for individuals. The informational efficiency challenge of the blockchain could be understood through the framework of the organization theory in the next part.

## 2.3 The potential impact of the blockchain on informational efficiency within organizations: A theoretical framework

Participants inside a community, and more precisely in the blockchain community, have the objective to exchange information to each other (monetary exchange in the case of Bitcoin, but the exchanged coin can be replaced by any other kind of information). The blockchain is indeed a technology that has an impact on information transactions and on the way to exchange. The access of information related to transactions is different from existing formal organizations and has the potential to improve the informational efficiency within organizations. Therefore, this part presents the theoretical framework for modeling

[13] An opinion leader is defined as "users who actively participate in the community and have high reputation, play important role in leading consensus in the social community".

the blockchain, by considering the organization theory and the role played by communities and organizations.

### 2.3.1 Issues faced by organizations

#### 2.3.1.1 The firm as a node of contracts

According to the neo-classical approach, economic agents are rational which means they possess a perfect information with some deterministic uncertainty. Their capacity to compute is total and their objective is to take decisions in order to optimize the expected utility of their wealth. In this theory, the firm is only a production function in which the price is fixed by a market driven only by the law of supply and demand. The firm is a black box that use inputs (resources, labor and raw materials) to provides outputs (sales). It is considered as an economic agent itself respecting the rationality assumption and, therefore, whose objective is to maximize its profit. This theory faces some limits especially the hypothesis related to the rational behavior of the economic agents. The interest in explaining the inner workings of the firm comes with (Coase, 1937). A part of the existing literature regarding organizations presents the firm in terms of "contracts" and attempts to find the most efficient organizational form. Because of their importance in the organization theory literature, we emphasize three main schools of thinking: the transaction costs theory of Williamson, the agency theory and the incomplete contracts and property rights theory that we will present briefly in this part.

- The transaction costs theory

  Coase (1937) questions the neo-classical point of view regarding the market and first determined the conditions of the existence of the firm. He highlights the presence of transaction costs on the market to justify the existence of the firm. These costs exist because agents spend time and money to make exchanges. They take two forms: information acquisition costs, bargaining and enforcement costs. The first type of costs appears before entering the market when an agent spends time and money to obtain information related to the exchange conditions (e.g. the seller or the product). The second cost appears after obtaining the information: sometimes, experts are necessary to understand better the information and to better negotiate the transaction conditions. Therefore, an agent has the choice between a spontaneous market system based on the "cost of using the price mechanism" or a deliberate organization (firm) system based on internal coordination mechanisms.

Based on Coase works, Williamson supports and develops the transaction costs theory and provides a new definition of transaction costs. Williamson (1985) suggests two kinds of transaction costs: *ex-ante* and *ex-post*. *Ex-ante* costs occur before the agreement, and as stated by Coase, concern the search for information and the negotiation phase during which it is necessary to find a partner, write a contract with specialists and set up some guarantees. This implies either to set up "complete contracts" in which all possibilities are taken into consideration (conflicts, solutions, guarantees) or "incomplete contracts" that are dynamic (solutions may be found at the moment when the problem occurs and adapted to this problem). *Ex-post* costs occur after the agreement at the moment when the contract is not adapted to the situation, notably due to unexpected events or conflicts.

First, Williamson shows that, in reality, agents cannot have access to the perfect information and their capacity to compute is limited due to cognitive and technical limitations. This is referred to as "bounded rationality" (Simon, 1988). Second, the opportunistic behavior occurs generally after the contract signature when a partner no longer sees his interest in this contract and does not make the efforts expected by the partners. In other words, because the agent has not access to the all the relevant information and has cognitive biases, he cannot handle all possible situations when he signs a contract. Therefore, all contracts are incomplete and the opportunistic behavior risk is higher especially when unexpected events happen.

Contrary to the neo-classical view in which products are homogeneous, the "asset specificity" concept classifies different products according to their level of reuse. The more (less) specific the asset is, the more (less) difficult will be to use it again. According to its specificities, an asset can be classified into 6 classes: site (localization), physical asset (specialized machine), human asset (knowledge), dedicated asset (one-shot investment), reputation (brand) and time (coordination) (Lavastre, 2001), (Ruzzier, 2009). The more the asset is specific, the stronger the dependence is between co-contractors and the choice of exchange through the firm (the hold-up theory) (Coriat and Weinstein, 2010). An additional criterion presented by Williamson is "uncertainty" which is the degree to which the future state of the world cannot be anticipated. Predicting the future and its entire possibilities is a difficult task because time is included in the transaction and agents are boundedly rational. Uncertainty can be internal, such as the strategic behavior of firms or external, such as an objective state of the world (e.g. technology, rules). Finally, the "frequency" is the number of times one exchanges with the same partner. The more a transaction is frequent, the less there is a risk of opportunism and bounded rationality. Bounded rationality may be solved using contracts, experts, and specialists to gain advice, while opportunism can be reduced with contractual clauses and lawsuits, and specificity can be overcome with provisions and cost sharing.

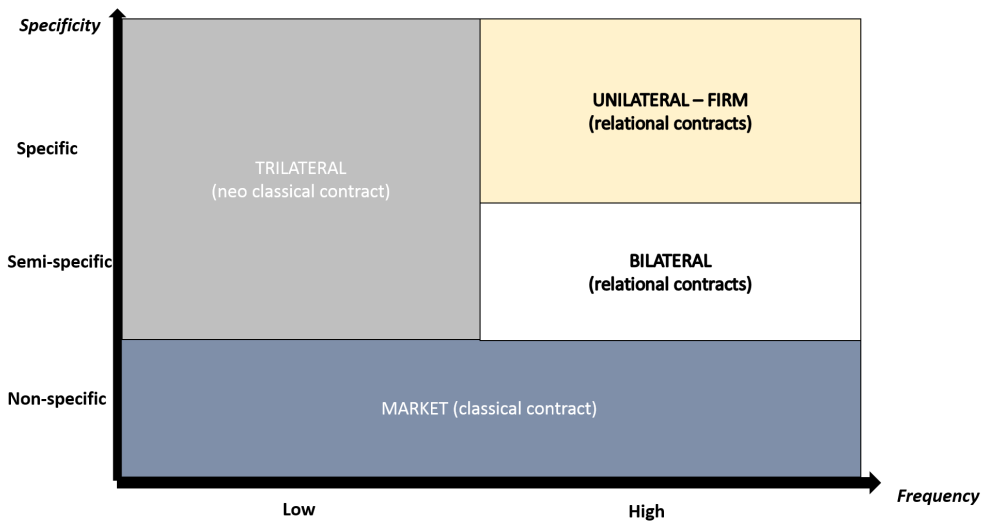


**Figure 2.3 Forms of governance according to (Williamson, 1979)**
This figure is adapted from (Williamson, 1979) and presents the different possible forms of governance according to the frequency and the specificity.

Figure 2.3 - *Forms of governance according to (Williamson, 1979)* shows that the first possible choice for a transaction is the market. Exchanges on the market happen when the asset's specificity is low (there is exists a possibility to reuse the asset) and regardless of the frequency. On the market, there is no close relation between producers and customers which implies that the competition can protect against opportunism, for example, the purchase of standard equipment and material (Williamson, 1979).

The second choice is trilateral: the specificity is higher but the frequency is lower, which implies that a third-party is needed to solve conflicts based on a long run contract with adaptation rules. If the asset is moderately specific, the contract should be classical (civil or legal such as purchasing customized equipment). If the asset is highly specific, the contract should be more sophisticated (e.g. design a plan with an architect) (Williamson, 1979).

In the third choice, the asset specificity is moderate and the frequency criteria is high, which leads to a bilateral framework, for example sub-contracting. The contract is a kind of quasi-integration (e.g., purchasing customized material) (Williamson, 1979).

Finally, a fourth choice is a unified system, the "firm" in which both specificity and frequency are high, especially when the uncertainty is high. This is the case of vertical integration in which coordination is internalized. The firm is a kind of contract in which employees accept to obey orders from managers because they receive an amount of money in exchange (wages).

- The agency theory

The agency theory is another branch of the contract theory that explains the concept of the firm through the conflict of interests between those who own the firm and those who manage it (Berle and Means, 1932). Following the neo-classical hypothesis that economic agents are rational and their objective is to maximize their expected utility, this stream of the literature focuses on the key role of information. Based on the property rights, and notably the most efficient organization forms (Alchian and Demsetz, 1972), Jensen and Meckling (1976) define the firm as a "nexus of contracts" in which every relationship inside the firm can be formalized by an agency relationship, due to information asymmetries, and notably between investors and management where the former (principal) give their power to the latter (agent) through a contract. According to these authors, the most efficient form of organization from the shareholders' view is the firm. The objective of the firm is to optimize every agency relationship (and therefore every contract) by minimizing agency costs. These costs encompass monitoring and incentive expenses to align the principal's interest to the agent's one, expenses supported by the agent to ensure the commitment to the principal and the residual loss incurred by the principal due to monitoring and bonding. This theory has several implications: (1) The firm is defined only as a legal definition according to a contract-based view. In the neo-classical theory, only individuals constitute and define the firm whilst the agency theory defines the firm through contracts between individuals; (2) The firm's assets are owned by individuals (capital ownership), (3) There is no ownership of the firm (Fama, 1980)[14]; (4) There is no conceptual distinction between a firm and a market as the firm is a private market; (5) There is no authority relationship inside the firm (only opportunities of contracts). Therefore, there is no distinction between contracts (for example the employment contract is similar to the commercial contract).

- The Incomplete Contracts Theory

  Grossman, Hart and Moore formalize the transaction costs theory (Grossman and Hart, 1986), (Hart and Moore, 1990) in a dual way: while their view shares similarities with Williamson and Coase, they operate a distinction between the firm and the market. They emphasize the authority power of the firm on its employees and they consider the incompleteness of contracts. Recalling that a contract is incomplete when all the future situations are not taken into consideration, renegotiations are unavoidable when an unexpected event occurs. If Williamson finds the source of the incompleteness of contracts in the agents' bounded rationality, the authors

[14]"Ownership of capital should not be confused with ownership of the firm. Each factor in a firm is owned by somebody. The firm is just the set of contracts encompassing the way inputs are joined to create outputs and the way gains from outputs are shared among inputs. In this "nexus of contracts" perspective, ownership of the firm is an irrelevant concept" (Fama, 1980).

of the incomplete contract theory believe that individuals are rational and they find two causes of contract incompleteness. The first one is the transaction costs inside the clauses added in the contracts (Grossman and Hart, 1986), and the second is the ability for a third-party to verify (complete contract) the information related to contractors (Hart and Moore, 1988). A third-party requires enough information about the co-contractors to verify the clauses inside the contract. Therefore, the proposed solution to check and adapt the contract in case of uncertainty and unexpected events lies on property rights (for Williamson the solution consisted in the authority power of the owner) in order to motivate the individuals to make efforts without contracts. The firm is defined as a set of (non-human) assets owned by individuals inside the firm under property rights and unified control (Blair and Stout, 1999).

#### 2.3.1.2 The alternative and cognitive approach of the firm

According to the aforementioned theories, there are lot of differences that can be summarized in Table 2.2 - *Differences between contractual and cognitive approaches of the firm*. Notably, the hypothesis of Williamson about the bounded rationality and the implied hypothesis concerning the opportunistic behavior are questioned. The opportunist behavior is difficult to observe and the main answer is most of the time the use of a reward as an incentive whilst it is not all the time required for every individual (Foss and Klein, 2005).

In general, the three theories based on the contractual approach do not take into consideration the production aspect of the firm whereas this is an important purpose for an organization. The firm is considered as a node of contracts and not as a special entity that owns the assets. Contracts are directly written with the stakeholders (Chandler, 1992). The firm can be transferable and exchanged (Coriat and Weinstein, 2010). Alternative research in the field shows that capabilities could be an explanation on the nature of the firm. The firm's resources are the assets used to produce activities and organizations processes, competencies are the abilities of the firm to compete with other organizations. When these competencies and resources are combined to obtain a sustained competitive advantage, they are referred as capabilities (knowledge base of the firm) (Foss, 1996). The sustainability of the firm and the in/outsourcing decisions depend

**Table 2.2 Differences between contractual and cognitive approaches of the firm**

This Table presents the differences between the three conceptual approach and the cognitive approach of the Organization theory. The table is translated and adapted from the article of (Chaudey 2011) available on the website SES ENS LYON

| **Theory** | **Issue theory** | **Rationality** | **Information** | **Firm's Nature** |
|---|---|---|---|---|
| **Transaction costs Theory** | Decision making process *a posteriori* and commitment execution mechanism. Frontiers firm issues. | Limited | Incomplete and asymmetric | Governance structure |
| **Agency Theory** | Incentive reward pattern. | Perfect | Complete and asymmetric | Node of incentive-based contracts |
| **Incomplete Contracts Theory** | Property rights allocation and decision-making to limit the incompleteness of the contracts. | Limited | Incomplete and symmetric | Non-human assets collection |
| **Cognitive Theory** | Capability-based decision making. | Satisfaction instead of maximisation rationality | Limited and heterogeneous | Set of routines and node of competences |

on the capabilities of the firm (Jain and Thiertart, 2013). These authors show that capabilities serve as a shift parameter for the firm to decide between in-sourcing or out-sourcing firm activities (Foss and Klein, 2005). Resources are also an important aspect studied within the organization theory (Penrose, 1959), especially how to control and manage these knowledge and capabilities while taking into account conflicts of interest and cooperation relationships (Foss and Klein, 2005). The alternative approach is based on cognitive aspects and more precisely focuses on the capabilities and learning processes inside firms to explain the heterogeneity of their performance and sustainability. There are three main streams in this approach: (1) The behaviorist approach (March and Simon, 1993), (Cyert and March, 1963); (2) The competence-based approach Penrose (1959); (3) The evolutionary theory (Nelson and Winter, 1982).

First, behaviorists study a given firm by considering its internal structure in which the "decision making process" of individuals depends on each other. This approach differs from the contractual approach where only external forces put some pressure on the firm. They also seek to optimize utility as a "satisfaction" rather than a pure "maximization". The concept of knowledge is at the core of the theory, therefore, the firm is defined as a coordinated and adaptive system led by individuals who have different knowledge, information and preferences and for whom information processing is limited (March and Simon, 1993), (Cyert and Kamien, 1998). The firm is a complex organization in which individuals' behaviors who have their own objectives, find together the objective of the firm, notably by a collective learning process. These authors highlight the process of "routine" as a standard inside the firm, able to manage conflict interests and their relative costs for managers.

Second, Penrose (1959) studies the growth of the firm notably by focusing on the entrepreneur's role, a concept rarely used in the organization theory (Foss and Klein, 2005). She defines the firm as an administrative organization and a set of information (resources) that could be tangible or intangible. For example, the competences, mainly, the organizational resources gathered to improve the performance of the firm, are intangible resources. The allocation of resources as well as the creation of new resources are an arbitrary choice of managers. The firm's objective is to use these resources in order to produce goods and services and make profit. The means of production evolve over time and create new opportunities for the firm.

Finally, Prahalad and Hamel (1990) define a firm based on its "core capabilities" and not on a set of resources. What is important is the use of special resources to create a competitive advantage not reproducible by other firms. In this way, the Evolutionary Theory, based on biology (heredity)[15], explains the

[15]First, economic agents inherit genes which are routines. These routines shape their behavior. Second, economic agents are not static, they evolve and look for new possibilities (innovations) in the mutation step. Third, a selection happens and maintain the best innovations adapted at the existing environment (the firm).

firm explained as a set of routines (problem-solving) (Nelson and Winter, 1982) and learning processes[16] between agents in order to develop competences.

In these alternative cognitive approaches, competences and learning processes are the key for in/outsourcing the activities and explain the heterogeneity of the firms; even in the same sector. These theories support the heterogeneity of the different types of existing firms that differ from each other by their competences. There is no more a best efficient way of organization like in the contractual approach. Compared to the contractual approach, competences become the node of the firm instead of contracts and therefore, the role of stakeholders is emphasized (compared to the formal shareholder approach).

### 2.3.2 Solutions brought by blockchain

Even if the first purpose of the blockchain is the union of participants sharing the same ideology to create their own space of exchange without the intervention of the traditional monetary and financial systems, the blockchain technology is more than a simple "disruptive technology"[17] (Iansiti and Lakhani, 2017), (Chris Berg and Potts, 2017). We argue that blockchain may have an impact on the firm by reducing some costs, and changing its governance. If the blockchain technology allows for some improvements within the organization theory in the large sense (transaction costs theory, agency costs and the incompleteness of contracts) by providing answers to some of its limitations, its implementation can generate in turn other new risks.

#### 2.3.2.1 Blockchain as a practical answer to criticisms addressed to the organization theory

- The transaction costs theory

  As mentioned previously, bounded rationality and opportunism exist because of a time effect. With blockchain, exchanges are almost instantaneous. The new applications of the blockchain are constantly improving the speed of transactions. In addition, advantages of blockchain regarding

[16]The learning process is cumulative (new competences are built on previous competences), collective learning process, incorporated in routines specific to individuals (not transferable), and dynamic (new routines imply new learning process).

[17]A disruptive technology is defined as "technology that changes the bases of a competition by changing the performance metrics along which firms compete" (Hienerth and Lettl, 2011).

transparency, decentralization, and access rights imply that individuals can have access to more information. They can therefore better interpret and be "more rational". Smart Contracts exist in order to put on "paper" (in reality, on code) all the possible situations and conditions of a contract realization. Blockchain thus reduces the opportunistic behavior (MacDonald et al., 2016), (Larios-Hernandez, 2017) and its relative risk (Pietrewicz, 2018).

Williamson and Nakamoto are both trustless regarding human behavior. Consequently, they find two alternatives in order to avoid any opportunistic behavior: a contract for Williamson and a technology for Nakamoto. Let us recall that for Williamson, an opportunistic behavior can include "lie, stealing and cheating". However, this kind of behavior is avoided by blockchain technology because of the whole cryptographic process. On the one hand, a blockchain decreases the *ex-ante* opportunism risk because it is impossible to change or censor the information since it is recorded in the ledger. On the other hand, the time when the information is added in the blockchain remains sensitive, especially for objects traceability[18]. The integrity of the information inside the blockchain is immutable but the integrity of the information before it is recorded in the ledger requires some human intervention or legal regulations.

In the *ex-post* case, the blockchain can also change the agents' behavior. Smart Contracts are supposed to take into consideration all the possibilities and conditions of a contract execution. In this sense, a partner fulfills automatically his commitment because the contract is automatically executed. However, if the contract is incomplete or if a participant simulates that there are mistakes, solutions still do not appear obvious.

Regarding the criteria based on transactions, blockchain has an impact on "uncertainty", "specificity" and "frequency". Uncertainty may decrease thanks to Smart Contracts which take into consideration most possibilities and because bounded rationality and opportunism are smaller than before. Blockchains are also based on cryptographic and technical ways which can have their own limits. Uncertainty is enhanced by the use

[18]For example, a guitar has an engraved identification number. Since this number is written in the blockchain, it can no longer be changed or modified even if number on the guitar itself may be altered by an opportunist individual.

of new technologies (attacks or bugs) as well as a potential crisis can increase the uncertainty. Therefore, while some types of uncertainties mentioned before will decrease, new sources of uncertainty will appear. The specificity of an asset is also questioned regarding potential uses of blockchains. According to Williamson (1979), the specificity of an asset implies different contracts but the flexibility of a blockchain allows to be applied for all forms of governance. For example, blockchain is used for a wide diversity of specific assets, such as highly specific assets (e.g., medical information) as well as lowly specific assets (e.g., goods exchanged on the cryptocurrency market). Entry costs for blockchain adoption makes it adapted to a large volume of transaction (money transfer) or to transactions likely to be standardized (donation-based insurance). Finally, with blockchain, frequency does not matter because exchanges may be performed with people and organizations who do not know each other. The different aspects of blockchain can allow to exchange with the same partner on various occasions. In some circumstances, the transaction time is maybe the only limit that could dampen some partners when using blockchain (some minutes for Bitcoin but a few seconds for other cryptocurrencies). Blockchain applications result in a decrease of transaction costs, which is confirmed empirically with Bitcoin in the article of (Kim, 2017). They find that the transaction costs of Bitcoin is lower than on the retail foreign exchange market.

- The agency theory

  The concepts of transparency and information asymmetries (Akerlof, 1970), (Jensen and Meckling, 1976), (Myers and Majluf, 1984) are important for the blockchain. The agency theory explains that frictions on the market such as information asymmetries and moral hazard have a negative impact on the market's efficiency and on the firms' decision making. With blockchain, notably its public version, all agents can access the whole information because the entire exchange history is incorporated within the blockchain. The market transparency seems to be improved in a secured way and with some cost-effectiveness (Collomb and Sok, 2016), (Shermin, 2017). In other words, blockchain decreases the complexity (transparency, token-incentives, fewer transactions) and consequently agency costs decrease (Tapscott and Tapscott, 2017). Moreover, the moral hazard issue is reduced because blockchain is based on a consensus-based system between users: it can be considered as a game in which multiple parties coordinate without communicating directly Shermin (2017) or as a coordination game with multiple equilibria (Biais et al., 2017). In addition, the question about decentralization and coordination is raised, where it is stated that using blockchain can improve higher social welfare and consumer surplus because entry and competition are enhanced (Biais et al., 2017) (Cong and He, 2017).

- The incomplete contracts theory

  A contract is supposed to be complete if all future situations are taken into consideration. In the incomplete contracts' theory, the incompleteness of the contract is due to added clauses and the verification process of the contract. Therefore, property rights are set up to avoid these costs of verification. In the case of the blockchain, the verification costs are reduced (Catalini and Gans, 2018) because the smart contract is auto-executed without the necessity to include a third-party. No clause can be added after the contract is executed, but it has to be implemented in the code itself, which directly implies a higher effort to take into consideration the potential unexpected events *ex-ante*. The property right solution is also adapted in the blockchain case because of the existence of the smart property that controls the access rights of some individuals to the blockchain (Hopf et al., 2018).

- The alternative and cognitive approaches

  The previous part described some alternatives against the contract view approach of the theory of the firm. The firm is considered as a node of competences instead of contracts involving the knowledge and the competences of all stakeholders within the firm. The blockchain is based on a community view involving several stakeholders (see Figure 2.2), combining the expertise of the developers as well as the efforts of the miners to validate the transaction process and the users activities to make the entire process work. There is no hierarchical authority because the system is fully distributed between each participant regardless of their roles.

Therefore, the blockchain system allows to allocate different resources, information, and capabilities of every different stakeholder (that can be involved in every function of the firm such as governance by a learning process) without need of a controlling authority (third-party).

#### 2.3.2.2 Blockchain new risks

The blockchain characteristics (such as transparency, decentralisation, consensus mechanism in a secured way) decrease organizations costs (such as transaction costs and agency costs) and improve informational efficiency because the access to information is faciliated. However, blockchain does not come without limitations, especially because of its novelty. There are weaknesses related to blockchain concerning its operational limits, the apparition of new costs and ethical issues.

- Operational limitations

  Despite promising benefits and potential applications, the blockchain technology faces some limits. Scholars have mainly pointed out technical issues (Figuet, 2016), (Tschorsch and Scheuermann, 2016). First, the wallet process[19] that lets individuals and organizations manage their account and cryptocurrencies is not fully secured. Some websites attempt to manage both accounts and security keys. Tschorsch and Scheuermann (2016) suggest that some kinds of wallets are less secure. The best way to secure is the paper wallet (e.g. keys as physical documents) and brain wallet (e.g. passphrase[20]). However, many users store keys on less secure softwares and websites as well as on hardwares (i.e. offline using separate devices).

  The second issue concerns transactions. The original blockchain (Bitcoin blockchain) has been initially planned for a relatively low transaction volume. Bitcoin recorded 361,155 transactions per day in 2017 and the increasing volume of transactions is already a major issue and debate in the Bitcoin community. Generalizing the technology to other domains would require blockchains to be able to consider a larger volume of exchanges as well as faster execution speed. Both features would ensure an

[19] A wallet is a software that stores private and public keys required in the blockchain system and used to exchange with each other, see the part 2.2.1.

[20] A passphrase is a password with the form of a sentence for mnemonic reasons.

advantage to blockchain over human intervention (Lamberti et al., 2017). Another issue is the fact that a transaction cannot be reversed without the agreement of all partners. In order to generalize blockchain as a technology transaction applied inside existing organizations, it appears necessary to change this rule in the protocol. Another major risk is the "double spending" problem because computer attacks may double-spend a coin and damage or even destroy the network. Tschorsch and Scheuermann (2016) state that without a 51% attack[21], a double spending can occur by force or luck, meaning that "a transaction that even has one confirmation can still be reversed".

Other possible risks are related to bugs and  which cause a network failure. An attack of this type was launched in the Bitcoin network on April 10, 2013, on the site Mt.Gox, an older exchange platform of Bitcoins causing the temporary suspension of trading of Bitcoin and a temporary paralysis of the website. More generally, the security of blockchains is based on cryptographic principles. However, if these principles were to be seriously compromised, the whole system would be less secure, thus causing considerable losses (Civitarese and Mendes, 2018), (Shanaev et al., 2018).

To summarize, the Ethereum founder, Vitalik Buterin, presents the blockchain trilemma concept. The ideal blockchain has to maximize the three properties of the trilemma: decentralization, network security, and Scalability. In practice, a blockchain can respect only two on the three below properties and more precisely, is somewhere inside the triangle, Figure 2.4 - *The blockchain Trilemma concept*. Technically speaking, you can choose only one edge of the triangle (e.g., a couple of property such as security-Scalability, Scalability-decentralization, decentralization-security). For example, the network is secured with a large number of nodes but the Scalability will be limited and longer because all the nodes must validate the transaction.

[21] One node possesses the majority of the network.

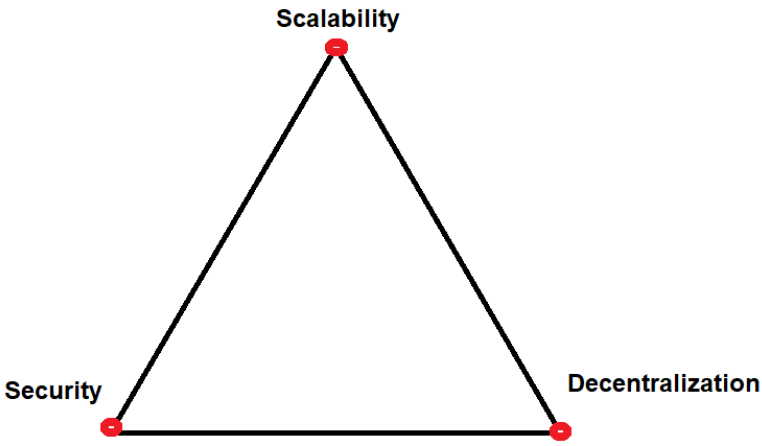


**Figure 2.4 The blockchain Trilemma concept**
This figure shows the blockchain Trilemma concept of Vitalik Buterin.

- New costs

  In addition to these operational limits due to the novelty of the technology, blockchains could also generate new types of costs.

  First, while Smart Contracts reduce part of transactions costs, negotiation costs become more complex and time-consuming because Smart Contracts require time and expertise to ensure that all possibilities are taken into consideration by the contract (Chartier-Rueg and Zweifel, 2017). Smart Contracts may face technical issues such as TheDAO example[22] (Lamberti et al., 2017). Another indirect cost is the fact that Smart Contracts attempt to control exchanges and predict almost every possible future situation, implying less uncertainty. However, sometimes uncertainty can have positive effect on projects. With locked-in contracts, serendipity has a smaller chance to appear and give new opportunities/targets for potential customers (Chartier-Rueg and Zweifel, 2017).

[22]Created in 2016, “The DAO”, is a crowdfunding and investor-directed venture capital project based on the Ethereum blockchain. Participants are investors who own the “tokens” (e.g. Bitcoin), and contractors who submit projects and ask for financing. Even if “The DAO” project was promising with a fundraising reaching 160 million dollars in 4 weeks, the project failed due to a huge attack related to a flaw in the code. The mistake provoked an important divorce in the community (called Fork) leading to the creation of Ethereum Classic (ETC) and Ethereum (ETH) (Shermin, 2017).

Second, full transparency promoted by blockchains is not ideal because secrecy and privacy are required for business making. Hence, private blockchains may control access to information. Moreover, sometimes transparency or decentralization is not really suitable. Decentralization, even more in a public blockchain (with transparency), is a huge issue to manage because the number of participants is high and the information must be reliable (Chartier-Rueg and Zweifel, 2017). Therefore, new costs appear *ex-ante* regarding the blockchain setting up (rules, access, and writing of the protocol) as well as *ex-post* costs in order to verify the veracity of information inserted in the blockchain. Then, if the known agency problem decreases with transparency and decentralization, new agency issues may arise because of the inherent complexity of computer systems and programming which imply huge entry barriers (Wright and DeFilippi, 2015), (Shermin, 2017).

- Ethical implications

  Another question associated to blockchains concerns their ethical nature. Blockchains appear as a technology prone to reinforce ethics thanks to its advantage of transparency (all users can be aware of what happens) and decentralization (the power is held by every user). On this basis, Bitcoin could be viewed as an ethical kind of payment (Angel and McCabe, 2015). However, some blockchain features should be improved in terms of ethics and social responsibility.

  Using blockchains based on Proof-of-Work requires a lot of electricity, representing for Bitcoin the same amount than the annual consumption in Ireland (O'Dwyer and Malone, 2014). Researchers in Cambridge show that the Bitcoin consumption is 0.25% of the world energy electricity consumption based on their index, Cambridge Bitcoin Electricity Consumption Index (CBECI)[23]. Proof-of-Stake also knows ethical issues because it is restricted to the only token holders (Lamberti et al., 2017).

  Another issue is privacy and data confidentiality within blockchains (Lamberti et al., 2017). On the one hand, blockchains, especially in their initial version (blockchain of Bitcoin), can lead to infringements to privacy (this

[23]https://cbeci.org

is why private blockchains are required in some cases, e.g. health). On the other hand, a total prohibition of blockchains would also be an infringement to individual freedom, especially because the movement comes from citizens (Wright and DeFilippi, 2015).

Blockchains raise the question of the role of humans in the process. One could think that human experts would always be required in Smart Contracts for technical and regulation reasons (Shermin, 2017). Within an "algorithm governance" (Wright and DeFilippi, 2015) computers would inevitably control or at least influence some decisions of companies' and individuals' lives. In other words, our choices would be based on a prescriptive and deterministic way (Wright and DeFilippi, 2015). A response to this criticism would be to enforce regulation and supervision on these aspects, a so-called "lex cryptographia" (Wright and DeFilippi, 2015) that would be a bottom-up process, firstly based on issues already observed, and then developed along with the extension of blockchain-based technology.

These drawbacks are examined in the literature, and notably in the computing field in order to improve key technical aspects such as security, costs and ethics. Addressing these issues would stimulate the growth of blockchain opportunities for managerial aspects as well as for the society.

The strengths and weaknesses of the blockchain technology are summarized in Table 2.3 - *Strengths and weaknesses of the blockchain* based on its main characteristics: (1) Transparency; (2) decentralization; (3) Consensus-based mechanism; (4) Smart Contracts; (5) Secured; (6) Immutability; and (7) Instantaneous exchanges.

The blockchain has the potential to be adopted within organizations because it plays a challenging role in the transaction process using a special community to act together and avoiding the hierarchical existing way of thinking. But, how is the blockchain technology implemented in practice ? How can it be appropriated by organizations?

**Table 2.3 Strengths and weaknesses of the blockchain**

This Table summarize the part showing the strengths and the weaknesses of the blockchain based on its main characteristics.

| **Characteristics** | **Strengths** | **Weaknesses** |
|---|---|---|
| Transparency | (1) Higher access to information; (2) decrease transaction costs (Kim, 2017); (3) Decrease agency costs (Tapscott and Tapscott, 2017); | Restricted for business with sensitive data |
| Decentralization | (1) Increase stakeholders' participation; (2) Higher social welfare (Biais et al., 2017), (Cong and He, 2017) | (1) Restricted for business with sensitive data; (2) Privacy and data confidentiality (freedom) |
| Consensus | (1) Decrease opportunistic behavior (MacDonald et al., 2016), (Larios-Hernandez, 2017); (2) Decrease moral hazard issue (Shermin, 2017) (Biais et al., 2017) | (1) Energy consumption (PoW; (O'Dwyer and Malone, 2014)), (2) Social inertial effect (PoS; (Lamberti et al., 2017) |
| Smart Contracts | (1) Change the *ex-post* opportunism; (2) Decrease Uncertainty; (3) Decrease verification costs (Catalini and Gans, 2018); Possibility of property rights (Hopf et al., 2018) | (1) Increase negotiation costs (Chartier-Rueg and Zweifel, 2017); (2) Decrease of uncertainty implies less opportunities (Chartier-Rueg and Zweifel, 2017); (3) Human intervention (Shermin, 2017) |
| Secured | (1) Decrease the complexity; (2) Decrease agency costs (Tapscott and Tapscott, 2017) | (1) Wallets (Tschorsch and Scheuermann, 2016); (2) Transactions: volume, speed and reverse (Lamberti et al., 2017); (3) Attacks and bugs (Shanaev et al., 2018) (Civitarese and Mendes, 2018); (4) Trilemma concept; (5) Financial losses (theDAO, (Lamberti et al., 2017)); (6) Entry barriers implies new agency issues (Shermin, 2017), (Wright and DeFilippi, 2015) |
| Immutability | Decrease *ex-ante* opportunism | Human intervention |
| Instantaneous | Decrease transactions costs (Kim, 2017) | Human intervention |

## 2.4 The appropriation process that leads to the extension of blockchain within organizations

The blockchain technology appropriation seems to be a bottom-up approach which started in the Bitcoin community (mainly online forums), outside any existing companies. The concept is first adopted in the industry by means of collaborations of companies in the finance sector. It then reached other industries progressively (Lamberti et al., 2017). This part presents the appropriation of this new innovative technology within the firm. First, we present the appropriation process, more precisely, the appropriation of this new management tool through internal communities. Second, we expose the different evolution of the blockchain technology by providing four possible cases of blockchain and then giving some examples through the time. Finally, we analyze the blockchain evolution through the theoretical framework.

### 2.4.1 Appropriation process

#### 2.4.1.1 The management tool appropriation

Ruggles (1997) presents some definitions on "management knowledge" characterized by 3 concepts: knowledge generation (what is new), knowledge codification (the ability to re-use knowledge) and knowledge transfer (transfer and absorption of knowledge). "Tools" are defined as "technologies which support the performance of activities or actions"; whereas "knowledge tools" are "technologies broadly defined which enhance and enable knowledge generation, codification and transfer". In other words, a knowledge tool has the objective to make the work easier by allowing resources in a better efficient way to the required tasks. They handle "data management tools" (generate, access, store and analyze data) and "information management tools" (the manipulation of information). There exist several definitions about the concept of "management tool", even the name of this concept varies ("management tool", "business tool", "tools", "objects", "artefacts") (Dominguez-Péry, 2011). Moidson (1997) defines a management tool as the link between variables that come from the organization through reasoning and knowledge in order to increase the rationality in the organization. To generalize, a management tool is a mix of knowledge, expertise, materials and rules in an organization in order to increase the collective improvement of this organization, (Dominguez-Péry, 2011). The main idea is that individuals create efficiency in interaction with tools. A potential issue is that the technology goes faster than man reaction (Moidson, 1997). Consequently, the question is the appropriation of this kind of tools by individuals within an organization (Dominguez-Péry, 2011).

In the same vein, Guillemot and Kocoglu (2010) show that Information and Communications technology (ICT) tools are faster than traditional management tools. They emphasize that management tools and ICT tools are different but complementary for the firm[24]. The blockchain technology can concern every kind of firms because it seems to be an ICT tool as well as a management tool. Indeed, its IT aspect (computing innovation that works with an Internet connection) has a management goal because it can be used to increase the organization operations through a collective effort.

In general, the main question is how to implement in practice a new management tool inside a firm. The resistance can come from three dimensions of a management tool: (1) The material dimension (related to the concrete and tangible supports of the tool), (2) The managerial philosophy dimension (related to the work behavior implying by the tool such as organizational procedure or incentive adoption), (3) The relationship dimension (the relationship between participants about the old habits in previous tools) (Hatchuel and Weil, 1992), (Detchessahar and Journé, 2007), (Dominguez-Péry, 2011). A technological and organizational change requires some instrumental coherence (the objective is to increase the performance of the firm) and psychological coherence (related to experiences of the future users of the management tool) (Bourguignon and Jekins, 2004). Social groups are a community that build social values and norms. They are averse to change their routines and habits, especially if they are influenced by cultural and political aspects. The main challenge is to reduce the gap between novelty and old habits. It could be effective if strategies of different functions inside firms (Marketing, Human resources, Information Systems...) are promoted by their experts (Tripier, 1994) and are coherent with the organizational strategies. Dominguez-Péry (2011) supports that a manage-

[24]They highlight that the industry effect has a higher impact than the size effect on the appropriation of the management tools compared to ICT tools. Depending on the industry to which a firm belongs, management tools will be preferred to ICT tools. For example, large companies in finance and real estate invest in both tools but with a preference for ICT tools whereas industries (groups) are interested in both tools but prefer management tools.

ment tool needs to have formal rules related to the participants' roles in order to be accepted by the organization. Another possibility is the flexibility of the management tool appropriation. The use of a tool will change the tool itself to be adaptable to the actors (due to psychological and experiences effects), the situation (due to political and management situations) (Orlikowski, 1992), (Mintzberg, 1973) and because of the time effect (Dominguez-Péry, 2011). The innovative technology itself will shift from the original purpose of its creation to new uses (Ciborra, 1997), (Ciborra, 1999). The following part 2.4.2 will show the shift in the use of blockchain through its evolution. If the purpose of Bitcoin was initially to create a particular monetary system decorrelated to any existing financial pressures, financial institutions themselves plan to reuse this technology for their own needs.

A management tool provides values for the firm (Dominguez-Péry, 2011), such as a "guarantee value" meaning the tool has a value if the organization adopts it whatever the effective use of this tool is. It is the case of blockchain because of a high media coverage of its potential, making every firm aware to implement it for their activity. The "structural value" is the design engineering related to the tool (e.g., the technical value of the innovation). Blockchain is a technical innovation notably because it solves the double-spending problem in computing sciences. The effective value of a tool can be determined *ex-post* according to the successive steps of its evolution and adoption by different stakeholders, called "built value". The existence of a "use value" arises when the conception and the implementation are inter-related and evolve together. We will see later that it is the case for the blockchain, firstly created by an informal IT and libertarian community providing value for these participants of the community, and whose characteristics and applications were changed by other stakeholders and communities (in the broad sense) such as existing businesses looking for value creation inside the firm.

#### 2.4.1.2 The community impact

The question of the community inside the firm is relevant to understand the appropriation of a new management tool, especially when the new management tool comes from an outsider informal community. The concept of communities and more precisely communities of practice comes from (Brown and Duguid, 1991). Following this concept, numerous researches focus on a special community and analyze the link between a particular community and the firm. For example, Füller et al. (2008) focus on the brand communities and the appropriation of a new product[25]. In this research, we focus on the communities related to the virtual world of the blockchain.

A virtual user's community can be built by shared skills and practices through informal social network where the users exchange their knowledge and their opinion about a shared topic (Hienerth and Lettl, 2011), generally motivated by one lead user. Early adopters have the lead of a market or a technology long before the majority of the users. Early adopters are the interlocutors of potential future adopters sharing with them common points such as skills, experience and activities. The frequency of talks between them allow for lower opportunistic behavior and lower cost of learning (Benghozi, 2008).

Innovation that comes from outside the firm can create value inside the firm and become a standard[26] if it meets several requirements. First, the firm has to manage a relationship with the outsider community in order to integrate innovation that comes from this community. Creating value for the company must go hand in hand with avoiding conflicts. However, this relationship can have different levels and various impacts. If the firm has a huge influence on the community, it can control the community and create more value for the company. This gain is not obtained without efforts. The firm has to handle managerial issues related to community resources, norms and values, licenses, conflict interests about work, control and ownership. This is what Dahlander and Magnusson (2005) called the "symbiotic approach" of the firm–community relationship. Another approach is the "commensalistic" one, where the firm has to manage internal conflicts (such as encouraging the acceptation of an innovation controlled by an outsider community), because the firm does not merely influence the community. This approach can easily turn to the "parasitic approach"

[25]These authors focus on why, how and which personalities aspects of a brand communities are required to appropriate a new product development such as creativity, community identification, brand passion, trust and knowledge influence the diffusion (sharing) of their information about a product. Extraversion and openness of personality aspects have an impact on brand passion, creativity and community identification. The main driver to involve the brand community in the innovative process of a new product is their own interest emphasized by knowledge and innovative skills.

[26]A standard equipment is defined as "a product or product/technology combination that is widely adopted by many classes of users and defines the core performance metrics along which firms compete" (Hienerth and Lettl, 2011).

where the firm focuses only on its own benefit and does not take into account the community at all (Dahlander and Magnusson, 2005). Second, innovation that comes from outside the firm can become a standard inside the firm on the long run. The study of (Hienerth and Lettl, 2011) is twofold. First, they study the role of lead users and peer communities in innovation appropriation as a standard equipment in an industry. Second, they present the barriers that peer communities face in the appropriation of innovation process. They propose a longitudinal research design in the medical and the sporting equipment industry. If the starting point comes from the lead users' ideas, community members provide feedbacks on these ideas by testing the innovation and, if they agree, they spread the innovation inside and outside the community. They play the role of intermediaries between first adopters and the early majority of users.

### 2.4.2 Blockchain evolution

The blockchain technology has the general potential to change organizations, but in order to be incorporated by firms themselves, this IT management tool has to be flexible in its characteristics to adapt its services to the firms' needs especially in specialized industries. First, we present the four possible cases based on the two-level dimension previously described. Second, we describe historically the evolution illustrated by some examples of blockchain projects in different industries. Third, we analyze this evolution and the effective appropriation from an informal community towards the firm.

#### 2.4.2.1 A 2-dimension level analysis

In the first part, we present the two-dimension level, the openness dimension regarding the users' access right and the permission dimension of the miners' access right. Some researches show the differences between the two components of each dimension separately, such as the technical differences between permissionless and permissioned blockchain (Wust and Gervais, 2017) or the main differences between the public and private versions of the ledger (Guo and Liang, 2016).

The barrier to entry in a public blockchain is low because access rights are fully open to every user as long as these users have an Internet connection, implying a strong network effect. Decentralization is absolute, without any control by a third party (Buterin, 2015b), (Collomb and Sok, 2016). This decentralization can have a negative effect on coordination and can also challenge confidence (Biais et al., 2017). Cryptocurrencies use a public blockchain such as Bitcoin. In general, public blockchains are preferably used for Client-to-Client exchange (Buterin, 2015b), (Biais et al., 2017). The private version is adapted for data protection (privacy) and allows to have control over the technology (to manage the rules or interfere if bugs occur). Contrary to the public version, a private ledger is scalable, increases centralization, decreases transparency, and is likely to be used for Business-to-Business exchange regarding database management, settlement-delivery activities and auditing (Buterin, 2015b), (Collomb and Sok, 2016).

In this part, we summarize the differences in a table of two-dimensions comparisons and therefore present four cases: The Public Permissionless blockchain, the Private Permissionless blockchain, the Public Permissioned blockchain and the Private Permissioned blockchain, Figure 2.5 - *The two-levels dimension mapping* and Table 2.4 - *Two-levels dimension analysis of the blockchain*.

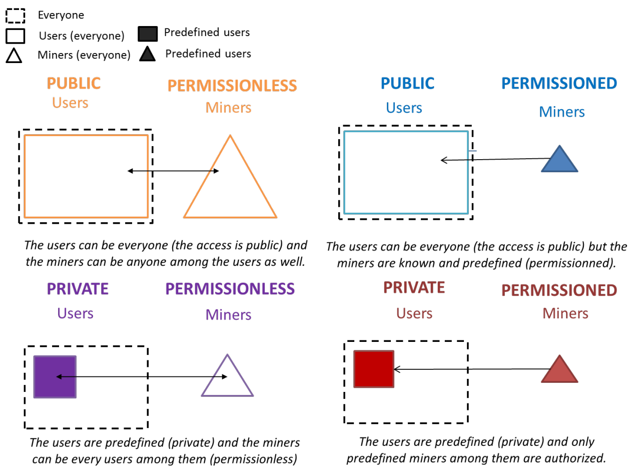


**Figure 2.5 The two-level dimension mapping**
This figure maps the two-dimension analysis about the access rights for the miners and users' groups. Own representation.

**Table 2.4 Two-level dimension analysis of the blockchain**

This table presents the two-level dimensions of the blockchain based on the openness dimension (user) and the permission dimension (miners) by providing four possible cases of blockchains: the public permissionless, the public permissioned, the private permissionless and the private permissioned.

| | | **Permission**<br><br>Related to the required data for validation (write and commit). | |
|---|---|---|---|
| | | **Permissionless**<br><br>No restriction, miners are anonymous. | **Permissioned**<br><br>Restriction, miners need a permission to read and write in the ledger. |
| **Openness**<br><br>Related to the access (view and read) of the data inside a bloc after validation. | **Public**<br>No restriction on reading and download the validated data inside the blockchain and anyone can send transaction. | Users: Anyone<br>Miners: Anyone<br>Governance: Decentralized<br>Consensus: PoW<br>Reward: Needed<br>Anonymity: High (pseudonymous)<br>Trust: Low<br>Scalability: high in favor of node scalability (low in favor performance-scalability)<br>Immutability: High<br>Finality: Low<br>Throughput: Low<br><br>*Ex: Ethereum, Bitcoin* | Users: Anyone<br>Miners: Known and authorized<br>Governance: Centralization<br>Consensus: PoS<br>Reward: Needed<br>Anonymity: High<br>Trust: High<br>Scalability: Medium<br>Immutability: Medium<br>Finality: Medium<br>Throughput: High<br><br>*Ex: EOS, Ripple (global financial transaction system)* |
| | **Private**<br>Restriction (limited and predefined) on the access of data inside the blockchain and on sending transactions. | Users: Known and authorized predefined<br>Miners: All predefined user can participate to validation<br>Governance: Decentralization<br>Consensus: FBA<br>Reward: No need<br>Anonymity: Low – Medium<br>Trust: Low<br>Scalability: High - Medium<br>Immutability: Medium<br>Finality: High<br>Throughput: High<br><br>*Ex: Monet, LTO Network, Holochain* | Users: known and authorized<br>Miners: only the network operator / member of consortium (among the users,<br>only special has the right)<br>Governance: centralization<br>Consensus: PBFT, multisignature<br>Reward: No need<br>Anonymity: Low<br>Trust: High<br>Scalability: High in favor performance scalability (low in favor of node scalability)<br>Immutability: Low<br>Finality: High<br>Throughput: High<br><br>*Ex: Hyperledger Fabric Entreprise, Ethereum alliance,<br>Quorum, Libra* |

- **Case 1: Public permissionless blockchain**

  In this first case, all the users can read and join (*public* dimension), and every user can be a miner able to write commit and validate the transactions (*permissionless* dimension). This blockchain is the original one described by (Nakamoto, 2008) in the Bitcoin system. The main advantage of this blockchain is the absence of a trusted third party even if the trust in miners is moderate due to their anonymity (pseudo-anonymity in the case of Bitcoin). These blockchains are very immutable and the waiting time until a given transaction is added to the blockchain is low (the Bitcoin community suggests a waiting time of 6 blocks to be sure that a transaction is recorded and confirmed.). The mechanism consensus is generally the Proof-of-Work because it requires an external proof to the system, the computational power. Due to the energy consumption issue (O'Dwyer and Malone, 2014), some other applications of public permissionless blockchain try to replace the Proof-of-Work (Bitcoin) by the Proof-of-Stake (future improvement of Ethereum). Regarding the Scalability, it is in favor of node Scalability instead of performance Scalability. According to Wust and Gervais (2017), a company needs to use a public permissionless blockchain if it is necessary to store data between multiple participants using online trusted third party[27], but the identity of the miners remains anonymous. In other words, the permissionless public blockchain is useful if the firm needs to manage a ledger with many copies accessible to each user and in which the verification of the integrity of the ledger is handled by many miners[28].

  The main examples of the public permissionless blockchain are the original innovation of cryptocurrencies applications such as Bitcoin or Ethereum (see part 2.2).

- **Case 2: Private permissionless blockchain**

  In this second case, only authorized users can join and read the data inside the ledger (*private* dimension). Among the predefined users, everyone can be a miner and be involving in the validation of transactions and in the consensus system (*permissionless* dimension), that corresponds most of

[27] Meaning the writing and validating right is delegated to the third party.
[28] https://www.chyp.com/

the time to the Federated Byzantine Agreement algorithm that does not require a token incentive. This consensus mechanism has some advantages such as a high Throughput, low transaction costs, and high Scalability in a governance of decentralization where the users can decide who to trust. Thus, anonymity is moderated because only some users are authorized to join the network. Trust is mitigated because, on the one hand, the users are identified while, on the other hand, the miners can be any member in the authorized group users and sometimes they have very different interests to each other. The Immutability is moderated as well and the Finality is immediate. Smart Contracts that are executed on the private permissionless blockchain, allow to define who has the right to read the data by creating, for each contract, a private associated blockchain ("sidechain").

Three examples of projects are Holochain, LTO Network and Monet[29]. Holochain[30] is a web hosting project with the objective to create a decentralized Internet. The idea is to decentralize the computing resources by sharing the resources of every node on the network to realize micro-transactions solving the problems of the energy consumption (Harris-Braun et al., 2018).

In the business-to-business (B2B) industry, the LTO Network project[31] has the objective to improve a "trust flow" and provide an equal collaboration between huge organizations (firms, multinationals and governments), while taking into consideration the data privacy and the General Data Protection Regulation (GDPR) compliance. In this project, the smart contract (called, in this case, Live contract) implies the creation of a blockchain for every Live contract (Schmitz et al., 2018).

Finally, Monet[32] is a project for multiple temporary blockchains deployed using mobile devices without a third-party coordination. There is a possibility to create bridge between main stable blockchains and temporary blockchains to transfer some information during a short period of time (Arrivets, 2018).

[29]https://medium.com/ltonetwork/the-rise-of-private-permissionless-blockchains-part-1-4c39bea2e2be

[30]https://holochain.org/

[31]https://lto.network/

[32]https://monet.network/about.html

- **Case 3: Public permissioned blockchain**

  In this third case, all the users are allowed to participate (*public* dimension) but the miners need an authorization (*permissioned* dimension). The consensus mechanism requires a token because it is based on the ownership of the token (see Proof-of-Stake). Trust in the validation process is high because miners are identified and they can lose their tokens if the system is attacked. Anonymity of users is high because it is a public blockchain, thus anyone can join the network. The governance is centralized because the miners are known. In technical terms, the Scalability, Immutability, and Finality have a moderate level. In this case, the decision making for a company to use a public permissioned blockchain is always the need to store data with multiple players through online trust third-party in which all miners are identified and not all are trusted. Thus, a data check is required publicly (Wust and Gervais, 2017).

  Some main examples are the private cryptocurrency systems such as Ripple and EOS. Ripple[33] is created by a company and focuses on international micro-payment transactions between banks and financial institutions (Schwartz et al., 2015). The objective is to provide a universal clearing currency in the interbank exchanges. Instead of exchanging directly dollars versus euros, the dollar is exchanged in ripples and then in euros in order to speed the process and decrease its costs.

  In 2018 Daniel Larimer, "Block.one", creates the blockchain EOS[34] that becomes the main competitor of Ethereum providing the same services of decentralized applications via Smart Contracts (Brent Xu a et al., 2018). The main differences are the speed (3000 transactions per second for EOS versus 15 transactions per second for Ethereum), no transactions fees and the application of the Delegated Proof-of-Stake[35].

[33] https://Ripple.com/

[34] https://eos.io/

[35] An extension of the Proof-of-Stake in which the users select "witnesses" through a voting process that will validate the transaction when the witness possesses the most tokens. See the list of terms and abbreviations.

- **Case 4: Private permissioned blockchain**

  Finally, in this fourth and last case, only authorized users can join and read the ledger (*private* dimension) and only few among them are predefined to be miners (*permisioned* dimension). Thus, anonymity is low because every agent is predefined and identified in the system. Trust in miners is very high because the consensus mechanism used is a Practical Byzantine Fault Tolerance or multisignature: if the miners behave badly, they can lose their membership access. In addition, the private permissioned blockchain allows to increase the speed of the transaction validation (Finality is immediate), the Throughput, and the Scalability in favor of performance Scalability (it works for small as for huge networks).

  The blockchain is not necessarily immutable because the centralized governance that decides who can participate in the limited group and who among them can take part in the validation process could influence the possibility to modify the history of the blockchain. The main advantages are the non-necessity of any mining process as well as low transaction costs. The main issue is to decide precisely who are the authorized participants. Sybil attacks[36] risks are reduced because the identity of every participant and its right to access are known. Wust and Gervais (2017) show that the decision to choose this fourth case is the same as for the public permissionless but the verification in this case does not require to be public.

  The main examples of the private permissioned ledger are the Hyperledger Fabric blockchains (Androulaki et al., 2018), Entreprise Ethereum Alliance (Burnett et al., 2018), Quorum by J.P. Morgan (Morgan, 2018), Libra (Amsden et al., 2018). These examples allow to run many malleable and flexible blockchains according to the needs of the business companies in different industries such as bank, payment infrastructures, and supply chain. Therefore, blockchain applications that come initially from financial needs are now adapted to non-financial applications.

[36] When one node takes the control of the network by creating several nodes. See the list of terms and abbreviations.

To conclude, from the most open to the most restricted cases, the public permissionless blockchains such as Bitcoin and Ethereum could be compared to the Internet whereas the private permissioned blockchain looks like more an Intranet [37].

#### 2.4.2.2 The evolution of the Blockchain in practice across three generations

We present hereafter three levels of applications of blockchain according to the three historical stages of blockchain implementation. The first one concerns the cryptocurrencies family or "blockchain 1.0", the second one concerns applications linked to finance and insurance industries or "blockchain 2.0" and finally the third one "blockchain 3.0" concerns other domains (Lamberti et al., 2017).

Since the creation of Bitcoin, more than 860 currencies were recorded (Hileman and Rauchs, 2017). The top-10 based on market cap is presented in Table 2.5 - *Top-10 cryptocurrencies* and Figure 2.6 - *Top-10 cryptocurrencies*.

**Table 2.5 Top-10 cryptocurrencies**

On July 7th, 2019, 2,322 currencies and 19,242 markets are recorded on the Coinmarketcap website.

| Rank | Cryptocurrencies | Market cap ($) | Percentage (%) |
|---|---|---|---|
| 1 | Bitcoin | 204 263 638 041 | 65 |
| 2 | Ethereum | 28 913 920 463 | 9 |
| 3 | Ripple | 13 903 704 209 | 4 |
| 4 | Litecoin | 6 359 274 784 | 2 |
| 5 | Bitcoin cash | 6 119 268 064 | 2 |
| 6 | EOS | 4 341 606 828 | 1 |
| 7 | Binance Coin | 4 170 043 168 | 1 |
| 8 | Tether | 3 871 830 883 | 1 |
| 9 | Bitcoin SV | 2 888 963 361 | 1 |
| 10 | Others | 37 661 215 062 | 12 |
| | **Total** | 312 493 464 863 | **100** |

[37] https://medium.com/blockchainspace/2-introduction-to-blockchain-technology-eed4f089ce5d

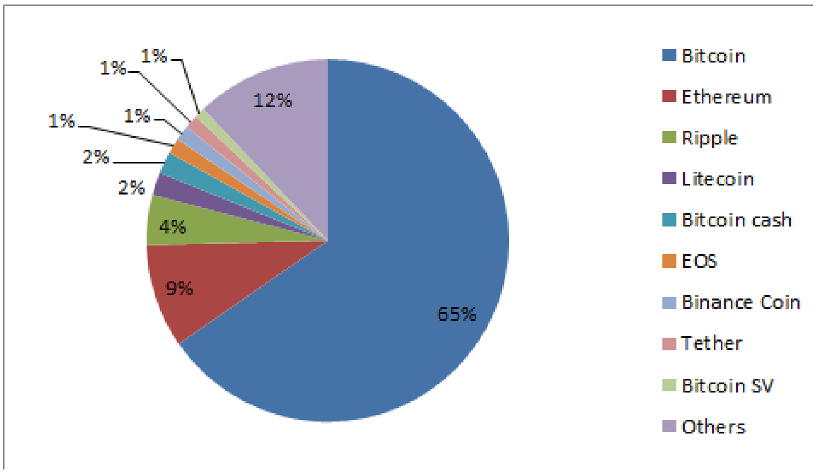


**Figure 2.6 Top-10 cryptocurrencies**
On July 7th, 2019 the number of cryptocurrencies is 2,322 and 19,242 markets for $ 312 493 464 863 of total market capitalization. The data comes from the website coinmarketcap.com.

These cryptocurrencies have different uses and characteristics. Some cryptocurrencies are devoted to humanitarian support (FoldingCoin), micropayment (ReddCoin), anonymity and privacy (Monero and Dash), or even intended for financial professionals (Diamond). Companies may also be willing to create their own cryptocurrencies (Paycoin, Whoppercoin of Burger King). A majority of these cryptocurrencies are based on the Bitcoin concept and change or improve some of its features. For example, the maximal number of units is fixed at 21 million for Bitcoin, 84 million for Litecoin but is virtually infinite for Ether. In the same vein, the time between transactions amounts to 10 minutes for Bitcoin, 2.5 minutes for Litecoin, seconds for DASH and Ripple (White, 2015), (Collomb and Sok, 2016) (Hileman and Rauchs, 2017). Other projects aim to offer a blockchain platform that companies or organizations could use in their own project (Wood, 2014), (Cong and He, 2017), (Hileman and Rauchs, 2017). For example, Ethereum is an articulation between a cryptocurrency and a blockchain service in which Smart Contracts are run (DeFilippi and Mauro, 2014), (Wood, 2014), (Buterin, 2015a), (Shermin, 2017).

The “blockchain 2.0” deals with finance and insurance (Lamberti et al., 2017). Blockchains may be used in corporate finance (Yermack, 2017) and on financial markets through a special crypto-security market (Lee, 2016), (Wright and DeFilippi, 2015) or a new futures contracts market (Collomb and Sok, 2016). According to Cong and He (2017), blockchains and Smart Contracts may have a strong interest for FinTech industry in trusted payments and trading finance. Many big names of the financial industry are involved in research on blockchain: (1) By grouping their expertise to create a blockchain, for example Corda in a consortium of 200 professionals (R3), Hyperledger or Ethereum Enterprise Alliance; (2) By creating an internal group of works in many banks such as J.P. Morgan (Quorum), Goldman Sachs. (3) Multinational financial services also show their interest such as Visa (B2B Connect, payments services between firms and financial institutions), American Express (rewards program for customer that use blockchain for record-keeping and cryptocurrency for reward points), MasterCard (a faster blockchain for payments between merchants and customers). (4) Even some public financial institutions are interested such as the French government ("mini-bons"), the Royal Bank of Canada ("Project Jasper") (Lannquist, 2018).

Insurance companies are also interested in blockchain technology (Wright and DeFilippi, 2015), (Lamberti et al., 2017). For instance, blockchains can improve the design of index insurance by decreasing operating costs (e.g. measure of excessive temperature or rainfall). The issue is critical for weather insurance which can procure automatic payments as soon as the trigger of the contract is reached. Blockchain is a suitable platform to improve the "pay-per-use" associated with Internet of Things technology. Axa with Utocat launched the fizzy project, a flight insurance. When a flight is delayed, a payment is automatically sent to the insured through a smart contract recorded on a blockchain.

In what Lamberti et al. (2017) called the "blockchain 3.0", we find other domains such as real estate, government, health, science or connected objects (Wright and DeFilippi, 2015). In Brooklyn, an application exists regarding solar energy. Transactive Grid has the objective to manage the excess and the lack of energy between houses through a blockchain platform (Ethereum). Blockchain can also be useful for health care, especially for organ donation or any personal information with respect of the privacy issue, as well as for traceability of objects, e.g. recording the route and transactions of a precious object. For instance, a number is associated with a diamond: on the one hand, the number is engraved on the diamond with a special tool and on the other hand, the number is recorded on the blockchain (Everledger Application or DeBeers announcement), where at this time the falsification problem is solved. A remaining problem is the association between the number and the object. The first issue is to decide who adds this number. The second issue is the impossibility to change the number in the future. Other sectors are involved in traceability in their supply chain and blockchain research such as the retail sector with Carrefour (the whole food supply chain becomes publicly visible for all stakeholders), Alibaba or Walmart, the transportation sector with Airbus, Lufthansa and Air France, Volkswagen and Renault and Toyota, the shipping sector with Maersk (Lannquist, 2018). Blockchain can be associated with connected objects, e.g. cars, hotels, or rents (Wright and DeFilippi, 2015). Slock.it based on the Airbnb concept wishes to use blockchain with any location. For example, a sensor is fixed on a car which detects the use and launches the smart contract linked to a blockchain. Some telecom firms are also working on connected object such as Cisco or secured communication such as Orange (Lannquist, 2018). Another profession likely to use this technology is notaries. Administrative papers and verification functions could be transferred to the blockchain. Governments also pay attention to this technology for many services: elections, personalized systems, political programs, and constitutional rights (Wright and DeFilippi, 2015), (Lamberti et al., 2017).

#### 2.4.2.3 The current trend: from public permissionless to private permissioned blockchains

At first, the blockchain is considered as a new technology tool managed by an active community. This community has the ownership of the protocol (everyone can access and modify the code because it is open source) and decides about the rules and decisions (through discussion forums on the Internet). The success of this community to make the technology works is because the blockchain is public (for users) and permissionless (for miners).

Thus, everyone is a potential participant to the eco-system and there is no third-party to interfere in the decisions. Even if the community has some lead users such as Nakamoto who has an influence on the entire community, anyone can use the ledger and send transactions as well as anyone has the choice to be part of the consensus mechanism through the mining process (in the Bitcoin case) and directly work on the blockchain. Moreover, the negotiation and decision processes are located outside the blockchain on some other websites and forums.

This technology firstly appears with cryptocurrencies applications whose objective is to replace all intermediaries. Nevertheless, as their intermediary role progressively drops, banks and financial institutions have been interested in the technology itself, noting its innovative nature and the possibility of adapting the technology to their needs. The cryptocurrency is just an information that can be replaced by any other information that needs to be stored or exchanged without a required third-party to verify and ensure the security of the process. Thus, the technology of the blockchain 2.0 age is viewed as an ICT tool allowing to improve the exchanges inside financial institutions themselves. It could increase the rapidity of some exchanges and also decrease the related transaction costs.

In the last wave (blockchain 3.0 age), several industries find that this technology can be viewed as a management tool allowing companies to change the way they are organized or governed. Potential implications are then much larger. However, the technology needs to adapt itself to the constraints of the firm such as the confidentiality of sensitive data, the knowledge of participants' identity in order to ensure the security and the traceability of the information in a confidential and controlled manner. This is the reason of the implementation of different degrees of permission and openness restrictions (public/private, permissionless/permissioned). In practice, the blockchain appears as incorporated into the firm when it fosters the innovation process in a private and controlled way (the private permissioned blockchain).

All the existing or planned blockchains in the private permissioned case are in reality a consortium of several famous companies that create together different and flexible possibilities to use the technology with the final objective to create standards. For instance, IBM trust Food based on Hyperledger has the objective to create international standards related to the traceability in the food industry (already used by Walmart, Nestle, Carrefour, Unilever).

Management tools can have different values for a firm such as: (1) "guarantee" when the technology is adopted by the firm whatever the use, for example the passing fad of the blockchain by companies; (2) "structural" is the technical value of the tool, for example the solution of the double spending for the blockchain; (3) "built" deals with successive steps of the tool evolution by different actors, this what we observe in the blockchain evolution from a public and permissionless version of a virtual community to a private and permisioned version of a business community; and finally (4) "use" when the creation and the implementation are inter-linked by Proof of Concepts (POC) and others collective work inside the firm (Dominguez-Péry, 2011).

The evolution of the blockchain considered as a management tool can be compared to the Internet evolution, notably the TCP/IP innovation as this type of "foundational" technology requires more time than a "disruptive" technology. Iansiti and Lakhani (2017) determine four phases of appropriation based on the degree of novelty and the amount of complexity and coordination: (1) Single use (Bitcoin); (2) Localization phase (private blockchain for the financial sector); (3) Substitution phase (the blockchain 2.0); (4) Transformation with the use of Smart Contracts (the blockchain 3.0). The impact of the blockchain inside the firm is therefore a long-term process. At the beginning, consequences are lower costs in the transaction process as well as a transformation of the business model of the firm, whereas in the long run, blockchains may become standards inside organizations and industries, (Carson et al., 2018).

### 2.4.3 Towards new institutions?

Blockchain is original in the sense that this concept is more than a single technology. It could appear as a full-blown institution of governance, beside every organization form such as the firm and the market. MacDonald et al. (2016) suggest that blockchain looks like a "catallaxy" in which multiple agents participate without a bundle and whose process is based on market price systems. Especially, a part of the literature deals with the concept of governance and blockchain. First, in the corporate governance, blockchain has an influence with regards to different stakeholders (managers, institutional investors, small shareholders, auditors) (Yermack, 2017) and more generally it could be a new model of governance. For Reijers et al. (2016), it has a potential of a "new institution" among firms and markets following the properties of commons (Ostrom, 1990), more precisely the Common Based Peer Production[38] (Rozas et al., 2018). Regarding the political field, blockchain is associated to institutions (Davidson et al., 2018) and defined as "crypto-economy" governed by entrepreneurs instead of governments, (Allen, 2016). The field of entrepreneurship is also affected by the technology notably the new ways of raising funds (ICO) and involving stakeholders in new projects (Chen, 2018).

[38]"Emergent model of socio-economic production in which groups of individuals cooperate with each other to produce shared resources without a traditional hierarchical organization."

The ongoing development of Libra initiated by David Marcus from Facebook and the blockchain-based startup of Chainspace acquired by Facebook in 2019 shows the adoption of an innovation from an informal community in the Public Permissionless version of cryptocurrency to a Private Permissioned version with the intention to revolutionize the payment industry. The objective of Libra is to provide a monetary ecosystem far away from fiat currency without traditional banking systems and using the existing instant mailbox such as Whatsapp or Messenger.

The fundamental rationale remains the same as Nakamoto's one but, this time, users will belong to private networks (the authorized users are the ones who have a Facebook account all around the world) and miners will require an authorization to be part of the validation process using the delegated Proof-of-Stake consensus algorithm. Indeed, only the Libra Association's members could be admissible, and among them, only firms inside Fortune 500 and which invested in the Libra Investment Tokens. Compared to the cryptocurrency system, the Libra project involves many businesses together: payment services (Visa, Mastercard, Paypal, Stripe, Pay , Mercado Pago), e-commerce and sharing economy (Uber, Lyft, Spotify, Calibra, Ebay, booking.com, Farfetch), telecom (Free, Vodafone), cryptocurrency businesses (coinbase, Xapo, Bison Trails, Anchorage), investment funds (Ribbit Capital, Thrive Capital, Andreessen Horowitz, Union Square Ventures, Creative Destruction Lab), R&D (Breakthrough Initiatives) and NGOs (Women's World Banking, Mercy Corps, Kiva). Technical improvements will aim to increase the number of transactions per seconds from 7 for Bitcoin to 1000 for Libra (and even more in the future) using the "sharding" process[39].

Using its market power and influence, Facebook has the potential to deeply change monetary institutions, by creating a new way to exchange. Yet, money creation is a historical prerogative of sovereign nation states and unsurprisingly the reaction of the governments has been fearful. Indeed, the US Congress requests the Libra suspension with the following arguments: protection of individual data, trading and financial stability, and national security concerns related to cyber risks for the global economy. Libra's story is ongoing and it has to be written.

[39]This technique entails a "specific type of database setup where multiple partitions create many pieces of a database that are then referred to as shards". https://www.techopedia.com/

## 2.5 Conclusion

The purpose of this paper is to explain how the blockchain developed within informal communities has the potential to be adopted into organizations. The blockchain comes from a virtual informal community composed of many stakeholders that cooperate together in a consensus process designed to perform transactions between each other without requiring a third-party. Blockchain is an innovative object related to storing, sharing and exchanging information. Because of these features, we link the blockchain with a theoretical framework related to the organization theory and which refers to: (1) the transaction costs theory; (2) the agency theory; (3) the incomplete contracts theory; and (4) the alternative and cognitive approach of the firm. We find that blockchains solve different organizational management issues because of their main characteristics: transparent and instantaneous exchanges, decentralization, consensus-based mechanism, secured and immutable ledger (e.g, Table 2.3). The strengths and the weaknesses of this innovation challenge its appropriation by businesses because it has the potential to create value. Through an illustrated literature review, we study the blockchain according to a two-level dimension analysis from a community perspective. We present four cases of potential flexible blockchains based on the access rights of the miners' communities (permission) and the users' communities (openness). We highlight that the trend of evolution of blockchain practices begins with public permissionless blockchains (cryptocurrency ones) to private permissioned blockchains (formal and existing industries) with the potential to revolutionize the formal current institutions and governance.

This research has several implications.

First, the theoretical implications are to provide a theoretical framework for the blockchain based on the organization theory. The novelty of blockchain and its famous application to Bitcoin open a variety of perspectives for research in technical and computer sciences as well as in social sciences. The main contribution is to confront several potential theories (contractual and cognitive approaches) in the organizational perspective to find an appropriate theoretical framework. A second contribution is the analysis of this subject from a community perspective, which is an important aspect of the blockchain and very little studied in the management science literature. This article is to create a bridge between theory and practice, by proposing a theoretical framework for blockchain based on the organization theory, and by showing how this particular IT management tool coming from an outside informal community is appropriated by the existing organizations to create value.

Second, managerial implications arise from the nature and applications of the blockchain. The major advantage of blockchain is the expected savings for perishable (traceability) as well as non-perishable goods (exchange system such as Bitcoin). Therefore, the blockchain technology concerns any kinds of exchanges and aims to reorganize the exchanges between individuals. Concerning firms, blockchain use implies more collaboration and less hierarchy. Instead of focusing on transactions, managers can focus more on other stimulating missions such as leadership to motivate people in the firm. Employees can become an expert member of the company (Chartier-Rueg and Zweifel, 2017). Thanks to this leadership and the technology, investors may be more active, accounting could be in real-time and reflect more accurately the reality. Each stakeholder can be attributed the possibility to speak up by votes or idea suggestions which represent "innovative forms of self-governance" (Wright and DeFilippi, 2015). The use of blockchains may be a solution for firms that face difficulties to build a business model based on public web community to create value (Chanal and Caron-Fasan, 2010).

Finally, Wright and DeFilippi (2015) suggest cities based on blockchain in which citizens feels more involved and can vote using this technology. These authors go further and imagine extending this system to a "self-governing state". This contract can be a way to include individuals in the financial and monetary system (Wright and DeFilippi, 2015), (Larios-Hernandez, 2017). In general, excluded individuals prefer using cash, while services provided by fintechs and services based on blockchains would promote the use of safer alternative means of payment such as mobile phones. Especially, developing countries are interested in this technology related to their economic, social and political challenges (Kshetri, 2017). In South Africa, customers use Bitcoin to exchange money using their smartphones. Then, when excluded individuals wish to have access to loans, they may use informal and decentralized way, without any bank account. Blockchain is able to emphasize the role of micro-finance and of micro-insurance in developing countries. By extension, other services, either financial or not, can benefit from blockchains (Kewell et al., 2018). Since blockchain use is being developed in management, public policies raise the question of the effectiveness and the promotion to use this technology in companies as well as for customers' and citizens' rights. Concerning the later, public policies have first to regulate the use of blockchains so that this technology becomes more than a single tool but also a contract in itself. Two issues should be prioritized: the (non-)reversibility of transactions and the litigations in the execution of Smart Contracts. New jobs appear which mix programming and law competencies according to the execution of a blockchain-based contract (Wright and DeFilippi, 2015). New legal questions arise regarding the suitability of decentralization for every environment, the terms of contracts at any time and the legal status concerning the Decentralization Autonomous Organization structures. Generally speaking, to avoid fraud and illegal markets, blockchains require some kind of regulation and legal frame notably to set up responsibilities (Wright and DeFilippi, 2015). The question of the territory is also important. In the future, every government would establish its own regulation regarding blockchains. In a global world, national laws compete with each other, and in a virtual world, the lack of regulations may impede the development of blockchains (the Libra case). Thus, the creation of new international standards appears as a critical issue.

The main limits of this research are the lack of empirical evidences to confirm our analysis. Questionnaires and interviews with experts or companies that have implemented blockchains and to what extent could support our work and more precisely assess the importance of each of the advantages and disadvantages identified with respect to blockchain. Future research may focus on more specific applications of the blockchain such as the Initial Coin Offering (ICO) concept thus appear a new way of raise funds for new projects in the blockchain community. The number of ICOs is increasing in recent years (4,000) with heterogeneous projects. The related-information is scattered on different online databases. A potential work related to this phenomenon is to create a database about financial and human resources characteristics on ICOs to study the factors of their success. Research perspectives could also include studies on financial markets related to Bitcoin features given its popularity and also its high volatility.

## References


Akerlof, G. A. (1970). The market for "Lemons": Quality uncertainty and the market mechanism, *The Quarterly Journal of Economics* **84**(3): 488–500.

Alchian, A. A. and Demsetz, H. (1972). Production, information costs, and economic organization, *The American Economic Review* **62**(5): 777–795.

Allen, D. (2016). Discovering and developing the blockchain cryptoeconomy, *SSRN Elec. Journal* .

Amsden, Z., Arora, R., Bano, S., Baudet, M., Blackshear, S., Bothra, A., Cabrera, G., Catalini, C., Chalkias, K., Cheng, E., Ching, A., Chursin, A., Danezis, G., Giacomo, G. D., Dill, D. L., Ding, H., Doudchenko, N., Gao, V., Gao, Z., Garillot, F., Gorven, M., Hayes, P., Hou, J. M., Hu, Y., Hurley, K., Lewi, K., Li, C., Li, Z., Malkhi, D., Margulis, S., Maurer, B., Mohassel, P., de Naurois, L., Nikolaenko, V., Nowacki, T., Orlov, O., Perelman, D., Pott, A., Proctor, B., Qadeer, S., Rain, Russi, D., Schwab, B., Sezer, S., Sonnino, A., Venter, H., Wei, L., Wernerfelt, N., Williams, B., Wu, Q., Yan, X., Zakian, T. and Zhou, R. (2018). The libra blockchain, *White paper* .

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., Caro, A. D., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolic, M., Cocco, S. W. and Yellick, J. (2018). Hyperledger fabric: A distributed operating system for permissioned blockchains, *White paper* .

Angel, J. J. and McCabe, D. (2015). The ethics of payments: Paper, plastic, or bitcoin?, *Journal of Business Ethics* **132**(3): 603–611.

Arrivets, M. (2018). MONET: Mobile and ad hoc blockchains, *White paper* .

Benghozi, P.-J. (2008). Les communautés virtuelles : structuration sociale ou outil de gestion, *Entreprises et Histoire* **2**(43): 67–81.

Berle, A. and Means, G. (1932). *The Modern Corporation and Private Property*, Routledge Classics.

Biais, B., Bisière, C., Bouvard, M. and Casamatta, C. (2017). The blockchain folk theorem, *Working paper* **TSE-817**.

Blair, M. M. and Stout, L. A. (1999). A team production theory of corporate law, *Virginia Law Review* **85**(2): 247–328.

Bohr, J. and Bashir, M. (2014). Who use bitcoin? An exploration of the bitcoin community, *Conference: 2014 Twelfth Annual Conference on Privacy, Security and Trust* .

Bourguignon, A. and Jekins, A. (2004). Changer d'outils de contrôle de gestion ? De la cohérence instrumentale à la cohérence psychologique, *Finance Contrôle Stratégie* **7**(3): 31–61.

Brent Xu a, d. D. L., Cole, Z. and Blakely, N. (2018). EOS: An architectural, performance, and economic analysis, *White paper* .

Brown, J. S. and Duguid, P. (1991). Organizational learning and communities-of-practice: Toward a unified view of working, *Organization Science* **2**(1): 40–57.

Burnett, D., Coote, R., Nevile, C. and Noble, G. (2018). Enterprise ethereum alliance, enterprise ethereum client specification v2, *White paper* .

Buterin, V. (2014). DAOs, DACs, DAs and more: An incomplete terminology guide.
**URL:** *https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/*

Buterin, V. (2015a). A next generation smart contract and decentralized application platform, *Ethereum White Paper* .

Buterin, V. (2015b). On public and private blockchains.
**URL:** *https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/*

Carroll, J. M. and Bellotti, V. (2015). Creating value together: The emerging design space of peer-to-peer currency and exchange, *Conference Paper ACM Conference on Computer Supported Cooperative Work and Social Computing* .

Carson, B., Romanelli, G., Walsh, P. and Zhumaev, A. (2018). Blockchain beyon the hype: What is the strategy business value?, *Digital McKinsey* .

Castro, M. and Liskov, B. (1999). Practical byzantine fault tolerance, *Proceedings of the Third Symposium on Operating Systems Design and Implementation* **New Orleans**.

Catalini, C. and Gans, J. (2018). Some simple economics of the blockchain, *NBER Working Paper* .

Chanal, V. and Caron-Fasan, M.-L. (2010). The difficulties involved in developing business models open to innovation communities: The case of a crowdsourcing platform, *M@n@gement* **13**(4): 318–341.

Chandler, A. (1992). What is a firm? a historical perspective, *European Economic Review* **36**(2-3): 483–492.

Chartier-Rueg, T. C. and Zweifel, T. D. (2017). Blockchain, leadership and management: Business as usual or radical disruption?, *EUREKA: Social and Humanities* (4): 76–110.

Chaum, D. (1983). Blind signatures for untraceable payments, *Advances in Cryptology Proceedings of Crypto* **82**(3).

Chen, Y. (2018). Blockchain tokens and the potential democratization of entrepreneurship and innovation, *Blockchainberkeley.blog* .

Chris Berg, S. D. and Potts, J. (2017). Blockchain industrialise trust, *SSRN Elec. Journal* .

Ciborra, C. U. (1997). Do profundis? Deconstructing the concept of strategic alignement, *Scandinavian Journal of Information Systems* **9**(1): 67–82.

Ciborra, C. U. (1999). Notes on improvisation and time in organization, *Accounting Management and Information Technology* **9**(2): 77–94.

Civitarese, J. and Mendes, L. (2018). Bad news, technical development and cryptocurrencies stability, *SSRN Elec. Journal* .

Coase, R. (1937). The nature of the firm, *Economica New Series* **4**(16): 386–405.

Collomb, A. and Sok, K. (2016). Blockchain and distributed ledger technologies (DLT): What impact on financial markets ?, *Opinions and debats* **15**.

Cong, L. W. and He, Z. (2017). Blockchain disruption and smart contracts, *SSRN Elec. Journal* .

Coriat, B. and Weinstein, O. (2010). Les théories de la firme entre “contrats” et “compétences”, *Revue d’économie industrielle* **1-2**(129-130): 57–86.

Cyert, J. and March, R. (1963). *A Behavioral Theory of the Firm*, Englewood Cliffs.

Cyert, R. and Kamien, M. (1998). Behavioral rules and the theory of the firm, *in* C. Rowley (ed.), *Readings in Industrial Economics*, Palgrave Macmillan, chapter 6, pp. 91–102.

Dahlander, L. and Magnusson, M. G. (2005). Relationships between open source software companies and communities: Observations from Nordic firms, *Research Policy* **34**(4): 481–493.

Davidson, S., DeFilippi, P. and Plotts, J. (2018). Blockchain and the economic insitutions of capitalism, *Journal of Institutional Economics* **14**(4): 639–658.

D’avolio, G., Gildor, E. and Shleifer, A. (2002). Technology, information production, and market efficiency, *Economic Policy for the Information Economy. Federal Reserve Bank of Kansas City* .

DeFilippi, P. and Mauro, R. (2014). Ethereum: The decentralised platform that might displace today’s institutions, *Internet Policy Review - Journal on Internet Regulation* .

Detchessahar, M. and Journé, B. (2007). Une approche narrative des outils de gestion, *Revue française de gestion* **5**(174): 77–92.

Dierksmeier, C. and Seele, P. (2018). Cryptocurrencies and business ethics, *Journal of Business Ethics* **152**(1): 1–14.

Dominguez-Péry, C. (2011). *Valeurs et outils de gestion, de la dynamique d’appropriation au pilotage*, Hermes Science Publications.

Fama, E. (1980). Agency problems and the theory of the firm, *Journal of Political Economy* **88**(2): 288–307.

Figuet, J.-M. (2016). Bitcoin et blockchain : quelles opportunités ?, *Revue d'économie financière* **123**(3): 325–338.

Foss, N. J. (1996). Capabilities of the theory of the firm, *Revue d'économie industrielle* **77**(3): 7–28.

Foss, N. J. and Klein, P. G. (2005). The theory of the firm and its critics: A stocktaking and assessment, *CORI Working Paper* (3).

Füller, J., Matzler, K. and Hope, M. (2008). Brand community members as a source of innovation, *The Journal of Product Innovation Management* **25**(6): 608–619.

Garg, M. (2019). Relation between searches for bitcoin and searches for the characteristics of bitcoin users in canada.

Grossman, S. J. and Hart, O. D. (1986). The costs and benefits of ownership: A theory of vertical and lateral integration, *Journal of Political Economy* **94**(4): 691–719.

Guillemot, D. and Kocoglu, Y. (2010). Diffusion des outils dans les entreprises françaises. Une approche synthetique, *Réseaux* **4**(162): 165–197.

Guo, Y. and Liang, C. (2016). Blockchain application and outlook in the banking industry, *Financial Innovation* **2**(24).

Harris-Braun, E., Luck, N. and Brock, A. (2018). Holochain scalable agent-centric distributed computing, *White paper* .

Hart, O. D. and Moore, J. (1988). Incomplete contract and renegociation, *Econometrica* **56**(4): 755–785.

Hart, O. D. and Moore, J. (1990). Property rights and the nature of the firm, *Journal of Political Economy* **98**(6): 1119–1158.

Hatchuel, A. and Weil, B. (1992). *L'expert et le systeme : gestion des savoirs et metamorphose des acteurs dans l'entreprise industrielle ; suivi de Quatre histoires de systemes-experts*, Economica.

Hienerth, C. and Lettl, C. (2011). Exploring how peer communities enable lead user innovations to become standard equipment in the industry: Community pull effects, *The Journal of Product Innovation Management* **28**(s1): 175–195.

Hileman, G. and Rauchs, M. (2017). Global cryptocurrency benchmarking study, *White paper* .

Hopf, S., Loebbecke, C. and Avital, M. (2018). Blockchain technology impacting property rights and transaction cost regimes, *Working Paper* .

Iansiti, M. and Lakhani, K. R. (2017). The truth about blockchain, *Harvard Business Review* .

Jain, A. and Thiertart, R.-A. (2013). Capabilities as shift parameters for the outsourcing decision, *Strategic Management Journal* **35**(12): 1881–1890.

Jensen, M. C. and Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure, *Journal of Financial Economics* **3**(4): 305–360.

Joffre, O. and Trabelsi, D. (2018). Le crowdfunding, concepts, réalités et perspectives, *Revue française de gestion* **4**(273): 69–82.

Kang, K., Choo, J. and Kim, Y. (2019). Whose opinion matters? Analyzing relationships between bitcoin prices and user groups in online community, *Social Science Computer Review* .

Kewell, B., Adams, R. and Parry, G. (2018). Blockchain for good?, *Strategic Change* **26**(5): 429–437.

Kim, T. (2017). On the transaction cost of bitcoin, *Finance Research Letters* **23**: 300–305.

Kshetri, N. (2017). Potential roles of blockchain in fighting poverty and reducing financial exclusion in the global south, *Journal of Global Information Technology Management* **20**(4): 201–204.

Lamberti, F., Gatteschi, V., Demartini, C., Pranteda, C. and Santamaria, V. (2017). Blockchain or not blockchain, that is the question of the insurance and other sectors, *IT Professional* **PP**(99).

Lannquist, A. (2018). Blockchain in enterprise: How companies are using blockchain today, *Blockchainberkeley.blog* .

Larios-Hernandez, G. J. (2017). Blockchain entrepreneurship opportunity in the practices of the unbanked, *Business Horizons* **60**(6): 865–874.

Lavastre, O. (2001). Les coûts de transactions et Olivier E. Williamson : retour sur les fondements, *Xieme Conferance de l'Association Internationale de Management Strategique* .

Lee, L. (2016). New kids on the blockchain: How bitcoin's technology could reinvent the stock market, *Hastings Business Law Journal* **12**(2).

Libra, A. (2019). An introduction to Libra, White Paper.
**URL:** `https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US.pdf`

MacDonald, T., Allen, D. and Potts, J. (2016). Blockchains and the boundaries of self-organized economies: Predictions for the future of banking, *Banking Beyond Banks and Money* pp. 279–296.

March, J. and Simon, H. (1993). *Organizations*, Wiley-Blackwell.

Mintzberg, H. (1973). Strategy-making in three modes, *California Management Review* **16**(2): 44–53.

Moidson, J.-C. (1997). Du mode d'existence des outils de gestion. Les instruments de gestion à l'epreuve de l'organisation, *Politiques et Management Public* **15**(4): 177–178.

Morgan, J. (2018). Quorum whitepaper, *White paper* .

Munksgaard, R. and Demant, J. (2016). Mixing politics and crime – The prevalence and decline of political discourse on the cryptomarket, *International Journal of Drug Policy* **35**: 77–83.

Myers, S. C. and Majluf, N. S. (1984). Corporate financing and investment decisions when firms have information that investors do not have, *Journal of Financial Economics* **13**(2): 187–221.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system, *White paper* .

Nelson, R. and Winter, S. (1982). *An Evolutionary Theory of Economic Change*, Harvard University Press.

O'Dwyer, K. J. and Malone, D. (2014). Bitcoin mining and its energy footprint, *ISSC CIICT* .

Orlikowski, W. J. (1992). The duality of technology: Rethinking the concept of technology in organizations, *Organization Science* **3**(3): 398–427.

Ostrom, E. (1990). *Governing the Commons: The Evolution of Institutions for Collective Action*, Cambridge University Press.

Penrose, E. (1959). *The Theory of the Growth of the Firm*, Wiley.

Pietrewicz, L. (2018). Token-based blockchain financing and governance: A transaction cost approach, *Working Paper* .

Prahalad, C. K. and Hamel, G. (1990). The core competence of the corporation, *Harvard Business Review* .

Reijers, W., O'Brolchain, F. and Haynes, P. (2016). Governance in blockchain technologies and social contract theories, *Working Paper* .

Ron, D. and Shamir, A. (2018). Quantitative analysis of the full bitcoin transaction graph, *Financial Cryptography and Data Security* pp. 6–24.

Rozas, D., Tenorio-Fornés, A., Diaz-Molina, S. and Hassan, S. (2018). When ostrom meets blockchain: Exploring the potentials of blockchain for commons governance, *SSRN Elec. Journal* .

Ruggles, R. (1997). Tools for knowledge management: An introduction, *in* R. Ruggles (ed.), *Knowledge Management Tools*, Butterworth-Heinemann.

Ruzzier, C. A. (2009). Asset specificity and vertical integration: Williamson's hypothesis reconsidered, *Working Paper-Harvard Business School* (9-119).

Schmitz, R., Daniels, A., Migchelsen, M., Stam, S. and Broersma, M. (2018). LTO network, visionary paper, *White paper* .

Schwartz, D., Youngs, N. and Britto, A. (2015). The Ripple protocol consensus algorithm, *White Paper* .

Shanaev, S., Shuraeva, A., Vasenin, M. and Kuznetsov, M. (2018). Cryptocurrency value and 51% attacks: Evidence from event studies, *SSRN Elect. Paper* .

Shermin, V. (2017). Disrupting governance with blockchains and smart contracts, *Strategic Change* **26**(5): 499–509.

Simon, H. (1988). *Administrative behavior: A Study of Decision making Processes in Administrative*, Macmillan.

Szabo, N. (1997a). Formalizing and securing relationships on public networks, *First Monday - Peer-rewieved Journal of the Net* **2**(9).

Szabo, N. (1997b). The idea of smart contracts, *White Paper* .
**URL:** http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html

Szabo, N. (1998). Secure property titles with owner authority, *White Paper* .
**URL:** http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/securetitle.html

Tapscott, D. and Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, New York: Penguin Random House.

Tapscott, D. and Tapscott, A. (2017). How blockchain will change organizations, *MIT Sloan Management Review* **58**(2): 10–13.

Tripier, P. (1994). Hatchuel (armand), weil (benoit) l'expert et le systeme suivi de quatre histoires de systemes experts, *Revue française de sociologie* **35**(1): 137–139.

Tschorsch, F. and Scheuermann, B. (2016). Bitcoin and beyond:a technical survey on decentralized digital currencies, *IEEE Communications Surveys & Tutorials* **18**(3): 2084–2123.

Vukolić, M. (2015). The quest for scalable blockchain fabric: Proof-of-Work vs. BFT replication, *Open Problems in Network Security* pp. 112–125.

White, L. (2015). The market for cryptocurrencies, *Cato Journal* .

Wilkin, C. L. and Chenhall, R. H. (2010). A review of IT governance: A taxonomy to inform accounting information systems, *Journal of Information Systems* **24**(2): 107–146.

Wilkof, M. (1989). Organisational culture and decision making: A case of consensus management, *R&D Management* **19**(2): 185–200.

Williamson, O. (1975). *Markets and Hierarchies: Analysis and Antitrust Implications*, Free Press a division of Macmillan.

Williamson, O. (1981). The economics of organization: The transactions cost approach, *American Journal of Sociology* **87**(3).

Williamson, O. (1985). *The Economic Institutions of Capitalism: Firms, Markets and Relational contracting*, Free Press a division of Macmillan.

Williamson, O. E. (1979). Transaction-cost economics: The governance of contractual relations, *The Journal of Law and Economics* **22**(2): 232–261.

Wood, G. (2014). Ethereum: A secure decentralized generalised transaction ledger, *White paper* .

Wright, A. and DeFilippi, P. (2015). Decentralized blockchain technology and the rise of lex cryptographia.

Wust, K. and Gervais, A. (2017). Do you need a blockchain?, *Crypto Valley Conference on Blockchain Technology* .

Yelowitz, A. and Wilson, M. (2015). Characteristics of bitcoin users: An analysis of google search data, *Applied Economics Letters* **22**(13): 1030–1036.

Yermack, D. (2017). Corporate governance and blockchains, *Review of Finance* **21**(1): 1–31.

## Chapter 3

# On the nature and financial performance of Bitcoin

Bitcoin is a major cryptocurrency, calling financial stability into question due to its high returns for investors as well as its high levels of risk. The objective of this article is to raise the question about the true nature of Bitcoin and to study empirically its performance. After questioning the nature of Bitcoin as a currency and justifying its asset nature, this research aims to test empirically its performance using traditional models such as the CAPM and Fama-French 3-Factors models. We use daily data from September 2010 to December 2016 and find that, while integrating Bitcoin in portfolio highly improves its diversification, it also provides positive and significant risk-adjusted returns in the World, European and Asia-Pacific regions. These results are robust to variables commonly used for assessing investors' behavior.

## 3.1 Introduction

Bitcoin is a cryptocurrency, and therefore a part of the so-called ”electronic currency” family (Nakamoto, 2008). On January 4th, 2017, the Bitcoin price was equal to $1,126, thus reaching the threshold of $1,000 for the second time in its history. Incredibly unexpected, and even more so, the price raised to more than $10,000 one year after reaching $19,395.85 on December 18th, 2017, Figure 3.1 - *Bitcoin market price*.

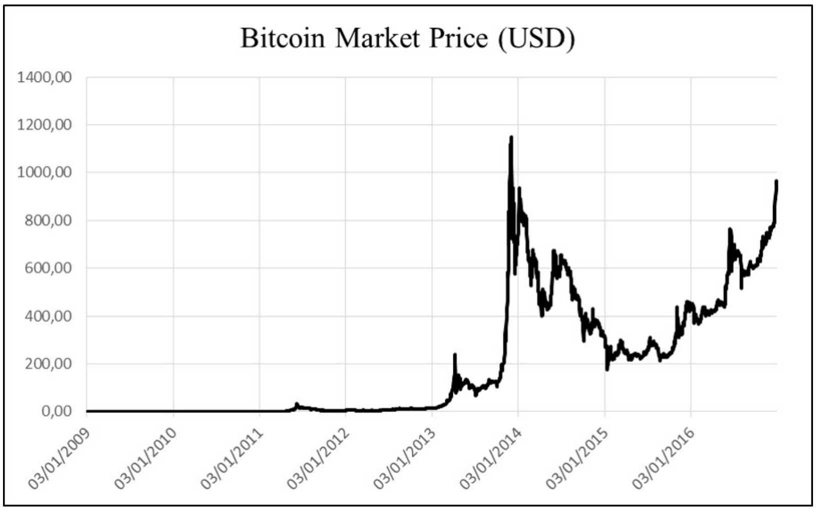


**Figure 3.1 Bitcoin market price**
This figure shows the Bitcoin Market Price expressed in US dollars (USD) over the period January 2009 – December 2016.

Electronic currencies, which are recorded on a computer or other electronic devices, may take two forms: digital cash and cryptographic currency. The former is a simple digital version of physical money. The latter, which is studied in this article, uses cryptographic principles to ensure security. This type of currency is developed in a decentralized system that uses the blockchain technology.

Whilst Bitcoin has common characteristics with currencies (Bitcoin is indeed an exchange medium), and with gold (the monetary creation of Bitcoin looks like that concerning gold), we hereafter consider Bitcoin as a financial contract, and more specifically common stock. Bitcoin indeed has specific economic and legal profiles, risk-return characteristics, and its liquidity bring it close to the common stock family (Glaser et al., 2014), (Baur et al., 2016).

The objective of this article is to raise the question about the true nature of the Bitcoin and to study empirically the Bitcoin's performance. Figure 3.2 - *Research questions of the second study* presents these sub-research questions, their methodologies and main findings. The justification of studying the performance of Bitcoin relies on the fact that it is a relatively young, risky financial innovation, not yet well assimilated by the market. Bitcoin is affected by informational asymmetries between investors, mainly because many of them do not understand the technology behind it. Consequently, the market value of this financial contract may differ from its true value, that is, the value on a market without informational asymmetries, thus providing opportunities to earn positive risk-adjusted returns. In line with this view, the objective of some mutual funds is to track Bitcoins. This suggests the possibility of earning superior risk-adjusted returns by trading this financial contract.

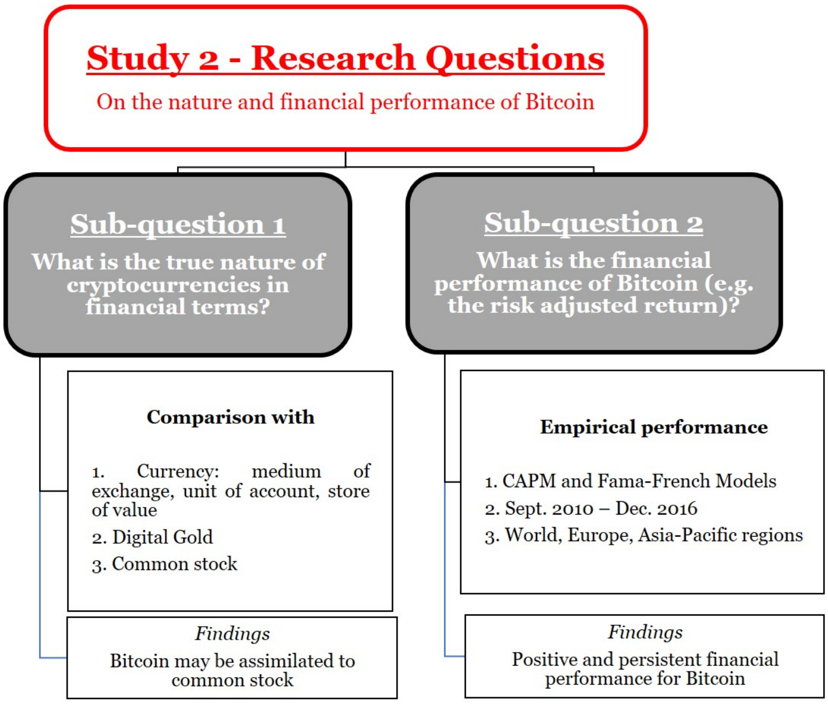


**Figure 3.2 Research questions of the second study**
This figure presents the sub-research questions of the second study.

In most existing articles, the performance of Bitcoin is assessed by using simple measures, such as the Sharpe ratio (Brière et al., 2015), (Burniske and White, 2017). The problem with this measure is that it does not take into account the huge potential for portfolio diversification with Bitcoins. Being highly uncorrelated with most existing assets, most of the Bitcoin variability can be diversified away, which strengthens its performance. Based on this important aspect, and on the premise that Bitcoin has the nature of a financial contract, our paper is the first, to our knowledge, that attempts to measure its performance by using models such as the capital asset pricing model (CAPM), which uses the market portfolio as a benchmark, and also the three-factor (Fama and French, 1992) model, hereafter FF, and also other extensions of these models by considering other factors related to Bitcoin.

To take into account the international dimension of Bitcoin, we use the global market portfolio as a benchmark and the global versions of the FF factors (Fama and French, 2012).

To test Bitcoin performance, we estimate the risk-adjusted return ($\alpha$) with these models for the period between September 22$^{nd}$, 2010 and December 30$^{th}$, 2016 for different regions: World, Europe, Asia-Pacific and China. In addition, we take into consideration the market sentiment variable in our models to check the robustness of our results and to take into account behavioural aspects that are plausibly related to Bitcoin.

The rest of this chapter is organised as follows. Section 2 presents Bitcoin characteristics. Section 3 describes the models used to assess Bitcoin performance and the data sets used in our study. Section 4 discusses the results. Section 5 proposes some robustness tests related to the violations of the regression model assumptions, mainly the normality of errors, and also to some behavioural aspects. Section 6 presents the conclusion.

## 3.2 About the nature of Bitcoin

The nature of Bitcoin is subject of debate. Academics and professionals suggest various definitions and do not always agree on whether Bitcoin is a currency, a commodity, a “safe” investment such as gold, a debt contract or common stock. In this section, we present Bitcoin characteristics, and we attempt to show that Bitcoin has also the characteristics of an asset, more precisely common stock (Glaser et al., 2014), (Baur et al., 2016).

### 3.2.1 What is Bitcoin?

Bitcoin is basically a payment system that is independent from any government and operates without a third party (such as a Central Bank). Any participant in this system may check the behavior of other participants to ensure the reliability of transactions and system stability. In other words, the well-functioning responsibility is not assumed by a third party. All participants have the possibility to know the transactions made by everyone. However, the identity of participants remains pseudo-anonymous, in the sense that the identity is hidden by a pseudonym, the Bitcoin "address", which is a number sequence.

There are three ways to obtain Bitcoins: exchanging money, selling goods and services or mining. The first two ways, which are exchanging money and selling goods or services through e-businesses that accept Bitcoin units, make Bitcoin behave like a fiat currency. However, a fundamental aspect that makes Bitcoin behave like a financial asset is that one may create Bitcoins through the mining process, whose underlying technology is named "blockchain". This is a secured and distributed database that contains the history of transactions. The technology may be considered as a ledger that stores all exchanges realised on the network (Nakamoto, 2008), (Tschorsch and Scheuermann, 2016). This ledger is composed of blocks linked to each other. Each block contains a transaction list of some exchanges. Special users, named miners, create a block locally by choosing different pending transactions. Then, each new block is drawn by a mathematical process, comparable to Sudoku. When a miner finds the grid solution, he/she wins a predetermined number of Bitcoins, and other participants must start again the competition with another grid. Grid difficulty is adjusted so that miners may find the grid solution with an interval of 10 min on average between each discovery (Antonopoulos, 2015).

Miners are compensated for their work of integrating transactions to the blockchain and making the system reliable. They obtain a number of Bitcoins when they succeed to add a block to the blockchain. This compensation is predefined in advance and the number of released Bitcoins decreases with time because the maximum number of Bitcoins is capped at 21 million.

### 3.2.2 Is Bitcoin a currency ?

From an economic perspective, the question whether Bitcoin has common characteristics with currency is subject to debate. According to its basic properties, a currency should be a convenient medium of exchange, a stable unit of account and a durable store of value (Grant, 2014). Bitcoin is a medium of exchange, in the sense that a high number of businesses, such as Dell, Microsoft or PayPal, are willing to accept Bitcoins (Figuet, 2016).

The popularity of using Bitcoins is based on the user's anonymity and the system transparency (because it uses the blockchain technology). However, participants could be reluctant to participate in this new system because Bitcoin has no legal basis; companies make the choice to use Bitcoin or not; the fixed costs of adopting this technology are high (sophisticated technical knowledge is needed); and there are network externalities effects (if few businesses accept Bitcoin, few consumers may accept them, which in turn implies that few companies decide to accept them). Resolving this "vicious circle" is difficult because Bitcoin is not regulated by an institution, and there is no possibility to make loans on the market (Kancs et al., 2015). Empirical studies confirm the controversial property of "medium of exchange" based on the fact that users do not entirely turn to Bitcoin for this property (Baur et al., 2016).

Bitcoin may be considered to some extent as a "unit of account". However, merchants do not display prices in Bitcoin for two reasons. First, its supply is inelastic (a Bitcoin price of a given product needs many digits after the comma). Second, volatility does not ensure price stability. Because of high volatility, merchants are forced to change frequently the price of their products. So, prices are usually displayed in US dollars and are then converted in Bitcoins at the time when the transaction takes place (Figuet, 2016).

Finally, whilst Bitcoin has features that make it behave like a "store of value", the possible cybersecurity risks reduce trust in this currency. The trade-off between inflation and deflationary pressure, as well as the unstable purchasing power make it difficult to consider Bitcoin as a store of value.

To conclude, Bitcoin is different from traditional money because it does not fully respect the fiat currency properties, and in particular, there is no issuer responsible for it. In fact, Bitcoin is governed by a protocol run by a network of computers that are distributed around the World; government monetary policies have no direct impact on it.

In economics, there are different perspectives related to a currency. Another point of view is to see currency through institutionalist economics as a "unit of account". Based on this, Bitcoin could be considered as a "currency" in the sense of money being a "social institution" (Lakosmki-Laguerre and Desmedt, 2015).

### 3.2.3 Is Bitcoin "digital" gold or cash ?

Some researchers consider the possibility that Bitcoin acts like a commodity, more precisely as gold, for some reasons: supply is limited, meaning a weak inflation rate; monetary creation is based on the "mining" process; there is no control by any government; and Bitcoin acts as a medium of exchange (Dyhrberg, 2016a), (Dyhrberg, 2016b). Precious commodities such as gold are relatively safe, and Bitcoin may often play a role of safe investment (Bouri et al., 2016). For example, after the Cyprus crisis in 2012-2013, some depositors exchanged euros for Bitcoins because of the bankruptcy of banks and also because of increased taxes on deposits. The second peak at $1,000 was linked to the international context in both developed and emerging countries. Chinese depositors turned toward Bitcoin because of the Yuan drop and Chinese restrictions on capital outflows (this trend was accelerated by Donald Trump's election in the USA). Likewise, unstable monetary policies in emerging countries (inflation in Venezuela, demonetization in India, liquidity crisis in Zimbabwe) encouraged local depositors to turn to Bitcoin. Empirically, Bitcoin appears to be a weak safe investment reserved to some special cases but not during financial crises (Baur et al., 2016), (Bouri et al., 2016).

While Bitcoin may act as a safe investment in some cases, we can observe major differences with precious commodities such as gold. First, Bitcoin is capped at 21 million and the release of new Bitcoins is divided by two approximatively every four years until the maximum number of Bitcoins is reached. However, the supply for gold is not known. Moreover, even if the price of Bitcoin increases, its capitalization ($117,353,600,811 on November 2017[1]) is much lower than for gold ($7,747,981,667,403 on November 2017[2]). Second, the price of Bitcoin is independent from that of gold. The factors affecting the

[1]https://coinmarketcap.com
[2]http://onlygold.com

value of these two assets are different. Finally, gold (or any commodity) has physical shape, whilst Bitcoin possesses a virtual one. An alternative complementary category is proposed by Selgin, a category named "Synthetic commodity money" that is both commodity-money and fiat money (Selgin, 2015). In our case, Bitcoin could be compared to gold for the former and to dollar for the later (Baur et al., 2016). Dyhrberg (2016a) and Dyhrberg (2016b) test empirically the relationship between Bitcoin and gold/dollar. Bitcoin appears to be positioned between gold (store of value) and dollar (medium of exchange). Finally, Bitcoin could also be assimilated to cash or to a cash equivalent. But a cash equivalent implies that the asset must be highly liquid and convertible into a known amount of cash. Bitcoin is convertible, but it is not enough liquid to be considered as cash equivalent. Bitcoin cannot be deposited into banks and cannot be withdrawn using ATM (Raiborn and Sivitanides, 2015).

### 3.2.4 Bitcoin as common stock

While Bitcoin does not fully conform to the criteria of medium of exchange, store of value, or unit of account, the academic literature considers more and more the alternative view that Bitcoin acts as an asset (Yermack, 2015). Amongst various assets, the similarity between Bitcoin and common stock, which is the argument that we put forward in this paper, is justified by its high risk–high reward profile. Owning Bitcoins implies owning a portion of (1) the intangible asset represented by a specific technology, blockchain, and (2) of the human capital represented by experts running code and using mathematical procedures in order to enhance the credibility of the system. Bitcoin may therefore be considered as an investment that generates benefits in the same way as common stock.

Some empirical studies implicitly consider Bitcoins as a financial contract because they test diversification possibilities with Bitcoin or assess its performance through performance measures used for financial contracts, such as the Sharpe ratio (Bouri et al., 2016), (Burniske and White, 2017). Glaser et al. (2014) show that users are not mainly interested in Bitcoin as an alternative transaction system for paying goods or services, but rather as an alternative investment vehicle for transaction purposes, mostly for speculation. Two results contribute to this view. First, the interest of users influences the Bitcoin's volume traded at the exchange but has no effect on the volume within the Bitcoin system. Second, Bitcoin returns react on events related to the Bitcoin's security and infrastructure. While Bitcoin seems to be mainly affected by positive events such as new exchange launches or legal successes, it is also affected by negative events such as system bugs, thefts, hacks or exchange breakdown. In 2015, two mutual funds have been created to track Bitcoins for investors: Bitcoin Investment Trust and ARK Investment Management. Bitcoin Investment Trust (BIT) works as an exchange trade fund (ETF) and tracks Bitcoin, whilst ARK Investment Management creates two innovation funds which integrate the first one (BIT). The similarity between Bitcoin and financial contracts is also supported by the US Internal Revenue Service (IRS) in 2014[3]. IRS considers Bitcoin as property, and its holders are considered as market investors. After the DAO case[4], in 2017, the SEC announced that tokens linked to this project should have been considered as securities (common stocks) because the objective of these tokens is to generate earnings for investors taking risks to support the project.

## 3.3 Performance models

Existing academic and professional studies assess Bitcoin performance mostly with simple measures such as the Sharpe ratio, which adjust returns for total (specific and diversifiable) risk.

$$SharpeRatio = \frac{R_p - R_f}{\sigma_p} \tag{3.1}$$

The volatility of Bitcoin being very strong, this measure potentially underestimates performance. The low correlation of Bitcoin with other existing assets and currencies implies a huge potential for diversification, which needs to be accounted for in performance measures. Furthermore, the international dimen-

[3]ttps://www.irs.gov/pub/irs-drop/n-14-21.pdf

[4]DAO is the first "Decentralized Autonomous Organization" which is "an organization operating through a computer program that provides rules of governance to a community. These rules are transparent and immutable because they are written in the blockchain" according to blockchainInfo. DAO was created in 2016 with the objectives of crowdfunding using the Ethereum platform (the second payment platform which provides both a cryptocurrency, named Ether, and a blockchain platform). In a short period (four weeks), the project involved 20,000 participants and reached $160m. A failure in the code provoked a huge attack by hackers, which implied the closure of the structure.

sion of Bitcoin is another important aspect that needs to be integrated into a performance analysis.

We estimate performance relative to the traditional CAPM and international benchmarks in order to take into consideration diversification effects.

The first traditional model considered in this paper is the CAPM model:

$$E(R_i) = R_f + \beta \times [E(R_m) - R_f] \tag{3.2}$$

where $E(R_i)$ is the expected return of the common stock, $R_f$ is the risk-free rate, $E(R_m)$ the expected market return, and $[E(R_m) - R_f]$ measures the expected excess rate of return. The empirical specification of this model is:

$$R_t - R_{f,t} = \alpha + \beta \times (R_{m,t} - R_{f,t}) + \epsilon_t \tag{3.3}$$

where $R_t$ is the Bitcoin's return during period t, $R_{f,t}$ is the risk-free rate considered as the one-month T-Bill return, $R_{m,t} - R_{f,t}$ is the return of the market's portfolio proxy in excess of the risk-free rate, and $\epsilon_t$ is the disturbance term.

In addition, we estimate performance relative to the (Fama and French, 1992) three-factor model, which is widely used to assess the performance of financial contracts, such as the performance of actively managed portfolios. The use of common-stock-based indices to assess performance is justified by the similarities of Bitcoin with common stock, as argued previously.

$$R_t - R_{f,t} = \alpha + \beta_1 \times (R_{m,t} - R_{f,t}) + \beta_2 \times SMB_t + \beta_3 \times HML_t + \epsilon_t \tag{3.4}$$

where the two added factors, $SMB_t$ (Small Minus Big) and $HML_t$ (High Minus Low) are the returns of the zero-investment factor-mimicking portfolios for size and book-to-market (B/M) equity as proposed by (Fama and French, 1992).

The $SMB$ (Small Minus Big) factor is the average return on 3 small portfolios minus the average return of three big portfolios , based on the firm's market capitalization ("size premium"). The underlying explanation, which is of empirical nature, is that smaller firms tend to outperform large firms. The $HML$ (High Minus Low) factor is the average return on two value portfolios (high book-to-market) minus the average return on two growth portfolios ("value premium"). The underlying empirical explanation is that firms with higher book-to-market tend to outperform firms with lower book-to-market. Both variables are the results of six value-weight portfolios constructed based on size and book-to-market: two groups according to market capitalization: big and small; three groups according to B/M: value, neutral and growth.

$$SMB = \frac{SV + SN + SG}{3} - \frac{BV + BN + BG}{3} \tag{3.5}$$

$$HML = \frac{SV + BV}{2} - \frac{SG + BG}{2} \tag{3.6}$$

Where $SV$ is Small Value, $SN$ is Small Neutral, $SG$ is Small Growth, $BV$ is Big Value, $BN$ is Big Neutral and $BG$ is Big Growth.

We also use the return on $Gold$ and on $Bonds$ as additional factors in our performance models, as it is common in the existing literature. The specifications of the third model is as follows:

$$\begin{aligned} R_t - R_{f,t} = \alpha + \beta_1 \times (R_{m,t} - R_{f,t}) + \beta_2 \times SMB_t + \beta_3 \times HML_t \\ + \beta_4 \times R_{Gold,t} + \beta_5 \times R_{Bonds,t} + \epsilon_t \end{aligned} \tag{3.7}$$

Where $R_{Gold,t}$ is the return on $Gold$, $R_{Bonds,t}$ is the return on $Bonds$.

The risk-adjusted return generated by Bitcoin is measured by the constant coefficient ($alpha$) from estimating the models specified by equations 3.3, 3.4, 3.7. We consider global benchmarks because Bitcoin is used across the World and is not linked to a special country. In their paper published in 2012, Fama and French apply their three- and five-factor models at an international level. They construct global portfolios using global size and B/M breakpoints for four regions to allocate the stocks of these regions to size and B/M portfolios (Fama and French, 2012).

The data for benchmarks' returns are taken from the Kenneth R. French's website for both Global, European and Asia-Pacific analyses[5]. The World region is composed of Australia, Austria, Belgium, Canada, Switzerland, Germany, Denmark, Spain, Finland, France, Great Britain, Greece, Hong Kong, Ireland, Italy, Japan, Netherlands, Norway, New Zeeland, Portugal, Sweden,

[5]http://mba.tuck.dartmouth.edu/pages/faculty/ken.french/

Singapore, and the United States. The European region contains Austria, Belgium, Switzerland, Germany, Denmark, Spain, Finland, France, Great Britain, Greece, Ireland, Italy, Netherlands, Norway, Portugal, and Sweden. The Asian-Pacific region refers to Australia, Hong Kong, New Zealand and Singapore. Data for $Gold$ and bond indices benchmarks ($Gold$ bullion USD/troy ounce rate, and Pimco Invest Grade Corporate Bond Exchange-Traded Fund, respectively) come from the Datastream database. Finally, Bitcoin prices come from the blockchain.info (now blockchain.comb website[6].

We also replicate our analyses for the Chinese market, where more than 90 percent of the transactions on Bitcoin occur. We construct the size and B/M factor-mimicking portfolios on the Chinese market by following the same procedure as the one used by Fama and French for constructing their factor-mimicking portfolios on the US market (Wang and Xu, 2004),(Meng and Ju, 2013), (Cheung et al., 2014), (Xu and Zhang, 2014), (MSCI, 2016). The data are extracted from Datastream, precisely the Shenzhen market. $R_{Mkt} - R_f$ is computed with the MSCI Index China related to the market and $R_f$ is the Chinese Government Bond 10 year. In addition to the $SMB$ and $HML$ factors, MSCI factors are equally tested in the regressions such as the MSCI China Small Cap - MSCI China Large Cap as a proxy of the $size$ and the MSCI China Value Local - MSCI China Growth Local is a proxy for the $value$. We obtain:

$$R_t - R_{f,t} = \alpha + \beta_1 \times (R_{m,t} - R_{f,t}) + \beta_2 \times size_t + \beta_3 \times value_t + \epsilon_t \quad (3.8)$$

$$\begin{aligned} R_t - R_{f,t} = \alpha + \beta_1 \times (R_{m,t} - R_{f,t}) + \beta_2 \times size_t + \beta_3 \times value_t \\ + \beta_4 \times R_{Gold,t} + \beta_5 \times R_{Bonds,t} + \epsilon_t \end{aligned} \quad (3.9)$$

We estimate the above-specified models over the period from September 22$^{nd}$, 2010 to December 30$^{th}$, 2016. The starting date is relatively recent because Bitcoin is a recent innovation. We use daily returns in order to have a sufficient number of observations for our regressions, and thus obtain 1,638 daily observations over the specified period.

[6]https://www.blockchain.com

## 3.4 Results

### 3.4.1 Univariate results

The market price of Bitcoin over the analysis period presented in Figure 3.1 shows its incredible fluctuation[7] implying a huge risk-return coupling. Indeed, Table 3.1 - *Descriptive statistics* presents descriptive statistics for Bitcoin, common stock indices of selected countries, MSCI indexes (for the World, Europe and Asia-Pacific regions), commodities indexes (oil, $Gold$ and commodity index), the bond index (Pimco) and currencies (dollar index, Yen, euro and Yuan). The Bitcoin's risk-return profile is, not surprisingly, very atypical, with a mean annualized return of 568.82 percent for a standard deviation of 111.69 percent and a high spread between minimum and maximum returns. These results are similar to those found in the literature (Brière et al., 2015), (Baur et al., 2016), (Bouri et al., 2016). For comparison, the S&P 500 exhibits an annual return of 19.74 percent for a standard deviation of 17.73 percent. The dollar index has a mean return of 25.15 per cent for a standard deviation of 30.43 percent and $Gold$ has a mean return of –2.14 percent for a standard deviation of 20.50 percent.

We also note that Bitcoin returns exhibit a positive skewness of 0.68, meaning they are skewed to the right. Almost all the other variables exhibit a negative skewness, except oil, and two currencies, Yen and Yuan. Note that existing empirical studies on Bitcoin obtain positive or negative skewness coefficients. Furthermore, Bitcoin has a heavy-tailed distribution with a kurtosis of 15.98 which indicates a higher number of tail events in Bitcoin returns (Baur et al., 2016). This result is similar to others found in the literature. The empirical distribution of the returns is presented in Figures 3.3 - *Bitcoin return analysis – Histogram* and 3.4 - *Bitcoin return analysis – QQplot*. Normality tests such as Shapiro–Wilk, Kolmogorov Smirnov, Cramer Von Mises and Anderson Darling, presented in Table 3.2 - *Bitcoin return normality test*, reject the null hypothesis of normal distribution.

[7]The Bitcoin price goes further the years after the study was realized reaching $19,000 in December 2017. The recent period of time will be integrated in Chapter 4.

**Table 3.1 Descriptive statistics**

This table presents summary statistics (annualized mean, annualized volatility, skewness and kurtosis) based on daily returns for Bitcoin, stock indices (represented by S&P500 and Nasdaq for the USA, FTSE100 for the UK, DAX30 Germany, NIKKEI225 for Japan and CAC40 for France), MSCI indexes for the World, Europe and Asia-Pacific regions, commodity indexes (Gold, Oil and Commodity), bonds index (Pimco) and currencies (Dollar, Yen, Euro and Yuan). The sample is drawn from the blockchain.info (now blockchain.com) website and the Datastream database over the period September 22nd, 2010 to December 30th, 2016.

| **Variable** | **N** | **Mean (%)** | **SD (%)** | **Skewness** | **Kurtosis** |
|---|---|---|---|---|---|
| **Bitcoin** | **1,638** | **568.82** | **111.69** | **0.68** | **15.98** |
| S&P500 | 1,638 | 19.74 | 17.73 | -0.48 | 5.02 |
| FTSE100 | 1,638 | 5.63 | 23.02 | -0.74 | 7.29 |
| DAX30 | 1,638 | 8.95 | 28.49 | -0.32 | 3.42 |
| NIKKEI225 | 1,638 | 11.71 | 24.65 | -0.48 | 4.69 |
| CAC40 | 1,638 | 5.94 | 28.94 | -0.33 | 4.06 |
| Nasdaq | 1,638 | 22.31 | 20.02 | -0.45 | 3.83 |
| MSCI World | 1,638 | 13.50 | 16.33 | -0.57 | 4.55 |
| MSCI Europe | 1,638 | 6.54 | 23.75 | -0.48 | 4.24 |
| MSCI Asia-Pacific | 1,638 | 7.40 | 19.79 | -0.37 | 3.12 |
| Oil | 1,638 | -7.25 | 29.02 | 0.37 | 4.59 |
| Gold | 1,638 | -2.14 | 20.50 | -0.82 | 7.57 |
| Commodity Index | 1,638 | -2.95 | 25.54 | -0.11 | 13.03 |
| Bonds | 1,638 | 6.16 | 5.83 | -0.32 | 1.55 |
| Dollar Index | 1,638 | 25.15 | 30.43 | -0.98 | 19.28 |
| Yen | 1,638 | 7.21 | 11.75 | 0.22 | 4.27 |
| Euro | 1,638 | 5.00 | 11.37 | -0.03 | 1.48 |
| Yuan | 1,638 | 0.80 | 2.50 | 1.56 | 29.77 |

**Table 3.2 Bitcoin return normality test**

This table presents the normality test for Bitcoin returns. The sample is drawn from the blockchain.info (now blockchain.com) website over the period 2010-2016. The normality hypothesis is based on Shapiro-Wilk test: if the p-value is lower than alpha, the null-hypothesis of normality is rejected.

| | **Shapiro Wilk** | **Kolmogorov Smirnov** | **Cramer Von Mises** | **Anderson Darling** |
|---|---|---|---|---|
| **Statistics** | **0.79***** | **0.16***** | **18.44***** | **94.04***** |
| p-value | 0.0001 | 0.010 | 0.005 | 0.005 |

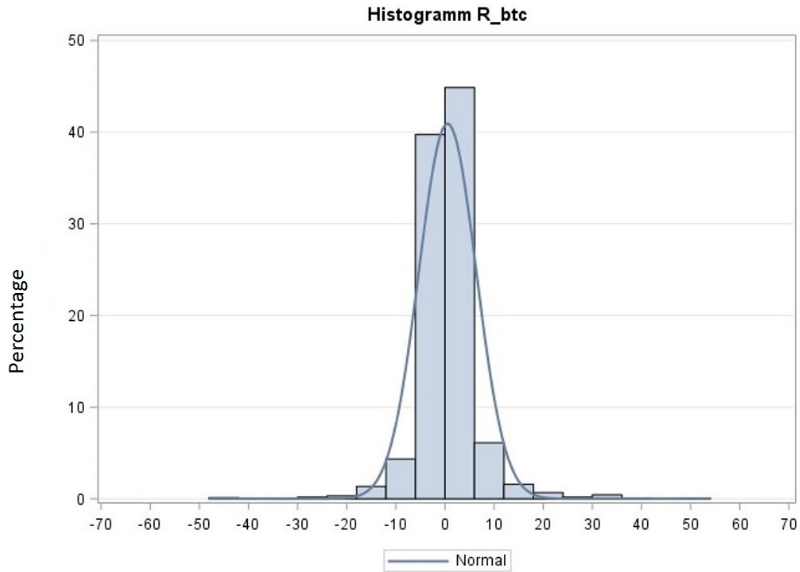


**Figure 3.3 Bitcoin return analysis - Histogram**
This figure shows the histogram of Bitcoin related to the normal distribution.

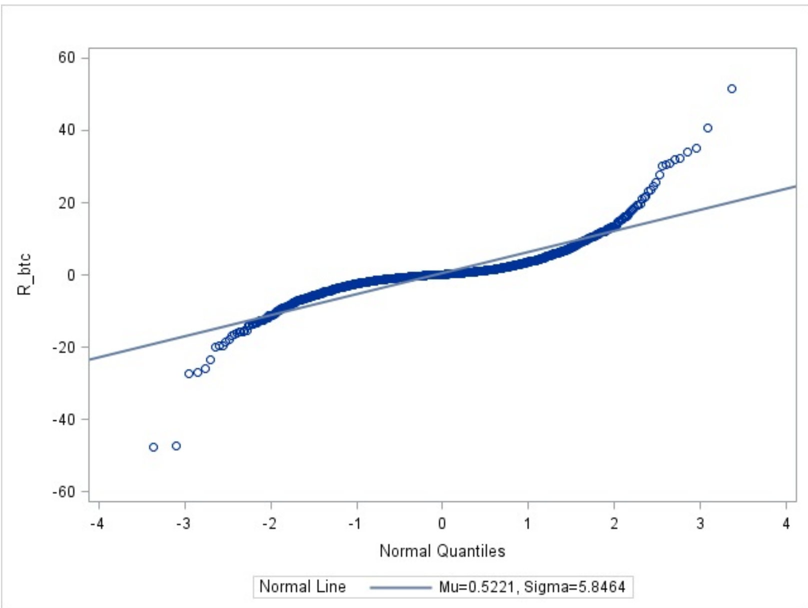


**Figure 3.4 Bitcoin return analysis - QQplot**
This figure shows QQ plot curve for Bitcoin returns.

**Table 3.3 Correlation coefficients between Bitcoin and various asset classes**

This table presents Pearson correlation coefficients between Bitcoin returns and asset classes such as stock indices (represented by S&P 500 and Nasdaq for the USA, FTSE 100 for the UK, DAX30 for Germany, NIKKEI225 for Japan and CAC40 for France), MSCI indexes for the World, Europe and AsiaPacific regions, commodity indexes (Gold, oil and commodity), bond index (Pimco) and currencies (dollar, yen, euro and Yuan). The sample is drawn from the blockchain.info (now blockchain.com) website and the Datastream database over the period September 22nd, 2010 through December 30th, 2016. If the p-value is higher than 5 per cent, then the null hypothesis of no-correlation (rho = 0) is accepted. ***, ** and * indicate that the coefficient is significant at 1%, 5% and 10% level, respectively.

| | | | | | |
|---|---|---|---|---|---|
| *Stock Index* | | | | | |
| | **S&P500** | **FTSE100** | **DAX30** | **NIKKEI225** | **CAC40** |
| **Bitcoin** | 0.04* | 0.03 | 0.04 | 0.00 | 0.04 |
| p-value | 0.097 | 0.242 | 0.150 | 0.914 | 0.080 |
| *MSCI Index* | | | | | |
| | **MSCI World** | **MSCI Europe** | **MSCI Asia-Pacific** | | |
| **Bitcoin** | 0.04 | 0.04 | 0.00 | | |
| p-value | 0.109 | 0.139 | 0.899 | | |
| *Commodities* | | | | | |
| | **Oil** | **Gold** | **Commodity Index** | | |
| **Bitcoin** | 0.04 | 0.04 | 0.00 | | |
| p-value | 0.152 | 0.137 | 0.971 | | |
| *Bonds* | | | | | |
| | **Bonds** | | | | |
| **Bitcoin** | 0.01 | | | | |
| p-value | 0.616 | | | | |
| *Currencies* | | | | | |
| | **Dollar Index** | **Euro** | **Yuan** | **Yen** | |
| **Bitcoin** | -0.01 | -0.03 | 0.00 | -0.01 | |
| p-value | 0.647 | 0.308 | 0.881 | 0.672 | |

Table 3.3 - *Correlation coefficients between Bitcoin and various asset classes* presents the Pearson correlation coefficients. Not surprisingly, Bitcoin is lowly correlated to the various indices considered in this study, which is in line with the previous literature (Yermack, 2015), (Brière et al., 2015), (Baur et al., 2016), (Bouri et al., 2016), (Kajtazi and Moro, 2017). For example, Brière et al. (2015) find that Bitcoin is lowly correlated with other indices over a three-year period, except for the World inflation-linked $Bonds$ and $Gold$. For our seven-year period, Bitcoin appears to be weakly correlated even to the bond index and $Gold$. Therefore, Bitcoin has a strong impact on diversification.

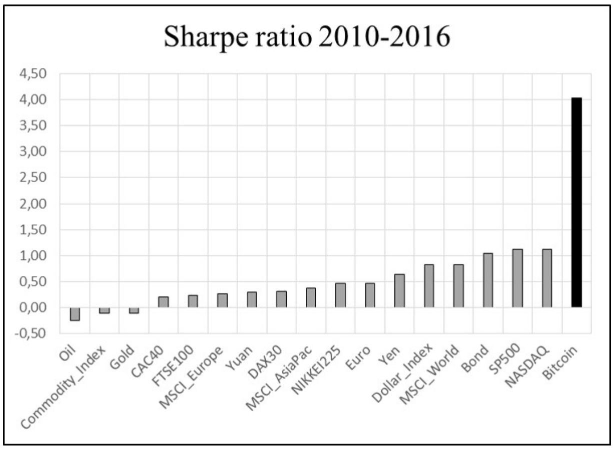


**Figure 3.5 Sharpe ratios**
This figure shows the Sharpe ratio for Bitcoin (red) and other assets over the period September 2010 – December 2016.

The diversification effect as well as the particular risk-return profile of Bitcoin asks the performance effect of Bitcoin. First, we study its performance using a simple measure, the Sharpe ratio, (see Table 3.4 - *Sharpe ratios*, Figures 3.5, 3.6, 3.7, 3.8). Bitcoin has the highest Sharpe ratio, 5.09, as compared to 1.11 for S&P 500, for example. Bitcoin recorded its highest ratio in 2013 because of the peak of US $1,000 reached in December 2013. This ratio increased from 2010 to 2013 before decreasing in 2014 (after the closure of Mt. Gox[8]). Afterwards, this ratio increased again from 2014 to 2016. During 2013, the Sharpe ratio of bond, euro, Yen and Yuan was negative.

[8]Mt. Gox was a Bitcoin exchange platform based in Tokyo and created in 2010.

**Table 3.4 Sharpe ratios**

This table presents Sharpe ratios per year for Bitcoin, Stock indexes (represented by S&P500 and Nasdaq for the US, FTSE100 for the UK, DAX30 Germany, NIKKEI225 for Japan and CAC40 for France), MSCI indexes for the World, Europe and Asia-Pacific regions, Commodity indexes (*Gold*, Oil and Commodity), the bond index (Pimco), and currencies (dollar, yen, euro and yuan). The data come from the Datastream database, the blockchain.info (now blockchain.com) and Kenneth R. French websites over the period September 22nd, 2010 to December 30th, 2016 in the World, Europe and Asia-Pacific regions.

| Variable | **2010** | **2011** | **2012** | **2013** | **2014** | **2015** | **2016** | **2010-2016** |
|---|---|---|---|---|---|---|---|---|
| N | 73 | 260 | 261 | 261 | 261 | 261 | 261 | 1,638 |
| **Bitcoin** | **8.87** | **9.53** | **14.46** | **112.37** | **-0.77** | **1.87** | **2.33** | **5.09** |
| S&P500 | 4.70 | 0.11 | 1.53 | 3.64 | 1.46 | 0.10 | 1.09 | 1.11 |
| FTSE100 | 1.95 | -0.13 | 1.01 | 1.97 | -0.49 | -0.42 | -0.02 | 0.24 |
| DAX30 | 3.10 | -0.54 | 1.56 | 2.22 | -0.70 | -0.09 | 0.19 | 0.31 |
| NIKKEI225 | 4.36 | -0.53 | 0.92 | 1.64 | -0.28 | 0.67 | 0.28 | 0.48 |
| CAC40 | 0.62 | -0.50 | 1.02 | 1.82 | -0.74 | 0.03 | 0.30 | 0.21 |
| Nasdaq | 5.46 | -0.04 | 1.43 | 4.14 | 1.26 | 0.49 | 0.66 | 1.11 |
| MSCI World | 4.13 | -0.27 | 1.58 | 3.40 | 0.72 | -0.03 | 0.74 | 0.83 |
| MSCI Europe | 1.60 | -0.41 | 1.18 | 2.20 | -0.53 | -0.16 | 0.00 | 0.28 |
| MSCI Asia-Pacific | 4.63 | -0.73 | 1.32 | 1.41 | -0.22 | 0.24 | 0.27 | 0.37 |
| Oil | 7.25 | 0.79 | 0.17 | 0.07 | -3.18 | -1.18 | 2.02 | -0.25 |
| Gold | 3.39 | 0.63 | 0.43 | -1.39 | -0.16 | -0.86 | 0.66 | -0.10 |
| Commodity Index | 4.96 | -0.21 | -0.04 | -0.27 | -0.63 | -0.65 | 0.79 | -0.12 |
| Bond | -0.28 | 1.09 | 3.31 | -0.40 | 2.33 | -0.20 | 1.66 | 1.06 |
| Dollar Index | 1.89 | 1.56 | 0.37 | 1.87 | 0.85 | 0.16 | 0.16 | 0.83 |
| Yen | -1.92 | -0.63 | 1.97 | 2.16 | 2.23 | 0.05 | -0.29 | 0.61 |
| Euro | -0.70 | 0.33 | -0.21 | -0.66 | 2.89 | 1.15 | 0.38 | 0.44 |
| Yuan | -2.88 | -2.91 | -0.83 | -3.22 | 1.51 | 2.01 | 2.93 | 0.32 |

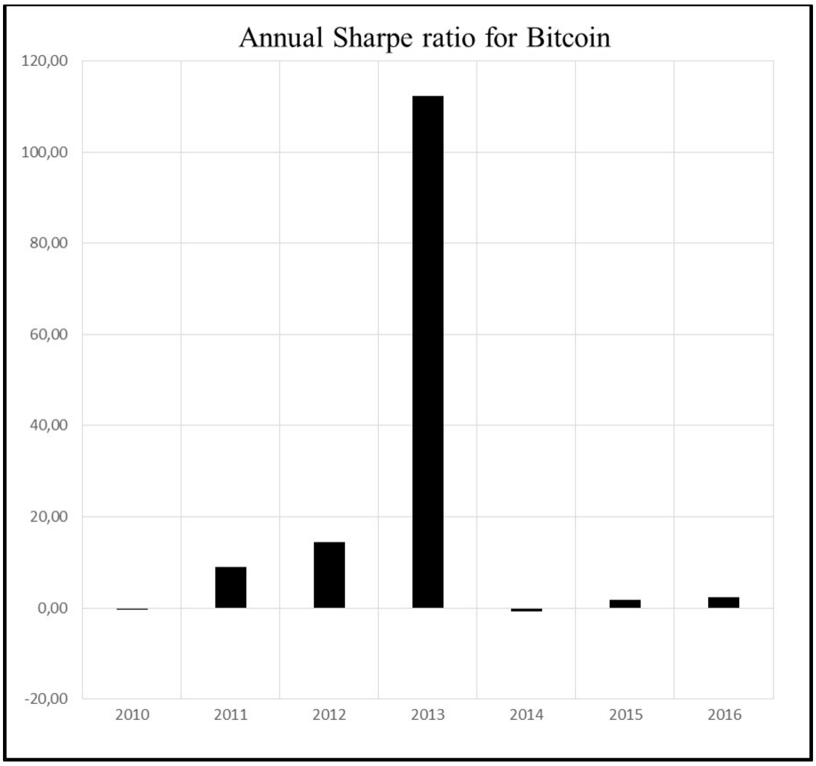


**Figure 3.6 Annual Sharpe ratio for Bitcoin**
This figure shows the Bitcoin Sharpe ratio per year over the period 2010-2016.

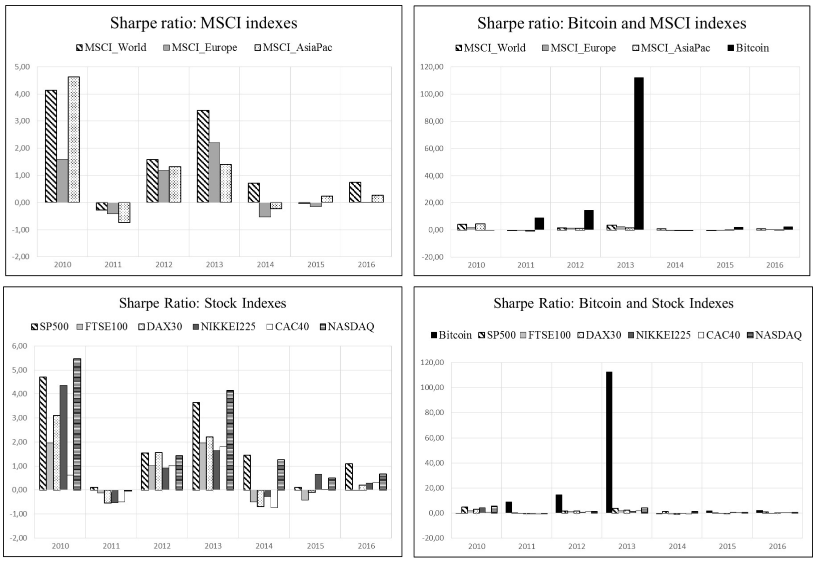


**Figure 3.7 Sharpe ratio: MSCI Indexes, Stocks Indexes and Bitcoin**
This figure shows the Sharpe ratio for MSCI Indexes, Stocks Indexes and Bitcoin per year over the period 2010-2016.

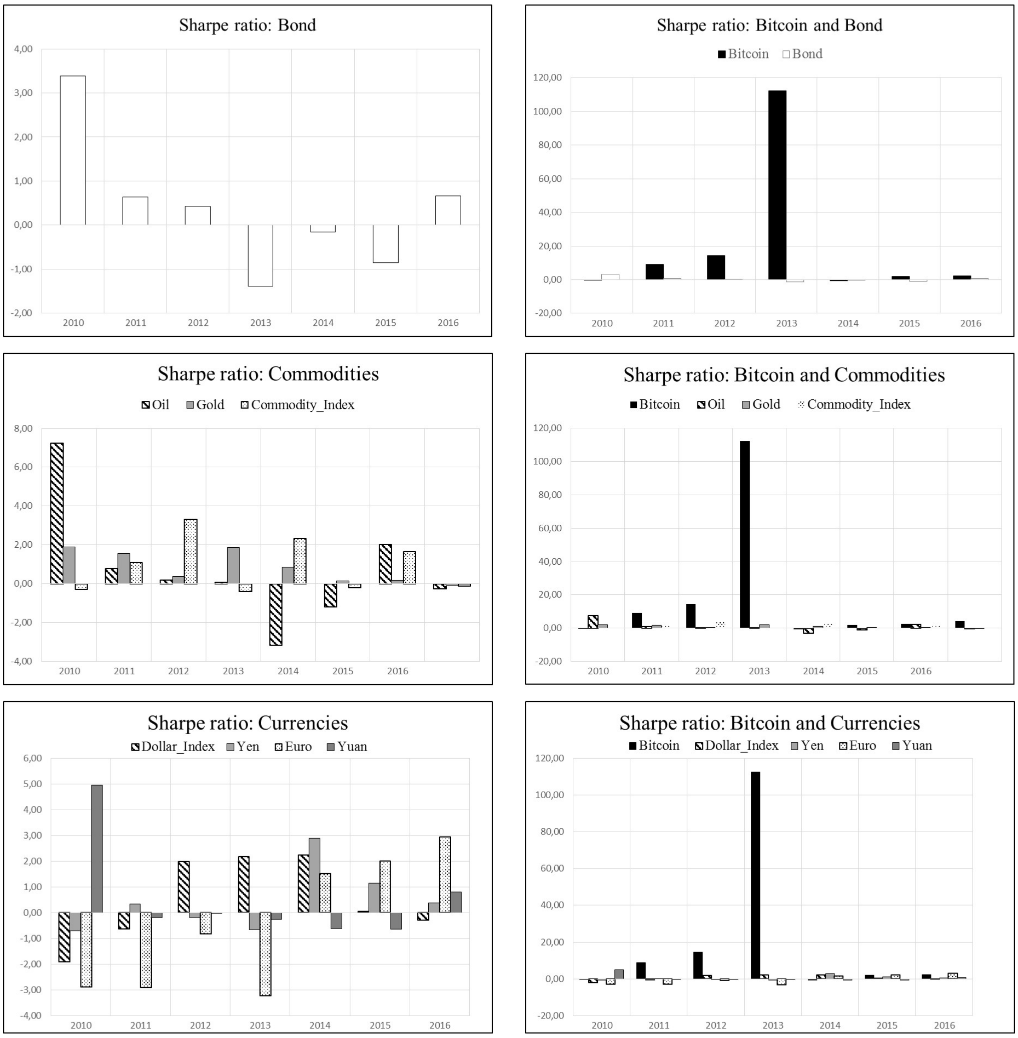


**Figure 3.8 Sharpe ratio: Bonds, Commodities, Currencies and Bitcoin**
This figure shows the Sharpe ratio for Bond, Commodities, Currencies and Bitcoin per year over the period 2010-2016.

### 3.4.2 Multivariate results

This section estimates the performance of Bitcoin by the alpha (risk-adjusted return) of the regression models in equations 3.3, 3.4, and 3.7. Table 3.5 - *Descriptive statistics of variables used in regressions* shows the descriptive statistics for the dependent and independent variables for the three regions presented above (e.g. World, Europe and Asia-Pacific). Bitcoin has higher return and higher risk than the global market portfolio and the Fama–French factor-mimicking portfolios. Table 3.6 - *Correlation matrix* presents Pearson correlation coefficients and shows that Bitcoin is lowly correlated with these portfolios.

**Table 3.5 Descriptive statistics of variables used in regressions**

This table presents summary statistics (mean, standard deviation, sum, minimum, maximum, annualized mean and annualized volatility) of daily returns expressed in $ for the dependent variable ($R_{Bitcoin} - R_f$) representing Bitcoin return minus the risk-free rate (proxied by the one-month US Treasury Bill) and for independent variables ($R_{Mkt} - R_f$, which represents the excess return of the market portfolio, $SMB$, which is the size premium, $HML$, which is the value premium, and $Bonds$ and $Gold$). The data come from the Datastream database, the blockchain.info (now blockchain.com) and Kenneth R. French websites over the period September 22nd, 2010 to December 30th, 2016 in the World, Europe and Asia-Pacific regions. All results are in percentages.

| Region | N | Mean (day) | SD (day) | Sum | Min | Max | Mean (year) | SD (year) |
|---|---|---|---|---|---|---|---|---|
| **World** | | | | | | | | |
| $R_{Bitcoin} - R_f$ | 1,638 | 0.52 | 5.85 | 855.15 | -47.83 | 51.53 | 568.99 | 111.70 |
| $R_{Mkt} - R_f$ | 1,638 | 0.04 | 0.84 | 60.21 | -5.12 | 4.16 | 14.36 | 16.14 |
| $SMB$ | 1,638 | 0.00 | 0.33 | -2.11 | -1.86 | 1.92 | -0.47 | 6.35 |
| $HML$ | 1,638 | 0.00 | 0.29 | 2.69 | -1.20 | 1.58 | 0.60 | 5.62 |
| $Gold$ | 1,638 | -0.01 | 1.07 | -9.72 | -10.16 | 5.43 | -2.14 | 20.50 |
| $Bonds$ | 1,638 | 0.02 | 0.30 | 26.81 | -1.58 | 1.12 | 6.16 | 5.82 |
| **Europe** | | | | | | | | |
| $R_{Bitcoin} - R_f$ | 1,638 | 0.52 | 5.85 | 855.15 | -47.83 | 51.53 | 568.99 | 111.70 |
| $R_{Mkt} - R_f$ | 1,638 | 0.02 | 1.16 | 40.16 | -8.80 | 5.60 | 9.36 | 22.12 |
| $SMB$ | 1,638 | 0.01 | 0.48 | 11.62 | -2.13 | 3.28 | 2.62 | 9.22 |
| $HML$ | 1,638 | -0.01 | 0.45 | -14.26 | -2.17 | 1.84 | -3.13 | 8.57 |
| $Gold$ | 1,638 | -0.01 | 1.07 | -9.72 | -10.16 | 5.43 | -2.14 | 20.50 |
| $Bonds$ | 1,638 | 0.02 | 0.30 | 26.81 | -1.58 | 1.12 | 6.16 | 5.82 |
| **Asia-Pacific** | | | | | | | | |
| $R_{Bitcoin} - R_f$ | 1,638 | 0.52 | 5.85 | 855.15 | -47.83 | 51.53 | 568.99 | 111.70 |
| $R_{Mkt} - R_f$ | 1,638 | 0.02 | 0.91 | 25.11 | -5.70 | 4.67 | 5.75 | 17.42 |
| $SMB$ | 1,638 | -0.01 | 0.47 | -10.48 | -3.41 | 4.79 | -2.31 | 9.07 |
| $HML$ | 1,638 | 0.02 | 0.45 | 27.84 | -1.82 | 1.95 | 6.40 | 8.60 |
| $Gold$ | 1,638 | -0.01 | 1.07 | -9.72 | -10.16 | 5.43 | -2.14 | 20.50 |
| $Bonds$ | 1,638 | 0.02 | 0.30 | 26.81 | -1.58 | 1.12 | 6.16 | 5.82 |

Table 3.7 - *Performance using the CAPM (Model 1), FF (Model 2) and extensions (Model 3)* presents the results of the regression analyses. The Bitcoin's factor loadings are low and insignificant for all the factors considered, and this is true for all regression specifications. The regressions' intercept, $\alpha$, is positive and highly significant, with daily values between 0.52 per cent and 0.53 per cent across models and regions (which represents between around 540 percent and 580 percent per annum). The Asia-Pacific region provides a slightly higher $\alpha$ than Europe, regardless the model. It can, therefore, be affirmed that investing in Bitcoin gives the possibility to earn, both from an economic and statistical perspective, highly significant positive risk-adjusted returns, regardless the region. Table 3.8 - *Bitcoin's $\alpha$ based on Model 2 (Fama and French three-factor model)* presents the Bitcoin's $\alpha$ by year and by region. $\alpha$ is measured by running the above-specified regressions for each year. Overall, $\alpha$ is relatively higher between 2010 and 2014, and mostly during 2013, with a value of 1.5 per cent per day and exhibits lower values during more recent periods. Over time, the market becoming more efficient and more mature relative to this financial innovation, Bitcoin performance has decreased. In particular, informational asymmetries between investors, notably linked to technology understanding, decrease, which may explain this pattern. According to the literature, Bitcoin is inefficient on the sub-period 2010-2013 and moves towards efficiency afterwards (Bartos, 2015), (Urquhart, 2016). The trend is consistent with the Sharpe ratio trend presented in the previous subsection.

**Table 3.6 Correlation matrix**

This table presents the correlation matrix between the excess return of the Bitcoin ($R_{Bitcoin} - R_f$) and independent variables ($R_{Mkt} - R_f$, $SMB$, $HML$, $Gold$, $Bonds$). The sample is drawn from the Datastream database, the blockchain.info (now blockchain.com) and Kenneth R. French websites over the period from September 22, 2010, to December 30, 2016, in the World, Europe and Asian-Pacific regions. ***, ** and * indicate that the coefficient is significant at 1%, 5% and 10% level respectively.

| | $R_{Bitcoin} - R_f$ | $R_{Mkt} - R_f$ | $SMB$ | $HML$ | $Gold$ | $Bonds$ |
|---|---|---|---|---|---|---|
| **World** | | | | | | |
| $R_{Bitcoin} - R_f$ | **1** | **0.04** | **-0.03** | **0.02** | **0.04** | **0.01** |
| | | 0.1181 | 0.2224 | 0.4238 | 0.1369 | 0.6158 |
| $R_{Mkt} - R_f$ | | **1** | **-0.39***** | **0.16***** | **0.07***** | **-0.11***** |
| | | | 0.0001 | 0.0001 | 0.0030 | 0.0001 |
| $SMB$ | | | **1** | **-0.15***** | **0.14***** | **0.14***** |
| | | | | 0.0001 | 0.0001 | 0.0001 |
| $HML$ | | | | **1** | **-0.04*** | **-0.09***** |
| | | | | | 0.0741 | 0.0005 |
| $Gold$ | | | | | **1** | **0.18***** |
| | | | | | | 0.0001 |
| $Bonds$ | | | | | | **1** |
| **Europe** | | | | | | |
| $R_{Bitcoin} - R_f$ | **1** | **0.03** | **-0.04*** | **0.03** | **0.04** | **0.01** |
| | | 0.1725 | 0.104 | 0.2685 | 0.1369 | 0.6158 |
| $R_{Mkt} - R_f$ | | **1** | **-0.69***** | **0.46***** | **0.09***** | **-0.07***** |
| | | | 0.0001 | 0.0001 | 0.0003 | 0.0028 |
| $SMB$ | | | **1** | **-0.37***** | **0.01** | **0.13***** |
| | | | | 0.0001 | 0.5556 | 0.0001 |
| $HML$ | | | | **1** | **0.00** | **-0.14***** |
| | | | | | 0.9949 | 0.0001 |
| $Gold$ | | | | | **1** | **0.18***** |
| | | | | | | 0.0001 |
| $Bonds$ | | | | | | **1** |
| **Asia-Pacific** | | | | | | |
| $R_{Bitcoin} - R_f$ | **1** | **0.03** | **-0.01** | **-0.04*** | **0.04** | **0.01** |
| | | 0.1724 | 0.6203 | 0.09 | 0.1369 | 0.6158 |
| $R_{Mkt} - R_f$ | | **1** | **-0.35** | **-0.36***** | **0.16***** | **0.02** |
| | | | 0.0001 | 0.0001 | 0.0001 | 0.3638 |
| $SMB$ | | | **1** | **-0.13***** | **0.02** | **-0.01** |
| | | | | 0.0001 | 0.3363 | 0.7337 |
| $HML$ | | | | **1** | **-0.12***** | **-0.01** |
| | | | | | 0.0001 | 0.7287 |
| $Gold$ | | | | | **1** | **0.18***** |
| | | | | | | 0.0001 |
| $Bonds$ | | | | | | **1** |

**Table 3.7 Performance using the CAPM (Model 1), FF (Model 2) and extensions (Model 3)**

This table presents regression estimates for the 3 models in equations 1,2,3. The sample is drawn from the Datastream database, the blockchain.info (now blockchain.com) and Kenneth R. French websites over the period September 22nd, 2010 to December 30th, 2016 in the World, European, and Asia-Pacific regions. ***, ** and * indicate that the coefficient is significant at 1%, 5% and 10% level respectively.

| Region | $\alpha$ | $R_{Mkt} - R_f$ | $SMB$ | $HML$ | $Bonds$ | $Gold$ | $R^2$ | Adjusted $R^2$(%) | Annual $\alpha$(%) |
|---|---|---|---|---|---|---|---|---|---|
| *World* | | | | | | | | | |
| Model 1 | **0.51*** ** | **0.27** | | | | | 0.15 | 0.09 | 545.53 |
| p-value | 0.0004 | 0.1181 | | | | | | | |
| Model 2 | **0.51*** ** | **0.21** | **-0.29** | **0.25** | | | 0.19 | 0.0001 | 548.75 |
| p-value | 0.0004 | 0.2645 | 0.5396 | 0.6216 | | | | | |
| Model 3 | **0.51*** ** | **0.17** | **-0.45** | **0.29** | **0.20** | **0.26** | 0.0035 | 0.0005 | 544.03 |
| p-value | 0.0004 | 0.3596 | 0.3569 | 0.5595 | 0.1506 | 0.5966 | | | |
| *Europe* | | | | | | | | | |
| Model 1 | **0.52*** ** | **0.17** | | | | | 0.11 | 0.05 | 558.91 |
| p-value | 0.0003 | 0.1725 | | | | | | | |
| Model 2 | **0.53*** ** | **0.03** | **-0.38** | **0.17** | | | 0.18 | 0 | 577.23 |
| p-value | 0.0003 | 0.8639 | 0.366 | 0.6455 | | | | | |
| Model 3 | **0.52*** ** | **-0.01** | **-0.46** | **0.21** | **0.19** | **0.25** | 0.33 | 0.03 | 574.75 |
| p-value | 0.0003 | 0.9515 | 0.2739 | 0.5699 | 0.1652 | 0.6052 | | | |
| *Asia-Pacific* | | | | | | | | | |
| Model 1 | **0.52*** ** | **0.22** | | | | | 0.11 | 0.05 | 560.97 |
| p-value | 0.0003 | 0.1724 | | | | | | | |
| Model 2 | **0.53*** ** | **0.10** | **-0.14** | **-0.49** | | | 0.23 | 0.04 | 583.18 |
| p-value | 0.0003 | 0.5777 | 0.6826 | 0.1762 | | | | | |
| Model 3 | **0.53*** ** | **0.07** | **-0.17** | **-0.47** | **0.16** | **0.12** | 0.32 | 0.02 | 580.55 |
| p-value | 0.0003 | 0.7044 | 0.6248 | 0.1943 | 0.2409 | 0.7974 | | | |

**Table 3.8 Bitcoin's $\alpha$ based on Model 2 (Fama and French three-factor model)**

This Table presents the regression results for model 2, year by year, in equation 2. The sample is drawn from the Datastream database, the blockchain.info (now blockchain.com) and Kenneth R. French websites over the period 2010 - 2016 in the World, Eu-rope and Asian-Pacific regions. We run year by year model 2 to estimate alpha evolution in the World, European and Asia-Pacific regions. ***, ** and * show that the coefficient is significant at 1%, 5% and 10% level respectively.

| Region | **2010-2016** | **2010** | **2011** | **2012** | **2013** | **2014** | **2015** | **2016** |
|---|---|---|---|---|---|---|---|---|
| *World* | | | | | | | | |
| $\alpha$ | **0.51*****  | 0.47 | 0.73 | 0.61*** | 1.42*** | -0.24 | 0.29 | 0.20 |
| p-value | 0.0004 | 0.7115 | 0.1834 | 0.0037 | 0.005 | 0.3157 | 0.2318 | 0.2077 |
| annualized $\alpha$ (%) | 548.75 | 452.47 | 1300.36 | 810.92 | 17076.26 | -57.98 | 189.34 | 106.43 |
| *Europe* | | | | | | | | |
| $\alpha$ | **0.53***** | 0.4383 | 0.83 | 0.64*** | 1.55*** | -0.25 | 0.30 | 0.19 |
| p-value | 0.0003 | 0.7315 | 0.1361 | 0.0024 | 0.0024 | 0.2864 | 0.2308 | 0.2221 |
| Annualized $\alpha$ | 577.23% | 393.47% | 1940.03% | 914.80% | 27716.86% | -59.84% | 193.25% | 99.73% |
| *Asia-Pacific* | | | | | | | | |
| $\alpha$ | **0.53***** | 0.38 | 0.81 | 0.68*** | 1.47*** | -0.27 | 0.24 | 0.23 |
| p-value | 0.0003 | 0.7648 | 0.143 | 0.0014 | 0.0026 | 0.2533 | 0.3257 | 0.1507 |
| Annualized $\alpha$ | 583.18% | 297.41% | 1799.39% | 1089.78% | 20653.39% | -62.49% | 140.02% | 129.16% |

As most Bitcoin transactions take place in the Chinese market, we replicate our analyses and estimate $\alpha$ with the three models in which the market, size and B/M factor-mimicking portfolios are composed exclusively of common stocks traded in the Chinese market. These factors are built according to the procedure used by Fama and French used for forming size and B/M portfolios; this procedure is explained in detail on the Kenneth French's website. In addition, we used the MSCI China Small Cap - MSCI China Large Cap as a size factor and the MSCI China Value Local - MSCI China Growth Local as a value factor to compare our results. Table 3.9 - *Descriptive statistics of variables used in regressions for the Chinese market* displays the descriptive statistics for the dependent and independent variables for the China market. Table 3.10 - *Correlation matrix on the Chinese market - Fama-French Factors* and 3.11 *Correlation matrix on the Chinese market - MSCI Factors* present the correlation coefficients between Bitcoin and the explanatory variables used in our regressions in the Chinese market. As for the other regions, Bitcoin has a low correlation with the size and B/M factor-mimicking portfolios in China. This result suggests diversification benefits by including Bitcoin in a portfolio composed of common stocks in the Chinese market.

**Table 3.9 Descriptive statistics of variables used in regressions for the Chinese market**

This table presents summary statistics (mean, standard deviation, sum, minimum, maximum, annualized mean and annualized volatility) of daily returns expressed in $ for the dependent variable ($R_{Bitcoin} - R_f$) representing Bitcoin return minus the risk-free rate (proxied by the Chinese Government Bond 10 year) and for independent variables ($R_{Mkt} - R_f$, which represents the excess return of the market portfolio, $SMB$, which is the size premium, $HML$, which is the value premium constructed based on Fama and French factor-mimicking portfolio on the Shenzhen market, $size$ is the MSCI China Small Cap - MSCI China Large Cap and $value$ is the MSCI China Value Local - MSCI China Growth Local. The data come from the Datastream database, the blockchain.info (now blockchain.com) and Kenneth R. French websites over the period 23 September 2010 to December 30$^{th}$, 2016 in the World, Europe and Asia-Pacific regions. All results are in percentages.

| | **N** | **Mean (day)** | **SD (day)** | **Sum** | **Min** | **Max** | **Mean (year)** | **SD (year)** |
|---|---|---|---|---|---|---|---|---|
| $R_{Bitcoin} - R_f$ | 1,637 | 0.60 | 6.76 | 975.27 | -48.18 | 63.80 | 774.14 | 129.15 |
| $R_{Mkt} - R_f$ | 1,637 | 0.01 | 1.55 | 15.60 | -7.71 | 9.38 | 3.54 | 29.61 |
| $SMB$ | 1,637 | 0.06 | 0.49 | 90.57 | -2.98 | 2.11 | 22.37 | 9.32 |
| $HML$ | 1,637 | 0.04 | 0.76 | 64.51 | -4.14 | 3.05 | 15.47 | 14.46 |
| $Size$ | 1,637 | -0.01 | 0.82 | -13.41 | -4.99 | 9.96 | -2.95 | 15.68 |
| $Value$ | 1,637 | 0.00 | 0.64 | 3.40 | -5.53 | 3.04 | 0.76 | 12.25 |

**Table 3.10 Correlation matrix on the Chinese market - Fama French Factors**

This table presents the correlation matrix between the dependent variable ($R_{Bitcoin} - R_f$) and independent variables ($R_{Mkt} - R_f$, $SMB$, $HML$, $Gold$, $Bonds$). The sample concerns the period between September 23, 2010, and December 30th, 2016. ***, ** and * show that the coefficient is significant at 1%, 5% and 10% level respectively.

| Variable | $R_{Bitcoin} - R_f$ | $R_{Mkt} - R_f$ | $SMB$ | $HML$ | $Gold$ | $Bonds$ |
|---|---|---|---|---|---|---|
| $R_{Bitcoin} - R_f$ | **1** | **0.08*****| **0.01** | **0.04** | **0.01** | **0.02** |
| | | 0.001 | 0.637 | 0.130 | 0.653 | 0.333 |
| $R_{Mkt} - R_f$ | | **1** | **0.05*** | **0.35***** | **0.05**** | **-0.06**** |
| | | | 0.061 | 0.0001 | 0.045 | 0.024 |
| $SMB$ | | | **1** | **0.14***** | **0.02** | **-0.02** |
| | | | | 0.0001 | 0.498 | 0.343 |
| $HML$ | | | | **1** | **0.04*** | **-0.05*** |
| | | | | | 0.074 | 0.067 |
| $Gold$ | | | | | **1** | **0.18***** |
| | | | | | | 0.0001 |
| $Bonds$ | | | | | | **1** |

**Table 3.11 Correlation matrix on the Chinese market - MSCI Factors**

This table presents the correlation matrix between the dependent variable ($R_{Bitcoin} - R_f$) and independent variables ($R_{Mkt} - R_f$, $Size$, $Value$, $Gold$, $Bonds$). The sample concerns the period between September 23, 2010, and December 30th, 2016. ***, ** and * show that the coefficient is significant at 1%, 5% and 10% level respectively.

| Variable | $R_{Bitcoin} - R_f$ | $R_{Mkt} - R_f$ | $Size$ | $Value$ | $Gold$ | $Bonds$ |
|---|---|---|---|---|---|---|
| $R_{Bitcoin} - R_f$ | **1** | **0.08***** | **-0.03** | **0.02** | **0.01** | **0.02** |
| | | 0.001 | 0.238 | 0.510 | 0.653 | 0.333 |
| $R_{Mkt} - R_f$ | | **1** | **-0.14***** | **-0.29***** | **0.05**** | **-0.06**** |
| | | | 0.0001 | 0.0001 | 0.045 | 0.024 |
| $Size$ | | | **1** | **-0.26***** | **0.09***** | **0.01** |
| | | | | 0.0001 | 0.001 | 0.608 |
| $Value$ | | | | **1** | **-0.02** | **-0.03** |
| | | | | | 0.338 | 0.233 |
| $Gold$ | | | | | **1** | **0.18***** |
| | | | | | | 0.0001 |
| $Bonds$ | | | | | | **1** |

The $\alpha$ values estimated with the three performance models on the Chinese market are presented in Table 3.12 - *Bitcoin's $\alpha$ on the Chinese market.* As for the other regions, the $\alpha$ values are economically and statistically highly significant and slightly higher than those obtained in other regions (World, Europe and Asia-Pacific). Despite that the Chinese market is known to be more mature with respect to the Bitcoin than other markets (Kajtazi and Moro, 2017), our results show, as for the other regions, strong possibilities to earn positive performance.

**Table 3.12 Bitcoin's $\alpha$ on the Chinese market**

This table presents the regression results for the 3 models in equations 1,2 and 3 for the Chinese Market. The data needed to construct the proxies for the Chinese market, the size and the B/M indices are extracted from the Datasteam database, while the data needed for computing the Bitcoin's returns are extracted from blockchain.info (now blockchain.com). The period of analysis is from September 23, 2010, and December 30th, 2016. ***, ** and * show that the coefficient is significant at 1%, 5% and 10% level respectively.

| Model | $\alpha$ | $R_{Mkt} - R_f$ | $SMB$ | $HML$ | $Bonds$ | $Gold$ | $R^2$ | Annual $\alpha$(%) |
|---|---|---|---|---|---|---|---|---|
| Model 1 | **0.59***** | **0.35***** | | | | | 0.65 | 763.61 |
| p-value | 0.0004 | 0.0011 | | | | | | |
| Model 2 - FF | **0.58***** | **0.33***** | **0.09** | **0.08** | | | 0.66 | 737.77 |
| p-value | 0.0005 | 0.0036 | 0.7846 | 0.7248 | | | | |
| Model 3 - FF | **0.57***** | **0.34***** | **0.10** | **0.09** | **0.91** | **58.02** | 0.75 | 704.46 |
| p-value | 0.0007 | 0.0031 | 0.7697 | 0.7047 | 0.9538 | 0.2545 | | |
| Model | $\alpha$ | $R_{Mkt} - R_f$ | $Size$ | $Value$ | $Bonds$ | $Gold$ | $R^2$ | Annual $\alpha$(%) |
| Model 2 - MSCI | **0.59***** | **0.40***** | **0.34** | **-0.06** | | | X | 771.29 |
| p-value | 0.0004 | 0.0005 | 0.1279 | 0.8396 | | | | |
| Model 3 - MSCI | **0.58***** | **0.41***** | **0.35** | **0.05** | **0.99** | **61.17** | 0.92 | 737.02 |
| p-value | 0.0005 | 0.0004 | 0.1137 | 0.8552 | 0.9505 | 0.2293 | | |

## 3.5 Robustness checks

### 3.5.1 Regression specification

The Bitcoin risk-return profile being atypical, it is important to check for problems that may appear with our regressions. Tables 3.13 - *Collinearity: Test of independent variables* and 3.14 - *Residual analysis* show that our regressions do not seem to suffer from problems related to multicollinearity (the VIF is always lower than 4), time series correlation between residuals (the Durbin–Watson statistic is close to the value of 2) and the White's tests show that the homoscedasticity hypothesis cannot be rejected in most cases.

**Table 3.13 Collinearity: Test of independent variables**

This table shows collinearity test of independent variables. The sample is drawn from the blockchain.info (now blockchain.com) and Kenneth R. French websites over the period 2010 to 2016 for the World. Europe and Asia-Pacific regions and for the 3 models in equations 1, 2 and 3. VIF is the variance inflation factor: if VIF is higher than 4 and TOL is lower than 0.25, then the variable is considered collinear with the dependent variable.

| | **World** | | **Europe** | | **Asia-Pacific** | |
|---|---|---|---|---|---|---|
| | VIF | TOL | VIF | TOL | VIF | TOL |
| **Model 1** | | | | | | |
| $\alpha$ | 0 | . | 0 | . | 0 | . |
| $R_{Mkt} - R_f$ | 1 | 1 | 1 | 1 | 1 | 1 |
| **Model 2** | | | | | | |
| $\alpha$ | 0 | . | 0 | . | 0 | . |
| $R_{Mkt} - R_f$ | 1.2 | 0.8 | 2.13 | 0.47 | 1.40 | 0.71 |
| $SMB$ | 1.2 | 0.8 | 1.9 | 0.5 | 1.2 | 0.81 |
| $HML$ | 1.0 | 1.0 | 1.3 | 0.8 | 1.3 | 0.80 |
| **Model 3** | | | | | | |
| $\alpha$ | 0 | . | 0 | . | 0 | . |
| $R_{Mkt} - R_f$ | 1.2 | 0.8 | 2.17 | 0.46 | 1.43 | 0.70 |
| $SMB$ | 1.2 | 0.8 | 2.0 | 0.5 | 1.2 | 0.80 |
| $HML$ | 1.0 | 1.0 | 1.3 | 0.8 | 1.3 | 0.80 |
| $Bonds$ | 1.1 | 0.9 | 1.1 | 1.0 | 1.1 | 0.94 |
| $Gold$ | 1.1 | 0.9 | 1.1 | 0.9 | 1.0 | 0.97 |

**Table 3.14 Residual analysis**

This table presents the residuals analysis from the long-run regressions in the World, Europe and Asia-Pacific regions. The sample is drawn from the blockchain.info (now blockchain.com) and Kenneth R. French websites over the period 2010 to 2016 in the World, Europe and Asia-Pacific regions for the three models in equations (1), (2) and (3). The residuals autocorrelation hypothesis is tested using the Durbin-Watson statistic: if the Durbin-Watson statistic is around 2, then the residuals are considered uncorrelated. The homoscedasticity hypothesis is tested based on the White test: if the p-value is lower than 5 per cent, the null hypothesis of homoscedasticity is rejected. The normality hypothesis is based on the Shapiro-Wilk test: if the p-value is lower than 5 per cent, the null hypothesis of normality is rejected.

| | Autocorrelation<br>Durbin-Watson | Homoscedasticity<br>White | Normality<br>Shapiro-Wilk |
|---|---|---|---|
| **World** | | | |
| Model 1 | **1.72** | **3.54** | **0.79** |
| p-value | | 0.1701 | 0.0001 |
| Model 2 | **1.71** | **10.10** | **0.79** |
| p-value | | 0.3426 | 0.0001 |
| Model 3 | **1.72** | **27.51** | **0.79** |
| p-value | | 0.1216 | 0.0001 |
| **Europe** | | | |
| Model 1 | **1.72** | **1.14** | **0.79** |
| p-value | | 0.5667 | 0.0001 |
| Model 2 | **1.71** | **3.61** | **0.79** |
| p-value | | 0.935 | 0.0001 |
| Model 3 | **1.72** | **22.74** | **0.79** |
| p-value | | 0.3017 | 0.0001 |
| **Asia-Pacific** | | | |
| Model 1 | **1.71** | **0.01** | **0.79** |
| p-value | | 0.9967 | 0.0001 |
| Model 2 | **1.71** | **6.36** | **0.79** |
| p-value | | 0.7039 | 0.0001 |
| Model 3 | **1.72** | **23.52** | **0.79** |
| p-value | | 0.264 | 0.0001 |

Another important problem resides in the normality of Bitcoin returns. Non-normal returns imply, under the hypothesis that explanatory variables are not stochastic, non-normal errors, in which case the estimators of the regression coefficients are no more efficient. Figure 3.3 - *Bitcoin return analysis - Histogram* and 3.4 - *Bitcoin return analysis - QQplot* show that Bitcoin returns are skewed to the right, with a skewness of 0.68, and exhibit a “heavy-tailed” distribution, with a kurtosis of 15.98 (see also Table 3.2 - *Bitcoin return normality test*). Our results are similar to those obtained in previous empirical studies (Baur et al., 2016). Despite that returns look like being normally distributed, normality tests such as Shapiro–Wilk reject the null hypothesis of normality.

We use the residual augmented least squares (RALS) estimators, compared to the generalized method of moments (GMM) estimator based the moment condition (Hansen, 1982), to measure Bitcoin performance in a more robust way.

This estimation technique is known to provide a more efficient estimation of regression coefficients without imposing specific restriction on the returns' distribution (Gallagher and Taylor, 2000), (Im and Schmidt, 2008). This technique has proved to be useful in analyzing, for example, the performance of hedge funds as measured by their $\alpha$. Heuson and Hutchinson (2015) show that, for such funds, the error generated by regression models depends systematically on skewness. OLS assessment errors prove to be economically significant, and RALS estimation technique proves to be robust to this bias.

The OLS regression model is defined as:

$$y_t = \phi' z_t + u_t \tag{3.10}$$

where $t = 1, ..., T$ is the time, $z_t = (1x_t')'$ where $x_t$ is a $(k-1)*1$ time series vector at time t, $\phi = (\alpha\beta')'$ is the parameter vector where $\alpha$ is the intercept and $\beta$ is the $(k-1)*1$ parameter of interest vector, and $u_t$ is the iid residuals.

Heuson and Hutchinson (2015) explains that the model is based on the kurtosis and skweness assumptions. More precisely, the consequence of an excess kurtosis in the residual is that the standardized fourth central moment of the series exceeds three:

$$E(u_t^4 - 3\sigma^4) = E[u_t(u_t^3 - 3\sigma^2 u_t)] \neq 0 \tag{3.11}$$

Therefore, $u_t^3 - 3\sigma^2 u_t$ is correlated with the residuals, $u_t$, but not correlated with the regressors, because $x_t$ and $u_t$ are independant.

The standardized third central moment is not zero if the errors are skewed:

$$E(u_t^3 - \sigma^3) = E[u_t(u_t^2 - \sigma^2)] \neq 0 \tag{3.12}$$

Equally, $u_t^2 - \sigma^2$ is correlated with the residuals $u_t$ but not with the regressors as well.

In this case, Im and Schmidt (2008) states that the 3.10 has to be augmented by $\widehat{w}_t$:

$$\widehat{w}_t = [\widehat{u}_t^3 - 3\widehat{\sigma}_t^2\widehat{u}_t)(\widehat{u}_t^2 - \widehat{\sigma}_t^2)]' \tag{3.13}$$

Where $\widehat{u}_t$ is the residuals and $\widehat{\sigma}_t$ is the standard residual variance estimated from the OLS regression of equation 3.10.

$$y_t = \alpha + \beta' z_t + \gamma' \widehat{w}_t + \epsilon_t \tag{3.14}$$

The RALS estimator is computed such as:

$$\beta^* = (\widetilde{X}' M_{\widetilde{W}} \widetilde{X})^{-1} \widetilde{X}' M_{\widetilde{W}} Y \tag{3.15}$$

Where, $M_{\widetilde{W}}$ is the idempotent matrix:

$$M_{\widetilde{W}} = I_T - \widetilde{W}' (\widetilde{W}' \widetilde{W})^{-1} \widetilde{W}$$

Where $I_T$ is the $T \times T$ identity matrix, $\widetilde{N} = (\widetilde{n}_1 \widetilde{n}_2 ... \widetilde{n}_T)'$, $\widetilde{n}_t = n_t - T^{-1} \sum_1^T n_t$ for $(N, n) = (X, x), (Y, y), (W, w)$ and $t = 1, ...T$.

The asymptotic distribution of the RALS estimator is given by:

$$\sqrt{T}(\beta^* - \beta) \rightarrow N(0, \sigma_A^2 Var X_t)^{-1})$$

$$\sigma_A^2 = \sigma^2 - \frac{\mu_3^2(\mu_6 - 6\mu_4\sigma^2 + 9\sigma^6 - \mu_3^2) - 2\mu_3(\mu_4 - 3\sigma^4)(\mu_5 - 4\mu_3\sigma^2) + (\mu_4 - 3\sigma^4)^2(\mu_4 - \sigma^4)}{(\mu_4 - \sigma^4)(\mu_6 - 6\mu_4\sigma^2 + 9\sigma^6 - \mu_3^2) - (\mu_5 - 4\mu_3\sigma^2)^2} \tag{3.16}$$

In practice, $\sigma_A^2$ is estimated ($\widehat{\sigma}_A^2$) by replacing each of the $\mu_i$ with the corresponding sample moment using the residuals coming from the OLS regression (e.g. see equation 3.10).

The covariance matrix for $\beta^*$ is estimated by:

$$\widehat{V}(\beta^*) = \widehat{\sigma}_A^2 (\widetilde{X}' M_{\widetilde{W}} \widetilde{X})^{-1} \tag{3.17}$$

The efficiency gain from the RALS regression compared to the OLS regression is measured by the statistic $\rho$:

$$\widehat{\rho} = \widehat{\sigma}_A^2 / \widehat{\sigma}^2$$

$\rho$ is small for large efficiency gains. If the distribution is normal, OLS is more efficient that RALS and $\rho = 1$.

We use the RALS model to estimate $\alpha$ for each of the three performance models used in our article and for each one of the four regions studied.

The qualitative interpretations of our results do not change; they are even reinforced. The RALS $\alpha$ is highly significant both economically and statistically. In the World, Europe, Asia-Pacific and China regions, the RALS $\alpha$ is between 0.52 per cent and 0.59 per cent per day, which is similar to the OLS $\alpha$. The RALS t-statistic is about 4.43, which is higher than the t-statistic with the OLS procedure (the latter is, on average, of about 3.6).

### 3.5.2 Behavioral aspects

Performance results can be controversial if in reality the economic value of Bitcoin is close to zero. Cheah and Fry (2015) apply econometric modelling on Bitcoin prices and find empirical evidence that Bitcoin exhibits speculative bubbles and has a fundamental value of zero. However, other authors find that speculation does not explain the high volatility of Bitcoin and find evidence that Bitcoin has positive economic value (Dwyer, 2015), (Blau, 2017), (Hayes, 2018). More recently, a part of literature in the cryptocurrency field is focus on modeling the economic value of the cryptocurrency, (Biais et al., 2018), (Pagnotta and Buraschi, 2018), (Sockin and Xiong, 2018), (Bhambhwani et al., 2019), (Easley et al., 2019), (Kristoufek, 2019), (Wheatley et al., 2019).

The low correlation between Bitcoin and asset classes together with the high a obtained in the World, Europe and Asia-Pacific regions may be indicative of a speculative bubble. In this section, we attempt to control for speculative behavior on Bitcoin by using market sentiment as a control variable. Including such control variables is also a way to test the robustness of our results regarding the Bitcoin's performance.

Market sentiment takes into consideration the fact that the Efficient Market Hypothesis does not necessarily apply on the real market. The value of an asset may deviate from its fundamental value because of market's imperfections, such as information asymmetry under noise, or investors' behavior. Market sentiment, or investor sentiment, measures the investors' behavior on the market based on their expectations. Prices reveal this expectation, and consequently are an indicator to appraise investor sentiment. If an investor expects that prices are going to increase, thus leading to returns higher than the average, then he/she is bullish and enters on the market with a buyer attitude. On the contrary, a bearish investor expects that prices are going to decrease, and therefore s/he enters the market with a seller attitude. Bullish investors expect positive and greater returns than the fundamental value, whilst bearish investors expect a smaller return on the market

Based on the literature and especially on the article of Brown and Cliff (2004), we identify four proxies for the market sentiment variable, among which three are related to trading and one is related to derivatives, in order to capture the attitude of investors relative to Bitcoin. The first one, named $Trade1$, is the ratio of advancing issues on declining issues:

$$Trade1 = Advancing/Declining \tag{3.18}$$

where advancing (declining) issues are the number of stocks that increased (decreased) between two dates (in our daily case, between the day before and the day after). This variable captures the market movement on a long or short run. A positive (negative) and significant $Trade1$ variable reveals a bullish (bearish) market: the number of advancing issues exceeds (is lower than) the declining ones. When the market is neutral, the ratio equals 1.

The second proxy, $Trade2$, is based also on advancing and declining issues but taking into consideration the volume as follows:

$$Trade2 = (Advancing/Advancing\_volume)/(Declining/Declining\_volume) \tag{3.19}$$

where advancing (declining) issues are the number of stocks that increased (decreased) between two dates (in our daily case, between the day before and the day after). Advancing (declining) volume represents the total volume for advancing (declining) stocks. A positive (negative) and significant $Trade2$ variable reveals a bullish (bearish) market: the number of advancing issues exceeds (is lower than) the declining ones. When the market is neutral, the ratio equals 1.

The third variable related to the trading group, $Trade3$, deals with new highs and new lows and captures the relative market strength.

$$Trade3 = High/Low \tag{3.20}$$

This variable compares the number of stocks reaching new highs and the number of stocks reaching new lows. More precisely, it compares the number of stocks having reached a 52-week high and the number of securities which having hit a 52-week low. A bullish (bearish) sentiment is captured when there are more stocks trading at their highs (lows) than the period before.

Finally, the last variable considered in our analysis is "Put-to-Call"(hereafter $PtC$) based on the Chicago Board Options Exchange:

$$Ptc = Puts/Calls \tag{3.21}$$

A put (call) is the right to sell (buy) an underlying asset at a given price in the future. Buying put (call) means a bearish (bullish) behavior while selling put (call) means a bullish (bearish) attitude). A bearish (bullish) sentiment is detected when the ratio put/call is high (low).

We add these four variables in the models estimated above and present our results in Tables 3.15 - *Controlling for market sentiment in the CAPM (Model 1)*, 3.16 - *Controlling for market sentiment in the FF model (Model 2)*, and 3.17 - *Controlling for market sentiment in the FF extended model (Model 3*. Two of the trade variables, $Trade1$ and $Trade3$, are not significant, whilst $Trade2$ is highly significant. We also note that $\alpha$ is significant in most of the model specifications, except when the derivatives variable ($PtC$) is considered, in which case a is no more significant in all model specifications. $Trade2$ is negative, whereas we expected a positive sentiment market variable. These results suggest that investors' behavior does influence Bitcoin's performance, but overall the performance continues to be positive and significant after controlling for this effect.

**Table 3.15 Controlling for market sentiment in the CAPM (Model 1)**

This table controls Bitcoin performance by including proxies for market sentiment in the CAPM model (Model 1). We use four proxies of market sentiment: $Trade1$ is the ratio of advancing issues on declining issues; $Trade2$ is the ratio of advancing issues on declining issues including volume; $Trade3$ is the ratio of new highs on news lows; $PtC$ is the ratio of puts to calls. The sample is drawn from the blockchain.info (now blockchain.com) website, Datastream, and the NYSE and CBOE website and covers the period between September 22nd, 2010 and December 30th, 2016.

| | $\alpha$ | $R_{Mkt} - R_f$ | **Trade1** | **Trade2** | **Trade3** | **Ptc** | $R^2$**(%)** | **Adj** $R^2$ | **Annual** $\alpha$ **(%)** |
|---|---|---|---|---|---|---|---|---|---|
| **Model 1** | **0.51***** | **0.27** | | | | | 0.15 | 0.09 | 545.53 |
| p-value | 0.0004 | 0.1181 | | | | | | | |
| **Model 1a** | **0.68**** | **0.42** | **-0.13** | | | | 0.18 | 0.05 | 1095.19 |
| p-value | 0.0188 | 0.126 | 0.4475 | | | | | | |
| **Model 1b** | **0.89***** | **0.20** | | **-0.34***** | | | 0.6 | 0.47 | 2473.01 |
| p-value | 0.0001 | 0.2433 | | 0.0074 | | | | | |
| **Model 1c** | **0.50***** | **0.26** | | | **-0.001** | | 0.14 | 0.01 | 514.60 |
| p-value | 0.0041 | 0.1459 | | | 0.9526 | | | | |
| **Model 1d** | **0.33** | **0.27** | | | | **0.263** | 0.14 | 0.01 | 1428.02 |
| p-value | 0.7498 | 0.1659 | | | | 0.8696 | | | |

**Table 3.16 Controlling for market sentiment in the FF model (Model 2)**

This table controls Bitcoin performance by including proxies for market sentiment in the FF model (Model 2). We use four proxies of market sentiment: $Trade1$ is the ratio of advancing issues on declining issues; $Trade2$ is the ratio of advancing issues on declining issues including volume; $rade3$ is the ratio of new highs on news lows; $PtC$ is the ratio of puts to calls. The sample is drawn from the blockchain.info (now blockchain.com) website, Datastream, and the NYSE and CBOE website and covers the period between September 22nd, 2010 and December 30th, 2016.

| | $\alpha$ | $R_{Mkt} - R_f$ | SMB | HML | **Trade1** | **Trade2** | **Trade3** | **Ptc** | $R^2$**(%)** | **Adj** $R^2$ | **Annual** $\alpha$ **(%)** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Model 2** | **0.51*****| **0.21** | **-0.29** | **0.25** | | | | | 0.19 | 0.01 | 548.75 |
| p-value | 0.0004 | 0.2645 | 0.5396 | 0.6216 | | | | | | | |
| **Model 2a** | **0.69**** | **0.36** | **-0.34** | **0.21** | **-0.13** | | | | 0.22 | -0.03 | 1125.55 |
| p-value | 0.0177 | 0.2051 | 0.4794 | 0.6854 | 0.4337 | | | | | | |
| **Model 2b** | **0.89***** | **0.16** | **-0.28** | **0.09** | | **-0.34***** | | | 0.62 | 0.37 | 2422.31 |
| p-value | 0.0001 | 0.414 | 0.5575 | 0.8581 | | 0.0087 | | | | | |
| **Model 2c** | **0.50***** | **0.20** | **-0.33** | **0.21** | | | **-0.0004** | | 0.18 | -0.07 | 514.07 |
| p-value | 0.0042 | 0.3145 | 0.5029 | 0.6757 | | | 0.9628 | | | | |
| **Model 2d** | **0.38** | **0.21** | **-0.32** | **0.22** | | | | **0.20** | 0.18 | -0.07 | 292.68 |
| p-value | 0.7197 | 0.3321 | 0.5126 | 0.667 | | | | 0.9016 | | | |

**Table 3.17 Controlling for market sentiment in the FF extended model (Model 3)**

This table controls Bitcoin performance by including proxies for market sentiment in the extended FF model (Model m 3). We use four proxies of market sentiment: $Trade1$ is the ratio of advancing issues on declining issues; $Trade2$ is the ratio of advancing issues on declining issues including volume; $Trade3$ is the ratio of new highs on news lows; $PtC$ is the ratio of puts to calls. The sample is drawn from the blockchain.info (now blockchain.com) website, Datastream, and the NYSE and CBOE website and covers the period between September 22nd, 2010 and December 30th, 2016.

| | $\alpha$ | $R_{Mkt} - R_f$ | SMB | HML | Bonds | Gold | **Trade1** | **Trade2** | **Trade3** | **Ptc** | $R^2$(%) | **Adj** $R^2$ | **Annual** $\alpha$ **(%)** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Model 3** | **0.51*****| **0.17** | **-0.45** | **0.29** | **0.20** | **0.26** | | | | | 0.35 | 0.05 | 544.03 |
| p-value | 0.0004 | 0.3596 | 0.3569 | 0.5595 | 0.1506 | 0.5966 | | | | | | | |
| **Model 3a** | **0.72**** | **0.34** | **-0.51** | **0.25** | **0.21** | **0.26** | **-0.15** | | | | 0.4 | 0.02 | 1257.34 |
| p-value | 0.0138 | 0.2256 | 0.305 | 0.6232 | 0.1409 | 0.6039 | 0.3687 | | | | | | |
| **Model 3b** | **0.88***** | **0.13** | **-0.44** | **0.14** | **0.17** | **0.37** | | **-0.33***** | | | 0.77 | 0.39 | 2366.90 |
| p-value | 0.0001 | 0.5103 | 0.3791 | 0.7856 | 0.2227 | 0.4629 | | 0.0096 | | | | | |
| **Model 3c** | **0.50***** | **0.16** | **-0.48** | **0.26** | **0.20** | **0.25** | | | **0.00** | | 0.35 | -0.03 | 526.39 |
| p-value | 0.0038 | 0.4118 | 0.3332 | 0.6107 | 0.1541 | 0.6213 | | | 0.9033 | | | | |
| **Model 3d** | **0.55** | **0.15** | **-0.48** | **0.26** | **0.20** | **0.26** | | | | **-0.07** | 0.35 | -0.03 | 638.77 |
| p-value | 0.6014 | 0.4791 | 0.3308 | 0.6045 | 0.1542 | 0.6026 | | | | 0.9639 | | | |

## 3.6 Conclusion

Bitcoin is a cryptocurrency that appeared in 2008. The growth of its value exhibits a very volatile price and provides a very specific risk-return profile for investors. After briefly justifying the asset nature of Bitcoin, most precisely its common-stock-like nature, our article focuses on its main objective, which is to empirically test its performance. Even if Bitcoin belongs to cryptocurrencies, this asset does not seem to respect all properties of a fiat money (medium of exchange, unit of account and store of value). Indeed, its economic and legal characteristics, together with its risk-return profile, make it look mostly like a financial contract. Its specific risk-return profile leads us to consider that Bitcoin may be assimilated to common stock. Fundamentally, we find that Bitcoin is lowly correlated to existing asset classes, which provides opportunities for portfolio diversification, and generates highly significant risk-adjusted returns, of similar magnitude for global, Europe and Asia-Pacific regions. The same result applies for the Chinese market. These results are stable to the specifications of our regression models, which reside in the CAPM, Fama–French three-factor models, and their extensions that includes other factors. Our results are robust to econometric methodologies that account for non-normality problems with the regressions' errors and to market sentiment variables.

After controlling for market sentiment with the $PtC$ variable, the Bitcoin's $\alpha$ is no more significant in all model specifications and for all regions. It could be useful in further research to test the market sentiment associated to Bitcoin performance by using additional proxies, such as the proxy of closed-end fund which we find in the international market sentiment literature (Lee et al., 1991). Another proxy is the fear and greed Index which takes in consideration different proxies of market sentiment (market momentum, put and call, safe haven demand, stock price breadth and stock price strength, market volatility and junk bond demand) in only one index. Research could be improved by performing a more robust analysis to test whether Bitcoin is a speculative bubble. The high performance obtained by Bitcoin in the regions analyzed in this paper, and the low correlation with existing assets may be a consequence of this.

## References


Antonopoulos, A. (2015). *Mastering Bitcoin*, O'Reilly Media.

Bartos, J. (2015). Does bitcoin follow the hypothesis of efficient market?, *International Journal of Economic Sciences* **IV**(2): 10–23.

Baur, D. G., Hong, K. and Lee, A. D. (2016). Virtual currencies: Media of exchange or speculative asset?, *SWIF Institute Working Paper* (2014-007).

Bhambhwani, S., Delikouras, S. and Korniotis, G. (2019). Do fundamentals drive cryptocurrency prices?, *SSNR Elec. Journal* .

Biais, B., Bisière, C., Bouvard, M., Casamatta, C. and Menkveld, A. (2018). Equilibrium bitcoin pricing, *SSNR Elec. Journal* .

Blau, B. (2017). Price dynamics and speculative trading in bitcoin, *Research in International Business and Finance* **41**: 493–499.

Bouri, E., Molnár, P., Azzi, G., Roubaud, D. and Hagfors, L. I. (2016). On the hedge and safe haven properties of bitcoin: Is it really more than a diversifier?, *Finance Research Letters* **20**: 192–198.

Brière, M., Oosterlinck, K. and Szafarz, A. (2015). Virtual currency, tangible return: Portfolio diversification with bitcoins, *Journal of Asset Management* **16**(6): 365–373.

Brown, G. and Cliff, M. (2004). Investor sentiment and the near-term stock market, *Journal of Empirical Finance* **11**(1): 1–27.

Burniske, C. and White, A. (2017). Bitcoin: Ringing the bell for a new asset class, *Ark Invest Research* .

Cheah, E.-T. and Fry, J. (2015). Speculative bubbles in bitcoin markets? An empirical investigation into the fundamental value of bitcoin, *Economics Letters* **130**: 32–36.

Cheung, C., Hoguet, G. and Ng, S. (2014). Value, size, momentum, dividend yield, and volatility in China's A-share market, *The Journal of Portfolio Management* **41**(5): 57–70.

Dwyer, G. (2015). The economics of bitcoin and similar private digital currencies, *Journal of Financial Stability* **17**(C): 81–91.

Dyhrberg, A. H. (2016a). Bitcoin, gold and the dollar – A GARCH volatility analysis, *Finance Research Letters* **16**: 85–92.

Dyhrberg, A. H. (2016b). Hedging capabilities of bitcoin. Is it the virtual gold?, *Finance Research Letters* **16**: 139–144.

Easley, D., O'Hara, M. and Basu, S. (2019). From mining to markets: The evolution of bitcoin transaction fees, *Journal of Financial Economics* **134**(1): 91–109.

Fama, E. F. and French, K. R. (2012). Size, value, and momentum in international stock returns, *Journal of Financial Economics* **105**(3): 457–472.

Fama, E. and French, K. (1992). The cross-section of expected stock returns, *The Journal of Finance* **XLVII**(2): 427–465.

Figuet, J.-M. (2016). Bitcoin et blockchain : quelles opportunités ?, *Revue d'économie financière* **123**(3): 325–338.

Gallagher, L. A. and Taylor, M. P. (2000). Measuring the temporary component of stock prices: robust multivariate analysis, *Economics Letters* **67**(2): 193–200.

Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. C. and Siering, M. (2014). Bitcoin - Asset or Currency? Revealing users' hidden intentions, *Twenty Second European Conference on Information Systems*.

Grant, J. M. (2014). Is bitcoin money?: Implications for bitcoin derivatives regulation and security interest treatment of bitcoins under article 9 of the uniform commercial code, *New York University (NYU), School of Law* .

Hansen, L. P. (1982). Large sample properties of generalized method of moments estimators, *Econometrica* **50**(4): 1029–1054.

Hayes, A. S. (2018). Bitcoin price and its marginal cost of production: Support for a fundamental value, *Applied Economics Letters* **Forthcoming**.

Heuson, A. J. and Hutchinson, M. C. (2015). Which hedge fund managers deliver alpha?, *SSRN Elec. Journal* .

Im, K. S. and Schmidt, P. (2008). More efficient estimation under non-normality when higher moments do not depend on the regressors, using residual augmented least squares, *Journal of Econometrics* **144**(1): 219–233.

Kajtazi, A. and Moro, A. (2017). Bitcoin, portfolio diversification and Chinese financial markets, *SSRN Electronic Journal* **10**.

Kancs, D., Ciaian, P. and Miroslava, R. (2015). The digital agenda of virtual currencies. Can bitcoin become a global currency?, *Publications Office of the European Union, JRC Technical report* .

Kristoufek, L. (2019). Is the bitcoin price dynamics economically reasonable? Evidence from fundamental laws, *Physica A: Statistical Mechanics and its Applications* **Online**(120873).

Lakosmki-Laguerre, O. and Desmedt, L. (2015). L'alternative monétaire bitcoin : une perspective institutionnaliste, *Revue de la régulation* **18**(2).

Lee, C., Shleifer, A. and Thaler, R. (1991). Sentiment and the closed-end fund puzzle, *The Journal Of Finance* **46**(1): 75–109.

Meng, Z. and Ju, R. (2013). Explanatory power of three-factor model on A-share market of Shanghai exchange in China, *Conference on Advances in Social Science, Humanities and Management* .

MSCI (2016). A global implementation of the Fama-French 5-factor model, *MSCI Research Insight* .

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system, *White paper* .

Pagnotta, E. and Buraschi, A. (2018). An equilibrium valuation of bitcoin and decentralized network assets: Non-technical summary, *SSRN Elec. Journal* .

Raiborn, C. and Sivitanides, M. (2015). Accounting issues related to bitcoins, *Journal of Corporate Accounting and Finance* **26**(2): 25–34.

Selgin, G. (2015). Synthetic commodity money, *Journal of Financial Stability* **17**(92-99).

Sockin, M. and Xiong, W. (2018). A model of cryptocurrencies, *Working Paper* **NBER AP**.

Tschorsch, F. and Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies, *IEEE Communications Surveys & Tutorials* **18**(3): 2084–2123.

Urquhart, A. (2016). The inefficiency of bitcoin, *Economics Letter* **148**: 80–82.

Wang, F. and Xu, Y. (2004). What determines Chinese stock returns?, *Financial Analysts Journal* **60**(6): 65–77.

Wheatley, S., Sornette, D., Huber, T., Reppen, M. and Gantner, R. (2019). Are bitcoin bubbles predictable? Combining a generalized Metcalfe's Law and the log-periodic power law singularity model, *Royal Society Open Science* **6**.

Xu, J. and Zhang, S. (2014). The Fama-French three factors in the Chinese stock market, *China Accounting and Finance Review* **16**(2): 210–227.

Yermack, D. (2015). Is bitcoin a real currency? An economic appraisal, *in* D. L. K. Cheun (ed.), *Handbook of Digital Currency Bitcoin, Innovation, Financial Instruments, and Big Data*, chapter 2, pp. 31–43.

## Chapter 4

# Speculative bubbles and contagion effect in the cryptocurrency market

The high performance obtained by cryptocurrencies is due to their high returns as well as their high volatility. This article aims to analyze the speculative bubble aspect of the cryptocurrency market by studying its multiple potential bubbles over the entire period of Bitcoin, Ether, Litecoin and Ripple using the Phillips, Shi and Yu Model (PSY) methodology (Phillips et al., 2015) taking into consideration heteroskedasticity issues (Phillips and Shi, 2018). Second, we study the main peak/burst of the cryptocurrency market at the end of 2017 using the Log Period Power Model (LPPL) of (Johansen et al., 2000). The results suggest some periods of bubbles implying an effect between cryptocurrencies.

## 4.1 Introduction

The cryptocurrency market is a specific market on which only cryptocurrencies are traded. This market performs particularly well for investors, unlike assets in more traditional markets (such as common stocks), as we demonstrated in Chapter 2 of this thesis. These findings are robust regardless the region (World, Europe, Asia-Pacific and China) and the inclusion of market sentiment variables. However, this market, which is fully electronic and dematerialized, is vulnerable regarding cyber-attacks, especially on exchange platforms. An example for this is the recent hack of the exchange platform, named Coincheck (loss of $400 million in January 2018 for its customers).

In addition, trust in cryptocurrencies is often questioned, notably regarding their cryptographic principles as well as the high volatility of their price. The Bitcoin value progressively increased during the period 2015–2016, reaching $1,002.5 on January 2nd, 2017. It continued to grow at an exponential rate reaching $19,395.83 on December 18th, 2017 (i.e. an increase of 90% in approximately one single year) before experiencing a 40% decrease in the following days ($13,668 on December 25th, 2017) and a continuous decrease in the following months until it reached the value of $6,000 in September 2018. This volatility raises the question of the cryptocurrencies economic value and more specifically the existence of speculative bubbles.

As the Chairman of the US Federal Reserve, Alan Greenspan, stated in 2002, "We at the Federal Reserve considered a number of issues related to asset bubbles–that is, surges in prices of assets to unsustainable levels. As events evolved, we recognized that, despite our suspicions, it was very difficult to definitively identify a bubble until after the fact–that is, when its bursting confirmed its existence."[1]. Theoretically, a bubble is defined as the deviation of the value of a given asset from its fundamental value, creating a mispricing phenomenon. In practice, the detection is not an easy task because it may require estimating "the true" value of an asset.

Based on famous historical bubbles such as the "Tulip mania" or the "Dot-com bubble", Chang et al. (2016) find common sources of the bubble development: the "showmanship" of the promoters (that convince investors about a new

[1]Remarks by Chairman Alan Greenspan;Economic volatility at a symposium sponsored by the Federal Reserve Bank of Kansas City, Jackson Hole, Wyoming August 30th, 2002.

asset and inflate the prices) and the speculation about new products, ventures or technologies. They highlight the "positive feedbacks loop" of this phenomenon, a concept shared by (Filimonov and Sornette, 2013). Indeed, Filimonov and Sornette (2013) define financial bubbles as "transient upward accelerations of the observed price above a fundamental value. The paradox is that the determination of a bubble requires, in this definition, a precise determination of what the fundamental value is. The fundamental value is in general poorly constrained. In addition, a transient exponential acceleration of the observed price that would be taken as the diagnostic of a developing bubble is not distinguishable from an exponentially growing fundamental price". Different empirical methodologies have been used to detect and predict a bubble and more precisely a crash after an important exponential increase in prices. These methodologies estimate a bubble detection using the fundamental value. The Philipps, Shi and Yu (PSY) methodology model based on the work of (Phillips et al., 2011), (Phillips et al., 2015) and (Phillips and Shi, 2018) does not require knowing the fundamental value and aims to detect multiple bubbles over time for an asset. In the same vein, the LPPL based on the work of Johansen et al. (2000) suggests a model for the detection but also for the prediction of the critical time of crash without using the fundamental value. This model is widely used for research on financial markets, (Sornette and Zhou, 2002), (Zhou and Sornette, 2003), (Lin et al., 2009), (Sornette et al., 2009), (Jiang et al., 2010); and more recently, for research on cryptocurrency markets where the fundamental value of traded assets remains an important issue, (MacDonnell, 2014), (Cheah and Fry, 2015), (Fry and Cheah, 2016).

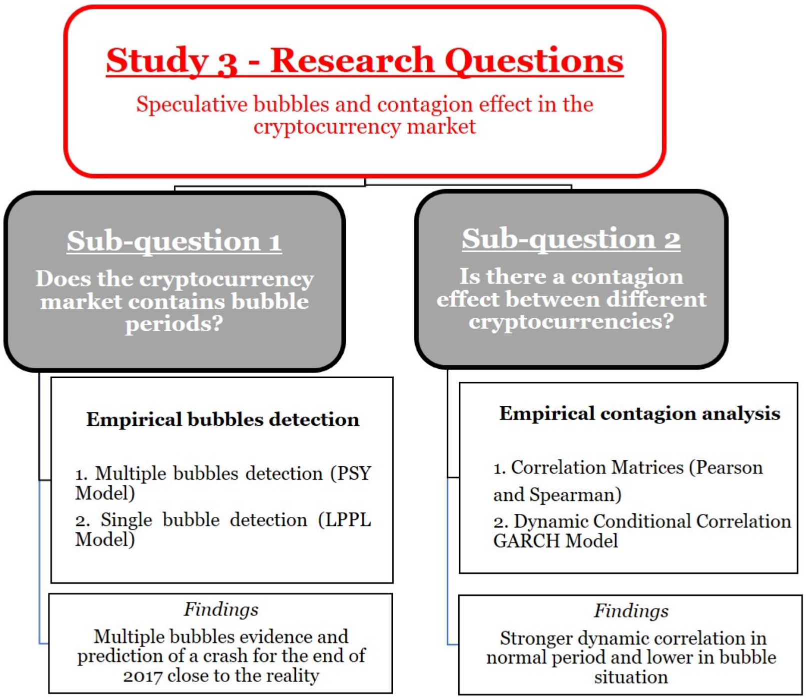


**Figure 4.1 Research questions of the third study**

This figure presents the sub-research questions of the third study.

Ignoring the fundamental value of the cryptocurrency, this study aims to detect multiple bubbles in the cryptocurrency market, using the four main cryptocurrencies as proxies: Bitcoin, Ether, Ripple and Litecoin. The research is performed using the (Phillips and Shi, 2018) methodology taking into consideration the heteroskedasticity issues, a methodology largely used in the literature for Bitcoin, (Bouri et al., 2019), (Geuder et al., 2018). We focus our study on the main peak/burst in 2017 in the cryptocurrency market using the LPPL method (Johansen et al., 2000). Figure 4.1 - *Research questions of the third study* presents these sub-research questions, their methodologies and main findings.

The main contributions of this article are to examine multiple bubbles on the four main cryptocurrencies including Bitcoin, and more precisely, the major peak/burst of the cryptocurrency market related to the December 2017/January 2018 period which has not been studied much in the literature. In addition, this research allows to highlight the correlation effect between the different cryptocurrency to each other. As robustness tests, first, we analyze the contagion between these four cryptocurrencies using the methodology of Dynamic

Conditional Correlation Method (Engle and Sheppard, 2001). Second, we test the fundamental value estimations suggested by researchers in the recent literature to confirm our results, (Wheatley et al., 2019).

The rest of this chapter is structured as follows. The literature review is presented is Section 2. Section 3 describes the methodology. Section 4 discusses the results about multiple bubbles and the 2017's bubble analyze. Section 5 proposes some robustness tests related to contagion and to fundamental value. Section 6 presents the conclusion.

## 4.2 Literature review

### 4.2.1 Speculative nature of the cryptocurrencies

If the fundamental value of the cryptocurrencies is zero (Cheah and Fry, 2015), then the cryptocurrency phenomenon would just be a long run speculative bubble. A stream of the literature focuses on estimating the fundamental value of cryptocurrencies. The main factors that drive the fundamental value are: (1) The cost of production (mining[2]) (Garcia et al., 2014), (Corbet et al., 2017), (Hayes, 2017), (Hayes, 2018), (Pagnotta and Buraschi, 2018), (Bhambhwani et al., 2019); (3) The market size (Fantazzini et al., 2017); (2) The users and their behaviors and more precisely the network of users in a decentralized manner[3] (Abadi and Brunnermeier, 2018), (Pagnotta and Buraschi, 2018), (Sockin and Xiong, 2018), (Bhambhwani et al., 2019), (Wheatley et al., 2019); (4) Transactions fees (Biais et al., 2018), (Easley et al., Forthcoming); and (5) other financial and economic aspects such as return, volatility, liquidity (Corbet et al., 2017), exchange rates, traded volume (Kristoufek, 2019).

It is possible to find some evidences of bubbles on the cryptocurrency market even if the fundamental value is non-negative. In this case, the price does not collapse to zero at the end of the bubble but to its fundamental value (Hayes, 2018).

The dynamics of cryptocurrencies since their creation seems to be similar to the DotCom phenomena in the 2000's (Ofek and Richardson, 2003). The success of cryptocurrencies is compared to the one of the World Wide Web as their share similar innovative features (Folkinshteyn et al., 2015) such as a

[2]See the list of terms and abbreviations

[3]see figure 1.3 in Chapter 1 and the list of terms and abbreviations part.

lead-user[4] via a white paper, a technology that gathers several IT innovations, a nature combining ubiquity, open-source and decentralization, as well as the creation of new standards. These characteristics seems to be factors of bubbles creation similar to the DotCom ones (Chang et al., 2016).

In the previous Chapter 3, we argue that Bitcoin may be assimilated to financial assets (common stocks) by presenting a literature review about the investment role of Bitcoin compared to the use as a means of exchange. A stream of the literature presents the speculative investment aspect of cryptocurrencies (Baek and Elbeck, 2014), (Yermack, 2017), (Baur et al., 2016), the participants intentions (Glaser et al., 2014) and short-term, speculation intention (de la Horra et al., 2019).

### 4.2.2 The financial bubble literature and methods for their detection

In the outstanding bubble literature, scholars distinguish between "irrational" and "rational" bubbles (Dale et al., 2005).

On the one hand, irrational bubbles are based on heterogeneous expectations and multiple equilibrium; the rationality, homogeneity and symmetric information assumptions are not satisfied. On the market, there exist irrational behaviors of investment that makes the price moves away from its fundamental value. Investments strategies based on optimistic expectation, fashion or fads (Shiller, 2005) and psychological behaviors such as herding behavior can generate bubbles (Vissing-Jorgensen, 2003), (Dale et al., 2005), (Brunnermeier, 2008), (Cheah and Fry, 2015). Empirical works show that this psychological impact through the optimistic/pessimistic behaviors of investors (Harrison and Kreps, 1978), in short-sale constraints (Miller, 1977), in the Internet Bubble (Ofek and Richardson, 2003), in large volume and high volatility (Scheinkman and Xiong, 2003).

On the other hand, rational bubbles are based on rational anticipations that could create mispricing and therefore a bubble creation. If investors know that the actual price is not the fundamental value of the asset, but they are willing to pay more because the expectation of selling later at a higher price is greater than a crash price (Flood and Hodrick, 1990), (Dale et al., 2005), (Gurkaynak, 2008), (Hafner, 2018).

[4] A lead-user has an influence to influence and convince new entrants to invest in the innovation. See Chapter 2.

Dale et al. (2005) present distinction between the "rational intrinsic bubbles" and "rational extrinsic bubbles". The former is defined by a misevaluation of the fundamental value "systematically and persistently", and that occurs during innovation process when it is difficult to estimate the fundamental value (Froot and Obstfeld, 1991). The "rational extrinsic bubbles" happen when the bubbles are growing based on exogenous events in an uncertain environment (Azariadis, 1998) particularly if it is affected by information asymmetry between traders. Numerous researchers study the "rational bubbles" and its detection measures inside different markets, such as the burst probability, (Blanchard and Watson, 1982).

According to (Brunnermeier, 2008), several methods exist to detect bubbles in a rational expectation and symmetric information. The first one is the regression analysis tool (Flood and Garber, 1980) which uses the unit root test and co-integration test notably to compare the explosive behavior of stock prices and dividends (Diba and Grossman, 1988). They prove the positive relationship between the stationarity of the stock prices and the stationarity of the dividends in normal situations whereas this link stops when the bubble situation appears (the bubble process is non-stationary). They test the null-hypothesis of no bubble where dividends and stocks prices should be co-integrated using most of times the Dickey Fuller Test. Evans (1991) reverses the idea that the unit root test is a good tool to reject the alternative hypothesis (existence of bubbles). A rejection of bubble existence hypothesis is sometimes due to model failure West (1987). These authors adapt the model with both bubble and no-bubble hypotheses sequentially using the Haussman coefficient restriction test. This test faces some issues: non-stationarity, the order of AR, econometric models choices issues (sample and periods bias) (Gurkaynak, 2008).

Another method is called the "variance bounds tests" (LeRoy and Porter, 1981), (Shiller, 2005). The idea is to compare the *ex-post* "rational price" (determined by the dividends that the investor will actually receive) with the actual price on the market. If the market is efficient, both should be similar. The Shiller test shows if the actual volatility of an asset price exceeds the bounded variance obtained *ex-post* in the "rational" price. However, the variance bound can be biased in practice through sample bias (Flavin, 1983), times-series use instead of cross-section one (Kleidon, 1986), non-stationarity problems of prices and dividends (Marsh and Merton, 1986), time-variation aspects using dividend/price ratio (Flood et al., 1986), (Campbell and Shiller, 1988).

The ratio dividend/price is also used to detected bubbles using the Augmented Dickey Fuller unit root analysis (Taipalus, 2012), Phillips-Perron test (Diba and Grossman, 1988) and its extension such as the Generalized sup ADF test (Phillips et al., 2011), (Phillips et al., 2015), or the wild bootstrap which takes in consideration heteroskedasticity issues (Phillips and Shi, 2018). Cryptocurrencies does not have dividends. There exist as well other markets such as the foreign exchange market are not concerned by dividends and may be modelled by other models of bubble detection (e.g. the uncertainty bubble model of (Woo, 1987)), (Frankel and Froot, 1990). Previously (in Chapter 2), we argued that cryptocurrency shares important features with financial assets and more precisely common stocks. We decide to focus our analysis on bubble detection methods applied on the stock market.

There exists a general method based on physical discipline called Log Periodic Power Law Model (Sornette et al., 1996), (Sornette and Johansen, 1997), (Sornette, 2003), (Lin et al., 2009), (Lin and Sornette, 2009), (Sornette, 2009) that does not require the use of the fundamental value and has been applied on different markets. The LPPL model was applied in finance for the first time by Sornette to test the market crash of October 1987, then for real-estate markets in the US during the mid-2006 bubble (Sornette and Zhou, 2002), in the UK during the mid-2004 bubble (Zhou and Sornette, 2003), and on the commodity market with the oil bubble in July 2008 (Sornette et al., 2009), and the gold market (Johansen and Sornette, 1990). The same model was applied for stock markets crashes, the 1990s Nasdaq bubble (Phillips et al., 2011), the Chinese stock market (2005-2007 and 2008-2009) (Jiang et al., 2010), and more recently on the cryptocurrency market (see the previous literature on section 4.2). Whilst the prior literature performs *ex-post* estimation of the crash occurrence (i.e. when the crash already happened using historical data), recent studies of these authors attempt to predict crashes using actual data. Their research is therefore kept secret until the estimated date of the crash has passed (The Financial Bubble Experiment[5]). The intuition is that price time series are defined by a power law and log-periodic oscillation until a critical time when the price could crash. We will present the model in more detail in the next part 4.3.2.1.

[5]https://www.ethz.ch/content/specialinterest/mtec/chair-of-entrepreneurial-risks/en/financial-crisis-observatory.html

### 4.2.3 Cryptocurrencies and bubble aspects

Since the creation of the so-called "cryptocurrencies" such as Bitcoin in 2008 (Nakamoto, 2008), scholars define their nature without any emerging consensus. The existing literature shows evidence that cryptocurrencies may be considered either as a currency (Grant, 2014), (Kancs et al., 2015), (Figuet, 2016), as a commodity such as gold (Selgin, 2015), (Dyhrberg, 2016a), (Dyhrberg, 2016b), (Bouri et al., 2016) or as an asset such as common stocks (Baur et al., 2016), (Glaser et al., 2014), (Yermack, 2017) (see chapter 2). Godsiff (2015), Umeh (2016) and Gangwal and Longin (2018) highlight that cryptocurrencies generate speculative bubbles due to their asset nature rather than a currency, in addition to the rapid increase of its price beside its high volatility.

Following this idea, recent research attempts to show the inefficiency of the cryptocurrency market, (Urquhart, 2017), (Nadarajah and Chu, 2017) and reveal empirically some evidences of bubbles using different methodology of bubble detection. If we take a look at the graph of Bitcoin price in Figure 4.2 - *The top-4 cryptocurrencies prices in USD*, we can notice a first peak/burst in the end of 2013 when Bitcoin's price reached, for the first time, a value of $1,000. This first peak/burst was studied in the existing literature. Using a battery of detection tests based on the (Johansen et al., 2000) works, Cheah and Fry (2015) detect that the crash of December 2013 was preceded by a bubble. One year later, the same authors analyze the peak of December 2013 using a second cryptocurrency, Ripple, in addition to Bitcoin. The authors find that: first, the existence of negative bubbles[6] for both of the aforementioned cryptocurrencies and second, the existence of a spillover from Ripple to Bitcoin (Fry and Cheah, 2016). Analyzing the factors that drive the value of Bitcoin, MacDonnell (2014) confirms the same conclusion regarding the Bitcoin prices crash in December 2013. The results also confirm that the LPPL model is relevant to detect a single bubble on the cryptocurrency market. To detect multiple bubbles, some researches use Philipps, Shi and Yu (**PSY**) methodology (Phillips et al., 2011) and (Phillips and Shi, 2018) based on the unit root analysis (Fantazzini et al., 2017). During the 2011–2013 period, an explosive behavior in Bitcoin prices (Malhotra and Maloo, 2014) and three bubbles are detected by (Cheung et al.,

[6]Fry and Cheah (2016) define a negative bubble as the result of dramatic prices falls compared to a speculative bubble that is the result of dramatic price increases.

2015).

In 2017, the price of Bitcoin was again growing exponentially (see Figure 4.2). Using the same method mentioned before, Corbet et al. (2017) find that Bitcoin and Ether are in a phase of bubble on November 9th, 2017. This second period, at the end of 2017, shows an incredible increase of prices reaching in December 2017, ($19,395.83 for Bitcoin, Figure 4.2).

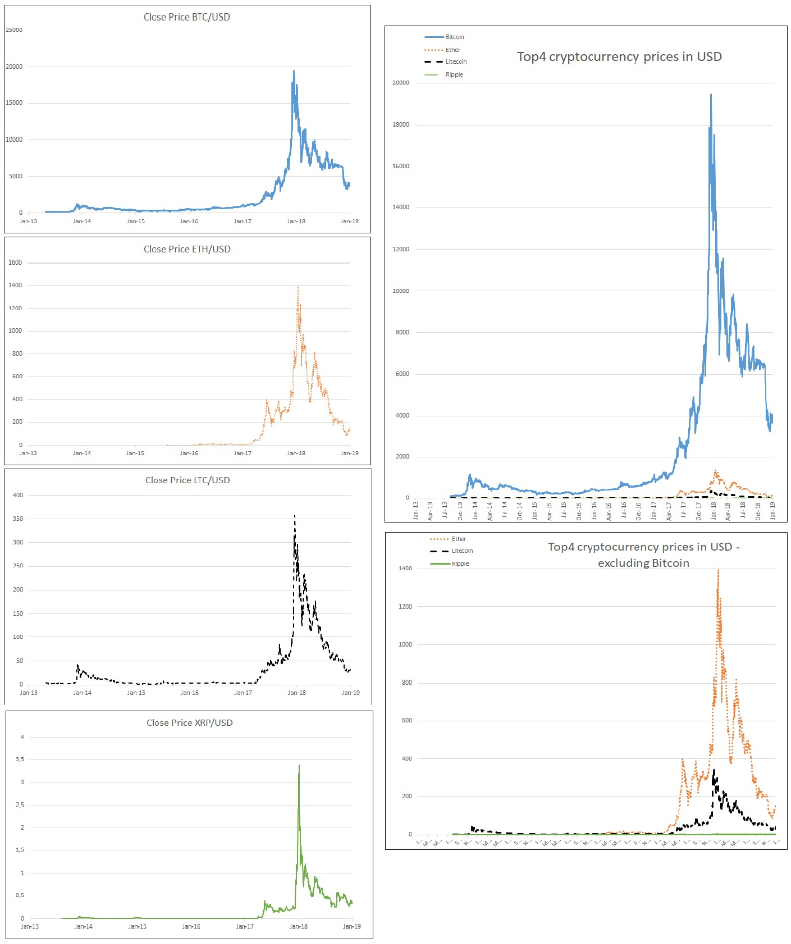


**Figure 4.2 The top-4 cryptocurrencies prices in USD**
This figure shows the Bitcoin (blue), the Ether (dotted-orange), the Litecoin (dashed-black) and the Ripple (green) prices expressed in US dollars (USD) over the period October 2013 to July 2019.

Some other researchers studied, more recently, a multiple bubble detection during a larger period, in favor of the presence of bubble in the cryptocurrency markets (Hafner, 2018), (Su et al., 2018), (Bouri et al., 2019), (Li et al., 2019), (Vogiazas and Alexiou, 2019), (Wheatley et al., 2019). A part of the literature does not support the bubble evidence in 2017 for Bitcoin, (Chaim and Laurini, 2019) and for Ripple (Fry, 2018).

In this chapter, we extend the work of (Geuder et al., 2018) and (Wheatley et al., 2019) by studying the cryptocurrency market on a longer period of time and using four different cryptocurrencies in order to highlight the differences between them (contagion).

## 4.3 Methodology

This chapter aims to present the methodology used for the multiple bubbles detection and the single detection and prediction of the biggest peak/burst of cryptocurrency market at the end of 2017.

According to the previous literature (see part 4.2), we find the PSY methodology (Phillips et al., 2011), (Phillips et al., 2015) appropriate to analyze the multiple bubbles detection. There is no need to know the fundamental value to apply this bubble detection test. The methodology is frequently applied in the literature. We apply this methodology for several cryptocurrencies; such as Bitcoin, Ether, Litecoin and Ripple, for a period of time longer than analyzed before. We apply the most recent evolution of the PSY methodology based on the article (Phillips and Shi, 2018) taking into consideration the heteroskedasticity issue.

The LPPL model (Johansen et al., 2000) is largely used in the cryptocurrency market, see the part 4.2.3. The model does not require to know the fundamental value as well, and the price dynamics of the cryptocurrency behave in the sense of the LPPL bubble definition (before a crash, the prices are super-exponential and oscillate until a critical time). Cagli (2019) find that the cryptocurrency prices are explosive.

In this part, we present both, PSY and LPPL, models, in theory and its implementation, as well as the data used in the research.

### 4.3.1 Multiple bubbles detection

#### 4.3.1.1 The PSY Model

The PSY model is firstly presented in the articles of (Phillips et al., 2011) and (Phillips et al., 2015). Here, we apply the most recent evolution of the model based on (Phillips and Shi, 2018). The novelty in this procedure is the mitigation of a potential heteroskedasticity problem using a bootstrap procedure. The idea is to detect in real time the bubbles using a recursive evolving algorithm employing the Augmented-Dickey Fuller (ADF) model.

The null hypothesis is the "normal situation" of the market behavior in which prices follow a martingale process:

$$y_t = g_T + y_{t-1} + u_t \tag{4.1}$$

Where $y_t$,$y_{t-1}$ is the price at time $t$ and time $t-1$. $g_T = k\tau^{-\gamma}$ captures any small drifts asymptotically negligible being smaller than the martingale component, where $k$ is a constant, $\gamma > 1/2$ and $\tau$ the sample size. The regression model is :

$$\Delta y_t = \mu + \rho y_{t-1} + \sum_{j=1}^{p} \phi_j \delta y_{t-j} + u_t \tag{4.2}$$

Where $\rho$ is the lag term related to the serial correlation, selected by information criteria; the errors, $u_t$, are assumed independent and identically distributed, $\mu$ is the intercept but there is no time trend. The null hypothesis is : $\mu = g_T$ and $\rho = 0$ and the ADF statistic is the t-ratio of the least squares estimate of the coefficient $\rho$. For more details notably related to the recursive evolving algorithm, see the article of (Phillips and Shi, 2018).

The bubble identification model is presented, hereafter. The present value asset price is defined as:

$$P_t = \sum_{i=0}^{\infty}((\frac{1}{1+r_f})^i \underset{t}{\mathbb{E}}(D_{t+i}) + B_t \tag{4.3}$$

Where $P_t$ is the price of the asset, $D_t$ is the payoff received from the asset, $r_f$ is the risk-free rate, $\mathbb{E}_t(.)$ is the conditional expectation according to the information at time $t$, $B_t$ is the bubble component which satisfies the submartingale

(Diba and Grossman, 1988):

$$\mathop{\mathbb{E}}_{t}(B_{t+1}) = (1 + r_f)B_t \tag{4.4}$$

In normal situation, with no bubble, the degree non-stationarity of the asset price depends on the dividend. In bubble situation, the price dynamic is explosive and could be modelled by an explosive process:

$$\log P_t = \delta_T \log P_{t-1} + u_t \tag{4.5}$$

Where $\delta_T = 1 + c\tau^{-\eta}$ is the auto-regressive coefficient, where $c > 0$ and $\eta in(0, 1)$, therefore $\delta_T > 1$ is still in its general vicinity. If we detect a martingale process of the prices from a mildly explosive process, we detect the bubble situation. The null-hypothesis of the PSY test is:

$$H_0 : \mu = g_T \text{ and } \rho = 0$$

And the alternative hypothesis is:

$$H_A : \mu = 0 \text{ and } \rho > 0$$

#### 4.3.1.2 Fitting the PSY Model and its implementation

We use the procedure of (Phillips and Shi, 2018) using a bootstrap process in order to mitigate the heteroskedasticity issue and to fix the multiplicity issue in recursive procedure. The number of observations in the window over which the size has to be tested are $\tau_0$ and $\tau_b$.

- **First Step**: Based on the full sample of time and on the null-hypothesis of $\rho = 0$, run the regression model of the equation 4.2 to obtain the estimated residual $e_t$

- **Second Step - Wild Bootstrap**: For a sample size $\tau_0 + \tau_b - 1$, generate a bootstrap sample by :

$$\delta y_t^b = \sum_{j=1}^{p} \hat{\phi}_j \delta y_{t-j}^b + e_t^b \tag{4.6}$$

Where $\hat{\phi}_j$ are the OLS estimates obtained in the first step, the initial values are $y_i^b = y_i$, $i = 1, ..., j+1$ and $e_t^b = w_t e_l$ are the residuals where $w_t$ is randomly drawn from the standard normal distribution and $e_l$ is randomly drawn with replacement from the estimated residuals $e_t$ of the first step.

- **Third Step**: Compute the PSY test statistic sequence and its maximum value.

- **Fourth Step**: Repeat the second and third steps for $B = 999$ times.

- **Fifth Step**: The critical value is given by the 95% percentiles of the maximum statistic sequence.

To implement the previous algorithm, we follow the article of (Phillips and Shi, 2018) by using the R package "psymonitor"[7].

### 4.3.2 The main boom: 2017's peak/burst

#### 4.3.2.1 The LPPL Model

Crashes are unpredictable events with a low probability of occurrence and with huge consequences when they occur (the Black Swan Theory, (Taleb, 2007)). The picture is different in (Sornette et al., 1996), (Sornette and Johansen, 1997), (Johansen et al., 2000), (Sornette, 2003), (Lin and Sornette, 2009), (Lin et al., 2009). These articles focus on extreme events (outliers), called "dragon kings", considering the latter as rare and predictable, (Sornette, 2009).

They suggest to use a statistical model adapted from physics: the Log-periodic Power Laws model (LPPL)[8] in order to predict the crash of an endogenous bubble, (Johansen et al., 2000). The LPPL model defines "a bubble as a transient faster than exponential growth resulting from positive feedbacks" (Filimonov and Sornette, 2013). They show that the hyperbolic dimension of the prices growth (the growth rate growth itself) explaining the "faster than exponential" concept until reaching a critical point (singularity) where the probability of crash is high (Sornette and Cauwels, 2014) and can be explained by two main parts:

[7] https://cran.r-project.org/web/packages/psymonitor/index.html
[8] The main issue is to detect when a system reach a critical point.

1. **Power Law**: concerns the super exponential growth of price until a critical time where prices burst.

2. **Log periodicity**: concerns the price oscillations that go faster until the critical time.

The model hypotheses appear to fit the cryptocurrency market: the assets pay no dividend and there is no need for incorporating the interest rate. In addition, the model does not consider risk aversion, information asymmetries and market clearing conditions.

In this model, there are two kind of traders, rational ones who act in the same way, represented by a single agent, and noisy ones who by their herding behavior, are at the origin of the bubble growing until a moment (the critical time) where the crash happens (large number of orders have the same short position). All traders have to decide between buying or selling depending on the decision of others and on external influences. In the LPPL model, the "order state" that is, a state in which all traders take similar decisions (namely short positions) is considered as a bubble, whereas the "disorder state" concerns the normal market conditions when sell and buy orders coexist. In addition, a bubble can be self-sustained (meaning that the bubble can continue to grow up by itself) because of the positive feedbacks related to increasing risk and interaction between agents. In this model, the crash is defined by a probability distribution implying that rational agents receive a higher return to compensate the risk they take if the crash happens.

Johansen et al. (2000) present two levels of modeling. At the macro modeling level, a higher probability of crash implies an acceleration in the price increase, meaning that investors ask for a higher return because they take a higher risk in a bubble situation. The probability that numbers of investors will assume the same sell position simultaneously (causing the crash) is the hazard rate, $h(t)$ to explain the imitative process:

$$\frac{dh}{dt} = Ch^{\delta} \tag{4.7}$$

where $C$ is a positive constant, $\delta$ is the average number of interactions among the investors minus 1. To respect the singularity (critical point) in finite time $\delta > 1$, and therefore $h(t)^{\delta}$ captures the number of interactions between investors, $\delta$, is high (low), it will increase (decrease) the hazard rate.

By integrating 4.7, we obtain:

$$h(t) = (\frac{h_0}{t_c - t})^{\alpha} \tag{4.8}$$

where

$$\alpha \equiv \frac{1}{\delta - 1}$$

Where $t_c$ is a critical time, $\alpha$ is including between 0 and 1 to avoid that the price goes to infinity when $t$ is approaching $t_c$. More precisely, $\alpha > 0$ and $\delta > 1$ to have a critical point in finite time and a growth of h(t) such as $t$ is approaching $t_c$ and $\alpha < 1$ to make the price not diverging at the critical time. Therefore, we obtain $2 < \delta < \infty$ constraining the fact that an investor has to be in interaction with at least two agents.

The higher the price is compared to its fundamental value, the higher the hazard rate and the probability of crash will be because of self-fulfilling crisis principle. The idea is that a crisis happens because investors believe in it and they will generate the crisis by themselves.

$$\frac{dh}{dt} = Dp^{\mu} \tag{4.9}$$

where $D > 1$ is a constant and $\mu > 0$.

The self-fulfilling phenomenon is shown by the equation 4.9. The hazard rate (and thus the confidence) depends on the price movement departing from its fundamental value. When the price moves away from its fundamental value, the hazard rate increases and therefore, the price increases again to compensate the increasing risk taken in a bubble situation.

At the micro level, agents trade in a network in which the local behavior can have an impact on the general behavior, named "local self-reinforcing imitation" and modeled by the hierarchical diamond lattice. Each agent indexed by $i = 1, ..., I$ can be connected to other agents where $N(i)$ represents the number of agents connected to agent $i$. $s_i \in -1, +1$ are the only two states in which the agent can be. $-1$ means the agent is in bearish/selling situation whereas if the agent is in bullish/buying situation, the state is $+1$. The state of agent $i$ is defined by the Markov Process:

$$s_i = sign\left( K \sum_{k \in N(i)} s_j + \sigma \epsilon_i \right) \quad (4.10)$$

Where the function $sign$ is equal to $+1$ if the input is positive (if $x > 0$ thus $sign(x) = +1$) or equal to $-1$ if the input is negative (if $x < 0$ thus $sign(x) = -1$), $\epsilon$ is an independent and identically distributed random variable, $K > 0$[9] is a constant called "coupling strength" measures the tendency toward the imitation (leading to the order situation where only state; buy or sell is prominent) , as for $\sigma$ measures the tendency towards idiosyncratic behavior (leading to the disorder situation where buy and sell states coexist). Based on Isin model (Onsager, 1944), there exists a critical threshold, $K_c$, that allows to show the trade-off between the order situation (tendency to imitation) versus the disorder situation (tendency to idiosyncratic behavior).

1. When $K < K_c$, the imitation is small enough to be in the disorder situation. The sensibility to small global influence is low.

2. When $K \longrightarrow K_c$, agent formed groups to act in the same sense and take the same position. The sensitivity to small global influence is growing.

3. When $K > K_c$, the imitation behavior is large enough to be in order situation (all the agents take the same state).

The global situation is depending on the influence spread between agents making the state of some agent changing. The susceptibility quantity represents the degree of sensitivity to global influence (captured by $G$):

$$s_i = sign\left( K \sum_{k \in N(i)} s_j + \sigma \epsilon_i + G \right) \quad (4.11)$$

The average state of the market is: $M = (1/I) \sum_{i=1}^{I} s_i$.

- If $G = 0$, $E[M] = 0$
- If $G > 0$, $M > 0$
- If $G < 0$, $M < 0$

[9]The average of $K_{ij}$ is always positive even if they are some $K_{ij}$ that are negative.

Therefore, $E[M] * G >= 0$.

The susceptibility is defined such as:

$$\chi = \left.\frac{dE[M]}{dG}\right|_{G=0} \tag{4.12}$$

Johansen et al. (2000) argue that the "susceptibility" quantity measures "the ability of the system of agents to agree on an opinion" based on three explanations. The first one is the fact that the susceptibility is the sensitivity of the average state ($M$) to a small global influence. Second, the susceptibility is the variance of the average state (M) a constant time around its expectations of zero impacted by the random idiosyncratic shocks $\epsilon_i$. Third, the susceptibility measures proportionally the impact on a second agent of an intervention of a first agent to be in a certain state.

The asset price dynamics is based on the rational expectations and risk neutral hypothesis where the price follows a martingale process, $E_t[p(t')] = p(t), \forall t' > t$, a necessary condition to respect the no arbitrage hypothesis.

There exists $j$, a jump process (because there is a non-zero crash probability) where $j = -1$ before crash and $j = +1$ after the crash at time $t_c$. The hazard rate (i.e. the probability of the crash happen in the next time assuming that the crash is not yet occurred) is $h(t) = q(t)/[1 - Q(t)]$ where $q(t)$ is the probability density function of $t_c$, $Q(t)$ is its cumulative distribution function. When a crash occurs, the price falls by $k$ percent. The price dynamic is measured as:

$$dp = \mu(t)p(t)dt - kp(t)dj \tag{4.13}$$

$$E[dp] = \mu(t)p(t)dt - kp(t)[P(dj = 0) \times (dj = 0) + P(dj = 1) \times (dj = 1)] \tag{4.14}$$

$$E[dp] = \mu(t)p(t)dt - kp(t)[0 + h(t)dt] \tag{4.15}$$

$$E[dp] = \mu(t)p(t)dt - kp(t)h(t)dt \tag{4.16}$$

$E[dp]$ has to be zero because of the non-arbitrage and rational expectation conditions, therefore $\mu(t)p(t)dt - kp(t)h(t)dt = 0$ and by consequence, $\mu(t) = kh(t)$ putting in the last equation, the price dynamic is given by $d(\ln p(t)) = kh(t)$ where the solution is:

$$\ln\left[\frac{p(t)}{p(t_0)}\right] = \kappa \int_{t_0}^{t} h(t')\,\mathrm{d}t' \tag{4.17}$$

As stated previously, the price goes faster to compensate the risk taken by investors in situation when the probability of the crash is high. The price depends on the buy and sell orders of the traders impacted by neighbors in a network, therefore, the choice of the network is crucial. Johansen et al. (2000) presents two particular forms. The first one is the "two-dimension grid" based on the Isin model (Onsager 1944) in which every trader is connected to 4 others traders (Nord, Sud, Est, West) in a uniform way. $K$ captures the tendency toward imitation whereas $\sigma$ captures the idiosyncratic behavior, the ratio $K/\sigma$ measures the tendency of imitation relative to idiosyncratic behavior. As we previously described in 4.3.2.1, $K_c$ is the critical size that make the situation goes to disorder (when $K < K_c$, in this case $\chi$ is finite) toward orders (when $K$ is approaching $K_c$ and therefore in which $\chi$ goes to infinity according to power law):

$$\chi \approx A(K_c - K)^{\gamma} \tag{4.18}$$

Where $A > 0$ is a constant, $\gamma > 0$ is the critical exponent of the susceptibility.

$K(t_c) = K_c$ and prior the time $t_c$, $K_c - K(t) \approx constant \times (t_c - t)$. Therefore, the hazard rate and the susceptibility have the same behavior in the network at the critical time.

$$h(t) \approx B \times (t_c - t)^{-\alpha} \tag{4.19}$$

Where $B > 0$ is a constant, $\alpha \in [0;1]$ to maintain the price not to go to infinity when the time is approaching the critical time $t_c$ (if the bubble has not crashed yet). The hazard rate becomes unbounded near the critical time $t_c$ where $t_c$ is the most probable time for the crash to occur but the crash can happen before the critical time $t_c$. There exists a probability to reach the critical time without having a crash $1 - Q(t_c) > 0$ in order to respect the rational expectation hypothesis (traders cannot anticipate the crash). Putting equation 4.19 in equation of the price dynamic 4.17, we obtain the law of price before the crash:

$$\log[p(t)] \approx \log[p_c] - \frac{\kappa B}{\beta} \times (t_c - t)^{\beta} \qquad (4.20)$$

Where $p_c$ is the price at the critical time $t_c$, $\beta = 1 - \alpha \in [0; 1]$, $\log[p(t)]$ follows a power law with a finite upper bound $\ln[p(c)]$. To compensate the unbounded probability of crash approaching $t_c$, the expected return becomes unbounded.

Because the 2-dimension network is not a representation of the reality of the financial markets, Johansen et al. (2000) suggest another network, the "hierarchical diamond lattice". The financial markets are structured in interaction between different investors connected to each other. These connections are of different sizes and relationships (family, friends, work, professional status based on hierarchical system) and by consequence are differently impacted by their environment.

The principle of the hierarchical diamond lattice is presented in Figure 4.3 - *Hierarchical diamond lattice*:

1. Two traders are linked to each other.

2. The link between the two previous traders is replaced by a diamond of 4 links.

3. Each new links of the previous diamond is replaced by a new diamond.

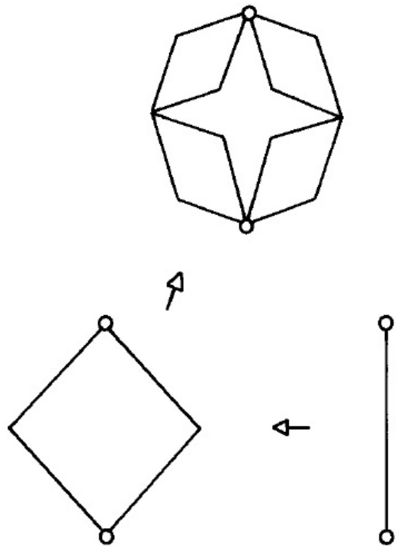

**Figure 4.3 Hierarchical diamond lattice**
This table presents the steps of the hierarchical Diamond Lattice. The figure is the first figure of (Johansen et al., 2000)

After $p$ iterations, we obtain in the network, $\frac{2}{3}(2+4^p)$ traders and $4^p$ links between them. Each trader has a number of relationships comprised between $[2; 2^p]$[10]. In the hierarchical diamond lattice, the properties are the same as in the 2-dimension network: a critical point $K_c$, when $K < K_c$ the susceptibility is finite, when $K$ is approaching $K_c$, the susceptibility goes to infinity. The difference is the fact that the critical exponent could be a complex number. The first order expansion of the general solution is:

$$\chi \approx \mathrm{Re}[A_0(K_c - K)^{-\gamma} + A_1(K_c - K)^{-\gamma+i\omega} + ...] \tag{4.21}$$

$$\chi \approx A_0'(K_c - K)^{\gamma} + A_1'(K_c - K)^{\gamma}\cos[\omega\ln(K_c - K) + \psi] + ... \tag{4.22}$$

Where $Re[.]$ is the real part of a complex number and $A_0'$, $A_1'$, $\omega$ and $\psi$ are reals. This equation shows the "power law" part as well as the "log-periodicity"

[10]The original traders have $2^p$ connections, most traders have 2 connections and the remaining traders have a number of connections between these bounds.

part (the presence of oscillations that explode reaching the critical time). More precisely, $K_c - K$ represents the periodicity and $\frac{\omega}{2\pi}$ the log-frequency. In the hierarchical lattice diamond, the hazard rate is defined as:

$$h(t) \approx B_0(t_c - t)^{-\alpha} + B_1(t_c - t)^{-\alpha} cos[\omega \ln(tc_t) + \psi'] \tag{4.23}$$

Finally, the price dynamic before the critical time $t_c$ and before the crash is:

$$\ln[p(t)] \approx \ln[p_c] - \frac{\kappa}{\beta} B_0(t_c - t)^{\beta} + B_1(t_c - t)^{\beta} cos[\omega \ln(tc_t) + \phi] \tag{4.24}$$

Where $\phi$ is a phase constant. Oscillations only appear before the critical time. At the critical time, the local maxima of this function tends to zero separated by intervals of time in geometric progression (the consecutive time intervals ratio is a constant).

$$\lambda \equiv e^{\frac{2\pi}{\omega}} \tag{4.25}$$

The novelty of this model is to estimate the critical date, $t_c$, on which the crash occurs in addition to detect if a bubble occurs or not. Based on this context, Johansen et al. (2000) model the equation for the evolution of asset prices before a crash with 7 parameters (3 linear: $A$, $B$ and $C$; and 4 non-linear: $\beta$, $\omega$, $\phi$ and $t_c$):

$$y_t = A + B \times (t_c - t)^{\beta} \times [1 + C \times \cos(\omega \times \log(t_c - t) + \phi)] \tag{4.26}$$

where $y_t$ is the log prices, $A > 0$ is the value of $y_t$ if the bubble remains until the critical time $t_c$, $B < 0$ is the decrease in $y_t$ over time before the crash if $C$ is 0, $C$ is the magnitude of fluctuations around exponential growth, $t_c > 0$ is the critical time, $t < t_c$ is any time in the bubble before the critical time $t_c$, $t_c$ is the critical time when the hazard rate becomes large[11], $\beta$ is the exponent of power law growth (power law accelerations of price) and the condition $0 <= \beta < 1$ is due to $\beta = (n-2)/(n-1)$ where $n$ is the number of the nearest neighbors of

[11]According to Sornette et al. (2012) "This critical time $t_c$ of the model is interpreted as the end of the bubble, which is often but not necessarily the time when a crash occurs in the actual system."

each agent in the noise trader network, $\omega$ is the frequency of fluctuations during the bubbles and $0 < \phi < 2\pi$ is the shift/phase parameter.

To fix the problem of local/global minimum, equation 4.26 can be rewritten as:

$$y_t = A + B \times f_t + C \times g_t \tag{4.27}$$

where $y_i$ is the log price,

$$f_t = (t_c - t)^\beta \tag{4.28}$$

$$g_t = (t_c - t)^\beta \cos(\omega \times \log(t_c - t) + \phi)] \tag{4.29}$$

In order to identify a bubble, $\beta$ and $\omega$ have to follow the following constraints obtained empirically, (Brée and Joseph, 2013). Johansen (2003) finds the following thresholds using different markets and time periods.

$$B < 0 \tag{4.30}$$

$$0.33 - 0.18 \leq \beta \leq 0.33 + 0.18 \tag{4.31}$$

$$6.36 - 1.56 \leq \omega \leq 6.36 + 1.56 \tag{4.32}$$

Equation 4.27 allows to estimate an OLS model to obtain A, B and C. However we have to find [$\beta$, $\omega$, $\phi$ and $t_c$] in the first instance.

#### 4.3.2.2 Fitting LPPL model and implementation

In order to implement the LPPL model, first, we follow the work of Filimonov and Sornette (2013) that modify the model in order to obtain three non-linear parameters instead of four. The variable $C$ is decomposed into two variables ($C_1$ and $C_2$) containing the phase $\phi$ in order to obtain three non-linear parameters ($\beta$, $\omega$ and $t_c$) and four non-linear parameters ($A$, $B$, $C_1$ and $C_2$).

We define:

$$X = (t_c - t) \tag{4.33}$$

$$C_1 = C \times \cos\phi \tag{4.34}$$

$$C_2 = C \times \sin\phi \tag{4.35}$$

And finally, we obtain this equation:

$$y_t = A + B \times X^\beta + C_1 \times X^\beta \cos(\omega \times \log(X)) + C_2 \times X^\beta \sin(\omega \times \log(X)) \quad (4.36)$$

Thus, there are three non-linear parameters instead of four. Filimonov and Sornette (2013) modify the aforementioned conditions (see section 4.3.2.1) called the "stylized features of LPPL" (Lin et al., 2009) :

$$B < 0 \quad (4.37)$$

$$0.1 \leq \beta \leq 0.9 \quad (4.38)$$

$$6 \leq \omega \leq 13 \quad (4.39)$$

$$C_1^2 + C_2^2 < 1 \quad (4.40)$$

The conditions on parameter $B$ and $\beta$ allow to respect the "faster-than-exponential" growing of the prices. The parameter $\omega$ is within a range [6;13] so that it is not too fast (otherwise, they would correspond to the random part of the data), or too slow (otherwise, they would contribute to the trend) (Lin et al., 2009). Finally the condition on parameters $C_1$ and $C_2$ guarantees that the hazard rate remains positive (MacDonnell, 2014),(Brée and Joseph, 2013).

We implement the LPPL model using Evolution Algorithm in R[12] using the function CMA_ES (Covariance Matrix Adaptation Evolution Strategy)[13]. CMA_ES is a Evolutionary algorithm based on a stochastic search method. The Evolutionary algorithm runs on a continuous search space compared to the Genetic Algorithm that operates on trees. The former algorithm is used for non-linear non-convex with unconstrained or bounded constraint optimization problems. The efficiency of the CMA_ES algorithm has been tested and validated by various studies (Hansen and Kern, 2004), (Hansen, 2011), (Hansen, 2016), (Hansen, 2017).

[12] Based on the code on https://github.com/gchevalley/LPPL/blob/master/data/DJA.csv

[13] https://cran.r-project.org/web/packages/cmaes/cmaes.pdf

### 4.3.3 Data

For both methodologies, we apply the analysis for four cryptocurrencies: Bitcoin, Ether, Ripple and Litecoin. More precisely, we extract their daily closing prices in USD from the Coindesk[14] and the Coinmarketcap[15] websites, which are financial databases of cryptocurrencies, frequently used in the literature. For detection of multiple bubbles, the sample period studied starts on the August 8$^{th}$, 2013 for Bitcoin and Ripple, on the April 28$^{th}$, 2013 for Litecoin and since the August 8$^{th}$, 2015 for Ether until July 2$^{nd}$, 2019, Figure 4.2.

In the second step, we focus our analysis on the main boom in the cryptocurrency prices at the end of 2017. The supposed phase of a growing bubble reached its peak on December 18$^{th}$, 2017 for Bitcoin ($19,395.83) and for Litecoin ($358,34), on January 7$^{th}$, 2018 for Ripple ($3.38) and on January 14$^{th}$, 2018 for Ether ($1,397.27), Table 4.1 - *The actual peaks of the main boom in the cryptocurrency market*.

**Table 4.1 The actual peaks of the main boom in the cryptocurrency market**

This table presents the main peaks of the main boom in the cryptocurrency market ranking by date. The main peak for Bitcoin is the December 18, 2017 for a price of $19,395 dollars.

| Cryptocurrency | Peak | Price | source |
|---|---|---|---|
| Bitcoin | 18-12-2017 | 19,395.83 | Coindesk |
| Litecoin | 18-12-2017 | 358.34 | Coinmarketcap |
| Ripple | 07-01-2018 | 3.38 | Coinmarketcap |
| Ether | 14-01-2018 | 1,397.27 | Coindesk |

The size of the window as well as the choice of the starting and ending date is a sensitive task in the LPPL model implementation. Brée and Joseph (2013) suggest that the starting day is the “day on which the index reaches its lowest value” and more precisely “the lowest value prior to the change in trend”, (Johansen and Sornette, 2001).

Based on the literature and graphical analysis, we consider different starting and ending dates, Table 4.2 - *The windows samples for the LPPL model* and we

[14] https://www.coindesk.com/
[15] https://coinmarketcap.com/

**Table 4.2 The windows samples for the LPPL model**

This Table shows the different windows applied in the expanding and shrinking windows process for Bitcoin, Ether, Ripple and Litecoin to analyze their main boom through the LPPL model.

| | Starting date | Ending date |
|---|---|---|
| | **Bitcoin's window** | |
| Window 1 | 01/10/2017 | 17/12/2017 |
| Window 2 | 01/01/2017 | 18/12/2017 |
| Window 3 | 01/04/2017 | 19/12/2017 |
| Window 4 | 01/01/2017 | 30/11/2017 |
| Window 5 | 01/01/2017 | 09/12/2017 |
| | **Ether's window** | |
| Window 1 | 01/11/2017 | 13/01/2018 |
| Window 2 | 01/05/2017 | 13/01/2018 |
| Window 3 | 01/05/2017 | 06/01/2018 |
| Window 4 | 01/11/2017 | 06/01/2018 |
| | **Litecoin's window** | |
| Window 1 | 01/10/2017 | 17/12/2017 |
| Window 2 | 05/11/2017 | 17/12/2017 |
| | **Ripple's window** | |
| Window 1 | 01/11/2017 | 06/01/2018 |
| Window 2 | 07/12/2017 | 06/01/2018 |

apply two different rolling window procedures. The first one is the expanding window which allows the ending date to be flexible and the second one is the shrinking window process, for which the starting date varies (Jiang et al., 2010).

## 4.4 Results

### 4.4.1 Univariate results

Table 4.3 - *Descriptive statistics* presents the descriptive statistics for Bitcoin, Ether, Ripple and Litecoin. Panel A presents the statistics for the respective sample period of the four cryptocurrencies expressed in USD prices. Ripple and especially Ether are analyzed on a smaller period of time because they were created after Bitcoin and Litecoin. Panel B (panel C) shows the same statistics in prices (returns) for the same period of time between August 8$^{th}$, 2015 and

July 2nd, 2019. Bitcoin has the highest mean, standard deviation, sum, min and max visible on Figure 4.2 and confirmed in the literature (Cagli, 2019), whereas in term of returns, the mean is almost the same. Ether displays the highest daily return (0.33 %) - standard deviation (7.45%).

Cryptocurrency prices exhibit a positive skewness and a positive kurtosis (Ripple has the highest one) in prices, whereas in returns, the skewness of Bitcoin and Ether is mildly negative and positive for Litecoin and Ripple. The kurtosis is largely high especially for Ether and Ripple. These results are similar to those obtained in the literature (Fry, 2018), (Geuder et al., 2018). The kurtosis is lower with a longer period of time.

**Table 4.3 Descriptive statistics**

This table presents the descriptive statistics of the prices of cryptocurrency for their respective period of time (panel A). for the same period of time August 08.2015 until July 2. 2019 (panel B) and for their returns (panel C).

| **cryptocurrency** | **N** | **Mean** | **SD** | **Sum** | **Min** | **Max** | **Skewness** | **Kurtosis** |
|---|---|---|---|---|---|---|---|---|
| *Panel A* | | | | | | | | |
| Bitcoin | 2258 | 2,581.76 | 3,466.14 | 5,829,618.00 | 68.43 | 19497.40 | 1.74 | 2.86 |
| Ether | 1,427 | 206.48 | 257.77 | 294,644.60 | 0.43 | 1396.42 | 1.67 | 2.74 |
| Litecoin | 2,258 | 0.18 | 53.63 | 77,858.49 | 0.00 | 3.38 | 2.44 | 6.75 |
| Ripple | 2,160 | 0.18 | 0.33 | 392.77 | 0.00 | 3.38 | 3.86 | 23.07 |
| *Panel B* | | | | | | | | |
| Bitcoin | 1,425 | 3,864.30 | 3,802.19 | 5,506,561.12 | 210.50 | 19497.40 | 1.14 | 1.07 |
| Ether | 1,425 | 206.55 | 257.88 | 294,338.74 | 0.43 | 358.34 | 1.67 | 2.74 |
| Litecoin | 1,425 | 50.52 | 61.81 | 71,988.26 | 2.63 | 1396.42 | 1.79 | 3.45 |
| Ripple | 1,425 | 0.27 | 0.38 | 384.50 | 0.00 | 3.38 | 3.25 | 16.78 |
| *Panel C* | | | | | | | | |
| Bitcoin | 1,425 | 0.003 | 0.04 | 3.65 | -0.21 | 0.23 | -0.21 | 4.76 |
| Ether | 1,425 | 0.003 | 0.07 | 4.66 | -1.30 | 0.41 | -3.40 | 67.86 |
| Litecoin | 1,425 | 0.002 | 0.06 | 3.34 | -0.40 | 0.51 | 1.23 | 11.80 |
| Ripple | 1,425 | 0.003 | 0.07 | 3.89 | -0.62 | 1.03 | 3.04 | 41.02 |

The correlation between cryptocurrency returns are all positive and significant at 1% level, as shown by panel A (Pearson) and panel B (Spearman) in Table 4.4 - *Correlation matrices*. These results are similar to those obtained in the existing literature Huynh (2019).

**Table 4.4 Correlation matrices**

This table presents the Pearson (Panel A) and the Spearman (Panel B) coefficient between Bitcoin, Ether, Litecoin and Ripple returns over the period of time August 08, 2015 through July 03, 2019. If the p-value is higher than 5 per cent, then the null hypothesis of no-correlation (rho = 0) is accepted. ***, ** and * indicate that the coefficient is significant at 1%, 5% and 10% level, resp.

| | **Bitcoin** | **Ether** | **Litecoin** | **Ripple** |
|---|---|---|---|---|
| *Panel A: Pearson* | | | | |
| **Bitcoin** | **1** | **0,4*** ** | **0,62*** ** | **0,33*** ** |
| | | <.0001 | <.0001 | <.0001 |
| **Ether** | | **1** | **0,39*** ** | **0,25*** ** |
| | | | <.0001 | <.0001 |
| **Litecoin** | | | **1** | **0,38*** ** |
| | | | | <.0001 |
| **Ripple** | | | | **1** |
| *Panel B: Spearman* | | | | |
| **Bitcoin** | **1** | **0,43*** ** | **0,67*** ** | **0,44*** ** |
| | | 0 | 0 | 0 |
| **Ether** | | **1** | **0,47*** ** | **0,44*** ** |
| | | | 0 | 0 |
| **Litecoin** | | | **1** | **0,51*** ** |
| | | | | 0 |
| **Ripple** | | | | **1** |

Figures 4.4 - *Cryptocurrency returns - Histogram* and 4.5 - *Cryptocurrency returns - QQplot* present the empirical distribution of the returns of the four cryptocurrencies. Normality tests such as Shapiro-Wilk, Kolmogorov Smirnov, Cramer Von Mises and Anderson Darling, presented in Table 4.5 - *Cryptocurrency returns normality tests*, reject the null hypothesis of a normal distribution.

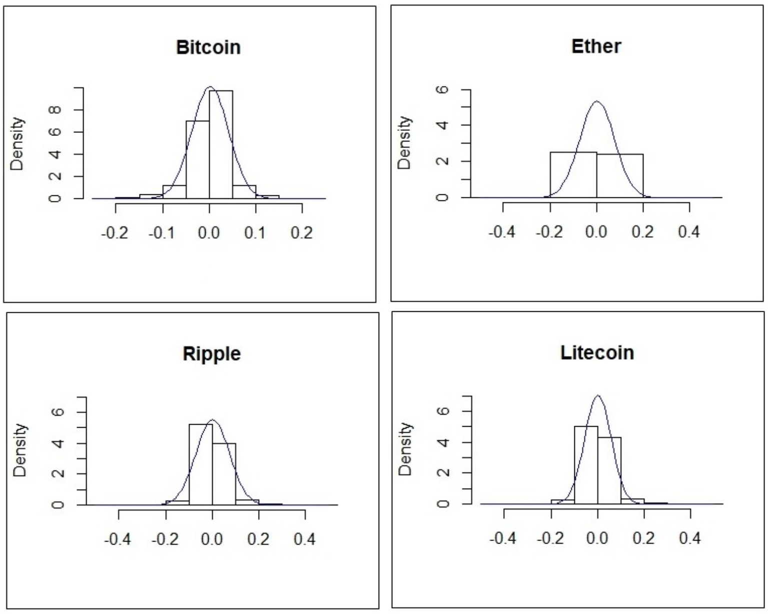


**Figure 4.4 Cryptocurrency returns - Histogram**
This figure shows the histogram of Bitcoin, Ether, Litecoin and Ripple daily returns related to the normal distribution. Data come from the Coindesk website over the period August 8th, 2015 to July 2nd, 2019.

**Table 4.5 Cryptocurrency returns normality tests**

This table presents the normality test for Bitcoin, Ether, Ripple and Litecoin daily returns. The sample is drawn from the coinmarketcap website over the period 2015–2019.

| | **Shapiro** | **Kolmogorov** | **Cramer** | **Anderson** |
|---|---|---|---|---|
| **Bitcoin** | **0.91*** ** | **0.13*** ** | **7.74*** ** | **39.76*** ** |
| p-value | <0.0001 | <0.0100 | <0.0050 | <0.0050 |
| **Ether** | **0.79*** ** | **0.12*** ** | **8.63*** ** | **45.91*** ** |
| p-value | <0.0001 | <0.0100 | <0.0050 | <0.0050 |
| **Litecoin** | **0.86*** ** | **0.13*** ** | **9.59*** ** | **49.41*** ** |
| p-value | <0.0001 | <0.0100 | <0.0050 | <0.0050 |
| **Ripple** | **0.72*** ** | **0.17*** ** | **16.92*** ** | **88.95*** ** |
| p-value | <0.0001 | <0.0100 | <0.0050 | <0.0050 |

### 4.4.2 Multiple bubble detection - PSY results

Table 4.6 - *Multiple bubbles - Occurrence* presents the numbers of bubbles detected by the PSY model for all considered cryptocurrencies based on their entire period of time, on the same period of time (2015–2019) and by year. We notice that Litecoin records the highest numbers of bubbles (22) since 2013

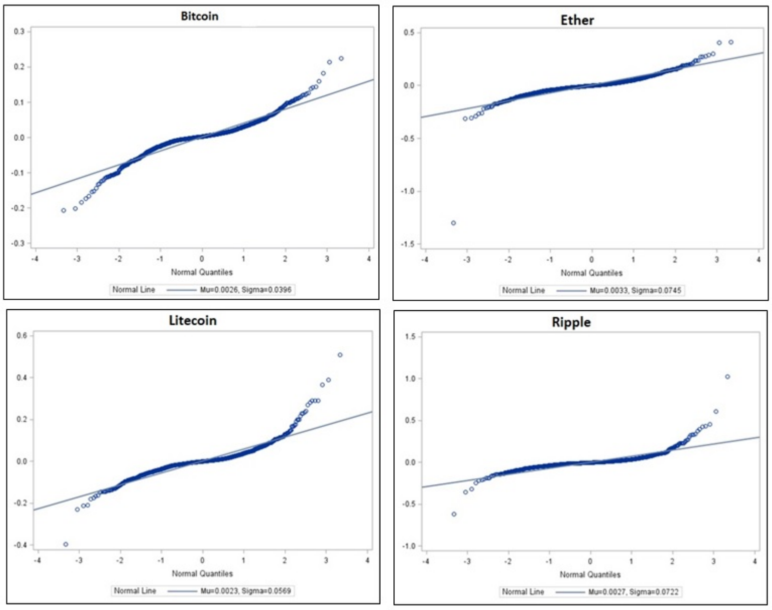


**Figure 4.5 Cryptocurrency returns - QQplot**
This figure shows QQ plot curves for Bitcoin, Ether, Litecoin and Ripple daily returns. Data come from the Coindesk website over the period August $8^{th}$, 2015 to July $2^{nd}$, 2019.

compared to 16 for Bitcoin since 2013 as well. However, on the smallest period (August 2015–July 2019), Bitcoin records the highest number of bubbles (17). Ripple is the cryptocurrency with the smallest number of bubbles detected. If we consider the occurrence by year, the highest bubble years are 2013 and 2017[16]. The year of 2013 and 2017 appear graphically as a potential bubble in the graph 4.2. These two years are tested in the literature (on the part 4.2.3) to be a bubble. The boom of the end of 2013 represents the first boom in the cryptocurrency market where Bitcoin reaches for the first time the threshold of $ 1,000. The year of 2017 is the year where the cryptocurrency market reaches its highest boom, Table 4.1.

[16]N.B: For year X (e.g., 2017), if a bubble window detected spreads until X+1 (e.g. December 2017 until January 2018), we count this bubble for year X (e.g, 2017).

**Table 4.6 Multiple bubbles - Occurrence**

This table presents the number of detected bubbles through the PSY model for Bitcoin, Ether, Ripple and Litecoin according to their entire period, the same period of time (August 2015-July 2019) and by year.

| | **Entire Period** | **2015-2019** | **2013** | **2014** | **2015** | **2016** | **2017** | **2018** | **2019** |
|---|---|---|---|---|---|---|---|---|---|
| **Bitcoin** | 16 | 17 | 3 | 1 | 1 | 3 | 5 | 0 | 3 |
| **Ether** | 12 | 12 | 0 | 0 | 0 | 3 | 7 | 1 | 1 |
| **Litecoin** | 22 | 13 | 3 | 1 | 2 | 2 | 8 | 0 | 6 |
| **Ripple** | 10 | 6 | 1 | 2 | 0 | 0 | 7 | 0 | 0 |

Tables 4.7 - *Multiple bubbles - Bitcoin and Ether* and table 4.8 - *Multiple bubbles - Litecoin and Ripple* present the dates and the length of the detected bubbles by cryptocurrency. We notice that the period of time of the end of 2017 is present. Regarding the boom of the end of September 2017, knowing the actual date of boom for Bitcoin and Litecoin is December 18$^{th}$, 2017, the bubbles detected are from September 18$^{th}$, 2017 to January 16$^{th}$, 2018 (Bitcoin) and from November 24$^{th}$, 2017 to December 21$^{st}$, 2017 (Litecoin). While, the PSY model detects for Ripple the window of December 13$^{th}$, 2017 until January 13$^{th}$, 2018 (and its actual date is January 7$^{th}$, 2018) and two consecutive windows for Ether, December 11$^{th}$, 2017 - December 21$^{st}$, 2017 and December 23$^{rd}$, 2017 until January 15$^{th}$, 2018 (actual crash: January 18$^{th}$, 2018).

It seems that the least precise bubble is the bubble of Bitcoin which is the dominant cryptocurrency of the market. When Bitcoin crashes, this information seems to be contagious to the other cryptocurrencies with long time impact (the time between the first crash and the last one is almost 1 month) thus providing more precise bubble detection.

The results are consistent with the existing literature (Geuder et al., 2018), (Bouri et al., 2016).

**Table 4.7 Multiple bubbles - Bitcoin and Ether**

This table presents the bubbles windows and their length found using the PSY model for Bitcoin and Ether.

| Starting Date | Ending Date | Length |
|---|---|---|
| | *Bitcoin* | |
| 22/10/2013 | 24/10/2013 | 3 |
| 29/10/2013 | 30/10/2013 | 2 |
| 03/11/2013 | 04/12/2013 | 32 |
| 03/10/2014 | 07/10/2014 | 5 |
| 03/11/2015 | 04/11/2015 | 2 |
| 03/06/2016 | 08/06/2016 | 6 |
| 11/06/2016 | 20/06/2016 | 10 |
| 21/12/2016 | 07/01/2017 | 18 |
| 21/02/2017 | 07/03/2017 | 15 |
| 12/03/2017 | 16/03/2017 | 5 |
| 27/04/2017 | 14/07/2017 | 79 |
| 18/07/2017 | 13/09/2017 | 58 |
| 18/09/2017 | 16/01/2018 | 121 |
| 07/04/2019 | 08/04/2019 | 2 |
| 09/05/2019 | 02/06/2019 | 25 |
| 20/06/2019 | 30/06/2019 | 11 |
| | *Ether* | |
| 23/01/2016 | 30/01/2016 | 8 |
| 02/02/2016 | 15/02/2016 | 14 |
| 22/02/2016 | 17/03/2016 | 25 |
| 01/03/2017 | 07/03/2017 | 7 |
| 10/03/2017 | 02/04/2017 | 24 |
| 13/04/2017 | 16/04/2017 | 4 |
| 18/04/2017 | 20/04/2017 | 3 |
| 24/04/2017 | 24/06/2017 | 62 |
| 11/12/2017 | 21/12/2017 | 11 |
| 23/12/2017 | 15/01/2018 | 24 |
| 27/01/2018 | 31/01/2018 | 5 |
| 15/05/2019 | 16/05/2019 | 2 |

**Table 4.8 Multiple bubbles - Litecoin and Ripple**

This table presents the bubbles windows and their length found using the PSY model for Litecoin and Ripple.

| Starting Date | Ending Date | Length |
|---|---|---|
| | *Litecoin* | |
| 07/11/2013 | 08/11/2013 | 2 |
| 18/11/2013 | 19/11/2013 | 2 |
| 21/11/2013 | 04/12/2013 | 14 |
| 13/08/2014 | 18/08/2014 | 6 |
| 13/01/2015 | 22/01/2015 | 10 |
| 28/06/2015 | 09/07/2015 | 12 |
| 28/05/2016 | 06/06/2016 | 10 |
| 11/06/2016 | 19/06/2016 | 9 |
| 02/04/2017 | 08/04/2017 | 7 |
| 12/04/2017 | 18/04/2017 | 7 |
| 20/04/2017 | 26/05/2017 | 37 |
| 31/05/2017 | 14/07/2017 | 45 |
| 16/07/2017 | 27/07/2017 | 12 |
| 31/07/2017 | 14/08/2017 | 15 |
| 16/08/2017 | 12/09/2017 | 28 |
| 24/11/2017 | 21/12/2017 | 28 |
| 16/03/2019 | 17/03/2019 | 2 |
| 02/04/2019 | 11/04/2019 | 10 |
| 26/05/2019 | 29/05/2019 | 4 |
| 31/05/2019 | 02/06/2019 | 3 |
| 07/06/2019 | 08/06/2019 | 2 |
| 10/06/2019 | 25/06/2019 | 16 |
| | *Ripple* | |
| 29/11/2013 | 05/12/2013 | 7 |
| 22/11/2014 | 29/11/2014 | 8 |
| 01/12/2014 | 02/01/2015 | 33 |
| 30/03/2017 | 02/04/2017 | 4 |
| 04/05/2017 | 26/05/2017 | 23 |
| 28/05/2017 | 29/05/2017 | 2 |
| 31/05/2017 | 09/06/2017 | 10 |
| 13/06/2017 | 14/06/2017 | 2 |
| 17/06/2017 | 25/06/2017 | 9 |
| 13/12/2017 | 13/01/2018 | 32 |

### 4.4.3 The 2017 boom - LPPL results

Tables 4.9 - *LPPL fitting model for Bitcoin prices*, 4.10 - *LPPL fitting model for Ether prices*, 4.11 - *LPPL fitting model for Litecoin prices* and 4.12 - *LPPL fitting model for Ripple prices* report the main relevant results for all cryptocurrencies regarding the expanding windows when the iteration is 600. We also performed the analysis for the shrinking windows and by increasing the number of iterations (1,000, 10,000, 100,000) but for a space convenience, we do not present these results. The detection of bubble is linked to the constraints applied to the parameters (see sections 4.3.2.1 and 4.3.2.2). If the above conditions on the parameters, $\beta$ and $\omega$, are met, then the detection of a bubble is positive, and we obtain a significant estimated critical time, $t_c$. Table 4.9, 4.10, 4.11, 4.12 display the main significant results when the above conditions are met and when the critical date is estimated close to the actual date (e.g, see table 4.1) using the expanding window process.

Based on the significant results, Table 4.9 displays the estimated critical time, $t_c$, close to the reality, for Bitcoin. The best window is from October 1st, 2017 to November 11th, 2017 which estimates the crash date on December 19th, 2017 (one day after the effective crash). The second window that starts in January 2017 provides only results that respect constraints presented in the section 4.3.2.1 (83 results) and exhibit an estimated $t_c$ around December 17th, 2017 (one day before the effective crash). The third window does not give us any acceptable results to analyze with respect to the constraints from sections 4.3.2.1 and 4.3.2.2. More precisely, for Bitcoin, we observe that the more $t_2$ (the ending date of the window) is close to the effective crash date, the more the LPPL model fits a $t_c$ close to the effective date. We can notice, as well, that the identification of a bubble depends on the respect of the criteria (4.3.2.2 and 4.3.2.1): most of the estimated results that indicate a bubble are the ones which follow the constraints of the section 4.3.2.1.

**Table 4.9 LPPL fitting model for Bitcoin prices**

This Table presents the main results of the LPPL analysis using expanding windows. This method consists to make the ending date flexible whereas the starting date fix (October 1, 2017 for "Window 1" and January 1, 2018 for "Window 2"). This table displays only the windows results that respect the criteria from the section 4.3.2.1 and 4.3.2.2 and provides an expected date in December. $t_1$ is the starting date of the window, $t_2$ is the ending date of the window, $t_c$ is the critical time and *Excepted date* is its corresponding date. $\beta$, $\omega$, $t_c$, $A$, $B$, $C_1$ and $C_2$ are presented in the Equation 4.36.

| $t_1$ | $t_2$ | $t_c$ | **Expected date** | $\beta$ | $\omega$ | $A$ | $B$ | $C_1$ | $C_2$ |
|---|---|---|---|---|---|---|---|---|---|
| **Window 1 - criteria from section 4.3.2.2** | | | | | | | | | |
| 2017-10-01 | 2017-11-24 | 2017.976 | 2017-12-23 | 0.58 | 6.86 | 9.82 | -3.34 | 0.17 | -0.01 |
| 2017-10-01 | 2017-12-03 | 2017.988 | 2017-12-27 | 0.44 | 6.14 | 10.44 | -3.88 | -0.05 | 0.16 |
| **Window 1 - criteria from section 4.3.2.1** | | | | | | | | | |
| 2017-10-01 | 2017-11-20 | 2017.930 | 2017-12-07 | 0.24 | 5.01 | 10.47 | -3.06 | 0.03 | 0.13 |
| 2017-10-01 | 2017-12-08 | 2017.937 | 2017-12-09 | 0.15 | 5.52 | 11.05 | -3.31 | 0.09 | 0.01 |
| 2017-10-01 | 2017-11-30 | 2017.965 | 2017-12-19 | 0.50 | 5.08 | 10.00 | -3.52 | -0.21 | 0.03 |
| 2017-10-01 | 2017-11-22 | 2017.950 | 2017-12-14 | 0.32 | 5.82 | 10.32 | -3.20 | 0.11 | 0.09 |
| 2017-10-01 | 2017-12-03 | 2017.988 | 2017-12-27 | 0.44 | 6.14 | 10.44 | -3.88 | -0.05 | 0.16 |
| 2017-10-01 | 2017-11-29 | 2017.989 | 2017-12-28 | 0.24 | 5.06 | 12.29 | -5.64 | -0.11 | -0.14 |
| **Window 2 - criteria from section 4.3.2.1** | | | | | | | | | |
| 2017-01-01 | 2017-12-10 | 2017.944 | 2017-12-12 | 0.49 | 5.00 | 9.80 | -3.00 | 0.01 | 0.21 |
| 2017-01-01 | 2017-12-11 | 2017.947 | 2017-12-13 | 0.47 | 5.06 | 9.89 | -3.08 | 0.01 | 0.20 |
| 2017-01-01 | 2017-12-13 | 2017.950 | 2017-12-14 | 0.46 | 5.57 | 9.97 | -3.18 | 0.04 | 0.18 |
| 2017-01-01 | 2017-12-14 | 2017.953 | 2017-12-15 | 0.46 | 5.45 | 10.01 | -3.21 | 0.03 | 0.18 |
| 2017-01-01 | 2017-12-16 | 2017.958 | 2017-12-17 | 0.44 | 5.02 | 10.08 | -3.25 | -0.02 | 0.20 |
| 2017-01-01 | 2017-12-15 | 2017.996 | 2017-12-30 | 0.26 | 5.98 | 11.94 | -5.04 | -0.02 | 0.16 |

**Table 4.10 LPPL fitting model for Ether prices**

This Table presents the main results of the LPPL analysis using expanding windows. This method consists to make the ending date flexible whereas the starting date fix (November 1, 2017 for "Window 1" and May 1, 2018 for "Window 2"). This table displays only the windows results that respect the criteria from the sections 4.3.2.1 and 4.3.2.2 and provides an expected date in January. $t_1$ is the starting date of the window, $t_2$ is the ending date of the window, $t_c$ is the critical time and *Excepted date* is its corresponding date. $\beta$, $\omega$, $t_c$, $A$, $B$, $C_1$ and $C_2$ are presented in the Equation 4.36.

| $t_1$ | $t_2$ | $t_c$ | **Expected date** | $\beta$ | $\omega$ | $A$ | $B$ | $C_1$ | $C_2$ |
|---|---|---|---|---|---|---|---|---|---|
| **Window 1- Criteria from section 4.3.2.2** | | | | | | | | | |
| 2017-11-01 | 2017-12-22 | 2018.013 | 2018-01-05 | 0.33 | 6.03 | 8.72 | -5.78 | 0.05 | 0.07 |
| 2017-11-01 | 2017-12-23 | 2018.036 | 2018-01-13 | 0.63 | 6.99 | 7.81 | -6.58 | 0.17 | 0.14 |
| 2017-11-01 | 2018-01-05 | 2018.073 | 2018-01-25 | 0.29 | 6.04 | 9.46 | -5.72 | 0.18 | -0.14 |
| **Window 1 - Criteria from section 4.3.2.1** | | | | | | | | | |
| 2017-11-01 | 2017-12-22 | 2018.013 | 2018-01-05 | 0.33 | 6.03 | 8.72 | -5.78 | 0.05 | 0.07 |
| 2017-11-01 | 2017-11-26 | 2018.040 | 2018-01-14 | 0.19 | 5.04 | 22.49 | -23.42 | 0.48 | -0.66 |
| 2017-11-01 | 2018-01-02 | 2018.053 | 2018-01-18 | 0.19 | 5.09 | 10.02 | -5.73 | 0.23 | 0.08 |
| 2017-11-01 | 2017-12-31 | 2018.063 | 2018-01-22 | 0.30 | 5.07 | 8.62 | -4.47 | 0.24 | 0.22 |
| 2017-11-01 | 2018-01-05 | 2018.073 | 2018-01-25 | 0.29 | 6.04 | 9.46 | -5.72 | 0.18 | -0.14 |

**Table 4.11 LPPL fitting model for Litecoin prices**

This Table presents the main results of the LPPL analysis using expanding windows. This method consists to make the ending date flexible whereas the starting date fix (October 1, 2017 for "Window 1" and November 5, 2017 for "Window 2"). This table displays only the windows results that respect the criteria from the sections 4.3.2.1 and 4.3.2.2 and provides an expected date in December. $t_1$ is the starting date of the window, $t_2$ is the ending date of the window, $t_c$ is the critical time and *Excepted date* is its corresponding date. $\beta$, $\omega$, $t_c$, $A$, $B$, $C_1$ and $C_2$ are presented in the Equation 4.36.

| $t_1$ | $t_2$ | $t_c$ | **Expected date** | $\beta$ | $\omega$ | $A$ | $B$ | $C_1$ | $C_2$ |
|---|---|---|---|---|---|---|---|---|---|
| **Window 1- Criteria from section 4.3.2.2** | | | | | | | | | |
| 2017-10-01 | 2017-11-11 | 2017.9379 | 2017-12-10 | 0.73 | 10.52 | 4.14 | -0.45 | -0.01 | -0.28 |
| **Window 1- Criteria from section 4.3.2.1** | | | | | | | | | |
| 2017-10-01 | 2017-12-07 | 2017.986 | 2017-12-27 | 0.48 | 5.45 | 5.36 | -3.13 | -0.13 | -0.29 |
| **Window 2- Criteria from section 4.3.2.2** | | | | | | | | | |
| 2017-11-05 | 2017-12-09 | 2017.939 | 2017-12-10 | 0.29 | 6.05 | 5.41 | -2.66 | 0.05 | -0.03 |
| 2017-11-05 | 2017-11-29 | 2017.941 | 2017-12-11 | 0.46 | 7.63 | 5.30 | -3.75 | 0.12 | 0.02 |
| **Window 2- Criteria from section 4.3.2.1** | | | | | | | | | |
| 2017-11-05 | 2017-12-09 | 2017.939 | 2017-12-10 | 0.29 | 6.05 | 5.41 | -2.66 | 0.05 | -0.03 |
| 2017-11-05 | 2017-11-29 | 2017.941 | 2017-12-11 | 0.46 | 7.63 | 5.30 | -3.75 | 0.12 | 0.02 |
| 2017-11-05 | 2017-12-10 | 2017.951 | 2017-12-14 | 0.26 | 5.65 | 6.06 | -3.62 | 0.06 | 0.07 |
| 2017-11-05 | 2017-12-08 | 2017.961 | 2017-12-18 | 0.27 | 5.65 | 6.21 | -3.79 | -0.04 | 0.07 |

**Table 4.12 LPPL fitting model for Ripple prices**

This Table presents the main results of the LPPL analysis using expanding windows. This method consists to make the ending date flexible whereas the starting date is fixed (November 1, 2017 for "Window 1" and December 7, 2017 for "Window 2"). This table displays only the windows results that respect the criteria from the sections 4.3.2.1 and 4.3.2.2 and provides an expected date in January $t_1$ is the starting date of the window, $t_2$ is the ending date of the window, $t_c$ is the critical time and *Excepted date* is its corresponding date. $\beta$, $\omega$, $t_c$, $A$, $B$, $C_1$ and $C_2$ are presented in the Equation 4.36.

| $t_1$ | $t_2$ | $t_c$ | **Expected date** | $\beta$ | $\omega$ | $A$ | $B$ | $C_1$ | $C_2$ |
|---|---|---|---|---|---|---|---|---|---|
| **Window 1- Criteria from section 4.3.2.2** | | | | | | | | | |
| 2017-11-01 | 2017-12-08 | 2017.981 | 2017-12-25 | 0.33 | 6.03 | -1.05 | -0.89 | -0.17 | -0.02 |
| **Window 1- Criteria from section 4.3.2.1** | | | | | | | | | |
| 2017-11-01 | 2017-12-04 | 2017.972 | 2017-12-22 | 0.30 | 6.29 | -0.75 | -1.46 | -0.04 | 0.09 |
| 2017-11-01 | 2017-12-09 | 2017.979 | 2017-12-24 | 0.33 | 5.74 | -1.06 | -0.86 | -0.13 | -0.10 |
| 2017-11-01 | 2017-12-08 | 2017.981 | 2017-12-25 | 0.33 | 6.03 | -1.05 | -0.89 | -0.17 | -0.02 |
| 2017-11-01 | 2017-12-26 | 2018.029 | 2018-01-11 | 0.19 | 5.82 | 6.85 | -12.17 | -0.38 | 0.36 |
| **Window 2- Criteria from section 4.3.2.1** | | | | | | | | | |
| 2017-12-07 | 2017-12-26 | 2018.046 | 2018-01-18 | 0.21 | 5.35 | 14.65 | -25.52 | 0.76 | -0.46 |

The Ether "bubble" ends a few days after the Bitcoin's one (January 14th, 2018). In the same vein, we fit the LPPL model according to different windows, the first window is the 60-days one starting on mid-November 2017 which corresponds to the first strong increase in the Ether price (see Figure 4.2). Then the price slightly decreased before it grew up again in May. This is why the second window starts in May 2017. Table 4.10 presents the main results regarding Ether for both windows and according to the different constraints discussed in sections 4.3.2.1 and 4.3.2.2. In the same sense, only the window which starts in November 2017 ("window 1") provides significant results (13 for constraint from the section 4.3.2.2 and 24 for constraint from the section 4.3.2.1). The best result is given by the window of November 1st, 2017 to November 26th, 2017 with a critical time of January 14th, 2018 (the actual date). Similarly, the starting and ending dates of the windows play a significant role in fitting the critical time (the nearest $t_1$ and $t_2$ provide a closer $t_c$ related to the reality).

The Litecoin's burst occurs the same date as the Bitcoin's one, on December 18th, 2017, however we find significant estimated critical date, $t_c$, far away from the actual date and the results are less stable than for Bitcoin. We find similar results for Ripple: a significant estimated critical date not close to the actual one with results that converge less or do not respect the criteria of sections 4.3.2.1 and 4.3.2.2. One potential explanation is that Ripple and Litecoin bursts were not a bubble as suggested by (Fry, 2018).

Table 4.13 - *The bests fitting LPPL windows* and Figures 4.6 - *LPPL fitting Bitcoin market prices*, 4.7 - *LPPL fitting Ether market prices*, 4.8 - *LPPL fitting Litecoin market prices* and 4.9 - *LPPL fitting Ripple market prices* that show the most robust window we obtain confirm our explanation.

**Table 4.13 The bests fitting LPPL windows**

This Table presents the bests fitting LPPL model for Bitcoin, Ether, Litecoin, Ripple respecting the criteria 4.3.2.1 and 4.3.2.2 and appearing when the number of iteration increases.

| $t_1$ | $t_2$ | $t_c$ | **Expected date** | $\beta$ | $\omega$ | $A$ | $B$ | $C_1$ | $C_2$ |
|---|---|---|---|---|---|---|---|---|---|
| | | | **Bitcoin** | | | | | | |
| 2017-10-01 | 2017-11-30 | 2017.963 | 2017-12-19 | 0.51 | 5.00 | 9.96 | -3.51 | -0.22 | 0.01 |
| | | | **Ether** | | | | | | |
| 2017-11-01 | 2018-01-06 | 2018.051 | 2018-01-17 | 0.29 | 5.10 | 8.83 | -4.79 | 0.27 | 0.05 |
| | | | **Litecoin** | | | | | | |
| 2017-11-05 | 2017-12-08 | 2017.967 | 2017-12-19 | 0.11 | 7.11 | 9.61 | -6.94 | 0.02 | -0.05 |
| | | | **Ripple** | | | | | | |
| 2017-11-01 | 2017-12-26 | 2018.022 | 2018-01-09 | 0.51 | 5.19 | 1.92 | -9.73 | -1.18 | -0.28 |

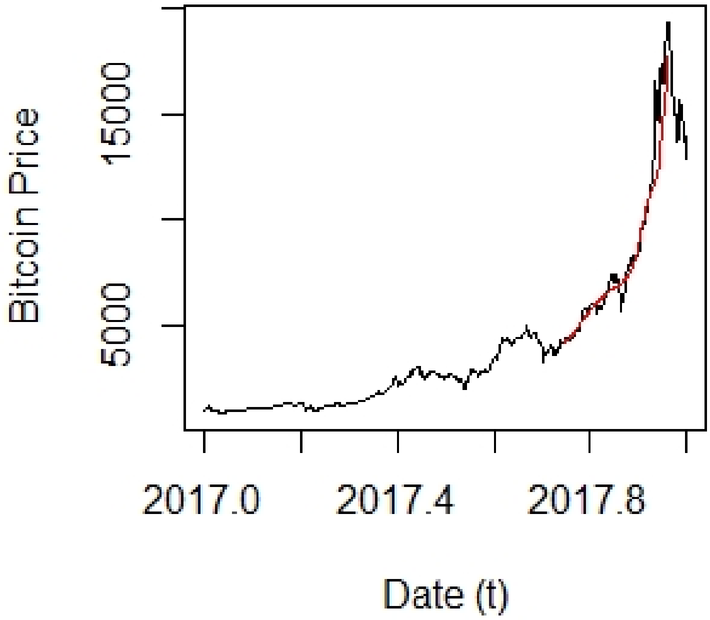


**Figure 4.6 LPPL fitting Bitcoin market prices**
This figure shows the fitting LPPL model for Bitcoin Market Price expressed in US dollars (USD) over the period October 1, 2017 to November 30, 2017. The red line is the LPPL equation 4.36.

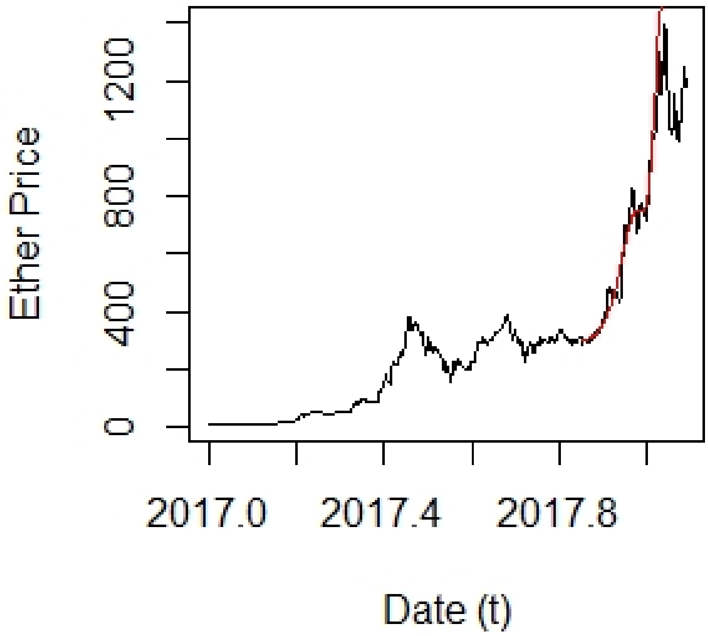


**Figure 4.7 LPPL fitting Ether market prices**
This figure shows the fitting LPPL model for Ether Market Price expressed in US dollars (USD) over the period November 1, 2017 to January 6, 2018. The red line is the LPPL equation 4.36.

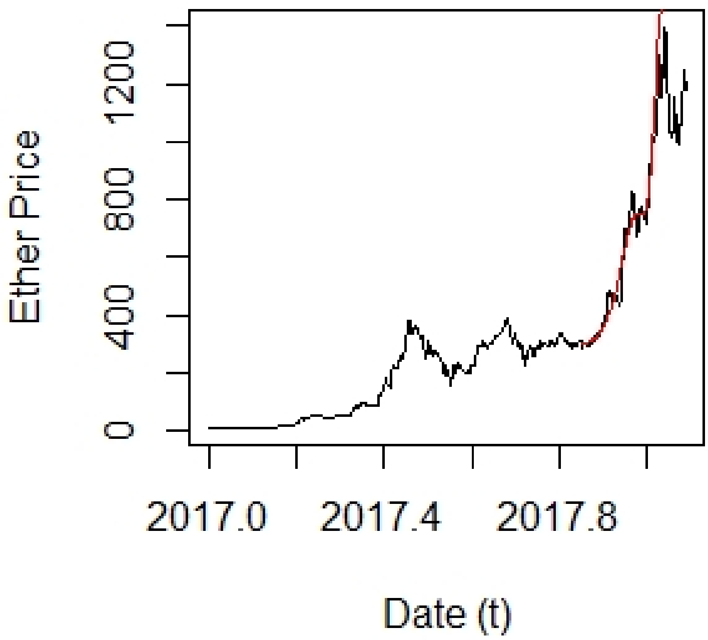


**Figure 4.8 LPPL fitting Litecoin market prices**
This figure shows the fitting LPPL model for Litecoin Market Price expressed in US dollars (USD) over the period November 5, 2017 to December 8, 2017. The red line is the LPPL equation 4.36.

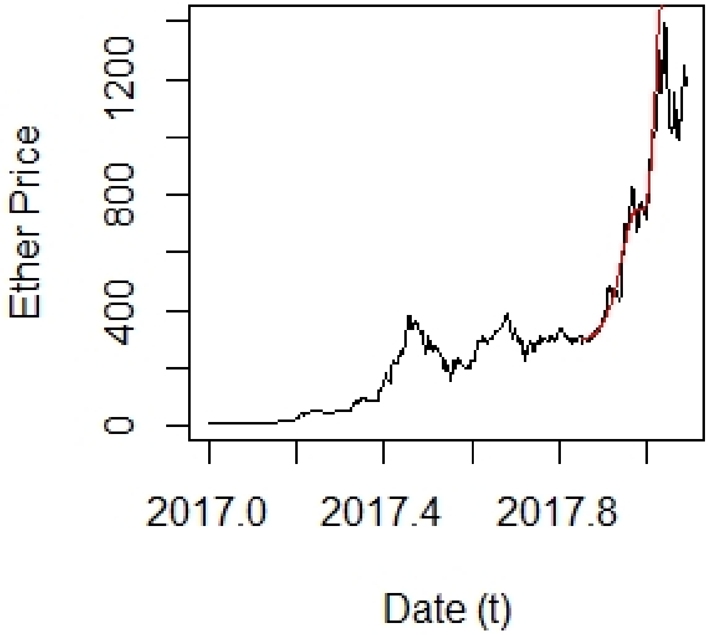


**Figure 4.9 LPPL Ripple market prices**
This figure shows the fitting LPPL model for Ripple Market Price expressed in US dollars (USD) over the period November 11, 2017 to December 26, 2017. The red line is the LPPL equation 4.36.

The most robust windows of Litecoin and Ripple are less stable than the ones of Bitcoin and Ether. For example, when we estimate the model for the most robust window of Ripple (November 1st, 2017 until December 26th, 2017), the estimated $t_c$ vary between a couple of days or the estimators does not respect the criteria 4.3.2.2 and 4.3.2.1. These results are confirmed by Tables 4.14 - *Numbers of significant results of LPPL - Expanding windows* and 4.15 - *Numbers of significant results of LPPL - Shrinking windows*[17].

[17] These tables display the occurrence for the analyze based on 600 iterations. We did also the work for 1,000, 10,000 and 100,000 iterations which confirm our results.

**Table 4.14 Numbers of significant results of LPPL - Expanding windows**

This Table presents the occurrence of the significant results according to the criteria of 4.3.2.2 and 4.3.2.1 and among them, the ones that provides a critical time, $t_c$, close to the actual crash date by cryptocurrencies.

| | BTC | ETH | LTC | XRP |
|---|---|---|---|---|
| *Window 1* | | | | |
| Total | 75 | 69 | 75 | 64 |
| Criteria 4.3.2.2 | 9 | 13 | 13 | 12 |
| *Close to $t_c$* | 2 | 3 | 0 | 1 |
| Criteria 4.3.2.1 | 17 | 24 | 10 | 11 |
| *Close to $t_c$* | 6 | 5 | 0 | 4 |
| *Window 2* | | | | |
| Total | 348 | 255 | 40 | 28 |
| Criteria 4.3.2.2 | 55 | 7 | 4 | 0 |
| *Close to $t_c$* | 0 | 0 | 2 | 0 |
| Criteria 4.3.2.1 | 83 | 18 | 6 | 1 |
| *Close to $t_c$* | 6 | 0 | 4 | 1 |
| *Window 3* | | | | |
| Total | 258 | | | |
| Criteria 4.3.2.2 | 47 | | | |
| *Close to $t_c$* | 0 | | | |
| Criteria 4.3.2.1 | 38 | | | |
| *Close to $t_c$* | 0 | | | |

**Table 4.15 Numbers of significant results of LPPL - Shrinking windows**

This Table presents the occurrence of the significant results according to the criteria of 4.3.2.2 and 4.3.2.1 and among them, the ones that provides a critical time, $t_c$, close to the actual crash date by cryptocurrencies.

| | Bitcoin | Ether | Litecoin | Ripple |
|---|---|---|---|---|
| *Window 1* | | | | |
| Total | 534 | | | |
| Criteria 4.3.2.2 | 34 | | | |
| *Close to $t_c$* | 6 | | | |
| Criteria 4.3.2.1 | 174 | | | |
| *Close to $t_c$* | 72 | | | |
| *Window 2* | | | | |
| Total | 76 | 302 | 600 | 600 |
| Criteria 4.3.2.2 | 3 | 7 | 83 | 22 |
| *Close to $t_c$* | 2 | 0 | 0 | 0 |
| Criteria 4.3.2.1 | 43 | 163 | 49 | 39 |
| *Close to $t_c$* | 26 | 0 | 2 | 10 |
| *Window 3* | | | | |
| Total | 600 | 203 | | |
| Criteria 4.3.2.2 | 41 | 111 | | |
| *Close to $t_c$* | 19 | 0 | | |
| Criteria 4.3.2.1 | 304 | 3 | | |
| *Close to $t_c$* | 152 | 0 | | |
| *Window 4* | | | | |
| Total | 600 | 490 | | |
| Criteria 4.3.2.2 | 80 | 161 | | |
| *Close to $t_c$* | 0 | 5 | | |
| Criteria 4.3.2.1 | 175 | 57 | | |
| *Close to $t_c$* | 0 | 22 | | |
| *Window 5* | | | | |
| Total | 600 | | | |
| Criteria 4.3.2.2 | 196 | | | |
| *Close to $t_c$* | 17 | | | |
| Criteria 4.3.2.1 | 39 | | | |
| *Close to $t_c$* | 2 | | | |

We notice that the peak/burst of Ripple and Litecoin are faster (their potential bubble last fewer days than Bitcoin and Ether), steeper (their price curve becomes almost a vertical line) and with less oscillations than Bitcoin and Ether. We can question a potential contagion between cryptocurrencies, perhaps the peak/burst of Ripple and Litecoin is a consequence of Bitcoin and Ether dynamics. The crash information takes time to be spread to the other cryptocurrencies (more than 1 month) and suggests the inefficiency of the market with possibility of arbitrage.

Indeed, Bitcoin and Ether dominate the cryptocurrency market, (see the general introduction of the dissertation) which is denoted by their price level compared to Ripple and Litecoin because cryptocurrency prices depend on the supply and the demand, Figure 4.2.

Based on the fixed windows, we run stationarity tests (unit root tests) because if the logarithm price in bubble phase is attributed to a deterministic LPPL component, the residuals of the LPPL fitting can by modeled by a mean-reversal Ornstein-Uhlenbeck, (Lin et al., 2009), (Lin and Sornette, 2009). For the best windows, we use Augmented Dickey-Fuller, Phillips-Peron and KPSS tests[18] Table 4.16 - *Stationarity test of the fitting LPPL residuals* presents the stationarity tests for the fitting LPPL residuals. We find that residuals from fitting LPPL model for Bitcoin for the window of October 1st, 2017 to November 30th, 2017 are stationary. This result confirms the robustness obtained by the different optimizations that always display this window as the best one to predict the actual crash. The other cryptocurrencies exhibit mixed stationary results.

For Ether and Ripple, two tests on three validate the stationarity tests, resp. Phillips-Perron and KPSS for Ether and ADF and Phillips-Perron for Ripple. As for Litecoin, it records mainly non-stationary residuals according to ADF and KPSS tests. These results may explain the fact that the Litecoin best window and result are less robust than the Bitcoin ones.

[18]The null-hypothesis of ADF and Phillips-Pero is unit root (non-stationarity) whereas the null-hypothesis for KPSS is stationarity.

**Table 4.16 Stationarity test of the fitting LPPL residuals**

This Table presents the stationarity tests of the fitting LPPL residuals for both Bitcoin, Ether, Litecoin and Ripple of the results found in table 4.13. We ran 3 differents tests, Augmented-Dickey Fuller (ADF), Phillips-Perron where the null-hypothesis meaning the residuals are not stationary and KPSS where the null-hypothesis meaning the residuals are stationary.

| | **ADF** | **Phillips-Perron** | **KPSS** |
|---|---|---|---|
| **BTC** | **-3.97** | **-19.38** | **0.05** |
| p-value | 0.02 | 0.06 | >0.1 |
| **ETH** | **-2.99** | **-21.85** | **0.06** |
| p-value | 0.17 | 0.03 | 0.10 |
| **LTC** | **-2.08** | **-17.807** | **0.94** |
| p-value | 0.54 | 0.06 | <0.01 |
| **XRP** | **-4.07** | **-29.787** | **0.64** |
| p-value | 0.01 | <0.01 | 0.02 |

In addition, we notice that sometimes the estimated crash, $t_c$, is not the actual crash but a "small" decrease in prices that actually happened with a different impact than actual crashes. For example, the LPPL for Bitcoin suggests an expected crash on November 12$^{th}$, 2017 ($t_c$ is 2017,864) based on the window of October 1$^{st}$, 2017 to November 3$^{rd}$, 2017. During this period the Bitcoin price is reaching \$7,400 the November 9$^{th}$, 2017 before decrease at \$5,675 few days after (November 13$^{th}$,2017).

## 4.5 Robustness

The results obtained in previously part 4.4 suggest a contagion effect in the cryptocurrency market. The PSY results show that the model estimates with increased precision bubbles for cryptocurrencies which crash is the first one (Bitcoin). In the LPPL results, we obtain that the least cryptocurrencies used by investors are those which results are the least stable, especially because the boom/burst occurs faster and without oscillations, thus challenging the definition of a bubble, perhaps as a reaction to bubbles/ bursting of bubbles of the two largest cryptocurrencies (Bitcoin and Ether).

The first robustness test we perform is to study the contagion between cryptocurrencies using DCC - GARCH Model of (Engle and Sheppard, 2001). The second robustness test presented in this part is the fundamental value analysis.

### 4.5.1 Contagion analysis

Contagion in the cryptocurrency market is a recent research field. The first study by (Fry and Cheah, 2016) finds a spillover from Bitcoin to Ripple. More recently, the problem is extended to other cryptocurrencies and consider longer periods of time. Using Granger Causality and Student-t Copulas, Huynh (2019) confirms that Bitcoin has a spillover effect on the cryptocurrency but Ether seems to be an independent cryptocurrency in the market. The explanation could due to the fact that Ethereum is a platform for Smart Contracts projects in addition of providing the cryptocurrency (Ether). The influence of Bitcoin on other cryptocurrencies is confirmed by a battery of others tests in (da Gama Silva et al., 2019). Ferreira and Pereira (2019) go further and study the contagion effect using the Detrended cross-correlation Analysis correlation before and after the 2017 boom. In this part, we will study the contagion between cryptocurrencies using the DCC-GARCH Model (Engle and Sheppard, 2001), (Orskaug, 2009), (Tsay, 2013).

The DCC-GARCH is a class of multivariate GARCH models that aims to decompose the covariance matrix ($H_t$) into conditional standard deviations diagonal matrix of time varying deviation from univariate GARCH ($D_t$) and a time varying correlation matrix ($R_t$). Orskaug (2009) presents the Dynamic Conditional Correlation GARCH model as follows:

$$r_t = \mu_t + a_t \tag{4.41}$$

Where $r_t$ are the log-returns of n assets at time t, $a_t$ are the mean-corrected returns from n assets with zero expected value and covariance matrix, $H_t$ and $\mu$ is the expected value of the conditional $r_t$.

$$a_t = H_t^{1/2} z_t \tag{4.42}$$

Where $H_t^{1/2}$ is a Cholesky factorization of $H_t$ (the conditional variances matrix of $a_t$).

The conditional correlation matrix is defined as:

$$H_t = D_t R_t D_t \tag{4.43}$$

The DCC structure can be extended as:

$$Q_t = (1 - \sum_{m=1}^{M} \alpha_m - \sum_{n=1}^{N} \beta_n)\bar{Q}_t + \sum_{m=1}^{M} \alpha_m (a_{t-m} a'_{t-m}) + \sum_{n=1}^{N} \beta_n Q_{t-1} \quad (4.44)$$

Where to ensure $R_t$ to be positive definite, $Q_t$ is a positive-definite matrix as well as $\alpha$ and $\beta$ (which both capture the dynamic dependence of the correlation) has to respects the following conditions: $\alpha >= 0$ and $\beta >= 0$ and $\alpha + \beta < 1$. $\bar{Q}_t$ is unconditional covariance matrix of the standardized residuals.

The articles of (Engle and Sheppard, 2001) and (Tsay, 2013) present more details about the DCC-GARCH methodology.

Our analysis is based on cryptocurrency returns of Bitcoin, Ether, Litecoin and Ripple on the period 2015–2019 and using R functions such as the *dccfit* and *dccspec* of the *rmgarch* package[19].

#### 4.5.1.1 Univariate Results

In this analysis, we are studying the correlation using the cryptocurrency returns, Figure 4.10 - *The top-4 cryptocurrencies returns* validating stationarity tests (Table 4.17).


**Figure 4.10 The top-4 cryptocurrencies returns**
This figure shows the Bitcoin, the Ether, the Litecoin and the Ripple returns over the period August 2015 to July 2019.

[19]https://rdrr.io/rforge/rgarch/man/dccfit-methods.html

| | **ADF** | **Phillips-Perron** | **KPSS** |
|---|---|---|---|
| *Panel A: cryptocurrency returns* | | | |
| **Bitcoin** | **-10,04** | **-1479,20** | **0,15** |
| p-value | < 0,01 | < 0,01 | > 0,1 |
| **Ether** | **-10,16** | **-1397,10** | **0,25** |
| p-value | < 0,01 | < 0,01 | > 0,1 |
| **Litecoin** | **-10,62** | **-1461,90** | **0,16** |
| p-value | < 0,01 | < 0,01 | > 0,1 |
| **Ripple** | **-9,64** | **-1671,00** | **0,16** |
| p-value | < 0,01 | < 0,01 | > 0,1 |
| *Panel B: cryptocurrency pirces* | | | |
| **Bitcoin** | **-2,58** | **-8,71** | **10,16** |
| p-value | 0,334 | 0,624 | <0,01 |
| **Ether** | **-1,81** | **-7,08** | **6,72** |
| p-value | 0,659 | 0,715 | <0,01 |
| **Litecoin** | **-2,67** | **-13,02** | **7,29** |
| p-value | 0,293 | 0,384 | <0,01 |
| **Ripple** | **-3,65** | **-25,43** | **6,41** |
| p-value | 0,028 | 0,023 | <0,01 |

**Table 4.17 Cryptocurrency returns and prices stationarity test**
This table presents the stationarity test for Bitcoin, Ether, Ripple and Litecoin returns (panel A) and prices (panel B). The sample is drawn from the coinmarketcap website over the period 2015–2019.

This table 4.17 shows the unit root results using ADF, Phillips-Peron and KPSS: all cryptocurrency returns are stationary contrary to cryptocurrency prices. Variables are integrated at I(0) (Huynh, 2019). The simple correlation matrices in Table 4.4 show that every cryptocurrency is linearly correlated to each other.

Figure 4.11 - *Autocorrelation of cryptocurrencies series* shows that the four series of cryptocurrency returns are not autocorrelated (not more than 5% outside the bound). Figure 4.12 - *Autocorrelation of cryptocurrencies series squares* presents the square autocorrelation. Most of time, the autocorrelation function is decreasing (first lags are highest than the last ones), the series present a pattern implying the square returns series is not uncorrelated. By definition, if the return series is dependent, this same series at square should be uncorrelated. However, it is not the case (the square series is not uncorrelated), therefore the series are correlated and it is relevant to use a GARCH model. Another condition to use a GARCH model is the fact that the return series has heavy tail (excess kurtosis greater than 0) largely supported for the four cryptocurrencies in Table 4.3.

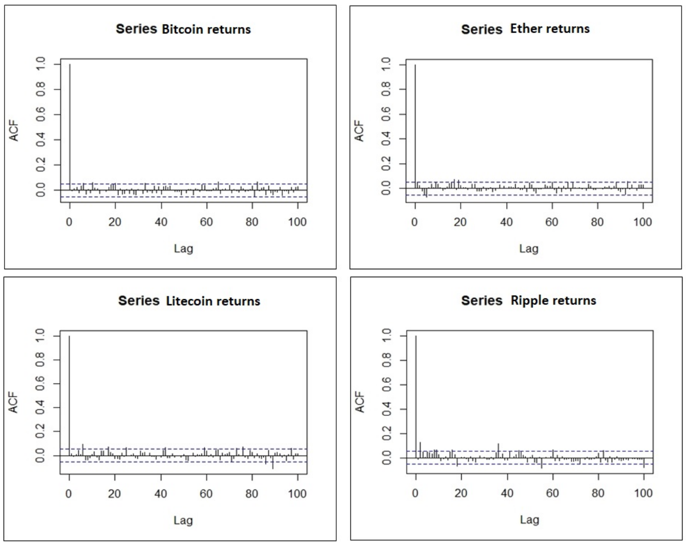


**Figure 4.11 Autocorrelation of cryptocurrencies series**
This figure shows the autocorrelation functions for Bitcoin, Ether, Litecoin and Ripple returns series.

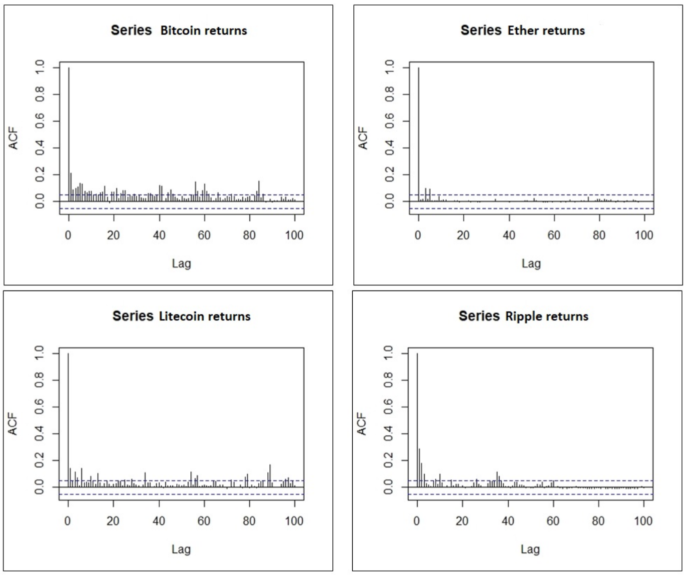


**Figure 4.12 Autocorrelation of cryptocurrencies series squares**
This figure shows the autocorrelation functions for Bitcoin, Ether, Litecoin and Ripple returns series squares.

4.5.1.2 DCC-GARCH Model

First, we are choosing the DCC-GARCH model that is DCC(1,1)[20], Table 4.18 - *Information related DCC-GARCH results*.

**Table 4.18 Information related DCC-GARCH results**

This table presents the information related to the results obtained in Table 4.19 using the DCC-GARCH analysis.

| | |
|---|---|
| Distribution | mvlaplace |
| Model | DCC(1,1) |
| N Parameters | 32 |
| VAR GARCH DCC UncQ | [0+24+2+6] |
| N Series | 4 |
| N Obs | 1325 |
| Log-Likelihood | 10632 .08 |
| Av .Log-Likelihood | 8 .02 |
| *Information criteria* | |
| Akaike | -16 |
| Bayes | -15 .875 |
| Shibata | -16 .001 |
| Hannan-Quinn | -15 .953 |
| Elapsed time | 4 .111489 |

Table 4.19 - *DCC-GARCH results* presents the results of the DCC-GARCH estimation. If we look at the $\alpha$ and $\beta$ of every cryptocurrency returns. They are all positive and significant expects for Bitcoin and Ripple's $\alpha$. The additive condition about $\alpha + \beta$ is respected for all the cryptocurrency except Bitcoin but they are not jointly insignificant. Finally, the information related to joint significance of $dcca1$ and $dccb1$ are both significant. Therefore, the DCC-GARCH is better to use than the Constant Conditional Variance.

[20]According to the *dccspec* function.

**Table 4.19 DCC-GARCH results**

This table presents the results for the effect of Bitcoin, Ether, Litecoin and Ripple using the DCC-GARCH method.

| | Estimate | Std. Error | t value | Pr(>\|t\|) |
|---|---|---|---|---|
| | | *Bitcoin* | | |
| mu | 0.002 | 0.002 | 0.903 | 0.366 |
| ar1 | 0.013 | 0.063 | 0.198 | 0.843 |
| omega | 0.000 | 0.000 | 0.134 | 0.894 |
| alpha1 | 0.102 | 0.158 | 0.647 | 0.517 |
| beta1 | 0.869 | 0.321 | 2.709 | 0.007 |
| gamma1 | -0.107 | 0.125 | -0.857 | 0.392 |
| delta | 2.499 | 0.543 | 4.601 | 0.000 |
| | | *Ether* | | |
| mu | 0.000 | 0.002 | 0.159 | 0.874 |
| ar1 | 0.041 | 0.042 | 0.974 | 0.330 |
| ar2 | 0.108 | 0.050 | 2.142 | 0.032 |
| omega | 0.000 | 0.000 | 2.291 | 0.022 |
| alpha1 | 0.234 | 0.064 | 3.638 | 0.000 |
| beta1 | 0.700 | 0.076 | 9.205 | 0.000 |
| gamma1 | -0.030 | 0.059 | -0.502 | 0.616 |
| | | *Litecoin* | | |
| mu | 0.001 | 0.001 | 0.448 | 0.654 |
| omega | 0.000 | 0.000 | 1.512 | 0.131 |
| alpha1 | 0.065 | 0.019 | 3.492 | 0.000 |
| beta1 | 0.899 | 0.027 | 32.945 | 0.000 |
| | | *Ripple* | | |
| mu | -0.003 | 0.001 | -1.912 | 0.056 |
| ar1 | 0.018 | 0.043 | 0.408 | 0.683 |
| omega | 0.000 | 0.000 | 1.157 | 0.247 |
| alpha1 | 0.369 | 0.228 | 1.620 | 0.105 |
| alpha2 | 0.000 | 0.202 | 0.000 | 1.000 |
| beta1 | 0.609 | 0.283 | 2.147 | 0.032 |
| | | *Joint* | | |
| dcca1 | 0.044 | 0.008 | 5.826 | 0.000 |
| dccb1 | 0.953 | 0.009 | 110.827 | 0.000 |

Figure 4.13 - *The dynamic correlation coefficients* presents the correlation of volatilities over time between each couple of cryptocurrencies (Bitcoin, Ether, Litecoin and Ripple). All correlations are between -0.4 and 0.8. The graph shows that during the cryptocurrency market crash of the end of 2017, there is a drastic fall in correlation between each cryptocurrency (Ether, Litecoin and

Ripple) and Bitcoin. Whilst the correlation between Ether and Litecoin is stable even during the crash, the correlation Ether–Ripple and Litecoin–Ripple is slightly decreasing.

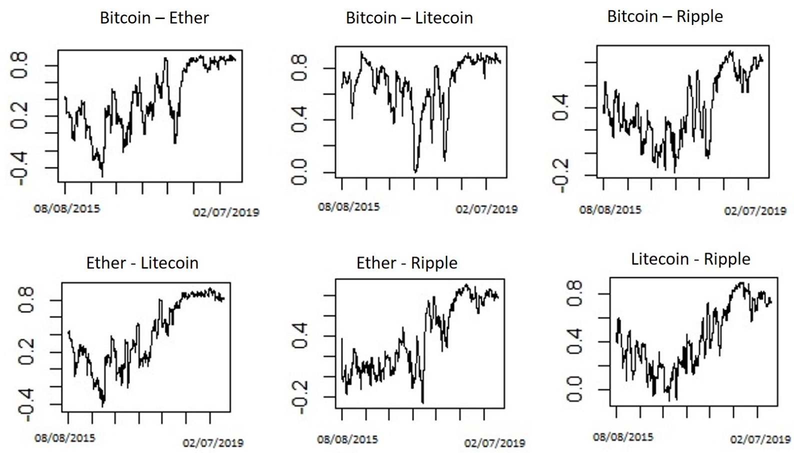


**Figure 4.13 The dynamic correlation coefficients**
This figure shows the dcc correlation over time for Bitcoin, Ether, Litecoin and Ripple since 08/08/2015 to 02/07/2019

### 4.5.2 Cryptocurrencies' fundamental value model

As presented in the literature review 4.2.3, the fundamental value of the cryptocurrency is the subject of ongoing debate. In this part, we choose to present and test the model of Wheatley et al. (2019).

It depends on its active user in the network using the Metcalfe's Law. The more there are users in a network, the more the network is valued.

They find that the equation for the market cap of Bitcoin is:

$$p = e^{-3} u_i^{2\prime} \tag{4.45}$$

Where $u_i$ is the smoothed active users represented by the number of the active addresses in the Bitcoin network and $p$ the Metcalfe's Law value (the predicted market capitalization).

We apply this model, only for Bitcoin, on the period of October 1st, 2013 to July 3rd, 2019 using variables as the market capitalization of Bitcoin and the number of unique Bitcoin addresses from Quandl[21].

Figure 4.14 - *Predicted and actual market capitalization of Bitcoin* compares the actual market capitalization of Bitcoin and its predicted market capitalization obtained with the model of estimation of (Wheatley et al., 2019). These two curves are really close to each others, confirming the intuition of (Wheatley et al., 2019), over a longer period of data.

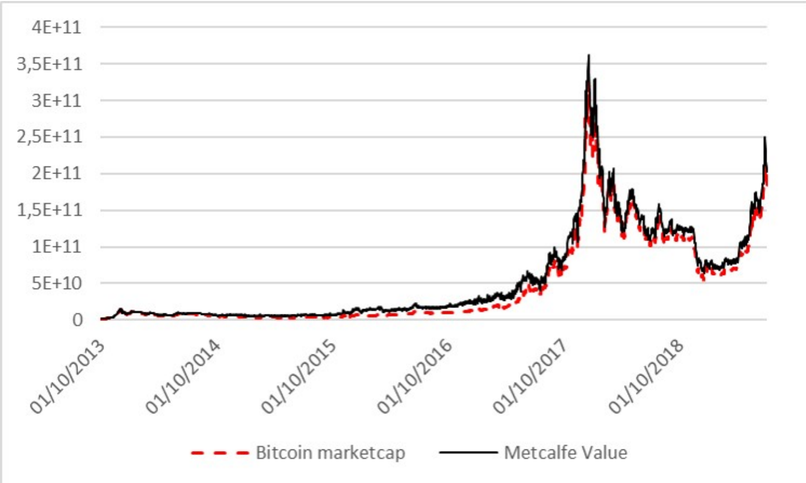


**Figure 4.14 Predicted and actual market capitalization of Bitcoin**
This Figure presents the actual market capitalization of Bitcoin and its prediced market capitalization obtained through the model of (Wheatley et al., 2019).

## 4.6 Conclusion

This chapter aims to analyze the bubble aspect of the cryptocurrency using four proxies; Bitcoin, Ether, Ripple and Litecoin by using the PSY model, (Phillips and Shi, 2018) to detect several periods of bubbles, and the LPPL model (Johansen et al., 2000) to focus our study on the main boom in the cryptocurrency market at the end of 2017. In the multiple bubble study, we find several periods of bubbles notably in 2013 and in 2017 and the results are more accurate for recent periods. Regarding the main boom analysis of the end of 2017, the LPPL model detects a critical time more precise and more stable for Ether and Bitcoin than for Ripple and Litecoin. Cryptocurrencies seems to be correlated to each other suggesting a possible contagion effect inside the market. This correlation

[21]https://www.quandl.com/

varies over times and the correlation with Bitcoin is less strong during the crash period of the end of 2017. As another robustness test, we test the fundamental value estimation model of (Wheatley et al., 2019). We confirm the robust comparison between users and market capitalization.

Regarding the methodology and robustness, it could be interesting to check other diagnostic tests (Lin and Sornette, 2009), and sensitivity tests, such as the Lomb spectral analysis used in (Jiang et al., 2010) to confirm the robustness of our results in the LPPL model. To avoid the problem of non-stationarity of prices, a work is ongoing about applying the LPPL model using returns instead of prices, based on (Chang et al., 2016), (Lin et al., 2009), (Lin et al., 2014). The contagion analysis is slightly analyzed. We could also extend the analysis to interdependence tests (Forbes and Rigobon, 2002) and to go further in the study of the contagion in “normal” situations versus in “bubble” situation (Kohn and Pereira, 2017).

After a general decrease in prices on the cryptocurrency market without any exponential increase before in November 2018, a new price increase is appeared (Bitcoin exceeds again the $10,000 in the end of June 2019) that could be tested using (Phillips and Shi, 2018) and (Johansen et al., 2000) models. The hypotheses of the LPPL model are constrained because it is a physical model applied to finance. In practice, because markets are not perfect, some frictions are present, such as information asymmetries. The suggestion of contagion effect within the market implies a transfer of information between cryptocurrencies over time (there is one month of gap between the Bitcoin crash and the Ether one for example). This presupposes arbitrage opportunities between cryptocurrencies and also between platform exchanges that provides slightly different prices. Some existing research shows how Bitcoin is related to monetary policy decisions, such as a “store of refuge” during the Cyprus crisis in 2014, or related to the Federal Reserve monetary policy. It could be interesting to take into consideration these information asymmetries, risk aversion and external impact of political news, to reflect and analyze better the cryptocurrency market.

Finally, additional research may also focus on the issue whether Bitcoin has an economic value. Based on the different estimation models of fundamental value recently appears in the literature, we could develop them to find the best estimate possible of factors that drive the fundamental value of cryptocurrency.

## References

Abadi, J. and Brunnermeier, M. (2018). Blockchain economics, *Working Paper* **v3**.

Azariadis, C. (1998). Self-fulfilling prophecies, *Journal of Economic Theory* **25**: 380–96.

Baek, C. and Elbeck, M. (2014). Bitcoins as an investment or speculative vehicle? A first look, *Applied Economics Letters* **22**(1): 30–34.

Baur, D. G., Hong, K. and Lee, A. D. (2016). Virtual currencies: Media of exchange or speculative asset?, *SWIF Institute Working Paper* (2014-007).

Bhambhwani, S., Delikouras, S. and Korniotis, G. M. (2019). Do fundamentals drive cryptocurrency prices?, *SSRN Electronic Journal* .

Biais, B., Bisière, C., Bouvard, M., Casamatta, C. and Menkveld, A. (2018). Equilibrium bitcoin pricing, *SSNR Elec. Journal* .

Blanchard, O. J. and Watson, M. W. (1982). Bubbles, rational expectations and financial markets, *Crises in the Economic and Financial Structure* pp. 295–316.

Bouri, E., Molnár, P., Azzi, G., Roubaud, D. and Hagfors, L. I. (2016). On the hedge and safe haven properties of bitcoin: Is it really more than a diversifier?, *Finance Research Letters* **20**: 192–198.

Bouri, E., Shahzad, S. J. H. and Roubaud, D. (2019). Co-explosivity in the cryptocurrency market, *Finance Research Letters* **29**: 178–183.

Brée, D. and Joseph, N. L. (2013). Testing for financial crashes using the Log Periodic Power Law model, *International Review of Financial Analysis* **30**: 287–297.

Brunnermeier, M. (2008). Bubbles, *in* S. Durlauf and L. Blume (eds), *The New Palgrave Dictionary of Economics*, pp. 578–583.

Cagli, E. C. (2019). Explosive behavior in the prices of bitcoin and altcoins, *Finance Research Letters* **29**: 398–403.

Campbell, J. Y. and Shiller, R. J. (1988). The dividend-price ratio and expectations of future dividends and discount factors, *The Review of Financial Studies* **1**(3): 195–228.

Chaim, P. and Laurini, M. (2019). Is bitcoin a bubble?, *Physica A: Statistical Mechanics and its Applications* **517**: 222–232.

Chang, V., Newman, R., Walters, R. and Wills, G. (2016). Review of economic bubbles, *International Journal of Information Management* **36**(4): 497–506.

Cheah, E.-T. and Fry, J. (2015). Speculative bubbles in bitcoin markets? An empirical investigation into the fundamental value of bitcoin, *Economics Letters* **130**: 32–36.

Cheung, A., Roca, E. and Su, J. (2015). Crypto-currency bubbles: An application of the Phillips-Shi–Yu (2013) methodology on Mt. Gox bitcoin prices, *Applied Economics* **47**(23): 2348–2358.

Corbet, S., Lucey, B. and Yarovaya, L. (2017). Datestamping the bitoin and ethereum bubbles, *Finance Research Letter* .

da Gama Silva, P. V. J., Klotzle, M. C., Pinto, A. C. F. and Gomes, L. L. (2019). Herding behavior and contagion in the cryptocurrency market, *Journal of Behavioral and Experimental Finance* **22**: 41–50.

Dale, R. S., Johnson, J. E. V. and Tang, L. (2005). Financial markets can go mad: Evidence of irrational behaviour during the south sea bubble, *The Economic History Review* **LVIII**(2): 233–271.

de la Horra, L., de la Fuente, G. and Perote, J. (2019). The drivers of bitcoin demand: A short and long-run analysis, *International Review of Financial Analysis* **62**: 21–34.

Diba, B. and Grossman, H. (1988). Explosive rational bubbles in stock prices?, *The American Economic Review* **78**(3): 520–530.

Dyhrberg, A. H. (2016a). Bitcoin, gold and the dollar – A GARCH volatility analysis, *Finance Research Letters* **16**: 85–92.

Dyhrberg, A. H. (2016b). Hedging capabilities of bitcoin. Is it the virtual gold?, *Finance Research Letters* **16**: 139–144.

Easley, D., O'Hara, M. and Basu, S. (Forthcoming). From mining to markets: The evolution of bitcoin transaction fees, *Journal of Financial Economics* .

Engle, R. F. and Sheppard, K. (2001). Theoretical and empirical properties of dynamic conditional correlation multivariate GARCH, *NBER Working Paper* **8554**.

Evans, G. W. (1991). Pitfalls in testing for explosive bubbles in asset prices, *The American Economic Review* **81**(4): 922–930.

Fantazzini, D., Nigmatullin, E., Sukhanovskaya, V. and Ivliev, S. (2017). Everything you always wanted to know about bitcoin modelling but were afraid to ask, *Applied Econometrics* **45**: 5–28.

Ferreira, P. and Pereira, E. (2019). Contagion effect in cryptocurrency market, *Journal of Risk and Financial Management* **12**(3): 1–8.

Figuet, J.-M. (2016). Bitcoin et blockchain : quelles opportunités ?, *Revue d'économie financière* **123**(3): 325–338.

Filimonov, V. and Sornette, D. (2013). A stable and robust calibration of the log-periodic power law model, *Physica A: Statistical Mechanics and its Applications* **392**(17): 3698–3707.

Flavin, M. A. (1983). Excess volatility in the financial markets: A reassessment of the empirical evidence, *Journal of Political Economy* **91**(6): 929–956.

Flood, R. and Garber, P. (1980). Market fundamentals versus price-level bubbles: The first tests, *Journal of Political Economy* **88**(4): 745–770.

Flood, R., Hodrick, R. and Kaplan, P. (1986). An evaluation of recent evidence on stock market bubbles, *NBER Working Paper* **1971**.

Flood, R. P. and Hodrick, R. J. (1990). On testing for speculative bubbles, *Journal of Economic Perspectives* **4**(2): 85–101.

Folkinshteyn, D., Lennon, M. and Reilly, T. (2015). A tale of twin tech: Bitcoin and the WWW, *Journal of Strategic and International Studies* **10**(2).

Forbes, K. J. and Rigobon, R. (2002). No contagion, only interdependance: Measuring stock market comovements, *The Journal of Finance* **57**(5): 2223–2261.

Frankel, J. A. and Froot, K. A. (1990). Chartists, fundamentalists, and trading in the foreign exchange market, *American Economic Review* **80**(2): 181–185.

Froot, K. A. and Obstfeld, M. (1991). Intrinsic bubbles: The case of stock prices, *The American Economic Review* **81**(5): 1189–1214.

Fry, J. (2018). Booms, busts and heavy-tails: The story of bitcoin and cryptocurrency markets?, *Economics Letters* **171**: 225–229.

Fry, J. and Cheah, E.-T. (2016). Negative bubbles and shocks in cryptocurrency markets, *International Review of Financial Analysis* **47**: 342–352.

Gangwal, S. and Longin, F. (2018). Extreme movements in bitcoin prices : A study based on extreme value theory, *Working Paper* .

Garcia, D., Tessone, C., Mavrodiev, P. and Perony, N. (2014). The digital traces of bubbles: feedback cycles between socio-economic signals in the bitcoin economy, *Journal of the Royal Society Interface* **11**.

Geuder, J., Kinateder, H. and Wagner, N. F. (2018). Cryptocurrencies as financial bubbles: The case of bitcoin, *Finance Research Letters* **Online**.

Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. C. and Siering, M. (2014). Bitcoin - Asset or Currency? Revealing users' hidden intentions, *Twenty Second European Conference on Information Systems*.

Godsiff, P. (2015). Bitcoin: Bubble or blockchain, *Smart Innovation, Systems and Technologies* **38**: 191–203.

Grant, J. M. (2014). Is bitcoin money?: Implications for bitcoin derivatives regulation and security interest treatment of bitcoins under article 9 of the uniform commercial code, *New York University (NYU), School of Law* .

Gurkaynak, R. S. (2008). Econometric tests of asset price bubbles: Taking stock, *Journal of Economic surveys* **22**(1): 166–186.

Hafner, C. (2018). Testing for bubbles in cryptocurrencies with time-varying volatility, *SSNR Elec. Journal* .

Hansen, N. (2011). CMA_ES: A stochastic second order method for function-value free numerical optimization, *MSRC* .

Hansen, N. (2016). The CMA evolution strategy: A tutorial, *Working Paper* .

Hansen, N. (2017). Function-value-free second-order stochastic optimization with CMA-ES, *Presentation* .

Hansen, N. and Kern, S. (2004). Evaluating the CMA evolution strategy on multimodal test functions, *Parallel Problem Solving from Nature* **VIII**: 282–291.

Harrison, J. M. and Kreps, D. M. (1978). Speculative investor behavior in a stock market with heterogeneous expectations, *The Quarterly Journal of Economics* **92**(2): 323–336.

Hayes, A. S. (2017). Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin, *Telematics and Informatics* **34**(7): 1308–1321.

Hayes, A. S. (2018). Bitcoin price and its marginal cost of production: Support for a fundamental value, *Applied Economics Letters* **Forthcoming**.

Huynh, T. L. D. (2019). Spillover risks on cryptocurrency markets: A look from VAR-SVAR Granger causality and Student's-t Copulas, *Journal of Risk and Financial Management* **12**(2): 1–19.

Jiang, Z.-Q., Zhou, W.-X., Sornette, D., Woodardb, R., Bastiaensen, K. and Cauwels, P. (2010). Bubble diagnosis and prediction of the 2005-2007 and 2008-2009 Chinese stock market bubbles, *Journal of Economic Behavior & Organization* **74**(3): 149–162.

Johansen, A. (2003). Characterization of large price variations in financial markets, *Physica A: Statistical Mechanics and its Applications* **234**(1-2): 157–166.

Johansen, A., Ledoit, O. and Sornette, D. (2000). Crashes as critical point, *International Journal of Theoretical and Applied Finance* **3**(2): 219–255.

Johansen, A. and Sornette, D. (2001). Bubbles and anti-bubbles in Latin-American, Asian and Western stock markets: An empirical study, *International Journal of Theoretical & Applied Finance* **4**: 853–920.

Johansen and Sornette (1990). Financial “anti-bubbles”: Log-periodicity in Gold and Nikkei collapses, *International Journal of Modern Physics* **10**(4): 563–575.

Kancs, D., Ciaian, P. and Miroslava, R. (2015). The digital agenda of virtual currencies. Can bitcoin become a global currency?, *Publications Office of the European Union, JRC Technical report* .

Kleidon, A. (1986). Variance bounds tests and stock price valuation models, *Journal of Political Economy* **94**(5): 953–1001.

Kohn, M.-B. H. and Pereira, P. L. V. (2017). Speculative bubbles and contagion: Analysis of volatility’s clusters during the DotCom bubble based on the dynamic conditional correlation model, *Cogent Economics & Finance* **5**: 1–28.

Kristoufek, L. (2019). Is the bitcoin price dynamics economically reasonable? Evidence from fundamental laws, *Physica A: Statistical Mechanics and its Applications* **Online**(120873).

LeRoy, S. F. and Porter, R. D. (1981). The present value relation: Tests based on implied variance bounds, *Econometrica* **49**(3): 555–574.

Li, Z.-Z., Tao, R., wei su, C. and Lobont, O.-R. (2019). Does bitcoin bubble burst?, *Quality & Quantity* (1).

Lin, L., Ren, R. E. and Sornette, D. (2009). A consistent model of ’explosive’ financial bubbles with mean-reversing residuals, *International Review of Financial Analysis* **33**: 210–225.

Lin, L., Ren, R. and Sornette, D. (2014). The volatility-confined LPPL model: A consistent of “explosive” financial bubbles with mean-reverting residuals, *International Review of Financial Analysis* **33**: 210–225.

Lin, L. and Sornette, D. (2009). Diagnostics of rational expectation financial bubbles with stochastic mean-reverting termination times, *European Journal of Finance* **19**(5).

MacDonnell, A. (2014). Popping the bitcoin bubble: An application of log-periodic power law modeling to digital currency, *Working Paper* .

Malhotra, A. and Maloo, M. (2014). Bitcoin – Is it a bubble? Evidence from unit root tests, *SSRN Electronic Journal* .

Marsh, T. A. and Merton, R. C. (1986). Dividend variability and variance bounds tests for the rationality of stock market prices, *The American Economic Review* **76**(3): 483–498.

Miller, E. M. (1977). Risk, uncertainty, and divergence of opinion, *The Journal of Finance* **32**(4): 1151–1168.

Nadarajah, S. and Chu, J. (2017). On the inefficiency of bitcoin, *Economics Letter* **150**: 6–9.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system, *White paper* .

Ofek, E. and Richardson, M. (2003). DotCom Mania: The rise and fall of internet stock prices, *The Journal of Finance* **LVIII**(3): 1113–1137.

Onsager, L. (1944). Crystal statistics. A two-dimensional model with an order-disorder transition, *Physics Review* **65**(3-4): 117–149.

Orskaug, E. (2009). Multivariate DCC-GARCH model - With various error distributions, *Norwegian University of science and Technology* .

Pagnotta, E. and Buraschi, A. (2018). An equilibrium valuation of bitcoin and decentralized network assets: Non-technical summary, *SSRN Elec. Journal* .

Phillips, P. and Shi, S. (2018). Real time monitoring of asset markets: Bubbles and crises, *Cowles Foundation Discussion Paper* (2152).

Phillips, P., Shi, S. and Yu, J. (2015). Testing for multiple bubbles: Historical episodes of exuberance and collapse in the S&P 500, *International Economic Review* **56**(4): 1043–1078.

Phillips, P., Wu, Y. and Yu, J. (2011). Explosive behavior in the 1990s Nasdaq: When did exuberance escalate asset values?, *International Economic Review* **52**(1): 201–226.

Scheinkman, J. A. and Xiong, W. (2003). Overconfidence and speculative bubbles, *Journal of Political Economy* **111**(6): 1183–1219.

Selgin, G. (2015). Synthetic commodity money, *Journal of Financial Stability* **17**(92-99).

Shiller, R. (2005). *Irrational Exuberance*, Princeton University Press.

Sockin, M. and Xiong, W. (2018). A model of cryptocurrencies, *Working Paper* **NBER AP**.

Sornette, D. (2003). *Why Stock Markets Crash: Critical Events in Complex Financial Systems*, Princeton.

Sornette, D. (2009). Dragon-kings, black swans and the prediction of crises, *International Journal of Terraspace Science and Engineering* **2**(1): 1–18.

Sornette, D. and Cauwels, P. (2014). Financial bubbles: Mechanisms and diagnostics, *arXiv Working Paper* .

Sornette, D. and Johansen, A. (1997). Large financial crashes, *Physica A: Statistical Mechanics and its Applications* **245**: 411–422.

Sornette, D., Johansen, A. and Bouchaud, J.-P. (1996). Stock market crashes, precursors and replicas, *Journal de Physique I* **6**: 167–175.

Sornette, D., Woodard, R., Yan, W. and Zhou, W.-X. (2012). Clarifications to questions and criticism on the Johansen–Ledoit–Sornette financial bubble model, *ETH Risk Center Working Paper* (11-004).

Sornette, D., Woodard, R. and Zhou, W.-X. (2009). The 2006-2008 oil bubble and beyond, *Physica A: Statistical Mechanics and its Applications* **388**(8): 1571–1576.

Sornette, D. and Zhou, W.-X. (2002). The US 2000-2002 market descent: How much longer and deeper?, *Quantitative Finance 2* **6**: 468–481.

Su, C.-W., Li, Z.-Z., Tao, R. and Si, D.-K. (2018). Testing for multiple bubbles in bitcoin markets: A generalized sup ADF test, *Japan and the World Economy* **46**: 56–63.

Taipalus, K. (2012). Signaling asset price bubbles with time-series methods, *Bank of Finland Research Discussion Papers* (7).

Taleb, N. N. (2007). *The Black Swan: The Impact of the Highly Improbable*, Random House.

Tsay, R. (2013). *Multivariate Time Series Analysis*, Wiley.

Umeh, J. (2016). Blockchain: Double bubble or double trouble?, *ITNOW* **58**(1): 58–61.

Urquhart, A. (2017). Price clustering in bitcoin, *Economics Letter* **159**: 145–148.

Vissing-Jorgensen, A. (2003). Perspectives on behavioral finance: Does "irrationality" disappear with wealth? Evidence from expectations and actions, *NBER Working Paper* **18**.

Vogiazas, S. and Alexiou, C. (2019). Bitcoin: The road to hell is paved with good promises, *Economic Notes, Review of Banking, Finance and Monetary Economics* **48**(1).

West, K. D. (1987). A specification test for speculative bubbles, *The Quarterly Journal of Economics* **102**: 553–80.

Wheatley, S., Sornette, D., Huber, T., Reppen, M. and Gantner, R. (2019). Are bitcoin bubbles predictable? Combining a generalized Metcalfe's Law and the log-periodic power law singularity model, *Royal Society Open Science* **6**.

Woo, W. T. (1987). Some evidence of speculative bubbles in the foreign exchange markets, *Journal of Money, Credit and Banking* **19**(4): 499–514.

Yermack, D. (2017). Corporate governance and blockchains, *Review of Finance* **21**(1): 1–31.

Zhou, W.-X. and Sornette, D. (2003). 2000-2003 real estate bubble in the UK but not in the USA, *Physica A: Statistical Mechanics and its Applications* **329**(1-2): 249–263.

# Chapter 5

# General Conclusion

## 5.1 Main findings and contributions

Initiated with Bitcoin, cryptocurrencies provide new and interesting avenues of research in the field of finance. This thesis examines cryptocurrencies and their underlying technology, the blockchain, from an informational efficiency perspective. The blockchain is a technology aimed to record and share information in a transparent and decentralized manner. Based on this information-based system (the blockchain), cryptocurrencies are traded by investors who benefit from this highly transparent and distributed system. Cryptocurrencies display a particularly high risk and return profile, uncorrelated to other main financial assets.

Our analysis focuses first on the structure of cryptocurrencies and the underlying technology, the blockchain, by adopting a managerial perspective. Second, we discuss the nature of cryptocurrencies and analyze their performance from a financial perspective. Third, taking into account the high volatility of cryptocurrencies, we question their speculative bubble nature. The conceptual and empirical findings bring contributions to both academics and practitioners from these three different perspectives.

Chapter 2 focuses on the blockchain technology impact in terms of informational efficiency within organizations. The chapter provides a theoretical framework for the blockchain built around the contractual approach (transaction costs, agency issues, incomplete contracts and property rights theories) as well as the cognitive approach of the organization theory. Blockchain unique characteristics (transparency, decentralization, consensus mechanism, cryptographic security, Smart Contracts) fuels some related concepts to these theories and also imply new issues for academic research. For instance, the consensus-based mechanism designed to secure the transactions has the potential to control for potential opportunistic behaviors and decreases moral hazard issues. However, the two main consensus mechanisms can be either energy consuming (Proof-of-Work) or leading to some social inertial effects (Proof-of-Stake). In the contractual approach of organization theory, the blockchain takes the form of Smart Contracts designed to solve opportunistic behavior issues and manage uncertainty. These contracts decrease audit costs because the system is automated. Most challenges are post-contract and increased negotiation costs. Smart Contracts attempt to take into consideration as many possible situations, thus reducing unexpected but sometimes beneficial opportunities. Sometimes, unexpected events create new business opportunities. The human intervention is required to build a smart contract and reduce the occurrence of technical issues. Such issues can also appear because the entire system is based on cryptographic principles not immune to potential bugs, attacks, or technology evolution implying potential financial losses. The cost of entry is high but allows a decrease in complexity (less intermediaries and more direct exchanges), decreasing agency costs. The transparency characteristic increases the access to information and therefore decreases transaction costs and agency costs. The decentralization of powers through the distributed network increases the participation of each stakeholder inside the organization and increases the potential of social welfare. Transparency and decentralization are sometimes controversial for businesses regarding sensitive and confidential data. For this reason, users' access (transparency) and miners' rights (decentralization of power) vary according to the project set up by the company. We highlight a two-level dimensional analysis based on both community dimensions (users and miners) and define four possible cases of blockchain (public/private and permissionless/permissioned). The evolution of the blockchain starts from the public permissionless blockchain (similar to the Bitcoin cryptocurrency) toward the private permissioned blockchain (Facebook's cryptocurrency project, Libra) creating the potential for new institutions and standards.

This chapter has theoretical implications because it provides a conceptual study on the blockchain topic in management research, especially regarding the organization theory. We propose an original approach through the community concept and an illustrated literature review with several examples of blockchain projects. Managerial implications are also an important contribution particularly for companies by increasing stakeholders' participation: managers could strengthen their leadership, employees could become expert members, and investors could become more aware of the reality and be more active in real time. Blockchain technology is also source of public policy contributions because it has the potential to change the way the society is organized by integrating individuals at the core of decisions (through distributed networks). This technology could help to enhance the financial integration of excluded individuals, promote e-voting as well as create new jobs (in the IT field because the technology is based on computing and cryptographic principles as well as in legal domain because this new technology requires new adapted rules to protect individuals in their exchanges). The interest of this subject for public policy is also the regulation of blockchains. Different legal issues arise such as the (non)reversibility of transactions and potential conflicts in the execution of Smart Contracts. In a globalized world, national laws compete with each other and, in a virtual world, the lack of regulation can hinder the development of blockchains (case of Facebook's Libra). The creation of new international standards thus appears to be a crucial issue.

Chapter 3 questions the true nature of Bitcoin by comparing it to: (1) Currencies; (2) Gold; (3) Common stocks. The first initial intuition is to compare Bitcoin (and by extension cryptocurrencies) to traditional currencies. However, Bitcoin does not respect the three fundamental economic properties of a standard currency: medium of exchange, unit of account and store of value. Bitcoin allows individuals to exchange goods and services with each other and seems to play a medium of exchange role. However, the costs of entry prevent businesses to accept it as mean of payment, the lack of legal framework and the impossibility to make loans on the cryptocurrency market differentiates it from medium of exchange property. Bitcoin is divisible but its volatility and inelastic supply do not truly validate the unit of account property. Finally, the particular economic model based on the inflation/deflation issue, the high volatility of prices and the risk in cybersecurity, which reduces trust in Bitcoin, make it difficult to be considered as a stable store of value.

The second hypothesis compares Bitcoin to gold. While both may play the role of safe haven in specific market phases, have a limited supply, a monetary creation lies on “mining process” and there is no control by any goverment, Bitcoin and gold have also differences. The supply rules are divergent, more precisely the maximum number of Bitcoin is fixed and their release is divided periodically whereas gold mining can be subject to forecasts but without precise rules. The market capitalization of gold is much larger than for Bitcoin and their prices uncorrelated. In addition, compared to gold, Bitcoin has no physical form. Therefore, Bitcoin, and by extension cryptocurrencies, cannot be fully assimilated to gold.

Another possibility analyzed in this thesis is that Bitcoin may be assimilated to financial assets and more precisely common stocks. The particular high-return and high-risk profile of Bitcoin makes it similar to common stock. Bitcoin can be viewed as a share of intangible assets such as the blockchain technology and the human capital of experts. This argument is supported by empirical research (Glaser et al., 2014), (Yermack, 2015), (Baur et al., 2016) and by legal frameworks with security-based definitions of the Internal Revenue Service (2014) and the Securities and Exchange Commission (2015). In practice, mutual and hedge funds use cryptocurrencies as financial assets: Pantera Capital exists since 2013 and integrates five cryptocurrency funds in two venture funds devoted for institutional investors. CoinCapital, created in 2016 and integrating 40 cryptocurrencies and blockchain startups and ICOs, is a solution for individual investors. Other funds can be oriented by region. In 2016, PolyChain Capital is created by Olaf Carlson-Wee and dedicated for the world’s investors, while First Block Capital concerns Canadian investors. Recently, in 2019, CMCC Global venture capital group of Hong Kong launched the Liberty Bitcoin Fund for accredited investors in Asia. Finally, the Bitcoins Reserve fund focuses exclusively on arbitrage opportunities between the different cryptocurrency exchange platforms.

If the Bitcoin is assimilated to an investment opportunity, it is important to analyze its performance. The Sharpe Ratio is one widely-used measure of performance but in our view this measure is insufficient. Based on the previous assumption that Bitcoin, and by extensions cryptocurrencies, can be assimilated to financial contracts, more precisely to common stocks, we estimate the Bitcoin performance using CAPM, Fama-French and other extended models widely used in the context of the stock market. We find that Bitcoin exhibits a strong and highly significant annualized alpha regardless of the regions (World, Europe, Asia-Pacific). Our findings are robust to model specification, to taking into account residuals (RALS) non-normality issues and to market sentiment variables (such variables are used in order to capture a speculative behavior of the cryptocurrency market).

The main contributions of chapter 3 are twofold. First, the study provides a clear discussion about the true nature of cryptocurrencies and the interest to compare them to financial assets such as common stocks. Second, the study is the first, to our knowledge, to provide solid, academic-based financial performance measures based on the CAPM and Fama-French models for cryptocurrencies.

In Chapter 4, we show that cryptocurrencies have a true fundamental value based on our literature review. However, periods of bubbles are identified notably at the end of 2013 and at the end of 2017. First, we analyze the entire period of time for the four main cryptocurrencies (Bitcoin, Ether, Ripple and Litecoin) using the methodology of (Phillips and Shi, 2018) and we notice that Ripple and Litecoin provide better information detection. The second analysis focuses on the peak/burst at the end of 2017 which is: (1) Graphically apparent; (2) Detected in the first step by the methodology of (Phillips and Shi, 2018). Despite its importance (Bitcoin reach \$19,395.83 the December 18$^{th}$, 2017), this peak/burst is insufficiently studied in the literature.

The LPPL model is a bubble detection model that provides the probable critical crash time of the bubble. Our findings show that estimation dates of the crash for Bitcoin and Ether are more accurate than for Ripple and Litecoin. These last two cryptocurrencies do not seem to exhibit a bubble behavior at the end of 2017, price variation seem to be a reaction to Bitcoin and Ether. Such correlation between cryptocurrencies regarding their prices dynamics seems to highlight a contagion on the cryptocurrency market. We add a robustness test using the DCC-GARCH model. We find that dynamic correlation coefficients decrease during the period of the crash (end of 2017) with Bitcoin. Furthermore, the capitalization estimation model of (Wheatley et al., 2019) is confirmed, the expected capitalization based on the user factor and the capitalization have the same dynamics.

The third study contributes to cryptocurrency literature by examining multiple bubbles in the cryptocurrency market for four cryptocurrencies as well as the major peak/burst in the end of 2017. The other main contribution lies in the analysis of a contagion phenomenon within the cryptocurrency market.

## 5.2 Limits and further research

The first study is a conceptual approach of the blockchain technology phenomenon without in-depth empirical evidence to support our results. Questionnaires and interviews with experts or companies that have implemented blockchains could also confirm our anlaysis. Further research may deal with more precise applications related to organizations. More precisely, the study of new ways of raising funds using cryptocurrencies and blockchains could be interesting for future research in corporate finance. Initial Coin Offering (ICO)[1] could make the bridge between the managerial approach of the first study and the financial approach of the second study. ICOs can be considered as a way of raising funds for new projects in the blockchain community and provide some financial support for funding innovations.

The number of ICOs is increasing in recent years as well as the creation of STOs and IEOs (see chapter 1). The corresponding data are numerous and scattered in different databases accessible online. The objective of such future research may be twofold. The first work will to provide a general database of ICOs and IEOs by merging, organizing and completing the data from different existing databases (this work is ongoing process) with financial information on the project itself as well as human resources information on the team's project. Second, the research will study such ICO-related projects in order to predict their success based on available financial information but also on the team's characteristics.

In the second study, market sentiment variables, used in the section dedicated to robustness, could be extended by two additional proxies. The first one is the closed-end funds, which are widely used in the international market sentiment research. The second one is the fear and greed index, which take into

[1] As well Security Token Offering (STO)s and Initial Exchange Offering (IEO)s, see chapter 1 and the list of terms and abbreviations.

account different proxies for market sentiments (market momentum, put and call, safe haven demand, stock price breadth and strength, volatility and junk bond demand). The study could also be extended to cryptocurrencies in addition to Bitcoin, especially for comparisons of financial performance measures. Finally, the theoretical part about the real nature of Bitcoin could be reinforced by taking into account the recent regulations set up in different countries[2].

Finally, the third study meets some limits. First, some additional robustness tests could be applied to confirm our LPPL results: (1) Sensitivity tests such as the CLIPS graphical tool (Geraskin and Fantazzini, 2013) and the Lomb spectral method (which provides the same results as the Fourier spectral analysis but adapted to irregular samples) (Jiang et al., 2010); (2) Diagnostic tests related to stationary issues using a mean-reverting Ornstein-Uhlenbeck process (Lin and Sornette, 2009). A future improvement will be to apply the LPPL model using returns instead of prices in order to avoid the problem of prices nonstationarity (Feigenbaum, 2001) (Sornette and Johansen, 2001), (Chang et al., 2016), (Lin et al., 2009), (Lin et al., 2014). Second, the contagion analysis between cryptocurrencies was studied only briefly. It would be interesting to use other tests (Forbes and Rigobon, 2002) and to consider the contagion in "normal" situations versus in "bubble" situations following (Kohn and Pereira, 2017). Third, we observe a new price increase in the cryptocurrency market that could be interesting to study with additional models that would take in consideration information asymmetries, risk aversion and external political news. Fourth, a theoretical future research in this sense could contribute on the recent research about the fundamental value of cryptocurrencies. Finally, we argue that cryptocurrencies are similar to common stock but perhaps we are witnessing the emergence of a new class of assets that requires in any case some innovative market indexes to highlight the market trend (for example CRIX (Trimborn and Hardle, 2016), CRYPTO20 (Schwartzkopff et al., 2017) and the Bloomberg Galaxy Crypto In-

[2]A study on the cryptocurrency market reactions to regulatory-based cryptocurrency events is underway. Using thirty cryptocurrencies and about fifteen events, we are applying a short and long run event study. The short-term event study is based on the methodology of (Armstrong et al., 2010). First, we provide an overall impact of regulatory (positive or negative) events on the cryptocurrency market. Second, we specify the amplitude of the impact according to several characteristics (related to market microstructure, notably informational efficiency measures as well as cryptocurrency particularities). The long-term impact will compare performance measures over several years (the model is still under definition).

dex (Bloomberg, 2019))[3].

Cryptocurrencies represent an amazing innovation that generates in turn new innovations related to blockchain technology, the cryptocurrencies themselves, financial tools such as indices or new fundraising methods. In some ways, cryptocurrencies are a challenge for the informational efficiency in the traditional financial markets and inside existing organizations. They create a new way to exchange information using a distributed and more transparent system that accompanies the digitisation and globalisation of the economy.

## References


Armstrong, C., Barth, M., Jagolinzer, A. and Riedl, E. (2010). Market reaction to the adoption of IFRS in Europe, *The Accounting Review* **85**(1): 31–61.

Baur, D. G., Hong, K. and Lee, A. D. (2016). Virtual currencies: Media of exchange or speculative asset?, *SWIF Institute Working Paper* (2014-007).

Bloomberg (2019). Index methodology: Bloomberg Galaxy Crypto Index, Index Methodology.
**URL:** `https://data.bloomberglp.com/indices/sites/2/2018/05/BGCI-Methodolgy.pdf`

Chang, V., Newman, R., Walters, R. and Wills, G. (2016). Review of economic bubbles, *International Journal of Information Management* **36**(4): 497–506.

Feigenbaum, J. A. (2001). A statistical analysis of log-periodic precursors to financial crashes, *Quantitative Finance* **1**(3): 346–360.

Forbes, K. J. and Rigobon, R. (2002). No contagion, only interdependance: Measuring stock market comovements, *The Journal of Finance* **57**(5): 2223–2261.

Geraskin, P. and Fantazzini, D. (2013). Everything you always wanted to know about log periodic power laws for bubble modelling but were afraid to ask, *European Journal of Finance* **19**(5).


[3]An ongoing project is to create a smart index balancing cryptocurrencies and gold.

Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. C. and Siering, M. (2014). Bitcoin - Asset or Currency? Revealing users' hidden intentions, *Twenty Second European Conference on Information Systems*.

Jiang, Z.-Q., Zhou, W.-X., Sornette, D., Woodardb, R., Bastiaensen, K. and Cauwels, P. (2010). Bubble diagnosis and prediction of the 2005-2007 and 2008-2009 Chinese stock market bubbles, *Journal of Economic Behavior & Organization* **74**(3): 149–162.

Kohn, M.-B. H. and Pereira, P. L. V. (2017). Speculative bubbles and contagion: Analysis of volatility's clusters during the DotCom bubble based on the dynamic conditional correlation model, *Cogent Economics & Finance* **5**: 1–28.

Lin, L., Ren, R. E. and Sornette, D. (2009). A consistent model of 'explosive' financial bubbles with mean-reversing residuals, *International Review of Financial Analysis* **33**: 210–225.

Lin, L., Ren, R. and Sornette, D. (2014). The volatility-confined LPPL model: A consistent of "explosive" financial bubbles with mean-reverting residuals, *International Review of Financial Analysis* **33**: 210–225.

Lin, L. and Sornette, D. (2009). Diagnostics of rational expectation financial bubbles with stochastic mean-reverting termination times, *European Journal of Finance* **19**(5).

Phillips, P. and Shi, S. (2018). Real time monitoring of asset markets: Bubbles and crises, *Cowles Foundation Discussion Paper* (2152).

Schwartzkopff, D., Schwartzkopff, L., Botha, R., Finlayson, M. and Cronje, F. (2017). CRYPTO20: The first tokenized cryptocurrency index fund, *White Paper* .

Sornette, D. and Johansen, A. (2001). Significance of log-periodic precursors to financial crashes, *Quantitative Finance* **1**(4): 452–471.

Trimborn, S. and Hardle, W. K. (2016). CRIX an index for blockchain based currencies, *Discussion Paper* **021**.

Wheatley, S., Sornette, D., Huber, T., Reppen, M. and Gantner, R. (2019). Are bitcoin bubbles predictable? Combining a generalized Metcalfe's Law and the log-periodic power law singularity model, *Royal Society Open Science* **6**.

Yermack, D. (2015). Is bitcoin a real currency? An economic appraisal, *in* D. L. K. Cheun (ed.), *Handbook of Digital Currency Bitcoin, Innovation, Financial Instruments, and Big Data*, chapter 2, pp. 31–43.

**Chapter 6**

# Résumé en français

Les cryptomonnaies sont une innovation récente qui alimente de nombreux travaux de recherches. Différentes tentatives visant à créer des moyens d'échanges électroniques sont apparues depuis les années 1990 comme "ecash", basée sur les signatures électroniques (Chaum, 1983), (Chaum, 1990), "B-money" à l'origine de la preuve de travail de (Dai, 1999), "Ripplepay", le précurseur du Ripple créé par Ryan Fugger 2004, ou encore "Bit Gold" (Szabo, 2005), un projet très similaire à celui du Bitcoin. Ces tentatives sont pour la plupart restées des projets ou ont échoué sans jamais atteindre le succès du Bitcoin. Celui-ci se démarque de ses prédécesseurs car il réussit à résoudre le problème de la double-dépense sans la nécessité d'impliquer un tiers de confiance dans la vérification des échanges.

En 2008, après la crise des *subprimes*, le système monétaire et financier traditionnel est fragilisé. La confiance dans les institutions et plus généralement dans le système monétaire est remise en cause. C'est la raison pour laquelle Satoshi Nakamoto crée la première cryptomonnaie, le Bitcoin ("bit" pour l'unité monétaire informatique et "coin" pour pièce de monnaie). Une cryptomonnaie est définie par la Banque des règlements internationaux comme étant électronique, pair-à-pair, universellement accessible et non émise par une banque centrale. L'idée principale de Satoshi Nakamoto est de créer un système de paiement international qui fonctionne sans tiers de confiance institutionnel comme les banques centrales, les banques commerciales, les institutions financières ou les gouvernements. Le tiers de confiance est remplacé par la technologie Blockchain, définie comme étant "une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle"[1]. Cette technologie peut être représentée comme un grand livre de comptes public, anonyme et infalsifiable qui contient l'historique complet des transactions (depuis sa création à son état actuel). La sécurité et la viabilité de la blockchain sont assurées par tous les participants qui forment un consensus.

Les faibles coûts d'échange et de transaction par rapport aux systèmes monétaires traditionnels, la protection de la vie privée des investisseurs ainsi que l'aspect publique, accessible, fiable et inviolable des transactions, confèrent au Bitcoin le potentiel d'attirer de nombreux utilisateurs et investisseurs. Le succès du Bitcoin permet de développer cette innovation. Premièrement, la technologie de la blockchain peut être développée à différentes applications autres qu'un système de moyen de paiement. Ses aspects techniques lui permettent d'être mise en place dans des secteurs où il est nécessaire de stocker, transférer et échanger des données par l'intermédiaire d'un tiers, tels que le secteur financier, les assurances, les objets connectés ou encore les chaînons de la chaîne logistique. Deuxièmement, le marché des cryptomonnaies s'est considérablement développé ces dernières années avec la création de nombreuses autres cryptomonnaies à la suite du Bitcoin. Certaines sont consacrées à l'aide humanitaire (Foldingcoin (Ross et al., 2018)), au micropaiement (ReddCoin), à la protection de l'anonymat (Monero et Dash (Duffield and Diaz, 2018)), à des opérations financières (Ripple (Schwartz et al., 2015)), ou encore à des utilisations purement commerciales (NEM (Nem, 2018)). Les entreprises peuvent également chercher à créer leur propre cryptomonnaie dans un objectif de fidélisation de la clientèle (Whoppercoin of Burger King) ou d'amélioration des échanges (Facebook's Libra (Amsden et al., 2018), (Libra, 2019)). La majorité des innovations sont des améliorations du Bitcoin. Ethereum est une plateforme de blockchain qui permet d'exécuter des contrats automatisés que l'on appelle les *smart contracts* et des applications décentralisées. L'Ether est la cryptomonnaie utilisée comme moyen de paiement pour le service de plateforme d'Ethereum (Buterin, 2015). Si le Bitcoin est parfois défini comme de "l'or numérique", le Litecoin est la version en "argent" notamment parce qu'elle vise à faciliter les petites transactions de manière rapide. De plus, le nombre maximal d'unités est fixé à 21 millions pour le Bitcoin, à 84 millions pour le Litecoin et il est pratiquement infini pour l'Ether. Dans la même veine, le temps entre les transactions est de

[1] D'après la définition de Blockchain France.

10 minutes pour le Bitcoin, de 2,5 minutes pour le Litecoin, et de seulement quelques secondes pour les cryptomonnaies Dash et Ripple. Plus récemment, des jetons (tokens) adossés aux cryptomonnaies ont été lancés dans l'objectif de lever des fonds pour des projets au travers des opérations d'*Initial Coin Offering* (ICO). Une ICO est une méthode de levée de fonds par laquelle des jetons sont émis et adossés à des cryptomonnaies lors du lancement d'un projet et pour une courte période de temps. Dans cette thèse, nous concentrerons notre analyse principalement sur la technologie de la blockchain et les cryptomonnaies.

Le succès des cryptomonnaies est tel que leur nombre s'élève quasiment à 2 500 en août 2019 (soit 11 ans après la création du Bitcoin) après être resté stable autour de 500 dans les années 2016. Le nombre de cryptomonnaies n'est pas le seul indicateur de l'évolution considérable et rapide du marché des cryptomonnaies. Leur capitalisation boursière totale a bondi de 19 700 % entre janvier 2013 (1,6 milliard de dollars américains) et juillet 2019 (317 milliards de dollars), atteignant même le montant de 830 milliards de dollars au 7 janvier 2018. En moyenne annuelle, la capitalisation boursière a ainsi augmenté de 141 %. Le marché est largement dominé par Bitcoin dont le cours est aussi un bon indicateur pour démontrer l'attractivité de cette cryptomonnaie. Toutes choses étant égales par ailleurs, le cours est basé sur l'équilibre entre l'offre et la demande, ce qui implique qu'un prix plus élevé est dû à une demande plus élevée. Le prix du Bitcoin est très volatile et impressionnant avec un profil de rentabilité-risque annuel très particulier : 269 % de rentabilité pour 116 % de volatilité depuis sa création jusqu'à la mi-juillet 2019. Les autres cryptomonnaies suivent les mêmes tendances que le Bitcoin mais à une plus petite échelle.

Les cryptomonnaies sont un sujet de recherche multidisciplinaire. Le premier et principal domaine qui s'intéresse à ce sujet est celui des sciences et technologies, avec 556 publications (38 %) sur la période 2013-2018 en informatique, 308 (21 %) en ingénierie et 181 (12 %) en télécommunications. Les sciences économiques et de gestion ne représentent que 8 % (114 publications) de l'échantillon total des publications entre 2013 et 2018. En incluant les années 2012 et 2019, cette proportion augmente à 18 % (279 publications) (Merediz-Sola and Bariviera, 2019). Les études bibliométriques montrent l'expansion croissante de la recherche sur les cryptomonnaies et la blockchain (Dabbagh et al., 2019), (Merediz-Sola and Bariviera, 2019). Depuis le début de cette thèse (2016), le nombre de publications, toutes disciplines confondues, a augmenté de façon spectaculaire. Par exemple, sur la base de la collection de *Web of Science Core Collection*[2], Dabbagh et al. (2019) trouvent 176 publications liées au Bitcoin en 2016 et 262 en 2018 tandis que Merediz-Sola and Bariviera (2019) trouvent 192 publications sur le Bitcoin en 2016 et 384 en 2018. Les recherches sur d'autres mots-clés tels que blockchain, cryptocurrency, ethereum ou *smart contracts* montrent la même tendance à la hausse (Dabbagh et al., 2019).

Ce sujet est pertinent pour les domaines de l'économie et de la gestion parce que les cryptomonnaies et leur technologie (la blockchain) posent des problèmes importants concernant la diffusion de l'information entre les parties prenantes au sein des entreprises. De plus, ils offrent un moyen supplémentaire de créer de la valeur pour les investisseurs par le biais d'investissements dans les cryptomonnaies et de l'adoption d'une blockchain pour les entreprises.

Devant la nouveauté de ce sujet, la pertinence du sujet de recherche de cette thèse dépend de la dynamique des cryptomonnaies et de ses projets innovants liés à la blockchain. Les sciences sociales ont commencé à étudier ce nouveau phénomène, notamment avec des études en économie et en gestion. Le sujet est divisé en deux grandes revues de littérature, l'une portant sur la technologie de la blockchain et l'autre sur les cryptomonnaies.

La littérature sur la technologie de la blockchain considère celle-ci comme une innovation disruptive, source d'une évolution considérable dans le domaine de la gestion. En effet, la blockchain a été elle aussi un sujet d'intérêt ces dernières années avec 483 publications entre 2013 et 2018 (Dabbagh et al., 2019). La littérature souligne ce potentiel d'innovation dans le secteur financier ainsi que dans d'autres secteurs (Lamberti et al., 2017), et de façon plus générale, pour les organisations (chapitre 2). Certains auteurs tentent de modéliser le système de la blockchain en utilisant la théorie des jeux (Biais et al., 2017), (Shermin, 2017). En effet, la blockchain représente un défi pour les organisations existantes avec un impact potentiel sur les différents coûts ainsi que sur la conception des contrats, tels que (1) les coûts de transaction (MacDonnell, 2014), (Larios-Hernandez, 2017), (Kim, 2017), (Pietrewicz, 2018) ; (2) les frais d'agence (Collomb and Sok, 2016), (Tapscott and Tapscott, 2017) ; (3) le car-

[2]Un service d'indexation de citations appartenant à Clarivate Analytics.

actère incomplet des contrats par la mise en œuvre des *smart contracts* (Szabo, 1997), (Cong and He, 2017), (Catalini and Gans, 2018).

Au sein de la littérature sur les cryptomonnaies, les économistes ont été les premiers dans le domaine des sciences sociales à étudier ce phénomène. En effet, le Bitcoin, considéré bien souvent comme une monnaie, offre une nouvelle façon d'échanger et d'acheter des produits et services. Par conséquent, les premières études se concentrent sur sa nature monétaire ainsi que ses propriétés (Grant, 2014), (Kancs et al., 2015), (Lakosmki-Laguerre and Desmedt, 2015), (Baur et al., 2016), (Figuet, 2016). Dans un second temps, s'agissant du profil rentabilité-risque particulier des cryptomonnaies et plus précisément du Bitcoin, la recherche en finance a été initiée en testant ses performances avec des mesures simples (Brière et al., 2015), (Burniske and White, 2017). La création de fonds communs de placement (e.g. Bitcoin Investment Trust et ARK Investment Management en 2015), de fonds spéculatifs (e.g. Pantera Capital en 2013), ainsi que la décision de l'Agence du gouvernement fédéral des États-Unis qui collecte l'impôt sur le revenu et des taxes diverses (Internal Revenue Service, IRS) de déterminer les cryptomonnaies comme un actif, soutiennent un intérêt financier de considérer le Bitcoin comme un investissement.

L'une des contributions de cette thèse est de donner un argument sur la nature des cryptomonnaies et de donner un aperçu de leur performance financière avec des modèles pertinents fondés sur le Modèle d'Evaluation des Actifs Financiers (MEDAF) et le modèle de Fama-French à trois facteurs (Fama and French, 1992), pas encore considérés dans la littérature à notre connaissance (chapitre 3, cet article a été publié dans *Journal of Risk Finance*).

La poursuite de l'analyse du marché des cryptomonnaies, qui connaît une très forte volatilité, conduit à considérer leur efficience (Urquhart, 2017), (Nadarajah and Chu, 2017) et plus précisément leur aspect spéculatif. Les recherches actuelles se concentrent sur les périodes de bulles potentielles indépendamment les unes des autres, par exemple en étudiant la fin de l'année 2013 lorsque le prix du Bitcoin a atteint pour la première fois 1 000$ (MacDonnell, 2014), (Cheah and Fry, 2015), (Fry and Cheah, 2016) et beaucoup moins la fin de l'année 2017 lorsque le prix du Bitcoin dépassait 19 000$ (Corbet et al., 2017), (Fry, 2018), (Chaim and Laurini, 2019), (Wheatley et al., 2019). Les premières analyses complètes sur la détection de bulles sur une longue période et concernant plusieurs cryptomonnaies (pas seulement le Bitcoin) sont très récentes (Hafner, 2018), (Su et al., 2018), (Bouri et al., 2019), (Li et al., 2019), (Vogiazas and Alexiou, 2019), (Wheatley et al., 2019). En utilisant deux modèles de détection différents adaptés de (Phillips and Shi, 2018) et de (Johansen et al., 2000), nous effectuons une recherche globale de détection de bulles multiples avec un focus sur le pic de 2017 pour différentes cryptomonnaies, mettant ainsi en évidence certains effets de corrélation et même de contagion sur le marché des cryptomonnaies (Chapitre 4).

La nouveauté, l'attractivité, le faible coût des transactions ainsi que l'énorme volatilité des prix sur le marché des cryptomonnaies soulèvent la question de l'efficience de ce marché. L'efficience du marché représente "un marché dans lequel les prix reflètent toujours pleinement l'information disponible" (Fama, 1970). Fama explique dans ce célèbre article que le marché est imbattable s'il est efficient ("hypothèse des marchés efficients", HME). Cette théorie repose sur plusieurs hypothèses : (1) les investisseurs sont rationnels ; (2) l'information doit être librement disponible (elle n'est pas coûteuse et son accès est possible et facile pour tous), ce qui permet aux investisseurs de l'analyser instantanément ; (3) il n'y a ni frais de transaction ni taxes ; (4) le marché est liquide et aucun investisseur ne peut influencer le prix en vendant ou en achetant un nombre important de titres. L'information est un élément clé de l'HME parce que les prix doivent être réactifs à l'information. Cependant, il existe différents types d'informations, tels que l'information passée, présente, publique et privée, ce qui implique différents niveaux d'efficience. Une forte efficience signifie que personne ne peut battre le marché, que l'information soit passée, présente, publique ou privée. Un initié qui prend une décision financière sur la base de ses propres informations privées envoie un signal révélateur au marché car les transactions sont transparentes pour les autres investisseurs. Dans l'efficience semi-forte, l'information privée permettrait de battre le marché, alors que l'information publique est directement intégrée par les prix. Dans la forme faible d'efficience, on ne peut pas battre le marché en utilisant l'information passée, seules l'information privée et publique permettent de le battre.

Dans la pratique, il existe des frictions telles que les asymétries d'information et les coûts de transaction qui réduisent l'efficience du marché. Le marché des cryptomonnaies semble moins affecté par de telles frictions. En effet, la technologie de la blockchain permet de réduire les coûts de transaction et d'améliorer la transparence et l'accessibilité de l'information pour les agents économiques, tels que les parties prenantes d'une entreprise si le processus est appliqué aux entreprises ou aux investisseurs sur le marché des cryptomonnaies. La blockchain ainsi que les investissements sur le marché des cryptomonnaies créent de la valeur en réduisant les frictions liées à l'information.

Pour être davantage efficient, un marché doit respecter quatre caractéristiques : (1) une disponibilité de l'information ; (2) un grand nombre d'investisseurs capables d'analyser l'information ; (3) une protection juridique des investisseurs ; (4) un marché secondaire liquide avec des coûts de transaction faibles (D'avolio et al., 2002). Ces auteurs étudient l'impact des nouvelles technologies sur l'efficience des marchés des actions et constatent que les technologies permettent de démocratiser ce marché en augmentant le nombre d'investisseurs et en réduisant les coûts de transaction (tels que les coûts de collecte et d'exécution des transactions). Lee et al. (2017) étudient la relation entre les technologies de l'information et de la communication (TIC) et la capitalisation boursière, et trouvent une relation positive entre les deux. Les TIC améliorent l'efficience sur le marché des actions (Abadi et al., 2013) ainsi que sur le marché immobilier (Kummerow and Lun, 2005) en raison de leur impact à long terme sur les organisations.

### Questions de recherche

Par conséquent, les problèmes de recherche abordés par cette thèse sont centrés autour de la notion d'efficience du marché des cryptomonnaies, en considérant que la technologie sous-jacente, la blockchain, joue un rôle central dans ce sens.

Premièrement, notre analyse se concentre sur la blockchain en considérant les cryptomonnaies comme une application importante de cette technologie. Les cryptomonnaies reposent principalement sur les informations qui sont stockées et transférées grâce à la blockchain. La blockchain permet de réduire les frictions telles que les asymétries d'information grâce à sa transparence et sa décentralisation entre tous les participants au processus. Elle permet également de réduire les coûts de transaction grâce à la rapidité et à la simplicité du processus de validation par rapport aux services existants. En effet, ces services nécessitent la présence d'un tiers, mais aussi du temps, des efforts et de l'argent pour exécuter correctement les transactions. L'efficience informationnelle liée à la blockchain peut s'expliquer par l'arbitrage entre les coûts d'acquisition de l'information et les performances générées par cette technologie grâce aux avantages informationnels. Pour les analyser, nous retenons un cadre théorique lié aux perspectives contractuelles de la théorie des organisations (coûts de transaction, problèmes d'agence et préoccupations liées aux droits de propriété). La blockchain peut être considérée comme un outil de gestion flexible pour les entreprises existantes et futures, visant à améliorer leurs services dans plusieurs secteurs pour lesquels l'information doit être stockée et échangée. Par conséquent, dans cette première étude, nous nous interrogeons sur *le potentiel général (forces et faiblesses) de la technologie de la blockchain en termes d'efficience informationnelle et comment la blockchain développée au sein d'une communauté informelle peut être adoptée par les organisations, améliorant ainsi leur efficience*. Le cas des cryptomonnaies est au centre de notre analyse.

Avant de commencer à analyser le marché des cryptomonnaies lui-même, il est nécessaire de comprendre *quelle est la véritable nature des cryptomonnaies en termes financiers*. Sont-elles des "monnaies" comme leur nom l'indique ? Ou bien s'agit-il plutôt d'une sorte de "réserve de valeur", souvent décrite comme de l'or numérique ? Sont-elles semblables à des actifs financiers comme les actions ? Après une discussion sur la nature des cryptomonnaies, nous fondons notre analyse sur l'hypothèse que les cryptomonnaies représentent des actifs financiers et plus précisément qu'elles peuvent être assimilées aux actions. Les arguments à l'appui de cette hypothèse sont développés dans notre thèse. Après avoir analysé la nature du Bitcoin, nous *analysons la performance financière des cryptomonnaies* (la rentabilité ajustée au risque), et plus précisément celle du Bitcoin en utilisant une large base de données. Notre objectif est de déterminer si le Bitcoin sur-performe ou sous-performe par rapport au marché des actions. Le cadre théorique utilisé pour tester la performance financière en supposant l'hypothèse de l'efficience du marché sont les modèles du MEDAF et de Fama-French à trois facteurs (Fama and French, 1992). Si le marché est pleinement efficient, alors le prix intègre toute l'information et il n'y a donc aucune possibilité de battre le marché et de gagner de l'argent en investissant dans des actifs spécifiques, tels que le Bitcoin. La constatation d'une performance financière positive et persistante pour le Bitcoin nous amène naturellement à nous demander s'il ne s'agit pas d'une bulle spéculative. Cette hypothèse est soutenue par l'importante volatilité du Bitcoin.

La troisième grande analyse porte donc sur *l'aspect de bulle spéculative des cryptomonnaies*. Pour ce faire, nous choisissons des modèles théoriques de détection de bulles qui ne nécessitent pas de déterminer leur valeur fondamentale, comme le modèle de détection de bulles multiples de (Phillips et Shi ; 2018) ainsi que le modèle de détection et prévision de bulle unique de (Johansen et al. ; 2000a). Nous appliquons ces modèles pour plusieurs cryptomonnaies qui sont corrélées entre elles, ce qui implique que l'effet de contagion doit être également testé. En effet, la contagion est influencée par le niveau d'asymétrie d'information sur le marché (Kodres and Pritsker, 2002).

Plus précisément, notre recherche s'appuie sur trois études présentées dans cette thèse de doctorat. Premièrement, au niveau macro, nous nous concentrons sur l'innovation de la technologie de la blockchain et son potentiel d'amélioration de l'efficience pour les organisations et les entreprises. Deuxièmement, nous étudions le marché des cryptomonnaies en soulevant la question de leur nature dans une perspective financière et en testant leurs rentabilités ajustées au risque. Troisièmement, nous étudions les aspects spéculatifs des bulles et la contagion/corrélation entre les cryptomonnaies à l'intérieur de ce marché. Ces trois études sont brièvement décrites ci-dessous.

### Première étude

L'innovation technologique de la blockchain a d'abord été créée pour le développement des cryptomonnaies au sein d'une communauté informelle spéciale. L'idée était de créer un nouvel écosystème indépendant des institutions financières existantes et des entreprises formelles. Dans cet écosystème collaboratif, les individus échangent entre eux directement par le biais de la technologie blockchain. Rapidement, cette technologie démontre son potentiel et ses avantages au sein-même des organisations formelles existantes pour améliorer les transferts d'information (transparence accrue, moins d'intermédiaires) et créer de la valeur. Par conséquent, la première étude de la thèse vise à expliquer comment la blockchain développée au sein des communautés informelles a le potentiel d'être adoptée dans les organisations.

Tout d'abord, nous fournissons un cadre théorique pour la technologie de la blockchain centré sur la théorie des organisations. Le raisonnement se fonde sur l'approche contractuelle (théories des coûts de transaction, de l'agence, des contrats incomplets et des droits de propriété), ainsi que sur l'approche cognitive basée sur les capacités (théories comportementale, des ressources et évolutionniste). Les caractéristiques uniques de la blockchain (transparence, décentralisation, mécanisme de consensus, sécurité cryptographique, contrats intelligents) alimentent certains concepts liés à ces théories et impliquent également de nouveaux enjeux pour la recherche universitaire. La blockchain traite fondamentalement de l'information parce qu'il s'agit d'un outil de stockage et d'échange de données, plus transparent et distribué, ce qui implique plusieurs améliorations en termes d'efficience informationnelle. La blockchain a le potentiel d'augmenter l'accès à l'information pour les participants (en particulier les utilisateurs), de diminuer les coûts de transaction et d'agence grâce à sa transparence, sa rapidité et sa simplicité, et le tout de façon plus sécuritaire. Les comportements opportunistes sont donc davantage contrôlables par la blockchain grâce à la mise en œuvre de *smart contracts* qui prennent en compte autant de situations futures que possible. En pratique, le processus de validation des transactions est réparti entre les participants (mineurs) par le biais d'un mécanisme de consensus. Ce processus s'inscrit dans la perspective de la théorie des parties prenantes. En effet, toutes les parties prenantes sont impliquées dans l'écosystème sur la base d'une technologie qui fonctionne selon des principes cryptographiques. Cependant, la blockchain est aussi source d'autres problèmes (tels que les risques opérationnels ou les questions éthiques) qui présentent un subtil compromis à prendre en considération, en équilibrant ses forces et ses faiblesses.

Par exemple, le mécanisme de consensus conçu pour sécuriser les transactions présente le potentiel de contrôler les comportements opportunistes potentiels et de diminuer les problèmes d'aléa moral. Cependant, les deux principaux mécanismes de consensus peuvent être soit consommateurs d'énergie (Preuve de travail), soit entraîner certains effets d'inertie sociale (Preuve d'enjeu). Dans l'approche contractuelle de la théorie des organisations, la mise en place des *smart contracts* adossés aux blockchain permet de résoudre les problèmes de comportement opportunistes et de gérer l'incertitude. Ces contrats réduisent les coûts de vérification parce que le système est automatisé. Par conséquent, la plupart des défis sont post-contractuels et augmentent les coûts de négociation. Les *smart contracts* s'efforcent de prendre en considération autant de situations que possible, réduisant ainsi des opportunités inattendues mais qui auraient pu créer de nouvelles occasions d'affaires.

L'intervention humaine est nécessaire pour construire ces contrats afin de réduire l'apparition de problèmes techniques. De tels problèmes peuvent également apparaître parce que tout le système est basé sur des principes cryptographiques qui ne sont pas à l'abri d'éventuels bugs, attaques ou évolutions technologiques impliquant des pertes financières potentielles. Le coût d'entrée est donc élevé mais permet de diminuer la complexité (moins d'intermédiaires et plus d'échanges directs), et donc les coûts d'agence. La caractéristique de transparence augmente l'accès à l'information et, par conséquent, réduit les coûts de transaction. La décentralisation des pouvoirs par le biais du réseau accroît la participation de chaque partie prenante au sein de l'organisation et augmente le potentiel de bien-être social. Transparence et décentralisation sont parfois controversées pour les entreprises en ce qui concerne les données sensibles et confidentielles. Pour cette raison, l'accès des utilisateurs (transparence) et les droits des mineurs (décentralisation du pouvoir) varient en fonction des projets mis en place par l'entreprise.

Pour cette raison, la deuxième partie de l'étude propose une analyse bidimensionnelle des caractéristiques de la blockchain et de son évolution en mettant l'accent sur la communauté, par le biais d'une analyse illustrée. Nous concentrons notre recherche sur deux participants principaux dans la blockchain : (1) *les utilisateurs* qui peuvent lire le registre et échanger des informations (une pièce de monnaie, dans le cas du Bitcoin) grâce à la dimension d'*ouverture* ; (2) *les mineurs* qui participent au mécanisme de consensus pour valider les transactions grâce à la dimension de *permission*. Les droits d'accès respectifs de ces deux types de participants à la blockchain peuvent évoluer en fonction de son utilisation dans un nouveau projet organisationnel et des objectifs de ce projet (par exemple, un projet avec des données sensibles et confidentielles ne sera pas traité comme un projet public). Nous présentons quatre cas de blockchain possibles basés sur ces deux dimensions (dimension d'*ouverture*

: publique ou privée ; dimension *permission* : avec ou sans permission). Plus précisément, nous soulignons que la tendance de l'évolution des blockchains va des blockchains publiques sans permission (celles des cryptomonnaies) vers des blockchains privées avec permission (industries formelles et par exemple le projet Libra de Facebook). Cette évolution crée l'opportunité de nouvelles institutions et de normes. La blockchain pourrait apparaître comme une véritable institution de gouvernance impliquant plusieurs organisations ensemble. Par exemple, la blockchain Libra de Facebook a le potentiel de rassembler des organisations ayant des objectifs différents tels que les services de paiement, le commerce électronique et l'économie de partage, des entreprises de cryptomonnaies, des fonds d'investissement et des organisations non gouvernementales.

Ce chapitre a des implications théoriques parce qu'il fournit une étude conceptuelle sur le thème de la blockchain dans la recherche en management, particulièrement concernant la théorie des organisations. En effet, nous proposons une approche originale à travers le concept des communautés et une revue de littérature illustrée par plusieurs exemples de projets liés à la blockchain. Les implications managériales sont également une contribution importante, en particulier pour les entreprises qui pourraient, grâce à la technologie blockchain, augmenter la participation de leurs parties prenantes : les managers pourraient renforcer leur leadership, les employés pourraient devenir des membres experts, et les investisseurs pourraient être plus conscients de la réalité et être plus réactifs en temps réel. La blockchain est également source de contributions en matière de politiques publiques puisque notre recherche démontre que la blockchain a le potentiel de changer la façon dont la société est organisée en intégrant les individus au cœur des décisions (en utilisant des réseaux distribués). Cette technologie pourrait contribuer à améliorer l'intégration financière des personnes exclues, à promouvoir le vote électronique et à créer de nouveaux emplois (dans le domaine des technologies de l'information parce que la technologie est basée sur des principes informatiques et cryptographiques, ainsi que dans le domaine juridique car cette nouvelle technologie nécessite de nouvelles règles adaptées pour protéger les individus dans leurs échanges). Un autre enjeu de politiques publiques porte également sur la réglementation de l'utilisation des blockchains. Différentes questions juridiques se posent comme la (non)réversibilité des transactions, les litiges dans l'exécution des *smart contracts*. Dans un monde globalisé, les lois nationales se font concurrence et, dans un monde virtuel, l'absence de réglementation peut entraver le développement de blockchains (cas du controversé Libra de Facebook). La création de nouvelles normes internationales apparaît donc comme une question cruciale.

### Etude 2

La question qui émerge de la première étude est de déterminer la "vraie" nature des cryptomonnaies. Pour cette raison, la deuxième étude a deux objectifs. Le premier est de fournir une réponse claire liée à la nature des cryptomonnaies, permettant ainsi d'utiliser des modèles spécifiques existant dans la littérature en fonction de leur nature. Nous montrons que le Bitcoin partage des similitudes avec les monnaies, avec l'or, et avec les actifs financiers, plus précisément les actions.

La première idée est de comparer le Bitcoin (et par extension les cryptomonnaies) aux monnaies traditionnelles en se basant sur leurs trois propriétés économiques fondamentales, à savoir : intermédiaire des échanges, unité de compte et réserve de valeur. Il ressort de l'analyse que le Bitcoin ne semble pas respecter entièrement ces trois propriétés. Certes, le Bitcoin permet aux individus d'échanger des biens et des services entre eux et semble donc jouer un rôle d'intermédiaire des échanges. Toutefois, les coûts d'entrée empêchent les entreprises de l'accepter comme moyen de paiement, le cadre juridique fait défaut et il n'existe aucune possibilité d'accorder des prêts sur le marché des cryptomonnaies. Le Bitcoin est divisible mais sa volatilité et son offre inélastique ne valident pas les propriétés attendues d'une unité de compte. Enfin, le modèle économique particulier fondé sur la question de l'inflation/déflation (l'offre du Bitcoin est fixe), la forte volatilité des prix et les risques liés à la cybersécurité, réduisent la confiance dans le Bitcoin. De fait, le Bitcoin peut difficilement être considéré comme une réserve de valeur stable.

La deuxième hypothèse compare le Bitcoin à l'or. Les deux actifs sont indépendants des gouvernements et jouent parfois le rôle de valeur de refuge. Tous deux présentent une offre monétaire limitée et une création monétaire basée sur un processus de minage, au sens propre ou figuré. Cependant, la création monétaire du Bitcoin est divisée périodiquement et de manière claire dans son code informatique tandis que l'extraction de l'or n'a pas de règles précises. La valeur du stock mondial d'or est beaucoup plus importante que la capitalisation boursière du Bitcoin et leurs prix sont indépendants les uns des autres. De plus, par rapport à l'or, le Bitcoin n'a pas de compensation physique. Par conséquent, le Bitcoin, et par extension les cryptomonnaies, ne peuvent pas être assimilés à de l'or.

Une autre possibilité analysée dans cette thèse est que le Bitcoin puisse être assimilé à des actifs financiers et plus précisément à des actions. Le profil particulier de rentabilité élevée et de risque élevé du Bitcoin le rend semblable à celui des actions. Le Bitcoin peut être considéré comme étant un investissement dans la technologie blockchain (actif incorporel) et dans le capital humain des experts associés. Cet argument est étayé par des recherches empiriques (Yermack, 2015), (Glaser et al., 2014), (Baur et al., 2016) et par des cadres juridiques avec les définitions aux Etats-Unis de l'Internal Revenue Service (2014) et de la Securities and Exchange Commission (2015). L'IRS considère les cryptomonnaies comme des actifs et la SEC considèrent les jetons basés sur les cryptomonnaies comme étant des valeurs mobilières. Dans la pratique, les fonds communs de placement et les fonds de couverture utilisent les cryptomonnaies comme actifs financiers, par exemple dans les fonds suivants : Pantera Capital, CoinCapital, PolyChain Capital ou le très récent fonds Liberty Bitcoin Fund. Par conséquent, si le Bitcoin est assimilé à une opportunité d'investissement, il est important d'analyser sa performance.

Dans ce cadre, après avoir fait valoir que les cryptomonnaies ressemblent davantage à des actions qu'à des devises ou à de l'or, le deuxième objectif de cette étude est d'étudier empiriquement la performance du Bitcoin avec des mesures plus pertinentes que celles déjà utilisées dans la littérature. Le ratio de Sharpe est une mesure de rentabilité largement utilisée, mais qui nous apparaît insuffisante. Nous étudions la performance en mesurant la rentabilité ajustée au risque par grandes régions sur la base du MEDAF et du modèle de Fama-French à trois facteurs (Fama and French, 1992) ainsi que d'un modèle élargi ajoutant deux autres facteurs (or et obligations). Nous utilisons les prix quotidiens du Bitcoin de septembre 2010 à décembre 2016 à partir du site web "blockchain.info" ainsi que les facteurs internationaux globaux du site internet officiel des professeurs Eugene Fama et Kenneth French[3], pour les régions du monde, de l'Europe et de

[3]http://mba.tuck.dartmouth.edu/pages/faculty/ken.french/index.html

l'Asie-Pacifique. De plus, nous étendons l'analyse en étudiant la performance en Chine car le marché chinois des cryptomonnaies couvre 90 % des transactions du Bitcoin. Nous construisons nous-mêmes les portefeuilles et les facteurs Fama-French chinois pour la Chine et nous les comparons aux facteurs MSCI Chine (facteur taille et facteur valeur). Les données chinoises (taille et *book-to-market* des entreprises du marché chinois Shenzhen, MSCI China Small Cap - MSCI China Large Cap, MSCI China Value Local - MSCI China Growth Local), le cours de l'or et les indices obligataires de référence proviennent de la base de données Datastream.

Nos résultats montrent que l'intégration du Bitcoin dans un portefeuille améliore sa diversification et procure une rentabilité positivement ajustée au risque et significative quelle que soit la région. Nous constatons que le Bitcoin présente un alpha annualisé fort et très significatif quelle que soit la région (Monde, Europe, Asie-Pacifique).

Nous testons également la robustesse de nos résultats à l'aide de méthodes économétriques qui tiennent compte des problèmes de non normalité des erreurs des régressions (méthode RALS (*residual augmented least squares*) utilisée dans la littérature sur les *hedge funds*). Nous intégrons également des variables relatives au sentiment du marché. Le contrôle de ces questions ne modifie pas qualitativement nos résultats et confirme donc notre analyse.

Les principales contributions de la deuxième étude sont doubles. Premièrement, cette étude propose une discussion claire sur la nature des cryptomonnaies et l'intérêt de les comparer à des actifs financiers tels que les actions. Deuxièmement, elle est la première, à notre connaissance, à fournir des mesures de performance financière solides et académiques basées sur les modèles du MEDAF et de Fama-French à trois facteurs.

**Etude 3**

Les performances élevées du Bitcoin mesurées dans la deuxième étude interrogent sur l'existence d'une bulle spéculative sur le marché des cryptomonnaies. Tout d'abord, la littérature récente tente de modéliser la valeur fondamentale des cryptomonnaies et démontre que celle-ci est différente de zéro, ce qui implique que les cryptomonnaies ne sont pas seulement une bulle. Toutefois, des bulles peuvent exister même si un actif possède une valeur fondamentale car, par définition, les bulles sont caractérisées par des prix qui s'écartent de leur valeur fondamentale. Il est donc très probable que la dynamique du marché des cryptomonnaies comprenne des périodes de bulles apparaissant notamment dans les prix du Bitcoin à la fin des années 2013 et 2017. De plus, les aspects novateurs des cryptomonnaies, notamment leur technologie (la blockchain), pourraient accentuer des mouvements spéculatifs. Une telle réaction liée aux nouveaux produits ou technologies peut expliquer la création et le développement d'une bulle (Chang et al., 2016). De plus, ce phénomène semble être comparable à la bulle Internet du début des années 2000.

L'objectif de la troisième étude est également double. Tout d'abord, nous analysons le marché des cryptomonnaies sur la période allant de 2013 à juillet 2019 en utilisant un modèle récent de détection de bulles multiples (Phillips and Shi, 2018). Ensuite, nous nous concentrons sur le principal pic/éclatement du marché des cryptomonnaies qui s'est produit à la fin de 2017 en utilisant le modèle LPPL (*Log Period Power Model*) de (Johansen et al., 2000). L'étude est appliquée aux quatre principales cryptomonnaies, ce qui inclut le Bitcoin, mais aussi l'Ether, le Ripple et le Litecoin, en utilisant leurs cours de clôture quotidiens en USD provenant des sites internet coindesk et coinmarketcap.

Tout d'abord, nous analysons l'ensemble de la période de temps pour les quatre principales cryptomonnaies (Bitcoin, Ether, Ripple et Litecoin) en utilisant la méthodologie de (Phillips and Shi, 2018) et nous remarquons que le Ripple et le Litecoin obtiennent une détection plus précise des bulles. La deuxième analyse se concentre sur le pic/éclatement à la fin de 2017 qui est : (1) apparent graphiquement ; (2) détecté dans la première étape par la méthodologie de (Phillips and Shi, 2018). Malgré son importance, ce pic/éclatement n'est pas suffisamment étudié dans la littérature. Le modèle LPPL est un modèle de détection de bulles qui estime la date d'éclatement la plus probable de la bulle. Nos résultats montrent que la prévision de la date de crash est plus ajustée pour le Bitcoin et l'Ether que pour le Ripple et le Litecoin. Ces deux dernières cryptomonnaies ne semblent pas former de bulle à la fin de 2017 mais leur cours évolue principalement en réaction au Bitcoin et à l'Ether. Une telle corrélation entre les cryptomonnaies en ce qui concerne leur dynamique de prix semble mettre en évidence une contagion sur leur marché. Nous allons plus loin que les études traditionnelles de détection des bulles, notamment en mettant l'accent sur un fort effet de contagion entre les différentes cryptomonnaies. En particulier, les informations fournies par l'évolution du cours du Bitcoin semblent influencer la dynamique des autres. C'est pourquoi, dans la section robustesse, nous testons la contagion entre ces 4 cryptomonnaies à l'aide du modèle DCC-GARCH (Engle and Sheppard, 2001). Nous constatons que le coefficient de corrélation dynamique diminue à la fin de l'année 2017 avec le Bitcoin. De plus, nous testons l'un des modèles d'estimation de la valeur fondamentale (Wheatley et al., 2019). Nous confirmons ainsi que la capitalisation du Bitcoin et le nombre d'utilisateurs ont la même dynamique.

La troisième étude contribue ainsi à la littérature sur les cryptomonnaies en examinant les bulles multiples sur le marché des cryptomonnaies pour les quatre plus importantes cryptomonnaies ainsi que le pic/éclatement majeur à la fin 2017. Une autre contribution réside dans l'analyse et la mesure d'un phénomène de contagion au sein du marché des cryptomonnaies.

**Limites et future recherches**

La première étude est une approche conceptuelle du phénomène technologique de la blockchain. Des questionnaires et des entrevues avec des experts ou des entreprises qui ont mis en place des blockchains pourraient empiriquement confirmer notre analyse. D'autres recherches pourraient porter sur des applications plus précises liées à la blockchain et aux organisations. Plus précisément, l'étude de nouvelles façons de lever des fonds à l'aide de cryptomonnaies et de la blockchain pourraient être intéressantes pour de futures recherches dans le domaine de la finance d'entreprise. Les méthodes de levées de fonds appelées *Initial Coin Offering* (ICO) pourraient faire le pont entre l'approche managériale de la première étude et l'approche finance de marché de la deuxième étude. Les ICOs peuvent être considérées comme un moyen de recueillir des fonds pour de nouveaux projets dans la communauté de la blockchain et être un soutien pour le financement des innovations. Le nombre d'ICO est en augmentation ces dernières années, ainsi que la création de nouvelles méthodes plus réglementées et régulées comme les *Security Token Offering* (STO)[4] et les *Initial Exchange*

[4]Une STO peut être assimilées à un processus d'introduction en bourse (IPO) mais sur le marché des cryptomonnaies avec des règles légales spécifiques.

*Offering* (IEO)[5]. Les données à leur propos sont nombreuses et dispersées dans différentes bases de données accessibles en ligne. L'objectif de cette future recherche peut être double. Le premier travail consistera à fournir une base de données générale sur les ICO, STO et IEO, en fusionnant, organisant et complétant les données des différentes bases de données existantes (ce travail est en cours) afin de collecter des informations financières sur le projet lui-même ainsi que des informations sur les ressources humaines de l'équipe du projet. Deuxièmement, la recherche étudiera ces projets afin de prédire leur succès à partir des informations financières disponibles, mais aussi à partir des caractéristiques de l'équipe.

Dans la deuxième étude, les variables de confiance du marché, utilisées dans la section consacrée à la robustesse, pourraient être complétées par deux variables supplémentaires. La première considère les fonds d'investissement fermés (*closed-end funds*), qui sont largement utilisés dans le cadre de la recherche sur l'opinion du marché international. Le deuxième est l'indice *Feer and Greed*, qui prend en compte différentes approximations des sentiments du marché (l'effet *momentum*, les options de vente et d'achat (*put* et *call*), la demande de valeurs refuges, l'ampleur et la profondeur (*breadth and strength*) du marché, la volatilité et la demande des obligations "pourries" (*junk bond demand*). L'étude de performance pourrait également être étendue à d'autres cryptomonnaies que le Bitcoin, en particulier pour comparer les résultats des mesures de performance financière entre les différentes cryptomonnaies. Enfin, la partie théorique sur la nature réelle du Bitcoin pourrait être renforcée en tenant compte des réglementations récentes mises en place dans différents pays[6].

---

[5]Une IEO est une méthode de levée de fonds en cryptomonnaies auditées et réalisée par des plateformes d'échanges.

[6]Une étude sur les réactions du marché des cryptomonnaies aux événements de régulation liées à celles-ci est en cours. A partir d'une trentaine de cryptomonnaies et d'une quinzaine d'événements, nous appliquons une étude d'évènements à court et moyen terme. L'étude de l'événement à court terme est basée sur la méthodologie de (Armstrong et al., 2010). Premièrement, nous présentons l'impact global des événements réglementaires (positifs ou négatifs) sur la rentabilité des cryptomonnaies. Deuxièmement, nous spécifions l'amplitude de l'impact en fonction de plusieurs caractéristiques (liées à la microstructure du marché, notamment les mesures d'efficience informationnelle ainsi que des caractéristiques propres aux différentes cryptomonnaies). L'impact à long terme compare la performance entre les cryptomonnaies sur plusieurs années pré- et post- évènements (le modèle utilisé reste encore à définir).

Enfin, la troisième étude présente certaines limites. Tout d'abord, des tests de robustesse supplémentaires pourraient être appliqués pour confirmer nos résultats, notamment pour la méthode LPPL comme : (1) des tests de sensibilité tels que l'outil graphique CLIPS (Geraskin and Fantazzini, 2013) et la méthode spectrale de Lomb (qui fournit les mêmes résultats que l'analyse spectrale de Fourier mais adaptée aux échantillons irréguliers) (Jiang et al., 2010) ; (2) des tests de stationnarité utilisant le processus stochastique de retour à la moyenne de Ornstein-Uhlenbeck (Lin and Sornette, 2009). Une amélioration future consistera à appliquer le modèle LPPL en utilisant les rentabilités plutôt que les prix afin d'éviter le problème de non-stationnarité des prix (Feigenbaum, 2001) (Sornette and Johansen, 2001), (Chang et al., 2016), (Lin et al., 2009), (Lin et al., 2014). Deuxièmement, l'analyse de la contagion entre les cryptomonnaies n'a été étudiée que brièvement. Il serait intéressant d'utiliser d'autres tests (Forbes et Rigobon ; 2002) et de considérer la contagion dans des situations "normales" versus dans des situations de "bulles" (Kohn et Pereira ; 2017). Troisièmement, nous observons une nouvelle hausse des prix sur le marché des cryptomonnaies qu'il pourrait être intéressant d'étudier avec d'autres modèles qui prendraient en considération les asymétries d'information, l'aversion au risque et les événements liés à l'actualité pouvant influencer le marché des cryptomonnaies. Quatrièmement, une recherche théorique future dans ce sens pourrait étudier plus en avant la valeur fondamentale des cryptomonnaies. Enfin, nous soutenons que les cryptomonnaies sont similaires aux actions, mais nous assistons peut-être à la création d'une nouvelle classe d'actifs qui nécessite en tout état de cause des indices de marché innovants pour mettre en évidence la tendance du marché (par exemple le CRIX (Trimborn and Hardle, 2016), CRYPTO20 (Schwartzkopff et al., 2017) et l'indice de Bloomberg Galaxy Crypto (Bloomberg, 2019))[7].

Pour conclure, les cryptomonnaies et la blockchain sous-jacente représentent des innovations financières singulières, porteuses d'un fort potentiel de rentabilité tout en étant associées à des risques conséquents. Leur adoption à plus grande échelle par les organisations et les entreprises permet de développer des cryptomonnaies elles-mêmes, ainsi que des outils financiers comme les indices ou de nouvelles méthodes de collecte de fonds. Par leurs caractéristiques et

[7]Un projet en cours est la création d'un smart index entre les cryptomonnaies et l'or avec l'Imperial College London.

leur fonctionnement, les cryptomonnaies représentent un défi pour l'efficience informationnelle sur les marchés financiers traditionnels et, au-delà, au sein des organisations existantes. Elles créent une nouvelle façon d'échanger des informations plus distribuée et transparente qui accompagne la numérisation et la mondialisation de l'économie.

## References


Abadi, H. R. D., Faghani, F. and Tabatabaee, S. M. (2013). Impact of information technology development on stock marketdevelopment.empirical study in the world's leading capital markets, *International Journal of Academic Research in Accounting, Finance and Management Sciences* **3**(1): 382–390.

Amsden, Z., Arora, R., Bano, S., Baudet, M., Blackshear, S., Bothra, A., Cabrera, G., Catalini, C., Chalkias, K., Cheng, E., Ching, A., Chursin, A., Danezis, G., Giacomo, G. D., Dill, D. L., Ding, H., Doudchenko, N., Gao, V., Gao, Z., Garillot, F., Gorven, M., Hayes, P., Hou, J. M., Hu, Y., Hurley, K., Lewi, K., Li, C., Li, Z., Malkhi, D., Margulis, S., Maurer, B., Mohassel, P., de Naurois, L., Nikolaenko, V., Nowacki, T., Orlov, O., Perelman, D., Pott, A., Proctor, B., Qadeer, S., Rain, Russi, D., Schwab, B., Sezer, S., Sonnino, A., Venter, H., Wei, L., Wernerfelt, N., Williams, B., Wu, Q., Yan, X., Zakian, T. and Zhou, R. (2018). The libra blockchain, *White paper* .

Armstrong, C., Barth, M., Jagolinzer, A. and Riedl, E. (2010). Market reaction to the adoption of IFRS in Europe, *The Accounting Review* **85**(1): 31–61.

Baur, D. G., Hong, K. and Lee, A. D. (2016). Virtual currencies: Media of exchange or speculative asset?, *SWIF Institute Working Paper* (2014-007).

Biais, B., Bisière, C., Bouvard, M. and Casamatta, C. (2017). The blockchain folk theorem, *Working paper* **TSE-817**.

Bloomberg (2019). Index methodology: Bloomberg Galaxy Crypto Index, Index Methodology.
**URL:** `https://data.bloomberglp.com/indices/sites/2/2018/05/BGCI-Methodolgy.pdf`

Bouri, E., Shahzad, S. J. H. and Roubaud, D. (2019). Co-explosivity in the cryptocurrency market, *Finance Research Letters* **29**: 178–183.

Brière, M., Oosterlinck, K. and Szafarz, A. (2015). Virtual currency, tangible return: Portfolio diversification with bitcoins, *Journal of Asset Management* **16**(6): 365–373.

Burniske, C. and White, A. (2017). Bitcoin: Ringing the bell for a new asset class, *Ark Invest Research* .

Buterin, V. (2015). A next-generation smart contract and decentralized application platform, *White Paper* .

Catalini, C. and Gans, J. (2018). Some simple economics of the blockchain, *NBER Working Paper* .

Chaim, P. and Laurini, M. (2019). Is bitcoin a bubble?, *Physica A: Statistical Mechanics and its Applications* **517**: 222–232.

Chang, V., Newman, R., Walters, R. and Wills, G. (2016). Review of economic bubbles, *International Journal of Information Management* **36**(4): 497–506.

Chaum, D. (1983). Blind signatures for untraceable payments, *Advances in Cryptology Proceedings of Crypto* **82**(3).

Chaum, D. (1990). Untraceable electronic cash, *in* S. Goldwasser (ed.), *Advances in Cryptology - CRYPO'88*, pp. 319–327.

Cheah, E.-T. and Fry, J. (2015). Speculative bubbles in bitcoin markets? An empirical investigation into the fundamental value of bitcoin, *Economics Letters* **130**: 32–36.

Collomb, A. and Sok, K. (2016). Blockchain and distributed ledger technologies (DLT): What impact on financial markets ?, *Opinions and debats* **15**.

Cong, L. W. and He, Z. (2017). Blockchain disruption and smart contracts, *SSRN Elec. Journal* .

Corbet, S., Lucey, B. and Yarovaya, L. (2017). Datestamping the bitoin and ethereum bubbles, *Finance Research Letter* .

Dabbagh, M., Sookhak, M. and Safa, N. S. (2019). The evolution of blockchain: A bibliometric study, *IEEE Access* **7**.

Dai, W. (1999). B-money.
**URL:** `http://www.weidai.com/bmoney.txt`

D'avolio, G., Gildor, E. and Shleifer, A. (2002). Technology, information production, and market efficiency, *Economic Policy for the Information Economy. Federal Reserve Bank of Kansas City* .

Duffield, E. and Diaz, D. (2018). Dash: A payments-focused cryptocurrency, *White Paper* .

Engle, R. F. and Sheppard, K. (2001). Theoretical and empirical properties of dynamic conditional correlation multivariate GARCH, *NBER Working Paper* **8554**.

Fama, E. (1970). Efficient capital markets: A review of theory and empirical work, *The Journal of Finance* **25**(2): 383–417.

Fama, E. and French, K. (1992). The cross-section of expected stock returns, *The Journal of Finance* **XLVII**(2): 427–465.

Feigenbaum, J. A. (2001). A statistical analysis of log-periodic precursors to financial crashes, *Quantitative Finance* **1**(3): 346–360.

Figuet, J.-M. (2016). Bitcoin et blockchain : quelles opportunités ?, *Revue d'économie financière* **123**(3): 325–338.

Fry, J. (2018). Booms, busts and heavy-tails: The story of bitcoin and cryptocurrency markets?, *Economics Letters* **171**: 225–229.

Fry, J. and Cheah, E.-T. (2016). Negative bubbles and shocks in cryptocurrency markets, *International Review of Financial Analysis* **47**: 342–352.

Geraskin, P. and Fantazzini, D. (2013). Everything you always wanted to know about log periodic power laws for bubble modelling but were afraid to ask, *European Journal of Finance* **19**(5).

Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. C. and Siering, M. (2014). Bitcoin - Asset or Currency? Revealing users' hidden intentions, *Twenty Second European Conference on Information Systems*.

Grant, J. M. (2014). Is bitcoin money?: Implications for bitcoin derivatives regulation and security interest treatment of bitcoins under article 9 of the uniform commercial code, *New York University (NYU), School of Law* .

Hafner, C. (2018). Testing for bubbles in cryptocurrencies with time-varying volatility, *SSNR Elec. Journal* .

Jiang, Z.-Q., Zhou, W.-X., Sornette, D., Woodardb, R., Bastiaensen, K. and Cauwels, P. (2010). Bubble diagnosis and prediction of the 2005-2007 and 2008-2009 Chinese stock market bubbles, *Journal of Economic Behavior & Organization* **74**(3): 149–162.

Johansen, A., Ledoit, O. and Sornette, D. (2000). Crashes as critical point, *International Journal of Theoretical and Applied Finance* **3**(2): 219–255.

Kancs, D., Ciaian, P. and Miroslava, R. (2015). The digital agenda of virtual currencies. Can bitcoin become a global currency?, *Publications Office of the European Union, JRC Technical report* .

Kim, T. (2017). On the transaction cost of bitcoin, *Finance Research Letters* **23**: 300–305.

Kodres, L. and Pritsker, M. (2002). A rational expectations model of financial contagion, *The Journal of Finance* **57**(2): 769–799.

Kummerow, M. and Lun, J. C. (2005). Information and communication technology in the real estate industry: Productivity, industry structure and market efficiency, *Telecommunications Policy* **29**: 179–190.

Lakosmki-Laguerre, O. and Desmedt, L. (2015). L'alternative monétaire bitcoin : une perspective institutionnaliste, *Revue de la régulation* **18**(2).

Lamberti, F., Gatteschi, V., Demartini, C., Pranteda, C. and Santamaria, V. (2017). Blockchain or not blockchain, that is the question of the insurance and other sectors, *IT Professional* **PP**(99).

Larios-Hernandez, G. J. (2017). Blockchain entrepreneurship opportunity in the practices of the unbanked, *Business Horizons* **60**(6): 865–874.

Lee, S., Alford, M., Cresson, J. and Garner, L. (2017). The effects of information communication technology on stock market capitalization: A panel data analysis, *Business and Economic Research* **7**(1): 261–272.

Li, Z.-Z., Tao, R., wei su, C. and Lobont, O.-R. (2019). Does bitcoin bubble burst?, *Quality & Quantity* (1).

Libra, A. (2019). An introduction to Libra, White Paper.
**URL:** https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US.pdf

Lin, L., Ren, R. E. and Sornette, D. (2009). A consistent model of 'explosive' financial bubbles with mean-reversing residuals, *International Review of Financial Analysis* **33**: 210–225.

Lin, L., Ren, R. and Sornette, D. (2014). The volatility-confined LPPL model: A consistent of "explosive" financial bubbles with mean-reverting residuals, *International Review of Financial Analysis* **33**: 210–225.

Lin, L. and Sornette, D. (2009). Diagnostics of rational expectation financial bubbles with stochastic mean-reverting termination times, *European Journal of Finance* **19**(5).

MacDonnell, A. (2014). Popping the bitcoin bubble: An application of log-periodic power law modeling to digital currency, *Working Paper* .

Merediz-Sola, I. and Bariviera, A. (2019). A bibliometric analysis of bitcoin scientific production, *Research in International Business and Finance* **50**: 294–305.

Nadarajah, S. and Chu, J. (2017). On the inefficiency of bitcoin, *Economics Letter* **150**: 6–9.

Nem (2018). NEM technical reference version 1.2.1, *White Paper* .

Phillips, P. and Shi, S. (2018). Real time monitoring of asset markets: Bubbles and crises, *Cowles Foundation Discussion Paper* (2152).

Pietrewicz, L. (2018). Token-based blockchain financing and governance: A transaction cost approach, *Working Paper* .

Ross, R., Molina, M. and Beard, B. (2018). Waste not, want not: Your computer could help cure cancer, *White Paper 4.0* .

Schwartz, D., Youngs, N. and Britto, A. (2015). The Ripple protocol consensus algorithm, *White Paper* .

Schwartzkopff, D., Schwartzkopff, L., Botha, R., Finlayson, M. and Cronje, F. (2017). CRYPTO20: The first tokenized cryptocurrency index fund, *White Paper* .

Shermin, V. (2017). Disrupting governance with blockchains and smart contracts, *Strategic Change* **26**(5): 499–509.

Sornette, D. and Johansen, A. (2001). Significance of log-periodic precursors to financial crashes, *Quantitative Finance* **1**(4): 452–471.

Su, C.-W., Li, Z.-Z., Tao, R. and Si, D.-K. (2018). Testing for multiple bubbles in bitcoin markets: A generalized sup ADF test, *Japan and the World Economy* **46**: 56–63.

Szabo, N. (1997). The idea of smart contracts, *White Paper* .
**URL:** `http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html`

Szabo, N. (2005). Bit gold.
**URL:** `https://unenumerated.blogspot.com/2005/12/bit-gold.html`

Tapscott, D. and Tapscott, A. (2017). How blockchain will change organizations, *MIT Sloan Management Review* **58**(2): 10–13.

Trimborn, S. and Hardle, W. K. (2016). CRIX an index for blockchain based currencies, *Discussion Paper* **021**.

Urquhart, A. (2017). Price clustering in bitcoin, *Economics Letter* **159**: 145–148.

Vogiazas, S. and Alexiou, C. (2019). Bitcoin: The road to hell is paved with good promises, *Economic Notes, Review of Banking, Finance and Monetary Economics* **48**(1).

Wheatley, S., Sornette, D., Huber, T., Reppen, M. and Gantner, R. (2019). Are bitcoin bubbles predictable? Combining a generalized Metcalfe's Law and the log-periodic power law singularity model, *Royal Society Open Science* **6**.

Yermack, D. (2015). Is bitcoin a real currency? An economic appraisal, *in* D. L. K. Cheun (ed.), *Handbook of Digital Currency Bitcoin, Innovation, Financial Instruments, and Big Data*, chapter 2, pp. 31–43.

## LIST OF ABBREVIATIONS

**DCC** Dynamic Conditional Correlation . . . . . . . . . . 19, 186, 187, 190

**EMH** Efficient Market Hypothesis . . . . . . . . . . . . . . . . . . . . . . 11

**FBA** Federated Byzantine Agreement . . . . . . . . . . . . . . . . . 37, 38

**GDPR** General Data Protection Regulation . . . . . . . . . . . . . . . . . 67

**ICO** Initial Coin Offering . . . . . . . . . . . . . . . . . . . . 5, 6, 75, 79, 210

**IEO** Initial Exchange Offering . . . . . . . . . . . . . . . . . . . . . . 210

**IoT** Internet of Things . . . . . . . . . . . . . . . . . . . . . . . . . . . 4

**LPPL** Log Period Power Model . 18, 19, 137, 139, 140, 144, 145, 147, 150, 151, 159–161, 171, 184, 185, 193, 194, 209, 211

**PBFT** Practical Byzantine Fault Tolerance . . . . . . . . . . . . . . 37, 38

**PoS** Proof-Of-Stake . . . . . . . . . . . . . . . . . . . . . . . . 37, 38, 58

**PoW** Proof-Of-Work . . . . . . . . . . . . . . . . . . . . . . . 37, 38, 58

**PSY** Phillips, Shi and Yu Model . . . 137, 139, 147–150, 166, 168, 185, 193

**SEC** Securities and Exchange Commission . . . . . . . . . . . . . 17, 99

**STO** Security Token Offering . . . . . . . . . . . . . . . . . . . . . . . 210

## LIST OF TERMS

**Bitcoin** The first cryptocurrency created by Satoshi Nakamoto in 2008. The objective is to create a decentralized payment system that works without third-party (such as central banks, commercial banks, financial institution or government). The third-party is replaced by the blockchain technology (see below). The white paper is (Nakamoto, 2008) and its website is https://bitcoin.org. . . . . . . . . . . . . . . . . . . . . . . . . . viii–x, 1–11, 14, 16–19, 27, 28, 30–36, 39, 40, 51, 53–56, 59, 61, 64, 66, 70, 71, 73, 75–79, 91–113, 115–122, 124, 125, 127–131, 137, 138, 140, 142, 145–147, 161–169, 171, 176–178, 181, 183–194, 205–209, 211

**Blockchain** Blockchain is a secured technology of storage and transmission of information without the requirement of a third-party. The security and the viability are ensured by all participants in a consensus eco-system. Blockchain is considered as a distributed and immutable database that contains the entire historical background of transactions (from its creation to its current state). . . viii, x, 4–6, 8–10, 12–18, 27–32, 34–41, 49–79, 92, 95, 96, 98, 99, 104, 106, 108, 111, 113–115, 117, 119–121, 128–130, 205–208, 210, 212

**Cryptocurrency** the Bank for International Settlements defines a "cryptocurrency" as an electronic, peer-to-peer and universally accessible money that is not issued by a central bank. . . . . . . viii, ix, xi, 1–3, 5–19, 28, 30, 34, 35, 39, 51, 53, 64, 66, 68, 70–72, 74, 76, 77, 91, 92, 99, 124, 131, 137–142, 144–147, 151, 161–168, 182–191, 193, 194, 205–212

**Decentralization** "Blockchains are politically decentralized (no one controls them) and architecturally decentralized (no infrastructural central point of failure) but they are logically centralized (there is one commonly agreed state and the system behaves like a single computer)." (Buterin, 2017).

13, 27, 28, 35, 50, 52, 54, 56, 57, 64, 67, 77, 79, 142, 205, 206

**Delegated Proof-of-Stake** an extension of the Proof-of-Stake in which the users select "witnesses" through a voting process that will validate the transaction when the witness possesses the most tokens (Xu et al., 2018). . 68

**Double-spending problem** The double-spending problem arises when two different transactions are made with the same coin. . . . . . . 1, 3, 34, 35, 61

**Efficient Market Hypothesis** Efficient Market Hypothesis (EMH) represents "a market in which prices always fully reflect available information", (Fama, 1970). There are three forms of EMH: weak (past information are integrated by prices), semi-strong (public and past information are integrated by prices) and strong (past, public and private information are integrated by prices). . . . . . . . . . . . . . . . . . . . . . 11, 14, 125

**Ether** The cryptocurrency of the Ethereum plateform. Ethereum is a blockchain-based platform service to run smart contracts (see below). The white paper is (Buterin, 2015) and its website is https://www.ethereum.org/. . 5, 7, 19, 71, 99, 137, 140, 146, 147, 161–169, 176, 177, 179, 181, 183–189, 191–194, 209

**Finality** Number of validated blocks (how long) a user has to wait to be sure the block, in which his transaction is located, is validated and written in the blockchain. . . . . . . . . . . . . . . . . . . . . . . 37, 39, 67–69

**Fork** The splitting of a ledger in two ledgers (modification of the codes) due to block conflicts or rules conflicts (in the code). If two persons mine two different blocks and validate them at the same time, it creates a fork on the blockchain. . . . . . . . . . . . . . . . . . . . . . . . . . 34, 55

**Immutability** Something which can never be modified or deleted. Possibility to no change the history of the blockchain. . . . . 37, 39, 57, 58, 67, 68

**Initial Coin Offering** The Initial Coin Offering (ICO) is a fundraising method in which specific tokens (see below) are issued and priced in cryptocurrencies at the launch of a blockchain project and for a small period of time. In return for the tokens sold, the organization at the origin of the project receives the money in cryptocurrency.After the project, the token holders can trade their tokens in a secondary market or sometimes use it in the project itself. . . . . . . . . . . . . . . . . . . . . . . 5, 79, 210

**Initial Exchange Offering** In the vein of ICO (see below), Exchange Initial Offering is a fundraising method audited and conducted by exchange platforms. Issuers are charged fees and a percentage of sale dedicated to exchange platforms. Participants have to create an account on the exchange platform. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 6

**Litecoin** Created in 2011 by Charlie Lee, Litecoin is a cryptocurrency based on the Bitcoin protocol but with some differences (transactions validation speed, mining process accessibility, economic mode). Because its supply is limited to 84 million units, it is often called the “silver coin”. Its website is https://litecoin.org/. 5, 7, 19, 70, 71, 137, 140, 146, 147, 161–168, 170, 176, 177, 180, 181, 183–185, 187–189, 191–193, 209

**Miners** Blockchain participants who write in the ledger and validate transactions through the consensus mechanism. 16, 29–38, 40, 52, 63–68, 73, 76, 77, 95, 206

**Mining** The main purpose is the process of adding transactions to the blockchain by participants called miners. The process has to be resource-incentive and difficult to protect the integrity of the blockchain using consensus mechanism (see Proof-of-Work and Proof-of-Stake) but easily verifiable by the participants in the network reaching a consensus. To recognize their efforts, miners receive a reward for their works, new cryptocurrency. The monetary creation is the second purpose of the mining process. 33, 39, 69, 73, 95, 97, 141, 208, 210

**Proof of Ownership** Proof of Ownership is a method within Blockchain to track the owners of a certain information over the time (the coins in the case of cryptocurrency). . . . . . . . . . . . . . . . . . . . . . . . . 33

**Proof-of-Stake** Consensus mechanism system to validate transactions in a block that will be added to the blockchain based on the share held in the cryptocurrency. . . . . . . . . . . . . . . . . . . . 2, 38, 56, 66, 68, 76, 206, 243

**Proof-of-Work** Consensus mechanism system to validate transactions inside a block that will be added to the blockchain based on the computational power. . . . . . . . . . . . . . . . . . . . . . 2, 33, 34, 38, 56, 66, 206

**Ripple** In 2004, Ripplepay is created by Ryan Fugger. The objective is to create a distributed monetary system for financial services where individuals lend and borrow money directly to each other without the requirement of a bank.In 2012, Opencoin is created driven by Jed McCaleb and Chris Larsen and in 2013 the organization changed its name to become Ripple Labs providing the cryptocurrency Ripple. The objective is to provide a universal clearing currency in the interbank exchanges. The white paper is (Schwartz et al., 2014) and its website is https://ripple.com/. 2, 5, 7, 19, 68, 70, 71, 137, 140, 145–147, 161–168, 170, 176, 177, 181, 183–193, 209

**Scalability** Ability to reach a higher throughput (see below) when the number of users is growing (node-scalability, performance-scalability (Vukolić, 2015)). . . . . . . . . . . . . . . . . . . . . . . . . 37, 39, 54, 66–69

**Security Token Offering** A type of Initial Public Offering (IPO) in the cryptocurrency market with specific legal market rules. STO issues "security token" (digital asset recorded on the blockchain and representative financial instrument (common stocks, debt, real-estate, commodity…). It is basically a regulated ICO based on traditional banking and financial rules. 6

**Smart Contracts** A smart contract is a software-based contract that runs automatically when its conditions are met. 1, 5, 9, 10, 16, 35, 50, 55, 57, 58, 67, 68, 71, 72, 75, 79, 186, 205–207

**Sybil attack** Sybil attack is a peer-to-peer network attack in which one individual takes the control of the network by creating several nodes or accounts. In the cryptocurrency domain, it is one individual who operates several nodes on the blockchain network. . . . . . . . . . . . . . . . . . . . . 69

**Throughput** Transactions by period of time to be validated by the consensus (e.g. performance). . . . . . . . . . . . . . . . . . . . . . 37, 39, 67, 69

**Token** A token is a digital asset that can be issued and exchanged on an existing blockchain. Similar to cryptocurrencies, they are exchanged in a distributed network without third-party. Contrary to cryptocurrency, they are not based on their own blockchain and are not issued by mining process. Most of tokens are based on the ERC20 protocol of Ethereum. Tokens are easily created by any Internet user, generally, a tech or crypto start-up, with the objective of raising funds for a project (generally a decentralized app). Tokens are issued generally through Initial Coin Offerings process (see above definition). After their issuance, they are tradable on exchange platform or use in the project itself (right of usage, access or vote, mean of payment, reputation…). . . . . . . . . . . . 2, 5, 39, 51, 56, 67, 68

**Users** Blockchain participants who send transactions, read and analyze the data inside the ledger. 4, 5, 16, 18, 28–40, 52, 53, 56, 60, 62–69, 73, 76, 77, 95, 96, 98, 141, 142, 192, 206, 209

**Wallet** Secure storage solution (physical or digital) for cryptocurrencies. It can take the form of client software, application, encrypted and secure file or a simple piece of paper. In any case, the wallet contains a public key (cryptocurrency address) known from everyone and a private key only known by the cryptocurrency owner. . . . . . . . . . . . . . . . . 39, 53

## Abstract

The innovation introduced by cryptocurrencies and their underlying technology, blockchain, opens new avenues for research in finance. This PhD dissertation proposes three essays on cryptocurrencies, essays that use the theoretical framework of markets' informational efficiency.
The first study aims to explain how the blockchain developed in informal communities is adopted and incorporated by organizations. This study uses the contractual and cognitive approaches of the organization theory in order to provide a theoretical framework for the blockchain technology. Through an illustrated literature review, a two-level analysis presents the potential uses of blockchain based on information access for participants. The objective of the second study is twofold. First, it raises the question about the true nature of Bitcoin. After comparing Bitcoin with currencies, gold and common stocks, we base our analysis on the assumption that cryptocurrencies may be assimilated to common stocks. Second, the financial performance (risk-adjusted return) of Bitcoin is empirically assessed using traditional models such as the CAPM and Fama-French three-factor models. We find that while integrating Bitcoin in portfolio highly improves its diversification, it also provides positive and significant risk-adjusted returns in the World, European and Asia-Pacific regions. The high Bitcoin's volatility and performance lead us naturally to focus on the speculative bubble aspect of cryptocurrencies, which is the focus of the third study. The analysis uses the PSY model of Phillips and Shi, 2018. Second, we focus the analysis on the main peak/burst of the cryptocurrency market at the end of 2017 using the Log Periodic Power Law (LPPL) model. The results suggest periods of bubbles implying a contagion effect between cryptocurrencies. The conceptual and empirical findings of this dissertation contribute to prior literature on cryptocurrencies on academic grounds. Our findings are also important for businesses and for investors that are interested in the cryptocurrency and blockchain potential as well as for policymakers in charge of their regulation.

Keywords: Cryptocurrencies, Efficiency, Blockchain, Bitcoin, Performance, Speculative Bubble

## Résumé

Les innovations apportées par les cryptomonnaies et leur technologie sous-jacente, la blockchain, ouvrent de nouvelles voies de recherches en finance. Cette thèse de doctorat est composée de trois essais portant sur les cryptomonnaies et est centrée autour de la notion d'efficience informationnelle des marchés. La première étude vise à expliquer comment la blockchain, développée au sein de communautés informelles, est adoptée et intégrée par les organisations. Cette étude apporte un cadre théorique à la technologie blockchain, cadre qui s'appuie sur les approches contractuelle et cognitive de la théorie des organisations. Grâce à une revue de la littérature illustrée, une analyse à deux dimensions présente les possibles utilisations de la blockchain fondées sur l'accès à l'information pour les participants. L'objectif de la seconde étude est double. Premièrement, elle soulève la problématique de la réelle nature du Bitcoin. Après avoir comparé le Bitcoin aux monnaies, à l'or et aux actions, nous basons notre analyse sur l'hypothèse que les cryptomonnaies peuvent être assimilées aux actions. Deuxièmement, la performance financière (la rentabilité ajustée au risque) du Bitcoin est mesurée en utilisant des modèles traditionnels tels que le MEDAF et le model de Fama-French à trois facteurs. Nous trouvons que l'intégration du Bitcoin dans un portefeuille améliore considérablement sa diversification, tout en apportant des rentabilités ajustées au risque positives et significatives dans le monde, l'Europe et l'Asie-Pacifique. La forte volatilité du Bitcoin ainsi que sa haute performance nous conduisent à analyser le caractère de bulle spéculative des cryptomonnaies, ce qui est l'objet de la troisième étude. Nous analysons cet aspect en utilisant le modèle PSY de Phillips and Shi, 2018. Deuxièmement, nous analysons le plus important pic/éclatement du marché des cryptomonnaies à la fin des années 2017 à l'aide du modèle LPPL (Log Periodic Power Law). Les résultats suggèrent des périodes de bulles avec effet de contagion entre les cryptomonnaies. Les analyses théoriques et empiriques de cette thèse contribuent à la littérature académique sur les cryptomonnaies. Nos résultats sont également importants pour les entreprises et pour les investisseurs qui s'intéressent au potentiel des cryptomonnaies et de la blockchain, ainsi que pour les décideurs politiques responsables de leur régulation.

Mots-clés : Cryptomonnaies, Efficience, Blockchain, Bitcoin, Performance, Bulle spéculative