Everything you always wanted to know about bitcoin modelling but were afraid to ask

Dean Fantazzini* Erik Nigmatullin † Vera Sukhanovskaya ‡ Sergey Ivliev §

Abstract

Bitcoin is an open source decentralized digital currency and a payment system. It has raised a lot of attention and interest worldwide and an increasing number of articles are devoted to its operation, economics and financial viability. This article reviews the econometric and mathematical tools which have been proposed so far to model the bitcoin price and several related issues, highlighting advantages and limits. We discuss the methods employed to determine the main characteristics of bitcoin users, the models proposed to assess the bitcoin fundamental value, the econometric approaches suggested to model bitcoin price dynamics, the tests used for detecting the existence of financial bubbles in bitcoin prices and the methodologies suggested to study the price discovery at bitcoin exchanges.

Keywords: Bitcoin, Crypto-currencies, Hash rate, Investors' attractiveness, Social interactions, Money supply, Money Demand, Speculation, Forecasting, Algorithmic trading, Bubble, Price discovery.

JEL classification: C22, C32, C51, C53, E41, E42, E47, E51, G17.

Applied Econometrics, forthcoming

*Moscow School of Economics, Moscow State University, Leninskie Gory, 1, Building 61, 119992, Moscow, Russia. Fax: +7 4955105256 . Phone: +7 4955105267 . E-mail: fantazzini@mse-msu.ru .

†Bocconi University, Milan (Italy); nigmatullin.erik@gmail.com

‡Perm State National Research University; Laboratory of Crypto-Economics and Blockchain systems; vera-sukhanovskaya@yandex.ru

§Perm State National Research University; Laboratory of Crypto-economics and Blockchain systems; ivliev@gmail.com. This is the working paper version of the paper *Everything you always wanted to know about bitcoin modelling but were afraid to ask*, forthcoming in Applied Econometrics.

1 Introduction

Bitcoin is an online decentralized currency that allows users to buy goods and services and execute transactions, without involving third parties. It was launched in 2009 by a person or (more likely) by a group of people operating under the name of Satoshi Nakamoto. Bitcoin belongs to the large family of "cryptocurrencies", which are based on cryptographic methods of protection. The main characteristic of these currencies is their decentralized structure: there is no central authority which issues and regulates the currency, and transactions are executed using a peer-to-peer crypto-currency protocol without intermediaries. Introductory surveys about bitcoin structure and operation can be found in Becker et al. (2013), Segendorf (2014), Dwyer (2014), Böhme et al. (2015), or simply in Bitcoin (2015). Several central banks also examined bitcoin, see Velde (2013), Lo and Wang (2014), Baden and Chen (2014), Ali et al. (2014), and ECB (2012, 2015). Discussions of bitcoin as a potential alternative monetary system can be found in Rogojanu and Badea (2014) and Weber (2016), while the economics of bitcoin mining are examined in Kroll (2013). Analyses of the legal issues involved by using bitcoin can be found in Allen (2015) and Murphy et al. (2015).

The goal of this article is to review the econometric and mathematical tools which have been proposed so far to model the bitcoin price and several related issues. To our knowledge, such a review is missing in the financial literature and it can be of interest to both market professionals and researchers alike, given the early stages of the empirical literature devoted to bitcoin.

The rest of the paper is organized as follows. Section 2 introduces crypto-currencies with a particular focus on bitcoin, and briefly explains how bitcoin works. Section 3 reviews the studies devoted to the analysis of the characteristics of bitcoin users, while Section 4 discusses the main models proposed to assess the bitcoin fundamental value, ranging from market sizing to the bitcoin marginal cost of production based on electricity consumption. Section 5 describes several econometric approaches suggested to model bitcoin price dynamics, starting with cross-sectional regression models involving the majority of traded digital currencies and then moving to univariate and multivariate time series models, till models in the frequency domain. Section 6 reviews the tests employed for detecting the existence of financial bubbles in bitcoin prices and which can be broadly classified into two large families, depending on whether they are intended to detect a single bubble, or (potentially) multiple bubbles. Section 7 examines the methodologies suggested to estimate the information share of various bitcoin exchanges with respect to the information generated by the whole market, which is of great importance for both short-term traders and long-term investors who want to know which exchange reacts most quickly to new information. Section 8 briefly concludes and highlights several possible avenues for further research.

2 Definition of Crypto-currencies and Bitcoin

2.1 How Bitcoin works

2.1.1 Digital signatures and cryptographic hash function

The Bitcoin network uses cryptography to validate transactions during the payment processing and create transaction blocks. In particular, Bitcoin relies on two cryptographic schemes: 1) digital signatures and 2) a cryptographic hash function. The first scheme allows the exchange of payment instructions between the involved parties, while the second is used to maintain the discipline when recording transactions to the public ledger (known as *Blockchain*). It should be noted that none of these schemes is unique to Bitcoin, since they are widely used to protect commercial and government communications. A short description of how the Bitcoin network works is reported below, while more details can be found in Becker et al. (2013), Segendorf (2014), Dwyer (2014), Böhme et al. (2015), or simply in Bitcoin (2015).

Digital signatures are used to authenticate digital messages between a sender and a recipient, and they provide:

(i) *Authentication*: the receiver can verify that the message came from the sender;

(ii) *Non-repudiation*: the sender cannot deny having sent the message;

(iii) *Integrity*: the message was not altered in transit.

The use of digital signatures includes public key cryptography, where a pair of keys (open and private) are generated with certain desirable properties. A digital signature is used for signing messages: the transaction is signed using a private key, and then transferred to the Bitcoin network. All the members of the network can verify that the transaction came from the owner of the public key, by taking the message, the signature, the public key and by running a test algorithm.

A cryptographic hash function takes as input a string of arbitrary length (the message m), and returns the string with predetermined length (the hash h). The function is deterministic, which means that the same input m will always give the same output h. In addition,the function must also have the following properties:

(i) *Pre-image resistance:* for a given hash h, it is difficult to find a message m such that hash$(m) = h$

(ii) *Collision resistance*: for a given message m_1 it is hard to find another message m_2 such that hash (m_1) = hash (m_2). In other words, a change in the message leads to a change in the hash.

The output of the hash function looks like to be random, although it is completely deterministic. The Bitcoin network mainly uses the secure hash algorithm SHA-256 / type Secure Hash Algorithm (SHA-2),

designed by the National Security Agency and published by the National Institute of Standards and Technology, see Dang (2012) for details.

2.1.2 Possession of bitcoins and bitcoin addresses

From a technical standpoint, bitcoins stay in the Bitcoin network on bitcoin-addresses. The ownership of a certain number of bitcoins is represented by the ability to send payments via the Bitcoin network using the bitcoins attached to these addresses. The ability to send payments to other bitcoin addresses is controlled by a digital signature, which include a public key and a private key. In particular, every bitcoin address is indexed by a unique public ID, which is an alphanumeric identifier, which corresponds to the public key. The private key controls the bitcoins stored at that address. Any payment (i.e. a *message*) which involved this address as the sending address must be signed by the corresponding private key to be valid. In straight terms, the possession of bitcoins at a specified bitcoin address is given by the knowledge of the private key corresponding to that address.

At any point in time, every bitcoin address is associated with a bitcoin balance, which is public information. Each existing or proposed (broadcasted) transaction can be checked for compliance with the past transaction history, i.e. it is possible to verify that the transferred bitcoin do exist at the corresponding bitcoin address.

2.1.3 A transaction in the block chain

The agents who process transactions in the Bitcoin network use a set of bitcoin addresses called *wallet*, which is the set of bitcoin addresses that belong to a single person/entity. Each transaction record includes one or more sending addresses (inputs) and one or more receiving addresses (outputs), as well as the information about how much each of these addresses sent and received. An example of a typical transaction is shown in Fig. 1.

In the example Alisa sends to Bob an amount of 8 BTC. This transactions has two inputs (2 and 7 BTC) and two outputs (8 and 1 BTC), where the transaction involving 1 BTC can be considered essentially as the change of the transaction, which is returned back to Alice. Since each transaction can have multiple sending addresses and receiving addresses, it is often impossible to link a specific sending address to a specific receiving address. The consequence of this is that you cannot assign a serial number to a specific bitcoin and trace its path in the Bitcoin network.

Transaction processing in the Bitcoin network is based on mechanisms which ensure that (a) the verification of each transaction is distributed among several network members; (b) the record of each transaction is discrete with respect to time, i.e. the transactions are linearly ordered with successive time stamps; (c) the participants in the payment network compete and are rewarded for the recording of the

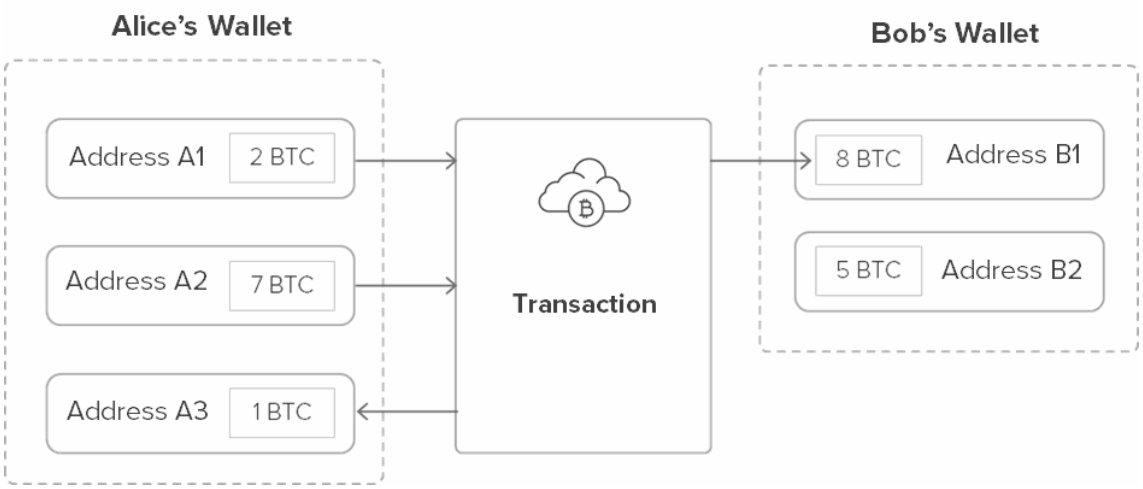

Figure 1: A typical transaction in the Bitcoin network

transactions in a [Bitcoin network] block; (d) multiple nodes cross-check each recorded transaction.

2.1.4 Starting a transaction

Suppose Alice wants to send Bob 1 bitcoin using the Bitcoin network. To do this, Alice and Bob must have a bitcoin address. Let's call them ID_Alice and ID_Bob. Then, Alice needs to send and digitally certify the authenticity of the message, of this type

"ID_Alice sends ID_Bob 1 bitcoin."

After Alice signs the transaction message with her private key and sends it, any participant in the Bitcoin network can verify Alice sent the message, and the message has not been altered. Moreover, as we discussed earlier, the digital signature guarantees that no one else could sign the message, so that Alice cannot deny that it has signed the message.

2.1.5 Checking a transaction

Before executing a transaction, the Bitcoin protocol must verify two aspects of the communication: first, whether it was Alice who sent the message. The digital signature scheme ensures that only the owner of the private key for that address may sign a message; secondly, to check whether there are sufficient funds in the address to ensure the completion of the transaction.

Although the record keeping and the verification of transactions are the main features of electronic payment systems, these functions are usually carried out through private registries, supported by trusted third parties. Decentralized systems such as Bitcoin, replace the third-party intermediaries and store transaction records on a public ledger, which is maintained by a distributed information system.

2.1.6 Updating the Blockchain

After the initial check of the transaction signed messages, validation nodes in the Bitcoin network begin to compete for the opportunity to record a transaction in the Blockchain. First, in the block of the transaction, competing nodes start putting together transactions, which were executed since the last record in the Blockchain. Then, the block is used to define a complex computing task. The node that first solves this task proceeds to record the transactions on the Blockchain and collects a reward.

The task which the competing nodes try to solve is based on one of the encryption schemes described above - the hash function. First, the block of the newly broadcasted transactions is again used as input for a cryptographic hash function to obtain a hash called *digest*. This digest, together with a one-time random code *nounce* (that is an alphanumeric string) and the hash of the previous block are used in another hash function that produces the hash of the Blockchain for the new block. The problem that the nodes have to solve includes finding such a random code, so that the hash of the new Blockchain has certain properties (in this case has a number of initial zeros). The first of the competing nodes which will find the right random code, transfers this information to the other participants in the network, and the Blockchain is updated. The implementation of this scheme is the so-called *Hashcash* - a proof that the system is operating properly (proof-of-work), and whose aim is to ensure that the computers use a certain amount of computing power to perform a task (see Beck (2002) for more details).

The nodes that perform the process of the proof-of-work in the Bitcoin network are called *miners*. These miners use their computing resources in this process with the goal to obtain the reward offered by the Bitcoin Protocol. Usually the reward is a predetermined number of newly created bitcoins. The rest of the reward (which is currently much smaller), is a voluntary transaction fee paid by those executing the transaction to the miners for transaction processing. The initial idea was that these voluntary contributions would replace the predetermined compensation of newly created bitcoins when this amount will tend to zero over time and a new incentive will be needed to stimulate the miners to process the transactions in the Bitcoin network (see Nakamoto (2009) for details).

2.2 Statistics of the Bitcoin network

2.2.1 Capitalization

At the time of writing this paper, more than 15 million bitcoins have been mined. The price of one bitcoin in first four months of 2016 was in the range of 400-460 USD (see Fig.2). Therefore, the total value of all issued bitcoins was close to 7 billion U.S. dollars. The market capitalization of bitcoin is approximately 10 times higher than the second largest crypto currency, so that bitcoin is (currently) the undisputed leader.

The value of a digital currency is highly dependent on the number of participants, which in turn attracts more participants, powering a network effect. Therefore, bitcoin enjoys a significant first-mover advantage which has three aspects:

- the more users it has, the more useful Bitcoin becomes: there are more places where you can spend bitcoins, and business partners with whom you can exchange bitcoins, which in turns attracts more users;
- currencies require trust, but it can only be obtained over time, so that, ceteris paribus, the oldest currency has a natural advantage over competitors;
- the greater the volume, the higher the transaction fees, which attracts more miners and makes the network more secure, which in turn again attracts more users and traded funds.

With currencies that serve as a store of wealth, there is an additional lock-in effect as it is takes effort to transfer that wealth into other currencies. Thus, there are multiple effects in place that makes it very hard to dethrone Bitcoin. At this point in time, Bitcoin is the strongest leader among crypto currencies.

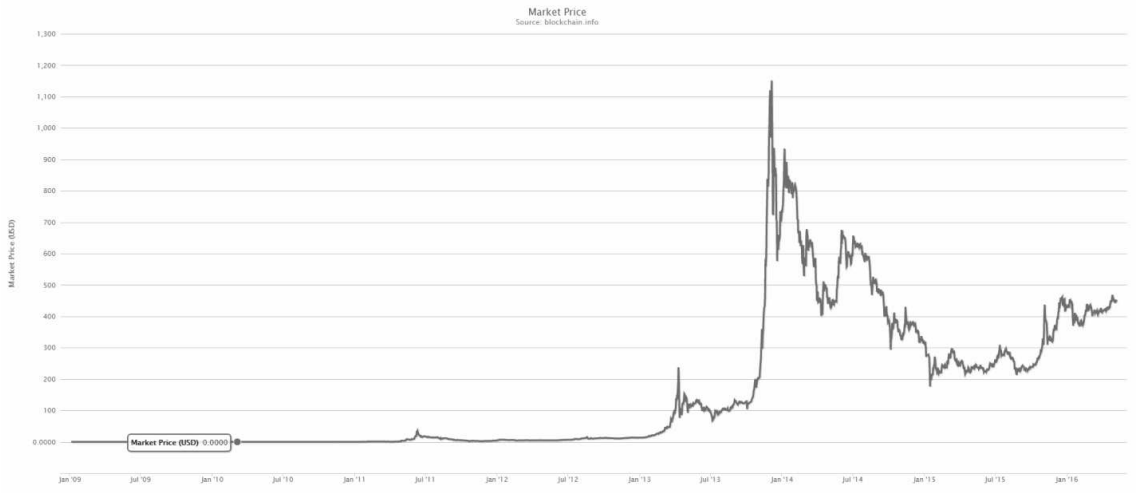

Figure 2: Market price of 1 Bitcoin in US dollars (2009-2016)

2.2.2 Network power

The value of the miners' hardware exceeds $ 300 million, while the total computing power supporting the

Bitcoin network is approximately 800 Peta-hashes/s (see Fig. 3).

The total daily revenue from fees paid to miners for recording transactions and validating new blocks is approximately 1,2-1,5 million US dollars. The number of open bitcoin wallets is higher than 15 million. On average in 2015, bitcoin users make more than 200 thousand transactions per day (see Fig.4).

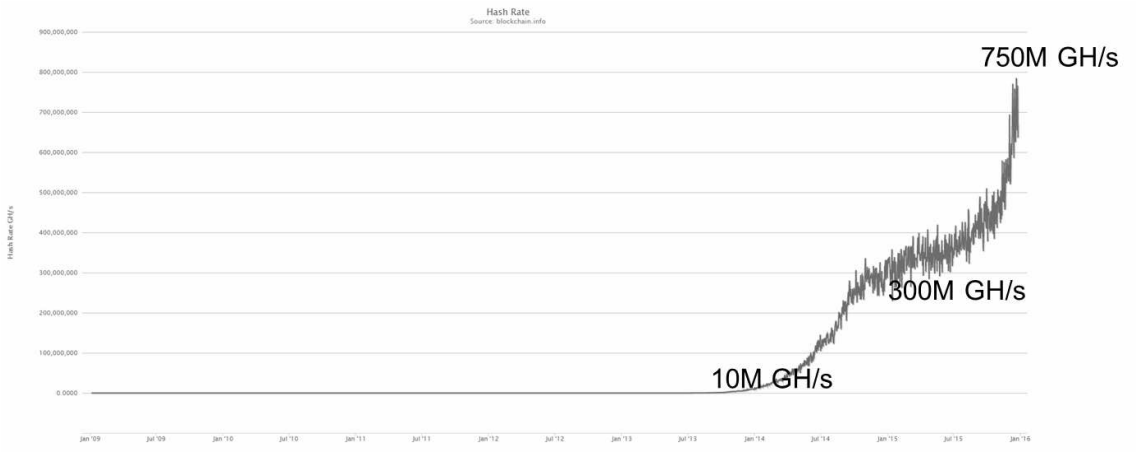

Figure 3: Computing power in the Bitcoin network: 01.01.2009 - 31.12.2015

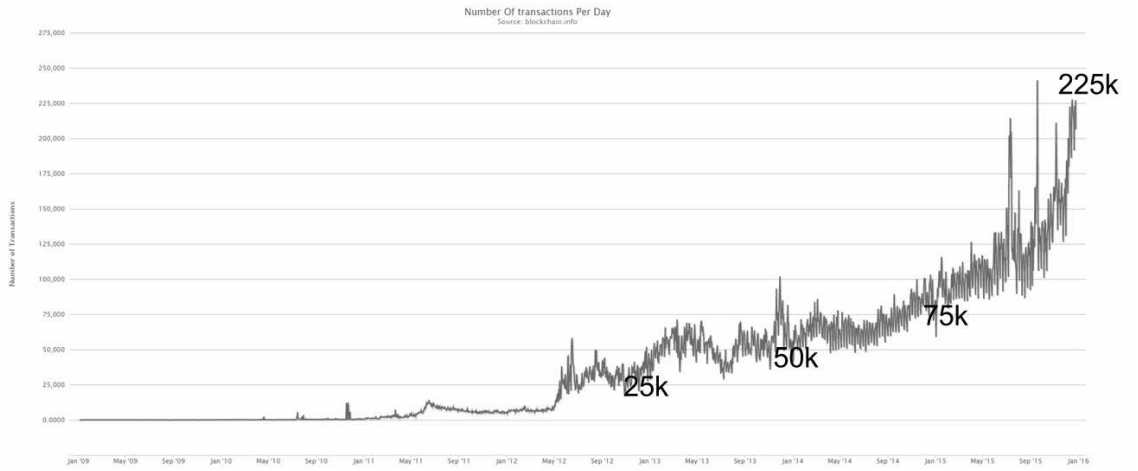

Figure 4: Number of transactions in the Bitcoin network: 01.01.2009 - 31.12.2015

The number of transactions has a natural limit related to the block size (1Mb or about 1500 transactions). Considering the average time required for mining a new unit (10 min), the theoretical limit of the Bitcoin network is currently 7 transactions per second, or about 600 thousand transactions per day. The bitcoin community is actively looking for an optimal solution to increase the block size. Among the main initiatives, we cite the *SegWit* software which would increase the block size approximately 1.5-2 time, and *Lightning Network* designed to build a liquidity network hub for micro-payments using secure p2p channels with the opportunity to significantly reduce costs.

3 Who uses Bitcoin? A review of econometric analysis of Bitcoin users

The Bitcoin system has attracted attention worldwide and the number of scientific papers devoted to it is steadily increasing, see Bohme et al. (2015) and `https://en.bitcoin.it/wiki/Research` for more details. Unfortunately, a very limited number of studies has been devoted to the analysis of the characteristics of Bitcoin users, which could give a better understanding of this phenomenon and its future perspectives. The relative scarcity of academic interest in this field should not come as a surprise, given the extreme difficulty to gather data about Bitcoin users, who mostly want to remain anonymous. A couple of works tried to overcome this problem by interviewing a dozen of Bitcoin users, see Baur et al. (2015) and Huhtinen (2014).

Bohr and Bashir (2014) were the first to analyze a larger structured dataset, consisting of a survey conducted in 2013 by Lúí Smyth, at that time a digital anthropology researcher at the University College London. This survey consists of 1193 responses collected from February 12, 2013 through April 4, 2013. Bohr and Bashir (2014) tried to answer three research questions:1) what predicts the accumulation of wealth among Bitcoin users; 2) what predicts optimism about the near- and long-term value of Bitcoin; 3) what attracts people to Bitcoin. The first issue was examined by performing a simple regression of the self-reported amount of bitcoins owned (transformed to their log base 2 values to avoid skewness) against a set of Bitcoin users' characteristics extracted from the survey:

- the user *Age* and the user *Age* squared to account for nonlinearity;
- a variable named "*Installation*", which refers to when respondents first downloaded the Bitcoin client (software that connects to the Bitcoin network), and ranges from 1 = the first quarter of 2009 to 17 = the first quarter of 2013, and which is then centered on the mean;
- a dummy variable named "*Miner*" to account for whether or not individuals had ever gone through the process mining bitcoins themselves;
- an interaction term "*Installation* x *Miner*", to test whether early Bitcoin miners obtained a large advantage in Bitcoin accumulation versus late adopters of Bitcoin;
- a dummy variables named "*Bitcoin sins*", which is 1 if the respondent admitted to mining bitcoins through someone else's hardware without their permission (via malware), or to steal someone else's bitcoins;
- a dummy variables named "*Lives in U.S*";

- a dummy variables named "*Illicit goods*", which is 1 if the respondent admitted to purchasing narcotics, gambling services, or other illicit goods with their bitcoins.

- a dummy variables named "*Bitcoin talk*", which is 1 if the respondent indicated that he/she uses Bitcoin-specific platforms to talk with others about Bitcoin;

- a dummy variables named "*Investor*" , which is 1 if the respondent self-described their role within the context of Bitcoin as an investor.

- integer variables named "*profit*" and "*community*" ranging from 1 = not motivating to 5 =very motivating, for whether the respondents considered profit or community as motivating factors for their initial involvement with Bitcoin

Bohr and Bashir (2014) found that age was a statistically significant factor in predicting the amount of bitcoin a respondent held: young respondents hold fewer bitcoins, but the amount approximately double every 10 years reaching a maximum between 55 and 60 years old, similarly to accumulation across other asset classes. The interaction term *Installation cdot Miner* is significant, confirming that mining bitcoins was easier during the early days of its operation, so that early adopter miners gained an advantage in Bitcoin accumulation. Those who actively participated in bitcoin online communities owned twice as much bitcoin as those who do not, while those users who self-identified themselves as investors had accumulated about four times as many bitcoins as those who did not. Ceteris paribus, Bitcoin users who purchased illicit goods, such as narcotics, had up to 45% more bitcoin holdings than those who bought only legal goods

Bohr and Bashir (2014) then performed two additional regressions, where the near-term (four months from time of survey) and the long-term (six years from time of survey) expected values of one bitcoin in USD where regressed against the previous set of variables: older users were found to be less optimistic than younger users, with optimism peaking at about age 35, while the higher is the level of social engagement on online forums, the higher the predicted price. Interestingly, the later Bitcoin installers were more optimistic about the near-term value, while miners were more pessimistic than non-miners regarding the long-term value of Bitcoin.

In a second stage of their analysis, Bohr and Bashir (2014) divided users based on their description of Bitcoin in relation to anonymity freedom, and banking system, and analyzed these three groups using logistic regression. They found that users' political identity was not a factor in predicting whether respondents valued bitcoin for its anonymity, and the only significant variable that suggested a preference for anonymity was whether a user was a miner or not. Users who favored bitcoin for its potential to disrupt the banking system were found to be above the age of 40, residing outside the US and identified themselves

politically as greens. Finally, users who like bitcoin for its freedom-promoting qualities were found to politically identify as libertarian, residing outside the US and aged between 30 and 39. Interestingly, the authors themselves are well aware of the limits of their dataset and ask the reader to consider their results with caution: the (self-selected) sample may not be representative of the full population of Bitcoin users and it considers only the English-speaking bitcoin community. Besides, the survey is quite out of date being collected before the implosion of the now bankrupt exchange Mt.Gox which lost hundreds of thousands of coins. Despite these limits, it is definitely a start and a stimulus to future research.

Yelowitz and Wilson (2014) attempted to solve the problem of a small dataset by using the Google Trends data to examine the determinants of interest in Bitcoin. Google Trends can be used either to extract data for precise search terms or for general topics, where in the latter case related searches are also considered. More specifically, they built proxies for four possible Bitcoin users classes -computer programming enthusiasts, speculative investors, Libertarians and criminals-, as well as for Bitcoin interest for each US state. They searched topics for Bitcoin (under the category 'Currency'), Computer Science (under the category 'Discipline'), whereas for the remaining clienteles – Illegal Activity, Libertarians and Speculative Investors – they used the search terms 'Silk Road', 'Free Market' and 'Make Money', respectively. We remark that the Google Trends data represent how many web searches were performed for a particular keyword (or keywords) in a given week and in a given geographical area, relative to the total number of web searches in the same week and area. The resulting index is then rescaled by Google between 0 and 100 dividing it by its largest value and multiplying the result by 100. For each US state, Yelowitz and Wilson (2014) initially computed a 31-month time series (from January 2011 to July 2013) for the relative popularity of Bitcoin and each clientele grouping. They then used Google Trends to measure relative state-level popularity of each search term for the full period and scaled each state-series relative to the most popular state. This type of analysis has two limits: Google samples its database everytime a query is requested, so that an exact replication is not possible, even though the qualitative results do not change (see also section 4.4. in Fantazzini and Toktamysova (2016) for a discussion of this issue); Google Trends gives a value of zero, if the number of searches it too low[1]. Out of 1488 (48 states$\times$ 31 months) potential observations, Yelowitz and Wilson (2014) used 794 with non-zero values. Following Stephens-Davidowitz (2014), they normalized each search rate to its z-score and estimate the following panel regression:

$$BITCOIN_{jt} = \beta_0 + \beta_1 X_{jt} + \delta_j + \delta_t + \varepsilon_{jt}$$

where $BITCOIN_{jt}$ is Bitcoin interest in state j in month t, X_{jt} is clientele interest, and δ_j and δ_t are state and time fixed effects. Each state-month is weighted by state population in July 2011, and the

[1] https://support.google.com/trends/answer/4355213?hl=en&ref_topic=4365599

standard errors are corrected for non-nested two-way clustering at the state and time levels, see Cameron et al., (2011) for details. Yelowitz and Wilson (2014) employed a large set of model specifications, progressively including additional controls for state and time, control variables like unemployment rate and unrelated 'placebo variables', interaction terms of the original variables with bitcoin prices. Moreover, some specifications were estimated using data from 2012 onwards (when Bitcoin was more popular) or for the 24 US states with at least 20 monthly observations. In all cases, they found a positive association between Bitcoin interest and their two clientele groups of computer programming enthusiasts and those possibly engaged in illegal activity, while no significant association with those interested in the Libertarian ideology or in investment motives.

The work by Yelowitz and Wilson (2014) solved some problems of the analysis by Bohr and Bashir (2014), but it is still related only to the US bitcoin community and its data were collected before the bankruptcy of the exchange Mt.Gox. Nevertheless, it proposed some ideas that will be later included into more complex models suggested for modelling bitcoin price dynamics, and which will be reviewed in section 5.

4 What is bitcoin's fundamental value? A review of financial and economic approaches

The value of bitcoin has been subject to strong volatility over the past years, raising the question of whether it is purely a bubble. One way to answer this question is to use tests for financial bubbles and we will review them in section 6. Another possibility is to try to assess its intrinsic (or fundamental) value. In this regard, two approaches have been proposed so far: market sizing and the (marginal) cost of production based on electricity consumption.

4.1 An upper bound: *Market Sizing*

Market sizing is basically the process of estimating the potential of a market and this is widely used by companies which intend to launch a new product or service. This approach has been recently used by some financial analysts and researchers to get a ballpark estimate for Bitcoin's fair value.

Woo et al. (2013) in a Bank of America Merrill Lynch report estimated separately the value of bitcoin as a medium of exchange and as store of value and then summed them up to get a rough estimate of bitcoin fair value. More specifically, to compute the value as medium of exchange, they considered two uses for bitcoin: *e-commerce* and money transfer. As for the former, they first get an estimate of the money velocity by dividing the US personal consumption (C_{US}) expenditures by the household checking

deposits and cash (HS_{US}) and compute the average of this value over the past 10 years. Then they multiply the money velocity for the total B2C e-commerce sales in the previous year, assuming that the velocity for on-line sales is the same as the velocity for all US household spending. Third, they assume that Bitcoin will grow to account for the payment of 10% of all on-line shopping ($Bitcoin_{share}$), so that they estimated that US households would want to have a balance of $1bn worth of Bitcoins. Finally, given that US GDP was approximately 20% of world GDP, they multiply the previous amount by 5, getting to $5bn worth of Bitcoins for the total global on-line shopping. In formulas, we have:

$$V_{e-commerce_t} = \frac{1}{10}\left(\sum_{i=1}^{10}\frac{C_{US_{t-i}}}{HD_{US_{t-i}}}\right)\cdot \text{B2C}_{t-1}\cdot Bitcoin_{share}\cdot\frac{GDP_{world_{t-1}}}{GDP_{US_{t-1}}}$$

Woo et al. (2013) highlighted that, in addition to its role as a mean for payment for on-line commerce, Bitcoin can be used for *transfer of money*. They considered the three top players in the money transfer industry - Western Union, MoneyGram, and Euronet - (with about 20% of the total market share) and assumed that Bitcoin could become one of the top three players in this industry. They then put forward the strong assumption that Bitcoin's market capitalization could be used as its enterprize value, so that they add the average market capitalization of Western Union, MoneyGram and Euronet (approximately $4.5bn), to the maximum market capitalization of Bitcoin's role as a medium of exchange:

$$V_{money\,transfer_t} = \frac{1}{3}\left(MK_{WU_t} + MK_{MG_t} + MK_{E_t}\right)$$

Woo et al. (2013) suggested that the closest assets to bitcoin as a *store value* are probably precious metals or cash. Particularly, bitcoins and gold share three characteristics: they do not pay any interest, the supply of both is limited, and both are more difficult to trace than most financial assets (except cash). Considering that the outstanding value of gold bar/coins/ETFs (in 2013) was approximately $1.3trn and that bitcoin is much more volatile that gold, Woo et al. (2013) assumed that the market capitalization of Bitcoins cannot go above $300bn: moreover, assuming that Bitcoin were to eventually acquire the reputation of silver and that gold price was (in 2013) approximately 60 times that of silver, they suggested that the Bitcoin market capitalization for its role as a store of value could reach $5bn. Interestingly, they noted that this value is close to the value of the total US silver eagles minted since 1986 (around $8bn - 12k tons). Therefore, a simple rough way to get the Bitcoin market capitalization as a store of value is:

$$V_{store\ of\ value_t} = 0.6\cdot TSM_t\cdot P_{silver,t}$$

where TSM_t is the total sum of all US silver eagles minted since 1986 at time t, while $P_{silver,t}$ is the

price for 1 troy ounce of silver at time t.

Finally, Woo et al. (2013) computed the potential bitcoin fair value as the sum of the maximum market capitalization for Bitcoins for its role as a medium of exchange and as a store of value, divided by the total number of bitcoin in circulation (TB_t), thus obtaining a maximum fair value of Bitcoin approximately equal to $ 1300:

$$P_{bitcoin_t} = \frac{(V_{e-commerce_t} + V_{money\,transfer_t} + V_{store\,of\,value_t})}{TB_t}$$

A different approach for market sizing is employed by Bergstra and de Leeuw (2013), who compared Bitcoin with a high tech startup which will either become dominant on its market or it will fail, following an idea suggested by Yermack (2013). They supposed that if Bitcoin will be successful and survive till 2040, then it will represent half of all money world wide. Given the technical novelty of the Bitcoin system, they assigned a very low probably (p) this to happen: one in a 100.000. Assuming that the total money mass (MM) in 2040 will be 10^{14} Euro (as a pure guess), their estimate for the bitcoin price is

$$P_{bitcoin_t} = \frac{MM_{2040}}{TB_{2040}} \cdot p_t = \frac{10^{14}}{2 \cdot 10^7} \cdot 10^{-5} = 50\ euro$$

Finally, a similar approach is investigated by Huhtinen (2014), who considered the current money aggregates M2 for USD, EUR and JPY, and alternative scenarios for the portion of money supply that could be replaced by bitcoin, instead. He argues that the most realistic replacement level for the three world currencies is 0.1% and it could be achieved with a bitcoin valuation of EUR 1573.

4.2 A lower bound: *the marginal cost of bitcoin production*

Market sizing can give an idea of the bitcoin potential in the medium-long term, but it is clearly unsatisfactory to explain the short term dynamics of the bitcoin price. In this regard, Garcia et al. (2014) were the first to suggest that the fundamental value of one bitcoin should be at least equal to the cost of the energy involved in its production through mining, and this cost should be used as a lower bound estimate of bitcoin fundamental value More specifically, they divided the cumulated mining hash rate in a day by the number of bitcoins mined, to obtain the number of SHA-256 hashes needed to mine one bitcoin. They then used an approximation of the power requirements for mining of 500 W per GHash/s, which was the average efficiency of the most common graphics processing units used to mine bitcoins between 2010 and 2013 (at the end of 2015 this is much lower), and an approximation of electricity costs of \$0.15 KWh^{-1}, which was an average of US and EU prices.

More recently, a more refined model for the cost of bitcoin production was developed by Hayes

(2015a,b) and we discussed it below in details. Hayes (2015a,b) highlights that rational agents would not undertake production of bitcoins if they incurred a real loss in doing so, and the variables to consider to decide whether to mine or not are substantially five: 1) the cost of electricity, measured in cents per kilowatt-hour; 2) the energy consumption per unit of mining effort, measured in watts per GH/s (1 W/GH/s=1 Joule/GH), which is a function of the cost of electricity and energy efficiency; 3) the bitcoin market price; 4) the difficulty of the bitcoin algorithm; 5) the block reward (currently 25 BTC), which halves approximately every four years. In a competitive commodity market, an agent would undertake mining if the marginal cost per day (electricity consumption) were less than or equal to the marginal product (the number of bitcoins found per day on average multiplied by the dollar price of bitcoin). Hayes (2015a,b) argues that the speculative and money-like properties of bitcoin (like mean of exchange and store of value) can surely add a subjective portion to any objective attempt to estimate bitcoin intrinsic value. However, the marginal cost of production determined by energy consumption might set a lower bound in value around which miners will decide to produce or not.

Hayes (2015a,b) develops his model by assuming that a miner's daily production of bitcoin depends on its own rate of return, measured in expected bitcoins per day per unit of mining power. The expected number of bitcoins expected to be produced per day can be calculated as follows:

$$BTC/day^* = [(\beta \cdot \rho)/(\delta \cdot 2^{32})] \cdot sec_{hr} \cdot hr_{day} \tag{1}$$

where β is the block reward (currently 25 BTC/block) , ρ is the hashing power employed by a miner, and δ is the difficulty (which is expressed in units of GH/block). The constant sec_{hr} is the number of seconds in an hour (3600), while hr_{day} is the number of hours in a day (24). The constant 2^{32} relates to the normalized probability of a single hash per second solving a block, and is a feature of the 256-bit encryption at the core of the SHA-256 algorithm which miners try to solve. These constants which normalize the dimensional space for daily time and for the mining algorithm can be summarized by the variable θ, given by $\theta = 24\ \text{hr}_{day} \cdot\ 3600\ /\ 2^{32}\ \text{sec}_{hr} = 0.0000201165676116943$. Equation (1) can thus be rewritten compactly as follows:

$$BTC/day^* = \theta \cdot (\beta \cdot \rho)/\delta \tag{2}$$

Hayes (2015a,b) sets $\rho = 1000$ GH/s even though the actual hashing power of a miner is likely to deviate greatly from this value. However, Hayes (2015a,b) argues that this level tends to be a good standard of measure under current circumstances.

The cost of mining per day, E_{day} can be expressed as follows:

$$E_{day} = (\text{price per kWh} \cdot 24\,hr_{day} \cdot \text{W per GH/s})(\rho/1000\,GH/s) \tag{3}$$

Assuming that the bitcoin market is a competitive market, the marginal product of mining should be equal to its marginal cost, so that the \$/BTC (equilibrium) price level is given by the ratio of (cost/day) / (BTC/day):

$$p^* = E_{day}/(BTC/day^*) \tag{4}$$

This price level can be though as a price lower bound, below which a miner would operate at a marginal loss and would probably stop mining. Alternatively, given the bitcoin market price, Equation (4) can be inverted to find lower bounds (or break-even values - as defined by Hayes (2015a,b)) for the other variables that determine bitcoin profitability. For example, given an observed market price (p) and mining difficulty, the break-even electricity cost in kilowatt-hours is given by

$$\text{price per kWh}^* = [p(BTC/day^*)/24\,hr_{day}]/\text{W per GH/s} \tag{5}$$

Similarly, given a known cost of production and observed market price, one can solve for a break-even level of mining difficulty:

$$\delta^* = (\beta \cdot \rho \cdot sec_{hr} \cdot hr_{day}/[(E_{day}/p) \cdot 2^{32}] \tag{6}$$

Finally, given a market price, cost of electricity per kilowatt-hour, and mining difficulty, we can find the break-even energy efficiency,

$$\text{W per GH/s}^* = [p(BTC/day^*)/(\text{price per kWh} \cdot 24hr_{day})] \tag{7}$$

Equation (4) shows that if real-world mining efficiency will increase (as it is widely expected due to more efficient mining hardware), the break-even price for bitcoin producers will tend to decrease. For example, Garcia et al (2014) found that the average mining efficiency over the period 2010-2013 was approximately 500 Watts per GH/s, while currently, if we use equation (7) or look at the best mining hardware available[2], the average energy efficiency seem to be close to 0.60-0.90 Watts per GH/s. Moreover, equations (2) and (4) show that a smaller block reward β, everything else remaining the same, will increase the bitcoin price: given that the block reward is expected to be halved in 2016 down to 12.5 BTC, if the bitcoin price will not increase, this will indicate that the energy mining efficiency will

[2] `https://en.bitcoin.it/wiki/Mining_hardware_comparison`

have compensated the decreased block reward. In this regard, a small numerical example can be of help: suppose that the world average electricity cost is approximately 13.5 cents/KWh (as in Hayes 2015b) and the average energy efficiency of bitcoin mining hardware is 0.75 J/GH. Then, the average cost per day for a 100 GH/s mining rig would be approximately equal to $(0.135 \cdot 24 \cdot 0.75) \cdot (1{,}000\ /1{,}000) =$ \$243/day. The number of bitcoins that a 100 GH/s of mining power can find in a day with a current difficulty of 60883825480 is equal to 0.0082602265269544 BTC/day. Given that the marginal cost and the marginal product should be theoretically equivalent, the \$/BTC price is given by equation (4): (2.43 \$/day) / (0.0082602265269544 BTC/day) $\approx$ \$294.18/BTC, which is not too far from the current market values of \$290-\$300/BTC. Interestingly, if we keep the previous data and we halve the Bitcoin reward to 12.5 BTC, the bitcoin fair price should be $\approx$ \$588.36/BTC: will we see a rally in the next months?

5 Modelling bitcoin price dynamics

Almost all empirical analyses devoted to bitcoin prices employed time series methods. However, a small number of studies used simple cross-sectional regressions which may prove useful because crypto-currencies are very recent, highly speculative and volatile, so that time series methods can be misleading and uninformative given the short time span involved (Hayes, 2015b). For sake of generality, we review both approaches.

5.1 Econometric analyses with cross-section data

Hayes (2015b) performed a regression using a cross-sectional dataset consisting of 66 traded digital currencies (known collectively as *altcoins*) based on a theoretical model developed in Hayes (2015c). The natural logarithm of the altcoin market prices on September 18, 2014 -express in terms of bitcoins- was regressed against a set of five variables:

- the natural logarithm of the *computational power in Giga-Hashes per second*;
- the natural logarithm of the *number of (alt-)coins found per minute*, computed by dividing the reward for each mined block and the time between blocks;
- *the percentage of coins that have been mined thus far* compared to the total that can ever be found;
- a dummy variable for which *computational algorithm* is employed ('0' for SHA-256 and '1' for scrypt).
- the *number of calendar days from inception of the altcoins* through September 18, 2014.

Hayes (2015b) found that a higher computational power employed in mining for a cryptocurrency, the higher its price: this result can be expected given that the amount of mining power is a proxy for the overall use of the altcoin considered. Moreover, a rational miner would only seek to employ mining resources if the marginal price of mining exceeded the marginal cost of mining. Hayes (2015b) also found that the number of 'coins' found per minute is negatively correlated to the altcoin price, which is expected given that scarcity per mined block tend to lead to a greater perceived value. Another interesting result is that the altcoins based on the scrypt algorithm are more valuable than those based on SHA-256d, *ceteris paribus*. The former algorithm was proposed as a solution to prevent specialized hardware from brute-force efforts to out-mine others for bitcoins, so that it requires more computing effort per unit than the equivalent altcoin using SHA-256. Instead, Hayes (2015b) found that the percentage of altcoins mined thus far compared to what is left to be mined has not statistical influence on the altcoin price: he suggests that this is due to the fact that altcoins can be divisible down to 8 decimal places by construction, and that number of decimal places can be increased, potentially without limit. It is our opinion, instead, that the most likely reason is rather the possibility to increase the total altcoin money supply, provided a majority of miners agree. Hayes (2015b) also found that the longevity of the cryptocurrency is not related to altcoin price, which may be due the very short time span considered (the vast majority of altcoins are less than two years old).

In general, these results can be of great interest to those who want to introduce a successful altcoin: necessary conditions seem to be the adoption of the scrypt algorithm (or another even more difficult protocol) and keeping the number of coins found per minute at a relative low level, which can be accomplished by increasing the time needed to mine a single block and by reducing the reward per each new block successfully mined. Instead, increasing the computational power dedicated to the altcoin mining is more difficult and partially out of the control of the altcoin creator, unless very large (and expensive) investments are made in the altcoin IT infrastructure.

5.2 Econometric analyses with time series data

Kristoufek (2013) is the first author to propose a multivariate approach which focused on the speculative component of the Bitcoin value, showing that both the bubble and bust cycles of Bitcoin prices can be partially explained by investors' interest in the currency. In this regard, the numbers of search queries on Google Trends and Wikipedia are used as proxies for investors' interest and attention. More specifically, Kristoufek (2013) employed a bivariate Vecto-AutoRegression (VAR) model for the weekly log-returns of bitcoin prices and Google Trends data,

$$\Delta \mathbf{Y}_{t-1}=\alpha+\Phi_1\Delta \mathbf{Y}_{t-1}+\Phi_2\Delta \mathbf{Y}_{t-2}+...+\Phi_p\Delta \mathbf{Y}_{t-p}+\varepsilon_t \tag{8}$$

and a bivariate Vector Error Correction (VEC) model for the daily bitcoin log-prices and Wikipedia search data,

$$\Delta \mathbf{Y}_{t-1}=\alpha+\mathbf{B}\Gamma \mathbf{Y}_{t-1}+\zeta_1\Delta \mathbf{Y}_{t-1}+\zeta_2\Delta \mathbf{Y}_{t-2}+...+\zeta_{p-1}\Delta \mathbf{Y}_{t-(p-1)}+\varepsilon_t \tag{9}$$

where $\mathbf{B}$ are the factor loadings while Γ represents the cointegrating vector. Moreover, Kristoufek (2013) employed a trivariate VECM with bitcoin log-prices and two variables - Q_t^+ and Q_t^- - measuring positive and negative feedback, respectively:

$$\begin{aligned} Q_t^+ &= Q_t \mathbf{1}_{\left(P_t-\frac{1}{N}\sum_{i=1}^{N}P_{t-i+1}\right)>0} \\ Q_t^- &= Q_t \mathbf{1}_{\left(P_t-\frac{1}{N}\sum_{i=1}^{N}P_{t-i+1}\right)<0} \end{aligned} \tag{10}$$

where Q_t is the Google/Wikipedia search data at time t and $\mathbf{1}$ is an indicator function equal to 1 if the condition in $(\cdot)$ is met and 0 otherwise, while N is the number of periods taken into consideration for the moving average (N=4 weeks for Google Trends, N=7 days for Wikipedia). Kristoufek (2013) suggested these two variables can be used as proxies for search-term activity connected with positive (Q_t^+) and negative (Q_t^-) feedback.

Kristoufek (2013) found a significant bidirectional relationship, where search queries influence prices and viceversa, suggesting that speculation and trend chasing dominate the bitcoin price dynamics. Interestingly, he found that when prices are higher than the recent trend, this will increase investors' attention, and this action will further increase prices. Similarly, when prices are below their recent trend, the growing investors' interest will push prices further down: needless to say, such a market may often give rise to price bubbles, as we will review at length in section 6.

Garcia et al. (2014) extend the set of variables used by Kristoufek (2013) by considering a dataset consisting of price data, social media activity, search trends and user adoption of Bitcoin. More specifically, they considered the following variables:

- the *number of new Bitcoin users* adopting the currency at time t, proxied by the number of downloads of the Bitcoin software client;
- the *bitcoin price* expressed in three world currencies (USD, EUR and CNY);
- *information search*, proxied by normalized daily Google search data (or by daily views of the Bitcoin wikipedia webpage as a robustness check);

- *information sharing* (or *online word-of-mouth communication*) proxied by the daily number of Bitcoin-related tweets B_t per million messages in the Twitter feed T_t, calculated as $(B_t/T_t)\times 10^6$. These data were downloaded from `http://topsy.com` and considered the daily number of tweets containing at least one of the following terms: 'BTC', '#BTC', 'bitcoin' or '#bitcoin' . As a robustness check, Garcia et al. (2014) also considered an alternative measure of information sharing represented by the number of 'reshares' of the messages posted on the oldest, regularly active public Facebook page dedicated to Bitcoin.

Garcia et al. (2014) estimated a four-variate VAR(1) model with first-differenced data ranging from January 2009 up to October 2013 and found two positive feedback loops: a reinforcement cycle between search volume, word of mouth and price -which they called *social cycle*-, and a second cycle between search volume, number of new users and price -denoted as *user adoption cycle*-. The first cycle shows that increasing Bitcoin popularity leads to higher search volumes, which leads to increased social media activity, which then stimulates the purchase of bitcoins by individual users, thus driving the prices up and eventually feeding back on search volumes. The second cycle shows that new Bitcoin users download the software client after getting information online about the Bitcoin technology. The increase in the number of users subsequently drives prices up, given that the number of bitcoins does not depend on demand but grows with time in a determined fashion. Garcia et al. (2014) also found a negative relation from online searches to prices, showing that three of the four largest daily price drops were preceded by the large increases in Google search volume the day before. In this regard, they showed that online search activity responds faster to negative events than prices, so that search spikes are early indicators of price drops. A set or robustness checks confirmed the previous findings.

Garcia and Schweitzer (2015) extended the previous VAR(1) model with additional social signals but, more interestingly, for the first time they implemented an algorithmic trading strategy based on this VAR model, showing the possibility of high profits, even taking risk and trading costs into account. More specifically, they used the following variables ranging between February 2011 and December 2014:

- the daily *closing bitcoin prices* of each day t at 23.59 GMT from `coindesk.com`;
- the *daily volume* of BTC exchanged in 80 online markets for other currencies from `bitcoincharts.com`.
- the *daily amount of Block Chain transactions*, as measured by `blockchain.info` every day at 18.15.05 UTC, which they approximated to 00.00 GMT of the next day.
- the amount of downloads of the most popular Bitcoin client from `http://sourceforge.net/projects/bitcoin`;
- the *normalized daily Google trends search volume* for the term 'bitcoin';

- *the daily amount of unique tweets about Bitcoin* binned in 24-hour windows starting at 00.00 GMT using data from `topsy.com` ;

- the *average daily valence of Bitcoin-related tweets*: in psychological research, valence aims at quantifying the degree of pleasure or displeasure of an emotional experience, see Bradley and Lang (1999), Russell (2003), Garcia and Schweitzer (2012) for more details. Garcia and Schweitzer (2015) measured the average daily valence using the lexicon technique proposed by Warriner et al. (2013), which improves the previous ANEW lexicon method by Bradley and Lang (1999) with more than 13000 valence-coded words. They computed the daily average Twitter valence about Bitcoin for day t in two steps: first, they measure the frequency of each term in the lexicon during that day, and second, they computed the average valence weighting each word by its frequency.

- the *daily polarization of opinions in Twitter around the Bitcoin topic*, computed as the geometric mean of the daily ratios of positive and negative words per Bitcoin-related tweet. Opinion polarization tries to measure the semantic orientation of words into positive and negative evaluation terms, see Osgood (1964). Garcia and Schweitzer (2015) used the LIWC psycholinguistics lexicon-based method by Pennebaker et al. (2007) and expand its lexicon of stems into words by matching them against the most frequent English words of the Google Books dataset, see Lin et al. (2012) for details. In the end, Garcia and Schweitzer (2015) considered 3463 positive and 4061 negative terms. It is important to remark that polarization can be considered a complementary dimension to emotional valence, because it measures the simultaneous coexistence of positive and negative subjective content, rather than its overall orientation, see Osgood (1964), Tumarkin and Whitelaw (2001).

Garcia and Schweitzer (2015) found that only valence, polarization and trading volume have significant effects on bitcoin price. These selected variables are then used to implement several trading strategies, which are then compared to traditional strategies like the Buy and Hold strategy, the Momentum strategy (that predicts that price changes at time $t+1$ will be the same as at time t), and several others, see Garcia and Schweitzer (2015) for details. They found that a combined strategy involving the previous three variables is the best one over their back-testing period, even when taking risk and trading costs into account. To our knowledge, the work by Garcia and Schweitzer (2015) is the only one so far which performed a large-scale forecasting back-testing analysis.

Buchholz et al. (2012) expanded the set of variables which may affect the bitcoin price, considering not only BitCoin attractiveness -measured by Google Trends data-, but also accounting for the impacts of BitCoin supply and demand. To measure the latter, they considered the total supply of bitcoins in existence, the total number of bitcoin transactions per day, the total value of bitcoin transactions

(measured in bitcoins) per day, and the average value of transactions in bitcoins per day (given by total transaction value divided by total number of transactions). Unfortunately, Buchholz et al. (2012) employed only bivariate VAR and VEC models without using the full set of variables, potentially leading to an omitted-variable bias. They also computed a GARCH-in-mean model, where they consider the volatility component in the mean equation as a proxy for demand for bitcoins; however, the lack of control variables in the mean equation is again rather problematic. Moreover, several interesting variables which were discussed at the beginning of their work (like the data on historical news articles and blogs from *LexisNexis*) were not examined in their empirical analysis. Despite these shortcomings, the work by Buchholz et al. (2012) can be considered a seminal paper since it provided several important hints which were later included in subsequent broader analyses.

Glaser et al. (2014) extended previous research by studying the aggregated behavior of new and uninformed Bitcoin users within the time span from 2011 to 2013, to identify why people gather information about Bitcoin and their motivation to subsequently participate in the Bitcoin system. The main novelty is the use of regressors that are related to both bitcoin **attractiveness** and bitcoin **supply and demand**. More specifically, they used the following variables:

- *daily BTC price data*,
- *daily exchange volumes* in BTC,
- *Bitcoin network volume*, which includes all Bitcoin transfers caused by monetary transactions within the Bitcoin currency network,
- *daily views on the English Bitcoin Wikipedia page* as a proxy for measuring user attention,
- *dummy variables for 24 events gathered from* `https://en.bitcoin.it/wiki/History`, including significant events that may have affected the Bitcoin community. The events focus either on exceptional positive (new exchange launches, legal successes or significant news articles) or negative (major system bugs, thefts, hacks or exchange breakdown) news which are directly related to the Bitcoin system, security and infrastructure.

Glaser et al. (2014) are the first to consider both exchange (EV) and network volumes (NV): their idea is that if a customer want to buy bitcoin to pay for goods or services, exchange and network volumes will share similar dynamics, otherwise only exchange-based volumes will be affected. To verify this hypothesis, they employed the following auto-regressive model augmented with the previous lagged variables and GARCH effects:

$$\begin{aligned}
&\Delta Y_t = a_0 + \sum_{i=1}^{7} a_i \Delta EV_{t-i} + \sum_{j=1}^{7} a_{j+7} \Delta NV_{t-j} + a_{15} \Delta Wiki_{t-1} + \sum_{j=16}^{n} a_j \Delta C_{j,t-1} + \varepsilon_t \\
&\varepsilon_t \sim N(0, h_t) \\
&h_t = b_0 + b_1 \varepsilon_{t-1}^2 + b_2 h_{t-1}
\end{aligned} \tag{11}$$

where Δ represents the first difference operator, Y_t stands for either Bitcoin network or exchange volume, *Wiki* for the Wikipedia Bitcoin traffic and C_j represents lagged returns for the previous control variables, and for lagged exchange or network volume. The conditional volatility follows a GARCH(1,1) process. They found that the both increases in Wikipedia searches and in exchange volumes do not impact network volumes, and there is no migration between exchange and network volumes, so that they argued that (uninformed) users mostly stay within exchanges, holding Bitcoin only as an alternative investment and not as a currency. In a second step, they used a similar approach to analyze bitcoin returns:

$$\begin{aligned}
&r_t = a_0 + \sum_{i=1}^{7} a_i r_{t-i} + a_8 \Delta Wiki_{t-1} + a_9 Igood_t + a_{10} Ibad_t + \sum_{j=11}^{n} a_j \Delta C_{j,t-1} + \varepsilon_t \\
&\varepsilon_t \sim N(0, h_t) \\
&h_t = b_0 + b_1 \varepsilon_{t-1}^2 + b_2 h_{t-1}
\end{aligned} \tag{12}$$

where r_t is the open-to-close Bitcoin return at date t, while $Igood_t$ and $Ibad_t$ are event dummies for positive and negative news. Glaser et al. (2014) found that Bitcoin users seem to be positively biased towards Bitcoin, because important negative events, like thefts and hacks, did not lead to significant price corrections.

Bouoiyour and Selmi (2015), Bouoiyour et al. (2015) and Kancs et al. (2015) are the first studies to consider three sets of drivers to model bitcoin price dynamics: **technical drivers (bitcoin supply and demand)**, **attractiveness indicators** and **macroeconomic variables**.

The variables used by Bouoiyour and Selmi (2015) and their descriptions are presented in table 1.

Bouoiyour and Selmi (2015) investigated the long-run and short-run relationships between bitcoin prices and the previous set of variables by using the auto-regressive distributed lag (ARDL) bounds testing procedure proposed proposed by Pesaran and Shin (1999). This approach has several advantages: first, it is a single-equation cointegration method which can be estimated by OLS; second, it allows to model both short-run and the long-run dynamics; third, this procedure can be used irrespective of whether the underlying regressors are I(0) [i.e. stationary], I(1) [i.e. not-stationary], or fractionally integrated. Lastly, it is a relatively more efficient estimation method in small samples compared to alternative cointegration methods. However, this procedure will not work with I(2) regressors, when there is more than 1 cointegration relationship or with endogenous regressors. The ARDL model employed by Bouoiyour and Selmi (2015) is reported below:

Variable	***Explanation***
	Technical drivers
The exchange-trade ratio (ETR)	Bitcoins are used primarily for two purposes: purchases and exchange rate trading. The Blockchain website provides the total number of transactions and their volume excluding the exchange rate trading. In addition, the ratio between volume of trade (primarily purchases) and exchange transactions is also provided.
Bitcoin monetary velocity (MBV)	It is the frequency at which one unit of bitcoin is used to purchase tradable or non-tradable products for a given period. In the Bitcoin system, the monetary velocity of BitCoin circulation is proxied by the so-called *BitCoin days destroyed*. This variable is calculated by taking the number of BitCoins in transaction and multiplying it by the number of days since those coins were last spent.
The estimated output volume (EOV)	It is similar to the total output volume with the addition of an algorithm which tries to remove change from the total value. This estimate should reflect more accurately the true transaction volume. A negative relationship between the estimated output volume and bitcoin price is expected.
The Hash Rate	The estimated number of giga-hashes per second (billions of hashes per second) the bitcoin network is performing. It is an indicator of the processing power of the Bitcoin network
	Attractiveness indicators
Investors' attractiveness (TTR)	daily Bitcoin views from Google, because it is able to properly depict the speculative character of users
	Macroeconomic variables
The gold price (GP)	Bitcoin does not have an underlying value derived from consumption or production process such as gold.
The Shangai market index (SI)	The Shangai market is considered one of the biggest player in Bitcoin economy and it is considered as a potential source of Bitcoin price volatility.

Table 1: Drivers of bitcoin price (BPI) employed by Bouoiyour and Selmi (2015)

$$\begin{aligned}\Delta \ln BPI_t = a_0 + \sum_{i=1}^{n} a_{1i}\Delta \ln BPI_{t-i} + \sum_{i=0}^{m} a_{2i}\Delta \ln TTR_{t-i} + \sum_{i=0}^{l} a_{3i}\Delta \ln ETR_{t-i} + \sum_{i=0}^{h} a_{4i}\Delta \ln MBV_{t-i} + \\ + \sum_{i=0}^{v} a_{5i}\Delta \ln EOV_{t-i} + \sum_{i=0}^{r} a_{6i}\Delta \ln HASH_{t-i} + \sum_{i=0}^{s} a_{7i}\Delta \ln GP_{t-i} + \sum_{i=0}^{z} a_{8i}\Delta \ln SI_{t-i} + \\ + b_1 \ln BPI_{t-1} + b_2 \ln TTR_{t-1} + b_3 \ln ETR_{t-1} + b_4 \ln MBV_{t-1} + b_5 \ln EOV_{t-1} + b_6 \ln HASH_{t-1} + \\ + b_7 \ln GP_{t-1} + b_8 SI_{t-1} + \varepsilon_t \end{aligned} \tag{13}$$

Using a dataset spanning between 05/12/2010 and 14/06/2014, Bouoiyour and Selmi (2015) found that in the short-run, the investors attractiveness, the exchange-trade ratio, the estimated output volume and the Shangai index have a positive and significantly impact on Bitcoin price, while the monetary velocity, the hash rate and the gold price have no effect. Instead, in the long-run, only the exchange-trade ratio and the hash rate have a significant impact on bitcoin price dynamics. These results hold also with the inclusion of a dummy variable to account for the bankruptcy of a major Chinese bitcoin trading company in 2013, with oil prices, the Dow Jones index and a dummy variable to consider the closure of the Road Silk by the FBI in October 2013. Similar results are also provided by the variance decomposition for the Bitcoin price and Granger-causality tests computed using a VEC model (however,

the coefficient estimates for this latter model are not reported).

Kancs et al. (2015) employs a full multivariate VEC model as in (9), similarly to Kristoufek (2013), using daily data for the 2009-2014 period. However, differently from the latter work and in the same line of research of Bouoiyour and Selmi (2015), they considered three types of drivers to model bitCoin price dynamics: bitcoin supply and demand, bitcoin attractiveness, and global macroeconomic and financial factors. The variables used by Kancs et al. (2015) and their descriptions are presented in table 2.

Variable	***Explanation***
Bitcoin supply and demand	
Number of bitcoins	The historical number of total BitCoins which have been mined to account for the total stock of BitCoins in circulation.
Number of transactions	Number of unique BitCoin transactions per day
Number of addresses	Number of unique BitCoin addresses used per day
Days destroyed (monetary velocity)	BitCoin days destroyed for any given transaction, calculated by taking the number of BitCoins in a transaction and multiplying it by the number of days since those coins were last spent
Attractiveness indicators	
Views on Wikipedia	Volume of daily BitCoin views on Wikipedia. It is a good measure of potential investors' interest, but it does not differentiate on whether the information is used to guide investment decisions or online BitCoin denominated exchange of goods and services
New members	It is the number of new members on online BitCoin forums extracted from *bitcointalk.org* . It captures the size of the BitCoin economy but also attention-driven investment behavior of new BitCoin members
New posts	It is the number of new posts on online BitCoin forums extracted from *bitcointalk.org* . It captures the effect of trust and/or uncertainty, as it represents the intensity of discussions among members.
Macroeconomic variables	
Exchange rate	Exchange rate between the US dollar and the Euro. It is chosen because the bitcoin price is expressed in dollars
Oil price	Oil prices are extracted from the US Energy Information Administration[3]
Dow Jones	Dow Jones stock market index

Table 2: Drivers of bitcoin price employed by Kancs et al. (2015).

In terms of short-run effects, Kancs et al. (2015) found that bitcoin prices are influenced by its own lagged prices, the total number of bitcoins in circulation, by bitcoin monetary velocity and Wikipedia views. In terms of long-run effect, bitcoin demand related variables (e.g. days destroyed, number of addresses) seem to have a stronger impact on bitcoin price than supply side drivers (e.g. number of bitcoins). As expected by theory, an increase of the number of bitcoins in circulation leads to a decrease in bitcoin price, whereas an increase in the size of the bitcoin economy (proxied by the number of addresses) and its velocity lead to an increase in bitcoin price. The variables related to bitcoin attractiveness have the strongest and statistically the most significant impact on bitcoin price: the number of new members has a negative impact on bitcoin price, implying that attention-driven investment behavior

of new investors dominates, whereas the number of new posts has a positive impact on bitcoin price, reflecting an increasing acceptance and trust in the Bitcoin system. Similarly to Kristoufek (2013), the number of Wikipedia views has a statistically significant and positive effect on bitcoin prices. Kancs et al. (2015) found that all macroeconomic variables considered do not significantly affect BitCoin price in the long-run, thus confirming similar evidence in Bouoiyour and Selmi (2015) and supporting the idea of Yermack (2013) that bitcoin is relatively ineffective as a tool for risk management against adverse market developments and it cannot be easily hedged against other assets that are driven by macroeconomic developments. In general, the results reported in Kancs et al. (2015) confirms that bitcoin attractiveness factors are still the main drivers of bitcoin price, followed by traditional supply and demand related variables, while global macro-financial variables play no role. Kancs et al. (2015) stressed that he speculative short-run behavior of bitcoin investors may not be not necessarily an undesirable activity (absorbing excess risk from risk averse participants and providing liquidity on the BitCoin market), but it may increase price volatility and create price bubbles as well as causing extensive hoarding of bitcoins.

Differently from the previous works, Kristoufek (2015) and Bouoiyour et al. (2015) analyzed the bitcoin price from a frequency domain perspective. Kristoufek (2015) used a continuous wavelet approach (wavelet coherence) to examine the evolution of correlations over time [14/09/2011-28/02/2014] and over different frequencies between the bitcoin price and a wide set of variables, including supply-demand fundamentals, speculative and technical drivers. He found out that fundamental factors such as the trade-exchange ratio and the bitcoin supply play substantial roles in the long-run. Interestingly, the Chinese stock index is an important source of Bitcoin price evolution, while the contribution of gold price dynamics seems minor. Moreover, he finds that bitcoin prices are also driven by investors' online interest, which is driving prices further up during episodes of explosive prices, and further down during rapid price declines, similarly to what found by Kristoufek (2013) and Garcia et al. (2014). Unfortunately, this kind of analysis suffers from some drawbacks as highlighted by Bouoiyour et al. (2015): noisy data, such as bitcoin prices, may strongly bias the estimated relationships, and this bias may even be magnified in a time–frequency framework, see Ng and Chan (2012) for a larger discussion. Moreover, a wavelet analysis with only two variables like in Kristoufek (2015) has a problem similar to a simple regression without control variables where the estimated parameters can be strongly biased. These issues stimulated Bouoiyour et al. (2015) to use the conditional frequency-domain Granger causality approach proposed by Breitung and Candelon (2006). This approach allows to use several potential control variables and it can distinguish between long-run trends, business cycles or short-run dynamics. Besides, it shows the presence of causal links between two variables even in case of non-linear dependence, and it is robust to the presence of volatility clustering, see Bodart and Candelon (2009). Given the importance of this method, we describe it in details below.

Let consider z_t=$[x_t, y_t]$ be a two-dimensional time series vector with the following finite-order VAR representation:

$$\Theta(L)z_t = \varepsilon_t \tag{14}$$

where $\Theta(L) = I - \Theta_1 L - \cdots - \Theta_p L^p$ is a 2×2 lag polynomial, the vector error term ε_t is a multivariate white noise with $E(\varepsilon_t) = \mathbf{0}$ and $E(\varepsilon_t \varepsilon_t') = \mathbf{\Sigma}$, where $\mathbf{\Sigma}$ is positive definite, and deterministic terms are not considered for ease of exposition. Let $\mathbf{G}$ be the lower triangular matrix of the Cholesky decomposition $\mathbf{G'G}$=$\mathbf{\Sigma}^{-1}$ such that $E(\eta_t \eta_t) = I$ and η_t=$\mathbf{G}\varepsilon_t$. If the system (13) is assumed to be stationary, the MA representation is given by

$$z_t = \Phi(L)\varepsilon_t = \begin{bmatrix} \Phi_{11}(L)\ \Phi_{12}(L) \\ \Phi_{21}(L)\ \Phi_{22}(L) \end{bmatrix} \begin{bmatrix} \varepsilon_{1t} \\ \varepsilon_{2t} \end{bmatrix} = \begin{bmatrix} \Psi_{11}(L)\ \Psi_{12}(L) \\ \Psi_{21}(L)\ \Psi_{22}(L) \end{bmatrix} \begin{bmatrix} \eta_{1t} \\ \eta_{2t} \end{bmatrix} \tag{15}$$

Using this representation, the spectral density of x_t can be expressed as follows:

$$f_x(\omega) = \frac{1}{2\pi} \left\{ |\Psi_{11}(e^{-i\omega})|^2 + |\Psi_{12}(e^{-i\omega})|^2 \right\} \tag{16}$$

and the measure of causality suggested by Geweke (1982) is defined as

$$M_{y \to x}(\omega) = \log \left[\frac{2\pi f_x(\omega)}{|\Psi_{11}(e^{-i\omega})|^2} \right] = \log \left[1 + \frac{|\Psi_{12}(e^{-i\omega})|^2}{|\Psi_{11}(e^{-i\omega})|^2} \right] \tag{17}$$

If the measure $|\Psi_{12}(e^{-i\omega})|$=0, then y does not Granger cause x at frequency ω . A similar derivation can be obtained if z_t are I(1) and co-integrated, see Breitung and Candelon (2006) for more details. Breitung and Candelon (2006) proposed a simple approach to test for the null hypothesis of non-causality (i.e. $\Psi_{12}(e^{-i\omega})|$=0 using,

$$\Psi_{12}(L) = -\frac{g^{22}\Theta_{12}(L)}{|\Theta(L)|}$$

where g^{22} is the lower diagonal element of $\mathbf{G}^{-1}$ and $|\Theta(L)|$ is the determinant of $\Theta(L)$. It follows that y does not cause x at frequency ω if

$$|\Theta_{12}(e^{-i\omega})| = \left| \sum_{k=1}^{p} \theta_{12,k} \cos(k\omega) - \sum_{k=1}^{p} \theta_{12,k} \sin(k\omega) i \right| = 0$$

where $\theta_{12,k}$ is the (1,2)-element of Θ_k . It follows that a necessary and sufficient set of conditions for $|\Theta_{12}(e^{-i\omega})|$=0 is given by

$$\sum_{k=1}^{p} \theta_{12,k} \cos(k\omega) = 0 \quad (18)$$

$$\sum_{k=1}^{p} \theta_{12,k} \sin(k\omega) = 0 \quad (19)$$

Since $\sin(k\omega)=0$ for $\omega=0$ and $\omega=\pi$, restriction (19) can be dropped in these cases. Breitung and Candelon (2006) proposed to test the linear restriction (18) and (19) by rewriting the VAR equation for x_t as follows:

$$x_t = \alpha_1 x_{t-1} + ... + \alpha_p x_{t-p} + \beta_1 y_{t-1} + ... + \beta_p y_{t-p} + \varepsilon_t \quad (20)$$

The null hypothesis of no granger causality at frequency ω $M_{y\to x}(\omega)=0$ is equivalent to testing the following linear restrictions

$$H_0 : R(\omega)\beta = 0 \quad (21)$$

where $\beta=[\beta_1,..., \beta_p]'$ and

$$R(\omega) = \begin{bmatrix} \cos(\omega) & \cos(2\omega) & \cdots & \cos(p\omega) \\ \sin(\omega) & \sin(2\omega) & \cdots & \sin(p\omega) \end{bmatrix}$$

The ordinary F-statistic for (21) is asymptotically distributed as $F(2,T-2p)$ for $\omega\in(0,\pi)$. Such a method can be similarly extended to cointegrated VARs by replacing x_t in regression (20) with Δx_t, whereas the right-hand side of the equation remaining the same, see Breitung and Candelon (2006, 2007) for more details. Interestingly, in the case the set of variables have a different order of integration [for example $x_t \sim I(0)$ and $y_t \sim I(1)$], or simply there is uncertainty about the cointegration rank, Breitung and Candelon (2006) suggested to follow the approach by Toda and Yamamoto (1995) and Dolado and Lu tkepohl (1996): they showed that the Wald test of restrictions involving variables which may be integrated or cointegrated of an arbitrary order, has a standard asymptotic distribution if the VAR model with optimal lag length k is augmented with a redundant number of lags d_{max} , where d_{max} is the maximal order of integration that we suspect might occur in the our set of variables. The coefficient matrices of the last d_{max} lagged vectors in the model can be ignored and we can test linear or nonlinear restrictions on the first k coefficient matrices using the standard asymptotic theory. This approach can also be used to establish standard inference for the frequency domain causality test.

The approach in (20) can be easily extended to test for causality in higher dimensional systems. For

example, if we add a third variable in (20) so that we get,

$$x_t = \alpha_1 x_{t-1} + ... + \alpha_p x_{t-p} + \beta_1 y_{t-1} + ... + \beta_p y_{t-p} + \gamma_1 z_{t-1} + ... + \gamma_p z_{t-p} + \varepsilon_t \tag{22}$$

To test the null hypothesis of conditional Granger causality $M_{y \to x|z}(\omega)=0$, we can use the usual F-statistic to test the linear restrictions (21) on the parameter vector $\beta=[\beta_1,..., \beta_p]'$. However, Hosoya (2001) showed that the specification in (22) may give spurious inference on causality in some cases and he suggested to use the F-statistic to test the linear restrictions (21) in the following modified regression:

$$x_t = \alpha_1 x_{t-1} + ... + \alpha_p x_{t-p} + \beta_1 y_{t-1} + ... + \beta_p y_{t-p} + \gamma_0 w_t + \gamma_1 w_{t-1} + ... + \gamma_p w_{t-p} + \varepsilon_t \tag{23}$$

where w_t are the residuals from a regression of z_t on x_t, y_t and the past lags of all these variables.

Bouoiyour et al. (2015) used the previous frequency-domain framework to test for unconditional [i.e. using the specification in (20)] and conditional Granger causality [i.e. using the specification in (22)] with bitcoin prices and a set of explanatory variables, to investigate the main factors influencing bitcoin price dynamics under different frequencies. First, they showed that bitcoin prices (BPI) Granger-causes the exchange-trade ratio (ETR) in the short- and the medium-run cyclical component, whereas the null hypothesis of no Granger causality from ETR to BPI is not rejected at any frequency. This last result is different from what found by Kristoufek (2015), who found a significant causality from ETR to BPI, which becomes stronger in the long term. The results by Bouoiyour et al. (2015) did not change when moving from unconditional causality to conditional causality analysis, where the employed control variables were the Chinese market index and the hash rate.

Bouoiyour et al. (2015) also found that investors' attractiveness (TTR) -as proxied by Google search data- Granger causes bitcoin price at higher frequencies, which can be expected because the interest in the Bitcoin system tends to increase gradually over time. Instead, the reverse causal causality from BPI to TTR is significant at the lower frequencies, which may indicate that investors buy bitcoins mainly for speculative reasons. Interestingly, these results changed considerably when the Hash rate and the Chinese stock market index were considered as control variables in a conditional causality analysis: in this case, there was no significant causal relationship from BPI to TTR, while the reverse causality from TTR to BPI was significant at both lower and higher frequencies. This evidence highlights the importance of the Chinese market and the Bitcoin technology in explaining these causalities: the former may strongly influence short term speculative activities, while the latter may imply that higher investors' interest increases the amount of hardware devoted to bitcoin mining , thus resulting in a higher technical difficulty and subsequent higher bitcoin prices to cover the increased computational and power costs. Robustness checks including additional control variables such as the monetary Bitcoin velocity and the

estimated output volume do not change substantially the previous evidence. These findings are quite similar to those reported by Kristoufek (2015).

In general, the analyses performed using frequency domain-based methods confirmed that the main drivers of bitcoin price dynamics are still mainly of speculative nature. However, there are several other significant factors involved, not all of them related to speculation, and the possibility to see the bitcoin technology employed for a much larger fraction of business transactions in the long term cannot be excluded.

Finally, we remark that there are also other papers which tried to model bitcoin price dynamics. However, they are less comprehensive than the previous ones, the datasets are smaller and almost all of them are not peer-reviewed. We refer the interest reader to the *bitcoinwiki* webpage devoted to "*publications including research and analysis of Bitcoin or related areas*" available at `https://en.bitcoin.it/wiki/Research` for more details.

6 Detecting Bubbles and explosive behavior in bitcoin prices

The strong volatility in bitcoin prices has sparked a strong debate whether a "substantial speculative component" (Dowd, 2014) can be an harbinger of a large financial bubble. Several statistical tests have been developed for testing the existence of financial bubbles and some of them have been recently used with bitcoin prices. These tests can be broadly grouped into two large families: tests intended to detect a single bubble, and tests intended to detect (potentially) multiple bubbles.

6.1 Testing for a single bubble

MacDonell (2014) was the first to test for the presence of a bubble in bitcoin prices using the Log Periodic Power Law (LPPL) approach proposed by Johansen et al. (2000) and Sornette (2003a,b). We describe below its main structure, while we refer the interested reader to the previous three works as well as to the recent survey by Geraskin and Fantazzini (2013) for more details.

The Johansen-Ledoit-Sornette (JLS) model considers the presence of two types of agents in the market: traders with rational expectations and "noise" traders, who represent irrational agents with herding behavior. Moreover, traders are organized into networks and can have only two states (buy or sell), while their trading actions depend on the decisions of other traders and on external shocks. Over time, agents can then create groups with self-similar behavior which can determine a bubble situation, which is considered a situation of "order", compared to the "disorder" of normal market conditions. According to this model, a bubble can be a self-sustained process due to the positive feedbacks generated by the increasing risk and the agents' interactions, see Geraskin and Fantazzini (2013) for details. A

textbook presentation of LPPLs for bubble modelling is given by Sornette (2003a), while the ex-ante diagnoses of several bubble episodes were discussed by Sornette and Zhou (2006), Sornette,Woodard, and Zhou (2009), Zhou and Sornette (2003), Zhou and Sornette (2006), Zhou and Sornette (2008) and Zhou and Sornette (2009).

The expected value of the asset log price in a upward trending bubble according to the LPPL equation is given by,

$$E[\ln p(t)] = A + B(t_c - t) + C(t_c - t) \cdot \cos[\omega \ln(t_c - t) - \phi] \tag{24}$$

where $0 < \beta < 1$ quantifies the power law acceleration of prices and should be positive to ensure a finite price at the so-called critical time t_c, which is interpreted as the end of the bubble; ω represents the frequency of the oscillations during the bubble; $A > 0$ is the value of $[\ln p(t_c)]$ at the critical time t_c, $B < 0$ the increase in $[\ln p(t)]$ over the time unit before the crash, $C \neq 0$ is the proportional magnitude of the oscillations around the exponential growth, while $0 < \phi < 2\pi$ is a phase parameter. It has to be noted that A, B, C and ϕ, are just units distributions of betas and omegas and do not carry any structural information, see Sornette and Johansen (2001), Johansen (2003), Sornette (2003a), Lin et al. (2014) and references therein.

The first condition for a bubble to take place within the JLS framework is $0 < \beta < 1$, which guarantees that the crash hazard rate accelerates, while the second condition proposed by Bothmer and Meister (2003) is that the crash rate should be non-negative, so that

$$b = -B\beta - |C|\sqrt{\beta^2 + \omega^2} \geq 0 \tag{25}$$

Lin et al. (2014) added a third condition, requiring that the residuals from fitting equation (24) should be stationary. Lin, Ren, and Sornette (2014) used the Phillips-Perron (PP) and the Augmented Dickey-Fuller (ADF) to test for stationarity, whereas Geraskin and Fantazzini (2013) suggested to use the test by Kwiatkowski et al. (1992), given the higher power of this test when the underlying data-generating process is an AR(1) process with a coefficient close to one.

The calibration of LPPL models can be difficult due to the presence of many local minima of the cost function where the minimization algorithm can get stacked, see Fantazzini (2010), Geraskin and Fantazzini (2013) and Filimonov and Sornette (2013) for more details and for some possible solutions.

MacDonell (2014) used the LPPL model to forecast successfully the bitcoin price crash that took place on December 4, 2013, showing how LPPL models can be a valuable tool for detecting bubble behavior in digital currencies.

Cheah and Fry (2015) tested for the presence of financial bubbles in Bitcoin prices using a test proposed by Fry (2014) and whose starting point is the same as Johansen et al. (2000). More specifically,

Cheah and Fry (2014) assumed that,

$$P(t) = P_1(t)(1-k)^{j(t)} \text{ where}$$
$$dP_1(t) = [\mu(t) + \sigma^2(t)/2]P_1(t)dt + \sigma(t)P_1(t)dW_t$$

where W_t is a Wiener process, $j(t)$ is a jump process

$$j(t) = \begin{cases} 0 \text{ before the crash} \\ 1 \text{ after the crash} \end{cases}$$

while k represents the % loss in the asset value after the crash. Before a crash, we have that $P(t) = P_1(t)$ and using the Ito's lemma it is possible to show that $X_t = \log(P(t))$ satisfies

$$\begin{aligned} &dX_t = \mu(t)dt + \sigma(t)dW_t - vdj(t), \\ &v = -\ln[(1-k)] > 0 \end{aligned} \tag{26}$$

Then, Fry (2014) and Cheah and Fry (2015) introduced the following two assumptions:

Assumption 1 (*Intrinsic Rate of Return*): the intrinsic rate of return is assumed constant and equal to μ:

$$E[X_{t+\Delta} - X_t | X_t] = \mu\,\Delta + o(\Delta) \tag{27}$$

Assumption 2 (*Intrinsic Level of Risk*): the intrinsic level of risk is assumed constant and equal to σ^2:

$$Var[X_{t+\Delta} - X_t | X_t] = \sigma^2\,\Delta + o(\Delta) \tag{28}$$

Moreover, supposing that a crash has not occurred by time t, they get

$$E[j(t+\Delta) - j(t)] = \Delta h(t) + o(\Delta) \tag{29}$$

$$Var[j(t+\Delta) - j(t)] = \Delta h(t) + o(\Delta) \tag{30}$$

where $h(t)$ is the hazard rate. Using eq. (27) in assumption 1 together with eqs. (26) and (29), it follows that

$$\mu(t) - vh(t) = \mu; \quad \mu(t) = \mu + vh(t) \tag{31}$$

which shows that the rate of return must increase in order to compensate an investor for the risk of a crash.

Fry (2014) and Cheah and Fry (2015) showed that in a bubble not only prices have to grow, but also volatility must diminish. Using eqs. (26), (28) and (30), they get

$$\sigma^2(t) + v^2 h(t) = \sigma^2; \quad \sigma^2(t) = \sigma^2 - v^2 h(t) \tag{32}$$

The key equations (31) and (32) show that during a bubble an investor should be compensated for the crash risk by an increased rate of return with $\mu(t) > \mu$ (where μ is the long-term rate of return), whereas market volatility decreases, representing market over-confidence (Fry, 2012, 2014). Moreover, it is possible to test for the presence of a speculative bubble by testing the one-sided hypothesis

$$H_0 : v = 0 \;\; H_1 : v > 0 \tag{33}$$

Fry (2014) further showed that, given the previous assumptions, the fundamental asset price when there is no bubble ($v = 0$) is given by :

$$P_F(t) = E(P(t)) = P(0)e^{\tilde{\mu}t} \tag{34}$$

where $\tilde{\mu} = \mu + \sigma^2/2$. Instead, during a bubble ($v > 0$),

$$\begin{aligned} &X_t = N(X_0 + \mu t + vH(t), \sigma^2 t - v^2 H(t)), \quad \text{where} \\ &H(t) = \textstyle\int_0^t h(u)du \end{aligned} \tag{35}$$

so that the asset value is given by

$$P_B(t) = E(P(t)) = P(0)e^{\tilde{\mu}t + \left(v - \frac{v^2}{2}\right)H(t)} \tag{36}$$

Equations (34) and (36), together with a proper hazard function $h(t)$, can then be used to compute the bubble component in the asset price, defined as the "average distance" between fundamental and bubble prices. Fry (2014) and Cheah and Fry (2015) used the following hazard function

$$h(t) = \frac{\beta t^{\beta-1}}{\alpha^\beta + t^\beta} \tag{37}$$

so that the bubble component is given by,

$$\text{Bubble component} = 1 - \frac{1}{T}\int_0^T \frac{P_F(t)}{P_B(t)}dt = 1 - \frac{1}{T}\int_0^T \left(1 + \frac{t^\beta}{\alpha^\beta}\right)^{-\left(v - \frac{v^2}{2}\right)} dt. \tag{38}$$

where T is the sample dimension. It follows from (34) that if $\tilde{\mu} < 0$ the fundamental asset value is zero:

$$\lim_{t \to \infty} P_F(t) = 0 \tag{39}$$

Following MacDonell (2014), Fry (2015) tested for the presence of a bubble in bitcoin prices from January 1st 2013 till November 30th 2013, before the price crash of December 2013. He rejected the null hypothesis (33) and found that the parameter $\tilde{\mu}$ is not statistically different from zero, which is compatible with a long-term fundamental value of zero. Moreover, he found that the bubble component amounts to approximately 48.7% of observed prices. These results are confirmed by several robustness checks.

6.2 Testing for multiple bubbles

The previous tests are designed to test for the presence of a single bubble and can be used to detect multiple bubbles only if repeated with a moving time window, as done by Sornette et al. (2009) Jiang et al. (2010), Geraskin and Fantazzini (2013) and Cheah and Fry (2015). Tests specifically designed for detecting multiple bubbles were recently proposed by Phillips and Yu (2011), Phillips et al. (2011) and Phillips et al. (2015) and they share the same idea of using sequential tests with rolling estimation windows. More specifically, these tests are based on sequential ADF-type regressions using time windows of different size, and they can consistently identify and date-stamp multiple bubble episodes even in small sample sizes. These tests were employed by Malhotra and Maloo (2014) to test for the presence of explosive behaviour in bitcoin prices. We will focus below on the generalized-supremum ADF test (GSADF) proposed by Phillips, et al. (2015) -PSY henceforward- which builds upon the work by Phillips and Yu (2011) and Phillips et al. (2011), because it has better statistical properties in detecting multiple bubble than the latter two tests.

This test employs an ADF regression with a rolling sample, where the starting point is given by the fraction r_1 of the total number of observations, the ending point by the fraction r_2, while the window size by $r_w = r_2 - r_1$. The ADF regression is given by

$$y_t = \mu + \rho y_{t-1} + \sum_{i=1}^{p} \phi_{r_w}^i \Delta y_{t-i} + \varepsilon_t \tag{40}$$

where μ, ρ, and $\phi_{r_w}^i$ are estimated by ordinary least squares, and the null hypothesis is of a unit root $\rho = 1$ versus an alternative of a mildly explosive autoregressive coefficient $\rho > 1$. The backward sup ADF test proposed by PSY (2015) fixes the endpoint at r_2 while the window size is expanded from an initial fraction r_0 to r_2, so that the test statistic is given by:

$$BSADF_{r_2}(r_0) = \sup_{r_1 \in [0, r_2 - r_0]} ADF_{r_1}^{r_2} \tag{41}$$

It is important to note that the test by Phillips et al. (2011) is a special case of the BSADF test with $r_1 = 0$, so that the sup operator becomes superfluous.

The generalized sup ADF (GSADF) test is finally calculated by repeatedly performing the BSADF test for each endpoint $r_2 \in [r_0, 1]$:

$$GSADF(r_0) = \sup_{r_2 \in [r_0, 1]} BSADF_{r_2}^{(} r_0) \tag{42}$$

The limiting distribution of (42) under the null of a random walk with asymptotically negligible drift is given by the Theorem 1 in PSY (2015), while critical values are obtained by numerical simulation. In case the null hypothesis of no bubbles is rejected, the starting and ending points of one (or more) bubble(s) can be found in a second step: the starting point is given by the date -denoted as T_{re} - when the sequence of BSADF test statistics crosses the critical value from below, while the ending point -denoted as T_{rf} - when the BSADF sequence crosses the corresponding critical value from above:

$$\begin{aligned} \hat{r}_e &= \inf_{r_2 \in [r_0, 1]} \left\{ r_2 : BSADF_{r_2}(r_0) > cv_{r_2}^{\beta_T} \right\} \\ \hat{r}_f &= \inf_{r_2 \in [\hat{r}_e + \delta \log(T)/T, 1]} \left\{ r_2 : BSADF_{r_2}(r_0) < cv_{r_2}^{\beta_T} \right\} \end{aligned} \tag{43}$$

where $cv_{r_2}^{\beta_T}$ is the 100(1 - β_T)% right-sided critical value of the BSADF statistic based on $\lfloor T_{r2} \rfloor$ observations, and $\lfloor \cdot \rfloor$ is the integer function. δ is a tuning parameter which determines the minimum duration for a bubble and is usually set to 1, see Philips et al. (2011), PSY (2015) and references therein, thus implying a minimum bubble-duration condition of $\ln(T)$ observations. However, different values can be used depending on the data frequency, see Figuerola-Ferretti et al. (2016) for a discussion.

Malhotra and Maloo (2014) tested for the presence of multiple bubbles using the GSADF test with a dataset ranging from mid-2011 till February 2014: they found evidence of explosive behaviour in the bitcoin-USD exchange rates during August – October 2012 and November, 2013 – February, 2014. They suggested that the first episode of bubble behaviour (August – October 2012) could be attributed to the sudden increase in media attention towards bitcoin, whereas the second episode to a large set of reasons including the US debt ceiling crisis, the shutdown of Silk Road by the FBI, the rise of Chinese exchange BTC-China, and the increasing number of warnings issued by regulatory authorities and central banks worldwide following the shutdown of the Japanese exchange Mt.Gox.

7 Price discovery

Brandvold et al. (2015) are the first (and so far the only ones) to study the price discovery process in the Bitcoin market, which consists of several independent exchanges. This topic is frequently discussed in the bitcoin community because knowing which exchange reacts most quickly to new information (thus reflecting the value of Bitcoin most precisely), is clearly of outmost importance for both short-term traders and long-term investors. The price discovery literature employs mainly three methodologies: the information share method by Hasbrouck (1995), the permanent-transitory decomposition by Gonzalo and Granger (1995) and the structural multivariate time series model by de Jong et al. (2001) which is an extension of class of models originally proposed by Harvey (1989). Brandvold et al. (2015) used the method by de Jong et al. (2001) because it has the advantage that the information share is uniquely defined, unlike the information share computed with the Hasbrouck's (1995) model, and it takes the variance of innovations into account, unlike Gonzalo and Granger (1995), so that a price series with low innovation variance gets a low information share. Given its importance, the model by de Jong et al. (2001) is described below.

This multivariate model by de Jong et al. (2001) was proposed to estimate the information share of various exchanges with respect to the information generated by the whole market. The prices are composed of two components, one common (unobserved) underlying random walk and an idiosyncratic specific noise for each exchange. The random walk component is interchangeably referred to either as the efficient price or the fundamental news component. It follows immediately from this model structure that the exchanges' prices are cointegrated by construction, while the idiosyncratic component can be due to specific conditions at an exchange, traders' strategic behaviour, or other shocks.

The theoretical setup in Brandvold et al. (2015) assumes n individual exchanges and m corresponding markets, with $m = n$, whereas a market for an exchange is defined as all the other exchanges combined. Brandvold et al. (2015) denote P^e as the vector of exchange prices, P^m as the vector of market prices, while U^e and U^m represents the vectors of idiosyncratic shocks for the exchanges and the markets, respectively. P^*denotes the efficient price, $p^e = \ln P^e$, $u^e = \ln U^e$ and $p^* = \ln P^*$, so that the logarithm of the n-vector of exchange prices and the m-vector of market prices are given by:

$$\begin{aligned} p_t^e &= p_t^* + u_t^e \\ p_t^m &= p_t^* + u_t^m \end{aligned} \tag{44}$$

where p^* is a random walk. This is a special case of an unobserved components structural model, see Harvey (1989) for more details. If we denote the log-returns of the efficient price over the interval $(t-1,t)$ as denoted $r_t = p_t^* - p_{t-1}^*$, then the model assumptions are given below:

$$
\begin{aligned}
&E[r_t^2] = \sigma^2 \\
&E[r_t u_{it}^e] = \psi_i \\
&E[r_t u_{jt}^m] = \psi_j \\
&E[r_t u_{i,t+l}^e] = \gamma_{li}, \quad l \geq 0 \\
&E[r_t u_{j,t+l}^m] = \gamma_{lj}, \quad l \geq 0 \\
&E[r_t u_{i,t-k}^e] = 0, \quad k \geq 0 \\
&E[r_t u_{j,t-k}^m] = 0, \quad k \geq 0 \\
&E[u_{it}^e] = \Omega^e \\
&E[u_{it}^e u_{jt}^m] = \Omega, \quad i = j \\
&E[u_{i,t-k}^e] = 0, \quad k \neq 0 \\
&E[u_{it}^e u_{j,t-k}^m] = 0, \quad k \neq 0
\end{aligned}
\tag{45}
$$

where i refers to exchange i, j to market j, while ψ , γ are $(n \times 1)$ vectors and Ω, Ω^e are $(n \times n)$ matrices.

The fundamental news component r_t can be correlated with concurrent and future idiosyncratic components, but is otherwise uncorrelated. Instead, the idiosyncratic components are serially uncorrelated and they reflect the noise present in intradaily data. These restrictions on the correlation structure are needed to identify the model, see Harvey (1989) details. Given the previous structure, the log-returns of observed prices are defined as followed:

$$
y_{it} = p_{it} - p_{i,t-1} = p_t^* + u_{it} - p_{t-1}^* - u_{it-1} = r_t + u_{it} - u_{it-1} \tag{46}
$$

so that the vectors of exchanges prices and market prices are given by,

$$
\begin{aligned}
Y_t^e &= \iota r_t + u_t^e - u_{t-1}^e \\
Y_t^m &= \iota r_t + u_t^m - u_{t-1}^m
\end{aligned}
\tag{47}
$$

where ι is a vector of ones with $n = m$ elements. Given the assumptions in (45), the serial covariances of Y_t are

$$
\begin{aligned}
&E[Y_t Y_t'] = \sigma^2 \iota\iota' + \iota\psi' + \psi\iota' + 2\Omega \\
&E[Y_t Y_{t-1}'] = -\psi\iota' - \Omega + \gamma\iota' \\
&E[Y_t Y_{t-2}'] = -\gamma\iota'
\end{aligned}
\tag{48}
$$

Similarly, the serial covariance between an exchange and its corresponding market, that is the covariance between an element in vector Y^e and the corresponding element in vector Y^m , is given by

$$
\begin{aligned}
E[y_{jt}y_{it}] &= \sigma^2 + \psi_j + \psi_i + 2\omega_{ij} \\
E[y_{jt}y_{i,t-1}] &= -\psi_j - \omega_{ij} + \gamma_j \\
E[y_{jt}y_{i,t-2}] &= -\gamma_j
\end{aligned} \tag{49}
$$

while the first order autocorrelation for exchanges is

$$
\rho_{1,ii} = \frac{-(\psi_i + \omega_{ii}^e - \gamma_i)}{\sigma^2 + 2(\psi_i + \omega_{ii}^e)} \tag{50}
$$

The parameter ψ_i -which is the covariance between the fundamental news component and the idiosyncratic component- is of crucial importance because it shows how the market learns after a price change from an individual exchange: a high value for ψ_i implies that a price update from that exchange has an high information content for the whole market. To explain this issue, consider the covariance between the fundamental news component and a price change at an exchange:

$$
Cov(y_{it}, r_t) = \sigma^2 + \psi_i \tag{51}
$$

which is derived from (45) and (46). It follows immediately that the n covariances between the exchange updates and the fundamental news component are determined by n+1 parameters, so that an identifying restriction is needed. In this regard, de Jong et al. (2001) suggested the idea that the information generated by the price update of each exchange should be equal on overage to σ^2, the variance of r_t . Therefore, if we consider the average covariance between the price change of a selected exchange and the fundamental news,

$$
\sum_{i=1}^{n} \pi_i Cov(y_{it}, r_t) = \pi'(\sigma^2 \iota + \psi) = \sigma^2 + \pi'\psi \tag{52}
$$

where π is a vector of weights adding to one (to be defined below), then the assumption that σ^2 is the unconditional covariance of a exchange price change and the news component imposes the restriction $\pi'\psi = 0$. This restriction is sufficient to identify the model parameters and also leads to a definition of π_i as the activity share of an exchange, defined as the fraction of trades that happened on exchange i, or simply, the probability that a trade took place on exchange i (Brandvold et al., 2015). If we multiply the covariance between the fundamental news component and the price change of exchange i -eq. (51)- with the probability π_i , we get a measure of how much information is generated by the price change of exchange i. Dividing this by the total information generated in the market σ^2, we obtain the information share for exchange i:

$$
IS_i = \frac{(\sigma^2 + \psi_i)\pi_i}{\sigma^2} = \pi_i \left(1 + \frac{\psi_i}{\sigma^2}\right) \tag{53}
$$

de Jong et al. (2001) and Brandvold et al. (2015) highlighted that this definition of information share has some appealing properties. First, the information shares add to 1, thus simplifying interpretation and making it trivial to add or remove exchanges from the model. Second, the joint information share of two exchanges simply equals the sum of their individual information shares. Third, an exchange with a contemporaneous covariance between its idiosyncratic component and the fundamental news component greater than zero $\psi_i > 0$) has a higher information share than activity share.

The estimation procedure of the model parameters consists of two steps: first, the sample covariances $\mathrm{E}[y_{jt}y_{i,t-k}]$, where k=0,1,2, and the autocorrelations $\rho_{1,ii}$ are estimated, then the structural parameters are computed using (49)-(50) and a nonlinear program solver. Besides, some parameters can be found directly: given that σ ^{2}is the variance of r_t and given the assumption by Brandvold et al. (2015) that the seven exchanges in their dataset represent the whole Bitcoin market, σ^2 can be computed as the variance of the aggregated return of the seven exchanges. Similarly γ can be computed directly using the sample covariance between the market returns and its corresponding exchange returns lagged two intervals This leaves only ω^e_{ii}, ω_{ij}, ψ_i and ψ_i to be estimated in a second step. The objective function used by Brandvold et al. (2015) to find the remaining parameters with a nonlinear programming solver is given below:

$$Z = \sum_{i=1}^{n} |\pi_i \psi_i| = 0 \tag{54}$$

subject to the following set of constraints

$$\begin{aligned}
&\rho_{1,ii} = \tfrac{-(\psi_i+\omega^e_{ii}-\gamma_i)}{\sigma^2+2(\psi_i+\omega^e_{ii})} && (i = 1,\ldots,n)\\
&E[y_{jt}y_{i,t-1}] = -\psi_j - \omega_{ij} + \gamma_j && (i = j = 1,\ldots,n)\\
&E[y_{jt}y_{i,t-2}] = -\gamma_j && (i = j = 1,\ldots,n)\\
&E[y_{it}y_{j,t-2}] = -\gamma_i && (i = j = 1,\ldots,n)\\
&\omega^e_{ii} \geq 0 && (i = 1,\ldots,n)
\end{aligned} \tag{55}$$

Brandvold et al. (2015) tried also alternative objective functions and starting values, but the estimated parameters showed only minimal differences. Brandvold et al. (2015) highlighted that there is no agreement in the financial literature on how to measure the trading activity of a specific exchange relative to all trading activity in the market (i.e π_i), so that they preferred to use a linear combination of trading volume and number of trades. However, they also highlight that the choice of π_i only affects the magnitude of the information share, but not the relation between information and activity share, that is whether ψ_i is positive or negative (Brandvold et al. 2015). In this regard, they suggested to also consider the simple case of equal π_i for each exchange to verify the robustness of the model results.

Brandvold et al. (2015) used data from seven exchanges: Bitfinex, Bitstamp, BTC-e (Btce), BTC China(Btcn) and Mt.Gox (Mtgox), Bitcurex and Canadian Virtual Exchange (Virtex). The original tick data were transformed into 5 minutes intervals and covered the period April 1st 2013–February 25th 2014, till the bankruptcy of Mtgox. They found that the two exchanges with positive ψ for the entire period were Btce and Mtgox, thus indicating that these exchanges were more informative than their competitors. Similar evidence was provided by the information share, which was highest for Btce and Mtgox (0,322 and 0.366, respectively). However, Brandvold et al. (2015) highlighted that, even if the other exchanges have negative ψ and lower information share, they still provide information to the market, only less informative. Brandvold et al. (2015) also investigated how the information share changed over time: the information share of Btcn first increased from 0.040 in April 2013 to 0.325 in December 2013 because some large Chinese companies (like Baidu) started accepting Bitcoin as payment, but then its information share fell to 0.124 in January 2014 after the Chinese government banned payment companies from clearing Bitcoin. Mtgox had the largest information share at the beginning (0.667), then it gradually decreased over time, with a last jump in January and February 2014, related to the increasing uncertainty about its possible bankruptcy.

Brandvold et al. (2015) further examined what happened during and after the price shock on October 2nd 2013, when the owner of the Silk Road marketplace was arrested by American authorities and the site was shut down, see Konrad (2013) for details. They found that Btce is the only exchange with positive ψ in this period, and has a significant higher information share than activity share. They argues that either a large fraction of informed traders switched to Btce in this period, or simply that traders at Btce suddenly became more informed. Moreover, they also highlighted that Btce is renowned in the Bitcoin community for having a good API for traders to place trading bots, which can react extremely quickly, and this may help explaining why Btce contributed more to the price discovery process in this period than its competitors.

8 Conclusions

We reviewed the econometric and mathematical tools which have been proposed so far to model the bitcoin price and several related issues. More specifically, we first reviewed the methods employed to determine the main characteristics of bitcoin users, finding that the majority of users seem to be computer programming enthusiasts and people possibly engaged in illegal activity, whereas only a small part seem to be driven by political reasons or by investment motives. Nevertheless, these analyses are plagued by several limitations, like the possibility that the samples examined may not be representative of the full population of users and the speed with which bitcoin markets and users change over time, so that all analyses may be quickly out of date. We then examined the main models proposed to assess the bitcoin fundamental value, ranging from market sizing –which is more suitable for the medium-long term-, to the bitcoin marginal cost of production based on electricity consumption, which represents a lower bound in the short term. Moreover, we described several econometric approaches suggested to model bitcoin price dynamics, starting with cross-sectional regression models involving the majority of traded digital currencies and then moving to univariate and multivariate time series models, till models in the frequency domain. In general, all these methods confirmed that the main drivers of bitcoin price dynamics are still mainly of speculative nature, followed by traditional supply and demand related variables, while global macro-financial variables play no role. We then reviewed the tests employed for detecting the existence of financial bubbles in bitcoin prices and which can be broadly classified into two large families, depending on whether they are intended to detect a single bubble, or (potentially) multiple bubbles. Most of these tests examined the months before the price crash that started in December 2013, while one analysis looked for multiple bubbles over the sample 2011-2014, finding evidence of explosive behavior in the bitcoin-USD exchange rates during August – October 2012 and November, 2013 – February, 2014. Finally, we examined a recent study dealing with the price discovery process in the Bitcoin market, which is of great importance for both short-term traders and long-term investors who want to know which exchange reacts most quickly to new information, thus reflecting the value of Bitcoin most precisely and efficiently.

This review clearly shows that there are several possible avenues for further research. For example, econometric methods for market risk management with bitcoin prices are almost non-existent: the only work to our knowledge which fitted several parametric distributions to estimate the Value at Risk (VaR) and the Expected Shortfall (ES) is the one by Chu et al. (2015). Unfortunately, they considered only unconditional estimates which neglect conditional heteroskedasticity and therefore are not advisable for an extremely volatile time series such as the bitcoin price, see in this regard Fantazzini (2009) and Weiß (2011,2013) for large scale simulation and empirical studies about VaR and ES for linear portfolios. Moreover, despite the changes in local regulations, arrival of new investors, police intervention (Silk

Road) and massive improvements in mining hardware, there is no research work dealing with structural breaks and long memory in bitcoin prices. Besides, there is a large body of the econometric and statistical literature dealing with forecasting with structural breaks and this can be of interest for bitcoin algorithmic trading, see Zhao (2015) for a recent Monte Carlo Study of several algorithms. Furthermore, all models examined so far are (log-)linear but, considering the behavior of bitcoin prices, nonlinear models could be useful particularly for forecasting purposes, see Tong (1990), Franses and Dijk (2000), Wood (2006) and Terasvirta et al. (2011) for a discussion at the textbook level. Probably, the most interesting discrepancy that we found when preparing this review is that IT related papers focused mainly on electricity costs and energy and computational efficiency, whereas economic related papers rarely considered these factors. Therefore, another avenue of future research is a multi-disciplinary analysis able to consider all these aspects together.

References

[1] Ali R., Barrdear J., Clews R., Southgate J. (2014). The economics of digital currencies. *Bank of England Quarterly Bulletin*, Q3, 276-287.

[2] Allen H.J. (2015). $ = €= Bitcoin? Suffolk University Legal Studies Research Paper Series, Research Paper 15-33.

[3] Badev A., Chen M (2014). Bitcoin: Technical background and data analysis. *Finance and Economics Discussion Series*, n. 2014-104, Divisions of Research and Statistics and Monetary Affairs, Federal Reserve Board, Washington, D.C.

[4] Baur A. W., Bühler J., Bick M., Bonorden C. S. (2015). Cryptocurrencies as a Disruption? Empirical Findings on User Adoption and Future Potential of Bitcoin and Co. In *Open and Big Data Management and Innovation*, pp. 63-80. Springer International Publishing.

[5] Becker, J., Breuker, D., Heide T., Holler, J., Rauer H.P., Böhme R. (2013). Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency. In *The Economics of Information Security and Privacy*, pp. 135-156. Springer Berlin Heidelberg.

[6] Bitcoin.org, (2015). Official Site Offering Documentation, Forums and the Open Source Client Software Which Permits to Send and Receive Bitcoins. *bitcoin.org* .

[7] Bradley M.M., Lang P.J. (1999). Affective norms for English words (ANEW): Instruction manual and affective ratings (pp. 1-45). Technical Report C-1, The Center for Research in Psychophysiology, University of Florida.

[8] Böhme R., Christin N., Edelman B., Moore T. (2015). Bitcoin: Economics, Technology, and Governance. *The Journal of Economic Perspectives*, 29(2), 213-238.

[9] Bouoiyour J., Selmi R. (2015) What Does Bitcoin Look Like? *Annals of Economics and Finance*, 16(2), 449–492.

[10] Bouoiyour J., Selmi R., Tiwari A.K. (2015) Is bitcoin business income or speculative foolery? new ideas through an improved frequency domain analysis. *Annals of Financial Economics*, 10, 1550002.

[11] Bohr J., Bashir M. (2014). Who uses bitcoin? an exploration of the bitcoin community. In *Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference*, pp. 94-101. IEEE.

[12] Bothmer H.C.G.V., Meister C. (2003). Predicting critical crashes? A new restriction for the free variables. *Physica A*, 320, 539-547.

[13] Bergstra J.A., de Leeuw, K. (2013). Bitcoin and Beyond: Exclusively Informational Monies. *arXiv preprint*, arXiv:1304.4758.

[14] Bodart V., Candelon B. (2009) Evidence of interdependence and contagion using a frequency domain framework. *Emerging Markets Review*, 10 (2), 140-150.

[15] Böhme, R., Christin, N., Edelman, B., Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *The Journal of Economic Perspectives*, 29(2), 213-238.

[16] Brandvold M., Molnár P., Vagstad K., Valstad O.C.A. (2015). Price discovery on Bitcoin exchanges. *Journal of International Financial Markets, Institutions and Money*, 36, 18-35.

[17] Breitung J., Candelon B. (2006) Testing for short and long-run causality: a frequency domain approach. *Journal of Econometrics*, 132, 363-378.

[18] Breitung J., Candelon, B. (2007). Testing for multistep causality. Mimeo Maastricht University.

[19] Buchholz M., Delaney J., Warren J., Parker J. (2012). Bits and Bets, Information, Price Volatility, and Demand for Bitcoin. Economics 312. Available at http://www.bitcointrading.com/pdf/bitsandbets.pdf

[20] Cameron A.C., Gelbach J. B., Miller D. L. (2011). Robust inference with multiway clustering. *Journal of Business and Economic Statistics*, 29(2), 238-249.

[21] Cheah E.T., Fry, J. (2015). Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin. *Economics Letters*, 130, 32-36.

[22] Chu, J., Nadarajah, S., Chan, S. (2015). Statistical Analysis of the Exchange Rate of Bitcoin. *PloS one*, 10(7), e0133678.

[23] De Jong F., Mahieu R., Schotman P., Van Leeuwen I. (2001). Price discovery on foreign exchange markets with differentially informed traders. Tinbergen Institute Discussion Paper Series, No. TI 99-032/2.

[24] Dolado J., Lutkepohl H. (1996). Making wald tests work for cointegrated VAR systems. *Econometric Reviews*, 15, 369–386

[25] Dowd, K. (2014). *New Private Monies: A Bit-Part Player?* Institute of Economic Affairs.

[26] Dwyer, G. P. (2015). The economics of Bitcoin and similar private digital currencies. *Journal of Financial Stability*, 17, 81-91.

[27] ECB (2012). *Virtual Currency Schemes*. ECB report, October 2012.

[28] ECB (2015). *Virtual Currency Schemes - A Further Analysis*. ECB report, February 2015.

[29] Fantazzini D. (2009). The effects of misspecified marginals and copulas on computing the Value at Risk: A Monte Carlo study. *Computational Statistics & Data Analysis*, 53(6), 2168-2188.

[30] Fantazzini D. (2010). Modelling Bubbles And Anti-Bubbles In Bear Markets: A Medium-Term Trading Analysis. In *Handbook of Trading*, ed. by G. Gregoriou, 365-388. McGraw-Hill.

[31] Fantazzini D., Toktamysova Z., (2016). Forecasting German car sales using Google data and multivariate models, *International Journal of Production Economics*, forthcoming, http://dx.doi.org/10.1016/j.ijpe.2015.09.010.

[32] Figuerola-Ferretti I., Gilbert C., Mccrorie J. (2016). Testing For Mild Explosivity And Bubbles In LME Non-Ferrous Metals Prices, *Journal of Time Series Analysis*, 36(5), 763–782.

[33] Filimonov V., Sornette, D. (2013). A stable and robust calibration scheme of the log-periodic power law model. *Physica A*, 392(18), 3698-3707.

[34] Fry J.(2014). Multivariate bubbles and antibubbles. *The European Physical Journal B*, 87(8), 1-7.

[35] Franses P., Dijk V. (2000). *Nonlinear time series models in empirical finance*. Cambridge University Press.

[36] Garcia D., Tessone C. J., Mavrodiev P., 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(99), 20140623.

[37] Garcia D., Schweitzer F. (2012). Modeling online collective emotions. In *Proceedings of the 2012 workshop on Data-driven user behavioral modelling and mining from social media*, pp. 37-38. ACM.

[38] Garcia, D., & Schweitzer, F. (2015). Social signals and algorithmic trading of Bitcoin. *Royal Society open science*, 2(9), 150288.

[39] Geraskin P., Fantazzini D. (2013). Everything you always wanted to know about log-periodic power laws for bubble modeling but were afraid to ask. *The European Journal of Finance*, 19(5), 366-391.

[40] Glaser F., Zimmermann K., Haferkorn M., Weber M.C., Siering, M. (2014). Bitcoin-Asset or Currency? Revealing Users' Hidden Intentions. ECIS 2014 (Tel Aviv). Available at SSRN: http://ssrn.com/abstract=2425247 .

[41] Gonzalo J., Granger C. (1995). Estimation of common long-memory components in cointegrated systems. *Journal of Business and Economic Statistics*, 13(1), 27-35.

[42] Harvey, A.C. (1989). *Forecasting, structural time series models and the Kalman filter*. Cambridge University Press.

[43] Hasbrouck J. (1995). One security, many markets: determining the contributions to price discovery. *Journal of Finance*, 50, 1175–1199.

[44] Hayes A. (2015a). A Cost of Production Model for Bitcoin. Available at SSRN 2580904.

[45] Hayes A. (2015b). Cryptocurrency Value Formation: An Empirical Analysis Leading to a Cost of Production Model for Valuing Bitcoin. Available at SSRN 2648366.

[46] Hayes, A. (2015c). The Decision to Produce Altcoins: Miners' Arbitrage in Cryptocurrency Markets. Available at SSRN 2579448.

[47] Hosoya Y. (2001). Elimination of third-series effect and defining partial measures of causality. *Journal of Time Series Analysis*, 22, 537–554.

[48] Huhtinen T. P. (2014). Bitcoin as a monetary system: Examining attention and attendance. Master's thesis, Department of Finance, Aalto University School of Business.

[49] Jiang Z.Q., Zhou W.X., Sornette D., Woodard R., Bastiaensen K., Cauwels P. (2010). Bubble diagnosis and prediction of the 2005–2007 and 2008–2009 Chinese stock market bubbles. *Journal of Economic Behavior and Organization*, 74(3), 149-162.

[50] Johansen A. (2003). Characterization of large price variations in financial markets. *Physica A*, 324, 157-166.

[51] Johansen A., Ledoit O., Sornette D. (2000). Crashes as critical points. *International Journal of Theoretical and Applied Finance*, 3(2), 219-255.

[52] Kancs D.A., Ciaian P., Miroslava R. (2015). The Digital Agenda of Virtual Currencies. Can BitCoin Become a Global Currency? Institute for Prospective and Technological Studies, European Commission - Joint Research Centre. Report No. JRC97043.

[53] Konrad A. (2013) Feds Say They've Arrested 'Dread Pirate Roberts' Shut Down His Black Market 'The Silk Road'. *Forbes*. Available at http://www.forbes.com/sites/alexkonrad/2013/10/02/feds-shut-down-silk-road-owner-known-as-dread-pirate-roberts-arrested

[54] Kristoufek, L. (2013). BitCoin meets Google Trends and Wikipedia: Quantifying the relationship between phenomena of the Internet era. *Scientific reports*, 3, Article number: 3415.

[55] Kristoufek, L. (2015). What are the main drivers of the Bitcoin price? Evidence from wavelet coherence analysis. *Plos One*, 10(4): e0123923 .

[56] Kroll J.A., Davey I.C., Felten E.W. (2013). The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In *Proceedings of WEIS* , Vol. 2013.

[57] Kwiatkowski D., Phillips P., Schmidt P., Shin Y. (1992). Testing the null hypothesis of stationary against the alternative of a unit root. *Journal of Econometrics*, 54, 159-178.

[58] Lin Y., Michel J.B., Aiden E.L., Orwant J., Brockman W., Petrov S. (2012). Syntactic annotations for the google books ngram corpus. In *Proceedings of the ACL 2012 system demonstrations*, pp. 169-174. Association for Computational Linguistics.

[59] Lin L., Ren R.E., Sornette D. (2014). The volatility-confined LPPL model: A consistent model of 'explosive' financial bubbles with mean-reverting residuals. *International Review of Financial Analysis*, 33, 210-225.

[60] Lo S., Wang J.C. (2014). Bitcoin as money?. *Current Policy Perspectives*, 14-4, Federal Reserve Bank of Boston.

[61] MacDonell, A. (2014). Popping the Bitcoin Bubble: An application of log-?periodic power law modeling to digital currency. University of Notre Dame working paper.

[62] Malhotra A., Maloo, M. (2014). Bitcoin–is it a Bubble? Evidence from Unit Root Tests. Available at SSRN: http://ssrn.com/abstract=247637 .

[63] Murphy E.V., Murphy, M. M., Seitzinger M.V. (2015). *Bitcoin: questions, answers, and analysis of legal issues*. US Congressional Research Service 7-5700, R43339, October.

[64] Ng E.K., Chan J.C. (2012). Geophysical applications of partial wavelet coherence and multiple wavelet coherence. *Journal of Atmospheric and Oceanic Technology*, 29(12), 1845-1853.

[65] Osgood C.E. (1964). Semantic differential technique in the comparative study of Cultures. *American Anthropologist*, 66(3), 171-200.

[66] Pennebaker J.W., Chung C.K., Ireland M., Gonzales A., Booth R.J. (2007). The development and psychometric properties of LIWC2007. See LIWC.net .

[67] Pesaran M.H., Shin, Y. (1999). An autoregressive distributed-lag modelling approach to cointegration analysis. *Econometric Society Monographs*, 31, 371-413.

[68] Phillips P.C.B., Yu J. (2011). Dating the timeline of financial bubbles during the subprime crisis. *Quantitative Economics*, 2(3), 455–491.

[69] Phillips P.C.B., Shi S., Yu J. (2015). Testing for Multiple Bubbles: Historical Episodes of Exuberance and Collapse in the SP500. *International Economic Review*, 56 (4), 1043-1078.

[70] Phillips P.C.B., Wu Y., Yu J. (2011). Explosive Behavior In The 1990S Nasdaq: When Did Exuberance Escalate Asset Values?. *International Economic Review*, 52(1), 201–226.

[71] Rogojanu, A., Badea, L. (2014). The issue of competing currencies. Case study – Bitcoin. *Theoretical and Applied Economics*, 21(1), 103-114.

[72] Russell J.A. (2003). Core affect and the psychological construction of emotion. *Psychological review*, 110(1), 145-172.

[73] Segendorf, B. (2014). What is Bitcoin. *Sveriges Riksbank Economic Review*, 2, 71-87.

[74] Sornette D. (2003a). *Why Stock Markets Crash* (*Critical Events in Complex Financial Systems*). Princeton University press.

[75] Sornette D. (2003b). Critical market crashes. *Physics Reports*, 378(1), 1-98.

[76] Sornette D, Johansen A. (2001). Significance of log-periodic precursors to financial crashes. *Quantitative Finance*, 1(4), 452-471.

[77] Sornette D., Zhou W.X. (2006). Predictability of Large Future Changes in major financial indices. *International Journal of Forecasting*, 22: 153-168.

[78] Sornette D., Woodard R., Zhou, W.X. (2009). The 2006-2008 Oil Bubble: Evidence of Speculation, and Prediction. *Physica A*, 388: 1571-1576 .

[79] Stephens-Davidowitz, S. (2014). The cost of racial animus on a black candidate: Evidence using Google search data. *Journal of Public Economics*, 118, 26-40.

[80] Terasvirta T., Tjostheim D., Granger C. (2011). *Modelling nonlinear economic time series*. Oxford University Press, Amsterdam.

[81] Toda H.Y., Yamamoto T. (1995). Statistical inference in vector autoregressions with possibly integrated processes. *Journal of Econometrics*, 66, 225–250.

[82] Tong H. (1990). *Non-linear time series: a dynamical system approach*. Oxford University Press, Oxford.

[83] Tumarkin R., Whitelaw R.F. (2001). News or noise? Internet postings and stock prices. *Financial Analysts Journal*, 57(3), 41-51.

[84] Velde, F. (2013). *Bitcoin: A primer*. Chicago Fed Letter, December.

[85] Warriner A.B., Kuperman V., Brysbaert M. (2013). Norms of valence, arousal, and dominance for 13,915 English lemmas. *Behavior research methods*, 45(4), 1191-1207.

[86] Weber B. (2016). Bitcoin and the legitimacy crisis of money. *Cambridge Journal of Economics*, 40(1), 17-41.

[87] Weiß G.N. (2011). Are Copula-GoF-tests of any practical use? Empirical evidence for stocks, commodities and FX futures. *The Quarterly Review of Economics and Finance*, 51(2), 173-188.

[88] Weiß, G. N. (2013). Copula-GARCH versus dynamic conditional correlation: an empirical study on VaR and ES forecasting accuracy. *Review of Quantitative Finance and Accounting*, 41(2), 179-202.

[89] Woo D., Gordon I., Iaralov V. (2013). Bitcoin: a first assessment. *FX and Rates,* December 2013, Bank of America Merrill Lynch.

[90] Wood S. (2006). *Generalized additive models: an introduction with R*. Chapman and Hall / CRC, Boca Raton.

[91] Yelowitz A., Wilson, M. (2015). Characteristics of Bitcoin users: an analysis of Google search data. *Applied Economics Letters*, 22(13), 1030-1036.

[93] Yermack, D. (2013). Is Bitcoin a real currency? An economic appraisal. National Bureau of Economic Research working paper n. w19747.

[93] Zhao Y. (2015). Robustness of Forecast Combination in Unstable Environment: A Monte Carlo Study of Advanced Algorithms . Working paper n. 2015-04, Towson University, Maryland.

[94] Zhou W.X., Sornette D. (2003). 2000-2003 Real Estate Bubble in the UK but not in the USA. *Physica A*, 329: 249-263.

[95] Zhou W.X., Sornette D. (2006). Is There a Real-Estate Bubble in the US?. *Physica A*, 361: 297-308.

[96] Zhou W.X., Sornette D. (2008). Analysis of the real estate market in Las Vegas: Bubble, seasonal patterns, and prediction of the CSW indexes. *Physica A*, 387: 243-260.

[97] Zhou W.X., Sornette D. (2009). A case study of speculative financial bubbles in the South African stock market 2003-2006. *Physica A*, 388: 869-880.