UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI "M.FANNO"

CORSO DI LAUREA MAGISTRALE / SPECIALISTICA IN ECONOMIA E FINANZA – ECONOMICS AND FINANCE

TESI DI LAUREA

Cryptocurrencies and asset bubbles

RELATORE:

CH.MO PROF. BRUNO MARIA PARIGI

LAUREANDO/A: EUGENIO BEDESCHI

MATRICOLA N. 1137343

ANNO ACCADEMICO 2017 – 2018

UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI "M.FANNO"

CORSO DI LAUREA MAGISTRALE / SPECIALISTICA IN ECONOMIA E FINANZA – ECONOMICS AND FINANCE

TESI DI LAUREA

Cryptocurrencies and asset bubbles

RELATORE:

CH.MO PROF. BRUNO MARIA PARIGI

LAUREANDO/A: EUGENIO BEDESCHI

MATRICOLA N. 1137343

ANNO ACCADEMICO 2017 – 2018

Il candidato dichiara che il presente lavoro è originale e non è già stato sottoposto, in tutto o in parte, per il conseguimento di un titolo accademico in altre Università italiane o straniere.

Il candidato dichiara altresì che tutti i materiali utilizzati durante la preparazione dell'elaborato sono stati indicati nel testo e nella sezione "Riferimenti bibliografici" e che le eventuali citazioni testuali sono individuabili attraverso l'esplicito richiamo alla pubblicazione originale.

Firma dello studente

____

Ringraziamenti:

Ringrazio il professor Parigi per l’impegno profuso nell’aiutarmi a redigere questa tesi. Tanti preziosi consigli sono stati fondamentali per arrivare a questo risultato.

Ringrazio il professor Cappuccio per l’assistenza e i consigli nella stesura della parte econometrica della tesi. Senza la sua guida i risultati sarebbero stati inferiori.

Ringrazio i miei genitori e la mia famiglia per il supporto e tutti i sacrifici. Senza di loro non sarei qui.

Ringrazio le mie amiche e i miei amici, raggi di sole per la mia vita.

Index:

Introduction

Virtual currencies are financial innovations which started to capture growing interest from academics and the public. The distinctive features fueled the debate which now involves important institutions like central banks. Other than practical characteristics the discussion focused also on the exuberance of investors, who poured money into cryptocurrencies and produced the staggering rises in prices we have seen many times in news headlines.

This thesis aims to explore both sides of the discussion, the innovative features and the probable bubble in one of these cryptocurrencies: Bitcoin, the first one of a long series of virtual currencies.

The first section describes how these currencies work, and how they are different from a traditional fiat currency. It will be evident how, even if they show interesting characteristic they have some drawbacks considering an extensive use in the economy. The second section stresses why a central bank should consider about switching to a virtual currency, capturing advantages a fiat currency can’t provide. In the third section I will focus on Bitcoin, the biggest virtual currency by far considering market capitalization. I will discuss how investors perceive it as a hybrid asset class, and if considering its practical uses it is possible to have an idea of its fundamental value. In the last section I will consider the very likely possibility that Bitcoin is a financial bubble since its high price seems unjustified. I gathered many evidences pointing to investors exuberance and showed how returns are mainly driven by popularity and no economic factor. Lastly, I applied an econometric procedure to verify whether the price had an explosive behavior.

1.1 Security guaranteed by cryptography

A digital currency system is composed by a software that makes intensive use of cryptographic technology, a block chain storing information, digital wallets which resemble bank accounts and public ledgers where all transactions are recorded. The system is decentralized, meaning it's maintained by its users: there is no superior institution supervising the transfers of coins. The stability of the system is ensured by the information protocol (block chain), which aims to eliminate all the transaction factors which are based on trust (Szetela, Mentel, Gędek 2016), in fact each user doesn't know its counterparty and has to be sure not to incur in any fraud.

Moreover the absence of a central authority creates the need for a distributed verification of transactions together with the updating and accounting of transfers. Members of the network are incentivized to update the ledger and validate transfers by the processes called mining and validation. Cryptocurrencies in fact rely on two different methods to register new transfers: the proof of work (mining) or the proof of stake (validation). Proof of work is the most popular and according to Gervais et al. (2016) in 2016 powered the blockchains of more than 90% of the total market capitalization of existing digital currencies.

- The proof of work is characterized by miners who solve computationally costly problems to update the ledger, who are awarded new coins and transaction fees: something valuable to each user. The trust in the currency is established by having a competition for the right to update the record (Chiu and Koeppl 2017).
  This competition safeguards the ordering of each transaction on the block chain and on the ledgers. Transactions are placed in groups called blocks and are linked together to form the information protocol: the block chain. Each block has a reference to the previous block so that if someone would alter a specific block (for example tampering a transfer) each subsequent block would change as well. Mining consists in each miner grouping some transactions and proposing the next block to the network, so it happens to have many different proposed blocks at the same time.
  Here competition starts: to add a new block a miner has to guess a number which is the solution to a very hard cryptographic puzzle (Courtois et al., 2014): the text of the block is run together with information from the previous block and a random guess through a cryptographic hash function until the output is below a certain value.
  Cryptographic hash functions are a special class of hash functions that convert some input into a string of data of fixed size (the hash). A hash function is deterministic, in the sense that the same input always results in the same output, and should make

infeasible for two inputs to have the same output. The function produces the hash, a string of code, from the inputs, which the structure of cryptocurrencies' blockchain requires to be under a certain value (Figure 1).

By their nature the cryptographic hash functions used in these systems, like SHA 256 for Bitcoin, are structured in a way that finding the random guess such that the output is under the requested threshold takes a long time, and computational power. Numbers are guessed and together with the new transactions and information from the previous block are run through the SHA 256 until the resulting code meets the requirements. The information from the previous block is nothing more than the hash which was produced from the last block: so the last output of the cryptographic function is part of the subsequent input, all the blocks are linked.

A common feature of these functions is that it is impossible to get the input looking at the output (which is known to be under a certain value), so that the missing part of the input has to be guessed. The correct number which contributes to the creation of the right output is the so-called proof of work, which together with the block (containing the new transactions) is broadcast to the network. As any other participant can now verify that the proof of work and the proposed block plus the previous information, once hashed, give the right output, the new block is added to the chain.

This point is crucial: the right proof of work is difficult to find, it is time consuming, but the verification takes virtually no time. The miner is compensated with new coins and transaction fees to compensate for the energy spent finding the right proof of work. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended (Nakamoto, 2008).

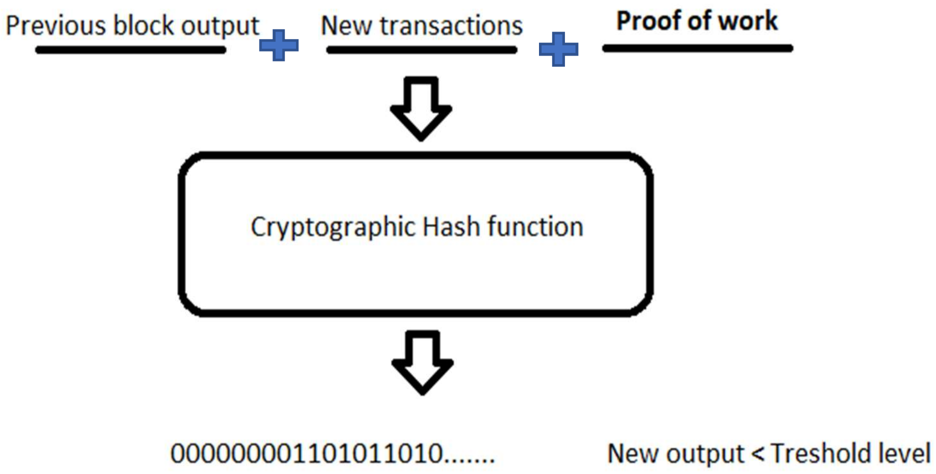


Figure 1. Mining the right proof of work

As a new block is created all the network participants update their block chains, as they always consider the longest chain to be the correct one and will keep working on extending it (Nakamoto, 2008). The use of these cryptographic hash functions grants security to the system, as each block is connected to the previous. If a malicious agent would like to alter a block (the transactions inside it) he would need to find the proof of work for that block (the input is changed) and find the proofs of work of all the subsequent blocks, which, in turn, will have their inputs changed. All in a very short period, as in the meantime the whole network keeps working and adding blocks on the "original" chain, which is very likely to extend the length of the accepted one. In a proof of work system security relies on the principle that no entity should gather more than 50% of the processing power because such an entity can effectively control the system by sustaining the longest chain (Gervais et al. 2016).

- The proof of stake is a different system which selects members who group transactions building the new blocks, and gain transaction fees. These members are called validators and receive an authorization by the network who allows them to update the blockchain. There is no competition in this case: each time a member of the network is selected and entitled to build the new block. The validator is chosen randomly, but it is easier to be selected if one owns a lot of cryptocurrency and has owned it for a long time (Siim 2018). The rationale behind proof of stake is that users with the highest stakes in the system have the most interest to maintain a secure network, as they will suffer the most if the reputation and price of the cryptocurrency would diminish because of attacks or frauds (BitFury Group 2015).

> Also the validator's coins are put into a vault for a period, and in case the validator validates a fraud transaction, he loses his stake as well as their right to participate in any such future events (Sharma 2018). The coins are the network's insurance: if after the creation of the new block the network detects irregularities the validator loses the stake. As long as the stake is higher than what the validator gets from approving fraudulent transactions the network can trust he is doing his job honestly, as he is incentivized to behave correctly.

The difference between proof of work and proof of stake systems leads also to very different environmental footprints. In the proof of stake case, when there is no competition energy spent is smaller as only one miner works to create the next block, something doesn't happen for example in the Bitcoin system where all the miners compete, and, as we will see later, burn a consistent amount of energy.

The cryptocurrency is the electronic token which is transferred between digital wallets relying on the cryptographic technology of the software. Digital tokens are associated to wallets on public ledgers which keep track of every transfer ever happened. In fact the ledger determines who has the right to spend the tokens and in which amount, there are no tokens kept in the wallet, which is simply an address or the public key plus a private key. This address is a string of code, composed by numbers or letters which anyone can see, and it is strictly linked to the private key, another string of numbers or letters, which needs to be kept hidden. In a cryptocurrency ecosystem, the public key can be considered as the participant's account number whilst the private key represents the participant's ownership credentials (Herbert and Litchfield, 2015). As just said the two keys are related, but there is no way to determine the private key knowing the public key. To transfer coins to another wallet or address, one needs to sign the transaction with the private key. This is simply done by putting both the private key and the transaction details (how many coins and to whom) into the relative cryptocurrency software. Then the program produces a digital signature which is sent to the network which can verify its authenticity by simply comparing this signature (which varies each time, depending on the transaction) and the public key, known to the network. This happens because the two keys, the private and the public are strictly linked. The private key is a function which produces the digital signature, then the network putting together the public key, the message and the signature can prove if the sender actually owns the private key, without the need to reveal it. Through the software each member of the network can understand if that digital signature was genuinely produced by the private key looking at the public key. Since the digital signature depends on the transaction or "the message" sent to the network, it is unique every time and can't be reused by malicious agents to steal tokens from one's address. Once a transaction is validated the network verifies that the sender has enough currency to send by running through the address history which is found on any ledger. This can be done by anybody since both the address (or public key) and the ledger are public. Hereafter the transaction can be included into a new block, which will seal the process of transferring coins from an address to another.

Cryptocurrency provides safety to the user: as long as the private key is kept secret there is no way to move the money from one address to another: a digital signature can't be produced. Furthermore the blockchain in a proof of work system relying on the hash function, prevents the substitution or alteration of whatever transaction, as it is extremely costly and unlikely for a malicious agent to control enough computing power to redo all the proofs of work and create an alternative long enough block chain. This agent is in a race versus all the network to produce the longer block chain, as the length determines the shared and recognized chain among users. This can happen theoretically only if more than the half of the computing power of the network is under control of this single individual. Moreover the cryptocurrency protocol adjusts the proof of work difficulty targeting an average number of blocks per hour. This compensates for the increasing hardware speed and computational power of the network, as it is easier to find proof of works the more computations are done in the system. For example, as reported by BitInfoCharts.com, the Bitcoin protocol targets a new block every 10 minute while Litecoin targets 2.5 minutes.

Instead in a proof of stake the system security is guaranteed by the stake which will not be given back if fraudulent transactions are approved.

1.2 Deflationary structure

As of 22/4/2018, the total market capitalization of cryptocurrencies is just under 400 billion dollars according to Coinmarketcap data, Bitcoin represents the 38% followed by Ethereum (15%) and Ripple (9%). Bitcoin, Ripple and many others have a predetermined limit on the coins which can be mined. Imagining one of these cryptocurrencies to be used extensively in an economy has very important implications.

The supply limit gives to the users the benefit of no devaluation risk, as according to the protocol new currency can't be created. On the contrary fiat currencies have this risk, as a central bank can deliberately decide to print more. At that same time this feature can be a drag as there can't be an expansion of money supply to respond to negative demand shocks. This could even worsen tough situations, tending to exacerbate recessions and could lead to a deflationary spiral, as during the Great Depression under the gold standard (Dong et al. 2016) or during the 1990s in Japan. Fiat currencies certainly have a devaluation risk but have a crucial advantage over virtual currencies when it comes to monetary policy. In fact, adopting a virtual currency with a cap on supply the policy makers would lose the option to increase money supply, lowering the nominal interest rate and leading to an increase in spending and investments, to smooth the business cycle. Moreover such a cryptocurrency would exert a deflationary force on the economy since the money supply would not increase in concert with economic growth (Yermack 2013). Because of this, the gold standard and sterling or U.S. dollar based international reserve systems evolved to economize on limited reserves (Redish, 1993,and Bordo, 1981). Yermack (2013) shares the same opinion: the gold standard probably collapsed as worldwide production of gold did not keep pace with economic growth. We can directly compare a cryptocurrency with predetermined number of coins to the gold as they have the same supply issues.

In a deflationary environment, consumers delay spending because expect future prices to be lower and businesses, especially relying on debt financing, will reduce investments as assets lose value rapidly as time goes by. For every economic agent, including the government, spending in the future is better than spending today, this leads to a deterioration in the demand of goods so that the deflationary process is reinforced, and economic growth is harmed. Fixed money supply leads to negative inflation as the economy grows, particularly if it gets built into price expectations that can magnify the negative impulse and increase the economic costs (Elwell 2012).

The fixed number of coins that can be created assures network participants from the central bank artificially devaluating the currency, but creates the problem of structural deflation into the economic system. As the cryptocurrency can’t be printed deliberately agents are reassured about its value, but such a rigidity is an issue.

Furthermore, this structural problem can even be worsened if some private keys are lost, leading to a loss of coins. As there is no way to obtain a private key from the public one, if the first is lost we can understand how the money supply is not only fixed but susceptible to irreversible reduction. Coins on addresses whose private keys are lost are frozen and gone forever.

1.3 No LORL

Beyond the problems of structural deflation and inflexibility to respond to shocks in the economy, current virtual currency systems don’t contemplate a lender of last resort. The global financial crisis showed the importance of institutions that can provide emergency liquidity both to financial institutions and lenders. For example, in March 2008 the Federal reserve offered up to 200 billion dollars to banks and financial institutions in 28-day cash loans and let the biggest investment banks on Wall Street borrow up to 200 billion dollars in U.S. treasuries, posting toxic mortgage-backed securities as collateral. According to Dong et al. (2016) even with flexible supply rules, it is hard to see how a decentralized virtual currency could generate the type of liquidity response needed during a financial crisis.

The lender of last resort, during periods of instability and financial distress protects individuals who have deposited funds and financial institutions trying to prevent customers from panicking and withdrawing. Bank runs occur in these periods when customers, afraid about institutions' insolvency withdraw funds as soon as possible, knowing there are not enough resources to satisfy any depositor. Cash isn't enough to pay back each customer since a bank keeps only a small percentage of total deposits as cash and engages in its normal operations such as lending to others: deposits are invested to generate long term assets, which if liquidated would result probably in a loss. In the situation where the bank's reserves fail to satisfy customers' requests the lender of last resort injects its funds so that withdrawals are met, and the bank remains solvent.

The most famous economic model describing bank runs is the Diamond and Dybvig's (1983), where it is shown that there are two possible Nash equilibria: depositors think the bank is solvent and withdraw only when needed, or depositors don't trust the bank and rush to withdraw knowing there is not enough cash to satisfy anybody. Note that also the second Nash equilibrium is self-fulfilling as any customer, expecting the bank to be insolvent, redeems its funds leading to the institution's insolvency. Any agent rationally expects the bank to fail and this ultimately happens as anyone withdraws. Introducing a government deposit insurance or a lender of last resort, which aids banks during distress, can eliminate the bad Nash equilibrium: the lender guarantees each depositor will have its cash in case of need, therefore the risk of not being able to redeem deposits its eliminated. If the lender of last resort proving this kind of insurance and aid to the banks is credible, the insurance is ultimately never used, but runs are anyway prevented.

Then in an economic system relying on a virtual currency, commercial banks are more susceptible to runs because there is not a trusted third party safeguarding the stability of the system. The decentralized currency environment bases its foundation on the absence of a central authority, the central bank, which in modern economies is usually acting as the lender of last resort. The system is a peer to peer network and even if there was a central authority providing this service, how would members decide when the lender must act? Also, for the cryptocurrencies with fixed supply, the lender couldn’t print money and rely just on resources kept aside.

1.4 No insurance on deposits

No form of insurance has been developed for owners of any virtual currency comparable to the deposit insurance bank customers enjoy in advanced economies. Deposit insurance is a measure designed to protect bank depositors, normally up to a certain amount, from losses caused by a bank’s inability to pay obligations when due. This insurance, which now is present in many countries, promotes financial stability. As reminded above banks, collect deposits, lend long-term and if bank’s borrowers fail to repay bank’s creditors (including depositors) risk loss. Banks in financial trouble are exposed to runs but, with the presence of deposit insurance, which is often provided by the sovereign, depositors are less inclined to withdraw, and panic situations are rare.

Virtual currency protocols don’t contemplate a “deposit insurance” function, therefore if a bank would choose to fund its activities in virtual currency and lend virtual currency, it would be much more fragile than banks utilizing a fiat currency, with sovereign deposit insurance. This is probably one of the reasons why a bank relying on virtual currencies for funding and lending doesn’t exist. The only services which collect and lend cryptocurrencies are peer to peer platforms like Ethland, where members borrow and lend to others. Therefore the platform can’t be the defined a bank as it limits its activities to bringing together potential borrowers and lenders, who bear all the risks.

1.5 Problems about usual currency functionalities

Typically, a currency conforms to three classical properties: it is a medium of exchange, a unit of account and a store of value.

- As a medium of exchange actual cryptocurrencies perform poorly. According to data available on BitInfoCharts.com the average daily number of Bitcoin transactions for the past two years has been well under 350.000, for both Ripple and Ethereum under 1 million. Differences in volumes are mainly due to the absolute value of these currencies, as a Bitcoin is worth more than ten times an Ethereum and more than ten thousand times one Ripple. Perhaps even assuming that all these transactions were conducted to acquire products and services, and it is known that in the period these assets have been targeted by speculators, the combined value of these transactions pales in front of transactions processed by competing services like Visa. The credit card company reported an average of 227 million daily transactions in 2016; the figure rose to 304 million the following year. With more than 7,6 billion people in the world, with many executing multiple transactions a day, crypto currencies seem to have a negligible market presence, even completely neglecting speculation. On top of that Glaser et al. (2014) found that most users of Bitcoin treat their investments as speculative assets rather than as a means of payment.

Moreover the majority of businesses do not accept virtual currencies to clear payments. Bitcoin, which is the most popular, at the end of May 2018, is only accepted in 12.633 venues, according to coinmap.org, which maps on daily base the number and location of businesses accepting Bitcoins around the world. Some large retailers like Dell, Microsoft and Expedia allow for Bitcoin payments but they never receive it (Kroeger and Sarkar, 2016), they rely on third parties like Circle Internet Financial who for a fee receive Bitcoins and send dollars to the retailer.

Finally, the last issue regarding virtual currencies as effective means of exchange regards the number of transactions the relative network can handle. For example, Ripple has the smoothest system and is able to process up to 1.500 transactions per second, still well under the 24.000 of Visa. On the contrary the Bitcoin protocol can process just 7 transactions per second. The amount of transfers that can be registered into the relative blockchain every second has to do with the time it takes to add a new block to the chain. This time is set arbitrarily by the protocol: for example, Bitcoin allows for just one block to be mined every ten minutes. The time is kept under control requiring different effort to find the proof of work: if the computational power on line is relatively high, the threshold for a successful mining is set very low. The lower the number the more the time required.

- For a currency to be effective as a unit of account, consumer should be able to use is it as a numeraire when comparing prices of alternative goods. Crypto currencies share the common theme of volatility; hence retailers have to recalculate prices on a day to day bases if not on an hour to hour basis. This practice is very costly, a less volatile currency is likely to keep these menu costs down. Yermack (2013) argues that this issue could be solved if the whole economy used the crypto currency in transactions, but as of today no place in the world adopts a virtual currency as main means of exchange.

  Another problem regarding certain cryptocurrencies and their unit of account function is that they are relatively expensive. As of mid-April 2018 a single Bitcoin costs around

8.000 $, one Ethereum 600 $, a Bitcoin cash 1.100 $: to quote prices for most of the goods purchased daily the price needs to be quoted in four or more decimal places. An ice cream would cost 0,00032 Bitcoin or 0,0045 Ethereum. There are no any other currencies in the world for which prices are quoted in these units: to the consumer it could be misleading to switch to such quotes, to a retailer would imply adopting new electronic labeling and make most of the software products which accommodate for only few decimal points useless. Sometimes economies have prices which divert from small integers, but this usually happens in the opposite way: the same ice cream would cost 327 ¥ in Japan. The impact of heuristic in marketing research has been proved for example by Markowitz at al. (2009). One problem is the difficulty of computations for consumers confronting prices of goods: with prices expressed in decimals, something the consumer is not used to, the smallest error would imply paying a good ten times more.

- Finally, the last function a currency has to satisfy is the store of value. Virtual currencies have no intrinsic value such the commodity content of gold and don't pay dividends. Neither they have extrinsic value such as the value assigned to traditional fiat currencies by the trusted public issuing authority (Mersch 2018). In fact, the trust in a central authority is substituted by the safeness of the algorithms shaping the platform.

  To own a coin an agent exchanges his goods or services recognizing they have the same value. Later when the currency is spent the agent expects to receive a similar value. Cryptocurrencies are much more volatile than fiat currencies making them less likely to be used by consumers, who don't want the risk to experience sudden devaluation. For example, the daily volatility of Bitcoin and Ethereum against the dollar during the last two years was five times more than the volatility of established fiat currencies like the Pound or Yen (see table 1.1).

Table 1.1

Currency pair	EUR/USD	JPY/USD	GBP/USD	BTC/USD	ETH/USD
Daily standard deviation	0,478%	0,709%	0,722%	3,960%	6,595%

Daily volatility of exchange rates from Investing.com from 01/01/2016 to 01/01/2018. Rates for Ethereum/USD are from 10/03/2016.
Standard deviation calculated as Sample standard deviation.

Not to mention the fact that it is easy to see huge daily swings in cryptocurrencies' values: on the same period considered in table 1.1 there were 113 days when Bitcoin appreciated or depreciated more than 5% against the USD, more than one day a week. Bitcoin prices appear to be particularly susceptible to market sentiments and dramatic boom-bust episodes (Cheah & Fry, 2015) undermining the store of value function this virtual currency might play. Kroeger and Sarkar (2016) share the same opinion on Bitcoin: large exchange rate volatility and negligible correlation with traditional currencies undermines its usefulness as a unit of account or a store of value. The same reasoning can be applied to other virtual currencies which share similar volatilities: as VCs exhibit wild fluctuations in value, they can't be trusted as a store of value (Mersch 2018).

Becoming more spread among the public doesn't seem to help a virtual currency to mature. If we consider Bitcoin, which was the first virtual currency and still the most popular we can see how volatility didn't reduce as it became better known and accepted more frequently by businesses (for example the first physical venue accepting Bitcoin was recorded by Coinmap.org in March 2013). In table 1.2 I report the daily volatility of Bitcoin exchange rate with USD from 2011 when the price was still around 0. The first year considered in this sample shows the daily volatility was 8,20%, which decreased the following year before increasing again to 6,41% in 2013. From 2014 it began to decrease and reached a low of 1,90% in 2016, still far from an established fiat currency as seen in the three examples in table 1.1. In 2017 and 2018 volatility increased to values closer to 2013 and 2011 values rather than keeping decreasing.

Table 1.2

	2011	2012	2013	2014	2015	2016	2017	2018
Daily standard deviation	8,20%	3,49%	6,41%	3,32%	2,92%	1,90%	4,51%	5,16%

Daily volatility of exchange rates between BTC and USD from Bitcoin.com from 01/01/2011 to 17/01/2018. Standard deviation calculated as Sample standard deviation.

2 Could central bank be interested in adopting a digital currency?

Decentralized crypto currencies are exerting pressure on central banks, which started to pay more attention to these virtual currencies and blockchain technology: the People's bank of China aims to develop a nationwide digital currency based on blockchain technology; the Bank of Canada and Monetary Authority of Singapore are studying its usage for interbank payment systems; the Deutsche Bundesbank has developed a preliminary prototype for blockchain-based settlement of financial assets (Koeppl 2017). In fact, coopting the technology central banks could maintain more power and control over policy than ever before (Ranskin and Yermack 2016).

The advantages of the adoption of virtual currency based on block chain technology are multiple and they come mainly from the independence from any central authority, and decentralized form of record keeping. First the block chain adoption allows for high security and transparency: each transaction is recorded on the ledger and it is very hard, if not impossible, to alter the register. As of today, it never happened to any crypto currency ledger to be altered. The public ledger allows any user to see the complete record of transactions, from user to user. The legitimacy of records is purely driven by the mathematical rules that allow for new blocks (containing new transfers) to be added to the chain, therefore removing the need for sponsor (the central bank) to play the role of enforcer or gatekeeper on the network (Ranskin and Yermack 2016). Eventually all the central bank policies could be reduced to a set of algorithms acting through the virtual currency protocol. Monetary policy, and growth of money supply for example would be preemptively set into the code, leaving no room for trust issues.

Other important issues the virtual currency could solve replacing the paper currency, thanks to its transaction recording system, are the various creating the "Curse of cash" (Rogoff, 2016).

2.1 The curse of cash, replacement of paper currency

In the Curse of cash (2016), Rogoff describes the many problems economies and societies have to face due to the high reliance on cash. Fiat currencies entails inevitably tangible cash, notes and coins, which once minted are practically out of central bank control. Cash, which is not traceable, ends eventually in the underground economy. The author argues that cash facilitates too much financing of tax evasion, corruption, terrorism, drugs and human trafficking, especially large denomination notes. Tangible currency seems to be the safest way for routine use to largescale criminals or businesses to hide illicit revenues, moreover is the most liquid means. No comparable properties are found in other assets or commodities like gold, and diamonds which often are subject to reporting requirements once sold.

Another famous problem of paper money is that it reduces the possibility of central banks to conduct a completely effective monetary policy. As the economy falls in a very deep recession the central bank could want to reduce the nominal interest rates below zero, to encourage consumption and investments even more. As such negative interest rates erode wealth kept idle in bank accounts this would be a very powerful tool. Lowering interest rates to negative levels would temporarily raise aggregate demand and strongly incentivize banks to lend out excess reserves (Rogoff, 2016). Instead in presence of high cash balances, the situation of U.S., Japan and the Euro area, among others, this measure is ineffective as the nominal interest for whoever holds cash is 0 and can't be lower. Therefore, monetary policy is bounded, as paper currency nullifies the effect of possible negative rates.

A virtual currency replacing completely actual paper currency could help alleviate these problems. As coins are not tangible and are registered on a ledger the central authority could effectively enforce a negative rates policy because cash couldn't be hoarded anymore. Also, with the complete history of transactions available illicit funds and activities could identified more easily or at least, removing cash, criminals should find another way to move or exploit their proceeds.

2.2 Elimination of zero boundary of monetary policy and Improved transactions transparency (at the expense of privacy)

Following the financial crisis, short term interest rates in most countries have fallen sharply in many of the most important economies in the world, namely U.S., Euro area and U.K. In Japan interest rates have been under 2% since the 1994. Additionally, all these central banks have engaged in unconventional monetary policy operations to sustain economic growth and inflation. Q.E. programs were extensively used, still inflation targets remain far to be met: in Europe last reading was 1.3% year-on-year and in Japan was 1.1%. Both central banks despite massive Q.E. programs and record low interest rates haven't succeeded in stimulating inflation to their 2% target. According to Haldane (2015) the need for unconventional measures arose from a technological constraint: the inability to set negative interest rates on currency.

A central bank's balance sheet has on its liability side deposits from banks and currency with the public. Monetary policy under normal conditions involves managing the interest rates on the reserves banks must keep. It is possible to set negative interest rates on bank reserves, but it is impossible to do the same on currency. There is an incentive to switch to currency whenever interest rates on reserves turn negative Haldane (2015).

With a digital currency controlled by the central bank each person would have a number of coins accredited on the ledger. Whether this ledger is public or administered exclusively by the central bank, the zero-lower bound of monetary policy is eliminated. Monetary policy would become much easier for the central bank to implement under a digital currency system (Ranskin and Yermack 2016) as not only interest on reserves but also on currency could be handled. The central bank would gain the ability to set negative interest rates on public deposits and probably meet its inflation and growth targets more easily. Since all deposits are registered on the ledger there is no way to hoard cash. This measure could be very effective but, as Ranskin and Yermack (2016) underline it could be difficult for citizens to see the broad public benefits of an interest policy carrying the erosion of some of their cash from computer memory.

A central bank-controlled ledger, and the ability to track each transaction ever happened on the chain, would also allow for easier inspection of an individual's finance. The authority could determine how much money the person ever owned and where he or she spent it. Thinking about illegal activities who rely on cash the concept has a very important implication: whatever cash transfer used to pay and finance crime which today leaves no proof, would leave an indelible trace on to the block chain. The fight against crime would find its best ally in the elimination of the most liquid and accepted means of transfer: paper currency. Rogoff (2016) shares the same opinion: circumscribing cash will not end crime and terrorism, but it would deal them a significant blow as a new and perhaps less effective means would be needed.

These benefits wouldn't come without disadvantages, as people would be giving away their financial privacy to the government. That's probably a reason why many hold cash and an eventual switch to virtual currency would take a long time. A strong regulation and supervision on who can control and use these data would be required in order not to create temptation for abuse.

2.3 Possible Elimination of banks with ledger kept by central bank

The switch from paper currency to a cryptocurrency backed by the central bank could have another implication other than helping fighting crime and empowering monetary policy. With a virtual currency once the protocol has been defined any agent has a private key and an address, to send and receive money. Reducing each deposit form to inputs on a ledger simplifies drastically accounting issues and this could undermine the role of commercial banks. According to Koning (2014) in the case of a central bank-maintained ledger, consumers and businesses would be permitted to open accounts at the central bank itself. Central banks historically have not taken deposits from the public, because the incredible volume of required record-keeping and customer contact would be overwhelming (Winkler, 2015). Digital technology overcomes these concerns (Raskin and Yermack 2016); exploiting computer storage and cloud servers it would be easy to process and keep track of large numbers of transactions. Not to mention the normal capabilities of the blockchain, which allows to have the complete history of verified transactions.

In the case the public were allowed to keep accounts directly at the central bank, deposits would shift gradually outside commercial banks. Since the central bank is perceived as more stable this is a natural implication. Hence the entire industry would shrink, as with less deposits it couldn't finance the same amount of assets. In such a scenario, where the deposit taking function would be not reserved to commercial banks the danger for this sector of the economy would be real. Banks would lose their main source of funds and the economy would have access to a smaller offer of credit unless these institutions raised more and more capital. Lending would inevitably be reduced and probably costlier, as nowadays banks' main source of finance are deposits which are remunerated at very low rates (much lower than equity).

Less credit in the economy is the potential drawback, but there are also benefits. Private accounts at the central bank would solve many problems of the current banking system. As commercial banks would be financed with more and more capital, substituting lost deposits, bank runs, and bailouts would become even more rare.

With more equity on the balance sheets the stability of the banking system would increase, and government intervention would be reduced. This would be a consequence from the change in the banks' liabilities structure: as banks would be financed mainly with capital, moral hazard problems should be relieved: institutions relying more on proprietary capital and on less third-party funds don't take excessive risk. Therefore, the need for government emergency intervention could be significantly reduced. Government bailouts in troubled situations could be avoided, as financial institutions, becoming smaller and smaller, due to the outflow of deposits, would become less dangerous to the financial system and the economy.

2.4 Credibility of a fixed scheme determining quantity of money in circulation

As Dong et al. (2016) stress most cryptocurrencies systems (including Bitcoin), contemplate a limit on the amount of currency that may ultimately be issued. This is exactly the opposite of fiat currency, which can be created deliberately by the central bank. In fact, the limit on virtual money supply, together with the use of cryptographic features, was specifically designed to enhance the trust in this means of transfer. As supply is limited the public is ensured that the risk of arbitrary devaluation of the currency is eliminated. This risk is real in economic systems where agents use fiat currency and rely on the trust of the central bank and the government.

In the case the central bank has problem establishing trust among the public the switch to a fixed-supply scheme crypto currency would be helpful. Digital currencies could offer a country struggling with a mismanaged money supply a way of creating stability (Raskin and Yermack 2016).

Countries experiencing high inflation rates like Argentina or experiencing severe currency devaluation like Iran are examples of how a digital currency could and did offer benefits to an economy. In 2012 the riyal, the official Iran currency, fell from 20.160 to 36.500 against the USD in a matter of two months, a devaluation greater than 50%. Raskin (2012) reports how some Iranian switched to Bitcoin to preserve their wealth.

The case of Argentina is somewhat similar as the country experienced inflation rates higher than 10% for the last 7 years, reaching 40% in early 2016. Popper (2015) explains how Bitcoin is a principle choice like the USD for Argentinians who want to get rid of Pesos. According to the author, thanks in large part to their country's history of financial instability, a small yet growing number of Argentinians were using Bitcoin as a store of value and a medium of exchange. Also, a small number of freelancers were using the virtual currency to get paid by overseas client. They were adding the benefit of capital control avoidance to the store of value perceived in Bitcoin (Popper 2015). The fact that a Bitcoin wallet can be accessed using encrypted connections making transfers anonymous makes it hard for authorities to control the problem since what is reported is just the public address, not reconcilable to a real identity. In this case Argentina could try to tax Bitcoin wallets, something like what's happening in the US (where Bitcoin is taxed whenever is bought sold or traded), but its users have ways to hide their belongings, possibly sending them abroad.

Hyperinflation like the one experienced for many years in Argentina could lead a central bank to adopt a virtual currency with a fixed supply scheme to regain the public trust. As the protocol defines the money supply people are reassured the central bank can't devalue the currency arbitrarily. The built-in scarcity of Bitcoin lead people to think about it as a digital gold.

Ecuador is an example of a government trying to capture some of the cryptocurrency benefits. With the 24/7/2014 resolution Ecuador national assembly decreed the establishment of a national virtual currency, the dinero electrónico. It is used alongside the USD, the official national currency, adopted in 2000 as an attempt to slow its very high inflation. Officially the currency would also help the country to save money from replacing deteriorated notes with new ones. Perhaps the virtual currency issued directly by the central bank doesn't include a complex system with a fixed supply as Bitcoin or Ripple. It is a simpler payments system, that citizens can use to exchange the virtual currency controlled by the government and tied to the dollar (Rosenfeld, 2015). It is a centralized currency, but since it is not founded on a protocol contemplating a clear and stable money supply, the benefits of trust are missing. People still rely on the central bank and government to assume the currency has some value, in this case Ecuadorians trust the USD, to which the dinero electrónico is tied.

2.5 Necessity to provide the needed flexibility to the scheme to smooth business cycles

Summarizing the cryptographic innovations a virtual currency brings to policy makers are multiples. Substituting paper money with a series of entries onto a ledger guarantees all the currency is traceable, threatening crime and improving monetary policy. Security and stability are ensured by the structure of keys and cryptographic functions, which also contribute to establish the high level of trust in institutions missing in some countries. A predetermined money supply can rule out the possibility of sudden devaluations, which the government might enact to push exports or cut the real value of debt denominated in local currency. Also, for countries which rely on currency issued by a third country, the switch to a virtual currency entails an additional benefit. These countries forego any seigniorage benefit since they can't print their official currency, but they still incur costs to replace spoiled notes. Even by adopting one of the established crypto currencies could provide the trust the government lacks and be a source of savings.

These benefits come also with a potential drawback. How virtual money is minted and transferred is at the foundation of the entire system, but as explained before, if the money supply is capped, as time goes by and the limit is reached, the risk is deflation. According to Dong et al. (2016) a central bank issued virtual currency could be designed in principle to allow for an expansion of the money supply. The possibility is the creation of a more flexible protocol, without a cap on total supply, preserving anyway the trustworthiness of the predetermined scheme. The protocol could contemplate since the beginning a growth in the money supply together with transaction volumes or the gross domestic product.

The definition of this flexible protocol leaves open the door to solve many of the virtual currencies' problems outlined above. Other than solving the structural deflationary threat (not setting a cap on money supply), the scheme could entail expansions of monetary base to respond to temporary shocks and a lender of last resort function. In this way a central bank could maintain the benefits of a virtual currency and the typical monetary policy instruments to stabilize the business cycle. The key point is to balance the tradeoff between the gains from flexibility and the potential loss of trust. Outlining in detail in advance how new coins can be minted is crucial: for example, how money supply could be expanded if consequent quarter on quarter gross domestic product figures drop by a certain amount. Specifications like this one can help the central bank maintain credibility and avoid the new money to be viewed like mere entries on a ledger which can be modified pressing a keyboard key.

Moreover as, Raskin and Yermack (2016) suggests there would be an expansion in the monetary policy tools. The concept of open market operations to stabilize the economy could translate directly the intervention on people's balances, that could even be targeted to certain subsegment of citizens. For example, the target could be a certain area, hit severely by a shock or a specific demographic group. The effectiveness of these policies could be real, also the central bank could see real time the effects of these policies as the transactions flow onto the ledger. With the data provided the regulator would learn much more about the economy, the financial sector and effects of shocks and policies. Therefore, adopting a well-defined currency protocol and maintaining the ledger the central bank would gain even some innovative tools to understand and intervene in the economy.

2.6 Introducing the cryptocurrency

Introducing a cryptocurrency backed by the government could be relatively easy in countries which already rely heavily on electronic payments and less on cash. Northern European countries like Sweden, where cash in circulation has dropped to the lowest level since 1990

(Billner 2018), and Denmark, where only 23% of payments are carried out in cash (Danmarks Nationalbank 2017), are an example.

The introduction of this new currency should be gradual, as should be the phasing out of paper money (Rogoff 2016). This to give time to consumer and businesses to adapt to and gain trust in the new means of transfer. For a quite long period of time both paper and virtual currency should be accepted, so that there is no sudden transition. Koning (2014) in its "Fedcoin" hypothesis outlines how the two different types of moneys would coexist in the transition. The central bank, in this case the federal reserve, would provide perfect convertibility between the two liabilities, paper and electronic money. As a consequence a coin can be created only when a note is destroyed. Vice versa a coin can be destroyed only if a new note is printed. As the virtual currency is bound to the physical by a precise exchange rate and can be converted back into notes, the difference between the two types of currencies is extremely thin. As time goes by the shift to virtual currency could be accelerated for example not allowing to exchange from virtual to paper anymore. Another very important step the government should take to legitimate the new currency is to accept tax payments made with it. As Davies (2017) argues, by insisting a person can't pay taxes with anything else, governments create a guaranteed demand for the otherwise worthless pieces of paper they create. So, the same could be done with new virtual currency, as the government accepts it for tax payments, the same should be done by other agents in the economy. In Ecuador the government followed this step, as the central banks officially states all public-sector institutions accept Dinero electrónico as a means of payment.

Ultimately the most important issue the government should face is privacy. Particularly with a centralized crypto currency and ledger as described by Koning (2014). The power of knowing in any moment the finances of each citizens is something very hard to accept for the public, many people hold currency purposely to hide their belongings. The Ecuadorian central bank maintains a centralized system; hence it is very easy to check how much money there is on an account. However, since in this case the virtual currency coexists with the paper currency this problem isn't real as citizens afraid of the government can hold cash. Before the implementation it should be well defined when and how the authority should investigate movements on an account.

3 What could explain the price of Bitcoin?

Bitcoin is the most prominent virtual currency, it was the first and thanks to its first mover advantage it’s still the most popular. According to Coinmarketcap data, Bitcoin represents just less than 38% of the whole market capitalization of all cryptocurrencies, which are more than 1.600. At present the total market value of coins is a little above 140 billion dollars. Trading in this virtual token has increased very rapidly over the last years: as reported by Yahoo! finance the average volume of Bitcoin traded in 2014 was 5,2 million a day, it quadrupled the following year, kept increasing and exploded in 2017 with more than 500 hundred million coins traded each day. The figure doubled in the first months of 2018. Figure 3.1 shows Bitcoin price since its very beginning. Until April 2011 it was worth less than a dollar, two years later, in April 2013 it surpassed 133 dollars. At the end of 2013 broke the 1.000 dollars mark before deflating to 200 in January 2015. Then the climb began and in almost three years, on 17/12/2017 it closed at its all-time high of 19.194 dollars (+9.597% from January 2015). The price declined rapidly to less than a half of the peak value, and at present, 1/5/2018 stands at 8.985 $.

Figure 3.1

What could sustain such evaluation? Why people around the world decided to invest so heavily in this virtual currency? Is it really worth is price or is it just the next bubble? I try to give an answer in these last two chapters.

3.1 Currency or commodity?

Investors sees Bitcoin surely as a financial innovation and place it in between a currency and a commodity. Like others form of money Bitcoin can be exchanged for some good and services, even if they are mainly online stores, physical store acceptance is very rare (as previously reported, a little more than 12.600 stores accept it). Aside from being accepted as a means of exchange, Bitcoin hasn't much in common with traditional money as, apart from a line of computer code, it has no physical presence. Whelan (2013) argues that Bitcoin is very similar to the dollar, he stresses how they both have no intrinsic value and they are primarily used as means of exchange with the main difference being that there is no institution backing Bitcoin.

Bitcoin has also some peculiarities that make it similar to commodities: Bitcoin is fairly liquid as one can exchange any currency for bitcoin at any time, but due to its scarcity it has liquidity limitations like other commodities (Dyhrberg 2016). A commodity usually is defined as a basic good used in commerce, like copper, livestock or oil. The prerogative of these commodities is they get consumed during the process; Bitcoin certainly doesn't share this aspect and therefore has much more in common with another commodity: gold. Both play an instrumental role in trade. They are scarce and with a finite supply: gold production is restricted to some geographical areas and new mines are hardly discovered; similarly, Bitcoin has a built-in scarcity, the supply is limited at just under 21 million. This feature of Bitcoin was purposely designed to mimic the gold scarcity, also the process of mining and its evolution in time was designed to resemble the production of gold. As time goes by mining new Bitcoins is harder, more time and computations are required. Another similarity is that both gold and bitcoin supply is not controlled by any state or institution, and both products have the same means of exchange (Weber 2016). Moreover both derive most of their value from the fact they are scarce and costly to extract (Dyhrberg 2016), they have little or no intrinsic value. Gold has some intrinsic value: it is used in jewelry, electronics and aerospace for example, but it is likely this doesn't justify its current market value (Dyhrberg 2016). Gold derives its value mainly from its store of value function, something that Bitcoin doesn't completely share: it is scarce, but its high volatility makes it unlikely to be seen as a comparable safe haven. Furthermore, Bitcoin requires a technical network and energy input to exist, if it loses the critical mass of computation, it becomes utterly unfeasible and therefore could be seen as a store of value within but not outside the network (Peetz and Mall 2017).

As we have seen it is difficult to reconcile Bitcoin to an existing financial asset. Dyhrberg (2016) explores if Bitcoin behaves like a well-known financial asset or as something in between a commodity and a currency, analyzing its volatility and how its price responds to movement in gold and the euro dollar exchange rate. Her analysis shows that Bitcoin has many similarities to both gold and the dollar, it is somewhere in between a currency and a commodity due to its decentralized nature and limited market size (Dyhrberg 2016). Medium of exchange characteristics are clear and the virtual currency reacts directly to the federal funds rate which suggests that Bitcoin behaves like a currency. Anyway, it doesn't behave exactly like a currency as it is unregulated and decentralized. Most aspects of Bitcoin are similar to gold as they react to similar variables in Dyhrberg's model, it possesses similar hedging capabilities and reacts symmetrically to good and bad news. Her conclusion is that Bitcoin in the market has a position between gold viewed as pure store of value and a currency as pure medium of exchange. Therefore, it could be a useful tool for portfolio management, risk analysis and market sentiment analysis (Dyhrberg 2016).

3.2 Real assets since it is software using energy?

As just said Bitcoin isn't a regular financial asset, also because it doesn't pay dividend and doesn't represent a claim on any right. To mine Bitcoins, finding the right proof of work to create a new block, a sensible amount of energy is needed. Peetz and Mall (2017) following the definition of Soddy (1926), argue that as Bitcoin is a software needing energy to exist, is a real asset. As a real asset, such as the internet itself the law of entropy applies: continuous blockchain and software usage isn't sustainable unless energy is always affordable and available, as a continuous stream of fresh energy is necessary for the continuous working of any working system (Soddy 1926). As of the first days of May 2018 according to the Bitcoin energy consumption index, to add new blocks to the blockchain an estimated 64 TWh of energy are needed each year.

The amount of electricity that the Bitcoin network consumes to work, mine new coins and settle transactions is close to the Czech Republic consumption according to the IEA (2017), an industrialized country where more than 10 million people live. The same amount of energy could power more than 6 million American households on an annual basis. The price of Bitcoin incentivizes people to run power intensive computers as mining can provide a consistent stream of income. The amount of resources invested is so heavy that by December 2017 the aggregate computing power of the bitcoin network was nearly 100.000 times larger than the world's 500 fastest supercomputers combined (Holthaus 2017). As Bitcoin network grows, the right proof of work to mine new coins are harder and harder to find and require more computations and therefore energy. The difficulty increases as the network automatically targets a number of blocks to be mined in an hour, adjusting for the online computational power. Holthaus (2017) claims that at current growth rate, the electricity demanded by this cryptocurrency network could equal the world consumption by the first months of 2020. In practice, the energy consumption should decline over time as I will explain. This amount of energy to process transactions is really inefficient compared to other systems: one single transaction according to the Bitcoin energy consumption index data requires 878 KWh, while Visa with less than a quarter of the same amount of energy proceeds 100.000 transfers on its circuit.

Miners are willing to invest this great amount of energy as the price of Bitcoin, which averaged at little more than 8 thousand dollars in April 2018, justifies the investment. Fortunately, for the stability and the future feasibility of the network Bitcoin's energy consumption is defined to fall in the long run (Lee 2017). Energy consumption isn't tied to the number of transactions, which is fixed. Instead, the amount of energy burnt is linked to the amount of coin awarded after each block is created and the Bitcoin price. Currently this reward is 12,5 Bitcoins, which halves every four years. Lee (2017) does argue that the system will not necessarily impose higher environmental costs as revenues from mining new coins will be halved every four years. When the mining industry's revenue falls by half, its energy consumption should fall by the same proportion, since, if it didn't fall, mining would become an unprofitable activity (Lee, 2017). As noted above Bitcoin has some useful properties, but as a mean of payments, at least for number of transactions processed per second (see section 1.5) and environmental impact, it seems inferior to others established competitors like Visa. Still its high price justifies huge investments by miners.

3.3 International transfers

International transfers represent clearly an advantage for Bitcoin users. While the international money transfer market involves numerous intermediaries in addition to central banks (Raskin and Yermack 2016), Bitcoin structure makes borders transparent. Virtual currency can be transferred from a wallet to another, no matter where they are located on the network. Also, the time is reduced importantly: the transaction can be incorporated into a new block within 10 minutes and assumed to be verified after 60 minutes. On the contrary with providers like Western Union the transfer, between countries, could take some days.

Bitcoin supporters have promoted the currency's ability to lower transaction costs, especially in terms of fees. These lower costs could be captured both for small and big transfers. Many companies have flourished proposing remittances services around Bitcoin. For example, Abra founded in 2014, counting also American Express as an investor, offers digital wallets to customers who can receive and send money without visiting a branch and without paying fees. BitPesa is very popular in Kenya, and as Abra, gives the ability to send money to those who don't even have access to a bank account. Coins.ph similarly serves the Philippine market offering a virtual wallet that allows users to buy and sell Bitcoins, also allows to exchange coins for Philippine pesos. These services primarily appeal to people who send or receive remittances and they charge no fees other than transaction fees charged by Bitcoin network. Cost advantages are determinant also for big transfers. As reported by the Boston Fed (2014) large-scale money transfers may also be cheaper if done through the Bitcoin network as wire transfers in the United States can run as much as 30 $ per transfer domestically and 50 $ internationally.

The potential disadvantages of these services are due to the conversion process. Sending money from a country to another via one of these services introduces a new step in the conversion process, for example to send money from the United States to Philippines first USD are converted into BTC, which are sent to the new wallet and converted again into PHP. Essentially users add a third currency, instead of going directly from USD to PHP. This could increase frictions as we know BTC is extremely more volatile than traditional currencies, some value may be lost even if transfers are very fast. Such a transfer could require even just 30 minutes, as three blocks are needed, one for each transaction. The last potential disadvantage can be liquidity: BTC are exchanged into currency through an exchange, now if users have to convert BTC into USD they can easily find a counterparty, but for third world currencies on a local exchange this can be hard. To conclude even if transfers are usually low cost in terms of fees it must be considered the potential loss caused by the high volatility of Bitcoin and possible low liquidity.

Bitcoin and services rotating around it are targeting mainly the market for remittances: in a 2014 report Godman Sachs underlined that the average cost for remittances was 9,8% compared to an average of 1% charged by Bitcoin wallet application providers. Since then many things have changed, and the cost advantage Bitcoin provided is in question. Traditional remittances services have cut costs for users significantly and increased their speed: in its 2017 annual report on remittances prices worldwide the World Bank points out that the average cost for sending 200 $ has been reduced from 9% to 7,2% in the last four years. International transfers once the niche where Bitcoin services had no competitors, because of their low or null fees, are now offered by traditional money transfers services for very low charges as well. For example, Western Union, the incumbent in this market, charges no fees to transfer 200 $ from a US bank account to India (but earns 0,3% exchanging dollars for rupees). However, the transfer is quite slow, taking 4-5 business day as reported on the corporate site.

As traditional providers have cut costs, the cost for Bitcoin transfers has increased dramatically over the years. The network contemplates some transaction fees, as miners are compensated for the mining effort with fees and new coins. The higher the transaction fee a person is willing to pay the higher the probability the miner will include it into the newest block, so that he will receive that fee. As the new Bitcoins created are always less (by design), fees become more and more important for the miner compensation. As Easley et al. (2018) show transaction fees have a crucial role in affecting both users and miners, which exit and entry the network if they find profitable using it to transfer money or mine (validating transactions). As reported on Bitinfocharts.com during the first years of Bitcoin history the cost of a transaction was almost zero, in 2013 was near 0,1 $ per transaction and since then in increased to more than 1 $. This is a very sensible increase in percentage terms and there have been periods when costs exploded to even 20 $ (December 2017, and January 2018). This has to do with the constraints on block size (how many transactions can be recorded into a block), which were intended to decrease the system's vulnerability to attack (Easley et al. 2018). The protocol determines how many blocks can be mined per period and through the block size how many transactions can be cleared. Therefore, when Bitcoin users increase the entire system faces bottlenecks and transaction costs skyrockets because some user, to see their transaction settled, are willing to pay miners more.

Bitcoin could be valuable to people when it comes to its use as a secure and fast medium of transfer, but as we have seen competitors have worked to become more cost competitive. Potentially they could also adopt a similar blockchain technology to quicken their transfers. Also, when competitors where improving, costs for Bitcoin were surging, eroding part of the advantage. Pondering also the volatility risk and the liquidity risk that could emerge in some countries with underdeveloped exchanges, I think it's hard to justify the staggering increase in Bitcoin price with its usefulness for cross border transfers: consumers today can choose between many competitors that have improved their offers reducing costs, while Bitcoin transfers have become more expensive.

3.4 Money laundering and capital control avoidance

Perhaps most of the fundamental value in Bitcoin can be explained by illegal activities.

> *"Bitcoin just shows you how much demand for money laundering there is in the world. That's all it is."*
>
> -Larry Fink, BlackRock CEO

The substantial economic function of money laundering is to transform potential purchasing power into an effective one (Masciandaro 1999). It is structured upon the revenues originated by illegal activities and the concealment of the sources of that income. Bitcoin seems to be a perfect tool for laundering criminal proceeds as all transactions bypass the regulated banking system, making the tracking of money movement difficult for public authorities (Lu 2018). Illegal funds can be used to acquire Bitcoins, which then are sent to some other wallet: as the transaction takes place it's impossible to know who received the coins, the ledger keeps track of the transactions, but the address is not linked to any person. Once the coins are transferred they can be exchanged for some fiat currency and spent. This is possible because the purchasing or selling of Bitcoins does not require user identification, the wallet address is just a number, and Bitcoin exchanges do not need to keep a proper documentation of their users and transactions (Lu 2018). Furthermore, transactions can be executed on the dark web, hiding the real IP address of users, making almost impossible for authorities to even understand where the transactions were originated. For example, using the TOR network it is possible to conceal the user's location: the message is sent through encrypted connections to other nodes of the network, each of them, in turn, only knows which node gave the data and which node it is giving data to. No individual node ever knows the complete path the data has taken. Very easily the transaction spreads across multiple jurisdictions, creating uncertainty about which country's authority has the power to launch a criminal investigation (Lu 2018). Also, there can be issues regarding which country's regulations should be applied.

Beyond transforming potential into effective purchasing power laundering illegal funds, Bitcoin mining and trading activities allows for easy capital controls avoidance. For example, the Chinese government in 2016 introduced several exchange control methods to curb capital outflows, including complex approval procedures for sending money out of the country (Clover 2016). But simply converting Renmimbis to Bitcoin and sending them to a whichever foreign address, which will convert them back into local currency allows to avoid the restrictions.

Otherwise investing Renmimbis to buy mining equipment and electricity allows to convert the Chinese currency into Bitcoins. In fact, China had become the centre of the cryptocurrency universe, for at its peak bitcoin trading in the country accounted for 90% of the world's total transactions (Qinqin, et al. 2017). Then the figure was reduced to 30% at the end of September 2017 as regulations were tightened. The situation escalated in February 2018 with the People's Bank of China issuing a statement that "it would block access to all domestic and foreign cryptocurrency exchanges and ICO websites." (Seth 2018).

The phenomenon is not confined to China, as wherever internet is available it is possible to launder, hide and move wealth across borders with little cost. The Europol head, Rob Wainwright, said in 2014 that virtual currencies were being used as an instrument to facilitate crime, particularly in regard to the laundering of illicit profits. The security and anonymity Bitcoin provides imposes a great cost on society making easier to break laws. Following Masciandaro (1999), Bitcoin lowers the aggregate transaction costs for money laundering operation, as this technology has low technical costs (mainly due to the volatility risk of the coins during transfers) and helps avoiding regulation: as stressed by Bryans (2014) it enables money launderers to move illicit funds more efficiently than ever.

A known example of the effectiveness of Bitcoin into a money laundering scheme is the Alexander Vinnik case. He was as the operator of BTC-e, an exchange used to trade the digital currency Bitcoin since 2011 and was convicted in July 2017. He was accused to launder more than 4 billion dollars for people involved in crimes ranging from computer hacking to drug trafficking (Gibbs 2017). Vinnik obtained funds also from the 2014 Mt Gox hack, when more than 450 $ million worth of digital coins were stolen, and laundered them through BTC-e and Tradehill, another San Francisco-based exchange he owned which allowed users to trade coins against a variety of fiat and virtual currencies. Greek police described Vinnik as a "an internationally sought 'mastermind' of a crime organization" (Gibbs 2017) and US authorities allege he facilitated crimes including hacking, fraud, identity theft, tax refund fraud, public corruption and drug trafficking.

3.5 Broad estimation of fundamental value of Bitcoin using amount of illegal transactions

Beyond money laundering and capital control avoidance Bitcoin has been widely used as a means for purchases in the underground economy. The main reason is its anonymity, that together with other technological tools (like TOR network) makes very hard for officials to pursue criminals and their activities.

Silk Road marketed itself as the anonymous marketplace, and operated from 2011 to October 2013 when the FBI shut it down. The second version, Silk Road 2.0, was closed in November of the following year by the FBI and Europol. On these marketplaces it was possible to buy drugs and forged passports (Matthews et al. 2014) along with fake driver's licenses (Hong 2015). The accepted currency for purchases was Bitcoin and the platform gained from a commission on transactions. In its sealed complaint against the founder, the FBI argues that total revenue generated from sales was 9.519.664 Bitcoins, and the total commissions collected by Silk Road from the sales amounted to 614.305 Bitcoins. These figures, converted at the time exchange rate, were equivalent to roughly $1,2 billion in revenue and $79,8 million in commissions. Silk road connected a total of 146.946 buyers to 3.877 vendors in the period.

Marketplaces like Silk Road using Bitcoin as a means of payments for illegal products were and are very common. Black Market Reloaded operated until November 2013 and sold illegal drugs, stolen credit cards and firearms. In July 2017 the FBI, the Drug Enforcement Agency and the Dutch National Police partnered to shutter AlphaBay and Hansa. The sites were accused of allowing thousands of vendors to sell illegal drugs, of which Europol said there were 250,000 listings on AlphaBay alone, with 200.000 members and 40.000 vendors (Gibbs and Beckett 2017). Both the sites operated through the above-mentioned TOR network, to guarantee anonymity to users, who paid through digital currencies such as Bitcoin. AlphaBay filled the void left by Silk Road and hosted daily transaction totaling hundreds of thousands of dollars, according to FBI director Andrew McCabe it was ten times larger than Silk Road (Gibbs and Beckett 2017).

3.6 Quantity theory of money application

During the years Bitcoin has been not only used by criminals to launder illegal income (Vinnik case), but also directly from people who wanted to buy unlawful items. Both big transfers (from a country to another) and small transfers (retail users buying prohibited goods) are real. Since Bitcoin facilitates all these activities, I try to give a broad estimation of the fundamental value of Bitcoin using the Quantity theory of money. This theory states that the general price level of goods and services is directly proportional to the amount of money supplied.

$$MV = PQ$$

M is the total amount of money in circulation on average during the period of interest. Since the supply of Bitcoin is capped and can be constantly monitored this number can be obtained easily. *V* is the velocity of the currency: the average frequency across transactions with which a coin is spent, and it is monitored and reported on Bitcoin.com daily. *P* is the Bitcoin value of a dollar the target of this estimation (1/USD). Lastly *Q* is the amount of transaction that are likely to be conducted in Bitcoin. This value is in USD, and should be an estimate of all the illicit transactions that could be executed through the Bitcoin network.

The Q entry has to be estimated as there are no official reports on how much illicit funds or items are laundered and bought through Bitcoin. To estimate this figure, I consider the estimated value of global crime activities, which could find in Bitcoin a powerful tool. Global Financial Integrity (GFI) is a non-profit research and advisory organization, which produces analysis of illicit financial flows, aiding governments to find solutions. In its 2017 report the value of total crime activities was estimated between 1,6 and 2,2 trillion USD. The research produced this estimate summing different kind of activities such as drug, human, weapons and organs trafficking, counterfeiting and crude oil theft.

In table 3.1, I try to estimate the price of Bitcoin in USD through the Quantitative theory of money. For Bitcoin velocity and money supply I used the average daily values from 01/01/2017 and 31/12/2017 available at Bitcoin.com. The average money supply during 2017 was 16.423.994 coins. The average velocity was 53,70. For the quantity of transactions, I used the mean value estimated by GFI, 1,9 trillion USD.

Due to the volatility of velocity (0,74% as annualized standard deviation) and the fact that Q is a broad estimation obtained aggregating many data, different values are also shown. Each value around the average velocity is increased or reduced by 1%, instead the quantity of transaction values differs by 10% between each other.

Rearranging the formula, the value in USD of a single Bitcoin is $\frac{Q}{MV}$

					V			
		52,12	52,64	53,17	**<u>53,70</u>**	54,24	54,78	55,33
	1.427	1.668	1.651	1.635	1.619	1.603	1.587	1.571
	1.570	1.834	1.816	1.798	1.780	1.763	1.745	1.728
	1.727	2.018	1.998	1.978	1.958	1.939	1.920	1.901
Q	**<u>1.900</u>**	2.220	2.198	2.176	2.154	2.133	2.112	2.091
	2.090	2.442	2.417	2.393	2.370	2.346	2.323	2.300
	2.229	2.686	2.659	2.633	2.607	2.581	2.555	2.530
	2.529	2.954	2.925	2.896	2.867	2.839	2.811	2.783

Table 3.1, Estimation of Bitcoin price in USD using the quantity theory of money with different values for Velocity and Quantity of transactions. The central value of Velocity is its 2017 average value and it is increased or decreased at each step by 1%. The central value of quantity of transaction starts is the 2017 GFI average estimate with every other value differing from the previous by 10%; values are in billion dollars. The 2017 average values are highlighted.

The starting values (the averages of velocity and quantity of transactions) give a USD value of a coin equal to 2.154. I would say this estimation is quite extreme: the 2.154 $ result considers that all the criminal activities all over the world would see the Bitcoin as the medium for laundering or clearing transactions. It is very unlikely that in 2017 and even in the future all the criminals had and would switch to Bitcoin for their businesses. Anyway, it suggests how the value of Bitcoin is inflated. In the day, 18/05/2018, a single coin is worth 8.090 $, just less than four times the value derived from this estimation. Estimation that is very optimistic as Q probably is too high: with a greater transactions value a single coin is worth more as this variable is at the nominator in the formula. Therefore Bitcoin value is directly proportional to the amount of transactions considered, while is indirectly proportional to the velocity. Even considering the result obtained using the lowest velocity and highest amount of dollar transaction a single coin would be worth 2.954 dollars, much less than current values. And to produce this estimation I needed to assume that Bitcoin was used in 2017 to conduct more than 2,5 trillion dollars of transactions: a figure superior to the highest estimation of the Global Financial Integrity for all illicit flows around the world which stood at 2,2 trillion. Also I had to consider a 52,12 value for velocity, 3% less than the 2017 observed average value.

4 Bitcoin, the latest financial bubble

"I can calculate the motion of heavenly bodies, but not the madness of people."

-Isaac Newton after the South Sea Company bubble bust

On the 22nd May 2010 a developer named Laszlo Hanyecz, spent 10.000 Bitcoins to pay for two pizzas. The value of those pizzas was 25$ (Kostarelis 2017), and the value of a coin was 0,0025$. Exactly eight years later those same coins are worth 7.993$ each, and the pizzas 79,9 million dollars. The value has doubled just less than 22 times, almost three times a year. Such evolution in price has captured the attention of economists and the media, who started the debate over Bitcoin and cryptocurrencies. Many like Robert Shiller have pointed this asset is just the latest bubble and a perfect example of "Faddish human behavior" (Lahiff 2018).

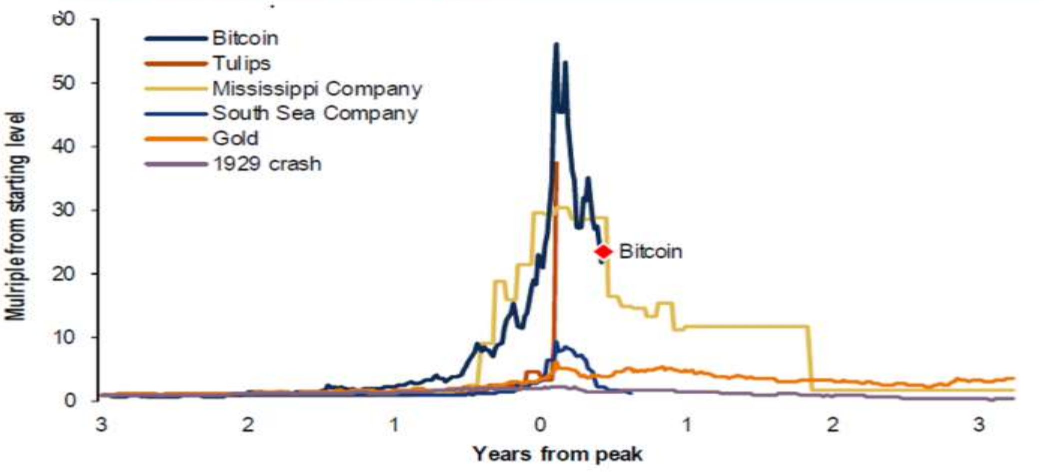
The first asset price bubble in history was the Dutch "Tulip Mania" in 1636-37. Prices for tulip bulbs went up by several hundred percent in the autumn of 1936. Some exotic varieties of bulbs had even larger increases in prices (Kindleberger and Aliber 2011). Like all the bubbles this reached a peak and then the prices fell causing panic among investors.

The world's first international crisis caused by a bubble came in 1825, led by large capital inflows from England to Latin America. This caused a boom in the stock market as well. The increase in capital outflows from England damaged the gold reserves of the Bank of England (BOE) which raised its rates to manage the situation. The raise led to a stock market crash. At the same time the sudden stop of capital flows to Latin America led to defaults, banking panics and currency crashes throughout the region (Kamalodin 2011). History repeated itself in 1890: large inflows caused a land property boom in Latin America, once again the BOE and other European Central banks raised their policy rates to maintain the level of gold reserves (Atkinson 2012). The stop led to a banking crisis and debt default in Argentina which spread all around the world when the London based Barings Brothers, which was heavily exposed to Argentine debt, defaulted. Other two financial bubbles fueled by easy credit and excessive speculation (Atkinson 2012) happened particularly in US stock market in 1907 and from the early twenties to 1929.

The period following the Great Depression and WWII was less exuberant in terms of asset price bubbles, probably thanks to stricter regulation on the financial sector and the Bretton Wood agreement fixing the exchange rates (Atkinson 2012). Once the agreement broke down in 1971, capital flows around the world increased. Another time Latin America was at the center of the stage in 1982, when the record amount of capital that developed nations had invested was moved back when central banks undertook stricter monetary policy. A debt crisis started and spread around the world, Citibank and Chase were bailed out (Kamalodin 2011). Between the 1980's and 1990's a great asset price bubble invested Japan, both in real estate and in stock prices. At its peak (1989) the value of Japanese equities was 1,5 times the value of US equities and 45% of world's total market capitalization. The value of real estate was so inflated that by selling all of the properties in Metropolitan Tokyo one could have bought all the property in the United States (Kamalodin 2011). The bubble was fueled by easy mortgage lending and low interest rates (Atkinson 2012). The next major financial bubbles started in the US and spread all around the world. The first, the dot.com bubble, was caused by both hysteria over the new age and massive capital flows from the rest of the world to the US. The bubble started forming around the 1995 and during the following years the market value of stocks increased from 60% of GDP in 1982 to 300% of GDP in 1999 (Kindleberger and Aliber 2011). Eventually the bubble popped in the early 2000's with stock prices falling. The last major bubble is known as the Subprime Mortgage Crisis. US interest rates too low for too long and the easing of mortgage lending standards, driven by international demand for high yielding MBS and the wrong assumption that house prices could only go up and in any case that they could not go down anywhere, inflated real estate prices in US and in relevant cities all around the world. When US house prices declined in 2006, the bubble started to pop, major investment banks Bear Stearns and Lehman Brothers were in trouble, the latter defaulted holding 613$ billion in debt (Mamudi 2008) and the Great Financial Crisis started.

Bitcoin could be the next bubble in this timeline even if its eventual crash could have limited effects on the real economy thanks to its relative smaller size. Looking at the 17/12/2017 high the total market cap of Bitcoin was around 326 billion dollars, and the market value of all crypto currencies which peaked the 7/1/2018 was close to 830 billion. Compared to the dot.com bubble and its relative size with respect to the real economy those numbers are very small. Certainly the magnitude in the increase in price has no equal, as can be seen in figure 3.7.

Figure 3.7 The greatest asset price bubbles in history



Source: BofA Merrill Lynch Global Investment Strategy, Global Financial Data, Garber (2000), Frehen (2012), Bloomberg

4.1 Asset showing many Bubble evidences

The increase from less than 10 cents to more than 19.000$ certainly poses some questions. Such a movement has captured the attention of many scholars that have debated whether speculation or fundamental value was the determinant. As we have seen in the previous chapter is hard to justify the Bitcoin price looking at its potential uses, even with the most optimistic hypothesis. On the contrary there is plenty of evidence that this asset is very likely to be the tool for speculators who try to ride this bubble selling the asset to the next fool.

- Newness and psychological aspects

  As Hofrichter (2018) argues Bitcoin embodies the “New-era” thinking: as a financial innovation, bringing all the features, which were described above, it gathers a lot of attention from the public. It is perceived as a monetary innovation like the internet age (Hofrichter 2018). Even if, as we have seen, Bitcoin has many, and probably more efficient, alternatives in each of its uses. This is a typical bubble scenario where there is great disagreement between investors on the fundamental value of the asset. This certainly happened for Bitcoin and cryptocurrencies with people arguing they can substitute central banks. Google searches has had a proved effect on prices and volume as studied by Kristoufek (2013), Bouoiyour and Selmi (2015), and Ciaian (2016). Bitcoin price formation seems to be influenced by investors who rush to buy as more news comes in.

- Risks and limits to arbitrage

  As most investors start buying fearing of missing out the latest hot investment, arbitrageurs who see the price unjustified by fundamentals could try to profit selling the asset and eventually aligning the price back to a fairer value. Omitting for a while the many risk arbitrageurs face, short selling Bitcoin for a long time was impossible. As Yermack writes in 2013 "Bitcoin can't be sold short", and no derivatives like swaps or forwards available for other currencies existed at the time. The situation was the same in 2014 as reported by the Boston FED: shorting coins was impossible since there was no lending market or Bitcoin derivatives. The first witness of short selling is from 2016, by Kroeger and Sarkar, who point out how it was possible, but only on the Bitfinex exchange (based in Hong Kong) and entailing additional fees. For this period prices could go only up, as at most an investor could have sold its own coins. The situation changed and in November 2017, as summarized in an interview by Charles Hayter, co-founder of market tracker CryptoCompare, all the options to short in common markets were becoming available in the Bitcoin market. At last, even futures were created: in December 2018 they were tradable on the Chicago Mercantile Exchange and as the San Francisco Fed suggests: "The rapid run-up and subsequent fall in the price after the introduction of futures does not appear to be a coincidence" (Hale et al. 2018).

  Beyond the long-time constraint to short Bitcoins arbitrageurs face at least two other important risks, which can be summarized in the famous phrase from Keynes: "The market can remain irrational longer than you can remain solvent":

  - Fundamental risk: the mispricing can get worse, eventually the price should converge to fundamental, but it could happen after the trader's investment horizon. The trader could even run out of capital if prices keep rising. For a short seller the potential loss is infinite as the price can theoretically grow to infinite.
  - Synchronization risk: each arbitrageur is uncertain about the timing of other arbitrageurs. Also, he has the desire to minimize the holding costs, which grow with time as Bitcoins need to be borrowed for someone who owns them. Timing uncertainty and cost minimization cause each trader to delay the arbitrage, hence the mispricing continues.
- Launch of related financial instruments: new products related to the bubbling asset proliferated. For example the futures from CBOE and CME are available since December 2017. ICOs, initial coin offerings, where new companies creating a virtual currency protocol collect funds from the public exchanging the coins flourished to capture part of the capital flowing in this market. The first ICO was held in 2013 (Barnett

2017). As reported by CoinSchedule statistics in 2016 more than 94 million dollars were raised, the amount exploded to over 3,8 billion in 2017, with more than 1 billion raised in December, precisely when Bitcoin was peaking. In the first five months of 2018, more than 7,5 billion dollars have been raised.

- Lack of financial regulation. For a long time, the absence of rules concerning cryptocurrencies posed no barriers and rules to capital flowing into Bitcoin and other currencies. The combination of credulous buyers and low barriers for scammers were bound to lead to a high level of fraud when the money involved got large (Popper 2018). The fact that the funds flows in the virtual currencies market became huge almost overnight, before there were good regulatory or even self-regulatory models in place, made the problem acute according to Popper (2018). People were attracted into investing by past returns and prospect of easy gains. Also, ICOs attracting new investors have been prone to scams and securities law violations as reported by the SEC, Shifflett and Coulter (2018), Chohan (2018), and Koetsier (2017).

4.2 News and popularity driving returns

As we have seen Bitcoin shows many characteristics typical of a financial bubble. As a consequence, the evolution in price shouldn't be justified in a major way by fundamental elements. Polasik et al. (2015) show in fact how, among many factors influencing supply and demand and the economy, only the amount of popularity is able to explain the change in price. Returns tend to be elevated whenever newspaper articles mention Bitcoin more frequently and whenever the number of people searching for it on Google increases (Polasik et al 2015).

Returns of Bitcoin are analyzed with respect to popularity, represented by changes in the number of searches for the keyword "Bitcoin" relative to all Google searches, liquidity factors, such as volume traded and coin supply, and macroeconomic factors like OECD inflation, unemployment and industrial production. The last three factors have been shown to affect stock returns and bond risk premia by Asprem (1989), Chen, Roll, and Ross, (1986), Ludvigson and Ng, (2009), therefore are considered also for this asset. To capture the currency features of Bitcoin the money supply (the number of coins) is considered together with a foreign currency like the USD. To measure the influence of the last variable, the growth rate in the USD broad index (calculated by the FED) is included among the regressors, which measures a weighted average of foreign exchange values of the dollar against currencies of the US major trading partners.

They work on monthly data, from April 2011 to March 2014, and find that among all the factors considered the only significant to determine Bitcoin returns are the popularity and volume traded. No macroeconomic factor is statistically significant, the same for money supply or USD appreciation/depreciation relative to other currencies. A one per cent increase in Google searches increased returns by about 53 to 62 basis points. Furthermore, they found that the tone in news, whether laudatory leads to price inflation. Volume significance is consistent with the presence of network effect (Polasik et al 2015): as the network enlarges, users find more value in it. To control for simultaneity and endogeneity problems, as it could well be that price change drives the amount of Google searches, and not the opposite as Polasik et al. suspect, they employ an instrumental variable. The popularity proxy is instrumented using, among many, exogenous variables and a popularity proxy for "Cryptography". The instrumental regression, which should alleviate endogeneity problems, gives similar findings to the previous regression. Also, the results lead the researcher to believe that problems related to weak instruments don't occur.

4.3 Is popularity still an important driver?

The period covered in the previous research leaves out much of the Bitcoin run: the last data are from March 2014, when the price was "only" around 450 $. To verify whether the situation has changed, or if popularity still is an important driver for Bitcoin returns I conducted a similar research. I exploited the data reported in table 4.3, whose descriptive statistics are in table 4.4. Since Google Trend data (reporting popularity) weren't available for earlier periods, I did use monthly data from December 2012 to January 2018. Therefore the data covers a part of the previous research and all the run up to a 19.500 $ price for a single coin.

I wanted to test whether returns can be explained only by popularity among the public or by macroeconomic variables, OECD data on inflation, unemployment and industrial production, which have been shown to affect returns for stocks and bonds, and currency features like volume traded or money supply. I also considered the movements of the USD against a basket of foreign currencies. To look for correlation among these factors, I worked on monthly data over the period, regressing the dependent variable, Bitcoin returns, over all other variables, trying to build a model able to explain the price evolution.

In table 4.1 I report results: in column (1) and (2) I estimated with OLS the regression of Bitcoin returns over all the explanatory variables, the first column reports default standard errors while the second has standard errors robust to heteroscedasticity. In column (3) and (4) I estimated with instrumental variables: the variable Newness is instrumented with all exogenous variables plus two excluded instruments I will describe in a few lines. Column (3) shows default standard errors while column (4) shows robust standard errors.

- According to column (1) in table 4.1, my results are very similar to those obtained in the previous research: it turns out popularity (the variable Newness) is still significant in explaining Bitcoin returns and a one percent increase in the amount of Google searches leads to a positive return of 82 basis points. The regression has a quite high R^2: 56,1%. Volume is no longer significant as previously was. All the other coefficients are, as before, statistically not significant: no macroeconomic variable influencing bond or stock returns seems to affect Bitcoin price, which looks like is immune from influences from the real economy. The same happens for coins supply or USD movements relative to other currency: it seems they are unable to influence Bitcoin returns.
- Then I controlled for the possible endogeneity of Newness and I followed Polasik et al. (2015), exploiting the number of Google searches for “Cryptography” over the period as an instrument. Unfortunately it was not statistically significant in my case, as any other exogenous variable previously employed. Therefore I searched for new instruments and I found that the number of Google searches for the keywords “Virtual currency” and “Financial bubble” could be used as instruments for the variable Newness over the considered period. I conducted a 2sls regression of Bitcoin returns over all previous variable with Newness instrumented using the two instruments[1]. Results are reported in table 4.1, column (3): as before only popularity is statistically significant in explaining monthly returns, no other variable seems to have an influence. Each percentage increase in popularity leads to 85 basis point of excess return for Bitcoin.

  I tested the weakness of instruments and found they are not weak: both variables are efficient in instrumenting Newness. The Cragg-Donald F statistic for weak instruments had a 35,29 value, while the 10% critical value reported by Stock and Yogo (2005) was 19,93. I also conducted the Sargan test, to verify that the instruments were uncorrelated with the structural error term, and the result was positive, in the sense that the H_0 of uncorrelation was accepted with a p-value of 0,2680. Then, since instruments were

---

[1] Estimations obtained with the STATA routine ivreg2 entering the following command: ivreg2 BTC_RETURNS (NEWS= BUBBLE VC) VOLUME SUPPLY IP INFLATION U USD

proved to be strong, I tested for the exogeneity of Newness with the Hausman test, the null hypothesis of exogeneity was accepted with the p-value being 0,7803: the quantity of Bitcoin searches on Google seems to be exogenous, a shock hitting the returns.

Lastly, I controlled for homoscedasticity in residuals. The Pagan-Hall (1983) heteroscedasticity test after the instrumental regression signaled heteroscedasticity, as the null hypothesis of homoscedasticity was rejected as the p-value I obtained was 0,0025[2].

- Therefore I repeated the instrumental regression with the robust option for standard errors, in table 4.1 column (4) are reported the new standard errors[3]. The results change slightly, still only Newness is significant in explaining Bitcoin returns. I tested again for weakness in instruments, but with robust standard errors: the Montiel-Pflueger (2013) robust weak instrument test suggests the two instruments are strong, I obtained a value of 35,28 when the 5% critical value was 19,294[4]. The Hansen J-test (1996) (the Sargan test when robust option is exploited) signals there may be some problem of correlation between the instruments and the structural error term, the p-value of the test is 0,0667 which leads me to reject the null of uncorrelation if I consider a 10% significance level, but to accept the null if I consider a 5% level. I accepted the null of uncorrelation with the structural error term, but results need to be taken with caution as the p-value leads me to accept or reject the null depending on the confidence interval I choose.
  Finally I tested for the exogeneity of Newness using the Sargan-Hansen (1982) test statistic which is robust to heteroscedastic errors: the p-value of the test is 0,8764 which is a strong evidence towards the null hypothesis of exogeneity. I concluded that I can’t reject the null hypothesis that the popularity variable is exogenous.

---

[2] Statistic obtained with the STATA command: ivhettest, after the instrumental regression.

[3] Estimations obtained with the STATA routine ivreg2 entering the following command: ivreg2 BTC_RETURNS (NEWS= BUBBLE VC) VOLUME SUPPLY IP INFLATION U USD, robust.

[4] Statistic obtained with the STATA command: weakivtest, after the instrumental regression.

Table 4.1 – Regression of Bitcoin returns

	(1)	(2)	(3)	(4)
	OLS	OLS, with robust s.e.	IV	IV, with robust s.e.
CONSTANT	2,1357 (9,2678)	2,1357 (6,7582)	2,1988 (8,6460)	2,1988 (6,2730)
NEWNESS (% change, month on month)	0,8243 (0,1032)	0,8243 (0,3091)	0,8493 (0,1269)	0,8493 (0,3214)
VOLUME (Δ millions)	7,53*e^{-06} (8,48*e^{-06})	7,53*e^{-06} (7,67*e^{-06})	7,53*e^{-06} (7,91*e^{-06})	7,53*e^{-06} (7,45*e^{-06})
SUPPLY (Δ millions)	-1,2509 (3,9267)	-1,2509 (2,5497)	-1,2766 (3,6632)	-1,2766 (2,4641)
IP	-0,0248 (0,0741)	-0,0248 (0,0527)	-0,0254 (0,0691)	-0,0254 (0,0495)
INFLATION	0.6798 (12,7331)	0,6798 (9,1964)	0,3603 (11,9221)	0,3603 (9,0156)
U	10,4922 (25,7395)	10,4922 (21,6690)	10,4872 (24,0057)	10,4872 (20.2480)
USD (% change, month on month)	-4,6885 (5,5645)	-4,6885 (3,4209)	-4,7926 (5,2010)	-4,7926 (3,4001)
R-squared	0,5616	0,5616	0,5611	0,5611
Adj. R-squared	0,5037			
F-statistic	9,70	2,70	6,15	2,23
Prob(F-statistic)	0,0000	0,0182	0,0000	0,0463

- Hence, I focused again on the first OLS model in table 4.1 column (1), and verified whether residuals where hetero or homoscedastic and if the model was well specified. I conducted the White test for residuals, the null hypothesis of this test is homoscedasticity: the p-value of the test is 0,0078, so there was strong evidence of heteroscedasticity. Then, also in this case, it is better to use the robust option for standard errors: the regression is shown in table 4.2 column (1). Table 4.2 also shows other two specifications of the model in columns (2) and (3), both estimated with OLS without robust option, since, as I'll show, it wasn't necessary.
- To control if the model was well specified I used the Ramsey reset test, which checks for misspecification, looking whether non-linear combinations of fitted values help explain the dependent variable. The test had a value of 50,92 translating into a 0,0000

p-value indicating the model wasn't correctly specified. The test doesn't suggest why the model needs improvement, probably it had omitted variables. Therefore I included as a regressor the square of Newness to see if nonlinear effects were present: this variable was statistically significant, and the Ramsey reset test value improved to a value of 29,86. I went on, including the third power: again it was significant, and the model was better specified (the Ramsey reset test p-value increased to 0,0003). Lastly, I included the forth power of Newness, see table 4.2 column (2). It was significant and finally the reset test indicated the model was well specified with a p-value of 0,2828. Also, including powers of Newness I no longer have heteroscedasticity in residuals: The White test, with a p-value of 0,3420 now signaled homoscedasticity in residuals, no need to use the robust option here.

- After I dropped all the non-statistically significant variables: all the exogenous variables and Newness^2, which was not significant. The final results can be seen in table 4.2 column (3). There are three regressors besides the constant: Newness, Newness^3, Newness^4, all significant at a 1% level of significance. The White test accepts homoscedasticity hypothesis with a 0,8235 p-value and it is well specified according to the 0,3358 p-value of the reset test. We can see that the R^2 has reached 87,5% from 56,1% of the initial model (columns (1) and (3) in table 4.2).

Table 4.2 – Regression of Bitcoin returns

	(1)	(2)	(3)
	OLS, with robust s.e.	OLS	OLS
CONSTANT	2,1357 (6,7582)	3,2344 (4,6932)	0,0738 (0,037)
NEWNESS (% change, month on month)	0,8243 (0,3091)	0,4702 (0,1590)	0,5061 (0,1496)
NEWNESS^{2}		0,1083 (0,2708)	
NEWNESS^{3}		-0,8272 (0,3442)	-0,7203 (0,1879)
NEWNESS^{4}		0,4412 (0,1045)	0,4097 (0,0742)
VOLUME (Δ millions)	$7,53*e^{-06}$ ($7,67*e^{-06}$)	$6,37*e^{-06}$ ($4,31*e^{-06}$)	
SUPPLY (Δ millions)	-1,2509 (2,5497)	-0,4462 (1,9867)	
IP	-0,0248 (0,0527)	-0,0251 (0,0375)	
INFLATION	0,6798 (9,1964)	5,3562 (6,3964)	
U	10,4922 (21,6690)	7,2753 (13,2518)	
USD (% change, month on month)	-4,6885 (3,4209)	-4,8661 (2,8210)	
R-squared	0,5616	0,8964	0,8752
Adj. R-squared		0,8757	0,8687
F-statistic	2,70	43,27	133,30
Prob(F-statistic)	0,0182	0,0000	0,0000

As can be seen in figure 3.8 the last specification of the model (with nonlinear effects) is quite good at fitting the observed values. In figure 3.8 I plotted both the scatter plot (black dots) and the predicted values using the regression in table 4.2 column (3); on the two axis we have the dependent variable (Bitcoin returns) and the independent variable (Newness). Including the powers of Newness the model is able to capture also the outliers, like the two observations where the number of Google searches more than tripled (the increases are greater than 200%).

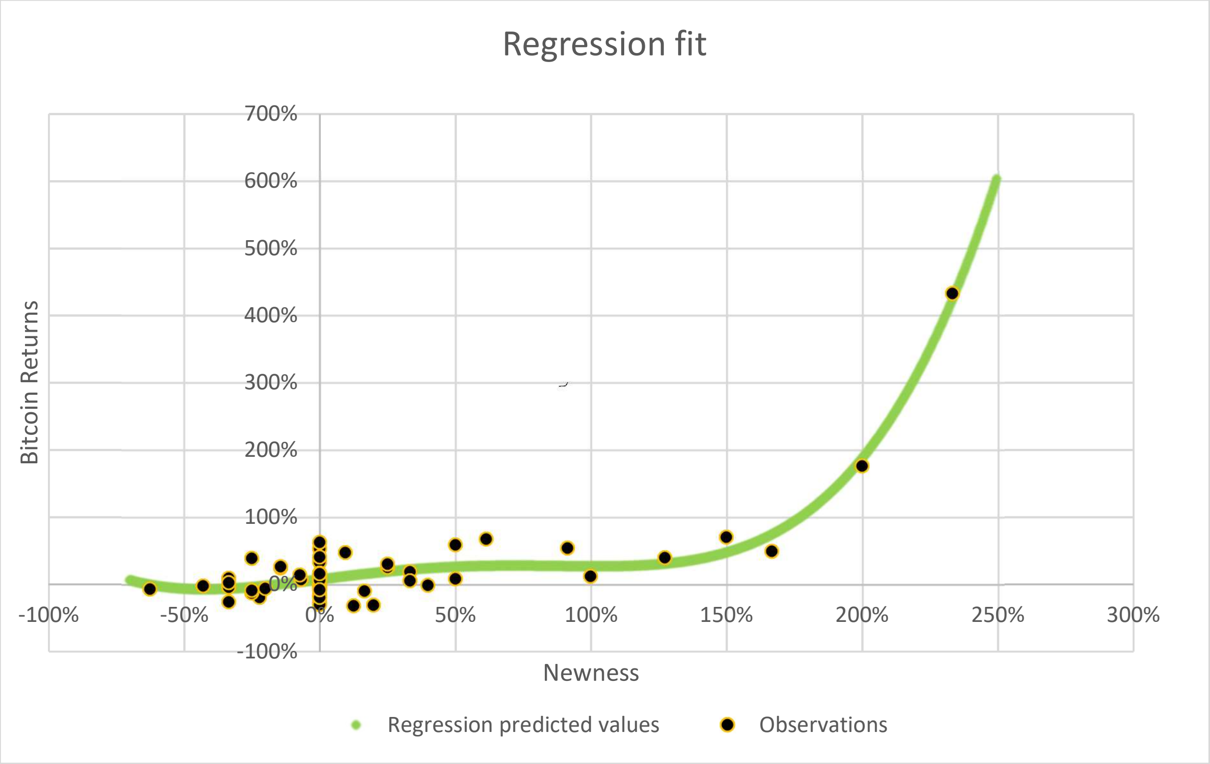


Figure 3.8 plots the sample of observation, and the predicted values using the regression which exploits Newness, Newness^3 and Newness^4

Now I will focus on the two specifications of the model reported in columns (1) and (3) of table 4.2. Recalling that Popularity is the monthly percentage increase of Google searches, it has now a much lower effect on Bitcoin returns than the initial 82 basis points for small increases. In fact considering the three parameters together (Newness, Newness^3 and Newness^4) a 1% increase in the amount of Google searches for the "Bitcoin" keyword leads to an extra 16 basis point in Bitcoin returns. The effect of popularity is smaller, still it is the only significant variable explaining returns. But once I focus on bigger increases in the independent variable its effect through Newness, Newness^3 and Newness^4 has a greater impact on returns. As can be seen in in figure 3.9 which plots the dependent variable in relation to the independent variable, the nonlinear effects (represented by the powers) creates an explosive evolution once certain values are reached. We can see that high popularity values, which are present in the sample, have a greater and greater effect on returns because of the nonlinear effects.

In figure 3.9 it is reported also the relation between Newness and returns identified in the parameter in the original regression, table 4.2 column (1). Once we have an increase of more than 196% in popularity (two times in my sample), the effect on prices is greater if we focus on the last model, table 4.2 column (3). Moreover for decreases in popularity the effect over returns is smoothed once we take into consideration the last model: we can see that the green line (which considers also nonlinear effects) is always above the blue line (only linear effect). It is worth noticing that when popularity diminishes returns seems to be only slightly affected if I exploit the last model. If I consider all the possible negative values, which are between -100% and 0 since Newness is the month on month percentage change, the largest predicted decrease in returns should happen when popularity decreases by 42% translating into a -14,65% return in Bitcoin prices. Returns should be even positively affected by huge decreases in Google searches: from -72% to -100% the predicted effect is positive.

Concluding this last model which includes nonlinear effects suggests that prices are pushed up by increments in popularity, the more so if increments are very high, on the contrary when popularity diminishes prices are only slightly affected (they remain high): in fact the model predicts that popularity affects returns by values between -10% and -14,65% only if the amount of Google searches drops by values between 21% and 59%. For other values the negative effect is lower in absolute value.

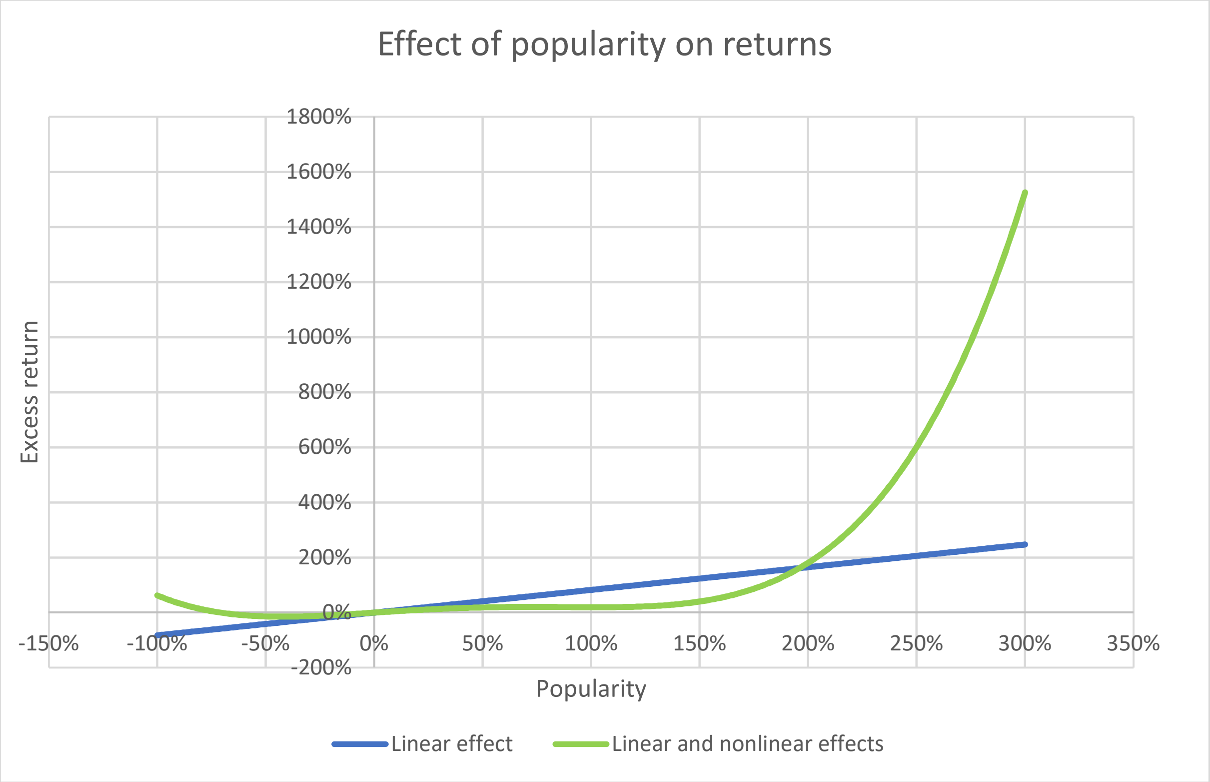


Figure 3.9 plots the different effects of Popularity over Bitcoin returns depending on the selected model. Since Popularity is a month on month percentage change the lowest value considered is -100% (the smallest ever possible); the highest considered is +300%. In my sample the smallest value is -63% while the highest is +233%.

Additionally to control for autocorrelations in residual in the final model I conducted the Breusch-Godfrey tests. I test conducted the test considering autocorrelations up to the tenth order: there is no residual autocorrelation up to the tenth lag, the p-value is equal to 0,6559, therefore H_0 (no serial autocorrelation) is accepted.

Table 4.3, monthly data from December 2012 to January 2018

Variable	Definition	Source
BTC_RETURNS	Monthly returns of Bitcoin prices.	Bitcoin.com
NEWNESS	Percentage monthly growth of number of Google searches including "Bitcoin" as keyword. The search data was scaled, the highest value being 100.	Google trends
VIRTUAL CURRENCY	Percentage monthly growth of number of Google searches including "Virtual currency" as keyword. The search data was scaled, the highest value being 100.	Google trends
FINANCIAL BUBBLE	Percentage monthly growth of number of Google searches including "Financial bubble" as keyword. The search data was scaled, the highest value being 100.	Google trends
VOLUME	Absolute monthly change in volume traded (in millions).	Yahoo! Finance
SUPPLY	Absolute monthly change in coins created (in millions).	Bitcoin.com
IP	Monthly industrial production, OECD countries.	OECD, Key Short-Term Economic Indicators
INFLATION	Monthly inflation, OECD countries.	OECD, Key Short-Term Economic Indicators
U	Monthly harmonized unemployment, OECD countries.	OECD, Key Short-Term Economic Indicators
USD	Percentage growth rate in the US dollar broad index (FED), which measures a weighted average of foreign exchange values of the dollar against currencies of the US major trading partners.	Saint Louis FED

Table 4.4, descriptive statistics for monthly data from December 2012 to January 2018

Variable	Mean	Standard deviation	25th percentile	Median	75th percentile
BTC_RETURNS	20,04%	63,02%	-6,85%	7,60%	28,25%
NEWNESS	17,17%	56,20%	-3,33%	0,00%	22,50%
VIRTUAL CURRENCY	5,81%	28,56%	-14,12%	0,00%	18,57%
FINANCIAL BUBBLE	3,24%	22,03%	-13,39%	5,13%	16,82%
VOLUME	845,53	7013,25	-118,54	30,65	305,22
SUPPLY	0,10	0,03	0,06	0,11	0,13
IP	107,38	2,19	106,49	107,34	107,88
INFLATION	1,46%	0,61%	0,86%	1,50%	1,97%
U	6,85%	0,78%	6,28%	6,83%	7,58%
USD	0,31%	1,11%	-0,57%	0,49%	1,03%

4.4 PSY procedure to identify bubble in Bitcoin

As just suggested Bitcoin prices have been largely influenced by popularity which brought into the market many investors who wanted to try and speculate, maybe with too much exuberance. Exuberance which probably created a bubble in the Bitcoin price.

Identifying financial bubbles is hard, but very important for policy makers, who would like to intervene before events escalate. Phillips, Wu, Yu (PWY, 2011) developed a method based on the augmented Dickey-Fuller (ADF) test to identify a bubble and the points in time of origination. The procedure was later refined in 2015 by Phillips, Shi and Yu, (PSY), who generalized the tests to overcome problems arising from multiple bubbles in the considered sample. The earlier version of this procedure was used to test for bubbles in NASDAQ (Phillips et al 2011), and in gold (Baur and Glover 2012). The later version (PSY) was applied to identify speculative bubbles from 1871 to 2010 in the S&P 500 (Phillips, Shi, Yu 2015).

Since Bitcoin doesn't pay any dividend, and this feature is very similar to gold (analyzed by Baur and Glover 2012) I will apply the PSY procedure to detect the presence of bubbles.

The approach works on the following regression where X_t is the asset price at time t:

$$X_t = \mu + \delta X_{t-1} + \sum_{j=1}^{J} \varphi_j \Delta X_{t-j} + \epsilon_t \qquad (1)$$

$$Where\ \epsilon_t \sim iid(0;\sigma^2)$$

Extensive use of the augmented Dickey-Fuller test is made on this regression. The test tests the null hypothesis that a unit root is present in a time series (here the observations of price). The alternative hypothesis is different depending on the version of the test that is used. For the purposes of these test the alternative is always right-sided as I will explain in a few lines.

The ADF test is conducted repeatedly on different fractions of the full sample:

- SADF, supremum ADF test

  The earlier version (PWY) of the test relies on repeated estimation of the ADF model on a forward expanding sample sequence, and the test is obtained as the supremum value of the corresponding ADF statistic sequence. The greater than or equal to any other test value is chosen as the result of the supremum ADF test (SADF).

  In this case the test is a right-sided unit root test to detect explosive behavior in equation (1). The null hypothesis is H_o: $\delta = 1$, no explosivity. Instead the alternative hypothesis is

H_1: $\delta > 1$, identifying an explosive evolution of X_t, here the Bitcoin price. The sample of observation is considered a continuous segment from 0 to 1: 0 represents the beginning, the first observation, while 1 is the whole sample.

Each time the test is conducted on a different window of estimation: r_W. r_W is the fraction of the sample where the test is computed, the starting point of the window is denoted as r_1 and the endpoint is r_2. r_W expands in length from r_0 to 1. r_0 is the smallest sample window considered where the test can be computed, it is defined in equation (2) and depends on how many observations are present in the sample.

The right-sided ADF test is estimated repeatedly on r_W, which expands each time adding the following observation. In figure 4.1 it is shown how the different r_W are constructed for the purpose of this test: the arrows represent different windows of estimation (r_W), each starts from r_1 and ends at r_2. In the SADF all the different r_W has the same starting point: 0, r_1 is fixed while r_2 moves. So the test estimates the statistic for all the r_W, which share the same starting point, but have a different endpoint consisting in an additional observation than the previous r_W and an observation less than the following r_W. Recalling that we have a minimum width (r_0), the size of the window corresponds always to its endpoint (r_2), since the start point is 0. ($r_W = r_2 - 0 = r_2$). The ADF statistic for a sample that runs from 0 to r_2 is denoted as $ADF_0^{r_2}$.

The PWY test statistic is the supremum of the test results, based on the forward recursive regression and is defined as:

$$SADF\ (r_0) \ = \ \sup_{r_2 \in [r_0,1]} ADF_0^{r_2}$$

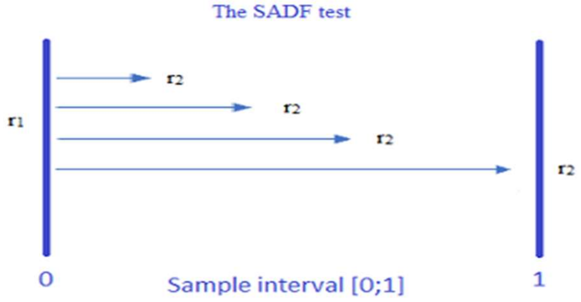


Figure 4.1

The width, or the minimum window length, denoted as r_0 is based on a lower bound of 1% of the full sample (Phillips, Shi, Yu 2015) and takes the value of:

$$r_0 \ = \ 0{,}01 \ + \ 1{,}8 \, / \, \sqrt{T} \tag{2}$$

Where *T* is the number of observations in the sample. If *T* is small, r_0 needs to be large enough to ensure there are enough observations for an adequate initial estimation (Phillips, Shi, Yu 2015).

- GSADF, generalized supremum ADF test

  The later version (PSY) provides a different test for identifying bubble phenomena when there may be multiple bubbles in the data (Phillips, Shi, Yu 2015). The difference with respect to the previous test is that the window of analysis over the sample (r_W) has also a variable starting point (previously it was fixed at the beginning of the sample). The endpoint of estimation, r_2, varies as before from r_0 (minimum width of the window) to 1, but the starting point, r_1, changes as well from 0 to r_2-r_0.

  Figure 4.2 shows how interval are constructed, in this case, since also the starting point varies, we have many more subsamples where the test is computed: as before we conduct the tests over r_W starting from 0, but we include r_W which start with observations different from the first one. r_1 can be at maximum r_2-r_0 so that the minimum width r_0 is preserved: in that case the interval would have the minimum length and begin from r_2-r_0 and end at r_2 (the width being: $r_W = r_2 - (r_2-r_0) = r_0$). Hence this test exploits a rolling window. The test is the generalized version of the SADF, therefore takes the name of GSADF. The statistic is the largest ADF statistic in this double recursion (since both r_1 and r_2 change) over all feasible windows defined by r_1 and r_2:

$$GSADF\ (r_0)\ =\ \sup_{\substack{r_2\in[r_0,1]\\ r_1\in[0,r_2-r_0]}}\ \left\{ADF_{r_1}^{r_2}\right\}$$

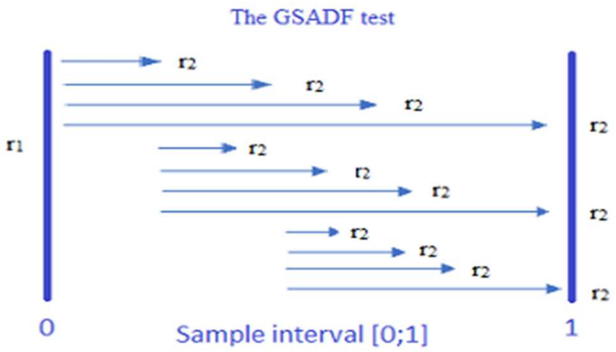


Figure 4.2

4.5 Bubble identification through SADF and GSADF tests

To verify whether Bitcoin prices showed bubble behavior in the recent past I'm going to use the SADF and GSADF summary statistics to identify explosive behavior in the data. Both these tests exploit right sided ADF tests where the null hypothesis is always $\delta = 1$, there is a unit root in the process identified by equation (1), therefore no explosivity in price[5]. As the ADF tests employed are right sided, if the null is rejected δ is greater than one, detecting explosivity in price evolution.

I applied the summary SADF and GSADF tests to Bitcoin daily prices from 31/12/2013 to 2/5/2018 available on Yahoo! Finance. The observations are in total 1.585, with the smallest window r_0, calculated according to equation (2), amounting to 0,05521 of the whole sample, or 87 observations. In table 4.5 I report the values of the two tests together with the critical values obtained from Monte Carlo simulations of 2.000 replications of 1.585 observations. From table 4.5, the SADF and GSADF statistics for the full series are 7,3294 and 7,6362, both above their 1% right-tail critical values, giving strong evidence that Bitcoin had explosive subperiods in the considered sample. The null of a unit root in all the subperiods is rejected in favor of the alternative of $\delta > 1$.

Both the tests consider different subsamples of the full sample and test whether in each one the price follows equation (1), where δ should be equal to 1 through right sided ADF tests. Since both the tests take the resulting sup value among the different test results (one result for each different r_W of estimation), and those sup values are greater than the critical values I can conclude there is at least a bubble subperiod in the sample. The difference between the two is simply how subsamples are built, the GSADF allows for both the starting and the end point to move, therefore there are more subsamples considered. According to these results I can conclude that between 31/12/2013 and 2/5/2018 there was at least a bubble period in Bitcoin prices.

---

[5] Following Phillips, Shi, Yu (2015) in the analysis of S&P 500 data, I used in calculations a lag of order J=0

Table 4.5 - Summary statistics			Finite sample critical values		
	Test statistic		90%	95%	99%
SADF	7,3294		1,2968	1,6291	2,0981
GSADF	7,6362		2,1823	2,4042	2,8646
Critical values of both tests are obtained from Monte Carlo simulations with 2.000 replications (sample size 1.585, like the 1.585 daily observation exploited). The smallest window has 87 observations.					

4.6 PSY procedure to identify bubble periods

The PSY procedure (2015) aims also at detecting bubbles in real time, using data only up to the point of analysis for ongoing assessment, giving an early warning diagnostic that can assist regulators in monitoring. They utilize a flexible window for estimations similar to the rolling window described above.

- BSADF, backward supremum ADF test

  In particular, they exploit the backward sup ADF test (BSADF). The BSADF performs a sup ADF (SADF) test on a backward expanding sample sequence where the endpoint of each sample is fixed at r_2 (the sample fraction corresponding to the endpoint of the window) and the starting point varies from 0 to $r_2 - r_0$ (the sample fraction corresponding to the origination of the window). Again the origination can vary from 0 to $r_2 - r_0$ so that in the last case the minimum width of estimation is respected: $r_W = r_2 - (r_2 - r_0) = r_0$. In figure 4.3, I show how the intervals of estimations are built: they all have the same endpoint, but a different starting point. As in the SADF statistic described above, we have one among the starting point and the endpoint of the interval which is fixed. In this case r_2 is fixed, while the starting point moves backwardly each time adding one observation.

  The corresponding ADF statistic sequence is $\{ADF_{r1}^{r2}\}_{r1\in\,[0,r2-r0]}$ and the backward SADF is the supremum value of the ADF statistic sequence.

  The backward SADF statistic is then defined as:

$$BSADF_{r_2}\,(r_0) \;=\; \underset{r_1\in[0,r_2-r_0]}{sup}\;\{\,ADF_{r_1}^{r_2}\}$$

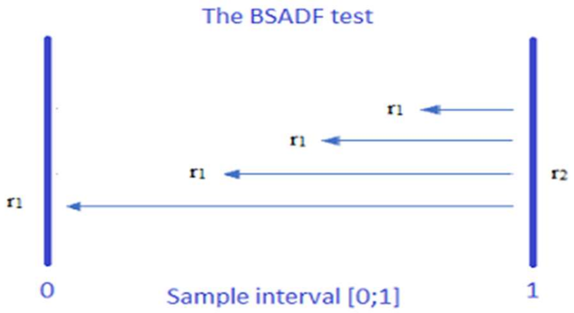


Figure 4.3

The origination date of a bubble is the first chronological observation whose BSADF statistic exceeds the critical value of the BSADF statistic. The termination date on the contrary is calculated as the first chronological observation whose statistic falls below the critical value. For a bubble identification, the duration should exceed a minimal period which can be set arbitrarily, so that a bubble isn't identified as soon as a single statistic is above the critical value.

- PSY test, a generalized version of the BSADF

  Phillips, Shi, Yu (2015) started from the BSADF test, recommending using a double recursive test procedure to generalize the test to enhance bubble identification with available data. According to the authors this procedure should enhance identification accuracy when the data may include one or more collapsing bubble episodes, which could result in finding pseudo-stationary behavior using other tests.

  PSY make inference on the statistics sequence produced by a GSADF test implementing the backward sup ADF test repeatedly for each $r_2 \in [r_0;1]$. Figure 4.4 reports how interval for estimations are built: as in the GSADF test described above, both the starting point r_1, and the endpoint r_2 can now move. On the contrary in the BSADF test only the starting point, r_1, could. As the BSADF test is repeated on each different r_2, it generates a sequence of test statistics.

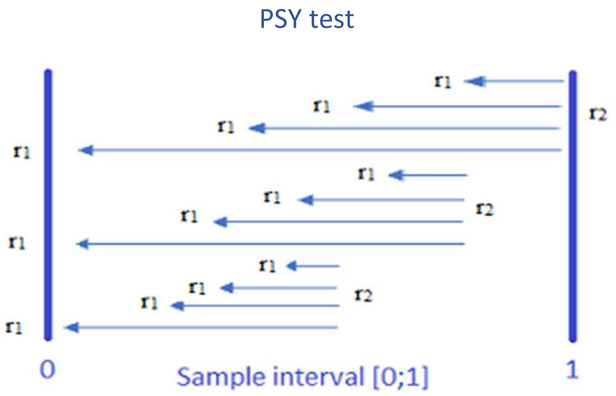


Figure 4.4

In this case the GSADF can be written as:

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

More simply here the GSADF statistic sequence is produced by a BSADF test implemented each time for a different r_2, see figure 4.4.

As for the BSADF test, for each possible endpoint in the whole sample the ADF test is implemented multiple times, each time changing the starting point of the subsample, then the greater value of the test statistics is chosen. Therefore with the PSY procedure a sequence of values is generated: one value for each possible r_2.

As before, to date-stamp the beginning and the end of a bubble the origination date (the first test statistic which is above the critical value) and the termination date (the first test statistic which is under the critical value) are identified.

4.7 PSY procedure application

According to the results obtained above at point 4.5 there is evidence of exuberance in Bitcoin prices over the period. The SADF and the GSADF tests employed suggested there was at least a subperiod in the whole sample where the prices followed and explosive behavior. To try to identify the precise subperiod it is necessary to use the PSY procedure: a GSADF implementing the BSADF test (as figure 4.4). Again extensive use of right-sided ADF test is made, to test whether the process generating Bitcoin prices follows equation (1)[6], where $\delta = 1$ (H_0) or $\delta > 1$ (H_1).

I report the results in figure 4.5. The sequence of results was compared with the 95% and 99% SADF critical values, obtained from Monte Carlo simulations (2.000 observation with 1.585 observations)[7].

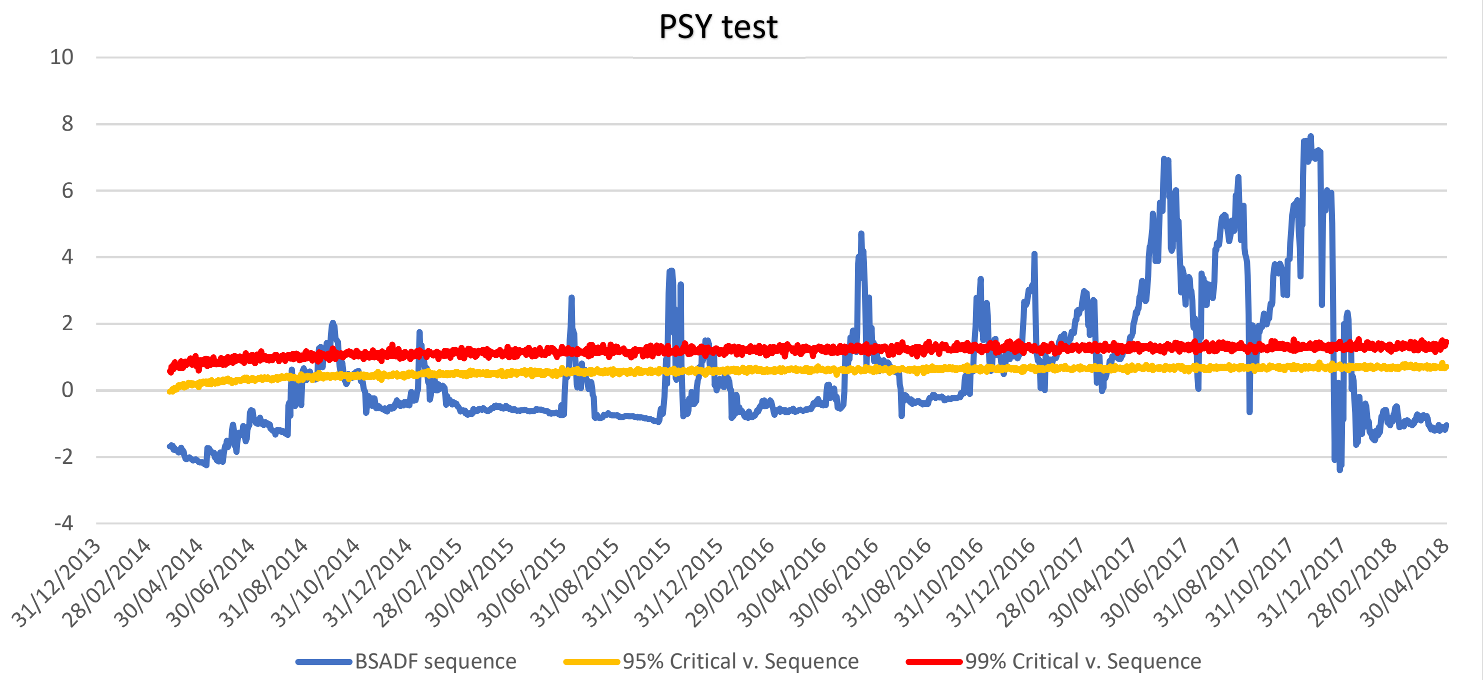


Figure 4.5, PSY test and bubble date-stamping

The results identify many periods of exuberance, the BSADF sequence rises beyond both the 99% (red sequence) and the 95% (orange sequence) critical value sequences many times, detecting explosivity in price. The test identifies multiple bubbles in the sample. It is worth noticing that according to the test the first three exuberance periods last for just a few days, or even just one day if one considers the 99% critical values sequence. Therefore since these episodes last for a very short time I can’t conclude there is enough evidence to identify a bubble.

On the contrary during June 2016 we have a first longer period of exuberance lasting almost two months (considering the 95% critical values) and one month (considering the 99% critical values). From the end of 2016 the behavior of Bitcoin becomes even more explosive, with the price almost doubling at year end considering the values at the beginning of the year. Since October 2016 the BSADF sequence is almost always above the 95% critical values (orange

---

[6] Also in these calculations I Followed Phillips, Shi, Yu (2015) in the analysis of S&P 500 data, and I used in calculations a lag of order J=0

[7] Again r0 is determined following equation (1) and it is equal to a fraction of 0,05521 of the whole sample, or 87 observations

sequence) until the first week of January 2018. I have very similar results considering the 99% critical values (red sequence): from April 2017 to the end of December the BSADF sequence is always above the 99% critical values. With these evidences I can conclude that Bitcoin price experienced a bubble period at least for the whole 2017.

The PSY test also suggests that the bubble seems to have deflated at the beginning of 2018, when the test statistic sequence returns under both the 99% and 95% critical values. In fact from an all-time closing high of 19.187$ on 16/15/2017 the price rapidly halved: at close on 1/2/2018 the price had dropped to 9.181$.

Concluding the PSY procedure succeeds in detecting multiple bubbles in Bitcoin prices in the considered period. The model denotes price exuberance, especially during 2017 where price rose from 800$ to 19.000$: the model signals an ongoing bubble. Therefore, beyond unclear and not incredible fundamental value, popularity themes driving returns, the PSY procedure gives the last evidence of the Bitcoin financial bubble. As already suggested by the summary SADF and GSADF test statistics from 2014 to May 2018 a bubble was present in Bitcoin prices, the PSY procedure identifies the precise periods.

Conclusions:

Virtual currencies and blockchain technology can be powerful innovations, both for citizens, and for policy makers. The way payments and transfers are conducted can be improved by new possibilities and security. Coming to monetary policy a virtual currency could widen the ways of intervention for a central bank, but balance is needed as privacy of citizens is questioned. Drawbacks of this technology as deflationary risk can be overcome building the currency protocol, in the meantime preserving the advantage of a predetermined money supply.

Cryptocurrencies as of today are probably an experiment as circulation for practical means (transactions) among the public is not so relevant. Bitcoin brings valuable innovation in the field of finance and economics, even if all of its features can be improved, and find in other systems better alternatives (quantity of transactions per second as an example). The clearest reason that could justify its increase in price are illicit activities which exploits the anonymity of Bitcoin and its ability to cross borders easily in a few minutes. But even considering the amount of illicit activities, the price in the recent past seems unsustainable. In fact, evidences of a financial bubble in Bitcoin are plentiful: the most evident being that only popularity is able to explain part of its returns, while many other economic factors seem to be insignificant. Ultimately a confirmation of bubble is found exploiting the PSY procedure: from 2014 to 2018 multiple bubbles are identified, the longest lasting for all 2017.

Probably the innovation brought by Bitcoin and Blockchain played the greatest role in enchanting investors who poured money into the market. Only the idea of a currency controlled by its own users and no central authority is revolutionary. Anyway, in the end the price collapsed, and I think the main reason is to attribute to the many ways to short Bitcoin that became available. For a long time, the impossibility to short put a kind of martingale on the evolution of price, which could only go up as this asset became more popular.

References:

1. Szetela, B., Mentel, G., Gędek S. (2016). Dependency Analysis between Bitcoin and Selected Global Currencies
2. Gervais, A., Ghassan, O. K., Wust, K., Glykantzis, V., Ritzdorf, H., Čapkun, S., (2016). On the Security and Performance of Proof of Work Blockchains.
3. Chiu, J., Koeppl, T. (2017). The Economics of Cryptocurrencies Bitcoin and Beyond.
4. Courtois, N.T., Grajek, M., Naik, R., (2014). Optimizing SHA256 in Bitcoin Mining
5. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
6. Siim, J., (2018). Proof-of-Stake
7. BitFury Group (2015). Proof of Stake versus Proof of Work
8. Sharma, T., K., (2018). How exactly is proof of stake implemented?
9. Herbert, J., Litchfield, A., (2015). A Novel Method for Decentralised Peer-to-Peer Software License Validation Using Cryptocurrency Blockchain Technology
10. Dong, H., Habermeier, K., Leckow, R. Haksar, V., Almeida, Y., Kashima, M., Kyriakos-Saad, N., Oura, H., Saadi Sedik, T., Stetsenko, N., and Verdugo-Yepes, C. (2016). IMF staff discussion note. Virtual Currencies and Beyond: Initial Considerations.
11. Bordo, M.D., 1981, "The Classical Gold Standard: Some Lessons for Today," Federal Reserve Bank of St. Louis Review, (May), pp. 2–17.
12. Redish, A., 1993, "Anchors Aweigh: The Transition from Commodity Money to Fiat Money in Western Economies," Canadian Journal of Economics: pp. 777–795.
13. Yermack, D., 2013. Is Bitcoin a real currency? An economic appraisal.
14. Elwell, C., K. 2012. Deflation: Economic Significance, Current Risk, and Policy Responses.
15. Andrews L., A., (2008). Fed assumes the role of lender of last resort. The New York Times. March, 12, 2008.
16. Douglas W. Diamond; Philip H. Dybvig (1983). Bank Runs, Deposit Insurance, and Liquidity.
17. Bruhl, V., 2017, Virtual Currencies, Distributed Ledgers and the Future of Financial Services, Intereconomics, 52/6.
18. Glaser, F., Haferhorn, M., Weber, M.C., Zimmarmann, K., Siering, M.b (2014) "Bitcoin – Asset or currency? Revealing users' hidden intentions."ECIS 2014 Tel Aviv
19. Cheah, E. -T., & Fry, J. M. (2015). Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin. Economic Letters, 130, 32–36.
20. Kroeger, A., Sarkar, A (2016). Is Bitcoin Really Frictionless? Liberty Street Economics, 23 Match 2016.
21. Thomas, Manoj and Vicki Morwitz, 2009, "Heuristics in Numerical Cognition: Implications for Pricing" in Vithala R. Rao ed., Handbook of Pricing Research in Marketing (Northampton, MA: Edward Elgar Publishing)
22. Mersch, Y., (2018). Virtual or virtueless? The evolution of money in the digital age. Official Monetary and Financial Institutions Forum, London, 8 February 2018.
23. Raskin, M., Yermack, D., (2016). Digital currencies, decentralized ledgers, and the future of central banking.
24. Rogoff, K., (2016). The Curse of Cash.
25. Haldane, Andrew G., 2015, "How Low Can You Go?"
26. Konig, J.P., 2014. Fedcoin. Available at http://jpkoning.blogspot.com/2014/10/fedcoin.html.
27. Winkler, Robin, 2015, "Fedcoin: How Banks Can Survive Blockchains," Konzept 6, 6-7.

28. Raskin, Max, 2012, “Dollar-Less Iranians Discover Virtual Currency,” Bloomberg News, November 29
29. Popper, Nathaniel, 2015, “Can Bitcoin Conquer Argentina?” The New York Times, April 29
30. Rosenfeld, E., 2015. Ecuador becomes the first country to roll out its own digital cash
31. Billner, A., 2018. ‘No Cash’ Signs Everywhere Has Sweden Worried It’s Gone Too Far
32. Danmarks Nationalbank. Report n. 24, 12/12/2017. Danish households opt out of cash payments
33. Davies. D., 2017. How I guesstimated the value of Bitcoin in 2014.
34. Weber, W. E. (2016), A Bitcoin Standard: Lessons from the Gold Standard, Bank of Canada Staff Working Paper, 2016–14
35. Whelan K., 2013. How is Bitcoin different from the dollar?
36. Haubo Dyhrberg, A., (2016). Bitcoin, gold and the dollar –A GARCH volatility analysis
37. Peetz, D., Mall, G., (2017). Why Bitcoin is not a currency but a speculative real asset
38. Soddy, F., (1926). Wealth, Virtual Wealth and Debt, George Allen & Unwin 1926, page 56
39. International energy agency report (2017). Key world energy statistics
40. Holtaus, E., 2017. Bitcoin could cost us our clean-energy future
41. Croman, Kyle; Eyal, Ittay (2016). "On Scaling Decentralized Blockchains"
42. Lee, T., B., (2017). Bitcoin’s insane energy consumption, explained
43. L, S., Wang, J., C. 2014, Federal reserve bank of Boston. Bitcoin as Money?
44. Goldman Sachs 2014, Global macro research. All about Bitcoin
45. World bank 2014. Remittances prices worldwide. 23/9/2017
46. Easley, D., O’Hara M., Basu, S., (2018). The Evolution of Bitcoin Transaction Fees
47. Masciandaro, M., (1999). Money Laundering: The Economics of Regulation
48. Lu, L., 2018. Bitcoin: Speculative Bubble, Financial Risk and Regulatory Response
49. Clover, C., 2016. ‘China’s capital curbs hit EU companies’, Financial Times, 7 December 2016, p 6.
50. Bryans, D. (2014). Bitcoin and money laundering: mining for an effective solution. Indiana Law Journal, 89(1), 441–472
51. Qinqin, P., Yujian W., Wei, H., 2017 ‘China Steps Up Curbs on Virtual Currency Trading’, Caixin, 08 September 2017
52. Seth, S., 2018. Is Bitcoin Banned in China?
53. Matthews, Christopher M; Sidel, Robin. Two Charged in Alleged Bitcoin-Laundering Scheme. VentureWire; New York (Jan 27, 2014)
54. Hong, Nicole (2015-05-29). "Silk Road Founder Ross Ulbricht Sentenced to Life in Prison". Wall Street Journal.
55. FBI, (2014). "Sealed Complaint 13 MAG 2328: United States of America v. Ross William Ulbricht". 27 September 2014. https://web.archive.org/web/20140220003018/https://www.cs.columbia.edu/~smb/UlbrichtCriminalComplaint.pdf
56. Gibbs, S., (2017). 'Criminal mastermind' of $4bn bitcoin laundering scheme arrested
57. Gibbs, S., Beckett, L. (2017). Dark web marketplaces AlphaBay and Hansa shut down
58. Kostarelis, S., 2017. The first-ever Bitcoin transaction was used to buy two pizzas – today, it’s worth $150 million
59. Lahiff, K., 2018. Bitcoin is a bubble and a perfect example of ‘faddish human behavior,’ says Robert Shiller
60. Atkinson, P., 2012. Asset price bubble identification and response.

61. Kamalodin, S., 2011. Asset Bubbles, Financial Crises and the Role of Human Behaviour Department Paper, Utrecht: Rabobank, 2011.
62. Kindleberger, Charles P., and Robert Z. Aliber. Manias, Panics, and Crashes. New York: Palgrave Macmillan, 2011.
63. Mamudi, S., 2008. Lehman folds with record $613 billion debt".Marketwatch. 2008-09-15
64. Hofrichter, S., 2018. Beyond the Bitcoin Bubble, the Benefits of Blockchain
65. Balcilara, M., Bourid, E., Guptac, R., Roubaudb, D., (2017). Can volume predict Bitcoin returns and volatility? A quantiles-based approach
66. Kristoufek, L., 2013. BitCoin Meets Google Trends and Wikipedia: Quantifying the relationship between Phenomena of the Internet Era. Scientific Reports 3, Article number: 3415
67. Ciaian, P., Rajcaniova, M., Kancs, D.A., 2016. The economics of BitCoin price formation. Appl. Econ. 48 (19), 1799–1815.
68. Bouoiyour, J., Selmi, R., Tiwari, A., 2015. Is Bitcoin business income or speculative foolery? New ideas through an improved frequency domain analysis. Ann. Financ. Econ. 10, 1550002.
69. Hale, G., Krishnamurthy, A., Kudlyak, M., Shultz, P., 2018. How Futures Trading Changed Bitcoin Prices. San Francisco FED.
70. Barnett, C., 2017. Inside the meteoric rise of ICOs
71. Popper, N., 2018. As Bitcoin Bubble Loses Air, Frauds and Flaws Rise to Surface
72. Shifflett, Shane; Jones, Coulter (May 17, 2018). "Buyer Beware: Hundreds of Bitcoin Wannabes Show Hallmarks of Fraud". Wall Street Journal. Retrieved May 18, 2018
73. SEC, "ICO – HOWEYCOINS If You Responded To An Investment Offer Like This, You Could Have Been Scammed – HoweyCoins Are Completely Fake!". *Investor.gov.* U.S. Securities and Exchange Commission. Retrieved May 18, 2018.
74. Usman Chohan, U., 2017 Initial Coin Offerings (ICOs): Risks, Regulation, and Accountability
75. Koetsier, J., 2017. Hundreds of Millions of Dollars Via Initial Coin Offerings
76. Polasik, M., Piotrowska, A., Wisiniewski, T., P., Kotkowski, R., Lightfoot, G., (2015). Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry
77. Asprem, M. (1989). Stock prices, asset portfolios and macroeconomic variables in ten European countries. Journal of Banking & Finance, 13(4-5), 589–612. doi:10.1016/0378-4266(89)90032-0
78. Chen, N., Roll, R., & Ross, S. A. (1986). Economic forces and the stock market. The Journal of Business, 59(3), 383–403.
79. Ludvigson, S. C., & Ng, S. (2009). Macro factors in bond risk premia. Review of Financial Studies, 22(12), 5027–5067. doi:10.1093/rfs/hhp081
80. Stock J., H., and Yogo, M., 2005. Testing for Weak Instruments in Linear IV Regression
81. Pagan, A. R., and D. Hall. 1983. Diagnostic tests as residual analysis. Econometric Reviews 2: 159-218.
82. Hansen, L. P., J. Heaton, and A. Yaron. 1996. Finite sample properties of some alternative GMM estimators. Journal of Business and Economic Statistics 14: 262-280.
83. Montiel Olea, J. L., and C. E. Pflueger. 2013. A robust test for weak instruments. Journal of Business and Economic Statistics 31: 358-369
84. Hansen, Lars Peter (1982). "Large Sample Properties of Generalized Method of Moments Estimators". Econometrica. 50 (4): 1029–1054
85. Phillips et al. (2011). Explosive behavior in the 1990s NASDAQ: When did exuberance escalate asset values? International Economic Review 52 (2011), 201–26

86. Phillips, P., C., B., Shi, S., Yu., J. 2015. Testing for multiple bubbles: historical episodes of exuberance and collapse in the S&P 500
87. Baur, D., G., Glover, K., J. (2012). A gold bubble?