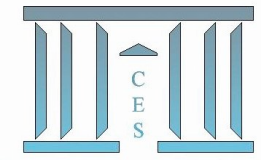
UNIVERSITÉ PARIS 1
PANTHÉON SORBONNE

Documents de Travail du
Centre d'Economie de la Sorbonne

CES Working Papers



The Digital World: I – Bitcoin: from history to real live

Dominique GUEGAN

2018.11

Maison des Sciences Économiques, 106-112 boulevard de L'Hôpital, 75647 Paris Cedex 13
https://centredeconomiesorbonne.univ-paris1.fr/
ISSN : 1955-611X

The Digital World : I – Bitcoin : from history to real live

Dominique GUEGAN

University Paris1 Panthéon Sorbonne, LabEx ReFi

Ca'Foscari University in Venezia, IPAG Business school

Abstract

Bitcoin can be considered as a medium exchange restricted to online markets, but it is not a unit of account and a store of value, and thus cannot be considered as a money. Bitcoin value is very volatile and traded for different prices in different exchanges platforms, and thus can be used for arbitrage purpose. His behavior can be associated with a high volatile stock, and most transactions in Bicoin are aimed to speculative instruments. The high volatility in Bitcoin and the occurrence of speculative bubble depend on positive sentiment and confidence about Bitcoin market : several variables my be considered as indicators (volume of transactions, number of transactions, number of Google research, wikipedia requests). The star of the crypto-currencies has attained the 19 716 dollars in December 2017 and decreased to 6707 dollars March 29, 2018. In capitalization it is at this time the 30th mondial currency. We explain some limits and interests of the Bitcoin system and why the central bankers and regulators need to take some decision on its existence, and in a second paper we suggest what could be the possible evolution of the Bitcoin Blockchain.

I – Introduction and history

At the origin a financial crisis….. in 2008 and we know what is happening…

Concommitment arrives a publication by Satoshi Nakamoto of a paper on Proof of Work (PoW) with description of a new currency even if at this time it exists a lot of digital currencies. This one is based on a cryptographic protocol permitting to make secure transactions (thanks to the Hash functions and the Merkel tree) avoiding the double spend thanks to the incentives provided to the miners. This protocol is in open source with no third intermediary, and spend speudo-anonymity due to the way of the creation of cryptographic digital private key.

The Bitcoin system was invented in 2008, the first bitcoins were created on January 3, 2009. Their number is limited to 21 million units and divisible up to the eighth decimal place. Satoshi Nakamoto claimed to have worked on bitcoin from 2007 to 2009. In 2008, he published a document on a mailing list describing bitcoin digital currency. In February 2009, he posted an announcement about his work on the P2P Foundation site. On January 3, 2009, the first block is created. In February 2009, the first version of the Bitcoin software was released on the P2P Foundation website and, to make the network working, Satoshi Nakamoto put his computer to work and thus created the first bitcoins.

In this paper we analyse the Bitcoin system and the way to make transactions. Then we question some classical problematics link with Bitcoin environment. We discuss the economy around Bitcoin, the Bitcoin's protocol based on cryptography as other competitive protocols. The recent positions of the regulators are introduced. A summary of references are provided at the end.

II - What is Bitcoin?

Bitcoin is a virtual currency based on the technology called Blockchain using cryptographic protocol. Thus, Bitcoin is not issued by a central bank. The quantity of units in circulation is not controlled by any central authority or government but by a software algorithm. Bitcoins are created by a "mining" process done by the users of the Bitcoin network. The participants of this network called miners provide their computing power, verify and record payments into a public ledger called Blockchain. In return of this service they receive transactions fees and newly mined Bitcoins. Bitcoins can be stored in local wallets.

How works the Bitcoin blockchain?

The Bitcoin Blockchain stores all transactions since the system was created. The database is stored in a decentralized manner in a peer-to-peer network that discards double spending attempts and authenticates valid transactions in a long term blockchain built using a hash-based proof-of-work mechanism: there is no centralized third party that holds the database because it is replicated over the entire database.

A transaction involves debiting certain accounts to credit other accounts. A Bitcoin transaction is irrevocable and cannot be canceled. A new block of transactions is created every ten minutes, and contains a maximum of 1megabyte (1MG), about 7 transactions per second are solved. The blocks are linked to each other since each block refers to the previous one, which is why we speak of Blockchain. The transactions are done through the network thanks to the miners who solve a complex mathematical problem provoding their computing power and in return receiving transactions fees and a certain number of Bitcoins as soon as they validate a block containing at most IMB of transactions.

The number of Bitcoins evolves over time because the miners are paid in bitcoins created each time a new block is built. Thus, all the bitcoins in circulation are created following the constitution of blocks. The remuneration linked to the constitution of a block evolves regularly, and is halved every 210,000 blocks. Thus the remuneration that was 50 bitcoins per block originally in 2009 is currently 12.5 bitcoins per block and diminuishes every four years. Knowing that there is an average of one new block every 10 minutes, the overall number of bitcoins follows a regular geometric sequence whose limit is 21 millions in total. In March 2018, 16,90 million bitcoins have been created.

In practice, to build the blocks, thousand players in the world compete simultaneously to solve this mathematical problem but as soon as is done by one miner, the proof's verification is easier and done by all the network which permits to validate the transaction. Thus, this system which is in open source is also based on the consensus of the entire system. Note that to falsify a transaction in the last block in progress, it requires computing power equivalent to the sum of the computing power of the entire network (this attack is known as the Sybil attack). Although theoretically this could be possible with a little luck, it is *nearly* physically impossible to change a transaction that has taken place several blocks back because it would require in a limited time to be able to recalculate all the blocks passed until the present moment.

How to exchange Bitcoin?

To be able to own and exchange bitcoins, one must have the equivalent of an account number. These account numbers are governed by cryptographic public key and private key. To give

bitcoins to a given account, you only need to know the public key of the person; on the other-hand to move an account it is necessary to hold the private key that can encrypt transactions. An account is identified by a number made from a 160-bit cryptographic fingerprint (20 bytes). There is thus a maximum of 2 ^ 160 possible bitcoin addresses (about 10 ^ 48). A bitcoin address occupies 25 bytes. As an example, here is the first bitcoin address that received bitcoins: 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa. To make a transaction, one sends a request to the Bitcoin network which validates it. The transactions stored in the Blockchain are not only "A gives x Bitcoins to B", but scripts that may contain a few lines of code. It needs about 1 hour to finalize a transaction in means, even if for a non negligeable number of transactions those are never done[1].

III - Permanent questions

Pseudo-Anonymity

The Bitcoins are stored in a wallet, and it is necessary to secure them. It is the responsibility of the owner to do it: on a USB key, or on a computer having no link with internet (to avoid hacking), or on a dedicated platform. When an account (wallet) is created the owner provides information on his/her identity to the platform where the account is created. Now when Bitcoins are exchanged in fiat currencies the identity of the owner is also known. So, the process is not anonymous.

When a person sends and receives bitcoins his/her personal identity is not known, however achieving reasonable anonymity with Bitcoin can be quite complicated and perfect anonymity may be impossible. Sending and receiving bitcoins is like writing under a pseudonym. If authors' pseudonym is ever linked to their identity, everything they ever wrote under that pseudonym will now be linked to them. In Bitcoin's system, the pseudonym is the address to which one receives Bitcoin. Every transaction involving that address is stored forever in the blockchain. If this address is ever linked to an identity, every transaction will be linked to it. One way to increase the anonymity is to use for instance multiple wallets[2]. Nevertheless knowing the merchants that allow bitcoin transactions, and looking at the merchants leak payments information, this can reveal information on transactions on the blockchain if the link includes the amount and the time of the purchase.

In another side, anonymity concerns only public blockchains like Bitcoin, and the anonymity problem for blockchain technologies is a technological challenge as well as a political one. For instance, there are currently talks to ban anonymous and pseudonymous currencies like Bitcoin in China and South Korea for unidentified users (in order to ban unsupervised investments).

Sustainability

If you are interested by the environmental, social and corporate governance with respect to Bitcoin system some questions arise.

Indeed, due the huge energy used to mine Bitcoin, we could end up in a situation within a few years where the electricity consumption of bitcoins mining would be equivalent to a country like the Netherlands. Thus, one can identify different reasons for which Bitcoin is not sustainable : (i)

[1] https://core.jochen-hoenicke.de/queue/#2h

[2] A simple and lightweight software wallet allowing to manage multiple wallets is MultiBit.

the era of costless bitcoin transactions is long gone. The fees to make transactions are costly, they have ranged from $1 to $25 (December 2017) per transaction, even if in March 2018 the fees have decreased. They depend on the network's available capacity. The situation makes small, day-to-day payments, from coffee purchases to bus ticket sales, increasingly impractical[3] the use of Bitcoins. (ii) In energy terms, meanwhile, a recent analysis[4] estimated that a single Bitcoin transaction requires 215 kilowatt-hours of electricity to process, that is the equivalent of what an average American household consumes in one week. (iii) The power necessary for work is huge and increases continuously. This contributes to the concentration of miners (pools) which is also an important risk for the safety of the Bitcoin's network. (iv) Moreover, the production of electricity used to mine Bitcoin is polluting, mainly because of the electricity produced in China from coal plants. The miners are trying to locate where the electricity is the cheapest and where the temperatures are fresh: in January 2018, an estimate made by Coinschedule proposed the following distribution: China (11MW), Georgia (60MW), USA (27 MW), Canada (18MW), Sweden (10MW), Iceland (5MW), Estonia (2MW). (v) The bitcoin 's reputation already has for opaque governance, cyber crime and dark market trade, even if practically it seems that changes have been done concerning these activities. (vi) Bitcoin can be used to exchange non-financial data coded as a standard transaction with the possibility of introducing objectionable content (for example links to pirate content or malware). But there is no way to remove these illegal contents. (vii) The speculative behavior is also questionnable, even if the recent spike in the price in December 2017 (19 000 dollars) has delighted cryptocurrency speculators and early investors the world over, with the decision by one of the world's top derivatives exchanges, CME Group, to launch bitcoin futures December 10, 2017. Nevertheless the CME's plans to list bitcoin futures might not be enough to dissuade responsible investment managers from shunning the asset class in an environmental, social and governance-friendly indices in the long term.

During the last years, it appears that bitcoin's primary use is for speculation rather than transaction, the energy wastage serves very little constructive social purpose. Nevertheless we need to have in mind that this energy-intensive system is due to the underlying proof-of-work concept which requires a lot of computing power, in which the parties involved try to perform the computations as quickly as possible using dedicated hardware. It is admitted that this offers a secure system with all the advantages of blockchain technology, but as it is energy demanding in the future this point has to be studied carefully and alternatives need to be developped.

Security problems

Some effort is required to protect the owner's privacy with Bitcoin. All Bitcoin transactions are stored publicly and permanently on the network, which means anyone can see the balance and transactions of any Bitcoin address. However, the identity of the user behind an address remains unknown until information is revealed during a purchase or in other circumstances. This is one reason why Bitcoin addresses should only be used once. We recall now some risks link with the security of the Bitcoin environment.

Risks which concern the transactions. (i) Any transaction issued with Bitcoin cannot be reversed, they can only be refunded by the person receiving the funds. That means people should take care to do business with persons and organizations one knows and trusts, or who have an established reputation. (ii) Each transaction's confirmation takes between a few seconds and 90 minutes, with

[3] Until a new protocol is developed, for instance ther lightning protocol.
[4] See Motherboard site

10 minutes being the average. If the transaction pays too low a fee or is otherwise atypical, getting the first confirmation can take much longer, sometimes several days, sometimes it is never done. (iii) The possession of bitcoins is based on the retention of the private key associated with the account. This key is held only by the user, and its loss (for example in the case of formatting the hard disk where it is stored), creates definitive loss of associated bitcoins: it is estimated that to date about 3 million bitcoins were lost. (iv) In the bitcoin blockchain, miners use their computational power in exchange for a given amount of bitcoins for every solved block, plus transaction fees. When the amount of bitcoin reaches its predetermined market cap, block will only be solved for transaction fees. The earning of farm holders will then be greatly reduced, which may lead in most of them leaving the Bitcoin's hashing market for more profitable markets. It will then be easy for a farm with subsequent hashing power to take control of the Bitcoin blockchain. This incentive problem is already a concern for small transactions, which can be pending for a very long time before they become worth solving for miners (their associated fees being lowers). This may lead to a centralization of small payments in private businesses which would greatly reduce the purpose of the blockchain (no needs to have a trusted party) in the first place. Currently, 20% of the transactions are still not included in the Blockchain after 30 days. (v) Finally the illicit transactions are a latent question for Bitcoin environment. In that case a kind of cyber-security tried to discover the origin of the traffic. As the system is decentralized and anonymous in part, the difficulty to follow the transactions is immense. Indeed, there is no payment service provider to turn to (in case of fraudulent transaction), nor central dispute resolution body.

Risks which oncern the exchange's platforms. Businesses need to keep control of the payment requests they are displaying to their customers. If the blockchain Bitcoin has never been hacked and has been running continuously since January 3, 2009, nevertheless, the ecosystem around Bitcoin has had to deal with many incidents (hackage of platforms), including: (i) In February 2014, the most popular trading platform, MtGox, which accounted for over 70% of global Bitcoin transactions went bankrupt, resulting in the loss of the equivalent of more than $ 450 million; (ii) In August 3, 2016, the Bitfinex site which was the most used trading platform, is stolen about 120 000 bitcoins, the equivalent of about $ 65 million (note that the platform has not gone bankrupt but absorbed this loss); (iii) In December 2017, Nice Hash (virtual currency exchange platform and shared mining system) was hacked and lost around $ 3 million: it is the payment system that has been compromised; (iv) In January 2018, the coincheck Tokyo trading platform was hacked after being stolen for the equivalent of $ 530 million. When a platform bankrupts it is nearly impossible for the users to get their money back, because it does not exist any kind of insurance for deposit of bitcoins. Indeed, no insurance is considered relatively to the Bitcoin protocol. A lot of platforms closed, implying irreversible losses for depositors in the half of cases. The question is how to regulate these platforms.

The Sybil attack to the Bitcoin network is also a permanent risk. The proof of work protocol is statistically secured if at least 51% of the nodes are controlled by honest nodes and the transaction is old enough in the blockchain (6 blocks old for Bitcoin's). If one node concentrates the 51% of the power of the network it can make a fork and takes the control of the transactions. In 2017 the major party of the computing power dedicated to mining is owned by pools (Antpool, F2pool, BTCC Pool, Bit Fury) mainly located in China. If these pools agree, the 51% attack is possible: This is the cartel problem. Another possibility is the selfish mining attack: In a selfish attack, the attacker will not publish his valid solutions to the rest of the network. He will keep mining in

order to be one step ahead in the chain. When the other miners of the network are close to finding a solution, the attacker will release his solution effectively claiming block rewards.

Scalability

Scalability is currently the Achilles heel of the blockchain technology. The current Bitcoin protocol takes at least 60 minutes to process a transaction, Ethereum (which is another cryptocurrency based on another public Blockchain protocol) is about 5 minutes long. It is a concern for smart contracts that may interact with IoT (internet of things) where information flows at a high frequency. This scalability question for Bitcoin could be solved in part with the development of the lightning protocol.

IV - Bitcoin and real life

Several points make the use of Bitcoins in real life uncertain… volatility – speculative instrument - bubble

Volatility. The price of a bitcoin can unpredictably increase or decrease over short period of time due to its young economy, novel nature, and illiquid markets. Bitcoin should be seen like a high risk asset, and a recommandation is to say that one should never store money that one cannot afford to lose with Bitcoin. Bitcoin is too volatil to measure value, trade or save.

A speculative instrument. Starting from a capitalization of 20 billion dollars in January 2017, outstanding capitalization of crypto-currencies exceeded 100 billion in June 2017 and reached more than 750 billion in January 2018. Bitcoin is relatively rare (limited to 21 million units), and since the system is in fashion, the price of this asset has grown strongly, rising from $ 1,000 in January 2017 to a high of more than $ 19,000 in December 2017, making this currency a very speculative cryptocurrency. Nevertheless, it must be kept in mind that bitcoin has no underlying and is theoretically worth nothing: its price follows supply and demand. If it multiplied by 19,000 in six years (it was worth $ 1 in April 2011), nothing prevents it being divided (or multiplied) by 1,000 in the coming years. It is not uncommon to see changes of more than 10% (up or down) of its price. Bitcoin lost 60% of its value between December 2017 and March 2018, but Bitcoin has already experienced other bearish periods, in 2013, 2015, and more in 2017 of quite great importance. The current fall is accompanied by a significant drop in transactions: in March 2018 we denote 150,000 transactions per day against 490,000 for example in December 2017.

An attractive framework. Chicago was approved by the CFTC (regulator of banks) to launch the first futures and options in December 2017. This recognition could influence the high volatility observed on the price at the end of December 2017. For the moment, regulators (American and European) have mainly warned about the risky side of these products, while recognizing the opposite that this method of financing has "some strengths" (Jerome Powell, President of the US Federal Reserve). In France, in November 2017 Tobam, a player recognized in the French management has launched a fund "Bitcoin fund" to invest on the crypto-currency for investors. This fund registered with the AMF is not regulated or supervised.

It is not a currency. Bitcoin is not a currency from monetary point of view (references are France, Germany, US, China, South-Korean, Canada, Japan, etc.) . As the circulation of Bitcoin is slow and quantity of Bitcoins limited, from an economical point of view, Bitcoin is not adapted to the demand for money, cannot help to revive the economy (credit), nor to control inflation. In the case of the purchase of a property, the transactions cannot be canceled, even if the property is not

delivered. It can make the exchanges difficult. One can encounter difficulty in converting Bitcoins into Euros (for instance) (no guarantee of convertibility of the currency by the public authorities). The circulation speed of the Bitcoin is low: only 4% of the bitcoins in circulation are weekly use. This is more like a casino economy, and since there is currently no regulation, no central bank ensures the stability of the value.

From an ethic point of view. Bitcoin escapes for the moment the tax authorities, escapes the declaration of gains, and users are not equal (miners are privileged). It concerns a restricted population: the users are essentially adepts of new technologies or people wanting to free themselves from the guardianship of the states. Knowledge of computer science and computer security is required to successfully protect the wallets and their contents.

Different forms of Bitcoins. Due to the difficulty to the developers of Bitcoins and miners to have consencus on the internal system, a new Bitcoin emerges in December 2017, the Bitcoin Cash. Parallely, we observe since end of 2017 a surge in cryptocurrency markets, prices have gone up. The website coinmarketcap.com shows a list of the top cryptocurrencies, and we can observe that some of the coins that started under $1 going up in value by 100 percent or more in a week. We can ask if the investors try to find the next « bitcoin », transferring the « bubble » observed on the Bitcoin on another currency (Ethereum, Litecoin, Bitcoin Cash, etc.). The Bitcoin system is also affected by the non stability for the fees' transactions. Indeed, miners can priviledge transactions with high fees, and the time to be sure that a transaction holds is also varying.

It exist an impact of Bitcoins on industry. Indeed it is possible to buy goods with Bicoins. Industries that have begun to accept Bitcoin as payment are mostly online companies themselves. The company Cheapnam, that provide services which involve domain name registry, is accepting bitcoins as a mode of payment. Other digital companies like WordPress, which provides resources to set up professional and private blogs accept bitcoins. The company Steam, which is a computer game distributor and a general gaming platform accepts these currencies too. Virgin Galactic accepts bitcoin as a payment method. The same also holds true for a car company, Tesla which accepts Bitcoins. KFC in Canada has decided to accept Bitcoins payments for online orders, in March 2018 for a limited period.

Effect of Bitcoin on Banks. The potential impact of the digital currency on the central banking should not be taken lightly. The Bank for International Settlements (BIS), jointly owned by the world's leading central banks, noted in November 2017 that Bitcoin could interrupt the ability of central banks to exert control over the economy, as well as issuing money. As of now, many central banks are closely observing developments in the growth of Bitcoin. Many others, however, have already responded by sending out proposals for the issuance of digital version of their fiat currencies. The central banks of Canada and Ecuador are the first to explore such opportunities. In recent years, the influence of Bitcoin has brought change to variety of industries. In two months, between December 2017 and February 2018, Bitcoin has lost more than two-thirds of its value, hence the need for more precise control of international financial institutions, market regulators and large European banks, as well as Bank for International Settlements (BIS): "Bitcoin becomes at the same time a bubble, a sponzi assembly and an environmental disaster" (Agustin Carsten, February 6, 2018).

The uncertainty observed at the moment is also due to the decision of the Chinese authorities to put a stop to the mining activity on its territory, the hackage of a Japanese cryptocurrency exchange platform, the decision of major US banks to ban transactions with credit cards, as well

as by the likely interventions of regulators in the coming months. Without questionning the financial system or provoking a systemic risk within the world finance, it can perhaps reinforce the crisis of confidence of this same financial system.

We see previously some of the limits concerning the use of Bitcoin, for security, sustainability, volatility, nevertheless this technology can be intresting probably for cross-border payments when countries have a poorly developed banking system.

V – Why and what we need to regulate ?

One of the biggest issues facing the cryptocurrency and blockchain industry today is how this new economy works with the traditional economy, particularly in terms of regulation and integration with existing financial institutions. The difference between fiat money and digital currencies is that fiat money is issued by central banks, while issuers of digital currencies are decentralized.

Concerning Bitcoin, some papers have summarized the reasons why it is important to have some answers or information from the regulators because of the various risks posed by this cryptocurrency. Some of these risks are remote, others are immediate. The difficulty of the regulation of such a system is difficult as there is no central authority that administers and controls the system. The regulation concerning the illegal uses of these cryptocurrencies is well documented. The other aspects are the wallets'providers and the exchange services. Thus besides money laundering, terrorist financing and taxes fraud, Bitcoin system raises a lot of security risks, economic and financial risks as we explained in the previous sections. It is the reason why recently the State Financial Authorities, in different countries, make some advices to the investors and the providers even if no specific regulation arises.

Indeed, since the amount of exchanges and the price attained by Bitcoin, in December 2017 some regulators decide to warn against this crypto-currency. Some months ago the President of Europe, Mario Draghi has explained that the crypto-currencies do not represent a threat for the monopol of Central Banks which are alone habilitated to « battre la monnaie ». This position was shared by the French representant of the board of the BCE, Benoit Coeuré, who alerts on the speculative behavior of this crypto-currency. This behavior depending on several facts : the fascination for this currency due to its novelty, the finding that it seems possible to win a lot of monney very quickly, the interest developped by the ICO (Initial Coin Offering), the fact that the demand is increasing a lot based on an offer whose support is tied, the fact that this currency is intensively used for threft and laundering. Nevertheless it appears very difficult for the countries to speak with the same voice on this subject. March 18, 2018, the FSB, which coordinates the financial regulation for the G20 countries, rejected calls from several countries asking for regulation of cryptocurrencies including bitcoin. Nevertheless we observe that the parliament of the European council took an amendment on the fight against money laundering and the financing of terrorism. Following this directive, anonymity will not be possible on exchanges platforms for crypto-currencies : they will be obliged to identify their users.

The "Autorité des marchés financiers" (AMF) and the French Prudential Supervisory Authority (ACPR) warned investors against investing in bitcoins, highlighting the risks of capital loss and the lack of regulation on the market. Both regulators believe that bitcoins, sometimes "misstated" as "virtual" or "cryptocurrency" currencies, cannot be considered as "financial instruments", and like the other "virtual assets", "do not enter within the scope of direct supervision of the AMF ". In the same way, "they cannot be described as currencies or be considered as means of payment

in the legal sense of the term. As a result, they are therefore not subject to the regulatory framework for means of payment". "Investors are therefore exposed to very high risk of loss in the event of a downward correction and do not benefit from any guarantee or protection of the invested capital," note the two regulators, pointing out that" those who invest in bitcoin do so entirely at their own risk".

At the same time we observe that a lot of major banks around the world, in the United States, United Kingdom, Australia, Canada and Europe, banned credit card purchases of cryptocurrencies, and in some cases debit card purchases opting that they are trying to protect their customers from a risky unregulated market. However, there is no denying the obvious threat that cryptocurrencies pose on many banks. Many financial institutions are aware that they are losing control and they have made it clear that banning the trade of cryptocurrency is an attempt to regain some of that control. While all this is happening, a positive outcome from the recent SEC/CFTC hearing has eased some the fears. Also, another positive statement has also given hope. Mario Draghi, president of the European Central Bank, stated: "Recent developments, such as the listing of Bitcoin futures contracts by US exchanges, could lead European banks too to hold positions in Bitcoin, and therefore we will certainly look at that." Cybersecurity coordinator for the White House and special assistant to Mr Trump, Rob Joyce, said that US is still studying the pros and cons of cryptocurrencies before launching any regulations. Speaking at the Munich Security Conference in Germany, Mr. Joyce made it clear that there needs to be a better level of understanding of cryptocurrencies risks and benefits before the authorities attempt any form of regulation.

Thus we see that the positions of regulators and central banks remain prudent even if they take into account the importance that this kind of market in the future, and their positions can evolve with time.

VIII Conclusion

For cryptocurrencies enthusiasts the true purpose is to create a new form of economic power that will be the harbinger of a new society. A society where economic power is outside and beyond the control of the state, and the monstrous banking and financial sectors that they have fused with. The debate is opened. (i) Can Bitcoin become the most value asset in history not only because it is a better form of money, but because of the astounding personal economic power it creates ? (ii) Can we be able to create a new and more egalitarian society using the power of the blockchain and the internet ? (iii) Considering only the energetic costs, is the system less energy consuming than gold mining or the banking system ? (iv) Is Bitcoin socially sustainable ? (v) Is blockchain technology an interesting application for a sharing framework for medical data, energy generation and distribution among micro-wind, solar, micro-hydro small power generating systems connected as micro-grids at the citizen level, for the management of legal transactions among companies ? (v) Are the related blockchain technologies possible drivers of social changes and from this perspective ?

For a lot of questions we have no answer for the moment, we will debate on some of the questions in the second joint paper, but the most important point is to understand the different concepts and the way in which they work. It is mandatory to diffuse a complete information to the investors. In any case, the cryptography which is the technology behind the cryptocurrencies cannot solve all the questions. The knowledge of the different protocols is a key point, their risks have to be anlysed. Even if the regulators try to follow the line, the regulation and the knowledge

of all the developments are still in their infancy. For now, governments are managing this technology on a case-by-case basis

Some benchmarks from academic references

The reference paper on Bitcoin is the paper of Nakamoto (2008). Presentation of some altcoins with their protocols are developed in Bitfury Group (2015), see also ECB (2015) and Guégan (2017b). Ethereum has been introduced by Buterin (2015), see also Woods (2016) and some comments in Guégan (2017). For information on the rules considered in US and Europe concerning Bitcoin we refer to Guégan and Soritopoulou (2017), and a lot of references therein and for an introduction to the risks on ICO to Guégan (2018). Statistics on Bitcoin are provided in Papparlado et al. (2017), concerning mining we refer to Pappalardo et al. (2017b), costs relative to the network Bitcoin are discussed in Aste (2017).

Aste T. (2017) The fair cost of Bitcoin proof of work, WP, UCL, London

Bitfury group (2015) Proof of Stake versus proof of work, mimeo, US.

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

European Central Bank (2015) Virtual Currency Schemes : A further analysis, 9. Franckfort, Germany.

Guégan D. (2017) Blockchain publique et contrats intelligents (Smart Contrats) :) Les possibilités ouvertes par Ethéreum… et ses limites, Revue Banque, N° 814, Dec. 2017.

Guégan D. (2018) Les ICO une nouvelle façon de lever des fonds sans contrainte ?, Revue banque, N° 817, Feb 2018.

Guégan D., Soritopoulou A. (2017) Bitcoin and the challenge for regulation, Capital Markets law Journal, Issue 4.

Nakamoto S. (2008) A Peer-to-Peer electronic Cash System, https :// bitcoin.org/bitcoin.pdf

Pappalardo G, G. Caldarelli, T. Aste (2017a) The Bitcoin pees network, WP, UCL, London, UK.

Pappalardo G, T. Di Matteo, G. Caldarelli, T. Aste (2017b) Blockchain inefficiency in the Bitcoin Peers network, WP, UCL, London, UK.

Wood G. (2016) Ethereum : a secure decentralized generalized transaction ledger, yellow paper.