

Hueber, O. (2019). Sidechain and volatility of cryptocurrencies based on the blockchain technology. *International Journal of Community Currency Research* 23(2), 35-44.
<https://doi.org/10.15133/j.ijccr.2019.012>

This article is published under a *Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA)*: <https://creativecommons.org/licenses/by-nc-sa/4.0/>



© The Author(s), 2019



International Journal of Community Currency Research

VOLUME 23 ISSUE 2 (SUMMER 2019) 35-44

SIDECHAIN AND VOLATILITY OF CRYPTOCURRENCIES BASED ON THE BLOCKCHAIN TECHNOLOGY

Olivier Hueber

Université Côte d'Azur, CNRS-GREDEG; France; olivier.hueber@univ-cotedazur.fr

ABSTRACT

A cryptocurrency market based on the blockchain technology is characterized by the coexistence of a steady-state supply and a volatile e-money's demand. In this study a cointegration test establishes a long-run relationship between the internal demand of Bitcoins and prices. From this result, we propose to restrain the intrinsic volatility of any cryptocurrency based on the Blockchain technology by introducing a sidechain pegged to the parent chain.

KEYWORDS

Sidechain, Community currencies, Blockchain, Bitcoin, Demurrage.

1. INTRODUCTION

One of the most unusual characteristics about the economics of bitcoin is the juxtaposition of the certainty of supply and the uncertainty of demand. Cryptocurrencies based on the blockchain technology (like the Bitcoin) are not issued according a traditional money market mechanism allowing the confrontation of supply and demand. The supply of bitcoins is programmed to grow along a pre-determined path. The demand of bitcoins is volatile and subject to shocks. A shock to money demand combined with fixed money supply makes the purchasing power of Bitcoin highly volatile. Moreover, the predetermined pace of the Bitcoin creation promotes speculation. If the exchange rate Bitcoin/USD can be easily calculated, it is not the case concerning the internal value of the Bitcoin that is its level of inflation. Given a fixed supply of Bitcoins, the exchange-rate of Bitcoin in US Dollar (BTC/USD) relies strongly on the volume of transactions which is some way an expression of the demand. By focusing on the link between the external value of the Bitcoin and its internal value, we can develop a better understanding of the dynamics on the Bitcoin's demand. If the transaction volume explains partly the volatility of the bitcoin, it then becomes necessary to find a solution to stabilize such a transaction volume. The solution adopted here lies in the introduction of a sidechain pegged to the Bitcoin's blockchain (the parent chain) while adding a demurring mechanism. A sidechain pegged to a parent chain makes possible the convertibility of all the private cryptocurrencies blockchain's technology based. Furthermore, introducing a demurrage mechanism into the sidechain contributes significantly to a decrease of the speculation on Bitcoins.

The outline of the paper proceeds as follow: Section 2 presents a literature review. Section 3 reports the methodology and the data. Section 4 discusses the empirical results and propose a solution. Section 5 concludes the paper.

2. LITERATURE REVIEW

As Sanchez (2016) explained, an inelastic supply with a volatile demand reinforces the instability of Bitcoin. Luther and White (2014) assert that the unstable purchasing power of the Bitcoin precludes it from becoming a major currency. According to Selmi, Tiwari and Hammodeh (2018) such a volatility makes partly Bitcoin market's riskier but a more profitable market for investors. Contrary to common beliefs, Bouoiyour, Selmi, Tiwari and Olayeni (2016) demonstrated that bitcoin is not a speculative bubble. They assert that the long-term fundamentals are the major contributors of Bitcoin price variation. Gandal & al. (2018) pointed out that suspicious trading activity likely caused the unprecedented spike in the BTC/UST exchange rate in late 2013, when the rate jumped from around \$150 to more than \$1,000 in two months. Griffin and Shams (2018) raise some manipulations of the price of the Bitcoin in US dollar due to substantial distortive effects in cryptocurrencies.

There is an important and ancient literature aimed at coordinating private currencies and public currencies among themselves. We can mention the debate initiated by Adam Smith (1776, Book II, chapter II) on free banking in Scotland. Smith viewed that banks can be left free in their paper-money policies because convertibility between different private currencies was enough to prevent excessive issuance (White, 1984). With the emergence of the first private electronic currencies in the 1990s, the debate on the necessary or non-coordination between public and private currencies has been revived.

The original idea was to coordinate these different electronic currencies through a clearing house (Aglietta and Scialom, 2002). The solution of creating an international automated clearing house online has been investigated but it turned out hard to implement because of the difficulty to find a common standard measurement of value (Heller 2017). The invention of the blockchain technology, about ten years ago, has completely revolutionized the way of conceiving the coordination between private electronic currencies and their links with central banks. The central question has become of how to link together different electronic currencies running on a blockchain technology (Back and al. 2014).

3. DATA AND ESTIMATION METHOD

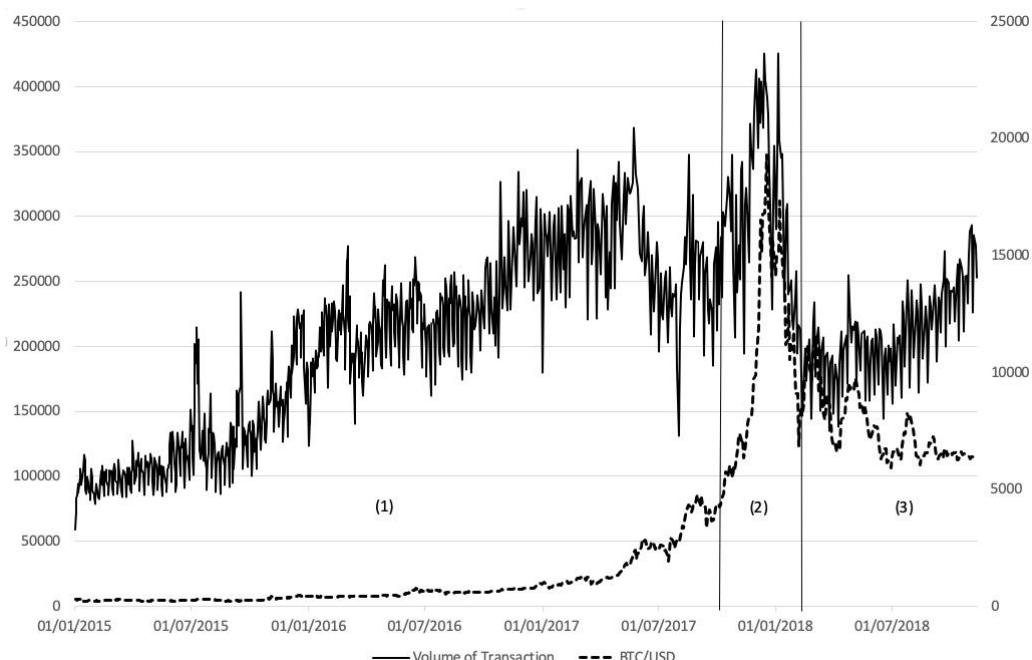
It is well-known that goods or services with inelastic supply (like the petrol or the gas) greater react to demand variations than items with elastic supply. With the Bitcoin, no supply adjustment is possible neither in the short run than in the long run. In the long-run, the pace of Bitcoin's supply slow-down slightly because the difficulty of

mining increases with the power of the network. Along with the inelastic Bitcoin supply, the community's users grows. Such a growing of the number of bitcoin's users pushes up prices that is, the internal value of the Bitcoin which can be estimate by its external value in a public money with legal tender. Therefore, it is difficult to estimate the internal value of the Bitcoin, but it is possible to consider that this value results from an arbitration between Bitcoin's internal demand - measured by the volume of transactions - and the external value of Bitcoin denominated in US dollars. By volume of transaction, we mean the total number of Bitcoin transactions confirmed in the last 24 hours. As for the BTC / USD exchange rate, we use the average market price in USD on the main bitcoin trading places exchanges.

By focusing the long-term relationship between the demand of Bitcoin and the exchange rate BTC/USD, we can divide such a relation in three periods. The first period, from the beginning of the year 2015 to the end of the year 2017, is linked with the take-off of the Bitcoin's adoption by e-money users. During this period of 836 days, the volume of transactions rose in correlation with the value of the Bitcoin in USD. The second period is related to the Bitcoin's speculative bubble from the end of the year 2017 to March 2018. During these approximatively three months the speculation bubble was created and finally burst (see figure 1).

Since the bubble burst, the relation still exists but inversely changed. We can observe an inverse relation between the volume of transactions in Bitcoins and the external value of the Bitcoin in US dollar. While the rules governing the bitcoin supply, are extremely clear and measurable, bitcoin demand is rather opaque. However, there are a few quantifiable variables that we do know about bitcoin demand notably with regards of the number of bitcoin transactions performed each day. The existence of a cointegration relationship should exist between the two-following time-series namely the daily volume of transactions which is an indicator of the demand and the exchange rate of the Bitcoin in US dollar which is an indicator of the external value of the Bitcoin.

Figure 1- Exchange-Rate (BTC/USD) and Daily volume of transactions in Bitcoins during the take-off period



Source: Blockchain Luxembourg S.A.

In the aim of testing such a relation, we perform a cointegration test following the Johansen's approach. The two studied daily time series - provided by Blockchain Luxembourg S.A. - start from the first January 2015 and end the 10 November 2018 that are 1018 observations for each series (see table 1.). By using the Brockwell-Davis methodology (1996), we transform these two-time series by the means of the Box-cox equation, with the value of lambda fixed to zero, in the aim of obtaining their log values.

Variable	Observations	Obs. with missing data	Obs. without missing data	Minimum	Maximum	Mean	Std. deviation
Box-Cox(Volume of Transaction)	1018	0	1018	10,985	12,960	12,124	0,385
Box-Cox(BTC/USD)	1018	0	1018	5,173	9,867	6,736	1,314

Table 1 - Descriptive analysis

3.1. Unit root tests

We apply two-unit root tests on the transformed series (log values Box-Cox): a Dickey-Fuller test (DF) and a Phillips-Perron test (PP). The model with an intercept is the one that best describes our data. In all cases in the table below the computed p-values are greater than the significance level alpha=0,05, one cannot reject the null hypothesis H0 (see table 2.). There is a unit root in each of the two-time series.

	Volume of Transaction		BTC/USD	
	Dickey-Fuller test (ADF(stationary) / k: 10	Phillips-Perron test (PP(no intercept) / Lag: Short)	Dickey-Fuller test (ADF(stationary) / k: 10	Phillips-Perron test (PP(no intercept) / Lag: Short)
Tau (Observed value)	-3,012	0,712	-2,099	1,980
Tau (Critical value)	-3,392	-1,941	-3,392	-1,941
p-value (one-tailed)	0,127	0,869	0,548	0,989
alpha	0,05	0,05	0,05	0,05

Table 2 - Unit root Tests

In the aim of checking that a linear relationship between those two series I(1) that produces an I(0) series exist we perform a cointegration test following Johansen's approach. The minimum AIC value gives a VAR order estimation of 4 for our system which means 2 lags in difference for the Vector Error Correction Model (see table 3.). It then becomes possible to check that a linear relationship between those two I(1) series that produces an I(0) series exists.

3.2. Cointegration Tests

Both series have non zero means with no drift and the cointegration relationship as stated at the beginning is not expected to have a linear trend. Therefore, the deterministic trend seems suitable for our test. Again, a model with intercept seems appropriate and we use the Akaike Information Criterion (AIC). In bold, the minimum AIC value gives a VAR order of 3 for our system which means 3 lags in difference for the Vector Error Correction Model (VECM). We can check that there is a good agreement between the chosen criteria (see table 3).

Number of lags	AIC	HQ	BIC	FPE
1	-9,994	-9,986	-9,974	0,000
2	-10,094	-10,080	-10,055	0,000
3	-10,234	-10,212	-10,176	0,000
4	-10,254	-10,225	-10,177	0,000
5	-10,253	-10,217	-10,156	0,000

Table 3 - VAR order estimation

The results for both tests, the max eigen test (or lambda test) and the trace test agree on the rank(1) of cointegration of the system or equivalently on the existence of 1 cointegrating relationship between the two series (see table 4 and table 5.). P-values and critical values for both tests are estimated using the surface regression approach described in MacKinnon-Haug-Mechelis (1998).

H0 (Nbr. of cointegrating equations)	Eigenvalue	Statistic	Critical value	p-value
None	0,023	23,680	15,892	0,002
At most 1	0,003	3,452	9,164	0,500

Table 4 - Lambda max test

Lambda max test indicates 1 cointegrating relation at the 0,05 level.

H0 (Nbr. of cointegrating equations)	Eigenvalue	Statistic	Critical value	p-value
None	0,023	27,132	20,262	0,005
At most 1	0,003	3,452	9,164	0,500

Table 5 - Trace test

Trace test indicates 1 cointegrating relation at the 0,05 level.

Finally, the factorization of the cointegrating matrix is given in the form of the impact matrix (alpha) and the cointegrating coefficients (beta) following the normalization proposed by Johansen (see tables 6 and 7.).

Box-Cox(Volume of Transaction)	0,015	0,005
Box-Cox(BTC/USD)	-0,004	0,002

Table 6 - Adjustment coefficients (alpha)

Box-Cox (Volume of Transaction)	-3,411	-0,648
Box-Cox (BTC/USD)	0,487	-0,019
Intercept	37,849	8,956
Normalized to beta. beta = Id.		

Table 7 - Cointegration coefficients (beta)

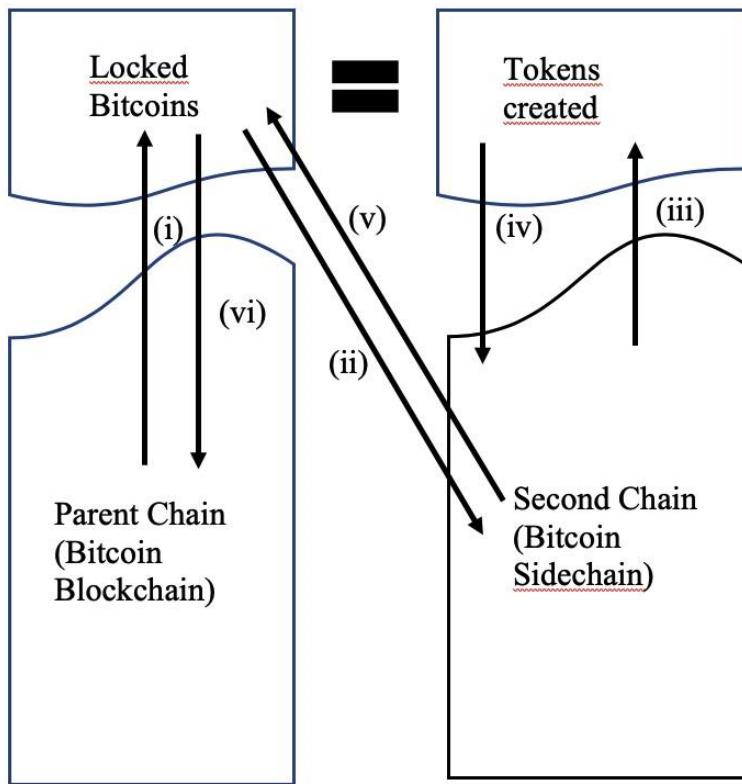
Considering an inelastic supply, the cointegrating relation found here indicate that at least in part, the bitcoin's volume transaction drives prices that is, the internal value of the Bitcoin

4. VOLATILITY OF THE BITCOIN AND THE SIDECHAIN TECHNOLOGY

The cointegration test above leads us to conclude that one cointegrating relationship exists between the volume of transaction in Bitcoins and the external value of the Bitcoin. As the volume of transactions partly explains the volatility of Bitcoin, it is necessary to propose a device allowing to act on the volume of transactions. The solution proposed here lies in the implementation of the sidechain technology in the aim of seamlessly coordinating many cryptocurrencies based on the blockchain's technology.

The sidechain technology is a technology able to connect several blockchains among themselves. A sidechain is a blockchain "pegged" to the main blockchain allowing transfers of key information from one chain to the other. A sidechain is a private blockchain similar to other private blockchains but there is some control over who can send transactions. This sets it apart from open systems, such as bitcoin or ethereum, that any user can join. Instead of being a self-contained system like some other private blockchains, a sidechain is designed as a layer that sits on top or beside of the parent blockchain (for instance the Bitcoin's blockchain). The movement of tokens in the parent chain is basically on another layer within the sidechain, but users and companies have control over their funds since they're tied to the parent blockchain. The sidechain validates data from other blockchains. It is possible to promote the emergence of new gateways between different blockchains. Monetary units can be transferred from one blockchain to another and return back. For instance, n Bitcoins on a blockchain in Bitcoins can be converted into n' other digital currency into the blockchain of this other digital currency with a possibility of reversing anytime the transfer. Such gateways between different blockchains are called sidechains technologies. Sidechains are blockchains that are interoperable with each other. A sidechain can carry digital currencies, in which users are able to seamlessly transfer digital money from one blockchain to another. The sidechain mechanism appears to be the solution to a problem well known by economists namely the competition between different private currencies. With a sidechain, digital money users can import the currency of another blockchain.

With the sidechain technology the volatility character of cryptocurrencies blockchain based is cleared. Bitcoin's users are even going to save bitcoins because they know that they can convert anytime their bitcoins in other cryptocurrencies private or public. With the sidechain mechanism a blockchain cannot borrow more funds that it is engaged to do it. Consequently, the risk is cancelled. The other advantage of the sidechain is to minimize competition between blockchains because all the blockchains can rely on one or a small number of blockchains. Despite the bidirectional transferability between the parent chain and sidechains, both are isolated. As pointed out by Adam Back and al. (2014) in the case of a cryptographic break (or malicious design) in a sidechain, the damage is entirely confined to the sidechain itself. Sidechain technologies appear to be a way for the public banking system driven by public central banks to regain control on the proliferation of private digital currencies like the bitcoin. A central public blockchain denominated in a public currency like the Euro or the US Dollar could be created. Such a public and "official" blockchain could overcome the threat of digital bearer money, like the Bitcoin, on the public character of the money. One solution to transfer assets from a parent chain to a sidechain is to provide proofs of possession in the transferring transactions themselves. When moving assets from one blockchain (i.e; the parent chain) to another (i.e; the sidechain), a transaction on the first blockchain is beforehand created for locking the assets. The protocol is the following (see figure 2).

Figure 2 - Tokens issuance protocol from the Bitcoin's blockchain towards a second sidechain

(i) An amount of as-yet unspent Bitcoins is locked. The unspent Bitcoins must beforehand be identified because the Bitcoins are not perfectly fungible. One Bitcoin cannot be replaced by another. The locked Bitcoins holder publishes its public key and proves its property by signing with its private key. The locked Bitcoins are sent to a specially formed Bitcoin address designed for this purpose. The locked bitcoins can only be unlocked only if somebody can prove they're no longer being used elsewhere in the network. The locked Bitcoins have a demurrage fee that ensures its circulation. Demurrage is a cost associated with owning or holding the currency. Such a demurrage fee was proposed by Silvio Gesell (1929) to eliminate the privileged position held by money compared with capital goods

(ii) A message containing a proof that a fix number of Bitcoins are locked with the public key of its holder is sent to the Liquid blockchain. The message is coded by the Secure Hash Algorithm SHA-256.

(iii) Peg-in process: The sidechain creates the exact same number of tokens than the locked bitcoins and gives to the locked bitcoins holder the control of them. For every bitcoin pegged into the sidechain one token of the sidechain is unlocked or created.

(iv) The tokens holders can use them to settle transactions in the community of the Second Chain Network.

(v) Peg-out process: The transfer back on to the Parent Chain requires the Locked Bitcoin holder to go through a Federation member of the Second Chain.

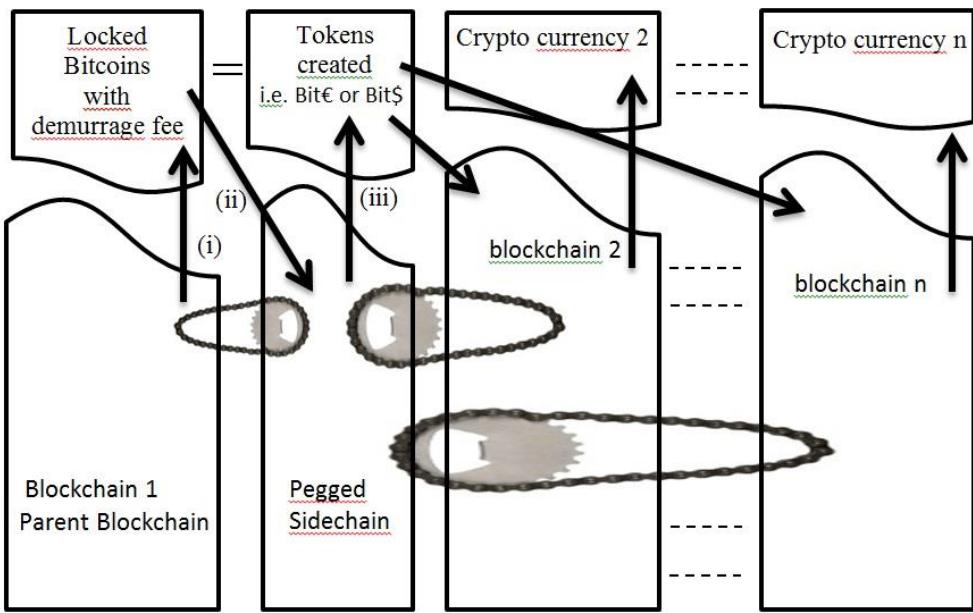
(vi) The locked bitcoins on the parent chain can be unlocked only if a federation member proves they're no longer being used elsewhere in the Second Chain.

In a symmetric two-way peg mechanism, the reverse process is also possible. The holder of newly created tokens in the second sidechain in counterpart of the locked bitcoins has to import proofs of work from the second sidechain to the parent sidechain in order to prove its property of the locked bitcoins. With such a sidechain mechanism, Bitcoins are immobilized on the Bitcoin network (parent chain). Consequently, neither new bitcoins have been created nor destroyed. What is new is the coins (tokens) created on the second chain in counterpart of

the locked number of Bitcoins on the parent chain. Sidechains transfer existing bitcoins from the parent chain rather than creating new ones. They cannot cause unauthorized creation of bitcoins. The maintaining of the security and scarcity of the assets relies on the parent chain (Bitcoin blockchain). The parent chain could be the Bitcoin's one and the sidechain could be one of many public currencies (US Dollar or Euro for instance). A new "BitEuro" or "BitUSDollar" could be created as a sidechain by central banks. If, there is a widespread consensus that the new sidechain is an improvement, it may be more used than Bitcoin. The volatility can be strengthened by the introduction of a demurring process in the pegged sidechain mechanism. The protocol of e-money creation described above is linked to an alternate mechanism of demurrage. A demurring cryptocurrency loses its value over time if unspent. The bitcoins locked depreciate over time. The main advantage of the demurring process is to counterbalance the volatility character of the Bitcoin. Demurrage keeps the currency supply stable while still rewarding miners. It also mitigates the possibility of long-unspent locked coins and creates incentives to increase monetary velocity. A demurring money, called "Freigeld" by Silvio Gessel, has two interesting characteristics for any private cryptocurrency. First, Freigeld is convertible into other currencies and second, it is localized to a certain area (Freigeld is a community currency). If the locked bitcoins on the parent blockchain, like described in the protocol above, are subject to demurrage fees, their circulation is insured and less subject to any speculation or any arbitrage between different cryptocurrencies.

Suppose for example that a certain T-shirt can only be bought with tokens issued by the sidechain at the price of 50 tokens. Such a T-shirt is only available in the "shopping arcade" of the network of sidechain users. The US dollar / token exchange rate is 1 USD for 1 token and the bitcoin exchange rate in USD is 1 bitcoin for \$ 9497.87 (July 30, 2019 price). To obtain the 50 tokens needed to purchase the T-shirt, the bitcoins holder blocks on the parent chain of Bitcoins 0.0053 Bitcoins with a demurring rate of 5.2% per year (rate recommended by Sylvio Gessel in 1929). The sidechain creates 50 token ("Peg-in Process") in exchange for the Bitcoins locked on the main chain and the T-shirt is bought for 50 tokens. Because of the 5.2% per year demurring rate, the T-shirt seller does not really have an incentive to recover the blocked bitcoins with his 50 tokens. If it does after one year ("Peg-out Process"), it will recover only 0.0050244 bitcoins or 47.72 US dollars. It will only do so if the value of Bitcoin against the Dollar appreciates more than 5.2% per year or if the goods or services sold in the sidechain network are not very attractive in terms of quality / price ratio or exclusivity. In other words, the implementation of a demurrage device on the main chain improves the buy / sell relationships within the network of the sidechain. In addition, such a device pushes all sellers in the sidechain network to be competitive and / or provide exclusive goods and services. A demurrage device continuously stimulates economic growth through consumption, reinvestment, and diminishes speculation on private cryptocurrencies.

In the protocol described above (fig 2), sidechains can issue their own tokens. These tokens can be transferred to others blockchains and traded for other assets and currencies, all without trusting a central party (see Figure 3). A parent blockchain (here the Bitcoin Blockchain) has however to play the role of a trusted party for allowing a future redemption. The parent chain is a trusted party around which a monetary coordination of different cryptocurrencies is gradually built.

Figure 3 - Private Cryptocurrencies coordination with Blockchain of Bitcoins as a Parent Chain

The arrows (i), (ii) and (iii) in Fig. 3 are the same that those in Fig. 2. From the pegged sidechains, numerous blockchains can be pegged in their turn. The others pegged sidechains can be for instance Litecoin, Ethereum, community currencies, loyalty programs or something brand completely new.

Once the sidechain is operational, it is possible for users to exchange tokens (coins) between blockchains, without necessarily using the peg. This possibility reduces transaction costs.

5. CONCLUSION

Well beyond the famous bitcoin's case, the Blockchain's technology is spreading at a very high speed in many markets and not only in the cryptocurrency market. This multiplication of markets comprising both a predictable supply and a demand which is difficult to measure, must be taken into account. By examining the long-term time series on Bitcoins, we can demonstrate that there is a cointegrating relationship between the volume of the transactions, and the external value of Bitcoin expressed in US dollars. This allows us to better understand the determinants of demand for bitcoins namely, a speculative demand due to the rarefaction of Bitcoins over time and a transactional demand related to goods and services tradable on the Bitcoin market. These two components of demand combined with a steadily increasing supply make Bitcoin relatively volatile.

This volatility could be considerably reduced by the use of a sidechain attached to the main chain and including a demurring device. The implementation of a sidechain can gradually shape a reliable private cryptocurrency coordination. This coordination even goes beyond mere use of digital monies (private or public). Create a tradeable digital token can be used as a digital money, like the Bitcoin, but also can be used as a representation of an asset, a virtual share, a diploma, a proof of membership or anything else. Nothing prevents the various blockchains to exchange between them their own tokens. A Sidechain pegged to a parent blockchain forms a reliable cryptocurrency coordination comprising bridges between the different blockchains governing the various private electronic currencies. The study of such a coordination through the use of sidechains between on one side the proliferation of cryptocurrencies based on the blockchain technology and on the other side the public currencies with legal tender, must be deepened.

BIBLIOGRAPHY

Aglietta M., Scialom L., (2002). Les risques de la monnaie électronique. *L'Economie Politique*, n°14, pp.82-95

Back A., Corallo M., Dashjr L., Friedenbach M., Maxwell G., Miller A., Poelstra A., Timon J., Wuille P. (2014), Enabling Blockchain Innovations with Pegged Sidechains, commit 5620e43, 2014-10-22

Bouoiyour J., Selmi R., Tiwari A.K, Olayeni O.R., (2016) "What drives Bitcoin price?", *Economics Bulletin*, Vol. 36 No. 2 pp. 843-850

Brockwell P.J. and Davis R.A. (1996) . *Introduction to Time Series and Forecasting*. Springer Verlag, New York.

Gandal, Neil & Hamrick, JT & Moore, Tyler & Oberman, Tali. (2018). Price Manipulation in the Bitcoin Ecosystem. *Journal of Monetary Economics*. 95. 10.1016/j.jmoneco.2017.12.004.

Gesell S., (1929) "The Natural Economic Order: a Plan to Secure an Uninterrupted Exchange of the Products of Labour", Trans. Philip P. (1916), Berlin Neo-Verlag ed.

Granger C. & Newbold P. (1974). Spurious regressions in econometrics. *Journal of econometrics*, 2(2), pp.111-120.

Griffin, John M. and Shams, Amin, (2018) "Is Bitcoin Really Un-Tethered?", <http://dx.doi.org/10.2139/ssrn.3195066>

Heller D., (2017), "Do Digital Currencies Pose a Threat to Sovereign Currencies and Central Banks?", Policy Brief, Peterson Institute for International Economics, April

Johansen, S. (1988). Statistical analysis of cointegration vectors. *Journal of economic dynamics and control*, 12(2), pp.231-254.

Johansen S. (1991). Estimation and Hypothesis Testing of Cointegration Vectors in Gaussian Vector Autoregressive Models. *Econometrica: Journal of the Econometric Society*, pp.1551-1580.

Johansen S. (1995). Likelihood based inference in cointegrated vector autoregressive models. OUP catalogue.

MacKinnon, J. G., Haug, A. A., & Michelis, L. (1998). Numerical distribution functions of likelihood ratio tests for cointegration (No. 9803). Department of Economics, University of Canterbury.

Sanches D., (2016) On the inherent instability of private money, *Review of Economic Dynamics*, Vol 20, April 2016, Pages 198-214

Selmi, R., Tiwari and Hammodeh (2018) "Efficiency or speculation? A dynamic analysis of the Bitcoin market", *Economics Bulletin*, Vol.38 No. 4 pp. 2037-2046

Smith, Adam. 1981 [1776]. *An Inquiry into the Nature and Causes of the Wealth of Nations*. The Glasgow Edition of the Works and Correspondence of Adam Smith. Edited by R.H. Campbell and A.S. Skinner. Textual Editor W.B. Todd. Oxford: Clarendon Press. Reprinted, Indianapolis: Liberty Classics.

White L.H., (1984) *Free banking in Britain, Theory, experience and debate, 1800-1845*, Cambridge University Press, Cambridge.