Dipartimento di Economia e Finanza

Cattedra: Macroeconomic Analysis

A DECENTRALIZED MONETARY POLICY: AN ANALYSIS OF BITCOIN IN A CASH-IN-ADVANCE MODEL

RELATORE

Prof. Reichlin Pietro

CANDIDATO

Ianiro Annalaura

CORRELATORE

Prof. Nisticò Salvatore

ANNO ACCADEMICO 2013/2014

A Decentralized Monetary Policy: an Analysis of Bitcoin in a Cash-In-Advance Model

Summary

In the last year and a half, Bitcoin, and crypto-currencies more in general, have invaded the scenes of financial markets, soon becoming one of the most discussed and controversial issue society is dealing with. Bitcoin, the crypto-currency created by the mysterious Satoshi Nakamoto in 2009, has given birth to an innovative phenomenon, still rich of unexplored potential. These decentralized currencies may represent the alternative, the answer to the numerous unresolved problems brought about by the last financial crisis. It is too early to confirm whether or not this is true: crypto-currencies are still in their infancy, and, apart from Bitcoin, only few of them are worth of attention. The information on them is dispersive and often confusing, constituting a serious limit to their understanding and diffusion among the general public, which often react with diffidence and doubts to the many issues raised by crypto-currencies. For this reason, this work aims, to the extent of its author's limited capacities, to shed some light on the subject, in particular on Bitcoin, trying to explain its functioning and implications, especially under a monetary policy perspective. Before doing so, it is necessary to define money. This has always been a difficult task for economists, who, therefore, instead of defining money for what it is, looked at its essential function: money is a medium of exchange, a unit of account and a store of value. This functional definition makes it clear why in the course of history money has taken various forms: from cattle, the first exchange medium after pure barter, to shells, to the first examples of metal coins. Precious metal coins, which have also an intrinsic value, ruled for many centuries, until the first banknotes were issued. In the beginning, these banknotes were not linked to the value of some commodity, leading in many cases to an abuse in their emission and usage. In 1816 however, England began using gold as a back-up commodity for paper money. This marked the beginning of the so called Gold Standard. Despite the two World Wars and the Great Depression having shown the weaknesses of such system, the Gold Standard continued to live on. The Bretton Woods International Monetary Agreement kept it, even though without direct convertibility for all currencies: only dollars could be exchanged for real gold. This situation became soon unsustainable and thus it was abandoned. With the end of the convertibility of banknotes into gold or other commodities, it has begun the epoch of *fiat* money. *Fiat* money has no intrinsic value, but its worth is guaranteed by the government or the central bank, which issues it: it is the law that guarantees and allows its usage. The introduction of the Internet and the

World Wide Web, though, and its incredible diffusion, has changed the rules and expanded the landscape of money varieties. In particular, virtual currencies have emerged. They are basically private money, but with a digital nature: they have no physical entity, they are born, stored and used on computers and other electronically devices (smartphones, tablets, etc.), therefore they can be expected to gain always more importance as more advanced technologies are constantly developed. For some years the only type of virtual money has been the one used in side MMORPGs. These are web browser-based games in which many players interact with each other online. This type of games involves the creation of a virtual world, usually a fantasy or sci-fi one, in which every player build her own avatar and takes part into a story. Then, other web realities, like Facebook and Amazon, issued their own digital currencies, which could be used to purchase online content. In the last years, however, a new type of virtual currencies has emerged, the crypto-currencies. Crypto-currencies are virtual currencies that exploit cryptography to function. Crypto-currencies protocols heavily rely on cryptographic techniques throughout all the stages of the transaction. They can be used to purchase anything, as long as the parties involved in the transaction accept that particular crypto-currency. The first crypto-currency ever created is Bitcoin. In the intention of its creator, Satoshi Nakamoto, Bitcoin should be a mathematical answer to the need of performing anonymous, safe, immediate online payments (Nakamoto 2008). Even if in a still contained way, the phenomenon of virtual currencies, their interactions with real economies and implications, are being studied by academics, mainly under a microeconomic point of view. The macroeconomic analysis, instead, is just at the beginning, with some studies posing questions about the role of traditional money and central banks, now that virtual currencies, and crypto-currencies in particular, are on the scenes. The relevance of digital currencies for the monetary system is starting to be acknowledged even by central banks. In 2012, the ECB published a review on what they call virtual currency schemes, bringing up, as examples, the Bitcoin case and the Linden Dollars case. They try to set a rigorous approach to study this phenomenon, highlighting the risks that virtual currency schemes (how a particular virtual currency interacts within the community which it belongs to and, eventually, the real world, thanks to its specific retail payment system) could pose to the monetary system in terms of price stability, financial stability, payments system stability, lack of regulation, reputation (ECB 2012). Before looking at Bitcoin as a virtual currency scheme, its characteristics and functioning mechanism should be explained. Bitcoin is an electronic payment system, allowing transaction between two individuals directly. In fact, the Bitcoin system is decentralized, meaning that there is no central bank or authority, which controls it and guarantees its stability. All the transactions, instead, are based on a peer-to-peer network, whose integrity is kept by the nodes belonging to it. Bitcoin is defined as a crypto-currency, since cryptography is heavily used to enable every transaction. When we talk about Bitcoin transactions, we cannot consider them as traditional coin transactions: they represent entries in a global digital ledger. Therefore, suppose a party wants to transfer some Bitcoin to another, it has to specify the amount of coins involved in the transaction and apply a digital signature to the operation, so that her digital identity is tied to the transaction. It is important to highlight that identities in the Bitcoin network are not real, physical identities; they are numbers that act as a pseudonym for the real person behind the transaction, thus ensuring a high level of privacy. Once the transactions details are specified, they are broadcasted to the entire system. It is this public disclosure to all the nodes that guarantees the goodness of the operation to the recipient party. However, the latter still faces a problem: how can it be sure that the received Bitcoin have not already been spent? This phenomenon, known as double spending, is, in fact, one of the main problems afflicting electronic transactions. The main novelty of the Bitcoin system lies exactly in the way it deals with double spending. There are some nodes in the network, known as miners, whose task is essential to the survival and maintenance of the network itself: they collect all the transactions occurred within a certain time period in what is called a transaction block. In doing so, they give a sort of authenticity certificate to every transactions, allowing all the nodes to acknowledge each block as valid. This proof of work mechanism is the heart of the decentralized nature of the Bitcoin system and it is what controls the money supply, since miners are rewarded with brand new Bitcoin for each block they create, plus some optional fee users may decide to pay them with as a further incentive to their activity. Finally, money supply is limited: in 2140 the total amount of Bitcoin is reaching 21 million, with no further emissions. Far from being the perfect currency, Bitcoin indeed shows some concrete limitations, raising concerns both among its users and its critics. The major worries are the ones about protocol security, mainly involving forgery, and the possibility of thefts, both at a network and hardware level, and the ones about ethical and ideological issues about

Bitcoin usage, which should not be underestimated since one of the most important drivers leading to Bitcoin success is the ideology behind it.
The actual incentive compatibility of the mining system is one of the major concerns, but there are strong arguments to support it. The MtGox's case, instead, is exemplary to discuss security issues. MtGox was one of the major Bitcoin exchange platforms, counting thousands of users. In February 2014, it declared bankruptcy because of a bug, which led to a massive theft of Bitcoin from its accounts. However, MtGox's failure must not be considered as a failure of the Bitcoin protocol itself. The bug in question, the transaction malleability bug, has been known since 2011, and can be rendered harmless with software, which accurately reports balances and transactions. Indeed, other Bitcoin exchanges can perfectly manage it. Another case rising concerns about this crypto-currency is Silk Road's case. Silk Road was an online market for illegal products, especially drugs. It was indeed defined as the "E-bay for drugs". It resorted to Bitcoin as its only mean of payment, because of the anonymity of transactions and for years authorities had no idea how to close it. On October 2, 2013 the FBI managed to shut down the illegal website and arrest Ulbrich, Silk Road's founder, in a joint operation with the IRS Criminal Investigation Division, the ICE Homeland Security Investigation, and the Drug Enforcement Administration. However, on November 6, 2013 a new website, Silk Road 2.0 opened for business, aiming to be a direct successor to the previous project. As of today, this site is still operating. Silk Road, unfortunately, isn't the only example of this kind of illegal online markets, which can stay on business thanks to Bitcoin or other crypto-currencies. It seems like this trend is only going to increase, if governments and authorities do not take the right precautions and countermeasures. However, banning Bitcoin or virtual currencies more in general is not the right step in that direction. Instead, a reasonable starting point is trying to better understand the implications and potentialities behind digital currencies, and to conceive a way to integrate them in our realities, for example setting clear rules about taxation and other legal issues concerning them. At this point, after discussing the major characteristic and implications, Bitcoin can be analysed in the framework of virtual currency schemes. In particular, its effect on price stability, financial stability, payment system stability can be assessed. As of today, Bitcoin is not a threat to price stability. The size of the phenomenon is still contained; however its relevance is growing day by day, therefore the impact of Bitcoin on these aspects discussed above can change completely in the

future. For this reason, monetary authorities needs to be ready to deal with such an occurrence, monitoring the development of the crypto-currency, in order to continue to absolve their tasks to the best of their abilities. The same conclusion can be drawn for financial stability. However, Bitcoin weight in financial markets is growing and there are aspects of the crypto-currency, which could indeed become a menace, if they are not dealt in the proper way. For example, there is still no credit system related to Bitcoin, but if loans and debts in Bitcoin start to surface, then the interconnection of the crypto-currency with the financial system will become more complex and risky, especially as far as stability is concerned. Lastly, Bitcoin is still an unstable payment system, in which users bear themselves all the risks related to the transactions. If the number of people resorting to Bitcoin for retail transactions were to increase, then central banks should adopt some measures to protect the traditional payment system from the instability brought forth by the virtual one. As of today, Bitcoin, as a payment system, cannot be considered an actual threat, but this doesn't imply that it could become so in the near future. The main problem of Bitcoin as a virtual currency scheme, therefore as a new player in the monetary and financial scene, is its lack of regulation. Governments and authorities are having many problems when dealing with Bitcoin mainly because they don't know how to define it and its relationship with real currencies. Still, time is stringent: Bitcoin, and crypto-currencies more in general, have become a widespread reality, which cannot be ignored any longer. Governments and authorities need to lay out some clear guidelines to allow a more aware and responsible usage of virtual currencies. The main aim of this work, though, is that to try to introduce Bitcoin inside a neo-classical economy framework, a Ramsey Plan with money, specifically the cash-in-advance model. The CIA model and its results are well known to economics-literate readers, who are also aware of the difficulties of introducing money in a Ramsey Plan economy. Bitcoin is a currency completely different from traditional ones. Apart from its digital nature, which may be the first aspect making the difference, there are several characteristics that set Bitcoin apart from traditional money. In particular, Bitcoin is decentralised, without a central authority controlling it. Its growth rate is scheduled by an algorithm, setting a roof for its total supply. Simply these observations make it clear how complicated an attempt at modelling Bitcoin can be, especially inside a traditional neo-classical framework. Nevertheless, this effort could be a starting point for future analysis, in the event Bitcoin or crypto-currencies more in general shall increase their weight in our economy.

The following model is a variation of the classic Cash-in-advance model. Basically, there is the addition of Bitcoin balances, including the miners' reward and the active fee to the budget constraint; the cash-in-advance constraint holds for Bitcoin too, with a peculiarity: Bitcoin are multiplied by a liquidity incentive, dependant on the active fee, which further specifies Bitcoin holdings' purchasing power and their degree of substitution with traditional money; finally there is the addition of an effort disutility to the lifetime utility function, to represent the cost of mining activity. Furthermore, this effort can be also seen as the probability the agent has to solve the proof of work challenge. The equilibrium conditions are derived and analysed both in the short-term, and in the long-term (steady state). From the model it emerges that: consumption is influenced not by traditional money, but by Bitcoin, as long as their emission is not over; real traditional money balances depends on the amount of Bitcoin in existence; in the steady state, traditional money inflation and Bitcoin inflation are both equal to zero.

The basic assumptions of the classic CIA model still hold:

- Closed economy with a single physical good;
- The good is produced through a classical constant-return-of-scale production function, using capital and labour;
- There is a continuum of infinitely lived individuals of size 1;
- Firms are financed by loans only;
- The government increases the quantity of money at a fixed rate each period: $M_{t+1} = (1 + \zeta)M_t$, with $\zeta > 0$;
- The increase in money supply is given to individuals through a subsidy, like a helicopter drop: $S_t = M_{t+1} - M_t$;
- There is perfect competition and rational expectations.

To these we add some other assumptions to introduce Bitcoin:

- Time is still discrete, but each interval corresponds to the average time of adding a new block to the chain of Bitcoin transaction.
- There are three assets in the economy, one period loans, A, and money, m, and Bitcoin, B. Money and Bitcoin pay no interest and they are used for transaction; loans pay the nominal interest rate i.

- There is no credit market for Bitcoin, therefore loans can be only granted in money: if an agent wants to invest her Bitcoin, she needs to exchange them with traditional currency.
- Every individual is a miner and belongs to a pool. The number of pools is enough to prevent the formation of a dominant pool and to enable everyone to have a fair chance at getting a reward: if a member of a pool solves the proof of work algorithm, everyone belonging to that pool wins a reward proportional to their effort. Therefore, for each agent the cost of mining equipment can be negligible. Each period she tries to add a new block to the chain, spending a certain effort, α_t. This effort is a cost for the agent, therefore is source of dis-utility; however, the greater the effort, the greater the contribution to the pool winning the challenge, thus implying a greater slice of reward.
- The miner's reward is equal to the amount of newly emitted Bitcoin: $X_t = B_{t+1}^S - B_t^S$ (where B_t^S is Bitcoin supply at time t); and a passive fee, f_t^p, which is the sum of all the active fees paid to the miners in each time interval. X_t is decreasing in time, and once $t = T$, Bitcoin supply will reach its maximum and $X_t = 0$. From that point onward, miners will be rewarded only through users' fee.
- Each agent may choose to pay an active fee, f_t^a, to reward the miners for their effort and encourage them to confirm her transaction faster. However, once no more new Bitcoin will be issued, fees will become mandatory, as they will be the only reward for miners' activity.

Having set the assumption, the agent in this economy will have to maximize her utility:

$$\sum_{t=0}^{\infty} \beta^t [u(c_t) - \varphi(\alpha_t)]$$

Where:

- $0 < \beta < 1$
- $0 < \alpha_t < 1$
- $u(c_t)$ and $\varphi(\alpha_t)$ are such that:

$$u'(c_t) > 0 \, ; \, \varphi'(\alpha_t) > 0$$

$$u''(c_t) < 0 \, ; \, \varphi''(\alpha_t) < 0$$

$$\lim_{c_t \to 0} u'(c_t) = \infty \; ; \; \lim_{\alpha_t \to 0} \varphi'(\alpha_t) = \infty$$

$$\lim_{c_t \to \infty} u'(c_t) = 0 \; ; \; \lim_{\alpha_t \to 1} \varphi'(\alpha_t) = 0$$

As in the previous case there are two constraints to the maximization problem.

Budget constraint:

$$m_{t+1} + A_{t+1} + q_t B_{t+1} + p_t c_t + q_t f_t^a$$
$$= A_t(1 + i_t) + m_t + q_t B_t + S_t + q_t \alpha_t \left(X_t + f_t^p\right) + p_t w_t$$

This is the nominal budget constraint with Bitcoin, where:

- m_t is the demand of nominal balances of each individual at time t;
- A_t is the loan to the firms at time t;
- $p_t w_t$ is the nominal per-capita wage at time t;
- p_t is the price level at time t;
- $p_t c_t$ is consumption in money terms at time t.
- $q_t = \frac{p_t}{p_t^B}$ is the money price of Bitcoin, the exchange rate between traditional money and Bitcoin at time t.
- p_t^B is the price level in Bitcoin at time t.
- $\alpha_t\left(X_t + f_t^p\right)$ is the miner reward at time t, proportional to the effort spent.

CIA constraint:

$$M_t + q_t B_t \psi(f_t^a) \geq p_t c_t$$

Being a cash-in-advance model, the good market operates before the credit market. For this reason, the agent needs to hold in advance enough money and Bitcoin to purchase the consumption good.

$\psi(f_t^a)$ is a liquidity incentive, in order to encourage the payment of the active fee. It is such that $\psi(f_t^a) = \begin{cases} 1 \; for \; f_t^a = \frac{f^p}{\alpha} \\ \in (1, 1+\theta) for \; f_t^a > \frac{f^p}{\alpha} \\ \in [\varepsilon, 1) for \; 0 \leq f_t^a < \frac{f^p}{\alpha} \end{cases}$

$\frac{f^p}{\alpha}$ is the long-term equilibrium fee[1]; ε is a positive lower bound, θ is a number very close to zero. This liquidity incentive "punish" those users, who pay an active fee lower than its equilibrium value, by reducing the value of their Bitcoin holdings. The closer the fee is to its equilibrium value, the more encouraged miner will be to validate sooner that transaction, thus giving it more purchasing power than to a

[1] It is obtained by the budget constraint.

transaction with a lower fee. The active fee may be higher than its equilibrium value, as well, but the marginal increase in the liquidity incentive would be irrelevant. Indeed:

$$\lim_{f_t^a \to \infty} \psi(f_t^a) = 1 + \theta$$

Which is slighter greater than 1. Later on, we will explain better the role and the implications of this incentive.

Lastly, we add the NPG condition, as before:

$$\lim_{t \to \infty} \frac{A_t}{\prod_{t=0}^{\infty}(1 + i_t)} = 0$$

Instead of setting up the usual Lagrangian framework to solve the maximization problem, we can simply insert the budget constraint into the utility function (the consumption one), and taking into account the CIA constraint, we can analyse what happens to consumption utility when $M_{t+1}, B_{t+1}, A_{t+1}, \alpha_t, f_t^a$ change.

We obtain the following equations:

1) $M_{t+1}: \frac{u'(c_t)}{\beta u'(c_{t+1})} = \frac{p_t}{p_{t+1}} + \frac{\lambda_{t+1} p_t}{\beta u'(c_{t+1})}$
2) $B_{t+1}: \frac{u'(c_t)}{\beta u'(c_{t+1})} = \frac{q_{t+1}}{q_t}\left(\frac{p_t}{p_{t+1}} + \frac{\lambda_{t+1} p_t \psi(f_{t+1}^a)}{\beta u'(c_{t+1})}\right)$
3) $A_{t+1}: \frac{u'(c_t)}{\beta u'(c_{t+1})} = \frac{p_t}{p_{t+1}}(1 + i_{t+1})$
4) $\alpha_t: \varphi'(\alpha_t) = u'(c_t)\left(X_t + f_t^p\right)\frac{q_t}{p_t}$
5) $f_t^a: \psi'(f_t^a) = \frac{u'(c_t)}{p_t \lambda_t B_t}$

First of all, from equations 1) and 3), given that the nominal interest rate must be positive, λ_t must be positive too. Therefore the CIA constraint is binding.

Then, combining 1) and 2) together we obtain:

$$\frac{p_t}{p_{t+1}} + \frac{\lambda_{t+1} p_t}{\beta u'(c_{t+1})} = \frac{q_{t+1}}{q_t}\left(\frac{p_t}{p_{t+1}} + \frac{\lambda_{t+1} p_t \psi(f_{t+1}^a)}{\beta u'(c_{t+1})}\right)$$

Knowing that λ_{t+1} is positive, depending on whether the liquidity incentive is lower or equal to one, we can have three possible scenarios:

a) $0 < \psi(f_{t+1}^a) < 1$: it is a likely scenario, at least until Bitcoin supply is not over, since the fee payment is optional. Given this, we have:

$$\frac{\lambda_{t+1} p_t}{\beta u'(c_{t+1})} > \frac{\lambda_{t+1} p_t \psi(f_{t+1}^a)}{\beta u'(c_{t+1})} \Rightarrow \frac{\frac{\lambda_{t+1} p_t}{\beta u'(c_{t+1})}}{\frac{\lambda_{t+1} p_t \psi(f_{t+1}^a)}{\beta u'(c_{t+1})}} > 1$$

Therefore

$$\frac{q_{t+1}}{q_t} > 1 \Rightarrow q_{t+1} > q_t$$

Given that $q_t = \frac{p_t}{p_t^B}$, we have:

$$\frac{p_{t+1}}{p_{t+1}^B} > \frac{p_t}{p_t^B} \Rightarrow \pi_{t+1} > \pi_{t+1}^B$$

This result states that in presence of the liquidity incentive, which in this circumstance is smaller than 1, Bitcoin have less purchasing power than they could (in the CIA constraint Bitcoin holdings are lowered in value by the incentive), thus they are weaker than traditional money. For this reason, in order to avoid a crowding out of Bitcoin in favour of traditional currency, money inflation needs to be higher than Bitcoin inflation. The more the active fee is closer to its equilibrium value, the lower the gap between the two inflations needs to be. Therefore, we could look at the active fee also as the price Bitcoin users are willing to pay to promote Bitcoin and to make it an alternative to traditional money. Basically, the more they believe in Bitcoin potential as a currency, the higher active fee they will pay, since they want miner to keep playing their role as best as they can, guaranteeing the whole system functioning.

b) $\psi(f_{t+1}^a) = 1$: this is the long-term scenario, in which the active fee is equal to its equilibrium value. Thus we have:

$$\frac{q_{t+1}}{q_t} = 1 \Rightarrow q_{t+1} = q_t$$

$$\frac{p_{t+1}}{p_{t+1}^B} = \frac{p_t}{p_t^B} \Rightarrow \pi_{t+1} = \pi_{t+1}^B$$

Bitcoin and traditional money are substitutes, therefore any slight change in the inflations equivalence would imply a shift to the most valuable currency. In the steady state, since the active fee is going to be equal to its equilibrium value, $f^a = \frac{f^p}{\alpha}$, then Bitcoin inflation and money inflation will be equal. This means that monetary policy, in particular money emission, needs to take into account Bitcoin supply, as it will be shown later.

c) $\psi(f_{t+1}^a) > 1$: in this case, the active fee is higher than its equilibrium value. This implies:

$$\frac{q_{t+1}}{q_t} < 1 \Rightarrow q_{t+1} < q_t$$

$$\frac{p_{t+1}}{p_{t+1}^B} < \frac{p_t}{p_t^B} \Rightarrow \pi_{t+1} < \pi_{t+1}^B$$

The liquidity incentive makes Bitcoin more appealing than traditional money, therefore Bitcoin inflation needs to be higher than money inflation. However, Bitcoin users will not be willing to pay a fee higher than the equilibrium one. In fact, they face a trade-off between the liquidity incentive and the Bitcoin inflation. The higher the incentive, the higher is the inflation (thus Bitcoin looses purchasing power compared to traditional money). If, as we said before, one of the aims of the active fee is that of supporting the Bitcoin system and Bitcoin role as an alternative currency, once the fee is higher than the equilibrium fee, the liquidity advantage is compensated by the loss of competitiveness with real money in terms of inflation gap. The equilibrium fee, $\frac{f^p}{\alpha}$, is the fee that maximizes the marginal liquidity incentive, $\psi'(f_t^a)$; it is a saddle point for $\psi(f_t^a)$. More specifically:

$$\psi''(f_t^a) = \begin{cases} \geq 0 \; for \; f_t^a \in \left[0, \frac{f^p}{\alpha}\right] \\ < 0 \; for \; f_t^a > \frac{f^p}{\alpha} \end{cases}$$

From equations 2) and 3) we obtain:

$$1 + i_{t+1} = \frac{q_{t+1}}{q_t}\left(1 + \frac{\lambda_{t+1} p_{t+1} \psi(f_{t+1}^a)}{\beta u'(c_{t+1})}\right)$$

From 5):

$$\lambda_{t+1} = \frac{u'(c_{t+1})}{p_{t+1} B_{t+1} \psi'(f_{t+1}^a)}$$

Substituting this latter equation into the previous one, we have:

$$1 + i_{t+1} = \frac{1+\pi_{t+1}}{1+\pi_{t+1}^B}\left(1 + \frac{\psi(f_{t+1}^a)}{\beta B_{t+1} \psi'(f_{t+1}^a)}\right) \qquad (1)$$

As predictable, the nominal interest rate depends positively from the rate of inflation of traditional money: the higher the inflation, the higher the nominal interest rate. However, it depends negatively from the inflation rate of Bitcoin. Indeed, the nominal interest rate refers to loans in traditional money. Therefore, one should first exchange Bitcoin for traditional money and then lend that money to the firms, at the rate i_t. In doing so, there is a trade-off between Bitcoin purchasing power and the rate paid by the loans. When Bitcoin inflation rises, Bitcoin looses purchasing power, therefore, *ceteris paribus*, the nominal interest rate goes down; otherwise everyone would exchange Bitcoin for loans. A similar reasoning can be applied to the relationship between the nominal interest rate and the active fee, which determines the liquidity incentive, $\psi(f_{t+1}^{a})$. If the latter increase, the nominal interest rate needs to increase as well, to keep loans competitive. However, looking at the marginal liquidity incentive, the effect depends on whether the increase is under the equilibrium value or above it. In the first case, the increase in the fee determines an increase in the marginal liquidity incentive. Bitcoin haven't reached their full potential yet, thus the nominal interest rate can be lower. However, the effect of $\frac{\psi(f_{t+1}^{a})}{\psi'(f_{t+1}^{a})}$ on i_{t+1}will depend on which variation is stronger. In the case of an increase of the active fee increasing above the equilibrium fee, than $\psi'(f_{t+1}^{a})$ goes down. Indeed, when the fee is higher than its equilibrium level, it means that Bitcoin have surpassed money as a currency, thus the interest rate offered needs to rise, for loans to be competitive. As a consequence, the total impact of $\frac{\psi(f_{t+1}^{a})}{\psi'(f_{t+1}^{a})}$ on the nominal interest rate is positive. Lastly, the effect of Bitcoin holdings is a negative one: when they increase, the agent has more resources to invest; therefore the nominal interest rate can be lower.

From equations 3) and 4), we have:

$$\frac{\varphi'(\alpha_t)}{\varphi'(\alpha_{t+1})} = \beta\frac{(1+r_{t+1})}{(1+\gamma_{t+1})}(1+\pi_t^B) \quad (2)$$

Where $(1+\gamma_{t+1}) = \frac{(X_{t+1}+f_{t+1}^{p})}{(X_t+f_t^{p})}$ is the gross rate of growth of miners' reward.

This equation defines a sort of Euler Equation for the effort, α_t. We can see that the marginal rate of substitution for the effort, depends negatively on the rate of growth of the miner reward, meaning that if tomorrow the reward is going to be smaller (a reasonable assumption for Bitcoin, since their growth rate is decreasing), it pays off more spending a greater effort today to obtain the present reward, which is higher. On the other hand, the marginal rate of substitution is positively correlated to the real interest rate (the higher is the rate, which I can lend Bitcoin at, the higher is the marginal utility of the effort today, since I can invest the obtained reward) and to the inflation for Bitcoin prices (if Bitcoin are going to have less purchasing power tomorrow, I'd rather win a reward today).

Equation 3) gives us the classic Euler Equation:

$$\frac{u'(c_t)}{u'(c_{t+1})} = \beta(1+r_{t+1}) \quad (3)$$

From the supply side of the economy we have:

- $M_{t+1} = (1+\zeta)M_t$

- $B_{t+1}^S = (1 + \kappa_{t+1})B_t^S$
- $S_t = M_{t+1} - M_t$
- $X_t = B_{t+1}^S - B_t^S$

At the equilibrium:

- Money supply is equal to money demand: $M_t = m_t$;
- Bitcoin supply is equal to Bitcoin demand: $B_t^S = B_t$
- The lending market equilibrium is such that $A_t = p_{t-1}k_t$ (asset market clearing);
- Profit maximization: $f'(k_t) + (1 - \delta) = (1 + r_t)$ and $w_t = f(k_t) - k_t f'(k_t)$.
- Fees equilibrium: $f_t^a = \frac{f_t^p}{\alpha_t}$

Substituting these conditions inside the budget constraint and dividing by p_t, to obtain its real terms specification, we obtain:

$$c_t = f(k_t) + k_t - \delta k_t - k_{t+1} - (1 - \alpha_t)\frac{X_t}{p_t^B}$$

In this model with Bitcoin, consumption is not the same to the consumption of a Ramsey Model without money in it. The amount of Bitcoin emitted each period influences it. Each agent will consume the output minus the part of newly emitted Bitcoin, which she didn't get. Solving the proof-of-work challenge, the effort spent in mining increases the possibilities of consumption. Traditional money instead is still super-neutral. Indeed, in this economy money is given by the government for free, as a subsidy; on the contrary Bitcoin are "earned" and "issued" by the agents themselves. They are both used for transaction purposes, but, as far as Bitcoin are concerned, agents can choose if they want them or not, if they are valuable or not. This reflects in their consumption possibilities. The above result holds until Bitcoin supply is over, at which point the consumption goes back to its Ramsey Plan without money counterpart:

$$c_t = f(k_t) + k_t - \delta k_t - k_{t+1}$$

At this point, it is interesting seeing what happens to the traditional money balances demand function, expressed in real terms. From the CIA constraint we have:

$$\frac{M_t}{p_t} = c_t - \frac{B_t}{p_t^B}\psi(f_t^a)$$

Money balances have now found competition in Bitcoin. The more Bitcoin demand is, the lower is traditional money demand. Moreover, the liquidity incentive determines the rate of substitution between the two currencies. For $f_t^a = \frac{f^p}{\alpha}$, $\psi(f_t^a) = 1$, there is perfect substitution.

To conclude this brief analysis, we shall now look at the steady state of this economy.

From (3), we obtain:

$$r^* = \frac{1-\beta}{\beta}$$

This is the real interest rate of a Ramsey Plan without money.

From (2)

$$1 = \frac{(1+\pi_t^B)}{(1+\gamma_{t+1})} \Rightarrow \pi_t^B = \gamma_{t+1}$$

Since at the steady state $X_t = 0$ and $f_t^p = f_{t+1}^p$, $\gamma_{t+1} = 0$, therefore also $\pi^B = 0$. Once no more Bitcoin are introduced in the economy, Bitcoin inflation stops. This result comes out also from the steady state requirement of real balances being constant. In order to be so, the inflation rate, must be equal to the growth rate of the Bitcoin supply, which is zero. Moreover, given that at the steady state $f^a = \frac{f^p}{\alpha}$, from the previous result we have:

$$\pi = \pi^B = 0$$

Money inflation goes to zero as well, otherwise traditional money would be less competitive than Bitcoin. And since, for the same reason as above, real balances need to be constant, the inflation rate is equal to the growth rate, so:

$$\zeta = \pi = 0$$

Government need to stop issuing new money, for inflation to be equal to zero. This is a rather strong result: Bitcoin can stop money inflation. The crypto-currency has a strong impact on traditional money emission, and also demand. In fact:

$$\frac{M}{p} = c^* - \frac{B}{p^B}$$

Where $c^* = f(k^*) - \delta k^*$, which is the classic Ramsey Plan specification. In the long run consumption is influenced neither by money, nor by Bitcoin. Real money balances demand instead is not influenced by their own inflation, but by real Bitcoin holdings. From the model, it appears that the presence of Bitcoin in the economy can affect traditional money demand and therefore monetary policy. There can be competition between traditional currency and crypto-currency. This competition, if appropriately studied and understood, can actually bring benefits for the users: they are “in control” of Bitcoin and thus they have an instrument to react to monetary policy decisions. In particular, thanks to the liquidity incentive, they can show their support to the crypto-currency, their trust in it. Moreover, in the long-term inflation goes to zero, even the traditional money one. This occurs given the model assumption and specifications, but it can still imply a corrective effect on excessive inflationary monetary politics. Maybe it can have the beneficial effects of private money competition, advocated by Hayek. Ignoring the phenomenon can be a mistake, as well as reacting to it with rigidity. As it was said before, this is not the best model to fully capture the interactions between traditional currencies and crypto-currencies. A decentralized currency is not something easy to model, especially with traditional theories, inside a neo-classical framework, but nevertheless, I personally believe it is an effort worth some time. I also believe crypto-currencies interactions in real economies can become an interesting field of studying, opening the doors to new theories and solutions.