Hayek Money: the Cryptocurrency Price Stability Solution[1]

Abstract. Bitcoin has enabled competition between digital cryptocurrencies and traditional legal tender fiat currencies. Despite rapidly increasing acceptance, so far the affirmation of cryptocurrency as better money has been thwarted by dramatic deflationary price instability. Successful at disposing of any central monetary authority using the Bitcoin protocol, the bitcoin currency has accidentally thrown away the flexibility of a fully automatic algorithmic non-discretionary monetary policy allowing for elastic supply of money. Price stability can be achieved by dynamically rebasing the outstanding amount of money: the number of currency units in every digital wallet is adjusted instead of each single unit changing its value. The apparent awkwardness of this unfamiliar paradigm is discussed at length, proving that its only real novelty is about fairness and effectiveness. Furthermore, suggestions are provided about how to ease the effect of contractionary monetary policy. The proposed monetary base adjustment has neutral impact on the overall wallet wealth, as it does not introduce any arbitrary distortion into the intrinsic value dynamics of the wallet. The adjustment is based on a commodity price index determined with a resilient consensus process that does not rely on central third party authorities. It is posited in this paper that a digital cryptocurrency adopting elastic monetary standard is *Hayek Money*, so named from the Nobel Prize-winning economist: possibly the best money ever devised, a *good money standard* providing stable prices for a new economic era.

[1] Shortlisted as finalist for the Blockchain Awards at the Bitcoin Foundation Conference 2014, category Visionary Academic Paper, this work lost to the original Bitcoin breakthrough paper by Nakamoto (2008).
I am in debt to Stefano Cerutti, Eric Ehlers, and Sergey Shakhdinarov for fruitful discussions, sharp observations, and the proofreading of my tentative English prose. Kevin Dowd and Robert Sams: you made me feel less solitary in my line of thinking, thank you. My gratitude goes also to Andrea Bugin, Ignazio Cassan Magnago, Massimo Morini, and Leo Munter.

Introduction: A Short Summary.

The first section introduces money theory; the second section lines up excerpts from Friedrich Hayek's theory of concurrent private currencies, which is the main inspiration for this paper. A Bitcoin primer is provided in the third section. The outstanding currency amount rebasing process is illustrated in section four, where the concept of Hayek Money is defined. Its technical implementation on the block chain (i.e. the public ledger of transactions) is discussed in section five. Section six discusses at length the unfamiliar new paradigm of wallet balances being non constant. Section seven comprises comments, alternatives, and scenarios. Finally some conclusions are presented.

The expert reader can skip the sections he is knowledgeable about in order to alleviate the burden of this paper. He is warned though not to overestimate his confidence: the proposal of this work lies within the uncomfortable middle ground between money definition, cryptographic algorithms, game theory, and unfamiliar paradigm shifts. Not for the faint-hearted, but hopefully the patient reader will be rewarded with new interesting insights.

Section 1: About Money.

As human beings we are usually first exposed to the gift economy of our families and tight knit communities: goods and services are provided without an explicit agreement for immediate or future rewards, but the exchange of love, kindness, and confidence. As the relationship circle is enlarged this mutual trust weakens, but the urge and willingness to cooperate does not diminish: this is when the need for an exchange economy arises. Historically, the barter economy has been the first viable trade economy[3]: goods or services were immediately exchanged for other goods or services. Later on, the limited efficiency of the *coincidence of wants* required by the barter economy was surpassed by the use of *money* as *medium of exchange*, giving birth to the *trade economy*. Money has the special role of being half of every transaction: it has been elected to act as a pivot in the trade economy and because of its key role it has always enjoyed a peculiar attention. Money is a social relation instrument, an abstract invention, the most brilliant and powerful mechanism devised by the human species to increase cooperation: as such it rightly emanates a persistent allure[4].

What kinds of goods have been historically used as money? The goods better equipped, because of their properties, to fulfill three interdependent functions:

[3] David Graeber in "*Debt: The First 5,000 Years*" challenges the existence of a barter economy as a made-up narrative, humans having used credit systems long before the invention of coins or cash. Still he reinforces the role of money as unit of account: *Money was no more ever "invented" than music or mathematics or jewelry. What we call "money" isn't a "thing" at all, it's a way of comparing things mathematically, as proportions.*

[4] From this arises the often despised but ineradicable money hoarding attitude: the perverse paradox of considering money as a goal in itself, instead of as a means to obtain and enjoy other goods and services.

1. Medium of exchange: something that can be reliably swapped for something else. Its virtues should include fungibility, transportability, divisibility, recognisability, and resistance to counterfeiting;
2. Unit of account: other goods, services, and assets are priced in terms of money. Money is the unit of measurement of relative worth, so it should have stable value allowing for stable comparison of prices. In order to constrain money value its supply must be limited in some way, and controlled to match up demand;
3. Store of value: something that can be reliably saved, stored, and retrieved while retaining its usefulness over time. It should be non-perishable or with a low preservation cost. Often the store of value property is also presented as the ability to retain *constant* value over time, but this ability is instead related to being a good, i.e. stable, unit of account[5].

Many goods actively traded in the barter economy fall short of some requisite that would enable them to efficiently serve as money. Food and live cattle are perishable; diamonds lose value when divided into smaller parts, etc.

Money has always been essential for the economy, even if its nature has varied over time. Historically, gold has proven to be usable as money in practically every civilization because of its remarkable properties: resistance to corrosion and oxidation, high malleability, relative ease of purity assessment, and pleasant color. Gold has been the *commodity money* standard for thousands of years, and its supremacy has not required any kind of centrally planned endorsement. In that period the duty of the central authority was mainly the certification of gold purity: its stamp assured the coins had the proper weight and gold finesse from which their value originated. This responsibility has been often marred by *debasement*, the practice of lowering the intrinsic value of coins reducing the quantity of gold while maintaining the face value: central authorities hardly resisted the inclination to multiply money to sustain their expenditure.

The transportability of large amount of gold coins presented logistic and security problems; moreover, coins were often clipped and depreciated during use. In every society goldsmiths have worked gold obtaining splendid objects, and it was natural for them to develop private vaults: in the 17th century merchants started to use the goldsmiths of London as custodians of their gold, obtaining in return non-assignable receipts. Gradually these receipts evolved into transferable promissory notes payable on demand, a safe and convenient form of money backed by the goldsmith's promise to pay. The issuance of *representative money*, i.e. claims on commodity money granted by gold reserves, was the means by which pieces of paper of no intrinsic value were gradually accepted as money. It was then easy to realize that in the case of

[5] Even if the two concepts might partially overlap, it is of paramount relevance to understand that the value of money depends on supply and demand, which is unlikely to be stable over time. Please refer to subsection 5.3 for further discussion about this point.

representative money only a fraction of gold was really needed for redemption, as most representative money was generally used and exchanged without its gold claim being ever exercised. This marked the birth of *fractional receipt money*, in which the amount of issued representative money was greater than the gold reserve backing it. Issuers have since enjoyed a discretionary freedom, which can be abused lowering the ratio between gold reserve and money. Furthermore, representative and fractional money permits a huge increase of *seigniorage* revenues, seigniorage being the profit made by issuing money, especially the difference between its face value and its production cost.

Money is an intangible abstract concept, while *currency* is a tangible aspect of money when in actual use as a medium of exchange, especially in the form of circulating notes and coins. Money and currency are often used interchangeably because of their similar concepts, but economists do not, recognizing that currency is only one possible tangible instance of money[6].

Even in the case of equivalent *gold standard* monetary system, the increasing reliance on authority for redeeming representative money and the necessary trust about the authority not abusing its fractional basis privilege has led to the appearance of multiple currencies around the world, every one dependent on the local issuing authority. The geographical, cultural, and political proximity between issuer and currency users has always played a significant role. Geographical distance from the issuer obviously depreciated representative money by making its redemption more problematic; moreover, proximity ties were reinforced by the natural connection between a currency and its adoptive economy: the more healthy, vibrant, and rich the economy, the greater the number of transactions, with increased utility and value for the currency as consequence.

Different kinds of gold standard monetary systems have been used: all of them established on a unit of account based on a fixed quantity of gold. While gold standard was highly regarded, and often actively pursued[7], most governments have tried to progressively free their control of money from the constraints of a limited supply commodity such as gold. As a culmination of this process the United States ended the convertibility of the US dollar to gold in 1971. Nowadays we currently use *fiat money*[8], that is, money deriving its value only from government regulation or law. Law defines the money valid for meeting a financial obligation as having *legal tender*, in the attempt to seal the definitive bondage of money to the governing power.

It might be worthwhile to stress that money is a good in itself, despite its special role as the yardstick against which the value of every other good is measured. As such the

[6] In a digital world currency does not need not be physical objects, and possess its own degree of intangibility. In the case of crypto-currency the difference with money is even more blurred as the digital currency is so far basically the only instance of crypto-money: as a consequence distinction between money and currency are not really cared for in this paper.

[7] Among others: Lord Liverpool put the UK economy through a harsh deflation to restore the 1797 gold parity and US President William McKinley was accused of "*crucify*[ing] *mankind upon a cross of gold*".

[8] *Fiat* as in *fiat lux et lux fuit*, the creation action of calling money into being out of nothing.

value of money is governed by supply and demand. Everybody is familiar with the question of how many apples one can buy with a unit of currency; indeed the inverse question of how many units of currency one can buy with an apple is just as sound and legitimate. When the value of money changes, this fact becomes especially problematic because it is not just the value of one good that is changing, but the unit against which every other good is measured. The price system could be pictured as having all goods ordered in a sorted line according to their value, the currency unit being just one of those goods; as the values of all goods move according to supply and demand, the relative sorting is continually adjusted; when the value of money itself changes, not only the placement of money in the value line is affected, but also the scale of the line and the relative distance between all other goods.

Noise originating from changes in the value of money makes it harder to detect genuine fundamental changes in the relative prices of other goods. Blurred signals from the price system increase the resources wasted as protection against non-fundamental price changes. Price instability can also aggravate the distortionary effect of tax and social security systems, and historically it has often undermined social and political cohesion because of its unfair effects on the redistribution of wealth and income. Good money should provide stable prices to best perform its role as unit of account: this enables well-informed economic decisions by households and firms. Saving, borrowing, consumption, and investment are approached with the confidence that the value of one currency unit will be stable over time: efficient resource allocation facilitates high employment, economic growth, and overall financial stability.

The price system measures the value of goods relative to the value of money. An increase in the price level of goods and services signals a decrease in the value of money. Each unit of currency buys fewer goods and services: this reduction in the purchasing power per unit of money is called *inflation*. We have plenty of historical evidence that excessive inflation can discredit money to the point of nullifying its utility, e.g. Germany's 1923 hyperinflation depreciated the value of the paper Mark to one thousand billionth of the once equivalent gold Mark. Commodity money debasement and low reserve/money ratio for fractional money were all forms of inflation.

The opposite price reduction effect is called *deflation*: not as immediately and blatantly detrimental to money as inflation, deflation can nonetheless cause economic problems. Especially if coupled with slow growth or uncertain economic cycle, deflation encourages money hoarding as consumers and firms postpone expenditures and investments while waiting for prices to decrease even further. As non-essential spending falls, revenues fall and growth stalls. Whatever the economic scenario, since money increases its value compared to other goods, debts increase their real value relative to cheaper goods and services leading to the injustice of debtors having to repay their debts in more valuable currency. In a troubled economy this injustice

leads to increasing numbers of defaults, and losses from unpaid loans trigger further bankruptcies. As a consequence economic activity sinks leading to a deflationary spiral recession and perverse economic crisis. If (high) inflation is money's heart attack, (persistent) deflation is money's cancer.

Since the demand for money cannot be controlled, the only way to ensure price stability is to manage its supply. The regulation of the supply of money is the *monetary policy* core. A policy reducing the size of the money supply is referred to as contractionary or tightening policy and it is used as countermeasure for inflationary increasing prices. Conversely, an expansionary policy increases the size of the money supply devaluating the value of money and counteracting deflationary decreasing prices.

Monetary policy is usually delegated to central banks or equivalent monetary authorities. Considering that governments could regulate the money supply to favor their short-term interests against the common welfare provided by price stability, at least in most developed democratic nations these authorities are institutionally designed to be independent in order to limit possible money supply abuse. For an introduction to modern monetary policy the reader is referred to McLeay, et al. (2014). Here it will be enough to point out that most money in the modern economy is not available in the form of coins and notes, but as deposits and loans created by commercial banks; the privilege of creating deposits and loans is regulated by central banks. Central banks' intrinsic objective is to safeguard the value of their currency: as such, most of them implicitly or explicitly commit to keep inflation under control at a low and stable (non-zero) rate.

The understanding of the nature of money cannot help reveal as strikingly disturbing that money, the most special of all goods available in the trade economy, is a monopoly of governments and central banks. The common acquiescent acceptance of this state of things, even in relatively free market economies, is probably the single most surreal blindness of many economic theories.

Section 2: An Analysis of the Theory and Practice of Concurrent Currencies.

In "Denationalisation of Money" the Nobel Prize-winning economist Friedrich Hayek (1977) performs a deep analysis of the theory and practice of concurrent currencies. In the following paragraphs I choose to let him speak for himself as homage to his genius and as the next best alternative to the impossible wish of having him co-author this paper; only bold emphasis is mine. The reader should consider the following arbitrary raw summary as an encouragement to read the entire book.

It is an extraordinary truth that competing currencies have until quite recently never been seriously examined. ***There is no answer in the available literature to the question why a government monopoly of the provision of money is universally***

***regarded as indispensable**, […] nor can we find an answer to the question of what would happen if that monopoly were abolished and the provision of money were thrown open to the competition of private concerns supplying different currencies.*

*[Government monopoly] has the defects of all monopolies: one must use their product even if it is unsatisfactory, and, above all, it prevents the discovery of better methods of satisfying a need for which a monopolist has no incentive. […] **The opportunity to use a reliable money** that will not periodically upset the smooth flow of the economy **[is] an opportunity of which the public has been deprived by the government monopoly** […]*

The government monopoly of the issue of money was bad enough so long as metallic money predominated. But it became an unrelieved calamity since paper money (or other token money), which can provide the best and the worst money, came under political control. A money deliberately controlled in supply by an agency whose self-interest forced it to satisfy the wishes of the users might be the best. […]

*Though historical experience would at first seem to justify the belief that only gold can provide a stable currency, and that all paper money is bound to depreciate sooner or later, all our insight into the processes determining the value of money tells us that this prejudice, though understandable, is unfounded. **The political impossibility that governments will achieve it does not mean there is reason to doubt that it is technically possible to control the quantity of any kind of token money so that its value will behave in a desired manner**, and that it will for this reason retain its acceptability and its value. It would therefore now be possible, if it were permitted, to have a variety of essentially different monies. They could represent not merely different quantities of the same metal, but also different abstract units fluctuating in their value relatively to one another. In the same way, we could have currencies circulating concurrently throughout many countries and offering the people a choice. This possibility appears, until recently, never to have been contemplated seriously […]*

From Roman times to the 17th century, when paper money in various forms begins to be significant, the history of coinage is an almost uninterrupted story of debasements or the continuous reduction of the metallic content of the coins and a corresponding increase in all commodity prices […]

*I do not think it an exaggeration to say that **history is largely a history of inflation, and usually of inflations engineered by governments and for the gain of governments** […]*

Ever since the British Government in 1694 sold the Bank of England a limited monopoly of the issue of bank notes, the chief concern of governments has been not to let slip from their hands the power over money, formerly based on the prerogative of coinage, to really independent banks. For a time the ascendancy of the gold standard and the consequent belief that to maintain it was an important matter of prestige, and to be

driven off it a national disgrace, put an effective restraint on this power. […] But as soon as it was widely understood some 50 years ago that the convertibility into gold was merely a method of controlling the amount of a currency, which was the real factor determining its value, governments became only too anxious to escape that discipline, and money became more than ever before the plaything of politics.

Moreover, though there is every reason to mistrust government if not tied to the gold standard or the like, there is no reason to doubt that private enterprise, whose business depended on succeeding in the attempt, could keep stable the value of a money it issued.

Hayek then goes on to propose a scheme in which banks issue competing private currencies: *the purpose of this scheme is to impose upon existing monetary and financial agencies a very much needed discipline by making it impossible for any of them, or for any length of time, to issue a kind of money substantially less reliable and useful than the money of any other. As soon as the public became familiar with the new possibilities, any deviations from the straight path of providing an honest money would at once lead to the rapid displacement of the offending currency by others. […] The scheme would, to all intents and purposes, amount to a displacement of the national circulations only if the national monetary authorities misbehaved. Even then they could still ward off a complete displacement of the national currency by rapidly changing their ways. […] I do not think the scheme would prevent governments from doing anything they ought to do in the interest of a well-functioning economy […]*

I would announce the issue [of a currency] *unit with a distinct registered trade name* ***such as ducat [announcing at the same time the] intention to regulate the quantity*** *of the ducats* ***so as to keep their (precisely defined) purchasing power as nearly as possible constant****. I would also explain to the public that I was fully aware I could hope to keep these ducats in circulation only if I fulfilled the expectation that their real value would be kept approximately constant. And* ***I would*** *announce that I proposed from time to time to* ***state the precise commodity equivalent in terms of which I intended to keep the value of the ducat constant, but*** *that* ***I reserved the right****, after announcement,* ***to alter the composition of the commodity standard as experience and the revealed preferences of the public suggested****.*

It might be expedient that the issuing institution should from the outset announce precisely the collection of commodities in terms of which it would aim to keep the value of the 'ducat' constant. But it would be neither necessary nor desirable that it tie itself legally to a particular standard. Experience of the response of the public to competing offers would gradually show which combination of commodities constituted the most desired standard at any time and place. To achieve its announced aim of maintaining the purchasing power of its currency constant, the amount would have to be promptly adapted to any change of demand, whether increase or decrease. Indeed, so long as the bank succeeded in keeping the value of its currency constant, there would be little reason to fear a sudden large reduction of the demand for it.

It seems to me to be fairly certain that

a) *a* ***money generally expected to preserve its purchasing power approximately constant would be in continuous demand*** *so long as the people were free to use it*
b) *with such a continuing demand depending on success in keeping the value of the currency constant one could trust the issuing banks to make every effort to achieve this better than would any monopolist who runs no risk by depreciating his money,*
c) *the issuing institution could achieve this result by regulating the quantity of its issue, and*
d) *such a* ***regulation of the quantity of each currency would constitute the best of all practicable methods of regulating the quantity of media of exchange for all possible purposes****.*

Clearly a number of competing issuers of different currencies would have to compete in the quality of the currencies they offered […]

We have always had bad money because private enterprise was not permitted to give us a better one. In a world governed by the pressure of organised interests, the important truth to keep in mind is that we cannot count on intelligence or understanding but only on sheer self-interest to give us the institutions we need. ***Blessed indeed will be the day when it will no longer be from the benevolence of the government that we expect good money but from the regard of the banks for their own interest*** *[…]*

It was not 'capitalism' but government intervention which has been responsible for the recurrent crises of the past. Government has prevented enterprise from equipping itself with the instruments that it required to protect itself against its efforts being misdirected by an unreliable money […] The recognition of this truth makes it clear that ***the reform proposed is not a minor technicality of finance but a crucial issue which may decide the fate of free civilization****.*

Section 3: Bitcoin primer.

Hayek would have been happy to know that this blessed day has indeed arrived. Bitcoin has provided the breakthrough innovation[9] that finally enables competition between multiple private digital currencies and traditional legal tender fiat currencies. At the time of his writing the private money issuing banks scheme must have appeared as a theoretical exercise to most and probably quite unlikely even to Hayek himself. This did not stop his detailed analysis, an almost perfect match for the current scenario.

[9] "A stroke of genius" (David Andolfatto, vice president and head of research at the Federal Reserve Bank of St Louis).

3.1: Bitcoin the Protocol, and bitcoin the Currency.

Bitcoin is indeed a distributed peer-to-peer digital *cryptocurrency* that can be transferred instantly and securely between any two parties, using the Internet infrastructure and cryptographic security, with no need for a trusted third party. Its value is not backed by any single government or organization[10]: similarly to the not centrally planned affirmation of gold, bitcoin is a case of permission-less innovation in the history of money and trade.

Historically, barter empowered the exchange economy to enlarge the cooperation space outside the inner restricted relationship circle of the gift economy. Later on, money has been instrumental in removing the limits of the barter economy, giving birth to a trade economy that has expanded cooperation to incredibly far reaching geographical and cultural horizons. Anyway in the last twenty years it has become more and more clear that the banking system built around fiat currencies is not adequate to the new digital realm defined by mobile communication, Internet, and social networks. Even not considering the monetary manipulations and fiscal abuses perpetrated in recent decades, intercontinental wire transfers are neither instantaneous nor cheap, remittance flows are subject to relatively high fees, credit cards are ill-suited for online transactions and have changed very little in the last 50 years, banking services do not cover large part of the world population, interbank settlements can be cumbersome and costly. Compare this with the possibility to transfer instantly and securely across the globe the equivalent of few cents or millions of dollars, 24/7, with (almost) no fees, without third party approval or support. As everybody[11] gets used to carrying around in their mobile phones powerful computers, hours of video and audio entertainment, and immediate access to an immense amount of information, the expectation has raised to be able to pocket a whole efficient and fair monetary, financial, and banking system along with it. It is clear that bitcoin, and cryptocurrencies in general, are so far the only money able to cope with these new formidable challenges.

Bitcoin is not the first *private money* (see Dowd, 2014), not the first digital currency, and not even the first currency based on cryptography, but it has been the first to rely on peer-to-peer network decentralization to avoid *double spending*[12] while at the same time leveraging the lessons learned by the previous experiments. Proposed by Nakamoto[13] (2008), and released as open source free software the following year, it has

---

[10] bitcoin.org/en/faq, www.coindesk.com/information/

[11] "*Over the next two years, significant numbers of the unbanked will start making the transition from feature phones to smartphones. Top-of-the-line smartphones will always be expensive, but by 2015, off-contract prices for the least expensive smartphones will fall into the $30 range, bringing them within reach of a growing fraction of the unbanked [...] Mobile money is often justifiably lauded for providing a path to financial inclusion for the unbanked. But that's only the beginning. The combination of growing mobile money adoption and declining entry-level smartphone costs will spur much a broader move towards digital inclusion. Smartphones for the unbanked, far more than any new product announcement, will be the next revolution involving mobile phone technology.*" Looking For The Next Big Thing In Smartphones? Think Digital Inclusion In Developing Countries, Forbes, 2013, http://goo.gl/TDdmps

[12] Double spending is the possibility of effectively spending multiple times the same given amount of money.

[13] Satoshi Nakamoto is a pseudonymous, and it is not even clear if he is a person or group. He has worked on Bitcoin since 2007, but his involvement stops mid-2010, after he entrusted the Bitcoin SourceForge project and a copy of the alert key to Gavin Andresen, effectively his successor.

been announced by its author with a clear explanation in a forum post[14] on February 11, 2009: *The root problem with conventional currency is all the trust that is required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust […] One of the fundamental building blocks for such a system is digital signatures. A digital coin contains the public key of its owner. To transfer it, the owner signs the coin together with the public key of the next owner. Anyone can check the signatures to verify the chain of ownership. It works well to secure ownership, but leaves one big problem unsolved: double-spending. Any owner could try to re-spend an already spent coin by signing it again to another owner. The usual solution is for a trusted company with a central database to check for double-spending, but that just gets back to the trust model […] Bitcoin's solution is to use a peer-to-peer network to check for double-spending. In a nutshell, the network works like a distributed timestamp server, stamping the first transaction to spend a coin […] the result is a distributed system with no single point of failure.*

Bitcoin consists of the Bitcoin protocol and the bitcoin (BTC) currency (note that by convention the protocol name is written with uppercase B and is singular, while the currency name is written with lowercase b and may be plural).

The protocol defines how to maintain a public ledger of transactions allowing for a safe and secure way to transfer a unique piece of digital property from one user to another: everyone knows that the transfer has taken place and nobody can challenge its legitimacy. This public ledger is called the *block chain* because it is a sequential chain of blocks, with each block aggregating multiple transactions. It keeps a record of every transaction forever, tracing back to the very first genesis block. Data can be pruned to reduce the storage requirement and only a small number of nodes in the Bitcoin network really need to keep a full copy of the chain. The protocol is a major disruptive invention and has the potential to replace any central processing authority with a decentralized peer-to-peer cryptographically secure equivalent, improving efficiency and resilience[15].

In a way, the bitcoin currency is just the first powerful application of the Bitcoin protocol, aimed at replacing the well-established central bank supreme authority. *"A new electronic cash system that is fully peer-to-peer, with no trusted third party"* according to Nakamoto (2008b): the main difference to Hayek's scenario is indeed the complete disposal of issuer banks. The issuer concept was relevant in the world known by Hayek, and that is why he was naturally thinking about banks. In the cryptocurrency world, as long as the protocol implementation is free/open-source software, the issuer concept is severely demoted to be almost irrelevant. It only makes residual sense in order to ascertain the existence and reliability of a developer team in charge of the protocol code maintenance.

[14] http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source
[15] "Everything that can be decentralized will be decentralized" (David Johnston).

Bitcoin is, in Kevin Dowd's words, "*the first currency ever to achieve take-off despite having no commodity value. In this it differs from modern fiat currencies that also have no commodity value but which started off as convertible currencies and had the commodity link later severed*" (Dowd, 2014). Some people seems very concerned about this lack of intrinsic value, notably Alan Greenspan in a December 2013 interview noted that: "It's a bubble. It has to have intrinsic value. You have to really stretch your imagination to infer what the intrinsic value of Bitcoin is. I haven't been able to do it. Maybe somebody else can". In this match between the fact of bitcoin existence and the theory of "*it has to have intrinsic value*", it is again Hayek's realism to solve the dispute: "*Some people apparently find it difficult to believe that a mere token money which did not give the holder a legal claim for redemption in terms of some object possessing an intrinsic value (equal to its current value) could ever be generally accepted for any length of time or preserve its value. They seem to forget that for the past 40 years in the whole Western World there has been no other money than such irredeemable tokens. The various paper currencies we have had to use have preserved a value which for some time was only slowly decreasing not because of any hope of ultimate redemption, but only because the monopolistic agencies authorised to issue the exclusive kind of currency of a particular country did in some inadequate degree restrict its amount"* (Hayek 1990). In the history of the evolution, the point has been reached where an artificial digital good has been engineered to be used as money, and it just started to be used for real.

Bitcoins, being numerical entities, are obviously divisible: a *satoshi* is 0.00000001 bitcoin (1 BTC = 100 million satoshi), and is currently the smallest bitcoin fraction that can be handled. It is crucial to understand that bitcoins exist only as block chain documented transactions: there are no physical bitcoins to be found anywhere and the block chain is the only register of bitcoin ownership. A bitcoin wallet has a public address, namely a simple sequence of letters and numbers which can be also represented as QR code [Figure 1]. The number of bitcoins that are associated to a given address is certified by the block chain and visible to everybody. It is a common misconception that Bitcoin ensures anonymity, when in fact its design is pseudonymous: the Bitcoin address does not provide direct information about the private key owner, but all transactions are transparent to everybody's inspection.

1FEz167JCVgBvhJBahpzmrsTNewhiwgWVG

Figure 1: A Bitcoin wallet public address. It is mine: if you appreciate this article and the fact I have not patented the included proposal please consider sending a donation. Check the tips collected so far at blockexplorer.com/a/6vME7CC6D4.

The bitcoin wallet address is the *public key* of a *private/public* cryptographic key pair. Private/public asymmetric cryptography is an algorithm in which two mathematically linked separate keys perform complementary functions. The private key[16] is able to produce a digital signature: in the case of a bitcoin transaction it is used by the sender to sign the transaction's details, which of course include the currency amount and the receiver's wallet address, i.e. the receiver's public key. The sender's public key can be used by anyone to verify this signature, ensuring the transaction has not been modified and has originated from someone with access to the sender's private key. The sender's public key, being also the sender's wallet address, shows if the transaction amount is really available for spending by the sender. There is no need to register the keys anywhere in advance, as they are only used when required for a transaction.

Securing a bitcoin wallet consists of storing the private key safely: access to the private key enables the spending of the bitcoins associated to the public key wallet address. Bitcoins are effectively owned by whoever can spend them, since transactions cannot be technically reversed.

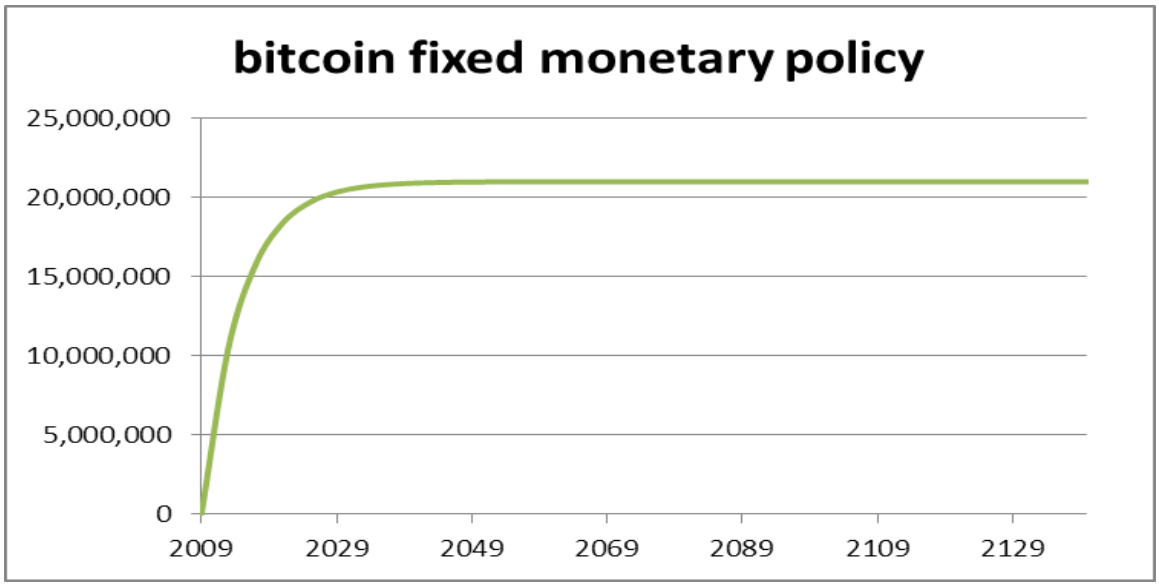

Figure 2: Bitcoin planned issuance: inelastic fixed supply, similar to gold scarcity paradigm.

Every transaction is instantaneously distributed to the Bitcoin peer-to-peer network, where it needs to be validated to avoid *double spending* of the currency amount available in a given Bitcoin address. Those providing the computing power required for processing and validating transactions, securing the network, and synchronizing the network nodes are called *miners*. They compete to be the first to process a new block of transactions: the reward for every block is paid with the issuance of new bitcoins. The per-block reward consisted of 50 BTC in 2009, halving every four years and asymptotically approaching zero. The block reward is indeed the only way new bitcoins are released and its size and schedule specify the *fully automatic, non-discretionary*

[16] Often called *secret* key.

bitcoin monetary policy: inelastic fixed supply, increasing at a decreasing rate asymptotically approaching zero [Figure 2]. The difference between the value of the block rewards and the costs associated to mining are the bitcoin seigniorage revenues. If the reader is familiar with the concept of money as a good, it is clear that its manufacturers deserve to be paid. Mining is decentralized processing rewarded by seigniorage revenues. It derives its suggestive name from the similarity of the bitcoin monetary rule with the progressive gold extraction scarcity paradigm.

3.2: Decentralized Validation of Transactions.

Miners validate the transactions included in a block by chaining the new block to the previous one in the chain: in this way transactions are published on the public ledger. A temporary fork of the block chain can happen in the case of different miners independently validating a block at the same time: at any moment the longer chain[17] becomes the consensus chain, resolving any inconsistency [Figure 3].

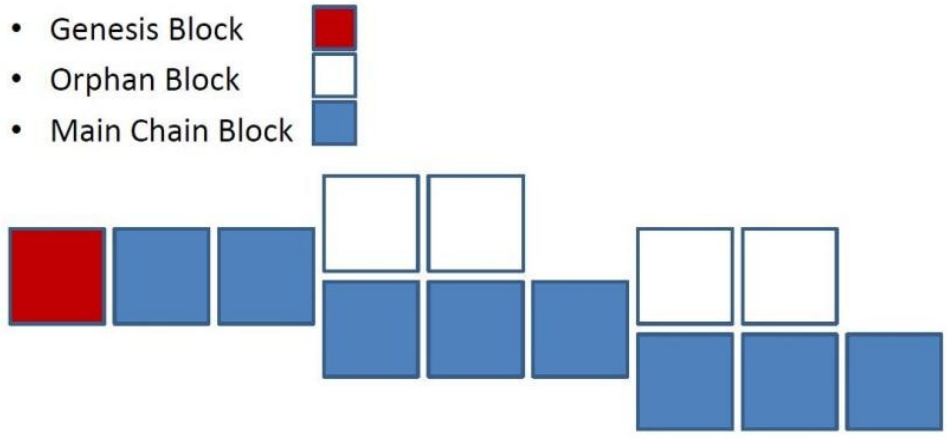

Figure 3: A stylized representation of possible block chain forks.

A new block of transactions is added by performing a mathematical *proof-of-work* based on hashing. A hash function is any algorithm that maps data of arbitrary length (in this case the block of transactions) to data of a fixed length, called the hash value. Typically a hash function is non-invertible, i.e. it is not possible to reconstruct the input data from the output data; Bitcoin uses the (Secure Hash Algorithm) SHA-256 hashing algorithm. The proof-of-work consists in finding for every new block of transactions a *nonce* (a random number used only once) included in the input data

InputData ≡ previous block hash, new block transactions, nonce

So that the following hashing constraint is satisfied:

SHA-256(InputData) <= target hash value.

[17]Actually the one with higher total combined difficulty, as defined later.

The SHA-256 function is applied to input data consisting of the previous block hash, the new block transactions, and the nonce [Figure 4]. The resulting hash value must be lower than an arbitrary target fixed by the protocol; if not, a different nonce is tried until the hashing constraint is satisfied. The nonce is introduced in order to make possible to satisfy the constraint, without it the hashing function would return a constant strictly deterministic result:

InputData ≡ previous block hash, new block transactions

SHA-256(InputData) = deterministic hash value.

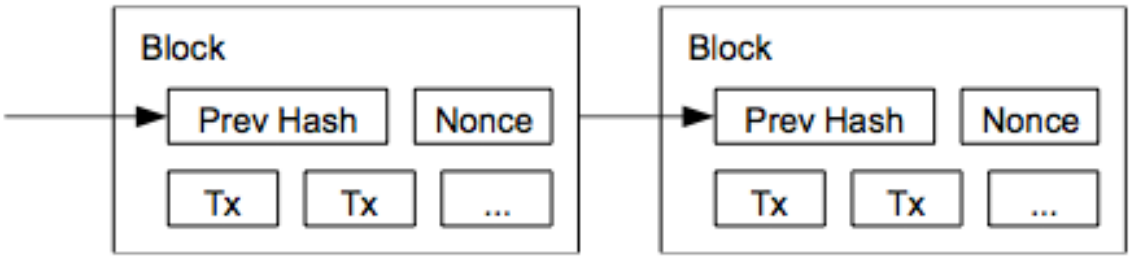

Figure 4: Bitcoin block chaining, sourced from the original bitcoin paper by Satoshi Nakamoto [5].

The lower the target, the more onerous the proof-of-work becomes: the protocol controls the proof-of-work *difficulty* with the target hash value, so making it harder or easier to find a nonce that satisfies the hashing constraint. The adjustment rationale is to ensure an average of one new block every ten minutes [Figure 5]: in the case of increasing network computing power and faster block generation the target hash value is lowered. On the contrary, verifying the hash value and the chain integrity is always computationally easy.

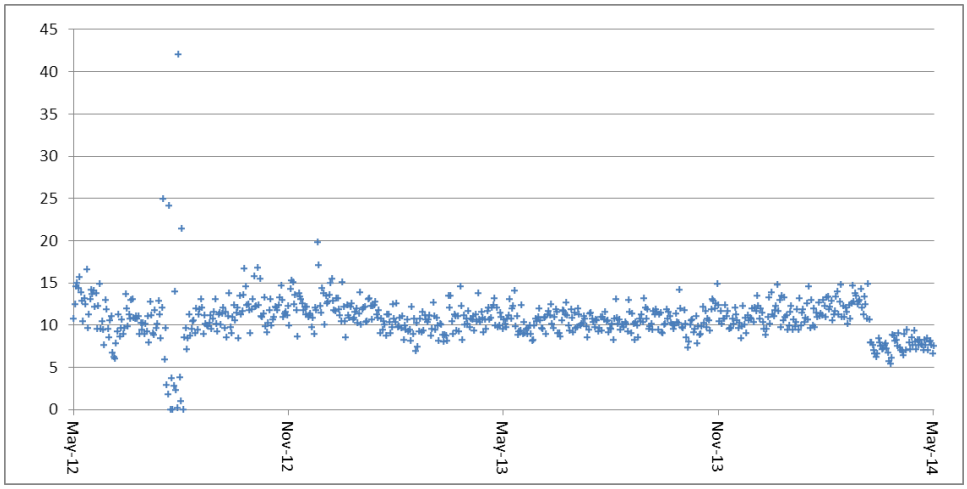

Figure 5: Bitcoin block average time creation in minutes. Source: blockchain.info

Nakamoto's original intention for a proof-of-work system was a *one-CPU-one-vote* mechanism: mining, i.e. decentralized processing, was to be a democratic decentralized feature. But growing interest in Bitcoin and high mining profitability has

skyrocketed the network hashing power (usually measured as the number of nonces tried in a second) from traditional CPU to GPU (graphics processing unit), then to ASIC (application specific integrated circuit, dramatically efficient in term of hashing power versus energy consumption ratio). Today it is impossible for anyone but ASIC server farms and hashing pools to actually have any role in mining.

3.3: Protocol Technical Issues.

Bitcoin has experienced an incredible growth in a very short time, has survived many critical events[18], and has been subjected to intense scrutiny. Its resilience is already a testament to its power and disruptiveness. Still the current implementation is not without limitations. These problematic aspects are well recognized by the community, which is trying to solve them. Without aiming to be exhaustive, the most notable implementation issues are:

- The amount of computing power *wasted* by mining. It can be argued that the costs associated with mining (hardware, power consumption, bitcoin inflation, etc.) are still minimal compared to the financial transaction industry costs. Their reduction would be welcomed anyway; also the possibility of devoting the proof-of-work computation effort toward some useful challenge is being explored;
- The clustering of mining resources. The proof-of-work approach is susceptible to a *51% attack*: any party with the majority of the hashing power would be able to create an evil chain longer than the legitimate one. While in many realistic cases such a cluster of hashing power could be better off with the honest reward for its mining activity, this consideration still does not protect Bitcoin from an agent whose interest is to destroy the network. *Proof-of-stake* is an alternative that recognizes mining privileges proportional to the amount of cryptocurrency owned: it leverages the evil agent disincentive to disrupt a network he must heavily invest into. This and other alternatives have been proposed, including mixed proofs;
- Ten minutes average time for first confirmation[19]. While this is blazingly fast compared to most payment networks, reducing the confirmation time even further would offer some benefit. This has to be balanced against the higher rate of growth of the block chain size[20];

[18] In October 2013 the FBI shut down Silk Road, an illegal dark-web marketplace that, in the attempt to escape law enforcement, operated as Tor hidden service and accepted bitcoin. In December 2013 China's Bank of People started using its moral suasion to effectively halt BTChina, at that time the main BTC exchange with 80% of the global trading volume: BTC/USD exchange rate dropped from 1200 to about 500USD. In February 2014 Mt. Gox, the second exchange by volume, filed for bankruptcy after months of rumors about its insolvency and possible fraud charges, driving prices down to about 400USD. For BTC, a five years old currency not backed by any governments or organizations, to be still alive and kicking is an impressive achievement.

[19] The transaction is instantaneous, but its confirmation needs to be performed by miners.

[20] Even more crucial would be the increase of wasted mining resources: assuming one minute for the new longer block chain to be notified to all nodes, shorter confirmation time implies higher percentage of the network mining time thrown away on the old shorter block chain by the nodes not yet notified.

- Lack of privacy. Bitcoin anonymity has been described earlier in this paper as a common misconception, since the protocol is in fact merely pseudonymous, but how bad pseudonymity is at preserving privacy might not have been fully appreciated yet. Consider for instance that the sending and receiving parties in a transaction can see how many bitcoins are in each other's wallets. If one has been naively using the same wallet to receive his or her monthly salary then his or her income and associated savings would be evident. Also any transaction involving well-known public wallets would reveal investments, spending habits, supported organizations, etc. If one party tries to defend its privacy using a dedicated transaction wallet, still the other party can trace back from that transaction wallet to the one originally providing the money to the transaction wallet. Flow-control tools can be devised to track bitcoin transactions back into the past and forward into the future as they happen. An even more problematic scenario may arise in regions where law enforcement is not effective: with a limited ability to hide their money, ordinary citizens could be easily forced into giving up their wallet content to criminal organizations. While mixing services make it more difficult to breach privacy and ever more sophisticated tools will smooth the management of thousands of transactions originating from thousands of wallets, there is nothing that could prevent a sufficiently skilled agent from systematically undermining privacy. Bitcoin simultaneously provides too much privacy for organized crime and too little for honest consumers. Possible improvements have been proposed[21];
- The block chain is governed by a very simple scripting language, limited in scope by design. While it has been so far good enough to accommodate new features such as multi-signature (multiple private keys required for spending money from a wallet), it is not adequate for the complex logic and artificial intelligence of contracts smarter than plain money transfers. Many *metacoins* have been exploiting the Bitcoin block chain, or using new alternative instances of the protocol, for transaction of non-currency digital goods and digital claims of non-digital rights and assets. Having recognized the limitation of the current protocol, people are working on the enhanced next-generation decentralized application platform for smart contracts, smart properties, and the creation of decentralized autonomous corporations[22]. This research avenue promises to combine the information available on the Internet with the ownership management of digital goods and rights allowed by the block chain invention with the software logic of a programming language. This mix might render anything from peer-to-peer *delegative democracy* to exciting new possibilities beyond the limit of our current imagination as technically feasible reality;
- Bitcoin has an impressive power that is still lacking appropriate tools and adequate ecosystem. On one hand anyone could send a multimillion dollars' worth transaction to another party anywhere in the world at any time any day

[21] zerocoin.org, darkwallet.unsystem.net
[22] www.ethereum.org

in an irreversible and nearly instantaneous way, without fees and without fear that the transfer could be stopped or the money seized. On the other hand regular people are not ready to accept the new *"data is money"* paradigm: these days it is still hazardous to commit a significant amount of money to the perceivable feebleness of the secure storage associated to a sequence of letters and numbers. Together with the price stability issue dealt with in this paper, this is probably the other major stumbling block for cryptocurrency widespread adoption. Improved software solutions [23] and hardware wallets are being developed to mitigate this problem; moreover, we can probably look forward to some non-naïve application of biometrics to be mixed in the cryptographic machinery.

Bitcoin is a very recent, new, and complex protocol: its architecture, governance, and ecosystem are clearly evolving at a fast pace. Many improvements have already been incorporated in the Bitcoin system itself, while others are pioneered by alternative cryptocurrencies.

3.4: Deflation and Volatility, Money Comparison, Monetary Rule Criticism.

Moving from the protocol to the bitcoin currency the two major issues currently observed are the huge deflationary trend and the extreme volatility of the USD/BTC exchange rate [Figure 6].

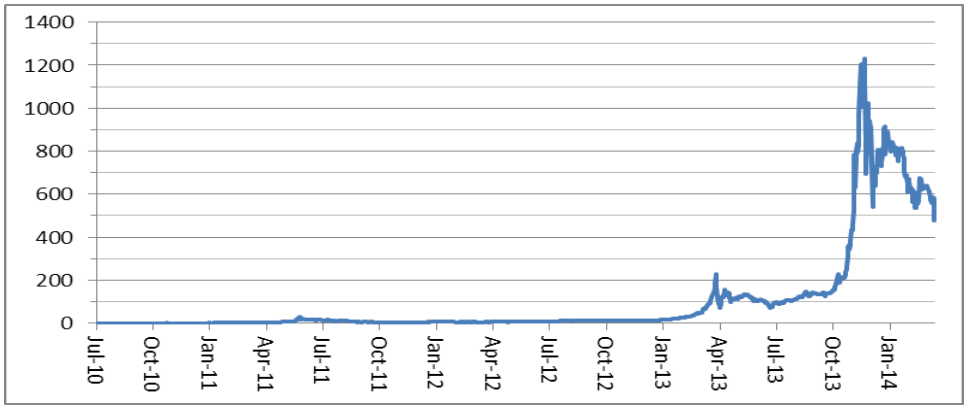

Figure 6: USD/BTC weighted close prices. Data is from the Mt. Gox exchange up to the end of 2013 and from the Bitstamp exchange in 2014.

As long as the number of people who appreciate the usefulness of the cryptocurrency continues to grow, demand for it keeps increasing: the bitcoin supply is not able to adapt, being inelastically fixed at a predetermined rate, so the BTC value is going up. The resulting deflation is unavoidable, given bitcoin monetary rule, and completely destroys any information available from the price system [Figure 7]. Bitcoin not having died of such an impressive deflation is a testament to how resilient the demand for cryptocurrencies is, especially because of its strength as medium of exchange.

[23] bitcoinarmory.com, electrum.org, greenaddress.it

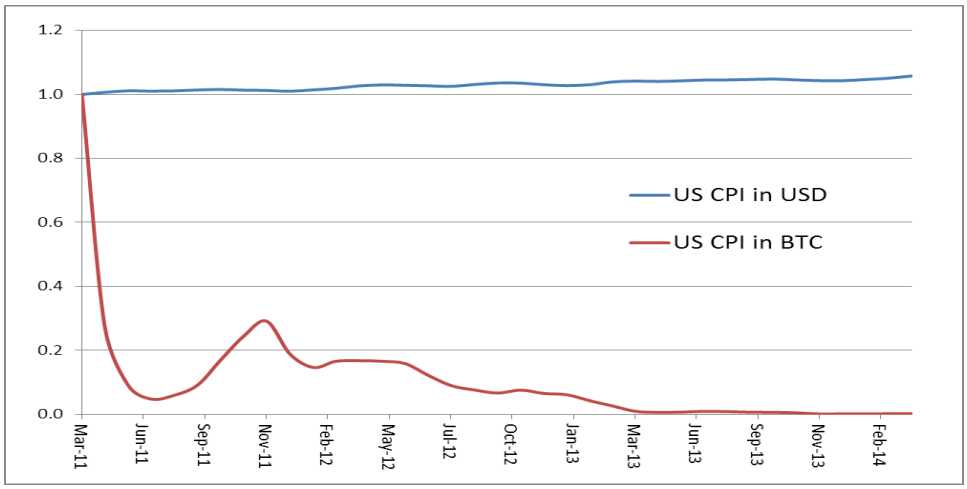

Figure 7: US CPI in USD and BTC: notice the dramatic BTC deflation. US CPI data are from InflationData.com

The cryptocurrency price stability can be salvaged with the proposal presented in this paper, with huge benefits for the money usefulness. The excessive volatility that destroy the monetary function of any means of payment will be controlled and tamed up to a point (see subsection 4.4). Of course volatility cannot be completely removed as it is an intrinsic property of demand dynamics. Volatility is the dispersion of value changes (returns) around the average change (return): bitcoin average daily change has been 0.91%, and its dispersion has been 6.70% [Table 1]. In plain words, bitcoin adoption does not increase at a steady rate and there is no way to force it into a constant growth:

- exchange volumes are still low, so the price is prone to severe shocks due to profit-taking sell-off and the fragility of the new ecosystems (exchange failures and frauds, bugs in the protocol, legal uncertainty, etc.);
- consumers and firms investing in bitcoins often have to resort to fiat currencies to cover their liabilities;
- bitcoin prices being too unstable and risky, there is scarcity of goods and services that can be bought using bitcoins: this prevents the growth of a bitcoin-based economy that would lower its volatility.

Daily Returns 17-jul-2010 / 29-mar-2014	USD/BTC
Mean	0.91%
Standard deviation	6.70%
Volatility	128.04%
Skewness	74.33%
Excess kurtosis	861.10%
Minimum return	-46.16%
Maximum return	45.10%
Value-at-Risk at 99% confidence	16.60%
Expected Shortfall at 99% confidence	24.38%

Table 1: USD/BTC daily returns statistics. Annualized volatility is $\sqrt{365}$ times the standard deviation.

The last point should be perused with piqued interest: lack of price stability also exacerbates the volatility problem. It is evident that Hayek, even if happy in these bitcoin-blessed days, would have been nonetheless the most ferocious critic of the complete lack of cryptocurrency price stability originating from bitcoin monetary rule of inelastic supply. His comments about the hypothesis of private money backed by gold are a perfect match for bitcoin too, just replace gold with bitcoin in the following paragraph (Hayek 1977): *It would turn out to be a very good investment, for the reason that because of the increased demand for gold the value of gold would go up; but that very fact would make it very unsuitable as money. You do not want to incur debts in terms of a unit which constantly goes up in value as it would in this case, so people would begin to look for another kind of money: if they were free to choose the money, in terms of which they kept their books, made their calculations, incurred debts or lent money, they would prefer a standard which remains stable in purchasing power.* The unfeasibility of a bitcoin loan is similar to that of a bitcoin salary: neither a borrower nor an employer would want to face the risk of seeing her debt or salary[24] liabilities growing a hundredfold in a few years. A manufacturing firm cannot accept an order in bitcoin with the risk of its value doubling or halving on a single bad day. Even the development of a derivative market could only hedge these risks with an implausibly high price. This is the cryptocurrency paradox: arguably the best ever kind of money by any metrics, marred by the severe inability to serve as reliable unit of account [Table 2]. This is the single major obstacle for the widespread adoption of cryptocurrencies. It is true that when it comes to the unit of account property, fiat currencies have displayed very bad track records too, but if we restrict our attention to the major currencies of developed countries in the last decade, good price stability has been achieved.

	Medium of Exchange	Store of Value	Unit of Account
Live cattle	●	●	●
Diamonds	●	●●●●	●●●
Gold	●●●	●●●●	●●●
Fiat coins and notes	●●●●	●●●○	●●○○
Cryptocurrencies	●●●●●	●●●●?	●●???

Table 2: Money comparison: please refer to Section 1 for definitions and an implicit justification of these subjective valuations. Extra ○ bullets are only for recent times in developed countries.

The statement of the problem is: in the successful attempt to get rid of any centralized monetary authority using the Bitcoin protocol, the bitcoin currency has inadvertently thrown away the flexibility of an elastic monetary policy. Nakamoto was well aware of the price stability issue: *The fact that new coins are produced means the money supply increases by a planned amount, but this does not necessarily result in inflation. If the supply of money increases at the same rate that the number of people using it increases, prices remain stable. If it does not increase as fast as demand, there will be deflation*

[24] Despite crypto-enthusiastic propaganda, the news of salaries paid in bitcoin is the typical journalistic deceptive misrepresentation: in all know cases the salary is always defined in term of fiat currency, and then just exchanged in bitcoin to the prevailing current exchange rate.

and early holders of money will see its value increase. Coins have to get initially distributed somehow, and a constant rate seems like the best formula (Nakamoto 2008b). His wording seems to suggest that a better approach did not occur to him at the time: this is understandable considering the monumental initial challenge of establishing a cryptocurrency for the first time ever. The insight gained since then should have made evident to everyone that in the historical *unicum* of introducing a radically new money bound for dominance, with the prospect of fast global adoption and skyrocketing intrinsic deflation, when the money supply most needs to be utterly elastic, then the choice of inelastic supply is simply a humongous mistake.

At this point the line of reasoning should hopefully be self-evident: in order to target purchasing power stability, the cryptocurrency outstanding amount must be elastically rebased in a fully automatic algorithmic non-discretionary way. A cryptocurrency adopting such an elastic supply is defined here as *Hayek Money*. If not self-evident, this idea has appeared at least consequential not only to the writing author, but also to Dowd (2014) that has recently and independently written: "*The ideal – one is tempted to say, the gold standard in this area – would be one or more cryptocurrencies that were able to achieve stable purchasing power through elastic but fully automatic and hence non-discretionary supply schedules when real demand changes, and which also have the ability to maintain state-of-the-art security*". Dowd ends his Hayek Money prophecy with a wish this author wholeheartedly supports: "*Going further, the ultimate possibility for those who believe in private money is that cryptocurrencies might eventually become so widely accepted that they drive government currencies out of circulation and expel the government from the monetary system once and for all*". Moving to elastic supply, the goal of getting rid of monetary authorities is not abandoned[25], only made easier by a better stronger cryptocurrency.

Section 4: Hayek Money.

In this section the aim is to control the elastic supply of cryptocurrency in order to counteract any tendency of an aggregate price index to rise or fall, keeping constant the purchasing power of the currency unit. This is performed in a fully automatic and non-discretionary way, with no need for a central authority. In principle what follows is equivalent to the policy adopted by central banks[26] to achieve their low and stable inflation targets (McLeavy, et al. 2014), the relevant difference being about the technical means adopted, their effectiveness and fairness. Compared to the inelastic fixed supply of bitcoins, the advocated monetary policy is utterly elastic. The impatient

[25] The central bank is replaced by its decentralized blockchain-based equivalent, which can be described as a Decentralized Autonomous Organizations, *an entity that lives on the internet and exists autonomously, but also heavily relies on hiring individuals to perform certain tasks that the automaton itself cannot do* [blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide], the individuals being the miners as it will be clear in Section 6.1.

[26] The contrarian reader is kindly urged not to challenge *in unfairly way* the parts of the present proposal that he might have unmindfully accepted for a long time from central banks.

reader is advised: all technical block chain implementation details are left for section 6.

Economic history and literature are rich with schemes to peg the value of the currency to a price index or price index derivative, in order to provide price stability: monometallic (gold) standards, bimetallism, and later the symmetallism proposed by Marshall (1887) and Edgeworth (1895); the *"fixed value of bullion" standard* proposed by Williams (1892); Fisher's *compensated dollar* (1911, 1912, 1913, 1914, and 1920); the *Commodity Reserve Currency* scheme suggested by Goudriaan (1932), B. Graham (1937, 1944), F. Graham (1942), and revisited by Friedman (1951); Hall's (1982) ANCAP basket; the by Miles (1984) and Sumner (1989, 1991, 1995) to use futures contracts, Kevin Dowd's (1994) quasi-futures contract, and later Dowd's (2000) price index option. For a review of this literature the reader is referred to Dowd[27] (1996, Chapter 14).

Because of its inelastic supply bitcoin has always been unfit to peg its value to anything, and as such it has been a terrible unit of account. The most vocals among the bitcoin economists and researchers have usually preferred to demote this issue as non-pertinent, stressing bitcoin's exceptional medium of exchange quality as the only relevant feature. As example, Šurda (2012) quotes Mises (1912): *Thus there would be an inevitable tendency for the less marketable of the series of goods used as media of exchange to be one by one rejected until at last only a single commodity remained, which was universally employed as a medium of exchange; in a word, money*. Šurda then juxtaposes Menger (1871): *But it appears to me to be just as certain that the functions of being a "measure of value" and a "store of value" must not be attributed to money as such, since these functions are of a merely accidental nature and are not an essential part of the concept of money*, mixing in the middle Schlichter (2011) which in his *Paper Money Collapse: The Folly of Elastic Money and the Coming Monetary Breakdown* writes: *All additional functions that can be assigned to money are the result of money being the accepted medium of exchange.* While it is easy to agree that any good which might be considered as money must possess the medium of exchange quality as relevant foundation, it is not clear why the unit of account quality should be disposed with. Moreover, it is questionable that the abuses perpetrated with representative money and fiat currencies make elastic money supply a folly. One is left with the impression of the cognitive dissonance of the Aesopian fox despising the unreachable grapes, which is in this case is also unduly inappropriate, as the cryptocurrency fox can reach indeed the price stability grapes.

One more common misconception is about bitcoin becoming more stable with increasing adoption: this is indeed true, but not at all sufficient for stable prices, as demonstrated by the need of monetary actions to stabilize even globally accepted currencies as Euro and US dollar.

[27] I am in debt with Kevin Dowd for having introduced me to the existing literature, kindly emending my sheer ignorance while at same time encouraging my jaunty contribution.

4.1: Fixed USD Exchange Rate.

Let us start with a very stylized case study: in the following the bitcoin usage is instrumental in taking advantage of the history of USD/BTC exchange rate; later on it will be clear that a new cryptocurrency might be best suited for the Hayek Money implementation. The case study will be incrementally refined, progressing toward a more realistic description of the monetary policy. Let us provisionally assume that the only good we are interested in is the US dollar: our consumer price index (CPI) is only comprised of 1USD, so in this case "increasing prices" (price inflation) means that more bitcoins are needed to buy one US dollar.

With respect to the 1USD consumer price index, bitcoin has experienced a huge price deflation so far. The weighted close price of the USD/BTC exchange rate was 1.0 on April 15th 2011 and has reached the level of about 500 on March 29th 2014, i.e. in March 2014 1 bitcoin could buy 500 US dollars or 0.002BTC could buy 1USD. The higher BTC value in March 2014 reflects a demand for bitcoin which has increased 500 times *relative* to the demand for US dollars, i.e. it might be that BTC demand has increased or USD demand has decreased (or more likely both effects were in action to varying degrees) resulting in an overall 500 fold appreciation of BTC relative to USD.

Because of the inelastic fixed supply of bitcoin monetary rule, no inflationary correction has been taken to counteract the 49,900% price deflation over the last three years. In an alternative world where the bitcoin monetary rule targeted price stability, the bitcoin supply could have been increased to match the 500 fold increase in bitcoin demand: considering that on March 29th 2014 the quantity of bitcoins in circulation was about 12.5M, it would have been enough to inflate their number 500 times to about 6250.0M. The monetary base increment should have been distributed pro-quota to every digital wallet, without unfair wealth redistribution. This action would have had no real impact on a wallet containing 1BTC on April 15th 2011, as on March 29th 2014 it would have been completely equivalent to own 1BTC worth 500USD or 500BTC each worth 1USD[28].

This outstanding currency amount *rebasing* should have been performed at least daily, so that a wallet steadily holding a single bitcoin from April 15th 2001 would have seen its amount peaking at over 1200 *rebased*-bitcoins (RBTC hereafter) in December 2013 when the USD/BTC rate reached 1200, and then down to 500RBTC on March 29th 2014. These huge amount swings would not have exogenously altered the wallet effective wealth, which would have varied only because of BTC demand changes relative to USD.

Let us assume that the price dynamics actually observed in the real world for USD/BTC exchange rate would not have been altered by the proposed rebasing process, as this does not alter any fundamental relative value dynamics, and let us

[28] The reader familiar with measure theory might recognize a change of numeraire here.

focus our attention on observing the hypothetical USD/RBTC exchange rate. Let us also assume for the sake of simplicity that instead of the continuous trading happening on the USD/BTC exchanges we have some kind of micro-interval between the end of one day and the open of the next, during which we can instantaneously perform the money stock rebasing process.

With these assumptions, starting from the USD/BTC parity observed at the close of April 15th 2011 (day *one*) we would have registered 1.00 as the first multiplicative rebasing index: the number of RBTC would have been made equal to the actual number of BTC. The next day (day *two*) the USD/BTC closed at 1.04 with a +4% daily change: in our alternative world the USD/RBTC would have opened at 1.00 and closed at 1.04. Anyway at the new close the multiplicative rebasing index would have been updated to 1.00*4%=1.04 and the outstanding number of RBTC would have been increased to 1.04 times the number of BTC. Because of the increased supply the RBTC would have lost value: on day *three* while USD/BTC opened at 1.04 the USD/RBTC would have opened at 1.00. Since USD/BTC closed on day *three* at 1.08 with a 3.85% daily change, the equivalent close price for USD/RBTC would have been 1.0385, incorporating the same 3.85% daily change. At the end of day *three* the rebasing index would have been updated to 1.00*4%*3.85%=1.08 and the RBTC monetary base would have been expanded to 1.08 times the number of BTC, to force the next day opening of USD/RBTC to be again 1.00. And so on and so forth.

It can be observed that, since we started from parity, the close price of USD/BTC in the real world would have been the RBTC rebasing index in our alternative world: the RBTC monetary stock would have expanded and shrunk according to the USD/BTC exchange rate leading to a number of RBTC equal to 500 times the number of BTC available on March 29th 2014. And this would have continuously anchored the USD/RBTC to parity.

Adapting the money supply would have provided the crucial benefit of dramatically improved rebased-bitcoin price stability, i.e. an online merchant could have easily provided RBTC prices exploiting the fixed USD/RBTC parity exchange rate, without the need for continually rebalancing them to compensate for the extreme bitcoin volatility. All of a sudden loans and salaries could be expressed in RBTC, and contracts involving future payments in RBTC would make economic sense: the promise to pay a given amount of RBTC would not be a hazardous commitment of dramatically uncertain value anymore. Prices and forward payment agreements would carry only the risk usually associated with using USD or any equivalent currency. The RBTC would have closed its gap as unit of account affirming its absolute supremacy as the best money ever devised.

4.2: Rebasing Process Reaction Lag.

In the accompanying HayekMoney spreadsheet[29] this rebasing process is simulated in the three-year period spanning from March 29th 2011 to March 29th 2014. Because of the extreme bitcoin volatility, the end-of-day rebasing process would really have changed the number of currency units in each wallet in a significant way, almost halving/doubling their number at peaks/troughs [Figure 8].

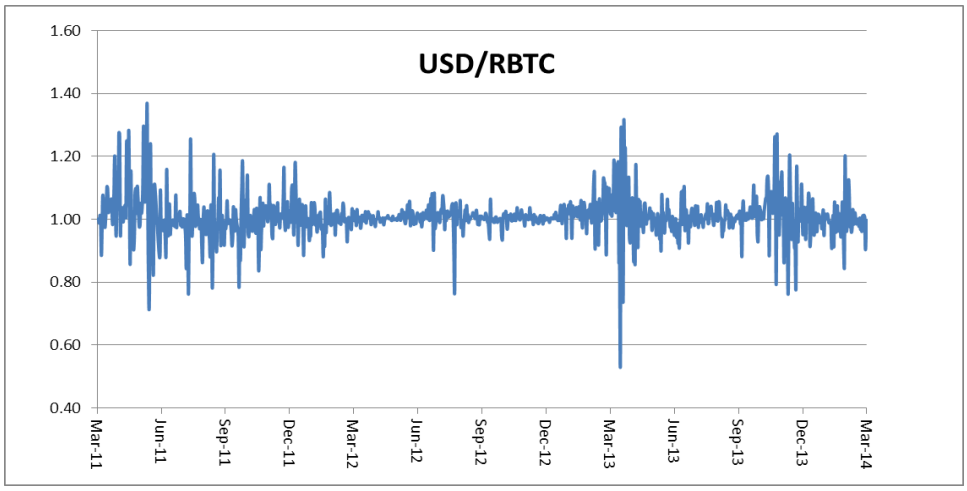

Figure 8: plot of the equivalent USD/RBTC.

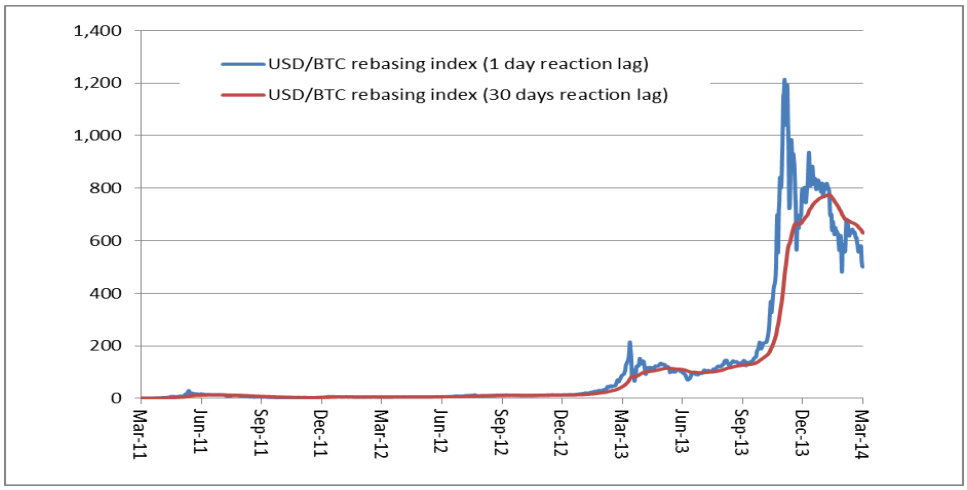

Figure 9: USD/BTC rebasing index with 1 and 30 days reaction lag.

It might be worthwhile to experiment with the introduction of some rebasing reaction lag. So far we have considered a reaction lag of one day: the rebasing index is fully updated at the end of the day. If the reaction lag is increased to 30 days this would imply that at the end of each day only 1/30 of the needed money stock adjustment is performed [Figure 9]. The following day the USD/RBTC exchange rate would set a new close price and a new updated adjustment would be needed: again only 1/30 of this new rebasing target would be performed, adding up to the previous day trend if both

[29] https://www.dropbox.com/s/bhu9tp2j22g6t3i/HayekMoney.xlsx; the QuantLibXL addin quantlib.org might be needed:
https://www.dropbox.com/s/08cqned83ufyhjo/QuantLibXL-vc110-mt-s-1_4_0.xll
https://www.dropbox.com/s/g4adcozt1r6ml70/QuantLibXL-vc110-x64-mt-s-1_4_0.xll

days have had the same price change direction, or partially cancelling out in the case of opposite directions. The benefit would be to avoid the significant swings caused by opposite changes offsetting each other.

Thirty days is an excessive lag chosen only for illustrative purposes: with such a large lag the USD/RBTC exchange rate spikes up to almost 4.0 and down below 0.50, which is too much for price stability [Figure 10]. In the next section rebasing at every new block creation will be advocated, i.e. every 10 minutes on average, in order to keep price stability under control. The idea of introducing a lag to avoid overreacting to market noise will need to be fine-tuned.

In the HayekMoney spreadsheet it is also possible to move away from bitcoin history and to play with a hypothetical *stablecoin* whose daily return distribution is equal to that of bitcoin, except for the fact that its sampling is random: this is equivalent to using the characteristic return distribution historically observed for bitcoin, but scrambling its chronology for many alternative realizations that historically did not happen. How to replace the bitcoin distribution altogether with an exogenous Gaussian one of a given mean and standard deviation is left as an exercise for the reader (with a hint in cell stablecoin!B2). The price stability can be achieved without problems in all those alternate worlds.

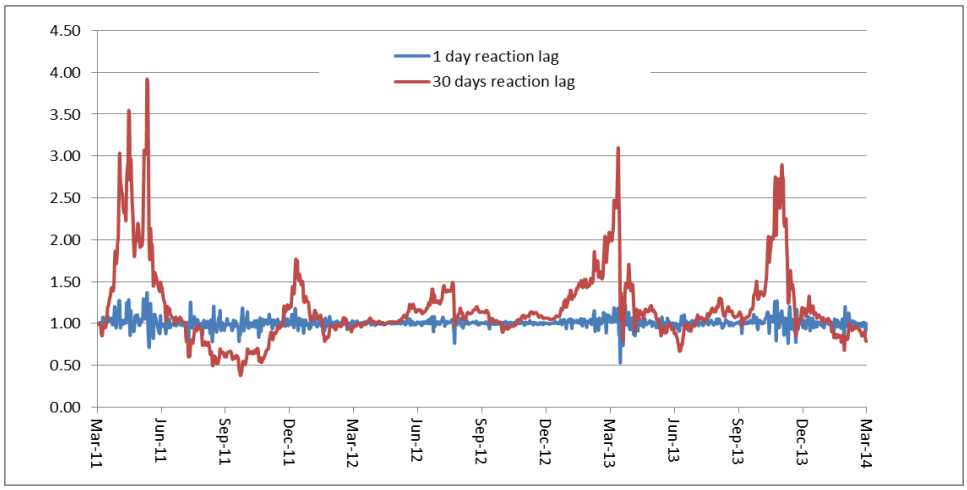

Figure 10: Plot of the equivalent USD/RBTC with 1 and 30 days reaction lag.

4.3: Adopting the USD Consumer Price Index.

So far our CPI only comprised 1USD: this fixed exchange rate scenario is a peculiar but relevant one, historically embraced by many currencies in the real world[30]. Because of this approach our cryptocurrency has inherited the USD monetary policy as far as inflation/deflation rate is concerned. While this might look acceptable to some superficial observer because of the low inflation rate experienced in recent years,

[30] Most notably all major currencies in the world adopted fixed exchange rates in the 1944 United Nations Monetary and Financial Conference at Bretton Woods. The so-called Bretton Woods system remained in place until the Nixon shock of unilaterally canceling the direct convertibility of the US dollar to gold in 1971.

nonetheless it would be a very dangerous link. In the likely scenarios where fiat currencies lose significant value because of cryptocurrency superior alternatives, prices in fiat currencies would experience a dramatic increase. With RBTC anchored to the USD, also RBTC prices would increase in the same way, completely destroying any price stability benefit.

So the next improvement is to move to a realistic consumer price index: for the sake of example we can start with the US one, as published by the Bureau of Labor Statistics. Indeed the definition of a full blown independent CPI would be a large task, probably unfeasible even in the real world for the current Bitcoin ecosystem. What is temporarily suggested here is to borrow the US consumer price index composition, delegate the price measurement to the Bureau of Labor Statistics, and correct the USD/RBTC exchange rate by the inflation index. This is conceptually equivalent to assuming the US CPI composition as the cryptocurrency consumer price index, then observe the price of included goods in RBTC, or if not possible, in USD and convert them into RBTC.

The inflation correction has a very limited impact in this case study since the US three years inflation in the period March 2011-2014 has been low at about 6% overall. Nonetheless the reader can notice that in our alternative world the USD/RBTC exchange rate would have correctly drifted to about 1.06 in March 2014 as a consequence [Figure 11]. This confirms that the inflation correction is of paramount importance to separate the cryptocurrency monetary dynamic from the USD one. One more point worth mentioning is that even if the USD/BTC is the most liquid exchange rate, our CPI is not constrained to be the US one. It could be that of the EU or UK, or a mix of them using the appropriate USD/EUR and USD/GBP exchange rates to calculate equivalent USD prices.

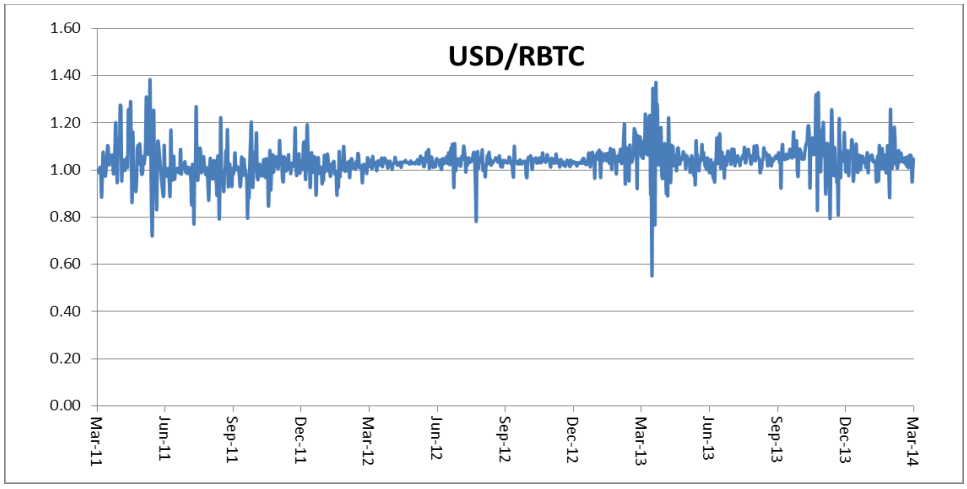

Figure 11: Plot of the equivalent USD/RBTC when US inflation is taken into account.

Adopting an existing CPI is a nice experiment in our simulation, but it would have its own share of problems in the real world. Of course having a central authority measuring inflation is not easily amenable to the third party zero-trust cryptocurrency

tenet: how to observe reference prices and exchange rates with a decentralized resilient approach is the focus of the sixth section. But even leaving this problem aside for a while, inflation measurement is a complex exercise of discerning the intrinsic relative value price changes of goods; moreover, the selection and maintenance of the market basket of representative goods is arbitrary.

4.4: The Cryptocurrency Commodity Price Index.

These considerations suggest using commodities as components of the price index. As Hayek wrote: *On the whole I would expect that [...] a collection of raw material prices [...] would seem most appropriate, both from the point of view of the issuing bank and from that of the effects of the stability of the economic process as a whole.*

Commodities are supplied without significant qualitative differentiation across markets: this approach is robust to market basket manipulations, avoids the problem of price changes due to shifts in manufacturing technological improvements, and can be based on commodity futures prices which are some of the most liquid and scrutinized financial prices. In the HayekMoney spreadsheet a simple *reference commodity basket* composed of 50% Brent Crude Oil and 50% Wheat is considered: the index is normalized to an initial March 29th 2011 value of 400USD. Using USD futures prices[31], a time series for this index can be constructed [Figure 12][32]: notice how bitcoin deflation has dramatically slashed the prices of the commodity basket.

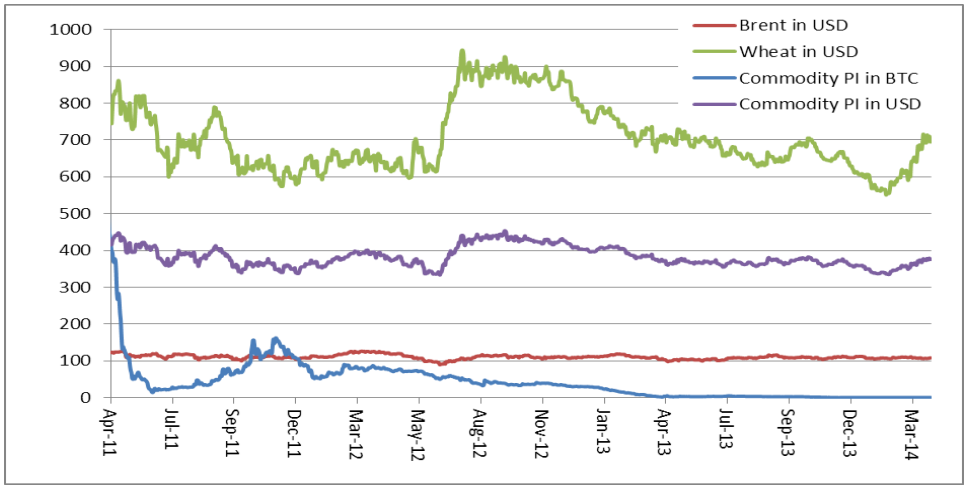

Figure 12: Commodity price index case-study in USD and BTC. Data from www.investing.com/commodities/

In the alternate world where the bitcoin monetary policy targets commodity price stability, one can normalize the basket price to (the arbitrary price of) 10RBTC: indeed a perfectly stable price for the basket is achieved [Figure 13]. Of course the prices of other commodities, goods and services will freely float in time: "stable prices" in economic jargon actually only refers to the basket price. We anchored money, the

[31] And ignoring quibbles about differences between spot and futures prices.
[32] Charts are plotted from April 15th to exploit the USD/BTC parity on that day, when the index was worth 415.92 in both USD and BTC.

yardstick of value measurement, to the weighted average of a few commodities deemed especially relevant, leaving the rest to move and reorder along the value line. This is not to be considered a limit: the price system should keep providing its genuine feedback about relative values. Of course different baskets can be considered, with different commodities and different weights.

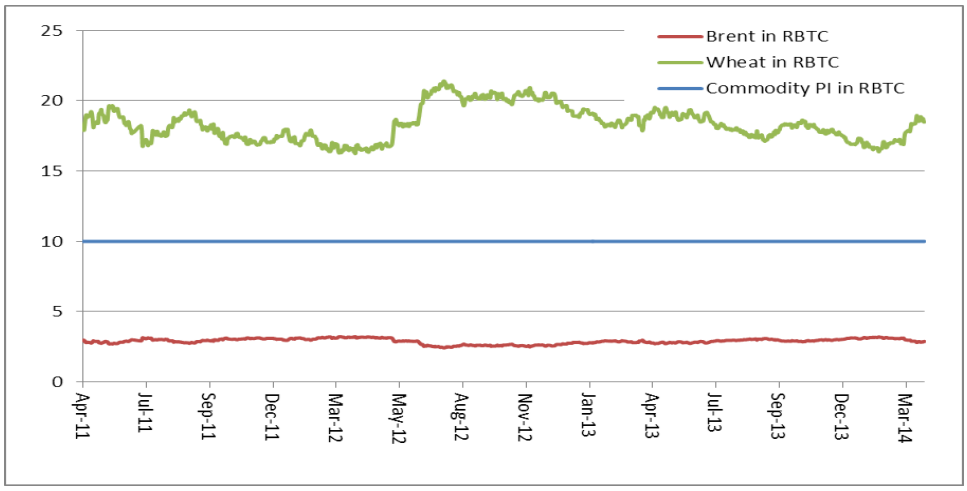

Figure 13: Commodity price index case-study in RBTC. Data from www.investing.com/commodities/

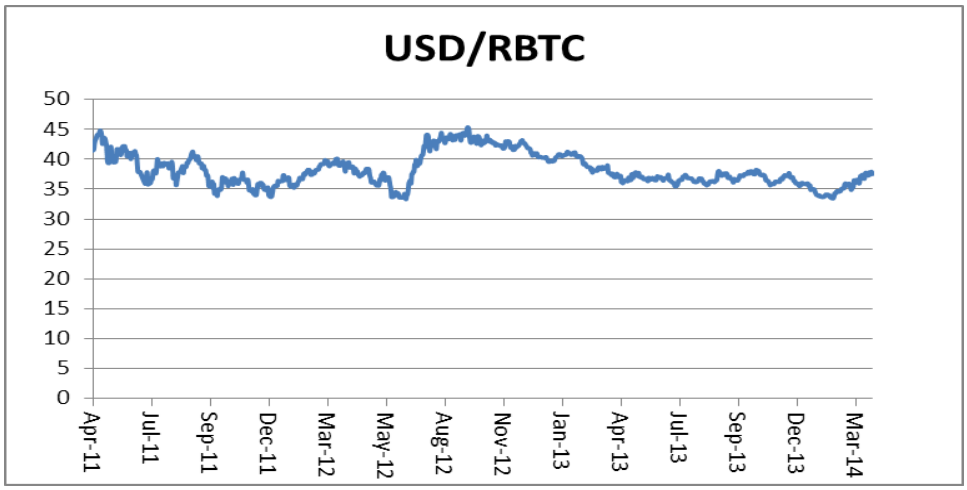

Figure 14: USD/RBTC exchange rate in the case of commodity price index parity.

The reader might wonder what has happened to general price stability along the parity path followed so far: from USD/RBTC, to inflation-adjusted-USD/RBTC, and finally Commodity-Price-Index/RBTC. In the latter case, are the prices of goods and services not included in the Commodity Price Index stable in some way? Or are they dramatically volatile? [Figure 14] answers these questions plotting the USD/RBTC exchange rate *in the case of commodity standard parity*: notice how reasonable the exchange rate volatility is now.

It might be even more convincing to plot normalized USD/EUR and USD/RBTC exchange rates to better appreciate how RBTC has finally joined the realm of currencies characterized by ordinary volatility levels [Figure 15].

[Table 3] shows how volatility has dropped from over 120% to about 21% (basically the commodity price basket volatility of 20.47% plus an additional contribution from the reaction lag). The skeptical reader will be quick to point out that this reduction is because most of the RBTC value variability has been dumped into elastic supply of the monetary base. But this is *exactly* what happens for any fiat currency, where the observed volatility is what is left after monetary policy has regulated the available money stock. It is just that finally the same sensible approach is available to cryptocurrency: the benefits of elastic monetary policy have been regained despite the absence of a central monetary authority.

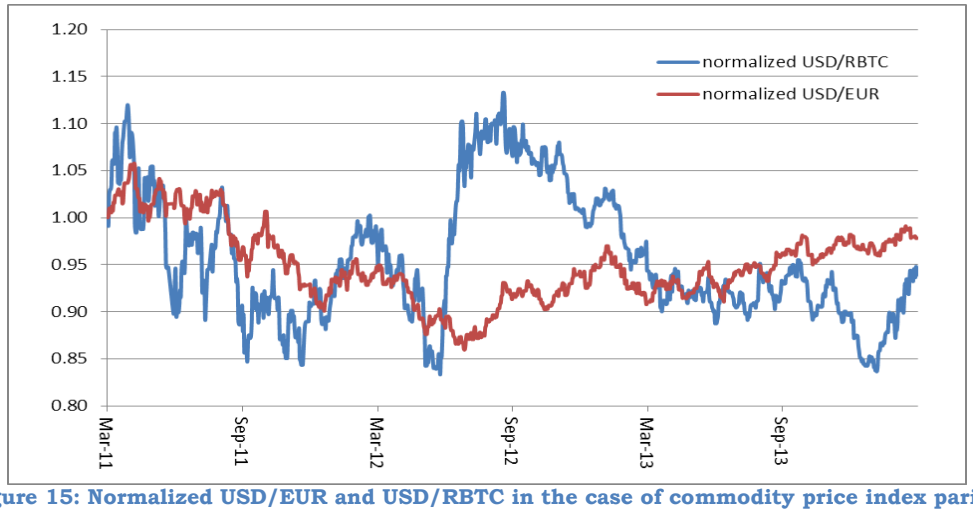

Figure 15: Normalized USD/EUR and USD/RBTC in the case of commodity price index parity.

Daily Returns 29-mar-2011 / 29-mar-2014	USD/RBTC	USD/BTC
Mean	0.00%	0.79%
Standard deviation	1.11%	6.30%
Volatility	21.21%	120.27%
Skewness	-42.83%	24.53%
Excess kurtosis	411.80%	842.33%
Minimum return	-5.52%	-46.16%
Maximum return	4.35%	36.93%
Value-at-Risk at 99% confidence	3.91%	17.76%
Expected Shortfall at 99% confidence	4.67%	25.66%

Table 3: Exchange rate daily returns statistics in the case of commodity price index parity. Annualized volatility is √365 times the standard deviation.

A similar exercise can be done with gold. The currency value can be normalized to 1500RBTC for the 100 troy ounces of gold represented by the CME futures contract, so that 15 currency units can always be exchanged for one troy ounce of gold [Figure 16, Figure 17, Figure 18, and Table 4]. This special choice of a 100% gold basket deserves proper attention as it is different from anything else ever tried before. The Hayek Money crypto-version of the gold standard is a new kind of representative money without reserve requirements. *It ought by now of course to be generally understood that the value of a currency redeemable in gold (or in another currency) is not derived from the value of that gold, but merely kept at the same value through the automatic regulation of its quantity* (Hayek 1990). Considering that the USD monetary

base is about 4 trillion[33], and that all the gold in the world is worth about 8 trillion USD[34], then a Hayek Money cryptocurrency indexed to gold could reach twice the USD monetary base with no problems. And when it will exceed the 8 trillion USD market cap[35], then gold will just become the physical instance of the digital cryptocurrency. In the Hayek Money world the unthinkable could become reality: gold as representative money backed by the digital Hayek Money cryptocurrency.

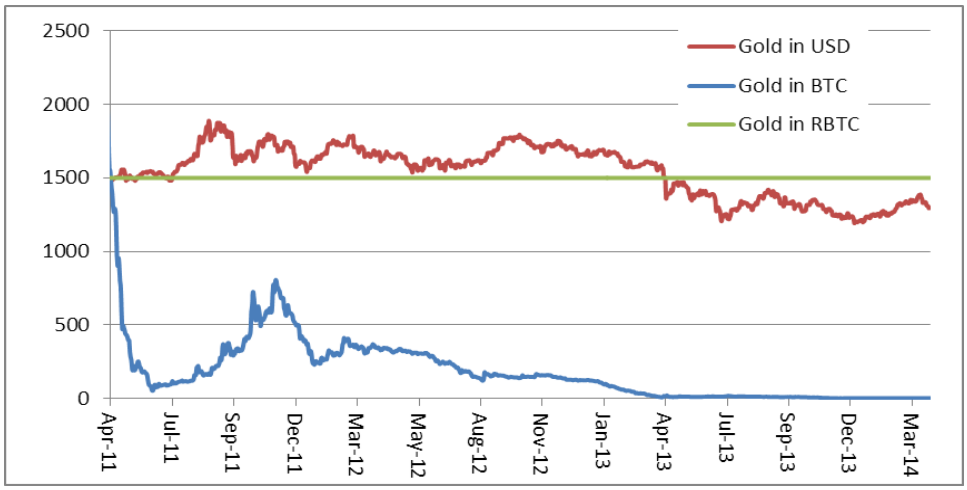

Figure 16: Price of 100 troy ounces of gold in USD and BTC. Data from www.investing.com/commodities/

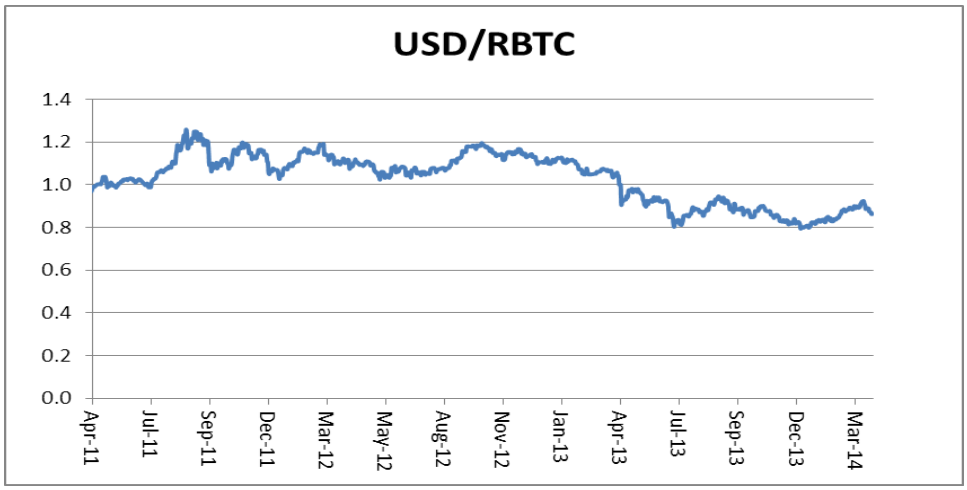

Figure 17: USD/RBTC exchange rate in the case of gold index parity.

For the time being this concludes the generic high-level explanation of how cryptocurrency price stability can be achieved. Cryptocurrencies adopting the monetary standard of elastic fully automatic non-discretionary supply regulated to achieve stable prices with respect to a (commodity) price index[36] are defined to be *Hayek Money*. The departure from Hayek's concurrent currencies scheme is about

[33] http://www.federalreserve.gov/releases/H3/Current/#t2tg1link
[34] http://onlygold.com/TutorialPages/All_The_Gold_In_The_World.asp
[35] If that will happen, it is dubious the USD will be still a useful market cap unit of measure…
[36] The difference between pegging to a price instead of a price index, taking into account the properties a good price index must have, is ignored here for the sake of simplicity. Moreover, the challenge of a distributed consensus average process for fixing a price (index) is huge enough to leave further analysis for future works.

how the volume of private currency can be regulated. In Hayek's scheme the issuing institution would need to buy/sell its currency against other currencies/securities/commodities and contract/expand its lending activities: this is how central banks operate. In the case of a cryptocurrency the obvious superior alternative is to enforce the monetary policy on the block chain itself, directly altering the number of currency units in every wallet. How this can be technically done without relying on a third party authority is the significant challenge of section 6.

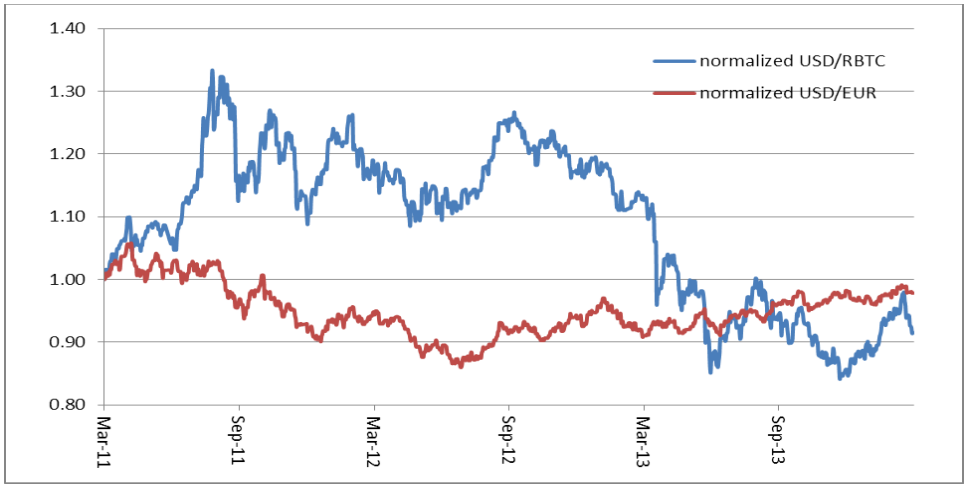

Figure 18: Normalized USD/EUR and USD/RBTC in the case of gold index parity.

Daily Returns 29-mar-2011 / 29-mar-2014	USD/RBTC	USD/BTC
Mean	0.00%	0.79%
Standard deviation	1.04%	6.30%
Volatility	19.82%	120.27%
Skewness	-123.13%	24.53%
Excess kurtosis	998.63%	842.33%
Minimum return	-9.35%	-46.16%
Maximum return	4.71%	36.93%
Value-at-Risk at 99% confidence	3.11%	17.76%
Expected Shortfall at 99% confidence	4.98%	25.66%

Table 4: Exchange rate daily returns statistics in the case of gold index parity. Annualized volatility is √365 times the standard deviation.

Section 5: About a new unfamiliar paradigm.

It could be now too late, the skeptical reader might have not made it so far, but comments are in order about this unfamiliar scenario: the idea of a wallet changing its number of coins without any direct inflows or outflows is surely an uncomfortable one. Currency volatility will not be discovered by price volatility anymore but by volatility of money amount instead: this is a historical, cultural, and psychological change of paradigm that will require some effort and time to be accepted. Early feedbacks to this paper have already proved that accepting this new paradigm will be one of the most controversial points.

5.1: Unit of Account Effectiveness.

If one considers the wallet as the ownership of a given quantity of that special good called money, it becomes less unnatural to accept that any change in the value of money should impact on money itself instead of (the prices of) other goods. **Even if prices are relative measure of value, money is a special good whose value changes are better not offloaded to other goods**: if the yardstick used to measure prices changes its length, it is less controversial to fix the yardstick, instead of updating the measured lengths of all other objects. Notwithstanding the familiarity of the price impact we are used to, impacting on wallets, i.e. adjusting the money amount instead of prices, is the least irrational and disjointed means of adapting to changes in the value of money. This is the only way to avoid that money, being the very special good used as unit measure of value, improperly damages the whole price system because of its own value volatility.

5.2: (Un)Fairness of the (Current) Elastic Supply of (Fiat) Money.

The proposed elastic supply monetary rule is not only much more effective than anything ever used by central bankers, but also dramatically fairer than anything ever tried by whatever monetary authority. As a matter of fact adjusting the monetary base is no novelty at all, as it is exactly what every central bank has been doing for every fiat currency. **The variability of the number of fiat currency units in our wallets does already happen, *mutatis mutandis* and with the aggravation of severe unfairness, even if the man on the street is not aware**:

- In case of deflationary decreasing prices the fiat currency monetary base is increased, usually according to the quite common central bank 2% annual inflation target. Any existing fiat currency unit accordingly diminishes its value pushing prices up. The newly issued fiat currency units are not proportionally distributed to all the fiat currency owners. In other words, the monetary policy action of increasing the currency stock deprives *every* wallet of part of its value and the resulting confiscated wealth is discretionary governed by central banks. **The reason why most of the wallets do not experience any increase in the number of currency units is just because they are denied of the *pro-quota* increase they would deserve**. Discussing further how this confiscated wealth is then used by banks to sustain government debts is outside the scope of this paper; the resulting effect of government debts having steadfastly increased in the last 45 years to the current astronomical levels will briefly be touched upon later in the paper.
- A converse kind of unfair rebasing happens for deflationary actions, when the fiat monetary base is reduced to counteract inflationary increasing prices. To understand this point the reader must be familiar with how the outstanding amount of money is increased by the central banks mainly encouraging the creation of new loans (McLeavy, et al. 2014). The money loaned by commercial

banks is effectively newly issued money and paying back the loan destroys that money. In case of increasing prices, the outstanding currency has to be shrunk so as to increase the value of the remaining money relative to the prices of other goods, thus pushing prices back down. Central banks cannot reach every wallet and subtract *pro-quota* the currency units to be destroyed: they achieve this effect mainly by increasing interest rates. On one hand, old loans and mortgages keep being paid back destroying money: this happens at higher cost because of the more valuable currency and it is exacerbated in case of floating interest rate indexation. On the other hand, the creation of new loans and mortgages slows because of their higher cost. So the net decrease in money outstanding amount is obtained with damage to those who have borrowed, and primarily affects those who would need to borrow, denting their wallets with higher interest rate costs or even preventing them from effectively borrowing for living expenses, investments, etc. This clearly hurts growth, while the wallets of those who are not in need to borrow are unaffected. The monetary policy action is again unfair: **the general loss of value experienced by money,** which pertain to each and every wallet and **whose burden should be carried by everyone *pro-quota*, is dumped instead into only a subset of wallets**.

- Rogoff (2014) advocates phasing out paper currency to allow for negative interest rates: *it is precisely the existence of paper currency that makes it difficult for central banks to take policy interest rates much below zero, a limitation that seems to have become increasingly relevant during this century […] today's environment of low and stable inflation rates has drastically pushed down the general level of interest rates. The low overall level, combined with the zero bound, means that central banks cannot cut interest rates nearly as much as they might like in response to large deflationary shocks. If all central bank liabilities were electronic, paying a negative interest on reserves (basically charging a fee) would be trivial. But as long as central banks stand ready to convert electronic deposits to zero-interest paper currency in unlimited amounts, it suddenly becomes very hard to push interest rates below levels of, say, -0.25% to -0.50%, certainly not on a sustained basis. Hoarding cash may be inconvenient and risky, but if rates become too negative, it becomes worth it.* Here the reader, so far uncomfortable with the proposal of an automated non-discretionary monetary rule which could reduce the number of currency units in his wallet, is presented with the much scarier scenario of a central bank able to perform the same action in a complete discretionary way. Furthermore, the reciprocal action of fair distribution of money in case of expansionary actions in not even considered. To top this all, Rogoff wonders: *even if there is a good case for allowing the central bank to pay a significant negative interest rate to fight a large deflationary shock, what is to stop a government from using negative interest rates as a wealth tax in normal times?* As Italians learned in 1992 when a one-time bank deposit levy of 6‰ was enforced, and more recently Cypriots

learned in 2013 when EU and IMF agreed on a one-time bank deposit levy of 6.7%, the answer can only be a resounding *nothing and no one will stop it!*

5.3: Preserving wallet purchasing power.

Price stability, i.e. preserving the value of a currency unit, has always been the Holy Grail of monetary theory, and Hayek Money has a chance to limit its elusiveness. Unfortunately the more ambitious goal of preserving the value of a wallet is a chimera, and it deserves to be clearly appreciated as airy-fairy wish. The money supply rebasing is only successful at keeping constant the purchasing power of one currency unit; keeping constant the purchasing power of a wallet is not possible. For the sake of holding reserve for future payments it would be nice indeed to be able to save a given amount of money and rest assured that its value would be maintained forever: unfortunately money is just a good, not the ultimate saving gift from a deity. **Supply and demand dictates the value of money relative to other goods: nothing can be done to escape the unavoidable debasement associated with decreasing demand for money**. Whatever the reason for the relative demand of money to decrease, the value of all wallets diminishes accordingly and can buy less goods and services. This is just a hard matter of fact. To keep the amount of money unchanged and having to deal with increased prices[37] is equivalent to having a reduced amount of money and stable prices.

As there is no way to effectively fix the value of the money unit without compensating every change in demand with a mirrored change in supply, **spreading the change in purchasing power of the monetary base across a larger or smaller money stock can salvage the value of the currency unit, but only that**. Even the fiat currency buying/selling defense that can be provided by central banks cannot escape this constraint: it tries to limit the monetary impact to just the large central bank wallet but its effectiveness is limited by the expendable resources.

Nonetheless there is good news for the implausible wish of stable wallet purchasing power: the more stable the prices, the more stable the demand for a currency, and this will lead to low wallet value volatility. Moreover, before reaching stability, Hayek Money cryptocurrency will be highly in demand, leading to an increase of the number of currency units in every reserve of money: the fundamental deflation effect of increased cryptocurrency adoption and gradual exit from the fiat currency world will make early cryptocurrency adopters progressively richer.

5.4: Reducing Volatility.

Even Hayek Money, possibly the best money ever devised, cannot eradicate the volatility of the value of money: volatility is an intrinsic property of demand dynamics.

[37] Prices cannot be artificially fixed in spite of supply/demand: this is a blessing for which we should thank God, as humans would otherwise surely instigate well intentioned disasters as epitomized by the communist social planning catastrophe.

The variation of demand over time cannot be artificially governed: nobody can alter this matter of fact and oppose the resulting change in value.

However, rebasing the monetary stock supply can absorb the volatility impact due to variable money demand, steering its instability effect away from prices and toward wallet amounts instead [Table 3][Figure 14]. Then the only remaining volatility would just be the variability of value of the reference commodity basket. The relevance of the volatility reduction obtained with elastic supply of money should not be underestimated in its feedback effect:

- As long as the currency unit keeps constant value, a sudden large variation of its demand will become unlikely, and rebasing the monetary base less intense;
- The noise due to the variable adoption rate and the need to resort to fiat currencies will be progressively reduced, providing another subsiding contribution to the reduction of monetary base adjustments;
- Moreover, the availability of stable prices will surely help, *ceteris paribus*, the growth of the economy using that given money.

5.5: Adaptation to the New Paradigm.

Most people use money without ever wondering why paper of no intrinsic worth is valuable. Entire populations have suffered for monetary abuses which have destroyed the value of their money, without really understanding how it happened. It might happen that a vast majority for some time will be so averse to owning money whose amount keeps changing, to forfeit the amount growth opportunity of Hayek Money cryptocurrencies; they might prefer to retain fiat currencies whose value they keep being robbed of, instead of adopting new amount-changing value-preserving money. It will be matter of educating people: there is some irony that it will be the introduction of the best money ever devised to carry the burden of teaching people about what money is, freeing them from centuries of money misappropriation and manipulations. The mission is not about persuading hopeless stubborn people, but saving the ill-informed ones.

The good news is that partial relief will soften the awkwardness of being introduced to the new paradigm of changing amount wallets:

- The huge appreciation of cryptocurrency that we have experienced in the last years will become orders of magnitude higher in the future because of (Hayek Money) cryptocurrency adoption growth. The resultant deflation will increase the value of crypto-money. So the very pleasant effect of a continuously increasing number of coins will have the honor of introducing people to variable amount wallets;
- Early Hayek Money adopters will enjoy impressive growth of their wealth. Many others will just follow the pioneers because of emulation, without further worries about the subtleties of money definition: all things considered, the

followers will just keep using money without a full appreciation of what money is and why Hayek Money is better than the previous alternative.

5.6: Reintroducing some unfairness to reduce awkwardness.

There might be ways to ease the edginess of changing amount wallets: e.g. transaction fees proportional to transaction amounts could be destroyed to reduce the monetary base[38]. This tightening bias could even be dynamically adapted to the urgency of monetary stock reduction: the percentage transaction fee might increase with the severity of price inflation. The suggested approach would have the merit of being countercyclical: increasing the percentage transaction fee according to the price inflation magnitude would slow non-essential expenditures, driving prices down and so reducing the need for contractionary measure.

This strategy could be improved if the paid fees would be frozen[39] instead of destroyed. The transaction percentage fee could still be increasing with the price inflation severity, but the fee amount would be just frozen as unspendable for a given number of blocks, and only destroyed after that period of time. If in the meantime an expansionary policy should be required, the frozen money would be unfrozen and not destroyed anymore. The frozen coins should not be regarded as potential first loss protection, as they are effectively immediately destroyed: they are instead the first coins candidate to be minted in the next coinage.

Another incremental twist might be to never destroy money, just to freeze it indefinitively until eventually unfrozen by a new expansionary cycle: in this case freezing would be equivalent to destroying, but remembering those affected by contractionary policy in order to proportionally compensate them if and when expansionary policy should prevail again.

The transaction fee mechanism being a benign countercyclical distortion of money dynamics, its fine tuning might prove to be quite powerful in reducing the direct effect on the wallets of contractionary monetary measures. Nonetheless the attentive reader will not miss how this reduction has been paid in terms of equity: money not used in transactions is unaffected by tightening monetary action. Fairness has been partially given up to fight awkwardness.

Section 6: Monetary rule implementation guidelines.

The goal of this section is to provide the basic elements of how the monetary rule might be implemented on the block chain. Of course most of these suggestions could

[38] I am in debt for this suggestion to Robert Sams and Giacomo Zucco.
[39] Even in the current Bitcoin protocol the concept of frozen money is present: the block reward paid to the miner for having successfully chained a block cannot be spent for the next 100 blocks. Indeed the just chained block could become orphan because of a competing longer chain: the reward temporary freezing avoids the chance of spending money which might not exist later.

and will be refined before actually being implemented in a new version of the Bitcoin protocol. As such they are provided here as the basis for a community driven analysis that will be carried out as open process in the coming months at www.hayekmoney.org. It will have to be investigated if the rebasing process could be implemented creating a new kind of meta-coin, with bitcoin as basecoin and the rebased-bitcoin as stablecoin. The advantage of this approach would be to leave bitcoin untouched, while storing the rebasing index in the available block chain data extensions, or in a new complementary block chain. Alternatively, a Bitcoin protocol change would be needed, or a protocol fork will be used for a new cryptocurrency.

Furthermore, as the historically realized variance of bitcoin is not needed anymore for simulations, in the following generic *basecoin* (non-rebased currency unit) and *stablecoin* (rebased currency unit) will be used. A caveat is needed: it might be sensible to conceal basecoin from the non-technical end user, so that only the stablecoin would be openly used and referred to. The basecoin should be considered just a hidden implementation detail. Similarly, the frozen amounts from transaction fees should not confuse the end-user experience, just being eventually released if and when possible.

Our attention will now be devoted to four guidelines: observation of commodity prices, the reaction lag of the rebasing process, the interaction between transactions and the rebasing process, and the commodity price index maintenance.

6.1: Observation of Commodity Prices.

The big challenge for the whole monetary policy is how to measure the commodity stablecoin prices in a decentralized way, with no central authority and without intrinsic dependencies from exchanges.

In a future world, when the block chain technology will have permeated and transmuted the way people usually transact, the commodity stablecoin prices will be simply read off other block chains registering the (ownership and) transactions of specific goods included in the price index. While this is very likely the final point of arrival, unfortunately petroleums, grains, and metals are not traded on a block chain yet and a robust process must be devised for the time being.

Miners are the natural candidates to observe commodity prices and report them on the block chain while validating each block. At the end of day *one* the close prices are observed on the financial markets, then every block validated between 0:00:00 UTC and 23:59:59 UTC of day *two* should include those close prices. Referring to the previous day, close prices introduce a one day lag but ensure the ability to have about 144 independent observations[40] of the same prices, so that averaging them is robust to the presence of spurious outliers. The first block in day *three* would then provide the average of the prices observed in the blocks of day *two*, i.e. it would fix the new *target*

[40] That is six observations per hour times twenty-four hours.

rebasing index. In the next subsection it will be clear how the rebasing process will actually use this index.

The proposed *observation cycle* does not really need to be one day[41], it could be any congruent amount of time, e.g. six hours, without loss of generality; the key point here is the ability to collect multiple observations of the same prices, without relying on a solitary single observation (or even few observations) which could be distortionary and easily manipulated. A continuously-rebased coin would be of course more appealing, avoiding *daily* operation in favor of the only natural time interval that makes sense for a cryptocurrency: the block validation unit interval. In the next subsection various means to react in a quicker and continuous way will be presented; for the time being, in absence of smarter proposals, some reaction lag is necessary to aggregate an observation *consensus average*.

The averaging process should discard a lower and higher percentile (e.g. 25%) of observations before calculating the consensus average of the remaining observation and fixing the new target rebasing index. All miners whose observed prices have been arbitrarily near the consensus average (e.g. below 2% discrepancy), i.e. inside the *rewarding interval*, share the extra consensus reward in addition to whatever they already got for the block validations in the previous day. Notice that in the case of identical observations, as it is likely to expect in regular times, all miners would share the consensus reward, as the discarded part would have no effect on the average.

All miners would have an incentive to provide fair observations, because any observation distant from the consensus average will not be rewarded. In regular times reaching consensus would not be an issue: public debate would surely designate the Chicago Mercantile Exchange USD close prices as the reference ones, and the conversion of these prices in stablecoin would be performed using the weighted close price of some reference USD/stablecoin exchange or even some average between multiple exchanges. Reference commodity prices manipulation, according to anything other than the prevailing consensus, would be financially disadvantageous.

The interesting point is that this consensus average would be reached even in turbulent times, and not just in the case of conflicting opinions about which exchange has to be considered as reference. Even if radical dramatic events are assumed as possible (CME shut down with no replacement, legal ban of stablecoin, censorship of public debate about reference commodity prices, etc.) the consensus process would be resilient. This strong confidence is based on what is known as *focal point* or *Schelling point* in game theory: even in absence of communication, miners have incentives to quote *focal* prices they assume will be the common consensus. The Nobel Prize-winning economist Schelling (1960) describes: "*focal point[s] for each person's expectation of what the other expects him to expect to be expected to do*". The example

[41] Even if the one day cycle is the most natural fit to the daily close price available from regular exchanges like the Chicago Mercantile Exchange.

of two people unable to communicate is often used: urged to select a square among a series of identical squares and rewarded only if they select the same one, they will look for a choice that might seem more natural, special, or relevant; if among these otherwise identical squares only one is red, then that is the one that will be chosen by both.

In our case, focal prices for the commodities included in the commodity price index are the unbiased prices observed for real in the free market; the red square everybody is incentivized to indicate as reference price is the true unadulterated observed price[42]. Without the need of explicit concert, miners' observations will gravitate toward the true observed value as the choice most likely to maximize the chance of being rewarded. Even in the absence of reliable exchanges the resilience of the consensus process would probably be stretched so far as to become itself a kind of distributed brokerage, a peer-to-peer distributed register of observed prices. Intrinsically different observations from distant black markets in Tokyo, Moscow, London, Cairo, New York, Melbourne, São Paulo, etc. would be averaged on the block chain providing a feedback effect on the prices available in those markets. The block chain would become a transparent board of prices maintained by miners in their *broker* role.

Given the public nature of the blockchain, miners are not really isolated from each other: they are always able to watch the consensus process as it progressively consolidates by the accumulation of observations. This could lead later observations to gravitate toward the average of the first ones, in order to maximize the reward likelihood. Anyway, this blockchain-endogenous effect would happen under the strict control of the miners' exogenous preference for an appreciating or devaluating currency. Here proof-of-stake becomes of paramount importance: the participation to the consensus process should be proportional to the stake in the monetary stock, so that any manipulation carried out by the 51% of the stakeholders would not really be manipulation, but instead legitimate maintenance of their own money by the majority of the money stakeholders.

The reached consensus average would provide feedback to the black market prices, as there would be pressure for prices distant from the blockchain reference level to adjust. Nonetheless, free market forces would be at play here: in case of persistent divergence between blockchain reference and black market prices, the distance would exacerbate because of reciprocal distrust, until the weaker party succumbed to the economically sounder one. All players would be incentivized not to manipulate the monetary rule in order to preserve its efficiency and avoid undermining the currency usefulness and value.

The consensus average process could even happen on a dedicated side-blockchain. If miners validate transactions on the main block chain with proof-of-work and are

[42] Robert Sams pointed out that *Prediction Market* might be a promising alternative scheme: see Paul Sztorc's TruthCoin at https://github.com/psztorc/Truthcoin.

compensated with new stablecoins (or basecoins), *brokers* could participate to the consensus average process on a side-blockchain with basecoin proof-of-stake and would be compensated with some monetary privilege, e.g. lower transaction fees, higher priority in releasing back into circulation frozen transaction fees, etc.

6.2: Commodity Price Index Maintenance.

Here we listen again to Hayek's lesson: *Changes in the importance of the commodities, the volume in which they were traded, and the relative stability or sensitivity of their prices (especially the degree to which they were determined competitively or not) might suggest alterations to make the currency more popular.* An extreme example would be a major breakthrough for green energy that would make petroleum useless.

From the protocol point of view our Brent/Wheat commodity price index is just composed of two numbers provided by miners, and these numbers are not technically constrained in any way. E.g.: in the case of a major Green-Energy Alternative breakthrough, Brent could be removed or replaced with the miners' agreement. Even more: actually nothing could ever stop the *majority* of miners from changing the commodity price index definition. This is another crucially strong argument in favor of proof-of-stake: in this case the miners' prerogative to change the index is not the abuse of an oligopolistic power anymore, but the proper right of the majority to rule about its own money.

Anyway reaching a majority agreement, especially without a facilitating central authority, might be hard and controversial, if possible at all. A more realistic and fair approach would be to create a *new-stablecoin* cryptocurrency using a new index, offering a limited-time chance to *burn* old-stablecoin and receive new-stablecoin in return. Burning is a well-defined concept and consists in sending money to a wallet which technically cannot spend it, i.e. a wallet address whose script always returns FALSE instead of checking the validity of private key signature and returning TRUE if money can be spent. This *proof-of-burn*[43] allows bootstrapping one cryptocurrency off another, smoothing the transition. Nobody would be forced to accept the new commodity price index, nobody would be forced to burn old-stablecoins at the switchover, and only market forces would select the prevailing currency and determine the relative exchange values.

6.3: Rebasing Process Reaction Blocks.

The target rebasing index, obtained through the consensus process described in subsection 6.1, does not need to be applied at once, with instantaneous jump in the monetary stock of stablecoin. Instead it is spread over multiple smaller increments, one per block: at every block, the distance between the *current rebasing index* and the target rebasing index is reduced by a fractional amount, i.e. the current *index adjustment*. To hasten this process is unnecessary, and Hayek (1990) again provides

[43] en.bitcoin.it/wiki/Proof_of_burn

his support here: *From the point of view of the issuing banks it would probably be desirable to allow a small, previously-announced, tolerance or standard of deviation in either direction. For in that event, and so long as a bank demonstrated its power and resolution to bring rates of exchange (or commodity prices in terms of its currency) promptly back to its standard, speculation would come to its aid and relieve it of the necessity to take precipitate steps to assure absolute stability.* Gradual index adjustment also provides the additional benefit of minimizing the jarring effects of opposite rebasing adjustments canceling each other: spurious temporary market price spikes would have a reduced impact on the monetary stock.

If at any given moment the commodity prices were frozen, then the gap between current and target rebasing index would be completely covered in a given number of blocks: this number defines the rebasing process *reaction blocks*. At every block two rebasing indexes are available: the target rebasing index fixed some blocks ago (or in that same block if it happens to be the first block of a new day) and the current rebasing index just updated in that block. The distance between target and current rebasing index would have been just reduced by the miner validating that block: this is a non-arbitrary update assuming the number of reaction blocks is fixed by the protocol. A third rebasing index is implicitly available in the previous day close commodity prices reported in that block, but this *forecast rebasing index* is not fixed yet and can only be estimated looking at the block prices contributed so far.

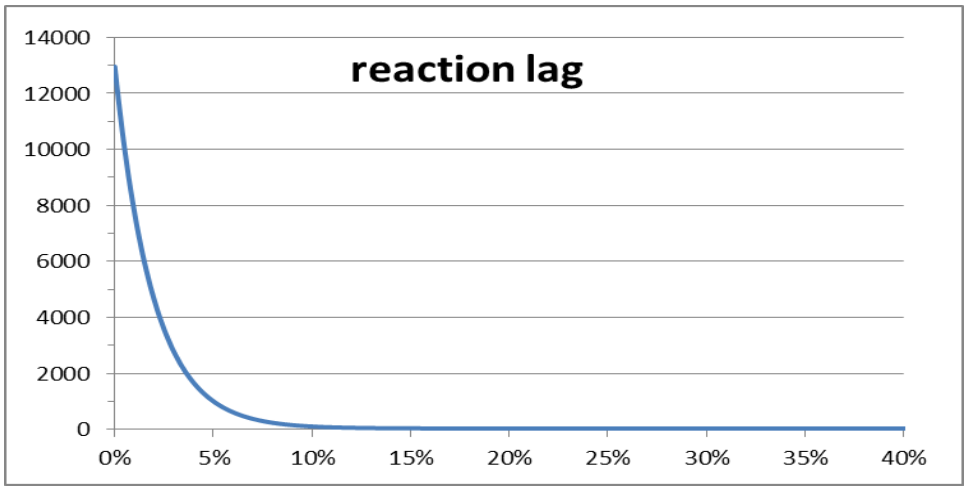

Figure 19: Reaction blocks as function of the distance between current and target rebasing index.

The number of reaction blocks should be a function of the distance between the current and target rebasing indexes. Small distances would be better handled with a high number of reaction blocks: ideally if this small distance does not increase over time it should not affect the monetary stock, as chances are high it might be just noise that will be cancelled out or even reversed in the successive days. On the contrary, large distances between current and target rebasing indexes should be dealt with quickly, to avoid losing confidence in price stability. One possible reaction blocks function is an exponentially decaying function $f(x) = \alpha e^{-\gamma x} + \delta$, where $x = \frac{|current - target|}{target}$

is the absolute value of the percentage ratio between the distance and the target index, δ is the number of reaction blocks for large distances, $\alpha + \delta$ is the number of reaction blocks for small distances, and γ controls the speed of transition between $\alpha + \delta$ and δ. Assuming 36 reaction blocks (a quarter of day) for large distances, 12924 blocks (ninety days) for small distances, and regulating the speed so that a 5% distance between current and target rebasing index is covered in 1008 blocks (one week) yields the function in [Figure 19].

A threshold might be added so that for distances below the threshold (e.g. 0.1%) no rebasing is performed. Of course a more radical choice of having a reaction lag of just one block, if deemed appropriate, is technically feasible with the proposed approach.

Other functions for the number of reaction blocks could be devised, especially using the distance between the forecast and current indexes instead of the one between target and current indexes. In this case the protocol would be quicker in reacting, starting to adjust the monetary stock to the previous day close prices immediately. In any case, a more sophisticated approach would be required to calibrate the reaction lag taking into account the higher uncertainty of the early forecasts based only on few observations compared to later ones. Without going into further details here, it would be enough if the index adjustment performed in a block were to be determined as a weighted average of the adjustments implied by the two alternative distances $\frac{|current-forecast|}{forecast}$ and $\frac{|current-target|}{target}$, with increasing weight for the former as more observations are available.

Finally, if the transaction percentage fee defined in subsection 5.5 will be implemented, its interplay with the reaction lag function will have to be devised. In the case of contractionary policy, when the target rebasing index is lower than the current one, the average transaction volume will affect the percentage transaction fee level in order to broadly ensure the convergence of the current rebasing index to its target level over the appropriate number of blocks.

6.4: Transactions and Rebasing Process.

A transaction in stablecoin is distributed to the network without sure prior knowledge of which block will include it, so the current rebasing index of that block is not known in advance. Two similar issues need to be clarified.

The first is if the transaction in a block has been processed before or after the application of the block rebasing index adjustment: either option is possible, but processing before rebasing might be better from the point of view of applying an index nearer in time to when the transaction has been published to the network.

A more complex issue pertains to transactions involving amounts near or equal to the overall amount of a given wallet. By the time such a transaction is processed it might be rejected because some intermediate rebasing has altered the amount of currency in

the wallet. This occurrence is surely unpleasant, even if its awkwardness will decrease when it becomes usual to own wallets with varying amount of currency. A last resort special transaction expressed in basecoin instead of stablecoin should be available to deal with these issues, namely for sweeping an address, i.e. emptying a wallet without leaking anything behind.

Section 7: Comparisons, Alternatives, and Scenarios.

Bitcoin has empowered us with the possibility to experiment with money in *a new territory of freedom* (Nakamoto 2008b), testing different competing alternatives in order to find out what the best kind of money would be. Since the cryptocurrency appearance, alternative money has only focused on improving the technological limits of the Bitcoin protocol: while this approach has its merit, it has not added a relevant contribution to the adoption of cryptocurrencies[44]. And a vast improvement is needed on the usability front, especially about the handling of life-changing amounts of money by regular people. A vibrant community is working on these technological aspects, and solutions are just a matter of time.

In this analysis it has been made clear that the current major problem for cryptocurrencies is their price instability: this drawback has been so far neglected, suffering from the disturbing lack of the proper attention and effort such an issue deserves. A way to engineer a new generation of Hayek Money cryptocurrencies with an embedded smart monetary rule has been provided in this paper. It is not an exaggeration to say that this improvement might be the powerful catalyst triggering a major switchover from fiat to crypto currencies.

7.1: Bitcoin in the Hayek Money Landscape.

Because of its historical relevance and predominant network effect bitcoin is the natural candidate to become the first Hayek Money cryptocurrency. Anyway, bitcoin monetary rule is a legitimate one: the gold scarcity paradigm[45]. Moreover, because of its leadership, bitcoin is rightfully conservative when it comes to integrating innovations and radical changes. Of course this will have the cost of following a path similar to that followed by gold: being surpassed in adoption and value by more efficient monies, only revamping its prestigious role during crises of the dominant currencies and recessive economic cycles.

Gold's pleasant color has played a significant role in its emergence as the dominant precious metal. A similar beauty effect has been behind the usage of shells as money,

[44] The main relevant exception is the Ethereum project, www.ethereum.org, which aims for the fascinating, overly ambitious goal of implementing the blockchain 2.0, empowering the Bitcoin protocol with a cornucopia of smart richer features.

[45] This has little to do with bitcoin being *digital gold*, as someone likes to say. In common with gold bitcoin only has scarcity and inelastic supply, but they are not fungible or equivalent in any way. Digital gold should be called a Hayek Money cryptocurrency targeting parity with the gold price, as described in Section 4.4.

and we might remember the delusion we had as kids when translucent sea stones dried up losing all their charm, revealing themselves as just broken glass bottle pieces. The pleasant effect of a scarce digital currency such as bitcoin is its intellectual breakthrough and the major improvement it represents compared to previous money: chances are that this translucent brilliancy could dry up compared to the abundant supply of superior Hayek-cryptocurrencies. Scarcity in the digital world makes sense only if it provides some pleasant non-replicable effect. This is also the stigma of the alternative first generation cryptocurrencies: only very few can survive and only as long as their specific characterizations cannot be made available in an equivalent Hayek Money.

Many circles inside the Bitcoin community are unapologetically defensive when it comes to the bitcoin currency criticism. Leaving aside intellectual dishonesty, many are rightfully concerned about their investments, and adverse to any innovation that might disturb their accumulated wealth or their dream of becoming rich by virtue of ever appreciating money. Indeed it would be ideal if the Hayek Money evolution could include and leverage the existing Bitcoin community without wasting its financial investments, cultural achievements, technological skills, and brilliant protagonists. Transitional bridges from bitcoin to Hayek Money cryptocurrencies should be considered of paramount importance.

7.2: Hayek Money Concurrent Cryptocurrencies.

The tribute to Hayek in the Hayek Money definition is not just tied to the price stability idea, which has always been recognized by many before him, but to pay homage to his vision of what money is and the endorsement of concurrent currencies: Hayek Money cryptocurrencies will compete in monetary policy definition and commodity basket standard, beside technical features. Every peculiar choice will bind the long-term fate of the currency to both the proper monetary policy befitting the user needs and the selected commodity standard having a relevant role in the reference economy. These two aspects will help to root the new finance more deeply in the real trade and production economy. It must be clear that it is not needed or advocated to keep reserve of the commodities included in the price index: indeed such an action would only create unnecessary complications, operational risks, unwanted centralization, etc. Considering the main four commodities sectors, two major alternatives are worth exploring: precious metals or a mix of petroleums, grains, and industrial metals. In the author's opinion, because of their money-like properties, it might be more sensible not to combine precious metals with other kinds of commodities.

In section four two possibilities have been explored. Leveraging the allure of gold, the most brilliant (no pun intended) protagonist of the history of money, a very strong cryptocurrency could be created. Even if less alluring, the usage of petroleums, grains, and industrial metals is not less promising. The definition of baskets including these commodities could be tailor-made in order to be relevant in peculiar markets, allowing

for a more efficient allocation of resources in that reference economy. A cryptocurrency adopting such a basket would be less anti-cyclical than a gold-based one, but probably in higher demand because of its greater usefulness.

7.3: Possible Impacts of Hayek Money.

The impact of the Hayek-cryptocurrencies will be literally disruptive, especially in the rich world. The seigniorage and inflation revenues that in different ways have been channeled through retail banks to sustain public debt in all major countries are going to subside. This will cause terrible banking and government debt crises, probably leading to many defaults. On the other hand, billions of unbanked people will finally have access to a barrier-free frictionless financial system which cannot be manipulated. Even if the overall global benefits might overcome the problems, this will not make the local changes less dramatic or even apocalyptic.

The weakness of the rich world is its outstanding debt, which has increased without effective limits since the end of the convertibility of the dollar to gold. In the past, excessive debts have found the exit strategy of hyper-inflation, often obtained as a fall-out effect (or explicit goal) of war. Since wars are fortunately less frequent in recent decades in the rich world, and a low stable inflation is the target of all main central banks, these exit strategies are not practicable. Invoking or asking virtuous debt behavior from governments has been ineffective so far: debts have ballooned to unprecedented levels, and will burst because of cryptocurrencies.

Undemocratic regimes are already considering banning cryptocurrencies. This would not be easy in democratic countries, as some specific usage of cryptocurrencies could be declared illegal, but it would be hard to justify arguments to prohibit them altogether. It is not unreasonable to imagine there might be minor nations granting legal tender to some Hayek-cryptocurrency, reinforcing the implausibility of an outright embargo. The destabilizing effect of Hayek-cryptocurrencies will disrupt the value of fiat currencies leading to hyper-inflationary prices in a world where social security will be compromised by countless defaults. As a result a huge pressure will grow to declare cryptocurrencies illegal, advocating banishment and supporting explicit or stealth technologic attacks. Centralized mining pools would be an easy target to shut down, and the resulting lower hashing power network will become fragile and exposed to easier 51% attack. It seems to me that proof-of-stake might be the only long-term defense: any agent determined to shut down the network would need to buy the majority of the cryptocurrency stock, enriching cryptocurrency owners. And wealthier cryptocurrency supporters would be then encouraged to launch a new cryptocurrency. Whatever technical means might turn out to be effective, the peer-to-peer distributed approach of the Bitcoin protocol and of the Hayek Money consensus process, supported by the insight of many people around the world, will hopefully resist the pressure. On a much bigger scale we will see a replica of the entertainment industry war against copyright infringing peer-to-peer sharing: let us

pray for a quick non-controversial outcome along the lines of how the entertainment industry is currently reshaping.

Any legal opposition to cryptocurrency might significantly slow its adoption, but cannot stop the gradual devaluation of fiat currencies compared to Hayek Money. As more people realize the erosion of their legal tender money and the inversely proportional appreciation of the outlawed Hayek Money, they will be progressively lured into a cautious but continuous migration. Then by contagious imitation this attractive transition process will dramatically grow in size and speed, fostered by the high returns implied by a massive Hayek Money adoption. We live in exponential times: the early adopters will become outrageously rich and the once lonely pioneers will soon lead a real stampede that will leave behind the fiat money economy in ruins. Stability will be reached only when the monetary base is large enough to satisfy the needs of billions of people, after wild and abrupt growth.

7.4: The Fate of Fiat Currencies.

Concerned about the destiny of government money, the reader can again read Hayek: *The appearance and increasing use of the new currencies would, of course, decrease the demand for the existing national ones and, unless their volume was rapidly reduced, would lead to their depreciation. This is the process by which the unreliable currencies would gradually all be eliminated. The condition required in order that this displacement of the government money should terminate before it had entirely disappeared would be that government reformed and saw to it that the issue of its currency was regulated on the same principles as those of the competing private institutions. It is not very likely that it would succeed, because to prevent an accelerating depreciation of its currency it would have to respond to the new currencies by a rapid contraction of its own issue.*

Traditional fiat currencies could defend themselves by issuing their own digital crypto-versions, declaring their monetary policy and implementing it on their own block chain. Adopting the Hayek-cryptocurrency standards could be pragmatically effective if it is not too late to the game, but it would also severely undermine the existing financial and banking system, which might oppose the change leveraging on the founded fear of systemic instability. Assuming the opposition could be overcome[46], this approach would still rely on a third party authority and so it would not be compliant with the *zero-trust* ethic dear to many libertarians and anarchists. Even considering that it would represent a step forward in terms of transparency and accountability, the centralized block chain would grant the money authority leviathan an increased controlling power over everybody's money, a tight grip which could not be escaped.

7.5: Further Research; www.hayekmoney.org.

Many avenues of research deserve further analysis in the near future:

[46] And it would as soon as the banking and financial system realizes that Bitcoin cannot be stopped, so better strengthen the intensity of its power reducing its extension.

- How effective would it be to destroy transaction fee money as contractionary monetary rule? The awkwardness of variable balance wallet does really need to be amended?
- Which other monetary rules might be worth implementing on the block chain?
- How to effectively implement the monetary rules at the Bitcoin protocol level? Should Ethereum be used instead?
- Is the consensus average process robust to attacks and manipulations? Should it be modified to make it more resilient?
- How to effectively bootstrap a new cryptocurrency? How to leverage the bitcoin growth so far? Should Hayek Money cryptocurrencies be a rebasing of bitcoin or totally alternative cryptocurrencies?
- Different communities are interested in the prices of different commodities: this will lead to multiple Hayek-cryptocurrencies defined by diverse commodity price indices representing different transnational economic systems. As aggregate prices of different collections of commodities will move differently, every Hayek-cryptocurrency will have its own diverse monetary dynamics. Such currencies will flourish and suffer together with the economic systems that originate them.
- It is not clear how to lend money in a Hayek-cryptocurrency framework. Peer-to-peer lending on a non-fractional basis, bit-shares, bit-bonds, and crowd funding will be available: however, will they scale up to the levels required by a well-functioning global economy? If this will not be the case, it is not clear yet if and how lending can be reinstated as monetary policy tool[47].

The www.hayekmoney.org website aims to stimulate and review future efforts in these directions, with a commitment to both the theory and the execution of Hayek Money cryptocurrencies.

Conclusions. About a new era

I wish I could say that what I propose is a plan for the distant future, that we can wait. […] We have not got that much time. We are now facing the likelihood of the most unpleasant political development, largely as a result of an economic policy with which we have already gone very far.

My proposal is not, as I would wish, merely a sort of standby arrangement of which I could say we must work it out intellectually to have it ready when the present system completely collapses. It is not merely an emergency plan. I think it is very urgent that it become rapidly understood that ***there is no justification in history for the existing position of a government monopoly of issuing money****. It has never been proposed on the ground that government will give us better money than anybody else could. […]*

[47] Regardless, many people will not be concerned by the issue, as they will be too busy celebrating the end of the fractional-reserve banking. Few others, the writing author included, will also celebrate the death of the deceiving concept of *risk-free* rate of interest.

I think we ought to start fairly soon, and I think we must hope that some of the more enterprising and intelligent financiers will soon begin to experiment with such a thing. The great obstacle is that it involves such great changes in the whole financial structure that, and I am saying this from the experience of many discussions, no senior banker, who understands only the present banking system, can really conceive how such a new system would work, and he would not dare to risk and experiment with it. I think we will have to count on a few younger and more flexible brains to begin and show that such a thing can be done (Hayek, 1977).

Bitcoin is now challenging generations of established political and economic theory. Even more, it is already challenging the financial infrastructure of the whole global economy. A stable Hayek-cryptocurrency will dramatically accelerate the transition to a new era. The first Hayek cryptocurrency might be bitcoin or an alternative coin; in any case the adoption of such a superior currency could be hampered but hardly halted.

Human civilization moved from barter to money thousands of years ago. We now have a chance to move from money to *good money*, i.e. from continually debased money to dynamically rebased money. This is the magnitude of the revolution made possible by the Bitcoin protocol: Hayek Money, the *good money standard* providing stable prices for a new economic era.

This enticing prospect requires responsible actions by good willing people to help smooth the transition. Hayek Money is an opportunity for increased equality, justice, and wellness, but these beneficial effects cannot be expected to be fairly spread around with no effort. The echo of T. S. Eliot's warning from the era of European totalitarianisms still sounds dramatically true:

> *They constantly try to escape*
> *From the darkness outside and within*
> *By dreaming of systems so perfect that no one will need to be good.*
> *But the man that is shall shadow*
> *The man that pretends to be.*

Bibliography.

K. Dowd (1996).
Competition and Finance

K. Dowd (2014).
New Private Monies, The Institute of Economic Affairs

T. S. Eliot (1934).
choruses from *The Rock*.

F. A. Hayek (1977).
A Free-Market Monetary System, Journal of Libertarian Studies, Volume 3, Number 1.
https://mises.org/daily/3204

F. A. Hayek (third edition 1990, first edition 1977).
Denationalisation of Money - The Argument Refined, The Institute of Economic Affairs.
mises.org/books/denationalisation.pdf

M. McLeay, A. Radia, and R. Thomas (2014).
Money in the modern economy: an introduction, Bank of England Quarterly Bulletin 2014 Q1.
bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q101.pdf
Money creation in the modern economy, Bank of England Quarterly Bulletin 2014 Q1.
bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q102.pdf

S. Nakamoto (2008).
Bitcoin: A peer-to-peer electronic cash system.
www.bitcoin.org/bitcoin.pdf

S. Nakamoto (2008).
satoshi.nakamotoinstitute.org/emails/cryptography/

K. Rogoff (2014)
Costs and benefits to phasing out paper currency, Presented at NBER Macroeconomics Annual Conference

T. C. Schelling (1960, First Edition).
The strategy of conflict. Cambridge: Harvard University Press. ISBN 0-674-84031-3.