Bitcoin and Cryptocurrencies*

Or How Inflation Will Come About in Cybermoney

Bastiaan Quast†

February 8, 2014

In 2009 the online currency **Bitcoin** was launched by an anonymous developer known by the pseudonym Satoshi Nakamoto. The protocol was based on a 2008 white paper by the same author (Nakamoto 2008), and every aspect of it is public and open source. This quickly led to the launching of several alternative online currencies, based on the Bitcoin protocol. These currencies have recently become known as **cryptocurrencies**.

There are some key benefits to cryptocurrencies, a few of which I will mention here. Firstly, the system is self-regulating, meaning that no government or institution controls it. For the user that means that their holdings cannot be used as a policy instrument. Conventional fiat currencies are owned by a government, which means that they can be used to e.g. stimulate economic growth by printing extra money, which lessens the value of individuals holdings.

Secondly, users control their own holdings on their own computer, which eliminates the need for a bank. This brings the advantage that users are not dependent on open hours, waiting lines, or e-banking websites, it also means no fees. Additionally a user's holdings cannot be wiped out by his or her bank bankrupting after speculative investing or something of that sort.

*Centre for Finance and Developent Student Working Paper

†PhD Candidate, The Graduate Institute, Geneva; Research Assistant, Centre for Finance and Development, Geneva; bastiaan.quast@graduateinstitute.ch

Thirdly, transactions are as easy, instant, and costless as sending an email. Bitcoin exists online digitally, which means that there is no physical counterpart that needs to be moved, such as with gold, or paper money. Additionally, it is equally valid across countries, which means that there is no need to exchange it. This makes Bitcoin an ideal mechanism for remittances, which nowadays can cost as much as 10 percent. Additionally no government can apply capital restrictions on these remittances.

Lastly, the instant nature of transactions means it is well suited for online retailing. Credit card transactions seem instant, but in fact are not. A significant percentage is in fact reversed after initial clearance. This is very costly for retailers, this often occurs after packaging of shipping has started.

From a technical perspective there are many innovative features to cryptocurrencies, and I will begin by highlighting the key ones. After this I will focus on two economic aspects, which have been thought to be problematic, namely the lack of inflation and also socially wasteful mining. Although these aspects might seem unrelated, they have a common solution.

Bitcoin is a confusing term. It is both a monetary unit of denomination, such as Swiss franc, euro, or pound sterling, as well as, a monetary system as a whole, including the protocol, the network, and the software. To distinguish between the two, the system **Bitcoin** is written with a capital letter B, the monetary unit is **bitcoin**, with a small letter b.

Bitcoin is built from the ground up to be decentralised and anonymous. All software is open source and publicly available. Anybody can perform any function within the network (user or node), there is no central or essential node, there is redundancy in every aspect.

The essential principle is that every user has a piece of software on their computer, a **wallet**, which contains a set of **public addresses** (like bank account numbers), each address is mathematically linked with a **private key** (like a password). Using this secret key, users can create a digital **signature**, to prove that they are the owner of an address. This signature, together with a transaction is sent to a **bitcoin miner**. The miner is a node in the network, which verifies that the address and signature are linked, after which the transaction is recorded in the public ledger, or **blockchain** and disseminated throughout the network.

There are a number of other features which are important to highlight. Bitcoins are created through a process called **mining**, this is a computationally intensive process used as the mechanism for transaction verification. The Bitcoins created as a reward for mining becomes incrementally smaller,

until finally becoming zero. This is predicted to be around the year 2140, and at that point around 21 million bitcoins will have been created. There will never be more bitcoins in the system. Furthermore, bitcoins will be lost if private keys are lost, these will never be recovered. The system is thus strictly deflationary. To keep transactions of every size possible, bitcoins are highly granular, every bitcoin can be divided into a hundred million **satoshi** (named after the pseudonym of the creator).

As the value of bitcoin goes up, more people will choose to engage in the lucrative mining. As extra computational power comes in, the difficulty of mining automatically goes up, which means more computing power is used for the same transactions. This is necessary to safeguard the integrity of the network.

Having established the key features of the Bitcoin system, we will now focus on two often heard economic concerns about the Bitcoin system. Namely the issue of deflation and the issue of socially wasteful mining.

As mentioned above, there will only ever be around 21 million bitcoins, and some will be lost, this makes the system deflationary, which is troubling to economists. Deflation provides a disincentive to spend, causing economic slowdown (see e.g. Fisher 1933). Since deflation causes the price of products to fall, it incentivises people to save ans spend later. Additionally, these savings are not invested properly, since deflation simultaneously provides a disincentive for borrowers, by making future paybacks more expensive, raising the effective interest rate.

The second issue is the value of the mining process. As described above, the process of mining is the solving of computational problems, in order to secure the integrity of the Bitcoin network. However, the actual social value of the arithmetic solution itself is zero, since it has no application other than Bitcoin integrity. As the number of bitcoins is limited, and more money is invested in it, the value can only increase. The increase in value will make it more lucrative to engage in bitcoin mining, which means more computational power will be devoted to this. To keep the system secure in face of this extra computing power, the difficulty goes up. However, if the extra power had not come in, this would not have been necessary. The extra computers which engage in bitcoin mining thus do not add any social value.

It has to be noted, that the bar for social value is being set very high. Extraction, storage, and transfer of value is a resource intensive enterprise. Consider the gold mining industry (note, this is the origin of the term **bitcoin mining**). The extraction of gold is a very resource intensive, dangerous, and

pollutive process. After the extraction, purification, and molding, most gold is stored highly guarded in vaults. Finally then, gold can be utilised to conduct transactions, which involves shipping bars of gold across the ocean under maximum security, only to be stored in another highly protected vault, on arrival (see e.g. Friedman and Schwartz 1967).

The solution for both these lies in the multiplicity of cryptocurrencies. As mentioned above, every aspect of Bitcoin is open and publicly accessible, it is therefore relatively easy to start an alternative Bitcoin, and this has been done. There are in fact many currencies based on the Bitcoin protocol, collectively referred to as cryptocurrencies. It is relatively easy and cheap to construct a number cryptocurrency, whereby the number of available coins can be set by the creator. The most popular alternative to Bitcoin is called Litecoin, its main difference is that it processes transactions faster, and the total number of coins is four times as high. Aside Litecoin, there are many other alternative cryptocurrencies, most of which never gain momentum and the value of which remains only trivially above zero. However, a significant number does succeed. The momentum mechanism could perhaps best be compared with a positive variation on currency attacks (Obstfeld 1986, 1995, 1996). Unlike the creation of new coins in an existing cryptocurrency, the creation of new cryptocurrencies is relatively cheap.

The key point to observe here, is that cryptocurrencies do have value, but only as a transaction mechanism. Hereby the biggest bottleneck is probably the number of cryptocurrencies that merchants are willing the accept simultaneously. However, due to their similarity, it is very straightforward for e.g. merchants to accept multiple currencies. When we combine the value with the relatively cost-less creation of cryptocurrencies, we see an equilibrium in the number of cryptocurrencies that is far higher than in the current situation.

Inflation is impossible within the Bitcoin network, as well as within most other cryptocurrencies. However, inflation in the cryptocurrency economy is still possible, through an expansion the number of cryptocurrencies.

It is also through this multiplicity that wasteful mining will be limited. As noted above, cryptocurrencies have value, because they are effective mechanisms for transactions. However, this is the only source of value. If a cryptocurrency becomes too expensive (which causes excessive mining), a new, lower valued, cryptocurrency will arise. Since the value of this currency is lower, but it is equally effective in transactions, value will flow out of the overvalued cryptocurrency and into the undervalued one. This lowers the

value of the overvalued cryptocurrency, and less mining will be done here, reducing the waste.

In conclusion, cryptocurrencies such as Bitcoin have an enormous potential as a transaction mechanism, giving users control of their own holdings and making transactions instant and costs negligible. Two commonly heard issues with cryptocurrencies are deflation and wasteful mining. It can be shown that these issues are not pervasive, when the cryptocurrency economy as a whole is considered. Cryptocurrencies derive their value only from being an efficient transaction mechanism, if they appear to become overvalued (causing excessive mining), other cryptocurrencies will arise. This will increase the total number of cryptocoins (between all cryptocurrencies), which will drive down the price, and limit excessive mining.

References

Fisher, Irving. 1933. "The debt-deflation theory of great depressions." *Econometrica: Journal of the Econometric Society:*337–357.

Friedman, Milton, and Anna Jacobson Schwartz. 1967. *A monetary history of the United States, 1867-1960.* Princeton University Press.

Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." `http://bitcoin.org/bitcoin.pdf`.

Obstfeld, Maurice. 1986. "Rational and self-fulfilling balance-of-payments crises."

———. 1995. *The logic of currency crises.* Springer.

———. 1996. "Models of currency crises with self-fulfilling features." *European economic review* 40 (3): 1037–1047.