

The Economics of Bitcoin and Cryptocurrencies

Bastiaan Quast

April 8, 2014

The Graduate Institute

Maison de la Paix

Chemin de Eugene Rigot 2

Case Postal 136, 1211 Geneve 21

Geneva

Switzerland

About the author

Bastiaan Quast is a PhD Candidate in Development Economics at The Graduate Institute of International and Development Studies in Geneva.

He holds a Master in Quantitative Economics and Finance from the University of St. Gallen in Switzerland as well as a Bachelor in Theoretical Philosophy and a Bachelor in Economics from the University of Groningen in The Netherlands.

Contents

1	Introduction	1
I	The Basics	3
2	What is Bitcoin?	4
3	How Does Bitcoin Work?	6
4	Benefits and Drawbacks	8
	A Self-Regulating System	9
	No middlemen	9
	Virtually Instant Transactions	9
	Full Reliance on the Protocol	10
	Severe Consequences of Being Hacked	10
	Increased Reliance on the Internet	11

<i>CONTENTS</i>	iv
5 Why use Bitcoin?	12
6 Is Bitcoin Money?	14
Legal Tender	16
7 Is Bitcoin Legal?	18
Currency or Financial Asset?	18
 II The Economics	 20
8 Cryptocurrency competition: Hayek's Paradise	21
Faith in Markets	23
9 Cryptocurrencies and Inflation	24
10 Bimetallism in Bitcoin and Litecoin?	26
11 Perfect Foresight	28
 III The Social Value	 29
12 Is Mining Socially Wasteful?	30
13 Proof of Stake Cryptocurrencies	33
Interest: Unfair free money?	33
14 Conclusion	34

<i>CONTENTS</i>	v
Bibliography	36
Glossary	37

Chapter 1

Introduction

In 2009 the online currency **Bitcoin** was launched by an anonymous developer known by the pseudonym Satoshi Nakamoto . Initially the project remained fairly low key, having only a small number of geeks actively participating. However, in 2013 Bitcoin quickly became a mainstream phenomenon as it was reported on in the mainstream media such as by The BBC, The Economist, Time Magaine, and many more. This increased attention created a surge in the uptake of Bitcoin both as an investment as well as transaction mechanism. However, Bitcoin also has a dark side, being initially used mostly to purchase illicit goods on online marketplaces such Silk Road, The , websites that are generally only available through the dark web. However, the rise in popular attention has also brought the attention of regulators, which has caused many of the illegal marketplaces

to be taken offline, as well as introduced a range of fiscal regulation, dealing with bitcoin. This book provides a laymens introduction to the basic principles of Bitcoin and other online currencies, as well as discuss how this new phenomenon can be viewed from an economic perspective, and what that would mean for the development of such systems.

The Bitcoin system was based on a 2008 white paper by the same author (Nakamoto 2008).

Besides the fact that Bitcoin exist only digitally, its defining characteristics are decentralisation and openness. 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. A currency based on cryptography, such as Bitcoin, is know as a cryptocurrency .

Cryptocurrencies come with an extensive new terminology, for reference, a glossary is provided in the back of the book.

Part I

The Basics

Chapter 2

What is Bitcoin?

A short answer is that it is an online anonymous currency which is not controlled by a government or any single entity. However, from a technical as well as a from a social perspective there are many innovative features to Bitcoin . For instance, users hold his funds himself. Meaning that there is no need for a middleman, such as a bank. This prevents fees and eliminates risks associated with bank insolvency.

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

Bitcoin is a confusing term. It is both a monetary unit of denomination, such as Swiss franc, euro, or pound sterling, as

well as, the monetary system as a whole, including the protocol, the network, and all participants. To distinguish between the two, the monetary system Bitcoin is written with a capital letter B, whereas the monetary unit of account is bitcoin, is written with a small letter b. Besides these two, there is the original Bitcoin software, which is called **Bitcoin-Qt**, using this software package, or others, computer can connect to the Bitcoin network and perform transactions.

Chapter 3

How Does Bitcoin Work?

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).

Chapter 4

Benefits and Drawbacks

There are many benefits to using cryptocurrencies such as Bitcoin, some apply now other may come to be if and when cryptocurrencies become more adopted in more conventional places. Some key benefits include:

- a self-regulating system, no unexpected interventions
- no need for middlemen, such as banks
- virtually instant transactions

However, there are also a number of important drawbacks, such as:

- Extreme reliance on the Bitcoin protocol
- Severe consequences of being hacked

- Increased Reliance on the Internet

A Self-Regulating System

The Bitcoin 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.

No middlemen

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.

Virtually Instant Transactions

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.

Full Reliance on the Protocol

If there is an error in an online banking system this has the potential to create enormous problems. However, in situations like these, the banking system can always fall back on the underlying legal system. For Bitcoin there is no such fallback mechanism, if a critical error were to be found in the system, it would render not only have the potential for things to go wrong, it would eliminate the trust in the system, yet more than any other system, Bitcoin relies on this trust. Therefore a single error could wipe out the system.

Severe Consequences of Being Hacked

In any online sphere hacking has always been a problem, often it is made lucrative by stealing creditcard details or other personal information. However, when savings are stored in Bitcoin, the potential damage of being hacked is much greater than having your creditcard charged with something you did not buy, it could wipe out all of your savings.

Increased Relience on the Internet

Using Bitcoin as a payment mechanism is very effective since everything is conducted online, however, it also means that without availability of internet, everything comes to a halt. Although several methods for conducting offline transactions using Bitcoin have been devised, these methods remain very crude and often lack the ability to transfer exact amounts.

Chapter 5

Why use Bitcoin?

Having examined the technological side of Bitcoin , we can now consider some situations in which these innovations best come to fruition. In examining these situations we consider these merely from an effectiveness perspective, without regard for the morality of such possible situations, which is beyond the scope of this book.

- international remittances
- online transactions
- mobile payments
- evasion of capital controls
- evasion of taxation

- anonymous online transactions

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.

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.

Chapter 6

Is Bitcoin Money?

What is money? Sometimes it is obvious, well established currencies such as the US Dollar, the Japanese Yen or the Swiss Franc are. How about the Euro, it is not a national currency, it is not owned by a state, but rather by a collective of member state representatives. Zimbabwe owns their own currency, but this has become essentially useless. What if money is moved from one, bank account to another bank account at the same bank in the same country, through ebanking. No physical change will occur (save for a few bits on a computer driver somewhere in some remote datacentre). In some places sea shells or other rare commodities such as gold or ivory are accepted. Just as the number of possible moneys is almost infinite, so is the number of definitions, but a contemporary (pre-Bitcoin) consensus would dictate something like:

an object or entry in a record that is generally accepted as payment for goods and services and debts in a certain socio-economic context or country **CITE!!**.

We can observe a number of things from this definition. Firstly, money does not have to be an object (such as a coin), but can also be an entry in a record (such as a bank account balance). Secondly, it assumed to be generally accepted (though not universally). Thirdly, a money is not limited to only being accepted in a country, but can also be accepted in a certain context. Lastly, the existence of one money does not rule out the existence of others.

Bitcoin, the blockchain public ledger is a record. Generally accepted, but generally accepted within a certain context. Also, coexistence of moneys.

The question of whether Bitcoin is money is a complicated question, there are some standard which are used in academia to evaluate whether something is money or not. Besides this there are the issues of legal tender, and legal recognition. We will start by discussion the academic criteria for a money, after which we will look at legal tender and legal recognition. The standard criteria used in academia for analysing money are:

1. medium of exchange
2. unit of account or numéraire
3. store of value

These criteria can broadly be interpreted as follow. A medium of exchange

The criteria (1.) and (3.) are clearly fulfilled. Since cryptocurrencies are virtual goods, and multiple copies can be made, there is no degeneration over time. Furthermore, cryptocurrencies are a good medium of exchange, transactions are quick and relatively cost less. The unit of account is not a criterium that is currently well met. The volatility of cryptocurrencies vis-vis fiat currencies makes it difficult to denominate goods or services in these in cryptocurrencies. However, in that sense it is again similar to gold, which also has a highly volatile price as denoted in fiat currency.

Legal Tender

In discussion about the status of Bitcoin as money, the issue of legal tender is often heard. The discussion is somewhat misguided in the sense that legal tender is more of a means to an end, rather than a goal in its own right.

Legal tender is a rule in which a government imposes on the inhabitants of a territory, that within that territory everyone must accept the currency deemed legal tender, as payment for debt, goods, or services. Legal tender is thus a way for a government to create a market for a currency, this currency generally being the one controlled by the same government. There are many good reasons for doing so. It creates a certain level of certainty, if I want to buy something in Switzerland, I know that Swiss Francs will be a means of paying. In short, if somebody offers to pay in a currency that is legal tender in the relevant territory, the seller has to accept this.

At the time of writing, Bitcoin has not been deemed legal tender anywhere, so how problematic is this? As mentioned above, legal tender is means for government to create a market for a currency. Yet this is not the only way for a currency to establish itself. This book is being written in the city of Geneva, Switzerland. The city is almost completely surrounded by France. If we cross the French-Swiss border on one side, and continue on straight, we would cross back into France in just a few kilometers. Switzerland is not part of the European Monetary Union, nor even of the European Union, and therefore does not use the Euro, but rather the Swiss Franc as a currency. However, most of people working Geneva commute back to France. The cross border commute is so common, that nearly all places, including state owned enterprises such as the Geneva Public Transport (TPG) accept the euro. Despite the fact that the Euro is not legal tender in Geneva, it is accepted based on mutual consent. For clients it often favorable if they do not carry Swiss Francs, and retailers are awarded an exchange rate fee. Similarly, in many Latin-American countries, it is very common to accept the US Dollar as a form of payment.

Bitcoin seeks to establish itself through a popular mandate, rather than a government one. That is to say, by being a more competitive means of transaction for both the retailer and the customer. If Bitcoin is more favorable to both customer and retailer, then the customer can offer to pay in Bitcoin, and the retailer can choose to accept it. In it thus through being more interesting as a method of payment, rather than through a government mandate that Bitcoin seems to be accepted.

Chapter 7

Is Bitcoin Legal?

The short answer is yet, of course this does not mean that anything that you use Bitcoin for is legal. That is to say, it is still illegal to purchase illicit goods, or hide holdings from the tax bureau.

The legal standing of Bitcoin is different in many countries.

Currency or Financial Asset?

In the initial days of Bitcoin, especially when it was mainly used for purchasing illicit goods, some held the belief that most governments would perceive Bitcoin as a threat to their monopoly on currency and for this reason would ban it. This already being contrasted by governments of the EMU member states, who

have volutarily surrendered their monetary monopoly for what is essentially a 'foreign' currency. It turns out most government are more interested in taxing it, than they are in outlawing it. For this reason Bitcoin has in many places been classified as a financial instument. If Bitcoins are derived from mining, they are to be taxed under income tax. If Bitcoins are purchased these will be taxed as financial holdings. Again, the gold analogy holds.

In many places Bitcoin has been classified as a financial asset for purposes of taxation. This means that it is not recognised as a currency again for purposes of taxation. It several court rulings however, it has been found that Bitcoin does act as a currency. In both cases the legality of Bitcoin is underlines, however, the distinction can be relevant in some cases. For instance, in case of a bankrupcy (such as the 2014 Mt. Gox case) financial assets and currencies are treated quite differently.

Part II

The Economics

Chapter 8

Cryptocurrency competition: Hayek's Paradise

Bitcoin first become popular in several underground movements. As such it has been hailed as a major innovation in a self-identified movement known as crypto-anarchism . The main idea behind crypto-anarchism is that cryptography empowers individuals to protect themselves from harmful government meddling. It is not surprising that many of the economic principles on which Bitcoin is based, are commonly identified with government weary schools of thought in economic academia, such as the Austrian School and Monetary Economics.

CHAPTER 8. CRYPTOCURRENCY COMPETITION: HAYEK'S PARADISE

In a 1999 interview, Milton Friedman, the key proponent of Monetary Economics gave an interview to the tax-payers association of America in which he says:

The one thing that is missing -but will be invented very soon- is a reliable anonymous online e-cash

If we consider the cryptocurrency space as a whole we seem to approach the 'Decentralization of Money' as described by Friedrich Hayek (1976). Hayek describes a situation in which currencies are no longer owned by governments, but instead are owned by private companies. In this transnational currency space, the most currency or currencies most favorable to consumers would be adopted strongest and would become dominant. The situation of there being several competing cryptocurrencies in comes very close to the system as envisioned by Hayek. It also addresses some of the key criticisms of this vision, as raised for example by Milton Friedman...

PERHAPS A DISCUSSION OF GRESHAM'S LAW IN THIS CRYPTOCURRENCY COMPETITION

Although Hayek firmly believed in the self-regulating currency market, the market itself was made up of self-serving firms which owned and controlled the currencies. Cryptocurrencies go a step further, in making the currencies self-regulating and making only the individuals currency holders self-serving actors.

Faith in Markets

It is clear from the discussion of Hayek's view that denationalization of money relies on a highly effective market order. This seems problematic in several ways. Firstly, as history has shown, the fact that banks (which would be the issuers of currencies) have long run interest in acting in a certain way, does not lead to the decision makers acting in such a fashion, rather than in their own (short-run) interests, much the same as Hayek feels the government acts. Secondly, if a market for currencies is formed, the social capacity to come with any number of currencies is limited. This would thus lead to a situation where a relatively small number of currencies coexist, a situation of oligarchy would thus arise, rather than a effect market.

In recent years, there have been many economic insights into how, under a situation of information asymetry, market efficiency does not hold (STIGLITZ). In a situation where several dominant currencies have a lot of market power, it would not be hard to conceive of a situation where these companies could utilize their information advantage to extract rents from the public. We can now see how a cryptocurrency would fit this idea even more than a privately owned currency. All information about the currency is always recorded in the public ledger, and directly accessible on the internet.

Chapter 9

Cryptocurrencies and Inflation

As the value of a 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 de-

flationary, which is troubling to economists. A deflation in a currencies value 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 and 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.

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.

Chapter 10

Bimetallism in Bitcoin and Litecoin?

The situation of multiple currencies, especially in light of the gold analogy, brings to mind the idea of bimetallism, the monetary system where the currency is based not just on gold, but also on silver. The two being interchangeable at a fixed rate.

Also in the light of bimetallism, we can consider Gresham's law. Bad money drives out good. In the case of bimetallism, the most circulated specie will be the one which is currently considered to be undervalued by the official exchange rate. Meaning that if silver becomes more abundant, its relative value will decrease, and people will first spend their silver coins, before they spend their gold ones. Since exchange rates between cryptocur-

*CHAPTER 10. BIMETALLISM IN BITCOIN AND LITECOIN?*²⁷

rencies are freely floating, there is no 'bad money', since each currency is valued at market rate. Interestingly enough, the rate between Bitcoin and Litecoin seems to trade in a very narrow band, especially considering the volatility vis-a-vis fiat currencies.

However, there is a crowding out of sort. This is perhaps best compared to international currency competition. Where there is a competition for the privilege of being a reserve currency. A foreign investor can choose exchange his national fiat currency for e.g. the US Dollar or the Euro. In these markets, the good currencies drive out the bad.

Chapter 11

Perfect Foresight

In many economic models, agents expectations are modeled as being either, adaptive with respect to the past, perfectly rational, or in some extreme cases, having perfect foresight. The situation where agents exhibit perfect foresight is not intended as realistic economic modelling, as much as it is used a benchmark for economically optimal outcomes.

Bitcoin and most other cryptocurrencies have the interesting feature that the path of monetary expansion is almost perfectly predictable. The rate at which new bitcoins are mined is to a very large degree predetermined. Although the price of Bitcoin, and the associated computing power in the network cannot be predicted, the process automatically adjusts the difficulty of verification process every few minutes, leading to an extremely stable and predictable monetary growth path.

Part III

The Social Value

Chapter 12

Is Mining Socially Wasteful?

The value of the mining process is an often raised issue. 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 of verification automatically goes up.

However, had the extra power 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 moulding, 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, upon arrival (see e.g. Friedman and Schwartz 2008).

The system of fiat currencies is already much more efficient than this. There is no difficult extraction and purification process. Bank notes are printed by governments and provides with authenticity checks. Bank strike out debts against each other and only every so often is printed money actually transfered from one bank to the other. However, this is again a highly secured process of physically moving objects (in this case banknotes) from one location to the other. Often followed by a reverse transfer several days later.

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 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. 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 retailers are willing to accept simultaneously. However, due to their similarity, it is very straightforward for e.g. retailers to accept multiple currencies. When we combine the value with the relatively costless creation of cryptocurrencies, we see an equilibrium in the number of cryptocurrencies that is far higher than in the current situation.

As noted earlier, cryptocurrencies have value, because they are effective mechanisms for transactions. However, this is the only source from which their value derives. 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.

Chapter 13

Proof of Stake Cryptocurrencies

To counter the socially useless computing, the proof of stake concept has been invented.

Interest: Unfair free money?

The principles, inflation, and the consequences of less wasteful mining.

Chapter 14

Conclusion

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 cryptocurrencies (between all cryptocurrencies), which will drive down the price, and limit excessive mining.

Bibliography

- Fisher, Irving. 1933. “The debt-deflation theory of great depressions.” *Econometrica: Journal of the Econometric Society*:337–357.
- Friedman, Milton, and Anna Jacobson Schwartz. 2008. *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>.

Glossary

B

Bitcoin

The original cryptocurrency. 1, 4, 5, 12, 13, 21, 24

bitcoin

the unit of account in the Bitcoin system. 5, 7, 24

Bitcoin-Qt

The original Bitcoin software, it is still used, but many other packages have also been developed. 5

blockchain

the public ledger of the Bitcoin system, it contains all transactions ever recorded. 6

C

crypto-anarchism

A social view in which individuals are empowered and protected from an intrusive government through cryptography. 21

cryptocurrency

the generic term for online, cryptography based currencies, Bitcoin is the original cryptocurrency. 2

cryptography

techniques for secure communication. 21

D

deflation

the situations where the purchasing power of a monetary unit increases over time, generally believed to have adverse effects on the economy. 24, 25

M

miner

a computer which participates in the Bitcoin transaction verification process. 6

mining

the process of Bitcoin transaction verification, performed by a miner. 24

O

open source

software of which the source code is publicly available for inspection. 2

P

private key

the code which can be used to commit transactions. 6

S

satoshi

The atomic unit of account in the Bitcoin system, it is equal to 1/100,000,000 bitcoin, named after the Bitcoin creator Satoshi Nakamoto. 7

Satoshi Nakamoto

the pseudonym of the original Bitcoin inventor and creator. 1

signature

a digital code used to verify that the originator of a transaction owns the sending address. 6

Silk Road, The

An former online market place for mostly illicit goods, known for being the first large platform to adopt Bitcoin as a payment method. 1

W

wallet

the collection of private and public codes used to commit transactions. 6