The Economics of Bitcoin and Cryptocurrencies

Bastiaan Quast

May 8, 2014

The Graduate Institute

Mainson 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 also 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.

He has been following the Bitcoin system since 2010, and has been an active investor in Bitcoin. Unfortunately most of his Bitcoin were stolen, and finally the last were lost in the Mt.Gox bankcurpcy.

Contents

List of Figures

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 an introduction to the basic principles of Bitcoin and other online currencies, as well as discusses 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 .

In Part II we discuss the economics of Bitcoin and the economy of cryptocurrencies from the perspective of several economic schools of thought that have relevant literature on it, such as the Austrian School (chapter 10), Monetary Economics (chapter 8), and neo-Keynesianism (chapter 9).

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 relience on the Bitcoin protocol
- Severe consequences of being hacked

- Increased Relience 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 Relience on the Protocol

If there is an erro 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 potentional for things to go wrong, it would eliminate the trust in the system, yet more then any other system, Bitcoin relies on this trust. Therefore a single error could wipe out the system.

Severe Consequences of Being Hacked

In anyonline 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 fruitition. 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 Japanse 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 a gold or ivory are accepted. Just as the number of possible moneys is alsmost infiniate, so is the number of definitions, but a comptemporary (pre-Bitcoin) consensus would dictate somethink 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 existance of one money does not rule out the existance of others.

Bitcoin, the blockchain public ledger is a record. Generally accepted, but generally accepted within a certain context. Also, coexcistance 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 cryptocoins are virtual goods, and multiple copies can be made, there is no degeneration over time. Furthermore, cryptocoins 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 cryptocoins. 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 elicit 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

General Economics

In this part of the book we will look at the economics at play in the Bitcoin system, as well as in the larger cryptocurrency economy as a whole. We will begin with outlining some general observations about the mechanics which can be observed. In the next few chapters, we will then examine these mechanisms through the lenses of various economic schools of thought.

Inflation

The first issue which is always raised about Bitcoin is inflation, or rather the lack of it. Technically it is not entirely true that there is no inflation in Bitcoin, for the immediate future at least. There is inflation through the growth in money supply which is caused by the mining of additional bitcoins. However, the number of bitcoins being mined is decreasing, meaning that the money supply growths less and less every day, until is stop entirely around the year 2140. Furthermore, in case bitcoins are removed from circulation, for example because the private key is lost, or the stored in a wallet of which the password is lost, this permanently decreases the number of bitcoins in circulation, which has a deflationary effect.

In addition the slow mining of bitcoins and the possible permanent loss of them, there is the influx of value from traditional currencies. The fact that Bitcoin is becoming more widely adopted leads to an increased demand for bitcoins, with a fixed money supply, this increased demand can only result in a higher price level.

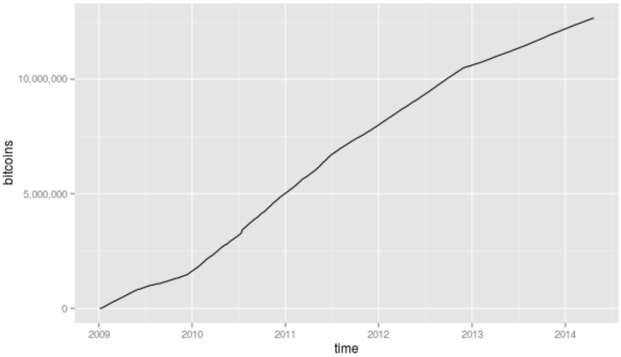
At the time of writing around thirteen million bitcoins have been mined, all of this has been mined since the inception of Bitcoin in 2009.

Currently bitcoins are still being mined, however, this is occuring at a decreasing rate. Since the parameters which determine the amount of bitcoins being mined are fixed. We can very accurately predict the growth of the amount of bitcoins in circulation, not taking into account bitcoins that are lost or otherwise taken off the market.

It is predicted that the last bitcoin will be mined around the year 2140, at which point around 21 million bitcoins will have been mined.

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 many economists.

Figure 8.1: Total Number of Bitcoins in Circulation



A deflation in a currency's 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, which causes the economy to come to a halt. 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.

Figure 8.2: Medium-Term Prediction of bitcoins

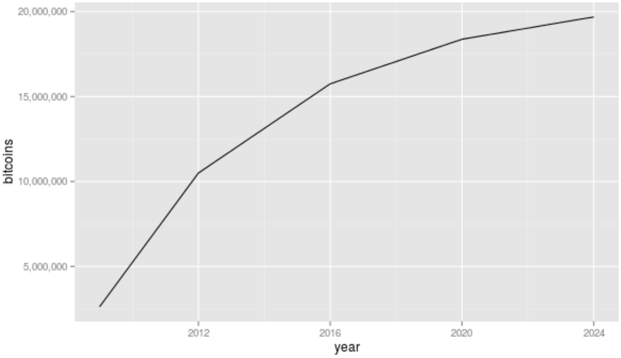
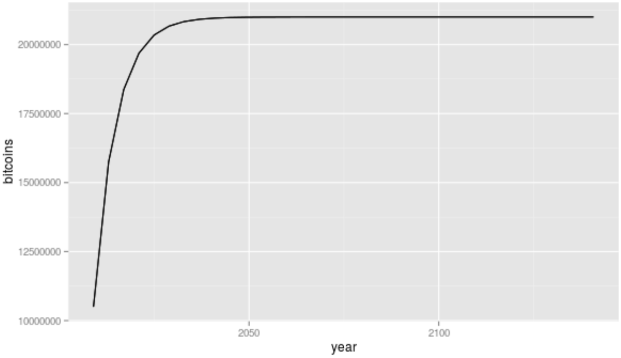


Figure 8.3: Long-Term Prediction of bitcoins



Chapter 9

Cryptocurrencies and Inflation

Inflation in currencies, not coins

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

Cryptocurrency competition: Hayek's Paradise

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

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 descibed by Friedrich Hayek (1976). Hayek describes a situation in which currencies are no longer owned by governments, but in stead 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 invisioned by Hayek. It also addresses some of the key critisisms of this vision, as raised for example by Milton Friedman...

PERHAPS A DISCUSSION OF GRESHAMS 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. **hayek1978denationalization** compares the faith in currency issuers to the faith commonly invested in banks (in the absense of a deposit quaranty system).

> The kind of trust on which private money would rest would not be very different from the trust on which today all private banking rests (or in the United States rested before the governmental deposit insurance scheme!). People today trust that a bank, to preserve its business, will arrange its affairs so that it will at all times be able to exchange demand deposits for cash, although they know that banks do not have enough cash to do so if everyone exercised his right to demand instant payment at the same time.

It is easy to see how this situation is less than ideal, yes people have put their money in banks, but only for lack of alternatives. The system is generally considered problematic. Hence the the rise of deposit insurances schemes, such as the one mentioned in the above quote.

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 then a effect market. Indeed Hayek expects this himself (**hayek1978denationalization**):

> With variable exchange rates, however, the inferior quality money would be valued at a lower rate and, particularly if it threatened to fall further in value, people would try to get rid of it as quickly as possible. The selection process would go on towards whatever they regarded as the best sort of money among those issued by the various agencies, and it would rapidly drive out money found inconvenient or worthless.

If the selection process continues until only the best remains, it is inevitable that substantial market power is attained by these select few parties which control these currencies.

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 sitution 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 11

Friedmans Good Reasons

In Milton Friedman (Friedman 1960; Friedman and Anna J Schwartz 1986) proposed a list of 'Good Reasons' why monetary arrangement have seldomly been left to the market.

1. the resource cost of a pure commodity currency and hence its tendency to become partly fiduciary
2. the peculiar difficulty of enforcing contracts involving promises to pay that serve as a medium of exchange and of preventing fraud in respect to them
3. the technical monopoly character of a pure fiduciary currency which makes essential the setting of some external

limit on its amount

4. the pervasive character of money which means that the issuance of money has important effects of parties other than those directly involved and gives special importance to the preceding features.

Chapter 12

Neo-Keynesianism and Bitcoin

Bitcoin has been heavily critisised by many economist, especially from the neo-Keynesian school. The primary reason for this is th lack of inflation and monetary discretion.

Part III

The Social Value

Chapter 13

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 Anna Jacobson 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.

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 the 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 14

Proof of Stake Cryptocurrencies

To counter the socially useless computing, the proof of stake concept has been invented. In a 2012 whitepaper King and Nadal (2012).

Interest: Unfair free money?

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

Chapter 15

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 cryptocoins (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. 1960. *A program for monetary stability.* Vol. 541. Fordham University Press New York.

Friedman, Milton, and Anna J Schwartz. 1986. “Has government any role in money?” *Journal of Monetary Economics* 17 (1): 37–62.

Friedman, Milton, and Anna Jacobson Schwartz. 2008. *A monetary history of the United States, 1867-1960.* Princeton University Press.

King, Sunny, and Scott Nadal. 2012. “PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake.” `http://www.peercoin.net/assets/paper/peercoin-paper.pdf`.

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, 26

bitcoin

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

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. 26

cryptocurrency

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

cryptography

techniques for secure communication. 26

D

deflation

the situations where the purchasing power of a monetary unit increases over time, generally believed to have adverse effects on the economy. 23

M

miner

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

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