The illusion of scale in segregated witness

Author: Craig Wright

Abstract

Money gains value through use. As a limited quantity of money chases a set value of wealth, we see the price increase linearly with the velocity of the system. The more use, the higher the price. Likewise, as use cases are limited we can expect a decline in price. This effect can be coupled together with scarcity. Bitcoin is a scarce economic good. Its value is retained from its use factor which as a settlement layer alone is severely limited. When proposed changes such as segregated witness are introduced into the system, value is not added into the system, rather than value being added, it is distributed between aspects that are detrimental to the growth of the system. This occurs because schemes such as segregated witness allow for the introduction of fractional reserve systems into bitcoin. With these, the velocity of the system is lowered and bitcoin becomes a pure settlement system such as Swift. In this, value was transferred from bitcoin into sidechains.

Keywords: Bitcoin, Scaling, Segregated Witness, economics

Electronic copy available at: https://ssrn.com/abstract=2993315

Introduction

The primary reason right now for introducing any change into the bitcoin network is scale. An inherent function of networks is to grow, to do this, it needs to maintain a transaction capability greater than the number of users. If bitcoin is to grow, this means the number of users on the system needs to grow significantly. This is our problem; the system has hit the maximum number of transactions and cannot accept any more users. This limit is not because of technical problems, it is because an arbitrary cap has been placed within the system. Right now, the equivalent way to look at this would be to think of the bitcoin protocol as an 8 Lane Hwy that has a single tollbooth managed by a half blind individual.

It is true that transactions get through, but the limits of the system are not even close to being tested. To scale adequately, bitcoin needs to be opened up to allow as many users as possible. As more users enter the system, the scarce nature of bitcoin will drive the price higher increasing the returns to the miners and hence making it more and more profitable even though more resources are needed. This is not about users of the system holding or storing Bitcoin, but rather using it for regular transactions as a true P2P system – as a true currency.

This is where the bait and switch, the magician's trick that is noted as segregated witness comes in.

SegWit opens the opportunity to introduce sidechains. These are less secure than on block scaling, but as it is yet to be tested, there can be only hope that they will be good enough. The problem is that it is not secure and it is not enough. The first issue comes from scarcity, the second concerns the actual scalability of the system.

Velocity of money

Many people fail to understand causality. The value of money comes from supply and demand like everything else in an economic system. Many people have argued that the value of bitcoin stems from its ability to act as a store of value. This is converse to the actual answer. It is confusing the effect with the cause. As an example of this type of reasoning, it is possible to notice the increase in global temperatures since the 1950s. At the same time, there has been a significant rise in the amount of coffee that has been consumed. We could demonstrate a strong correlation between these two events however neither is causal.

In the instance of the value of bitcoin, is not that it can act as a store of value that causes its price to rise, it is use and demand that creates the store of value. There are a number of overly simplistic formulas that enable us to visualise the representation of money as a factor of its use. One of the most common ones is the velocity of money. As it reflects bitcoin, we can formulate the Keynesian system into a more useful metric. Here we will define the following values:

M the measure of money supply

V the velocity of the money supply

P the overall price level

Y the value that represents the real GDP but which is designed as a measurement of wealth[1]

GDP is used as a proxy to measure the amount of wealth created by society in a year. It is not a terribly good measurement so when we are referring to Y in this argument we will refer to the amount of wealth

[1] The definition of wealth differs with there being few (if any), definitions of wealth that are sufficiently wide to cover only those items of wealth that retain and express value. All wealth has value, but the converse is not true. All value is not embodied or expressed in wealth.

Electronic copy available at: https://ssrn.com/abstract=2993315

generated that we may or may not be able to measure. We are not seeking exact answers to society but a relative understanding of the currency effects.

These values are related using the following equation:

$$P = MV / Y$$

From this simple equation, we can see that there is a direct relationship between the velocity of money and its overall use within society. The price of money (P) as related to the money supply times the velocity divided by the amount of wealth created by society. Bitcoin itself creates new and novel uses of the underlying technology. This has a small but negligible impact on the overall wealth produced in a society each year. Compared to the overall currency, this remains to be a statistically insignificant amount and we will work on the assumption that this is for the foreseeable future how this distribution will remain.

We see in the graph below, the relationship between the monetary base and the base velocity of money.

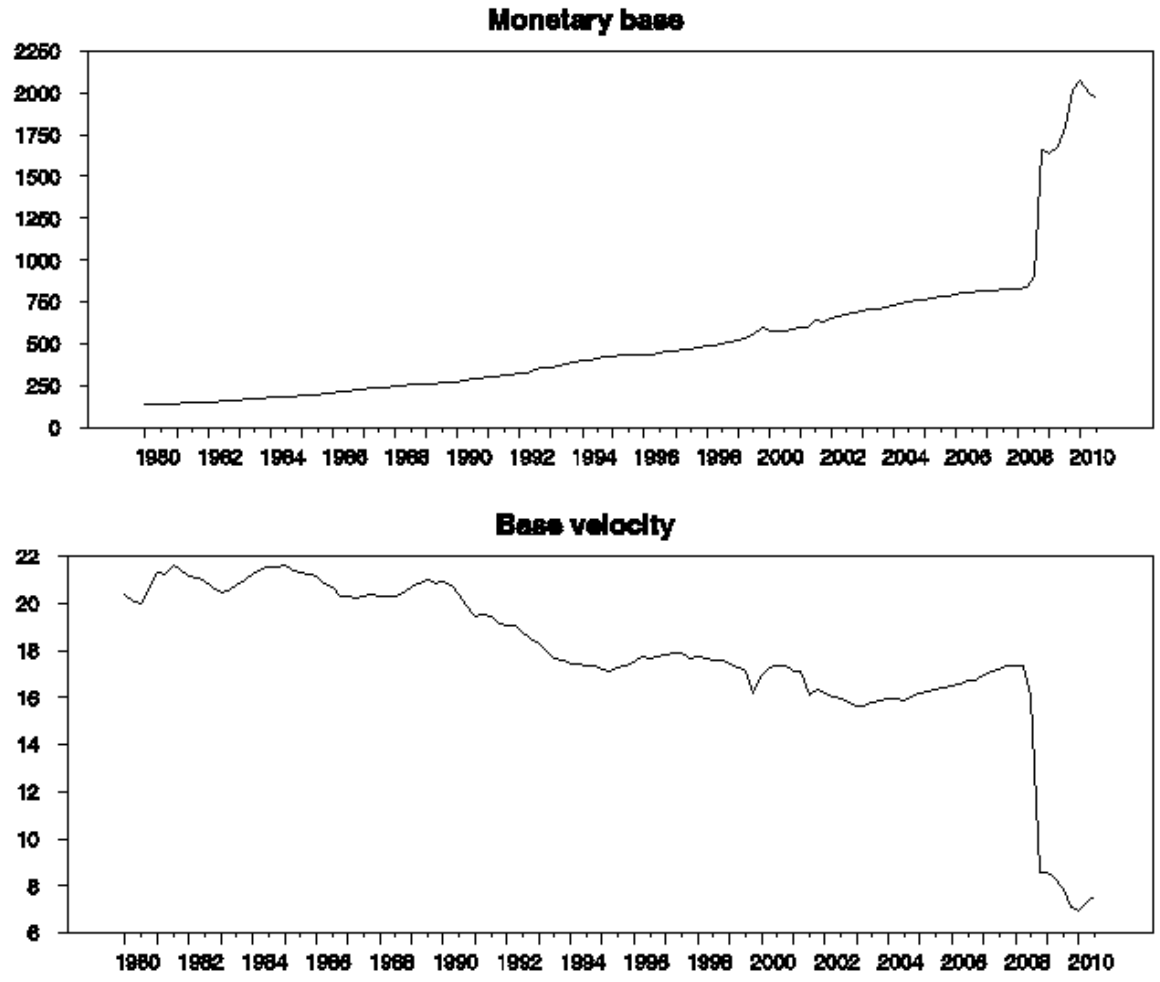

Figure 1: Top panel: level of monetary base, 1980:Q1 to 2010:Q3. Bottom panel: velocity of base.

In this figure presented in US dollars, we see how the introduction of new funds through quantitative easing failed to have the intended effect. More money was introduced, but as the monetary base was increased the amount of available money impacted the velocity. With no new wealth having been created the introduction of new money through quantitative easing simply led to an economic slowdown.

When we are modelling the system in bitcoin, we can start with the overall assumption that the value Y representing the created wealth within society will not change significantly. That is, the differential Delta Y that represents the difference to the economy with an expanded use of bitcoin through non-monetary means can be shown to be close to zero overall. This may vary in the future, but a reduction in the monetary supply further increases the value of money in any event for the amount left is smaller leaving the value greater as the amount of money in supply M is also decreased.

Taking this into account, we end up with a relationship between the variables P, M and V such that an increase in P implies an increase in MV.

$$P \Rightarrow MV$$

There are two ways to look at the system, we can look at the total amount of money available through bitcoin, or we can look at the amount that can be used. The growth of the bitcoin monetary supply is occurring at 12.5 BTC per block or approximately 1800 bitcoin per day. At present, there are close to 16 ½ million bitcoin in circulation[2]. At the current generation rate, there will be approximately 657,000 new bitcoin generated in a 12 month period. This is around 4% inflation in the present system.

Consequently, we can model the system with regards to the change in monetary supply as a factor of that inflation. Hence, assuming GDP and the amount of wealth in society remains approximately equal[3], we can see that the change in the value of bitcoin over the period (ΔP) is related to the amount of bitcoin and the velocity. This can be expressed using the following equation:

$$\Delta P \simeq 0.962 \times V$$

Effectively, being that the supply of bitcoin is stable and suffered little variability through the mining process we see that the overall impact of the price comes from a factor of velocity and uptake. The number of people using bitcoin at present is extremely low. Under 1% of the population uses bitcoin at any point or has even had any use at present. This impacts the price as the supply and demand equation alters to satisfy this effect.

Given the same number of users, and the introduction of a constant demand, we see that the system is a linear equation with the price level related directly to the velocity of money. With all systems, supply and demand set price. What is being overlooked is that for any constant demand level there is a linear relationship between price and velocity.

We can directly relate this to the overall scarcity of bitcoin. Given the overall ownership of bitcoin relates to a scarce good with a set limited supply, we now have two factors that we can say relate to the average price of bitcoin. Market supply will vary. Large holders who sell will cause increases in the amount of supply leading to a lower level of demand and hence a price drop. Changes that lead to people purchasing bitcoin inversely lead to an increase in the level of price compared to other currencies.

Taking all other things equal, we can now demonstrate that for each level of demand, the level of price to the market relates directly to the velocity. Consequently, every increase in the usability of bitcoin increases the overall value of the currency. As this is a direct linear relationship we can simply say that if we increased the ability to use bitcoin such that the velocity bitcoin spending increased by a factor of 100, the price would equally increase just on a use factor by 96.2 times. At the time of writing bitcoin is valued approximately 2,500 USD. An increase in the velocity of bitcoin making it simple to use and increasing the turnover of bitcoin within the community by a factor of 100 would increase the average price of each bitcoin to an estimated $240,000 USD.

---

[2] https://blockchain.info/charts/total-bitcoins

[3] This assumption is ignores the slow growth rate for this simplified argument.

Each block reward would then be valued at over $3 million USD.

Scarcity

This is further compounded by the limits imposed within bitcoin. With an imposed limit, we will see less than 20 million bitcoin within our life span and never more than 21 million, the total volume of bitcoin available without being divided into fractions is minimal when compared to the overall population. The imposition of a fixed maximum quantity that is introduced over time creates a level of scarcity within bitcoin. As adoption increases, the level of demand for the given amount of supply increases and hence the value of bitcoin increases.

Money cannot be studied as an isolated problem. To increase velocity, we need to increase use. As we increase use, we also increase the amount of demand. In the case of a static supply such as bitcoin, this leads to a deflationary effect where the value of bitcoin compared to other currencies increases faster than the linear effect from scaling velocity alone.

True value of money is to make trade simpler. Trade is difficult at best and near impossible without money. In being able to use money, financial transactions increase the satisfaction level of each person involved in a trade as each person would be expected to be able to complete more transactions that fulfil their needs wants, and desires. Money helps increase specialisation and the increased division of labour. It leads to mass production and mass consumption, and without quoting Adam Smith, we see that money helps others as we help ourselves.

One of the first factors involved with the selection of a good money is portability and transmissibility. Bitcoin is both simple to transmit and easy to move. Primarily, it has no weight and it can be easily transmitted from location to location and even across borders. An aspect of transmissibility that is often overlooked is liquidity. The ability to easily and quickly sell any amount without impacting the rate of the exchange impact price[4]. The more that an individual can sell compared to his holdings, the more value a particular currency has. Liquidity in use aids in increasing velocity.

Scaling

Ignoring all the economic consequences, what we have in segregated witness is the illusion of scaling.

Segregated witness introduces a 2 MB block and segregated witness at the same time. Increasing the block size is a scaling solution. Segregated witness is not. Segregated witness with a standard weight provides us 1.2 and 1.6 times the transactional throughput based on a 1 MB partial block and a 4 MB full block.

The reality of this is we have 4 MB masquerading as one. In a SegWit 2x option this is doubled.

Contrary to what people are being told, the witness information, that is the digital signatures are important. These have probative value.

This comes down to this idea that code is law once again and that they can just simply bypass everything related to the law. It does not matter what users do, it matters what exchanges and businesses do. These entities can be forced to comply and they will be. In some places, such as Victoria in Australia it is a criminal offence to delete data that is associated with financial transactions. For general users, pruning this information is not an issue. It is an issue for merchants and other companies. Under the legislative provisions they will be required to maintain the full data.

Consequently, SegWit is a scaling solution that is not providing scale, that is, an additional transactional increase against costs. It is the blocks that increase and at the same time, not segregated witness that

[4] 1. September 2013. “Bitcoin as medium of exchange now and unit of account later: The inverse of Koning’s medieval coins.” konradsgraf.com

provides any increase, as we are told. What we have is a typical magician's trick. It is a bait and switch. You look at the introduced information as they have you look away. What we really have is a 150% increase at a 400% cost. The simplicity of this is just increasing the block size provides 260% more throughput without SegWit.

Putting it another way, segregated witness has 62.5% overhead. That is, it reduces throughput by two thirds.

In many ways, this is the biggest confidence trick to have ever occurred within bitcoin. It makes Mt Gox seem mild.

I say this again so that anyone can understand it.

Segregated witness increases the amount of data storage and network traffic by 400% to gain a transactional throughput of 150%. Simply introducing a 4 MB block or in SegWit 2x and 8 MB block will gain 400% and 800% of the throughput respectively.

Sidechains

There are several problems with the concept of a side-chain being implemented in order to scale bitcoin. Firstly, more money leads to higher prices of goods. In regard to bitcoin, what this means is that the addition of additional sidechains lowers the price of bitcoin. It is in effect a form of inflation where the value of money is limited through the expansion of the money supply. People are not interested in money, they are interested in what they can buy with money. When someone holds bitcoin, it is not because they want bitcoin, it is because they want to be able to obtain something more valuable to them at a later point. Every individual has a subjective level of demand for the quantity of money they wish to save and hold. It is these differing subjective values held by each individual that lead to all market transactions.

Every individual utilises their holdings in money to bid in competition with others for the products they seek to obtain. Each side-chain operates in competition with all others. The argument is that a one-to-one peg will enable settlement on the Blockchain without any loss of functionality. In this argument, the point being made is that a complete one-to-one peg can enable settlement without bitcoin whilst also maintaining financial integrity.

Historically, use of gold certificates started with the argument that gold was difficult to transport adding a layer of cost to transacting. Initially, gold certificates were mapped one-to-one with gold. Like all systems of this type this quickly degraded into a fractional reserve system. The ability to peg multiple payments within sidechains leads to many separate fractional reserve systems. The first possibility involves multiple pegs to a single transaction. This of course assumes the integrity of the side-chain which naturally is lower than bitcoin itself. Further, there is nothing stopping the introduction of a peg that is associated with a side-chain being mapped in a manner that is not analogous to 1 to 1 mapping. Additionally, there are no set rules allowing for fixed mappings. Consequently, it is possible to map a side-chain at one rate and to subsequently alter this at a later time.

An additional problem is the introduction of sidechains with a restrictive cap on the number of transactions acts to limit the growth of bitcoin. The impact is that bitcoin becomes the ugly sister to side-chain based solutions. The limits restrict the growth of bitcoin to alternate side uses and when implemented through segregated witness, and destroy the capability to implement widespread adoption. One of the key requirements that would be needed in the widespread adoption of any cryptocurrency is the integration on chain of pseudonymous records[5] that can be analysed after the fact. Adding additional

[5] This is not KYC, but the ability to easily validate ownership and source of funds.

layers designed to obfuscate information only introduces negative repercussions, making the system less able to be widely adopted.

Sidechains act as a multiplier against the forms of money. In effect, it produces multiple monies on the one system. Multiple monies complicate trade. Each individual form of money used within the market increases the level of complexity involved in comparing prices. As the Internet becomes more and more universally distributed, the integration of multiple prices will become more important. The use of many sidechains complicates this.

By the 19th century, global commerce had settled upon only two separate precious metals. These were gold and silver. They formed the basis underlying the valuation of international currencies. This still proved difficult with many countries on a gold standard trading with others on a silver standard (including India and China). The difficulty in placing orders for international trade was exaggerated as the market ratios between gold and silver fluctuated. This volatility added risk and led to unanticipated gains and loss for the individual merchants. Generally speaking, the average merchant is knowledgeable when it comes to their own business that does not like to engage in risk in areas where they are less informed.

In the past, specialised merchants known as *arbitrageurs* would be employed to minimise the risk that resulted due to foreign trade and the associated fluctuations in international pricing. These middlemen would assume the burden of risk for a price allowing merchants to specialise in their own area without the need to worry further about foreign exchange. The introduction of sidechains and the creation of many types of money would lead to a scenario where these trusted third parties are reintroduced into the system. In a system based upon a single sound money, these trusted middlemen are no longer needed. Their role is released allowing them to produce goods and services that people want more than the creation of multiple types of money.

Throughout history, economic development has resulted in the decrease in the number of monies leading to increased efficiencies. The move towards introducing more monetary channels is not providing consumers with increased choice, it is an attempt to force people away from a simple solution. Bitcoin was designed to remove many of the trusted intermediaries, and certainly not as a methodology to create new middlemen.

Bimetallism

The use of both gold and silver for money in international trade resulted in problems. Merchants were required to maintain prices set in both gold and silver. This resulted in government manipulation. It provided the excuse for regulators to step in and set the price within the market. The consequence was a system where gold and silver could only be exchanged at set prices using the ratio officially published from the Treasury and generally procured at a bank. This is a system we would deem to be a price - controlled market. As with all good intentions, the results were unintended consequences that came through additional discoveries of silver.

The changing use pattern between gold and silver in different areas of the world led to arbitrage opportunities. The fallacy in all of these schemes is price fluctuation. Any initial peg naturally fails to take into account market reactions. A pegged currency created within sidechains is not the same as the underlying asset. This creation of artificial scarcity deems bitcoin as an asset that is difficult to transfer, a claim that could not be further from the truth. Scaling through the use of sidechains adds no additional scalability over increasing the block size and using native bitcoin transactions. The additional overhead in both settling the side-chain transaction within bitcoin and the side-chain transactions themselves leads to an increased set of data and hence less scalability.

Comparing this with segregated witness and the proposed scalability solution, we start to see that the system offers far less than it promises. For the addition of more data, we have additional cost. It is not

important that this is put onto a side-chain, it is important that it is part of the transaction. The introduction of the bait and switch transaction hiding some of the data does not reduce the transactional cost, rather, increases the overhead while calling the cost by a new name. It does not matter what name is used, a bit is a bit and any data transferred across a network is indistinguishable from the common Internet router's point of view.

Economics cannot be ignored. To do so invites disaster.

Conclusion

In this paper, we demonstrate that all changes come with associated costs. Stating that there is no need to account for data as it is weighted differently or is processed on a separate software function does not remove the economic costs associated with a system.

Further, deciding to discount information arbitrarily through centrally-controlled mandates fails to account for the true cost of the service. In deciding what the use case should be for each user, segregated witness is arbitrarily altering the market conditions associated with the use of bitcoin. In deciding that settlement is more important to them than the use of cash transactions for users, places the promoters of segregated witness in a position of arbitrary control.

The subjective nature of individual decisions leads to differing valuations. What one individual is willing to pay for a service will never match with another. This is the basis of trade; disparities in subjective valuation.

The limitation of segregated witness and its ability to introduce sidechains to bitcoin removes the key aspects of scarcity from the system. The change of bitcoin from a cash and payment system into a limited settlement system alters the fundamental nature of the environment and the economics of the system. Introducing sidechains leads to a scenario where bitcoin becomes the capital control system for a large fiat based environment. The proposed limitations associated with sidechains cannot be enforced. There is no way to ensure the one-to-one pegging of each bitcoin. More importantly there is no reason for this to exist as a solution. If each individual unit can be used on chain, we come to the realisation that we have not actually achieved any cost savings.

This leads to the sole solution that can logically follow. That is an initial small amount of bitcoin will end up propping large quantities of values held within sidechains. This introduces fractional reserve banking into bitcoin and destroys the scarcity factor. Without scarcity, bitcoin may as well be PayPal or any bank or credit system. Once we start to realise that it is scarcity that makes bitcoin valuable, and that coupled with the ability to trade quickly, safely, and across borders, we start to understand that any addition to the protocol that removes scarcity, and lowers the velocity, will limit the value that can be traded market. As we demonstrated above, when the value of the money supply is diluted, the value of wealth remains constant leading to a lower price for money. Further, limiting the velocity of money directly limits its price.

The simple answer to the economics of the system is to maintain scarcity and increase the velocity through enhanced use. It is using bitcoin that makes it valuable. It is only through its potential to use bitcoin that it becomes a store of value. The argument that we should develop a store of value using bitcoin is placing the cart before the horse. A store of value exists when an item has increasing value and that comes through increasing use. Removing and deleting use cases limits the use.

References

1. Bastiat, Frédéric. 2007 [1850]. The Law. Auburn, Alabama: Mises Institute
2. Böhm-Bawerk, Eugen von. 1962 [1881]. "Whether Legal Rights and Relationships are Economic Goods." Shorter Classics of Eugen von Böhm-Bawerk. South Holland, Illinois: Libertarian

Press; originally, “Rechte und Verhältnisse vom Standpunkte der volkwirtschaftlichen Güterlehre.” Innsbruck, Austria: Verlag der Wagner’schen Universitäts-Buchhandlung
3. Burke, Edmund (1990) [1774]. E. J. Payne, ed. Thoughts and Details on Scarcity. Indianapolis, IN: Liberty Fund, Inc.
4. Hoppe, Hans-Hermann. 14 May 2009. “‘The yield from money held’ reconsidered.” Mises Daily. mises.org/daily/3449
5. Menger, Carl. On the origins of money. 2009 [1892]. Auburn, Alabama: Ludwig von Mises Institute. Translation by C. A. Foley. Mises, Ludwig von. 1912. Theorie des Geldes und der Umlaufsmittel. Munchen und Leipzig: Ferlag von Duncker & Humblot. mises.org/document/3298/
6. Šurda, Peter. 2012. Economics of Bitcoin: Is Bitcoin an alternative to fiat currencies and gold? Thesis for the Vienna University of Economics and Business. dev.economicsofbitcoin.com/mastersthesis/mastersthesis-surda-2012-11-19b.pdf