

Wednesday, December 11, 2013



## Global Macro Themes – Bitcoin: The World’s Hardest Currency?

*As we have commented on in prior research notes the lot of a central banker is not a happy one in the present circumstances. With monetary policy so far away from what might be deemed “normal” there are plenty of things to keep a central banker awake at night. One fear comes from technology, something most investors would consider an unexpected source as technology is generally perceived to be a positive given its favourable impact upon the supply-side of an economy. However, we are talking about one specific application of technology – Bitcoin. In this research note we look into this virtual currency and consider the potentially far-reaching consequences. To pre-empt the rest of the note a little we disagree with those who argue that it is nothing more than a hi-tech Ponzi scheme. Rather it should be viewed as one of the world’s hardest currencies with considerable upside (albeit risky) potential.*

### A (Very Brief) History Of Money

Money has been around a long time, at least conceptually. Economic historians broadly agree that the earliest recognisable form of money was livestock in the period 9,000-6,000BC; a reflection of the dominance of agriculture at that stage in economic evolution. However, this barely represented much improvement from the preceding barter system in that cows fail to satisfy at least two of the six now universally agreed prerequisites for money<sup>1</sup> listed below:

1. Durable
2. Divisible
3. Portable/Convenient
4. Uniform/ Consistent
5. Store of value / Limited Quantity
6. Credible / History of Acceptance

In order to overcome the rather obvious shortfalls from using cows as an early form of money, the next stage of monetary innovation was to use shells<sup>2</sup> as they

---

<sup>1</sup> We will leave it to the reader to ascertain which of the six prerequisites cows invalidate as we assume it to be self-evident!

<sup>2</sup> Numerous other commodities have been used as money including salt, grain and tobacco. In the Yap Islands in Micronesia the islanders used large stones called Rais as a form of money, stones so huge that it takes upwards of twenty men to move them (so much for portability and

better satisfied the divisibility prerequisite. It was not until 1,000BC that the Chinese introduced the first metallic coins; a form of money that still endures today. China was also the first country to develop paper money during the Tang Dynasty around 700 AD. Even though this money was in paper form, the notes were valued in terms of silver and gold although in practice there was no such conversion. As such, the early forms of money were either actual commodities or were backed by commodities.

Commodities are not in infinite supply - they have a natural scarcity – and there is an associated cost of production/extraction. It is these two characteristics that made them attractive as a form of money as it satisfies the “store of value” prerequisite listed above. Unfortunately, because commodities are also useful articles of trade, by definition they have other uses than as a medium of exchange. This is a distinctly undesirable feature for any money. Changes in the nonmonetary demand for the commodity would, for example, be transformed into a monetary shock, exacerbating the economic effect. Equally, commodities are also vulnerable to supply shocks, such as finding new sources of higher-grade metal ores or cheaper extraction methods.

### **The Fiat Innovation**

Over the next several centuries, concomitant with increased financial sophistication and the establishment of the banking industry, money took a slightly more abstract form. Rather than commodities being used directly as money they were replaced by “representative” paper bank notes. Despite their reduced durability they could be cheaply reproduced to replace worn out bank notes and proved to be much more convenient to use. Moreover, as paper money is solely designed to act as a medium of exchange it has no nonmonetary uses, thereby overcoming the two pitfalls with commodity currencies mentioned in the previous paragraph.

That said, the transition to paper money was far from smooth. The key problem with this alternative form of money – also known as fiat money - is that it is not backed by anything other than the credibility of the issuing authority. Under a commodity-based monetary system, by virtue of being in his/her possession, an individual can readily verify ownership of the money. Under a fiat money system, by contrast, the owner necessarily relies on the trustworthiness of the note issuer. The reason why this is an issue is that the marginal cost of production of fiat money is negligible. Hence, the issuer has strong incentives to increase the supply of money until its market value falls below the (very low) cost of production.

Indeed, early innovations in fiat currency were beset with problems relating to excess supply. In 1661 Stockholms Banco, a private bank, issued Europe’s first

---

divisibility!). It would seem that the only limit of what can be used as a form of money is human ingenuity.

paper money and its failure just three years later was directly a result of printing too many bank notes relative to its collateral. Paving the way for future trends, the Swedish parliament eventually took over control of bank note issuance after Stockholms Banco lost its charter<sup>3</sup>.

However, even having the government act as the issuer of bank notes does not overcome this major problem with fiat money. In the 18<sup>th</sup> century provincial governments in the American colonies produced bank notes, money that was given value by virtue of the fact that they were able to extinguish tax liabilities<sup>4</sup>. Despite this, these bank notes failed to maintain their purchasing power (breaching the store of value prerequisite). In fact, there are numerous examples for government-issued fiat money having failed and the common root is fiscal overspending, often at times of war. Governments, when faced with escalating expenditures face a stark choice either raise money by increasing taxes, which is very transparent and politically unpopular, or by firing up the printing press, a much more subtle method. Even though debasing one's currency has disastrous long-run consequences it seems to be the better short-run choice politically.

In short, while both pure commodity and pure fiat money systems have benefits, they also have significant shortcomings; shortcomings that explain why neither system has proved historically robust.

The post World War II monetary system – Bretton Woods – can be thought of as a hybrid system. The fiat currencies of the major economies were pegged to the USD – reflective of its status as the predominate reserve currency – which was in turn pegged to the gold price<sup>5</sup> and the IMF was the clearing house for trade imbalances via the gold reserve fund. The system endured until 1971 when the Nixon government abandoned gold convertibility as persistent trade deficits and excessive government spending related to the Vietnam War<sup>6</sup> implied that foreign countries held more USDs than the US government could convert into gold at the prevailing fixed rate.

The breaking up of Bretton Woods, while traumatic in the short-run (Nixon was forced to implement temporary wage and price freezes to combat the potentially strong inflationary boost from the sharp depreciation in the USD that followed the ending of gold convertibility) the long-run consequences have been much more benign – at least to date. Since 1971, the global monetary system has been run as a pure fiat currency regime, with the value of money attributed to the inflation

---

<sup>3</sup> After a few name changes Stockholms Banco eventually became the Swedish Riksbank – the world's oldest central bank.

<sup>4</sup> This ability to repay debt, especially tax, is the most crucial characteristic for fiat money and is what provides it with any real value given it has no other intrinsic value.

<sup>5</sup> The exchange rate for the USD was fixed at USD35 per troy ounce of gold bullion.

<sup>6</sup> History, especially financial history, really does repeat!

credibility of central banks; institutions formally independent of the government<sup>7</sup>.

We would argue the single most important factor accounting for the relative stability of the global monetary system since the early 1970s has been the lack of serious military conflict and the accompanying fiscal pressure on governments.<sup>8</sup> Nevertheless, even in the absence of conflict, the current economic crisis has seen government debt levels soar and central banks have been active in employing the printing press – albeit as discretely as possible – suggesting that the present “pure” fiat money regime is under significant pressure.

### **Enter Technology**

As described above, money has tended to take one of two forms historically: commodity or fiat. This bipolar characterization of money is no longer all-inclusive. With exquisite timing in 2008, at the height of the financial crisis, Satoshi Nakamoto self-published a research paper<sup>9</sup> outlining the theoretical design of Bitcoin: a decentralised electronic cash system. Although e-cash systems have been contemplated since the early 1980s Nakamoto’s Bitcoin has some very neat and innovate features that overcome many of the problems associated with other e-cash systems. Not only was the Bitcoin system theoretically viable but also, as evidenced by the surge in interest from the general public - not to mention trading volume - in this virtual currency, it has become highly successful.

### **Bitcoin – An Overview**

The underlying rationale for the design of Bitcoin is very simple and is explained in the first few paragraphs of Nakamoto’s research publication. Despite the surge in commerce over the internet, the system still relies almost exclusively on financial institutions acting as “trusted third parties”. Bitcoin does away with this trust-based model thereby allowing transacting parties to conduct business bilaterally. As Nakamoto identifies the key to ensuring this outcome is for transactions to be non-reversible: once payment for a good or service is completed the involved parties cannot renege on the transaction. The proposed solution to this problem is to make transactions “computationally impractical to reverse” using standard cryptographic methods such as hash functions; a relatively straightforward<sup>10</sup> process. The really innovative element to Bitcoin’s

---

<sup>7</sup> No central bank is truly independent of the government as we argued in “Forward Rate Guidance: Digging Deeper”, 28 November 2013.

<sup>8</sup> Other economists take a differing view, especially those of a European persuasion who like to argue that it is the stable global monetary system (and especially EMU), which has brought about geopolitical stability.

<sup>9</sup> Nakamoto (2008) “Bitcoin: A Peer-to-Peer Electronic Cash System”

<sup>10</sup> When we say this is straightforward we do not mean that the mathematics is easily to understand for the general reader – it is far from it - but rather that the issue is well understood by mathematicians and computer scientists and software is available to encrypt transactions. For

design, however, is tackling double spending. The standard way to verify that money has not been spent twice – fraud in other words – is for a central authority to verify every transaction. Given that Bitcoin's designer(s)<sup>11</sup> *raison d'être* is to create a decentralised money system this needs to be overcome by some other means.

The innovative solution to this problem was the realization that to identify whether a transaction is valid is for all Bitcoin transactions to be time stamped and visible to all users, i.e. transactions are publically announced over a peer-to-peer network. Assuming that the majority of nodes in this network are “honest” once there is majority agreement that the transaction is valid, which is achieved by solving the cryptographic hash function to a specified degree of accuracy, it is considered as being verified. Hence, rather than rely on a single trusted entity, Bitcoin uses the power of the crowd to provide the necessary transaction verification. While the assumption that the majority of nodes in the network are honest might seem incredible, especially given the amount of fraud on the internet, it is not as strong as first appears because the Bitcoin system has been designed to be incentive compatible. Solving the complex mathematical problems required for transaction verification is rewarded by the release of new Bitcoins – a process called mining. By design it is easier to mine new Bitcoins than to compute fake histories for existing Bitcoins – a computation that gets harder as transaction histories get longer – so there is no incentive for “bad guys” to undermine the system.

The other design feature of Bitcoin that is ingenious, and which provides the greatest source of intrigue to economists, is that the supply of Bitcoins is predictable and eventually finite. Bitcoins can only be mined at a pre-specified growth rate, a rate that will steadily decline until the total supply is capped at 21 million<sup>12</sup>. In order to ensure that the production of Bitcoins is in line with the release schedule, the degree of difficulty in “mining” or verifying existing transactions is variable and a function of the number of “miners” or computer power employed. Hence, even if some individual, or more likely organisation, were to employ supercomputers to maximise their mining success, this would simply affect the share of Bitcoins<sup>13</sup> mined not the total amount.

To think about how Bitcoin fits within the spectrum of money classification types consider the following table, which is contained in a working paper on synthetic commodity currencies published by Selgin (2013).

---

a good layman's guide to Bitcoin and the mathematics used see Velde (2013) “Bitcoin: A Primer”, Chicago Fed Letter.

<sup>11</sup> Satoshi Nakamoto is widely thought to be a pseudonym and the true identity of the Bitcoin designer or designers is/are unknown. More on this later!

<sup>12</sup> Once the total supply of Bitcoins reaches the 21 million mark, mining Bitcoins will no longer be rewarded by the addition of new coins. Rather the process of transaction verification will be associated with a fee, one much smaller than that applied by commercial banks at present.

<sup>13</sup> Various websites such as <http://bitcoincharts.com> publish the total number of Bitcoins mined and also the degree of difficulty required to mine them.

### Base Money Types

<i>Scarcity</i>	<b>Absolute</b> <b>Contingent</b>	<i>Nonmonetary use?</i>	
		<b>Yes</b>	<b>No</b>
		Commodity	Bitcoin
		Coase Durable <sup>14</sup>	Fiat

Not only is the above table a useful method of classification but also it provides a useful guide for thinking about the pro and cons of the various money types. As discussed above, the major advantage of commodity money is the natural scarcity of supply, which allows it to serve as a store of value. However, the downside is that by virtue of it being a commodity it has nonmonetary uses as well, implying that demand and supply can fluctuate for reasons other than its role as money; a much less desirable property. By contrast, fiat money has no other nonmonetary use, which is its major pro. Its scarcity though is contingent on the credibility of the issuer (the central bank in almost all cases) and as outlined previously their track record over long periods of time is far from perfect. What is clear from the above table is that Bitcoin manages to combine both pros – its scarcity is absolute (by design) and it has no nonmonetary use. So, in theory, it represents significant improvement over the two existing types of money.

### Downsides To Bitcoin

That is not to say that Bitcoin has no drawbacks. The biggest by far relates to the credibility of the issuer, in this case the founder Satoshi Nakamoto. As mentioned in footnote 7 above, this name appears to be fictitious and there has been no verification of his/her/their identities. Given this anonymity how can Bitcoin be trusted? This often-heard criticism is clearly understandable. However, who would you rather trust a tech geek who has promised to limit the supply of its virtual money or central banks that have, both by word and deeds, promised to continue to issue money in sufficient quantity to ensure its real purchasing power declines? Not so obvious when you think about it in those terms. Moreover, this risk to Bitcoin was greatest at its inception, in that the anonymity of its creator would mean there no was take-up of Bitcoin and it would have been effectively stillborn. This clearly has not happened.

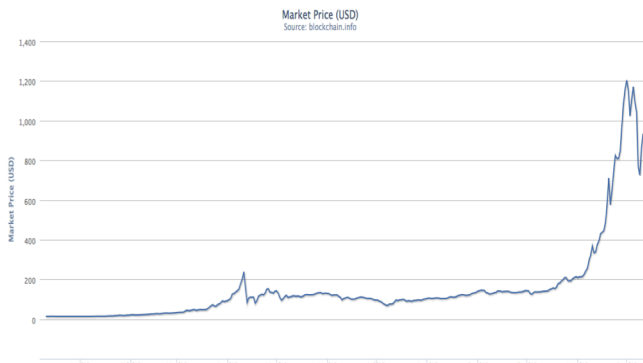
Having become, in some sense, established the most obvious threat is that the total supply of Bitcoins is not restricted to 21 million coins. If it were ever to be the case that actual supply exceeded this amount one of the key strengths of this virtual money would be invalidated and the whole edifice would come crashing down. There is no way *a priori* to rule out this possibility. But suffice to say the Bitcoin market is very transparent, with numerous companies monitoring and publishing the rate of production of Bitcoins consistent with the very open

<sup>14</sup> For the definition of a Coase durable, which is incidental to this research note, please see the research paper by Selgin (2013), "Synthetic Commodity Money".



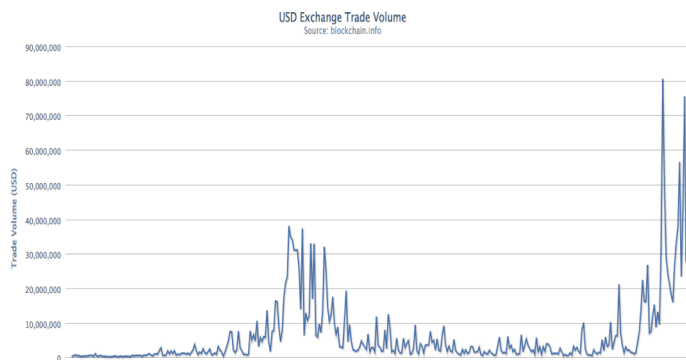
nature of the Bitcoin network. Any marked difference between actual production and the stated supply schedule would be, therefore, very easy to monitor mitigating this risk to some degree.

Another widely discussed drawback to Bitcoin is that the price associated with the conversion back into fiat money – several companies offer this service – is very volatile. Consider the graph below, which plots the price history of Bitcoins in USD terms. Within the space of one year the USD value of Bitcoin has gone up by nearly a factor a 10. Good news if you were long, bad news if you are Laszlo



Hanyecz who three years ago, when the virtual currency was in its infancy, purchased a pizza for 10,000 BTC. Back then this was equivalent to just USD 25, but at today's valuation would be worth USD 10 million – surely the world's most expensive pizza purchase!

Additionally intra-day volatility in Bitcoin is also very high, certainly compared with other forms of money (the volatility of money can be thought of as the inflation rate or the exchange rate versus other currencies). The reason for this is that the price is purely market driven, there is no market maker to smooth out imbalances between demand and supply. Hence, the price is sometimes required



to adjust dramatically. That said, due to the combination of increased production and an – ironically – a higher price, Bitcoin is becoming an increasingly liquid instrument as evidenced by the second chart below which shows daily trading volumes<sup>15</sup>.

While on the subject of the Bitcoin price, one of the ill considered criticisms of this virtual money is that it is nothing more than a fancy Ponzi scheme. The analogy stems from the fact that as Bitcoin pays not interest rate<sup>16</sup> the only way to generate a return is for the price of Bitcoin to keep rising, which relies on

<sup>15</sup> Hat tip (anon). A former boss of mine during a discussion of the gold market made this point about liquidity. His simple point being that the reason the gold market was not viewed by many professional investors as particularly liquid was not that there was insufficient gold, rather it's price was too low!

<sup>16</sup> As of now at least, this will be discussed later on in this research note.

other investors purchasing it later at a higher price. Superficially, the comparison appears valid. However, Bitcoin is a fully functioning virtual currency that allows anyone to make transactions, it is no more a Ponzi scheme than any other money. Moreover, assuming that the supply is eventually capped at 21 million, Bitcoins should – at a minimum – continue to rise in tandem with inflation, if not nominal GDP growth. Hence, even late adopters (the suckers in a true Ponzi scheme) still benefit. That said, it is true that early adopters, or investors, are likely to witness the greatest gains.

### **Valuing A Virtual Currency**

This is a very interesting exercise to engage in as an economist. How do you value a virtual currency that generates no cash flow? Impossible. Not quite, but the valuation we will derive needs have some very wide margins of error attached to it.

At a global level, the total stock of outstanding fiat money is approximately USD 50tr. Assuming no decline in the stock of money, which would be deflationary<sup>17</sup>, if Bitcoin were to completely replace fiat money then the 21 million Bitcoins that will be produced must equal the global supply of fiat currency. This implies that each Bitcoin would be worth a staggering USD 2mn. Now we admit that the assumptions we make are brave, but even if we apply very large margins of error around this valuation, it strongly suggests that around the USD 1,000 mark (at the time of writing it is just under this level) Bitcoins are still very undervalued. For those readers who think that such a high valuation makes Bitcoin totally impractical to use, they should note that Bitcoin has been designed to be divisible to eight decimal places. This degree of divisibility means that even if each coin was valued at USD 2mn payments equivalent to penny transactions can still be made.

At this point we should add a huge caveat to the above analysis; one that highlights another serious risk to Bitcoin. The USD 2mn valuation of Bitcoin is premised on Bitcoin replacing all existing fiat currencies. This is never going to happen. Governments enjoy monopoly rights to print their own currencies and they can force its usage by requiring taxes be paid in it. This is a huge advantage and they will not give it up. Moreover, as Bitcoins are stored in electronic wallets and there is not limit to the number of wallets that can be created by Bitcoin users, this effectively means transactions can be made anonymously. For users this can be a very valuable feature<sup>18</sup> but for governments it is a disaster as it opens up the prospect of it being used to pay for illegal activities. In fact, last month the FBI closed down Silk Road, an online marketplace used to buy and sell illegal drugs and which used Bitcoins for payment<sup>19</sup>. Such issues are very likely

---

<sup>17</sup> More on this point later.

<sup>18</sup> Especially if you are a member of the Eurozone as it would allow money to be transferred even with capital controls imposed as occurred in Cyprus – worth remembering!

<sup>19</sup> <http://www.reuters.com/article/2013/10/08/net-us-crime-silkroad-bitcoin-idUSBRE99113A20131008>. In 2012 the FBI set up a Virtual Currency Emerging Threats Working



to incentivise lawmakers to try and regulate Bitcoin, or *in extremis*, try to shut down the entire system. Given its highly decentralised network whether this is technically possible or not we must leave to more tech savvy individuals, but it is a certainly a valid concern<sup>20</sup>.

### **Deflationary Disquiet**

One major concern that has been voiced by numerous economists and financial commentators is that Bitcoin, by virtue of its (eventual) fixed supply characteristic is inherently deflationary. This is economically correct; a fixed money supply combined with an expanding real economy can only occur if the general price level declines. For many economists, and especially policymakers, deflation is an unambiguously bad thing. Falling prices provide consumers with an incentive to hold off making purchases in anticipation of lower future prices. This necessarily means lower economic activity as demand shrinks, leading to higher excess supply and yet more downward pressure on the general price level. Compounding this deflationary spiral is the fact that as the general price level declines the real value of debt – public or private – rises, increasing the probability of default, perpetuating a vicious spiral.

Our answer to this concern is: so what! We have always been vexed by the notion that deflation is a bad thing. If falling prices are so bad why do companies engage in seasonal sales to clear inventory? Moreover, has anyone complained that the price of personal computers/mobile phones and other hi-tech gadgetry have fallen in price (especially under the hedonistic adjustment mechanism applied in CPI calculations)? Of course not! Moreover, if deflationary pressures provide a check on debt accumulation (borrowers would know in advance that there would be no way to inflate the debt away) this would surely mitigate the need for all the macroprudential regulation policymakers have planned.

Under a fixed money supply regime (as Bitcoin will eventually become) the decline in the general price level<sup>21</sup> is directly proportional to the real increase in the provision of goods and services. If real economic output increases by 2% per year and the stock of money is unchanged the general price level must fall by an equivalent 2%. Similarly, if there were no change in real output, there would not be any pressure on the general price level to fall or rise. In other words the decline in the general price level (or deflation) under a fixed money supply regime is how every ones standard of living rises.

---

Group mandated to share information and track illicit actors' use of virtual currency with other countries; a clear indication of future intent.

<sup>20</sup> Governments could also make it financially unattractive to use Bitcoins by applying punitive taxes on transactions, although to the best of our knowledge no such plans have been made public.

<sup>21</sup> Note we are referring to the general, or aggregate, level of prices in an economy. Relative price changes could be much higher (or even positive) or much lower depending upon sectoral changes in demand and supply.

In answer to the issue of hoarding, has demand for personal computers, whose price level has dropped markedly since their creation, spiralled downwards? Again the answer is no. Individuals consume goods and services every day out of necessity. The notion consumers will hold off buying any good or service for any sustained length of time anticipating lower prices in the future is nonsensical.

On the related question of saving (hoarding is just a more extreme version of saving) what motivates an individual to refrain from consuming today in preference for tomorrow is complex. However, economic theory makes it clear that one of the strongest motivations is consumption smoothing. Consistent with the Life Cycle Hypothesis, individuals have differing saving rates at different times of their lives. Typically dissaving occurs in early adulthood and retirement but is positive for the bulk of employment. Such behaviour is certain to continue irrespective of anticipated changes in the general price level, especially if - as stated above - the pressure on the price level to change is directly proportional to changes in real activity<sup>22</sup>.

### **Utopian Dreams**

Interestingly, if Bitcoin were to become the predominant money of the global economy, there would be no role for central banks as the need for a single transaction verifying institution would cease. Indeed, in the very long run it is quite feasible that no banking system is required at all. Banks provide a financial mediation role matching savers to borrowers. But rather like the decentralised infrastructure of Bitcoin, there is no reason why this cannot be done in a decentralised fashion as well. There are already companies facilitating direct lending between private parties a process called peer-to-peer lending. Under this system the lender chooses the type of loan he/she wishes to make at a specified interest rate reflecting the perceived riskiness of the borrower: a lending system that would naturally compliment the decentralized Bitcoin system. Perhaps this might seem to be a utopian dream but it is worth remembering the words of Milton Friedman, who wrote the following in his 1962 publication *In Search of a Monetary Constitution*:

*“Money is too important to be left to central bankers”.*

---

<sup>22</sup> We acknowledge that either a sizeable and/or temporary drop in the general price level – for example as witnessed during the Great Depression - could trigger hoarding behaviour, as that is economically sensible. But more modest and sustained price declines, as would occur under a fixed money supply regime like Bitcoin, are unlikely to generate such a response as people need to consume to live.

**Disclaimer:** All rights reserved. The contents of this report do not constitute, and should not be construed as, investment research or advice. The opinions expressed herein are based on information gathered from various sources believed to be reliable but we cannot guarantee the accuracy or completeness of this information. Moreover, the information in this report is subject to change without notice and Black Swan Economic Consultants assumes no responsibility to update the information contained in this report. The views expressed, or implied in the report, including projections and statements about the future, should be treated as judgements and Black Swan Economic Consultants cannot be held responsible for any failure for them to prove accurate. Reference to specific securities are for illustrative purposes only and are not intended to be, and should not be interpreted as, recommendations to purchase or sell such securities. This report and the information contained therein may contain information that is privileged and confidential and is intended for the sole use of the intended recipient(s). If you are not the intended recipient, please contact Black Swan Economic Consultants as soon as possible. Reproductions, quotations or distribution of this report, or any part herein, via any media form without the express written permission of Black Swan Economic Consultants is strictly prohibited. Black Swan Economic Consultants is not liable for any loss or damage resulting from the use of its products.