Columbia University

Center on Capitalism and Society

Working Paper No. 92, August 2016

Can cryptocurrencies fulfil the functions of money?

Dr. Saifedean Ammous[1]

Abstract

This paper analyzes five cryptocurrencies' monetary supply growth, credibility, and stability, to evaluate whether these currencies have a viable monetary role as a medium of exchange, store of value, and unit of account. While all cryptocurrencies can theoretically serve as a medium of exchange, they are inherently too unstable to be used as a unit of account. Of the five, only Bitcoin could potentially serve as a store of value, due to its strict commitment to low supply growth, credibly backed by the network's distributed protocol and very large processing power. Other cryptocurrencies' low processing power, centralized control, and use as tokens for specific applications make them unlikely to fulfil any monetary function.

JEL classification: E42, E51

[1] Assistant Professor of Economics, Lebanese American University. Foreign Member, Center on Capitalism and Society, Columbia University. Email: sha2106@columbia.edu

1. Introduction

In 2008, pseudonymous programmer Satoshi Nakamoto introduced the design of a distributed peer-to-peer digital cash named Bitcoin. It was put into operation on the third of January 2009, as an obscure experiment among cryptography enthusiasts who transacted and mined the then-worthless tokens until they were listed on an exchange for a price of $0.000764. On May 22, 2010, the first real transaction was recorded in which Bitcoin served the function of a medium of exchange, at a rate of $0.0025 (Coindesk 2014). Since then, more than 140 million transactions have taken place with bitcoin, and the purchasing power of the currency has risen significantly, to around $600 per bitcoin at the time of writing, giving the total coin supply a market value around $10 billion. Bitcoin's success has prompted many imitators to launch similar cryptocurrencies with varying features and economic properties. More than 700 such cryptocurrencies exist at the time of writing.

This paper examines whether cryptocurrencies can have a monetary role by assessing how well they perform the three traditional functions of money: a medium of exchange, store of value and unit of account. Fulfilling the role of medium of exchange is a rather trivial requirement, of which any good, digital or physical, is capable, once it is acquired by someone for the purpose of selling it on later in exchange for another good. In this regard, cryptocurrencies have succeeded in fulfilling this role as they all exist on market exchanges and can be easily transferred between their owners. The more interesting monetary questions for cryptocurrency pertain to their ability to fulfil the two other functions of money: store of value and unit of account.

This paper assesses the suitability of cryptocurrencies for these roles by understanding and analyzing their 'monetary policy' in contrast to that of more conventional currencies. The five cryptocurrencies analyzed are bitcoin, ethereum, litecoin, ripple, and steem, and they were chosen because they have the largest market capitalization of cryptocurrencies at the time of writing, and because of their differing designs offering an object lesson in various aspects of cryptocurrency design, as will become apparent in the exposition below. Section II provides context by discussing traditional national currencies and gold, the rate of increase in their supply, and how they achieve the predictability and stability necessary to perform their monetary role. Section III describes the structure, economics and governance of the five cryptocurrencies, while Section IV compares their supply growth rates, predictability and stability to that of conventional currencies. Section V concludes by assessing these currencies' suitability for them performing the traditional functions of money.

2. Context: National currencies and precious metals

A comparison with national currencies is useful for providing some context for analyzing cryptocurrencies. Cryptocurrencies have no central banks, and have no mechanism to set interest rates and required reserve ratios for institutions that deal with them. These traditional tools of analyzing monetary policy will not be useful for analyzing cryptocurrencies. Cryptocurrencies can be better understood by examining the growth in the money supply, the predictability of the schedule for money supply growth, and the currency's likely stability. Central banks aim to keep prices relatively stable, and so design their monetary policies to ensure that money creation does not proceed at a pace which would cause prices to rise too quickly. They take into account expectations of money demand and plan money supply growth to meet it at a level that keeps consumer prices rising at a low and stable rate, in the range of 2% to 3%. Central banks also need to contend with deflationary financial crises that cause a collapse in the money supply. By injecting liquidity into the banking system, they seek to prevent money destruction and drops in prices (Bernanke 2002).

To place cryptocurrency supply growth in context, it is instructive to look at the supply growth trends of existing national currencies. The World Bank provides data on broad money growth for 167 countries, for the period between 1960 and 2015. The data for all countries is plotted in Figure 1[i], and country averages for the entire period can be found in Appendix 1. While the data is not complete for all countries and all years, the average growth of money supply came at around 32.16% per year.

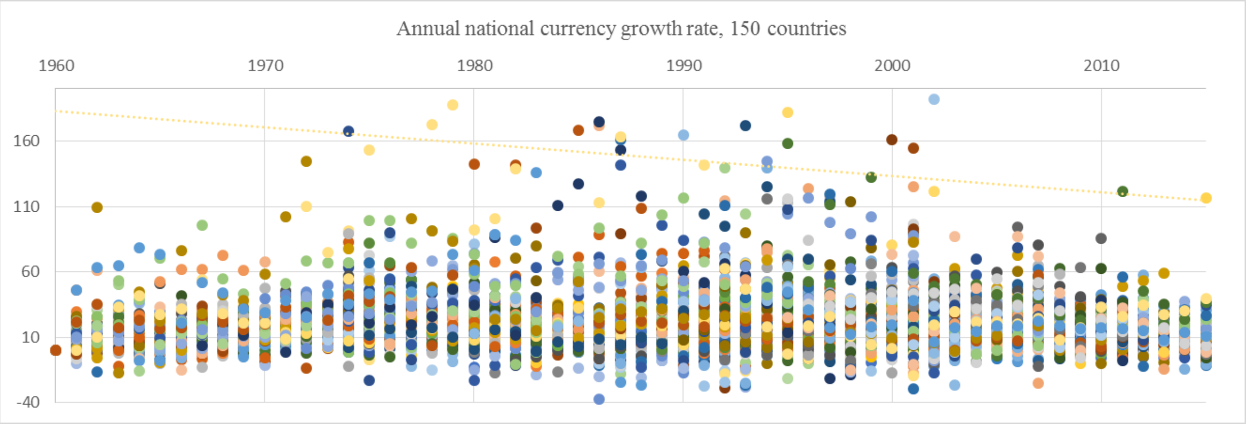


Figure 1: Broad money annual growth for 167 currencies 1960-2015. Source: World Bank

The 32.16% figure includes highly inflationary periods in developing countries which skew the results upward. During these periods, people in developing countries leave their national currency and buy durable items, commodities, gold, and foreign currencies. International reserve currencies, particularly the dollar and the euro, are easily available in most of the world, and constitute a significantly high portion of the global demand for a store of value, medium of exchange, and unit of account. Seeing as they constitute the main store-of-value options available for most people around the world, these currencies are a more instructive comparator to cryptocurrencies. And since these currencies have also grown more stable in value recently, compared to the 1970's, it is more instructive to look at a more recent period. OECD data shows that for OECD countries over the period between 1990 and 2015, annual broad money supply growth rate averaged 7.17%. Table 1 shows the average annual growth rate in the broad money supply for select countries for the 25 year period between 1990 and 2015.

Currency Region	Average annual supply increase (%)
Australia	8.81
Canada	6.54
China	20.14
Colombia	18.47
Denmark	6.34
Euro area (19 countries)	5.55
Iceland	11.12
India	16.48
Japan	2.01
Korea	12.06
New Zealand	7.59
Norway	6.65
OECD - Total	7.17
South Africa	12.42
Sweden	5.47
Switzerland	4.04
United Kingdom	6.90
United States	5.40

Table 1: Average percent annual increase in broad money supply (M3) for select currencies. Source: OECD.Stat.

The world's major national currencies generally have their supply grow at predictably low rates. Developed economies have generally had slower increases in the supply of their currencies than developing economies, who have witnessed faster price rises and several hyperinflationary episodes in recent history. The advanced economies have had their broad money grow at rates between 2 and 8%, averaging around 5%, and rarely climbing into double digits or dropping into negative territory. Developing countries have far more erratic growth rates, which fluctuate into the double digits and sometimes even the triple digits, while occasionally dropping into negative territory, reflecting the higher financial instability in these countries and currencies.

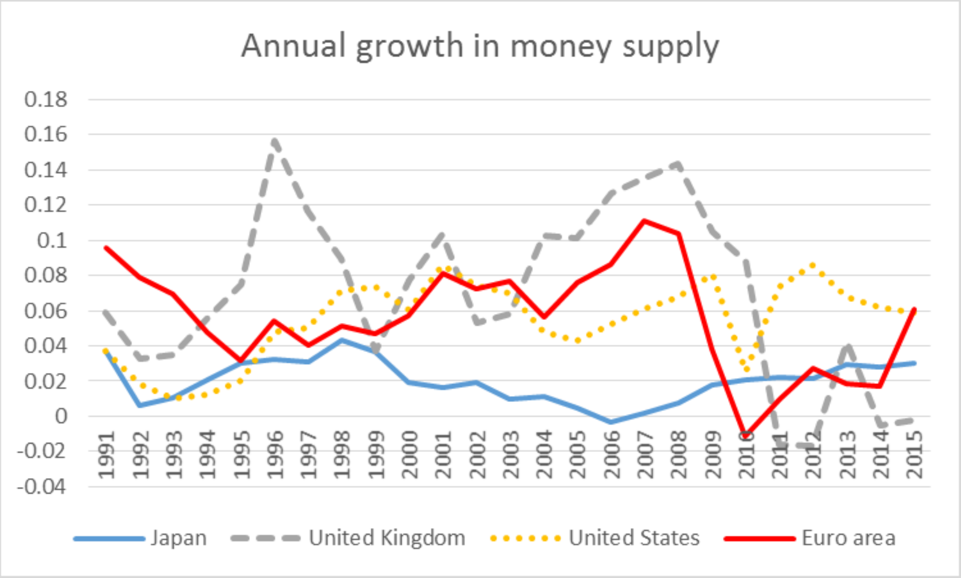


Figure 2: Broad money growth in Japan, UK, USA and the Euro area. Source: OECD.Stat.

Another popular store of value in the world economy today is gold, which continues to hold a monetary role in spite of not being any nation's official currency, as it is still used as a reserve asset by central banks and as a store of value by many individuals all over the world. Gold maintains its monetary role due to two unique physical characteristics that differentiate it from other commodities: Firstly, gold is so chemically stable that it is virtually impossible to destroy, and secondly, gold is impossible to synthesize from other materials, and can only be extracted from its unrefined ore which is extremely rare in earth. The chemical stability of gold implies that virtually all of the gold ever mined by humans is still more or less owned by people around the world. Humanity has been accumulating an ever-growing hoard of gold in jewelry, coins, and bars that is never consumed and never rusts or disintegrates. The impossibility of synthesizing gold from other chemicals means that the only way to increase the supply of gold is by mining gold from the earth, an expensive, toxic, and uncertain process in which humans have been engaged for thousands of years, with ever-diminishing returns. This all means that the existing stockpile of gold held by people around the world is the product of thousands of years of gold production, and is orders of magnitude larger than new annual production. Over the past seven decades, with relatively reliable statistics, this growth rate has always been around 1.7%, never exceeding 2%.

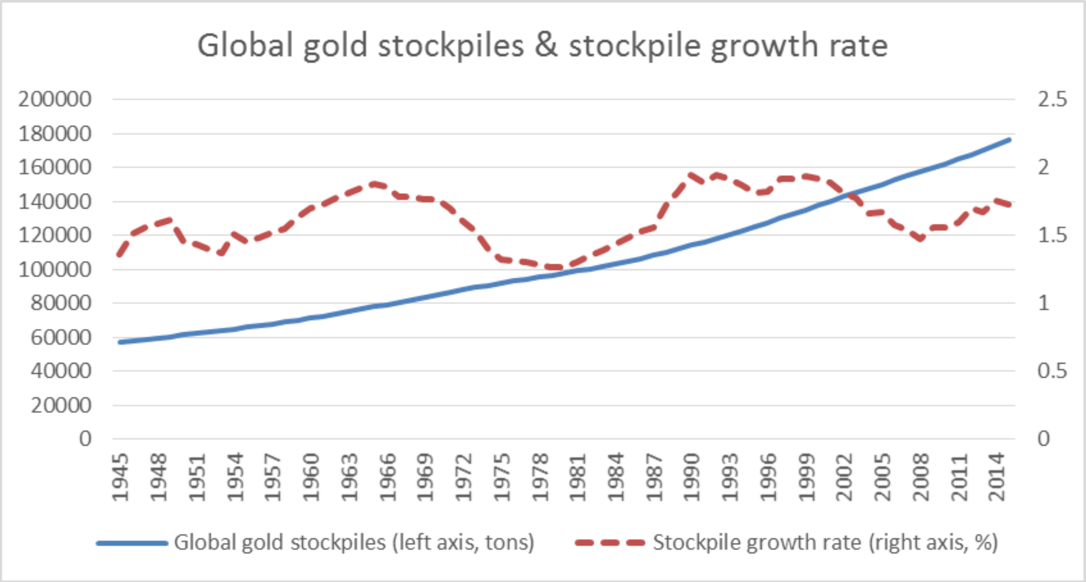


Figure 3: Global gold stockpiles and annual growth

A key characteristic that distinguishes good forms of money is that there is a strong predictability to their supply, which guarantees to holders that they will not unexpectedly witness a quick drop in the purchasing power of the currency, making them attractive as a store of value. In the case of gold, this is guaranteed by the physical characteristics of gold. In the case of national currencies, this is reliant on central bank credibility. In countries where central banks maintain a certain degree of independence and are able to resist political pressure to increase the money supply, central banks' credibility is high and the growth in the supply of the currency is predictable. Citizens as well as foreigners will use the currency as a store of value.

Central banks also have a mandate to ensure monetary and financial stability. As demand for their currency varies, central banks alter the parameters of their monetary policy in an attempt to prevent prices from fluctuating too quickly. If there is a financial panic or a deflationary collapse in the money supply due to financial institutions' insolvency or large-scale defaults, central banks stand ready to lend to these financial institutions to counteract this deflationary drop. Most modern developed country central banks have been successful in preventing their currencies' purchasing power from being too volatile, and in the financial crisis of 2008-9, they succeeded in preventing a large deflationary collapse.

In the case of gold, the new supply from mining is very predictable, making it largely insignificant to the determination of the price. The price is determined from buyers and sellers of existing stockpiles of monetary, industrial, and jewelry demand. While there is no equivalent of a central bank for gold, the world's central banks continue to hold a large fraction, estimated at around a sixth, of the world's total gold stockpile. Central Banks began reducing their total gold holdings in the late 1960's, but the reduction was at a very slow pace. Under the terms of the Central Banks' Gold Agreements, started in 2000, central banks have attempted to maintain the price of gold in a stable range by selling their gold reserves at a controlled pace, to prevent large dumping that drives the price down and devalues their holdings (Tcha, 2003). Since 2009, central banks have shifted from being gold sellers to gold buyers.

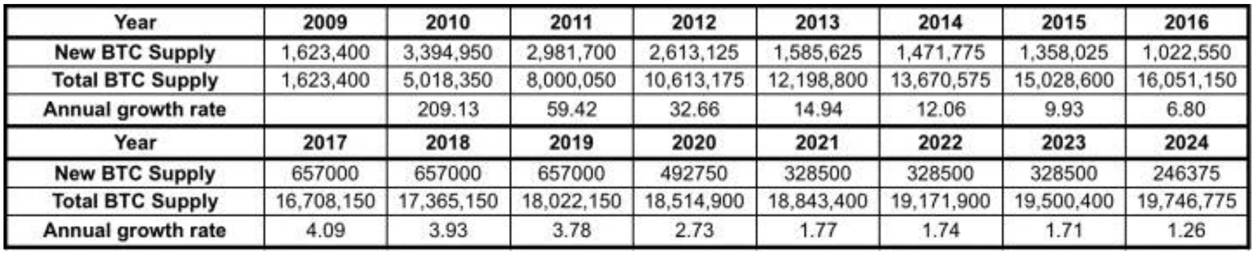
The next section of the paper examines five cryptocurrencies' monetary policy and design parameters to compare them to the traditional monetary assets.

3. Overview of Cryptocurrencies

It would be impractical to overview the monetary issuance strategies of all 700+ cryptocurrencies in existence, so a selection needs to be made. The five currencies with the highest market cap at the time of writing were chosen. Each one of them offers an instructive lesson from examining their issuance strategy that is representative of many other cryptocurrencies. As the first and most popular cryptocurrency, Bitcoin sets the standard for cryptocurrencies with its fixed supply cap and decreasing growth rate. Litecoin copies Bitcoin's monetary policy but with important differences in the network properties that carry significant implications on the credibility of the growth schedule. Ethereum has a currency, ether, which is needed to operate the smart contracts of the platform, with a higher issuance rate and a central authority in charge of it, which is set to change the policy in an unknown way in the next year. Ripple created a very large supply initially, most of which is owned by the currency issuers, fractions of which are sold to users. Steem is a currency issued as a reward for writing content in the social media network behind the currency, offering a good example of a cryptocurrency backed by an asset. A detailed treatment of each coin follows.

1. *Bitcoin*

Bitcoin is programmed to record all transactions into a new block every 10 minutes. When a member of the network verifies the transactions of a block, and solves the mathematical Proof-of-Work[ii] associated with it, they are rewarded with newly issued bitcoins. For the first 210,000 blocks, the reward associated with each block was 50 bitcoins. Starting November 28, 2012, after 210,000 blocks were mined, the reward was halved to 25 bitcoins, and on July 9, 2016, after a further 210,000 blocks were mined, the reward halved to 12.5 bitcoins per block. The reward is programmed to halve every four years, roughly, until the incremental addition of coins disappears around the year 2140. Table 2 shows the actual supply growth of BTC and its growth rate. Actual numbers are shown for years 2009-2015, while projections are used for all other years.



Year	2009	2010	2011	2012	2013	2014	2015	2016
New BTC Supply	1,623,400	3,394,950	2,981,700	2,613,125	1,585,625	1,471,775	1,358,025	1,022,550
Total BTC Supply	1,623,400	5,018,350	8,000,050	10,613,175	12,198,800	13,670,575	15,028,600	16,051,150
Annual growth rate		209.13	59.42	32.66	14.94	12.06	9.93	6.80
Year	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**	**2024**
New BTC Supply	657000	657000	657000	492750	328500	328500	328500	246375
Total BTC Supply	16,708,150	17,365,150	18,022,150	18,514,900	18,843,400	19,171,900	19,500,400	19,746,775
Annual growth rate	4.09	3.93	3.78	2.73	1.77	1.74	1.71	1.26

Table 2: Bitcoin supply and growth rate

The number of new coins issued is not exactly as predicted from the algorithm because new blocks are not mined precisely every 10 minutes. In 2009, when very few people had used Bitcoin at all, the issuance was far below schedule, while in 2010 it was above the theoretical number predicted from the supply. The exact numbers will vary, but this variance from the theoretical growth will decrease as the supply grows. What will not vary is the maximum cap of coins, and the fact that the supply growth rate will continue to decline as an ever-decreasing number of coins is added onto an ever-increasing stock of coins. By July 9, 2016, three-quarters of all bitcoins that will ever exist (15.75 million) had already been mined, and only one quarter remained to be mined over the coming decades. Whereas the supply was growing very quickly in the first few years, at a rate similar to highly inflationary and unstable developing country currency, it has dropped quickly as the block reward halved twice and the stockpile grew. At the time of writing, the annualized growth rate of the supply is dropping to around 4%, putting it in the range of strong developed country currencies. By the mid-2020's, the growth rate will drop to an annual rate lower than that of gold.

This issuance schedule is highly unlikely to be altered, and Bitcoin can be said to demonstrate very strong credibility in maintaining this schedule. In order for any change to happen to the bitcoin software, such as a change to the issuance model, more than 51% of the processing power behind Bitcoin needs to agree on that switch. The processing power behind Bitcoin is extremely large, at 19,444,470.77 PetaFlops. To put that number in context, the processing power behind the world's 500 top supercomputers combined is 567.35 PetaFlops (Top500.org, 2016). In other words, the processing power behind the Bitcoin network is more than 34,000 times larger than the world's top500 supercomputers combined. The use of Application-Specific-Integrated-Circuit miners which are optimized precisely for Bitcoin mining and the decentralization of mining into many locations make Bitcoin mining stronger than centralized systems which run into diminishing returns to scale due to overheating.

For somebody to 'hack' into the Bitcoin network and change the issuance schedule, they would be required to marshal processing power larger than 17,000 times the power of the world's top 500 supercomputers. Alternatively, more than half of the processing power behind the distributed Bitcoin network needs to vote to change the issuance protocol. Such a change is highly impractical, for several reasons. First, it would require agreement from a majority of miners, as well as the holders of Bitcoin, and the developers of the software. While the developers might not have a strong vested interest in keeping the supply fixed, the holders and miners do. Each individual miner and holder might favor a software edit that rewards them with more coins, but no such selfish change will be accepted by all others, whose holdings will be devalued. An increase in the supply that rewards all current holders and/or miners will increase the number of coins owned by them, but decrease their coins' purchasing power since it increases the supply, and damages the network's credibility and predictability, which would hurt the value proposition of Bitcoin, and reduce demand for it as a store of value. Secondly, it is very hard to coordinate among disparate nodes and miners with no central authority able to communicate effectively with all of them, or enforce any course of action on them. Bitcoin's pseudonymous creator has disappeared leaving behind nobody in a position of authority capable of affecting change to the protocol. In other words, a change to the bitcoin protocol would require a majority of members of a disparate leaderless network holding around $10billion worth of bitcoin to agree on a course of action that is highly likely to devalue their holdings. This helps explain why there has been no significant change to the fundamentals of the Bitcoin protocol in the 8 years it has been operating, and why even highly-publicized small technical changes to the size of a block have failed to gain any significant traction, in spite of the vocal support of significant bitcoin-related businesses and developers (Popper 2016). The only changes to the bitcoin software have been edits and bug fixes that allow it to run more effectively, not changes that alter the nature of the network or its economic incentives, which can be viewed as a very stable Schelling point from which no stakeholder has an incentive to defect. A consensual distributed network has a very strong resistance to change, much larger than what would be the case in a centralized and/or coercive network whose members are forced to abide by the decisions of the central authority. Anybody who wants to change the issuance protocol of Bitcoin will find it far easier to start their own cryptocoin than attempt to change Bitcoin. For all practical intents and purposes, the issuance model of bitcoin is set in cryptographic stone.

The flipside of this inflexibility is that Bitcoin lacks any form of authority that could try to stabilize the currency value or the economy dealing with it, in the manner of central banks. While the supply growth is fixed, the demand for the currency is purely market-determined. The purchasing power of a bitcoin will fluctuate wildly with changes in market demand. An increase in adoption will cause the price to rise quickly, while large liquidations of holdings will cause the price to drop significantly. Bitcoin may have credible and predictable low supply growth but it cannot be said to offer stability.

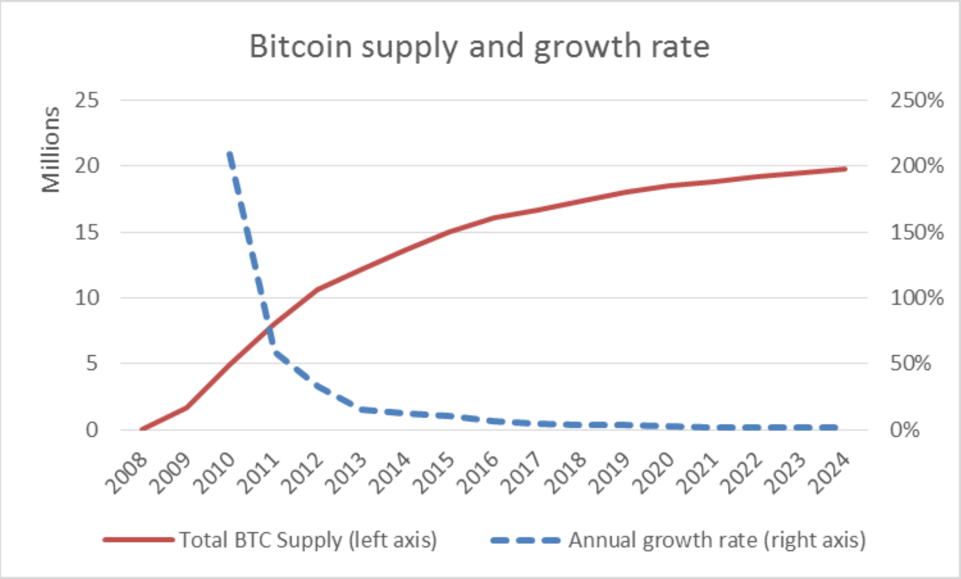


Figure 4: Bitcoin supply and supply growth rate

2. *Ether*

The second largest cryptocurrency by total market cap at the time of writing is ether, the token powering the Ethereum network, which bills itself as a smart contract platform whose contracts need ether tokens to run. Unlike Bitcoin, which can only be produced by mining, a significant quantity of ether was first introduced in August 2014 as part of a crowdfunding presale. Sixty million ether were granted to the contributors to the presale, and 12 million ether were granted to the developers of the currency and the Ethereum Foundation. The currency started trading in August 2015, after which mining of the currency began, at a rate of 5-8 ethers every 15-17 seconds, for a new annual supply theoretically ranging from around 9.3 to 16.8 million ether (Ethereum.org, 2014). In the first year of mining, up to August 2016, 10.7 million new ethers were produced, for an annual growth rate of 14.8%. Assuming the same number of ethers is issued in the coming year, the annual growth rate will be 12.9%. Figure 5 shows the growth in ether supply into the future under the minimum and maximum scenarios, as well as by projecting the growth of the first year to the future, while Figure 6 presents the potential annual growth rates in each scenario.

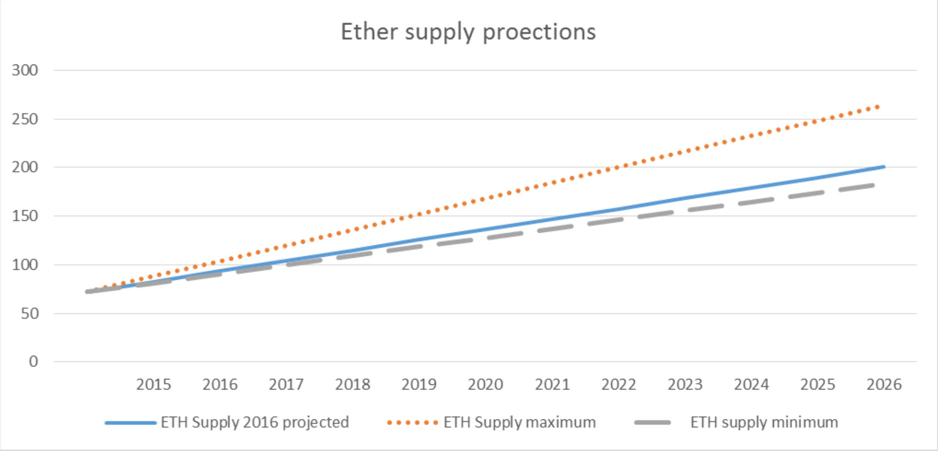


Figure 5: Ether supply projections

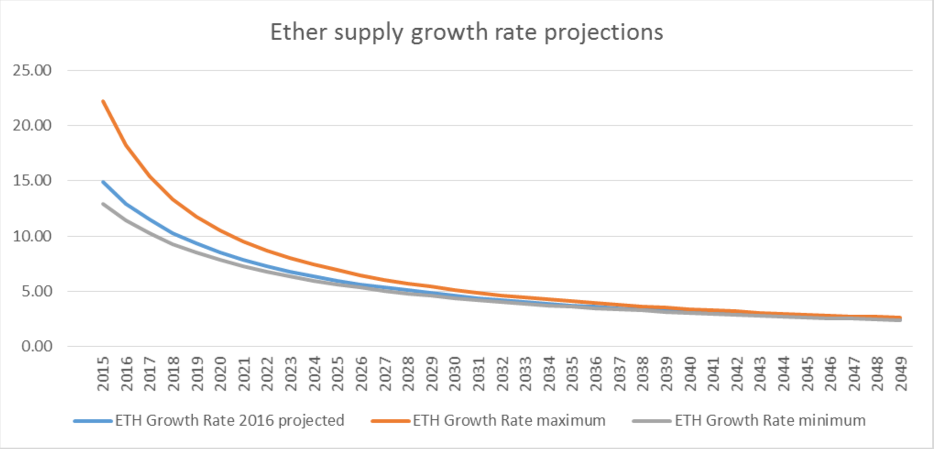


Figure 6: Ether growth rate projections

These projections, however, are probably inaccurate, since the developers behind Ethereum have announced that they plan to switch their protocol from relying on Proof-of-Work to Proof-of-Stake, and in the process, reduce ether issuance. Ethereum creator Vitalik Buterin has said in an interview that issuance will likely be reduced to somewhere between 0-2m ethers per year (Scott 2016). The Ethereum Foundation website explains that from 2017 onwards “The exact method of issuance and which function it will serve is an area of active research, but what can be guaranteed now is that (1) the current maximum is considered a ceiling and the new issuance … will not exceed it (and is expected to be much less)" (Ethereum.org, 2016).

Whether the switch to Proof-of-Stake happens, and what change it brings to the issuance of ether will be clear in due time, but what is clear now is the absence of a clear and credible commitment to a monetary issuance policy similar to that of bitcoin. The processing power behind Bitcoin is around 300,000 times larger than that behind Ethereum, meaning that a relatively small coordinated group of computers could succeed in altering the network's protocol by controlling a majority of the network. Secondly, the dedication of a large pre-mine stock of currency to the developers of the platform means that software development, processing power, and holdings of the currency are all concentrated to a large degree in the hands of the Ethereum Foundation, which has a large degree of discretion in changing the rules of the currency. The separation and distribution of powers in Bitcoin which makes changes to the parameters so difficult is not present in Ethereum.

This became apparent in the summer of 2016 after the hacking of the Decentralized Autonomous Organization (DAO), the first smart contract application of Ethereum, which held around $150m worth of ether at the time. In response to the DAO attack, the Ethereum foundation decided to "edit" the Ethereum blockchain to prevent the attacker from cashing out the ether they acquired. They succeeded in 'forking' the blockchain and introduced a new chain in which the attacker's loot had been placed in the control of the foundation. Yet they still did not succeed in bringing along all the members of the network, leading to some of them continuing to operate the old chain, which began to trade under the name Ethereum Classic. It is unclear whether both, either, or neither of the two chains will survive and continue to grow into the future. Given that another 'fork' is planned for 2017 to change the issuance supply, the future issuance policy of both chains remains far from predictable.

Further, ether is not really intended to perform the three traditional functions of money—medium of exchange, store of value or unit of account—as it is meant to be the token with which to operate the smart contracts of the Ethereum platform. Such smart contracts are effectively theoretical only at this point, and the first actual implementation, the DAO, was hacked within a few weeks of its inception. Given that it is not clear at all how much ether is needed to run a contract, how many contracts there will be, and how much demand there will be for the contracts, the currency is currently not being priced as a token for the smart contracts, but as a speculative asset for traders. The floating of ether as a free-trading currency is arguably an impediment to the success of the Ethereum smart contract platform, as it makes it impossible for potential users of these applications to estimate their actual costs, given that the cost will fluctuate with the currency. Further, the success of the smart contract platform itself would likely be self-defeating, as it would increase the demand for the currency, raising its price, and making current users face significantly higher prices for maintaining their contracts. Had the smart contract network been powered by a more stable currency, or even with bitcoin, whose value is not dependent on the Ethereum smart contract platform's popularity, it would offer a more realistic business proposition for potential users.

In conclusion, ether has a higher rate of issuance than Bitcoin at its current rate, with growth rates similar to developing country currencies in the foreseeable future. But more significant than current growth rates is that they are set to be changed and there is no predictability to what the future rates will be. The Ethereum Foundation cannot communicate credibility in maintaining their issuance schedule since they have not even specified what it would be, and even if they did, they maintain enough coding, processing power, and coin stockpiles to exercise a large amount of discretion in the future of the currency. All of these factors suggest that the ether coins are unlikely to attract significant demand as a store-of-value. The unpredictability in supply and the completely unknown demand for the coins for their use for smart contracts suggest ether is also unlikely to offer holders stability.

3. Ripple

The third largest cryptocurrency by market cap is ripple, which is produced by a private company also named Ripple, and is used to settle payments in other currencies and financial instruments over the network. Financial institutions, intermediaries and individuals working with Ripple will buy a stock of the currency with which to pay the transaction fees for every transaction they want to carry out. The transactions can be carried out in any fiat currency, digital currency, or financial asset, but the transaction fee must be paid with the ripple token (XRP). Every time a transaction takes place, the XRP used for it is destroyed irreversibly, meaning the supply is constantly shrinking.

100 billion XRPs were produced at the currency's inception, 20 billion of which were retained by the creators of the currency. The other 80 billion XRP were granted to Ripple Labs to fund operations. As of August 2016, around 64 billion of these were still owned by Ripple Labs, while around 15 billion XRP were distributed among users, developers, merchants, gateways, and market makers (Ripple.org 2016).

In July 2016, the first interbank international payment was made using the Ripple network (Crypto Coin News 2016), but it was merely a test transaction between two banks, and not a commercial transaction. It remains to be seen whether the Ripple network will gain actual commercial applications, and the benefits from the system remain largely hypothetical. Ripple claims to remove the need for intermediaries by adopting a distributed ledger, but given that the ledger is maintained by Ripple, this creates a vulnerable single point of failure, which is both a security liability and a Gordian knot of overlapping international rules and regulations that may in fact end up simply adding another layer onto the many existing layers in money transfers rather than simplifying them. Bitcoin's blockchain is secured through the extensive expenditure of processing power on proof-of-work calculations, which verifies the accuracy of all transactions without the reliance on trust in a third party. Without the proof-of-work calculations, Ripple's system relies on the security and honesty of Ripple Labs. Effectively, Ripple is not removing intermediation from international transfers, it is offering itself as an alternative to all existing channels of intermediation which have evolved over centuries of iterative success and failure. Ripple's success depends on banks and regulators worldwide abandoning current practices wholesale and migrating to a system built on trust in Ripple. The introduction of ripple as a trading currency is another significant obstacle to the success of the Ripple payments technology. Individuals or institutions looking to adopt the system have no possible way of calculating the cost of the transactions given that the cost is denominated in a currency that fluctuates in value. Had the price of the transactions been quoted in a standard currency, it might have the chance to demonstrate cost reductions to potential users, but as it stands, it can only advertise hypothetical improvements.

Yet, even if the payment network succeeds, it would be inaccurate to characterize XRP as a form of money, as it is not designed to be a medium of exchange, store of value, or unit of account; but only for processing transactions through the network. XRP is better understood as a token for using the Ripple network, not as a currency of its own right, in spite of actually trading on exchanges. The fact that the owners of the currency hold such a large stake in it will also prevent it from achieving wider adoption, as investors are unlikely to want to store wealth in a currency whose value can be controlled by the creators controlling 85% of the supply, who could crash the price if they dump their holdings. Further, the centralization of issuance in the hands of the Ripple firm means that there is no credible commitment to maintaining the supply at its current level, as is the case with Bitcoin and its proof-of-work secured algorithm. Should the currency achieve wide adoption, there is nothing to stop the owners of the currency from increasing its supply, devaluing holders' XRP stocks.

In conclusion, Ripple has no issuance schedule, but the ownership of 85% of the total supply by the currency creators makes that irrelevant. There is no possibility for the currency creators to demonstrate credibly what they will do with their large holdings, and there is no predictability to the demand for the XRP tokens, making the currency unstable.

4. *Litecoin*

Litecoin is one of the earliest cryptocurrencies to emerge, and is very similar to Bitcoin in most respects, as it was born out of making small modifications to the Bitcoin software. The most notable difference between the two currencies is that Litecoin generates a new block every 2.5 minutes, whereas Bitcoin does so every 10 minutes. Since Litecoin issues the same number of coin rewards per block and adopts the same halving schedule as Bitcoin, Litecoin's total supply is capped at 84 million coins, four times that of Bitcoin. Though there are more Litecoins than Bitcoins, the theoretical supply growth rates for Litecoin and Bitcoin are identical, but Bitcoin's supply growth rate is always lower than that of Litecoin at any given point in time since Litecoin issuance started in October 2011, almost three years after Bitcoin's.

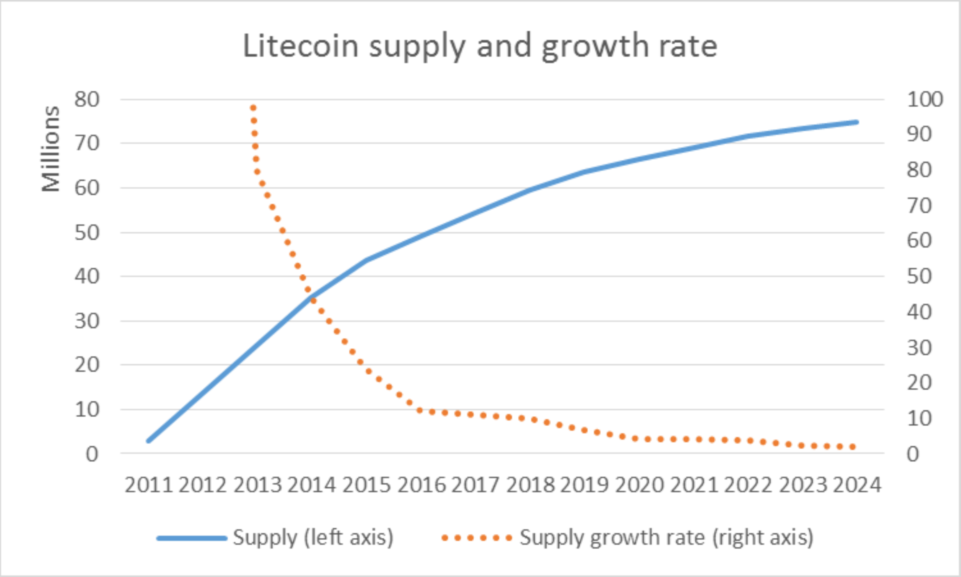


Figure 7: Litecoin supply and growth rate

While there is nothing to differentiate the monetary policy of the two currencies, the difference in the processing power is what has guaranteed Bitcoin the supremacy in attracting investments and in use for settling transactions. Bitcoin's hashing power is roughly a million times larger than that of Litecoin, making it a network far more secure and resistant to attacks, and making its monetary policy far more credible. It would not be very difficult for a relatively small amount of processing power to coordinate to constitute a majority of the network hashing power and to vote to alter the Litecoin issuance algorithm to reward a certain party with extra coin, or to alter the issuance schedule. Such a scenario may have also been possible in the very early days of Bitcoin, but it is today unfathomably difficult. This security and immutability of Bitcoin's monetary policy, along with its first mover advantage, make new investments overwhelmingly flow to Bitcoin, which has a market cap 20 times larger than that of Litecoin. This, in turn, drives computing power to also go towards securing the bitcoin network, since its mining rewards are the most valuable. The result is that even as Litecoin essentially copied Bitcoin, and supposedly improved on it by making transactions faster, it has never come close to having Bitcoin's processing power or market value.

5. Steem

The newest of the cryptocurrencies analyzed in this paper is STEEM, one of three tokens underpinning the Steem social media network, along with Steem Power and Steem Dollars. The mechanisms of the operation of the network are highly complex and cannot be summarized in this paper.[iii] These tokens are conditionally convertible to one another, and are used to reward those who produce content for the Steem website. Some restrictions exist on withdrawing Steem dollars from the system and selling them to incentivize long-term holding. Holders also get rights to vote on the value of content and the rewards accruing to content creators. STEEM supply is increasing at a level of 100% per year, 90% of which is reallocated to current holders, while 10% goes to fund content creators. With this high rate of supply increase, the creators state the supply would become so unfathomably large that it would exceed modern CPU processing capacity within some years, and so they perform a 10:1 reverse split every 3 years to bring the supply down. One could approximate the process with a 5% increase in the supply of STEEM every year, with the difference being that traditionally, increases in the supply of money tax holders, whereas in STEEM's model, because holders are rewarded by issuance in proportion to their stake, Steem's issuance is a tax on late adopters with smaller stakes and a subsidy to early adopters with large stakes. The supply growth cannot really be compared to that of regular currency, since it is a system that heavily rewards the very few earliest adopters at the expense of newcomers.

While rewarding the holders is meant to make the currency a more attractive store of value, it is only attractive for the very early adopters who have already accumulated large stakes and will continue to grow their stakes far faster than new adopters, since the larger the holdings, the larger the reward. It is far from clear that this sort of issuance schedule will appear favorable for new investors looking to invest in the currency: the gains accruing to them will be dwarfed by those accruing to the very early adopters and currency creators.

Unlike national currencies, gold, bitcoin, and litecoin, which are only meant to function as a currency; Steem can be grouped with ether and ripple in that their currencies are tokens to be deployed for a specific virtual application. On top of the variation in currency supply and demand determining its value, the popularity of the application plays an important role in determining the value of the currency. In the case of Steem, this application is a voting and rewards system on social media content. Many such social media platforms exist already, and their popularity is unpredictable and varies greatly with time. The ebb and flow of bloggers and readers to the platform would make the currency appreciate and depreciate, undermining its attractiveness as a store of value. On the other hand, the highly fluctuating purchasing power of the currency will in turn make the social media platform less attractive as a venue for bloggers who want to gain money form blogging. The restrictions on withdrawing the money make Steem not very liquid, and bloggers would naturally prefer payment in a more liquid instrument.

While the system does claim to employ a blockchain of sorts, it is only a blockchain in name as it bears no relation functionally to an actual distributed ledger secured via open proof-of-work. The operators of the social media network effectively control the blockchain and can offer no credible guarantee that they will not change the supply growth rate.

4. Analyzing supply growth, credibility and stability

1- Supply growth

Of all the cryptocurrencies studied here, and the ones this author has investigated, Bitcoin is the currency with the lowest growth rate for the foreseeable future. Bitcoin's supply growth rate has already passed through the initial phase of being very high, and has dropped to the range of the stable global reserve currencies. By the early 2020's, bitcoin's supply growth rate will drop below that of gold. Any new digital currency introduced from now on will face a virtually insurmountable obstacle in the shape of Bitcoin's low supply growth rate. If the new currency starts with a high supply growth rate, it would not be as attractive to potential investors as Bitcoin. If it starts with a low supply growth rate, it would be granting a low number of coins as reward to miners, and so would not attract significant processing power to protect the network, making it unattractive as a store of value. Cryptocoins compete for the same pool of holders and the processing power that secures their holdings. This linkage makes both new holders and miners better off using bitcoin, which only becomes more secure the more it is used. The obstacles to creating an attractive safe haven from a new digital currency can be likened to the obstacles to starting a new internet, separated from the existing internet. While it's not technically impossible, it must overcome significant hurdles.

Litecoin was introduced shortly after Bitcoin, and its supply growth rate is not much higher than Bitcoin, but will continue to be higher over time, though by the late-2020's both growth rates will drop below 1% and the difference between them will become negligible. Assuming Ethereum sticks to its current issuance schedule, the supply will continue to grow at a moderately high rate, not dropping below 5% until around the year 2030 and remaining above 1% for the rest of the century. Ripple's supply is completely controlled by the company behind it, while STEEM's supply will continue to grow in its eccentric schedule, increasing at roughly 5% every year, but disproportionally rewarding current holders.

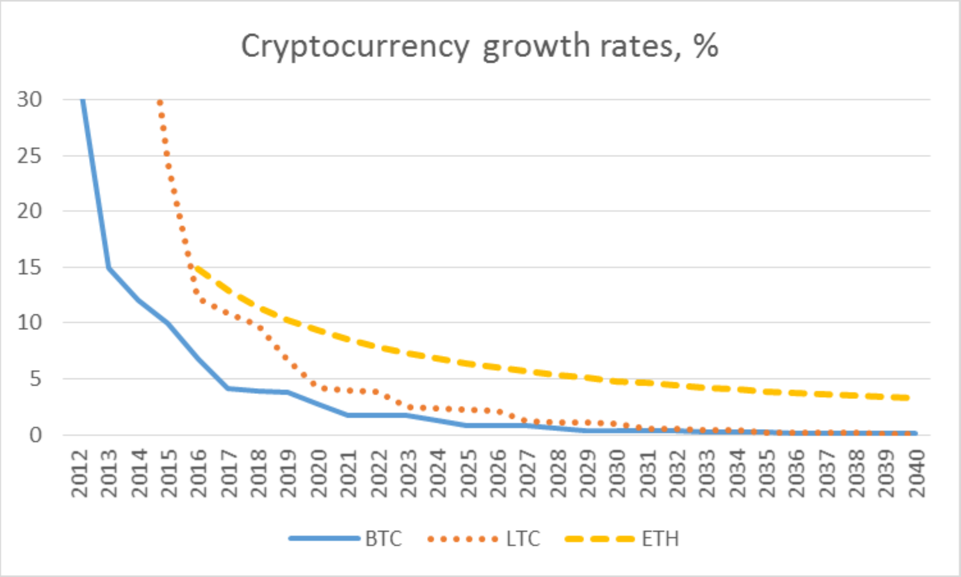


Figure 8: Bitcoin, ether and litecoin supply growth rates

When compared to national currencies and gold, Bitcoin has in its short life transitioned from a period of high supply growth similar to that of currencies undergoing severe devaluations, to currently having a rate similar to that of the world's most reliable safe haven currencies, in the single-digits. Bitcoin's supply is expected to grow at around 6% in 2016, and to continue declining after that to drop below 1% by the mid-2020s. Currencies with such a reliably low level of supply increase can attract safe haven demand, particularly from holders of currencies experiencing hyperinflation or high inflation. Even compared to the best reserve currencies, if they were to perform in the coming years in the same manner they have in the previous years, bitcoin will have significantly smaller cumulative supply growth than they will.

Figure 9 extrapolates the growth rate of the main global reserve currencies and gold over the past 25 years into the next 25 years, and increases the supply of bitcoin by the expected growth rates. By these calculations, the bitcoin supply will increase by 27% in the coming 25 years, whereas the supply for gold will increase by 52%, the Japanese Yen by 64%, the Swiss Franc by 269%, the US Dollar by 372%, the

Euro by 386%, and the British pound by 530%. If current trend with reserve currencies continue, bitcoin will have some appeal as a store of value. The appeal is enhanced by the ease of acquiring bitcoin online or in person, but a major obstacle to it is the ability of bitcoin holders to keep their bitcoins safe and the liquidity of the markets open for them to sell bitcoin.

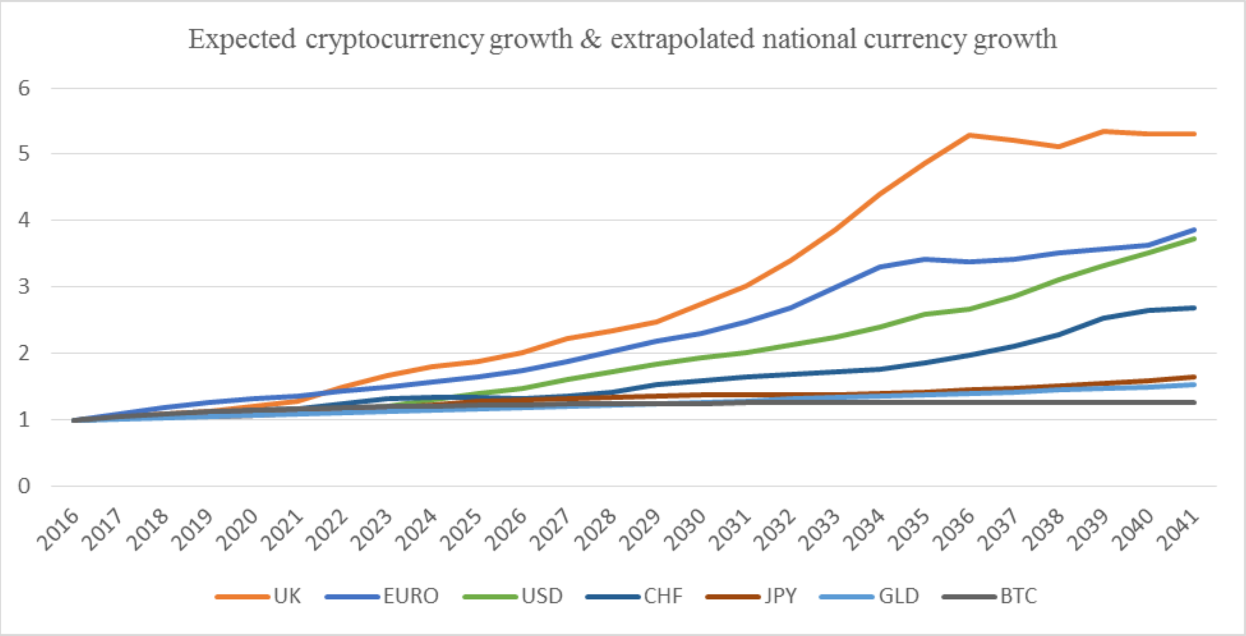


Figure 9: Expected cryptocurrency growth & extrapolated national currency growth

2- *Credibility*

More important than these projections is the credibility of cryptocoins in enforcing their supply growth rates. These currencies will only gain a significant monetary role if they can credibly demonstrate to potential holders and users that there will be no unexpected issuance of the supply. Of all the cryptocurrencies studies here, only bitcoin can be said to demonstrate a credible commitment to the announced issuance schedule. Unlike the other coins, there was no free allocation of coins to the coin's creators at the beginning. Every person who has legitimately obtained bitcoin has obtained it from buying it or mining it, both of which involved making an investment and taking a risk. The anonymity of the creator and the absence of a central body that can dictate changes to users, the distribution of bitcoin mining power and the strong economic incentive for miners to behave honestly, and the open source nature of the code all mean that the network will be extremely conservative in implementing changes. These changes go through a thorough process of testing by different coders, and once a large number of coders agree on a change, it is proposed for node operators to adopt. In the 8 years of existence, the only changes to the Bitcoin codebase have been to remove bugs and to allow Bitcoin to run more effectively and smoothly, but they did not change any of the economic parameters of the currency and payment system. There was only one incident of rolling back the bitcoin blockchain, after a vulnerability was exploited in August 2010 to produce billions of extra bitcoins. This happened when a relatively small number of people were using bitcoin, and the fork to fix the exploit was so obvious that it could easily garner a majority of nodes to support it. Since then, the code has been examined, used, and tested by far more people and no real exploit has been found, making the likelihood of any alteration of Bitcoin highly unlikely.

Ethereum has not even committed to a clear issuance schedule and the presence of a foundation that controls significant quantity of the money supply, the mining power, and the code base suggests they have a high degree of discretionary autonomy over deciding the supply growth rate. Litecoin remains a very small currency running on very little hashrate. It remains vulnerable to a 51% attack or to collusion among coders and miners to change the issuance schedule. Ripple and Steem, on the other hand, are centralized currencies controlled by single parties who can amend the supply at will. The parties behind these currencies are private entities. Unlike national currency issuers, there is no political or democratic oversight over these issuers, and so citizens are unlikely to place their trust in their currencies.

3- Stability

In the absence of a central bank with power to adjust the money supply, cryptocurrencies cannot be said to offer stability. The predictability of the supply does not translate to a predictability of the purchasing power, since the demand is highly volatile and unpredictable. All cryptocurrencies have fluctuated significantly in value since their introduction. The absence of a central bank with large discretionary powers for any of these currencies means that purchasing power stability is not really possible in the foreseeable future. The only point at which a cryptocurrency could become stable in value is when it is the only form of money used globally, and nobody is exchanging it with other currencies. This suggests cryptocurrencies are unlikely to be used as a unit of account.

For currencies used for specific applications, such as ether, ripple, and Steem, this instability is a significant hurdle to the success of the application itself, which would be better implemented in a currency independent of the application. For these applications to be useful, users need the ability to calculate revenues and costs with a sensible unit of account. If the Appcoin is freely trading, then the use of the app itself will affect the currency's value and cause it to fluctuate. Should an application become very popular, then the price of its appcoin will rise a lot, which will constitute a serious problem for users who already have commitments to use the platform in the future. For the contract or application to be useful, it must run with a measure of value that remains relatively stable over time.

On the other hand, applications and platforms can easily rise and fall in popularity, and that would mean that the value of the currency itself is dependent on the popularity of the application, which is unlikely to make it an attractive prospect as a currency. The marriage of an application with a freely-trading currency offers liabilities to both and advantages to neither. A far better solution would be to have the application run on a more stable currency, or on a native token with a fixed price and a supply arbitrarily determined by the application's designer. This would allow users to formulate an accurate measure of the costs and revenues from the application, and allow the application's producers to profit from directly selling access to their platform to users who want it. The model here is equivalent to casino chips. They are instantly redeemable into real money inside the casino, and their value is constant. Instant redeemability makes the supply irrelevant to their value. There are no known examples of casinos that have freely trading fluctuating chips, as such a casino would not attract gamblers as it leaves the outcome of their gambling out of their hands.

5. Cryptocurrencies and the functions of money

From the preceding analysis, it can be concluded that cryptocurrencies have a long way to go before being considered capable of fulfilling the three traditional functions of money. Being electronic currencies operational from any device connected to the internet, they can easily fulfil the role of a medium of exchange. However, technically fulfilling that role is one thing, and finding demand for being used as a medium of exchange is a different question, reliant on obtaining demand as a store of value or unit of account. Cryptocurrencies are currently wholly inadequate as a unit of account due to fluctuating demand and inflexible supply, and the absence of an authority that can manage the supply to maintain a constant value. Of the cryptocurrencies studied here, and arguably, of all cryptocurrencies, only bitcoin can attract demand as a store of value, due to the high degree of credibility and predictability to its supply and the resilience it has shown in eight years of existence.

Bibliography

Ammous, Saifedean. 2015. "Economics beyond Financial Intermediation: Digital Currencies' Possibilities for Growth, Poverty Alleviation, and International Development." *The Journal of Private Enterprise*, 30(3): 19-50.

Ammous, Saifedean. 2016. ‘Blockchain Technology: What Is It Good For?’ *Center on Capitalism and Society at Columbia University Working Paper #91*.

Bernanke, Ben S. 2002. “Deflation: Making Sure ‘It’ Doesn’t Happen Here.” Remarks before the National Economics Club, Washington, DC. Accessed: https://www.federalreserve.gov/boarddocs/Speeches/2002/20021121/default.htm

Crypto Coins News. (2016). Ripple Blockchain Payment from Canada to Germany Takes 20 Seconds - CCN: Financial Bitcoin & Cryptocurrency News. [online] Available at: https://www.cryptocoinsnews.com/ripple-blockchain-payment-transfer/ [Accessed 22 Aug. 2016].

CoinDesk. (2014). Bitcoin Pizza Day: Celebrating the Pizzas Bought for 10,000 BTC. [online] Available at: http://www.coindesk.com/bitcoin-pizza-day-celebrating-pizza-bought-10000-btc/ [Accessed 22 Aug. 2016].

Ethereum.org. (2016). What is Ether. [online] Available at: https://www.ethereum.org/ether [Accessed 22 Aug. 2016]

Larimer, Daniel, Ned Scott, Valentine Zavgorodnev, Benjamin Johnson, James Calfee, Michael Vandeberg. 2016. “Steem: An incentivized, blockchain-based social media platform.” [online] Available at: https://steem.io/SteemWhitePaper.pdf [Accessed 22 Aug 2016].

Popper, N. (2016). A Bitcoin Believer’s Crisis of Faith. [online] Nytimes.com. Available at: http://www.nytimes.com/2016/01/17/business/dealbook/the-bitcoin-believer-who-gave-up.html [Accessed 22 Aug. 2016].

Ripple. (2016). XRP Portal | Ripple. [online] Available at: https://ripple.com/xrp-portal/ [Accessed 22 Aug. 2016].

Scott, A. (2016). Vitalik Buterin: Ethereum's Price Rise Increases Our Sovereignty - Bitcoin News. [online] Bitcoin News. Available at: https://news.bitcoin.com/vitalik-buterin-ethereums-price-rise-increases-our-sovereignty/ [Accessed 22 Aug. 2016].

Tcha, M. (2003). Gold and the modern world economy. London: Routledge.

Top500.org. (2016). *TOP500 Supercomputer Sites*. [online] Available at: http://top500.org [Accessed 24 Aug. 2016].

Appendix 1: Average Annual increase in the broad money supply, 1960-2015. Source: World Bank

Country	Average	Country	Average
Afghanistan	18.77	Lesotho	13.85
Albania	15.14	Liberia	15.49
Algeria	17.26	Libya	16.29
Angola	293.79	Lithuania	21.44
Antigua and Barbuda	9.46	Macao SAR, China	14.52
Argentina	148.17	Macedonia, FYR	12.14
Armenia	100.67	Madagascar	14.97
Aruba	9.26	Malawi	23.84
Australia	10.67	Malaysia	14.21
Azerbaijan	109.25	Maldives	17.84
Bahamas, The	7.96	Mali	12.05
Bahrain	14.11	Mauritania	14.93
Bangladesh	17.61	Mauritius	15.41
Barbados	12.08	Mexico	27.85
Belarus	76.74	Micronesia, Fed. Sts.	2.98
Belize	10.09	Moldova	54.71
Benin	12.76	Mongolia	38.13
Bhutan	19.31	Morocco	11.65
Bolivia	184.28	Mozambique	29.83
Bosnia and Herzegovina	16.28	Myanmar	20.83
Botswana	20.12	Namibia	18.10
Brazil	266.57	Nepal	18.45
Brunei Darussalam	6.24	New Zealand	12.30
Bulgaria	40.66	Nicaragua	480.24
Burkina Faso	12.71	Niger	11.70
Burundi	14.69	Nigeria	24.18
Cabo Verde	14.48	Norway	9.54
Cambodia	26.19	Oman	15.37
Cameroon	11.23	Pakistan	15.09
Canada	11.92	Panama	13.06
Central African Republic	9.20	Papua New Guinea	12.60
Chad	11.20	Paraguay	20.96
Chile	56.15	Peru	198.00
China	21.82	Philippines	16.43
Colombia	22.13	Poland	38.68
Comoros	9.83	Qatar	18.00
Congo, Dem. Rep.	410.92	Romania	32.61
Congo, Rep.	12.27	Russian Federation	42.70
Costa Rica	22.42	Rwanda	15.07
Cote d'Ivoire	11.79	Samoa	13.32
Croatia	17.18	Sao Tome and Principe	30.44

Czech Republic	8.04	Saudi Arabia	15.49
Denmark	8.18	Senegal	9.81
Djibouti	6.93	Serbia	35.10
Dominica	9.86	Seychelles	14.09
Dominican Republic	18.84	Sierra Leone	26.78
Ecuador	12.96	Singapore	12.14
Egypt, Arab Rep.	16.59	Slovak Republic	10.70
El Salvador	9.54	Solomon Islands	15.38
Equatorial Guinea	23.90	South Africa	13.89
Eritrea	17.74	South Sudan	42.78
Estonia	29.35	Sri Lanka	15.97
Ethiopia	13.05	St. Kitts and Nevis	11.31
Fiji	11.26	St. Lucia	10.08
Gabon	12.74	St. Vincent & Grenadines	9.45
Gambia, The	16.76	Sudan	32.52
Georgia	24.47	Suriname	31.23
Ghana	32.15	Swaziland	15.58
Grenada	9.60	Sweden	7.94
Guatemala	14.90	Switzerland	6.50
Guinea	22.77	Syrian Arab Republic	16.48
Guinea-Bissau	51.60	Tajikistan	35.83
Guyana	18.05	Tanzania	22.25
Haiti	14.82	Thailand	14.08
Honduras	15.59	Timor-Leste	23.62
Hong Kong SAR, China	8.64	Togo	12.89
Hungary	12.75	Tonga	9.92
Iceland	23.33	Trinidad and Tobago	12.53
India	15.56	Tunisia	12.59
Indonesia	24.65	Turkey	43.53
Iran, Islamic Rep.	25.22	Uganda	38.11
Iraq	16.26	Ukraine	133.84
Israel	53.11	United Arab Emirates	18.41
Jamaica	19.23	United Kingdom	11.30
Japan	10.27	United States	7.42
Jordan	13.83	Uruguay	44.87
Kazakhstan	58.80	Vanuatu	7.29
Kenya	16.28	Venezuela, RB	27.62
Korea, Rep.	23.91	Vietnam	27.31
Kuwait	11.76	West Bank and Gaza	8.65
Kyrgyz Republic	22.33	Yemen, Rep.	18.19
Lao PDR	36.76	Zambia	26.76
Latvia	20.17	Zimbabwe	15.50
Lebanon	30.00	**All countries**	**32.16**

Footnotes

[i] Sixty-six observations exceeding 200% annual supply growth were removed from this plot for better visibility.

[ii] See Ammous, 2016, for an explanation of Proof-of-Work mining and how it ensures the network's security.

[iii] Interested readers are referred to the Steem white paper: *Steem: An incentivized, blockchain-based social media platform*.