The Quarterly Review of Economics and Finance 70 (2018) 38–51

Contents lists available at ScienceDirect

The Quarterly Review of Economics and Finance

journal homepage: www.elsevier.com/locate/qref

Can cryptocurrencies fulfil the functions of money?

Saifedean Ammous [a,b,*]

[a] Lebanese American University, Lebanon
[b] Center on Capitalism and Society, Columbia University, United States

ARTICLE INFO

Article history:
Received 9 March 2017
Received in revised form 23 March 2018
Accepted 25 May 2018
Available online 12 June 2018

JEL classification:
E42
E51

Keywords:
Bitcoin
Cryptocurrency
Digital currency
Monetary supply
Innovation
Volatility

ABSTRACT

This paper analyses the monetary characteristics of five cryptocurrencies to evaluate whether they can perform the functions of money. While all cryptocurrencies can theoretically and practically serve as a medium of exchange, they are unlikely to become common and liquid media of exchange unless they can illustrate utility in one of the other functions of money. Digital currencies' rigidly inflexible supply and wildly fluctuating demand make them too unstable to be used as a unit of account for the foreseeable future. Of the five, only Bitcoin has the potential to serve as a store of value, due to its strict commitment to low supply growth, credibly backed by the network's distributed protocol and credible demonstration of the absence of any authority capable of altering the supply schedule. Other cryptocurrencies' centralized control, and use as tokens for specific applications make them unlikely to fulfil monetary functions.

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 intermittently until they were listed on an exchange in October 2009 for a price of $0.000764 per bitcoin (New Liberty Standard, 2009). 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 per bitcoin (CoinDesk, 2014). Since then, more than 160 million transactions have taken place with bitcoin, and the purchasing power of the currency has risen significantly, to around $900 per bitcoin at the time of writing, giving the total tradable coin supply a market value around $150 billion. Bitcoin's success has prompted many imitators to launch similar cryptocurrencies with varying features and economic properties. More than 1000 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: medium of exchange, store of value and unit of account. Technically 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 can fulfill this role as they trade on online exchanges, can be easily transferred online, and can carry out thousands of transactions daily. It is an altogether different proposition for a good to become a widely accepted medium of exchange, and in this regard, digital currencies have a long way to go, particularly when compared to national currencies with their networks of established financial infrastructure. While the digital nature of cryptocurrencies is highly suitable for the role of medium of exchange, this role is unlikely to grow if these currencies cannot satisfactorily perform at least one of the other two 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 with the highest market value of their tradable supply in August 2016, were analyzed: bitcoin, ethereum, litecoin, ripple, and steem. These currencies' differing features offer insights applicable to many other similar cryptocurrencies. Section II pro-

* Corresponding author at: 1515 AKSOB, Lebanese American University, Chouran, 1102-2801, Beirut, Lebanon.
E-mail address: sha2106@columbia.edu

https://doi.org/10.1016/j.qref.2018.05.010
1062-9769/

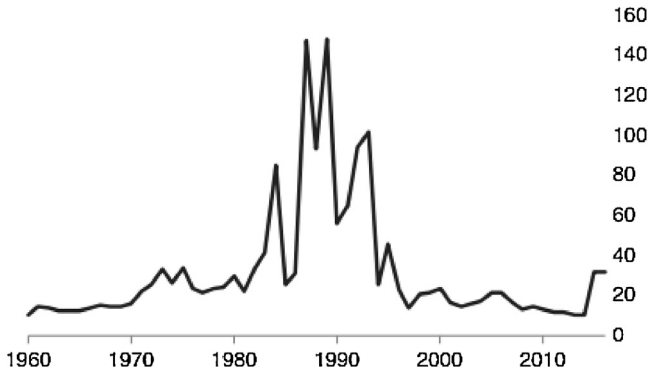

Fig. 1. Average broad money annual growth for 167 currencies 1960–2015 (% per year, excludes values higher than 200% for better visibility).
Source: World Bank.

vides 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 performing the traditional functions of money.

2. Context: national currencies and precious metals

A comparison with national currencies is useful for providing context for analyzing cryptocurrencies. While digital currencies have no central banks, and no mechanism to set interest rates and required reserve ratios for institutions that deal with them to control money supply growth, they have relatively clear paths of money supply growth which can be compared directly with other currencies. The analysis of the operational mechanisms of each currency can also shed light on the predictability of the schedule for money supply growth, and the currency's likely stability in market value, and how it compares to national currencies and gold.

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 Fig. 1,[1] and country averages for the entire period can be found in Appendix A. While the data is not complete for all countries and all years, the average growth of money supply is 32.16% per year.

The 32.16% figure includes highly inflationary periods in developing countries which skew the results upward. During these periods, people in developing countries sell their national currency and buy durable items, commodities, gold, and foreign currencies. International reserve currencies, particularly the dollar and the euro, are 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 become 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.

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

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

Source: OECD.Stat.

The world's major national currencies generally have their supply grow at predictably low rates. Developed economies have 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 usually 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 (Figs. 2–4).

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

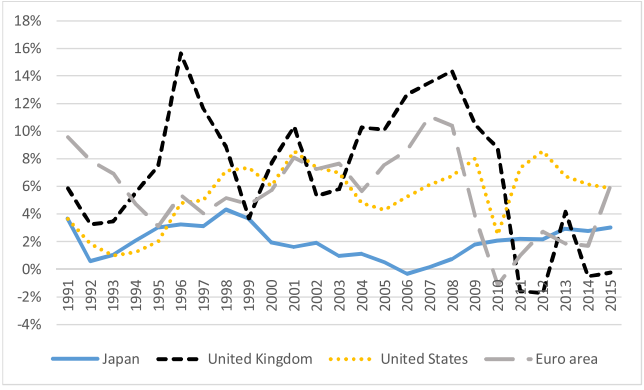

Fig. 2. Broad money growth in Japan, UK, USA and the Euro area (% per year).
Source: OECD.Stat.

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

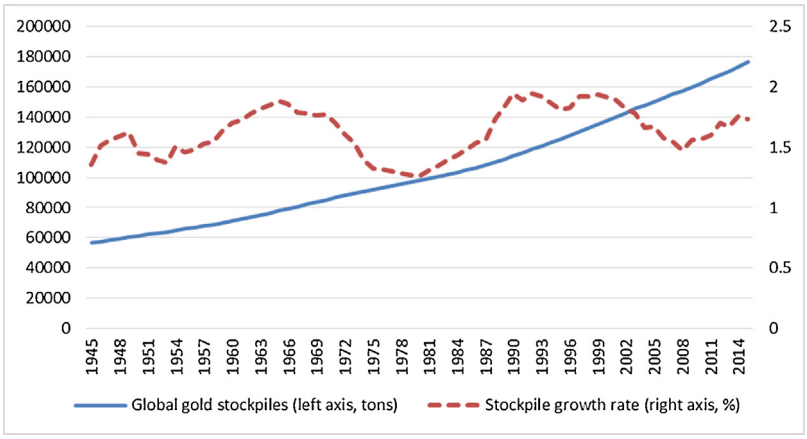

Fig. 3. Global gold stockpiles and annual growth (tons per year and % per year).

Source: US Geological Survey.

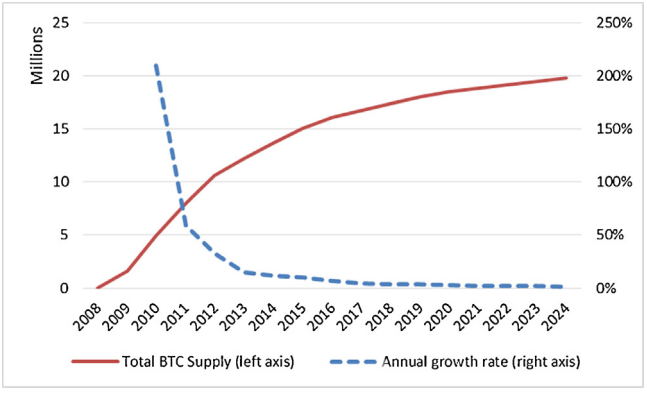

Fig. 4. Bitcoin supply and supply growth rate.

not consumed and does not rust or disintegrate. 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 and increasing costs. 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%.

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 monetary policy 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 financial institutions to counteract this deflationary drop in the money supply. Most modern developed country central banks have been successful in preventing their currencies' purchasing power from being too volatile.

In the case of gold, the new supply from mining is very predictable and miniscule compared to total stockpiles, 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 all 1000+ 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 a yet-to-be-determinedway 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.

Table 2
Bitcoin supply and growth rate.

Year	2009	2010	2011	2012	2013	2014	2015	2016	2017
Total BTC Supply, millions	1.623	5.018	8.000	10.613	12.199	13.671	15.029	16.075	16.775
Annual growth rate, %		209.13	59.42	32.66	14.94	12.06	9.93	6.80	4.35
Year	2018	2019	2020	2021	2022	2023	2024	2025	2026
Total BTC Supply, millions	17.415	18.055	18.527	18.855	19.184	19.512	19.758	19.923	20.087
Annual growth rate, %	3.82	3.68	2.61	1.77	1.74	1.71	1.26	0.83	0.82

Source: blockchain.info for data up to 2017. Author's projections based on Bitcoin algorithm from 2018 onwards.

3.1. Bitcoin

Bitcoin is programmed to record all transactions into a new block approximately every 10 min. When a member of the network verifies the transactions of a block, and solves the mathematical Proof-of-Work[2] associated with it, they are rewarded with newly issued bitcoins. Essentially, Bitcoin is a technology for the conversion of electricity and processing power into accurate records, rewarding members to the extent they expend resources on verification. Network members expend processing power on verifying validity of transactions, and verifying each other's verification in a highly complex iterative process that requires vast quantities of processing power and electricity but produces a ledger of ownership and transactions that is beyond dispute, without having to rely on the trustworthiness of any single third-party. Bitcoin is built on 100% verification and 0% trust.

For the first 210,000 blocks, the reward given to members with each block they verify 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.

The number of new coins issued is not exactly as predicted from the algorithm because new blocks are not mined precisely every 10 min. 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 around 4%, putting it in the range of developed country's international reserve 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. Bitcoin's software, which determines its economic parameters, is open source, and can be changed by anyone. But for any operator of the Bitcoin software to be able to communicate with the existing network, they must abide by the current network consensus rules. Should a user change the software, they will end up as part of another digital currency network, while the original network continues undisturbed. In other words, for as long as two people anywhere in the world choose to stick to the current Bitcoin consensus rules and economic parameters, Bitcoin in its current form survives (Table 3).

If some members of the Bitcoin network decided to change a parameter in the Bitcoin code by introducing a new version of the software that is incompatible with the rest of the network members, the result would be a fork, which eff ;ectively creates two separate currencies and networks. For as long as any members stay on the old network, they would benefit from the infrastructure of the network as it exists, the mining equipment, the network eff ;ect, and name recognition. In order for the new fork to succeed it would need an overwhelming majority of users, mining hashing power, and all of the related infrastructure to migrate at the same time. If it doesn't get that overwhelming majority, the likeliest outcome is that the two Bitcoins would trade versus one another on exchanges. Should the people behind the fork hope for their fork to succeed, they will have to sell their coins on the old fork and hope everyone else does the same, so that the price of it collapses and the price of the new fork rises, thus driving all the mining power and economic network to the new network. But because any change in any parameter in Bitcoin's operation is likely to have benefcial eff ;ects on some network members at the expense of others, it is unlikely that a consensus would form to shift to the new coin. More broadly, the majority of Bitcoin holders only hold it because they were attracted to the automated nature of its rules and their imperviousness to direction by third parties. Such individuals are highly unlikely to want to risk giving discretion for fundamental changes to the network to a new group proposing a new incompatible codebase. Whether such a majority exists or not is a moot point; what matters is that enough of them exist to make it always certain that they will continue with the current system parameters, unless their operation is compromised for some reason.

Barring such catastrophic failure in the current design, it is a safe bet that there will be a significant percentage of nodes choosing to stay with the old implementation, which automatically makes that choice far safer for anyone considering going onto a fork. The problem with deciding to go onto a fork is that the only way to help it succeed is by selling your coins on the old chain. Nobody wants to sell their coins on the old network to move to the new network, only to find that not everybody moved and the value of the coins on the new network collapses. In summation, no move to a new implementation with consensus rules can take place unless the vast majority is willing to shift together, and any shift without the majority shifting is almost certain to be economically disastrous for everyone involved. Because any such move to a new implementation likely gives the party proposing the change significant control over the future direction of Bitcoin, bitcoin holders, who are needed for this shift to succeed, are to a large extent ideologically opposed to any such group having authority over Bitcoin and are highly unlikely to support such a move. The existence of this group makes supporting a fork highly risky for everybody else. This

[2] See Ammous, 2018a, and Ammous, 2018b for an explanation of Proof-of-Work mining and how it ensures the network's security.

analysis may help explain why Bitcoin has resisted all attempts to change it signifcantly so far. The coordination problem of organizing a simultaneous shift among people with adversarial interests, many of whom are strongly vested in the notion of immutability for its own sake, is likely intractable barring any pressing reason for people to move away from current implementations.

This then makes the economic incentives of all parties involved in Bitcoin best served by adopting current consensus rules, which can be understood as a very strong Schelling point. The miners have to abide by the network consensus rules to receive compensation for the resources they spend on proof-of-work. The network members face a strong incentive to remain on the consensus rules to ensure they can clear their transactions on the network. Any individual coder, miner, or node operator is dispensable to the network. If they stray away from consensus rules, the most likely outcome is that they will individually waste resources. As long as the network provides positive rewards to its participants, it's likely that replacement participants will come up.

The consensus parameters of Bitcoin can thus be understood as being sovereign. To the extent that Bitcoin will exist, it will exist according to these parameters and specifications. This very strong status-quo bias in Bitcoin's operation makes alterations to its money supply schedule, or important economic parameters, extremely difficult. It is only because of this stable equilibrium that Bitcoin's monetary policy can be viewed to be immutable for all practical intents and purposes.[3]

In order for any change to happen to the bitcoin software, such as a change to the currency issuance model, the vast majority of nodes running the software need to agree to move simultaneously to a new software implementation, and to actively sell the currency of the old implementation.

The monetary schedule is essentially in a Mexican stand-off: while all members would hypothetically like to defect to a strategy that awards them more coins, they cannot pull off such a move because it would be met by opposition from all the others. 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 $150billion 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 9 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. Any party wanting to change the issuance protocol of Bitcoin will almost certainly end up with another digital currency with a far smaller hashrate securing it, while bitcoin continues as it is. For all practical intents and purposes, the issuance model of bitcoin is set in cryptographic stone; it can be copied, but not altered.

[3] A more thorough discussion of Bitcoin's immutability can be found in Ammous (2018a).

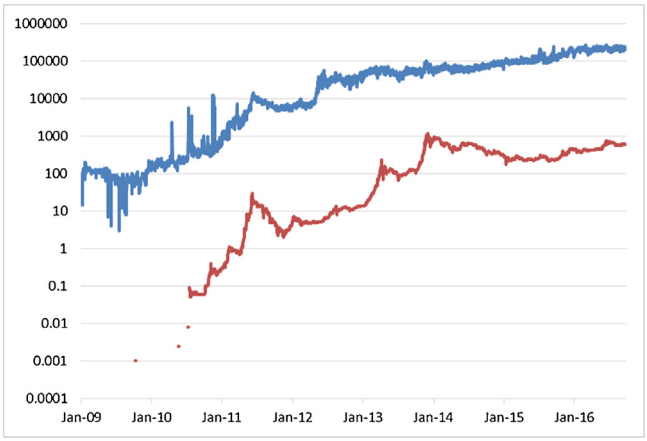

Fig. 5. Bitcoin transactions per day (top curve) and daily Bitcoin price in US Dollar (bottom curve), in logarithmic scale. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

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.

In 9 years of operation, Bitcoin's supply has continued to grow according to its predetermined algorithm, but the value of the bitcoin currency has increased along with the number of daily transactions. At the time of writing, around 200,000 daily bitcoin transactions take place, from a mere handful in 2009, Fig. 5 shows the rise in transactions and the bitcoin price in USD against a logarithmic scale. From its first recorded exchange rate of $0.000764, Bitcoin's value has increased almost a million-fold in 7 years. The growth in both transactions and price has come with a high degree of volatility. Fig. 6 shows the 30-day standard deviation of daily returns for the past 5 years of bitcoin trading. While the volatility appears to be declining, it remains very high compared to that of national currencies and gold. The 30-day volatility of the US Dollar Index is included in Fig. 6 to provide perspective.

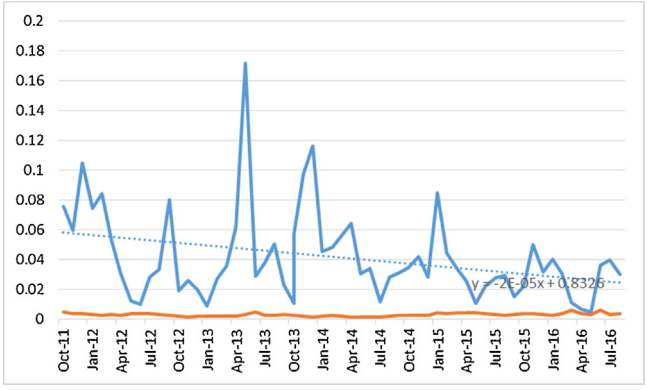

Fig. 6. Bitcoin (top curve) and USD (bor) volatility: standard deviation of daily returns over 30-day periods. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

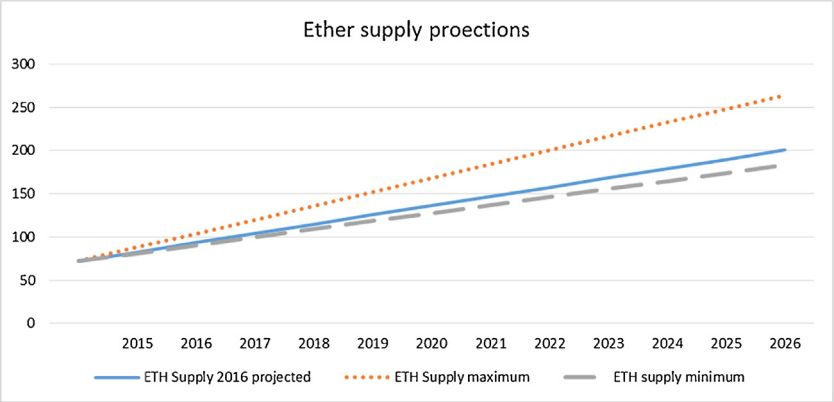

Fig. 7. Ether supply projections.

3.2. 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 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%. Fig. 7 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 Fig. 8 presents the potential annual growth rates in each scenario.

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 0–2 m 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 it is far more conceivable for a relatively small coordinated group of computers to alter ethereum'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, giving it some degree of discretion in changing the rules of the currency, which no such party holds in the Bitcoin network (Figs. 9–16).

This became apparent in the summer of 2016 after the hacking of the Decentralized Autonomous Organization (DAO), the first high-profile smart contract application of Ethereum, which held around $150 m 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, whose token 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, but the important conclusion from this episode was that Ethereum's blockchain cannot really be said to be an accurate immutable ledger

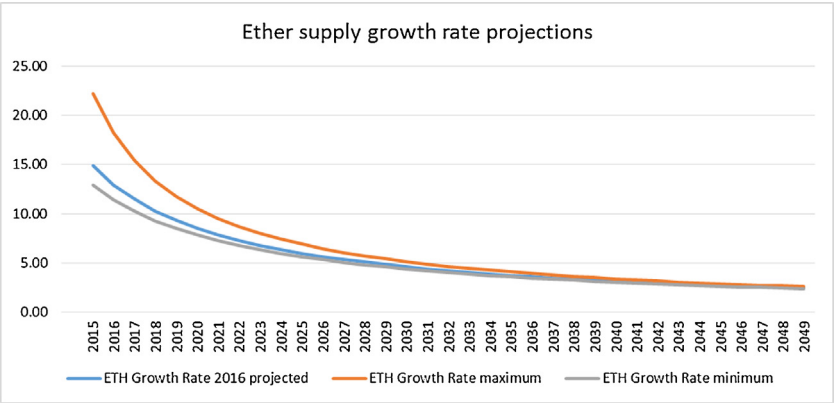

Fig. 8. Ether growth rate projections.

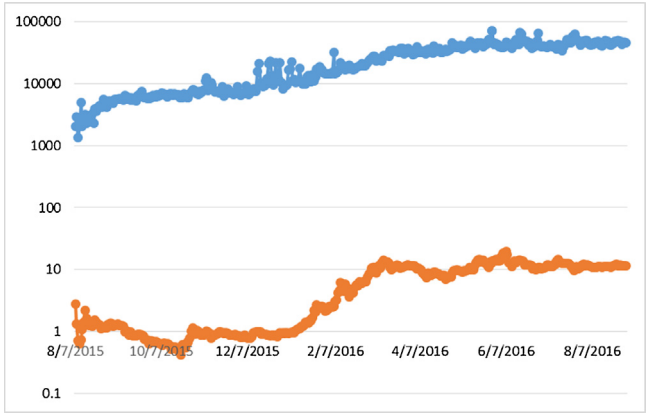

Fig. 9. Ether price in USD (orange) and transactions per day (blue), in logarithmic scale. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

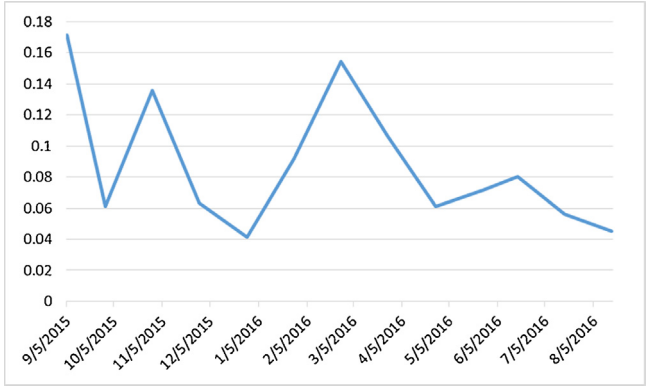

Fig. 10. Ether standard deviation of daily return over 30-days.

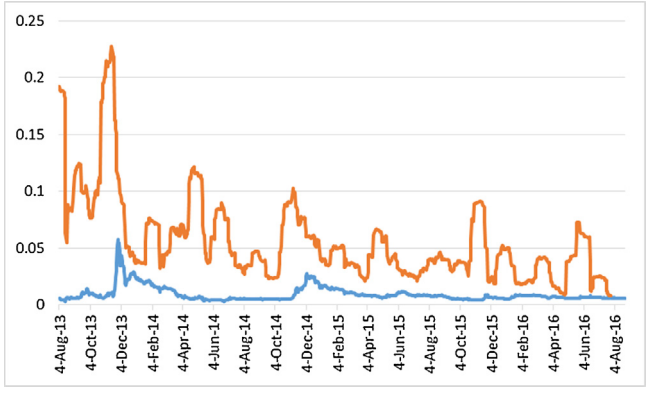

Fig. 11. Ripple price in US Dollars (in blue) and 30-day volatility (in orange). (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

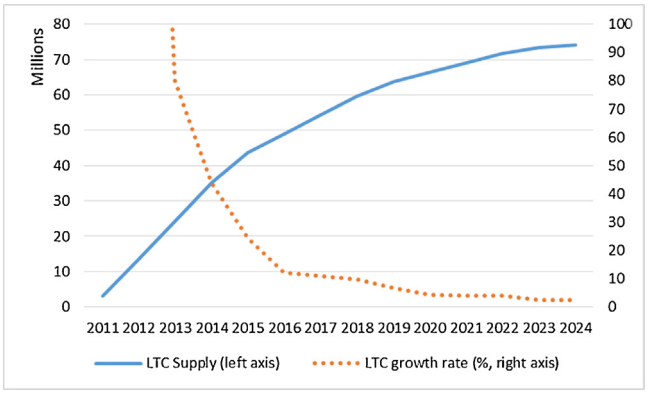

Fig. 12. Litecoin supply and growth rate.

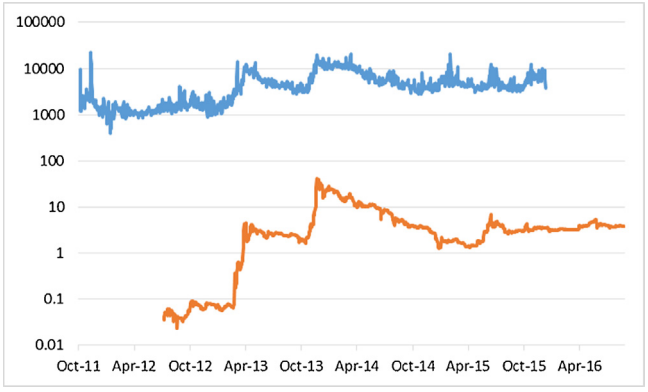

Fig. 13. Litecoin daily transactions (in blue) and price in USD (in orange). (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

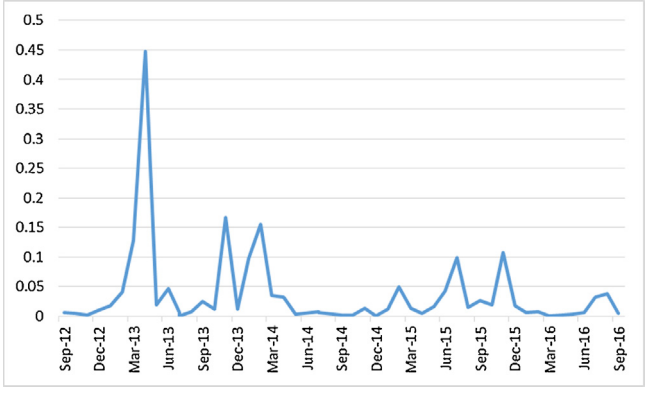

Fig. 14. Litecoin 30-day average standard deviation of returns.

of transactions, such as that of Bitcoin, as it was possible to roll the chain back due to one central party controlling a majority of the software development, coin stocks, and processing power.

Further, while ether is intended as a medium of exchange for operating contracts on the network, it is not intended to be a store of value or unit of account. Such smart contracts are effectively theoretical only at this point, and no single commercial implementation has been successfully deployed. 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's current valuation cannot be said to reflect any fundamentals for the currency as a token for the smart contracts. 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 potential users the possibility of accurately calculating costs and benefits.

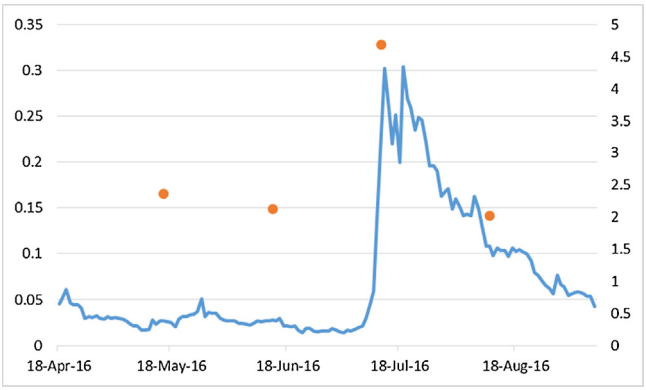

Fig. 15. Steem price in USD (in blue, right axis) and 30-day volatility (orange dots, left axis). (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

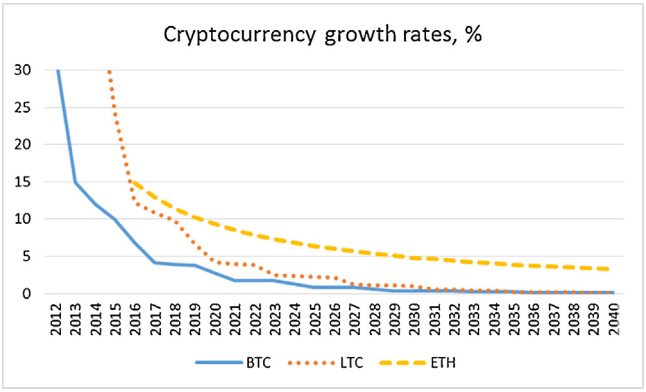

Fig. 16. Bitcoin, ether and litecoin supply growth rates.

The first sale of ether occurred during the Ethereum Foundation presale, between 22 July 2014 to 2 September 2014, at a rate of 2000 ETH per 1 Bitcoin. Based on Bitcoin's price at that time, the first traded value of ether is between $0.235 and $0.316. In the two years since then, ether's value has appreciated around 40 multiples of its original value in two years—a significant rise, but nowhere near as large as the rise in Bitcoin's purchasing power since its inception, bearing in mind Bitcoin has been around for seven years to ethereum's two.

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 control significant enough coding manpower, 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 not to be used as unit of account.

3.3. 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, 2016).

In July 2016, the first interbank international payment was made using the Ripple network (Coins 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 in 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 crashed if its creators decide to sell even a small fraction of their holdings, which are around 85% of the total supply. 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. Ripple Labs could choose to act as a central bank of their currency, buying and selling it to maintain its market value within a specific range, but they would need to demonstrate credibility of being able to achieve this suc-

cessfully over many years to inspire investor confidence. The high volatility in value of the ripple token since its inception, as shown below, suggests that this has not been a concern of the creators.

As would be expected from the foregoing analysis, the ripple token has failed to appreciate significantly since its inception, as it has not gained a role as a store of value. In three years since its inception, the market value of 1 ripple token is roughly the same as what it was when the tokens were first introduced, around $0.005. This does not mean that the token did not witness any volatility; on the contrary, the market price has been extremely volatile, and it witnessed some very large rises before dropping back to its current values.

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 likely to be unstable.

3.4. 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 min, whereas Bitcoin does so every 10 min. 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.

The number of transactions carried out in Litecoin has not seen a significantly increasing trend since the network's inception, oscillating between 1000 and 10,000 for most days. The earliest price this author could find for Litecoin was at $0.035 in July 2012. Since then, the price has been extremely volatile, and has appreciated around 100-fold, oscillating between $3 and $4 at the time of writing. This appreciation, while significant, is nowhere near as large as that of Bitcoin, and helps explain why the total market value of tradable litecoin is around $190 m, as compared to more than $10b for bitcoin.

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.

3.5. 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[4]. 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 eventually exceed modern CPU processing capacity, 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 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.

The Steem network has only been around for a few months, and so there is not much to be discerned from analyzing its data, but the value of the token is, at the time of writing, below the initial

[4] Interested readers are referred to the Steem white paper: Larimer et al. (2016) *Steem: An incentivized, blockchain-based social media platform.*

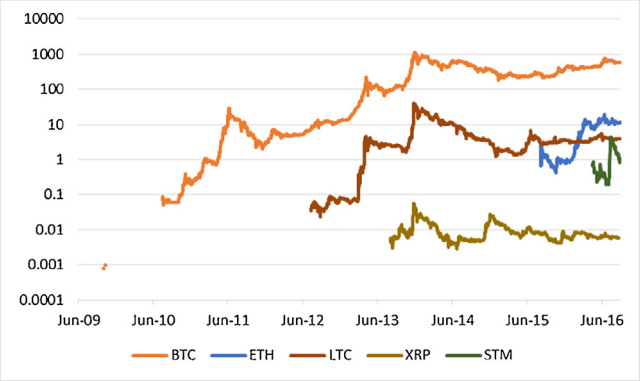

Fig. 17. Prices of digital currencies in USD, algorithmic scale.

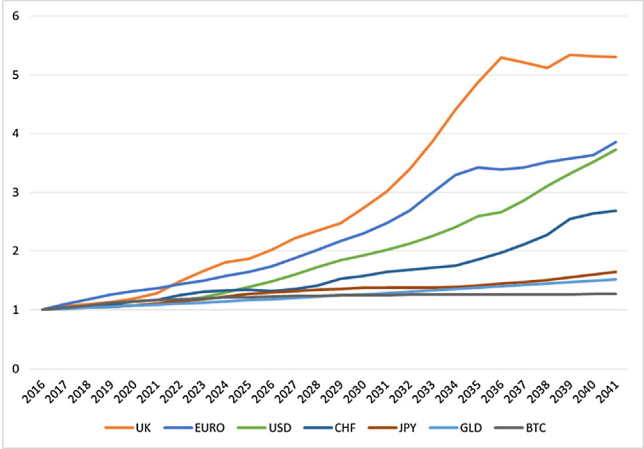

Fig. 18. Extrapolated national currency growth & expected bitcoin supply growth (2016 = 1).

price at which it traded, after having risen quickly and crashed back down a little slower. The volatility of the price has been quite high compared to the other cryptocurrencies.

4. Analyzing supply growth, credibility and stability

4.1. 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.

Litecoin was introduced shortly after Bitcoin, and its supply growth rate is not much higher than Bitcoin, and 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% per year, but disproportionally rewarding current holders.

Fig. 17 illustrates the appreciation in US Dollar value of digital currencies since their inception, showing that Bitcoin's appreciation has been far larger than all its competitors, almost approaching a million times its initial value, whereas Litecoin and Ethereum's tokens have 'only' appreciated around 100 and 40 times, respectively. Steem and Ripple have failed to appreciate significantly, which is to be expected from currencies that are not attractive as stores of value.

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.

Fig. 18 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 programmed 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 trends with reserve currencies continue, bitcoin will have some appeal as a long term store of value, for holders who are not bothered by the high volatility. The appeal is enhanced by the ease of acquiring bitcoin online or in person, but is hindered by the ability of bitcoin holders to keep their bitcoins safe.

4.2. 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 their supply will not be unexpectedly increased in a way which significantly devalues holders' coins—that there will be no unexpected increase of the supply. Whatever the supply schedule in theory, if there is no credible way for the currency to demonstrate to users that the issuance cannot be adjusted arbitrarily by any entity, it will not likely attract significant demand as a store of value. Of all the cryptocurrencies studied here, only bitcoin can be said to demonstrate a credible commitment to the announced issuance schedule. Unlike the other coins, there was no large 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 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. Only if a majority of nodes adopt a change to the protocol will it become effective. In nearly 9 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 major-

ity 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 any alteration of Bitcoin highly unlikely. Given the strong incentive for node operators to maintain the value of their currency, it is extremely unlikely to imagine a majority of them agreeing to any kind of proposal that would change the issuance parameters. Far more likely is that any proposed changes to the algorithm will either fail to garner a majority, or will split into a new digital currency.

The large appreciation of Bitcoin is likely not due to its small advantage in having a lower supply growth rate than other coins, but because it is the only digital currency that can credibly demonstrate a degree of serious commitment to its inflationary schedule, thus providing potential holders with guaranteed safety. Bitcoin can be understood as a sovereign piece of code, because there is no authority outside of it that can control its behavior. Only Bitcoin's rules control Bitcoin, and the possibility of changing these rules in any substantive way has become extremely impractical as the status-quo bias continues to shape the incentives of everyone involved in the project.

It is the sovereignty of Bitcoin code, backed by proof-of-work, which makes it a genuinely eff ;ective solution to the double-spending problem, and a successful digital cash. And it is this trustlessness which other digital currencies cannot replicate. Facing any digital currency built after Bitcoin is a deep existential crisis: because Bitcoin is already in existence, with more security, processing power and an established user base, anybody looking to use digital cash will naturally prefer it over smaller and less secure alternatives. Because the replication of the code to generate a new coin is almost costless, and the imitation coins proliferate, no single coin is likely to develop any sort of significant growth or momentum unless there is an active team dedicated to nurturing it, growing it, coding it, and securing it. Being the frst such invention, Bitcoin demonstrating its value as digital cash and hard money was enough to secure growing demand for it, allowing it to succeed when the only person behind it was an anonymous programmer who practically spent no money on promoting it. Being fundamentally knock-off ;s that are very easy to recreate, all altcoins do not have this luxury of real-world demand, and must actively build and increase this demand.

This is why virtually all altcoins have a team in charge; they began the project, marketed it, designed the marketing material, and plugged press releases into the press as if they were news items, while also having the advantage of mining a large number of coins early before anybody had heard of the coins. These teams are publicly known individuals, and no matter how hard they might try, they cannot demonstrate credibly that they have no control over the direction of the currency, which undermines any claims other currencies might have to being a form of digital cash that cannot be edited or controlled by any third party. In other words, after the Bitcoin genie got out of the bottle, anybody trying to build an alternative to Bitcoin will only succeed by investing heavily in the coin, making them eff ;ectively in control of it. And as long as there is a party with sovereign power over a digital currency, then that currency cannot be understood as a form of digital cash, but rather, a form of intermediated payment—and a very inefficient one at that.

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, and that helps explain why it has failed to garner anywhere close to the number of holders, transactions, or appreciation in price which Bitcoin have witnessed. Ripple and Steem, on the other hand, are centralized currencies controlled by single parties who can amend the supply at will. Unlike national currency issuers, there is no political or democratic oversight over these issuers to ensure they do not abuse their ability to increase the supply. According to Friedrich Hayek (1978), private providers of money can compete in a free market and make their currencies attractive by offering guarantees of maintaining their purchasing power. In reality, however, the parties behind these centrally-controlled cryptocurrencies have not even made a significant effort to express a clear and coherent supply increase schedule to their users. Further, given that these coins are centralized and have easily identifiable individuals behind them, it is highly unlikely that they would achieve any sort of monetary role in modern democracies where the function of money printing has been entrusted to a state-guaranteed monopoly that has never taken kindly to competitors.

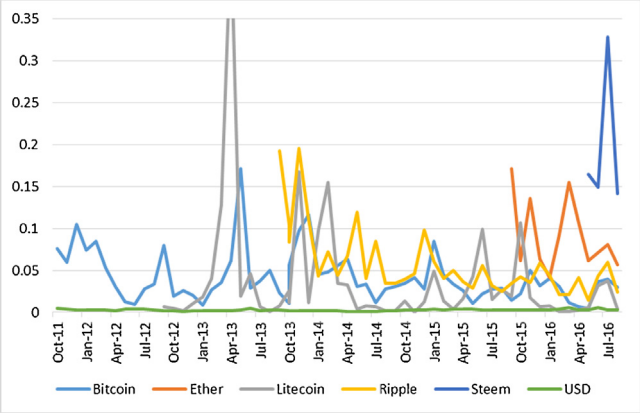

Fig. 19. standard deviation of daily returns over 30-day periods.

Bitcoin's advantage among cryptocurrencies is similar to the advantage enjoyed by the TCP/IP protocol operating the Internet. While it is possible to build a new protocol for operating a global network of machines separate from the internet, the costs of creating the infrastructure and new machines that are not compatible with the existing internet are so high as to make the concept impractical. Any entity that wants to communicate data on a network is far better off using the existing infrastructure of the internet and its array of compatible machines rather than building an alternative. Any improvements to the internet protocol will only come from machines that are compatible with the existing universal protocol. Equivalently for cryptocurrencies, users looking for a store of value are far better off investing in the Bitcoin network than attempting to build a new network. Any potential technical improvements which other coins may contain can be added to Bitcoin, but Bitcoin's security cannot be transferred to another digital currency.

4.3. Stability

It is difficult to draw any solid conclusions from the comparison of the volatility of cryptocurrencies to one another, since they have only been around for a brief period, some far more brief than the others. Fig. 19 plots the standard deviation of daily returns over 30-day periods for the available price data for all digital currencies, as well as the US Dollar for comparison. Bitcoin's volatility appears to be declining over time, making it the least volatile of the digital currencies, but there is nothing to guarantee such a trend will continue. One could also identify a trend of cryptocurrencies being more volatile in their earlier days and stabilizing in value as they mature, but with such a brief history, this is not a contention that can be well-supported by data. The only clear conclusion that can be

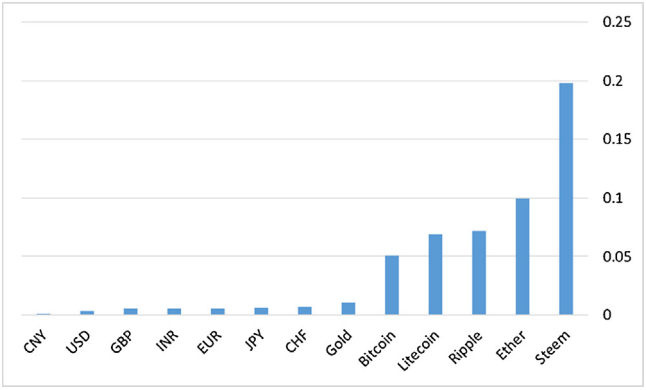

Fig. 20. Average standard deviation in daily returns over the period September 1, 2011 to September 1, 2016.

observed is that cryptocurrencies are far more volatile than fiat currencies, as evidenced by the orders of magnitude higher volatility of these currencies than the US Dollar (Fig. 20).

Examining price data for gold and major national and crypto currencies shows a marked difference in the volatility in the market price of these currencies. Daily returns were collected for the previous five years for gold, major fiat currencies and bitcoin, and for the longest periods available for the other, more recent, crypto currencies. With the exception of the Swiss Franc and Bitcoin, every cryptocurrency had a standard deviation at least an order of magnitude larger than every national currency. The most volatile national currency over the previous five years was the Swiss Franc, with a standard deviation in daily returns of 0.00699, while the least volatile cryptocurrency was bitcoin with a standard deviation in daily returns of 0.05072.

In the absence of a central bank with the 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, and can be expected to continue to do so indefinitely. The only point at which a cryptocurrency could conceivably become stable in value is when demand for holding the currency as a store of value no longer varies significantly, which can only conceivably be achieved when these currencies are held a large enough proportion of humanity that the marginal changes largely cancel out and cause little fluctuation of prices—a point highly unlikely to be reached any time soon. This suggests cryptocurrencies are unlikely to be used as a unit of account for market participants.

Table 3
Average daily percentage change and standard deviation in the market price of currencies per USD over the period of September 1, 2011 to September 1 2016. Shorter periods were used for Litecoin, Ripple, ETH, and Steem due to data limitations. Prices of all currencies measured in USD, while USD Index used for the US Dollar. National currency data from St Louis Federal Reserve Economic Data. Gold data from World Gold Council. Bitcoin data from coinbase.com, other cryptocurrencies from poloniex.com.

	Average % daily change	standard deviation
CNY	0.002	0.136
USD	0.015	0.305
GBP	0.005	0.559
INR	0.019	0.56
EUR	−0.013	0.579
JPY	0.02	0.61
CHF	0.003	0.699
Gold	−0.018	0.1099
Bitcoin	0.37	5.072
Litecoin	0.208	6.927
Ripple	0.236	7.206
Ether	0.847	9.949
Steem	1.483	19.753

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 to calculate revenues and costs with a sensible unit of account. If the application's coin 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 coin 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, and the only way to ensure that is to use a unit of account independent of the application so that its value is not driven by changes in the popularity of the application.

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 will likely increase the volatility of the value of the currencies, reducing their suitability as a store of value. 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 chips, as such a casino would not attract gamblers who could find themselves losing in real terms in spite of winning their bets.

For applications requiring a stable unit of account, this casino chip model appears the only viable model to maintaining a stable and predictable price for using the applications. Experience and theory suggest that methods of stabilizing the value of a freely-trading cryptocurrency will fail. A cryptocurrency whose value is pegged to a national currency is nothing but a riskier and less liquid method of holding that currency, and thus an inferior choice as store of value. Further, given that its price is pegged to the national currency it is likely to command less demand as a store of value than cryptocurrencies with predictably low inflation. In the absence of demand for it as a store of value and appreciation of its exchange rate, there will be very limited scope for financing the security of the network via seniorage for the miners maintaining the currency, and therefore very little security in the network. The first-mover advantage bitcoin maintains in terms of its low inflation rate and higher processing power makes any such attempt at a currency highly unlikely to succeed. NuBits was a relatively high profile attempt at producing such a currency (Wilmoth, 2014). The creators succeeded in stabilizing NuBits' exchange rate for around 18 months, but only with very low volumes of trade implying virtually nonexistent use (total volume traded in June 2016 was around $5000 per day, compared to around $60,000,000 for bitcoin) (Coin Market Cap, 2016). In June 2016, even with a very small illiquid market, the currency's peg collapsed and it lost around 75% of its value compared to the US dollar in a few days. It might be trivial for a currency issuer to maintain the fixed exchange rate for as long as demand is increasing for their currency, by increasing its supply to bring its price down. In the case of falling demand for the currency, the issuer can only stabilize its value against a national

currency by buying the outstanding supply with their reserves of the national currency. Such an operation will require accumulation of dollar reserves behind the currency, turning the issuers of the digital currency into a bank.

George Selgin (2013, 2014) suggests the intriguing possibility that a digital currency be programmed with an algorithm that can recreate any monetary rule found in the monetary economics literature, such as ensuring long-run supply growth while allowing for cyclical adjustments based on feedback from transactions volume. Alternatively, and relatedly, the currency could be programmed to have perfectly elastic supply schedule, or to target constant growth of NGDP, as economists Buchannan (1962) and Sumner (2011) suggest the Fed do, respectively. While such a possibility is interesting from a theoretical perspective, it faces significant barriers to actual implementation since it cannot demonstrate a credible commitment to any supply growth schedule by simply programming it and cryptographically securing it. What secures the supply schedule of a digital currency is not cryptography, which can always be reversed by the party that programmed it, but a distributed protocol reliant on open competition to solve proof-of-work problems, ensuring the strong incentive of all the maintainers of the network to adhere to the existing schedule. Even if a currency were to garner significant demand as a unit of account, store of value and medium of exchange, it would struggle to muster large amounts of processing power given Bitcoin's enormous first-mover advantage, and will likely remain far smaller network under the de facto control of the programmers who create it. With smaller hashing power, it is difficult for the currency to demonstrate credibility in maintaining any supply schedule, beyond the credibility of the parties issuing it. The currency would also not be credibly immune to a 51% attack to manipulate the supply or create fraudulent transactions. In short, without Bitcoin's first-mover advantage ensuring it the largest safest network, any other currency cannot credibly demonstrate that it is being run according to an algorithm that is tamper-proof. It would have been interesting to see how the growth in Bitcoin's processing and purchasing power would have fared with a different supply growth schedule, such as one of the aforementioned monetary rules, but that is a counter-factual we will never be able to witness. More than the particulars of Bitcoin's supply growth schedule, its distributed processing power advantage ensures that it will most likely remain the only digital currency running on an automatic algorithm impervious to tampering. It seems highly unlikely any currency will muster enough decentralized processing power to credibly demonstrate the monetary policies of the network cannot be altered. Future digital currencies, financial instruments, or user application tokens will likely be issued backed by Bitcoin if they aim to demonstrate security and credibility. This suggests Bitcoin might develop into an independent reserve currency of the internet, similar to gold's role during the era of the gold standard. Like gold, bitcoin's supply is not subject to the discretion of any party, and so offers an obvious choice for a reserve for anyone wanting to issue a currency whose supply they can demonstrate is limited.

5. Cryptocurrencies and the functions of money

Being electronic currencies operational from any device connected to the internet, cryptocurrencies can easily fulfil the monetary role of medium of exchange. However, it is one thing to technically fulfil that role, but finding demand for being used as a medium of exchange is a different question, enhanced by 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 resistance to manipulation and resilience it has shown in eight years of existence. It is conceivable that Bitcoin will continue to attract more demand as a store of value and gain a wider role as a medium of exchange, but the same cannot be said to most digital currencies, which seem to offer no advantages as a store of value or unit of account, and so are unlikely to attract demand as media of exchange.

Acknowledgment

The author gratefully acknowledges the contribution of the Lebanese American University Faculty Seed Fund towards his research on this topic.

Appendix A. 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**

References

Ammous, S. (2018a). Blockchain technology: What is it good for? *Banking & Finance Law Review*, *33*(3) (Issue 1, 2018).

Ammous, S. (2018b). *The bitcoin standard: The decentralized alternative to central banking*. New Jersey, NJ: Wiley.

Coin Market Cap, 2016. [Online]. Coinmarketcap.com.

CoinDesk. (2014). *Bitcoin pizza day: Celebrating the pizzas bought for 10,000 BTC*. (Accessed 22 August 2016). http://www.coindesk.com/bitcoin-pizza-day-celebrating-pizza-bought-10000-btc/

Coins News, C. (2016). *Ripple blockchain payment from Canada to Germany takes 20 s – CCN: Financial bitcoin & cryptocurrency news*. (Accessed 22 August 2016). https://www.cryptocoinsnews.com/ripple-blockchain-payment-transfer/

Ethereum org. (2016). *What is ether?* (Accessed 22 August 2016). https://www.ethereum.org/ether

Selgin George (2013), Synthetic Commodity Money. Working paper available on http://ssrn.com/abstract=2000118.

Selgin George (2014), Bitcoin: Prospects and Problems. Prepared for Hillsdale University's 2014 Free Market Forum, Indianapolis, Indiana, October 23–25.

Hayek, F. H. (1978). *Denationalisation of money: The argument refined*. London: Institute of Economic Affairs.

Larimer, D., Scott, N., Zavgorodnev, V., Johnson, B., Calfee, J., & Vandeberg, M. (2016). *Steem: An incentivized, blockchain-based social media platform*. (Accessed 22 August 2016). https://steem.io/SteemWhitePaper.pdf

New Liberty Standard. (2009). *2009 Exchange rate – New liberty standard*. Newlibertystandard.wikifoundry.com (Accessed 17 November 2016)

Popper, N. (2016). *A bitcoin believer's crisis of faith*. (Accessed 22 August 2016). http://www.nytimes.com/2016/01/17/business/dealbook/the-bitcoin-believer-who-gave-up.html

Ripple. (2016). *XRP portal | ripple*. (Accessed 22 August 2016). https://ripple.com/xrp-portal/

Scott, A. (2016). *Vitalik buterin: Ethereum's price rise increases our sovereignty – Bitcoin news*. Bitcoin News [Accessed 22 August 2016]. https://news.bitcoin.com/vitalik-buterin-ethereums-price-rise-increases-our-sovereignty/

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

Wilmoth, J. (2014). *NuBits seeks to end cryptocurrency volatility with USD Peg*. CCN: Financial Bitcoin & Cryptocurrency News (Accessed 23 Septenber 2016). https://www.cryptocoinsnews.com/nubits-seeks-to-end-cryptocurrency-volatility-with-usd-peg/