Inflation-Tracking Proof-of-Work Crypto-Currencies

Charanjit S. Jutla
IBM T. J. Watson Research Center
Yorktown Heights, NY 10598, USA
csjutla@us.ibm.com

Abstract

We show that Bitcoin and other existing egalitarian crypto-currencies are unstable as store-of-value as they fail to track inflation of local currencies closely, and the price dynamic is purely driven by speculation. Based on rational expectations equilibrium, we argue that if the coins awarded during mining are increased in proportion to increase in difficulty of the underlying cryptographic puzzle, then the price of the coin is likely to track inflation of local currencies closely over medium to long term. Further, a hyper-geometric tapering, instead of a geometric tapering, of the mining award over time is recommended for bootstrapping interest in the crypto-currency.

1 Introduction

The last decade has seen an explosion of cryptography based consensus protocols and *rare* digital tokens. As is well known, the field of (egalitarian) crypto-currencies started with publication of a white paper on Bitcoin [14] and its subsequent implementation and wide popularity. While the notion of digital money has existed for a while (see e.g. [7, 5]), and even some based on hash chains that were anonymous and allowed off-line transactions (see e.g. [17, 13]), none of these solved the double-spending problem without the use of a ledger maintained by a trusted authority. The key idea of Bitcoin was to use *proof-of work*, based on solving (computationally) hard NP-problems, to democratize the consensus protocol in a peer-to-peer setting. No registration of protocol participants is required, and hence neither an online availability of pre-defined quorum of participants is required. This allows for a decentralized ledger in an ad hoc network setting (see [4] for a more theoretical universally-composable treatment of Bitcoin functionality).

The idea "...to require a user to compute a moderately hard, but not intractable function..." was proposed by Cynthia Dwork and Moni Naor [10] in 1992 to combat spam email. However, the use of this concept of proof-of-work in making the consensus protocol egalitarian (or simply put, democratic) is surprisingly innovative, and has led to huge popularity of Bitcoin. Other cryptographic tools used in Bitcoin include (a) using a one-way function to implement a non-malleable time-stamped bulletin-board or ledger (aka blockchain; the one-way function is implemented simply using a cryptographic hash function [16] modeled as a random oracle [6]), and (b) digital signatures [18, 1, 2] to implement ownership and transfer/transactions of tokens recorded on the blockchain.

Despite the ingenious use of proof-of-work to implement a peer-to-peer permission-less consensus protocol for a time-stamped bulletin board, its actual utility to implement a crypto-currency is

mostly theoretical. Its continued popularity is more a case of public awe at the concept of proof-of-work, which in turn brings in decades of concepts developed in complexity theory and cryptography to popular discourse. While there are many well-known reasons for failure of Bitcoin to become a widely-adopted crypto-currency such as (i) (lack of) scalability of transactions, (ii) high carbon footprint, (iii) an hour or so of latency before a transaction is considered committed (with high probability), (iv) high transaction cost etc., we *now* highlight an extremely important issue based on behavioral economics that is not solved by any of the current egalitarian crypto-currencies. Before that, we should understand another concept called *proof-of-stake* that has been proposed as an alternative to proof-of-work. In the proof-of-stake consensus protocols, the ability for a participant in the peer-to-peer blockchain protocol to add a block is determined (e.g. proportionately) to their stake in the blockchain, for example the ownership of the rare tokens embedded in the history of the particular blockchain till that time. This, purportedly, avoids the high carbon footprint as no world-wide race to solve a computational challenge is required to add a new block. This also allows for a faster commitment and possibly larger scalability of transactions, and hence lower transaction cost as well. Achieving consensus in a sort of round-robin proof-of-stake protocol in an ad hoc setting, where legitimate participants may drop off suddenly, is rather complicated and security is hard to attain. Still, innovative schemes with various security guarantees under minimal network and honest-participation assumptions have been achieved (See [8, 9, 3]).

Unfortunately, while all the egalitarian crypto-currencies based on proof-of-work and/or proof-of-stake claim to bring fairness to the world economies or at least money control, they fail to be fair to people and nations that have worked hard to acquire wealth (over their life-time or ancestral history)[1]. While we are all in favor of disruptive technologies even if these have led to rise and fall of many a companies but arguably with an overall improvement in standard of living, the same cannot be said for disruptive monetary systems. While in the case of disruptive technologies, people who did not invest in these had at most a loss that can be termed an opportunity loss, but a disruptive monetary system acts like a bet against (savings and wealth of) all who did not invest in it early enough. This is abundantly clear in the case of Bitcoin, where half of all bitcoin to ever be issued, was issued in the first ten years of its existence. In contrast, gold, the store of value which Bitcoin is trying to mimic digitally, has been treasured for thousands of years, and we are still not sure if we have yet mined half of all the gold in the outer layer of Earth.

1.1 Unfairness to Current Wealth Holders.

To date 18 million bitcoins have already been mined, and only 2 million remain to be mined. Of these Satoshi Nakamoto, the founder owns one million bitcoins. This extreme scarcity of remaining coins means that if Bitcoin is to become the world reserve currency, even the most powerful nuclear-powered nations will be paupers compared to Nakamoto and other early investors. So, this extreme early ramp-up of mining in the design of Bitcoin is clearly one big flaw. We will also argue shortly that this fixation on a bounded supply is also a reason Bitcoin fails to be a good inflation tracker. But, before that we discuss why it is desirable to have a Bitcoin-like egalitarian currency to become a reserve currency of the world.

[1] A cynical viewpoint would hold that all wealth acquired is immoral/illicit, but we will stick with a more objective viewpoint.

1.2 Why is a digital egalitarian "store of value" important?

By now, even the fiercest proponents of Bitcoin have given up on Bitcoin being an enabler of day-to-day use currency because of lack of scalability of transactions. However, it is hoped that it becomes a store of value similar to gold. Most nations hold gold reserves as capital (or collateral) backing their paper (fiat) currencies. One could envision a similar role for an egalitarian digital store of value. This store of value serves as a good monetary vehicle for inter-nation trade, as well as a good balance sheet asset for raising debt to build national economies etc. For example, countries currently own gold and US dollar as reserve to bolster their balance sheets. However, the store of gold is not easily verifiable and a paper currency can lose its reserve status due to economic downfall. However, value stored on a blockchain, even in an encrypted form, can be proved to one or more parties, almost instantly, using non-interactive zero-knowledge proofs [19]. Thus, an egalitarian digital currency, if properly designed, has advantages over traditional stores of values such as gold and fiat currencies of developed countries. We next look at another extremely important factor determining the worth of a currency as store of value, i.e. the property of being an inflation hedge.

1.3 Inflation hedge/indicator.

A good store of value should also be stable in its value with respect to traditional store of value such as gold and also with respect to other currencies especially of countries that have strong economies, at least in the short term. In fact, its value should fluctuate proportional to the inflation of these strong economies and their local currencies in the medium to long term. Now, we mentioned how Bitcoin is already almost fully mined, whereas gold even after thousands of years still has lot to be mined. We now argue that this also makes Bitcoin a poor inflation index, and hence an unstable store of value.

First, the question of why all possibly mine-able gold has not been mined already is resolved by the cost of mining vs the current price of gold. Naively, a similar model applies to fair value of Bitcoin, but once again the rapid early mining of half of all Bitcoin leads to a paradoxical or at least an untenable situation, as we soon explain.

The cost of gold mining is determined by (a) laws of physics (e.g. lack of feasibility of stable fusion of smaller atomic mass elements, or just the chemistry of separating gold from igneous rocks), (b) prevalent labor cost as well as (c) equipment cost, and (d) land/mine acquisition cost. The current cost of mining gold is also (within an additive factor) more or less the current gold price. Thus, the rate of change or *marginal* cost of mining gold (in some currency X), and hence the marginal cost of gold itself, is a good reflection of inflation of an economy (in currency X). On the other hand, the cost of mining Bitcoin is determined by (i) current price of electricity, (ii) current price and current (parallel or sequential) speed of computers, (iii) current price of Internet connectivity, and (iv) the artificial parameter determining the hardness of cryptographic puzzles which is set in the protocol as a parameter rather than being a real world constraint (see Appendix A for more details). This last parameter, called *difficulty* (see Table 1), keeps the time needed to mine a Bitcoin (or next block) fixed to about 10 minutes, by dynamically changing difficulty of the puzzle based on average of previous few puzzle solving rates. Of course, another (artificial) protocol parameter is what fraction of all possible Bitcoins are deemed mined in a single puzzle being solved (i.e. single block being added). So, while (i)-(iii) are inflation indicators, the parameter (iv) is effectively being set in the Bitcoin protocol based on the current price of Bitcoin!

Year	Difficulty	#-bits Zero in HashPuzzle	Price (US $)	Coins Mined (per block)	Total Coins Mined	Ideal-1 Coins Mined (per block)	Total Mined (Ideal-1)
2009	1	32	0.04	50	0	10^{-12}	0
2012	10^6	52	4	25	7M	10^{-6}	10^{-7}
2015	$4 * 10^{10}$	67	315	18	12M	$4 * 10^{-2}$	0.1
2018	$2 * 10^{12}$	73	16K	12	15.5M	2	6K
2021	$16 * 10^{12}$	76	40K	6.25	18M	16	0.3M

Table 1: Bitcoin Difficulty and Price

This maybe counter-intuitive and not well understood, so we explain this in detail next. The upshot is that this makes Bitcoin a *poor inflation index*.

Note that the current price of Bitcoin (in currency X) determines the revenue a miner would get on successfully mining a block. For mining to be profitable, we can assume that this is within an additive factor of cost of mining a block. If the price of Bitcoin goes up drastically due to speculative reasons (for example, hoarding) and not due to underlying inflation, more Bitcoin miners would be attracted to the business. However, instead of this leading to more bitcoins being mined, which would naturally dampen the speculative price (as increased mining supply would counter decreased supply from hoarding), the Bitcoin protocol increases the parameter (iv) so that still the same number of bitcoins are mined per time interval [2]. We illustrate this with a simple setting where at price P per bitcoin, lets assume that there are N (equivalent) miners involved in mining Bitcoin. In a first setting, we will also assume that miners always sell their freshly mined coins at the market price. The expected revenue of each of the N miners is $k * P/N$ per block added to the Bitcoin blockchain (where k is the number of new coins that are awarded in each block being added to the Bitcoin blockchain), and hence also $k*P/N$ per every ten minutes. There is also additional revenue coming from transaction fees, but we will ignore this for the present discussion, as it will be more or less irrelevant. Now, suppose that due to speculation and increased demand of Bitcoin, the price of Bitcoin doubles to $2 * P$. This would naturally double the revenue of the current miners without any additional cost of mining. Thus, we can assume that this would invite new miners, and for simplicity lets assume that the number of (equivalent) miners increases to $2 * N$. Since double the computational power is now brought to bear on the hash problem, the difficulty parameter then doubles in a short amount of time. Regardless, with the number of miners doubled to $2 * N$, the average revenue of each miner is $k * 2P/2N$ per every ten minutes, which is same as before. Thus, while the price of Bitcoin has doubled, the Bitcoin mining revenue per mining cost remains the same, which is not surprising since equilibrium demands that this ratio be close to one [3]. But, more importantly, the total supply of bitcoins from world-wide mining remains the same, which is k per ten minutes.

In contrast, if gold price went up due to speculative reasons, the miners would invest more

[2] The reason this is done in the Bitcoin protocol is two fold: (a) to deter transactional instability from block chain forking, and more technically (b) to implement a global clock/timestamp consensus to be used in the protocol [14, 15].

[3] An astute reader may wonder as to what would encourage new rational miners to join in if the mining revenue per mining cost remains the same? One answer could be that they become less risk averse as the price of Bitcoin increases, hoping that increasing price implies increasing popularity and long term sustainability. Another reason could be that increasing price could lead miners to invest in better mining equipment in the hope that they monopolize mining. See Appendix A for more details on this.

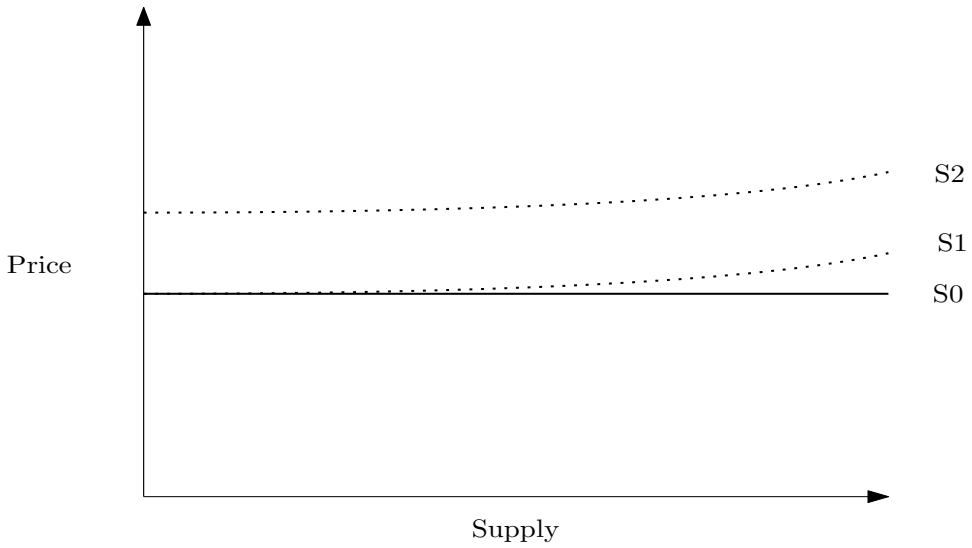

Figure 1: Keynesian Aggregate Supply Curve. S0: Pure Keynesian Supply Curve. S1: Keynesian Supply Curve after considering law of diminishing returns. S2: Same as S1, but shifted due to inflation of labor, equipment etc.

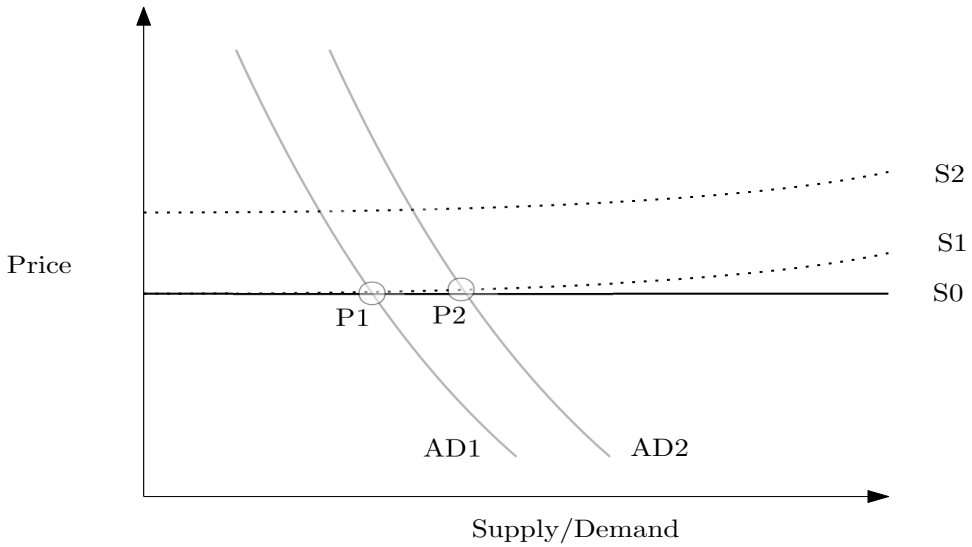

Figure 2: The aggregate demand curve overlaying supply curve. Due to speculation, the demand curve may shift right from AD1 to AD2. However, since the supply curve is essentially horizontal, the new equilibrium price P2 barely budges from P1.

labor/equipment to mine more gold per day and in the process limiting the speculative price increase to a reasonable level[4]. This is well know in macro-economics, and as explained by Keynes that the miners (or producers) in general will expand labor and equipment to increase supply to keep the price constant (see Figs. 1 and 2), as long as there is no underlying inflation in labor and equipment. Keynes, was mostly referring to this situation holding in depression, and he was

[4]Sometimes, speculation does correctly predict future inflation.

referring to overall industrial production. However, for currencies, in case of no underlying inflation, the same principle of *aggregate supply* holds, even in non-depression situations.

This inability of the Bitcoin protocol to allow increased supply to counter speculation, makes it a poor inflation index, and the price of Bitcoin is completely driven by speculation, as explained in more detail in Appendix A.

2 A Modified Bitcoin Protocol to Neutralize Speculation

The basic idea of the modified protocol is to mimic industrial production, or mining of precious metals such as gold. As explained above, and illustrated in Fig 1, whenever there is an increase in demand, or the demand curve shifts right (see Fig 2), the producers can simply increase supply by hiring more labor at the same rate as before as well as buy mining equipment at the same rate as before, *as long as there is no underlying inflation.* This way they can meet the increased demand at the same price as before (or maybe a small increase in price due to law of diminishing returns). Indeed a same phenomenon would ensue in the Bitcoin protocol, only if the number of coins being awarded (as mined) in each block increases proportionately to the difficulty parameter.

If the Bitcoin protocol were so modified, and assuming the hypothetical situation that the difficulty of the Bitcoin protocol followed the same trend over the period 2009-2021, we show in Table 1 how the number of coins being mined each year would change. We call this the Ideal-1 situation. Thus, in Table 1 we show in the last two columns how difficulty and overall mining in this ideal-1 situation would work out for Bitcoin – this is the scenario where difficulty dictates how much bitcoins per block a miner gets. We have arbitrarily set the *initial* Bitcoin mining rate at 10^{-12} bitcoins awarded per block. Of course, this data is not a good simulation, as the price of Bitcoin and hence mining supply would have been drastically different if the protocol was so modified. In fact, looking at the table (Table 1), the first two rows shows that the miners would have mined so little, that the price of Bitcoin would never have taken off at all, nor would it have attracted more miners and hence neither would have the difficulty increased. Thus, the issue remains how to make a coin worth some big value, as in a store of value? In the next sub-section we describe a scheme which incorporates decreasing mining awards over time as in Bitcoin and Dogecoin, but keeping the increase in awards in proportion to the difficulty as described in this sub-section.

2.1 The x-off-y Hypergeometric Scheme

The x-off-y scheme of awarding coins for each block mined is based on a hyper-geometric series, as opposed to a geometric series. Such a hyper-geometric series is front-loaded and the tail is much longer, essentially becoming constant as number of years tends to infinity. This is illustrated in Fig 3.

First, lets assume that difficulty remains constant at D_0. The (simple) hyper-geometric series $\phi_{a,q}$, parameterized by (a, q) is given by $\phi(k) = \prod_{i=0}^{k-1}(1 - q^i * a)$ for $k \geq 1$. In the x-off-y scheme, the initial, i.e. after first year, *reduction in coins mined per block* is y fraction. In other words, if at initiation, each block awarded N_0 coins, then after one year, each block awards $(1 - y) * N_0$ coins. Further, each subsequent year this reduction is itself reduced by x fraction. In other words, after the second year, each block awards $(1 - (1 - x)y) * (1 - y)N_0$ coins, and more generally after the

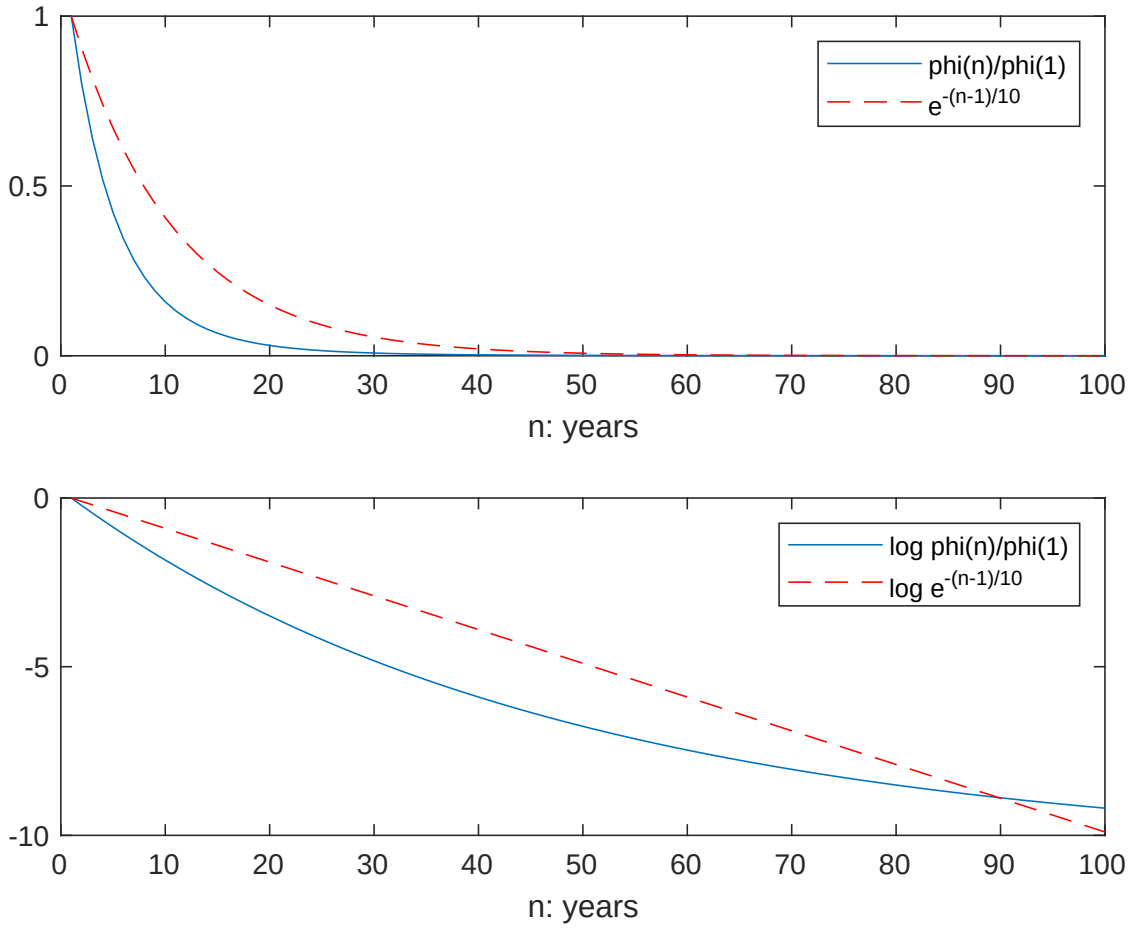

Figure 3: Hyper-geometric vs Geometric Series: (a) Normal Scale (b) Log Scale

k-th year each block awards $N_o * \phi_{y,1-x}(k)$. Thus, after the k-th year each block awards

$$N_0 * \prod_{i=0}^{k-1}(1-(1-x)^i * y).$$

If difficulty does not remain constant, then our scheme dictates that the number of coins awarded per block increases in proportion to increase in difficulty from block to block. Thus, if at the end of year one, the number of coins being awarded per block is N_1, and difficulty is D_1, then the first block in the next year will award $N_1 * (1-y) * D'/D_1$ coins, where D' is the difficulty of the first block in the new year. Similarly, if at the end of k years the number of coins awarded per block is N_k, and difficulty is D_k, then the number of coins awarded for the first block of the $k+1$-th year is

$$N_k * (1-(1-x)^{k-1} * y) * D'/D_k,$$

where D' is the difficulty of the first block in the $k+1$-th year. Of course, within a year, the coins awarded are increased or decreased based on the ratio of difficulty of consecutive blocks. Pseudocode for this scheme is given in Listing 1.

Now, we first ignore the transactions costs charged off transactions recorded in a block. Also, ignore the fluctuation in difficulty through time. In that case, in equilibrium, the price of a coin, say P_{k+1} at the start of the $k+1$-th year, will be

$$P_0 / \prod_{i=0}^{k-1} (1 - (1-x)^i * y)$$

For example, if y is twenty percent and x is two percent, then after fifty years, $(1-x)^{50-1} = 0.98^{50}$ is 0.372. Thus, after fifty years, the incremental yearly increase in price at equilibrium (ignoring inflation of local currency) will be a factor of $1/(1 - 0.372 * 0.2)$, which is 1.08. Similarly, after hundred years, the incremental yearly price increase (ignoring inflation) will be a factor of 1.028. On the other hand, the incremental increase in price after first year will be a factor of 1.25 or increase in price of 25%.

Since, $\ln(1-x)$ is close to $-(x + x^2/2 + x^3/3)$ for small x, the cumulative increase in price can be estimated by taking logarithm. Indeed, for the 2%-off-20% scheme, we have

$$\begin{aligned}
&\ln \prod_{i=0}^{k-1} (1 - (1-x)^i * y) = \sum_{i=0}^{k} \ln(1 - (1-x)^i * y) \\
&\approx \sum_{i=0}^{k-1} -(1-x)^i * y - (1-x)^{2i} * y^2/2 - (1-x)^{3i} * y^3/3 \\
&= -y * \frac{1-(1-x)^k}{x} - y^2/2 * \frac{1-(1-x)^{2k}}{1-(1-x)^2} - y^3/3 * \frac{1-(1-x)^{3k}}{1-(1-x)^3} \\
&\approx -y * \frac{1-(1-x)^k}{x} - y^2/2 * \frac{1-(1-x)^{2k}}{2x} - y^3/3 * \frac{1-(1-x)^{3k}}{3x}
\end{aligned}$$

$$\begin{aligned}
&= -.20 * (1 - .372)/.02 - .02 * (1 - .13)/.04 - .008/3 * (1 - .05)/.06 \\
&= -6.28 - 0.435 - 0.042 = -6.76
\end{aligned}$$

Thus, the cumulative increase in price (ignoring inflation of local currency) after fifty years is expected to be $e^{6.76} = 863$, i.e. about thousand-fold increase, whereas at that point the incremental increase per year based on rational expectations [12] will be about eight percent. Now, the gain in price based purely on decrease in mining award after first year is 25%. However, speculators may hoard the coins as the long term gain is supposedly much higher. However, any price increase above the rational expectations equilibrium will lead to more miners joining in. Indeed rather than buying at market price, it is beneficial to just mine the coins, as the cost of mining remains constant (even if difficulty rises, for in that case the awards are proportionately increased). Thus, speculation will remain under control as market demand will remain at most as high as market supply to maintain the price at the level of cost of mining currently or cost of mining in near future. The risk to speculation, i.e. speculation that prices-in future cost of mining, is of course the possibility that the scheme fizzles out and loses popular support. Thus the price of the coin is expected to track inflation over medium to long run, as price of digital mining (in any local currency) is a decent, although not perfect, inflation index.

2.2 Expected Number of Total Coins

Suppose, the initial parameters are so set that in the first year M_0 coins are awarded (via mining). Then assuming difficulty remains constant, during the next year the number of coins awarded will be $M_0 * (1 - (1-x)^0 * y)$, and the next year $M_0 * (1 - (1-x)^1 * y) * (1-y)$ etc. Thus, the total number of coins can be estimated, under rational expectations equilibrium, to be

$$M_0 * \left(1 + \sum_{i=0}^{\infty} \prod_{j=0}^{i} (1 - (1-x)^i * y) \right)$$

The q-Pochhammer symbol is defined by

$$(a,q)_k = \begin{cases} \prod_{j=0}^{k-1}(1 - a * q^j) & \text{if } k > 0 \\ 1 & \text{if } k = 0 \\ \prod_{j=0}^{\infty}(1 - a * q^j) & \text{if } k = \infty \end{cases}$$

Using the q-Pochhammer symbol, the estimate of the total number of coins in the x-off-y scheme, can then be conveniently written as $\sum_{n=0}^{\infty} M_0 * (y; 1-x)_n$. Since y is positive and less than one, and $1 - x$ (< 1) is close to one, we now estimate each of $(y; 1-x)_\infty$ using the Taylor series of $\ln(1-z)$.

$$\begin{aligned} &\ln \prod_{i=0}^{k-1} (1 - (1-x)^i * y) = \sum_{i=0}^{k} \ln(1 - (1-x)^i * y) \\ &\approx \sum_{i=0}^{k-1} -(1-x)^i * y - (1-x)^{2i} * y^2/2 - (1-x)^{3i} * y^3/3 \\ &= -y * \frac{1-(1-x)^k}{x} - y^2/2 * \frac{1-(1-x)^{2k}}{1-(1-x)^2} - y^3/3 * \frac{1-(1-x)^{3k}}{1-(1-x)^3} \\ &\approx -y * \frac{1-(1-x)^k}{x} - y^2/2 * \frac{1-(1-x)^{2k}}{2x} - y^3/3 * \frac{1-(1-x)^{3k}}{3x} \end{aligned}$$

Thus,

$$\prod_{i=0}^{k-1} (1 - (1-x)^i * y) \approx e^{-y * \frac{1-(1-x)^k}{x}} * e^{-y^2 * \frac{1-(1-x)^{2k}}{4x}} * e^{-y^3 * \frac{1-(1-x)^{3k}}{9x}}$$

As k goes to infinity, for $x > 0$, the above approaches $e^{-y/x} * e^{-y^2/4x} * e^{-y^3/9x}$, which is less than e^{-10} for $y = 0.2$ and $x = 0.02$. For finite k, the value is at least as much as the value for $k = \infty$. Thus, the expected number of coins issued till end of time is divergent[5]. On the other hand, for large k, for example $k \geq 50$, the expected number of coins awarded each year becomes almost constant, i.e. close to M_0/e^{10}.

[5]This divergence can also be obtained from the famous Ramanujan psi sum formula (see Appendix B). If one is so inclined that the scheme have an upper bound on the total number of coins, the Ramanujan formula shows that there should be an additional geometric taper at a fixed rate $z < 1$. However, its our opinion that this is a red herring, and the main goal is to design a currency that is stable and an inflation hedge and hence a good store of value.

3 Conclusion

While proof-of-work consensus protocols for timestamped ledgers allow decentralized transferable tokens, the mining token award scheme in Bitcoin and other similar crypto-currencies do not mimic industrial production and mining of precious metals. Thus, these digital tokens have no sound valuation model, and the value is driven solely by speculation. In this work we suggest modifying the mining token award to increase with increasing difficulty and argue that, under rational expectations equilibrium, this leads to a pricing of the token that reasonably tracks inflation of local currencies. Since such a scheme is then unlikely to give huge return to early investors, we also suggest tapering the mining award by a hyper-geometric series (instead of ad hoc or geometric series based taperings popular amongst existing crypto-currencies), so that early investors are reasonably, but not overly, incentivized. This assures a stable store-of-value that tracks inflation reasonably well over medium and long term. Further, it is fair to traditional wealth holders as they can adopt the tokens later without paying a tremendously large penalty, in contrast to the case with Bitcoin. Any party can start mining at any point and gain tokens at the same rate and cost as other extant miners, as long as the cumulative mining operations do not increase the price of electricity and equipment by too much. One problem that is still not resolved is the cost of electricity and equipment usage. Thus if a total of X dollars of wealth is to be transfered to the crypto-currency at any time then about the same amount of dollars must be spent on electricity and equipment around that time. However, this is still better than Bitcoin, where the price is driven so high by speculation that traditional wealth holders are best placed by not adopting Bitcoin at all, and yet the marginal electricity (and equipment) cost per coin mined is close to the price of the coin.

Listing 1: Psuedocode of x-off-y Scheme

```
//some of the following variables are initialized based on information
//in the most recent block in the blockchain
int n; //block_number
int Dn;      //difficulty of this block
int Dn_plus_1;    //difficulty of next block
time Tn_minus_1;  //time of creation of previous block
time Tn;     //time of creation of this block
time dTn_minus_10;//time to solve n-10 puzzle
time avgT; // average time to solve last 10 puzzles
time new_avgT; // average time to solve last 9 puzzles and this
double Cn; //coins awarded in this block, rounded to 2 decimal points
double Cn_plus_1; //coins awarded in next block
double x,y;
double xpower; //(1-x)^i, where i is the number of years (approx.)
double newxpower;

int dT = Tn - Tn_minus_1;
new_avgT = (avgT*10 - dTn_minus_10 + dT) /10;
if ((dT < 7 mins) and (new_avgT < 5 mins))
{ Dn_plus_1 = Dn +1;
  Cn_plus_1 = round(Cn * 100 * 2) /100;
}
else { Cn_plus_1 = Cn; Dn_plus_1 = Dn;}

if ((n % (365*24*6)) ==0)
{ newxpower = xpower*(1-x);
  Cn_plus_1 = round(Cn_plus_1 * 100 * (1- newxpower*y))/100;
}
```

References

[1] Digital Signature Standard: DSA, FIPS-PUB 186-4. `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf`. 1

[2] Digital Signature Standard: ECDSA, FIPS-PUB 186-4. `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf`. 1

[3] Christian Badertscher, Peter Gazi, Aggelos Kiayias, Alexander Russell, and Vassilis Zikas. Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018*, pages 913–930. ACM, 2018. 1

[4] Christian Badertscher, Ueli Maurer, Daniel Tschudi, and Vassilis Zikas. Bitcoin as a transaction ledger: A composable treatment. In *Advances in Cryptology - CRYPTO 2017 - 37th*

Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I, volume 10401 of *Lecture Notes in Computer Science*, pages 324–356, 2017. 1

[5] Mihir Bellare, Juan Garay, Charanjit Jutla, and Moti Yung. Varietycash: A multi-purpose electronic payment system. Third Usenix Workshop on Electronic Commerce, 1998. 1

[6] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *CCS '93, Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia, USA, November 3-5, 1993*, pages 62–73, 1993. 1

[7] David Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology: Proceedings of CRYPTO '82, Santa Barbara, California, USA, August 23-25, 1982*, pages 199–203, 1982. 1

[8] Jing Chen and Silvio Micali. Algorand. arXiv preprint arXiv:1607.01341, 2016. 1

[9] Bernardo David, Peter Gazi, Aggelos Kiayias, and Alexander Russell. Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 66–98. Springer, 2018. 1

[10] Cynthia Dwork and Moni Naor. Pricing via processing or combating junk mail. In *Proc. CRYPTO*, 1992. 1

[11] G.H. Hardy. Ramanujan. Cambridge University Press, 1940. B

[12] Robert E Lucas Jr. and Edward C Prescott. Investment under uncertainty. In *Econometrica: Journal of the Econometric Society*, pages 659 – 681, 1971. 2.1

[13] Charanjit Jutla and Moti Yung. Paytree: "amortized-signature" for flexible micropayments. Second Usenix Workshop on Electronic Commerce, Nov 1996. 1

[14] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. `https://bitcoin.org/bitcoin.pdf`, 2008. 1, 2

[15] Rafael Pass, Lior Seeman, and Abhi Shelat. Analysis of the blockchain protocol in asynchronous networks. In *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part II*, pages 643–673, 2017. 2

[16] Ron Rivest. The md4 message digest algorithm. In *Proc. CRYPTO*, 1990. 1

[17] Ronald Rivest and Adi Shamir. Payword and micromint: : Two simple micropayment schemes. `https://people.csail.mit.edu/rivest/pubs/RS96b.pdf`, May 1996. 1

[18] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978. 1

[19] Alfredo De Santis, Silvio Micali, and Giuseppe Persiano. Non-interactive zero-knowledge proof systems. In *Advances in Cryptology - CRYPTO '87, A Conference on the Theory and Applications of Cryptographic Techniques, Santa Barbara, California, USA, August 16-20, 1987, Proceedings*, pages 52–72, 1987. 1.2

A Bitcoin Mining Economics

We show that price of bitcoin cannot be stabilized by increased mining, and the price of bitcoin is completely driven by speculation.

We illustrate this with a simple setting where at price P per bitcoin, lets assume that there are N (equivalent) miners involved in mining bitcoin. In a first setting, we will also assume that miners always sell their freshly mined coins at the market price. The expected revenue of each of the N miners is $k * P/N$ per block added to the bitcoin blockchain (assuming k new coins are awarded in each block being added to the bitcoin blockchain), and hence also $k * P/N$ per every ten minutes. At equilibrium, this revenue should more or less equal the cost of mining of each miner per ten minutes. Since, we assume that all miners are equivalent, this means that their mining equipment is the same, as well their electricity cost and amortized cost of equipment. Suppose, each of the N equivalent miners can hash at the rate of h hashes per sec while consuming power Ω. Then, the total number of hashes per ten minutes is $600 * N * h$, and this then is capable of achieving one (on average) solution to a hash puzzle per ten minutes, where the hash puzzle requires $\log(600 * N * h)$ most-significant bits to be zero in a hash. Thus, the difficulty D, which is the number of msb bits zero in a correct solution minus 32, is $-32 + \log(600 * N * h)$. If electricity cost universally is ρ per unit power-sec, then the cost of electricity of each miner is $600 * \Omega * \rho$ per ten minute interval. Thus, at equilibrium, we can assume that $600 * \Omega * \rho + \theta = (k * P + \tau)/N$, where θ is the depreciation cost per ten minutes of the equipment of each miner, and τ is the transaction revenue per block mined.

Note that the cost of mining per ten minutes per miner is $600 * \Omega * \rho + \theta$, while in this much time an individual miner is expected to mine k/N bitcoins. Thus, the cost of mining a bitcoin is $(N/k) * (600 * \Omega * \rho + \theta)$. The number of miners N can also be derived from the difficult D above, as $N = 2^{D+32}/(600 * h)$, thus yielding that the cost of mining a bitcoin is $(2^{D+32}/(600 * h * k)) * (600 * \Omega * \rho + \theta)$. This is the original claim that the cost of mining depends on (i)-(iv).

Now, suppose that due to speculation and increased demand of bitcoin, the price of bitcoin doubles to $2 * P$. This would naturally double the revenue of the current miners without any additional cost of mining. Thus, we can assume that this would invite new miners, and it is reasonable to assume that the number of (equivalent) miners increases to $2 * N$: after a short delay, rational expectations equilibrium implies that N would keep increasing till the cost of mining approaches the price, which effectively means that N doubles. Since double the computational power is now brought to bear to the hash problem, the difficulty parameter then doubles in a short amount of time. Thus, the average revenue of each miner is $k * 2P/2N$ per every ten minutes, which is same as before. Thus, while the price of bitcoin has doubled, the bitcoin mining revenue per mining cost remains the same.

Of course, this assumed that all miners had the same mining efficiency. If this is not the case, the miners with a better mining efficiency, i.e. hash rate per electricity consumed (and amortized equipment cost), will have incentive to increase their mining as long as revenue rate $k * P/N$ remains above the electricity (and amortized equipment) cost for ten minute interval. Indeed, consider the earlier equilibrium equation $600 * \Omega * \rho + \theta = (k * P + \tau)/N$. Now suppose, one miner can increase

its efficiency $\Omega'_{D,N}$ by factor of two, while their θ increases by a factor of $\eta \geq 1$ (presumably, because they have a more expensive new technology). So, they will clone themselves M times, so that $600 * \Omega/2 * \rho + \eta\theta = (k * P + \tau)/(N + M)$, whereas other miners are suddenly facing loss as $600 * \Omega * \rho + \theta > (k * P + \tau)/(N + M)$. Thus, if the price of bitcoin remains stable, or even increases at underlying inflation rates, the miners in equilibrium face the threat of extreme loss at every equipment innovation. Thus, this dis-incentivizes every miner unless the transaction costs are high enough to give the miners a cushion.

Note that this is independent of the current price of bitcoin, which could be any multiple of the original P. Indeed the original investors can invest in technology to improve mining efficiency and hence become powerful miners, and since its in the original investors interest to increase the price of bitcoin they have the following strategy. Once they monopolize the mining business, they sell the mined bitcoins only at the rate to match the marginal demand. This should cover their cost of mining in the long run. As long as the marginal demand on average (over a medium term period) is higher than average mining rate (i.e. k), the price of bitcoin would keep going up. While the bitcoin protocol mandates that the mining rate k keep going down with time, the marginal demand will also depend on price of bitcoin. Thus, at some point, the average marginal demand may become substantially less than the mining rate, and then the price of bitcoin will start going down. This would obviously be detrimental to the late investors, as this relation of marginal demand being greater than the mining rate is the only driver of bitcoin price. Moreover, the marginal demand comes only from expectations of price increase, resulting in a cyclic relation.

B Ramanujan's Psi Sum Formula

The general q-Pochhammer symbol is defined by

$$(a,q)_k = \begin{cases} \prod_{j=0}^{k-1}(1-a*q^j) & \text{if } k>0 \\ 1 & \text{if } k=0 \\ \prod_{j=1}^{|k|}(1-a*q^{-j})^{-1} & \text{if } k<0 \\ \prod_{j=0}^{\infty}(1-a*q^j) & \text{if } k=\infty \end{cases}$$

For $0 < a, b < 1$ and $q, b < az$, Ramanujan's Psi Sum formula [11] is

$$\sum_{n=-\infty}^{\infty} \frac{(a;q)_n}{(b;q)_n} z^n \;=\; \frac{(az;q)_\infty (q/az;q)_\infty (q;q)_\infty (b/a;q)_\infty}{(z;q)_\infty (b/az;q)_\infty (b;q)_\infty (q/a;q)_\infty}$$

Note that if $b = 0$, then $(b;q)_k$, as well as $(b;q)_\infty$ are just one. Thus, setting $b = 0$ in the above identity we get for $0 < a < 1$, $0 < z \leq 1$

$$\sum_{n=-\infty}^{\infty} (a;q)_n \;=\; \frac{(az;q)_\infty (q/az;q)_\infty (q;q)_\infty}{(z;q)_\infty (q/a;q)_\infty} \tag{1}$$

Since $(1;q)_\infty$ is zero, the above sum is divergent unless $z < 1$.