Woodcoin: A peer to peer electronic currency built for longevity and stability

v1.0

Funkenstein the Dwarf

Oct. 31, 2014

Abstract:

We outline here the design considerations and implementation of woodcoin, in particular those which separate it from other cryptocurrencies. Woodcoin is a cryptocurrency very much like bitcoin. However the design of bitcoin explicitly models a non-renewable resource: gold. For woodcoin we more closely model a sustainable resource. In particular woodcoin avoids the time asymmetries of the bitcoin release model, maximizing the incentive to participate and the longevity of the coin at the same time. Our solution is logarithmic growth of the money supply. In addition, we outline the design considerations behind two other changes to the core protocol: mining with the Skein hash function and securing digital ownership with the X9_prime256v1 curve using ECDSA.

Introduction:

Six years ago the great wizard Satoshi Nakamoto delivered middle earth from the clutches of the counterfeiters by publicizing the proof of work algorithm in the first implementation of a public cryptocurrency: bitcoin [Nakamoto, 2008]. Our current work, woodcoin, is an experimental cryptocurrency which is built in much the same way as bitcoin, sharing in the code base with bitcoin and two of its successors: litecoin and quark. The objective of woodcoin is to take a very long view and design a coin that remains viable and stable extremely far into the future.

Release Schedule:

Crucial to the financial application and stability of a cryptocurrency is the reward schedule, or the release schedule. This might also be called the money supply inflation schedule. With a public cryptocurrency, this schedule is not private or discretionary but is planned in advance and is verifiable and audited (regulated) by all participants. Satoshi chose a model which very crudely simulated mining of a nonrenewable resource. A constant amount would be given out with every block, and then after a fixed amount of blocks (210,000 blocks or close to four years for bitcoin classic) this amount would be cut in half. This can be written as a geometric series:

$$R_n = \frac{k}{2^n} \tag{1}$$

Here R_n is the reward at some time step *n*, and *k* is an initial constant (*k*=50 for bitcoin classic).

This is known mathematically in common tongue as a geometric series, the sum of which converges rapidly with increasing *n*. The result is that after the first four years, half of the BTC ever to come out had been released. Further, there will be a time in the relatively near future when the reward per block approaches zero, and further mining will need to be incentivised by transaction fees alone. It is unclear how bitcoin and other cryptocurrencies will behave in this limit. The trouble is that the cost of performing a single block double spend is proportional to the mining reward.

It is these properties that we wish to improve on with a logarithmic release coin. For woodcoin we adopt instead of a geometric series a harmonic one, in which the reward is given by:

$$R_n = \frac{k}{n} \qquad (2)$$

In this case there is one immediate difference which is that the sum of the series does not converge. In theory this would mean an infinite money supply, however because we are limited with the smallest possible reward at 1 satoshi (10^{-8} LOG), there will also be a final limit.

However, the harmonic series grows incredibly slowly. The time of the final reward will arrive when $R_n = 10^{-8}$. For woodcoin we have chosen $k = 1000000$ and so we see the final LOG satoshi released at block $n = 10^{14}$, somewhere near what men would call Julian year 380 million. This maximum in money supply which will be reached in this year is just over 27,625,814 LOG.

While bitcoin released half the BTC in four years, we expect half the LOG to be released somewhere in the Julian year 2305.

The total LOG money supply at any block height *n* is determined by adding together all the rewards for the previous blocks:

$$S_n = \sum_{100}^{n} \frac{k}{n} \approx k \cdot \log(n + \gamma) - F \qquad (3)$$

where the approximation is due to the great wizard Euler. Here γ is the Euler-Mascheroni constant ~0.577, and *log* is the natural logarithm. *F* represents the size of the Forest, which is made from those initial blocks for which the wood not added to the supply:

$$F = \sum_{0}^{100} \frac{k}{n} = 5{,}187{,}377 \qquad (4)$$

The forest is introduced to eliminate the extremely high reward of early blocks and to model a rational use of a renewable resource.

Some cryptocurrencies have chosen to introduce at some point a fixed constant reward (e.g. dogecoin). This will mean eventually a linear inflation and depreciation of existing coin so we avoid this approach. Other coins have introduced a reward proportional to some externality such as the hashrate (e.g. peercoin). We also reject this approach due to the uncertainty it leaves in calculations of the money supply and the potential for linear future inflation. These approaches attempt to add to coin longevity by ensuring an interest in mining the coin, but at a cost. With the woodcoin approach, we ensure the longevity of a woodcutting incentive, but without the negative effects of unlimited or uncertain inflation.

The smooth release curve of woodcoin is perhaps best illustrated by plotting the total money supply versus the block number, which we show in Figures 1 and 2.

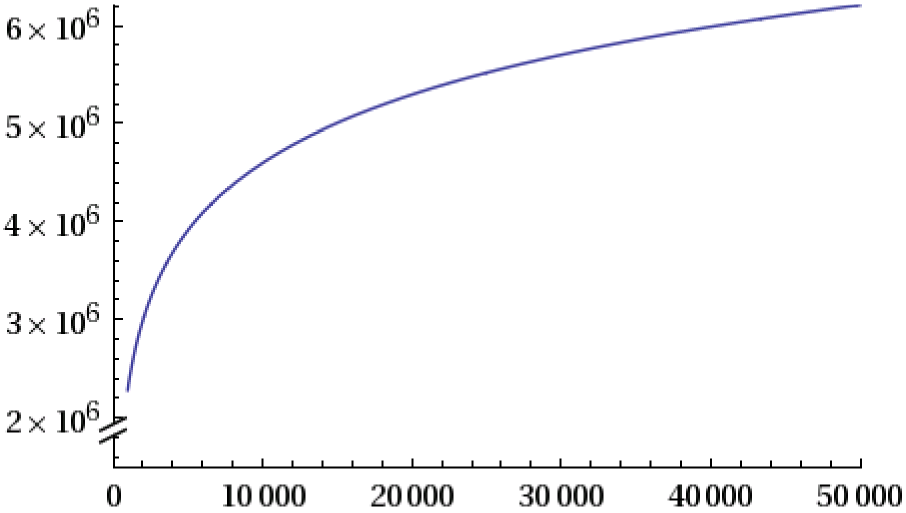

Figure 1. Woodcoin total supply for blocks 0 through 50000.

As one can tell by comparing Figures one and two, an important feature of the logarithmic function is the self similarity. At any block, the reward continues to drop and a woodcutter will have an advantage over any future woodcutter. The incentive to chop wood in the present moment therefore remains and is not artificially diminished.

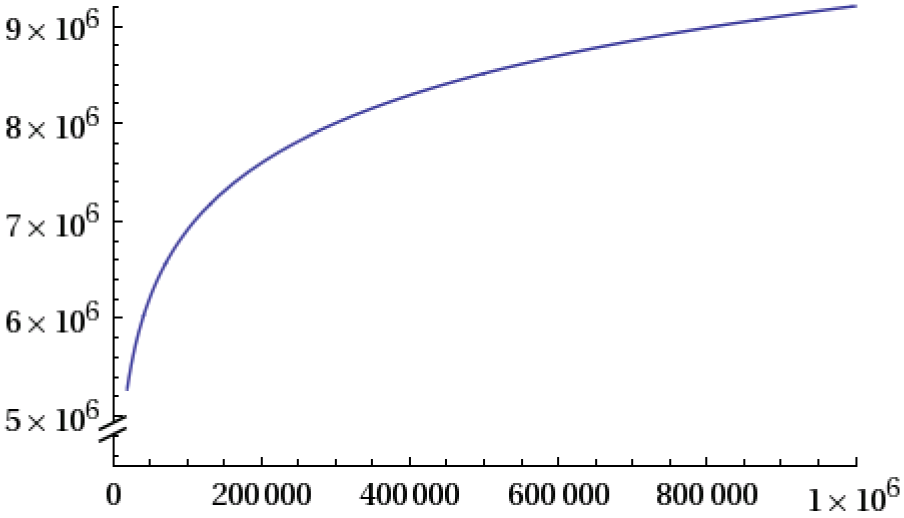

Figure 2. Woodcoin total supply for blocks 0 through 1 million.

Proof of Work Algorithm

In choosing a hash function for which to provide proof of work and form blocks which verify transactions, there is much diversity in the cryptocurrency world. Many coins choose functions which attempt to allow common CPUs to mine without giving an incentive to specialized hardware. If these coins succeed in gaining value, they will fail in this effort, as all algorithms could be performed faster on the right hardware. For our choice of hash function we are not trying to avoid ASIC or GPU woodcutting, but rather we are choosing a hash function that we find the most secure and understood in its implementations. The description and promotion of the Skein function is best left to its creators [Ferguson et al., 2008], and is beyond the scope of this paper. However we point out two facts about the Skein has function here:

1) It was created in part by Bruce Schneier

2) It was not selected by the NSA to be the official SHA3 hash function.

Elliptic curve choice for ECDSA

Perhaps the most important technology which makes a cryptocurrency possible is a digital signature algorithm that allows a participant to prove ownership of a coin, and therefore to spend it. This technology was first popularized in 1976 by the great wizards Whitfield Diffie and Martin Hellman. A proper discussion of the history is outside the scope of this paper, but it should be noted that their 1976 paper already predicted the rise of digital exchange commodities. Like most cryptocurrencies, we choose to use a different algorithm from the one introduced in that paper to form digital signatures: we use the Elliptic Curve Digital Signature Algorithm (ECDSA). Using this system requires the choice of a particular elliptic curve. After the curve is chosen, a private key can be chosen by selecting a point on this curve. Although we know of no practical weaknesses of any popular curve choice, we take the opportunity to introduce further cryptographic diversity and choose a different curve than most other cryptocurrencies, which use a curve known as secp256k1. The curve we use is known as ANSI X9.62 Prime 256v1 and it was published as a recommended curve for financial institutions before the turn of the century [ANSI, 1999].

Conclusions

In reading the above technical discussion of the properties of woodcoin, an important element has been left out. We have missed the forest by looking at the trees. Chopping wood is meant to be a fun new way to approach cryptocurrency, and to encourage us to leave the mines for a moment and marvel at the beauty of wood. Chopping wood is exhilarating, and while we woodcut we can think of this resource continuing far into the future due to our careful sustainable planning. We also remember the importance of maintaining a forest, a diverse ecosystem, and to consider and respect the intelligence of the trees and the gift of fresh cool air. As cryptocurrencies move forward, and nonrenewable energy sources become further depleted, it is expected that the dual use of chopping logs and heating of homes will become more prevalent. Wood is an important resource in other skills as well, and we hope to develop LOG to be used for a variety of other cryptocurrency applications as soon as atomic cross chain transactions are implemented.

“Block chains are log structured databases” - Funkenstein the Dwarf

References:

1) “Bitcoin: A peer to peer electronic currency”, Satoshi Nakamoto, Oct. 31, 2008

2) “The Skein Hash Function Family”, Niels Furguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, Jesse Walker, Nov. 15, 2008

3) ANSI X9.62, “Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)”, 1999