Primecoin: Cryptocurrency with Prime Number Proof-of-Work

Sunny King
(sunnyking9999@gmail.com)

July 7th, 2013

Abstract

A new type of proof-of-work based on searching for prime numbers is introduced in peer-to-peer cryptocurrency designs. Three types of prime chains known as Cunningham chain of first kind, Cunningham chain of second kind and bi-twin chain are qualified as proof-of-work. Prime chain is linked to block hash to preserve the security property of Nakamoto's Bitcoin, while a continuous difficulty evaluation scheme is designed to allow prime chain to act as adjustable-difficulty proof-of-work in a Bitcoin like cryptocurrency.

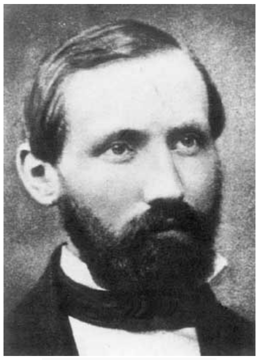
Introduction

Since the creation of *Bitcoin* [Nakamoto 2008], *hashcash* [Back 2002] type of proof-of-work has been the only type of proof-of-work design for peer-to-peer cryptocurrency. Bitcoin's proof-of-work is a hashcash type based on SHA-256 hash function. In 2011, ArtForz implemented scrypt hash function for cryptocurrency Tenebrix. Even though there have been some design attempts at different types of proof-of-work involving popular distributed computing workloads and other scientific computations, so far it remains elusive for a different proof-of-work system to provide minting and security for cryptocurrency networks.

In March 2013, I realized that searching for prime chains could potentially be such an alternative proof-of-work system. With some effort a pure prime number based proof-of-work has been designed, providing both minting and security for cryptocurrency networks similar to hashcash type of proof-of-work. The project is named *primecoin*.

Prime Numbers, An Odyssey

Prime numbers, a simple yet profound construct in arithmetic, have perplexed generations of brilliant mathematicians. Its infinite existence was known as early as Euclid over 2000 years ago, yet the *prime number theorem*, regarding the distribution of prime numbers, was only proven in 1896, following Bernhard Riemann's study of its connection to the Riemann zeta function. There remain still numerous unsolved conjectures to this day.



Bernhard Riemann
1826-1866

The world records in prime numbers have been largely focused on *Mersenne prime* 2^p-1, named after French monk Marin Mersenne (1588-1648), due to its long history and importance in number theory, and the fact that modulo 2^p-1 can be computed without

Édouard Lucas 1842-1891

division for the efficient Lucas-Lehmer test. Currently the top 10 largest known primes are all Mersenne primes.

Two well-known types of prime pairs are, *twin primes*, where both p and p+2 are primes, and *Sophie Germain* (1776-1831) *primes*, where both p and 2p+1 are primes. Extending the concept of Sophie Germain prime pairs, a chain of nearly doubled primes is named after Allan Cunningham (1842-1928), where *Cunningham chain of the first kind* has each prime one more than the double of previous prime in chain, and where *Cunningham chain of the second kind* has each prime one less than the double of previous prime in chain. A variation of the form is known as *bi-twin chain*, that is, a chain of twin primes where each twin pair basically doubles the previous twin pair.

Let's look at some small examples to better understand these prime chains. 5 and 7 are twin primes, 6 is their center. Let's double 6, arriving at 12, whereas 11 and 13 are twin primes again. So 5, 7, 11, 13 is a bi-twin chain of length 4, also known as bi-twin chain of one link (a link from twin 5, 7 to twin 11, 13). The bi-twin chain can actually be split from their centers, giving one Cunningham chain of first kind, and one Cunningham chain of second kind. Now if we split through centers 6, 12 of bi-twin chain 5, 7, 11, 13, those below the centers are 5, 11, a Cunningham chain of first kind, those above the centers are 7, 13, a Cunningham chain of second kind. I call the first center, the number 6 in this example, the *origin* of the prime chain. From this origin you can keep doubling to find your primes immediately adjacent to the center numbers.

There are also other prime formations known as *prime constellations* or *tuplets*, and *prime arithmetic progressions*. Of interest to these prime pairs and formations, is that their distribution seems to follow a similar but more rare pattern than the distribution of prime numbers. Heuristic distribution formulas have been conjectured, however, none of their infinite existence is proven (the *twin prime conjecture* being the most well known among them [Goldston 2009]), let alone their distribution.

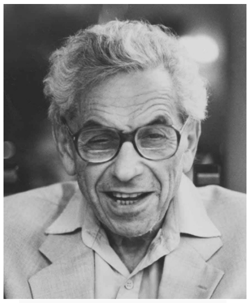
Efficient Verification of Proof-of-Work

In order to act as proof-of-work for cryptocurrency, the work needs to be efficiently verifiable by all nodes of the network. This would require the primes not to be too large, such as record-breakingly large. It then precludes Mersenne primes and leads to the use of prime chain as primecoin's work, since finding a prime chain gets exponentially harder (with our current theoretical and algorithmic understanding) as the chain length increases, yet verification of a reasonably sized prime is efficient.

So for the primecoin design three types of prime chains are accepted as proof-of-work: Cunningham chain of first kind, Cunningham chain of second kind, and bi-twin chain. The primes in the prime

Pierre de Fermat
1601-1665

chain are subject to a maximum size protocol in order to ensure efficient verification on all nodes.


Paul Erdős 1913-1996

The classical Fermat test [Caldwell 2002] of base 2 is used together with Euler-Lagrange-Lifchitz test [Lifchitz 1998] to verify probable primality for the prime chains. Note we do not require strict primality proof during verification, as it would unnecessarily burden the efficiency of verification. Composite number that passes Fermat test is commonly known as *pseudoprime*. Since it is known by the works of Erdös and Pomerance [Pomerance 1981] that pseudoprimes of base 2 are much more rare than primes, it suffices to only verify probable primality.

Non-Reusability of Proof-of-Work

Another important property of proof-of-work for cryptocurrency is non-reusability. That is, the proof-of-work on a particular block should not be reusable for another block. To achieve this, the prime chain is linked to the block header hash by requiring that its origin be divisible by the block header hash. The quotient of the division then becomes the *proof-of-work certificate*.

Block hash, the value that is embedded in the child block, is derived from hashing the header together with the proof-of-work certificate. This not only prevents the proof-of-work certificate from being tampered with, but also defeats attempt at generating a single proof-of-work certificate usable on multiple blocks on the block chain, since the block header hash of a descendant block then depends on the certificate itself. Note that, if an attacker generates a different proof-of-work certificate for an existing block, the block would then have a different block hash even though the block content remains the same other than the certificate, and would be accepted to the block chain as a sibling block to the existing block.

Block header hash is subject to a lower bound so performing hashcash type of work is of no help to prime mining. Varying nonce value generally does not help with prime mining, as prime mining is done typically by fixing the block header hash and generating a *sieve*. In one case, varying nonce and finding a block header hash that is divisible by a small *primorial number* – the product of all primes smaller than a given prime `p` – can help only slightly. It allows the prime miner to work on somewhat smaller primes, like maybe a few digits shorter, for prime numbers of typically 100 digits, only a very small advantage.

Difficulty Adjustability of Proof-of-Work

One of Bitcoin's innovations is the introduction of adjustable difficulty. This allows cryptocurrency to achieve controlled minting and relatively constant transaction processing capacity. The advent of GPU mining and later ASIC mining of SHA-256 hashcash proof-of-work did not impact its inflation model exactly due to this mechanism.

Of course, hashcash's linear difficulty model made it easy. For prime proof-of-work, it is not apparent how this could be achieved. Initially I thought about using prime size as an indicator of difficulty. However, a non-linear difficulty curve would negatively impact block chain security. Also, using prime size as difficulty indicator would interfere with efficiency of verification. Eventually I discovered that the remainder of Fermat test could be used to construct a relatively linear continuous difficulty curve for a given prime chain length. This allows primecoin to largely keep the security property of bitcoin.

Let k be the prime chain length. The prime chain is p_0, p_1, …, p_{k-1}. Let r be the Fermat test remainder of the next number in chain p_k. Now p_k/r is used to measure the difficulty of the chain. Even though the distribution of r/p_k is not strictly uniform, but experiments have shown that the difficulty adjustment behavior is reasonably good in practice. The prime chain length is then computed with a fractional length part:

$$d = k + (p_k-r)/p_k$$

Note if p_k passes probable primality tests then it should be considered as a chain of higher integral length.

A continuous length target adjustment is employed with similar features to the difficulty adjustment in ppcoin [King 2012]. Length target is stepped up or down through integral boundaries during length target adjustment, at fixed step-up/step-down threshold of `255/256 <-> 1`.

Main Chain Protocol

In bitcoin, main chain protocol ensures that block chain consensus can be reached as long as more than half of the network mining power reaches consensus. Conversely, an attacker needs more than 50% of total network mining power to control block chain. This security property depends on the linear difficulty model of hashcash. In primecoin, it is slightly weakened as the difficulty model is not strictly linear, so an attacker may only need somewhat less than 50% of total network mining power through manipulation of difficulty. At integral length boundaries, a constant ratio is introduced to approximate the ratio of difficulties between prime chains with length difference of 1. The level of block chain security is dependent on the accuracy of this estimate. As the state of art of prime mining progresses in primecoin network, this ratio should be adjusted as needed to ensure better security.

Minting Model

Primecoin is designed as a pure proof-of-work cryptocurrency, to complement the proof-of-stake design of ppcoin. Primecoin's proof-of-work mint rate is determined by difficulty. This approach was first experimented in ppcoin. The scarcity of the currency is not ensured by a fixed cap as in bitcoin, but regulated by Moore's Law via mining hardware advances and by algorithmic improvements. This design is a more natural simulation of gold's scarcity.

Moreover, pure proof-of-work cryptocurrency depends on the mining market for its security. *Network mining income*, the sum of all miners' income, is a direct measurement of the level of block chain security across competing pure proof-of-work cryptocurrency networks. A fixed cap scarcity model relies heavily on transaction fees to sustain network security. However a higher transaction fee reduces the competitiveness of a crypto-currency as payment-processing network. Since last year, bitcoin's share of network mining income has shrunk much faster than its capital market share.

Basically, for a pure proof-of-work design, it's not realistic to expect all three goals to sustain: high network security, low inflation and low transaction fee. This topic has been explored in ppcoin paper, however it would become more evident as the competition intensifies in cryptocurrency market and bitcoin's inflation rate drops further.

As Moore's Law approaches its limit, primecoin inflation rate would taper off and gives a slower drop toward zero. There is still good scarcity property similar to gold while network security is maintained without the need to raise transaction fee. The inflation in primecoin is designed to drop slower than ppcoin's proof-of-work minting, to compensate for the need of sustained energy consumption of pure proof-of-work cryptocurrencies.

Conclusion

Primecoin is the first cryptocurrency on the market with non-hashcash proof-of-work, generating additional potential scientific value from the mining work. This research is meant to pave the way for other proof-of-work types with diverse scientific computing values to emerge.

Around the time of this paper, several new cryptocurrencies have been released adopting other hash functions or composition of hash functions for hashcash proof-of-work. It appears there are market forces at play such that diversification of proof-of-work types is inevitable. It could prove difficult for any single type of proof-of-work to maintain dominance in the long term. I would expect proof-of-work in cryptocurrency to gradually transition toward energy-multiuse, that is, providing both security and scientific computing values.

Acknowledgement

I would like to thank Satoshi Nakamoto and Bitcoin developers whose brilliant pioneering work in Bitcoin made this project possible.

References

Back A. (2002): Hashcash – A denial of service counter-measure.
(http://www.hashcash.org/papers/hashcash.pdf)

Caldwell C. (2002): Finding primes & proving primality.
(http://primes.utm.edu/prove)

Goldston D. A. (2009): Are there infinitely many twin primes?
(http://www.math.sjsu.edu/~goldston/twinprimes.pdf)

King S., Nadal S. (2012): PPCoin: peer-to-peer crypto-currency with proof-of-stake.
(http://ppcoin.org/static/ppcoin-paper.pdf)

Lifchitz H. (1998): Generalization of Euler-Lagrange theorem.
(http://www.primenumbers.net/Henri/us/NouvTh1us.htm)

Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system.
(http://www.bitcoin.org/bitcoin.pdf)

Pomerance C. (1981): On the distribution of pseudoprimes.
Mathematics of Computation Volume 37 Number 156 OCT 1981