Itaru Kishikawa
Darpan Goyal

May 13, 2019
Professor Austin

Project Report

In this project, We are making a cryptocurrency that models “Primecoin”[1] called Itarucoin. Primecoin uses proof-of-work as Sybil-resistance. It searches and your computer is doing random number calculations to find prime numbers. There are two benefits of using this coin, the speed of the transaction and researching the mathematical problems.

Proof-of-work concept:

Primecoin provides an ideal proof-of-work system where the calculation itself is hard but is extremely easy to verify. Instead of useless SHA256 hashes offered by Bitcoin, it provides a chain of prime numbers as proof of work, known as Cunningham chains and bi-twin chains[2]. These chains have proven to be the first practical example of a useful proof-of-work system, apart from transaction validation.

Innovations by Primecoin:

1. Useful Proof-of-work: Mathematical Analysis

Primecoin helps mathematical research by producing prime number chains as we make the blocks. These prime number chains are posted on the Primecoin blockchain’s public ledger, which mathematicians and scientists can make use of. The distribution of prime numbers is one

of the most important discoveries in mathematics, and the study of prime chains leads to a series of interesting results for Riemann and the prime theorem. There is an association with the deeper nature of the seemingly random pattern of the prime number distribution. The prime distribution is not just an abstract concern for mathematicians. Riemann's work revealed the direct relationship between Riemann's zeta function and prime distribution, but it was later shown that Riemann's zeta function is also very relevant to other scientific fields such as physics. Therefore, the study of prime number distribution is an important part of the foundation of modern science[1].

This proof-of-work system gives three different kinds of chains as output: Cunningham chain I, Cunningham chain II and bi-twin chain. The first Cunningham chain has a chain of primes where each prime is one more than the twice the previous prime in the chain. The second Cunningham chain gives a chain of primes where each prime is one less than the previous prime in the chain. The third, bi-twin chain gives a chain of primes where each pair is basically the double of the previous pair in the chain. Verification of primality is done by a combination of The classical Fermat test [Caldwell 2002] of base 2 and Euler-Lagrange-Lifchitz test [Lifchitz 1998].

2. **Fast transaction confirmation:** Primecoin confirms blocks every minute instead of Bitcoin’s every 10 minutes and as a result, transactions are also confirmed 10 times as fast, in around 6 to 7 minutes.

3. GPU/ASIC resistant: Under the current model, Primecoin mining is inefficient on GPUs and development of ASIC for its mining is extremely expensive. Hence, it is one of the fairest coins to mine.

Novel Improvements:

Primecoin increases the difficulty of the proof-of-work computation smoothly over every block, instead of every 2016 blocks in Bitcoin. This self-adjusting difficulty is supposed to emulate gold scarcity and pricing, but the problem with Primecoin is, if the price goes up significantly, the difficulty will also increase significantly, causing a reduction in Primecoin generation rate. So instead of adjusting 86.5% every week, we could reach that every two months, potentially giving us a more sustainable and stable currency.

Implementation:

Our coins is pretty much same as Bitcoin except the proof work. Instead calculating the number of reading zero in the hash, we find the Cunningham chain that is the chain of prime numbers where the next term is the doubled the previous term and plus one, and it has to be the prime as well. The longer length, the harder problem so that we could use this theory to apply for the difficulty adjustment. Once the miner find the chain, we use Fermat Primality test to test the all the numbers are actually primes. The accuracy of this test is 99.9%. Once we verify the chain, and if it is valid, we add the block.

References

[1] “About Primecoin.” *Primecoin*, primecoin.io/about.php#advantages-xpm.

[2] Sunny King: “Primecoin: Cryptocurrency with Prime Number Proof-of-Work ”, July 7th, 2013, http://primecoin.io/bin/primecoin-paper.pdf

[3] Vitalik Buterin: “Primecoin: The Cryptocurrency Whose Mining is Actually Useful”, July 8th, 2013, https://bitcoinmagazine.com/articles/primecoin-the-cryptocurrency-whose-mining-is-actually-useful-1373298534/?fbclid=IwAR09N9o0atp9L4l802a3ziHSdr1fny3vz7gM_E5DF4d1jXYLWZtVzUDKCDQ