Woodcoin: Una moneda electrónica descentralizada construida para ser viable y estable

v1.0

Funkenstein the Dwarf

31 de Octubre de 2014

Resumen:

Presentamos aquí las consideraciones e implementaciones de diseño del woodcoin, en concreto aquellas que la diferencias de otras cripto-monedas. El woodcoin es una cripto-moneda muy similar al Bitcoin. Sin embargo el modelo en el que se basa el bitcoin es el de un recurso no renovable como el oro. Para el Woodcoin hemos elegido un modelo más sostenible. Concretamente el woodcoin evita las asimetrías del modelo de emisión del bitcoin, maximizando el incentivo para participar y la longevidad al mismo tiempo. Además hemos añadido otros dos cambios al código del núcleo: minado con la función hash skein y la propiedad digital asegurada con la curva X9_prime256v1 usando ECDSA

Introducción:

Hace seis años el gran mago Satoshi Nakamoto dió una sorpresa desagradable a los falsificadores del mundo entero cuando publicó el algoritmo de prueba de trabajo (proof of work) en la primera implementación de una cripto-moneda pública: el Bitcoin [Nakamoto, 2008]. Nuestro trabajo actual, el woodcoin, es una cripto-moneda experimental muy similar al bitcoin, compartiendo gran parte del código fuente con el y con dos de sus sucesores: litecoin y quark. El objetivo del woodcoin combina una visión a largo plazo y el diseño de una moneda viable y estable.

Calendario de emisión:

El calendario de emisión es muy importante para la estabilidad financiera y viabilidad de una cripto-moneda. Lo podemos llamar también calendario de inflación monetaria. En una cripto-moneda pública, este calendario no es privado o discrecional, este se planifica por adelantado y es verificable y auditable (controlado) por todos los participantes. Satoshi eligió un modelo que simula el minado de un recurso no renovable. La recompensa por bloque es una cantidad constante hasta que generan una cantidad prefijada de bloques (210,000 bloques o aproximadamente cuatro años) y entonces la recompensa se ve reducida a la mitad. Lo podemos describir con la siguiente función geométrica:

$$R_n = \frac{k}{2^n} \qquad (1)$$

Donde R_n es la recompensa en el momento n, y k es una constante inicial (k=50 en el Bitcoin).

A esto se lo conoce en matemáticas como una serie geométrica, la suma de las cuales convergen rápidamente con el aumento de n. El resultado es que tras los primeros 4 años, se han emitido más de las mitad de los BTC. En el futuro próximo cuando la recompensa por bloque se aproxime a cero, el único incentivo que tendrán los mineros serán solo las comisiones. Hoy en día, no está muy claro como el bitcoin y otras cripto-monedas se comportarán cuando alcancen este límite. El problema es que el coste de realizar un ataque de doble gasto es proporcional a la recompensa por el

minado.

Para mejorar las características de una moneda con emisión de tipo logaritmica, En el woodcoin hemos optado por usar una serie armónica en lugar de geométrica, en la cual la recompensa viene determinada por la siguiente función:

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

En este caso podemos observar una diferencia de forma inmediata, y es que la suma de las series no convergen. En teoría esto significa una cantidad ilimitada de dinero, pero debido a que la recompensa más pequeña posible es de 1 satoshi (10^{-8} LOG), la recompensa se ve limitada.

Las funciones armónicas se caracterizan por crecer muy despacio. El momento de la última recompensa llegara cuando $R_n = 10_{-8}$. Para el woodcoin hemos elegido $k = 1000000$ de este modo cuando el ultimo satoshi de LOG se emita en el bloque block $n = 10_{14}$, eso sucederá en algún momento del año juliano 380 millones. La cantidad máxima de monedas se alcanzará este año con aproximadamente 27,625,814 LOG.

Mientras más de la mitad de bitcoins fueron emitidos en los primeros 4 años, estimamos que la mitad de los LOG serán emitidos en algún momento del año 2305

La cantidad total existente de LOG en un bloque *n* se determina añadiendo todas las recompensas de los bloques anteriores como podemos observar en la siguiente función:

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

Esta aproximación se la debemos al gran mago Euler. Donde γ es la constante de Euler-Mascheroni ~0.577, y *log* es el logaritmo natural. *F* representa el tamaño del bosque , el cual está compuesto de lo bloques iniciales que no fueron añadidos al suministro de monedas.

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

El bosque se introduce para eliminar la recompensa extremadamente alta de los bloques iniciales y para modelar el uso racional de un recurso renovable

Algunas cripto-monedas han elegido asignar una recompensa fija por bloque (como por ejemplo:

dogecoin). Esto significa una inflación lineal y una depreciación de las monedas existentes por este motivo hemos evitado esta aproximación. Otras monedas han introducido una recompensa proporcional a factores externos como el hashrate (como por ejemplo peercoin). Rechazamos también esta aproximación debido a la incertidumbre que genera en los cálculos del suministro de dinero y las amenazas de una posible inflación futura. Estas aproximaciones intentan proporcionar longevidad a la moneda asegurando que haya interés en el minado de la moneda, pero lo hacen con un coste. Con la aproximación realizada por el Woodcoin, aseguramos la longevidad simulando el incentivo que obtendría un leñador, pero sin los efectos negativos de una inflación ilimitada o desconocida.

La suave curva de emisión del woodcoin está quizás mejor ilustrada con un gráfico que incluye la cantidad total de dinero frente al número de bloque, como mostramos en la figura 1 y 2.

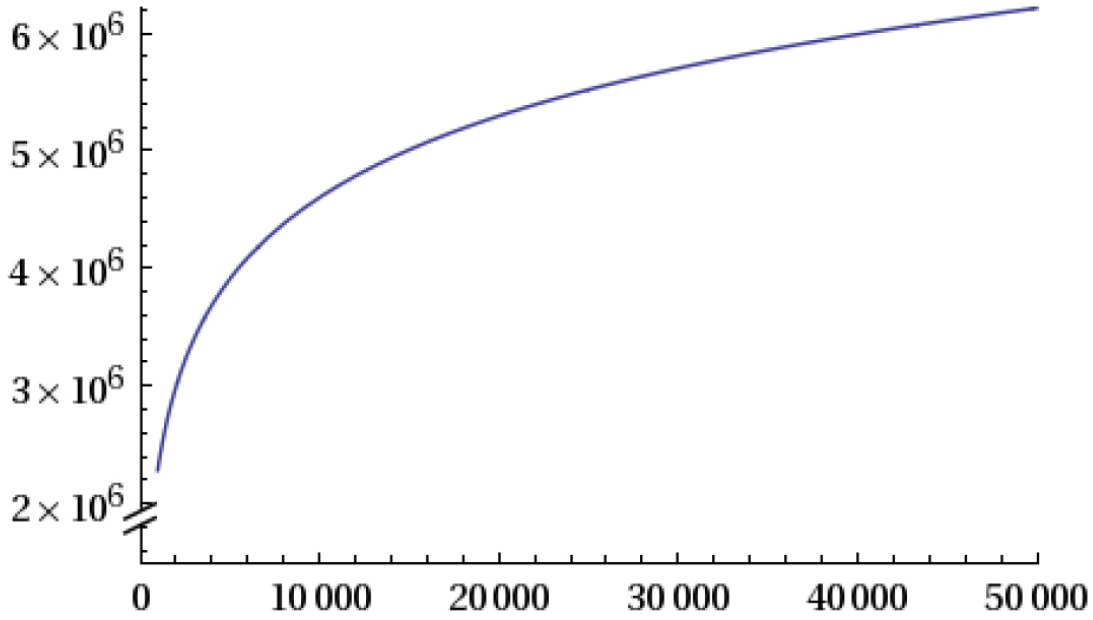

Figura 1. Cantidad total de Woodcoin desde el bloque 0 al bloque 50000

Como podemos observar comparando las figuras 1 y 2 , una característica importante de la función logarítmica es la autosimilaridad. En cualquier bloque, la recompensa continua decreciendo y un leñador tendrá ventaja sobre cualquier futuro leñador. El incentivo para cortar madera en el presente se mantiene y no disminuye de modo artificial.

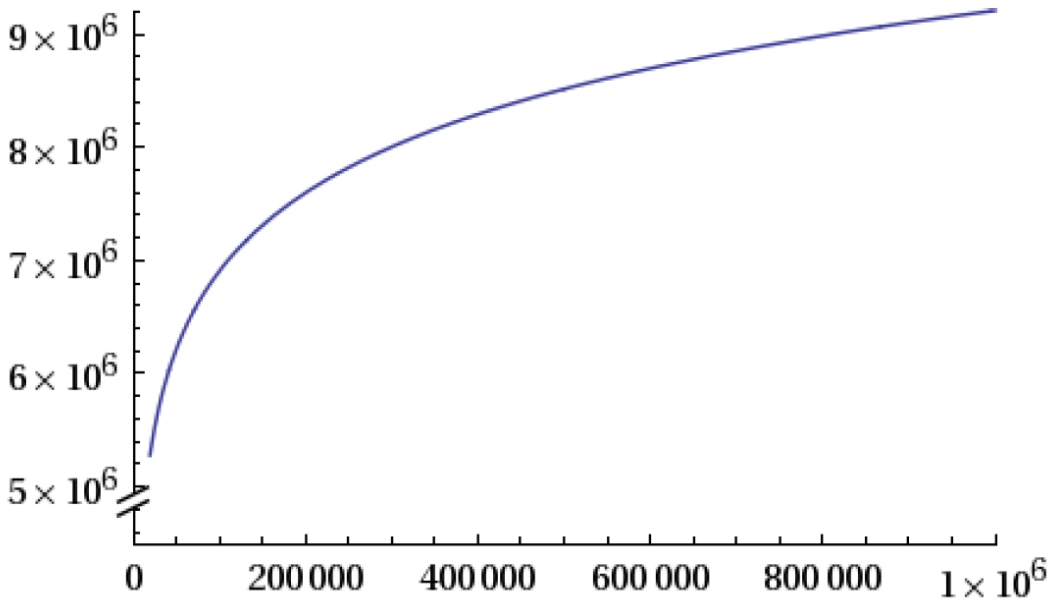

Figura 2. Cantidad total de Woodcoin desde el bloque 0 al bloque 1.000.000

Algoritmo de la prueba de trabajo

para elegir una función hash que suministre la prueba de trabajo necesaria para formar bloques en los cuales se verifican las transacciones, hay mucha diversidad en el mundo de las criptomonedas. Muchas monedas eligen funciones hash con el objetivo de permitir minar con CPU´s comunes sin incentivar el hardware especializado. Si estas monedas tienen éxito y ganan valor, fallarán en su intento, ya que los algoritmos tienen mejor rendimiento en un hardware especializado que será creado específicamente para realizar esta función. Para la elección de nuestra función hash no intentamos evitar los ASIC o las GPU, Por ello elegimos el más seguro y estudiado en sus implementaciones. La descripción y promoción de la función Skein se la dejamos a sus creadores [Ferguson et al., 2008], y no está en el objetivo de este documento. Sin embargo nos gustaría apuntar 2 hechos sobre la función Skein:

1) Fué creada por Bruce Schneier

2) no fué elegida por la NSA para ser la función hash oficial para SHA3.

Elección de la curva elíptica para ECDSA

Quizás la tecnología más importante que hace posible la existencia de las cripto-monedas es el algoritmo de firma digital que permite a los participantes probar la propiedad sobre sus monedas, y de este modo poder gastarlas. Esta tecnología fue popularizada originariamente en 1976 por los magos Whitfield Diffie y Martin Hellman. La discusión sobre esta historia esta fuera del objetivo de este documento, pero remarcamos que en sus documentos de 1976 ya predijeron el auge de los activos digitales. Como son las criptomonedas, hemos elegido un algoritmo para las firmas digitales diferente del introducido por ese documento: usamos el algoritmo de firma digital de curva elíptica (ECDSA). El usar este sistema requiere la elección de una curva elíptica concreta. Una vez se elige la curva, se puede elegir una clave privada seleccionando un punto de la curva. Aunque de momento no conocemos vulnerabilidades en la elección de las curvas más populares, aprovechamos la oportunidad para introducir mayor variedad criptográfica y elegimos una curva diferente a la de la

mayoría de cripto-monedas, las cuales usan la curva secp256k1. La curva usada por el woodcoin es conocida como ANSI X9.62 Prime 256v1 y fue recomendada para su uso por parte de instituciones financieras a finales de siglo [ANSI, 1999].

Conclusiones

En la lectura que hemos realizado sobre las características técnicas del woodcoin, hemos dejado atrás un elemento importante. Hemos olvidado el bosque y nos hemos centrado en los arboles. Cortar madera pretende ser una nueva forma divertida de aproximación a las cripto-monedas, y debe animarnos a dejar las minas y maravillarnos ante la belleza de la madera. Cortar madera es estimulante, y mientras cortamos madera podemos reflexionar que este recurso seguirá disponible debido a nuestra planificación sostenible. Recordamos también la importancia de mantener los bosques, un ecosistema diverso, y tener consideración y respeto hacia la inteligencia de los árboles y el aire fresco que nos proporcionan. A medida que las criptomonedas avancen , y las fuentes de energia no renovables se agoten, se espera que el uso de leña para calentar las casas se vuelva más frecuente. La Madera es un recurso importante también para otros usos, y esperamos que el desarrollo de LOG pueda ser utilizado por otras aplicaciones y cripto-monedas tan pronto como las transacciones atómicas transversales sean implementadas.

"Las cadenas de bloques son bases de datos logarítmicas estructuradas" - Funkenstein the Dwarf

Referencias:

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