# Peercoin: Cripto-Moneda *Peer-to-Peer* con *Proof-of-Stake*

*Sunny King, Scott Nadal*
*(sunnyking9999@gmail.com, scott.nadal@gmail.com)*
(Traducción al español por *MrBickle support@ecoining.com)*

*19 de agosto de 2012*

**Resumen**

Peercoin es una cripto-moneda *peer-to-peer* (red de pares o iguales) cuyo diseño viene derivado del Bitcoin de Satoshi Nakamoto. *Proof-of-Stake* (prueba de participación) reemplaza el *Proof-of-Work* (prueba de trabajo) para proporcionar la máxima seguridad a la red. En este diseño híbrido, el *Proof-of-Work* provee principalmente el minado inicial y no es esencial a largo plazo. El nivel de seguridad de la red no depende de la energía eléctrica así que a largo plazo es una cripto-moneda de gran eficiencia energética y un valor competitivo. El *Proof-of-Stake* está basado en la edad de la moneda y es generado en cada nodo mediante un esquema de hashing parecido al de Bitcoin pero con un espacio de búsqueda limitado. El histórico de la Cadena de Bloques (*Block Chain*) y el asentamiento de transacciones está aún más protegido con un mecanismo de puntos de control centralizados.

## Introducción

Desde la creación de Bitcoin (Nakamoto 2008), el *Proof-of-Work* ha sido el diseño predominante en las cripto-monedas *peer-to-peer*. El concepto de *Proof-of-Work* ha sido la columna vertebral del acuñado de moneda y del modelo de seguridad del diseño de Nakamoto.

En octubre de 2011 nos dimos cuenta de que el concepto de edad de la moneda, puede facilitar un diseño alternativo al Proof-of-Work de Bitcoin llamado Proof-of-Stake. Hemos formalizado desde entonces un diseño donde el *Proof-of-Stake* se usa para construir un modelo de seguridad de una cripto-moneda *peer-to-peer* y es parte del proceso de acuñado, mientras que el *Proof-of-Work* facilita principalmente la parte inicial de la generación de monedas y reduce su importancia con el paso del tiempo. Este diseño intenta demostrar la viabilidad de futuras monedas *peer-to-peer* que no dependan de la energía eléctrica. Hemos llamado a este proyecto Peercoin.

## Edad de la moneda

El concepto de edad de la moneda era conocido por Nakamoto al menos desde 2010 y usado en Bitcoin, por ejemplo, para ayudar a priorizar las transacciones, aunque no jugaba un rol fundamental en el modelo de seguridad de Bitcoin. La edad de la moneda es simplemente definido como el número de monedas que se tiene en un periodo. Un ejemplo fácil de entender: si Roberto recibiera 10 monedas de Alicia y las mantuviera durante 90 días podríamos decir que Roberto ha acumulado 900 días de edad de la moneda.

Adicionalmente, cuando Roberto gastó 10 monedas de las que recibió de Alicia, decimos que la edad de las monedas que Roberto ha acumulado con esas 10 monedas se ha consumido (o destruido).

Para facilitar el cómputo de la edad de la moneda, hemos introducido una marca de tiempo en cada transacción. Los protocolos relacionados con la marca de tiempo de cada bloque y transacción están reforzados para securizar el cálculo de la edad de la moneda.

## *Proof-of-Stake*

*Proof-of-Work* (prueba de trabajo) ayudó a nacer al mayor logro de Nakamoto, sin embargo, la naturaleza del

*Proof-of-Work* significa que la cripto-moneda es dependiente del consumo de energía, introduciendo pues un coste significativo en el mantenimiento de la red, del que se hacen cargo los usuarios mediante una combinación de inflación y tasas de transacción. Ya que el ritmo de acuñado disminuye en la red Bitcoin, se podría llegar a la situación de tener que subir las tasas de transacción para mantener el nivel deseado de seguridad en la red. Uno naturalmente se pregunta si debemos mantener el consumo de energía para tener una cripto-moneda descentralizada. Por tanto es un peldaño importante tanto teórica como tecnológicamente, demostrar que la seguridad de una cripto-moneda *peer-to-peer* no tiene que depender de la energía eléctrica.

El concepto llamado *Proof-of-Stake* fue debatido en los círculos del Bitcoin ya en 2011. En términos generales, *Proof-of-Stake* significa una prueba de la propiedad de la moneda. La edad de la moneda consumida por una transacción se puede considerar una forma de Proof-of-Stake. Independientemente, nosotros descubrimos el concepto de edad de la moneda en octubre de 2011, a través del cual nos dimos cuenta que el Proof-of-Stake puede reemplazar la mayoría de las funciones del *P*roof-of-Work con un rediseño cuidadoso del acuñado del Bitcoin y su modelo de seguridad. Esto es porque al igual que el Proof-of-Work, el *Proof-of-Stake* no puede ser fácilmente imitado. Por supuesto, este es uno de los requisitos críticos de cualquier sistema monetario, la dificultad de falsificar la moneda. Filosóficamente hablando, el dinero ha sido una forma de *'Proof-of-Work'* en el pasado, y por tanto debería ser capaz de sustituir al *Proof-of-Work* por si mismo.

**Generación de bloques mediante *Proof-of-Stake***

En nuestro diseño híbrido, los bloques están separados en dos tipos diferentes, bloques *Proof-of-Work* y bloques Proof-of-Stake.

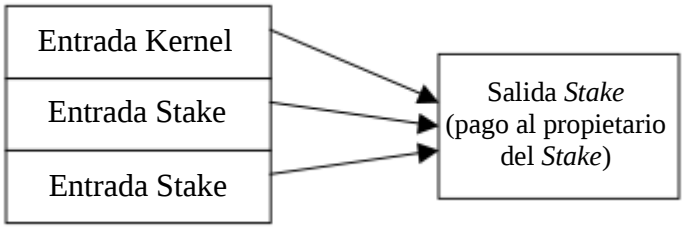


Imagen: Estructura de Transacción *Proof-of-Stake*

El *Proof-of-Stake* en el nuevo tipo de bloques es una transacción especial llamada "*coinstake*" (nombrada a partir de la transacción especial del Bitcoin llamada "*coinbase*"). En una transacción *coinstake* el dueño del bloque se paga a si mismo, consumiendo por tanto su edad de moneda, mientras genera un bloque en la red y acuña moneda mediante Proof-of-Stake. El primer parámetro del *coinstake* se llama kernel (núcleo) y requiere que cumpla cierto *hash* del protocolo, haciendo pues de la generación de bloques *Proof-of-Stake* un proceso estocástico similar al de los bloques Proof-of-Work. Sin embargo, una diferencia importante es que la operación de *hashing* está hecha sobre un espacio limitado de búsqueda (más específicamente un hash por cada output del *wallet* sin gastar por segundo) en lugar de un espacio de búsqueda ilimitado como en el *Proof-of-Work*. No hay por tanto un gasto significativo de energía involucrado.

*El hash que el kernel de Stake* debe cumplir es un hash por unidad de edad de moneda (moneda-día) consumido en el kernel (en contraste al *Proof-of-Work* de Bitcoin que es un valor fijado que se aplica a cada nodo). Por tanto cuando más edad de moneda sea consumida por el kernel, más fácil será cumplir el protocolo de *hash* objetivo. Por ejemplo, si *Bob* tiene una salida de *wallet* (monedero) que ha acumulado 100 años de moneda y espera generar un kernel en 2 días, entonces *Alicia* puede esperar aproximadamente sus 200 años de moneda de salida de *wallet* para generar un kernel en un día.

En nuestro diseño tanto el objetivo del hash *Proof-of-Work* como el de *Proof-of-Stake* se ajustan continuamente (en lugar de las dos semanas de ajuste del Bitcoin) para impedir saltos bruscos en el ritmo de generación de moneda de la red.

***Acuñado basado en Proof-of-Stake***

Un nuevo proceso de acuñado se introduce con los bloques *Proof-of-Stake* adicionalmente al acuñado

*Proof-of-Work* de Bitcoin. Un bloque *Proof-of-Stake* acuña monedas basándose en la edad de moneda consumida en la transacción *coinstake*. Un ritmo de acuñado de 1 céntimo por año de moneda consumido es el elegido para aumentar un bajo ritmo de inflación en el futuro.

Aunque mantenemos el *Proof-of-Work* como parte del proceso de acuñado para facilitar el acuñado inicial, es concebible que en un sistema puro *Proof-of-Stake* el acuñado inicial pueda efectuarse por si solo mediante un proceso similar al de la oferta pública inicial en la bolsa (IPO).

**Protocolo de la cadena principal**

El protocolo que determina qué cadena de bloques gana como cadena principal, se ha cambiado para consumir edad de moneda. Aquí cada transacción en un bloque contribuye su edad de moneda al valor del bloque. La cadena de bloques con más edad de moneda consumida es elegida como la cadena principal -en contraste al uso del *Proof-of-Work* en la cadena de bloques principal del protocolo de Bitcoin-, mientras que el trabajo total de la cadena de bloques se usa para determinar la cadena principal.

Este diseño minimiza algunas de las preocupaciones de un ataque 51% de Bitcoin, donde el sistema sólo se considera seguro cuando nodos buenos controlan al menos el 51% del poder total de minado de la red. El coste de controlar tal porcentaje de la prueba de participación debería ser mucho más alto que el coste de conseguir un porcentaje igual de poder de minado, aumentando por tanto el coste de un ataque para entidades poderosas. Además la edad de moneda del atacante es consumida durante el ataque, lo que hace más difícil al atacante continuar seguir impidiendo que las transacciones entren en la cadena principal.

**Puntos de control: Protección del histórico**

Una de las desventajas de usar la edad de moneda consumida para determinar la cadena de bloques principal es que disminuye el coste de un ataque en el histórico de la cadena de bloques. A pesar de que Bitcoin tiene una protección del histórico relativamente fuerte, Nakamoto introdujo puntos de control en 2010 como mecanismo para solidificar el histórico de la cadena de bloques, previniendo cualquier posible cambio a parte de la cadena de bloques anterior al punto de control.

Otra preocupación es que el coste de un ataque de gasto-doble podría haber disminuido también, ya que un atacante podría necesitar acumular tan solo cierta edad de moneda y forzar la reorganización de la cadena de bloques. Para hacer el comercio práctico mediante este sistema, hemos decidido introducir una forma adicional de puntos de control centralizados, a intervalos de tiempo cortos, de incluso varias veces al día, que sirven para congelar la cadena de bloques y finalizar las transacciones. Este nuevo tipo de punto de control se transmite de manera similar al sistema de alertas de Bitcoin.

*Laurie* (2011) argumentó que Bitcoin no ha solucionado completamente el problema del consenso distribuido ya que el mecanismo de punto de control no es distribuido. Hemos intentado diseñar un protocolo de puntos de control distribuido pero hemos encontrado difícil securizarlo contra un ataque dividido en la red. A pesar de que el mecanismo de transmisión de los puntos de control es una forma de centralización, lo consideramos aceptable hasta que una solución completamente distribuida esté disponible.

Otra razón técnica conlleva el uso de puntos de control centralizados. Para proteger contra un tipo de ataque de denegación de servicio (DOS) el kernel del *coinstake* debe ser verificado antes de que un bloque *Proof-of-Stake* pueda ser aceptado en la base de datos local (árbol de bloques) de cada nodo. Debido al modelo de datos de los nodos de Bitcoin (específicamente el índice de transacciones) es necesaria una fecha límite para los puntos de control que asegure la capacidad de todos los nodos de verificar la conexión de cada kernel del *coinstake* antes de aceptar un bloque en el árbol de bloques. Debido a estas consideraciones prácticas, hemos decidido no modificar el modelo de datos de los nodos, si no usar puntos de control centralizados. Nuestra solución consiste en modificar el cálculo de la edad de la moneda para requerir una edad mínima, como un mes, por debajo del cual la edad de la moneda es cero. Así pues los puntos de control centralizados se usan para asegurar que todos los nodos puedan estar de acuerdo acerca de las todas las transacciones más antiguas que un mes, permitiendo la verificación de la conexión del kernel *del coinstake*, ya que un kernel requiere una edad de la moneda superior a cero y por tanto debe usar una salida superior a un mes.

**Firmas de bloque y protocolo *Stake* duplicado**

Cada bloque debe ser firmado por su propietario para prevenir que el mismo *Proof-of-Stake* sea copiado y usado por atacantes.

Un protocolo de *Stake* duplicado está diseñado para defender contra un atacante que use un solo *Proof-of-Stake* para generar múltiples bloques como un ataque de denegación de servicio. Cada nodo recibe el par (kernel, marca de tiempo) de todas las transacciones *coinstake* que ha visto. Si un bloque recibido contiene un par duplicado, se ignora hasta que un bloque sucesor sea recibido como un bloque huérfano.

**Eficiencia energética**

Cuando el ritmo de acuñado *Proof-of-Work* se acerque a cero, cada vez habrá menos incentivo para acuñar bloques Proof-of-Work. En este escenario a largo plazo, el consumo de energía de la red puede descender a niveles muy bajos, mientras los mineros, desinteresados, dejan de minar bloques Proof-of-Work. La red Bitcoin se enfrenta a este riesgo a menos que el volumen de transacciones y sus tasas suban a niveles suficientemente altos que mantengan el consumo de energía. Bajo nuestro diseño incluso si el consumo de energía se acerca a cero, la red está aún protegida por el Proof-of-Stake. Podemos llamar a una cripto-moneda eficientemente energética si el consumo de energía *Proof-of-Work* se permite que se acerque a cero.

**Otras consideraciones**

Hemos modificado el ritmo de acuñado *Proof-of-Work* para que no esté determinado por la altura de bloque (Tiempo) si no por la dificultad. Cuando la dificultad de minado sube, el acuñado *Proof-of-Work* disminuye. Una curva más o menos regular es elegida en oposición a las funciones por pasos de Bitcoin, para impedir alterar el mercado artificialmente. Más específicamente, una curva continua es elegida en la que cada subida de la dificultad de 16 veces, divida por dos el número de monedas por bloque.

A largo plazo, la curva de acuñado *Proof-of-Work* no sería muy distinta a la de Bitcoin en términos de comportamiento inflacionario, dando continuación a la *Ley de Moore*. Consideramos sabio seguir la observación tradicional de que el Mercado favorece a una moneda con baja inflación frente a una con alta, a pesar de la crítica al Bitcoin de algunos famosos economistas, en nuestra opinión, debido a razones ideológicas.

*Babaioff et al.* (2011) estudió el efecto de la tasa de transacción y argumentó que esta tasa es un incentivo a los mineros para no cooperar entre ellos. Bajo nuestro sistema, no damos tasas de transacción a los propietarios del bloque. En lugar de eso, decidimos destruir las tasas. Esto quita el incentivo de no reconocer el bloque de otro acuñador. Sirve además como una fuerza deflacionaria para contrarrestar la fuerza inflacionaria del acuñado Proof-of-Stake.

Elegimos además  ejecutar las tasas de transacción a nivel de protocolo para defender contra un ataque de hinchado de bloque.

Durante nuestra investigación hemos descubierto además una tercera posibilidad además del *Proof-of-Work* y el Proof-of-Stake, *que hemos llamado Proof-of-Excellence* (prueba de excelencia). Bajo este sistema, una competición se lleva a cabo periódicamente para acuñar monedas basándose en el rendimiento de los participantes de la competición, imitando los precios de competiciones en la vida real. Aunque este sistema tiende también a consumir energía, consideramos interesante el concepto, ya que provee una forma más o menos inteligente de consumo de energía.

**Conclusión**

En cuanto el Mercado valide nuestro diseño, esperamos que los diseños *Proof-of-Stake* se conviertan potencialmente en una forma más competitiva de cripto-moneda *peer-to-peer* a los diseños *Proof-of-Work*, ya que eliminan la dependencia del consumo de energía, consiguiendo por tanto una inflación y unas tasas de transacción más bajas, con niveles de seguridad de la red comparables

**Reconocimientos**

Muchas gracias a Richard Smith por ayudar con las pruebas y varios trabajos relacionados con la red y los *forks*.

Nos gustaría también agradecer a Satoshi Nakamoto y a los desarrolladores de Bitcoin cuyo brillante acto pionero nos abrió la mente e hizo un proyecto como este posible.

**Referencias**

Babaioff M. et al. (2011): On Bitcoin and red balloons.
Laurie B. (2011): Decentralised currencies are probably impossible (but let's at least make them efficient). (http://www.links.org/files/decentralised-currencies.pdf)
Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system.
(http://www.bitcoin.org/bitcoin.pdf)