

Bitcoin y yo (Hal Finney)

Hal Finney, 19 de marzo 2013, 08:40:02 PM

Pensé que escribiría sobre los últimos cuatro años, un momento memorable para Bitcoin y para mí.

Para aquellos que no me conocen, soy Hal Finney. Me inicié en la criptografía trabajando en una versión anterior de PGP, en estrecha colaboración con Phil Zimmermann. Cuando Phil decidió comenzar PGP Corporation, yo fui uno de los primeros empleados. Hubiera trabajado en PGP hasta mi jubilación. Al mismo tiempo, me involucré con los Cypherpunks. Lideré, entre otras actividades, el primer remailer (servidor de correo) anónimo basado en criptografía.

Avanzado rápido hasta finales del 2008 y el anuncio de Bitcoin. Me he dado cuenta de que los criptógrafos que peinan canas (que ya contaba con más de 50 años) tienden a volverse cínicos. Yo era más idealista; siempre me ha apasionado la criptografía, el misterio y la paradoja de todo esto.

Cuando Satoshi anunció Bitcoin en la lista de correo de Criptografía, obtuvo una respuesta más bien fría en el mejor de los casos. Los criptógrafos han visto demasiados novatos con grandes planes para ser, en realidad, totalmente absurdos, de modo que reaccionan instintivamente.

Yo fui más positivo. Hace tiempo que he estado interesado en los sistemas de pago criptográfico. Además, tuve la suerte de conocer y mantener amplia correspondencia tanto con Wei Dai y con Nick Szabo, ambos reconocidos por haber ideado esquemas que más tarde se materializaron con Bitcoin. Yo mismo había intentado crear mi propia

criptomoneda basada en la prueba de trabajo, llamada RPOW (Reusable Proof-of-Work, Prueba de Trabajo Reutilizable). Así que Bitcoin me pareció algo fascinante.

Cuando Satoshi anunció el lanzamiento de la primera versión del software, lo descargue de inmediato. Creo que fui la primera persona, después de Satoshi en ejecutar Bitcoin. Miné el bloque 70 y algo, y fui el primer destinatario de una transacción de bitcoin, cuando Satoshi me envió diez monedas como prueba. Durante los siguientes días mantuve con Satoshi conversaciones por correo electrónico y le reporté varios fallos que acabó solucionando.

Hoy en día, la verdadera identidad de Satoshi se ha convertido en un misterio. Pero en ese momento, yo pensaba que estaba tratando con un joven de ascendencia japonesa, extraordinariamente inteligente y sincero. He tenido la suerte de conocer a muchas personas brillantes a lo largo de mi vida, así que reconozco los signos.

Después de unos días, Bitcoin ya funcionaba muy estable, así que lo dejé correr. Eran los días en que la dificultad era de 1, y se podían encontrar bloques fácilmente con una CPU, no hacía falta ni una GPU.

Miné varios bloques en el transcurso de los siguientes días, pero finalmente decidí apagarlo, porque mi ordenador se recalentaba y el ruido constante del ventilador me resultaba molesto. En retrospectiva, me gustaría haberlo mantenido encendido más tiempo, pero por otro lado me considero increíblemente afortunado por haber estado allí

desde el principio. Es como un vaso que podemos ver medio lleno o medio vacío.

No volví a saber de Bitcoin hasta finales de 2010, cuando me sorprendí al descubrir que el proyecto no sólo seguía en marcha, si no que los bitcoins habían pasado a tener valor

monetario. Desempolvé mi viejo monedero, y me sentí aliviado al comprobar que mis bitcoins seguían allí. Al ver que la cotización aumentaba, decidí guardar esas monedas

en una cartera offline, donde con suerte van a preservar su valor para mis herederos.

Hablando de herederos, tuve una sorpresa en 2009, cuando de repente me diagnosticaron una enfermedad mortal. A principios de ese año, me encontraba en un estado formidable, había perdido mucho peso y corría mucho. Había corrido varias medias maratones y comencé a entrenar para correr una maratón completa. Estaba preparado para participar en carreras de más de 20 millas, y cuando pensaba que estaba todo listo, en ese momento empezó todo a salir mal.

Mi cuerpo comenzó a fallar. Arrastraba mi forma de hablar, perdía fuerza en mis manos, y mis piernas tardaron en recuperarse de los esfuerzos. En agosto de 2009, me diagnosticaron Esclerosis Lateral Amiotrófica (ELA), también llamada la enfermedad de Lou Gehrig, por el famoso jugador de béisbol que la padeció.

La ELA es una enfermedad que mata a las neuronas motoras, que conducen las señales desde cerebro a los músculos. Inicialmente se manifiesta como debilidad y luego aumenta gradualmente hacia la parálisis. Por lo general es mortal en 2 a 5 años. Mis síntomas eran leves al principio y pude seguir trabajando, pero la fatiga y la imposibilidad de hablar me obligaron a retirarme a principios del 2011.

Desde entonces, la enfermedad ha continuado su inexorable progresión.

Hoy, estoy casi totalmente paralizado. Me alimento con una sonda y mi respiración es asistida a través de otro tubo. Uso el ordenador usando un sistema comercial de rastreo ocular que cuenta además con un sintetizador de voz, así que esta es mi voz ahora. Paso todo el día en mi silla de ruedas eléctrica. He desarrollado un interfaz utilizando una

placa de arduino para ajustar la posición de mi silla de ruedas con sólo mover mis ojos.

Ha sido un gran cambio, pero mi vida no es tan mala. Todavía puedo leer, escuchar música y ver televisión y películas. Recientemente descubrí que incluso puedo escribir código. Soy muy lento, probablemente 50 veces más lento que antes. Pero todavía sigo amando la programación y me pongo metas. Actualmente estoy trabajando en algo que Mike Hearn sugirió, utilizando las características de seguridad de los procesadores modernos, diseñado para admitir "Trusted Computing" (Computación de la Verdad), para fortalecer las billeteras de Bitcoin. El producto está casi listo para lanzarlo. Solo tengo que hacer la documentación.

Y por supuesto, los giros de los precios de los bitcoins me resultan divertidos. Al fin y al cabo, tengo ahorros en el juego, aunque mis bitcoins son más producto de la suerte que de mérito personal, con poco valor para mí. He vivido el crash de 2011. Lo he visto antes. Lo que fácil viene, fácil se va.

Esa es mi historia. Me considero un afortunado. A pesar de la ELA, mi vida es muy satisfactoria. Pero mi esperanza de vida es limitada. Las discusiones que he leído sobre cómo dejar en herencia tus bitcoins adquiere un interés más personal que académico para mí. Mis bitcoins se almacenan en nuestra caja de seguridad, y mi hijo e hija son conocedores de la tecnología. Creo que están lo suficientemente seguros. Me siento cómodo con mi legado.

Hal Finney † 04/05/1956 - 28/08/2014 (58 años) falleció a causa de la ELA.