

# EL FANTASMA DEL BITCOIN

*Texto de [Charlie Hall @Charlie\\_L\\_Hall](#)  
del 4 de septiembre de 2013*

*Traducción de [Pablo Sanzo @Pablosanzo](#)*

En busca de Satoshi Nakamoto, el hombre detrás de la moneda virtual más famosa, Polygon encuentra una inquietante economía digital que parece sacada de un videojuego.

Satoshi Nakamoto no existe. O, al menos, si lo hace, es uno de esos extraños individuos modernos que son imposibles de localizar.

Nakamoto es el creador de Bitcoin. Con el paso de los años desde el surgimiento de la moneda virtual, ha habido varias quijotescas expediciones para encontrarlo. Algunas han sido más minuciosas que otras.

Los investigadores han concluido alternativamente que él (¿o ella?) es o bien un sociólogo economista de Finlandia, un especulador financiero de America, un estudiante dublinés o la confabulación de uno o más informáticos. Algunas teorías sugieren que el pseudónimo es la adición de los nombres de cuatro corporaciones: **Samsung**, **Toshiba**, **Nakamichi**, y **Motorola**.

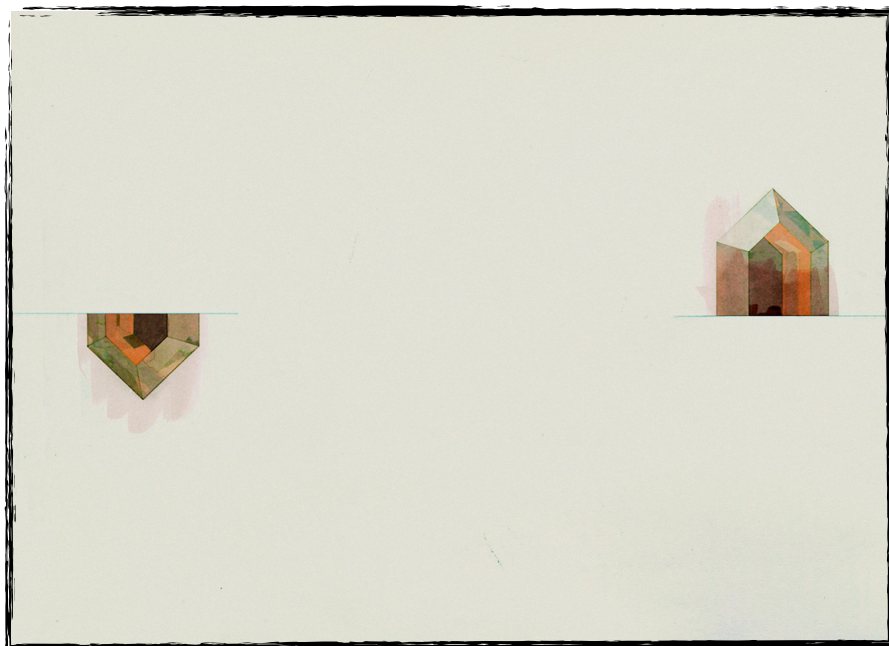
Estas teorías no pueden ser todas correctas. Son, muy probablemente, todas erróneas. En un mundo donde el anonimato no es ya esperado, donde la privacidad tiene los días contados, esta persona (o personas) ha mantenido su identidad un verdadero secreto. Incluso Osama Bin Laden fue finalmente encontrado. Y aún, hasta ahora, no lo ha sido Nakamoto. Esta persona es un mito contemporáneo.

En cualquier caso, Polygon se embarcó en búsqueda de Nakamoto

El viaje comenzó con un pequeño conjunto de pistas. Nakamoto publicó un documento en 2008, **un libro blanco describiendo Bitcoin**. De él desprendemos que su prosa es británica, su tono rico y su nombre japonés.

Mirando en detalle, podemos ver cómo al comienzo del documento Nakamoto presenta su información de contacto: una dirección de GMX.com. GMX.com es un servicio de email gratuito, privado y encriptado. A falta de un amigo turbio en la NSA, esta dirección nos era inútil.

¿O no lo era?



# ¿QUÉ ES UN BITCOIN?

En el mismo documento de 2008, Nakamoto describía el Bitcoin como una solución a un problema en el modo en que las instituciones financieras modernas manejan transacciones.

“El comercio en Internet,” escribía Nakamoto, “ha llegado al punto de depender en exclusiva de instituciones financieras sirviendo como terceras partes de confianza para procesar pagos electrónicos. Pero estas mismas instituciones tienen que protegerse a ellas mismas del fraude, lo que significa que tienen que mantener la habilidad de invertir transacciones fraudulentas en su nombre y en el de sus clientes.”

*“es la teletransportación del dinero,  
enchufar valor a un lado de  
Internet y que escurra por una  
tubería al otro lado del mundo.  
así de fácil.*

”

Tienes que confiar a la institución manejando tu dinero, y esa confianza es difícil de mantener para una institución.

Nakamoto sugería que el Bitcoin era la solución. Las transacciones en Bitcoin son “irreversibles”. En lugar de confianza, el intercambio en Bitcoin está basado en “prueba criptográfica”. El mismo tipo de algoritmos que protegían la identidad de Nakamoto en GMX.com son lo que hace este tipo de dinero tan único.

La voz calma y la reconfortante sonrisa del cajero del banco, la promesa de que “Yo me encargaré de eso por usted” si algo fuese mal, es reemplazada en la economía del Bitcoin por el frío cálculo matemático. Matemáticas increíblemente complejas.

El efecto que esto tiene en cómo el dinero fluye es revolucionario. En lugar de transferir dinero entre cuentas, permitiendo a bancos y otras instituciones financieras mediar en el intercambio, intercambiar Bitcoins es tan simple como entregarle a alguien un trozo de oro. Es la teleportación del dinero, enchufar valor a un lado de Internet y que escurra por una tubería al otro lado del mundo. Así de fácil.

De cara a seguir la pista a Nakamoto más allá tendría que haber aprendido más sobre criptografía y el papel que juega en crear y mantener la economía del Bitcoin. Así que decidí pedir un favor.



# LA CONEXIÓN RUSA

Hasta donde sé, Eugene Kaspersky, CEO y co-fundador de Kaspersky Lab (una empresa de seguridad en Internet), es el único graduado en una universidad avalada por la KGB que me sigue en Twitter. Le pregunté si, con su pasado en criptografía y seguridad informática, podría ayudarme a encontrar a Nakamoto. Dijo que no, pero que conocía alguien que podría.

Stefan Tanase es un investigador de seguridad senior en Kaspersky. Parte lo que hace para ganarse la vida consiste en rastrear Internet en busca de los más extraños peces en el mar. Virus, troyanos y gusanos son la exquisitez en el trabajo de Tanase, y los más exóticos especímenes acaban en su bandeja de entrada cada día.

Kaspersky me dijo que Tanase se especializaba en Bitcoin. Quizás el pudiera decirme quién era Nakamoto.

“Estaría orgulloso si pudiera responder a esa pregunta,” dijo Tanase. “La respuesta corta es que no tengo ni idea.”

*“así que comencé a imaginar los Bitcoins no como una pila de cosas físicas, sino como un vasto océano de código que ha sido creado por satoshi nakamoto.”*

La dirección de GMX.com era, más que probablemente, el final de una larga serie de cuentas ficticias diseñadas para ocultar la verdadera identidad de Nakamoto. Puesto que estaban encriptadas sería necesario algo como una orden judicial para abrirlas e investigarlas, y Nakamoto no ha hecho nada necesariamente incorrecto.

“Incluso cuando tomamos parte en investigaciones criminales que involucran casos de crimen federal, está normalmente limitado a analizar las capacidades técnicas del malware. Así que no es necesariamente nuestro trabajo el intentar encontrar [a Nakamoto]... Estamos más interesados en ver las grandes tendencias.”

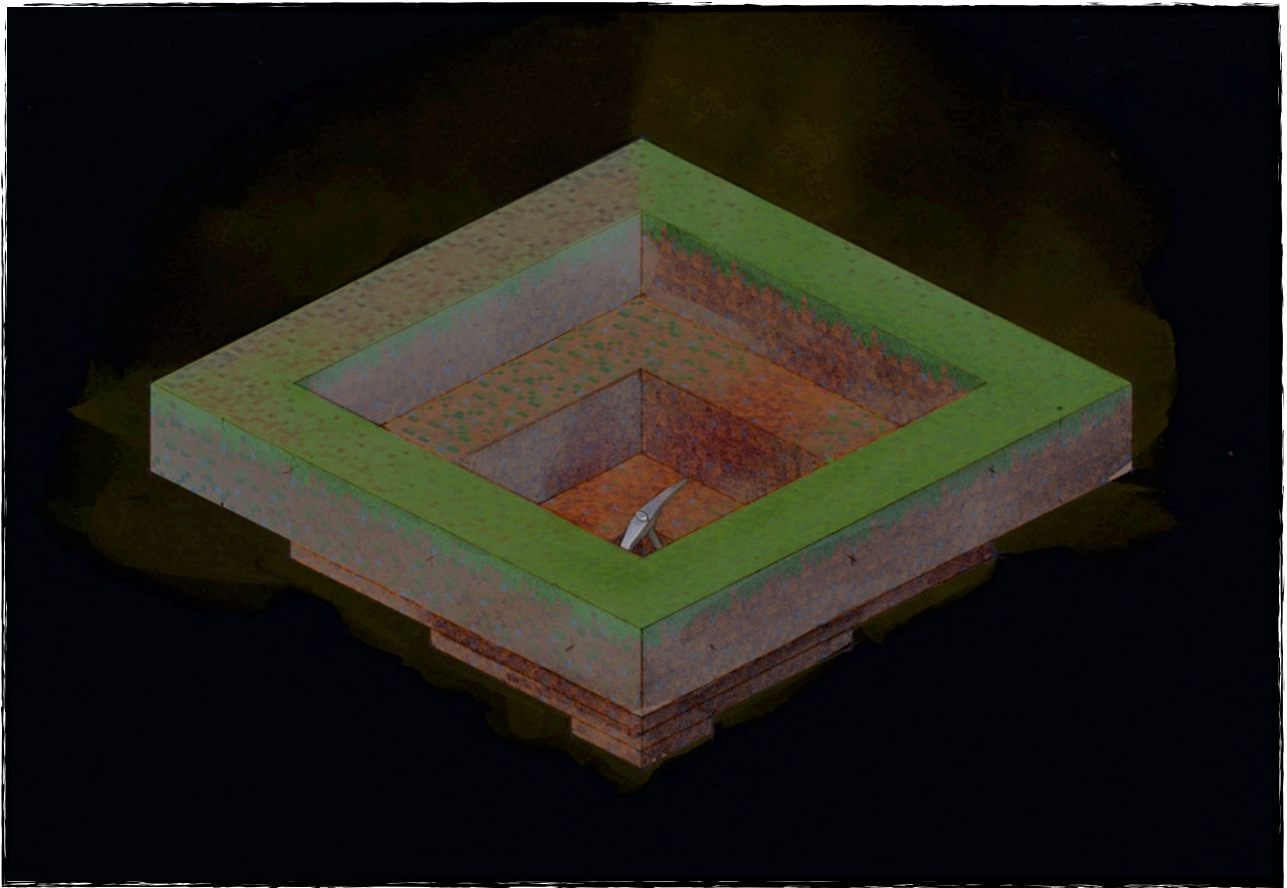
Así que sin la llave para abrir esa dirección del email, estaba cerrada permanentemente. Curiosamente, dijo Tanase, es así como funcionan los Bitcoins también. El sistema que Nakamoto diseñó depende de una criptografía increíblemente fuerte para bloquear los Bitcoins. Sin algo llamado la “llave privada”, una serie de caracteres que pulsas en el teclado, un Bitcoin es tan sólo un cacho de código en tu disco duro. Y no tiene necesariamente que ser tu disco duro dónde tus Bitcoins residen.

Dada la naturaleza de la criptografía, la llave privada sólo funciona para abrir la moneda, y no al revés. Debido a esto, el código para todos los Bitcoins en el mundo está abierto para todos los participantes en la economía Bitcoin. El intercambio en Bitcoins tiene lugar en todos los ordenadores que eligen tomar parte en el intercambio de Bitcoins por medio de una red de pares (P2P) compartida.

Nakamoto escribió en su libro blanco de 2008 que un “servidor sello de tiempo generaría “prueba electrónica del orden de las transacciones.” Cada Bitcoin que mueve es marcado de una modo matemático de modo que las transacciones no pueden ser falsificadas. Esto crea una incorruptible cadena de transacciones. La matemática apertura, cierre y gasto de estas monedas es verificado por todos los ordenadores en esta red de pares simultáneamente.

Así que comencé a imaginar los Bitcoins no como una pila de cosas físicas, sino como un vasto océano de código que ha sido creado por Satoshi Nakamoto. Las llaves privadas permiten a la gente acceder a ese océano y extraer sólo las monedas que les pertenecen, y transferir esa propiedad como quiera que deseen.

Lo que mantiene a Stefan Tanase con trabajo es el hecho de que el crecimiento de esta enorme red de pares ha creado una oportunidad sin precedentes para los cibercriminales de hacer dinero de los Bitcoins.



## ***LA FIEBRE DEL ORO***

Cuando alguien conecta su ordenador a la red de pares de Bitcoin está enchufando su CPU a la gran maquinaria que resuelve todas las mates, la criptografía, que hace el intercambio de Bitcoins funcionar. Y por sus molestias reciben Bitcoins.

Este proceso se llama “minería” de Bitcoins. Cualquiera puede descargar un minero, instalarlo en su ordenador y participar en la creación de las mates que apuntalan el sistema Bitcoin, y llevarse algunas monedas a cambio. Alimenta de electrones a un ordenador, y ese ordenador imprime dinero virtual. Cuantos más ordenadores estén involucrados, más rápido se genera el dinero.

Tanase me dijo que esto ha dado a los cibercriminales del mundo algo que hacer con todos los ordenadores que han infectado con malware, colecciones de máquinas llamadas “botnets”. Cuando un botnet no está ocupado participando en ataques a páginas web o enviando spam sobre blanqueo de dinero en Nigeria, puede ser utilizado para extraer Bitcoins.

*“debido a que el Bitcoin se ha hecho tan popular, hay más mineros honestos que cibercriminales y eso, según Tanase, protege la red Bitcoin de ser hackeada.”*

En este momento hay miles de botnets, pequeños y grandes, cientos de miles de ordenadores ganando Bitcoins para los cibercriminales. Las tarjetas gráficas de alta gama son mejores en minería que CPUs de alta gama, así que los PCs destinados a juegos son de hecho mejores para la minería que otros.

“Si intentas la minería tú mismo,” dijo Tanase, “y ves hasta dónde llegas con una tarjeta gráfica realmente buena, y después compruebas las estadísticas de la minería y ves a los máximos contribuidores, acabas con la sensación de que la mayoría -yo diría que la vasta mayoría- de ellos están probablemente usando operaciones de minería botnet. Porque cuando ves cuántos ingresos generan es realmente casi imposible hacerlo con hardware real, comprando miles de tarjetas gráficas.”

Debido a que el Bitcoin se ha hecho tan popular, hay más mineros honestos que cibercriminales y eso, según Tanase, protege la red Bitcoin de ser hackeada. Es un tipo de fiebre del oro virtual, donde más gente abre minas cada día, atraídos por el creciente precio del Bitcoin, cercano a los 100 dólares cada moneda a día de hoy.

Pero Nakamoto diseñó el algoritmo del Bitcoin de modo que hay un número fijo de ellos para extraer. Al igual que en California en 1849, hay un número fijo de tajadas que reclamar de la fortuna Bitcoin. A medida que el récord de



transacciones Bitcoin avanza, la matemática necesaria para registrar el progreso de todas ellas se vuelve más y más difícil de computar. El ritmo de nuevos Bitcoins siendo creados, dice Tanase, ha comenzado a decrecer. A día de hoy necesitas más poder de computación que nunca para crear monedas a un ritmo diferente al de un caracol.

Nakamoto sabía esto. Y es por ello que rompió la veda con su propia mina primero.



## ***BONITO SOMBRERO***

Hay pocos académicos mejor versados en la materia de economías virtuales que Yanis Varoufakis, anterior economista para Valve. A día de hoy se encuentra en la facultad de la Universidad de Texas, mientras que al tiempo sirve como consejero para el secretario general de la Organización para la Cooperación y el Desarrollo Económico (OCDE) en París.

Varoufakis es simultáneamente el economista teórico líder en la materia del intercambio de sombreros virtuales, y uno de los pocos invitados a contribuir a la constante conversación acerca de cómo las economías europeas deberían proceder tras los desastres económicos globales de este comienzo de siglo.

Necesitaba que me ayudase a dar más sentido a cómo la economía Bitcoin funciona, lo cual es bueno porque cuando hablé con él me dejó claro que no se preocupa lo más mínimo por la verdadera identidad de Satoshi Nakamoto.

*“el experimento Bitcoin es  
único en el sentido de que  
nadie lo controla.*

”

Varoufakis es un tipo ocupado, pero quería saber por qué se tomó el tiempo para escribir sobre Nakamoto [en su blog](#) allá por Abril. En él, Varoufakis casi destripa el Bitcoin, acercándose bastante a llamar a Nakamoto un idiota, alguien tan enamorado de su propia idea que no puede ver las grietas en el sistema que ha creado.

“Todas las otras economías [virtuales] que he estudiado están controladas centralmente,” me dijo Varoufakis. “No están controladas por bancos centrales, o por gobiernos. Están controladas por corporaciones. ... El experimento Bitcoin es único en el sentido de que nadie lo controla. De modo que, efectivamente, es un juego de herramientas que permite a cualquiera que las use ser copropietario de esa comunidad.”

“Toda comunidad monetaria permite pocos grados de libertad respecto a ella... para alterar la oferta de dinero y crear más de él, para crear instituciones de crédito que expanden la oferta monetaria.”

Varoufakis era cuidadoso de escoger sus palabras según hablábamos. Estas libertades que los miembros de una comunidad económica tienen pueden ser para bien o para mal, de ahí la palabra “alterar”. Crear una línea de crédito prestando dinero en exceso a la cantidad de metálico que se tiene realmente es igualmente “alterador” del valor de una moneda como gastar el doble de ella.

Obtener un préstamo del Banco de América, dijo Varoufakis, no es tan diferente a ser pagado en Bitcoins que alguien ha gastado fraudulentamente en otro lugar. Todo depende de las reglas del juego, y la simulación creada por la economía

virtual del Bitcoin recuerda a las reglas que existían durante lo que fue denominado el “patrón oro”.

Según esas reglas, cada dólar estadounidense estaba respaldado por una cantidad equivalente de oro guardada en algún lugar por el gobierno de los Estados Unidos. El dólar era algo así como un “se debe” de la Reserva Federal, un recibo por una pizquita del tesoro de la Reserva Federal. Añadiendo, o substrayendo, la cantidad de oro físicamente guardada en la Reserva Federal, el gobierno de los Estados Unidos podía cambiar el valor del dólar relativo a otras monedas del mundo.

Pero llegó el momento en el que la Reserva Federal necesitaba más flexibilidad de la que el patrón oro permitía.

“El patrón oro ha estado yendo y viniendo unos 100 años,” explicó Varoufakis. “Siempre que había una gran perturbación en la economía, en la sociedad, el patrón oro salía volando por la ventana... [como] durante la Primera Guerra Mundial o la Segunda, o la Gran Depresión... o después la guerra en Vietnam.”

El presidente Richard Nixon acabó con el patrón oro en 1971. Desde aquel tiempo los Estados Unidos han operado con algo conocido como dinero fiduciario.

“En otras palabras,” dijo Varoufakis, “tenemos dinero cuya cantidad es controlada por el estado - por la Reserva Federal en los Estados Unidos, por el Banco Central Europeo, por el Banco de Inglaterra, por el Banco de Japón - de manera que buscan la estabilidad de precios de otros modos, no mediante la vinculación de la oferta de dinero a una cantidad de metal físico.”

Sin el patrón oro, la Reserva Federal puede, a través de varios mecanismos, crear más dinero en la economía estadounidense. Pero del mismo modo que la cantidad finita de oro que se guarda en Fort Knox, hay sólo 21 millones de Bitcoins que existirán jamás. Es parte del algoritmo que Nakamoto creó. La escasez está grabada en el ADN del sistema, y es el único mecanismo que controla toda la economía virtual.

Un sistema construido con número sólo tiene números al volante. Y es ahí donde las cosas se ponen interesantes.

Lo que Nakamoto hizo al limitar el número de Bitcoins fue traer de vuelta el patrón oro. En lugar de agobiantes minas, los Bitcoins emergen de ordenadores

a lo largo de todo el mundo. Pero el concepto, la escasez del vehículo monetario, es el mismo.

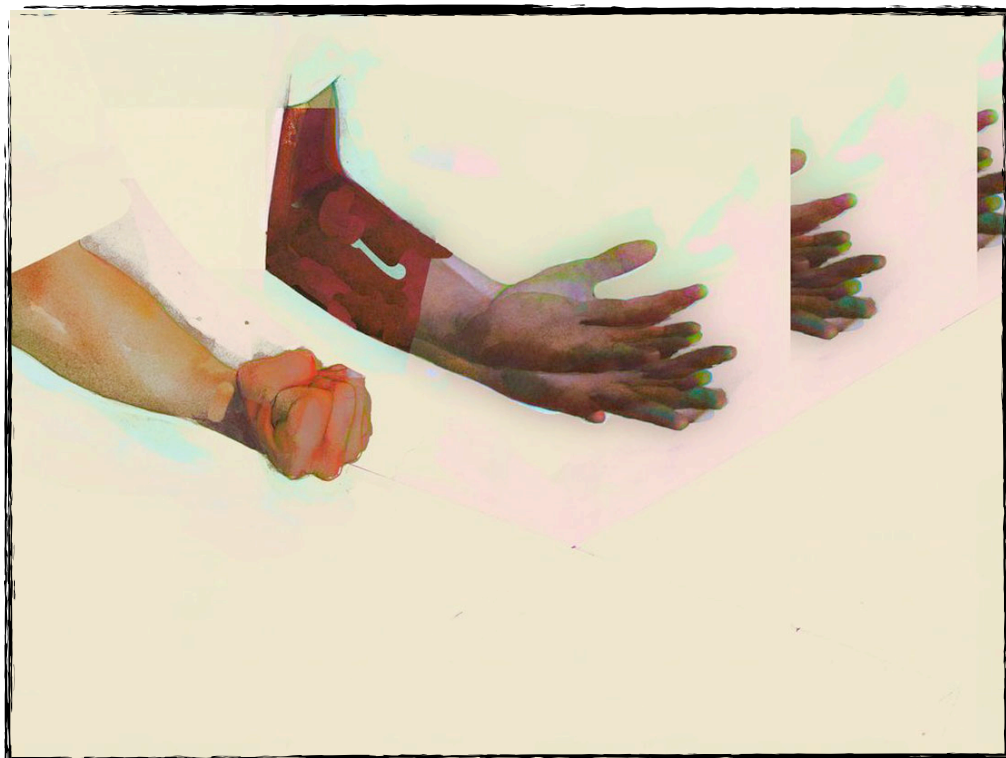
“Vamos a acabar con un número fijo de Bitcoins,” dijo Varoufakis. “Ya estamos forzando la máquina en el sentido que el ritmo de incremento en el número de Bitcoins disponibles está decayendo. Y seguirá haciéndolo. ... Cuando lleguemos [a los 21 millones] será como si todo el oro del mundo hubiese sido extraído.”

Un investigador de los Bitcoin, en un [post de blog](#) en Abril, demostró haber encontrado en la cadena de transacciones Bitcoin evidencia de que un minero tuvo empezado con ventaja sobre todos los demás en el mundo.

Es posible, incluso probable, que Nakamoto tenga muchos de los primeros Bitcoins en existencia, un alijo de casi 1 millón bajo su colchón virtual. Según las tasas de intercambio actuales, el tesoro de Nakamoto podría ser igual o superior a los 100 millones de dólares.

Esto significa que la mayor colección única de Bitcoins en el mundo pertenece a un sólo hombre.

Ya había llegado a la conclusión de que podría jamás encontrar a Nakamoto. Pero, con la ayuda de Varoufakis, era el momento de meterse dentro de su cabeza.



# ***JUEGO DE ÉLITE***

¿Te convierte quedarte con los Bitcoins en más poderoso dentro de esa economía virtual? Para Varoufakis, esa no es realmente la pregunta correcta.

“Lo que es preocupante sobre la economía Bitcoin [a día de hoy],” dijo Varoufakis, “es la desproporción entre la demanda de Bitcoins para propósitos especulativos sobre la demanda para propósitos transaccionales.” No hay suficiente gente intercambiando Bitcoins, y la gran parte de la moneda está quieta en las cuentas de la gente, gente como Nakamoto. Esto está creando una burbuja.

En tiempos de Grecia y Roma, el cambio se hacía literalmente cortando monedas en dos. Los Bitcoins también pueden ser subdivididos, hasta la 1/100,000,000 (-ésima) parte, una denominación apodada “Satoshi”. Pero VARoufakis dice que cuando el último Bitcoin sea extraído no habrá ni uno más, causando deflación. Al tiempo que la economía Bitcoin sigue creciendo, habrá la misma cantidad de dinero en el sistema, y las divisiones no serán suficientes para expandirlo lo suficiente.

*“lo que surgirá será una  
profundamente arraigada  
aristocracia Bitcoin, con Nakamoto  
y otros jugando el papel de señores  
feudales, jugadores de élite que no  
pueden ser derrocados a menos  
que decidan desprenderse de su  
botín  
”*

Lo que surgirá será una profundamente arraigada aristocracia Bitcoin, con Nakamoto y otros jugando el papel de señores feudales, jugadores de élite que no pueden ser derrocados a menos que decidan desprenderse de su botín. Y su único incentivo para deshacerse de ese botín es, naturalmente, por beneficio.

Pero si Nakamoto lanzase su fortuna a la economía Bitcoin a día de hoy en un esfuerzo de recoger ganancias y huir, podría contaminar el pozo. La gente huiría del Bitcoin; la moneda se vería devaluada incluso más rápido que cuando se acabe de extraer.

Empecé a pensar si quizás Nakamoto no se estaba guardando su botín por beneficio. Quizás se estaba aferrando a él a modo de interruptor de emergencia para todo el experimento Bitcoin. ¿Pero por qué querría pulsar ese botón?

Varoufakis esquivó la pregunta.

"No me gustan las teorías de la conspiración, y no me gusta proyectar sobre los demás las reflexiones de una mente suspicaz."

Suficientemente claro. Me dejó que sacase mis propias conclusiones. Por suerte, había una persona más con la que podría hablar.



# *UN UNIVERSO ALTERNATIVO*

Eyjolfur Guomundsson es doctor en economía ambiental y de recursos. En su posición como economista líder para el juego *Eve Online* de CCP, preside una de las economías intra-juego más grandes jamás creadas. *Eve* se ha convertido en el modelo de complejo y adictivo juego online masivo. Es ridiculizado por muchos como un juego tan turbio que se juega a sí mismo, mientras otros dicen que su comunidad se comporta más como una mafia virtual que cualquier tipejo duro cuya caricatura ha empuñado una pistola en un Grand Theft Auto.

Pero por encima de todo eso, *Eve* es un conjunto de negocios virtuales que operan en economía virtuales usando monedas virtuales. Ese es el anzuelo. Eso es lo que hace al juego excitante.

“Las monedas virtuales son básicamente como cualquier otra moneda,” me dijo Guomundsson. “Esto es, una medida de valor económica que es usada en un sistema. En un sistema de juego ... los diseñadores pueden decidir mantenerlo todo como un sistema cerrado o abierto”. Un sistema totalmente abierto es inusual en juegos, porque permite poner dinero en el sistema y después sacarlo como dinero real.

Puede, por ejemplo, vender tus sombreros y cartas de colección en la tienda Steam de Valve. Pero no puedes necesariamente sacar ese dinero de tu monedero Steam y comprar pañales o medicamentos en Walgreens. El único ejemplo vino a la mente de Guomundsson, o que he podido encontrar, es *Second Life*, cuya moneda intra-juego puede ser intercambiada por dólares y viceversa en un negocio de intercambio llamado LindeX.

*“las monedas virtuales son básicamente como cualquier otra moneda. esto es, una medida de valor económica*

*que es usada en un sistema.  
en un sistema de juego los  
diseñadores pueden decidir  
mantenerlo todo como un  
sistema cerrado o abierto*  
”

Prácticamente toda moneda virtual que existe en un videojuego es un sistema cerrado para permitir la existencia de diferentes reglas y diferentes regulaciones a aquellas que puedes tener en la vida real. No hay una Reserva Federal Galáctica controlando tipos de interés en *Eve*. Sólo hay una corporación, una corporación del mundo real en Islandia llamada CCP, diciéndote lo que puedes y lo que no puedes hacer con su moneda virtual.

Curiosamente, el mismo *Eve* contiene dos tipos de monedas. Uno de ellos, el ISK, existe sólo dentro del juego, mientras que PLEX puede ser comprado con dinero del mundo real. Diferentes reglas se aplican a cada economía monetaria una vez que existe en el juego, pero donde esas economías se encuentran dentro de *Eve* se parece mucho a donde el Bitcoin se encuentra con el Dólar. La mayor diferencia es que no puedes sacar el ISK o el PLEX de *Eve*. No hay forma legal de convertirlos en otra moneda.

“Monitorizamos con bastante cuidado las interacciones entre los jugadores,” dijo Guomundsson. “Si se te encuentra intentando vender bienes virtuales por dinero real eres instantáneamente expulsado del juego. Porque queremos mantener esto cerrado, porque queremos tener diferentes normas y diferentes regulaciones que aquellas que puedes encontrar en la vida real.”

Mientras que esto no impide que la economía interna de *Eve* crezca, mantiene a CCP fuera de la jurisdicción de las organizaciones monetarias internacionales. Erige un muro entre la moneda virtual y las reales.

¿Pero qué pasaría si ese muro se destruyese? Guomundsson me contó acerca de una ocasión en la que una moneda virtual hizo justamente eso.





## ***FIN DEL JUEGO***

En marzo de 2007 la moneda china QQ, una moneda virtual que se ganaba al jugar a mini-juegos online, **augmentó su valor** más del 70% en cuestión de semanas. Y eso fue porque los chinos empezaron a usar las monedas QQ fuera del mundo virtual, mediante varios medios, para comprar cosas físicas como CDs de música y maquillaje y servicios como sesiones eróticas de chat online. Jugando a un juego, la gente era capaz de crear valor en el mundo real.

Ganas monedas QQ es análogo a sacar Bitcoins, con una excepción. Las monedas QQ estaban mantenidas por compañías dentro de un estado soberano con su propia moneda fiduciaria, China. Pronto se formularon regulaciones para combatir la moneda QQ antes de que desestabilizase al Yuan.

Pero el Bitcoin no se puede combatir. No hay una organización a la que castigar por su propagación. Está suelta en libertad, un instrumento monetario de código abierto fuera del control de cualquier nación. Pero a ojos de Guomundsson, está

lejos de ser perfecta. Los Bitcoin son una burbuja, me dijo, parafraseando a Varoufakis. Las burbujas explotan.

*“la antigua palabra griega para dinero, para moneda, es 'nomisma' proviene del verbo 'imaginar'”*

¿Pero, y si hubiese un mejor Bitcoin? Guomundsson ve la semilla de esto en los medios sociales. Mientras que la confianza en las instituciones financieras es cara, y donde por contraste Bitcoin hace funcionar la económica confianza en las matemáticas, ¿y si la verdadera confianza viniese a existir a través de un sistema como Facebook, o Twitter?

“Tan pronto como la conectividad [en los medios sociales] llegue a niveles donde la gente comienza a confiar en los demás,” dijo Guomundsson, “y comienzan a confiar información con ese sistema social, tener valor intercambiado por algún medio de transacción es un fenómeno natural.”

Los miembros de una red social buscarán el valor, me dijo Guomundsson, del mismo modo que el agua busca su camino a través de una presa. Es una fuerza natural, un paso evolutivo. Es como el hombre primitivo comenzó a intercambiar en primer lugar.

“Una vez que consigues que ese intercambio de valor se haga de forma eficiente, la gente empieza a buscar por algo que puedan usar como moneda, que puede ser cualquier tipo de ítem virtual que está disponible en esa red social, o algo provisto por la propia red. De modo que el mundo está realmente en un lugar en el que no ha estado nunca jamás, y esto es algo de lo que no creo que ni muchos académicos o gobiernos se han dado cuenta hasta ahora.

Facebook y Twitter no son los precursores del final de nuestras economías, sin embargo.

“Facebook es un mal ejemplo,” dijo Guomundsson, “porque la esencia de Facebook se basa en minimizar el número de los grupos; quiere hablar con tus viejos colegas, quieres estar al día con los miembros de tu familia y demás, pero no estás realmente intentando conectarte con el resto del mundo.

“¿Y si alguien inventase una red social que se centra en la conectividad?” Guomundsson cree que un juego como Eve podría ser tal red, pero no es lo suficientemente grande, ni de lejos. Pero algún día podría serlo, o alguna como ella.

Me pregunto si quizás Nakamoto esperaba esto. Quizás su visión llegaba lo suficientemente lejos cuando concibió Bitcoin, que también concibió el final del Bitcoin. Quizás su botín, sus 100 millones de dólares, es el interruptor que se guarda. Quizás la jugada final de Nakamoto sea destruir Bitcoin de modo que otro, más perfecto, instrumento pueda hacerse con la economía global.

O quizás no. Quizás simplemente quiere hacerse rico, un escenario que tanto Varoufakis como Guomundsson creen improbable ya que sería catastrófico para el Bitcoin.

Nakamoto es o una persona mucho más inteligente de lo que creemos, u otro burdo ladrón más.

Pero un comentario que Varoufakis compartió sigue conmigo.

“La antigua palabra griega para dinero, para moneda, es 'nomisma.' Proviene del verbo 'imaginar.'

De modo que el dinero tiene valor en la medida que imaginamos que tiene valor, de acuerdo con los antiguos griegos. Lo sabían ya hace más de 2,000 años, y parece que olvidamos esa simple e importante noción a veces. 