

Cypherpunks | El origen y la filosofía detrás de Bitcoin

"Privacy is necessary for an open society in the electronic age. **Privacy is not secrecy.** A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. **Privacy is the power to selectively reveal oneself to the world.**"

— Eric Hughes, *A Cypherpunk's Manifesto* (1993)

Bebop

Publicado: 17/10/2022

Tags: Historia, Cypherpunk

Para entender el presente hay que mirar al pasado. En este clip de audio, os preparo una ruta hacia las entrañas de la corriente filosófica Cypherpunk. A lo largo de la ruta nos detendremos en 3 grandes paradas que marcaron la historia, el origen, el por qué y el cómo de la aparición de Bitcoin como lo conocemos hoy en día. Espero que lo disfruteis.

Link (MEGA) del podcast: <https://mega.nz/file/lH0HkCjI#8Q9LjAD-DXdGCT9GiVQcYcPcc2JRxLTtO4ngPBjaqJ0>

Especial agradecimiento a:

[@lunaticoin](#) [@alfremancera](#) [@satoshinakamotoinstitute](#) [@bitcoinmagazine](#)

California de los '70. Universidad de Berkeley, sociedad abierta. Contexto social liberal. Caldo de cultivo perfecto...

- UNIX: primer SO
- '76: la AECA otorga a la criptografía la categoría de arma. Al mismo tiempo y a modo reivindicativo Diffie-Helman-Merkel => Sistemas de clave asimétrica (dos claves, pública y privada)
- '81: empiezan las primeras conferencias cryptologia¹ en sta barbara, caifornia. David chau, crean correos electrónicos digitales intraqueables y firmas ciegas para pagos no traceables. Seguridad sin identificación: sistemas de transacción para hacer obsoleto al Big brother. Electronic cash intraceable (firmado por David Chaum. Moni Naor y Amos Fiat)
- '83: GNU

Por aquel entonces los procesadores de Intel padecían un problema inducido por partículas Alpha. El joven ingeniero Timothy C. May que trabajaba para Intel fue el encargado de descubrir y solucionar la falla. Gracias a su trabajo se pudo retirar a los 34, lo que hoy conoceríamos como libertad financiera. El resto de su vida la dedicó en cuerpo y alma al movimiento que despertó gracias al:

Manifiesto crypto-anarquísta

Un espectro está surgiendo en el mundo moderno, el espectro de la cripto anarquía.

La informática está al borde de proporcionar a grupos e individuos, la capacidad de comunicarse e interactuar entre ellos de forma totalmente anónima. Dos personas podrán intercambiar mensajes, hacer negocios y negociar contratos electrónicos, sin saber nunca el nombre real o identidad legal de la otra parte. Las interacciones sobre las redes serán intrazables, gracias al uso extendido de re-enrutado de paquetes encriptados en máquinas a prueba de manipulación que implementen protocolos criptográficos con garantías casi perfectas contra cualquier intento de alteración. Las reputaciones tendrán una importancia crucial, mucho más importante en los acuerdos que las calificaciones crediticias de hoy en día. Estos progresos alterarán completamente la naturaleza de la regulación del gobierno, la capacidad de gravar, de controlar las interacciones económicas, la capacidad de mantener la información secreta e incluso alterarán la naturaleza de la confianza y

de la reputación.

La tecnología para esta revolución (que de bien seguro será social y económica) ha existido teóricamente durante la última década. Los métodos están basados en el cifrado de clave pública, sistemas interactivos de prueba de cero-conocimiento, y varios protocolos de software para la interacción, autenticación y verificación. El foco hasta ahora ha estado en conferencias académicas de Europa y EE.UU., conferencias monitorizadas de cerca por la Agencia de Seguridad Nacional. Pero solo recientemente las redes de ordenadores y computadoras personales han alcanzado la velocidad suficiente para hacer las ideas realizables en la práctica. Y los próximos 10 años traerán suficiente velocidad adicional para hacer estas ideas factibles económicamente y, en esencia, imparables. Redes de alta velocidad, ISDN, tarjetas inteligentes, satélites, transmisores Ku-Band, ordenadores personales multi-MIPS, y chips de cifrado, ahora en desarrollo, serán algunas de las tecnologías que lo permitirán.

El Estado intentará, por supuesto, retardar o detener la expansión de esta tecnología, citando preocupaciones de seguridad nacional, el uso de esta tecnología por parte de traficantes de droga y evasores fiscales,,, y miedos de desintegración social. Muchas de estas preocupaciones serán válidas; la criptoanarquía permitirá la comercialización libre de secretos nacionales y la comercialización de materiales ilícitos y robados. Un mercado computarizado anónimo permitirá incluso el establecimiento de horribles mercados de asesinato y extorsión. Varios elementos criminales y extranjeros serán usuarios activos de la CryptoNet. Pero esto no detendrá la expansión de la cripto anarquía.

Al igual que la tecnología de impresión alteró y redujo el poder de los gremios medievales y la estructura del poder social, también los métodos criptológicos alterarán la naturaleza de las corporaciones y la interferencia del gobierno en las transacciones económicas.

La cripto anarquía, combinada con los mercados de información emergentes, creará un mercado líquido para cualquier material que pueda ponerse en palabras e imágenes. Y de la misma manera que una invención aparentemente menor como el alambre de espino hizo posible el cercado de grandes ranchos y granjas, alterando así para siempre los conceptos de tierra y los derechos de propiedad en las fronteras de Occidente, así también el descubrimiento aparentemente menor de una rama arcana de las matemáticas se convertirá en el alicate que desmantele el alambre de espino alrededor de la propiedad intelectual.

¡Levántate, no tienes nada que perder excepto tus propias cercos de alambre de espino!

La cripto anarquía, combinada con los mercados de información emergentes, creará un mercado líquido para cualquier material que pueda ponerse en palabras e imágenes. Y de la misma manera que una invención aparentemente menor como el alambre de espino hizo posible el cercado de grandes ranchos y granjas, alterando así para siempre los conceptos de tierra y los derechos de propiedad en las fronteras de Occidente, así también el descubrimiento aparentemente menor de una rama arcana de las matemáticas se convertirá en el alicate que desmantele el alambre de espino alrededor de la propiedad intelectual.

¡Levántate, no tienes nada que perder excepto tus propias cercos de alambre de espino!

Timothy C. May, 1998 [tcmay@netcom.com]

W.A.S.T.E.: Aptos, CA

Tim May reparte panfletos del discurso por una conferencia hacker y al recibir un feedback tan bueno se anima a mantener el contacto via mail con la gente interesada.

- '90: Empresa digicash por David chaum Equipo formado por Nick sabo, Eric huge, sistema de dinero electrónico basado en cryptografía para implementarlo en sistemas bancarios.
- '91: phil Zimmerman:PGP 1.0 (pretty Good privacy) modesto el hombre. Sistema de cifrado de cryptografía fuerte el cual fue publicado a internet por el mismo Phil. Por ese motivo tubo problemas con las autoridades estadounidenses. Quedó absuelto luego de múltiples investigaciones
- '91: unión de GNU/Linux
- '92: Mientras tanto Tim May , Eric Hughes y Johon Gilmour abrumados por el potencial del movimiento criptoanarquico, se reúnen i invitan a otros criptologos para idear formas de potenciar el movimiento. Se reúnen en la casa de Gilmour en Oclan. A la reunión se unen dos personajes más: Hal finey y Jude milhon asisten a la reunion
- A todo esto; jude milhon, activista y apasionada del género cyberpunk (género de ciencia ficción donde se plantea un futuro distòpico de tecnología avanzada con una gran desigualdad entre clases) suelta la broma de: vosotros sois cypherpunks (haciendo la analogía entre cypher: cifrage y punk como a parte reivindicativa y en contra del orden estableció)
- Eric Hughes 9 de Marzo 1993:

Manifiesto Cypherpunk

La privacidad es necesaria para una sociedad abierta en la era electrónica. La privacidad no es confidencialidad. Un asunto privado es algo que uno no quiere que todo el mundo sepa, pero un asunto secreto es algo que uno no quiere que nadie sepa. La privacidad es el poder de revelarse uno mismo al mundo de forma selectiva.

Si dos personas tienen algún tipo de trato, entonces cada una tiene un recuerdo de su interacción. Cada parte puede hablar de su propio recuerdo sobre el tema; ¿Cómo podría prevenirse esto? Se podrían aprobar leyes en su contra, pero la libertad de expresión, es aún más fundamental, para una sociedad abierta, que la privacidad. Nuestra intención no es restringir ningún discurso. Si muchas partes hablan entre ellas en un mismo foro, cada una puede hablar con todas las demás y agregar conocimientos sobre individuos y otras partes. El poder de las comunicaciones electrónicas ha permitido tal comunicación grupal, y esto, no desaparecerá simplemente porque nosotros queramos.

Dado que deseamos privacidad, debemos asegurarnos de que cada parte de una transacción tenga conocimiento solo de lo que es estrictamente necesario para tal transacción. Dado que cualquier información puede ser reproducida, debemos asegurarnos de revelar lo menos posible. En la mayoría de los casos, la identidad personal no es relevante. Cuando compro una revista en el quiosco y le doy dinero en efectivo al empleado, no hay necesidad de saber quién soy. Cuando le pido a mi proveedor de correo electrónico que envíe y reciba mensajes, mi proveedor no necesita saber con quién estoy hablando o qué estoy diciendo o lo que otros me están diciendo; mi proveedor solo necesita saber cómo hacer llegar el mensaje y cuál es mi tarifa por su servicio. Cuando mi identidad es revelada por el mecanismo subyacente de la transacción, no tengo privacidad. Aquí, no puedo revelarme selectivamente; aquí debo revelarme siempre.

Por esta razón, la privacidad en una sociedad abierta requiere sistemas de transacciones anónimos. Hasta ahora, el efectivo ha sido el principal sistema de este tipo.

Un sistema de transacciones anónimo, no es un sistema de transacciones secretas. Un sistema anónimo permite a las personas revelar su identidad cuando lo deseen y solo cuando lo deseen; esta es la esencia de la privacidad.

La privacidad en una sociedad abierta requiere criptografía. Si digo algo, quiero que sea escuchado solo por aquellos a quienes me propongo. Si el contenido de mi discurso es accesible para el mundo, no tengo privacidad. Encriptar es indicar el deseo de privacidad, y encriptar con criptografía débil es indicar no tener demasiado deseo de privacidad. Además, revelar la propia identidad con certeza cuando el anonimato es la norma, requerirá de firma criptográfica.

No podemos esperar que los gobiernos, las corporaciones u otras grandes organizaciones nos otorguen privacidad por pura caridad. Es beneficioso para ellos hablar de nosotros, y debemos esperar que lo hagan. Intentar impedir su discurso es luchar contra la realidad de la información. La información no solo quiere ser libre, anhela ser libre. La información se expande hasta llenar el espacio de almacenamiento disponible. La información es la prima más joven y fuerte del rumor. La información es más veloz, tiene más ojos, sabe más, pero comprende menos que el rumor.

Debemos defender nuestra propia privacidad si esperamos tener alguna. Debemos unirnos y crear sistemas que permitan que se realicen transacciones anónimas. La gente ha estado defendiendo su propia privacidad durante siglos con susurros, ocultación, sobres, puertas cerradas, apretones de manos secretos y mensajeros. Las tecnologías del pasado no permitían una privacidad fuerte, pero las tecnologías electrónicas sí lo hacen.

Nosotros, los Cypherpunks nos dedicamos a construir sistemas anónimos. Defendemos nuestra privacidad con criptografía, con sistemas de reenvío de correo anónimo, con firmas digitales y con dinero electrónico.

Los Cypherpunks escriben código. Sabemos que alguien tiene que escribir software para defender la privacidad, y como no podemos obtener privacidad a menos que todos lo hagamos, lo vamos a escribir nosotros mismos. Publicamos nuestro código para que nuestros compañeros Cypherpunks puedan practicar y jugar con él. Nuestro código es libre para todo el mundo que quiera usarlo. No nos importa mucho si no aprueba el software que escribimos. Sabemos que el software no puede

ser destruido y que un sistema ampliamente disperso no se puede destruir.

Los Cypherpunks deploran las regulaciones sobre criptografía, ya que el encriptado es fundamentalmente un acto privado. El acto de encriptar, de hecho, elimina información del ámbito público. Incluso las leyes contra la criptografía solo se extienden hasta la frontera de una nación, hasta donde alcanza el brazo de su violencia. La criptografía se extenderá ineludiblemente por todo el mundo, y con ella los sistemas de transacciones anónimas que habilita.

Para que la criptografía sea generalizada, debe ser parte de un contrato social. La gente debe unirse y desplegar estos sistemas para el bien común. La privacidad solo llega tan lejos como la cooperación entre miembros de cada sociedad. Nosotros los Cypherpunks buscamos tus preguntas e inquietudes y esperamos que te involucres para que no nos engañemos a nosotros mismos. Sea como sea, no nos desviemos de nuestro rumbo porque algunos puedan estar en desacuerdo con nuestras metas.

Los Cypherpunks estamos comprometidos en hacer de las redes un lugar más seguro para la privacidad. Procedamos juntos, a toda prisa, adelante.

Eric Hughes, 9 de Marzo 1993

El movimiento salió en la portada de la revista WIRED con el título:

Rebeldes con una causa. El discurso se propagó a las masas.

Se crea un a lista de correo con remailers anónimos (anteriormente creado por hal finei y huge). Acordaban reuniones una vez al mes en la empresa de John Gilmore. Se crean debates y el cyphernomicon (FAQ's) por Tim May

'94: Clipper Chip, back door por la NSA. eCASH David Chaum con digicash y hace una demostración de transacción anónima

'96: John Perry Barlow íntimo amigo de John Gilmore y crean la EFF (fundación sin ánimo de lucro para defender los derechos civiles en el medio digital)

El 8 de febrero de 1996 se firmó en Estados Unidos la Ley de Telecomunicaciones, la cual proponía transformar el mercado de las telecomunicaciones eliminando imposiciones que en el pasado habían limitado los alcances de las empresas. Entre otras cosas, la ley contenía el Decency Act, una cláusula que pretendía volver ilegal ciertos contenidos sensibles en internet. La Ley de Telecomunicaciones –precedente claro de leyes que se intentarían aprobar después, como CISA (Cybersecurity Information Sharing Act) – detonó la indignación de los usuarios de la Red, quienes por primera vez tuvieron que defender la autonomía cibernética ante los poderes de los Estados. John Perry Barlow, poeta, ensayista y ciberactivista, publicó esta declaración desde Davos, Suiza, el mismo día que la ley fue aprobada. A poco más de un año de su muerte – 7 de febrero del año pasado –, Tierra Adentro reproduce la declaración, en traducción de Luis Ham, para recordar (hoy como todos los días) la importancia de la libertad en el ciberespacio.

8 de febrero de 1996, en la ciudad de Davos, Suiza:

Declaración de independencia del Ciberespacio

Gobiernos del Mundo Industrial, vosotros, fatigados gigantes de carne y acero: vengo del Ciberespacio, el nuevo hogar de la Mente. En nombre del futuro os pido en el pasado, que nos dejéis en paz. No sois bienvenidos entre nosotros. No ejercéis ninguna soberanía sobre el lugar donde nos reunimos. No hemos elegido ningún gobierno, ni pretendemos tenerlo, así que me dirijo a vosotros sin más autoridad que aquélla con la que la libertad siempre habla:

Los gobiernos obtienen su poder del consentimiento de los gobernados. No habéis pedido ni recibido el nuestro. No os hemos invitado. No nos conocéis, ni conocéis nuestro mundo. El Ciberespacio no se halla dentro de vuestras fronteras. No penséis que podéis construirlo, como si fuera un proyecto público de construcción. No podéis. Es un acto natural que crece por medio de nuestras acciones colectivas.

No os habéis unido a nuestra gran conversación colectiva, ni creasteis la riqueza de nuestros mercados. No conocéis nuestra cultura, nuestra ética, o los códigos no escritos que ya proporcionan a nuestra sociedad más orden que el que podría obtenerse por cualquiera de vuestras imposiciones.

Proclamáis que hay problemas entre nosotros que necesitáis resolver. Usáis esto como una excusa para invadir nuestros límites. Muchos de estos problemas no existen. Donde haya verdaderos conflictos, donde haya errores, los identificaremos y resolveremos por nuestros propios medios. Estamos creando nuestro propio Contrato Social. Esta forma de gobierno se creará según las condiciones de nuestro mundo, no del vuestro. Nuestro mundo es diferente.

El Ciberespacio está formado por transacciones, relaciones, y pensamientos en sí mismo, que se extienden como una onda estacionaria en la telaraña de nuestras comunicaciones. El nuestro es un mundo que está a la vez en todas partes y en ninguna, pero no está donde viven los cuerpos físicos.

Estamos creando un mundo en el que todos pueden entrar, sin privilegios o prejuicios debidos a la raza, el poder económico, la fuerza militar, o el lugar de nacimiento.

Estamos creando un mundo donde cualquiera, en cualquier sitio, puede expresar sus creencias, sin importar lo singulares que sean, sin miedo a ser coaccionado mediante el silencio o el conformismo.

Vuestros conceptos legales sobre propiedad, expresión, identidad, movimiento y contexto no se aplican a nosotros. Se basan en la materia, y aquí no hay materia.

Nuestras identidades no tienen cuerpo, así que, a diferencia de vosotros, no podemos obtener orden por coacción física. Creemos que nuestra autoridad emanará de la moral, de un progresista interés propio, y del bien común. Nuestras identidades pueden distribuirse a través de muchas de vuestras jurisdicciones. La única ley que todas nuestras culturas reconocerían es la Regla Dorada. Esperamos ser capaces de construir nuestras soluciones particulares sobre esa base. Pero no podemos aceptar las soluciones que estáis tratando de imponer.

En Estados Unidos hoy habéis creado una ley, el Acta de Reforma de las Telecomunicaciones, que repudia vuestra propia Constitución e insulta los sueños de Jefferson, Washington, Mill, Madison, De Tocqueville y Brandeis. Estos sueños deben renacer ahora en nosotros.

Os atemorizan vuestros propios hijos, ya que ellos son nativos en un mundo donde vosotros siempre seréis inmigrantes. Como les teméis, encomendáis a vuestras burocracias las responsabilidades paternales a las que sois demasiado cobardes para enfrentaros por vosotros mismos.

En nuestro mundo, todos los sentimientos y expresiones de humanidad, desde las más viles a las más angelicales, son parte de un todo único, la conversación global de bits. No podemos separar el aire que asfixia del aire sobre el que se baten las alas.

En China, Alemania, Francia, Rusia, Singapur, Italia y los Estados Unidos estáis intentando rechazar el virus de la libertad erigiendo puestos de guardia en las fronteras del Ciberespacio. Éstos puede que impidan el contagio durante un corto lapso de tiempo, pero no funcionarán en un mundo que pronto estará cubierto por los medios de transmisión de bits.

Vuestras cada vez más obsoletas industrias de la información se perpetuarían a sí mismas proponiendo leyes, en América y en cualquier parte del mundo, reclamando la posesión de la palabra. Estas leyes declararían que las ideas son otro producto industrial, no más noble que el hierro oxidado. En nuestro mundo, sea lo que sea lo que la mente humana pueda crear, puede ser reproducido y distribuido infinitamente sin coste alguno. El trasvase global de pensamiento ya no necesita de vuestras fábricas para ser realizado.

Estas medidas, cada vez más hostiles y colonialistas, nos colocan en la misma situación en la que estuvieron aquellos amantes de la libertad y la autodeterminación que tuvieron que luchar contra la autoridad de un poder lejano e ignorante. Debemos declarar nuestros «yos» virtuales inmunes a vuestra soberanía, aunque continuemos consintiendo vuestro poder sobre nuestros cuerpos. Nos extenderemos a través del planeta para que nadie pueda encarcelar nuestros pensamientos.

Vamos a crear una civilización de la Mente en el Ciberespacio. Que sea más humana y hermosa que el mundo que vuestros gobiernos han creado hasta ahora.

John Perry Barlow, 8 de Febrero 1996

Cyperpunks en la actualidad:

- *Adam Back*
- *Nick Szabo*
- *Mad Blaze*
- *Jamison Loop*
- *Pavel Durov*

1 Cryptografia y cryptoanàlisis

Revision #1

Created 27 November 2024 23:02:36 by meowtoshi

Updated 27 November 2024 23:11:06 by meowtoshi