ÍNDICE

PRÓLOGO

El libro que estás a punto de leer se centra en una de las tecnologías más revolucionarias y transformadoras de la realidad que han aparecido en los últimos tiempos: Blockchain. Se trata de la tecnología subyacente del ya famoso Bitcoin, pero que excede con creces el ser un mero soporte a la evolución de la criptomoneda más importante.

El poder transformador que encierra es comparable al que tuvo en su momento la irrupción de la llamada internet 2.0. Tan comparables son ambos momentos de profundas transformaciones tecnológicas, que no solo comparten su poder transformador de la realidad, sino también las expectativas a veces desmedidas, y la cantidad de inversiones que se mueven en torno a esto, tanto de importantes empresas de primera línea que participan aportando grandes sumas de dinero en fondear start-ups, como proyectos gubernamentales en países del primer y tercer mundo por igual.

Considero que el mundo de hoy es el mundo del conocimiento, y la potencia de ese conocimiento unido a buenas ideas que surgen desde un entorno cambiante, horizontal, y continuamente en evolución. Es por eso que mi objetivo es permitirte comprender de manera cabal qué significan Blockchain y SmartContracts, no solo desde una perspectiva técnica, sino con una mirada abarcadora, pudiendo entender el impacto de cada uno de estos conceptos. También, busco explicarlos de la forma más sencilla, ya que el resultado de la aplicación de la tecnología no será algo que afecte solo a unos pocos, sino que se esparcirá entre nuestra vida cotidiana, posiblemente, de acá a unos cinco o diez años, y te afecte a ti y a tu entorno. Entonces, sin perder la exactitud técnica, podrás entender los entretelones de estos grandes conceptos.

El autor

Emiliano B. Ocariz es Ingeniero en Informática, Project Manager y profesor de informática. Apasionado desde pequeño por la programación y la tecnología, cuenta con más de 20 años de experiencia en desarrollo y como Arquitecto de Software estuvo al frente de la generación de aplicaciones World Class para empresas de primera línea en más de 30 países. Junto con su labor técnica, transmite sus conocimientos profesionales impartiendo cursos de las últimas tecnologías, tanto en forma presencial como mediante plataformas digitales de capacitación. Interesado desde hace años en el mundo de las criptomonedas y la tecnología blockchain, siguió de cerca su constante evolución y la explosión de aplicaciones diversas que hoy en día esta herramienta puede tener en la vida cotidiana. Actualmente escribe y transmite las últimas novedades que surgen en torno a esta interesante tecnología.

1 POTENCIAL BLOCKCHAIN

LA DEFINICIÓN DE BLOCKCHAIN

Si buscamos en wiktionary una definición de blockchain, encontraremos:

blockchain (*plural* **blockchains**)

1. A shared record of past transactions in a cryptocurrency network.

La definición nos cuenta que es un registro compartido de transacciones pasadas en una red de criptomonedas. Pero si las virtudes y la importancia de blockchain, o cadena de bloques, residiera en lo que expresa esta definición, sería muy poco el impacto real como tecnología dentro de un mundo en constante avance tecnológico.

Sin embargo, a lo largo de este libro, espero poder transmitir la importancia real y potencial que puede tener blockchain, no solo aplicada al mundo de las criptomonedas, sino a industrias y proyectos tan diversos, que los creadores de esta tecnología nunca podrían haber imaginado.

Otra de las definiciones que podemos encontrar nos refiere a blockchain como un registro, o base de datos, de transacciones descentralizada, autónoma, auditable y confiable. Y el sistema que garantiza la confianza al punto de permitir que individuos que no confían entre sí puedan interactuar de una forma segura sin un intermediario confiable. Es en este punto, la confianza sin intermediarios, donde radica la verdadera revolución y valor agregado que aporta esta tecnología. De esa forma, se pueden realizar transacciones más rápidamente, y sin los costos que implica la intervención de un agente externo con las credenciales y referencias que le den credibilidad suficiente para llevar adelante tal tarea de fiscalización y control.

¿CUÁNTO VALE Y CUÁNTO CUESTA LA CONFIANZA?

Para entender las implicaciones de la confianza, vamos a tener que volver brevemente sobre el concepto mismo de dicha palabra. Según la fuente que tomemos, es una creencia firme sobre la fiabilidad de una persona o entidad y que esta, de ninguna manera, nos defraudará con sus acciones presentes o futuras. Se asocia con otras palabras como veracidad, integridad, fidelidad. La confianza es también a menudo mencionada como una de las más altas virtudes del creyente, llave para adorar y acercarse a la gloria prometida por Dios. Dentro de una relación de amistad o pareja es algo que se construye muy lentamente, y es el cimiento para los mejores vínculos. Ese valor que le damos a la confianza, tan importante, también se refleja cuando esta confianza es traicionada, cuando se rompe ese lazo invisible. Cuanto mayor haya sido lo que se puso en juego, mayor será el dolor y sentimiento de pérdida al quebrantarse.

Podría considerarse que hablar de Dios, amistad y pareja es un ejercicio abstracto y alejado del tema principal que estamos tratando, pero poner el marco adecuado y poder dimensionar la importancia de ciertos temas, nos ayuda a encontrar más fácilmente el valor diferencial que explica el poder revolucionario de la tecnología.

Tomemos por caso, la compra de una propiedad, y pensemos por un momento en el proceso desde que se toma la decisión hasta que finalmente tenemos en nuestras manos la llave y hacemos uso de la misma. Seguramente, después de una larga búsqueda elegiremos la propiedad (casa, departamento o lo que fuera) de nuestro agrado, y una vez convencidos de haber elegido correctamente y establecido que consideramos justo, deberíamos proceder a efectuar la compra. En una compraventa de un inmueble aparecerán muchos intermediarios. Inmobiliarias, escribanos, bancos, registros públicos de propiedad, organismos de recaudación pública, entre otros. Cada uno de estos intermediarios justifica su acción principalmente en la falta de confianza. Vamos a analizar el costo real que implica esta falta confianza. Los bancos, si es que la operación se realiza con dinero de nuestras cuentas, son necesarios porque hasta ahora no existe una forma no centralizada de confiar en que la cantidad de dinero que decimos tener, es la que realmente tenemos y es nuestra única forma de asegurar que ese número de dinero pasa de unas manos a otras. Ahora, si efectuamos la operación con dinero en efectivo, el costo de la desconfianza se verá reflejado en cada uno de los cuidados que tendrá el comprador en el traslado de ese dinero, y el recelo del vendedor, recibiendo cada billete con la incertidumbre de la falsedad o no de cada uno. Por otro lado tenemos los registros de la propiedad y recaudación, que nos exigirán miles de papeles “en regla” para aprobar la transacción y dar por válida la compraventa.

Los escribanos e inmobiliaria por otro lado justifican en gran medida su labor en verificar que cada uno de estos papeles y complicados pasos sea realizado correctamente, y dar fe que todo se ajusta a la verdad y a las reglas.

Ahora, supongamos un mundo donde reina la confianza. Donde no dependamos de organismos centralizados para garantizar la veracidad de nuestra posesión de bienes y dinero, donde no necesitemos otros más que los involucrados en la transacción. De existir esta plena confianza y cierta descentralización de los registros, tomaríamos nuestro dinero y se lo daríamos al vendedor, el cual a su vez nos pasaría su título de propiedad, donde actualizaremos el registro de pertenencia, además de pagar los impuestos correspondientes y ahora pasaría a estar a nuestro nombre. Sencillo, rápido y sin intermediarios, disfrutaríamos mucho antes de tener la llave en la mano y disfrutar de la propiedad.

Entre ambos escenarios podemos, al menos de manera estimativa, apreciar el valor de la confianza y todos los mecanismos que inventamos, con intermediarios y registros, para suplir la falta de la misma, lo que consecuentemente implica costos y tiempos (que se podrían traducir en más costos) en cada una de nuestras transacciones.

Pusimos hasta ahora un único ejemplo, para ilustrar el punto, pero podríamos traer a colación ejemplos más cotidianos, como las comisiones que cobran los bancos en los movimientos de nuestro dinero. O quizás menos cotidianos, pero aún con mayor impacto, dentro de la cadena de suministro de un producto, todos los doble chequeos entre saltos de la cadena para evitar posibles falsificaciones, desde la materia prima hasta el producto final, más todos los trabajadores involucrados en cada uno de los pasos de elaboración. Todas las partes en la elaboración de un producto final nos llevan a preguntarnos, muchas veces con algo de incertidumbre, sobre la calidad de eso que estamos consumiendo. Aún con mayor preocupación, en el caso de que ese producto se trate de un medicamento. En general, pagamos más caro aquellos productos que en base a la reputación de su marca nos generan una confianza mayor. Suponemos que una buena marca tendrá una empresa que la respalde y haga todos los esfuerzos necesarios para mantener el valor de marca, contratando a proveedores certificados, realizando validaciones sobre la calidad de sus suministros, asegurando las condiciones de traslado y cadenas de distribución. Lograr que detrás del respaldo de una marca todos estos pasos se articulen para que día a día el producto tenga una calidad constante no solo es complicado y muy costoso, sino que a pesar de los mejores esfuerzos muchas veces no puede ser garantizado. Nuevamente la confianza vuelve a estar en juego, y queda en evidencia su valor en cada uno de los puntos de la cadena: en nosotros abonando más por el respaldo de la marca, en la empresa productora en el pago mayor a productores

certificados, en los controles que realice en forma pasiva o activa para verificar sus suministros, y todo esto se puede extender tantos pasos atrás en la cadena como se quiera hasta a llegar a las materias primas originales y a la idoneidad y salubridad de cada uno de los trabajadores involucrados.

LA TRANSFORMACIÓN DE LA CONFIANZA

Una vez que reflexionamos un poco sobre el valor intrínseco de la confianza, y los costos operativos que pagamos como sociedad e individuos para suplir con diversos mecanismos la falta de la misma, estamos en condiciones de apreciar en su justa medida la frase que explicamos antes sobre la naturaleza de blockchain.

Blockchain nos provee un mecanismo confiable y distribuido, esto significa, sin depender de una entidad central, que permite articular transacciones entre dos entidades o individuos que no tengan confianza mutua, incluyendo entre las posibles transacciones desde dinero u otros conceptos representables dentro de blockchain como tokens, hasta transacciones que para ser cumplimentadas deban seguir complejos procedimientos establecidos en un contrato inteligente.

Página a página iremos desgranando los sustentos que permiten atribuirle a Blockchain estas cualidades tan potentes y por qué no es desmesurado asignarle un poder transformador en la sociedad, si es que al menos una proporción de todos los proyectos que existen utilizándola, se concretan.

Por el momento, a modo de adelanto, debemos saber que si bien la posibilidad de establecer diferentes relaciones mutuas mediante esta tecnología reduce tiempos y costos, además de promover una participación más democrática, no está exenta de riesgos y desafíos que deberá afrontar para liberar verdaderamente todo su potencial en los próximos años.

2 BITCOIN

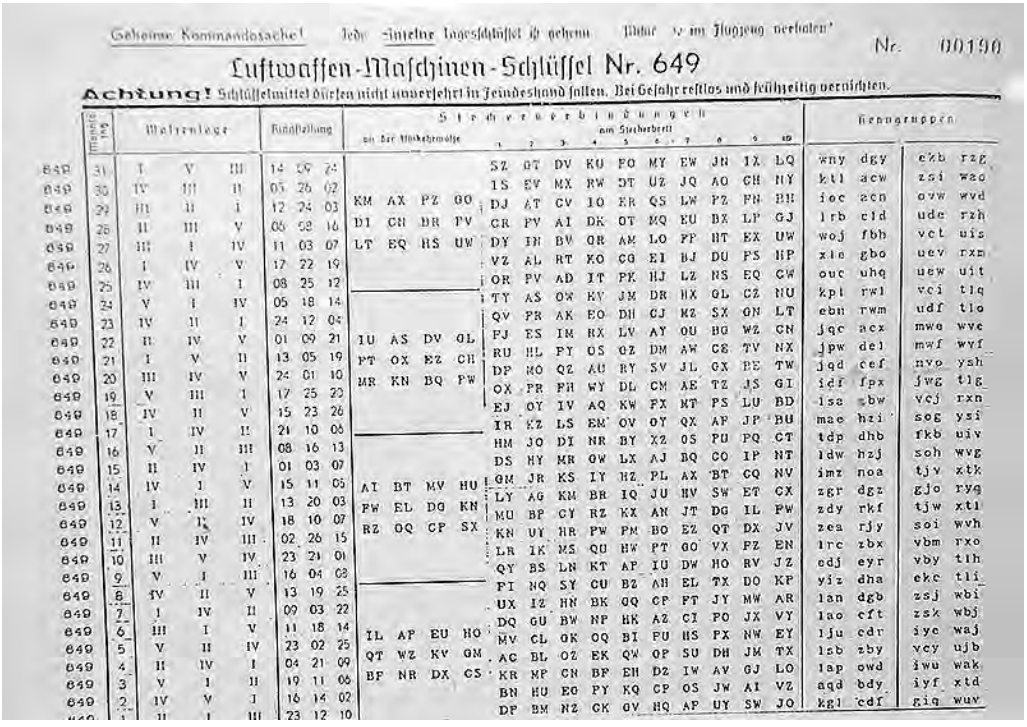
¿CÓMO SURGE EL "MOVIMIENTO BLOCKCHAIN"?

LA ESCRITURA OCULTA

El desarrollo de la criptografía es una de las bases que posibilitó la creación del Bitcoin y fundamentalmente del concepto de blockchain. La palabra proviene del griego "criptos", oculto, y "grafé", escritura, por lo tanto sería algo así como "escritura oculta". Claramente, oculta a los ojos u oídos de desconocidos, pero entendible para los amigos o aliados.

Los orígenes de la criptografía los podemos encontrar en los jeroglíficos egipcios y en la antigua Roma con el cifrado de emperador César o en el Manuscrito Voynich, considerado el "Santo Grial" de la criptografía histórica, pues a pesar de haber sido escrito en el siglo XV, aún no se pudo descifrar.

Más cercano en el tiempo, durante el siglo pasado, de la mano de investigaciones gubernamentales y militares fueron evolucionando las técnicas criptográficas. Durante la Segunda Guerra Mundial, con Alan Turing y su máquina para descifrar el código "Enigma" de la Alemania Nazi, popularizado por la película "The imitation game". Luego el proyecto "Magic" (magia) utilizado por la armada de Estados Unidos para descifrar el código PURPLE (púrpura) generado por Japón. Fue tanta la confianza de los japoneses en la invulnerabilidad de su sistema de cifrado, que hasta muchos años después prefirieron creer que entre sus filas había un infiltrado que divulgaba sus mensajes antes que aceptar que el código PURPLE no era tan seguro como suponían y había sido vulnerado.



Geheime Kommandosache! Jeder Einzelne Tagesschlüssel ist geheim! Nicht in's Flugzeug verboten!

Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und fristgerecht vernichten.

Tag	Walzenlage	Ringstellung	Steckerverbindungen an der Steckerbrett	Kenngruppen
649 31	I V III	14 09 24	SZ GT DV KU FO MY EW JN IX LQ	wny dgy ezb rzg
649 30	IV III II	05 26 02	IS EV MX RW DT UZ JQ AO CH NY	ktl acw zsi wzo
649 29	III II I	12 24 03	KM AX PZ GO DJ AT CV IO ER QS LW PZ FN BH	ioc zcn ovw wvd
649 28	II III V	06 08 16	DI CN BR PV CR PV AI DK OT MQ EU BX LP GJ	lrb cld ude rzh
649 27	III I IV	11 03 07	LT EQ HS UW DY IN BW OR AM LO FP HT EX UW	woj fbh vcl uis
649 26	I IV V	17 22 19	VZ AL RT XO CG EI BJ DU FS HP	xie gbo uev rxn
649 25	IV III I	08 25 12	OR PV AD IT PK HJ LZ NS EQ CW	ouc uhq uew uit
649 24	V I IV	05 18 14	TY AS OW KY JM DR HX GL CZ NU	kpi rwl vci tlq
649 23	IV II I	24 12 04	QV PR AK EO DH CJ MZ SX ON LT	ebn rwm udf tlo
649 22	II IV V	01 09 21	FJ ES IM HX LV AY OU BG WZ GN	jqc acx mwe wve
649 21	I V II	13 05 19	IU AS DV GL RU HL PY OS QZ DM AW CE TV NX	jpw del mwf wvf
649 20	III IV V	24 01 10	PT OX EZ CH DP MO QZ AU RY SV JL CX PE TW	jqd cef nvp ysh
649 19	V III I	17 25 23	MR KN BQ PW OX PR PH WY DL CM AE TZ JS GI	idf fpx jwg tlg
649 18	IV II V	15 23 26	EJ OY IV AQ KW FX MT PS LU BD	isa sbw vcj rxn
649 17	I IV II	21 10 06	IR KZ LS EM OV OY QX AP JP BU	mae hzi sog ysi
649 16	V II III	08 16 13	HM JO DI NR BY XZ OS PU PQ CT	tdp dhb fkb uiv
649 15	II IV I	01 03 07	DS HY MR OW LX AJ BQ CO IP NT	idw hzj soh wvg
649 14	IV I V	15 11 05	GM JR KS IY HZ PL AX BT CQ NV	imz noa tjv xtk
649 13	I III II	13 20 03	AI BT MV HU LY AG KM BR IQ JU HV SW ET CX	zgr dgz gjo ryg
649 12	V II IV	18 10 07	FW EL DG KN MU BP CY RZ KX AN JT DG IL PW	zdy rkf tjw xtl
649 11	II IV III	02 26 15	RZ OQ CP SX KN UY HR PW FM BO EZ QT DX JV	zea rjy soi wvh
649 10	III V IV	23 21 01	LR IK MS QU HW PT GO VX PZ EN	irc zbx vbm rxo
649 9	V I III	16 04 08	QY BS LN KT AP IU DW HO RV JZ	odj eyr vby tih
649 8	IV II V	13 19 25	FI NQ SY CU BZ AH EL TX DO KP	yiz dha ekc tli
649 7	I IV II	09 03 22	UX IZ HN BK GQ CP FT JY MW AR	lan dgb zsj wbi
649 6	III I V	11 18 14	DQ GU BW NP HK AZ CI PO JX VY	lao cft zsk wbj
649 5	V II IV	23 02 25	IL AP EU HO MV CL GK OQ BI FU HS PX NW EY	lju cdr iye waj
649 4	II IV I	04 21 09	QT WZ KV GM AC BL OZ EK QW OP SU DH JM TX	lsb zby vcy ujb
649 3	V I II	19 11 06	BF NR DX CS KR MP CN BP EH DZ IW AV GJ LO	lap owd iwu wak
649 2	IV V I	16 14 02	BN HU EO PY KQ CP OS JW AI VZ	aqd bdy iyf xtd
649 1	II I III	23 12 10	DF BM NZ CK GV HQ AF UY SW JO	kgl cdf giq wuv

Ilustración del cifrado del código Enigma

Entre ambas guerras mundiales, sobrevino la guerra fría, una guerra sin un enfrentamiento abierto pero llena de desconfianza entre los países. Su extensa red de espionaje y contraespionaje sirvió como incentivo para la generación de códigos criptográficos cada vez más complejos, intentando mantener las más oscuras conversaciones entre estados en secreto y a salvo del enemigo.

Dentro de este período de guerra fría y en un contexto donde las diferentes potencias llevaron al máximo su esfuerzo para mejorar y hacer seguros sus sistemas de comunicación, es donde se da un paso muy importante para el desarrollo de Blockchain: el sistema de criptografía asimétrica con clave pública-clave privada. En 1969, en Inglaterra se genera un documento secreto firmado por J. H. Ellis titulado “The possibility of secure non-secret digital encryption” (1), y siete años más tarde, en 1976 desde el otro lado del océano en Estados Unidos, se presentaba el trabajo de Whitlfield Diffie y Martin Hellman, el protocolo criptográfico Diffie-Hellman, un protocolo que puede utilizar canales inseguros y establecer claves entre partes que no han tenido contacto previo. Apenas un año más tarde se hizo público el sistema de clave pública generado en el Instituto Tecnológico de Massachusetts (MIT)

denominado RSA, ampliamente utilizado en firmas digitales. Los inventores de este mecanismo plantearon un texto cifrado a modo de acertijo que recién pudo ser resuelto casi veinte años después, con la ayuda de internet y computadoras potentes para esa época. El texto que pudieron descifrar tantos años después era simple y gracioso. Decía en inglés “Las palabras mágicas son Quebranta Huesos Sensible”. También en torno a este sistema de cifrado se lanzó en 1991 otra competición de factorización de números enteros, que preveía entregar sumas de dinero a quien cumpliera el desafío, incrementando la dificultad del mismo cada vez que resolvía un nivel de complejidad. Se comenzó por el RSA-100, y se completaron varios niveles del desafío, pero la mayoría aún permanecen sin ser descubiertos.

Otro de los grandes pasos fundacionales de blockchain es la responsabilidad del criptógrafo belga Jean Jacques Quisquater, que en mayo de 1999 publicó junto con Henry Massias y Xavier Serret Ávila un ensayo titulado "Design of a secure timestamping service with minimal trust requirements," como parte del proyecto TimeSec. En este documento presentan una propuesta para la marca de fecha y hora en los documentos digitales bajo la condición de tener los mínimos requerimientos de confianza, en un ambiente distribuido. Además de ser co-autor de este documento, Quisquater es inventor de un reconocido esquema criptográfico, el protocolo GQ, director de la Asociación Internacional de Investigación en Criptología, posee 17 patentes a su nombre, y múltiples reconocimientos y galardones. Xavier Serret Ávila también registra múltiples registros de patentes para la empresa “Intertrust Technologies Corporation”, donde vemos nuevamente colarse la palabra “confianza” (“trust”) en el eje de la escena.

En la historia fundacional también debemos mencionar a Ralph Merkle, uno de los creadores de los algoritmos de clave pública, también de gran importancia con su árbol de hash de Merkle, del cual hablaremos después más extensamente.

EL MANIFIESTO CRIPTO-ANARQUISTA

Además de los avances de la criptografía principalmente ligados a las guerras y luchas de poder entre los estados, en forma paralela a la caída del muro de Berlín y el fin de la guerra fría, encontramos un movimiento que en su espíritu representa la mayoría de las posibilidades que hoy blockchain pretende representar: el criptoanarquismo.

El criptoanarquismo surge en los noventa con las libertades individuales y la privacidad de los actos como estandartes, y la criptografía asimétrica como mecanismo para cumplirlo. Este movimiento se opone a la vigilancia de las redes informáticas por parte de los estados y evaden la censura, y se enmarca en un

movimiento más grande denominado cypherpunks o cyber-activismo. Inicialmente, este grupo de expertos en criptografía, programadores y científicos, divulgaba su filosofía y visión política mediante una lista de correo entre integrantes de una compañía con sede en la bahía de San Francisco. Comenzó con apenas tres integrantes y dos años después ya tenía más de 700 suscriptores.

Consideraban la posibilidad del anonimato y el uso de seudónimos como piezas claves para mantener una genuina libertad de expresión. Entre sus argumentos para defender el uso de seudónimos en vez de sus nombres reales, tomaban como ejemplo la publicación inicial de los ensayos que dieron cuerpo a la constitución de Estados Unidos. Estos escritos también habían sido inicialmente publicados bajo seudónimos.

Dentro de la producción que tuvo el grupo se cuentan proyectos de software, hardware de encriptación y hasta novelas de ficción como “Cryptonomicon”, de Neal Stephenson. Pero los documentos realmente fundacionales son el Manifiesto Cypherpunk y el Manifiesto Cripto-Anarquista. El primero fue escrito por Eric Hughes en 1993 y el segundo pertenece a Timothy C. May en 1992 y en sus líneas esboza alguna de las ideas del criptoanarquismo y sus efectos.

Vamos a resaltar algunos párrafos en forma textual traducidos al español, que tuvieron un gran poder predictivo de lo que hoy en día es capaz de lograr las criptomonedas y blockchain:

“Dos personas pueden intercambiar mensajes, hacer negocios y negociar contratos electrónicos, sin saber nunca el nombre auténtico, o la identidad legal, de la otra. 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 tratos que las calificaciones crediticias de hoy en día. Estos progresos alterarán completamente la naturaleza de la regulación del gobierno, la capacidad de gravar y de controlar las interacciones económicas, la capacidad de mantener la información secreta, e ***incluso alterarán la naturaleza de la confianza y de la reputación.****”*

(...)

“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 habilitadoras."

"El Estado intentará, por supuesto, retardar o detener la diseminación de esta tecnología, ***citando preocupaciones de seguridad nacional, el uso de esta tecnología por traficantes de drogas y evasores de impuestos*** *y miedos de desintegración social. Cualquiera de estas preocupaciones serán válidas; la cripto-anarquía 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 asesinatos y extorsiones****."*

Si quisieran leer los documentos completos en su idioma original, pueden hacerlo en las siguientes páginas web:

Manifiesto criptoanarquista:

https://www.activism.net/cypherpunk/crypto-anarchy.html

Manifiesto cypherpunk:

https://www.activism.net/cypherpunk/manifesto.html

CRISIS Y OPORTUNIDAD

Muchas veces, la crisis de unos es la oportunidad de otros. El año 2008 no fue la excepción, y mientras sucedía una de las peores crisis a nivel mundial, el Bitcoin se estaba gestando.

El 15 de septiembre de 2008 quiebra el banco estadounidense Lehman Brothers, el cuarto banco de inversión de Estados Unidos, que gestionaba para ese entonces más de 46.000 millones de dólares en hipotecas. Este hito fue una gran caída entre otras caídas, que habían comenzado casi dos años antes, como una crisis de confianza crediticia sobre las hipotecas "basura" (o también llamadas subprime). La desconfianza se extiende desde Estados Unidos a Europa, numerosos países entran en recesión, entre ellos Estados Unidos, Japón, Gran Bretaña, Alemania, España e Italia. Los países desarrollados son los más afectados con una contracción de la economía y repercute también en el plano social con millones de desempleados, aproximadamente 9 millones de empleos perdidos en 19 meses. Los mercados colapsan y las quiebras se suceden en diferentes países y en entidades que solían gozar con el mejor de los prestigios. Merrill Lynch, JPMorgan Chase, Citigroup y Goldman Sachs, BNP Paribas, HSBC, todas entidades financieras de gran importancia,

todas en serios problemas y con grandes recortes en sus actividades. La mayoría de las entidades tuvieron que recurrir a la ayuda estatal para sobrevivir.

Fue la peor crisis financiera desde la crisis de 1930 y como toda gran crisis previamente existen errores que luego propician que suceda. Se pasa desde una etapa en la que los bancos invierten en activos de alto riesgo pero con gran rentabilidad hasta que los inversionistas pretenden recuperar su dinero, sus expectativas se tornan negativas, el efecto se expande y la **pérdida de confianza** se contagia más rápido que el peor de los virus. Y el origen que desencadenó el problema fue tan simple como el que personas con pocos recursos pudieran comprar su vivienda mediante créditos hipotecarios. Y, obviamente, que finalmente esos créditos no se pudieran pagar. No solo esas personas se quedaron sin sus viviendas, sino que arrastró a una cantidad de gente desempleada a la calle tan grande como nadie hubiera imaginado. Tan simple y tan frágil era el sistema financiero (y lo sigue siendo), que cuando una ficha cayó, arrastró al resto sin contemplaciones.

Este contexto caótico, de crisis de confianza en los bancos y en todo el sistema financiero, fue el caldo de cultivo donde las ideas del criptoanarquismo (encarnadas ya en otra generación) tenían todas las posibilidades de crecer y esparcirse. Con una herramienta concreta -que respondía de una manera novedosa a la incertidumbre de unos, los defraudados por el sistema, y las ansias de libertad y anonimato de otros, los criptoanarquistas- aparece un personaje misterioso. En octubre de 2008, un tal "Satoshi Nakamoto", desde las penumbras, lanza el Bitcoin, una revolución en la concepción del dinero, que solo sería el comienzo de una historia aún más importante.

¿QUIÉN ES SATOSHI NAKAMOTO?

"I've moved on to other things. It's in good hands with Gavin and everyone."

"Pasé a otras cosas. Queda en buenas manos con Gavin y todos."

SATOSHI NAKAMOTO (REFIRIÉNDOSE AL DESARROLLO DEL BITCOIN)

Con estas palabras, Satoshi Nakamoto, creador del Bitcoin, empieza su último mail fechado el 23 de abril de 2011. Después de esto desaparece por completo, se desvanece sin haber dejado un solo rastro certero de quién es en realidad.

Hay mil especulaciones, la mayoría coincide que pudo haber sido un seudónimo, algunos creen que era un genio, otros creen que en realidad detrás de ese nombre se escondía un grupo de personas. Pero solo se le conoció por los mails que intercambió, y el código que generó, nada más. No se sabe su edad, ni su nacionalidad, ni nada personal.

Al más fiel estilo criptoanarquista, luego de ese último mail en el que deja su legado a otros integrantes del proyecto, se pierde en la más espesa de las penumbras. También lo podemos comparar con un superhéroe: contemplando su obra cumplida, simplemente vuelve a su refugio anónimo.

La cantidad de especulaciones alrededor de la figura de Satoshi son tantas que tendrían cuerpo para una novela, muy interesante, pero al menos por ahora, con un final lleno de dudas. Ya volveremos sobre el personaje detrás del Bitcoin, y los misterios que esconde, pero ahora veamos el porqué de la importancia de su creación.

Los primeros pasos del Bitcoin

El viernes 31 de octubre de 2008, Satoshi publicaba el whitepaper (libro blanco) en donde explica con detalles, en un lenguaje técnico, cómo funciona el Bitcoin. Al mismo tiempo que los titulares de la CNN hablan de derrumbes en las acciones y múltiples problemas financieros, una nueva moneda, esta vez virtual, se estaba gestando. Unos meses más tarde, en enero de 2009, el señor Satoshi, minaba el primer Bitcoin. En ese momento, podría haberse considerado a cada unidad de Bitcoin, como un juego, una abstracción. Durante 2009, el precio de un Bitcoin fue 0 dólares. Puede ser que Satoshi estuviera muy convencido del éxito de su moneda, pero eso no se trasladaba en ningún valor transable.