

## **BLOCKCHAIN** (cadena de bloques)

Las tecnologías disruptivas van acortando el tiempo de aceptación social, hasta ser completamente incorporadas en el quehacer diario.

1975 <i>Personal Computer</i> (lap PC).	Tiempo de aceptación:	16 a.
1983 Telefonía móvil.	Tiempo de aceptación:	13 a.
1990s Internet.	Tiempo de aceptación:	07 a.

Internet de las cosas:           “Revolución en las tareas”.  
 Promovida por exigencias profesionales  
 -Impulsada por telemedicina

Internet de las cosas (*Internet Of Things*, IoT) es el proceso que permite conectar los elementos físicos cotidianos a internet: desde los objetos domésticos comunes, como las bombillas de luz, hasta los recursos para la atención de la salud, como los dispositivos médicos; las prendas y los accesorios personales inteligentes; e incluso los sistemas de las ciudades inteligentes. Los dispositivos de IoT que se encuentran dentro de esos objetos físicos suelen pertenecer a una de estas dos categorías: son interruptores (es decir, envían las instrucciones a un objeto) o son sensores (recopilan los datos y los envían a otro lugar).

La primera idea de la telemedicina, tal y como la conocemos hoy en día, apareció en la edición de abril de 1924 de la revista *Radio News*. En ella, una ilustración futurista mostraba una máquina con televisión y micrófono que permitía a un paciente comunicarse con su médico. Sin embargo, los primeros usos de la telemedicina para transmitir vídeo, imágenes y datos médicos complejos se produjeron a finales de 1950 y principios de 1960. En 1959, la Universidad de Nebraska utilizó la telemedicina interactiva para transmitir exámenes neurológicos. Esta tecnología fue desarrollada originalmente para conectar a los pacientes que viven en zonas remotas con los médicos que trabajan en áreas urbanas. El crecimiento de la telemedicina desde mediados del siglo pasado es consecuencia de su desarrollo en el ámbito militar y de tecnología espacial. Fue por 1965 cuando empezaron a darse en EE UU los primeros casos de uso de la televisión para facilitar consultas médicas del ámbito de la salud mental entre especialistas de distintos centros. La expansión de internet a escala global desde mediados de los 90 del siglo pasado y los avances exponenciales en materia de digitalización y desarrollo de *big data*, en detrimento de las tecnologías analógicas, han sentado las bases de la versión más moderna de la telemedicina, se produce una auténtica revolución que incluye la educación del paciente, la transmisión de imágenes médicas, consultas de audio y vídeo en tiempo real, y las mediciones de signos vitales

Internet de la información:   “Revolución en el acceso y difusión de la información”.  
 -Promovida por los sectores militar y académico.  
 -Impulsada por Google, Facebook, Amazon.

**Internet** es un conjunto descentralizado de redes de comunicación interconectadas, que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen constituyen una red lógica única de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como *Advanced Research Projects Agency Network*: ARPANET, entre universidades en California (el primer nodo se estableció en UCLA, y fue la espina dorsal de internet hasta 1990) creada por encargo del Departamento de Defensa (DOD). A ARPANET se unieron la RAND Corporation (*Research And Development*) y el MIT (*Massachusetts Institute of Technology*), en EE UU, y el NPL (*National Physical Laboratory*) en el Reino Unido. La familia de protocolos de internet o pila de protocolos de Internet es un conjunto constituido por los protocolos de red clave que componen la arquitectura de internet y que permiten la comunicación efectiva y la transmisión de datos entre computadoras. En ocasiones se le denomina conjunto de protocolos TCP/IP, en referencia a los dos protocolos más importantes que la componen, que fueron de los primeros en definirse, y que son los dos más utilizados de la familia y ya señalados: protocolo de control de transmisión (*Transmission Control Protocol*, TCP) y protocolo de internet (*Internet Protocol*, IP).

2009 Internet del valor (cadena de bloques - *blockchain*): “Revolución en la transmisión y valor de los datos en internet”.

-Promovida por sector financiero.

-Impulsada por Bitcoin-2009 (Satoshi Nakamoto: pseudónimo usado por la persona o grupo que creó el protocolo Bitcoin, ), Ethereum-2014 (Vitalik Buterin, n. 1994).

(Bitcoin, «“B” mayúscula», se refiere al protocolo Bitcoin. bitcoin, «“b” minúscula», se refiere a la criptomoneda bitcoin).

---

*Blockchain*: base de datos distribuida y compartida entre diferentes participantes, protegida criptográficamente y organizada en bloques de transacciones. Es una base de datos descentralizada que no puede ser alterada.

*Blockchain*: pública -Bitcoin, Ethereum- (abiertas o sin permiso, descentralizadas, seudoanónimas), privada (cerradas o con permiso, distribuidas, anónimas) o híbrida

*Blockchain*: Los elementos:

Nodo (servidor) → sistema descentralizado

Protocolo estándar (Bitcoin, Ethereum -TCP/IP, HTTP, SMTP)

Red entre pares (P2P, *peer-to-peer*)

Token o criptomoneda: unidad de cuenta utilizada en las

*blockchains* públicas. Serie de dígitos o cadena

alfanumérica que representan un registro: bitcoin, ether.

Las claves:

Criptografía: codificación segura, inalterable, de las reglas del protocolo que rigen el sistema.

Cadena de bloques o *blockchain*: base de datos diseñada para el almacenamiento de los registros realizados.

Consenso: sustentado en un protocolo común.

*Blockchain: Historia.*

Desde la crisis financiera de 2008, el sector bancario experimentó dificultades para recuperar los niveles de rentabilidad pre-crisis. En la década de los 1990s, un grupo de personas, denominado *cypherpunks* aprovechó el potencial de internet para crear un sistema financiero abierto, sin entes centrales, que garantizara el anonimato, el control de la oferta monetaria y que fuera transparente. El resultado, espoleado por la crisis, llegó en 2008 con la creación de una criptomoneda: *bitcoin*. Ello encaró la descentralización en los pagos, sin necesidad de banco o de terceros para llevar a cabo las labores tradicionalmente desempeñadas por la banca. Fue, el primer caso, de uso de la tecnología *blockchain*, en 2009: Bitcoin. También, el inicio de un cambio radical en el ecosistema bancario, principalmente en la relación entre entidad y cliente.

Países líderes en tecnología de cadena de bloques:

Londres: referencia mundial en la gestión de servicios financieros (la *City*).

Zürich: CryptoValley.

New York, San Francisco: Wall Street, Silicon Valley.

Singapur: Centro de Innovación IBM de *blockchain*.

Movimientos filosóficos y sociales detrás del origen de la *blockchain* de Bitcoin:

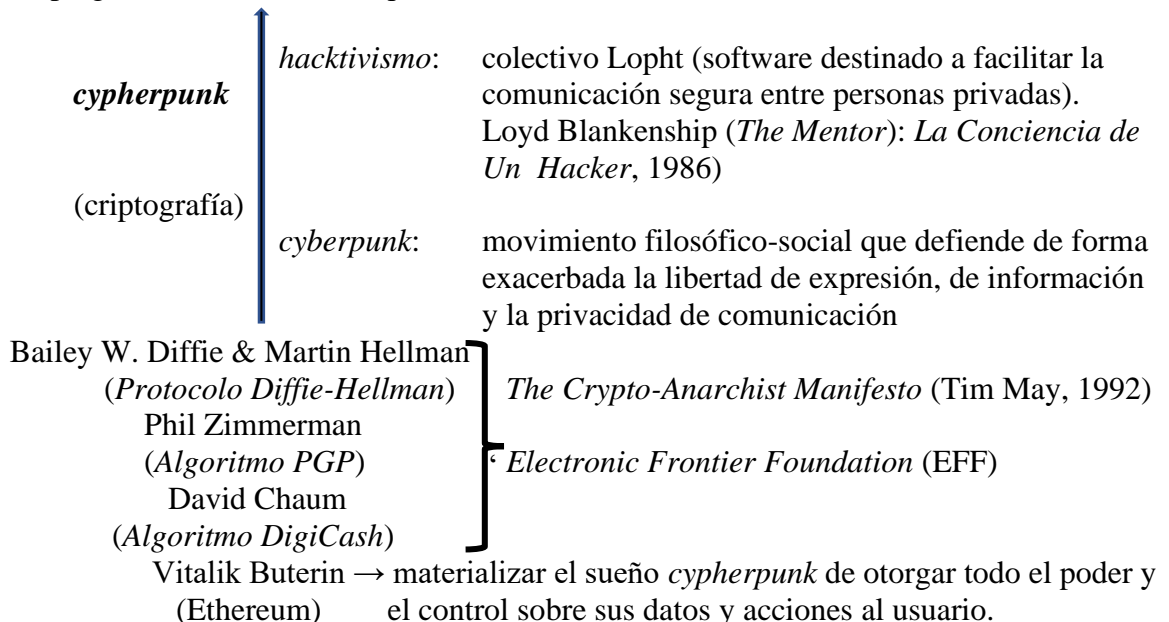
Hactivismo, cyberpunks, cypherpunks, libertarismo:

nueva forma de relación en internet.

reinterpretación de los conceptos: información, libertad, privacidad.

Steven Levy, *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*, 2001. Traducción de Dimitri Fdz. Bobrovski -*Cripto: cómo los informáticos libertarios vencieron al gobierno y salvaguardaron la intimidad en la era digital*- para Alianza Editorial, 2002.

Criptografía: NSA → acceso público



B.W. Diffie & M. Hellman = *Public Key Cryptography* = «https»

(David Kahn: *The Code-Breakers. The Comprehensive History of Secret Communication from Ancient Times to the Internet*, Simon & Schuster, 1997)

+ Ralph Merkle = *Merkle-Tree* = *blockchain* Bitcoin.

### **Impacto de la *blockchain* en las diferentes industrias:**

Banca: Abra, BitPesa, Circle. Aseguradoras. Telecomunicaciones y medios de comunicación. Energía. Industria 4.0 (cuarta revolución industrial). Farma y Salud. Pymes. Juego en-línea. ONG. Sector público.

### **Modelos de uso sectorial de la *blockchain*.**

Participación ciudadana y voto electrónico.

Ciudades inteligentes.

Música, imágenes, propiedad intelectual.

*Mediachain* (buscador de imágenes universal)

Identidad digital e internet descentralizado

*Blockstack*, creada Muneeb Ali & Ryan Shea (fin: desplazar a https).

Comercio electrónico

*OpenBazaar*-Obi (2016, entorno de confianza, frente a Amazon y/o Alibaba).

### **¿Cómo se compra o invierte en criptomonedas?**

. Cambio: a través de una casa de cambio o compra-venta.

. Intercambiando bienes y servicios: a cambio, se recibe un salario en criptomonedas.

. Minería: minando bloques en una *blockchain* basada en «prueba de trabajo» (*Proof of Work*, PoW). PoW es el protocolo de consenso más conocido y antiguo que consiste en que las partes de una red realicen con éxito un trabajo computacionalmente costoso para acceder a los recursos de dicha red. La principal característica de esta estrategia es su asimetría. El trabajo por parte del cliente es moderadamente difícil de realizar, pero la verificación por parte de la red es sencilla. Esto quiere decir, que la prueba de trabajo lleva mucho tiempo en producirse y es computacionalmente costosa. Pero verificarla es sencillo, pues la prueba diseña patrones que facilitan la verificación. Fue precisamente esta característica, la que llamó la atención de Satoshi Nakamoto a la hora de diseñar Bitcoin. Por eso se implementó el sistema *HashCash* (un sistema PoW propuesto por Adam Black, en 1997) en su reconocida criptomoneda. Usando el protocolo de *Proof of Work*, con cada nuevo bloque creado se deberá resolver un acertijo matemático que solo puede ser resuelto mediante prueba y error. Estos acertijos son resueltos por los *mineros*, haciendo millones de intentos (*hash* = picadillo), lo que conlleva el uso de una gran potencia de computación (minería) y el consecuente consumo de energía. Resolver el acertijo dará como resultado la creación del bloque, la confirmación de las transacciones involucradas en ese bloque y la generación de nuevos bitcoins que recibirá el *minero* como recompensa junto a las comisiones implícitas en cada una de las transacciones. El problema matemático consiste en encontrar los parámetros que den un determinado resultado. Lo especial de ese resultado es que es un *hash*, por lo que es imposible obtener los parámetros iniciales desde el hash, únicamente pueden ser generados mediante prueba y error.

*Initial Coin Offering* (ICO = Oferta Inicial de Moneda).

«salida a bolsa» de un protocolo descentralizado (la mayoría vinculados al protocolo Ethereum).

## **Manifiesto Hacker**

El 08/01/1986, Loyd Blankenship (n. 1965), *The Mentor*, después de haber sido detenido por crear el juego de rol *GURPS Cyberpunk*, escribió el «Manifiesto Hacker», publicado en la *ezone Phrack*. (*ezone*: revista digital *-online magazine*. *Phrack*: *ezone* escrita por y para los hackers, publicada por primera vez el 17/11/1985).

### ***The Conscience of a Hacker***

*« I am a hacker, enter my world...*

*Mine is a world that begins with school... I'm smarter than most of  
the other kids, this crap they teach us bores me...*

*Damn underachiever. They're all alike.*

*I'm in junior high or high school. I've listened to teachers explain  
for the fifteenth time how to reduce a fraction. I understand it. "No, Ms.  
Smith, I didn't show my work. I did it in my head..."*

*Damn kid. Probably copied it. They're all alike.*

*I made a discovery today. I found a computer. Wait a second, this is  
cool. It does what I want it to. If it makes a mistake, it's because I  
screwed it up. Not because it doesn't like me...*

*Or feels threatened by me...*

*Or thinks I'm a smart ass...*

*Or doesn't like teaching and shouldn't be here...*

*Damn kid. All he does is play games. They're all alike.*

*And then it happened... a door opened to a world... rushing through  
the phone line like heroin through an addict's veins, an electronic pulse is  
sent out, a refuge from the day-to-day incompetencies is sought... a board is found.*

*"This is it... this is where I belong..."*

*I know everyone here... even if I've never met them, never talked to  
them, may never hear from them again... I know you all...*

*Damn kid. Tying up the phone line again. They're all alike...*

*You bet your ass we're all alike... we've been spoon-fed baby food at  
school when we hungered for steak... the bits of meat that you did let slip  
through were pre-chewed and tasteless. We've been dominated by sadists, or  
ignored by the apathetic. The few that had something to teach found us will-  
ing pupils, but those few are like drops of water in the desert.*

*This is our world now... the world of the electron and the switch, the  
beauty of the baud. We make use of a service already existing without paying  
for what could be dirt-cheap if it wasn't run by profiteering gluttons, and*

*you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.*

*Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.*

*I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike ».*

### ***La Conciencia de un Hacker***

« Uno más ha sido capturado hoy. Está en todos los periódicos.  
 “Joven arrestado en Escándalo de Crimen por Computadora”,  
 “Hacker arrestado luego de traspasar las barreras de seguridad de un banco ...”  
 Malditos muchachos. Todos son iguales.  
 Pero tú, en tu sicología de tres partes y tu tecno-cerebro de 1950,  
 has alguna vez observado detrás de los ojos de un Hacker?  
 Alguna vez te has preguntado qué lo mueve, qué fuerzas lo han formado,  
 cuáles lo pudieron haber moldeado?  
 Soy un Hacker, entra a mi mundo ...  
 El mío es un mundo que comienza en la escuela ...  
 Soy más inteligente que la mayoría de los otros muchachos,  
 esa basura que ellos nos enseñan me aburre ...  
 Malditos sub-realizados. Son todos iguales.  
 Estoy en la preparatoria.  
 He escuchado a los profesores explicar por decimoquinta vez como reducir una fracción.  
 Yo lo entiendo.  
 “No, Srta. Smith, no le voy a mostrar mi trabajo, lo hice en mi mente ...”  
 Maldito muchacho. Probablemente se lo copió. Todos son iguales.  
 Hoy hice un descubrimiento. Encontré una computadora.  
 Espera un momento, esto es lo máximo. Esto hace lo que yo le pida.  
 Si comete un error es porque yo me equivoqué.  
 No porque no le gusto ...  
 O se siente amenazada por mi ...  
 O piensa que soy un engreído ...  
 O no le gusta enseñar y no debería estar aquí ...  
 Maldito muchacho. Todo lo que hace es jugar. Todos son iguales.  
 Y entonces ocurrió ... una puerta abierta al mundo ...  
 Corriendo a través de las líneas telefónicas  
 como la heroína a través de las venas de un adicto,

se envía un pulso electrónico,  
 un refugio para las incompetencias del día a día es buscado ...  
 una tabla de salvación es encontrada.  
 “Este es ... este es el lugar a donde pertenezco ...”  
 Los conozco a todos aquí ...  
 aunque nunca los hubiera conocido, o hablado con ellos,  
 o nunca vuelva a escuchar de ellos otra vez ...  
 Los conozco a todos ... Malditos muchachos.  
 Enlazando las líneas telefónicas otra vez. Todos son iguales ...  
 Apuesta lo que sea a que todos somos iguales ...  
 A nosotros nos han estado dando comida para bebés con cuchara en la escuela,  
 cuando estábamos hambrientos de carne ...  
 Las migajas de carne que ustedes dejaron escapar estaban masticadas y sin sabor.  
 Nosotros hemos sido dominados por sádicos, o ignorados por los apáticos.  
 Los pocos que tienen algo que enseñarnos encontraron alumnos complacientes,  
 pero esos pocos son como gotas de agua en el desierto.  
 Ahora este es nuestro mundo ...  
 El mundo del electrón y el conmutador, la belleza del budio.  
 Nosotros hacemos uso de un servicio que ya existe sin pagar  
 por lo que podría ser barato como el polvo,  
 si no estuviera en manos de glotones hambrientos de ganancias,  
 y ustedes nos llaman criminales.  
 Nosotros exploramos ...  
 y ustedes nos llaman criminales.  
 Nosotros buscamos detrás del conocimiento ...  
 y ustedes nos llaman criminales.  
 Nosotros existimos sin color, sin nacionalidad, sin prejuicios religiosos ...  
 y ustedes nos llaman criminales.  
 Ustedes construyeron bombas atómicas,  
 ustedes hicieron la guerra,  
 ustedes asesinaron, engañaron y nos mintieron  
 y trataron de hacernos creer que era por nuestro bien,  
 ahora nosotros somos los criminales.  
 Si, soy un criminal. Mi crimen es la curiosidad.  
 Mi crimen es el juzgar a las personas por lo que dicen y piensan,  
 no por lo que aparentan.  
 Mi crimen es ser más inteligente, algo por lo cual nunca me olvidarás.  
 Soy un Hacker, este es mi manifiesto.  
 Tu podrás detener este esfuerzo individual, pero nunca podrás detenernos a todos ...  
 después de todo, todos somos iguales ».

---

## **El Manifiesto Cripto Anarquista**

Timothy C. May (1951-2018). Ingeniero en electrónica y escritor de política que tuvo una gran influencia filosófica en Bitcoin. Como fundador del movimiento cripto-anarquista, creó la lista de correos de los *cypherpunks*, donde Satoshi Nakamoto discutiría la creación de una moneda criptográfica capaz de sustituir el dinero corriente.

*« Cypherpunks of the World, several of you at the "physical Cypherpunks" gathering yesterday in Silicon Valley requested that more of the material passed out in meetings be available electronically to the entire readership of the Cypherpunks list, spooks, eavesdroppers, and all. Here's the "Crypto Anarchist Manifesto" I read at the September 1992 founding meeting. It dates back to mid-1988 and was distributed to some like-minded technoanarchists at the "Crypto '88" conference and then again at the "Hackers Conference" that year. I later gave talks at Hackers on this in 1989 and 1990. There are a few things I'd change, but for historical reasons I'll just leave it as is. Some of the terms may be unfamiliar to you...I hope the Crypto Glossary I just distributed will help. (This should explain all those cryptic terms in my signature!) --Tim May ».*

### ***The Crypto Anarchists Manifesto***

*« A specter is haunting the modern world, the specter of crypto anarchy.*

*Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re-routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.*

*The technology for this revolution--and it surely will be both a social and economic revolution--has existed in theory for the past decade. The methods are based upon public-key encryption, zero-knowledge interactive proof systems, and various software protocols for interaction, authentication, and verification. The focus has until now been on academic conferences in Europe and the U.S., conferences monitored closely by the National Security Agency. But only recently have computer networks and personal computers attained sufficient speed to make the ideas practically realizable. And the next ten years will bring enough additional speed to make the ideas economically feasible and essentially unstoppable. High-speed networks, ISDN, tamper-proof boxes, smart cards, satellites, Ku-band transmitters, multi-MIPS personal computers, and encryption chips now under development will be some of the enabling technologies.*

*The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy.*



*Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. And just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which dismantle the barbed wire around intellectual property.*

*Arise, you have nothing to lose but your barbed wire fences! ».*

---

« *Ciferpunks* del mundo. Varios de ustedes en la reunión “física de ciferpunks” de ayer en Silicon Valley pidieron que gran parte del material aprobado en las reuniones sea accesible electrónicamente a los lectores de toda la lista de ciferpunks, espías, intrusos y demás. Aquí está el “Manifiesto Cripto Anarquista” que leí en septiembre de 1992 en la reunión de la fundación. Sus orígenes se remontan a mediados de 1988 y se distribuyó a algunos tecno-anarquistas afines en la conferencia “Crypto ’88” y de nuevo en la “Hackers Conference” de ese año. Posteriormente di charlas en Hackers sobre esto en 1989 y 1990. Hay algunas cosas que me gustaría cambiar, pero por razones históricas voy a dejarlo como está. Algunos de los términos pueden ser desconocidos para ustedes...espero que el Cripto Glosario que acabo de distribuir sea de ayuda. (¡Esto debe explicar todos los términos crípticos en mi materia!). –Tim May ».

### **El manifiesto cripto-anarquista**

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

La informática está al borde de proporcionar la capacidad a individuos y grupos de comunicarse e interactuar entre ellos de forma totalmente anónima. 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.

La tecnología para esta revolución (y seguramente será una revolución social y económica) ha existido en teoría 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 en Europa y EE.UU., conferencias monitorizadas de cerca por la Agencia de Seguridad Nacional. Pero solo recientemente las redes de computadores y ordenadores 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 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 será válida; 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. Varios elementos criminales y extranjeros serán usuarios activos de la CryptoNet. Pero esto no detendrá la extensión de la cripto-anarquía. 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 púas 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 púas alrededor de la propiedad intelectual.

¡Álzate, no tienes nada que perder excepto tus vallas de alambres de espino! ».

---