

Valerio Dalla Costa

# Pueblo *Bitcoin*

**EL AMANECER DE UNA  
NUEVA SOCIEDAD**

basada en una **moneda sana y honesta**

Derechos de autor © 2022 Valerio Dalla Costa

Todos los derechos reservados.

Este libro o parte del mismo no puede ser reproducido o utilizado de ninguna manera sin la autorización expresa por escrito del editor, excepto para el uso de breves citas en reseñas.

Autor: Valerio Dalla Costa  
[www.pueblobitcoin.com](http://www.pueblobitcoin.com)  
[info@pueblobitcoin.com](mailto:info@pueblobitcoin.com)



Revisión: Giacomo Zucco

Portada: Matteo Ducoli

Código ISBN: 9798883900548

## **A Roberto**

Papá, aunque en realidad nunca hayas sido un gran lector, le darás una ojeada al libro desde allá arriba... ¿verdad?



# ÍNDICE

<b>PREFACIO - CÓMO NACE LA MAGIA</b>	<b>9</b>
<b>INTRODUCCIÓN</b>	<b>13</b>
<b>PARTE 1 UN VISTAZO AL PASADO</b>	<b>21</b>
<b>Capítulo 1 - LA MONEDA EN LA HISTORIA</b>	<b>23</b>
Las primeras formas de dinero	26
Los metales preciosos	31
La moneda representativa	34
La moneda fiat	40
Un posible plan ₿	47
<b>Capítulo 2 - LA LLEGADA DE BITCOIN</b>	<b>49</b>
Los orígenes: ¿por qué?	51
Los orígenes: ¿cómo?	63
Los orígenes: ¿quién?	68
Los orígenes: ¿qué?	71
Los orígenes: ¿cuándo?	75
El nacimiento de bitcoin	80
Historias de revolución ordinaria	88

<b>PARTE 2 EN EL CORAZÓN DEL ORO DIGITAL</b>	<b>103</b>
<b>Capítulo 3 - EL PROTOCOLO BITCOIN</b>	<b>105</b>
¿Cómo funciona el oro digital?	111
Las transacciones paso a paso	114
Características de la blockchain	140
Todo es cuestión de incentivos	147
La estructura de una transacción	151
<b>Capítulo 4 - LA BILLETERA</b>	<b>157</b>
El concepto de llavero	159
Tipos de billeteras	173
Buenas prácticas de seguridad y privacidad	184
<b>Capítulo 5 - LIGHTNING NETWORK</b>	<b>193</b>
El problema de la escalabilidad	194
Principios de funcionamiento	204
Bitcoin y lightning network	213
<b>PARTE 3 PENSAMIENTOS DESDE EL PUEBLO</b>	<b>221</b>
<b>Capítulo 6 - LA MEJOR MONEDA DE LA HISTORIA</b>	<b>223</b>
Propiedades de una buena moneda	225
El poder de los efectos de la red	241
Revolución sin líder	246
<b>Capítulo 7 - CÓMO OCURREN LOS CAMBIOS</b>	<b>251</b>
Modelos invertidos	252
La revolución bitcoin	260
La relación con empresas e instituciones	264
Tempos de adopción	271

<b>Capítulo 8 -¿CUÁNTO VALE BITCOIN?</b>	<b>287</b>
Oferta y demanda	289
En busca de la escasez	293
El valor del oro digital	296
<b>Capítulo 9 - PRINCIPIO DE NO AGRESIÓN</b>	<b>307</b>
Tecnología opt-in	308
Una moneda ética e inclusiva	309
El mejor voto contra las guerras	314
El dinero y la preferencia temporal	323
Privacidad y libertad	331
<b>Capítulo 10 - PREGUNTAS Y RESPUESTAS</b>	<b>343</b>
1-¿Los delincuentes utilizan bitcoin?	344
2-¿Realmente consume mucha energía y es un peligro para el medio ambiente?	348
3-¿Quién está detrás de bitcoin?	360
4-¿Cómo encaja en el sistema fiscal?	365
5-¿Por qué debería informarme sobre bitcoin?	375
<b>CONCLUSIONES</b>	<b>379</b>
<b>AGRADECIMIENTOS</b>	<b>383</b>
<b>BIBLIOGRAFIA</b>	<b>385</b>
<b>INFORMACIÓN SOBRE EL AUTOR</b>	<b>391</b>



# PREFACIO

## CÓMO NACE LA MAGIA

29 de marzo de 2014.

Recuerdo perfectamente la primera vez en mi vida que oí hablar de Bitcoin. Me encontraba en una cabaña que había alquilado para un fin de semana en medio del bosque en Valle Camonica, en la provincia de Brescia. Conmigo estaban muchos amigos que habían sido invitados para celebrar mi recién obtenida licenciatura conseguida pocos días antes. Entre barbacoas, aperitivos, música y charlas, de repente, escuché por primera vez la palabra *Bitcoin* de boca de un amigo y eso despertó en mí un gran interés. Bitcoin... ¿*Bitcoin*? Bitcoin. ¿Una moneda nativa de Internet desvinculada del actual sistema económico y financiero y capaz de funcionar sola? ¡Suena bien! *Bitcoin...*

Desde hacía mucho tiempo, había sido muy crítico con el modo en el que funciona el sistema del euro y en general de las monedas *fiat*, gestionadas en monopolio por los bancos centrales y con curso legal. Eran temas sobre los que me había informado, por mera curiosidad, en años anteriores. Pero ¿existía una nueva moneda electrónica a nivel global con el potencial de proteger de la inflación a las personas que ahorran y además preservar su privacidad? ¿Una moneda descentralizada y basada en una red que no requiere confianza en un intermediario? La idea sin duda era estimulante; sin embargo, en ese momento no profundicé más, también porque en ese entonces prácticamente no había nada en términos de información, sobre todo en Italia.

Pasaron sólo unos meses cuando encontré en la red el vídeo de un empresario que, en unos quince minutos, presentó a grandes rasgos el fenómeno Bitcoin y para mí fue amor a primera vista.

«¿Pero esto realmente puede funcionar?», pensé. La incredulidad del caso junto a una buena dosis de escepticismo inicial fueron rápidamente reemplazadas por mucho, muchísimo, asombro, dando inicio a un loco y desesperado período de estudio (por decirlo de alguna manera) para buscar fuentes, textos, *blogs* y sitios de todo tipo, todo aquello que pudiera aportarme más detalles e información sobre el tema era muy valioso para satisfacer mi curiosidad. En ese momento, no había muchos sitios italianos, había algunos bien hechos (a los que les agradeceré siempre), otros menos útiles o incompletos, e incluso algunos engañosos. Mi búsqueda me llevó a informarme también y, sobre todo, a través de blogueros y sitios web extranjeros de todo el mundo.

Rápidamente aprendí cómo descargar mi primera *billettera* electrónica y cómo registrarme en un *intercambio* para tratar de comprar algunas monedas. En poco tiempo, comprendí cuál era la mejor manera de comprar y administrar mis primeros bitcoins, un proceso que sigue vigente en un mundo en constante evolución, y tan complejo como fascinante.

Pero sobre todo recuerdo, como si fuera ayer, la sorpresa y la emoción que sentí al verlos acreditados en mi primera billettera personal. De hecho, estas sensaciones aún siguen presentes hoy en día cada vez que recibo o envío fondos en bitcoins. Sí porque, entonces como hoy, considero este fenómeno mucho más grande que un simple protocolo informático, una red o una moneda electrónica (debes saber que Bitcoin es las tres cosas al mismo tiempo).

Bitcoin es una herramienta que te da una libertad formidable e inesperada. Es un nuevo paradigma completamente independiente y desvinculado del actual sistema económico, financiero, social y político. Es una especie de universo paralelo y autónomo que muestra posible un nuevo estilo de vida. Se trata de unas nuevas gafas con las que puedes observar, desde un punto de vista inédito, la realidad que vivimos, la sociedad, las dinámicas laborales y las relaciones entre las personas, todo.

Bitcoin abarca todos los aspectos de nuestra vida y nos obliga a cuestionar todo lo que hoy nos parece obvio y que damos por sentado, comenzando por el concepto de moneda, privacidad, libertad individual, importancia y gestión de nuestro tiempo, ahorros y trabajo. De nuestra propia vida.

Bitcoin ha abierto una caja de Pandora, ha hecho posible infinitas oportunidades y ha incentivado la creatividad, proyectos e ideas sin fin.

Con el descubrimiento de Bitcoin, de repente, todo lo demás pasó a tener poco o ningún interés.

Después de años de estudio e investigación –y muchos más por venir– he encontrado una sola palabra capaz de sintetizar y describir, al menos para mí, lo que Bitcoin representa:

*felicidad.*

Te deseo una buena lectura.



# INTRODUCCIÓN

Entender Bitcoin es extremadamente difícil, de hecho, todas las novedades nunca son inicialmente fáciles de comprender y asimilar y, en cierto sentido, con esta tecnología, este aspecto se acentúa aún más.

En primer lugar, por primera vez se intersecan ámbitos que hasta ahora habían permanecido sustancialmente sin relación e independientes entre sí. Hasta la invención de Bitcoin, estos temas eran como compartimentos estancos, aislados, independientes y competencia de especialistas en el campo, pero este nuevo sistema los ha cruzado y unido dando vida a un protocolo informático descentralizado que implementa una moneda electrónica.

Básicamente, hay cuatro áreas principales que Bitcoin une: la criptografía, el estudio de sistemas informáticos distribuidos (redes de ordenadores), la teoría de juegos y las teorías monetarias y económicas. Describámoslas brevemente para enmarcar mejor de qué estamos hablando.

- **Criptografía**

Como indica su nombre, (del griego *kryptós* «oculto» y *graphía* «escritura»), esta es una disciplina que tiene como objetivo ocultar el contenido de un mensaje. Se trata de un conjunto de técnicas que permiten transmitir un mensaje, pero manteniéndolo en secreto para todos excepto para las personas que tienen las claves para descifrarlo.

La criptografía se refiere a una disciplina antigua que ya había sido usada entre los griegos y los romanos, como lo demuestra, por ejemplo, Suetonio alrededor del 120 d. C. en su obra *De Vita Caesarum*. El historiador cuenta que Julio César solía utilizar códigos de cifrado para transmitir sus comunicaciones y mantener la confidencialidad con sus mensajeros. Se trataba de combinar las letras del alfabeto y sustituirlas por otras letras siguiendo una lógica precisa, de esta manera, el texto del mensaje resultaba completamente incomprensible a

los ojos de quien quería interpretarlo, pero no para el destinatario que conocía la clave para descifrar el contenido, así era posible mantener la confidencialidad de la información.

Este ejemplo, por supuesto, se trata de una técnica criptográfica primitiva y fácilmente descifrable, pero ya contenía los dos elementos fundamentales de un código de cifrado:

- el *algoritmo*, es decir, la regla con la que se modifica el mensaje original haciéndolo encriptado (o cifrado);
- la *clave*, es decir, el parámetro que permite descodificar (o descifrar) el mensaje.

Con el desarrollo de la informática y los procesadores de cálculo, la criptografía ha experimentado grandes avances, especialmente en el ámbito de la seguridad informática y en todos los casos en los que se requiere mantener la confidencialidad de los datos. Por ejemplo, hoy en día lo encontramos en los mensajes y archivos en soportes de almacenamiento, en los procedimientos de inicio de sesión para acceder a un sitio web o a una plataforma (para cifrar la contraseña del usuario), en las transacciones financieras bancarias (home banking) o en las comunicaciones inalámbricas (Wi-Fi y redes celulares).

Bitcoin utiliza un tipo de criptografía asimétrica, también llamada criptografía *de clave pública*, que utiliza contraseñas diferentes para cifrar y descifrar un mensaje. Hay una clave para cifrar (la clave pública que cualquiera puede ver) y una para descifrar (la clave privada que sólo conoce el destinatario) sin necesidad de intercambiar esta frase entre remitente y destinatario.

En realidad, veremos que Bitcoin no utiliza esta tecnología para cifrar, sino para firmar y verificar firmas utilizándola al revés: la clave privada que posee el remitente se utiliza para firmar el mensaje, mientras que la clave pública se utiliza para verificar las firmas.

La criptografía es una disciplina realmente fascinante y aún está en continua evolución. El término «criptomoneda» debería hacer referencia precisamente al hecho de que la moneda Bitcoin se basa en algunas criptográficas primitivas.

- **Estudio de sistemas informáticos distribuidos**

Cuando en informática se habla de *redes de ordenadores* se refiere al conjunto de redes de telecomunicaciones caracterizado por un conjunto de dispositivos *hardware*, en pocas palabras, sistemas informáticos distribuidos.

Con la llegada de la Internet global, la World Wide Web rápidamente se convirtió en el tipo dominante de red de ordenadores, permitiéndole a personas de todo el mundo utilizarla para comercio electrónico, aplicaciones interactivas, plataformas informáticas, telefonía, correo electrónico y mucho más. Como resultado de esto, el estudio de las redes de ordenadores ahora es prácticamente lo mismo que estudiar el Internet y sus aplicaciones, de hecho, ha reemplazado protocolos y arquitecturas informáticas que ya no son relevantes. Para apreciar algunas dinámicas de Bitcoin, como moneda digital nativa de Internet, se requiere de algo de conocimiento básico en este campo.

- **Teoría de juegos**

Los orígenes de la teoría de juegos se remontan al lejano 1654 y a Blaise Pascal y Pierre de Fermat con su análisis sobre el cálculo de probabilidades en los juegos de azar. La teoría en su forma actual se le atribuye a John von Neumann y Oskar Morgenstern con la publicación, en 1944, de *Theory of games and economic behavior*, así como a los aportes de destacados académicos como John Nash, premio nobel de Economía por sus investigaciones en este campo y al cual se le dedicó la exitosa película *Una mente brillante*.

La teoría de juegos se refiere a un método matemático que permite estudiar el comportamiento humano en situaciones de interacción estratégica orientada al beneficio de cada individuo. Es una disciplina que analiza la interacción entre individuos y su proceso de toma de decisiones en un contexto específico, mediante una representación matemática de los comportamientos humanos en circunstancias especiales en las que ciertos incentivos y condiciones pueden llevar a resultados predecibles por parte de los jugadores. Dentro de un juego típicamente podemos encontrar tres elementos fundamentales:

- **Jugadores:** son aquellas personas que toman las decisiones, básicamente, se refiere a los participantes.
- **Estrategias:** son las acciones que los jugadores están autorizados a realizar, teniendo en cuenta todas las posibles elecciones que pueden realizar los otros participantes.
- **Resultados:** son el producto de las estrategias elegidas por los diferentes jugadores. Los resultados pueden preverse sobre bases matemáticas siguiendo una lógica de mecanismos de incentivos.

Una de las aplicaciones más famosas de la teoría de juegos es el llamado *dilema del prisionero*, según estos resultados matemáticos y racionales que surgen en los desenlaces a veces pueden ser contraintuitivos.

Sin embargo, esta disciplina no se aplica sólo a conceptos abstractos, por ejemplo, la teoría de juegos les permite a las grandes empresas tomar decisiones estratégicas y económicas basadas en posibles acciones de los competidores del mercado. También puede describir muy bien la llamada «carrera armamentística» de los años 50 por parte de los Estados Unidos y la URSS durante la Guerra Fría. En este caso, los jugadores serían las potencias económicas mundiales y las estrategias serían las opciones de «armarse» o «desarmarse». La teoría de juegos explica fácilmente cómo, para ambas naciones, recurrir a los armamentos era la estrategia dominante, aunque el resultado final no era óptimo para ninguno de los dos participantes.

Para las dinámicas de Bitcoin, la teoría de juegos desempeña un papel vital. Constituye una de las razones por las que el sistema puede sostenerse y desarrollarse de manera descentralizada, sin la presencia de un coordinador central. Esto se logra a través de un mecanismo de incentivos capaz de mantener la red segura y sostenible, en la que, por un lado, se premian a los actores honestos, y por otro, se hace cada vez más difícil y económicamente inconveniente el comportamiento deshonesto dirigido a dañar el propio sistema.

- **Teorías monetarias y económicas**

Bitcoin es una moneda electrónica, por lo tanto, es imprescindible tener, al menos, un conocimiento básico de los principios del funcionamiento de la economía y las finanzas. Con el fin de comprender la magnitud de esta tecnología, es indispensable conocer las principales teorías pasadas y presentes y tener una idea general del funcionamiento del actual sistema bancario y crediticio. De todos modos, se trata de temas muy complejos de los cuales la literatura es inmensa y donde las teorías económicas dominantes son muy amplias y a menudo discordantes.

En particular, es imprescindible comprender qué es realmente el dinero y entender el papel central que tiene, y siempre ha tenido, este instrumento, en las civilizaciones de todas las épocas. Tema aún hoy profundamente desconocido y subestimado, pero que Bitcoin finalmente ha obligado a cuestionar, demostrando cómo la forma de dinero adoptada constituye, de hecho, los fundamentos sobre los que se apoya cualquier sociedad.

- 1. Criptografía**
- 2. Estudio de sistemas informáticos distribuidos**
- 3. Teoría de juegos**
- 4. Teorías monetarias y económicas**

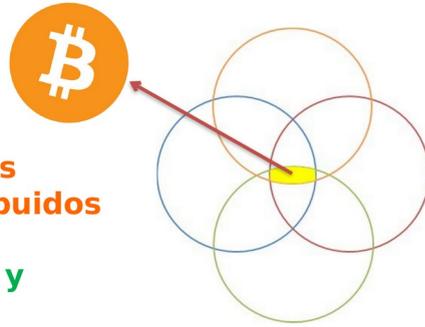


Figura 1. El Bitcoin se encuentra en la intersección de cuatro principales áreas temáticas.

Podríamos decir que estas cuatro áreas representan la estructura de esta tecnología. Probablemente, por esto Bitcoin sea difícil de entender y también de interpretar, pues muy pocas personas en el mundo pueden presumir de tener conocimientos y habilidades profundas en cada una de estas cuatro áreas. La mayoría de las personas pueden ser expertas y especialistas en uno de estos temas, incluso quizá de dos. Sin embargo, dado que los expertos sectoriales conocen muy poco sobre otras áreas, a menudo, no pueden comprender completamente la magnitud del fenómeno que están observando, ya que su perspectiva está limitada a un punto de vista restringido.

Para dar algunos ejemplos, existen grandes expertos y líderes mundiales en economía y política que; sin embargo, saben poco o nada de criptografía y de redes distribuidas de información. Por lo tanto, muchos tienen dificultades para comprender la esencia de Bitcoin y entender a cabalidad su funcionamiento descentralizado y las reglas estrictas de su protocolo informático. La mayoría de los programadores, aunque sean expertos en la escritura de software, generalmente suelen mostrar tener poca o ninguna conciencia de las teorías económicas y monetarias. Aunque interpretan correctamente la parte tecnológica de Bitcoin, a menudo, no pueden apreciar su enorme potencial desde un punto de vista social, político y filosófico.

En resumen, para comprender al menos la esencia de lo que está sucediendo en estos años, es necesario tener una visión general esforzándose por considerar simultáneamente todos los diferentes ámbitos en juego. Sólo de esta manera parece realmente posible comprender las novedades, apreciar el valor de esta tecnología revolucionaria e intuir sus enormes potencialidades.

Dada la infinita cantidad de información necesaria y la complejidad de todos los temas que Bitcoin aborda (prácticamente todos los relacionados con nuestra esfera privada y social), es muy difícil resumir todo en unas pocas líneas

de un texto divulgativo, de hecho, para ser sinceros, parece imposible. El tema es completamente nuevo, muy complejo, demasiado amplio e infinitamente extenso, es un pozo sin fondo, una especie de vórtice del cual, una vez que se entra, ya no es posible salir. Cuanto más nos informamos, más nos damos cuenta de cuán poco sabemos y todo lo que aún deberíamos conocer.

## PROPÓSITO

El descubrimiento de Bitcoin representa el comienzo de un verdadero camino de formación individual. Para muchos, Bitcoin se descubre poco a poco: al principio, tal vez se enmarque bajo una mala óptica o se toma poco en serio, viéndolo como un pasatiempo, un juguete para especuladores. Luego, lentamente, se intuye que hay algo mucho más profundo que se esconde allí, silencioso detrás de esta innovación.

En cualquier caso, este camino de formación debe comenzar en algún lugar y la idea de este libro nace precisamente con esta perspectiva: tratar de ofrecer a los lectores una introducción general al universo Bitcoin, buscando ayudar a las personas a comprender esta tecnología destinada a revolucionar nuestra sociedad.

En estos años de estudio la herramienta más importante que ha contribuido a la formación del autor ha sido, sin duda, la lectura de libros. De hecho, leer obliga a detenerse y a tomarse el tiempo necesario para reflexionar, obliga a ser activo en relación con las líneas que se encuentran frente a nuestros ojos, fuerza al lector a poner en marcha razonamientos, plantear nuevas dudas, imaginar nuevas soluciones y desarrollar un sano pensamiento crítico. Eso es exactamente lo que se necesita para comprender plenamente esta nueva tecnología.

Este texto divulgativo nace con el objetivo de proporcionar una visión general, pero lo más completa posible de esta fascinante innovación, con la intención de abarcar todos los principales aspectos que toca Bitcoin e intentando proporcionar un panorama general lo más lógico y coherente posible desde el cual comenzar tu propio camino formativo individual, con la esperanza de despertar el interés y el debate sobre el cambio histórico al que hemos estado asistiendo desde hace años.

Especialmente en el momento en que nació la idea de un *Villaggio Bitcoin*, una oficina/tienda física situada en los valles de Brescia y Bérgamo donde las personas puedan acercarse y «tocar con sus propias manos» una revolución aún ampliamente subestimada. El propósito de un punto físico centrado en una moneda digital como bitcoin es reunirse y compartir, con todas las personas interesadas, el asombro y la maravilla continua que esta

tecnología, destinada a cambiar profundamente nuestra vida, irradia todos los días.

## **ESTRUCTURA, DESTINATARIOS Y REQUISITOS**

La estructura del libro está dividida en tres partes distintas: una parte narrativa, una parte técnica y otra parte de análisis/reflexión, pensadas para sean lo suficientemente independientes entre sí. Esto significa que también podrían considerarse por separado, sin que eso afecte demasiado la comprensión general del texto.

### **PARTE 1. *UN VISTAZO AL PASADO***

En la primera parte, predominantemente narrativa, se recorre el papel que la moneda ha desempeñado en la historia del hombre hasta el actual sistema de la moneda *fiat*. Luego se cuenta y describe cómo se originó la tecnología Bitcoin: desde las motivaciones, los primeros experimentos, las problemáticas tecnológicas que se han debido enfrentar, el lanzamiento de la red y los primeros años de su desarrollo, una especie de crónica histórica con hechos, personajes y eventos que han llevado al nacimiento del fenómeno que conocemos hoy.

### **PARTE 2. *EN EL CORAZÓN DEL ORO DIGITAL***

En la segunda parte, más propiamente técnica, se explora el funcionamiento general del ecosistema Bitcoin ilustrando las tecnologías subyacentes. Se abordan las dinámicas de la blockchain, del algoritmo de la proof-of-work, de la importancia de la actividad de minería, ilustrando cómo pueden ocurrir las transacciones dentro de un sistema descentralizado y desintermediado, sin que los participantes de la red deban proporcionar datos sensibles o depositar su confianza en una entidad central.

Luego, se aborda el concepto de la billetera de bitcoin, fundamental para que los usuarios puedan conservar y gestionar sus propios fondos con plena autonomía. Para concluir, se presentan algunas dinámicas futuras y posibles desarrollos tecnológicos en los que se está enfocando el desarrollo en estos años. Entre estos se encuentran el protocolo Lightning Network, pensado para resolver el antiguo problema de la escalabilidad y para optimizar los intercambios en la vida cotidiana.

### **PARTE 3. *PENSAMIENTOS DEL PUEBLO***

En la última parte, más de análisis y reflexión, se consideran algunos aspectos de esta tecnología que se considera pueden tener impactos decisivos en la evolución de nuestra sociedad. Esto se hace a partir del análisis de las características de una buena moneda, pasando por considerar cómo la gente percibe estos grandes cambios, deteniéndose en el concepto de valor y en las dinámicas relacionadas con el precio de Bitcoin a lo largo del tiempo.

A continuación, se presentan reflexiones sobre las consecuencias de adoptar esta tecnología en el ámbito de las relaciones sociales y en los comportamientos individuales, así como sobre temas cada vez más relevantes como la privacidad, la protección del medio ambiente, las guerras o el tema fiscal. Por último, se intenta responder a algunas preguntas típicas que una persona puede plantearse cuando se enfrenta a situaciones nuevas e inéditas.

Todo está orientado a describir e imaginar los impactos sociales, políticos y filosóficos que Bitcoin está generando en todos los ámbitos de nuestra sociedad.

El enfoque es principalmente divulgativo, pensado tanto para personas que se acercan por primera vez a este nuevo mundo y buscan un punto de partida para informarse, como para aquellos interesados en profundizar y explorar el tema Bitcoin en sus múltiples facetas.

En la bibliografía se mencionan algunos de los textos, fuentes y material informativo que se consideran relevantes y significativos para profundizar en todos los ámbitos tratados o sólo mencionados marginalmente.

Los requisitos necesarios para abordar este texto tienen que ver, ante todo, con el interés y la curiosidad por explorar nuevos conceptos y nuevas dinámicas, pero la curiosidad por sí sola, probablemente, no es suficiente. Sobre todo, es necesario tener paciencia y un cierto grado de apertura mental: sólo cuestionando lo que hoy damos por «obvio» y por sentado, pues junto a un sano espíritu crítico y una actitud proactiva hacia el cambio se hace posible captar plenamente la esencia de la revolución Bitcoin.

**PARTE 1**

**UN VISTAZO AL PASADO**



## Capítulo 1

### LA MONEDA EN LA HISTORIA

Entre los diferentes aspectos que Bitcoin obliga a revisar y cuestionar se encuentra, ante todo, la cuestión de lo que, en realidad, es el dinero.

Sí, el dinero, la moneda, los billetes o como se les quiera llamar. El que utilizamos todos los días, el que intercambiamos constantemente con otras personas, el que intentamos ganar (y en cantidades cada vez mayores) durante nuestra vida. El que a menudo se ve como algo negativo, vinculado a episodios de corrupción, a emociones como la avaricia de las personas, al egoísmo o simplemente a comportamientos poco apreciados (como cuando se nos acusa de estar «demasiado apegados al dinero»).

En resumen, toda nuestra vida, nuestro trabajo y nuestro tiempo están estrechamente ligados al instrumento que es el dinero. Entonces, ¿por qué inventar una nueva moneda? Pocos sienten la necesidad de dotarse de una alternativa completamente desvinculada del actual sistema económico y financiero.

Para poder entender mejor este nuevo fenómeno, inevitablemente debemos partir del concepto de moneda y abrir un paréntesis –no demasiado breve, pero necesario– sobre el papel que esta ha desempeñado en la historia de la humanidad, empezando por sus orígenes y por las civilizaciones primitivas. Estamos hablando de una herramienta que cuenta con una evolución milenaria en la historia del hombre, incluso hay algunas fuentes que demuestran que la invención del dinero es anterior o concomitante a la invención de la escritura<sup>1</sup>.

---

<sup>1</sup> Excluyendo las formas anteriores de trueque, el primer dinero de la historia debe ser atribuido a los Sumerios. Apareció en el 3000 a. C., en el mismo período, lugar y contexto en el que nació la escritura y se hacía referencia a la cebada: cantidades fijas de granos de cebada, medidas en silos, eran utilizadas

## Pueblo **Bitcoin**

En primer lugar, debe quedar claro que el dinero no es más que una *tecnología*. Una herramienta buscada e inventada por el hombre para un objetivo preciso: facilitar la cooperación dentro de cualquier contexto socioeconómico. Así como el descubrimiento del lenguaje –que le permite a los individuos comunicarse fácilmente entre sí para agregarse y organizarse en pueblos– determinó el punto de inflexión en la evolución de las civilizaciones; también el dinero –que les permite a los individuos comunicar *valor*– siempre ha tenido un impacto crucial en la cooperación y el intercambio comercial necesarios para crear sociedades prósperas y duraderas.

Por lo tanto, el dinero es una herramienta inventada por el hombre y sólo por este. Fundamentalmente no es más que una especie de *convención social*, lo que lo caracteriza especialmente es la aceptabilidad, es decir, el hecho de que los individuos dentro de un determinado pueblo estén dispuestos a trabajar o vender bienes y servicios a cambio de un objeto aceptado por convención.

Lo curioso es que este objeto utilizado como medio de intercambio no tiene un valor intrínseco particular de uso directo, sólo adquiere valor como resultado de un acuerdo implícito que surge en la sociedad y que se retroalimenta y se refuerza con el tiempo. Por lo tanto, el valor del dinero depende sustancialmente de las *expectativas* sobre las decisiones de otros miembros de la comunidad: cuanto más un individuo espera que un objeto sea aceptado como medio de intercambio, más probable es que él mismo lo acepte a cambio de bienes o servicios.

Precisamente por ser producto de relaciones sociales, la moneda ha permitido a lo largo de la historia acceder fácilmente al agua, la comida, los cuidados, el sustento, la construcción de refugios y las herramientas de caza. A través de este instrumento, se han podido optimizar los intercambios de productos y servicios entre personas que no se conocen y que se encuentran fuera del círculo restringido de amigos.

De hecho, la moneda debe permitirles a los individuos especializarse en ciertas competencias cada vez más específicas. Imaginemos tener que ocuparnos personalmente de procurar comida todos los días buscando algún animal salvaje, pero también teniendo que conseguir agua de un pozo en el centro del pueblo, buscar materiales necesarios para construir un refugio en el bosque, adquirir conocimientos y técnicas para erigir una choza o estudiar para entender cómo encender un fuego y cocinar.

Intercambiar comida, bienes y servicios era fundamental para sobrevivir, incluso en los tiempos de los hombres primitivos, una necesidad inherente en la

como herramienta para valorar e intercambiar cualquier otro bien o servicio.

Fuente: *Sapiens*, de Yuval Noah Harari.

perspectiva de la cooperación para nuestra salvaguardia como especie. Sin la herramienta de la moneda, capaz de facilitar el intercambio con nuestros semejantes, nuestras posibilidades de supervivencia se reducirían drásticamente. Entonces, el dinero se presenta como una herramienta indispensable para optimizar el intercambio comercial y crear así bienestar y prosperidad, extendiendo los beneficios de este progreso también a otros individuos. Es decir, sirve para facilitar la difusión de conocimientos, competencias y cultura en áreas y fronteras cada vez más extensas. Para cualquier pueblo o sociedad que quiera evolucionar, crecer o prosperar en el tiempo y el espacio, el dinero se configura –en definitiva– como una herramienta básica y fundante.

Como herramienta tecnológica, la moneda debe cubrir esencialmente tres funciones:

1. **Reserva de valor.** Por esta función se entiende la capacidad de conservar el valor en el tiempo. De manera análoga a una batería que resulta tanto más idónea cuanto más consiga conservar la carga eléctrica acumulada en el tiempo, así una buena moneda resulta mucho más útil mientras más pueda garantizar que su valor almacenado no disminuya en el tiempo. Cuando se habla de «activo refugio» se entiende precisamente que se trata de su característica de poder conservar el valor a lo largo de los años, sin perder su poder adquisitivo.
2. **Medio de intercambio.** Un instrumento monetario debería ser funcional para hacer intercambios, tanto en el tiempo como en el espacio. Para cubrir mejor esta función debería, por ejemplo, ser fácil de transportar, práctico de dividir en fracciones más pequeñas y ser fungible además de ser simple de verificar para quien lo acepte como pago.
3. **Unidad de cuenta.** Una moneda adoptada por una sociedad se convierte en unidad de cuenta cuando el valor de todos los bienes y servicios se miden a partir de esta forma de dinero.

Hoy en día, la función de unidad de cuenta mundial está cubierta por el dólar estadounidense: todas las materias primas, bienes de primera necesidad o incluso el precio de Bitcoin se miden a partir del dólar precisamente porque este se reconoce como unidad de cuenta.

Entonces, intentemos esquematizar la historia milenaria de la moneda desde sus orígenes hasta nuestros días, una tarea difícil, si no imposible, de tratar en pocas líneas. En cualquier caso, no se pretende ser exhaustivos, el

## Pueblo **Bitcoin**

objetivo es más bien ofrecer una visión general sobre el tema para poder entender las motivaciones de esta nueva y fascinante novedad llamada Bitcoin.

**FIN DEL EXTRACTO**