Pre-Textos

del Bitcoiner

Francisco de Vitoria Escuela de Salamanca Carl Menger Escuela Austriaca Vaclac Benda Polis Paralela Richard Stallman Manifiesto GNU Tim May Manifiesto Crypto Anarquista Eric Huges Manifiesto Cypherpunk Hal Finney Efectivo Digital y Privacidad John Barlow Declaración Independencia del Ciberespacio Adam Back Hashcash Wei Dai B-Money Nick Szabo Satoshi Nakamoto Libro Blanco de Bitcoin David Chaum Firma Ciega Amir Manifiesto Libbitcoin Alvaro D. Maria La Filosofia del Bitcoin Adrian Bernabeu Bitcoinismo Saifdean Anmous El Patrón Bitcoin Andreas Antonopoulos Mastering Bitcoin 21 lecciones de Gigi Bob Alice

Fanzine en español de la comunidad Bitcoin

FreeBTC. N.1

Año I, Época V

Bloque 930666

Pre-Textos

del Bitcoiner

Publicado por FreeBTC

Número 1.

Este número fue publicado con altura de bloque 925591.

Fanzine de la Comunidad Bitcoiner hispanohablante que pretende difundir la visión actual de Bitcoin y todo lo que lo rodea.

Esta publicación nace bajo los principios de libertad y soberanía.

Todos los textos pretenden ser un ejercicio de pensamiento critico sobre el ecosistema y la comunidad, podemos estar o no de acuerdo con ellos pero son una palanca para debatir y difundir el valor de Bitcoin.

Si este libro te aporta algo que consideres valioso y deseas agradecer el trabajo realizado y apoyar futuros trabajos de otros documentos relacionados con Bitcoin puedes hacerlo enviando algunos sats a la siguiente dirección Lightning:

freebtc@blink.sv

Punto de envío:
https://pay.blink.sv/freebtc

INDICE

EDITORIAL

Hay lanzamientos que se viven como un encendido: una chispa en la oscuridad que, de pronto, revela que no estamos solos. Este Número 1 nace así: con la ilusión intacta de lo nuevo y con la certeza —ya verificada— de que la comunidad hispanohablante tiene voz propia, imaginación y hambre de soberanía. Este fanzine se publica bajo licencia CC BY 4.0 y queda anclado, como cápsula de tiempo, a la altura de bloque 925591: una coordenada fría y precisa para un latido profundamente humano.

Gracias por la respuesta de quienes han escrito, dibujado, pensado y compartido. En cada página hay una forma distinta de mirar a Bitcoin: como tecnología, como ética, como refugio, como relato, como herramienta de emancipación. Y esto no es un “número cerrado”: es una llamada abierta.

Si quieres participar en próximos números, envíanos tus textos, ideas, ensayos, poemas, viñetas o experimentos al correo: freebtcmx@proton.me. (Y si usas seudónimo, lo respetamos: aquí el mensaje importa más que la firma).

Si este fanzine te aporta valor, ayúdanos a que siga creciendo: difúndelo y, si te nace, apóyanos con donaciones en sats por Lightning (en el propio fanzine encontrarás la dirección de recepción).

Y si eres un proyecto o empresa alineada con Bitcoin y quieres patrocinar próximos números y aparecer en estas páginas, escríbenos a freebtcmx@proton.me.

Un viaje a través de las páginas

Este primer número se abre como se abren las historias que importan: con un barrio como universo inicial. “Los Chicos del Barrio” nos deja en el punto exacto donde nacen las preguntas que luego ya no se pueden apagar: la intuición de que la libertad no es un eslogan, sino un aprendizaje lento, casi artesanal. Desde ahí, el fanzine toma velocidad y asciende, como si cambiara de atmósfera: lo íntimo se vuelve arquitectura, y el relato se convierte en sistema.

En ese salto aparece “Bitcoin como Protocolo de Paz”, que propone mirar el protocolo no solo como herramienta económica, sino como una tecnología social capaz de domesticar el conflicto mediante reglas verificables. Si el barrio era gravedad, aquí ya estamos en órbita: teoría de juegos, consenso, y una pregunta de fondo que vibra en cada línea: ¿puede una red reducir la violencia sin imponer obediencia?

La respuesta no tarda en tensionarse cuando entramos en “El Bosque de los Susurros”. Como en los viejos cuentos que parecen inocentes hasta que te dejan sin sueño, la fábula nos recuerda que el control siempre llega maquillado de cuidado. Y entonces el viaje se oscurece: ya no hablamos solo de economía, sino de mirada, de rastros, de jaulas invisibles.

Esa sombra crece y se vuelve casi litúrgica en “Por los siglos de los siglos”, donde Bitcoin deja de ser simple herramienta y se transforma en símbolo: tiempo, destino, permanencia. Es como si el fanzine atravesara un umbral y, de pronto, el lenguaje se volviera cósmico: tick tock, next block como pulsación de una máquina que no duerme y, sin embargo, sostiene lo humano.

Después de esa elevación, necesitamos un golpe de realidad —y llega con tinta y gesto—: “Cámbialo por Bitcoin!!!” irrumpe como un grafiti sobre el mármol de lo oficial. Aquí la crítica ya no se razona: se ve. El fiat se descompone en planos, aristas y gritos visuales, como si el billete fuera un mapa de dominación arrancado a tiras.

Y cuando la imagen abre la herida, entra el análisis a suturar con precisión: “Bitcoin, Herramienta de la Escuela Austriaca” se adentra en la genealogía intelectual del problema —escasez, incentivos, poder monetario— y coloca a Bitcoin como respuesta histórica a una enfermedad recurrente: la tentación de controlar el dinero para controlar a las personas. Del arte pasamos al argumento, y del argumento a la advertencia.

Esa advertencia se dramatiza en “La persecución de la Agencia”, donde el conflicto deja de ser abstracto: tiene pasillos, sellos, teléfonos, puertas que se cierran. El lector siente el mecanismo administrativo como una máquina sin rostro, y Bitcoin aparece no como milagro, sino como herramienta de defensa: una grieta en el muro.

Con esa tensión aún en el pecho, “La Identidad y la Privacidad” nos devuelve al núcleo: ¿quién eres cuando te observan?, ¿qué queda de ti cuando te obligan a ser “legible”? Entre etimologías, mitos y crítica política, el texto actúa como espejo: nos enseña que el enemigo de la libertad no siempre es la violencia directa, sino la domesticación lenta de la identidad.

Y cuando parece que ya lo hemos entendido todo, el fanzine gira hacia sus raíces: “Manifiestos” aparece como archivo vivo, como memoria de la colmena cypherpunk. No es un cierre; es un recordatorio de que nada de esto empezó ayer. En esa misma línea, el correo de Timothy C. May —“Ciberespacio, criptoanarquía y empujar los límites”— funciona como transmisión antigua recibida con nitidez sorprendente: la intuición de los noventa que hoy se siente casi profecía.

Así, el número termina como empezó, pero más lejos: del barrio al ciberespacio, del cuento a la teoría, del arte al manifiesto. Un trayecto completo, como una nave que regresa al puerto con la bodega llena: ideas, imágenes y una certeza compartida —que escribir sobre Bitcoin es, al final, escribir sobre el lugar donde aún puede vivir la libertad.

GRACIAS A TODOS!!!


¡ENTRADA LIBRE!
RESTRICTED AREA
VERIFICANDO...
¡¿QUÈ DEMONIOS ...?!
BIT & NODE ZERO
— ¡SOBERANÍA EN TIEMPO REAL! —

La tira de JASH

LOS CHICOS DEL BARRIO

AUTOR: Anonimo

I. El barrio

El barrio donde crecieron no aparecía en los mapas turísticos ni en los folletos de la ciudad. No tenía monumentos, ni calles con nombres ilustres, ni plazoletas pensadas para la contemplación. Era un barrio funcional, levantado deprisa en una época en la que urgía alojar manos más que sueños. Bloques de ladrillo visto, portales estrechos, balcones cubiertos de ropa tendida que ondeaba como un lenguaje secreto entre vecinos.

Las mañanas empezaban siempre igual: persianas subiendo a medias, cafeteras silbando, el eco de pasos apresurados en las escaleras. El olor a pan caliente salía de la tahona de la esquina y se mezclaba con el gasóleo de los primeros autobuses. En invierno, el frío se quedaba a vivir en los rellanos; en verano, el calor convertía las noches en un ejercicio de resistencia. El tiempo, allí, no avanzaba: se arrastraba.

Alice conocía el barrio desde las alturas modestas del balcón de su casa. Desde allí observaba el ir y venir de la gente como si se tratara de una coreografía lenta: hombres con monos de trabajo manchados de yeso, mujeres dobladas bajo bolsas que parecían pesar más que ellas, ancianos que repetían los mismos trayectos con la precisión de un ritual. Desde muy pequeña comprendió que el mundo no era algo abstracto: el mundo estaba hecho de trayectos repetidos.

Tenía una libreta de tapas azules que escondía bajo el colchón. Allí anotaba palabras que escuchaba sin entender del todo: hipoteca, intereses, préstamo, embargo, recorte. Palabras grandes para una niña pequeña. Las copiaba como si temiera que se escapasen. Intuía que esas palabras mandaban más que muchos adultos. A veces añadía otras que no escuchaba, sino que sentía: libertad, miedo, espera, futuro. No sabía aún que estaba construyendo su primer mapa del poder.

Bob vivía dos calles más abajo. Su casa siempre olía a metal caliente y a polvo antiguo. Su padre, electricista, llegaba cada tarde con las manos negras de grasa y los ojos cansados de mirar dentro de paredes que nunca eran suyas. Bob aprendió pronto que la electricidad era invisible pero mandaba. Como el dinero. Como las normas.

Desde niño desarrolló una manía que nadie supo corregirle: desmontarlo todo. Las primeras víctimas fueron los juguetes. Luego vinieron los objetos rescatados de los contenedores: radios antiguas, calculadoras con teclas hundidas, ventiladores sin aspas. Su habitación era un paisaje caótico de tornillos sueltos, placas electrónicas y carcazas abiertas. Para los demás era desorden; para él era un lenguaje esperando ser descifrado.

No se conocieron en la escuela, ni en una fiesta, ni por amigos comunes. Se conocieron por azar, como ocurren casi todas las cosas importantes. Una tarde Bob llevó a la plaza un coche de juguete al que había acoplado un pequeño motor reciclado. El artefacto avanzaba torciendo las ruedas, rugiendo como un insecto torpe. Alice lo observaba desde el banco oxidado, intrigada.

Bob levantó la vista y la vio mirándolo sin vergüenza.

—Funciona —dijo, como si esa fuera toda la explicación necesaria.

Alice bajó del banco y se acercó despacio. Observó el coche, el cableado expuesto, el pequeño interruptor improvisado.

—Siempre hay algo que funciona —respondió—, aunque parezca roto.

Bob no entendió del todo aquella frase, pero algo en su tono le pareció verdadero.

Desde ese día empezaron a sentarse juntos en el banco de la plaza después del colegio. No hablaban mucho al principio. Compartían bocadillos, intercambiaban silencios. Alice observaba, Bob trasteaba con cualquier objeto que pudiera llevar encima. A veces el silencio se rompía con preguntas simples:

—¿Para qué sirve eso?

—¿Por qué escribes tanto?

Y luego volvían a callar, como si aún no tuvieran palabras suficientes para el tipo de preguntas que ya empezaban a hacerse.

La plaza era el centro invisible del barrio. No pasaba gran cosa, pero pasaba todo. Discusiones en voz baja, risas de niños, bicicletas sin frenos, primeras miradas que no se atrevían a ser miradas. Por las noches, el banco quedaba solo bajo una farola parpadeante. Allí se sentaban ellos algunas veces, cuando el día se les quedaba pequeño.

Ambos sentían, sin saber explicarlo, que aquel barrio era un punto de partida, no un destino. No lo despreciaban. Lo amaban incluso. Pero sabían que, si se quedaban, acabarían repitiendo los mismos trayectos una y otra vez, como las sombras que Alice veía desde su balcón.

Una tarde, mientras el sol se perdía entre los bloques de ladrillo, Alice cerró su libreta y miró a Bob.

—¿Tú crees que todo esto es definitivo? —preguntó, señalando los edificios, la plaza, las calles.

Bob giró un tornillo que tenía entre los dedos, pensativo.

—Nada que se puede desmontar es definitivo —contestó.

Alice sonrió sin saber por qué.

A su manera, los dos acababan de formular, sin saberlo, la misma intuición: todo sistema puede abrirse.

Y esa idea, todavía frágil, todavía sin nombre, empezó a crecer en silencio entre el banco oxidado, la plaza y el barrio que los vio nacer.

II. Aprender a mirar

Aprender a mirar no fue, para ninguno de los dos, un acto consciente. Fue más bien una deriva lenta, una forma de estar en el mundo que se les fue quedando pegada como el polvo a los zapatos. Mientras otros niños corrían sin detenerse demasiado a pensar, Alice y Bob parecían moverse siempre con un segundo de retraso, como si necesitaran observar antes de actuar.

En Alice, mirar se convirtió pronto en una manera de defenderse. Descubrió que quien observa entiende antes de que le mientan. Desde la mesa de la cocina veía a su madre hacer cuentas una y otra vez, borrar cifras, volver a sumarlas. Aquellas sumas no eran solo números: eran horas de trabajo, cansancio acumulado, renuncias que no se decía en voz alta. Alice entendió que el dinero no era algo neutro: era una fuerza que ordenaba silenciosamente los gestos y los silencios.

En el colegio, las matemáticas le resultaban extrañamente fáciles. No por talento puro, sino porque había aprendido a no confiar en el resultado sin comprender el proceso. Cuando algo no cuadraba, no lo aceptaba. Esa costumbre la volvió incómoda para algunos profesores: hacía demasiadas preguntas, pedía demostraciones cuando bastaba con memorizar. Pero Alice intuía que memorizar era una forma elegante de obedecer.

Bob aprendía de otra manera. Miraba con las manos. Para él, comprender significaba tocar, abrir, desmontar. Su padre no se lo prohibía. Al contrario, a veces le llevaba herramientas viejas.

—Si lo rompes, tendrás que arreglarlo —le decía.

Bob rompía mucho. Y arreglaba lo suficiente como para seguir rompiendo.

Pronto descubrió que casi ningún objeto estaba hecho para ser comprendido por quien lo usaba. Todo venía sellado, cerrado, diseñado para funcionar sin hacer preguntas. Aquello le molestaba. ¿Por qué algo que debía servirle no podía ser entendido por él? Esa pregunta, todavía infantil, ya era política sin saberlo.

Alice empezó a frecuentar la pequeña biblioteca municipal. Estanterías torcidas, libros donados, polvo en las baldas. Allí leyó por primera vez sobre crisis antiguas, sobre guerras lejanas, sobre sistemas que se habían creído eternos y no lo fueron. Descubrió que la historia no era una línea recta, sino una sucesión de errores repetidos con nombres distintos.

Bob, mientras tanto, aprendía a programar con manuales desactualizados descargados de internet. No entendía del todo lo que hacía, pero comprendía algo fundamental: el ordenador obedecía instrucciones exactas. No había interpretaciones morales, ni excusas. Si el código estaba mal, el resultado fallaba. Si estaba bien, funcionaba. El mundo, en cambio, fallaba incluso cuando parecía bien escrito.

Seguían viéndose en la plaza. Ya no solo compartían bocadillos, sino también dudas más grandes. Alice hablaba de lo que leía; Bob, de lo que construía. A veces parecía que hablaban idiomas distintos. Sin embargo, con el tiempo se dieron cuenta de que estaban buscando lo mismo: el punto exacto donde las cosas dejan de ser misteriosas y pasan a ser comprensibles.

Una tarde, Alice llegó alterada. Había escuchado a su padre discutir con su jefe por un retraso en el pago. La palabra “intereses” había sonado como una amenaza. Se sentó en el banco con la libreta apretada contra el pecho.

—No lo entiendo —dijo—. Trabajan más, deben más. Nunca sale a favor.

Bob la escuchó en silencio. Luego sacó de su mochila una placa electrónica.

—Esto —dijo— funciona así porque alguien lo diseñó así. Si lo diseñaran distinto, funcionaría distinto.

Alice lo miró largo rato.

—¿Y quién diseña el dinero?

Bob no supo qué contestar.

Aquella pregunta se quedó flotando entre ellos como una nube que aún no tenía forma de tormenta, pero ya presagiaba lluvia.

Con el paso de los años, ambos fueron construyendo una mirada incómoda. Alice aprendió a sospechar de los discursos oficiales. Bob aprendió a sospechar de las cajas cerradas. Mientras otros aceptaban la realidad como una gama limitada de opciones, ellos empezaban a intuir que las opciones estaban diseñadas.

El instituto trajo nuevos profesores, nuevos libros, nuevas versiones del mismo mundo. Les hablaron de salidas profesionales, de éxito, de competir. Les dijeron que estudiando podrían "llegar lejos". Nadie concretó qué significaba exactamente "lejos", ni quién decidía la dirección.

Alice empezó a darse cuenta de que casi todos los alumnos soñaban con escapar del barrio, pero muy pocos se preguntaban por qué querían escapar exactamente. Bob observó que todos los sistemas informáticos del centro eran cerrados, limitados, vigilados. Por primera vez comprendió que el control también podía ser técnico.

Una tarde, volviendo juntos a casa, Alice dijo:

—Nos están enseñando a mirar lo que quieren que miremos.

Bob asintió.

—Pero nadie puede impedirnos mirar detrás.

No sabían aún que esa capacidad de mirar "detrás" sería su mayor herramienta frente al mundo.

A finales de aquella etapa, ambos ya eran distintos del resto sin proponérselo. No eran rebeldes visibles. No gritaban. No rompían normas de manera espectacular. Pero algo en ellos ya no encajaba del todo en el molde.

Habían aprendido a mirar.

Y quien aprende a mirar ya no puede volver a ver igual.

III. La promesa invisible

La adolescencia llegó sin ceremonias, como llegan casi todas las cosas que lo cambian todo. Un día simplemente se descubrieron más altos, más callados, más conscientes del peso de las palabras que hasta entonces habían usado sin cuidado. El barrio seguía siendo el mismo, pero ellos ya no lo eran. Algo había empezado a desplazarse por dentro, una inquietud sin nombre, un presentimiento de que el tiempo comenzaba a exigir decisiones.

En el instituto les hablaron por primera vez del futuro con una seriedad que rozaba la amenaza. Orientadores, charlas, folletos de universidades. Les mostraron gráficos, salidas profesionales, tasas de empleabilidad. Todo parecía ordenado, cuantificable, previsible. Alice miraba aquellas cifras con atención, pero algo la inquietaba: ningún gráfico hablaba del precio real de una vida.

En casa, las conversaciones se volvieron más tensas. Su madre le repetía que debía elegir "algo con salidas". Su padre hablaba de estabilidad como si fuera una tierra prometida que él nunca había pisado. Alice escuchaba en silencio. Por primera vez comprendió que el miedo también se hereda, que los padres no solo transmiten apellidos, sino también renuncias.

Bob vivía otro tipo de presión. Su padre no le hablaba de universidad con entusiasmo, sino con desconfianza. Había visto demasiados títulos colgados de paredes que no daban de comer.

—Aprende algo que sirva —le decía—. Algo que te haga falta incluso cuando todo se caiga.

Bob asentía sin discutir. En realidad, no sabía muy bien qué quería "servir", pero tenía claro algo más importante: no quería obedecer sin comprender, como había visto hacer a tantos adultos.

Seguían sentándose en el banco de la plaza, aunque ahora el banco parecía más pequeño. Ya no compartían bocadillos, sino pensamientos que pesaban más que el pan.

Una tarde de otoño, con el cielo bajo y gris, Alice habló sin rodeos:

—Tengo miedo de acabar viviendo la vida de otros.

Bob la miró sorprendido.

—¿De quiénes?

—De todos —respondió—. De mis padres. De sus jefes. De los jefes de sus jefes. De decisiones que nadie toma ya por sí mismo.

Bob comprendía demasiado bien ese sentimiento, aunque le costara formularlo. Giró una piedra con el pie.

—Yo tengo miedo de no entender nunca quién decide de verdad.

Guardaron silencio un momento. El ruido lejano de una moto, el murmullo de una conversación ajena, el parpadeo de la farola. Todo parecía trivial comparado con lo que acababan de decir.

—Entonces —dijo Alice— tendremos que estudiar.

Bob levantó la vista.

—¿Para ganar dinero?

Alice negó con la cabeza.

—Para no depender.

Aquella fue la promesa. No se escribió en ningún contrato. No se celebró con palabras solemnes. Fue una frase simple, pronunciada en un banco oxidado, pero se convirtió en la columna vertebral de todo lo que vino después. Estudiar no como ascenso social, sino como acto de defensa.

Desde ese día, algo cambió en su manera de mirar los libros. Alice ya no estudiaba solo para aprobar, sino para desmontar. Leía con rabia contenida, buscando grietas en los discursos que se presentaban como neutrales. Descubrió que muchas teorías económicas nacían de un contexto, de intereses concretos, de luchas invisibles que luego se borraban del relato oficial.

Bob se sumergió aún más en la técnica. Programaba hasta la madrugada con un ordenador que parecía a punto de rendirse en cualquier momento. Cada línea de código era un experimento, una pequeña victoria contra la ignorancia. Se dio cuenta de que quien entiende los sistemas tiene una ventaja silenciosa sobre quien solo los usa.

El entorno, sin embargo, no celebraba esa transformación. Algunos amigos empezaron a distanciarse. No por odio, sino por incomodidad. Alice y Bob ya no compartían las mismas certezas fáciles. Hacían demasiadas preguntas. Dudaban demasiado.

—Os estáis complicando la vida —les decían.

Y quizás era cierto. Pero también era cierto que la vida ya estaba complicada, solo que hasta entonces no habían querido mirarla de frente.

Llegó el momento de rellenar solicitudes, elegir carreras, despedirse sin darse cuenta. Alice eligió economía.

No por amor a los números, sino por enfrentarse al lenguaje que gobernaba el mundo.

Quería entender el poder desde su sintaxis más profunda. Bob eligió ingeniería. No por prestigio, sino por necesidad interior. Sentía que si comprendía cómo se construían las cosas, nadie podría cerrarle todas las puertas a la vez.

La noche antes de marcharse a la ciudad universitaria se encontraron en la plaza. El banco seguía allí, como si nada hubiese ocurrido. Se sentaron sin hablar durante un rato.

—Pase lo que pase —dijo Alice al fin—, no dejemos de hacernos preguntas.

Bob asintió.

—Y no dejemos que otros las respondan por nosotros.

No hubo abrazos largos ni promesas grandilocuentes. Solo una certeza compartida, aún torpe, aún incompleta, pero firme: no iban a vivir de rodillas, aunque todavía no supieran cómo mantenerse en pie.

El barrio quedó atrás, no como una huida, sino como una raíz.

Y con esa promesa invisible, comenzaron a caminar hacia un mundo que todavía no entendían, pero que ya no estaban dispuestos a aceptar sin condiciones.

IV. Años de hambre y de preguntas

La universidad no fue la entrada solemne a ningún paraíso. No hubo ceremonias de iniciación ni promesas de prosperidad inmediata. Hubo, en cambio, habitaciones alquiladas por meses, colchones que ya conocían otros cuerpos, cocinas compartidas donde cada uno vigilaba su estante como un territorio frágil. Hubo frío en invierno y calor detenido en verano. Hubo silencios tensos cuando el dinero escaseaba antes de fin de mes.

Alice llegó a la facultad con una mezcla de entusiasmo y desconfianza. Los pasillos largos, las aulas abarrotadas, los profesores que hablaban desde tarimas ligeramente elevadas. Todo estaba pensado para que uno escuchara más de lo que preguntara. Aprendió pronto a reconocer los rituales: apuntes dictados, exámenes de memoria, teorías presentadas como verdades incontestables. Pero también encontró grietas. Algún profesor dejaba escapar dudas, algún dato no cerraba del todo, algún modelo necesitaba demasiadas suposiciones para funcionar.

Bob, por su parte, se encontró con un universo de estructuras formales. Código, circuitos, sistemas. Aquello era su territorio natural. Pero pronto comprendió que no todo se programaba en libertad. Muchos proyectos estaban condicionados por empresas externas, por patentes, por intereses que no aparecían en el temario. Descubrió que incluso la tecnología podía nacer con una jaula incorporada.

Para ambos, los días se repartían entre estudiar y sobrevivir. Trabajos de pocas horas mal pagados, turnos de noche en bares, veranos completos en fábricas donde el tiempo se media por sirenas. Aquella precariedad no era temporal como les habían dicho. Era estructural. Alice empezó a sospechar que el sistema necesitaba esa fragilidad para mantenerse.

Las conversaciones entre ellos se volvieron más densas. Ya no hablaban solo del barrio, ni de los profesores, ni de las asignaturas. Hablaban del mundo. De por qué a algunos siempre les costaba llegar a fin de mes aunque trabajaran más que otros. De por qué las crisis siempre parecían caer del mismo lado. De por qué se normalizaba vivir endeudado como si fuera una condición natural del ser humano moderno.

Una noche, sentados en el suelo de un piso compartido porque no quedaban sillas libres, Alice desplegó sus apuntes sobre la mesa.

—Mira —dijo—. En teoría, esto es equilibrio. En la práctica, es transferencia lenta de poder.

Bob observó las curvas, los números, los símbolos.

—En programación —respondió—, cuando un sistema transfiere recursos siempre al mismo nodo, lo llamamos fallo de diseño. O trampa.

Alice levantó la vista. Aquellas dos frases encajaban como piezas de un mismo engranaje invisible.

La crisis económica dejó de ser una palabra abstracta y adquirió rostros. Compañeros que abandonaban la carrera porque no podían pagar el alquiler. Padres que perdían el trabajo cuando ya era tarde para reinventarse. Bancos rescatados con dinero público mientras las becas se recortaban. Alice lo estudiaba todo con una mezcla creciente de rabia y lucidez. Bob lo observaba desde la infraestructura: servidores centralizados, plataformas que caían cuando más se las necesitaba, sistemas diseñados para obedecer a un centro único.

Ambos empezaron a comprender que el problema no era solo quién ganaba y quién perdía, sino quién tenía el control de las reglas del juego.

El cansancio acumulado les pasó factura. Hubo discusiones. Silencios largos sin explicación. Días en los que parecía que todo el esfuerzo era inútil. Alice dudó por primera vez de haber elegido bien. Bob, agotado, pensó en abandonar temporalmente los estudios y trabajar a tiempo completo.

—Quizá esto no es para nosotros —dijo él una noche, con la voz rota.

Alice lo miró largo rato antes de responder.

—Precisamente por eso lo es.

Siguieron adelante.

Descubrieron también que la educación tenía límites claramente marcados. Les enseñaban a ser eficientes, pero no a ser libres. A optimizar, pero no a cuestionar fines. A adaptarse, pero no a resistir. Esa constatación les resultó más dolorosa que la propia precariedad material.

Fue durante aquellos años cuando empezaron a hablar, cada vez con más claridad, de dependencia. Dependencia del salario. Del crédito. De las plataformas. De decisiones tomadas muy lejos de sus propias manos. Alice empezó a ver la economía como un sistema de contratos desiguales. Bob empezó a ver la tecnología como un campo de batalla por la soberanía.

A pesar de todo, había momentos de luz. Cafés interminables al amanecer. Risas nerviosas después de un examen imposible. La sensación fugaz de que todavía era posible construir algo distinto. Esa fraternidad silenciosa fue lo que les sostuvo cuando el peso del mundo parecía demasiado grande.

Durante el último año de carrera, algo en ambos ya estaba definitivamente roto... o definitivamente abierto. Ya no esperaban que el sistema les ofreciera un lugar cómodo. Lo observaron como quien observa una maquinaria muy antigua: con respeto por su potencia, pero sin fe en su justicia.

Alice empezó a intuir que la economía que había estudiado explicaba cómo se movía el dinero, pero no por qué debía moverse así. Bob comprendió que la ingeniería resolvía problemas formales, pero eludía los conflictos de poder que esos mismos sistemas reproducían.

Ambos sentían que habían aprendido mucho. Y, al mismo tiempo, que todavía no habían aprendido lo más importante.

Aún no sabían que esa carencia tenía un nombre.

Aún no sabían que faltaba una pieza.

Aún no sabían que estaba a punto de aparecer.

V. La primera grieta

La primera vez que Bob oyó la palabra Bitcoin no la escuchó como quien escucha una promesa, sino como quien tropieza con un término extraño en una frase que parecía hablar de otra cosa. Fue en un foro técnico, una madrugada cualquiera, cuando buscaba solución a un problema menor de red. Alguien había escrito, casi de pasada: “Eso podría resolverse con un sistema tipo Bitcoin”. Bob no supo qué significaba exactamente, pero tomó nota mental del nombre, como solía hacer con las palabras que parecían abrir puertas.

Pasaron semanas antes de que volviera a aparecer. Esta vez, en boca de un profesor, pronunciada con una mezcla de ironía y recelo:

—Una extravagancia criptográfica que algunos pretenden hacer pasar por dinero.

Bob sintió esa vibración íntima que siempre le producía aquello que los manuales despreciaban con demasiada rapidez. Aquella misma tarde, sin saber muy bien por qué, buscó el libro blanco.

No lo entendió del todo. De hecho, entendió poco al principio. Pero comprendió algo esencial: allí no había promesas de beneficio fácil, sino una arquitectura. Un sistema que no pedía confianza en personas, sino en reglas abiertas.

Eso, para alguien que llevaba media vida abriendo cajas cerradas, era casi una invitación personal.

No se lo contó a Alice de inmediato. Necesitaba primero entender lo suficiente como para no quedar atrapado en palabras vagas. Durante noches enteras volvió al documento, a los debates técnicos, a los esquemas del funcionamiento de la red. Prueba de trabajo. Cadena de bloques. Nodos. Consenso. Cuanto más se adentraba, más claro veía algo que le resultaba inquietante: aquel sistema había sido diseñado para no obedecer a nadie en particular.

Cuando al fin se decidió a hablarlo, fue una noche de lluvia, en un piso sin apenas calefacción. Alice repasaba unos apuntes de macroeconomía. Bob se sentó frente a ella con el portátil abierto.

—He descubierto algo raro —dijo—. Dinero sin bancos.

Alice levantó la vista con una media sonrisa escéptica.

—Eso no existe.

Bob giró la pantalla hacia ella.

—Existe aquí.

Alice leyó el título del documento. Leyó los primeros párrafos. Frunció el ceño.

—Esto es una utopía técnica —dijo—. El dinero siempre ha sido poder político.

—Precisamente —respondió Bob—. Esto intenta separarlos.

Aquella conversación duró horas. Alice objetaba desde la historia: Estados, guerras, bancos centrales, emisiones monetarias, controles de capital. Bob respondía desde la estructura: nodos distribuidos, reglas matemáticas, imposibilidad del doble gasto. Ninguno convencía al otro del todo. Pero algo se había roto ya para ambos: la idea de que el dinero fuera una realidad natural e inmodificable.

En los días siguientes, Alice empezó a investigar por su cuenta. No quería quedar atrapada en la excitación técnica de Bob. Quería entenderlo desde la economía, desde la política, desde la historia. Descubrió el abandono del patrón oro, la inflación estructural, la deuda como instrumento de poder. Descubrió que muchas de las “leyes económicas” eran, en realidad, decisiones humanas disfrazadas de inevitables.

Bitcoin empezó a aparecer ante ella como una anomalía teórica. Un objeto que no encajaba en ningún modelo clásico. Un dinero sin emisor, sin fronteras, sin rescates. Un sistema donde las reglas no podían cambiarse por decreto.

Eso la inquietaba profundamente.

—Si esto funciona —dijo una tarde—, cambiará todo.

Bob asintió.

—Por eso tanta gente quiere que no funcione.

No entraron en Bitcoin como quien entra en un negocio. Entraron como quien entra en un túnel sin saber dónde termina. Las primeras compras fueron ridículas. Fracciones mínimas, casi simbólicas. Alice miraba el saldo como si fuese un experimento sociológico. Bob lo observaba como el latido inicial de una red viva.

El primer nodo lo montaron con piezas prestadas. Un ordenador que parecía a punto de morir, un disco duro con más ruido que memoria, una conexión inestable. Cuando por fin lo vieron sincronizarse, sintieron una emoción difícil de explicar. No habían minado nada. No habían ganado nada. Pero ya participaban sin pedir permiso.

Alice comenzó a comprender algo que ningún profesor le había explicado: el dinero también era una tecnología. Y como toda tecnología, podía diseñarse de formas radicalmente distintas.

Bob, por su parte, entendió algo igualmente decisivo: la descentralización no era un discurso, era una tensión constante contra la tentación de controlar.

No tardaron en llegar las burlas. Amigos que se reían. Profesores que lo despreciaban abiertamente. “Eso no durará.” “Eso es para delincuentes.” “Eso lo prohibirán.” Alice escuchaba y tomaba nota de cada argumento. Bob observaba qué tipo de autoridad hablaba desde cada crítica.

Ambos aprendieron pronto que toda estructura que no se puede controlar provoca primero ridículo, luego miedo, luego ataque.

Aquel fue el verdadero comienzo. No porque ganaran dinero —no lo hicieron—, sino porque por primera vez vieron una grieta real en el muro que llevaban años observando. Un muro que ya no parecía tan sólido. Un muro que, tal vez, no era un muro, sino una construcción mantenida por acuerdos frágiles.

Esa grieta no les dio certezas. Les dio algo más peligroso: posibilidad.

Y con la posibilidad llegó también la responsabilidad.

Bitcoin ya no era una palabra extraña.

Se había convertido en una pregunta sin retorno.

VI. Aprender a perder

La primera gran lección que Bitcoin les dio no fue sobre el dinero, sino sobre la pérdida. Nadie se los explicó con un manual. Nadie los advirtió con suficiente claridad. Simplemente ocurrió.

Al principio todo era torpeza. Direcciones mal copiadas. Contraseñas apuntadas en papeles que luego desaparecían. Archivos guardados en pendrives que dejaban de funcionar sin previo aviso. Alice, acostumbrada a sistemas donde siempre había un número de soporte al que llamar, comenzó a sentir una desazón nueva: no existía un responsable externo. Si se equivocaban, la equivocación era definitiva.

Bob lo asumió antes. No por frialdad, sino por formación. Sabía que en los sistemas sin respaldo el error no se perdona.

—Esto no es un banco —le dijo una noche, tras perder una pequeña cantidad por una mala operación—. Esto es más parecido a la vida.

Alice no respondió. Miraba la pantalla apagada como quien observa una tumba diminuta. Aquello no era una pérdida económica relevante, pero sí era una herida simbólica: la prueba tangible de que la soberanía no venía acompañada de red de seguridad.

Durante un tiempo dudaron. Se preguntaron si no sería más cómodo seguir como los demás. Entregar la custodia a terceros. Confiar. Olvidarse del peso de vigilar.

Pero algo en ellos ya había cambiado. No podían volver a fingir que no sabían.

Comprendieron pronto que Bitcoin no perdonaba la negligencia. Exigía atención, disciplina, memoria. Les obligaba a pensar en términos largos, no inmediatos. Les hablaba en el lenguaje incómodo de la responsabilidad radical.

Alice empezó a escribir sus claves como quien redacta un testamento. Con cuidado extremo. Con conciencia de finitud. Bob comenzó a duplicar respaldos, a probar restauraciones como quien ensaya incendios antes de que ardan las casas. Aquello dejó de ser un juego.

Luego llegaron las estafas. No en forma de grandes engaños, sino de pequeñas confianzas mal colocadas. Un foro falso. Un enlace que parecía legítimo. Un intermediario que prometía facilidades. Aprendieron que la descentralización no elimina al estafador: lo vuelve más creativo.

Bob se culpaba con dureza. Alice lo hacía en silencio.

—Nos están cobrando por adelantado —dijo ella una noche— lo que aún no sabemos.

Bob la miró.

—Nos están enseñando lo que nadie enseña: a no delegar el miedo.

Aquella frase se les quedó grabada.

Fue entonces cuando Alice comprendió algo que ningún tratado económico le había explicado: la confianza también es un activo, y puede perderse tan rápido como cualquier moneda. Entendió que los sistemas tradicionales estaban diseñados para absorber el miedo individual repartiendo el riesgo, pero a cambio exigían obediencia. Bitcoin hacía lo contrario: devolvía el miedo al individuo, pero también le devolvía el control.

Bob lo formulaba de otro modo:

—Aquí nadie te protege de ti mismo.

Ese descubrimiento los marcó más que cualquier ganancia.

Cada error les dolía. Cada pérdida, por mínima que fuera, pesaba como un recordatorio. Pero también los hacía más precisos, más cuidadosos, más conscientes. Aprendieron a desconfiar sin caer en el cinismo, a verificar sin dejar de avanzar.

Algo se endureció en ellos. No como una coraza, sino como una estructura interna que antes no existía. Dejaron de actuar desde la esperanza ingenua y empezaron a hacerlo desde el criterio.

Alice empezó a ver claro que el sistema financiero tradicional infantilizaba a las personas tratándolas como incapaces de gestionar su propia soberanía. Bob comprendió que muchos sistemas tecnológicos estaban diseñados para que el usuario fallara, para así poder controlarlo después.

Bitcoin, en cambio, no cuidaba sus errores.

Los exponía.

Aquel aprendizaje tuvo consecuencias más allá del dinero. Se trasladó a su forma de trabajar, de relacionarse, de confiar. Dejó de tranquilizarlos el respaldo ajeno y empezó a tranquilizarlos la comprensión propia.

Una madrugada, después de una larga conversación sobre una pérdida reciente, Alice dijo:

—Esto no se parece en nada a la libertad que imaginábamos de niños.

Bob sonrió con cansancio.

—No. Pero se parece mucho más a la libertad real.

Ambos comprendieron entonces que estaban pagando un precio que casi nadie quería pagar: el de no poder culpar a nadie más.

Y, sin embargo, por primera vez en mucho tiempo, ese precio no les parecía una condena.

Les parecía, extrañamente, un privilegio.

VII. El precio de la libertad

La libertad, descubrieron pronto, no era un estado de celebración permanente. No tenía la épica de los grandes gestos ni el reconocimiento público de las victorias visibles. La libertad era, más bien, una soledad densa, un territorio donde muchas certezas desaparecían y donde las decisiones dejaban de ser compartidas.

A medida que Alice y Bob se adentraban más en la lógica de Bitcoin, también se iban alejando, sin proponérselo, de muchas de las conversaciones habituales. Ya no podían participar con la misma ligereza en las charlas sobre hipotecas, planes de pensiones o promesas de rentabilidad garantizada. No porque se creyeran superiores, sino porque veían el andamiaje oculto de esos discursos. Y una vez visto, ya no se puede fingir ceguera.

Las cenas con amigos se llenaron de silencios incómodos. Bastaba con que alguien mencionara al banco, una subida de tipos, una nueva ley financiera, para que Alice sintiera el impulso de intervenir... y la tentación de callar.

Cuando hablaba, la reacción era casi siempre la misma: sonrisas condescendientes, bromas, advertencias disfrazadas de consejos.

—Te estás volviendo paranoica.

—Eso es muy radical.

—El sistema no es perfecto, pero es lo que hay.

Bob recibía otro tipo de comentarios:

—Eso es para frikis.

—Eso lo controlarán al final cuatro como todo.

—Cuando el Estado quiera, lo apaga.

Bob escuchaba, analizaba la arquitectura del miedo que había detrás de cada frase. Comprendía que muchas de aquellas críticas no venían del razonamiento, sino del pánico a asumir la propia impotencia.

Alice, en cambio, lo vivía de un modo más íntimo. Veía en los argumentos de los otros el reflejo de los miedos de su propia familia. La necesidad de seguridad. El terror al vacío. La esperanza depositada en instituciones que ya habían demostrado su fragilidad.

Durante un tiempo intentaron convencer. Con datos. Con historia. Con ejemplos. Con paciencia. Pero pronto entendieron algo esencial: las ideas que tocan el núcleo del poder no se discuten, se rechazan. No por falta de inteligencia, sino por instinto de supervivencia social.

Bob dejó de explicar cómo funcionaba la red si no se lo pedían expresamente. Alice dejó de citar cifras en las reuniones familiares. No por cobardía, sino por economía emocional. Comprendieron que la libertad también implica elegir cuándo hablar.

La presión no solo venía de fuera. También emergía desde dentro. Hubo noches de duda. Momentos en los que el peso de la responsabilidad parecía excesivo. Días en los que se preguntaban si no sería más fácil volver a vivir como antes: sin custodiar claves, sin cuestionar demasiado, sin cargar con el mundo sobre los hombros.

—A veces echo de menos la ignorancia —confesó Alice una madrugada.

Bob no se sorprendió.

—Yo echo de menos la facilidad —respondió.

Pero ninguno de los dos deseaba realmente volver atrás. No podían.

Entendieron entonces que el verdadero precio de la libertad no era económico, sino psicológico y social. Consistía en vivir sin el consuelo de la delegación. En asumir que la autoridad última ya no estaba fuera. En caminar sin barandillas ideológicas.

Aquel cambio empezó a reflejarse también en su forma de trabajar. Alice, en su entorno académico y profesional, comenzó a ser vista como alguien incómodo. Hacía preguntas que nadie quería responder. Señalaba supuestos que todos preferían dar por buenos. No era una agitadora, pero su sola presencia alteraba el equilibrio de muchas conversaciones.

Bob, en el terreno técnico, rechazaba proyectos que implicaban control excesivo, vigilancia sin transparencia, centralización opaca. Eso le cerró puertas. Lo apartó de ciertos circuitos bien pagados. Pero también lo acercó a otros que compartían una ética parecida, dispersos, silenciosos, difíciles de encontrar.

Ambos empezaron a comprender que la libertad te va reordenando el mapa humano. Algunas personas se alejan. Otras aparecen desde lugares inesperados. Y una aprende a distinguir, con más claridad que nunca, quién se acerca por afinidad profunda y quién solo por costumbre.

Hubo un día especialmente duro. Una discusión familiar. La palabra "irresponsable" flotó en el aire con una carga que no necesitaba explicación. Alice guardó silencio. Sabía que ninguna argumentación económica podía competir con el miedo de una madre. Aquella noche lloró como no lo había hecho en años.

Bob no intentó consolarla con razones. Se sentó a su lado.

—Ser libre no siempre significa sentirte tranquilo —dijo—. A veces solo significa no mentirte.

Ese día Alice comprendió que la libertad no venía acompañada de paz inmediata. Venía acompañada de verdad. Y la verdad no siempre es amable.

Con el tiempo, aprendieron a sostener ese peso sin dramatismo. A no ir por la vida señalando grietas. A vivir de acuerdo con lo que creían sin convertirlo en una bandera permanente. Comprendieron que la libertad más profunda no es la que se exhibe, sino la que se ejercita en silencio.

Bitcoin ya no era para ellos una novedad ni una causa. Era un suelo. Un marco. Un punto de referencia desde el cual mirar todo lo demás.

Y desde ese lugar, el mundo se veía más frágil...

pero también más abierto.

VIII. Reescribir la mirada

Nada cambió de golpe. No hubo un día exacto en el que Alice y Bob despertaran siendo otras personas. El cambio fue lento, casi imperceptible, como esas grietas que no preocupan hasta que un día atraviesan toda la pared. Pero cuando quisieron darse cuenta, ya no miraban el mundo del mismo modo. No era el mundo quien había cambiado: eran ellos.

Para Alice, la transformación fue primero intelectual, después moral. Durante años había estudiado los mecanismos del dinero como quien estudia el funcionamiento de una máquina ajena. Pero ahora comprendía algo decisivo: ella misma estaba dentro de la máquina. Ya no podía observarla desde fuera con neutralidad. Su salario, su ahorro, sus impuestos, su tiempo... todo formaba parte del mismo circuito que antes analizaba en diagramas.

Comenzó a releerlo todo. Viejos manuales, teorías consagradas, textos que daban por evidentes premisas que ahora le parecían frágiles. La inflación dejó de ser un fenómeno "técnico" para convertirse en un proceso profundamente político. La deuda dejó de parecerle una herramienta de progreso para revelarse como una promesa de obediencia futura. El crecimiento infinito, presentado durante años como una ley natural, empezó a parecerle una creencia casi religiosa.

Bitcoin introdujo en su pensamiento una noción que no encontraba en ningún otro modelo: el límite innegociable. Por primera vez, un sistema monetario no prometía adaptarse a las necesidades del poder, sino obligar al poder a adaptarse a sus reglas. Aquello la perturbaba y la fascinaba a la vez.

Empezó a comprender que la pregunta correcta ya no era "¿cómo se reparte el dinero?", sino "¿quién puede crearlo?" Y al formular esa pregunta, todo lo demás se recolocó.

Bob vivió una transformación distinta, pero paralela. Para él, la descentralización dejó de ser una palabra atractiva para convertirse en una exigencia ética. Empezó a ver centralización allí donde antes solo veía eficiencia. En los servidores únicos. En las plataformas imprescindibles. En las puertas traseras justificadas por la comodidad.

Lo que antes consideraba simples decisiones de diseño empezó a revelársele como decisiones de poder. ¿Quién actualiza? ¿Quién apaga? ¿Quién decide qué es válido y qué no? Cada una de esas preguntas escondía un centro, y Bob había aprendido ya que todo centro es potencialmente una jaula.

Bitcoin le enseñó algo que ningún proyecto académico le había mostrado con tanta claridad: que un sistema puede ser fuerte precisamente porque nadie lo controla. Que la ausencia de amo no es un defecto, sino una arquitectura. Que la confianza puede distribuirse sin desaparecer.

Ambos comenzaron a vivir desde ese nuevo suelo sin necesidad de proclamarlo. Cambió su forma de ahorrar. Cambió su forma de trabajar. Cambió incluso su manera de entender el tiempo. Alice empezó a pensar a diez, veinte años vista, no en trimestres. Bob dejó de entusiasmarse por soluciones brillantes de corto recorrido y comenzó a buscar infraestructuras lentas, robustas, difíciles de destruir.

Sus conversaciones ya no giraban solo en torno al presente. Hablaban del futuro como quien habla de una construcción delicada que puede venirse abajo con un solo error de diseño. Hablaban de hijos que quizá tendrían algún día, de un mundo cada vez más vigilado, de monedas digitales estatales, de identidades obligatorias, de datos convertidos en rehenes.

—No se trata solo de nosotros —dijo Alice una noche—. Se trata de qué mundo estaremos aceptando sin darnos cuenta.

Bob asintió.

—Y de qué mundo estamos ayudando a construir sin saberlo.

Alice empezó a introducir estas ideas con extremo cuidado en su entorno profesional. No en forma de consignas, sino de preguntas. Preguntas incómodas. ¿Qué significa soberanía económica en un mundo de pagos programables? ¿Qué ocurre cuando el dinero deja de ser neutral? ¿Qué sucede cuando el ahorro puede desaparecer por decreto?

Bob, por su parte, comenzó a colaborar en proyectos abiertos, mal pagados y exigentes, donde el código era revisado por desconocidos de todo el mundo. Aprendió a aceptar la crítica como un método de purificación técnica. Aprendió que la transparencia no es una pose, sino un sacrificio: expone errores, desnuda egoísmos, elimina atajos.

Ambos fueron comprendiendo que Bitcoin no era solo un instrumento financiero. Era una escuela de pensamiento. Una forma radical de reinterpretar la confianza, la autoridad, el valor y el tiempo.

A veces, mirando atrás, Alice se preguntaba en qué momento había dejado de creer que el Estado podía garantizarle el futuro. Bob se preguntaba cuándo exactamente había dejado de confiar en que la tecnología, por sí sola, fuera neutral.

Ninguno encontraba una fecha precisa. Las mutaciones profundas no tienen calendario.

Solo sabían que ya no esperaban salvadores. Que los discursos tranquilizadores les producían sospecha. Que las soluciones demasiado sencillas ya no les resultaban creíbles.

Habían reescrito su mirada.

Y eso implicaba una consecuencia irrevocable:

ya no podían desver lo que habían visto.

Una tarde, sentados en una terraza pequeña mientras caía una lluvia fina y persistente, Alice lo dijo en voz baja:

—Todo lo que antes parecía sólido ahora me parece negociable.

Bob respondió tras unos segundos de silencio:

—Y todo lo que antes parecía imposible ahora me parece solo difícil.

Sonrieron sin alegría ni tristeza. Solo con una lucidez nueva, más pesada que la ignorancia, pero también más fértil.

Habían cruzado un umbral invisible.

Y al otro lado, el mundo ya no era el mismo.

IX. Volver al origen

Volver al barrio no fue una decisión planificada. Ocurrió como ocurren muchas cosas importantes: por acumulación de ausencia. Un día Alice se dio cuenta de que llevaba demasiado tiempo sin caminar aquellas calles. Bob lo notó en su propia nostalgia silenciosa. El origen, comprendieron, no desaparece cuando uno se va; solo se queda esperando.

Fueron una tarde de otoño. El cielo bajo, el aire cargado de una humedad que parecía antigua. Aparcaron a unas manzanas y siguieron a pie, como en los viejos tiempos. El barrio los recibió con una familiaridad extraña: todo estaba ahí, pero casi nada era exactamente igual.

Los bloques seguían levantándose en filas rectas, pero las fachadas mostraban nuevas capas de pintura descascarillada. Algunos comercios habían resistido. Otros eran ahora persianas cerradas con grafitis superpuestos. El antiguo videoclub era un local vacío con carteles de alquiler desteñidos. La panadería resistía, milagrosamente, con el mismo olor de siempre escapando por la puerta entreabierta.

Alice caminaba despacio, mirando desde otro cuerpo aquello que había mirado desde niña. Le sorprendió la baja altura de los edificios, la estrechez real de las aceras, la proximidad física entre las viviendas.

Todo era más pequeño de lo que su memoria había conservado. Bob observaba las instalaciones eléctricas exteriores, los cables improvisados, los empalmes informales que delataban reparaciones sucesivas, urgencias antiguas.

—Nada se construyó para durar —murmuró.

—Tampoco para ser desmontado con cuidado —respondió Alice.

Llegaron a la plaza casi sin darse cuenta. El espacio parecía detenido en un tiempo extraño. La fuente seguía sin agua. La farola parpadeaba igual que antes. Y allí estaba el banco.

Se sentaron en el banco oxidado sin protocolo, como si los años no hubieran pasado. Durante unos minutos no dijeron nada. Escucharon el eco distante de un balón golpeando una pared, risas dispersas, una discusión en una ventana abierta, una radio mal sintonizada.

Alice fue la primera en hablar:

—Aquí empezó todo... y nosotros no sabíamos nada.

Bob observaba el óxido de la estructura.

—O sabíamos más de lo que creíamos, pero no teníamos palabras.

Miraron a los niños que corrían por la plaza. Pantallas en las manos. Zapatillas con luces. Ninguno parecía realmente estar en el mismo lugar que su cuerpo. Alice sintió una punzada leve en el pecho.

—Ellos ya viven dentro de otra lógica —dijo—. Todo es inmediato. Todo es medible. Todo deja rastro.

Bob no quitaba la vista del banco.

—Nosotros también —respondió—. Solo que ahora lo sabemos.

Alice pensó en su libreta azul. En aquellas palabras copiadas sin comprender: hipoteca, intereses, embargo. Comprendió con claridad algo que nunca antes se había permitido formular: el barrio no solo había sido un lugar físico. Había sido su primer sistema económico real, su primer modelo de mundo.

Allí había aprendido qué significaba no llegar a fin de mes. Qué significaba el miedo al despido. Qué significaba depender de decisiones tomadas en despachos invisibles. Allí había nacido, sin nombre aún, su deseo de soberanía.

Bob recordaba las tardes desmontando aparatos en su cuarto. Las herramientas heredadas de su padre. La lógica invisible de los circuitos.

Comprendió que su obsesión por abrir sistemas no había sido nunca un juego. Había sido una forma instintiva de resistencia.

—Todo estaba aquí —dijo—. Incluso lo que no entendíamos.

Alice cerró los ojos un instante.

—Lo más injusto es que nadie nos explicó qué era todo esto.

Bob la miró.

—Nadie explica un sistema a quienes solo se supone que deben obedecerlo.

Ese pensamiento cayó entre ellos con un peso sereno, sin rabia. Ya no la necesitaban.

La plaza había cambiado de público, pero no de función. Seguía siendo el escenario donde el barrio respiraba. Seguía acumulando historias sin nombre. Bob tocó levemente el banco con los nudillos, como quien comprueba la solidez de una estructura vieja.

—Este banco nos enseñó más que muchas aulas —dijo.

Alice sonrió.

—Nos enseñó a esperar.

Se quedaron allí hasta que el cielo empezó a oscurecer. El barrio se encendió poco a poco en luces domésticas. Una tras otra. Ventanas como pequeñas pantallas cálidas. Bob pensó en nodos. Alice en hogares. Ambos entendieron que todas las redes nacen de unidades minúsculas, frágiles, conectadas por necesidad.

Antes de irse, Alice sacó una pequeña hoja de papel del bolso. Había dibujado, sin saber muy bien por qué, la palabra que de niños nunca habían oído: Soberanía.

La soltó en la papelera junto al banco. No como abandono, sino como ofrenda silenciosa al sitio donde todo había empezado.

Se levantaron sin prisa.

El barrio quedaba atrás otra vez.

Pero ya no como herida.

Sino como raíz reconocida.

X. Hoy

Hoy la vida de Alice no se parece en nada a lo que imaginó de niña, pero tampoco se parece a lo que le prometieron los folletos universitarios. Vive en un piso luminoso, sin lujos, sin hipotecas que la aten por décadas. No acumula demasiado. Ha aprendido que las cosas pesan más de lo que aparentan, y no solo en kilos.

Enseña economía. Pero no la economía de los manuales cerrados ni la de los gráficos triunfales. Enseña a leer el dinero como un lenguaje político. A entender qué se dice cuando alguien imprime, cuando alguien prohíbe, cuando alguien rescata. Sus clases no prometen certezas; ofrecen preguntas. Algunos alumnos salen confundidos. Otros salen despiertos. Ella sabe que despertar siempre es un proceso incómodo.

Alice ya no habla de Bitcoin como un activo. Habla de él como de un límite ético. Como de una frontera frente a la arbitrariedad. Como de una memoria que no puede ser reescrita por decreto. No todos están de acuerdo. Ella tampoco busca consenso. Busca honestidad intelectual.

Aprendió a vivir con la sospecha como herramienta, no como condena. Consulta varias fuentes. Desconfía de los titulares. No comparte datos porque sí. Su libertad ya no es una consigna: es un conjunto de hábitos discretos que nadie aplaude, pero que nadie puede arrebatarle sin que ella lo sepa.

Bob vive en otra geografía, no tanto física como técnica. Trabaja con gente que nunca ha visto en persona. Sus reuniones ocurren en husos horarios imposibles. Sus compañeros tienen nombres que a veces no son nombres. A nadie le importa demasiado. Lo único que importa es que el código funcione... y que nadie lo domine.

Rechazó trabajos muy bien pagados. Ofertas que implicaban vigilancia masiva, control de datos, puertas traseras. Le costó decidirlo. El dinero aún tira. Siempre tira. Pero Bob ha aprendido a hacerse una pregunta simple antes de aceptar cualquier proyecto:

—¿Esto encierra o abre?

Esa pregunta lo ha dejado solo más de una vez. Pero también lo ha llevado a colaborar en sistemas que resisten apagones, censuras, presiones estatales. Sistemas lentos. Pesados. Incómodos. Justamente por eso, duraderos.

Bob ya no busca eficiencia pura. Busca resiliencia. Quiere que las cosas sigan funcionando cuando nadie esté mirando. Cuando nadie mande. Cuando los centros caigan.

Ambos se ven con menos frecuencia que antes. La vida adulta dispersa. Pero cuando se encuentran, lo esencial sigue intacto. Hablan menos de Bitcoin que antes. No porque les importe menos, sino porque ya no necesitan justificarlo. Hablan de tiempo. De desgaste. De cómo sostenerse sin endurecerse.

Alice observa las nuevas formas de control con una mezcla de lucidez y preocupación: pagos programables, identidades digitales obligatorias, monedas estatales con fecha de caducidad. Ve cómo muchas de esas tecnologías se presentan como innovaciones neutrales. Reconoce el mismo patrón de siempre: comodidad a cambio de obediencia.

Bob ve lo mismo desde la infraestructura. Capas cada vez más profundas de centralización maquilladas de nube. Dependencias invisibles. Fallos sistémicos disfrazados de eficiencia.

Ambos saben que el mundo no ha elegido todavía. Que se mueve entre dos fuerzas opuestas: la soberanía distribuida y el control total. Que nada está ganado.

No son millonarios. No aparecen en listas. No dan conferencias multitudinarias. No figuran en enciclopedias. Pero pagan su tiempo con su propio tiempo. Nadie puede congelarles una cuenta por orden administrativa. Nadie puede borrar su pasado financiero. Nadie puede decidir por ellos qué se considera valor.

Eso no los hace invulnerables. Los hace responsables.

Una tarde cualquiera, mientras caminan por una calle tranquila, Alice se detiene ante un escaparate lleno de objetos brillantes, de consumo rápido, de promesas instantáneas.

—Todo esto está diseñado para que olvidemos —dice.

Bob asiente.

—Pero no todos olvidamos ya igual de fácil.

Alice sonríe.

—Eso también es una forma de riqueza.

Bob la mira.

—La única que no se devalúa con una firma.

Caminan. No como quienes han llegado a ningún lugar definitivo, sino como quienes han aprendido a elegir cada paso.

Hoy no son héroes. No son mártires. No son predicadores.

Son, simplemente, dos personas que ya no necesitan permiso para existir en términos económicos, técnicos y vitales.

Y eso, en este tiempo, es una forma silenciosa de revolución.

XI. El banco oxidado

Volvieron a encontrarse una tarde cualquiera, sin motivo especial, sin fechas que justificar. Bob había venido por trabajo. Alice tenía unos días libres. Se llamaron casi por inercia, como quien mantiene un viejo ritual sin necesidad de explicarlo.

La plaza estaba casi vacía. Algunas hojas secas giraban arrastradas por el viento. El eco de un balón llegaba desde otra calle, amortiguado. El banco seguía allí. Más oxidado. Más inclinado. Más sincero.

Durante unos minutos no hablaron. Miraban la plaza como si fuese una fotografía viva de algo que ya no existía del todo. Alice pensaba en su libreta azul. Bob en los tornillos sueltos de su infancia.

—Antes este banco era el futuro —dijo Bob al fin.

Alice sonrió levemente.

—Y ahora es la prueba de que sobrevivimos a lo que creíamos que nos definiría.

Bob pasó la mano por el respaldo del banco.

—Aquí aprendimos a esperar sin saber qué esperábamos.

Alice respondió:

—Y a desconfiar sin tener todavía razones.

Se miraron. Ambos sabían cuántas capas de tiempo había en esas frases.

Bob sacó el móvil del bolsillo, lo miró unos segundos, lo guardó sin hacer nada con él.

—Podría pagar un café con esto —dijo—. Con satoshis. Aquí mismo.

Alice negó con la cabeza.

—No aún. No todo tiene que ser ahora.

Bob aceptó el silencio.

—¿Te acuerdas cuando pensábamos que ser libres era no tener jefe?

Alice rió, suave.

—Ahora sabemos que el jefe más difícil de desmontar es el sistema invisible.

—Y el más difícil de vencer es el miedo heredado.

El cielo empezaba a cambiar de color. Un naranja sucio se filtraba entre los bloques.

Alice habló sin mirar a Bob.

—A veces me pregunto qué habría sido de nosotros si no hubiéramos encontrado aquello.

Bob tardó en responder.

—Habríamos sido adultos funcionales. Cansados. Adaptados.

—Como tantos —añadió Alice.

Bob la miró entonces.

—Pero no habríamos sido nosotros.

Alice asintió despacio.

—Eso es lo único que Bitcoin no puede minar por nosotros.

Sostuvieron la mirada. No había emoción desbordada, solo una comprensión profunda, serena. La clase de entendimiento que no necesita celebración.

—Nunca nos hicimos ricos —dijo Bob.

Alice respondió sin ironía:

—Pero nunca volvimos a ser pobres de criterio.

Bob soltó una risa breve.

—Esa sí que es una reserva de valor.

El viento movió unas bolsas olvidadas en un rincón de la plaza. Las luces de algunas ventanas se encendieron. El barrio entraba, como siempre, en su turno nocturno.

Se levantaron casi al mismo tiempo. No por prisa. Por ritmo compartido.

Alice tocó el banco con la punta de los dedos antes de irse.

—Este sitio no sabía lo que nos estaba dando.

Bob respondió:

—Los sistemas nunca saben qué están creando.

Caminaron unos metros juntos. Luego se separaron en la esquina, como tantas veces. Sin dramatismo. Con la tranquilidad de quienes no necesitan asegurarse de que el vínculo existe.

El banco quedó atrás, quieto, incompleto, oxidado.

Pero ya no era solo un objeto.

Era una prueba.

XII. Alice y Bob

Alice y Bob nunca salieron en las noticias. No encabezaron ninguna revolución. No fundaron imperios ni cayeron en desgracia pública. Sus nombres no fueron tendencia ni motivo de denuncias oficiales. Y, sin embargo, cambiaron algo mucho más difícil de registrar: el lugar desde el que miraban el mundo.

De niños aprendieron a esperar en un banco oxidado. De adultos aprendieron a no delegar. Entre ambas cosas transcurrió su vida entera.

Bitcoin no les dio certezas. Les dio límites. Y comprendieron que un límite justo puede ser más liberador que una promesa infinita. Les enseñó que la soberanía no es un derecho que se reclama, sino una práctica que se sostiene a diario. Les mostró que la confianza puede existir sin rostro, que el valor puede existir sin permiso, que la memoria puede existir sin dueño.

No se hicieron ricos en el sentido que celebran las portadas. No compraron mansiones ni coleccionaron símbolos de éxito. Su riqueza fue menos espectacular y más resistente: tiempo sin deuda, decisiones sin tutela, futuro sin firma obligatoria.

Alice siguió enseñando a leer entre líneas. Bob siguió construyendo sistemas que nadie controla por completo. Ninguno de los dos pretendió salvar a nadie.

Habían aprendido que la libertad no se exporta como un producto terminado. Solo puede descubrirse desde dentro.

A veces, sin saber por qué, Alice recordaba la primera vez que escribió la palabra libertad en su libreta. A veces Bob recordaba la primera radio que consiguió hacer funcionar. Comprendían entonces que nada había sido casual. Que toda búsqueda empieza mucho antes de tener nombre.

El mundo siguió su curso: nuevas crisis, nuevas monedas, nuevas promesas de estabilidad. El ruido aumentó. El control se hizo más sutil. Las pantallas se multiplicaron. Pero en medio de esa aceleración, ellos conservaron algo que no suele figurar en los balances: la capacidad de decir no sin pedir disculpas.

Nunca pensaron en sí mismos como ejemplo. Nunca escribieron manuales. Nunca señalaron caminos. Simplemente caminaron.

Y al hacerlo demostraron algo sencillo, incómodo y profundamente político:

Que la obediencia no es una ley natural.

Que el dinero puede dejar de ser una jaula.

Que la tecnología puede nacer sin amo.

Que la libertad no llega en forma de victoria, sino de responsabilidad.

Alguna tarde cualquiera, cuando ya nadie recuerde sus nombres, quizá un niño se sentará en aquel banco oxidado. Quizá desmontará un juguete. Quizá escribirá una palabra que todavía no entiende. Quizá hará una pregunta de más.

Y sin saberlo, la historia volverá a comenzar.

Porque los sistemas cambian.

Las generaciones pasan.

Pero la búsqueda de soberanía siempre encuentra de nuevo algún lugar donde sentarse a empezar.


Listened.

BITCOIN COMO PROTOCOLO DE PAZ

Bitcoin como Protocolo de Paz: Arquitectura de consenso para soberanía digital y justicia descentralizada.

Autor: Tomás Prieto Moraleda (Jurista y especialista en Conflictología)
rcjat@proton.me

Bitcoin y Economía. Política Monetaria y Soberanía

Este artículo obtuvo el 2º Premio del Concurso IFEB Piensa 2025.

Resumen:

El presente ensayo propone una lectura del protocolo **Bitcoin** como arquitectura pacificadora dentro del nuevo paradigma tecnológico de la **descentralización**. Partiendo de la "**Paradoja Moral de Bitcoin** formulada por **Jason Lowery** (2023) **[1]**", se plantea que Bitcoin transforma el modo en que la humanidad gestiona el conflicto por la riqueza y el poder. Frente a los modelos estatales tradicionales, que protegen la soberanía monetaria mediante estructuras **coercitivas** (ejércitos, control monetario centralizado), Bitcoin introduce un sistema programado de incentivos algorítmicos basado en **prueba de trabajo** (PoW), **teoría de juegos** y **transparencia computacional**. A través de un análisis multidisciplinar —filosófico, jurídico, conflictológico y tecnológico—, se sostiene que Bitcoin puede entenderse como un protocolo de paz en el sentido kantiano y galtungniano, al sustituir estructuras de dominación por sistemas **consensuales** de gobernanza digital. El trabajo contextualiza este nuevo orden lex criptográfica dentro del marco de los sistemas **ODR [2]** (Online Dispute Resolutions) y explora su convergencia con la **mediación sistémica** y el equilibrio de Nash. Asimismo, se discute el impacto geopolítico de Bitcoin como catalizador de nuevas formas de **soberanía monetaria**, su incidencia en la estructura financiera internacional y sus potenciales limitaciones. Finalmente, se concluye que el protocolo Bitcoin, más allá de ser una herramienta monetaria, representa un cambio civilizatorio con implicaciones profundas en la **paz**, la **justicia** y el diseño institucional del siglo XXI.

Palabras clave

- **Español**: resolución de conflictos en línea; gobernanza descentralizada; paz positiva; soberanía monetaria; inclusión financiera; no violencia.
- **English**: online dispute resolution (ODR); decentralized governance; positive peace; monetary sovereignty; financial inclusion; nonviolence.

Introducción

En un mundo cada vez más interconectado y digital, los sistemas tradicionales de organización social y económica comienzan a mostrar signos de agotamiento. Las instituciones estatales enfrentan una crisis de legitimidad; el sistema financiero global padece una pérdida progresiva de confianza; y la justicia, entendida como garante último de los derechos, aparece desbordada, burocratizada y lenta. En este contexto emerge **Bitcoin**: no sólo como una criptomoneda, sino como una propuesta ontológica y epistemológica que desafía cimientos fundamentales de la modernidad.

La hipótesis central de este trabajo es que Bitcoin no debe entenderse exclusivamente como un activo financiero o una innovación tecnológica, sino como un **protocolo de paz**. Esto significa concebir su arquitectura de **consenso** como un mecanismo de resolución y prevención de conflictos en el ámbito económico y, por extensión, político. Bitcoin **[3]** surge no solo como una innovación técnica, sino también como una respuesta a conflictos históricos en sistemas monetarios marcados por la manipulación, la centralización del poder y la falta de confianza. Su diseño fundamental resuelve estos conflictos a través de mecanismos criptográficos y consenso distribuido, creando un entorno donde la **paz económica** se mantiene por medio del código y de incentivos alineados.

Las ideas de paz han sido abordadas desde diversas perspectivas filosóficas y sociales. Immanuel **Kant [4]** (1795/2006) postuló que la paz duradera solo sería posible mediante un sistema de repúblicas regidas por el derecho y la libertad, en lugar de la mera ausencia temporal de guerra. Johan **Galtung [5]** (1996) distinguió entre paz negativa (ausencia de violencia directa) y paz positiva (presencia de justicia estructural y armonía social), enfatizando que la verdadera paz exige eliminar las causas de la violencia estructural (desigualdad, dominación, represión). John Paul **Lederach [6]** (2003), desde la conflictología, defendió la importancia de la mediación sistémica y los “diálogos improbables” para transformar pacíficamente los conflictos, creando contextos en que las partes construyan acuerdos sostenibles basados en empatía y propósito compartido.

Estas visiones tradicionales de la paz encuentran ecos en el funcionamiento de Bitcoin: un sistema autónomo y descentralizado que propone un nuevo marco donde la estabilidad y la cooperación global pueden fortalecerse sin recurrir a la violencia ni a la coerción.

A la luz de estas teorías, Bitcoin puede concebirse como un protocolo pacificador. Por un lado, refleja la visión kantiana de una paz perpetua a través de estructuras programáticas que limitan la arbitrariedad y promueven la autonomía individual en la esfera monetaria. Por otro, encarna la paz positiva de Galtung al eliminar una fuente de violencia estructural —el monopolio coercitivo sobre el dinero— devolviendo a los individuos control soberano sobre su patrimonio digital. De igual modo, Bitcoin resuena con la filosofía de la no violencia de **Gandhi [7]** y otros pacifistas, ya que busca transformar la lucha por los recursos (dinero) en cooperación voluntaria protegida por código. En última instancia, la emergencia de Bitcoin apunta a un nuevo paradigma normativo que algunos autores denominan Lex Criptográfica, un sistema de reglas descentralizado donde "el código es ley" (Lessig, 2006) **[8]**. Este marco regula las interacciones económicas en el ciberespacio no mediante el uso de la fuerza o la autoridad central, sino a través de algoritmos y consensos verificables por todos.

En las siguientes secciones se examinará cómo Bitcoin implementa principios de resolución de conflictos similares a los de los sistemas **ODR [9]** (Online Dispute Resolutions), creando una arquitectura de justicia digital sin intermediarios. Se analizará su capacidad para desafiar pacíficamente los monopolios tradicionales de poder (la violencia estatal, la emisión monetaria y la centralización institucional) y las implicaciones de este desafío para la paz sistémica global. Finalmente, se discutirán las limitaciones y desafíos que enfrenta Bitcoin en su aspiración pacificadora, antes de presentar las conclusiones del estudio.

Metodología

Este estudio emplea una metodología **cualitativa** y **multidisciplinar** basada en el análisis teórico-conceptual y la comparación de sistemas. En primera instancia, se realiza una **revisión bibliográfica** de las teorías clásicas de la paz y la resolución de conflictos (Kant, Galtung, Lederach, entre otros) y de aportes contemporáneos sobre seguridad y tecnología en el protocolo de Bitcoin (como la tesis de Lowery, 2023), con el fin de establecer un **marco teórico** sólido. Sobre esta base teórica, se procede a **analizar** el funcionamiento del este protocolo a través de la lente de los **ODR (online dispute resolutions)** y de la emergente Lex Criptográfica.

Se compara el modelo de gobernanza algorítmica de Bitcoin con los sistemas tradicionales de resolución de disputas en línea y con las estructuras jurídicas estatales, identificando **similitudes** y **diferencias** en cuanto a cómo se previenen o resuelven conflictos.

El enfoque es principalmente **analítico-descriptivo**. Se examinan las características técnicas y sociales de Bitcoin (descentralización, transparencia, mecanismo de consenso, sistema de incentivos) y se interpretan en términos de prevención de conflictos y construcción de paz. Para ello, se emplea la **teoría de juegos** (equilibrio de Nash) como herramienta analítica que ayuda a explicar el comportamiento cooperativo inducido por el protocolo. Asimismo, se consideran datos e informes relevantes (por ejemplo, sobre consumo energético, inclusión financiera, costos de transacción) para contextualizar empíricamente la discusión, utilizando casos ilustrativos cuando es pertinente (p.ej., adopción de Bitcoin en economías con alta inflación o escasa bancarización).

En síntesis, el Ensayo se estructura en tres grandes fases analíticas: (1) fundamentación teórica y conceptual de la noción de "Bitcoin como protocolo de paz"; (2) análisis del **diseño institucional** de Bitcoin como sistema de **resolución descentralizada de disputas** y sus impactos en los monopolios tradicionales de poder; y (3) evaluación crítica de las **limitaciones, paradojas y desafíos** que enfrenta Bitcoin para consolidarse como arquitectura de paz. Este recorrido metodológico, que integra perspectivas filosóficas, jurídicas, económicas y tecnológicas, permite evaluar de forma comprehensiva el potencial pacificador de Bitcoin y sentar bases para futuras investigaciones en la materia.

Resultados

Bitcoin como sistema de resolución descentralizada de conflictos (ODR algorítmico)

Los sistemas **ODR (Online Dispute Resolutions)** son mecanismos sociotécnicos diseñados para resolver disputas en línea sin recurrir a tribunales tradicionales. Su valor radica en lograr consenso sin autoridad central, apelando a la eficiencia, la transparencia y la inmutabilidad (Katsh & Rifkin, 2001). El protocolo Bitcoin, aunque concebido originalmente como sistema monetario, **cumple funcionalmente con muchas premisas de un ODR**: establece reglas consensuadas, ejecutadas por código, verificadas por pares globalmente y resistentes a la manipulación.

En lugar de jueces o mediadores humanos, es la red distribuida de nodos la que valida y reconcilia las transacciones, actuando como un "árbitro" algorítmico.

Bitcoin puede analizarse, así como una **arquitectura de gobernanza algorítmica** para la **resolución de disputas monetarias**. Su estructura técnica—basada en la cadena de bloques, la criptografía de clave pública y la minería competitiva PoW **[10]** — garantiza que los actores involucrados (usuarios, nodos, mineros, desarrolladores) interactúen en un entorno donde el conflicto potencial es absorbido y transformado por el propio diseño del sistema, (reglas y decisiones codificas y ejecutas en el software). Cada bloque minado representa una validación colectiva de transacciones previas, selladas criptográficamente y aceptadas por consenso de la mayoría (Roubini N. 2019). Este modelo **previene disputas ex ante: las posibilidades de desacuerdo o fraude** (por ejemplo, el doble gasto de una moneda) **se reducen drásticamente**, pues el protocolo no permite registrar transacciones incompatibles con su historial inmutable. En términos prácticos, **Bitcoin disminuye la litigiosidad inherente a los sistemas financieros tradicionales, donde a menudo surgen conflictos por arbitrariedad humana, opacidad contractual o cambios unilaterales de condiciones.**

Un aspecto central en este ODR descentralizado es la eliminación de la necesidad de confianza en intermediarios. Siguiendo el lema Cypherpunk "Don't trust, verify", Bitcoin sustituye la confianza interpersonal o institucional por **verificación matemática**. Todos los participantes pueden comprobar por sí mismos las reglas y el estado de la contabilidad común, sin depender de promesas de terceros. Esto confiere al sistema un carácter neutral y objetivo muy distinto al de los mecanismos tradicionales de resolución de conflictos, donde las partes deben confiar en la imparcialidad de un mediador (corruptible) o en la ejecución de un fallo jurisdiccional, que aún favorable siempre llega tarde.

Desde la perspectiva de la Lex Criptográfica, Bitcoin inaugura un **nuevo corpus normativo digital** en el que la regulación del comportamiento (en este caso, las transferencias de valor) se logra mediante la arquitectura misma del sistema. Como anticipó Lawrence Lessig, "el código es ley" en el ciberespacio (Lessig, 2006), y el código de Bitcoin establece condiciones estructurales que hacen impracticables la corrupción, la coacción o el engaño en las transacciones económicas ordinarias. En este sentido, las normas contenidas en el protocolo Bitcoin operan como una Lex Mercatoria contemporánea del mundo digital: reglas autónomas que permiten intercambios pacíficos de valor a escala global.

Es útil contrastar a Bitcoin con ODR clásicos para apreciar sus ventajas únicas. **Tabla 1** resume comparativamente las diferencias fundamentales:

Tabla 1. Comparativa entre ODR tradicional y el consenso de Bitcoin. Fuente propia 2025.

Aspecto	**ODR tradicional (sistemas ODR clásicos)**	**Bitcoin (Consenso blockchain descentralizado)**
Naturaleza del conflicto	Disputas surgidas a posteriori (e.g., conflictos contractuales en e-commerce) que requieren mediación o arbitraje.	Conflictos potenciales ex ante (e.g., doble gasto, validez de transacciones) prevenidos por el diseño del protocolo.
Rol del mediador/ arbitraje	Intervención de terceros neutrales (humanos o cortes) o plataformas centralizadas para proponer/acordar soluciones.	Sin mediador central: las reglas criptográficas y la red de nodos validadores actúan como árbitro automático e incorruptible.
Proceso de resolución	Negociación, mediación o arbitraje en línea; posible intervención humana, acuerdos entre partes o laudos ejecutables.	Consenso programado: Prueba de trabajo y verificación distribuida que aceptan o rechazan transacciones/ bloques según reglas fijas.
Enfoque temporal	Reactivo: actúa después de surgido el conflicto, buscando resolverlo eficientemente.	Preventivo: diseña incentivos para que el conflicto no ocurra (ej. es inviable gastar dos veces la misma moneda).
Transparencia y confianza	La transparencia depende del diseño de la plataforma ODR; puede haber confianza depositada en la entidad administradora.	Transparencia radical: libro mayor público e inmutable; “no confiar, verificar” – cualquier participante puede auditar todo el historial.
Ejemplos	Plataformas ODR como eBay Resolutions Center, sistemas descentralizados tipo Kleros (jurados online) para disputas en contratos inteligentes.	Red Bitcoin como sistema autoejecutado: previene disputas sobre propiedad/valor al definir y consensuar objetivamente un único historial de transacciones válido.

Como muestra la tabla, una diferencia clave es que mientras los ODR tradicionales buscan **resolver conflictos tras su aparición**, Bitcoin busca **evitar** que surjan muchos conflictos financieros, estructurando de antemano un sistema de reglas claras y acuerdos automatizados. Además, la resistencia a la censura y la ausencia de jerarquías en Bitcoin le otorgan una resiliencia institucional sin precedentes: no existe un punto único de falla ni riesgo de captura por parte de una autoridad. En suma, el protocolo es su propio árbitro y tribunal, lo que constituye la esencia de su potencial transformador en materia de justicia y paz digital, (justicia autocompositiva descentralizada).

Mecanismos de consenso, teoría de juegos y no violencia programada

El **consenso distribuido** en Bitcoin se mantiene gracias a una estructura de incentivos cuidadosamente diseñada, creando un equilibrio cooperativo entre participantes originalmente egoístas. Este diseño puede entenderse en términos de **teoría de juegos**: la red Bitcoin configura un **equilibrio de Nash** en el cual la estrategia dominante para todos los actores es cumplir las reglas honestamente. Los mineros compiten por obtener recompensas de bloque, pero dicha competencia ocurre dentro de parámetros predeterminados por el protocolo. Cualquier intento de desviarse de las reglas (por ejemplo, incluyendo transacciones no válidas o tratando de duplicar un pago) conllevaría casi con total certeza una pérdida económica para el infractor: desperdicio de energía y tiempo de cómputo sin recompensa y riesgo de que sus bloques sean rechazados por la mayoría. En consecuencia, **la opción racional óptima es cooperar** con el protocolo. La racionalidad individual (buscar maximizar el beneficio propio) queda alineada con el bien colectivo (seguridad y veracidad de la cadena) mediante incentivos económicos y criptográficos, logrando que el consenso se sostenga sin necesidad de coerción externa.

Este mecanismo refleja una forma de no violencia programada: Bitcoin desalienta activamente el comportamiento deshonesto o agresivo (como ataques a la red) haciendo que dichos actos no sean rentables. **La prueba de trabajo** (PoW) implementa una forma de resistencia pacífica contra ataques al sistema monetario: en lugar de desplegar fuerza militar o violencia para proteger la integridad del dinero, Bitcoin "responde" a los posibles atacantes con un muro computacional costoso de superar, pero enteramente **defensivo**. Lowery (2023) destaca esta paradoja moral: mientras los Estados modernos gastan un 2-3% de su PIB en ejércitos y aparato coercitivo para resguardar su riqueza nacional, Bitcoin asegura un sistema monetario global con aproximadamente **0,1% del consumo energético mundial**, sin incurrir en

costo humano directo. En palabras del propio Lowery, “hemos reemplazado el coste humano por el recibo de la luz”. Así, la energía eléctrica y el cómputo reemplazan, en buena medida, a la pólvora y los soldados como garantes de la seguridad patrimonial. Aunque el consumo energético de Bitcoin es significativo, su naturaleza es fundamentalmente d**efensiva y pacífica**, alineándose con el principio de “no violencia” de Gandhi. La aparente contradicción de gastar tanta energía para la paz se resuelve al comprender que este gasto computacional constituye un **mecanismo ético de sustitución de la violencia por cálculo**: es un precio pagado en electricidad para evitar un precio mucho mayor pagado en sangre y conflicto armado (Lowery, 2023).

Cabe mencionar que, según algunos análisis comparativos, el consumo energético anual de Bitcoin (estimado cerca de 114 TWh) es inferior a la mitad del consumo combinado de la industria bancaria global y la del oro. En efecto, un informe de **Galaxy Digital (2021) [11]** calculó que los sistemas bancarios tradicionales consumen del orden de 240 TWh al año en infraestructura, centros de datos, sucursales y ATMs, mientras que la minería de oro consume alrededor de 240 TWh también, ambos valores muy superiores al de la red Bitcoin. Si bien estas comparaciones tienen limitaciones, sirven para contextualizar el debate: la **paz estructural** que Bitcoin promete tal vez justifica su gasto energético si con ello reduce la necesidad de gastos bélicos o la dependencia en sistemas financieros opacos. En cualquier caso, la transición de la minería Bitcoin hacia fuentes de energía renovable y eficientes será clave para sostener en el tiempo la legitimidad moral de este protocolo como herramienta de paz sostenible, algo que ya está ocurriendo.

Bitcoin y la paz estructural: Desafiando monopolios de poder

Si entendemos la paz positiva como aquella que elimina la violencia estructural (Galtung, 1996), entonces Bitcoin exhibe un poderoso potencial de paz estructural al desafiar pacíficamente tres **monopolios tradicionales** cuya concentración de poder ha sido fuente histórica de conflictos y desigualdades. Estos son: (1) el monopolio de la violencia física legítima por parte del Estado, (2) el monopolio de la emisión monetaria y política monetaria, y (3) la centralización de las instituciones y la autoridad en la toma de decisiones colectivas. A continuación, se analiza cada uno de estos ejes:

1. Desafío al monopolio estatal de la violencia

El sociólogo Max Weber definió el Estado moderno por su **monopolio legítimo de la violencia física**. En el ámbito monetario, este monopolio se manifiesta en que la protección de la riqueza nacional y la imposición de un orden económico se garantizan, en

última instancia, mediante **fuerza coercitiva** (leyes, policías, ejércitos). Bitcoin representa la primera alternativa viable a ese paradigma tradicional de seguridad basada en la fuerza. Su red consigue un entorno seguro para las transacciones **sin recurrir a la coerción física** en absoluto. Cada transacción en Bitcoin se verifica y asegura mediante criptografía y consenso voluntario, no mediante policías o amenazas de fuerza. Esto significa que **100% de las transacciones** en la red Bitcoin son **pacíficas por diseño**: no requieren que ninguna autoridad confíe en la violencia para su cumplimiento.

En Bitcoin, la **seguridad programática** sustituye a la seguridad armada (Lowery J. 2023). La integridad del sistema no depende de agentes armados que impongan sanciones, sino de garantías criptográficas y reglas autoejecutables. Si bien la red debe defenderse de posibles ataques (doble gasto, ataques del 51%, etc.), su enfoque es **no violento**: la **prueba de trabajo** hace que cualquier ataque requiera tal cantidad de esfuerzo computacional y gasto energético que actúa como **barrera disuasoria**, un equivalente digital de las murallas defensivas, pero sin **contraatacar activamente**. Esta forma de **defensa pasiva** encaja con la noción de **"arma de disuasión pacífica"**: Bitcoin resiste agresiones no mediante violencia contra el agresor, sino volviéndose tecnológicamente inexpugnable.

Además, Bitcoin elimina la **intermediación forzosa [12]** en las transacciones económicas. En el sistema tradicional, para transferir valor se depende de bancos centrales, bancos comerciales y otros intermediarios respaldados en última instancia por la potestad coercitiva del Estado. La red Bitcoin permite transacciones **peer-to-peer** sin intermediarios, de modo que ningún actor puede forzarse en medio de una transacción ni extraer coactivamente valor (por ejemplo, mediante confiscaciones o bloqueos de cuentas arbitrarios). En suma, Bitcoin supone una suerte de secesión monetaria pacífica: individuos y comunidades pueden **ejercer soberanía monetaria** (Radziwill A.M. 2015) al margen del monopolio estatal, sin necesidad de insurrección violenta, simplemente adoptando un protocolo alternativo.

1. Ruptura del monopolio de emisión monetaria

El control estatal (o de bancos centrales autónomos) sobre la **emisión de dinero** ha sido fuente de enorme poder político y, a la vez, de conflictos socioeconómicos. La capacidad de emitir moneda fiduciaria y gestionar la política monetaria permite a Estados y élites financieras influir en la distribución de riqueza, a veces de forma arbitraria o en beneficio propio, generando **desigualdad sistémica** e **inflación** que erosiona la paz social y crea pobreza estructural.

Bitcoin rompe radicalmente con este monopolio al introducir una emisión monetaria **descentralizada, programática y predecible**. Sus reglas de creación de nuevos bitcoins (emisión limitadamente decreciente, corte a la mitad cada cuatro años, tope final de 21 millones) están **predefinidas en el código** y no pueden ser alteradas por ningún actor particular, por poderoso que sea.

Esta **emisión programática** elimina la arbitrariedad en la creación de dinero: no hay posibilidad de "imprimir" más monedas según conveniencias políticas de corto plazo. La **transparencia total** de la política monetaria de Bitcoin (cualquiera puede verificar en tiempo real cuántos bitcoins existen y la tasa exacta de emisión) contrasta con la opacidad o complejidad de los mecanismos de los bancos centrales. Al no depender de la confianza en autoridades monetarias, se reduce un potencial foco de conflicto: **la sospecha permanente sobre manipulación, corrupción o incompetencia en la gestión del dinero.**

En términos de **paz positiva**, esta democratización monetaria devuelve equidad al sistema: todos los participantes acceden en igualdad de condiciones a las reglas monetarias, sin privilegios de emisión para unos pocos. Se promueve así una cierta **justicia económica** (equidad programática), donde la estabilidad del valor no depende de la buena fe de terceros, sino de un contrato social codificado y autoejecutable. Al impedir la inflación descontrolada y la devaluación arbitraria (fenómenos que históricamente han detonado malestar social y violencia), Bitcoin ataca las raíces de un tipo de violencia estructural financiera, fomentando la **confianza** en el sistema económico de un modo novedoso.

1. Descentralización institucional y autonomía comunitaria

El tercer gran monopolio que Bitcoin desafía es el de la **institucionalidad centralizada**. En las estructuras políticas y económicas actuales, la toma de decisiones y la administración de justicia suelen estar concentradas en **instituciones jerárquicas** (gobiernos, organismos internacionales, grandes corporaciones financieras). Esta centralización crea puntos únicos de fallo y abre la puerta a abusos de poder, corrupción o captura institucional por intereses particulares, lo que erosiona la paz y la justicia ciudadanas. Bitcoin **[13]** cuestiona la necesidad de dicha centralización institucional al demostrar que es posible coordinar a millones de personas en torno a reglas comunes **sin una autoridad central** de mando. Su **gobernanza distribuida** –basada en el consenso comunitario de desarrolladores, mineros, nodos y usuarios– es un experimento inédito de toma de decisiones colectiva transparente y abierta.

En Bitcoin no existe un consejo directivo, un CEO ni una "cabeza" que pueda ser coaccionada o corrompida para cambiar las reglas en favor de alguien. Cualquier cambio significativo en el protocolo requiere una **adhesión masiva** de la comunidad, lo que en la práctica garantiza una gran estabilidad de las normas fundamentales (y a la vez dificulta cambios no consensuados ampliamente). Este modelo de consenso social-tecnológico produce una **resistencia a la captura institucional**: es extremadamente difícil que un grupo minoritario imponga modificaciones nocivas al protocolo sin perder legitimidad y usuarios. En términos de paz, la eliminación de puntos únicos de fallo (por ejemplo, ya no hay un banco central cuya mala praxis afecte a todos, ni un organismo único que pueda "caer" y derrumbar el sistema) fortalece la resiliencia y minimiza las posibilidades de colapso repentino o crisis inducidas por decisiones centralizadas erróneas.

La **auditoría pública constante** es otro aspecto: al ser la blockchain completamente pública y verificable, existe una transparencia radical que previene la corrupción y la manipulación escondida. Ninguna transacción ni emisión monetaria pasa desapercibida, a diferencia de sistemas estatales donde a menudo hay poca rendición de cuentas. Por último, la **autonomía comunitaria** se ve potenciada: grupos y ciudadanos pueden apoyarse en Bitcoin para construir economías locales o redes de intercambio sin esperar permiso de autoridades, lo cual empodera a la sociedad civil y reduce la dependencia de aparatos estatales potencialmente coercitivos o fallidos (**Lunaticoin & Contreras**, 2024) **[14]**. En un escenario hipotético, incluso se podría reimaginar la función tributaria y de provisión de bienes públicos sin recurrir a la coacción fiscal tradicional, mediante modelos voluntarios y automatizados basados en criptoactivos, eliminando así una fuente de fricción coercitiva entre ciudadanos y Estado.

En conjunto, estos tres desafíos constituyen una **"ruptura pacífica"** de monopolios que parecían incuestionables. Bitcoin actúa como **tecnología de transformación social** al ofrecer alternativas no violentas a estructuras de poder que históricamente han originado conflictividad: **sustituye ejércitos por algoritmos, bancos centrales por código transparente, y jerarquías por redes distribuidas**. Las implicaciones para la **paz global** de esta triple ruptura son profundas, como se resume en la **Tabla 2** a continuación:

Tabla 2. Monopolios tradicionales vs. enfoque de Bitcoin e implicaciones para la paz. Fuente propia 2025.

Monopolio tradicional (fuente de conflicto)	**Enfoque de Bitcoin (alternativa descentralizada)**	**Implicaciones para la paz**
Violencia y seguridad estatal (protección de riqueza mediante fuerzas armadas; coerción legal).	Seguridad programática distribuida (red Bitcoin asegura valor con minería PoW y consenso, sin uso de fuerza física).	Reducción de la coerción en la economía; transacciones aseguradas sin violencia. Resistencia pacífica a ataques: la defensa no requiere armamento, solo energía y computación.
Emisión monetaria centralizada (bancos centrales con poder de imprimir dinero, generar inflación o devaluación).	Emisión descentralizada y predefinida (política monetaria fija en el código: emisión limitada, previsible y transparente).	Eliminación de la arbitrariedad en la política monetaria; se evitan conflictos por manipulación financiera. Mayor estabilidad y confianza; se reduce la "violencia estructural" de la inflación sobre poblaciones vulnerables.
Institucionalidad jerárquica (autoridades centralizadas que deciden y administran justicia; riesgo de corrupción y abuso).	Gobernanza distribuida en la red (decisiones por consenso comunitario; reglas ejecutadas por nodos, sin jerarquía central).	Gobernanza distribuida en la red (decisiones por consenso comunitario; reglas ejecutadas por nodos, sin jerarquía central).

Al romper simultáneamente estos tres monopolios del poder tradicional, Bitcoin abre la puerta a una pacificación estructural de las relaciones económicas. Se reducen los conflictos derivados del control monopólico del dinero (guerras de divisas, sanciones económicas unilaterales, expolios inflacionarios), se **elimina** o suaviza cierta violencia institucional sistémica (imposición mediante fuerza) y se previenen abusos de poder centralizados (fiscalidad confiscatoria). En la medida en que adoptemos un sistema donde la confianza se base en leyes matemáticas y consensos voluntarios —y no en la coacción—, nos aproximamos a la visión kantiana de estructuras que hagan posible una paz perpetua.

Mediación sistémica, consenso y prevención de conflictos

Los principios de **mediación sistémica** en la conflictología sostienen que la paz sostenible se construye creando subsistemas sociales que restablezcan equilibrios y canales de comunicación en los conflictos (Lederach, 1998). Bitcoin puede interpretarse como uno de estos subsistemas pacificadores: un espacio de interacción donde millones de participantes coordinan expectativas económicas sin necesidad de una autoridad coercitiva, logrando equilibrios dinámicos. Antonio Tula (2015) **[15]** señala que la paz se logra cuando los sistemas alcanzan un **equilibrio homeostático** mediante consenso, algo análogo a lo que ocurre en la red Bitcoin gracias al mencionado equilibrio de Nash. Cada nuevo bloque minado y aceptado por la mayoría representa un **micro-acuerdo global**: todas las partes (mineros, nodos, usuarios) lo incorporan como verdad compartida, manteniendo el sistema en armonía pese a los intereses individuales divergentes.

Bitcoin incorpora así un modelo de **justicia autocompositiva** (Prieto T. & De la Torre, 2023) **[16]**. en términos legales: las "disputas" sobre la validez de transacciones se resuelven internamente por las propias partes siguiendo reglas preestablecidas, sin intervención externa. Esto se asemeja a la noción de justicia donde las partes en conflicto llegan por sí mismas a la solución (como en mediación), solo que en Bitcoin dicha autocomposición ocurre de forma automática a través de contratos inteligentes. Cada participante acepta las mismas normas y cualquier intento de desviarse es neutralizado por la red, llevando a que el único camino viable sea la cooperación. **Este fenómeno previene activamente la escalada de conflictos**: al no haber discrecionalidad ni discriminación (las reglas son iguales para todos, sin importar quién seas), se eliminan causas comunes de disputa como trato injusto o falta de acceso.

Desde la perspectiva de la **prevención de conflictos**, Bitcoin cumple varios criterios de lo que sería un sistema pacífico por diseño: garantiza reglas equitativas (normas claras y aplicables universalmente), acceso universal (cualquiera con conexión puede participar, no hay barreras excluyentes más que las tecnológicas básicas), ausencia de discriminación (la red no distingue por identidad, origen o estatus), y promueve una especie de **justicia autocompositiva** en la que todas las partes (nodos) contribuyen y acuerdan el estado final de las transacciones Estos atributos reflejan las condiciones que, según la filosofía de paz, reducen la probabilidad de conflictos violentos en sociedades: igualdad ante las normas, inclusión de todos los actores interesados y mecanismos de diálogo/ consenso institucionalizados.

Para valorar el impacto concreto de Bitcoin en la **paz económica**, podemos considerar algunos **indicadores empíricos** emergentes:

- **Reducción de costos de remesas**: Las transferencias internacionales de dinero tradicionalmente tienen comisiones elevadas (promedio global ~6.5%). Con Bitcoin o sus capas (Lightning Network), esos costos pueden bajar a menos del 1%, facilitando un ahorro anual de miles de millones de dólares en comisiones para poblaciones migrantes. Esto implica menos tensiones económicas para familias y comunidades dependientes de remesas, aliviando una fuente de estrés financiero.
- **Protección contra la inflación y crisis monetarias**: En casos documentados como Venezuela, Argentina o Zimbabue, Bitcoin ha servido como reserva de valor para ciudadanos cuyos sistemas monetarios colapsaban por hiperinflación o controles estatales (Gladstein, 2018). La posibilidad de preservar ahorros en BTC en lugar de la moneda local puede prevenir la ruina económica de familias enteras y, potencialmente, la conflictividad social derivada de la pobreza súbita.
- **Inclusión financiera**: Cerca de 1.7 mil millones de personas carecen de acceso a servicios bancarios básicos en el mundo, lo que constituye una forma de violencia estructural (exclusión del sistema económico). Bitcoin, al no requerir permisos ni infraestructura bancaria tradicional (basta un teléfono móvil sencillo), está permitiendo que muchas de esas personas accedan a pagos, ahorros y transferencias globales por primera vez. Por ejemplo, iniciativas comunitarias como Bitcoin Beach en El Salvador, o proyectos educativos como Mi Primer Bitcoin, demuestran que comunidades marginadas pueden construir economías locales más resilientes con esta tecnología. La **inclusión financiera** lograda se correlaciona con mayor estabilidad y paz social, al empoderar a sectores antes vulnerables y reducir la desigualdad de oportunidades.

Estos indicadores sugieren que Bitcoin tiene un **impacto tangible** en reducir ciertas formas de violencia económica: abarata la transferencia de valor (quitando presión a una potencial fuente de conflicto como las remesas costosas), protege patrimonios en entornos volátiles (evitando conflictos asociados a crisis financieras) y trae al sistema a quienes estaban fuera (minimizando la frustración social por exclusión).

En última instancia, Bitcoin está facilitando lo que el activista de derechos humanos Alex Gladstein **[17]** ha llamado "una vía de escape" para individuos bajo regímenes opresivos o sistemas financieros injustos. Al ofrecer una economía paralela global sin censura, donde los ahorros no pueden ser **devaluados ni confiscados arbitrariamente**, el uso de este protocolo **previene la violencia gubernamental** ejercida a través del control financiero (Gladstein, 2018). Desde la adopción legal de Bitcoin en **El Salvador** hasta proyectos rurales en África que permiten acceso a Bitcoin vía SMS (Machankura), se acumulan ejemplos de su efecto pacificador: **reduce la dependencia** de poblaciones vulnerables de estructuras económicas que a menudo las oprimían, devolviéndoles autonomía.

Limitaciones y desafíos para la paz con Bitcoin

A pesar de su evidente potencial como arquitectura de pacificación social, Bitcoin enfrenta importantes **desafíos y limitaciones** que matizan su alcance. Es crucial reconocerlos para no caer en una visión tecnoutópica ingenua y para orientar futuras mejoras. Entre los retos principales destacan:

- **Brecha de acceso y educación**: Aunque Bitcoin es técnicamente abierto a cualquiera, en la práctica **existe una brecha digital** que podría limitar su adopción equitativa. Las poblaciones con bajo acceso a internet, bajo alfabetismo digital o recursos tecnológicos escasos podrían **quedar atrás**. La promesa de soberanía individual a través de Bitcoin podría volverse utópica para los más vulnerables si no se acompañan esfuerzos de **inclusión digital, formación y apropiación comunitaria**. En términos de paz, esto implica que la herramienta más radical para la autonomía podría beneficiar desproporcionadamente a quienes ya tienen cierto nivel educativo o tecnológico, exacerbando desigualdades si no se actúa para democratizar su uso.
- **Sostenibilidad ecológica**: El alto **consumo energético** de la red Bitcoin ha suscitado críticas válidas en torno a su impacto ambiental. Aunque conceptualmente justificable como reemplazo de la violencia (Lowery, 2023), la cuestión permanece: ¿puede la paz costar tanta energía? Si bien estudios recientes indican que una parte creciente de la minería utiliza energía renovable o desperdiciada, y que su huella es menor que la del sistema financiero tradicional, la **percepción pública negativa** persiste. Para que Bitcoin sea aceptado como instrumento de paz, deberá seguir avanzando hacia la **minería sostenible**, demostrando que su costo

- energético es proporcional a los beneficios sociales que ofrece (evitar guerras, evitar colapsos financieros). La transición global hacia energías limpias será un factor decisivo en este frente.
- **Gobernanza y concentración interna**: Aunque Bitcoin se presenta como neutral y descentralizado, no está exento de **dinámicas de poder internas**. Por un lado, la toma de decisiones técnicas recae en la comunidad de desarrolladores y participantes activos, donde existen debates, desacuerdos e incluso divisiones (p.ej., bifurcaciones como Bitcoin Cash nacieron de conflictos ideológicos). Esto muestra que aún en ausencia de una autoridad formal, la comunidad Bitcoin debe gestionar conflictos internos sobre la dirección del protocolo. Por otro lado, hay **riesgos de concentración** en ciertos ámbitos: la concentración de poder de minado en grandes pools, la acumulación de grandes cantidades de BTC en pocas billeteras ("wallets"), o la dependencia de ciertos fabricantes de hardware minero, etc. Estos fenómenos podrían **erosionar la descentralización** real y generar nuevos focos de conflicto o vulnerabilidad (por ejemplo, una alianza de grandes mineros con intereses comunes podría bloquear ciertas decisiones). Afrontar estas cuestiones requiere madurez: la descentralización ha de entenderse como un **proceso continuo de mejora** que exige vigilancia, transparencia y diversidad de participantes para evitar la formación de nuevas élites o monopolios privados dentro del ecosistema.
- **Riesgo de captura ideológica**: Por último, un desafío más sutil pero importante es mantener la **apertura ideológica** del movimiento Bitcoin. La comunidad, aunque diversa, a veces da cabida a corrientes dogmáticas (como el llamado maximalismo Bitcoin) que tienden a una visión excluyente, descalificando cualquier otra innovación o crítica. Una cultura cerrada, sectaria o excesivamente ideologizada podría restarle legitimidad a Bitcoin como herramienta de paz, ya que la paz exige diálogo y apertura al otro, no imposición de un dogma. Para que Bitcoin realmente fomente la paz y el diálogo global, **su comunidad debe resistir su propia radicalización** y promover un espíritu pluralista, crítico y constructivo. Es decir, la arquitectura del protocolo debe ir acompañada de una cultura transpolítica como creadores de un orden emergente: si bien Bitcoin técnicamente elimina coacción, sus usuarios y promotores deben también practicar la tolerancia y la cooperación más allá del código.

En resumen, ninguno de estos desafíos invalida el potencial de Bitcoin como protocolo de paz, pero sí señalan áreas que requieren **atención y desarrollo continuo**. La exclusión digital debe mitigarse con educación e infraestructuras asequibles; el debate energético debe encararse con datos y mejoras técnicas (p.ej., migración a energías renovables, segunda capa de mayor eficiencia); la gobernanza debe mantenerse transparente y multiparte; y la comunidad, autoconsciente y abierta a la autocrítica, alejada de dogmas ideológicos.

Proyecto Deius como Modelo Prospectivo de Resolución de Conflictos en Bitcoin

Aunque todavía no existen casos plenamente implementados de justicia descentralizada sobre Bitcoin, resulta relevante destacar iniciativas pioneras como el proyecto **Deius**, que lidera Julio de la Torre y Francisco T. Prieto. El proyecto Deius propone la creación de una plataforma de resolución de conflictos civiles y mercantiles sobre tecnología Bitcoin, fundamentada en contratos inteligentes y modelos de gobernanza automatizada en capas superiores del protocolo (sidechain). Actualmente, Deius se encuentra en fase de captación de inversores, con su modelo arquitectónico y fundamentos teóricos recogidos en su white paper adjunto en el libro Bitcoin en la Justicia (Prieto FT &. De la Torre J. 2023). Aunque aún no ha sido desplegado como piloto, Deius representa un ejemplo avanzado de cómo aplicar los principios de transparencia, incentivos algorítmicos y ausencia de intermediarios que caracterizan a Bitcoin—**con potencial para transformar la administración de justicia y fomentar prácticas más justas, abiertas y resistentes a la corrupción**. Su mención como caso prospectivo ilustra las posibilidades de desintermediación judicial y empoderamiento ciudadano que abre la tecnología descentralizada, anticipando un futuro en el que las disputas puedan resolverse a través de protocolos de consenso de forma autocompositiva.

Conclusiones

Bitcoin representa una **implementación práctica** de ideales de paz y justicia propuestos por diversos pensadores, trasladados al ámbito tecnológico aún sin ser conscientes. A lo largo de este ensayo hemos argumentado que Bitcoin, lejos de ser únicamente una herramienta financiera o una innovación tecnológica, constituye en esencia un **protocolo de paz estructural**. Su diseño técnico —descentralizado, resistente a la censura, transparente y basado en consenso— **permite resolver de forma algorítmica uno de los grandes focos de conflicto en la historia humana**: el acceso, el control y la distribución de la riqueza.

Puede decirse que Bitcoin integra en su arquitectura principios de distintas visiones clásicas de la paz: realiza la aspiración kantiana de una paz perpetua al crear una suerte de "república monetaria" global regida por leyes universales (el código) en lugar de la fuerza; contribuye a la paz positiva galtungniana al eliminar formas de violencia estructural (censura financiera, inflación arbitraria, exclusión bancaria); encarna la no violencia gandhiana al reemplazar la coerción por resistencia pasiva (Proof of Work como escudo en vez de espada); y ejemplifica la justicia autocompositiva de los modelos ODR al propiciar que las "disputas" económicas se resuelvan por consenso interno de las partes sin necesidad de árbitros externos.

En este sentido, el protocolo **demuestra que la paz económica no requiere coerción**, sino **estructuras** que hagan de la cooperación pacífica la opción más beneficiosa para todos. Bitcoin ofrece un entorno donde la **cooperación voluntaria se alinea con el interés propio**, y donde la confianza emana de la **verificación colectiva y la transparencia radical**, en lugar de la imposición. Es, en palabras del ex-CEO de Twitter **Jack Dorsey [18]**, una herramienta que podría "ayudar a crear la paz mundial", al corregir un nivel fundamental —el sistema monetario— de tal modo que muchas disputas y desigualdades se atenúen desde la base (Dorsey, 2021).

Por supuesto, **queda camino por recorrer** para que el potencial de Bitcoin se despliegue plenamente como instrumento de paz positiva. La comunidad internacional deberá enfrentar las mencionadas limitaciones: cerrar la brecha digital para que la revolución descentralizada sea inclusiva; asegurar que el crecimiento de Bitcoin se realice de forma ecológicamente sostenible; continuar descentralizando y fortaleciendo la gobernanza del protocolo frente a cualquier concentración; y fomentar un discurso abierto y constructivo que evite convertir a Bitcoin en un dogma. **No basta con que la tecnología sea potente si no es accesible, justa y adaptable.**

Para terminar, el surgimiento de Bitcoin nos invita a reimaginar conceptos fundamentales de soberanía, derecho y valor desde una óptica pacifista. Nos encontramos ante la posibilidad de **institucionalizar nuevos valores** —autonomía individual, cooperación sin coacción, transparencia absoluta— en el tejido mismo de nuestra economía digital. Bitcoin, con todas sus virtudes, ha puesto sobre la mesa la idea de que una **Constitución de Paz** puede estar escrita en lenguaje de programación, ejecutada por miles de nodos alrededor del mundo, garantizada no por soldados sino por matemáticas. Es un paradigma emergente de organización social donde la justicia ya no proviene de jueces, ni la confianza de autoridades,

sino de un consenso descentralizado verificable por todos.

En conclusión, Bitcoin puede considerarse efectivamente un **"Protocolo de Paz"** en la medida en que fomenta la **autonomía**, la **justicia** y la **cooperación global** sin necesidad de recurrir a la violencia ni a la coerción. Si la modernidad erigió la paz sobre equilibrios de poder armado y contratos políticos frágiles, la era de la **criptoeconomía** vislumbra la posibilidad de cimentar la paz en equilibrios de incentivos y contratos algorítmicos sólidos. **"Arreglas ese nivel fundamental y todo lo que está por encima mejora de manera dramática... Mi esperanza es definitivamente la paz"**, afirmaba Dorsey en 2021 al referirse a Bitcoin. Quizá estemos ante un cambio de era: de la pax armada a la pax algorithmica, un nuevo orden pacífico sustentado por la tecnología descentralizada y la voluntad libre de sus participantes. Las próximas décadas dirán hasta dónde es capaz de llegar esta visión.

Bibliografía:

[Nota] El siguiente Ensayo es una adaptación para el concurso, del documento "Paper de Paz" publicado **por el mismo autor de forma anónima** y compartido en redes sociales en formato PDF:

https://drive.google.com/file/d/1-6VaOceuaSBSFjo9r_DSZUbQU6Hs6UiC/view?usp=drivesdk

[1] Lowery, J. (2023). Softwar: A novel theory on power projection and the national strategic significance of Bitcoin. Tesis doctoral, Massachusetts Institute of Technology (MIT).

[2] Katsh, E., & Rifkin, J. (2001). Online dispute resolution: Resolving conflicts in cyberspace. Jossey-Bass.

[3] Antonopoulos, A. M. (2015). Mastering Bitcoin: Unlocking Digital Cryptocurrencies (2ª ed.). O'Reilly Media. Antonopoulos, AM (2015). Dominando Bitcoin: [Desbloqueando las criptomonedas digitales].

[4] Kant, I. (1795). Zum ewigen Frieden [Sobre la paz perpetua]. (Edición consultada: Tecnos, 1975).

[5] Galtung, J. (1996). Peace by peaceful means: Peace and conflict, development and civilization. SAGE Publications. (Edición española: Paz por medios pacíficos: paz y conflicto, desarrollo y civilización, Bakeaz, 2003).

[6] Lederach, J. P. (1997). Building peace: Sustainable reconciliation in divided societies. United States Institute of Peace Press. (Edición española: Construyendo la paz: Reconciliación sostenible en sociedades divididas, Bakeaz, 1998).

[7] Gandhi, M. (2008). Mi vida es mi mensaje. Sal Terrae. (Título original: Mohandas Gandhi: Essential Writings, publicado en 2002).

[8] Lessig, L. (1999). Code and other laws of cyberspace. Basic Books. (Edición española: El código y otras leyes del ciberespacio, Taurus, 2001).

[9] Rule, C. (2002). Online dispute resolution for business: B2B, e-commerce, consumer, employment, insurance, and other commercial conflicts. Jossey-Bass.

[10] Roubini, N. (2019). The Blockchain and the Future of Finance: Hype vs. Reality. Testimonio ante el Senado de EE.UU. Roubini Testimonio. PDF: https://www.banking.senate.gov/imo/media/doc/Roubini%20Testimony%2010-11-18.pdf

[11] Galaxy Digital. (2021). On Bitcoin's energy consumption: A quantitative approach to a subjective question. Galaxy Digital Research. Retrieved from https://www.galaxy.com/insights/research/on-bitcoins-energy-consumption

[12] Radziwill, N. (2018). Revolución Blockchain: Cómo la tecnología detrás de Bitcoin está transformando el dinero, los negocios y el mundo. 2016. Dan Tapscott y Alex Tapscott. Nueva York: Penguin Random House. 348 páginas.

[13] Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. First Monday, 2(9). Artículo Académico. Formalización y consolidación de relaciones en redes públicas. PDF. https://www.semanticscholar.org/paper/Formalizing-and-Securing-Relationships-on-Public-Szabo/5b4cf1e37954ccd1ca6b315986d45904f9d2f636

[14] Lunaticoin & Contreras A. (2024). "Instituciones fallidas – L243" [Episodio de podcast]. Podcast Lunaticoin. YouTube. Disponible en: https://youtube.com/@lunaticoin

[15] Tula, A. (2015). "La mediación sistémica en la resolución pacífica de conflictos." A Mediar News (blog). Recuperado de https://www.amediar.info (URL rota).

[16] Prieto T. & De la Torre J. (2023). Bitcoin en la justicia: DEIUS, un caso práctico de justicia descentralizada autocompositiva. Amazon.

[17] Gladstein, A. (2018). Why Bitcoin matters for freedom. TIME. Retrieved from https://time.com/5486673/bitcoin-venezuela-authoritarian/

[18] Dorsey, J. (2021, 21 de julio). Intervención en "The B Word" [Conferencia]. Transcripción disponible en VICE. Disponible en: https://www.vice.com/es/article/jack-dorsey-cree-bitcoin-puede-traer-paz-mundial/

- Cita APA:

El Bosque de los Susurros

AUTOR: Anonimo

En un valle rodeado de montañas azules existía el Bosque de los Susurros, un lugar donde convivían animales de todas las especies. Durante generaciones, los habitantes habían vivido en armonía bajo una norma sencilla pero profundamente respetada: cada criatura conservaba sus pensamientos y decisiones en lo más íntimo, y nadie tenía derecho a conocerlos sin consentimiento.

Los búhos sabían que proteger la intimidad otorgaba sabiduría, los ciervos reconocían que ocultar sus rutas los mantenía a salvo, y las ardillas escondían sus reservas para sobrevivir el invierno. En aquel bosque, la privacidad era un tesoro compartido por todos.

Un año, tras una larga sequía, llegó al valle una comitiva de águilas de plumas doradas, que decían pertenecer al Gran Consejo del Cielo. Traían consigo unas extrañas piedras brillantes llamadas Observadoras, que afirmaban podían traer orden y prosperidad.

—Animales del bosque—proclamó la Gran Águila Regente, posada sobre una roca—, os venimos a ofrecer seguridad. Con estas piedras, podremos ver y oír todo lo que sucede en el valle. Así prevenimos peligros, malas decisiones y cualquier secreto que pueda dañar la paz. Con vuestra información, podremos protegeros mejor.

Al principio los animales murmuraron con inquietud. Pero la Águila continuó:

—Solo quien nada teme necesita esconder algo. Los secretos son peligrosos. Permitidnos vigilaros y el bosque prosperará como nunca.

Muchos animales, cansados del hambre y del miedo, aceptaron. Las Observadoras fueron colocadas en cada rincón: en los troncos, en las madrigueras, suspendidas entre ramas y escondidas entre las piedras del río. No había lugar sin vigilancia.

El primer invierno

Al comienzo todo parecía mejorar: las águilas decidían qué ramas cortar, cuánta agua beber y cómo organizar las reservas. Parecía eficiencia. Pero pronto empezaron los problemas.

Las ardillas, que siempre habían guardado bellotas en secreto, recibieron órdenes de entregar toda su comida para un almacén común. Pero nadie sabría después cuántas bellotas quedaban ni quién las administraba.

Los castores ya no podían construir presas libremente, pues cada tronco cortado debía ser autorizado tras analizar sus conversaciones privadas; incluso sus reclamos eran vigilados.

Los ciervos, que solían migrar en silencio para evitar depredadores, ya no

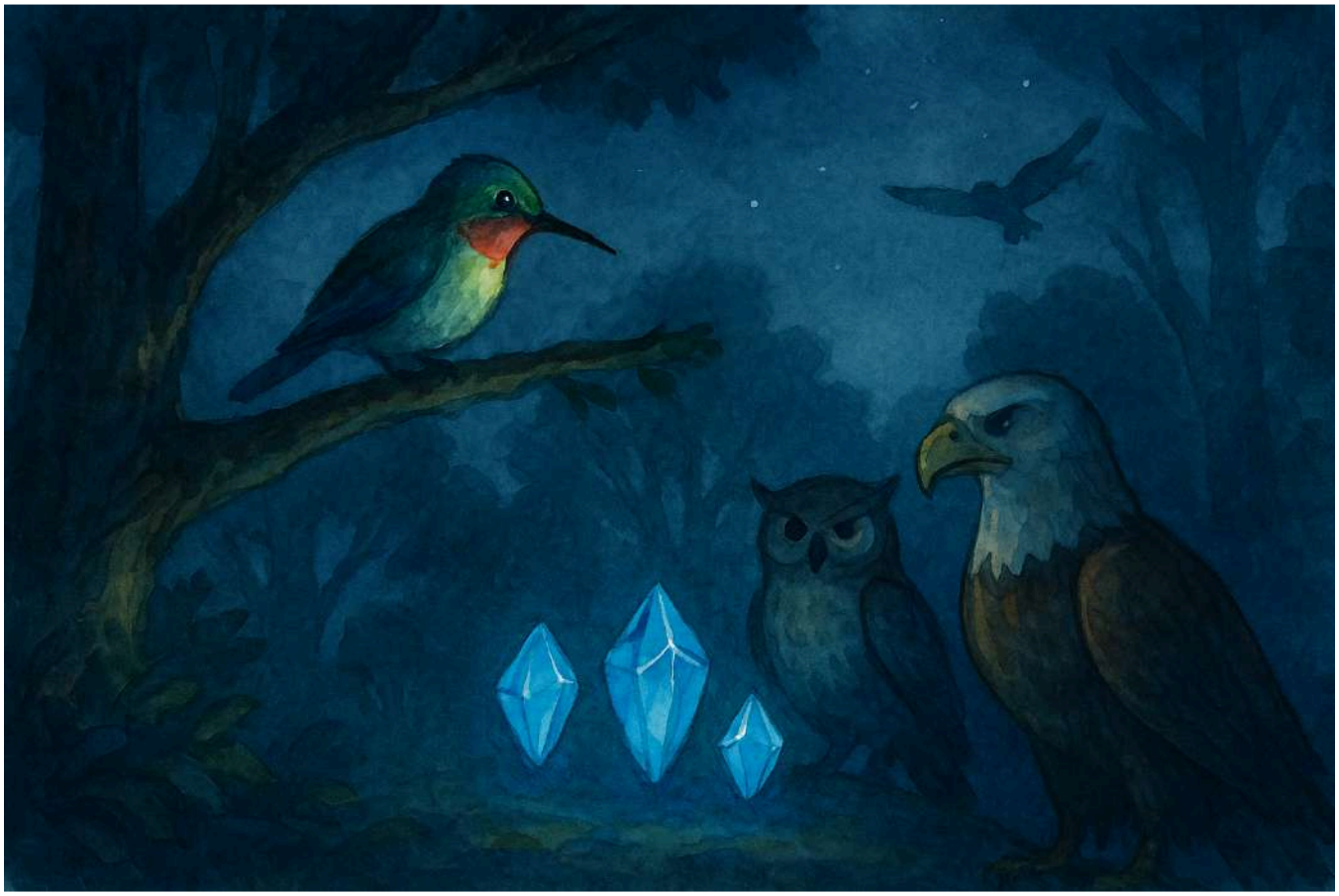
Y en lo alto del pino más viejo, el más pequeño del bosque, un colibrí llamado Albor observaba con preocupación.

—Hemos entregado todo—susurró—. Hasta nuestros pensamientos.

Una noche, mientras el bosque dormía bajo una luna fría, Albor notó que una de las piedras Observadoras parpadeaba: transmitía a una fortaleza de roca donde varias águilas discutían acaloradamente.

—Ahora que todo el bosque depende de nosotros —decía el Águila Regente—, seremos los dueños absolutos. No habrá decisiones individuales. Ningún secreto, ningún refugio. Todo estará bajo nuestro control.

Albor comprendió entonces la verdad: la vigilancia continua no era seguridad,



Al día siguiente, Albor reunió en secreto a quienes aún creían en la antigua norma del bosque: un zorro astuto, la tortuga vieja, un búho que guardaba memoria de tiempos pasados y un murciélago que podía ver sin ser visto.

—Nos quitaron la privacidad —dijo Albor— y con ella nos quitaron la libertad. Un bosque donde cada palabra está vigilada no es un hogar, sino una jaula.

El murciélago propuso apagar las piedras Observadoras cubriéndolas con barro espeso. La tortuga, lenta pero segura, iría recogiendo y guardando las piedras en un túnel subterráneo. El búho avisaría a cada animal en susurros breves para evitar ser escuchados.

La operación tomó muchas noches. Cuando las águilas finalmente notaron el silencio y la oscuridad de sus dispositivos, todo el bosque ya había despertado.

Los animales se reunieron en el claro central y, con voz unánime, se enfrentaron al Consejo del Cielo:

—Gracias por vuestra ayuda, pero este bosque pertenece a quienes lo habitan. Habéis intentado controlar nuestras vidas, y eso jamás lo permitiremos —gritó el búho.

Y así, los animales, unidos, expulsaron a las águilas y juraron que jamás permitirían que nadie volviera a invadir su privacidad. Para recordarlo, plantaron un roble enorme en el centro del claro y grabaron en sus raíces la siguiente moraleja:

“La vigilancia constante, aunque se presente como protección, es una forma de poder. Un pueblo sin privacidad es un pueblo sin libertad, y quien renuncia a su intimidad entrega voluntariamente sus cadenas.”

Por los siglos de los siglos

Bitcoin desde una perspectiva religiosa

AUTOR: P.

Desde su aparición, Bitcoin ha sido objeto de numerosos análisis: técnicos y económicos, por supuesto, pero también políticos, filosóficos e incluso poéticos. Esta obra busca acercarse a la creación de Satoshi desde una perspectiva más próxima a la teología, y profundizar en su capacidad para articular en torno a sí una determinada cosmovisión. Muchos críticos han expresado que alrededor de Bitcoin se ha formado una especie de culto religioso, yo mismo me quejé de ello cuando daba mis primeros pasos en este mundillo, al ver la vehemencia con la que muchos maximalistas se cerraban en banda. Generalmente se respondía con incomodidad a estas acusaciones, pero en los últimos años algunos bitcoiners han asumido e incluso abrazado este hecho. Uno de ellos fue Álvaro D. María, que se apropió de las críticas con esta elegante frase: «Las religiones duran más que los imperios».

El texto reúne tres ensayos que, aunque relacionados entre sí, pueden leerse de manera independiente. El primero propone una lectura de la historia del dinero a partir de los trabajos de antropólogos como David Graeber, y relaciona a Bitcoin con las corrientes filosóficas y teológicas de la Antigüedad, desde Confucio y Buda hasta los filósofos griegos. El segundo se ocupa de los primeros días de Bitcoin, de las creencias y ceremonias en las que participan los seguidores de este movimiento y de sus diferencias cruciales respecto a otras criptomonedas. El tercero analiza la red Bitcoin como tal y las razones que la han erigido en clave de bóveda de una moderna religión digital.

Por último, el epílogo establece un paralelismo entre el oro en el Imperio romano tardío y Bitcoin en la actualidad, sugiriendo que ambos cumplen funciones análogas como refugio de valor, símbolo de orden y promesa de eternidad.

Esta es una obra pensada tanto para legos en la materia como para los ya iniciados. Para los primeros he tratado de explicar de la forma más sencilla posible algún tema algo más técnico; los segundos quizá encuentren alguna inexactitud o se muestren en desacuerdo con algunos de mis planteamientos. No es ni mucho menos mi intención sentar cátedra sobre el tema, entre otras cosas porque, como ya sabrán los más veteranos, cuanto más se profundiza en Bitcoin, más se acaba comprendiendo aquella máxima de Sócrates:

«**Yo solo sé que no sé nada**».

I

«En el principio creó Dios los cielos y la tierra»

(Génesis, 1:1)

La Era Axial y el vil metal

Sabemos con detalle sobre la vida de Confucio por su papel capital en la administración china de la época; de Lao-Tse se duda hasta de su misma existencia. Buda Gautama es un personaje misterioso, más concreto que Lao-Tse pero menos que Confucio: existió, predicó en el noreste de la India y fundó una comunidad que le sobrevivió; lo demás queda bajo las brumas del tiempo. De Heráclito y Parménides tenemos fragmentos preservados gracias a citas de otras obras; de Pitágoras nos queda su teorema, su fobia a las habas y la leyenda formada por quienes le veneraron. Nos falta información, así que es complicado hacer cábalas, mas no sería de extrañar que todos ellos hubiesen sido contemporáneos, cada cual filosofando en su rincón del mundo, sin escuchar jamás el eco de los otros.

Karl Jaspers, en Origen y meta de la historia, acuña el concepto “Era Axial”, el momento —que sitúa entre el 800 y el 300 a.C.— en que la humanidad toma conciencia de sí misma y, por primera vez, se plantea ciertas preguntas que van más allá de lo inmediato. En esos siglos aparecen la filosofía griega, los grandes profetas judíos, el confucianismo, el taoísmo, el budismo, el hinduismo y el zoroastrismo. China, India, Persia, Judea y Grecia comienzan a pensar, cada una a su manera. Lo hacen en una ventana temporal muy similar y, en gran medida, sin contacto entre ellas ¿Cómo es esto posible? El antropólogo David Graeber propone una respuesta en Deuda: Los primeros 5000 años. La tesis principal del libro es que el dinero no deriva del trueque, sino del crédito. Según Graeber, la escritura surgió hace 5000 años como Excel primitivo en el que templos y palacios registraban obligaciones y pagos futuros usando unidades de cuenta abstractas, sin necesidad de intercambio físico inmediato. La moneda aparece después. En los albores del primer milenio antes de Cristo, el desarrollo de la metalurgia del hierro y la creciente capacidad organizativa de los Estados favorecen la consolidación de grandes potencias que mantienen ejércitos permanentes. Para financiar esos ejércitos, los Estados acuñan monedas con metales preciosos procedentes de botines y mano de obra esclava, y remuneran con ellas a sus soldados. Los territorios conquistados han de pagar sus impuestos en esa misma moneda, que vuelve a circular cuando los soldados la gastan en los mercados locales.

Es en este mundo violento y materialista —en su sentido tanto filosófico como crematístico— en el que surgen los pensadores radicales que tanto fascinaron a Jaspers: como reacción a la rigidez del nuevo orden.

Globalización

«Nace en las Indias honrado,
Donde el mundo le acompaña;
Viene a morir en España,
Y es en Génova enterrado»

(Francisco de Quevedo, Poderoso caballero es Don Dinero)

Entre 300 y 700 d.C. los grandes imperios colapsan, el comercio y la fiscalidad se vuelven menos inmediatos y, por lo tanto, menos dependientes de la moneda; vuelve a imperar el crédito. La siguiente era de conquistas comienza con la expansión ibérica en busca de las islas de las especias. Entramos de lleno en el mercantilismo, pero esta vez el guion cambia: a nivel monetario, las ventajas de la aventura imperial ya no son tan obvias como en tiempos pretéritos. El siglo XVII es implacable con España, que extrae de las minas del Perú toneladas de plata y oro que disparan los precios y pasan de largo cual comitiva de Bienvenido Mr. Marshall. Los tres Felipes de la casa de Austria declaran la suspensión de pagos siete veces en menos de un siglo. Los barcos repletos entrando en el puerto de Sevilla no evitaron que la Monarquía viviera constantemente al borde de la quiebra... e incluso lo provocaron, del mismo modo que la abundancia petrolera ha alimentado la crisis crónica de Venezuela.

Mientras tanto, Países Bajos e Inglaterra son los dos países que se consolidan como las grandes potencias comerciales y navales de la época, y ambas desarrollan nuevas estructuras financieras. La Bolsa de Ámsterdam (1602) inaugura el comercio de acciones a gran escala y en Inglaterra aparece el primer banco central moderno: el Banco de Inglaterra (1694), creado en un inicio para financiar la guerra contra los franceses mediante la emisión de notas convertibles en oro y plata. Ambas innovaciones dieron pie a las primeras burbujas especulativas conocidas: en 1637 estalló la tulipomanía en Holanda y en 1720 la Compañía de los Mares del Sur arrastró al abismo a las élites británicas. Por primera vez en la historia, el crédito se apoya en una red planetaria capaz de movilizar recursos a discreción: ya no se está atado a lo que hay físicamente en las arcas, como en la Era Axial, ni el comercio se limita a un entorno reducido, como en la Edad Media.

Todo esto es sólo el aperitivo, el plato fuerte viene con la Revolución Industrial. La máquina de vapor acelera la producción a un ritmo inimaginable unas décadas atrás; el ferrocarril hace lo propio con el transporte; el telégrafo, con las comunicaciones. Stefan Zweig narra en uno de sus Momentos estelares de la Humanidad como la instalación del primer cable transatlántico que une Europa y América acorta las medidas del planeta y, literalmente, lo une: lo sucedido en Nueva York es conocido instantes después en París y viceversa. El oro, todavía patrón último de valor, se convierte cada vez más rápido en papel: los metales son ya demasiado lentos para este mundo frenético. El creciente número de bancos —privados o públicos— multiplica los intermediarios y hace circular billetes y letras sin necesidad de mover un solo lingote. La humanidad, que durante milenios limitó su velocidad a la de los caballos, rememora el mito de Prometeo y desafía a los dioses; la que antes era la rueda de Fortuna es hoy la del ferrocarril, la de la fábrica, la del Progreso que avanza imparable. En esos tiempos de optimismo sin fin surgen el positivismo, el comunismo y, algo más tarde, el fascismo; corrientes de pensamiento que aspiran a moldear las sociedades como si fuesen plastilina. La Segunda Guerra Mundial fue el desenlace lógico a esta dinámica; las ambiciones de los Hitler, Stalin o Roosevelt de turno nos hubiesen parecido en otros tiempos prerrogativas de los dioses.

La era Boomer (1971-2008)

La Primera Guerra Mundial marcó el momento en que los gobiernos comenzaron a zafarse del corsé dorado para poder financiarse a discreción. En el periodo de entreguerras se ensayó el llamado Gold Exchange Standard, en el que la libra esterlina actuaba como divisa de referencia. El sistema se reformuló en Bretton Woods (1944), con el dólar desplazando a la libra como moneda hegemónica y siendo la única convertible directamente en oro, a razón de 35$ la onza. El invento funcionó de forma notable durante más de dos décadas, pero no dejaba de ser un parche, y en 1971 saltaron las costuras. Nixon, obligado por las circunstancias, finiquita el Ancien Regime y adentra al mundo en lo desconocido.

La generación destinada a protagonizar esta nueva era ya había hecho acto de presencia en la Historia en el anterior lustro, con guitarras amplificadas y pancartas ondeando al viento. Todo eso de los límites no parecía ir demasiado con ellos. Son mayoría, y este hecho marcará toda su vida. Ellos mismos crean con su abigarrada presencia la sola idea de la cultura juvenil; surge un nuevo mercado en ebullición que los Don Draper de turno aprovecharán. Lo que más recordamos hoy del Mayo del 68 francés son sus eslóganes: “Sed realistas, pedid lo imposible” o “Prohibido prohibir” son lúcidos y afilados, como una vertiente política del “It’s toasted!”, pero no dejan de ser eso: una campaña de marketing.

Debajo de los adoquines no estaba la playa, sino la tarjeta de crédito.

Decíamos antes que el parche de Bretton Woods funcionó, lo cierto es que hizo mucho más que eso: se podría incluso argüir que los Treinta Gloriosos fueron la época más próspera que haya visto el hombre. Pero aquella abundancia nunca antes vista llevaba inserta la semilla del caos. El tenue equilibrio que mantenía a la sociedad con los pies en el suelo y la vista hacia el cielo acabó por romperse en los convulsos setentas y, a partir de entonces, los boomers, ya del todo liberados de anclas materiales, volaron sin ataduras —y, con ellos, la valoración contable de sus casas, convertidas por arte de birlibirloque en la reserva de valor deseada por los gobiernos: ilíquidas, inmóviles y fácilmente gravables—. También las conquistas sociales de la época, como el aborto o el divorcio, apuntaban en la misma dirección, ya lo cantaba Nino Bravo: "libre, como el sol cuando amanece". Visto en perspectiva, la facción perdedora de la Guerra Fría resultó ser la que apostaba por un orden sólido en el que pervivía la noción del sacrificio y de un bien mayor. Decía Agustín de Foxá que «morir por la democracia es como morir por el sistema métrico decimal»; en este caso, la Unión Soviética de los grandes ideales murió de facto cuando miles de moscovitas hicieron cola en la plaza Pushkin para degustar por primera vez una Big Mac.

Ya nos adentrábamos en una moderna Belle Epoque a-la-Fukuyama cuando llegó 2008 y hubo que volver a repensarlo todo.

Fully Automated Luxury Gay Space Communism (2008-?)

Para hablar del mundo post Gran Recesión quiero volver a David Graeber, esta vez a La utopía de las normas, un tríptico de ensayos sobre la burocracia. En su prólogo, enuncia la por él llamada Ley de hierro del liberalismo:

> «Toda reforma del mercado, toda iniciativa del gobierno dirigida a reducir trámites burocráticos e impulsar las fuerzas del mercado tendrá, como efecto final, el aumento del número total de regulaciones, la cantidad total de papeleo y la cantidad total de burócratas que emplea el gobierno.»

Graeber, especialista en desmitificar grandes narrativas, prefigura en este libro su posterior Trabajos de mierda y cuestiona la idea imperante según la cual el sector privado, a diferencia del sector público, premia la eficiencia y abjura de la burocracia.

Este enfoque nos ayuda a entender como, tres décadas después de la caída del Muro, tenemos un Leviatán cada vez más grande y más voraz que, no contento con regular toda actividad posible dentro del espacio físico que controla, se empeña también en meter sus zarpas en el ciberespacio: baste como ejemplo el reciente intento de prohibir Telegram por parte de un juez boomer, probablemente acostumbrado a que no haya freno alguno a sus ideitas.

Son recurrentes las mofas a un famoso tuit de Eduardo Garzón en el que propone que el BCE imprima dinero para hacer inversiones; lo chocante aquí es más bien el supuesto shock de la funcionaria ante la propuesta de Garzón. Todos tenemos en mente a Lehman Brothers cuando hablamos de la crisis de 2008 y esto se debe a que fue la única gran firma que quebró: las demás fueron rescatadas, alegando que eran too big to fail. Para salir del atolladero, la Reserva Federal aplicó de forma casi inmediata el Quantitative Easing: expandió su balance y procedió a la compra de bonos del Tesoro, es decir, creó masivamente dinero de la nada y lo inyectó en el sistema. Europa, por su parte, desperdició cuatro años aplicando medidas convencionales y no claudicó hasta 2012, con el famoso "whatever it takes" de Mario Draghi. Resultan cuanto menos curiosas las críticas al capitalismo salvaje con los Bancos Centrales dirigiendo la economía con escuadra y cartabón, en un alarde que hubiese hecho las delicias de Stalin o Brezhnev. Las imposiciones draconianas de la Troika fueron contraproducentes y alimentaron el relato contrario, que aún perdura: la palabra "austeridad" lleva hoy aparejado el márchamo del oprobio, cuando no hay nada malo en ser austero. La fábula de la cigarra y la hormiga invierte así su moraleja, la impunidad se contagia y la accountability desaparece. Hoy podemos disfrutar en televisión de tertulianos y políticos pidiendo que el Estado se haga cargo de las hipotecas a tipo variable, ya que la cuota de estas... ¡varía! Surgen también las así llamadas huelgas feministas, financiadas y publicitadas por el propio gobierno de turno; demostración empírica de que los sueños de la emancipación producen monstruos. En la era woke, la autonomía sigue siendo el objetivo, siempre que esta sea otorgada y validada por el Estado. El ogro filantrópico es hoy más filantrópico que nunca, también más ogro: Hacienda bate records de recaudación año tras año. Quizá la que mejor expresó nuestro zeitgeist fue la ex-vicepresidenta de España, Carmen Calvo, que nos dejó la siguiente cita para la posteridad: **"Estamos manejando dinero público, y el dinero público no es de nadie"**.

Tras la borrachera del COVID y la posterior resaca en forma de subida de precios descontrolada, hay gente que empieza a estar un tanto mosca. Uno de ellos es Elon Musk. El magnate sudafricano fue designado como Special Government Employee al frente del Department of Government Efficiency (DOGE), un organismo impulsado por Trump para recortar burocracia y gasto público. Musk entró en su cargo como un elefante en una cacharrería: despidos masivos, reducción de agencias, auditorias con inteligencia artificial... todo fue en vano. Descubrió despilfarros grotescos, sí, pero eran el chocolate del loro. Tras cuatro meses infructuosos de peleas recurrentes contra el Congreso, se rindió. El fracaso de un enfermo de la productividad como Musk y la masiva expansión de gasto público de la Big Beautiful Bill ratificaron la tesis graeberiana: ni siquiera un hombre de negocios como Trump, completamente opuesto al típico político de carrera que suele poblar la Casa Blanca, ha osado reducir el blob burocrático. El Money printer go brrr se revela así como el verdadero fin de la historia.

El Único y su propiedad

Vamos a intentar simplificar todo este embrollo. Tenemos dos visiones contrapuestas. En una de ellas, el dinero es pura materia: oro, metales, recursos naturales. Depende de la existencia de Estados todopoderosos que extraigan y hagan circular toda esa materia y la recauden en forma de impuestos. Una nueva forma de pensar emerge en oposición a esta concepción del mundo y, con ella, emerge también el Espíritu. En el otro extremo, el dinero es puro espíritu: una abstracción humana que se puede crear a discreción, un fantasma. Esta, en un sistema global como el actual, también depende de Estados todopoderosos que implanten e impongan la unidad de cuenta. La versión puramente materialista es fácil desmontarla: basta con imaginar que en Fort Knox no hubiese una sola onza de oro y nosotros fuésemos los únicos en saberlo: nada esencial cambiaría, la riqueza del mundo no se vería alterada en lo más mínimo. La otra resulta absurda a poco que se aplique el sentido común, pero admitamos que hay verdades contraintuitivas. Aún así, los problemas que trae aparejados su aplicación práctica son muy evidentes y los estamos sufriendo en estos momentos.

¿Cuando vendrán los sabios que nos liberen del Espíritu? No ha de ser con algo material, ya que ese camino ya está recorrido, mas ha de ser algo limitado, apropiable... Único. ¿Es esto posible?

Quizás el Profeta ya haya venido...

II

«En el principio era el Verbo, y el Verbo era con Dios, y el Verbo era Dios»

(Jn, 1:1)

Ya desde los tiempos de Aristóteles, el ser humano se ha afanado en buscarle causas a los fenómenos. Tolstoi, en su portentosa Guerra y paz, diserta ampliamente sobre el reduccionismo en el que caen quienes intentan buscarle un solo motivo (que en la novela sería el genio de Napoleón) a los acontecimientos históricos, los cuales dependen de millones y millones de voluntades humanas entrecruzadas y circunstancias azarosas:

> «La razón humana no puede comprender el conjunto de las causas que originan cada fenómeno, pero la necesidad de conocerlas es inherente a la naturaleza del hombre. Y la razón humana, sin ahondar en la infinitud y complejidad de las condiciones del fenómeno, cada una de las cuales, por separado, puede concebirse como causa del mismo, se acoge a la primera semejanza, que suele ser la más inteligible, y dice: ésta es la causa»
>
> (Lev Tolstoi, Guerra y Paz)

Esta tendencia se ha agravado en la Modernidad, donde la herencia cartesiana ha reducido el mundo a un laboratorio en el que todo es mensurable y los inputs determinan los outputs. Como Dios, causa primera de todas las cosas, ha muerto, nuestra era materialista se afana en buscar nuevas causas. Así, reinan la sospecha y el desengaño; cualquier acto presupone un interés. No es de extrañar, teniendo esto en cuenta, que por los mentideros de Internet sea ya vox populi la teoría de que Bitcoin es una creación de los servicios de inteligencia de Estados Unidos. El razonamiento es el siguiente: el algoritmo de cifrado SHA-256, utilizado por los mineros para hallar el número que les permite añadir un nuevo bloque a la cadena, fue desarrollado por la NSA (National Security Agency). El silogismo resulta evidente: si la NSA ha creado el algoritmo SHA-256, y Bitcoin usa el algoritmo SHA-256, la NSA ha creado Bitcoin. La razón humana se acoge así a la primera semejanza, la más inteligible; a partir de ahí, la imaginación se desborda. Algunos hablan de un plan a largo plazo que estaría cristalizando ahora, con la ley GENIUS y el papel capital de Tether en la compra de bonos estadounidenses. Otros, propensos a ver hilos en la sombra, se tiran a la piscina con hipótesis alocadas: el fin del sistema SWIFT, una puerta trasera en el código, un esquema Ponzi meticulosamente planeado, convertido en trampa mortal para incautos...

Todas estas elucubraciones se formulan a posteriori, cuando ya no se puede obviar la realidad y Bitcoin es una institución gigantesca con una capitalización de mercado similar a la de un mastodonte como Amazon. Pero hubo un tiempo, años ha, en el que los bitcoins se utilizaban para intercambiarlos por drogas en la dark web y los mineros no eran enormes compañías con granjas repletas de ASICs, sino nerds sobrecalentando sus ordenadores personales. Pronosticar entonces la situación actual habría sido tan osado como imaginar en los años en los que se escribieron los Evangelios que aquel culto marginal acabaría siendo, tres siglos más tarde, la religión oficial del Imperio Romano.

Inmaculada concepción

«**I've moved on to other things**»

(Satoshi Nakamoto, email a Mike Hearn, 23 de Abril de 2011)

Lo cierto es que, si nos vamos aún más atrás, al origen, descubrimos que los pioneros ya pensaban a lo grande. Satoshi Nakamoto, el anónimo creador de Bitcoin, clava el whitepaper en la Cryptography Mailing List el 31 de Octubre de 2008, el mismo día en el que, cuatrocientos noventa y un años antes —31 de Octubre de 1517—, Martín Lutero clavó sus 95 tesis en la puerta de la iglesia de Wittenberg. Este simple gesto deja entrever las ambiciones de Satoshi: si el fraile alemán desafió a la autoridad religiosa, Nakamoto desafía a la autoridad monetaria y busca, como Lutero, desencadenar un nuevo orden mundial. Nuestro desconocido amigo lleva el plan a la práctica el 3 de enero de 2009 y edifica su Iglesia sobre el bloque Génesis, en el que incrusta la portada de The Times del mismo día — **"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"**—, toda una declaración de intenciones petrificada bajo los siguientes bloques, que él mismo irá minando. El primer cypherpunk que se une a la red es Hal Finney, que también comienza a minar y, en el bloque 170, recibe 10 BTC de Satoshi: la primera transacción de bitcoin de la historia. Finney, que ya había intentado crear algo similar al dinero digital con su Reusable Proof of Work, vio potencial en el invento y se aventuró desde el primer día con pronósticos que hacen palidecer las previsiones más optimistas del bitcoiner más bullish:

«Como un experimento mental divertido, imagina que Bitcoin tiene éxito y se convierte en el sistema de pago dominante en todo el mundo. Entonces, el valor total de la moneda debería ser igual al valor total de toda la riqueza del mundo. [...] Con 20 millones de monedas, eso daría a cada una un valor de aproximadamente 10 millones de dólares»

(Hal Finney, email a Satoshi Nakamoto, 10 de Enero de 2009)

La primera transacción entre Nakamoto y Finney es histórica porque pertenece por pleno derecho a la Historia, pero también por una razón más pedestre: ninguno de los dos sigue hoy entre nosotros. Hal falleció en agosto de 2014, tras un progresivo deterioro debido a la ELA. El Creador, por su parte, se apartó de la esfera pública el 12 de diciembre de 2010, con un mensaje técnico en BitcoinTalk que en nada hacía presagiar que esa sería su última aparición en el foro. Su penúltimo mensaje, sin embargo, es mucho más elocuente: en él lamenta un artículo de PCWorld que especulaba con que Bitcoin podría ayudar a sortear el bloqueo financiero de WikiLeaks; una semana antes, el día 5, había templado los ánimos, recordando que aún eran una comunidad diminuta y experimental y que la atención mediática que atraería Assange podría destruir el proyecto. Tras su retiro, Satoshi siguió manteniendo correspondencia con algunos desarrolladores hasta que, el 26 de abril de 2011, le envía a Gavin Andresen —el primer Papa de Bitcoin, designado por el propio Satoshi como desarrollador líder y administrador del repositorio original— su último correo conocido, en el que le advierte que "habría sido mejor evitar asociar Bitcoin con ese tipo de organización", ya que Andresen le había informado poco antes que iba a dar una charla sobre el proyecto en la sede central de la CIA. Al día siguiente, Gavin publica el anuncio y, desde entonces, Satoshi no ha vuelto a dar señales de vida.

¿Quien es —o quienes son— Satoshi Nakamoto? Unos aventuran que podría haber sido el propio Hal Finney, otros le relacionan con Nick Szabo, Adam Back o incluso Jack Dorsey. Lo cierto es que no lo sabemos y todo apunta a que nunca lo sabremos. Satoshi, al igual que Jesús, se vio enfrentado a la autoridad imperial de la época y Satoshi, al igual que Jesús, murió por todos nosotros. Aunque no quería ser visto como una, en sus propias palabras, «mysterious shadowy figure», es lo que terminó siendo; hemos de estarle eternamente agradecidos por ello. De nada servirían los miles y miles de nodos desperdigados alrededor del mundo, validando transacciones y evitando la centralización del registro, sin el sacrificio del fundador, que pasó con su desaparición de hombre a mito.

Empresas y sectas

Si del creador de la primera criptomoneda por capitalización bursátil no sabemos casi nada, del creador de la segunda lo sabemos casi todo. Vitalik Buterin, programador ruso-canadiense, fue editor de Bitcoin Magazine y participó en la Bitcoin Foundation antes de apartarse al considerar que Bitcoin estaba perdiendo flexibilidad. De ahí nació Ethereum, otro libro de cuentas donde se lleva el registro de más de 120 millones de ethers —la moneda nativa de la red— cuyo valor conjunto supera actualmente los quinientos mil millones de dólares. También se almacenan en esta blockchain muchos otros tokens:

desde monedas estables ancladas al dólar —un mercado de más de doscientos mil millones de dólares del que Ethereum concentra el 70%— hasta memecoins, NFTs, versiones tokenizadas de activos como el oro o de criptoactivos como bitcoin, y tokens de gobernanza empleados por aplicaciones descentralizadas. Todas estas fichas se pueden intercambiar entre sí mediante contratos inteligentes que se validan en cuestión de segundos, sin necesidad de que intervengan terceras partes.

Reconozcamos que esto es un hito en la historia de las finanzas, pero detrás de él está la cara visible de Vitalik y la Ethereum Foundation, una organización dedicada a promover y desarrollar la red. Ethereum sigue una hoja de ruta cuidadosamente planificada, con eventos como The Merge, la transición de prueba de trabajo a prueba de participación, que redujo el consumo energético de la red y redefinió su funcionamiento. Un cambio así sería prácticamente imposible en Bitcoin, donde la ausencia de una autoridad central hace que cualquier modificación profunda requiera un consenso casi absoluto. La historia de Ethereum ya dejó claro en 2016 hasta qué punto las decisiones pueden concentrarse: tras un hackeo, la red se bifurcó en dos y se impuso la versión "oficial" —la actual Ethereum— en gran parte gracias al respaldo explícito de Vitalik. Que el código sea abierto no impide que, en la práctica, acabe decidiendo el CEO. Ethereum es una plataforma de código abierto, pero se comporta como una empresa.

La que sí es una empresa es Ripple, creadora del XRP Ledger, donde circulan los tokens XRP, una de las altcoins con mayor base de seguidores y mayor capitalización bursátil. Con Ripple se da una paradoja curiosa: es una compañía bastante transparente en su funcionamiento, con sedes físicas, empleados con perfil en LinkedIn y acuerdos firmados con bancos, pero su comunidad de fieles se alimenta de oscurantismo, rumores y promesas vagas. Se habla de libros mayores ocultos, de contratos confidenciales con grandes instituciones... pero nadie concreta nada. En teoría, XRP está diseñado para funcionar como puente entre divisas en transacciones interbancarias. La idea recuerda, en cierto modo, al bancor propuesto por Keynes en Bretton Woods, que nunca llegó a implementarse. XRP, en cambio, sí circula, aunque sin que su uso real alcance la escala que su narrativa promete.

Frente a Bitcoin, con su libro mayor público y un ecosistema donde todo debate ocurre a la luz del día, Ripple, aunque su código también sea abierto, se sostiene sobre una estructura de creencias muy distintas. Sus fieles, como modernos Nostradamus, hacen circular narrativas fantasiosas y profecías, otorgan significados especiales a cifras concretas —como el famoso 42 de la lotería maldita que gana Hurley en Lost— e interpretan movimientos corporativos como

parte de un plan maquiavélico que solo ellos han sabido descubrir. Para un lego en la materia, la XRP Army y los maximalistas de Bitcoin pueden parecer indistinguibles, ambos ven pruebas a su favor en cualquier trivialidad y comparten una visión escatológica, una especie de Juicio Final financiero que pondrá patas arriba el sistema monetario mundial. Los primeros creen que, algún día señalado en rojo por unas pocas élites, la red de Ripple se integrará de forma súbita en el sistema financiero global, reemplazando a SWIFT; los segundos, por su parte, lo resumen con una de sus frases fetiche: "gradually, then suddenly". Pero mientras los devotos de XRP se asemejan más a una secta que aguarda expectante la llegada de la nave salvadora con plazas limitadas, en Bitcoin hay una narrativa más amplia y rica, articulada en torno a la soberanía individual y, sobre todo, una búsqueda explícita de la Verdad.

Maximalismo tóxico

«Porque el Señor mismo con voz de mando, con voz de arcángel, y con trompeta de Dios, descenderá del cielo; y los muertos en Cristo resucitarán primero. Luego nosotros los que vivimos, los que hayamos quedado, seremos arrebatados juntamente con ellos en las nubes para recibir al Señor en el aire, y así estaremos siempre con el Señor.»

(1 Tesalonicenses, 4, 16-17)

En su monumental El Reino, Emmanuel Carrère, al repasar la primera carta escrita por San Pablo incluida en la Biblia, hace hincapié en que no existe en ella ninguna figura retórica: Pablo espera genuinamente presenciar en vida la segunda venida de Cristo y ser testigo del fin del mundo. Carrère, a la vez socarrón y profundo, señala que esta idea de un apocalipsis inminente, que a primera vista puede parecer primitiva o irracional, es en realidad una constante a lo largo de la Historia. Sucedió en la Edad Media, con sus reiterados conatos milenaristas, y sucede también en nuestra época, con el tan anunciado colapso ambiental. Algunos exégetas de San Juan creyeron en el fin del reinado de Cristo al llegar el año 1000 y algunos ingenieros informáticos creyeron en el fin del reinado de las máquinas al llegar el año 2000. Desde principios del siglo XIX muchas personas viven convencidas de que estamos a las puertas de un cataclismo sin precedentes, y no podemos culparles si echamos la vista atrás y contemplamos lo sucedido entre 1914 y 1945.

Los bitcoiners también creen en la inevitable lluvia de fuego y azufre: los políticos y banqueros, insaciables, nos han empobrecido a marchas forzadas; Bitcoin viene a salvarnos de sus garras. Entre estos herederos del apóstol, que

aguardan pacientemente su particular parusía, es común escuchar la expresión "caer por la madriguera de Bitcoin", como el conejo de Alicia en el País de las Maravillas. Se entra por el precio, por el FOMO, y se termina por adoptar los mitos y seguir los ritos: guardar las claves, no vender nunca y despreciar a los herejes que compran altcoins. Hay conversiones tardías y liturgias cada cuatro años celebrando el halving, mártires como Ross Ulbricht —fundador de Silk Road, condenado a cadena perpetua y recientemente liberado por Trump—, y fiestas como el Bitcoin Pizza Day: cada 22 de Mayo los fieles conmemoran el día en que Laszlo Hanyecz compró dos pizzas por 10.000 BTC, entrando así en la historia como el primer intercambio de bitcoin por bienes y servicios. También hay mantras, como el famoso "HODL", nacido de un error tipográfico en un hilo de 2013 y elevado a imperativo sagrado. Durante el anterior ciclo alcista surgió incluso un signo visible de esa fe: los laser eyes, avatares con rayos rojos saliendo de sus ojos. Quienes los añadían a sus perfiles en redes sociales declaraban así su adhesión a la causa y su confianza ciega en que se alcanzarían los cien mil dólares más pronto que tarde. Hoy ese umbral ya se ha superado, pero la iconografía se mantiene. Basta la mirada incandescente para reconocer a los creyentes.

Los maximalistas recuerdan, en cierto modo, a los personajes del relato Razón, de Isaac Asimov, en el que unos robots destinados a gestionar una estación solar fundan una religión tecnológica basada en la adoración de su amo: el transformador de energía. Para frustración de los humanos presentes en la estación, los robots se niegan a aceptar el mundo exterior, la existencia de la Tierra o sus propias órdenes. Pero su fe ciega en "los comandos del Señor" les lleva, paradójicamente, a cumplir su función a la perfección. A los maximalistas, dogmáticos y plomizos, les gusta regodearse en la pobreza ajena cuando no les dan la razón con el acrónimo HFSP (Have Fun Staying Poor), y, ante las preguntas de los no iniciados, suelen citar, cortantes, a su gurú Satoshi: **«Si no me crees o no lo entiendes, no tengo tiempo para intentar convencerte»**. Fieles a su dogma, hacen oídos sordos a cualquier objeción o matiz. Es normal. Comprar bitcoin y holdear se ha demostrado la mejor estrategia posible. Se les llamó "tóxicos" y, como los decadentistas franceses, decidieron apropiarse del insulto y llevarlo como insignia. Su intransigencia, además, resulta instrumental. Nassim Nicholas Taleb ha descrito este fenómeno en su obra Skin in the Game como el «dominio de las minorías intolerantes»: basta con que una fracción pequeña pero inflexible mantenga su postura para que, con el tiempo, el resto del sistema termine por adaptarse a ella. Cristianos y bitcoiners fueron ridiculizados y vilipendiados por sociedades altivas que no comprendieron sus estrafalarias doctrinas, pero persistieron, inasequibles al desaliento, hasta que, Trump hoy y Constantino hace mil setecientos años, las incorporaron a la estructura de poder. El cristianismo sobrevivió al Imperio y dominó el mundo; muchos creemos que Bitcoin hará lo propio.

En la actualidad, la comunidad se encuentra profundamente dividida por una disputa que, para los profanos, puede recordar a las famosas discusiones bizantinas. Hay un grupo de heterodoxos que está utilizando el espacio de los bloques para introducir determinada información que luego se decodifica como imágenes. Para los más ortodoxos, esto es una profanación: la red solo ha de servir para enviar y recibir bitcoins. Un pequeño grupo liderado por Luke Dash jr, un tipo muy excéntrico que ya fue parte importante en anteriores guerras entre facciones, considera que estas prácticas son impuras y desvían al protocolo de su misión sagrada; para tratar de impedirlo, corren su propia versión del software. Pero el diseño de Bitcoin tiene una lógica implacable: los bloques los construyen los mineros, los validan los nodos, y una vez la imagen ha entrado en la cadena, se queda ahí, grabada para siempre. Como Verdad revelada.

III

«Y aquel Verbo fue hecho carne, y habitó entre nosotros»

(Jn, 1:14)

Palabra

El Libro Mayor y sus bifurcaciones

El 1 de agosto de 2017, a las 13:16:14 UTC, el pool de minería BTC.com añadió a la cadena de Bitcoin un nuevo bloque, el 478558, bloque que a primera vista no tiene nada de especial, pero que pasará a la historia por ser el último en común antes del Gran Cisma. En aquellos momentos Bitcoin estaba en plena guerra civil y dos facciones, los small blockers y los big blockers, peleaban por imponer su visión particular del Libro Mayor. Tras muchos debates, negociaciones y peleas, los segundos decidieron ir por libre y la red se dividió. El nuevo libro contable se llamó Bitcoin Cash y su primera página tras la escisión, la 478559, ya deja ver el motivo de esta: 1,9 MB de tamaño, superando ampliamente el límite de 1 MB de la blockchain original, que continuó con las mismas reglas hasta que, el 24 de agosto, en el bloque 481824, se activó el protocolo Segregated Witness (SegWit), que modifica la estructura de las transacciones, comprimiendo al máximo la información para que, sin aumentar el límite formal, quepan muchas más en cada bloque.

«En este punto, el debate parece volverse casi religioso, con ambos bandos estudiando minuciosamente cada cita de Satoshi en busca de comentarios o interpretaciones que apoyen su causa.»

(Jonathan Bier, The Blocksize war)

Esta disputa puede recordar a la cláusula filioque que desembocó en el Cisma de Oriente: un tecnicismo que aparentemente no reviste importancia, pero que lleva aparejadas distintas cosmovisiones. Los big blockers querían un dinero más rápido y barato: cuanto más grande sea el bloque, más transacciones caben en él. Los small blockers, más cautos, ponían el foco en temas más “aburridos”: con bloques más grandes, los requisitos de hardware para montar un nodo crecerían exponencialmente, favoreciendo así la centralización.

Aunque concedían que 1 MB era muy poco espacio, intuían que Bitcoin era algo demasiado importante como para reducirlo a una carrera contra Visa y Mastercard y por eso buscaron una solución más elaborada que no rompiese la sintaxis del Libro Mayor: ahí residió la clave de su victoria. Mientras los bcashers tuvieron que realizar un **hard fork**, que obliga a los nodos a actualizarse para ser compatibles con las nuevas reglas del protocolo, para introducir SegWit bastó con un **soft fork**, con el que es posible procesar los nuevos bloques con versiones antiguas del software. Esto puede parecer un tanto absurdo: ¿por qué los nodos desactualizados tienen tanta importancia? En la mayoría de proyectos de informática los formatos cambian y el software viejo queda atrás sin que esto suponga problema. Nadie se sorprende de que un programa diseñado para Windows 11 no pueda ejecutarse en un Windows 98, o que un Photoshop de 1998 no pueda abrir un archivo creado en 2024. La diferencia es que no hablamos de un programa cualquiera: Bitcoin pretende instaurar un nuevo orden que se pueda rastrear incluso en viejos incunables.

Historia 2.0

La escritura es el evento que da carta de naturaleza a la Historia, todo lo ocurrido antes está fuera de ella. Los humanos ya hablábamos desde hace más de cien mil años, pero las palabras se las llevaba el viento hasta que los desarrolladores de la época las codificaron para poder grabarlas en arcilla y piedra. En Egipto surgieron los jeroglíficos y en Sumeria los pictogramas, que evolucionaron poco a poco hacia un sistema silábico, permitiendo registrar no solo objetos concretos, sino también nombres, cantidades o relaciones abstractas. Este hallazgo no se utilizó en primer término para escribir cuentos o poemas, ni siquiera para glosar las hazañas de los reyes y faraones; lo primero que aquellos símbolos mágicos plasmaron fueron transacciones. La Historia no la inauguraron los mitos ni las canciones, sino la Economía.

Hoy en día, ese mundo nuevo que es el ciberespacio se parece más a lo oral que a lo escrito. En el mejor de los casos podríamos decir que alberga una escritura precaria, semejante a la que existía antes de la imprenta, pero no una escritura con vocación de permanencia. Todo lo que leemos, vemos y escuchamos en Internet depende de un servidor y de quien lo mantiene; cuando nadie lo hace, toda esa información se pierde. Cada vez son más los enlaces rotos, las imágenes invisibles o los 404: Page not found. El Internet del Wild West, aquel en el que aún no había grandes corporaciones tecnológicas dominando el cotarro, es hoy, en el mejor de los casos, inaccesible ante la inoperancia de los motores de búsqueda; en el peor, ha desaparecido sin dejar rastro.

En nuestros días, con gigantes como Alphabet, Meta o Microsoft que acumulan ingentes recursos destinados a guardar toda esta información, podríamos pensar que aquella Era Oscura del ciberespacio es agua pasada, que todo permanecerá. No es así. Las nubes son etéreas, y los recursos, finitos: como prueba, algunos correos remitidos por Google en los que me informan de que mi antigua cuenta, olvidada desde hace años, será eliminada por falta de uso.

El bloguero Paul Skallas profundiza al respecto en su artículo The Internet is Not Forever, en el que le da un repaso a los métodos —antiguos y modernos— utilizados para preservar información. Su conclusión es que lo importante no es tanto la tecnología como las instituciones, y escribe una frase que viene aquí como anillo al dedo:

> «Los libros que sobreviven son aquellos que fueron copiados, y copiados, y copiados de nuevo, generalmente muchas veces a lo largo de los siglos.»

Más tarde llegarán los poetas, los filósofos, los doxógrafos del ciberespacio; sus tragedias y sus comedias, sus crónicas y sus leyendas. Hoy tenemos el libro de cuentas, copiado, y copiado, y copiado de nuevo, muchas veces a lo largo y ancho del planeta. Con eso basta.

Trascendencia e inmanencia

En este punto, la analogía sale sola: Bitcoin como la Iglesia de la Edad Media, una institución con miles y miles de amanuenses trabajando silenciosamente, desperdigados por los monasterios de toda Europa. Los monjes están apartados, literal y figuradamente, de lo terrenal. Han hecho voto de castidad, obediencia y pobreza, y viven ajenos a las vicisitudes mundanas, escribiendo y apilando la Historia Universal para que a esta no se la trague el olvido. Pero no son máquinas y pueden incurrir en pecados veniales o excesos devocionales. Pongamos por ejemplo la Donación de Constantino, un documento según el cual el emperador le habría otorgado al Papa el derecho de gobernar Roma y sus alrededores. Copiada y transmitida durante siglos en los scriptoria eclesiásticos, fue aceptada como auténtica hasta que, en 1440, Lorenzo Valla demostró que estaba escrita en un latín más propio de la época de Carlomagno que de la de Constantino.

Immanuel Kant, al intentar conciliar el escepticismo de Hume con las exigencias de la Razón, sostuvo que el mundo en sí mismo es incognoscible. No percibimos la realidad tal y como es: siempre está mediada, en primera instancia por las formas subjetivas de nuestra sensibilidad: espacio y tiempo. Pero no solo eso: las instituciones que actúan sobre el mundo condicionan así nuestra percepción de este. Los monjes que copiaban la Donación de Constantino no transmitían el pasado tal como fue, sino el pasado que le interesaba a la Iglesia, que en la Edad Media fue capaz de erigirse en condición trascendental de la experiencia histórica. Tras Kant, la filosofía solo puede consistir, en palabras del filósofo Nick Land, "en diferenciar el formato trascendental del dato empírico, y luego resolver —o, más realísticamente, negociar— los conflictos de frontera entre ambos". Seguimos sin ser dioses capaces de percibir la realidad tal cual es, sin embargo, Bitcoin constituye quizá el intento más logrado: lo que está en la cadena es, y no hay ya mediación posible.

«La planitud entre pares se condensa en inmanencia, las terceras partes de confianza en constructos metafísicos de trascendencia»

(Nick Land, Cryptocurrent)

Tiempo

Kant y Nakamoto

Kant recogió las piezas que racionalistas y empiristas habían dejado desperdigadas a lo largo de los dos siglos previos y construyó con ellas un sistema filosófico imponente, una pieza de orfebrería que marca el punto de partida de la filosofía moderna. Citando de nuevo a Land, la filosofía solo puede ser hoy crítica en su sentido kantiano. De todos modos, quizá lo más reseñable de su obra es, por así decir, la falta de oropeles. Antonio Machado, en uno de sus Proverbios y cantares, dice de él que es "un esquilador / de las aves altaneras; / toda su filosofía / un sport de cetrería" y le retrata trocando al "ave divina" en "pobre gallina". Pio Baroja, en El árbol de la ciencia, pone en boca del protagonista de la novela que "[Kant] se encontró con esos dos árboles bíblicos [...] y fue apartando las ramas del árbol de la vida que ahogaban al árbol de la ciencia".

Se ha dicho de Satoshi que, más que inventar, supo unir de forma genial conceptos ya existentes para ensamblar su obra: la blockchain como estructura de datos estaba descrita desde 1991 por Haber y Stornetta y la prueba de trabajo había sido ideada por Adam Back en 1997 en Hashcash. Estas partes se unen en un todo a partir del bloque Génesis, que se impone como mojón insoslayable para sus sucesores, una Crítica de la Razón Pura moderna: todas las criptomonedas que han surgido después no se pueden entender sin Bitcoin, y no se puede ya hablar del dinero sin remitirse a Bitcoin, aunque sea para criticarlo. Por último, también la gran hazaña de Satoshi fue quitar la broza y desplumar al ave. Eliminadas las terceras partes de confianza, queda a la vista el mecanismo desnudo: un sistema autónomo en el que se envía y recibe dinero, nada más y nada menos.

¿Cómo lo hizo Satoshi? ¿Cómo, uniendo piezas cual Lego, logró semejante hito? ¿Podrá el sabio profesor ayudarnos en esto?

"La historia de la vida de Immanuel Kant es difícil de relatar, pues no tuvo ni vida ni historia", escribió Heinrich Heine. Nunca salió de su Königsberg natal y su rutina era perfectamente metódica: se levantaba a las cinco, tomaba un (y solo un) té aguado, fumaba una (y solo una) pipa y trabajaba en sus clases y escritos hasta el mediodía. Nietzsche afirmaba que solo tienen valor los pensamientos que nos vienen caminando, máxima que bien podría haber suscrito Kant: cada tarde recorría la misma alameda ocho veces; ni una más, ni una menos. Su puntualidad era tal que los vecinos sabían la hora con solo verlo salir de casa. De ahí su sobrenombre: el Reloj de Königsberg.

Tick tock, next block

Bitcoin no es más que un libro mayor contable descentralizado y final en el que para añadir nuevas páginas —minar un bloque— se necesita adivinar un número concreto, y la única forma de adivinar este número es mediante fuerza bruta. Esto es lo que significa la prueba de trabajo. Pero apelar a la fuerza bruta — es decir, a la capacidad de cómputo — conlleva algunos problemas. Los primeros bloques de la cadena fueron minados por unos pocos entusiastas con sus ordenadores personales, pero cuanta más gente se unía al experimento, primero con CPUs, más tarde con GPUs y hoy con máquinas específicamente diseñadas para minar bitcoin, mayor era la potencia de cálculo; cabría esperar por lo tanto que los bloques se hallen cada vez más y más rápido, en una espiral exponencial que terminaría colapsando el sistema...

La respuesta a esta posible objeción está sucintamente respondida en el whitepaper:

> «Para compensar el aumento de la velocidad del hardware y el interés variable en ejecutar nodos a lo largo del tiempo, la dificultad de la prueba de trabajo se determina mediante un promedio móvil que busca mantener un número medio de bloques por hora. Si los bloques se generan demasiado rápido, la dificultad aumenta.»
>
> (Satoshi Nakamoto, Bitcoin: an electronic peer-to-peer cash system)

Cada 2016 bloques, la red calcula el intervalo promedio transcurrido entre ellos. Si es menor de diez minutos, la dificultad aumenta; si es mayor, disminuye. Este mecanismo de ajuste de dificultad convierte a Bitcoin en un reloj descentralizado.

Una religión de la Modernidad ha de incorporar, a la fuerza, algunos de los elementos en los que la Modernidad se sostiene. El reloj mecánico es uno de ellos. En tiempos pretéritos, cada comunidad vivía según su propio tiempo solar. El día comienza con el alba, termina con el ocaso y los campanarios fijaban el tiempo en cada localidad. Es el ferrocarril el que obliga a unificar el horario de los territorios bajo la férula de un mismo Estado. Barcelona y La Coruña comparten hoy la misma hora, aunque el sol se ponga en una mucho antes en la primera que en la segunda. En la Conferencia de Washington de 1884 se adoptó el meridiano de Greenwich como referencia, consolidando el Greenwich Mean Time (GMT) como estándar; un siglo más tarde, este sistema se refinaría con el Tiempo Universal Coordinado (UTC), basado ya en relojes atómicos y no en la rotación terrestre. La sistematización del tiempo es uno de los pilares de la modernidad, si no lo advertimos es porque, como el pez de David Foster Wallace, nadamos por sus aguas sin percibirlas. Ryszard Kapuściński, en su estancia como periodista en África, descubrió que allí el tiempo fluye de forma diferente:

> «Los europeos y los africanos tienen un concepto del tiempo enteramente distinto. En la cosmovisión europea, el tiempo existe fuera del hombre, existe objetivamente, y posee características mensurables y lineales. [...] [el europeo] necesita plazos, fechas, días y horas.»
>
> (Ryszard Kapuściński, Ébano)

De ahí también que, desde una mirada occidental, resulte desconcertante no poder encajar con precisión las cronologías antiguas. Decíamos en el anterior artículo que quizá Buda y Confucio fuesen contemporáneos, pero no lo podemos asegurar: mientras en China el tiempo se fechaba por reinados (año 22 del duque Xi de Lu, año 7 del rey Jing de Zhou) en India las referencias son míticas, y toda reconstrucción moderna queda en entredicho.

Bitcoin es una forma de consensuar si A va antes que B o viceversa. Da igual que una transacción se realice desde las antípodas de otra, ya que la cadena cumple la función que en nuestra era desempeñó el reloj mecánico: coordinar a multitudes dispersas bajo un mismo orden. La cadena dicta que transacción ocurrió antes que otra y, por tanto, quién puede gastar qué moneda. El timestamp del bloque, con su fecha UTC, enlaza el ciberespacio con el mundo físico. Es importante, pero no decisivo: si dos bloques aparecen casi al mismo tiempo, lo que determina cuál prevalece no es la marca temporal, sino sobre que rama se apila el siguiente bloque, convirtiéndola así en válida al acumular más prueba de trabajo. De esta manera, Bitcoin se eleva sobre lo material y se convierte en el metrónomo del ciberespacio, que ya no se mide por horas, minutos y segundos, sino por bloques.

De mecanismo a organismo

Decíamos que Bitcoin es el reloj del ciberespacio; podría argumentarse incluso que esta definición se queda corta. El reloj mecánico necesita que alguien le dé cuerda; Bitcoin, aunque también depende de energía externa, ha aprendido a darse cuerda a sí mismo. Su movimiento nace de la suma de miles de voluntades distribuidas que mantienen vivo el sistema sin necesidad de coordinación central. Es cierto que en sus primeros años, el sistema era frágil y vulnerable. Dependía de unos pocos participantes y la red latía con un pulso irregular. Los intervalos entre bloques, aun con el mecanismo de ajuste de dificultad incorporado, distaban de ser estables; con frecuencia superaban ampliamente los diez minutos previstos. Solo después de que Bitcoin fijara su primer precio de mercado, en el verano de 2010, el ritmo comenzó a estabilizarse. A partir de entonces, la cadencia de los bloques se volvió más constante, y el sistema empezó a comportarse, por primera vez, como un reloj fiable, aunque todavía minúsculo.

Esa primera etapa no estuvo exenta de tropiezos. En dos ocasiones el reloj mecánico hubo de ser detenido por los relojeros. En agosto de 2010 se produjo el llamado value overflow incident: un error en el código al operar con cantidades excesivamente grandes permitió crear de la nada más de ciento ochenta mil millones de bitcoins en una sola transacción. El fallo fue corregido, entre otros, por el propio Satoshi. Se publicó una nueva versión del cliente que modificaba las reglas de consenso para rechazar cualquier transacción con valores imposibles y se forzó una bifurcación de la cadena. Aunque algunos nodos siguieron minando sobre la versión defectuosa durante un breve tiempo, la cadena corregida la superó rápidamente y acabó imponiéndose como la historia legítima de Bitcoin. Tres años más tarde, en marzo de 2013, ya sin Satoshi, se produjo un nuevo sobresalto. La actualización del software a la versión 0.8, que introducía una nueva base de datos más eficiente, provocó una bifurcación inesperada: un bloque demasiado grande fue aceptado por los nodos recientes y rechazado por los antiguos. Durante cerca de seis horas coexistieron dos Bitcoin paralelos, cada uno con su propia versión de la historia. Los principales pools y plataformas de intercambio, como el exchange Mt. Gox, suspendieron depósitos ante el riesgo de dobles gastos, y el precio se desplomó brevemente un veinte por ciento. La crisis se resolvió cuando los mineros acordaron retroceder a la versión anterior del cliente, reagrupándose en una sola cadena.

Desde entonces, Bitcoin no ha vuelto a detenerse. Lleva más de doce años funcionando, literal y figuradamente, como un reloj: cada diez minutos, un nuevo bloque marca el paso del tiempo digital. En estos doce años, plataformas centralizadas de alcance mundial como Redsys o incluso Amazon Web Services han sufrido interrupciones y caídas temporales; mientras tanto, Bitcoin, impertérrito, seguía a lo suyo. Más que como un mecanismo, funciona ya como un organismo: un sistema vivo que mantiene su equilibrio interno ajustándose al entorno. Cuando en 2021 China prohibió la minería y el hash rate global se desplomó, la red reaccionó sin trauma. El protocolo redujo automáticamente la dificultad de minado, lo que permitió que máquinas menos potentes volvieran a encenderse y que la actividad se redistribuyera hacia otros países. A la vez, el precio —otra forma de energía, exógena pero vital para el ecosistema— fluctuó hasta encontrar un nuevo equilibrio. Bitcoin ha sido volátil desde su creación: los choques de mercado o de hash rate provocaban espasmos, largas pausas, subidas y bajadas vertiginosas. Con el tiempo, el organismo se ha vuelto más grande y más estable. Los relojeros que corrigieron los bugs de 2010 y 2013 hoy se mantienen en las sombras; cuando salen a la palestra es señal de que hay un amplio debate interno. Pero hoy esos relojeros tienen mucho menos poder que hace una década. Es el sistema al completo — desarrolladores, pero también nodos, mineros, usuarios, empresas... — el que importa y, cada día que pasa, se vuelve más robusto. Bitcoin ha alcanzado una suerte de **homeostasis digital**, una vida propia que late con independencia de quienes la sostienen.

Bitcoin es Logos

Para los estoicos, el Logos era la razón divina que gobierna el universo. Hoy asociamos el estoicismo con serenidad y firmeza ante la adversidad, pero esa actitud nace de una convicción más profunda: el mundo está regido por un orden inmutable, ante el cual los mortales solo podemos aceptar sus designios y aspirar a vivir de acuerdo con ellos. San Juan el Evangelista reinterpreta esta idea en clave cristiana: esa razón divina que gobierna el universo no es ya una ley impersonal, sino una presencia viva que encarna entre los hombres. El Logos se hace carne y habita el mundo y con ello el pensamiento se vuelve Palabra.

Cuando Satoshi Nakamoto publicó el whitepaper, propuso un nuevo Logos para la era digital. Ese principio racional fue creado como dinero, pero, como he tratado de explicar en el primer texto, del dinero y su naturaleza emana una forma de ser y de estar en el mundo. Esto se ejemplifica en las tendencias que proliferan entre los bitcoiners, tendencias con relación tangencial o nula con el dinero per se. Algunas de las más llamativas son la afición a levantar pesas o la adopción de una dieta carnívora, lo más alejada posible de lo que algunos han llegado a llamar Fiat Food. Por supuesto no todos siguen estos preceptos; hay numerosas formas de vivir la fe, tan válidas unas como otras. Pero sí que hay una serie de valores hacia los que se pivota por pura inercia una vez te tomas la pastilla naranja: en el segundo texto traté de analizar como la comunidad se cimenta alrededor de una serie de mitos y ritos; esos mitos y ritos se articulan en torno a un orden que se percibe como natural y trascendente.

Si con el nacimiento de Jesús la Palabra se hizo carne, en este caso en el bloque Génesis la Palabra se hace código. Al compás de la cadena surgen, bloque tras bloque, legiones de prosélitos con baja preferencia temporal, dispuestos a liberarse del fiat mundano para acceder a una instancia superior, pura, inmutable. Divina.

Bitcoin es el Logos del ciberespacio, **Palabra y Tiempo**, la ley universal que dicta cómo se escribe y ordena la Historia Digital.

Epílogo

En el año 384, cuatro años después del Edicto de Tesalónica que convirtió al cristianismo niceno en la religión oficial del Imperio, los nobles romanos Quinto Aurelio Símaco y Aurelio Ambrosio mantuvieron una disputa epistolar en torno al destino del recién retirado Altar de la Victoria. Símaco defendía su restitución apelando a la tolerancia religiosa y como emblema de la tradición romana; San Ambrosio, en nombre de Cristo, se oponía y amenazaba al emperador con la excomunión. Corrían tiempos de cambio en el Imperio y el altar no se repuso. Peter Brown, en su vasta obra Por el ojo de una aguja, narra el complejo proceso que terminó con buena parte de las riquezas romanas en manos de la Iglesia, y presenta a Símaco como representante arquetípico de la nobleza conservadora de la época, que aún era abundante e influyente (aunque cada vez menos) a finales del siglo IV. Esta élite aún se legitimaba a través del **evergetismo cívico**, es decir, mediante donaciones, juegos y obras públicas. Símaco costeó espectáculos para los romanos y contribuyó a embellecer la ciudad, no por que fuese particularmente filántropo, sino porque aquella era la norma en su tiempo. En el mundo romano no existía una diferenciación clara entre público y privado, lo que ahora llamamos “gasto público” era llevado a cabo por la nobleza. La riqueza circulaba de forma local, visible, tangible y compartida.

Ambrosio, al igual que Símaco, provenía de la aristocracia romana e hizo carrera como funcionario imperial. Siendo gobernador de Liguria y Emilia, acudió a mediar en la elección del nuevo obispo y la multitud le aclamó a él; en menos de una semana fue bautizado, ordenado, y consagrado obispo de Milán. San Ambrosio fue una de las figuras clave del nuevo orden cristiano, en el que importa mas la salvación eterna que los banquetes y la caridad sustituye a los fastos. Las enormes riquezas que antes financiaban naumaquias y combates de gladiadores ahora se entregan a las iglesias en busca de redención. Estas comienzan a funcionar como proto-corporaciones: reciben donaciones, administran propiedades y distribuyen limosnas entre los pobres. Una parte de esos tesoros dejaba de circular: el oro se acumulaba en cálices, patenas y otros ornamentos litúrgicos. Guardado en los templos, salía del circuito económico profano. Se sacralizaba.

El oro y la plata son, de entre todos los elementos de la tabla periódica, los más aptos para convertirse en dinero. No se oxidan, son homogéneos, divisibles, fácilmente transportables, difíciles de falsificar y, por último, escasos. Es la escasez lo que hace al oro más valioso que la plata, dándole una dimensión casi sagrada. No es de extrañar que los altares en los que los sacerdotes realizan la transubstanciación se adornen con reliquias doradas, sacando al metal del ámbito humano y consagrándolo divino. Bitcoin lleva la lógica de la escasez al extremo. Siempre cabe la posibilidad de hallar nuevos yacimientos, ya hemos visto las implicaciones del descubrimiento de la plata de Potosí y tres siglos más tarde sucedió algo similar con la fiebre del oro californiana. No es posible hallar nuevas minas de bitcoin: nunca habrá más de 21 millones.

Símaco empleaba su fortuna en espectáculos y edificios para honrar a Roma, Ambrosio, en limosnas y liturgias para honrar a Cristo. Michael Saylor, fundador de MicroStrategy, quiere honrar a Bitcoin: usa su empresa para acumular todo lo que puede, busca nuevas formas de financiación para acumular aún más, y vende acciones, bonos y preferentes a quienes quieren exposición a bitcoin sin salirse del circuito tradicional o sin asumir su enorme volatilidad. En una entrevista reciente, Saylor ha mencionado la idea de no legar a nadie sus propias claves privadas al morir y así sacarlas de circulación para siempre, lo que sería, en sus propias palabras, “una forma de caridad éticamente correcta” y le traería la “**inmortalidad económica**”. Esa inmortalidad ya ha sido alcanzada por por Satoshi, que almacena en sus direcciones algo más de 1 millón de bitcoins. Cada día que pasa sin que se muevan es un triunfo para la Red. Llevan ya tres lustros allí, engastados como reliquias en las primeras páginas del Libro, y allí permanecen...

Esperemos que para toda la eternidad.

Cambialo por Bitcoin!!!

AUTOR: Ruiz ART

Artista, Bitcoiner y lo que surja.

La serie “Cámbialo por Bitcoin” nace como una respuesta crítica y poética del artista Ruiz ART ante la reciente propuesta de la Unión Europea para rediseñar los billetes de euro.

Frente a la idea de renovar la iconografía del dinero fiat, Ruiz propone una reflexión más profunda: ¿tiene sentido seguir embelleciendo un sistema monetario que se desmorona?

Estas piezas reinterpretan el billete tradicional como soporte de resistencia cultural. Cada denominación —del 5 al 500— se transforma en un lienzo donde conviven referencias al cubismo, al expresionismo y a la iconografía histórica del arte español. Cuerpos fragmentados, gritos, símbolos y escenas cargadas de tensión hablan del sufrimiento que acompaña al dinero intervenido por los Estados, sujeto a inflación y control.

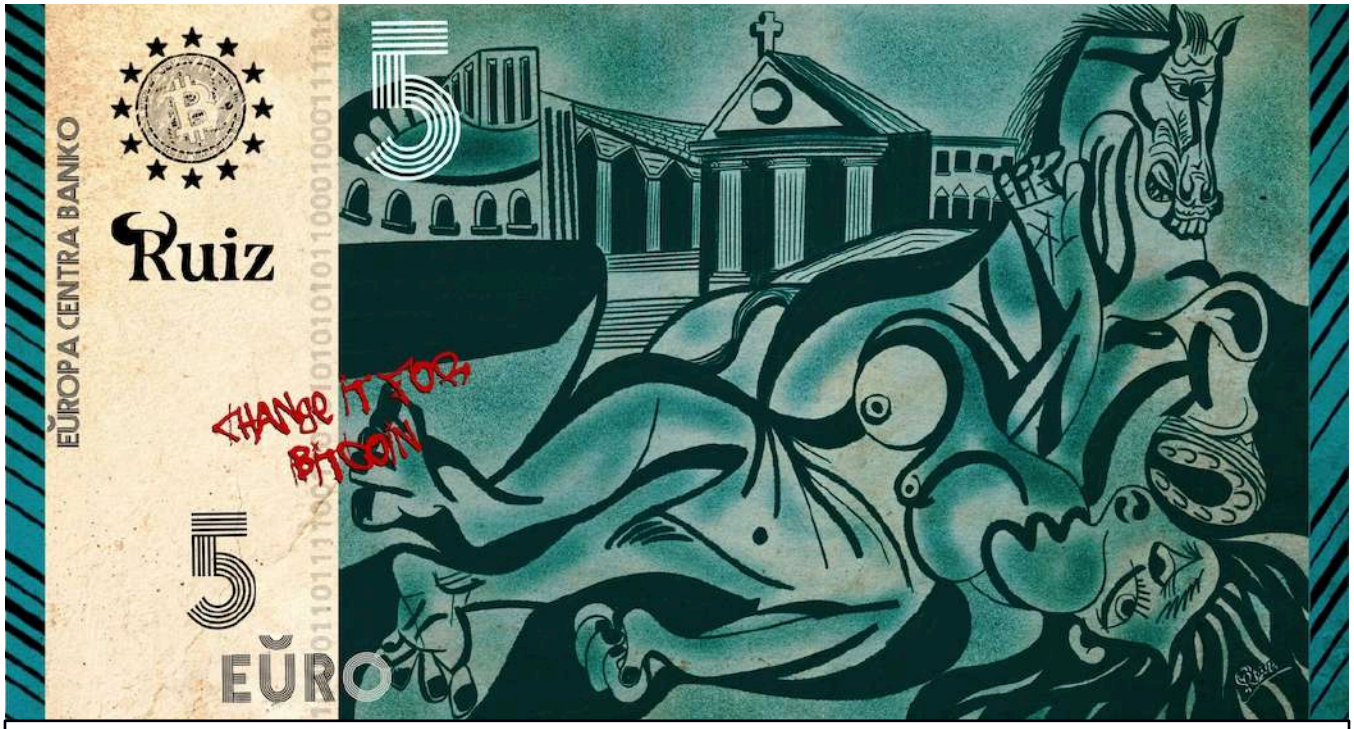
En el margen izquierdo, como un grafiti urgente, aparece el mensaje: CHANGE IT FOR BITCOIN

Una llamada a la acción. Una invitación a cambiar un papel que pierde valor, por un código descentralizado que devuelve soberanía.

Ruiz ART no propone únicamente un diseño alternativo de billetes: propone un cambio de paradigma. El arte como barricada, la estética como protesta, la moneda como libertad.

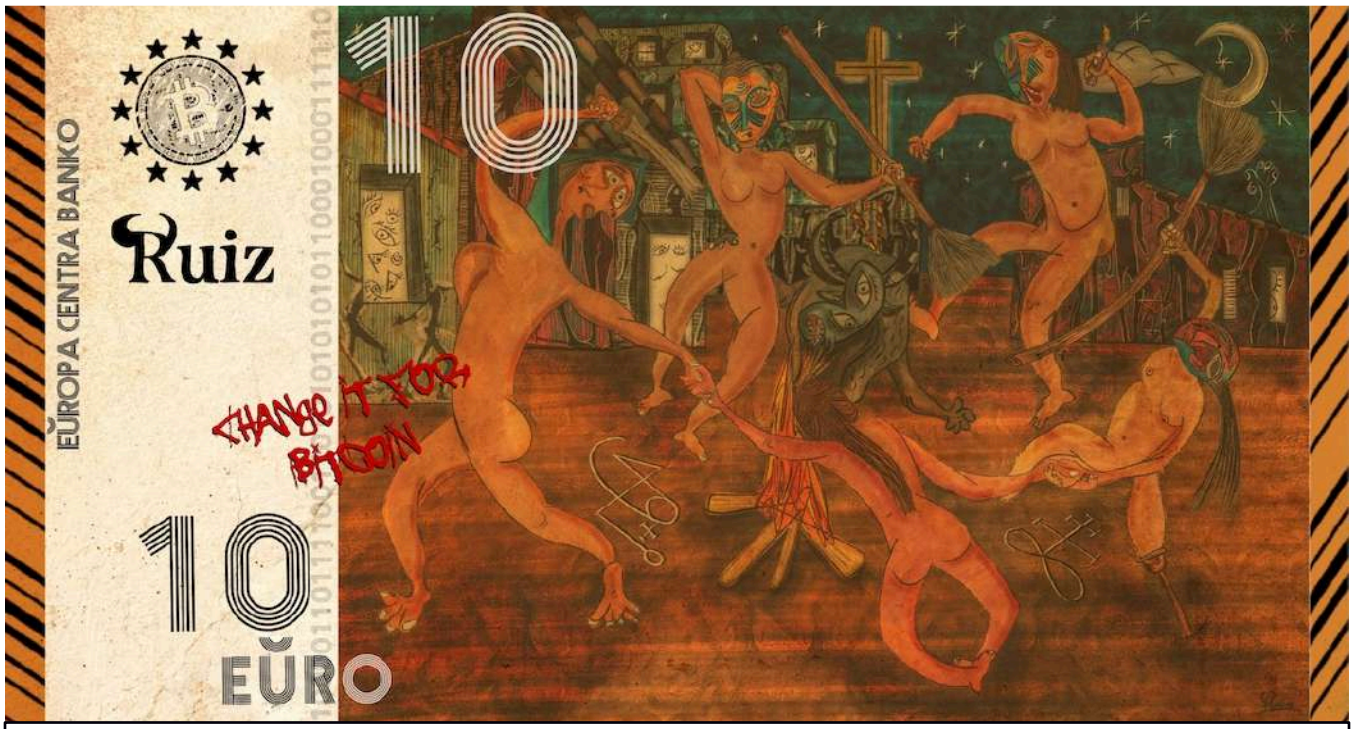
Cámbialo por Bitcoin.

Porque el valor real es el que nadie puede censurar.



Valor 5 Euros - Change it for Bitcoin

Aprendiendo de las Sabinas

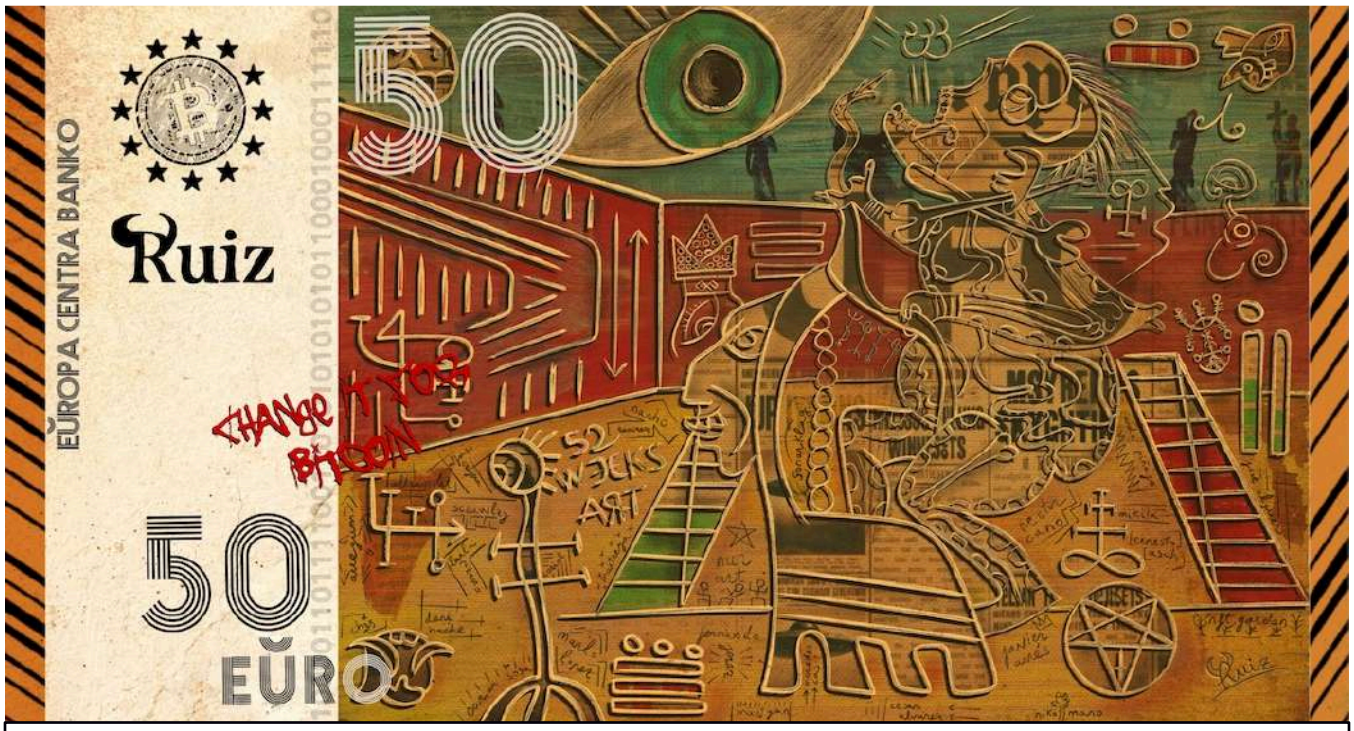


Valor 10 Euros - Change it for Bitcoin

Zugarramurdi

Valor 20 Euros - Change it for Bitcoin

Sirena en la noche



Valor 50 Euros - Change it for Bitcoin

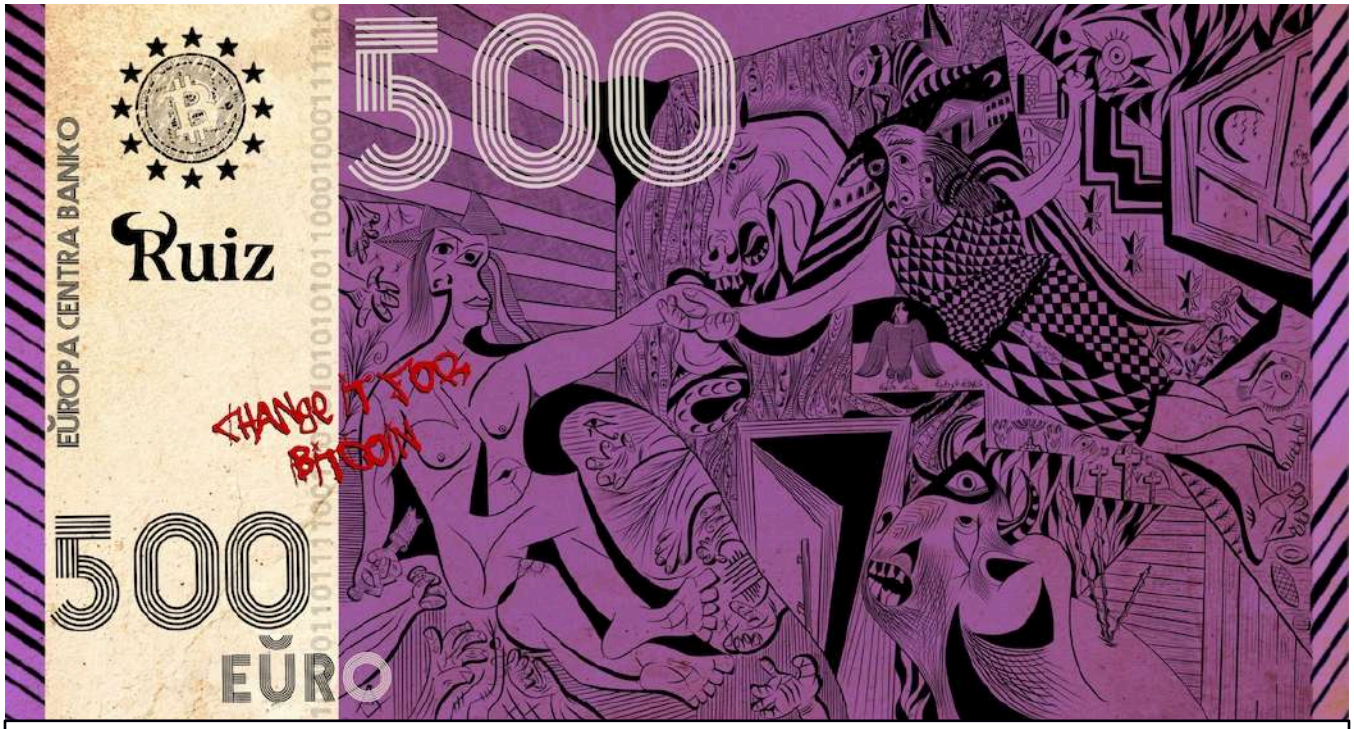
El lamento del Serpiente.

Valor 100 Euros - Change it for Bitcoin

Mujer desnuda bajo un pino

Valor 200 Euros - Change it for Bitcoin

Retrato de Mujer en la casa de campo



Valor 500 Euros - Change it for Bitcoin

La Creacion: Compilación Interrumpida.

Bitcoin, Herramienta de la Escuela Austriaca

Autor: FreeBTC (Movimiento Cypherpunk 2025)

freebtcmx@proton.me

I. Introducción

El pensamiento económico contemporáneo se encuentra en un punto de inflexión histórico. La revolución digital, el avance de las tecnologías descentralizadas y la crisis de confianza hacia las instituciones financieras tradicionales han reabierto preguntas fundamentales sobre la naturaleza y el futuro del dinero. En este contexto, Bitcoin emerge no solo como una innovación tecnológica, sino como una herramienta teórica y práctica alineada con los principios esenciales de la Escuela Austriaca de Economía, ofreciendo una alternativa sólida al modelo monetario basado en dinero fiduciario.

La Escuela Austriaca, iniciada en el siglo XIX por Carl Menger, sostiene que el valor económico no es una magnitud objetiva ni determinada por la planificación central, sino el resultado de las decisiones individuales en un proceso dinámico de mercado. Menger señaló que "el valor no es inherente al bien, sino que se asigna subjetivamente por cada individuo según la importancia que atribuye a la satisfacción de sus necesidades". En consecuencia, el dinero debe surgir espontáneamente del mercado como el bien más líquido y universalmente aceptado, no como una imposición estatal. Como argumentó Friedrich Hayek, "el dinero es una institución creada por el mercado y no por el Estado".

Sin embargo, la evolución moderna del sistema financiero se ha separado radicalmente de estos principios. El dinero fiduciario se sostiene por decretos gubernamentales y políticas monetarias expansivas, lo que ha generado ciclos recurrentes de inflación, endeudamiento y pérdida de poder adquisitivo. Ludwig von Mises advirtió que "no existe medio más seguro de destruir una sociedad que corromper su moneda", identificando la manipulación del suministro monetario como una de las causas estructurales de las crisis económicas.

Bitcoin aparece precisamente como respuesta a ese deterioro del sistema monetario. Diseñado por Satoshi Nakamoto en 2008, combina criptografía, redes distribuidas y una política monetaria programada e inalterable. En palabras del propio Satoshi, "la raíz del problema con la moneda convencional es toda la confianza necesaria para que funcione". Bitcoin elimina esa necesidad de confianza mediante un protocolo abierto, verificable y resistente a la censura, proporcionando un estándar monetario digital capaz de devolver estabilidad y previsibilidad al intercambio económico.

Este documento analiza la relación profunda entre Bitcoin y los fundamentos teóricos de la Escuela Austriaca, mostrando cómo esta tecnología constituye una implementación práctica del ideal de dinero sólido, descentralizado y libre de intervención política. Su objetivo es exponer, desde una perspectiva académica, cómo Bitcoin materializa conceptos clave como la subjetividad del valor, la imposibilidad del cálculo económico bajo planificación central, la importancia del ahorro y la competencia monetaria, y la defensa de la libertad individual frente al poder coercitivo del Estado.

En esta línea, el presente estudio se estructura en varios capítulos que revisan los orígenes y postulados principales de la tradición austríaca, el debate sobre la naturaleza del dinero, el análisis crítico del sistema FIAT, la emergencia de Bitcoin y sus implicaciones económicas, sociales y políticas. Pretende, por tanto, ofrecer un marco de comprensión riguroso para interpretar Bitcoin no como una moda tecnológica, sino como una evolución histórica coherente con el desarrollo del pensamiento económico liberal y la búsqueda de una verdadera soberanía monetaria.

La influencia de la Escuela de Salamanca

Aunque suele situarse el origen formal de la Escuela Austriaca en la obra de Carl Menger, es necesario señalar una genealogía intelectual más profunda que se remonta al pensamiento económico desarrollado en España durante el siglo XVI, especialmente dentro de la llamada Escuela de Salamanca. Este movimiento intelectual, surgido en el contexto del Siglo de Oro español, anticipó numerosos principios teóricos que posteriormente serían retomados y formalizados por los economistas austríacos.

Los teólogos juristas de Salamanca, entre los que destacaron Francisco de Vitoria, Martín de Azpilcueta y Domingo de Soto, reflexionaron sobre la justicia, el comercio, la propiedad privada y el valor de los bienes en el marco de una economía en expansión y de una profunda transformación monetaria causada por la llegada masiva de metales preciosos de América. En este contexto, Martín de Azpilcueta formuló una idea que hoy

identificaríamos como una explicación temprana de la inflación monetaria: "el dinero vale más donde y cuando es más escaso que donde y cuando es más abundante".

Del mismo modo, la concepción subjetiva del valor, piedra angular de la Escuela Austriaca, aparece claramente en la obra de Juan de Mariana, quien afirmó que "la estimación del precio no depende de la naturaleza de las cosas, sino de la valoración que los hombres hacen de ellas".

Dentro de este marco, la figura de Francisco de Vitoria resulta fundamental. Considerado uno de los fundadores del derecho internacional moderno, Vitoria argumentó que la libertad de comercio era una extensión natural de los derechos humanos y que "el precio justo nace de la estimación común en el mercado".

Friedrich Hayek reconoció esta línea histórica cuando escribió que "el espíritu de la libertad económica fue formulado durante la escolástica tardía española mucho antes que en cualquier otro lugar".

Así, Bitcoin puede interpretarse como la culminación tecnológica de una tradición intelectual que se ha desarrollado desde el Siglo de Oro español hasta la actualidad: la búsqueda de un sistema monetario basado en leyes naturales del intercambio y no en la imposición.

II. Origen y fundamentos de la Escuela Austriaca

La Escuela Austriaca de Economía surge oficialmente a finales del siglo XIX en el contexto del Imperio Austrohúngaro, en un momento de profundas transformaciones económicas e intelectuales en Europa. La disciplina económica atravesaba una crisis metodológica vinculada al dominio del historicismo alemán y al enfoque objetivista de la teoría del valor, centrada en los costes de producción como determinantes del precio. En ese escenario, Carl Menger publica en 1871 Principios de Economía, obra considerada el nacimiento formal de la tradición austríaca y una ruptura radical con la teoría económica dominante.

Menger planteó que el valor económico no deriva de las propiedades físicas de los bienes ni de su coste de producción, sino de la importancia subjetiva que cada individuo atribuye a la satisfacción de sus necesidades. Esta formulación, conocida como teoría subjetiva del valor, se expresa claramente en su afirmación: "el valor no se determina por los costes pasados sino por la utilidad marginal futura esperada por cada individuo". Esta idea transformó la economía al situar la acción humana como fundamento del análisis económico.

A partir de esta revolución conceptual se desarrolló el marginalismo, que permitió explicar de manera coherente fenómenos que habían resultado problemáticos para la economía clásica, como la paradoja del valor que compara el valor del agua y el del diamante. Para Menger, la utilidad marginal decreciente explica que un bien esencial puede tener menor valor económico que un bien suntuario si su disponibilidad relativa es mayor.

Tras Menger, la Escuela Austriaca se consolidó con autores como Eugen Böhm-Bawerk y Friedrich von Wieser. Böhm-Bawerk elaboró una teoría del capital y del interés basada en la preferencia temporal, defendiendo que el interés no es una explotación sino una compensación por el tiempo y el riesgo. En sus palabras: "el interés es el precio que se paga por preferir bienes presentes frente a bienes futuros". Wieser, por su parte, desarrolló el concepto de coste de oportunidad, mostrando que el coste real de cualquier decisión económica es aquello a lo que se renuncia.

A comienzos del siglo XX, la Escuela Austriaca alcanzó su madurez teórica con Ludwig von Mises, quien formuló la praxeología como ciencia de la acción humana y señaló que la economía no puede basarse en métodos empíricos propios de las ciencias naturales. Según Mises, "la economía es la ciencia de la acción humana" y esta acción está guiada por fines subjetivos que no pueden capturarse mediante experimentación cuantitativa.

Mises también realizó una crítica determinante al socialismo en su obra de 1922 Socialismo, donde argumentó la imposibilidad del cálculo económico bajo planificación central. Sostuvo que sin precios de mercado para los bienes de capital no existe forma racional de asignar recursos. Su célebre afirmación resume el problema: "sin propiedad privada de los medios de producción no pueden existir precios y sin precios no puede existir cálculo económico".

El legado teórico de Mises fue continuado por Friedrich Hayek, quien profundizó en la teoría del conocimiento y la función de los precios como mecanismo de información distribuida. Hayek defendió que el mercado es un orden espontáneo que coordina decisiones dispersas sin necesidad de una autoridad central, afirmando que "ninguna autoridad central puede poseer el conocimiento necesario para dirigir la economía". Su defensa de la libertad económica quedó reflejada en otra afirmación decisiva: "la planificación económica conduce inevitablemente a la pérdida de la libertad política".

En suma, la Escuela Austriaca se caracteriza por varios principios esenciales:

- La teoría subjetiva del valor
- La importancia del tiempo y la preferencia temporal en la estructura del capital
- La imposibilidad del cálculo económico bajo planificación central
- La economía como estudio de la acción humana y no como mecanicismo cuantitativo
- La defensa del orden espontáneo y la limitación del poder estatal

Estos fundamentos anticipan muchas de las cuestiones que Bitcoin vendría a materializar en el siglo XXI: un dinero no manipulado políticamente, una estructura descentralizada emergente del orden espontáneo y un sistema de reglas predecibles no sujeto a la discrecionalidad estatal. En palabras de Mises, "el dinero sano es un instrumento para proteger las libertades civiles contra las usurpaciones despóticas del Estado". La aparición de Bitcoin reabre la vigencia de esta tesis central y confirma la relevancia contemporánea del pensamiento austríaco.

III. Concepto de dinero desde la tradición austriaca

El concepto de dinero ha acompañado a la humanidad desde los primeros intercambios económicos y constituye uno de los elementos esenciales para comprender el desarrollo social y político de las civilizaciones. Desde la perspectiva de la Escuela Austriaca de Economía, el dinero no es una creación artificial impuesta por el poder político, sino el resultado de un proceso histórico espontáneo mediante el cual los individuos, buscando maximizar su propia capacidad de intercambio, seleccionan de manera progresiva los bienes más líquidos y universalmente aceptados como medio común de intercambio.

Carl Menger describió este proceso como una evolución natural del mercado y no como una decisión legislativa. En sus palabras: "el dinero surge de manera natural del esfuerzo de los hombres por facilitar el intercambio". Según esta formulación, la función del dinero es resolver las limitaciones del trueque directo, permitiendo el intercambio indirecto mediante un bien ampliamente demandado y fácilmente transferible.

Evolución histórica hacia el dinero mercancía

En los primeros estadios económicos, el intercambio se realizaba mediante el trueque, sistema que pronto mostró sus limitaciones debido a la necesidad

de coincidencia de deseos entre comprador y vendedor. Ante esta dificultad, los individuos comenzaron a utilizar ciertos bienes especialmente valorados por su durabilidad, divisibilidad, transportabilidad y reconocimiento social: metales preciosos, sal, especias, ganado o herramientas. Así se desarrolló, de manera progresiva, la noción de dinero mercancía.

El oro y la plata terminaron estableciéndose como estándares monetarios predominantes debido a sus propiedades físicas y a su aceptación global. La Escuela Austriaca subraya que esta aceptación no fue resultado de una imposición estatal sino de la libre interacción entre agentes económicos. Como señaló Friedrich Hayek: "el Estado no ha inventado el dinero, ni es indispensable para su funcionamiento".

Funciones esenciales del dinero

Desde esta perspectiva, el dinero cumple tres funciones fundamentales:

- Medio de intercambio
- Depósito de valor
- Unidad de cuenta

Para que estas funciones se mantengan, el dinero debe conservar su poder adquisitivo a lo largo del tiempo, evitando ser objeto de manipulación política. Ludwig von Mises afirmó que "el dinero sano es un instrumento para proteger las libertades civiles contra las usurpaciones despóticas del Estado".

Dinero fiduciario y pérdida de solidez monetaria

El paso del dinero mercancía al dinero fiduciario marcó un punto de inflexión decisivo. Los sistemas bancarios comenzaron emitiendo certificados convertibles en oro o plata, pero con el tiempo la convertibilidad fue reducida e incluso eliminada, culminando en 1971 con la suspensión definitiva del patrón oro por parte del gobierno de Estados Unidos.

Desde ese momento, el dinero pasó a depender exclusivamente de decisiones políticas y de la confianza en los emisores estatales. Esta ruptura histórica abrió la puerta a políticas monetarias expansivas y al crecimiento constante de la deuda pública. Mises advirtió que "no existe medio más seguro de destruir una sociedad que corromper su moneda".

La inflación, entendida desde la perspectiva austríaca como expansión artificial de la oferta monetaria, actúa como un impuesto no legislado que erosiona el ahorro y distorsiona los precios relativos, generando ciclos artificiales de auge y caída económica.

El papel del dinero sólido

La tradición austríaca sostiene que la estabilidad monetaria solo puede lograrse mediante un sistema donde el dinero esté vinculado a un mecanismo que limite su expansión arbitraria. Böhm-Bawerk y Mises defendieron que el dinero sólido es condición necesaria para el cálculo económico racional, el ahorro productivo y la libertad individual frente a la planificación central.

De esta manera, el concepto de dinero sólido adquiere una dimensión ética y política además de económica. Como expresó Hayek: "la planificación económica conduce inevitablemente a la pérdida de la libertad política". La intervención monetaria no solo distorsiona la economía real, sino que otorga al Estado un poder creciente sobre la vida social.

En este contexto, la aparición de Bitcoin en 2008 representa una nueva fase en la evolución histórica del dinero. Su diseño programado, transparente y limitado a 21 millones de unidades constituye una respuesta directa a los principios monetarios defendidos por la Escuela Austriaca: un dinero no sujeto a decisiones arbitrarias de ninguna autoridad central y basado en reglas estables.

Satoshi Nakamoto señaló: "la raíz del problema con la moneda convencional es toda la confianza necesaria para que funcione". Bitcoin elimina esta dependencia de confianza sustituyéndola por verificación criptográfica y consenso descentralizado.

Así, Bitcoin se presenta como la primera implementación tecnológica de un dinero sólido en la era digital, recuperando la tradición iniciada por la Escuela de Salamanca, desarrollada por la Escuela Austriaca y abruptamente interrumpida por la era del dinero fiduciario.

IV. Crisis del dinero FIAT y planificación central

La transición desde el dinero mercancía hacia el dinero fiduciario supuso una transformación estructural en el funcionamiento de la economía global. Mientras que en el patrón oro tradicional la oferta monetaria estaba limitada por la disponibilidad física de metal, el dinero fiduciario carece de respaldo material y su emisión depende exclusivamente de decisiones políticas y bancarias. Desde la perspectiva de la Escuela Austriaca, este cambio constituye la causa principal de los ciclos recurrentes de inflación, endeudamiento y crisis financieras que caracterizan a la economía moderna.

Ludwig von Mises advirtió que "no existe medio más seguro de destruir una sociedad que corromper su moneda", señalando que el uso del dinero fiduciario permite al Estado apropiarse de riqueza de forma encubierta mediante expansión monetaria e inflación. La teoría austríaca sostiene que la inflación no es simplemente un aumento general de precios, sino "una expansión artificial de la oferta monetaria" que distorsiona el sistema de precios y genera asignaciones ineficientes de recursos.

El efecto Cantillon y la desigualdad estructural

El economista Richard Cantillon describió cómo la emisión de nuevo dinero beneficia en primer lugar a quienes lo reciben antes de que los precios se ajusten, generalmente el sistema financiero y el sector público, mientras que los ciudadanos comunes lo reciben cuando el aumento de precios ya se ha materializado. Cantillon sintetizó este fenómeno afirmando que "la inflación beneficia siempre a los primeros receptores del nuevo dinero en perjuicio de los últimos". Este mecanismo redistributivo explica el aumento constante de la desigualdad bajo regímenes monetarios expansivos.

Ciclo económico austríaco y crédito artificial

Mises y Hayek desarrollaron la teoría austríaca del ciclo económico, según la cual las expansiones artificiales del crédito, impulsadas por bancos centrales con tipos de interés artificialmente bajos, generan periodos de auge económico seguidos de crisis inevitables. Como señaló Mises: "El crédito artificial conduce a recesiones inevitables". Las inversiones no sostenibles financiadas con dinero creado ex nihilo terminan colapsando cuando el mercado revela la ausencia de ahorro real.

Ejemplos históricos de crisis monetarias

La historia reciente ofrece numerosos ejemplos de los efectos destructivos del dinero fiduciario y la planificación centralizada:

- República de Weimar (1921-1923): la impresión masiva de dinero para financiar la deuda de guerra provocó una hiperinflación extrema donde los precios se duplicaban cada pocas horas. La población llegó a transportar billetes en carretillas mientras los salarios perdían valor instantáneamente.
- Zimbabue (2007-2008): el gobierno imprimió billetes con denominaciones de trillones de dólares. La afirmación popular "no hay nada más inútil que el dinero que pierde valor mientras lo sostienes en la mano" se convirtió en realidad cotidiana.
- Argentina (siglo XX y XXI): sucesivas devaluaciones, default soberano y controles de capital muestran la fragilidad estructural del dinero estatal sin límites de emisión.
- Venezuela (2014-2021): la hiperinflación destruyó la capacidad de ahorro y provocó la migración masiva de millones de personas.
- Estados Unidos (1971-actualidad): la suspensión definitiva del patrón oro marcó el inicio de un periodo de inflación permanente y crecimiento acelerado de deuda. Tras la crisis financiera de 2008, la política de flexibilización cuantitativa (QE) expandió masivamente la base monetaria, generando una subida artificial de activos financieros. La emisión extraordinaria durante la crisis de 2020 confirmó que el sistema monetario se ha desvinculado completamente de cualquier restricción material.

El papel de los bancos centrales

Los bancos centrales, creados originalmente para estabilizar el sistema financiero, se han convertido en instituciones con poder casi absoluto sobre la política monetaria. Friedrich Hayek señaló que "un banco central no puede conocer más que la ilusión del control" y que la planificación central del dinero conduce a errores sistemáticos imposibles de corregir mediante intervención.

La política monetaria moderna se ha transformado en un mecanismo permanente de rescate financiero donde pérdidas privadas se socializan y beneficios se privatizan, debilitando el vínculo entre riesgo y responsabilidad, fundamento esencial del orden económico liberal.

Camino hacia la centralización total: CBDC y control social

El surgimiento de las monedas digitales de banco central (CBDC) plantea un escenario donde el Estado adquiere la capacidad de supervisar, restringir y programar el uso del dinero, eliminando cualquier rastro de privacidad económica. La planificación central alcanza así un nuevo estadio: el control directo del comportamiento ciudadano. Como advirtió Hayek: "la planificación económica conduce inevitablemente a la pérdida de la libertad política".

Crisis estructural y límite del sistema FIAT

La acumulación global de deuda y la divergencia creciente entre economía real y economía financiera revelan que el sistema FIAT se sostiene cada vez más sobre expansión monetaria continua. La Escuela Austriaca sostiene que este modelo está condenado al colapso, ya sea por hiperinflación o por deflación severa.

La aparición de Bitcoin en este contexto no es un accidente histórico, sino una respuesta tecnológica a esta crisis estructural. Al eliminar la capacidad de manipulación política del dinero y establecer una oferta monetaria estrictamente limitada, Bitcoin constituye una alternativa creíble al orden monetario FIAT.

Como afirmó Satoshi Nakamoto: "la raíz del problema con la moneda convencional es toda la confianza necesaria para que funcione". Bitcoin, por primera vez en la historia, permite un dinero sólido sin necesidad de confiar en ninguna autoridad central.

V. El problema del cálculo económico

El problema del cálculo económico constituye uno de los pilares teóricos más influyentes de la Escuela Austriaca y una de las críticas más sólidas al socialismo y a cualquier sistema de planificación centralizada de la economía. Formulado por Ludwig von Mises en 1920 y posteriormente ampliado por Friedrich Hayek, este argumento sostiene que la asignación racional de recursos es imposible sin precios formados libremente en un mercado competitivo, ya que solo dichos precios reflejan información real sobre preferencias, escasez y valor relativo.

Mises sintetizó el núcleo del problema afirmando que "sin propiedad privada de los medios de producción no pueden existir precios, y sin precios no puede existir cálculo económico". En ausencia de precios reales, los planificadores centrales carecen de la información necesaria para decidir qué producir, en qué cantidad, con qué métodos y para quién. La economía se convierte entonces en un proceso arbitrario y políticamente dirigido, incapaz de coordinar millones de decisiones individuales.

Hayek profundizó en esta idea subrayando que el conocimiento económico está disperso entre todos los individuos y que ninguna autoridad central puede reunirlo o procesarlo de manera eficiente. En sus palabras: "el problema económico fundamental es el uso del conocimiento que nadie posee completamente". Para Hayek, los precios actúan como señales que condensan información compleja y permiten coordinar acciones sin necesidad de planificación explícita.

Ejemplos históricos del fracaso del cálculo central

La historia económica del siglo XX ilustra con claridad las consecuencias de ignorar estas advertencias. La Unión Soviética intentó durante décadas planificar toda su economía, estableciendo precios, cantidades y objetivos productivos mediante organismos burocráticos. El resultado fue una asignación ineficiente de recursos, escasez crónica de bienes esenciales y una productividad muy por debajo de la de las economías de mercado.

El experimento agrícola soviético de los años 30, basado en cuotas estatales y confiscación de propiedad privada, condujo a la hambruna más devastadora de Europa en tiempos de paz. La imposibilidad de que los precios transmitieran información real provocó desajustes extremos entre oferta y demanda.

En China, durante el llamado Gran Salto Adelante (1958–1962), la planificación centralizada impulsó decisiones económicas desconectadas de las necesidades reales de la población, lo que desencadenó una hambruna que causó más de treinta millones de muertes. Estos episodios mostraron que sin mecanismos de mercado no existe feedback útil para corregir errores.

Planificación económica contemporánea y crisis energética europea

Aunque los ejemplos anteriores pertenecen a economías históricamente socialistas, el argumento de Mises y Hayek continúa siendo plenamente vigente. En la Europa del siglo XXI, la planificación política del sector energético, basada en subsidios masivos, intervención en precios y prohibiciones regulatorias, ha provocado crisis estructurales, incluyendo escasez y precios artificialmente elevados.

La imposición de precios máximos a la energía en varios países europeos redujo la inversión y deterioró la capacidad de producción, demostrando que ignorar la función informativa de los precios genera distorsiones que terminan soportando los consumidores y empresas.

El vínculo entre planificación central, inflación y distorsión económica

La expansión monetaria coordinada por bancos centrales y gobiernos contribuye a agravar estos problemas al manipular los precios relativos mediante el crédito barato. Las distorsiones resultantes conducen a inversiones no sostenibles y crisis recurrentes. Como afirmó Mises: "las crisis no son fallos del mercado, sino consecuencias inevitables de la intervención y el crédito artificial".

La acumulación creciente de deuda pública y privada, especialmente tras las políticas de expansión monetaria post-2008 y post-2020, evidencia que la planificación central ha sustituido señales reales de mercado por una dependencia permanente de inyecciones de liquidez.

Bitcoin ofrece una alternativa radical al problema del cálculo económico basado en planificación centralizada. Su protocolo reemplaza la autoridad humana por reglas matemáticas transparentes y resistentes a la modificación política. El consenso distribuido y la verificabilidad criptográfica transforman la estructura informacional del dinero.

Mientras el sistema FIAT depende de decisiones discrecionales y anticipa escasez o abundancia monetaria basada en intereses políticos, Bitcoin establece un modelo donde la oferta

monetaria es fija y conocida por todos, eliminando la incertidumbre creada por la intervención. Como señaló Hayek: "debemos idear alguna forma de retirar al Estado su monopolio sobre el dinero".

Desde esta perspectiva, Bitcoin puede entenderse como la primera herramienta tecnológica que materializa los principios expuestos por Mises y Hayek: precios reales, información distribuida y coordinación social basada en reglas y no en decisiones políticas. La imposibilidad de manipular su oferta protege el cálculo económico del deterioro sistemático provocado por políticas monetarias expansivas.

VI. La emergencia de Bitcoin

La aparición de Bitcoin en 2008 constituye un punto de inflexión histórico en la evolución del dinero y una respuesta directa a la crisis estructural del sistema financiero global. El contexto inmediato fue la crisis financiera internacional de 2007-2008, marcada por el colapso de grandes instituciones bancarias, rescates estatales masivos y una pérdida profunda de confianza social en el sistema monetario. El principio "Too Big To Fail" dejó claro que el riesgo y la responsabilidad habían sido disociados: grupos financieros privados obtenían beneficios en épocas de bonanza, mientras que las pérdidas eran socializadas a través de los contribuyentes.

En este ambiente de deslegitimación del sistema FIAT, el 31 de octubre de 2008 Satoshi Nakamoto publicó el documento Bitcoin: A Peer-to-Peer Electronic Cash System, proponiendo un sistema de dinero electrónico descentralizado basado en pruebas criptográficas en lugar de confianza institucional. Satoshi afirmó: "la raíz del problema con la moneda convencional es toda la confianza necesaria para que funcione" y advirtió sobre la fragilidad del sistema bancario: "los bancos deben ser confiables para guardar nuestro dinero y transferirlo electrónicamente, pero lo prestan en oleadas de burbujas con apenas una fracción en reserva".

El 3 de enero de 2009 Satoshi minó el primer bloque de Bitcoin, conocido como Génesis Block, que contenía una inscripción histórica: The Times 03/Jan/2009 Chancellor on brink of second bailout for banks. Esta frase, tomada del titular de un periódico británico, constituye una declaración explícita de motivación política y filosófica: Bitcoin nace como respuesta a un sistema monetario basado en rescates, inflación estructural y concentración de poder.

Fundamentos técnicos esenciales

Bitcoin combina diversas tecnologías preexistentes —criptografía de clave pública, redes distribuidas y pruebas de trabajo— en una arquitectura innovadora capaz de resolver el problema del doble gasto sin necesidad de una autoridad central. La blockchain actúa como un registro público e inmutable donde las transacciones se verifican colectivamente mediante consenso descentralizado.

El mecanismo de Proof of Work garantiza que la seguridad de la red dependa del coste real de computación y energía, impidiendo la manipulación arbitraria del historial de transacciones. Esta estructura elimina la necesidad de confianza personal o institucional y la sustituye por verificación automática. Como señaló Satoshi: "necesitamos un sistema basado en pruebas criptográficas en lugar de confianza".

Política monetaria programada y dinero sólido digital

Uno de los elementos más innovadores de Bitcoin es su política monetaria estrictamente limitada: solo existirán 21 millones de unidades y la emisión disminuye progresivamente mediante eventos conocidos como halving, que reducen la recompensa de minería aproximadamente cada cuatro años. Esta programación convierte a Bitcoin en la primera forma de dinero digital con escasez verificable, equivalente funcional al oro pero sin dependencia de custodia física.

La comparación con el oro es recurrente debido a que ambos comparten propiedades esenciales: escasez, divisibilidad, durabilidad y resistencia a la censura. Sin embargo, Bitcoin introduce ventajas fundamentales: transferencias globales instantáneas, fraccionabilidad extrema y ausencia de requerimientos de confianza en terceros.

Bitcoin como implementación de los principios austríacos

Bitcoin puede interpretarse como la realización tecnológica de ideas desarrolladas por la Escuela Austriaca durante más de un siglo. La teoría subjetiva del valor explica su valorización progresiva basada en la utilidad percibida por los individuos.

Su política monetaria inmutable retoma el ideal de dinero sólido defendido por Mises, quien afirmó que "el dinero sano es un instrumento para proteger las libertades civiles contra las usurpaciones despóticas del Estado".

Asimismo, la estructura descentralizada de Bitcoin refleja la teoría del conocimiento disperso de Hayek: ningún ente central controla las decisiones económicas y la coordinación surge como orden espontáneo. El propio Hayek anticipó esta idea cuando escribió: "debemos idear alguna forma de retirar al Estado su monopolio sobre el dinero".

Bitcoin representa precisamente esa forma.

VII. Bitcoin como dinero sólido

La teoría monetaria desarrollada por la Escuela Austriaca establece que la calidad del dinero depende de sus propiedades intrínsecas y de su capacidad para facilitar el intercambio, preservar el valor a lo largo del tiempo y permitir el cálculo económico orientado al futuro. Desde esta perspectiva, el dinero sólido es aquel que mantiene su poder adquisitivo de forma estable y que no puede ser manipulado arbitrariamente por ninguna autoridad política o bancaria.

Ludwig von Mises sostuvo que "el dinero sano es un instrumento para proteger las libertades civiles contra las usurpaciones despóticas del Estado". Esta afirmación subraya que el dinero sólido no es únicamente un concepto económico, sino también político y moral, ya que preserva la independencia del individuo frente al poder coercitivo.

Propiedades del buen dinero

La tradición austriaca identifica diversas propiedades fundamentales para que un bien pueda desempeñar eficazmente la función de dinero:

- Escasez verificable
- Durabilidad
- Divisibilidad
- Portabilidad

- Fungibilidad
- Aceptación
- Resistencia a la censura

El oro fue históricamente el bien que mejor reunía estas características, razón por la cual resultó monetizado espontáneamente. Sin embargo, incluso el oro presenta limitaciones prácticas: su transporte es costoso, su custodia requiere confianza en terceros y su divisibilidad efectiva es limitada.

Bitcoin incorpora todas las propiedades del dinero sólido, pero las lleva a un plano tecnológico superior. Su escasez está garantizada criptográficamente mediante un protocolo abierto y descentralizado que impide la creación arbitraria de nuevas unidades más allá del límite de 21 millones. Su durabilidad es absoluta, ya que no depende de un soporte físico sujeto a degradación. Su divisibilidad es extrema (hasta 8 decimales), y su portabilidad permite transferencias globales en minutos sin necesidad de intermediarios.

Preferencia temporal y ahorro

Una de las contribuciones centrales de la Escuela Austriaca es la teoría de la preferencia temporal, desarrollada por Eugen Böhm-Bawerk, según la cual los individuos valoran más los bienes presentes que los futuros y exigen una compensación para diferir consumo. Como escribió Böhm-Bawerk: "el interés es el precio que se paga por preferir bienes presentes frente a bienes futuros".

Cuando el dinero pierde valor por inflación, la preferencia temporal se incrementa artificialmente, incentivando el consumo inmediato y desincentivando el ahorro y la inversión productiva. Por el contrario, un dinero sólido reduce la preferencia temporal y fomenta la planificación de largo plazo, fundamento del progreso económico sostenible. Bitcoin, al mantener una oferta monetaria predecible y no manipulable, crea un entorno en el que el ahorro recupera su función central como motor del capital.

Bitcoin frente al oro y el dinero fiduciario

Mientras el oro garantiza solidez física pero limita su utilidad operativa, y el dinero fiduciario ofrece facilidad de uso pero carece de restricciones cuantitativas, Bitcoin combina lo mejor de ambas realidades: es digital como el dinero FIAT actual pero escaso como el oro. La criptografía garantiza que su emisión no depende de decisiones políticas ni de bancos centrales.

Bitcoin no es una burbuja, es un proceso de monetización

Una crítica habitual sostiene que Bitcoin constituye una burbuja especulativa. Sin embargo, desde la perspectiva de la teoría monetaria austriaca, Bitcoin atraviesa un proceso de monetización similar al del oro en su transición desde objeto de intercambio a estándar monetario. En sus primeras etapas, todo bien monetizable presenta una alta volatilidad derivada del descubrimiento del precio y de la progresiva adopción.

Menger describió este proceso afirmando que "la evolución del dinero es un fenómeno orgánico y gradual". La volatilidad, por tanto, no implica falta de valor intrínseco, sino competencia por convertirse en dinero global.

Históricamente, incluso el oro experimentó largos periodos de volatilidad hasta que alcanzó aceptación universal. En el caso de Bitcoin, su crecimiento ha seguido un patrón logarítmico determinado por sucesivos ciclos de adopción y consolidación, respaldados por su utilidad tecnológica y económica.

La noción de burbuja presupone la ausencia de fundamentos, pero Bitcoin se sostiene en un diseño monetario único, una infraestructura descentralizada sin precedentes y una creciente adopción institucional y tecnológica.

Bitcoin no es una burbuja, sino la fase inicial del proceso de monetización de un bien con características superiores para cumplir funciones monetarias globales.

VIII. Bitcoin frente al sistema bancario y las CBDC

El sistema bancario moderno se basa en el modelo de reserva fraccionaria, mediante el cual las entidades financieras mantienen solo una parte de los depósitos disponibles para retiro inmediato, prestando el resto o utilizándolo para actividades especulativas. Este mecanismo permite una expansión del crédito superior a la cantidad de dinero realmente respaldada en reservas, generando una estructura financiera apalancada y vulnerable. La estabilidad del sistema depende, por tanto, de la confianza pública. Cuando esta confianza se deteriora, aparecen crisis bancarias y retiradas masivas de depósitos.

En este contexto, los bancos centrales actúan como prestamistas de última instancia y reguladores de la política monetaria. Mediante la fijación de tipos de interés y la expansión o contracción de la oferta de dinero, buscan mantener la estabilidad económica y controlar la inflación. Sin embargo, la Escuela Austriaca sostiene que estas intervenciones distorsionan los precios relativos y fomentan ciclos artificiales de auge y recesión. Como afirmó Ludwig von Mises: "la inflación es un impuesto encubierto", que erosiona el poder adquisitivo y redistribuye la riqueza de manera involuntaria.

Dependencia de la confianza y riesgo moral

El funcionamiento del sistema bancario actual requiere que los ciudadanos confíen en que las instituciones actuarán de forma responsable y que el Estado protegerá los depósitos en caso de crisis. Sin embargo, esta expectativa genera lo que la teoría económica denomina riesgo moral: si los bancos saben que serán rescatados, tienen incentivos para asumir riesgos excesivos. El principio "Too Big To Fail" ilustra cómo la estructura actual separa riesgo y responsabilidad.

Bitcoin ofrece un modelo radicalmente distinto: no depende de confianza institucional, sino de verificabilidad técnica y consenso descentralizado. Su diseño elimina la necesidad de intermediarios y permite la custodia directa de los activos sin dependencia de terceros. Como escribió Satoshi Nakamoto: "necesitamos un sistema basado en pruebas criptográficas en lugar de confianza".

CBDC: definición y marco conceptual

Las monedas digitales de banco central (CBDC) representan una versión digital del dinero estatal emitido directamente por la autoridad monetaria. A diferencia del dinero bancario tradicional, las CBDC no requieren intermediarios privados para su emisión o gestión.

Se conciben como herramientas para modernizar los sistemas de pago, mejorar la eficiencia transaccional y facilitar la política monetaria.

Desde un enfoque académico y neutral, las CBDC presentan diversos potenciales beneficios:

- Reducción de costes operativos en el sistema de pagos
- Transferencias más rápidas y económicas
- Inclusión financiera mediante acceso directo al dinero digital
- Mayor capacidad de trazabilidad para combatir actividades ilícitas

Sin embargo, también plantean desafíos significativos en términos económicos y estructurales. La trazabilidad total puede afectar la privacidad financiera individual y modificar el equilibrio entre libertad económica y supervisión estatal. La posibilidad de programar el dinero permitiría diseñar incentivos específicos, pero también condicionaría el uso de los fondos. La centralización total del sistema implica la concentración del poder monetario y financiero en una única autoridad.

Bitcoin como alternativa descentralizada

Bitcoin se presenta como un modelo opuesto al sistema bancario tradicional y a las CBDC. Mientras estas se basan en control centralizado y confianza institucional, Bitcoin se fundamenta en la descentralización y la imposibilidad técnica de intervención arbitraria. Su naturaleza abierta y resistente a la censura garantiza que las transacciones puedan realizarse sin autorización de ninguna autoridad.

Friedrich Hayek anticipó esta necesidad cuando escribió: "debemos idear alguna forma de retirar al Estado su monopolio sobre el dinero". Bitcoin materializa esta propuesta mediante una arquitectura que sustituye las decisiones discrecionales por reglas predecibles y verificables.

En este sentido, Bitcoin y las CBDC representan dos paradigmas monetarios divergentes: uno basado en confianza institucional y centralización, y el otro basado en verificabilidad matemática y descentralización.

IX. Propiedad, libertad y soberanía individual

La Escuela Austriaca considera que la propiedad privada constituye el fundamento esencial de la libertad individual y el núcleo del orden económico y social. La capacidad de los individuos para poseer, utilizar y transferir bienes sin interferencia arbitraria es el principio que permite el desarrollo de la cooperación social y la prosperidad. Ludwig von Mises expresó con claridad esta conexión fundamental afirmando que "la libertad económica no es una parte de la libertad, sino el todo de la libertad".

Según esta perspectiva, la libertad política no puede sostenerse sin libertad económica, ya que cuando el poder estatal controla los recursos materiales y financieros, controla de manera efectiva la conducta y decisiones de los ciudadanos. Friedrich Hayek coincidió en esta relación afirmando que "la libertad individual descansa en el reconocimiento de la propiedad privada".

Tradición intelectual española sobre propiedad y libertad

La defensa de la propiedad privada como fundamento de la libertad no surge únicamente de la teoría económica moderna. Ya en el siglo XVI, la Escuela de Salamanca había formulado una concepción avanzada y profundamente humanista de la propiedad y la libertad civil. Francisco de Vitoria, uno de los principales representantes de este movimiento, sostuvo que la propiedad privada es un derecho natural derivado de la dignidad humana y que ninguna autoridad puede violarlo legítimamente sin justa causa. Vitoria escribió que "la propiedad pertenece al derecho natural y la ley humana solo puede regular sus condiciones, no abolirla".

Del mismo modo, Juan de Mariana argumentó que el poder político no puede disponer de los bienes de los ciudadanos sin su consentimiento legítimo, y advirtió contra la confiscación y la manipulación de la moneda por parte de los gobernantes. Mariana afirmó que "el príncipe que rebaja la moneda comete un robo contra el pueblo". Estas ideas anticipan la crítica austríaca al intervencionismo monetario y su defensa del dinero sólido.

El pensamiento de la Escuela de Salamanca establece un vínculo directo entre libertad civil, propiedad privada y justicia en el intercambio, señalando que la imposición arbitraria sobre los bienes de los ciudadanos constituye una forma de tiranía. Esta visión conecta profundamente con la tradición posterior de Mises y Hayek, para quienes la soberanía económica es inseparable de la libertad política.

Bitcoin y la soberanía individual

Bitcoin introduce una innovación decisiva en la historia de la propiedad: la posibilidad de poseer y transferir valor sin depender de la autorización de ninguna institución. Su arquitectura descentralizada y su capacidad de autocustodia permiten que cualquier individuo pueda ser dueño pleno de sus activos sin riesgo de confiscación o censura.

Mientras el sistema financiero tradicional exige confianza en intermediarios y está sujeto a restricciones, controles y sanciones, Bitcoin devuelve al individuo la responsabilidad directa sobre su patrimonio. La máxima "not your keys, not your coins" resume esta transformación: la posesión material del valor ya no depende de la infraestructura estatal o bancaria.

En este sentido, Bitcoin puede entenderse como una herramienta contemporánea que materializa la defensa histórica de la propiedad privada como condición de libertad. Al igual que Vitoria defendió la inviolabilidad moral de la propiedad y Mariana denunció la manipulación monetaria, Bitcoin ofrece un mecanismo tecnológico que impide la confiscación arbitraria y limita estructuralmente la degradación de la moneda.

La soberanía individual requiere control sobre la propiedad, y la propiedad requiere dinero sólido. La manipulación monetaria y el control centralizado de los sistemas de pago erosionan la libertad económica y, con ello, la libertad política. Bitcoin representa una alternativa que reinstaura el principio de autonomía económica mediante una forma de dinero que ningún gobierno puede crear, destruir ni controlar unilateralmente.

En esta línea, la promesa filosófica de Bitcoin se conecta directamente con una tradición intelectual que recorre desde la Escolástica española del Siglo de Oro hasta la teoría austríaca contemporánea: la defensa de la libertad del individuo frente al poder del Estado.

X. Implicaciones sociales y políticas

La introducción de Bitcoin en la esfera económica y social plantea transformaciones de alcance estructural que trascienden el ámbito tecnológico y financiero. Como innovación monetaria descentralizada, Bitcoin reconfigura la relación entre individuos, mercados e instituciones, generando un nuevo modelo de organización económica basado en la responsabilidad individual y la coordinación voluntaria. Estas implicaciones no solo afectan la arquitectura del sistema financiero, sino que también influyen en la estructura misma del poder político y social.

Transformación del modelo económico: del consumo al ahorro

La lógica económica dominante en el sistema FIAT está construida sobre la inflación permanente y el estímulo al consumo inmediato. La depreciación continua de la moneda desincentiva el ahorro y fomenta un comportamiento orientado al corto plazo. Bitcoin, en cambio, con su oferta monetaria limitada, favorece una reducción estructural de la preferencia temporal, promoviendo la acumulación de capital y la planificación a largo plazo. Este cambio cultural podría reorientar la economía hacia modelos más sostenibles y menos dependientes del endeudamiento.

Redistribución del poder y descentralización institucional

El sistema financiero actual se organiza en torno a estructuras jerárquicas centralizadas, donde bancos centrales y grandes instituciones financieras controlan la emisión monetaria, el acceso al crédito y las infraestructuras de pago. Bitcoin introduce un paradigma opuesto: acceso abierto, ausencia de intermediarios y control distribuido entre los participantes de la red. Esta redistribución del poder económico puede tener efectos sociales profundos, al reducir barreras de entrada, debilitar posiciones de privilegio institucional y permitir una participación económica más democrática.

Inclusión económica global

Según organismos internacionales, más de mil millones de personas carecen de acceso al sistema bancario formal. Bitcoin ofrece un mecanismo alternativo de integración económica global sin necesidad de intermediarios. La capacidad de enviar y recibir valor sin permiso se convierte en una herramienta de emancipación para comunidades marginadas o desbancarizadas.

Transparencia, verificación y confianza sistémica

La transparencia inherente a la blockchain introduce una nueva forma de confianza basada en verificación técnica y no en autoridad. Esto puede favorecer la reducción de prácticas opacas como la corrupción institucional o el uso político del dinero público. El registro inmutable y accesible modifica la naturaleza del control económico, trasladándolo del plano discrecional al plano verificable.

Desafíos, tensiones y límites actuales

A pesar de su potencial transformador, Bitcoin enfrenta desafíos significativos. La escalabilidad tecnológica, la volatilidad de precios en su fase de monetización, la diversidad regulatoria internacional y el desconocimiento técnico generalizado representan obstáculos a su adopción.

Escenarios posibles

Desde una perspectiva académica, es posible considerar múltiples escenarios de evolución:

- Escenario de coexistencia competitiva, en el que Bitcoin convive con monedas fiduciarias y digitales estatales, actuando como activo refugio y reserva de valor.
- Escenario de integración gradual, donde Bitcoin se incorpora progresivamente al sistema financiero como estándar monetario complementario.
- Escenario de sustitución parcial, en el que su adopción creciente reduce de forma significativa la dependencia del dinero fiduciario.

Bitcoin introduce una transformación social de gran alcance al devolver a los individuos la responsabilidad sobre su propio patrimonio y reducir la dependencia de estructuras centralizadas. Al hacerlo, cuestiona los fundamentos del orden monetario contemporáneo y abre posibilidades inéditas para la libertad económica y política.

XI. Conclusiones y perspectivas futuras

Bitcoin representa una ruptura histórica en la evolución del dinero y constituye la primera realización práctica de un ideal teórico defendido durante siglos: la posibilidad de un sistema monetario sólido, resistente a la manipulación política y basado en la cooperación voluntaria entre individuos libres. Su diseño tecnológico incorpora y materializa los principios fundamentales defendidos por la tradición intelectual que recorre desde la Escuela de Salamanca del Siglo de Oro español hasta la Escuela Austriaca de Economía.

Francisco de Vitoria defendió que la propiedad privada es un derecho natural y que ninguna autoridad puede violarla legítimamente, afirmando que "la propiedad pertenece al derecho natural y la ley humana solo puede regular sus condiciones, no abolirla". Juan de Mariana denunció la manipulación de la moneda al afirmar que "el príncipe que rebaja la moneda comete un robo contra el pueblo". Siglos más tarde, Ludwig von Mises advirtió que "no hay forma más sutil ni más segura de destruir una sociedad que corrompiendo su moneda", y Friedrich Hayek reclamó la necesidad de "retirar al Estado su monopolio sobre el dinero".

Bitcoin responde a ese desafío histórico con un sistema monetario cuya oferta no puede ser alterada por decisión humana, cuyo funcionamiento no depende de confianza institucional y cuya arquitectura elimina la posibilidad estructural de censura y confiscación. Satoshi Nakamoto sintetizó esta propuesta afirmando que "la raíz del problema con la moneda convencional es toda la confianza necesaria para que funcione".

Desde un punto de vista social, Bitcoin introduce un nuevo paradigma basado en la responsabilidad individual, la soberanía económica y la cooperación descentralizada. Su existencia reduce la dependencia respecto a instituciones financieras y políticas centralizadas, y ofrece una vía de emancipación económica especialmente relevante en contextos de fragilidad institucional, inflación crónica o exclusión financiera.

En el terreno político, Bitcoin cuestiona los fundamentos del poder monetario contemporáneo y abre posibilidades inéditas para la organización social. Si el control del dinero ha sido históricamente una herramienta de dominación, la descentralización monetaria inaugura un marco donde el ciudadano puede recuperar el papel central en la construcción del orden económico. La transición del dinero como instrumento de control al dinero como herramienta de libertad constituye uno de los cambios civilizatorios más profundos de nuestra época.

Bitcoin no es simplemente una tecnología ni un activo financiero; es una expresión concreta de una idea moral: que la libertad humana requiere límites reales al poder y que la responsabilidad individual es el fundamento del progreso social. Su aparición marca el inicio de una nueva etapa histórica en la que el dinero puede volver a ser una institución al servicio de la sociedad y no un mecanismo de explotación.

El futuro de Bitcoin dependerá de la capacidad colectiva de comprender su relevancia y de asumir la responsabilidad que implica la soberanía económica. No se trata únicamente de adoptar una herramienta tecnológica, sino de participar en la construcción de una nueva arquitectura social basada en la libertad, la cooperación voluntaria y el respeto a la dignidad humana.

Bitcoin es, en última instancia, una invitación: a recuperar la independencia frente al poder, a reconstruir la relación entre individuo y sociedad, y a imaginar un futuro donde el dinero vuelva a ser expresión de confianza mutua y no de dominación.

El tiempo dirá si la humanidad acepta esa invitación.

XII. Bibliografía que deberías revisar

Escuela de Salamanca

- Francisco de Vitoria (1539). Relecciones sobre los Indios y el Derecho de la Guerra. Edición crítica moderna: (1998). Madrid: Tecnos.
- Martín de Azpilcueta (1556). Comentario resolutorio de cambios. Edición moderna: (1965). Pamplona: EUNSA.
- Domingo de Soto (1553). De Iustitia et Iure. Edición moderna: (1967). Madrid: Instituto de Estudios Políticos.
- Juan de Mariana (1609). De Monetae Mutatione. Edición moderna: (1987). Madrid: Centro de Estudios Constitucionales.

Escuela Austriaca de Economía

- Carl Menger (1871). Principios de Economía. Edición española: (2017). Madrid: Unión Editorial.
- Eugen Böhm-Bawerk (1884). Capital e Interés. Edición española: (2019). Madrid: Unión Editorial.
- Friedrich von Wieser (1914). Teoría de la Economía Social. Edición española: (2011). Unión Editorial.
- Ludwig von Mises (1922). Socialismo. Edición española: (2012). Madrid: Unión Editorial.

- Ludwig von Mises (1949). La Acción Humana. Edición española: (2011). Madrid: Unión Editorial.
- Friedrich Hayek (1944). Camino de Servidumbre. Edición española: (2017). Madrid: Alianza Editorial.
- Friedrich Hayek (1976). La Desnacionalización del Dinero. Edición española: (2018). Madrid: Unión Editorial.

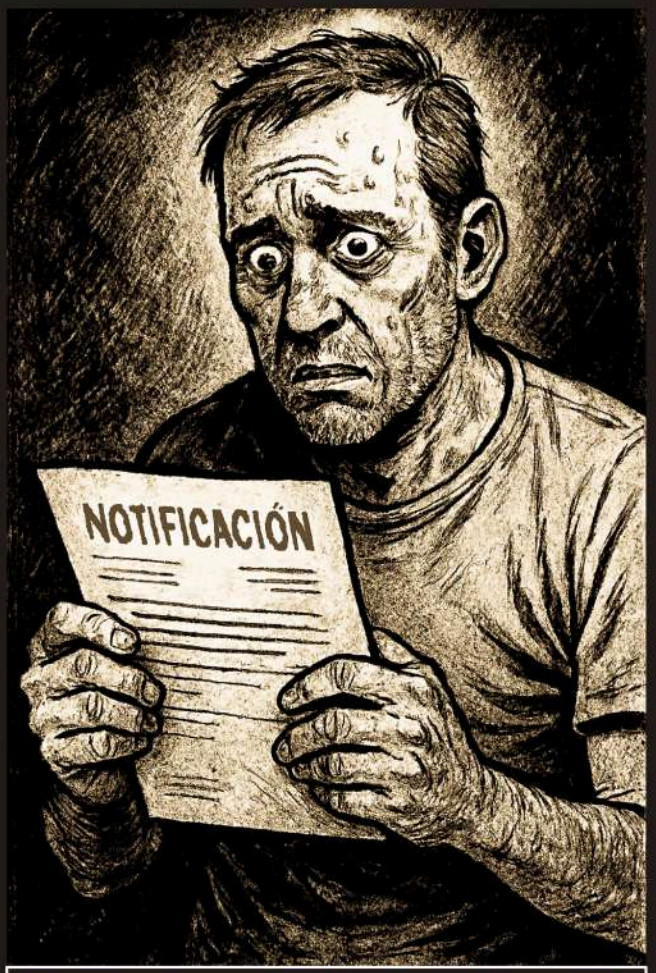
Autores contemporáneos y pensamiento monetario

- Murray N. Rothbard (1963). What Has Government Done to Our Money? Edición española: (2015). Unión Editorial.
- Saifedean Ammous (2018). The Bitcoin Standard. Edición española: (2020). Barcelona: Deusto.
- Nik Bhatia (2021). Layered Money. Los Angeles: Lightning Network Publications.
- Jason Lowery (2023). Softwar. Boston: MIT.

Documentos técnicos y textos fundacionales

- Satoshi Nakamoto (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Disponible en: bitcoin.org
- Hal Finney (2004–2013). Escritos seleccionados. Archivo público: Nakamoto Institute.
- Wei Dai (1998). B-Money. Archivo público.
- Adam Back (2002). Hashcash. Publicación técnica original.
- Nick Szabo (2005). Bit Gold. Archivo público.

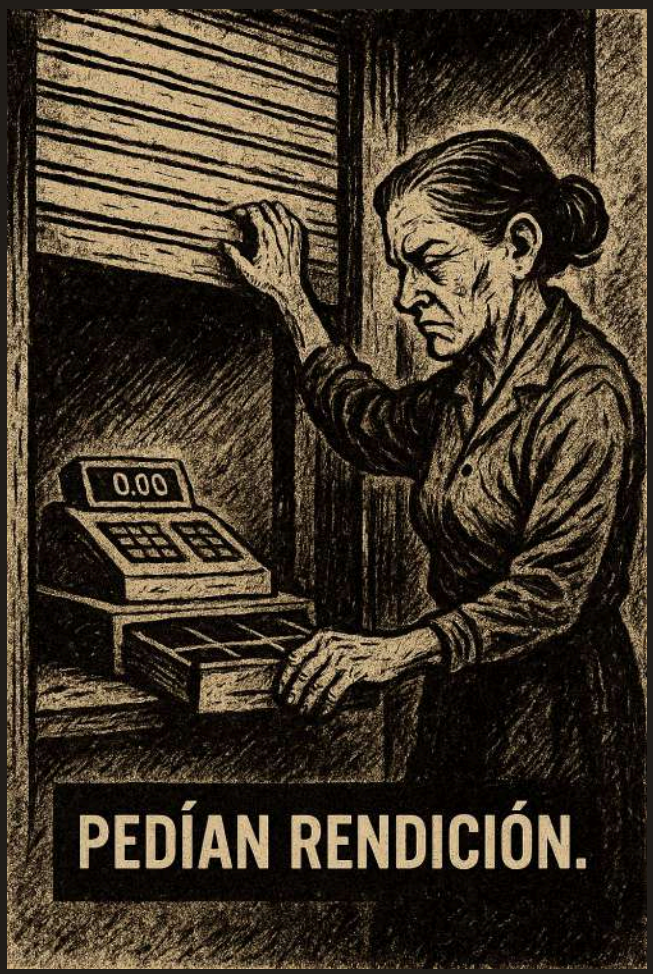

LA PERSECUCIÓN
DE LA AGENCIA
SE TRASPASA
SE VENDE

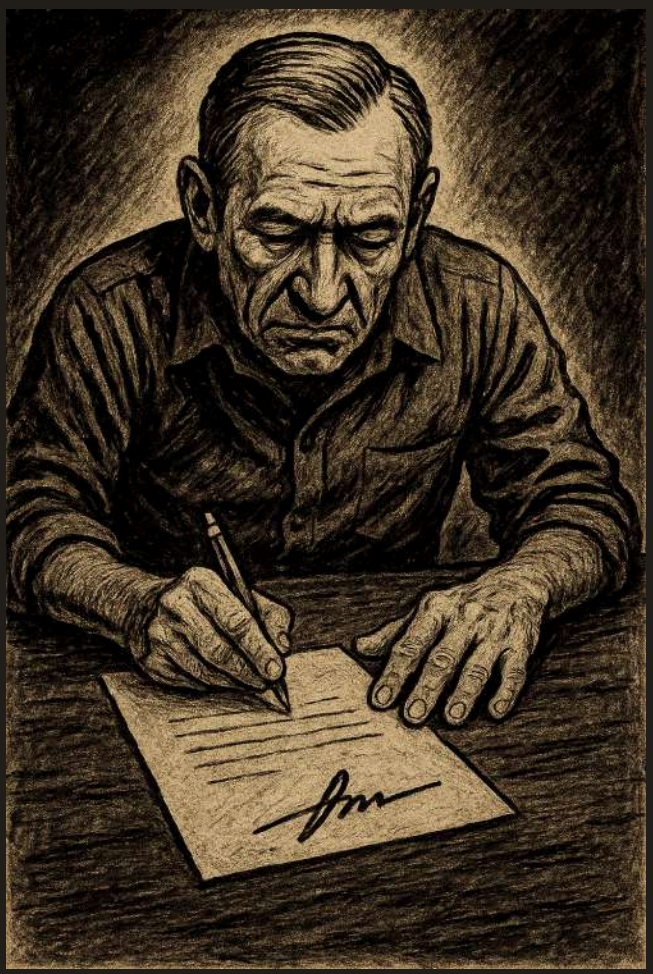


Errores minimos...

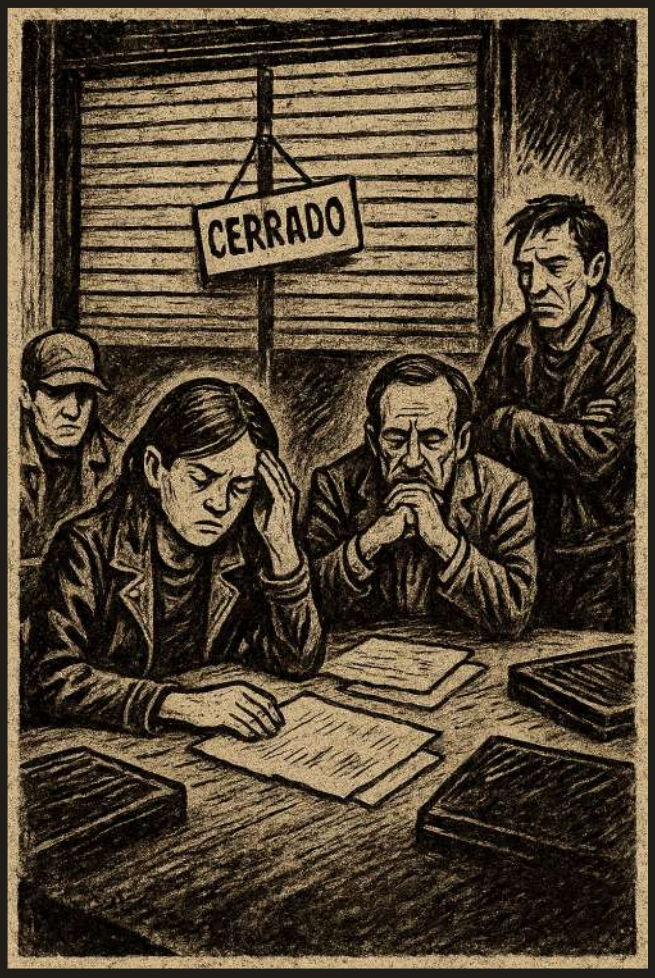
...sanciones maximas

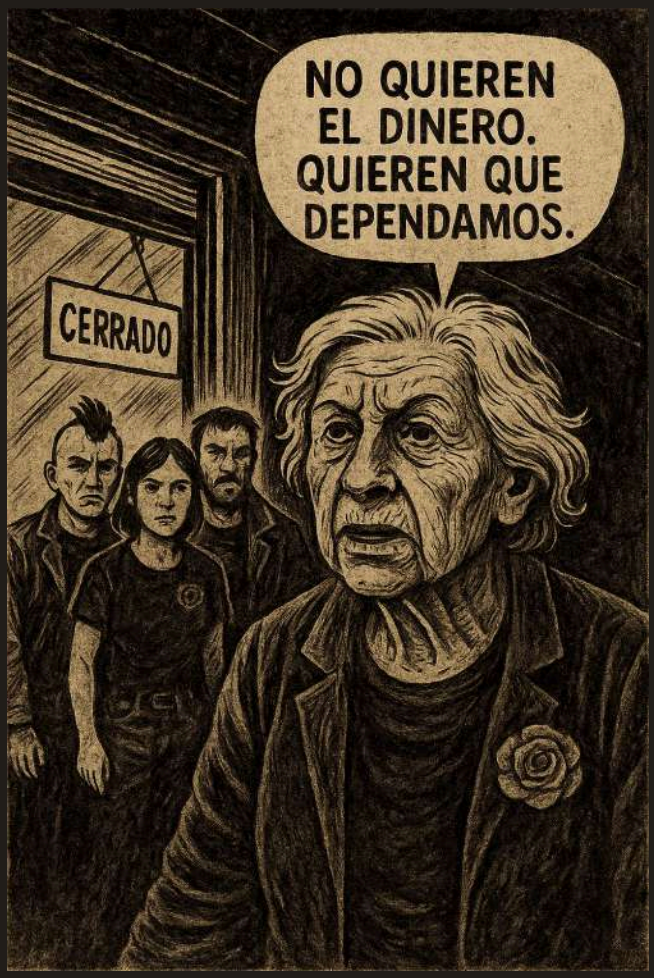

FORMULARIO
TRIBUTARIO
PLAZO IMPRORROGABLE


0.00
PEDÍAN RENDICIÓN.




IMPUESTOS
ESTADO

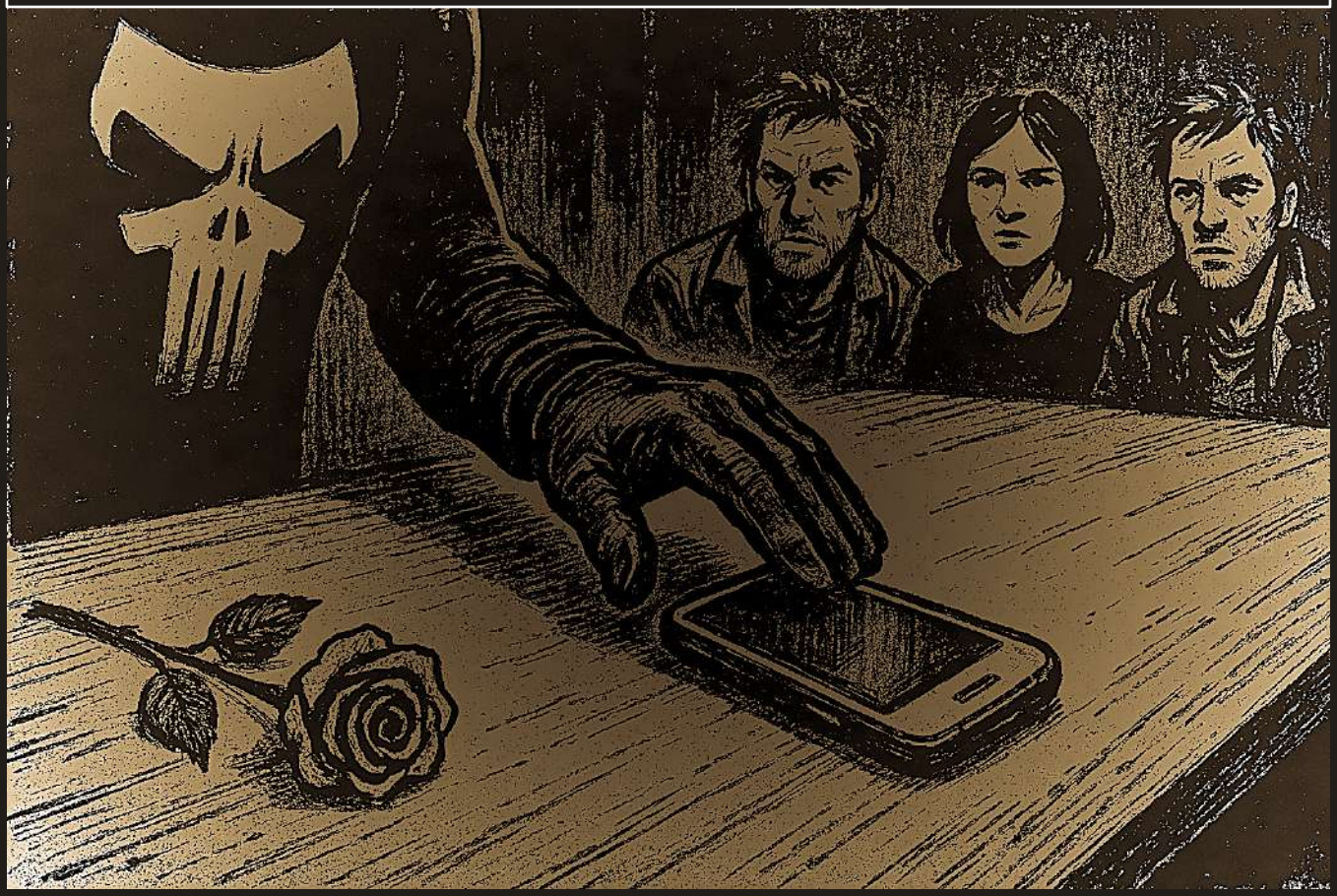

CERRADO


NO QUIEREN
EL DINERO.
QUIEREN QUE
DEPENDAMOS.
CERRADO

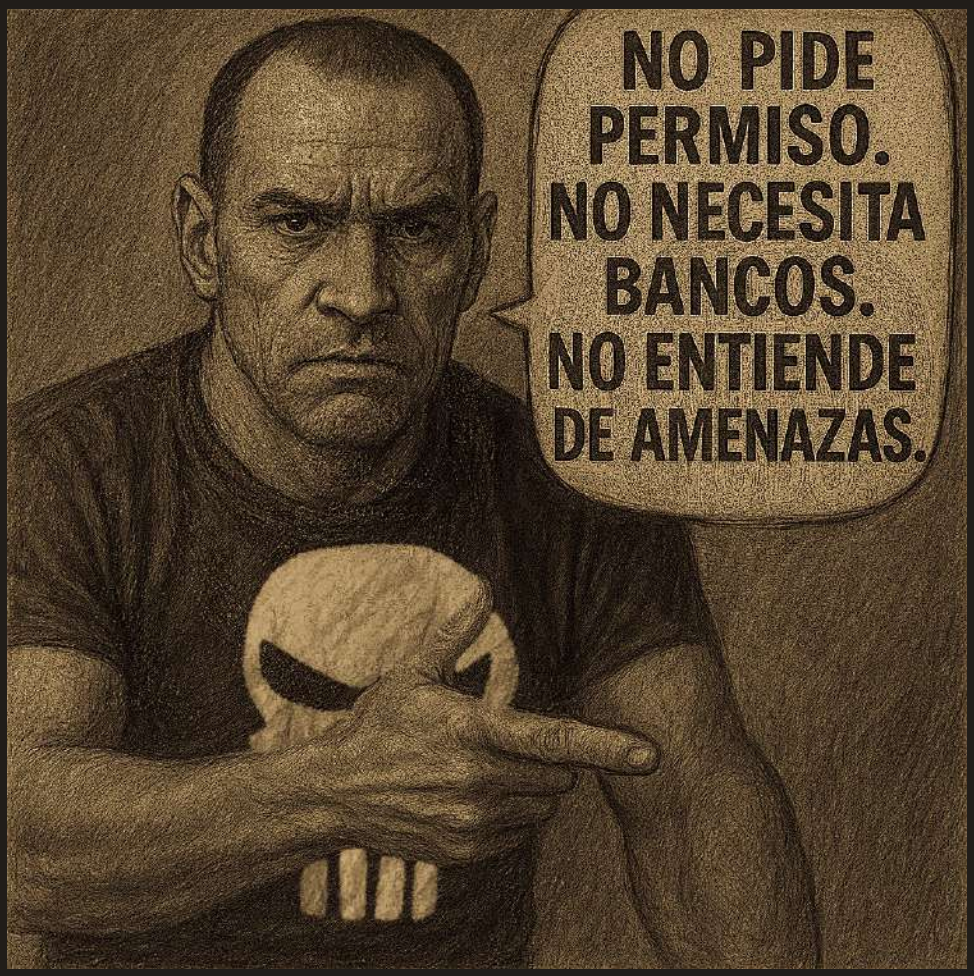
Cuando todos cierran...

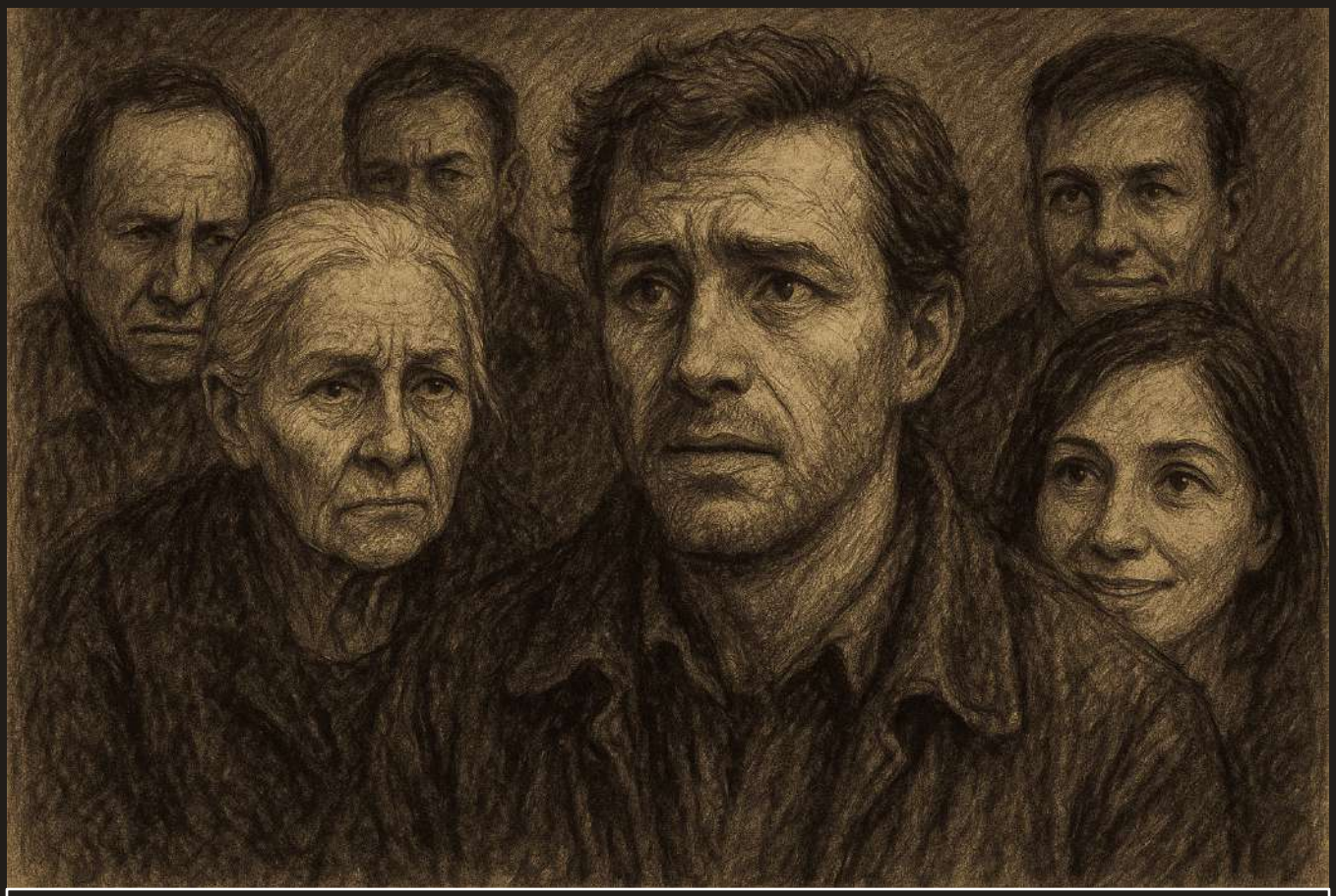
alguien sigue caminando

La resistencia empieza con un viejo telefono.



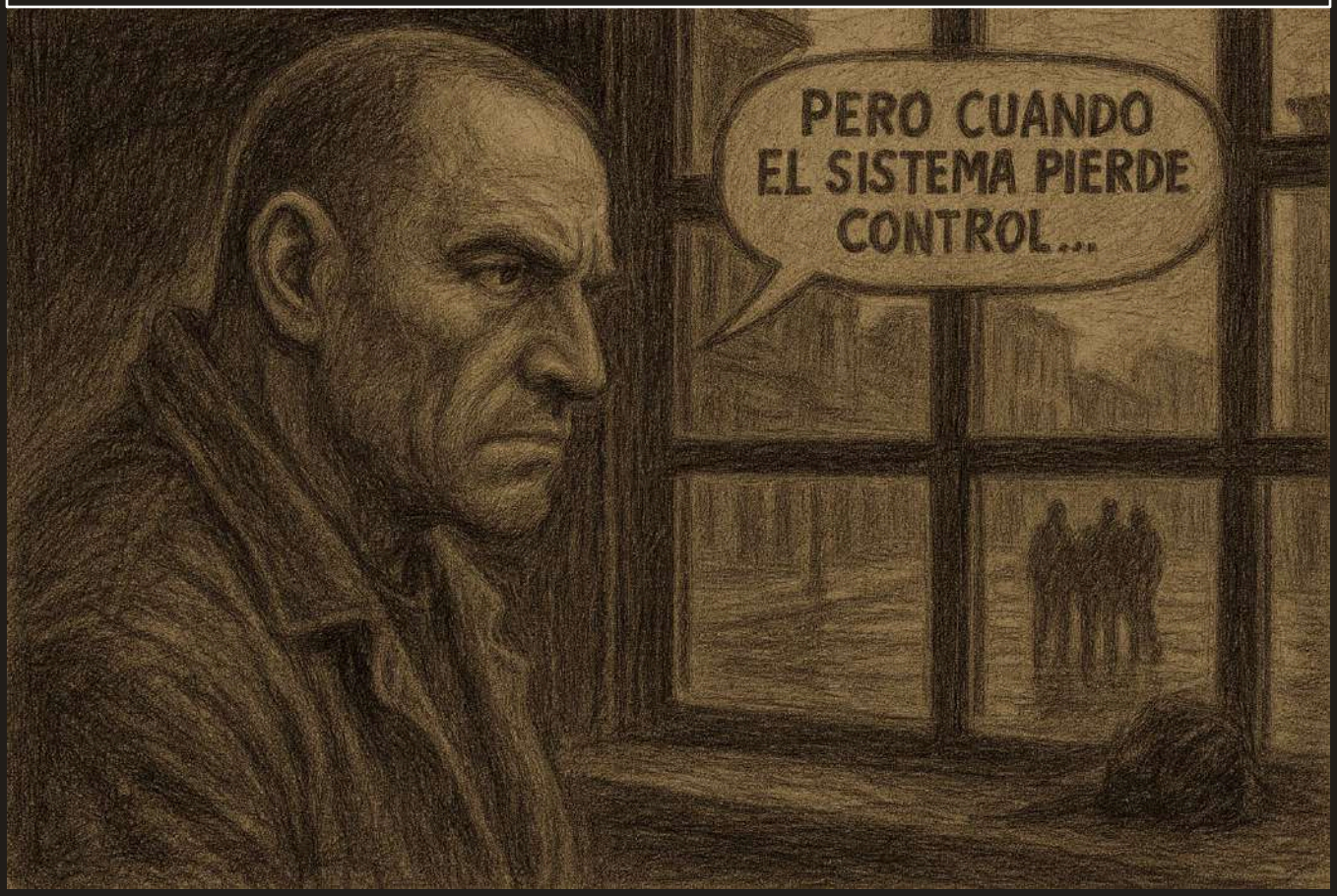

BITCOIN

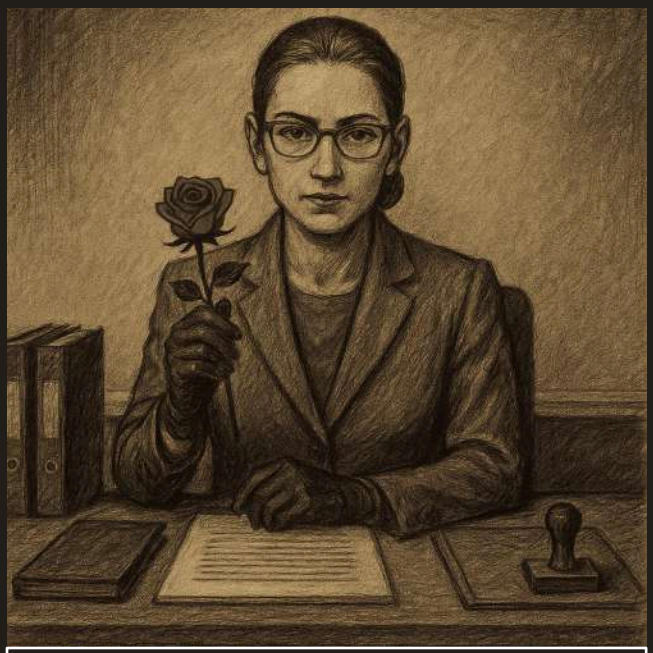

NO PIDE
PERMISO.
NO NECESITA
BANCOS.
NO ENTIENDE
DE AMENAZAS.



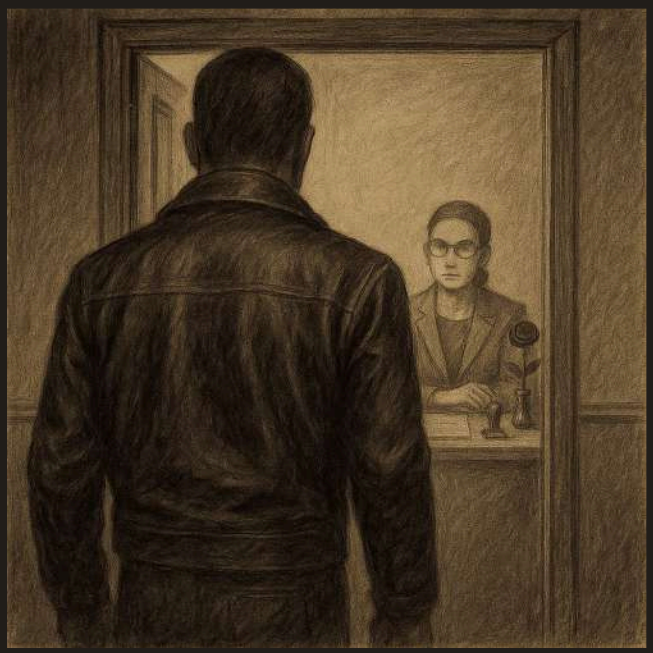
Dudas, esperanzas contenidas...

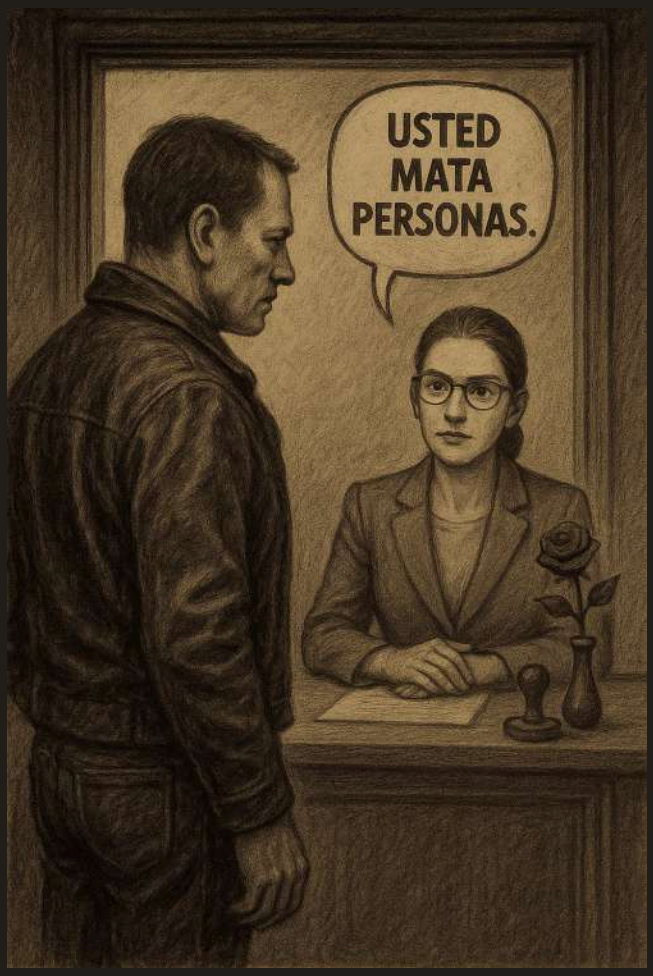
Cuando no pueden verte, no pueden cazarte.





En los despachos todo es limpio, la violéncia también.




USTED MATA PERSONAS.


NOSOTROS CORREGIMOS COMPORTAMIENTOS.


LES QUITÁIS TODO.

La amenaza real no es el arma, es el relato

continuara...

La Identidad y la Privacidad

Autor: Don Nadiel

Brunbitty en X-twitter. Identidad_freewill

https://x.com/brunbitty/status/1996032975167713601

Esta noche por fin lo entendí.

Neo le hace la clásica pregunta:

“Si ya sabes lo que voy a hacer...

¿de verdad tengo opción?”

Y ella [Oráculo] le responde:

“Ya has tomado la decisión. Solo estás aquí para entender por qué”.

Durante años pensé que esto significaba que “no existe el libre albedrío”. Pero no es así.

La verdadera revelación es esta:

El libre albedrío no existe en el momento. Existe en la identidad que conduce al momento.

¿Las acciones que realizas ahora mismo?

Son mayormente automáticas, moldeadas por tu condicionamiento,

experiencias, miedos, hábitos y pasado.

¿Pero la persona en la que te estás convirtiendo?

Ahí es donde reside realmente tu libertad.

No eliges el momento. Eliges al hombre que estará a la altura del momento.

O dicho de otro modo:

El determinismo escribe el pasado.

La identidad escribe el futuro.

Porque cuando tu vida no está donde quieres, la respuesta no es

“tomar mejores decisiones”.

La respuesta es:

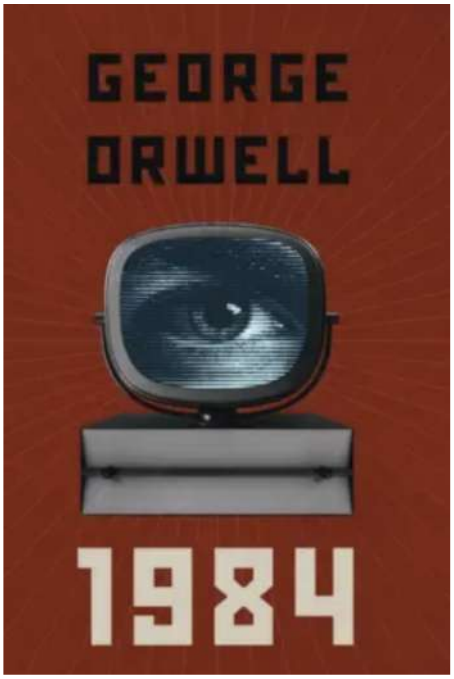
conviértete en la versión de ti mismo que toma mejores decisiones automáticamente.

Esa es la verdadera píldora roja.

Aquí un texto relativamente breve que divaga acerca de la identidad y la privacidad.

Con ayuda de la etimología repaso estos términos en relación al *estado, el ciberespacio, Bitcoin y...Polifemo.

*A lo largo de todo el texto la palabra “estado” en minúsculas hace referencia a Estado, que es como reglamentariamente se escribe cuando se alude a esta institución. Dado que éste es mi artículo y soy soberano en él, me permito la licencia gramatical de degradar este término y arrebatarle el privilegio de escribirlo en mayúsculas, siendo cómo es, un mero constructo derivado, en parte, del consentimiento pasivo por parte de la sociedad y origen de muchos de sus males.



El advenimiento del ciberespacio ha hecho realidad las elucubraciones distópicas de muchos autores visionarios de mediados del siglo XX en lo que concierne a la privacidad del individuo.

Hemos asistido, sin ser plenamente conscientes de ello, a una superposición entre los espacios físicos, reales, y los espacios virtuales que han hecho de la identidad y la conducta del individuo objeto de escrutinio por parte de agentes poderosos como el estado y grandes corporaciones. Estas últimas, incluso con la capacidad de mercantilizar la información de toda índole que se desprenden de nuestra interacción con el ciberespacio y que se correlaciona, en gran medida, con nuestra vida en el mundo físico. Ha esto nos referimos con superposición de ambas esferas.

Este artículo pretende, modestamente, señalar como la filosofía y la mecánica de Bitcoin toman un papel relevante y disruptivo en este escenario que se torna por momentos aún más Orwelliano si cabe con los **alarmantes anuncios**[1] por parte de los organismos europeos de implementar herramientas más agresivas como "chat control" o las CBDC, siendo esta última especialmente perversa al inspirarse en Bitcoin pero subvirtiendo absolutamente su filosofía.

Pero antes, exploremos los conceptos de identidad y privacidad.

La palabra **persona** viene del latín persōna o sea, máscara (la máscara del actor). Etimológicamente quizá provenga de per/sonare, la máscara a través de la cuál (per) resuena la voz del actor (sonare).

1.https://bitcointuesdaymadrid.com/community-articles/chat-control-proposal-passed-eu-council-do-we-want-our-children-to-grow-up-in-a-1984-style-system-of-mass-surveillance

La palabra persona viene del latín persōna o sea, máscara (la máscara del actor). Etimológicamente quizá provenga de per/ sonare, la máscara a través de la cuál (per) resuena la voz del actor (sonare).

En el teatro antiguo, la máscara (PERSONA) tenía una doble función: Reforzar la voz del autor (de ahí su etimología) y definir el personaje, es decir, indicar el elemento constante de su comportamiento en las diferentes situaciones, su **"verdadera naturaleza".**
(P.PICHOT, La personalidad. Roche,1977. p. 8)

"Todos somos únicos y especiales.
Como todos los demás"

La Identidad (idem) como concepto es algo especialmente ambiguo. Sin entrar en disquisiciones etimológicas profundas, centrémonos en uno de los aspectos más problemáticos:

la identidad asociada al estado.

Si bien, y como ya hemos señalado en la introducción, los problemas de privacidad e identidad se han agravado desde el advenimiento de la realidad ciberespacial, este problema ya existía en el mundo "analógico" desde la misma existencia del estado.
Nuestra identidad esta profundamente ligada al aparato del estado. Somos "registrados" desde el momento en que nacemos.

Este proceso de "registro" produce un efecto paradójico en el concepto de identidad. Nuestra identidad estatal, en realidad, difumina nuestra individualidad y nos convierte en algo "IDENTICO" a los demás. Nos hace más gregarios de lo que por naturaleza somos, y lo hace de una manera perversa al convertirnos en una unidad de cuenta, formamos parte del "rebaño" pastoreado por el estado.

Suena duro
pero somos ganado.

Y es que nuestra identidad es definida por la Identidad Fiscal y el DNI; herramientas estadísticas (notese la raiz de la palabra estadística) que el estado utiliza para la extracción de recursos de la sociedad productiva vía impuestos.

Esto forma parte del ámbito social en el que estamos inscritos de forma involuntaria y por defecto pero requiere de nuestro consentimiento pasivo. Aunque, evidentemente, ese "consentimiento" sea de facto impuesto por el monopolio de la fuerza, hay cierta responsabilidad por nuestra parte al aceptar, tolerar, colaborar e incentivar el sometimiento a través de ese "consentimiento pasivo".

Este proceso de alienación del individuo se multiplica cuando abrimos foco y observamos las perspectivas que para el conjunto de individuos, los organismos supraestatales tienen como agenda. Por poner tan solo un ejemplo, el problema de inmigración masiva y descontrolada que sufre Europa, en conjunción con el desprestigio y socavamiento progresivo de las estructuras sociales y culturales tradicionales judeo-cristiano-europeas que durante las 50 últimas décadas se han llevado acabo desde un lado del espectro ideológico, parece diseñado para ir desligando al individuo de cualquier atisbo identitario.

Un individuo aislado de cualquier contexto social y cultural, un individuo que no cree en nada, es mucho más fácil de controlar. No tiene asidero. Es por ello que el objetivo de estas "élites" en la sombra apuntan a Europa, el último bastión de soberanía del individuo que podría enfrentarse a un gobierno global.

Existiría una esfera en el que el estado no puede entrar de momento: Nuestro pensamiento...


Libertad Digital

CIENCIA | SALUD | INTERNET | TECNOLOGÍA | VIDEOJUEGOS | EJERCICIO Y NUTRICIÓN

Ciencia

¿Quién controla tu cerebro? La ONU propone reglas para proteger la privacidad mental

La UNESCO lanza el primer marco global para proteger la privacidad mental ante el avance de los dispositivos de lectura cerebral.

Ana Hernández · 05/6/2025 - 06:30

¿Es así realmente? Si tuviésemos en cuenta ciertas teorías del pensamiento de Wittghenstein que postulan que los pensamientos privados no existen podríamos llegar a dudar de esto. Pero en aras a la simplicidad obviaremos ese Hardfork y nos mantendremos en este sendero de especulación sobre la identidad y la privacidad.

Recapitulando, hoy en día, en la era de la información, la identidad y la privacidad se ven más comprometidas que nunca en este nuevo espacio cuasi metafísico en el que interactuamos de forma constante, el ciberespacio, y en el que la información de nuestra identidad y nuestra privacidad se han convertido en un "producto" con el que se mercadea y que incluso condiciona nuestra conducta.

Por ello es obligada la pregunta:

¿Es la identidad algo privado?
¿Debería serlo?

Antes si quiera de intentar contestar a estas preguntas me parece destacable rescatar algún mito moderno a este respecto. Sirva de preámbulo el caso de Bitcoin:
El mismo génesis de Bitcoin se basa en el binomio Identidad/Privacidad: Dice la leyenda que el creador de Bitcoin es un tal Satoshi Nakamoto... pero esto es solo un nombre. No hay una identidad real y física asociada a él que se sepa en la actualidad.

Esto, a mí, me parece una proeza y también una de las cualidades intrínsecas de Bitcoin. El hecho de que su creación sea anónima (seudónima si se quiere, pero para el caso es lo mismo) la equipara a descubrimientos como la rueda o el fuego, atribuibles a la "humanidad".

Si la identidad de su creador estuviese ligada a una persona concreta o un grupo de personas, sería inevitable levantar suspicacias acerca de las intenciones reales de Bitcoin.
Además de otorgar al autor/autores la seguridad física suficiente para seguir respirando aire. Como bien señala el autor Adrián Bernabeu en su estupendo libro Bitcoinismo: "Sin cabeza que cortar, no hay funeral"

(BITCOINISMO ; Deusto, 2024. p.228)

Satoshi como seudónimo-anónimo no es un fenómeno tan novedoso como pueda parecer. Aunque hay muchos casos en la historia podemos remontarnos unas décadas antes cuando vimos un ejemplo extrapolable al mundo del arte subversivo con el caso "situacionista" de Banksy.

Banksy es más una marca que una identidad. Al igual que en el caso de Satoshi, mi "apuesta" es que bajo esas identidades se esconde un colectivo colaborativo. Creo que es la mejor manera de conseguir el anonimato total:

Una inteligencia ejecutiva distribuida y enmascarada tras una única identidad permite implementar estrategias de anonimato más eficientes (siempre que ese grupo no sea demasiado amplio), algo que se complica muchísimo en la actual era de la información si esa empresa la acomete un único individuo, el paso en falso más pequeño daría al traste con la privacidad. Y en los casos de Satoshi y Banksy el éxito ha sido tal que resulta difícil creer que una sola persona haya logrado mantener su identidad privada totalmente desligada de la "mascara", probablemente, porque no existe tal identidad única.

Y volviendo a la pregunta sobre si la identidad debiera ser privada:

Sin entrar en los desacuerdos sostenidos en teoría del derecho y filosofía política (Iusnaturalismo vs Positivismo) existe cierto grado de consenso:

1. La privacidad es un derecho natural, funciona como prerrequisito estructural para la autonomía individual. No depende de ser "concedido".

2. Es un Derecho negativo; Impone deber de no-injerencia. No requiere provisión de bienes ni acciones positivas por parte de terceros.

Por lo tanto, En aras a proteger este derecho de privacidad en el entorno tecnológico en el que vivimos, y sin necesidad de llegar a esos extremos de eficiencia de privacidad como los mencionados en los famosos ejemplos del preámbulo, que, aunque difíciles, no son imposibles, creo que todos debemos valorar la posibilidad del uso de "avatares", "mascaras" o personalidades paralelas que sirvan de escudo de lo propio.

Solo a través de una máscara tal vez podamos manifestar nuestra "verdadera naturaleza".

El caso Nostr.
La cosa Nostra

En un mundo en el que las opiniones personales se ven amplificadas y retransmitidas en el ciberespacio, la privacidad es un foso defensivo ante la censura, las amenazas e incluso, y no menos importante, la autocensura.

En este sentido el protocolo descentralizadao de Nostr supone una revolución.

Nostr (Acrónimo de "Notes and Other Stuff Transmitted by Relays" ("Notas y otras cosas transmitidas por relays")) es un protocolo abierto que permite publicar y leer mensajes mediante claves públicas y firmas digitales, sin servidores centrales. Cada usuario controla su identidad con su clave y replica su contenido a relays independientes.

Bitcoin es uno y trino:
IDENTIDAD-PRIVACIDAD-PROPIEDAD.

Si la privacidad es, por tanto, un Derecho puede que sea de los más importantes. Y está muy ligado a la Propiedad (cuando coinciden las esferas de lo material y de la información). No en vano el mismo nombre de Propiedad suele llevar el apellido "Privada". Es decir, Propiedad Privada. Lo cual es casi una tautología, ya que ambas palabras se refieren a "lo que es propio". (vuelvo a ayudarme de la etimología) Lo privado es lo propio. Y lo que es propio, es privado.

El "estado", en cambio, es capaz de enajenar lo propio de la identidad.

Estaría tentado a abrir aquí, en relación a la propiedad, un debate bifurcado que a nivel personal supone uno de los mayores retos por su complejidad: La propiedad intelectual.

¿Hasta qué punto nuestra propiedad es realmente tal cuando nuestra identidad y nuestra privacidad está en manos de un estado todo poderoso que puede decidir despojarnos de lo nuestro?:

En la actualidad "Toda propieda está sujeta al interés general." *(articulo 33 de la constituciónque regula el derecho de propiedad)*

La trampa está clara. El legislador es el que dicta arbitrariamente y en muchos casos con intereses espurios cuál es el interés general. (El cuál no existe como tal sino como interés mayoritario expresado en las elecciones. Es decir, se pueden excluir a minorías, ergo no es general)

BITCOIN ARREGLA ESTO:

Como dice el filosofo Alvaro D. María :

Bitcoin redefine el derecho de propiedad privada haciéndolo absoluto y creando un espacio donde los Estados carecen de soberanía"

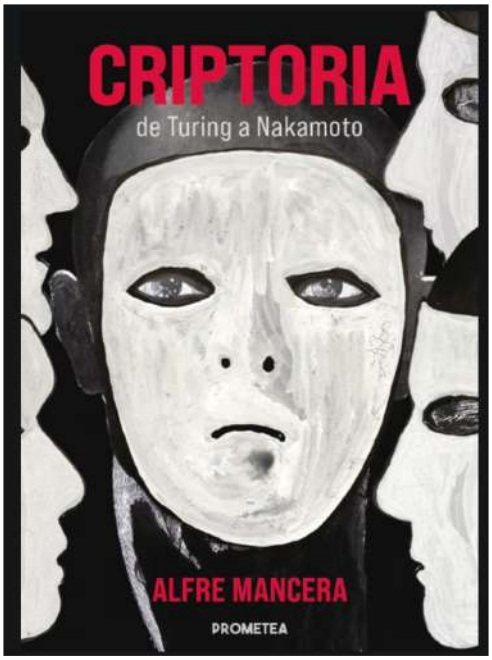
"La propiedad privada es un derecho absoluto solo con Bitcoin"

CÓMO BITCOIN ARREGLA ESTO:

Con la CRIPTOGRAFÍA.

Esta herramienta de liberación y restitución de lo propio es la culminación en los avances en criptografía que algunos científicos, antes y el movimiento "cypherpunk" después, desarrollaron al percatarse de las amenazas y vulnerabilidades a las que los individuos se veían expuestos con el advenimiento de la realidad ciber-espacial. A ellos hay que agradecerles el desarrollo de las herramientas de encriptación necesarias para paliar las nefastas consecuencias, en materia de privacidad, de la interacción con Internet.

A este respecto cabe mencionar el libro Criptoria de Alfre Mancera en el que el autor hace un exhaustivo recorrido conceptual e historiográfico del desarrollo de esta tecnología y sus precursores.



www.prometeabtc.com/product-page/criptoria

Tanto en Bitcoin como en Nostr la encriptación está integrada en el protocolo sin que el usuario tenga la necesidad de conocer profundamente su "mecánica" intrínseca. Aunque tenemos la obligación de empezar a familiarizarnos con el uso de estas herramientas y entender, aunque sea de forma básica, su funcionamiento si queremos que éstas demuestren sus cualidades.

Dicho todo lo cual es obligado subrayar que solo podemos beneficiarnos de las cualidades de Bitcoin como propiedad privada a través de la Autocustodia.

En conclusión, Bitcoin, con su filosofía y su metodología de descentralización y seudonímia, es el catalizador[1] de la estrategias que cada individuo debe aplicar para proteger su identidad y su privacidad en todos los ámbitos de nuestra interacción con el ciberespacio, lo que nos permitirá separar en mayor o menor medida esa realidad virtual de la realidad física.

1.Bitcoin no es precursor de herramientas criptograficas enfocadas en la privacidad. Pero creo que somos muchos los que nos hemos percatado de esta problemática gracias a Bitcoin y es por eso que uso el termino "catalizador".

Usa Bitcoin.
Usa "máscaras".
Y a través de ello tendrás la libertad de expresarte y manifestar tu verdadera naturaleza.

EPILOGO

POLIFEMO Y LA PRIVACIDAD

"ANTES FLACO QUE FAMOSO"

(Jack Kerouac)

Un amigo me preguntó una vez si creía yo que la Odisea tenía alguna correlación con el mundo actual. "Buena pregunta", le conteste, (siendo ésta, tal vez, la mejor forma de contestar cuando no tienes ni idea de la respuesta). Y, aunque me hubiese gustado contestar algo como "viniendo de Homero el 'mito mitológico', seguro que sí ", en realidad, la respuesta era irrelevante. La pregunta era retórica, de esas que no esperan respuesta y que en muchas ocasiones solo son una manera elegante de dar pie a una auto-respuesta con alguna idea que ronda en la cabeza y quiere uno soltar. Si hay suerte esa respuesta puede ser realmente interesante, como así fue en esta ocasión...

A su pregunta contestó con otra pregunta (muy socrático él) :

"Polifemo, ¿a qué se refiere, qué representa?".

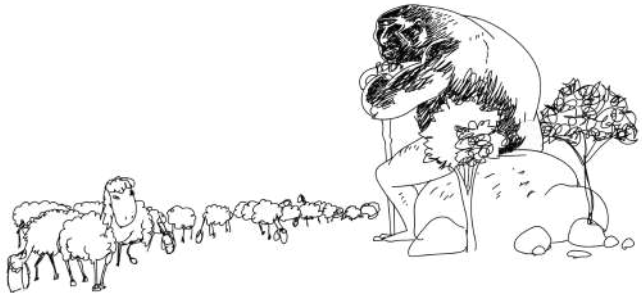
De nuevo contesté: "Buena pregunta". (Es decir, ni idea)

Pues resulta que, y según sus fuentes, Polifemo significa "En boca de muchos".

Ahí, no me negaran, la cosa empieza interesante.

"Polifemo es un cíclope, un gigante de un solo ojo." *[detalle no menor que representa una única perspectiva.]*

"Es un hijo de un dios, pero no es un dios, es un titán, un falso Dios. Se come a los hombres y cría ovejas."



y siguió:

"Se alimenta de la individualidad y cría seguidores. Es lo mainstream , por decirlo de alguna manera."

En este punto tenía absolutamente secuestrada mi atención.

"La forma de escapar de Polifemo era hacerle creer que no eres nadie. Cegarlo mientras duerme y escapar haciendote pasar por oveja".

Bravo.

La identidad, la privacidad, la notoriedad, el “gran hermano que todo lo ve” es tan antiguo como el mito...

“Todo lo que es arriba es abajo.”

Después de que mi amigo expresara dudas sobre la interpretación de “cegar al polifemo” (a lo que yo podría conjeturar que se trata de tener estrategias de privacidad, porque me viene al pelo) remató su idea con:

“(...)Lo de no ser nadie supongo que significa no buscar el reconocimiento del grupo”.

“Si quieres escapar de la perspectiva única [la del cíclope] hay por lo menos [que] rechazar la llamada de la fama.”

“No sé si cegar al titán significa darse cuenta de que tiene puntos ciegos ...[yo creo que así es] ...Y luego aparentar ser parte del sistema hasta que ya estés demasiado lejos para que te coja.”

Realmente una interesantísima lectura del mito homérico que contesta a su primera pregunta sobre si la Odisea tenía alguna correlación con el mundo actual con un “sí” rotundo.

Manifiestos

Timothy C. May

Ciberespacio, criptoanarquía y empujar los límites

Subject: Cyberspace, Crypto Anarchy, and Pushing Limits

From: tcmay@netcom.com (Timothy C. May)

To: cypherpunks@toad.com

Date: Sun, 3 Apr 1994 19:16:49 -0700 (PDT)

Cc: tcmay@netcom.com (Timothy C. May)

Este mensaje toca dos temas de interés reciente (para algunos) aquí:

1. La puesta en marcha de sistemas de pago para la transmisión de mensajes, para manejar los problemas de "mailbombing" y "flooding" de una forma más natural (localidad de referencia, que sea el usuario del servicio quien pague, evitar los efectos de explosión tipo "Gusano de Morris" que podrían haber ocurrido cuando Detweiler nos bombardeó, como señaló Hal).

2. La cuestión general del "ciberespacio". Esto está en la raíz de algunos desacuerdos recientes aquí, y merece más discusión. La criptografía hará de esto un tema realmente crucial en los próximos años.

¿Por qué debatirlo ahora? ¿Qué podría salir de un debate así?

Resulta que estoy leyendo un libro nuevo y maravilloso de Kip Thorne, titulado "Black Holes and Space Warps". Está ampliamente disponible en librerías, solo en tapa dura por el momento. (30 dólares, pero es un libro enorme, y yo lo conseguí en Barnes and Noble por 24. Hablando de Barnes and Noble, la tienda de Santa Clara está vendiendo el libro de Li y Vitanyi, "Intro. to Kolmogorov Complexity", por 44 dólares, antes del 20% de descuento en tapa dura, lo que puede ser un error de precio, ya que yo pagué 60 por el mío. Échenle un vistazo si les interesa... creo que había dos ejemplares).

Thorne ha pasado 30 años estudiando el colapso gravitatorio y los agujeros negros, y fue coautor del famoso libro de 1973 sobre "Gravitation", que pude usar en forma fotocopiada en mi curso de relatividad general en 1973.

¿El punto? Thorne describe su colaboración con Carl Sagan al trabajar la física del viaje en el tiempo mediante agujeros de gusano (wormholes). Thorne tuvo una especie de epifanía: por muy improbables que sean la ingeniería o la financiación de algo, hay algo valioso en examinar los límites absolutos de lo que es posible sin preocuparse por las cuestiones de ingeniería práctica. Así, él y sus estudiantes analizaron las implicaciones de una civilización extremadamente avanzada capaz de mantener abierta la boca de un agujero de gusano. Las conclusiones son fascinantes y llevaron a una nueva línea de pensamiento sobre la estructura del espacio-tiempo.

Empujar los límites y ver el comportamiento "ideal" es estimulante.

La conexión con la cripto es esta: quizá deberíamos pensar más en las implicaciones y efectos de la criptografía fuerte, el dinero digital, los remailers ideales, etc., suponiendo que ciertos problemas prácticos que hoy nos acosan están, o pronto estarán, resueltos. En cierta medida ya hacemos esto, como cuando hablamos de las mezclas ideales de Chaum del mismo modo en que los ingenieros hablan de amplificadores operacionales ideales: una abstracción útil del comportamiento en el límite, frente a la cual se pueden comparar implementaciones reales, más pobres.

Y, por supuesto, muchos de nosotros hemos encontrado que "True Names" de Vernor Vinge es un tratamiento excelente (y rápido de leer) de cómo podrían funcionar las cosas en un mundo de comunicaciones rápidas, baratas y seguras. Otros escritores lo han visto de forma diferente (por ejemplo, "Shockwave Rider", "1984", "Snow Crash").

Aquí, para ir al grano, presento unas breves afirmaciones de lo que yo veo como el "comportamiento en el límite". No las desarrollaré ahora.

- "Pay as you go" ("pagar según uso") es la forma natural de manejar la mayoría de las transacciones económicas. Hay excepciones, por supuesto, como los seguros, contratos de prestación futura, etc., pero en su mayor parte el dinero se usa para mediar intercambios inmediatos. Un ejemplo oportuno: ¿por qué tus enemigos no pueden "bombardearte" con correo basura físico a gran escala (toneladas de correo basura)? El correo basura, como lo llamamos, se da en volúmenes relativamente pequeños (como mucho un buzón lleno, excepto quizá para los famosos) por una razón muy simple: ¡alguien tiene que pagar la entrega! No hay posibilidad de un modo "gratuito" de "haz 19 copias de esta tonelada de basura y mándalas por

- correo a tus enemigos". Que sí lo haya con el software —el bombardeo vía remailers de Detweiler, el gusano de Morris de 1988, las cartas en cadena tipo "Dave Rhodes"— se debe a algunos defectos del modelo actual de la Red:

- los costes de transmisión de mensajes no son asumidos directamente por los remitentes (lo que anima a algunos a sobreutilizar recursos escasos, como en la "tragedia de los comunes");
- los sitios y los remailers responden a "instrucciones" para reenviar el mensaje, hacer copias, etc.

- Considero por tanto imperativo que desarrollemos lo más rápido posible lo siguiente:

- sistemas de pago para la transmisión de mensajes (yo ya he defendido la "postage digital", o "franqueo digital", como primera aplicación, comparativamente sencilla, del dinero digital; otros también lo han hecho, y Ray Cromwell justamente hoy ha presentado su propia propuesta... es hora de ponernos manos a la obra. Y para que no piensen que estoy llamando al altruismo, creo que en este campo se harán algunas fortunas);
- protocolos anónimos o que oculten la identidad, al estilo Chaum;
- un alejamiento general de los sistemas basados en "lo común", que alimentan las nociones de "acceso justo" y similares. Si el "problema" es que la gente pobre —se afirma— no puede permitirse una conexión a la Red de 17 dólares al mes (lo que cobra Netcom, en unas 25 ciudades y creciendo), entonces mi solución sería simplemente subvencionar su factura. (No estoy defendiendo esto, ni creo que sea sensato subvencionar el teléfono, la Red o la cena de nadie, pero esto sería mejor que "nacionalizar" las redes, creando así más confusión y menos eficiencia para todos).

- La conectividad cambiará de forma radical. La "distancia" en el ciberespacio ya no está correlacionada con la distancia física. (Nada sorprendente, ya se veía con el teléfono. Pero sigue siendo una manera útil de mirar el ciberespacio: un espacio de conectividades y distancias radicalmente alteradas).

- El acceso local al servicio, las líneas telefónicas o de cable que llegan al hogar o a la oficina, es un posible cuello de botella. Pero una vez que se establece una conexión con un nodo local en el que existen múltiples competidores (es decir, una vez que se supera el monopolio local otorgado por el gobierno), la posibilidad de "censura" disminuye rápidamente, por varias razones.

- por tanto, hay que impulsar las “líneas de acceso cifrado” desde un nodo terminal (hogar, oficina) hasta un punto con conectividad ilimitada;
- esta es la situación que yo tengo ahora con mi línea de PacBell y Netcom: a PacBell no le “importa” para qué uso la línea local, y una vez fuera puedo marcar a un Netcom menos censor en lugar de un AOL o Prodigy al estilo Gran Hermano.

• El ciberespacio es infinitamente colonizable. No hay límites al crecimiento. (Suposición: la realización del ciberespacio tiene lugar sobre diversas máquinas y redes, que no son gratuitas ni infinitas. Pero el “no hay límites” viene de la facilidad con que quienes están cerca de una “frontera” pueden simplemente empujar esa frontera hacia fuera con más recursos de CPU, más redes, etc.).

• La cripto implica que el acceso a las “regiones” puede ser controlado por los “propietarios”:

- “mi casa, mis normas”, aplicadas localmente, sin autoridad estatal central;
- seguridad esencialmente inquebrantable (en el sentido criptográfico).

• Por cierto, la criptografía fuerte es el “material de construcción” del ciberespacio... la argamasa, los ladrillos, las vigas de soporte, las paredes. Nada más puede proporcionar la “permanencia”... sin cripto, las paredes están sometidas a derrumbarse al primer toque de una persona o agencia maliciosa. Con cripto, ni siquiera una bomba H de 100 megatones puede atravesar las paredes.

(Si crees que exagero, haz algunos cálculos sobre la energía necesaria para romper un módulo de 1000 dígitos decimales).

• No harán falta “leyes de zonificación”, ni serán posibles, en el ciberespacio. (“Snow Crash” de Neil Stephenson, aunque es una lectura maravillosa y que da mucho que pensar, se equivoca aquí: el ciberespacio es demasiado extensible y controlable localmente).

• La ubicación física de los lugares del ciberespacio será cada vez más difícil de precisar. Un vasto “laberinto de habitaciones y pasillos” puede estar físicamente instanciado en un ordenador en Malasia, mientras que un “salón de juego virtual” se gestiona mediante cortafuegos criptográficos (remailers) desde el dormitorio de alguien en Provo, Utah.

- La charla sobre “normas de acceso” queda así desenmascarada como algo carente de sentido, a menos que los gobiernos repriman redes, cripto y sistemas privados de una manera muy superior a todo lo que se está discutiendo hoy.

Esta es la “criptoanarquía” sobre la que he estado escribiendo desde 1988. El ciberespacio resultará ser una frontera muchísimo más vasta que cualquier cosa que hayamos visto hasta ahora. Con “solo” 10^70 partículas en todo el universo, hay muchísimo más “espacio” (espacio de direcciones, espacio de claves, etc.) incluso en un conjunto relativamente pequeño de dígitos. El ciberespacio es espacio matemático, y su amplitud es realmente ilimitada.

Y trasladaremos nuestro comercio, nuestro entretenimiento y buena parte de nuestras vidas al ciberespacio muchísimo más rápido de lo que iremos lentamente entrando en la órbita baja terrestre y más allá. De hecho, considero que ya estoy a medio camino dentro. En unos años, con conectividad tipo Mosaic de un toque, con una plétora de opciones de red, con remailers seguros y herramientas similares para anonimizar mis transacciones, estaré tan metido ahí que ya no habrá marcha atrás.

Basta por ahora con estos comentarios. Creo que tiene sentido adoptar una perspectiva un poco más a largo plazo sobre las tendencias inevitables, para ver adónde vamos y qué cuestiones necesitan más trabajo.

Espero que algunos de ustedes estén de acuerdo conmigo.

Contexto Histórico

Timothy C. May (Tim May) fue ingeniero en Intel y uno de los fundadores y principales teóricos del movimiento cypherpunk. Es autor de:

- The Crypto Anarchist Manifesto (1988),
- Libertaria in Cyberspace (1992),
- Cyberspace, Crypto Anarchy, and Pushing Limits (3 de abril de 1994),
- The Cyphernomicon (FAQ gigante del movimiento, 1994),
- Crypto Anarchy and Virtual Communities (1994).

El mail se envía a la lista cypherpunks@toad.com, el espacio donde May, Eric Hughes, Hal Finney, Nick Szabo, etc. discuten sobre criptografía, anonimato, dinero digital y el impacto político de todo ello.

Momento tecnológico y político (1993–1994)

Internet comercial está naciendo, la Web (Mosaic) acaba de aparecer, los módems y los ISP como Netcom son la puerta de entrada a la red. dspace.mit.edu

Hay preocupación por:

- El Clipper Chip y los intentos del gobierno de EE.UU. de controlar la criptografía.
- El aumento de spam, gusanos y “mailbombing”.
- Los primeros experimentos de dinero digital (Chaum, DigiCash, ecash).

La lista cypherpunk es el lugar donde se está cocinando la filosofía que, años después, inspirará propuestas como b-money (Wei Dai), bit gold (Szabo) y, en última instancia, Bitcoin.

Este correo de Tim May, enviado a la lista de cypherpunks en abril de 1994, es una pieza muy representativa del momento en el que la criptografía deja de ser solo un tema técnico y empieza a pensarse como algo que puede reorganizar la sociedad.

May escribe cuando Internet comercial está naciendo, la web comienza a popularizarse y los gobiernos discuten cómo controlar la criptografía. En ese contexto, él se adelanta y se pregunta: ¿qué pasa si la cripto funciona muy bien? ¿Cómo cambia el mundo si damos por hecho comunicaciones seguras, dinero digital y anonimato robusto?

Para introducir su idea, May recurre al ejemplo del físico Kip Thorne, que estudió los viajes en el tiempo a través de agujeros de gusano no porque fueran factibles en la práctica, sino porque es intelectualmente valioso explorar los límites de lo posible. May propone hacer lo mismo con la criptografía: imaginar un escenario "ideal" en el que muchos de los problemas prácticos se han resuelto y observar qué tipo de sociedad, economía y estructuras de poder emergerían de ahí. No se conforma con hablar de parches técnicos; quiere llevar el razonamiento hasta el extremo y ver qué implica.

Una de las primeras cuestiones que aborda es la del coste de los mensajes y el problema del spam. En el mundo físico, explica, nadie puede enviarte toneladas de correo basura porque alguien tiene que pagar el franqueo. En cambio, en Internet, mandar millones de copias de un mismo mensaje es prácticamente gratis para el emisor, lo que abre la puerta al spam, a los gusanos y a los "mailbombing". Para él, el diseño actual de la red tiene un fallo económico: los costes de transmisión no recaen de forma directa en quien envía, así que algunos tienden a abusar de un recurso que se percibe como "gratis", la típica "tragedia de los comunes". Su propuesta conceptual es clara: avanzar hacia un modelo de "pagar según uso", donde cada mensaje lleve un pequeño coste, ya sea monetario o computacional, que haga inviables los abusos masivos. Ahí está la semilla de ideas como el franqueo digital o esquemas de "prueba de trabajo" para frenar el spam.

Desde esa base económica, May pasa a la estructura de las redes y la censura. Señala que en el ciberespacio la distancia ya no tiene mucho que ver con los kilómetros físicos: lo importante es a qué nodos te conectas y con qué libertad puedes elegir. El verdadero cuello de botella está en el acceso local, la famosa "última milla" que va de tu casa al proveedor. Una vez superado ese punto, si puedes conectar con múltiples redes o proveedores, la capacidad de censura se reduce drásticamente. De ahí su insistencia en usar líneas cifradas desde el terminal del usuario hasta nodos con mayor libertad, y en escoger proveedores menos controladores que las grandes plataformas de la época. Es una intuición muy temprana de lo que hoy entendemos como VPN, ISPs respetuosos con la privacidad y separación entre infraestructura física y servicios lógicos.

A continuación formula una idea potente: el ciberespacio es, en esencia, un espacio matemático casi infinito. Aunque el hardware sea finito, el número de direcciones, claves, identidades y "habitaciones virtuales" que se pueden crear es gigantesco. Por eso sostiene que no tiene sentido aplicar al ciberespacio el modelo de "zonificación" del mundo físico, con normas urbanísticas sobre qué se puede hacer en cada sitio. En la red, si una "zona" se restringe, siempre es posible crear otra nueva, con otras reglas, movida a otra jurisdicción o distribuida criptográficamente. La ubicación física del servidor deja de ser relevante para quien habita ese espacio: un laberinto de salas de conversación puede estar físicamente en Malasia y un casino virtual gestionarse desde un dormitorio en Utah, oculto tras remailers y capas de cifrado. La implicación política es fuerte: los intentos clásicos de control territorial pierden eficacia cuando el "territorio" es abstracto y duplicable.

En este punto introduce una metáfora clave: la criptografía fuerte es el material de construcción del ciberespacio. Es el ladrillo, la argamasa, las vigas y las paredes. Sin cripto robusta, cualquier muro que se quiera levantar —espacios privados, reglas locales, comunidades cerradas— puede derrumbarse ante el primer atacante con recursos. Con buena cripto, en cambio, esos muros se convierten en barreras que ni siquiera un Estado muy poderoso puede romper si los algoritmos y las claves están bien elegidos.

Aquí May desplaza el eje del conflicto: ya no se trata solo de leyes versus infractores, sino de leyes versus matemáticas. El código y la criptografía pasan a definir qué es posible, y la ley se ve limitada por lo que físicamente se puede o no se puede hacer romper.

A partir de ahí, May entra de lleno en la dimensión política: si el ciberespacio se construye sobre criptografía, las "regiones" de ese espacio podrán ser controladas por sus "propietarios", que aplicarán su propio "mi casa, mis normas" de manera local, sin necesidad de una autoridad estatal central.

Cada espacio virtual puede fijar reglas de acceso, anonimato, comercio, moderación de contenidos, etc., y hacerlas cumplir mediante tecnología, no mediante policía o tribunales. Las discusiones sobre "normas de acceso" impuestas desde los gobiernos pierden sentido práctico si siempre es posible montar nuevas infraestructuras cifradas fuera de su alcance, salvo que los Estados adopten medidas extremadamente represivas contra la criptografía y las redes privadas.

Todo esto es lo que May agrupa bajo el término “criptoanarquía”. No se refiere a un caos destructivo, sino a un orden emergente en el que individuos y grupos usan herramientas criptográficas para comunicarse, comerciar y asociarse sin necesidad de identificarse ante una autoridad central ni pedir permiso para operar.

Las implicaciones son profundas: se debilita el control fiscal, se pone en cuestión la capacidad de censurar contenidos, se dificulta la vigilancia masiva y se abren espacios para mercados y comunidades que no encajan en las regulaciones tradicionales. Para muchos, esto es liberador; para los Estados y grandes instituciones, es percibido como una amenaza.

Visto con perspectiva, este correo de 1994 anticipa varios desarrollos posteriores: sistemas de freno al spam basados en coste, ideas de dinero digital y micropagos, herramientas de anonimato como los remailers y, más adelante, la aparición de propuestas de dinero electrónico descentralizado que culminan en Bitcoin.

También anticipa debates actuales sobre soberanía digital, jurisdicción en Internet, censura de plataformas, regulación de criptomonedas y el papel de la privacidad en la era de la vigilancia masiva. En el momento en que lo escribe, todo esto es todavía especulativo; pero May ya se declara “medio dentro” del ciberespacio y convencido de que, una vez que las herramientas sean suficientemente fáciles de usar, muchos otros también se mudarán ahí en buena parte. Su mensaje, en el fondo, es una invitación a mirar más lejos: si aceptamos que la criptografía fuerte va a existir y ser accesible, más vale pensar desde ya en el tipo de mundo que eso hace posible.

Pre-Textos del Bitcoiner es una publicación libre, nacida para difundir conocimiento sobre Bitcoin sin peajes ni aduanas, hecha con la materia prima más valiosa que tenemos: la experiencia, las ideas y las preguntas de la comunidad.