

Bloques de un minuto: un análisis de la propuesta del tiempo entre bloques

Leo Beltrán

28 de octubre de 2026

Resumen

El CHIP-2025-03 propone bajar el tiempo objetivo entre bloques de Bitcoin Cash de diez minutos a uno. Los problemas que invoca son reales: la varianza de las confirmaciones, la contención de UTXO en DeFi y la dependencia de servicios que exigen confirmaciones. Pero el cambio no los elimina: los reescala. Y para hacerlo modifica una de las constantes fundacionales de la red, agrega una abstracción permanente al protocolo y traslada costos concretos —sobre todo a los clientes SPV— que todavía no se han cuantificado.

Mi pedido es concreto: que el CHIP no haga *lock-in* el 15 de noviembre de 2026, y que se vuelva a discutir para una actualización futura, una vez medidos los costos y agotadas las soluciones específicas para cada problema. No es un «nunca». Es un «todavía no».

Contexto

Bitcoin Cash produce hoy un bloque cada diez minutos en promedio. Como la prueba de trabajo es un proceso aleatorio, el tiempo entre bloques sigue una distribución exponencial: algunas confirmaciones llegan en segundos y otras tardan más de media hora, aunque el promedio se mantenga.

El CHIP-2025-03, «*Faster Blocks for Bitcoin Cash*», escrito por *bitcoincashautist*, propone reducir ese promedio a un minuto e introducir un sistema de «*ticks*» —unidades de tiempo idealizado— para que las reglas de consenso que hoy dependen de la altura de bloque sigan funcionando igual.¹ El CHIP nació en marzo de 2025 proponiendo dos minutos, y bajó a uno en abril de ese año después de modelar la latencia real de la red.²

Al momento de escribir esto, el CHIP figura como «*Proposed*» (su última edición es del 24 de octubre de 2026) y se discute como candidato para la actualización de mayo de 2027, cuya fecha de *lock-in* es el 15 de noviembre de 2026.^{3,4} Desde septiembre, un hilo específico recoge las declaraciones de apoyo y de rechazo de los actores del ecosistema.⁵ Hay rechazos y posturas

¹CHIP-2025-03 (versión del 24 de octubre de 2026), sección «[Blockchain Height Abstraction](#)»: define los *ticks* como unidad de tiempo idealizado (600 por bloque de 10 minutos, 60 por bloque de 1 minuto).

²*bitcoincashautist*, [post n.º 19](#), 2 de abril de 2025: modelo de latencia (pings < 300 ms; > 80 % de proveedores VPS con > 436 Mbit/s) y estimación de huérfanos < 1,99 % en el peor caso.

³CHIP-2025-03 (versión del 24 de octubre de 2026), [encabezado](#): «*Status: Proposed*», «*Last Edit Date: 2026-10-24*». El calendario de activación está en la sección «[Deployment](#)».

⁴*kzKallisti*, [post n.º 57](#), hilo «2027 protocol upgrade ideas», 8 de agosto de 2026: CHIP candidatos para 2027 y fecha de *lock-in* (15 de noviembre de 2026).

⁵Hilo «[CHIP-2025-03 Faster Blocks: gathering statements of support \(and dissent\)](#)», abierto el 15 de septiembre de 2026; último post revisado: 25 de octubre de 2026. Las posturas se siguen también en [Consensus.cash](#).

condicionales relevantes: algunas rechazan el cambio en sí, como yo, y otras rechazan activarlo **ahora**. El autor, por su parte, sostiene que nunca habrá unanimidad y que no se puede «frenar al caballo» por quienes disienten.⁶ Quedan pocos días para el *lock-in*, y por eso este ensayo termina con un pedido concreto.

1. Qué busca el CHIP

Antes de discutir una propuesta conviene entenderla en su mejor versión. Esto no es sencillo, porque el propio CHIP define su objetivo de una manera llamativa: ante la objeción de que su lista de beneficios cambiaba con el tiempo, el autor respondió que **el objetivo del CHIP son los bloques más rápidos**, y que la lista de beneficios describe cómo los experimentaría cada tipo de usuario, porque «el usuario promedio no existe».⁷ Tom Zander leyó esa respuesta como una confesión: «no hay otro objetivo que el cambio en sí».⁸

Los argumentos a favor son estos:

1. **Primera confirmación más rápida.** Hay situaciones en las que 0-conf no alcanza: transacciones riesgosas, *swaps* irreversibles entre cadenas (Thorswap, Sideshift), pasarelas multimoneda (BitPay, Bitgree) y billeteras multimoneda que no muestran fondos sin confirmar.⁹ Allí, el tiempo de bloque es el límite de velocidad visible. Con un minuto, el 95 % de las primeras confirmaciones llegaría en menos de tres minutos.¹⁰
2. **Confirmaciones múltiples más previsibles.** Para operaciones de alto valor, la espera tendría mucha menos dispersión.
3. **Recuperación más rápida en DeFi.** Cuando dos usuarios de un contrato como Cauldron chocan sobre el mismo UTXO, la espera para reintentar bajaría de diez o treinta minutos a uno o tres.¹¹
4. **Una «escala deslizante».** No es que un bloque de un minuto sea más seguro que uno de diez: un bloque de un minuto acumula, a grandes rasgos, una décima parte del trabajo. Lo que se gana es la posibilidad de elegir con más finura el punto entre velocidad y seguridad. Con la imagen de rnbrady: elegir entre «100 dólares de seguridad en un minuto y 1000 dólares en diez».^{12,13}
5. **Beneficios secundarios:** mayor granularidad para contratos con *locktime*, pagos más frecuentes a *pools* chicos, un algoritmo de dificultad que reacciona más rápido ante caídas de *hashrate* y una recuperación más rápida de la comisión mínima de la *mempool*.¹⁴
6. **El costo de no hacer nada.** El CHIP sostiene que mantener los diez minutos no es neutral: los usuarios nuevos forman su primera impresión frente a cadenas más rápidas, y cuanto

⁶bitcoincashautist, [post n.º 59](#), hilo «2027 protocol upgrade ideas», 8 de agosto de 2026: «You will never get unanimous. [...] There will always be those who disagree, can't hold the horse just for them.»

⁷bitcoincashautist, [post n.º 156](#), 29 de mayo de 2026, respuesta a JohnGalt: «The CHIP's goal is to deliver faster blocks»; «Average user doesn't exist».

⁸tom (Tom Zander), [post n.º 158](#), 1.º de junio de 2026: «There is no goal other than the change itself.»

⁹bitcoincashautist, [post n.º 157](#), 29 de mayo de 2026: usuarios reales de 1-conf (Bitgree, BitPay, Coinsbee, Thorswap, Sideshift). «Nobody wants to be a 1-conf user, everyone wants to be a 0-conf user.»

¹⁰CHIP-2025-03 (versión del 24 de octubre de 2026), sección «[Summary](#)»: «95% of single-confirmation transactions clearing in under 3 minutes, compared to 25% exceeding 14 minutes today». Desarrollo en «[Instant Improvement in 1-Confirmation Experience](#)».

¹¹bitcoincashautist, [post n.º 156](#), 29 de mayo de 2026: «Those users today wait 10-30 minutes when caught by a divergence event. With 1-minute blocks, the same users would wait 1-3 minutes.»

¹²rnbrady, [post n.º 154](#), 28 de mayo de 2026: «you get a sliding scale between \$100 of security in 1-min, and \$1000 of security in 10-minutes».

¹³BitcoinCashPodcast, [post n.º 161](#), 2 de junio de 2026: «faster blocks is sometimes a benefit to speed and sometimes a benefit to security».

¹⁴CHIP-2025-03 (versión del 24 de octubre de 2026), secciones «[Blockchain Time Granularity](#)», «[More Responsive Mempool Fee Decay](#)» e «[Improved Difficulty Adjustment Stability](#)».

más tiempo pase, más *software* asumirá diez minutos como fijo.¹⁵

La pregunta no es si estos beneficios existen, sino si justifican lo que cuestan y si este es el modo correcto de obtenerlos.

2. El problema es real, pero el cambio no lo elimina

2.1. La varianza, con los números correctos

Que el tiempo entre bloques siga una distribución exponencial tiene dos consecuencias. La primera es que **no tiene memoria**: llegue cuando llegue una transacción, la espera hasta el próximo bloque es, en promedio, de diez minutos. La segunda es que **la desviación estándar es igual a la media**. De ahí salen las cifras del propio CHIP: alrededor de una de cada cuatro transacciones espera más de 14 minutos ($e^{-1,4} \approx 25\%$) y una de cada siete espera más de 20 ($e^{-2} \approx 13,5\%$).¹⁶

Para quien necesita **una** confirmación, el cambio mejora la situación de verdad. Pero para quien necesita **varias** —el caso de los *exchanges*—, el beneficio no es el que suele imaginarse. Si un *exchange* define cuántas confirmaciones exige en función de la seguridad que quiere obtener, con bloques de un minuto multiplicará por diez la cantidad de confirmaciones.^{17,18} Kraken, por ejemplo, exige hoy 15 confirmaciones de BCH;¹⁹ con bloques de un minuto necesitaría unas 150 para obtener una seguridad comparable. **El tiempo medio de espera sería el mismo: unos 150 minutos.**

Lo que sí cambia es la dispersión. Con seis confirmaciones de diez minutos, la probabilidad de esperar más de 90 minutos es del 11,6 %; con sesenta confirmaciones de un minuto, cae al 0,03 %. En otras palabras: para los *exchanges*, el CHIP no ofrece **velocidad**, ofrece **previsibilidad**. Es un beneficio mucho más modesto que el que sugiere la frase «bloques diez veces más rápidos».

2.2. DeFi: mitigar un síntoma no es resolver el problema

La contención de UTXO en los contratos de acceso público es un problema legítimo: dos usuarios intentan operar sobre el mismo UTXO, los nodos ven versiones distintas de la *mempool* y una de las dos transacciones falla. Pero los bloques de un minuto no eliminan ese problema: solo acortan la espera hasta que se resuelve.

JohnGalt lo cuantificó: en condiciones adversas, la ventana de divergencia entre nodos después de cada bloque pasaría de cubrir alrededor del 99 % del intervalo a alrededor del 91 %. Su conclusión: «sin sincronización de la *mempool*, da igual que los bloques sean de un minuto o de diez».²⁰ Cuando un usuario reportó haber esperado 115 minutos por un bloque y concluyó que hacían falta bloques más rápidos,²¹ rnbrady respondió algo que resume mi postura: con bloques más rápidos, el mensaje de error seguiría apareciendo, solo que desaparecería antes; **«deberíamos resolver el problema por completo».**²²

¹⁵CHIP-2025-03 (versión del 24 de octubre de 2026), sección «[Status Quo](#)»: apartado «*The Cost of Inaction*»: «*The status quo is not a neutral choice.*»

¹⁶CHIP-2025-03 (versión del 24 de octubre de 2026), sección «[Motivation](#)»: «*Even with steady hash power, about one in four transactions waits over 14 minutes, and one in seven waits over 20 minutes.*»

¹⁷ShadowOfHarbringer, [post n.º 151](#), 28 de mayo de 2026: los *exchanges* escalarían a 10× confirmaciones.

¹⁸BitcoinCashPodcast, [post n.º 153](#), 28 de mayo de 2026: «*We are NOT trying to trick exchanges into 10x lower confirmations.*»

¹⁹rnbrady, [post n.º 150](#), 28 de mayo de 2026: Kraken exige 15 confirmaciones; «*I'm not aware of any exchanges that accept 1-conf.*»

²⁰JohnGalt, [post n.º 149](#), 28 de mayo de 2026: «*With 1-minute blocks, it is divergent for 55 seconds, about 91% of the interval*»; «*Without mempool synchronisation, it doesn't matter if blocks are a minute or 10 minutes.*»

²¹CashDragon, [post n.º 162](#), 29 de junio de 2026: espera de 115 minutos (bloque 957 389).

²²rnbrady, [post n.º 164](#), 29 de junio de 2026: «*We should solve the problem completely.*»

Si el problema es la contención en DeFi, conviene buscar una solución **específica para ese problema**, en la capa donde se genera, que no dependa de modificar el tiempo entre bloques. Hay caminos para explorar:

- **En servicios con infraestructura propia:** agrupar las solicitudes por aplicación y ordenarlas de modo que no se generen transacciones contradictorias.
- **En modelos totalmente descentralizados:** usar *double-spend proofs* (DSProofs) para avisarle al usuario de una posible colisión, e incluso estimar una probabilidad de éxito según cuántos nodos vieron cada versión.

Usar un problema real como justificación de un cambio que no lo resuelve tiene un costo adicional: el problema sigue ahí después de la activación, y ya no queda una justificación nueva para atacarlo.

2.3. Una solución permanente para un problema temporal

Buena parte de los casos que justifican el CHIP dependen de **terceros centralizados**: *exchanges* que exigen confirmaciones, pasarelas que no aceptan 0-conf y billeteras multimoneda que no muestran fondos sin confirmar. Ese es el problema temporal: la dependencia actual del ecosistema respecto de entidades que no controla.

Al mismo tiempo, las últimas actualizaciones de la red —CashTokens, la introspección nativa, los contratos más expresivos— apuntan precisamente a lo contrario: a que Bitcoin Cash dependa cada vez menos de esos intermediarios, y a que las finanzas descentralizadas y el autocustodio sean el motor de su uso. Hay algo contradictorio en modificar de forma permanente una constante del protocolo para acomodar mejor a los actores de los que la propia red está intentando independizarse.

El CHIP responde que el cambio también favorece el autocustodio y DeFi.²³ Pero en DeFi, como se vio, el cambio mitiga el problema sin eliminarlo.

3. Los costos

3.1. Clientes SPV: el costo central

Conviene precisar a quién afecta este costo, porque no todas las billeteras livianas funcionan igual:

- **Las billeteras SPV propiamente dichas**, como Flowee Pay, descargan la cadena de *headers* y piden a los nodos los bloques filtrados que contienen sus transacciones. Son las que verifican por su cuenta la inclusión de cada pago sin depender de un servidor de confianza, y son las más afectadas.
- **Las billeteras que usan el protocolo Electrum**, como Electron Cash, también descargan *headers*, aunque solo desde un *checkpoint* y no desde el bloque génesis.
- **Muchas billeteras móviles de BCH** consultan servidores Fulcrum y no guardan la cadena de *headers*. Su costo directo es menor, pero lo trasladan a esos servidores y dependen más de ellos.

Es decir: el costo recae con más fuerza justamente sobre las billeteras que menos dependen de terceros.

²³CHIP-2025-03 (versión del 24 de octubre de 2026), sección «[Reduced Reliance on Centralized Exchanges](#)»: «*faster confirmations also strengthen self-custody as a practical alternative to leaving funds on CEXes*».

Cada *header* ocupa 80 bytes. Con diez veces más bloques, el crecimiento anual pasa de unos 4,2 MB a unos 42 MB, cifra en la que coinciden el CHIP y las críticas.²⁴ El problema tiene tres dimensiones, aunque no pesan lo mismo.

1. Almacenamiento. La respuesta habitual es que el almacenamiento siempre se abarata. Pero ese supuesto no está garantizado, como mostró la suba de los precios de la memoria en 2026, impulsada por la demanda de servidores para inteligencia artificial.^{25,26} Aunque sea transitoria, muestra que no se puede dar por descontado el abaratamiento continuo para desestimar un costo que se acumula en cada dispositivo, para siempre.

2. Sincronización. Tom Zander, que desarrolla la billetera SPV de Flowee desde hace unos quince años, sostiene que las billeteras SPV escalan porque separan la carga de la red de la carga de cada billetera, y que pedirle a un nodo los bloques filtrados de a uno se vuelve lento cuando hay muchos más bloques. Su conclusión es tajante: «agreguen bloques de un minuto y SPV va a morir»; «hacerlo diez veces más lento es una sentencia de muerte».²⁷ Zander advierte además que las pruebas de laboratorio son optimistas: la red tiene nodos muy lentos y las conexiones móviles son muy irregulares, y la latencia no se puede eliminar porque una billetera no puede actuar sobre un bloque filtrado hasta recibirlo.²⁸ En números: una billetera que estuvo un mes sin conectarse tiene hoy que ponerse al día con unos 4300 bloques; con bloques de un minuto, con unos 43 000.

3. Dispositivos limitados. JohnGalt plantea el caso de una billetera que sincroniza *headers* por NFC al momento de pagar: una semana de *headers* hoy ocupa unos 80 KB y se transmite en un toque de un segundo y medio; con bloques de un minuto serían unos 800 KB y unos quince segundos de contacto —«ya no es tocar, es sostener»—.²⁹ Y no es una preocupación aislada de los opositores: kzKallisti, que no se opone al CHIP en principio, dijo en agosto que este problema de los pagos con tarjetas NFC le alcanzaba «por sí solo» para dudar, y propuso postergar el cambio a 2028.³⁰

Los defensores responden con mitigaciones: pedir los bloques en lotes más grandes,³¹ los filtros compactos (BIP-157/158),^{32,33} el precedente de Dogecoin^{34,35} y la poda de *headers* de CHIP-2026-02.^{36,37} Todas tienen algo en común: dependen de trabajo que todavía no está hecho o no está

²⁴CHIP-2025-03 (versión del 24 de octubre de 2026), sección «[Header Chain Growth](#)»: «Header chain growth rises 10x, from ~4.2 to ~42 MB/year» (frase del «[Reader's Guide](#)»).

²⁵The Register, «[DRAM prices expected to double in Q1 as AI ambitions push memory fabs to their limit](#)», 2 de febrero de 2026, con datos de TrendForce.

²⁶TrendForce, «[AI Server Demand Continues to Support Memory Prices in 3Q26](#)», 3 de julio de 2026.

²⁷tom (Tom Zander), [post n.º 41](#), hilo «2027 protocol upgrade ideas», 1.º de agosto de 2026: «Add one minute blocks and SPV will die»; [post n.º 44](#), 2 de agosto de 2026: «Making it 10 times as slow is a death sentence.»

²⁸tom, [post n.º 168](#), 4 de agosto de 2026: «Tests I did gave about 100 blocks per second»; «laboratory tests are very likely optimistic».

²⁹JohnGalt, [post n.º 149](#), 28 de mayo de 2026: «one week becomes about 10,080 headers, roughly 800 KB»; «With 10x more headers it now becomes not tap, but hold.»

³⁰kzKallisti, [post n.º 62](#), hilo «2027 protocol upgrade ideas», 8 de agosto de 2026: «This issue alone is enough to give me pause on Faster Blocks»; «it might be worth pushing to 2028».

³¹bitcoincashautist, [post n.º 48](#), hilo «2027 protocol upgrade ideas», 2 de agosto de 2026: «I changed this one line from 9 to 99 [...] the wallet jumped from syncing about 5 blocks / second to 50 blocks / second!»

³²nyusternie, [post n.º 47](#), hilo «2027 protocol upgrade ideas», 2 de agosto de 2026: BIP-157/158 y filtros compactos.

³³nyusternie, [post n.º 170](#), 4 de agosto de 2026: respuesta punto por punto a tom (post n.º 168) sobre la sincronización SPV, basada en BIP-157/158.

³⁴CHIP-2025-03 (versión del 24 de octubre de 2026), sección «[Reader's Guide](#)»: «Dogecoin has run 1-minute blocks since 2013».

³⁵bitcoincashautist, [post n.º 61](#), hilo «2027 protocol upgrade ideas», 8 de agosto de 2026: «Dogecoin has been running 1-minute blocks the entire time (since 2014) without breaking SPV or exchanges or anything else.»

³⁶CHIP-2025-03 (versión del 24 de octubre de 2026), sección «[Reader's Guide](#)»: «storage is already mitigated by Ectrum header merkle proofs, and header pruning via CHIP-2026-02 makes it fixed-size». Desarrollo en «[Header Chain Growth](#)».

³⁷bitcoincashautist, [post n.º 61](#), hilo «2027 protocol upgrade ideas», 8 de agosto de 2026: CHIP-2026-02, implemen-

desplegado. Hay que cambiar el código de billeteras de terceros, adoptar filtros compactos y activar otro CHIP. Si el costo para SPV se resuelve con esas mitigaciones, lo razonable es que lleguen antes que los bloques de un minuto, y no después.

3.2. Menos trabajo por bloque y centralización minera

A Calin Culianu, desarrollador principal de Bitcoin Cash Node, le parece «fundamentalmente incorrecto» tomar una cadena con unas doscientas transacciones por bloque y una fracción mínima del *hash* SHA-256 total, y dividirla por diez: unas veinte transacciones por bloque y «bloques mucho menos seguros».³⁸ El autor responde que el daño que puede causar un atacante depende de su *hashrate*, no del tiempo de bloque.

En su declaración de septiembre, Culianu desaprobó el CHIP «por ahora»: el código no estaba listo y era probable que tuviera errores nuevos.³⁹ Sus condiciones —terminar el código, probarlo más y hacerlo revisar— son, en esencia, las mismas que plantea este ensayo.⁴⁰

Un riesgo relacionado es la centralización minera. Los *pools* grandes pierden menos por bloques huérfanos que los chicos, así que cuanto mayor es la tasa de huérfanos, mayor es su ventaja relativa. La versión actual del CHIP estima esa tasa entre 0,41 % y 1,94 % según las condiciones modeladas, frente a un umbral tolerable de 2 %, ⁴¹ y el autor cita la experiencia de Dogecoin, con alrededor de 0,15 %. ⁴² Pero el peor caso modelado queda a apenas seis centésimas de punto porcentual del umbral que el propio CHIP define como tolerable. Cashrider pidió mayores márgenes de propagación y advirtió que la experiencia de otras redes no es directamente comparable con la de BCH. ^{43,44} albaDsl, por su parte, desaprobó el cambio porque la implementación no está lista, y porque teme que se esté cediendo demasiado margen de seguridad: un sistema con bloques más cortos es más rígido ante eventos catastróficos. ⁴⁵ El modelo existe, pero es un modelo: la tasa real recién se conocerá con la red funcionando.

3.3. Complejidad permanente

El CHIP resuelve técnicamente el problema de los contratos que dependen de la altura de bloque: los evalúa contra una escala normalizada (*tick* / 600), de modo que se comporten igual que hoy en tiempo real. ⁴⁶ Pero la solución tiene un costo propio: introduce una **abstracción**

tación de prueba en BCHN y poda de *checkpoints* en Electron Cash.

³⁸bitcoincashautist, [post n.º 179](#), 15 de septiembre de 2026, transmitiendo a Culianu: «*it feels fundamentally wrong to take a chain with like ~200 txns per block and .025% hash divide it by 10x — ~20tx per block and far less secure blocks at 0.0025% hash*». Respuesta: «*grief is a rate problem, and the rate is fixed by hashrate, not by block time*». La misma frase de Culianu aparece en su declaración (ver nota sobre el post n.º 4 del hilo de declaraciones). Las cifras de *hash* de la cita deben tomarse como ilustrativas: según CoinWarz, el 28 de octubre de 2026 BCH tenía unos 4,4 EH/s ([gráfico](#)), alrededor del 0,5 % del total de SHA-256.

³⁹cculianu (Calin Culianu), [post n.º 4](#), 15 de septiembre de 2026: «*Disapprove (for now)*. Rationale: code is not ready and likely to have new and exciting bugs.»

⁴⁰cculianu, [post n.º 13](#), 15 de septiembre de 2026: terminar el código «ASAP w/ more testing» y una revisión adicional.

⁴¹CHIP-2025-03 (versión del 24 de octubre de 2026), sección «[Increased Orphan Rate](#)»: «*Orphan rate rises modestly: 0.41–1.94% across our modeled conditions, against a 2% tolerable threshold*». Sobre la ventaja de los *pools* grandes: «[Mining Centralization Risk](#)».

⁴²bitcoincashautist, [post n.º 178](#), 6 de septiembre de 2026: Dogecoin ~0,15 % de huérfanos; modelo del CHIP 0,41–1,94 %; chipnet ~6 meses antes de la red principal.

⁴³Cashrider, [post n.º 172](#), 11 de agosto de 2026, sobre propagación y centralización: «*higher stale rates can create some advantage for miners with better connectivity and propagation infrastructure*».

⁴⁴Cashrider, [post n.º 186](#), 18 de septiembre de 2026: la experiencia de otras redes no es directamente comparable con la de BCH.

⁴⁵albaDsl, [post n.º 99](#), 30 de septiembre de 2026: «*I disapprove mainly because the implementation is not ready, but I'm also wondering if we are giving up too much of our safety margin with 1-min blocks*».

⁴⁶CHIP-2025-03 (versión del 24 de octubre de 2026), sección «[Transaction Locktime and Input Sequence](#)»: «*Height-mode nLocktime and nSequence are normalized to the 10-minute scale*»: una transacción es final en el bloque b si $T(b) >$

nueva y permanente, que cualquier persona que programe para Bitcoin Cash va a tener que entender y tener en cuenta. Ya hay alturas de bloque, *ticks*, confirmaciones medidas en bloques y confirmaciones medidas en *ticks*. mainnet_pat advirtió que los *ticks* parecen agregar complejidad y van a confundir a quienes lleguen nuevos al ecosistema.^{47,48}

La crítica más fuerte en este punto viene de quien tiene que escribir el código. Culianu explicó que, aunque los *ticks* simplifican el concepto, para quien los implementa es como si hubiera estallado una bomba en el código: «todo se tocó».⁴⁹ Sostuvo que el CHIP toca más de lo necesario y que «casa» con la prueba de trabajo cosas que antes no estaban atadas a ella, como el tamaño de bloque y nLockTime/nSequence.⁵⁰ De todo el CHIP, lo que menos le gusta es justamente la solución a los contratos: redefinir nLockTime para que la altura signifique una «altura abstracta en un espacio abstracto donde los bloques siguen siendo de diez minutos», lo que, según él, vuelve muy difícil razonar sobre esos campos.⁵¹ Y resumió: la implementación es una «pesadilla»; «se rompieron todas las pruebas».⁵² Su balance final es que hubo que aceptar concesiones y que, aunque los *ticks* se presenten como una simplificación, son una capa de abstracción que agrega complejidad al código y al nodo.⁵³

El autor y emergent_reasons responden que, sin *ticks*, habría que tocar los mismos lugares, pero ajustando a mano cada regla, con más riesgo de errores.^{54,55} Es un buen argumento a favor de los *ticks* si se cambia el intervalo, pero no a favor de cambiarlo. Quizás habría sido más simple tener bloques de un minuto desde el principio. Pero ese no fue el parámetro elegido, y cambiarlo ahora obliga a una capa de compatibilidad que la red va a cargar para siempre.

3.4. Costos de activación sin cuantificar

El CHIP describe los costos de activación —para nodos, minería, *exchanges*, billeteras livianas, exploradores, indexadores y aplicaciones DeFi— como «reales pero acotados».⁵⁶ JohnGalt pidió que se estimaran con números, consultando a cada equipo.⁵⁷ El autor respondió que la mayoría de los interesados reales —equipos de nodos, operadores de *pools*, *exchanges* y desarrolladores de billeteras— ya sigue la discusión o al menos la conoce.⁵⁸ Pero conocer la propuesta no es lo mismo que haber estimado cuánto cuesta adaptarse a ella. Cashrider planteó un riesgo con-

600 * L.

⁴⁷mainnet_pat, [post n.º 18](#), 16 de septiembre de 2026: «Approve, but with caution»; «The ticks approach seems to bring more complexity.»

⁴⁸mainnet_pat, [post n.º 184](#), 16 de septiembre de 2026: los *ticks* y los cambios en las API pueden confundir a quienes lleguen nuevos.

⁴⁹cculianu, [post n.º 226](#), 11 de octubre de 2026: «To someone that has to implement this – it's like a NUKE went off in the codebase. Everything got touched.»

⁵⁰cculianu, [post n.º 228](#), 11 de octubre de 2026: «you touched more than needed to be touched»; «What you did was marry lots of stuff now to PoW in a way where it wasn't explicitly married before. Including block size! Including nLocktime/nSequence!»

⁵¹cculianu, [post n.º 230](#), 11 de octubre de 2026: «Of all the things in this chip – the modification of nLocktime to have a changed meaning is the one I like the least.»

⁵²cculianu, [post n.º 237](#), 11 de octubre de 2026: «implementation is a nightmare for me. EVERY TEST BROKE.»

⁵³cculianu, [post n.º 243](#), 11 de octubre de 2026: «I'm not against the CHIP [...] I think it would be devastating at this point to the community if this were not to activate either now or 1 year from now. And I think we should do it.» También: «compromises had to be made»; «there is more complexity added to the code and to the node».

⁵⁴emergent_reasons, [post n.º 222](#), 11 de octubre de 2026, citando al autor: sin *ticks*, el cambio sería «the same change with the abstraction replaced by N ad-hoc re-derivations of it».

⁵⁵bitcoincashautist, [post n.º 227](#), 11 de octubre de 2026: «without ticks the same everything would've had to be touched – just touched in a different way».

⁵⁶CHIP-2025-03 (versión del 24 de octubre de 2026), sección «Activation Costs»: «The activation costs of this proposal are real but bounded.»

⁵⁷JohnGalt, [post n.º 149](#), 28 de mayo de 2026: «The CHIP should include or solicit third-party estimates: how much time node teams need, how much time mining pools need, how much time wallets need».

⁵⁸bitcoincashautist, [post n.º 156](#), 29 de mayo de 2026, sobre los costos: «Most actual stakeholders (node teams, pool operators, exchanges, wallet developers) are reading or at least aware.»

creto que esa señal no captura: el *software* de terceros que puede seguir funcionando aunque sus supuestos sobre confirmaciones, altura de bloque o seguridad hayan cambiado **en silencio**, sin que nadie lo advierta hasta después de la activación. Y preguntó qué criterio de preparación sería suficiente.⁵⁹ El propio CHIP reconoce que el riesgo principal es ese: que los servicios que acreditan depósitos por cantidad de confirmaciones pasen a exigir, sin saberlo, una décima parte del trabajo.⁶⁰ Y 1KBCH señaló que la mejora real para los usuarios depende, en definitiva, de las políticas de confirmación de Binance, OKX y Kraken,⁶¹ que nadie controla desde el protocolo.

Hay también un costo que ningún CHIP contabiliza: el **costo de oportunidad**. El tiempo de desarrolladores, revisores y miembros de la comunidad dedicado a coordinar este cambio no se dedica a otras cosas, incluidas las soluciones específicas de la sección 2.2.

3.5. Mejorar una experiencia empeorando otra

La experiencia de usuario tiene dos caras que el cambio pone en tensión: la **velocidad** con la que el usuario ve confirmada su transacción y la **seguridad** que cree que esa confirmación representa. Para buena parte de la gente, «confirmada en la cadena de bloques» significa «definitiva». Los bloques de un minuto mejoran la primera cara a costa de la segunda.

Conviene preguntarse, además, de quién es la experiencia que mejora. El beneficio más visible es para quien usa *exchanges* y servicios que exigen confirmaciones: un usuario que, en la visión de muchos de quienes construimos Bitcoin Cash, no es el usuario para el que se diseñó la red ni para el que se hicieron las últimas actualizaciones. Y la experiencia que puede empeorar es la de un comerciante.

Con bloques de un minuto, una confirmación representa alrededor de una décima parte del trabajo de prueba que representa hoy, algo que el propio CHIP reconoce.⁶² Joemar Taganna (Paytaca) lo planteó así: una primera confirmación de un minuto es más rápida, pero no equivale a la de diez minutos, y acumular el mismo trabajo sigue llevando el mismo tiempo.⁶³ A eso se suman los bloques huérfanos: con la tasa que estima el CHIP (0,41–1,94 %) y 1440 bloques por día, serían de seis a veintiocho bloques huérfanos diarios.

Cuando un bloque queda huérfano, sus transacciones vuelven a la *mempool* y casi siempre entran en el bloque siguiente. Pero:

- un comerciante que espera una confirmación puede ver que su pago pasa de «confirmado» a «sin confirmar» y vuelve a confirmarse un minuto después, lo que es, como mínimo, desconcertante;
- revertir un pago con una confirmación le cuesta a un atacante alrededor de diez veces menos que hoy, de modo que «una confirmación» deja de significar lo que significaba, sin que el comerciante lo sepa.

El costo cae sobre quien tomó la primera confirmación como sinónimo de seguridad, que es justamente la expectativa que la red le enseñó a tener. Aunque cada uno de estos episodios sea temporal, se mejora la experiencia de un usuario que no es el prioritario a costa de la confianza de uno que sí lo es.

⁵⁹Cashrider, [post n.º 172](#), 11 de agosto de 2026: «A program that continues running while its assumptions about confirmations, block height, elapsed time or security have silently changed may be much harder to notice.»

⁶⁰CHIP-2025-03 (versión del 24 de octubre de 2026), sección «[Silent Assumptions](#)»: el riesgo es que el acreditado por confirmaciones pase a valer, sin aviso, «1/10th the chainwork» (frase del «[Reader's Guide](#)»).

⁶¹1KBCH, [post n.º 51](#), 23 de septiembre de 2026: «Real UX Gain also base on Binance/OKX/Kraken conf-count Policy».

⁶²CHIP-2025-03 (versión del 24 de octubre de 2026), sección «[Security Analysis](#)»: análisis de la seguridad por confirmación; el CHIP admite que cada confirmación pasa a representar «1/10th the chainwork».

⁶³joemar_taganna (Joemar Taganna, Paytaca), [post n.º 49](#), 23 de septiembre de 2026: «A 1-minute first confirmation is faster, but it is not equivalent to today's 10-minute first confirmation.»

4. Principios

4.1. Agregar funcionalidades no es lo mismo que cambiar una constante

Bitcoin Cash cambió mucho desde 2017: firmas Schnorr, introspección nativa, CashTokens, contratos más expresivos. Pero esas actualizaciones **agregaron** capacidades sin alterar las constantes que definen el funcionamiento base de la red. El aumento del tamaño máximo de bloque podría parecer una excepción, pero no lo es: el límite de 1 MB no estaba en la versión original de Bitcoin, sino que Satoshi lo agregó en 2010 como una medida provisoria contra el *spam*, no como un parámetro de diseño.

El CHIP responde que BCH ya reemplazó tres veces su «latido», el algoritmo de ajuste de dificultad, y que lo que dañó a la red en el pasado fue la mala ejecución, no el cambio en sí.⁶⁴ Pero esos reemplazos cambiaron el **mecanismo** que mantiene el intervalo de diez minutos, no el intervalo. Mejoraron la forma de sostener la constante; no la redefinieron.

El intervalo de diez minutos, en cambio, está en el corazón del diseño original. Determina la emisión, el ajuste de dificultad, la seguridad por confirmación y toda la documentación, la literatura y el *software* acumulados durante más de quince años de Bitcoin. Modificarlo no es una actualización más: es cambiar uno de los puntos de coordinación sobre los que se construyó todo lo demás.

4.2. Quién decide, y qué parámetros conviene fijar

Hoy, con poca actividad en la red, las decisiones técnicas las toman en la práctica los desarrolladores. Si algún día la actividad alcanza para que los mineros vivan solo de las comisiones, es probable que sean ellos quienes tomen sus propias decisiones, por su cuenta o contratando desarrolladores para optimizar sus nodos. Por eso conviene ser cuidadoso con los parámetros que hoy fija un grupo de desarrolladores y que mañana va a heredar toda la red.

No todos los parámetros pesan igual en ese sentido. El tamaño de bloque es, en el fondo, algo que los incentivos de cada minero pueden equilibrar: cuántas transacciones procesar, cuánto se gana en comisiones y cuánto se arriesga de quedar huérfano. Por eso un límite como el de ABLA, activado en 2024, puede relajarse más adelante sin invalidar nada de lo que se construyó encima.

El intervalo entre bloques es otro tipo de decisión. No puede surgir de lo que decida cada minero: es necesariamente un parámetro de coordinación. Y no es fácil de revertir: una vez activados los *ticks*, los cambios en las API y el *software* adaptado, volver atrás sería tan costoso como el cambio original. Además, **el modelo de incentivos de la red no cambia en lo fundamental con el intervalo entre bloques**. Si el cambio no mejora los incentivos y solo cambia la experiencia de uso en un subconjunto de casos, el costo de tocar un parámetro de coordinación pesa más.

4.3. 0-conf: la respuesta que dimos durante años

Durante años, cada vez que alguien nos objetaba que Bitcoin no es instantáneo porque hay que esperar diez minutos, quienes defendíamos Bitcoin Cash respondíamos siempre lo mismo: 0-conf. Las transacciones son prácticamente instantáneas porque se propagan en segundos y porque el incentivo de los mineros es incluirlas en el próximo bloque. Bitcoin Cash construyó buena parte de su identidad sobre esa respuesta.

⁶⁴CHIP-2025-03 (versión del 24 de octubre de 2026), sección «[Bitcoin Cash Image Risks](#)»: «BCH has already replaced its “heartbeat” (the DAA) three times; what hurt in the past was poor execution, not change itself.»

El CHIP sostiene que 0-conf y las confirmaciones son complementarios: cubren casos de riesgo distintos, y con bloques más rápidos la ventana de vulnerabilidad de 0-conf se cierra antes.⁶⁵ Sobre el papel, quizás. Quien no sigue el foro no va a leer los matices: va a ver que la red que durante una década respondió «no hace falta esperar diez minutos» cambió su protocolo para no esperar diez minutos. Para un recién llegado, un periodista o un crítico, eso no se lee como una distinción entre casos de riesgo, sino como una admisión de que la respuesta no alcanzaba. Y esa lectura le cuesta credibilidad a 0-conf justo en los casos en los que sí funciona, que son los que más usamos.

Bigplayermaster planteó una idea cercana en el hilo de declaraciones: que hay que distinguir entre la velocidad y la percepción de velocidad, y que el dinero necesita reglas claras, predecibles y estables, porque huye de los activos cuyas reglas parecen cambiar.⁶⁶

0-conf

0-conf es una consecuencia práctica de las reglas del protocolo y de ciertas suposiciones sobre seguridad e inclusión en el próximo bloque. No es una garantía explícita de consenso.

4.4. Identidad

Hay una parte del debate que no es técnica, y el propio CHIP lo reconoce: la preocupación de que Bitcoin Cash «pierda su alma», como dijo kanat, o de que el cambio debilite su reclamo de legitimidad como continuidad de Bitcoin, como planteó BitcoinCashPodcast.^{67,68} Tom Zander, por su parte, describió la propuesta desde el principio como «una solución que busca un problema». ⁶⁹ El autor del CHIP respondió con ironía —el 20 % de los bloques ya dura dos minutos o menos: ¿son «bloques sin alma»?—, ⁷⁰ pero la objeción no era sobre bloques individuales, sino sobre la regla. En el hilo de declaraciones, rnbrady, kanat y Zander desaprobaron el cambio con la misma idea: «si no está roto, no lo arregles». ^{71,72,73} Una objeción social persistente es, en sí misma, un costo de coordinación.

5. Una observación secundaria: la adopción de comercios

En la experiencia de quienes trabajamos en la adopción directa de Bitcoin Cash con comerciantes, en Argentina y en otros lugares, el tiempo entre bloques nunca fue un obstáculo real cuando la comunicación pone el énfasis en los beneficios de la tecnología. Entre usuarios, las transacciones se aceptan de inmediato, y herramientas con soporte de 0-conf, como prompt.cash, ⁷⁴ se usan sin problemas para ventas en línea.

Donde 0-conf funciona, la espera de diez minutos no es el obstáculo.

⁶⁵CHIP-2025-03 (versión del 24 de octubre de 2026), sección «Zero-confirmation Transactions»: «They are not alternatives; they are complementary.»

⁶⁶Bigplayermaster, [post n.º 55](#), 24 de septiembre de 2026: «we need to distinguish between two things: speed and the perception of speed»; «money requires clear, predictable, and stable rules».

⁶⁷kanat, [post n.º 14](#), 7 de marzo de 2025: «If BCH goes to 2-minute blocks, it might win some short-term attention but lose its “soul” in the process.»

⁶⁸BitcoinCashPodcast, [post n.º 3](#), 2 de marzo de 2025: «a high risk endeavour that could seriously impact the legitimacy claim of BCH to “the real Bitcoin” legacy».

⁶⁹tom, [post n.º 6](#), 3 de marzo de 2025: «It is obviously written from the point of view of a solution searching for a problem.»

⁷⁰bitcoincashautist, [post n.º 15](#), 7 de marzo de 2025: «20% of BCH blocks had durations shorter or equal than 2 minutes, are they soulless blocks?»

⁷¹rnbrady, [post n.º 12](#), 15 de septiembre de 2026: «Disapprove. If it aint broke, don't fix it.»

⁷²tom, [post n.º 20](#), 16 de septiembre de 2026: «Disapprove. In balance doesn't seem to be a good idea.»

⁷³kanat, [post n.º 36](#), 20 de septiembre de 2026: «Disapprove. If it aint broke, don't fix it.»

⁷⁴[prompt.cash](#).

6. Lo que se puede hacer sin cambiar el intervalo

Si se miran uno por uno los problemas que el CHIP dice resolver, el cambio es menos favorable de lo que parece. En casi todos, el CHIP mitiga sin eliminar, y en la mayoría hay caminos que no requieren tocar una constante fundacional.

Problema	Qué hace el CHIP	Alternativa
Primera confirmación lenta y variable (<i>swaps</i> , pasarelas, billeteras multimonedas)	La acelera	DSPProofs con evaluación de riesgo y políticas escalonadas según el monto, que ya usan Bitgree y Thorswap ⁷⁵
Confirmaciones múltiples en <i>exchanges</i>	Da previsibilidad, no velocidad	Exigir confirmaciones según el valor y el riesgo, no un número fijo
Contención de UTXO en DeFi	Acorta la espera; la colisión sigue	Ordenar las solicitudes en la aplicación, repartir la liquidez en varios UTXO, extender los DSPProofs a contratos
Bloques de una hora o más por caídas de <i>hashrate</i>	Los acorta ⁷⁶	Estudiar la reacción del ajuste de dificultad como un problema propio
Granularidad del <i>locktime</i>	La mejora	El <i>locktime</i> por tiempo ya existe ⁷⁷
Primera impresión de los usuarios nuevos	Indirectamente	Billeteras que muestren los pagos con 0-conf como recibidos; comunicación

La otra objeción previsible es que estas alternativas dependen de terceros que, en casi una década, no adoptaron 0-conf. Pero el CHIP depende de lo mismo: si un *exchange* no actualiza su configuración, sus 15 confirmaciones pasan a valer una décima parte del trabajo, lo que el propio CHIP llama «supuestos silenciosos».⁷⁸ La diferencia está en qué se les pide. Con el CHIP, adaptarse a un protocolo nuevo; si no lo hacen, quedan menos seguros sin saberlo. Con las alternativas, adoptar herramientas que ya existen; si no lo hacen, nada empeora.

Las caídas de *hashrate* son el caso en el que los bloques de un minuto ayudan de verdad. Pero son el síntoma de otra cosa: la red tiene una porción mínima del *hash* total y depende de mineros que entran y salen. Ese problema merece un análisis propio, no una solución lateral que cambia todo lo demás.

7. El pedido: no en 2027

Mi pedido es concreto: que el CHIP-2025-03 no haga *lock-in* el 15 de noviembre de 2026, y que se vuelva a discutir para una actualización futura, una vez agotadas las alternativas. No es un «nunca»: hoy la carga de la prueba no está cumplida. Para activar un cambio de este tipo, tendría

⁷⁵bitcoincashautist, [post n.º 157](#), 29 de mayo de 2026: «Bitgree uses DSPs, but DSP-score-0 or DSP-fired transactions fall back to 1-conf»; Thorswap aplica niveles mínimos de confirmación según el monto.

⁷⁶CHIP-2025-03 (versión del 24 de octubre de 2026), «[Reader's Guide](#)»: «Hashrate drops degrade gracefully: 10% of normal hashrate yields ~10-minute blocks instead of ~100-minute ones.» Desarrollo en «[Improved Difficulty Adjustment Stability](#)».

⁷⁷cculianu (Calin Cuiianu), [post n.º 230](#), 11 de octubre de 2026: «If some contract was using height as a proxy for real world time, when there already is a TIME mode, that's on the contract.»

⁷⁸CHIP-2025-03 (versión del 24 de octubre de 2026), sección «[Silent Assumptions](#)»: los servicios que acreditan por cantidad de confirmaciones pasan a exigir una décima parte del trabajo: «a policy change, not a bug».

que demostrarse que **los beneficios superan con claridad la suma de los costos**: los de implementar, coordinar y mantener el cambio, y el costo de oportunidad de no dedicar ese esfuerzo a otra cosa. Como mínimo, antes de cualquier activación debería:

1. **Cuantificar los costos de activación** con estimaciones de los equipos que van a cargar con ellos (nodos, *pools*, *exchanges*, billeteras, indexadores y aplicaciones DeFi), y definir criterios de preparación que detecten el *software* de terceros que puede romperse en silencio.
2. **Desplegar primero las mitigaciones para SPV** —filtros compactos, sincronización por lotes, CHIP-2026-02— y verificar que funcionan con billeteras reales, no solo en teoría.
3. **Evaluar soluciones específicas** para cada problema invocado (contención en DeFi, previsibilidad para servicios que exigen confirmaciones), y mostrar por qué no alcanzan antes de recurrir a modificar una constante fundacional.
4. **Contar con una implementación completa y probada** en chipnet con tiempo suficiente, y con datos reales de tasa de huérfanos, no solo modelos.
5. **Lograr un apoyo amplio**, que no se limite a la ausencia de objeciones técnicas entre quienes participan del foro.

No es una postura aislada. Varios participantes del hilo de declaraciones condicionan su apoyo de la misma manera: SW9 apoya el CHIP en lo conceptual, pero no cree necesario forzarlo para el próximo ciclo si la implementación no está lista;⁷⁹ Fernando Pelliccioni (Knuth) aprueba los bloques de un minuto, pero se declara neutral respecto del *lock-in* de noviembre;⁸⁰ 2qx aprueba «si la implementación está lista a tiempo»;⁸¹ y albaDsl condiciona su voto a que Culianu dé por buena la implementación.⁸² ShadowOfHarbringer propuso incluso separar los *ticks* del cambio de intervalo: introducir primero la abstracción y decidir el tiempo de bloque más adelante.⁸³

Hoy esas condiciones no se cumplen. Postergar un ciclo tiene un costo de oportunidad acotado y recuperable; activar sin cumplirlas, un costo permanente.

8. Conclusión

La propuesta de bloques de un minuto parte de problemas reales y está técnicamente bien trabajada: modela la tasa de huérfanos, preserva los contratos existentes y reconoce sus costos. Pero no elimina los problemas que invoca: para los *exchanges*, ofrece previsibilidad y no velocidad; para DeFi, acorta la espera de un error que sigue ocurriendo; para los servicios centralizados que exigen confirmaciones, acomoda una dependencia de la que la red está intentando salir. A cambio, modifica una constante fundacional de Bitcoin, agrega una abstracción permanente al protocolo, traslada a los clientes SPV un costo cuyas mitigaciones todavía no están desplegadas, vacía de significado la primera confirmación para el comerciante que confiaba en ella y debilita, al menos en la percepción de quienes miran desde afuera, la respuesta —0-conf— que la comunidad dio durante una década.

La alternativa es más lenta y menos vistosa: resolver cada problema en la capa donde se genera, y trabajar la comunicación y el diseño de billeteras donde el problema es de expectativa. Pero ataca las causas y no los síntomas.

⁷⁹SW9, [post n.º 28](#), 18 de septiembre de 2026: «*I don't think it is necessary to push it for the next upgrade cycle if the implementation is not ready*».

⁸⁰fpelliccioni, [post n.º 89](#), 28 de septiembre de 2026: «*Approve (one-minute blocks); Neutral (November 2026 lock-in)*».

⁸¹2qx, [post n.º 22](#), 16 de septiembre de 2026: «*Approve of the concept, if implementation is ready in time*».

⁸²albaDsl, [post n.º 105](#), 5 de octubre de 2026: cambiaría su postura si Culianu da por buenos la implementación, las pruebas y la elección del parámetro.

⁸³ShadowOfHarbringer, [post n.º 6](#), 15 de septiembre de 2026: «*Would it be possible to separate the tick mechanism from the change to blocktime and make it two separate changes?*»

Una constante fundacional no debería cambiarse con apuro. Quien comparta estas preocupaciones puede decirlo en el hilo de declaraciones antes del 15 de noviembre.⁸⁴ Postergar la propuesta no la mata: le da el tiempo que necesita para hacerse bien.

Por eso mi respuesta es: todavía no, y no en 2027.

⁸⁴Para publicar una postura: «CHIP-2025-03 Faster Blocks: gathering statements of support (and dissent)», en Bitcoin Cash Research.