Un curso de Bitcoin gratuito y de código abierto desarrollado por Area Bitcoin

---

Índice - Bitcoin 4 All -
Dentro de Bitcoin: Cómo funciona Bitcoin?
(descentralización, blockchain y teoría de juegos)

---

6. Bitcoin no tiene competidores reales

6.1 Criptomonedas como empresas: marketing, líderes y centralización
6.2 Bitcoin es horizontal y colaborativo
6.3 Incentivos individuales que refuerzan el conjunto
6.4 Resiliencia frente a censura y ataques

---

7. Forks: versiones y conflictos

7.1 Qué es un fork
7.2 Soft forks: actualizaciones compatibles
7.3 Hard forks: divisiones irreconciliables

---

8. Seguridad y teoría de juegos

8.1 Incentivos para colaborar, no sabotear
8.2 Código abierto y transparencia
8.3 Ataques son caros e inútiles en la práctica

---

9. El problema de los generales bizantinos

9.1 Coordinación en sistemas descentralizados
9.2 Cómo Bitcoin resuelve este problema con prueba de trabajo, P2P y blockchain

---

10. Blockchain y prueba de trabajo

10.1 Mecanismo de consenso: input → output
10.2 Timechain: bloques cada ~10 minutos
10.3 Hashes: como costuras digitales que encadenan los bloques
10.4 Verificación distribuida y detección instantánea de alteraciones

---

11. Blockchain no es la innovación aislada

11.1 Sin descentralización, blockchain no sirve
11.2 Es sólo una base de datos lenta si no tiene consenso fuerte
11.3 Bitcoin no es solo blockchain — es sistema + incentivos + código abierto

Bitcoin 4 All - Texto completo

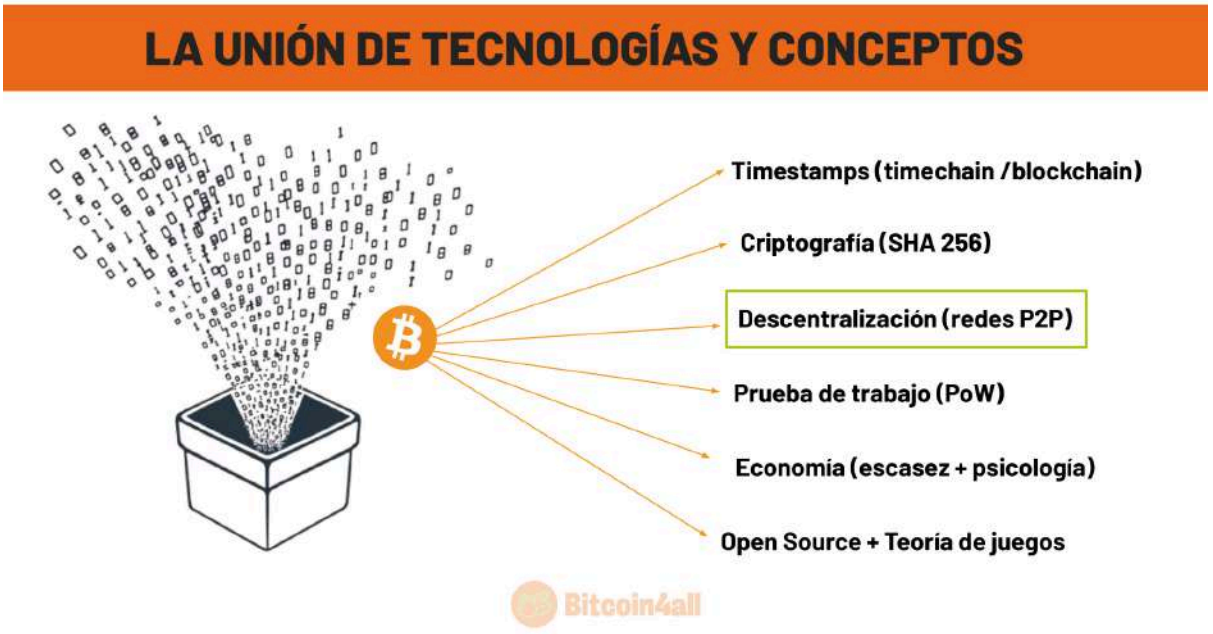
Bitcoin 4 All es un curso gratuito y de código abierto creado por Area Bitcoin. El objetivo es ayudar a más personas a comprender Bitcoin e inspirar a cualquier persona a convertirse en un multiplicador de la educación sobre Bitcoin.

Acerca de este libro electrónico

Publicado por Area Bitcoin – 2025

Dentro de Bitcoin: Cómo funciona Bitcoin?
(descentralización, blockchain y teoría de juegos)

En esta lección te sumergirás en el funcionamiento de Bitcoin, aprendiendo sus características, cómo funciona la blockchain, la minería, los halvings y conceptos técnicos fundamentales. No te preocupes si no lo entiendes todo a la primera. Es normal que necesites repasar y volver a ver varias veces para consolidar tu aprendizaje. Con el tiempo, los conceptos encajarán y tendrán cada vez más sentido.



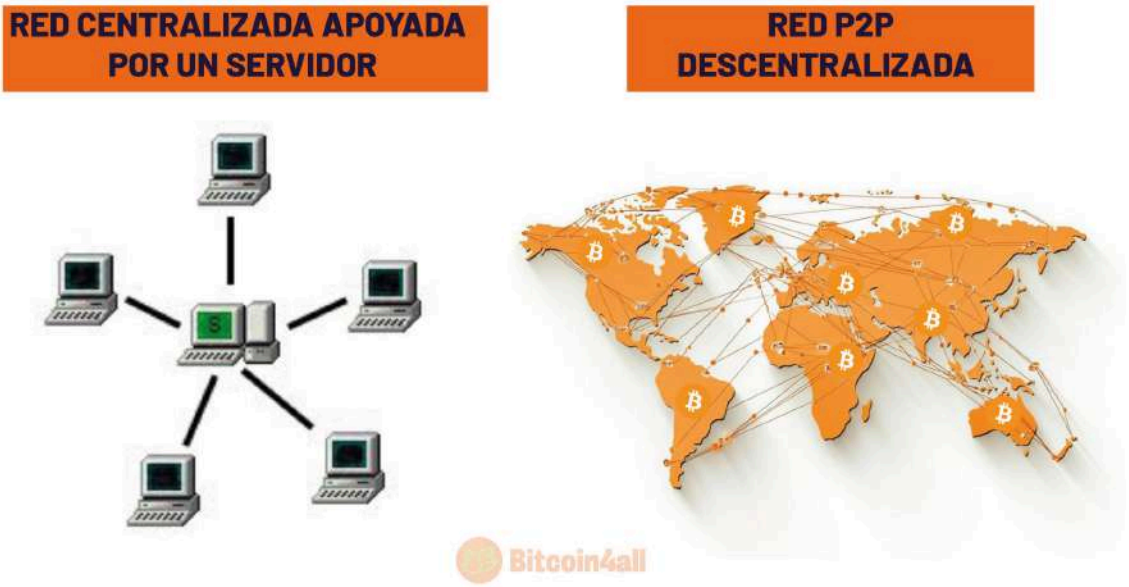
(Slide 88) - Bitcoin 4 All

Como has visto en la lección 1, Bitcoin es la combinación de varias tecnologías y conceptos. La descentralización es lo que separa a Bitcoin de cualquier otro invento de la historia reciente.

(Slide 89) - Bitcoin 4 All

Y lo que está ocurriendo en las últimas décadas es la acción de dos fuerzas tecnológicas que actúan al mismo tiempo: la descentralización y la desmaterialización de las cosas. La desmaterialización comenzó en la década de 1990 con las computadoras y los teléfonos inteligentes, que condensaron y desmaterializaron diversos dispositivos que antes sólo conocíamos en forma física. Radio, agenda, televisión, cámara fotográfica, calculadora, fax: todo eso se ha desmaterializado y digitalizado en la palma de tu mano, en tu teléfono móvil, en sólo 20 años. Se convirtió en todo en uno.

Bitcoin continúa ese cambio evolutivo y tecnológico, aportando ambos efectos a la economía y al dinero. En otras palabras, el Bitcoin descentraliza el acceso al valor para cualquier persona en cualquier parte del mundo sin restricciones de acceso y también desmaterializa el sistema financiero bancario de sucursales, cajas fuertes, cajeros automáticos y cajas fuertes. Y si Internet ya ha descentralizado la información y cambiado el mundo, imagina lo que puede hacer Bitcoin descentralizando el valor y el poder de decisión, así como desmaterializar los bancos centrales, los bancos comerciales y las propiedades del dinero sólido.



(Slide 90) - Bitcoin 4 All

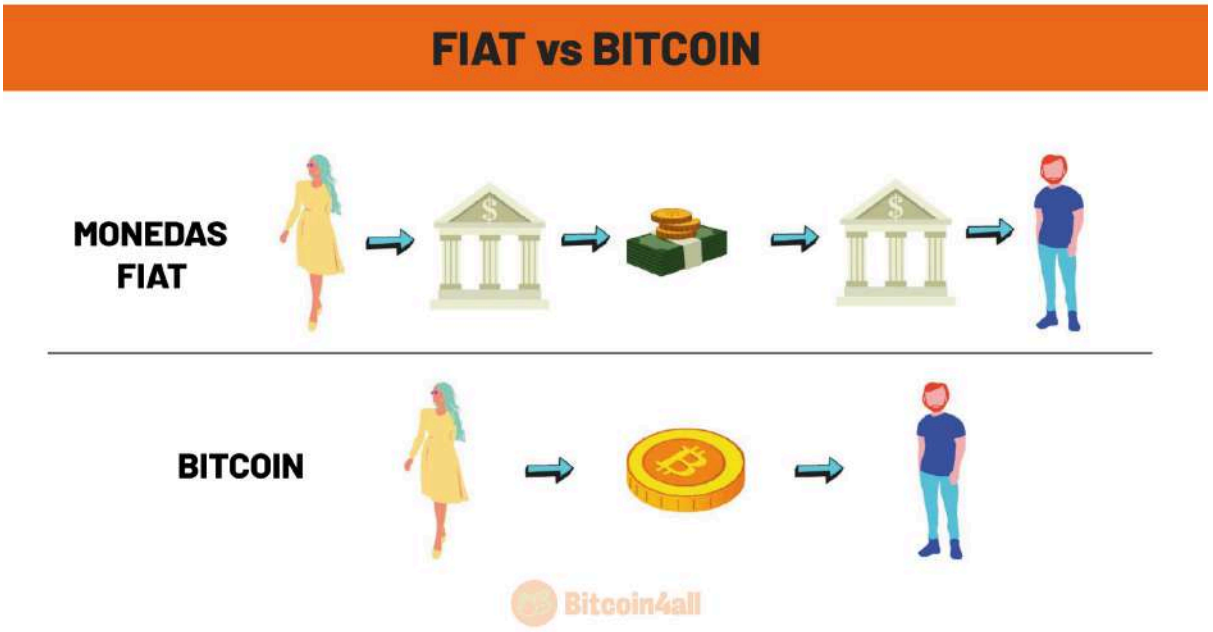
Bitcoin sólo puede hacer esto porque está descentralizado. Sin descentralización, Bitcoin sería solamente una empresa. La descentralización es lo que diferencia a Bitcoin del resto y le proporciona inmutabilidad. Si no hay nadie que tome decisiones por otras personas, significa que es una red difícil de cambiar. Para que se produzca cualquier cambio, casi todos los participantes tienen que estar de acuerdo con ello. Y eso no es nada fácil, ni en Bitcoin ni en ningún sistema que implique a miles de seres humanos tomando decisiones. La descentralización es lo que garantiza la inmutabilidad de las propiedades y que las reglas de Bitcoin sigan el mismo camino. Aporta la confianza de que nadie podría monopolizar o corromper el Bitcoin de forma autoritaria.

Bitcoin está descentralizado porque es una red entre iguales. Está formado por computadoras que se conectan entre sí y siguen unas normas que todos acuerdan. No hay un servidor central que coordine o almacene los datos, como ocurre en las redes centralizadas. También significa que no hay un único punto de fallo. Si alguna computadora conectada a la red se cae, es destruida o atacada, la red sobrevive y sigue funcionando porque hay miles de otras computadoras que cumplen la misma función de forma independiente.

(Slide 91) - Bitcoin 4 All

En la práctica, esto significa que en Bitcoin no hay intermediarios. Todo el mundo puede conectarse a la red sin depender de nadie, sin tener que pedir permiso y sin la posibilidad de que terceros se lo impidan. A diferencia del dinero fiduciario, que está centralizado y dependes de numerosas entidades, como el ministro de economía, el director del banco central, las entidades de pago, la fábrica de moneda, los bancos, etc. para acceder al sistema.

Los bancos centrales determinan las políticas monetarias: no tienes la opción de no seguir las reglas, estás obligado a ello. De ahí la expresión "curso forzoso". Los bancos comerciales, por su parte, facilitan el acceso al sistema. Para participar tienes que pedirles permiso y, si no cumples los requisitos, puede que no tengas cuenta bancaria o incluso que te la cierren, si ya la tenías.



(Slide 92) - Bitcoin 4 All

Otra gran diferencia es a la hora de realizar transacciones.

Actualmente, cuando realizas una transacción digital, tienes que pedir a tu banco que envíe una cantidad al banco de otra persona, y luego el banco de esa persona ingresa la cantidad en la cuenta correspondiente. En una transacción entre dos personas mediante el sistema bancario fiduciario, hay al menos un intermediario – un banco – entre dos personas. Si estas dos personas tienen cuentas en bancos diferentes, habrá dos bancos intermediando en la transacción.

Bitcoin es como hacer una transacción física con billetes de dinero, igual que cuando compras un producto y entregas los billetes directamente a la otra persona. Con Bitcoin envías el valor directamente al monedero de otra persona sin pasar necesariamente por algún tipo de intermediario fiduciario o banco. A menos que lo quieras: si eliges operar a través de casas de cambio, por ejemplo, pero es una opción, no una vía obligatoria. Eso cambia completamente el funcionamiento del sistema financiero, porque hoy en día el sistema fiat depende de estos intermediarios para transferir dinero en línea.

Fue mediante la criptografía, timestamps, las redes P2P y un sólido mecanismo de consenso como Satoshi Nakamoto consiguió digitalizar el sistema financiero en su conjunto, sin necesidad de gobiernos ni bancos.

(Slide 93) - Bitcoin 4 All

La red Bitcoin está formada por el código, los mineros y los nodos. El código es un conjunto de reglas en forma de códigos computacionales y criptográficos que guían a los participantes para coordinarse entre sí. Determina cómo se harán los registros y cómo debe funcionar la red Bitcoin. El código es público y cualquiera puede sugerir modificaciones, auditarlo en busca de errores e incluso copiarlo. Ese código es difícil de modificar y monopolizar. Lo ejecutan miles de participantes y para modificarlo de forma válida es necesario que prácticamente toda la red esté de acuerdo en ejecutar una versión modificada.

Puedes consultar el github de Bitcoin, donde los desarrolladores discuten las actualizaciones y donde también puedes contribuir si quieres. Dejaremos el enlace al Github de Bitcoin aquí debajo de la lección. El código funciona mediante software y el más utilizado es Bitcoin Core, una implementación de la versión original creada por Satoshi Nakamoto.

Los mineros, por su parte, son los participantes que proponen los bloques, insertan las transacciones y defienden la red de los ataques mediante la potencia computacional. Son los primeros en recibir bitcoins de la red con cada bloque minado.

Y el tercer tipo de participante en la red son los nodos. Los nodos son computadoras normales que comprueban que los mineros siguen el consenso determinado por el código. Los nodos son poderosos agentes de descentralización, porque desde ellos cualquiera puede tener una copia de la blockchain de Bitcoin en su propia computadora, decidir qué versión del código ejecutar y formar parte de la red Bitcoin con autonomía para enviar sus propias transacciones sin depender de nadie más. Aunque los mineros se unan para atacar

a Bitcoin, son los nodos los que tienen el poder de impedir que este ataque sea efectivo. Eso ya ocurrió incluso en la llamada guerras de bloques que tuvo lugar en 2016.

(Slide 94) - Bitcoin 4 All

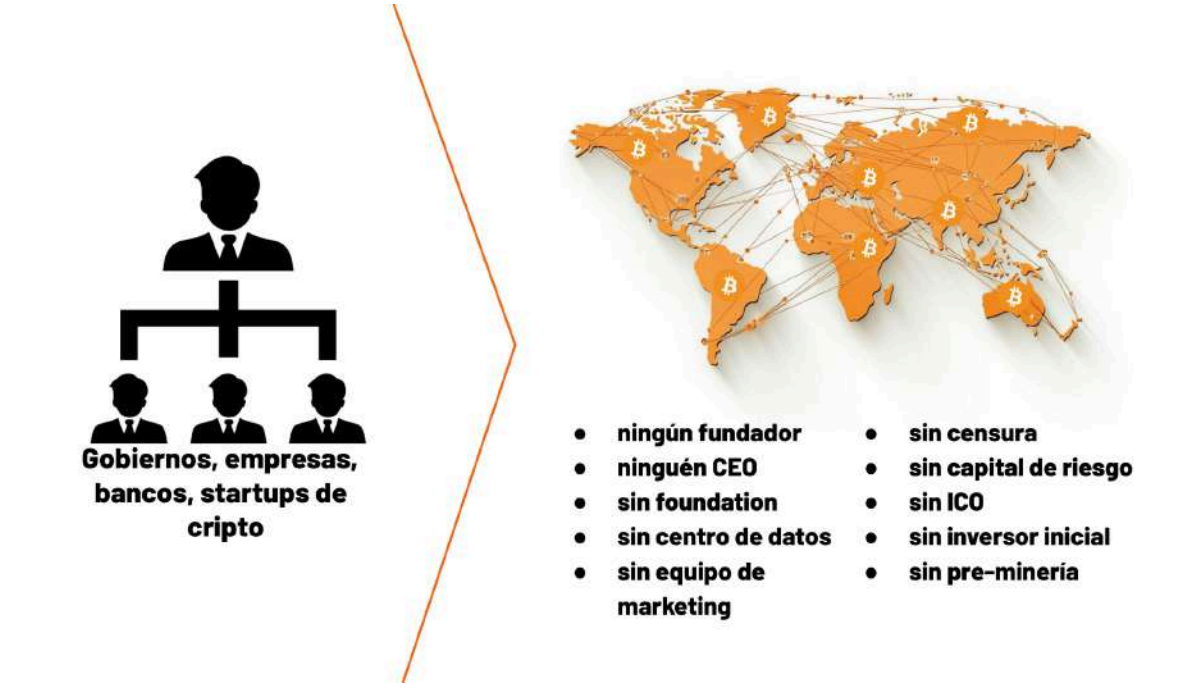
Según el sitio web Bitnodes, hay más de 65.000 nodos de Bitcoin operando en todo el mundo y la mayoría de ellos, el 65%, no tienen una ubicación exacta identificada. Son esos miles de nodos en computadoras normales conectadas entre sí los que hacen de la red Bitcoin el sistema informático más fuerte, resistente y accesible para que cualquier persona de cualquier parte del mundo pueda comprobarlo. Cualquiera puede dirigir un nodo y el coste es bajo, incluso puedes dirigir un nodo en una vieja computadora que tengas en casa.

Los nodos comprueban los registros todo el tiempo. Por eso la contabilidad de la red Bitcoin es bien cerrada, porque los nodos comprueban constantemente que las transacciones están concluidas y que el número de monedas que circulan es correcto. Es un sistema distribuido de registros, donde las cuentas siempre coinciden, y eso también es algo poderoso y único.

T

(Slide 95) - Bitcoin 4 All

Los bancos centrales no te permiten mirar sus cuentas internas ni dar tu opinión directamente en las reuniones. La contabilidad de los bancos centrales es privada y se lleva a cabo a puerta cerrada. La población depende de los datos proporcionados por el Banco Central y no puede verificar de forma independiente ni opinar directamente sobre las políticas monetarias. ¡El pueblo ni siquiera elige quién presidirá el Banco Central! En Bitcoin, cualquiera puede auditar la red y sugerir mejoras, ya que es de libre acceso.



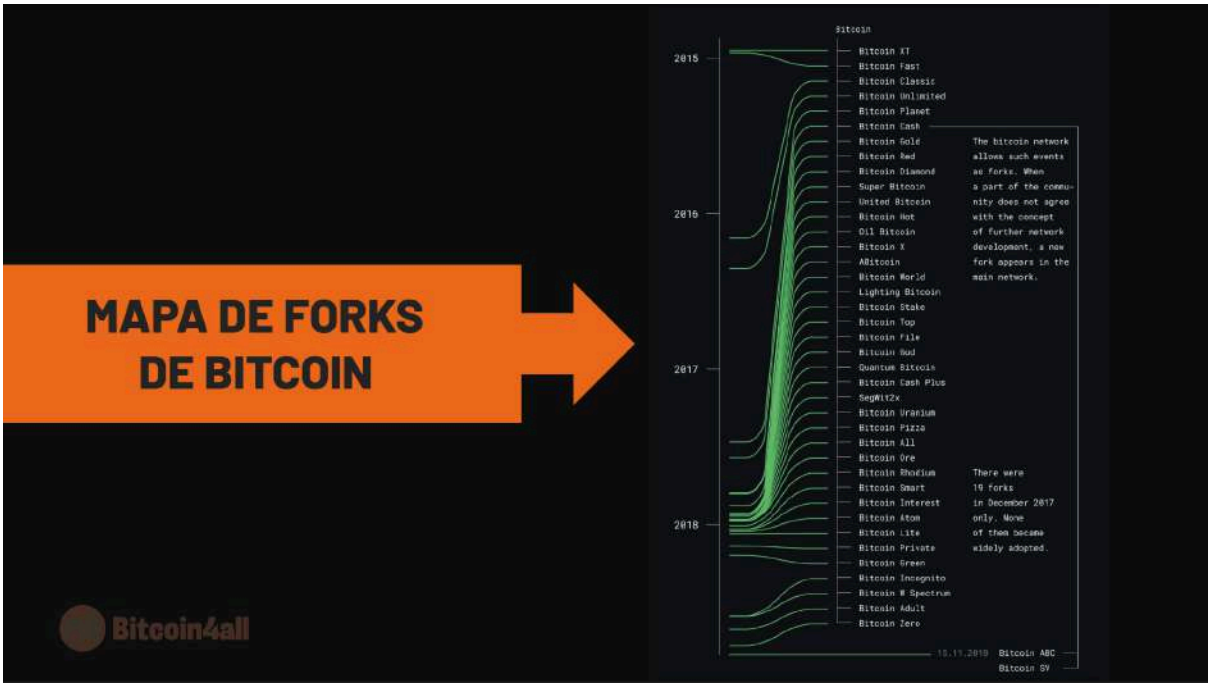
(Slide 96) - Bitcoin 4 All

Las estructuras centralizadas son siempre jerárquicas, como una empresa: hay un director general, alguien que toma decisiones sobre los próximos pasos, un equipo de marketing, un equipo de desarrollo de investigación, y todas trabajan a través de esta jerarquía de poder. Las empresas compiten entre sí para ganar el mercado. Las criptomonedas son como empresas y compiten entre sí por la cuota de mercado vendiendo utilidad, igual que hacen las empresas.

Bitcoin, en cambio, es horizontal, es colaborativo, simplemente existe y permite que cualquiera disfrute y participe en la red. No hay nadie que determine hacia dónde va el protocolo y cuál será la próxima actualización. Es el colectivo de usuarios, nodos y mineros el que define qué versiones del protocolo se ejecutarán sin que ni siquiera ellos se pongan de acuerdo entre sí. Por eso Bitcoin no tiene competidor, nada funciona como él. Bitcoin adopta el pensamiento adversario y utiliza estos incentivos individuales para fortalecer el conjunto.

Por eso Bitcoin es tan resistente. No puedes censurar o impedir que la gente acceda a ella, aunque no estén de acuerdo – a diferencia de los bancos, que cierran las cuentas de los usuarios continuamente y cambian las normas constantemente.

Muchos protocolos incluso afirman ser descentralizados, pero cuando los analizas en profundidad son todo lo contrario: son como empresas. Tienen líderes, concentran el poder de decisión, son fácilmente censurables y no sobrevivirían a los ataques de hackers ni a la censura gubernamental. Bitcoin, por otra parte, ha sufrido constantes ataques y lleva más de 10 años funcionando sin parar debido a su estructura resistente y descentralizada.

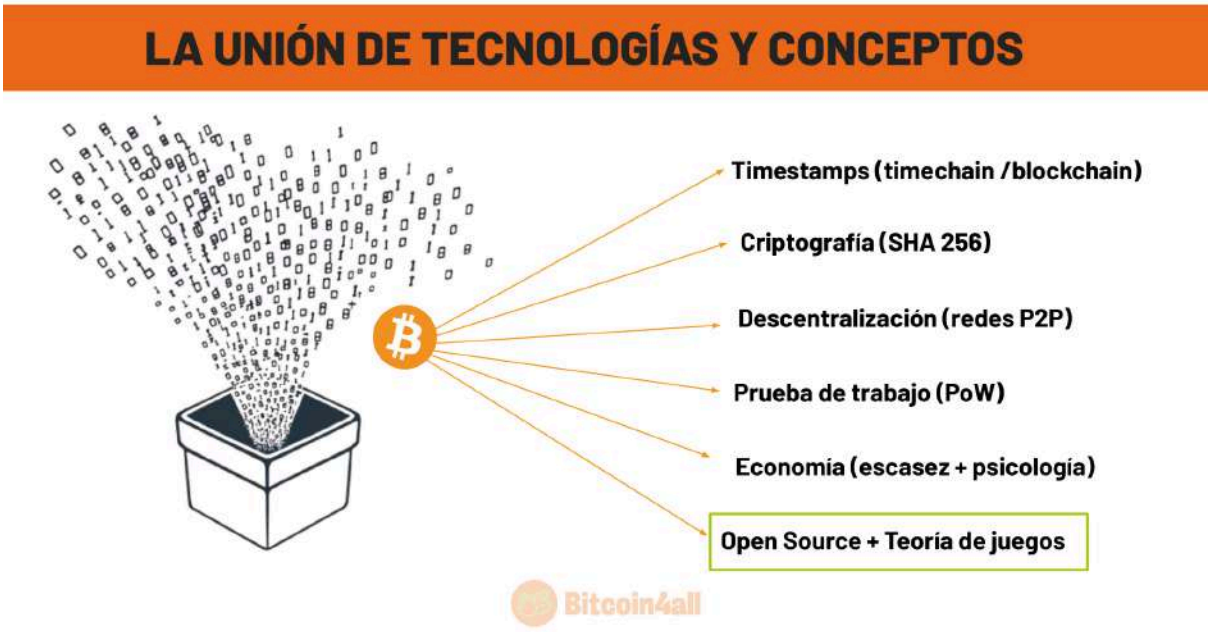


(Slide 97) - Bitcoin 4 All

Aunque ha habido cientos de copias, ninguna de ellas ha conseguido superar a Bitcoin, ni siquiera ninguna otra criptomoneda que haya surgido después. Esa imagen muestra los forks, es decir, las copias que ya se han hecho de Bitcoin de 2015 a 2018. Muchos de los forks se autodenominan "el verdadero Bitcoin" y han intentado robarle narrativa, visibilidad y liquidez, pero ninguno lo ha conseguido realmente. Ningún proyecto puede robar las propiedades y el efecto de red que tiene Bitcoin. Cualquier nivel de centralización es ya un punto de mutabilidad, un monopolio del poder de decisión y también un punto potencial de fallo que pueden explotar los atacantes.

(Slide 98) - Bitcoin 4 All

Satoshi sabía desde el principio que la descentralización era la clave de Bitcoin y una de las principales razones del fracaso de anteriores proyectos de dinero digital. Incluso lo escribió en 2009: "Mucha gente descarta automáticamente las monedas digitales porque muchas empresas han fracasado desde los años 90. Espero que sea obvio que fue la naturaleza centralizada que controlaba estos sistemas lo que causó este fallo".



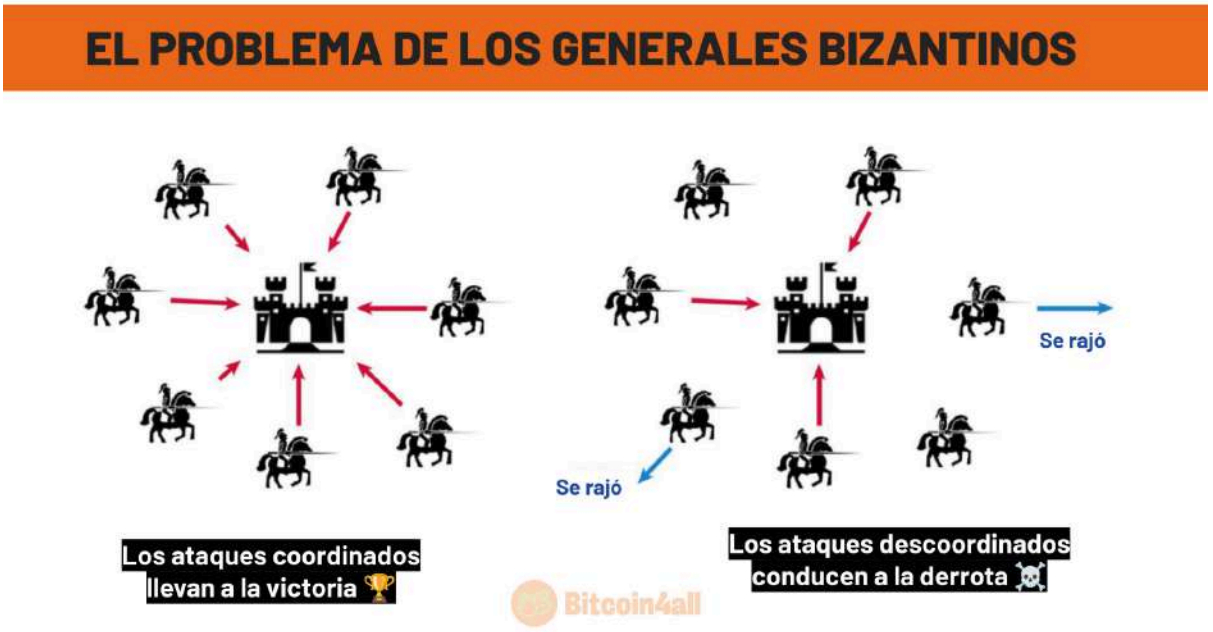
(Slide 99) - Bitcoin 4 All

La descentralización de Bitcoin es el resultado de una combinación única de factores que trabajan juntos para proteger la red. Para comprometer el sistema sería necesario un ataque que requiriera una coordinación extrema, enormes recursos financieros y una cantidad colosal de energía. Esa barrera casi infranqueable se sustenta en la aplicación práctica de la teoría de juegos, que anima a los participantes a colaborar entre sí para fortalecer la red en lugar de intentar piratearse o engañarse mutuamente.

En la teoría de juegos para Bitcoin, la colaboración siempre es más rentable que el sabotaje. Los mineros, los validadores y otros participantes tienen incentivos financieros y estructurales para actuar a favor de la red, ya que cualquier intento de atacarla sería extremadamente caro y, en la mayoría de los casos, inútil.

Además, para que esa colaboración sea posible y fiable, Bitcoin opera con total transparencia. Su código es open source, es decir, abierto y accesible a todos, lo que permite una auditoría continua y garantiza que no se cambien las reglas sin el consenso de la red. Esa alineación entre descentralización, incentivos económicos y transparencia es lo que hace de Bitcoin la red monetaria más sólida y segura jamás creada.

Satoshi incluso consiguió unir los puntos resolviendo uno de los problemas más antiguos: el problema de los generales bizantinos.



(Slide 100) - Bitcoin 4 All

Esa analogía intenta responder, a través de una situación de guerra, a cómo los sistemas informáticos podrían comunicarse de forma descentralizada. Hasta que apareció Bitcoin, no había respuesta a ese problema.

¿Has visto Juego de Tronos? Si sí, imagina ahora una escena de invasión de una ciudad como la de la serie. Esta ciudad se llama Bizancio y varios generales quieren atacarla. Han rodeado la ciudad y deben decidir juntos cuándo atacar. Si todos atacan al mismo tiempo, ganan la batalla porque ha habido coordinación. Si atacan en momentos diferentes, pierden porque están descoordinados y son susceptibles de ser atacados.

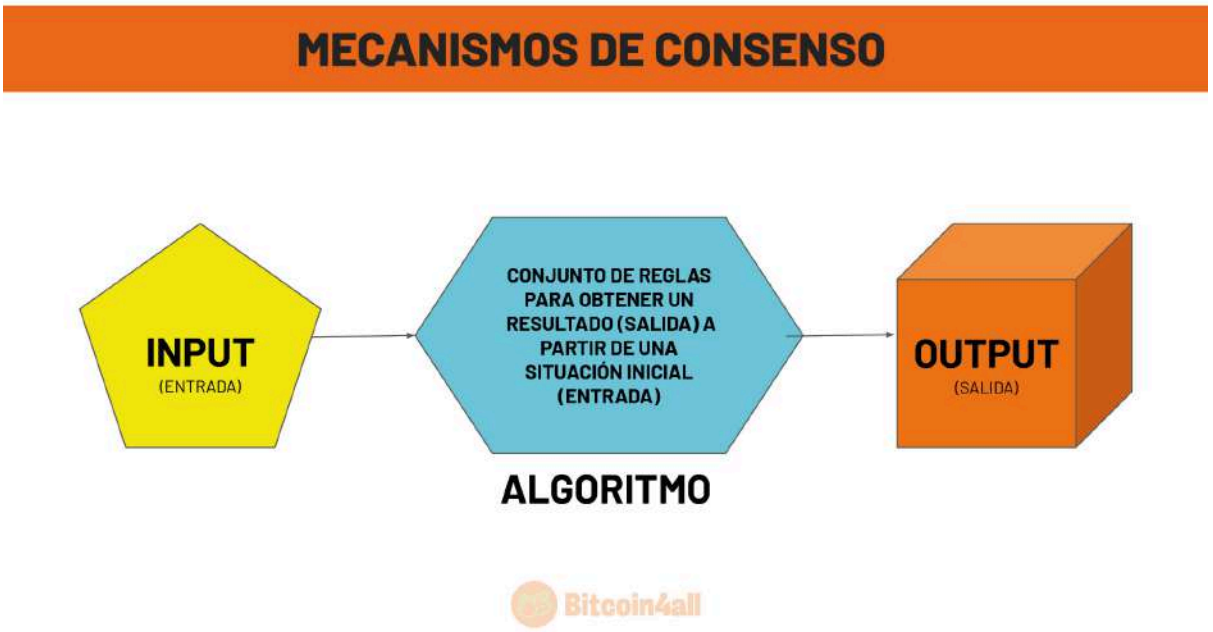
Los generales no tienen canales de comunicación seguros entre sí para crear esa acción coordinada. En primer lugar, porque están en distintas posiciones alrededor de la ciudad; en segundo lugar, porque no pueden estar seguros de que el mensaje llegue, las posibilidades de que un mensajero sea interceptado por el enemigo son muy altas.

Así que tienen que encontrar una forma de comunicarse, de ponerse de acuerdo sobre el momento adecuado para atacar. El primer general puede empezar enviando un mensaje de ataque a las 9 de la mañana, pero no tiene forma de saber si el mensajero ha entregado el mensaje o no. Esta incertidumbre podría llevar al primer general a renunciar a atacar. Dilemas como éste provocaron muchos fracasos en las monedas digitales que precedieron a Bitcoin.

Bitcoin ha conseguido resolver el problema de los generales bizantinos mediante: una coordinación completa a través de la prueba de trabajo, que establece un conjunto de reglas

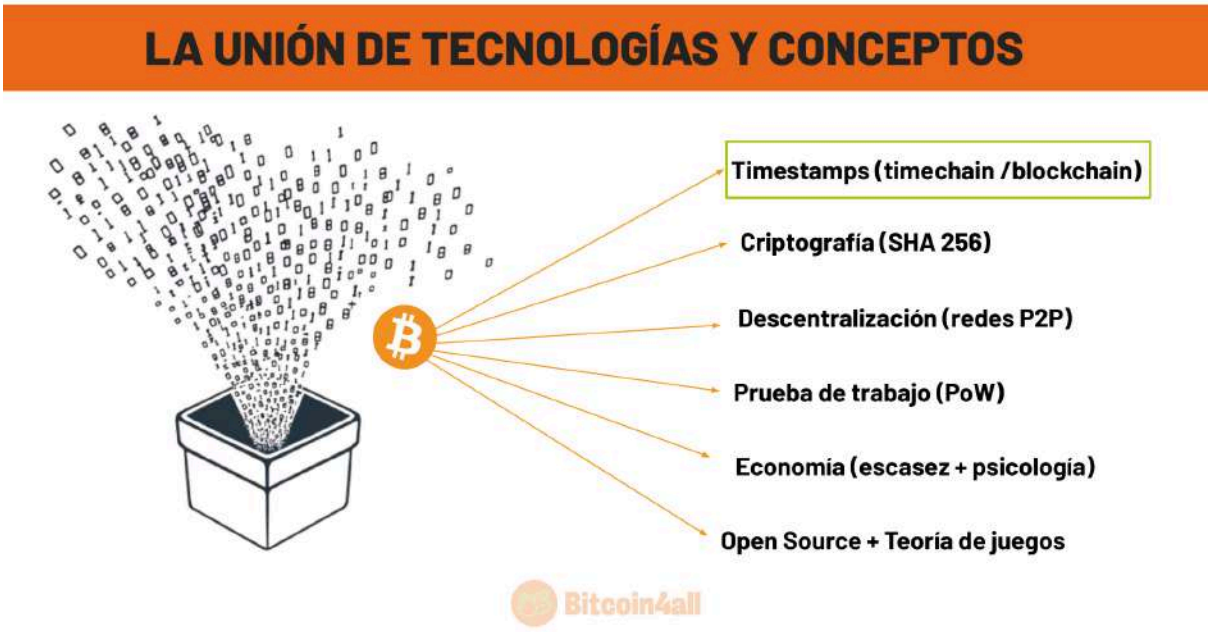
de procesamiento de red que coordina a todos; redes P2P que conectan a todos los participantes al mismo sistema; y a través de blockchain, un sistema de registros criptográficos encadenados que todos pueden verificar sin depender de ningún "mensajero" externo al sistema.

Mediante ese sistema, todos los generales podrían coordinarse en el momento adecuado para atacar Bizancio sin depender de terceros, de forma sincronizada, segura y sin que nadie dudara en atacar.



(Slide 101) - Bitcoin 4 All

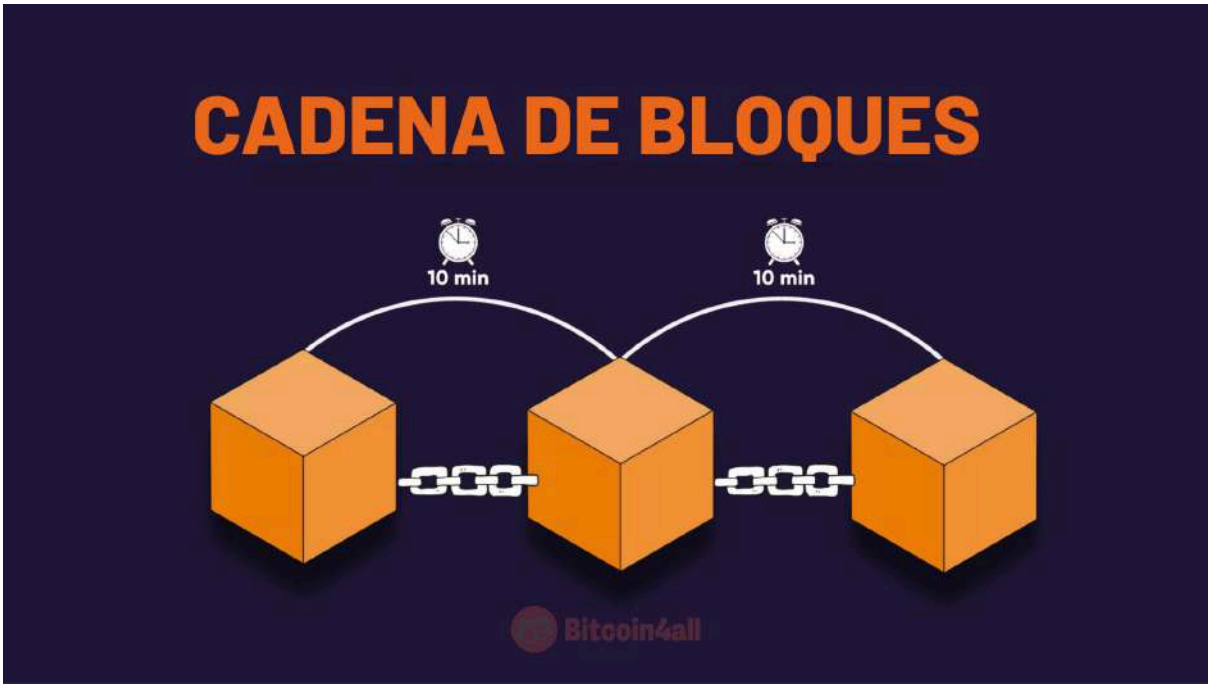
Acabo de hablar de prueba de trabajo y mecanismos de consenso. Esos términos son las reglas que guían el protocolo. Son algoritmos que establecen cómo se coordinará la red. Este conjunto de reglas busca, a partir de una situación inicial («input», una entrada), alcanzar un resultado final, («output», una salida).



(Slide102) - Bitcoin 4 All

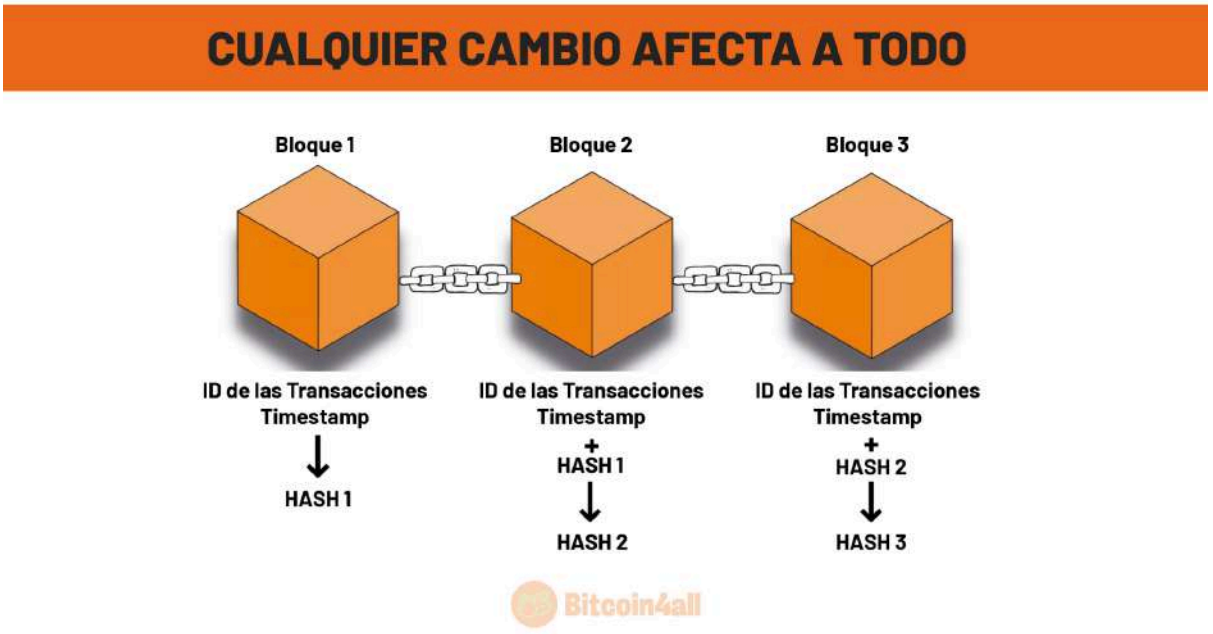
Todo eso funciona registrando la información en un sistema encadenado, distribuido e indeleble llamado blockchain. Satoshi utilizó timestamps y timechain para describir este mecanismo en el whitepaper de Bitcoin.

Hay gente que dice que la blockchain es la verdadera innovación detrás de Bitcoin, pero eso es basura. Blockchain es importante, pero por sí sola y sin otras propiedades, no es más que una base de datos lenta y cara, ¡tan centralizada como el Excel de una empresa!



(Slide 103) - Bitcoin 4 All

Blockchain, o timechain, significa cadena de bloques o de tiempo. Son bloques de información enlazados entre sí y procesados por la red cada 10 minutos de media. Eso significa que a menudo tarda menos de 10 minutos y otras veces puede tardar horas. Depende de la potencia de cálculo de los mineros y de la dificultad de la red.



(Slide 104) - Bitcoin 4 All

La inmutabilidad de los registros significa que no puedes eliminar o cambiar el bloque en medio de la cadena. Si tienes 200 bloques e intentas borrar o modificar el bloque del medio, los bloques vecinos se verán afectados, cambiando el hash.

Es como una costura digital. Si tiras del hilo en medio de una costura, se distorsionan todas las puntadas siguientes, ¿no? Bitcoin es muy similar. Si se cambia alguna información en un bloque, acaba distorsionando todos los bloques siguientes.

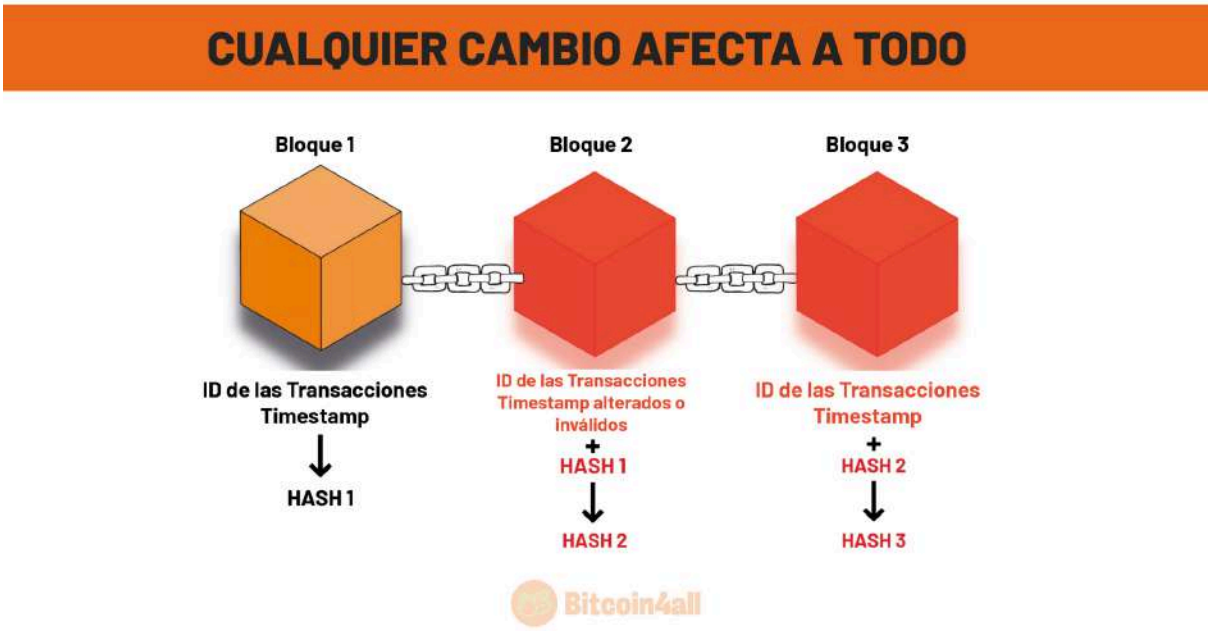
Digamos que ahora mismo estamos viendo la blockchain de Bitcoin. Cada bloque minado contiene información sobre las transacciones financieras realizadas en la red y sobre el propio bloque donde se registraron. Pero la red resume todas estas formaciones en un código llamado HASH. El hash es la frase criptográfica que resume toda la información dentro del bloque de información. Es a partir del hash cuando se produce la vinculación.

Una vez creado el Hash 1 del bloque 1, se insertará junto con el contenido del siguiente bloque, el bloque 2. Se mezclará aleatoriamente para formar el Hash 2.

El Hash 2 resume todo el contenido de su bloque y también del bloque anterior, porque el Hash 1 se ha insertado dentro del contenido del bloque 2 y así sucesivamente.

El Hash 3 será el resumen criptográfico del bloque 3, que contiene el Hash del bloque 2 anterior. Esas funciones Hash se utilizan para encadenar la red. En otras palabras, los

bloques siguientes siempre tendrán un resumen de los anteriores. Así es como se correlaciona siempre la información.



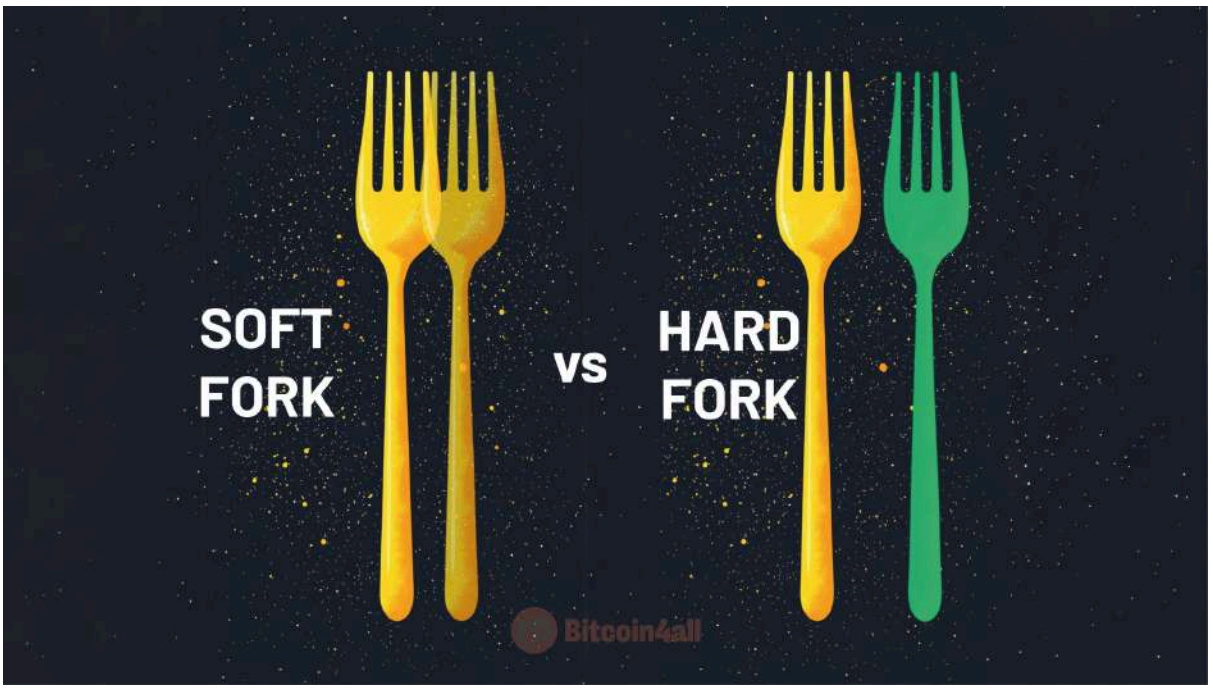
(Slide 105) - Bitcoin 4 All

Gracias a esa cadena de información, la red sigue confirmando todo antes de minar el siguiente bloque. Por tanto, si cambias algo en el bloque 1, el hash de todos los bloques siguientes también cambiará. Si cambias una coma, un espacio, una letra, lo que sea, cambia el hash. Si se cambia algo después de haberlo registrado en la cadena de bloques, los mineros o nodos que comprueban la red identificarán el cambio a través del hash y no aceptarán esa información como válida.

Ese mecanismo hace que sea absurdamente fácil comprobar si ha habido un ataque en el historial de transacciones, al tiempo que dificulta enormemente la edición efectiva de los registros anteriores. Eso se debe a que tanto los nodos como los mineros tienen copias de la blockchain de Bitcoin, por lo que, si alguna información del pasado se modifica y no coincide con las copias de sus computadoras, serán fácilmente identificables y no aceptarán ese bloque como válido.

Éste es uno de los factores de verificación constante que hace que la red Bitcoin sea muy segura y difícil de piratear. Es una red que consigue descentralizar la confianza, porque todo es perfecto, no se ha cambiado nada. Toda la información coincide. Esa facilidad de verificación y dificultad de manipulación es lo que hace que los registros de la cadena de bloques de Bitcoin sean inmutables.

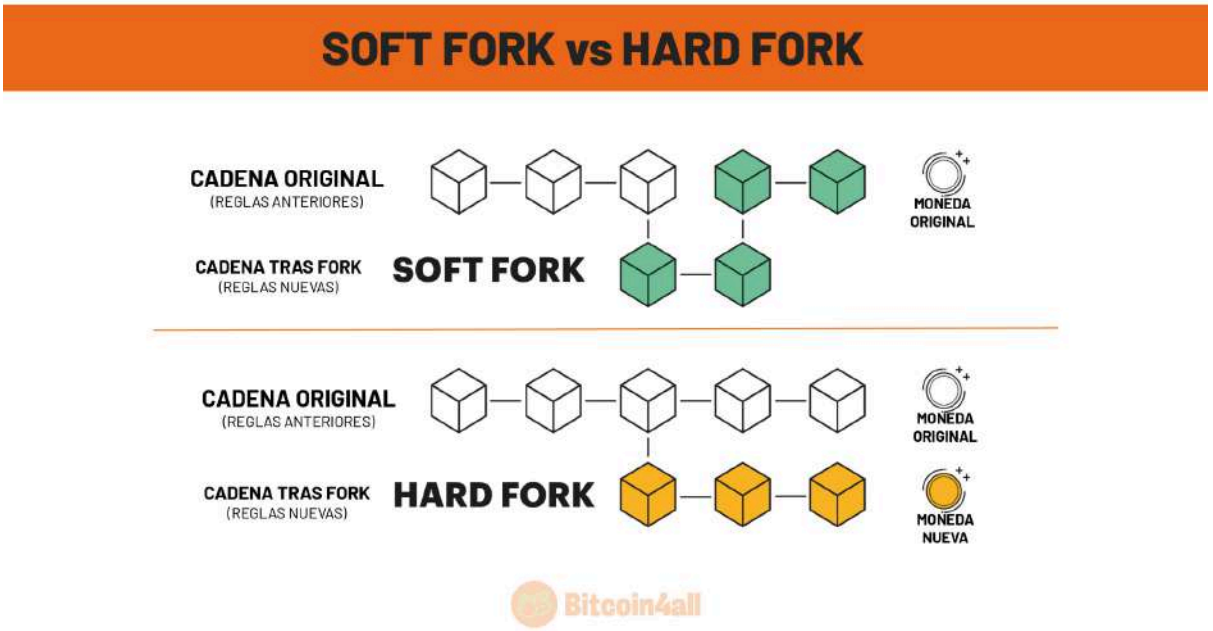
Aun así, si alguien decide cambiar el funcionamiento de la red, podría provocar un fork.



(Slide 106) - Bitcoin 4 All

Las actualizaciones de versión de la blockchain se llaman forks. Hay dos tipos de actualizaciones: soft forks y hard forks.

«Forks» viene de ramificación y también significa tenedor en inglés, por lo que verás imágenes de tenedores cuando alguien hable de forks. Los forks son diferentes versiones de las reglas iniciales.



(Slide 107) - Bitcoin 4 All

Entonces, ¿cuál es la diferencia entre esos dos tipos de forks, es decir, bifurcaciones?

Los soft forks se producen cuando la red realiza una actualización de forma que tanto los que ejecutan la versión antigua del código o software como los que ejecutan la nueva versión puedan coordinarse. Es un fork retrocompatible, opcional y no cambia el mecanismo de consenso. Sigue siendo la misma red y la misma moneda, sólo que con algunos detalles diferentes en las versiones.

Los hard forks, por otro lado, se producen cuando se realizan actualizaciones radicales, hasta el punto de cambiar el consenso del protocolo. Los que ejecutan la versión antigua no pueden coordinarse con los que ejecutan la nueva versión. Los usuarios antiguos no pueden unirse a la nueva red si no se actualizan. Como resultado, se crean una nueva moneda y una nueva red. Ese tipo de actualización obliga a los usuarios a actualizarse a la nueva versión.

Bitcoin no hace hard forks, sólo soft forks. Al fin y al cabo, hard forks son fuerzas centralizadoras, excluyendo a los usuarios que pueden no estar de acuerdo con la nueva versión y acabando con la inmutabilidad de la red. Hard forks se observan con más frecuencia en otros protocolos de criptomonedas y en blockchains de empresas privadas.

Bueno, en esa lección hemos empezado a profundizar en cómo funciona Bitcoin, pero eso es sólo una parte. Hay mucho más contenido para que aprendas. Absorbe todo ese conocimiento, dale un respiro a tu cerebro y cuando estés listo para continuar te esperamos en la próxima lección.