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

---

Índice - Bitcoin 4 All -
Dentro de Bitcoin: ¿cómo funciona Bitcoin?
Parte II (minería, halving y ciclos)

4.6 Principales pools: Foundry, Antpool, F2Pool, ViaBTC, Mara
4.7 ¿Los pools centralizan la red? El rol de los nodos

---

5. Halvings y política monetaria predecible

5.1 ¿Qué es el halving y cómo funciona?
5.2 Tasas en lugar de subsidio

---

6. Por qué el halving afecta el precio

6.1 El shock de oferta: menos BTC, creciente demanda
6.2 Ley de oferta y demanda
6.3 Quiénes son los hodlers y por qué no venden
6.4 Ciclos de mercado y fases:

---

7. El factor emocional en los ciclos

7.1 Índice de Miedo y Codicia
7.2 Revalorizaciones después de cada halving
7.3 ATH (All Time High) y sus tiempos después del halving
7.4 También hay caídas
7.5 Mínimos crecientes en cada ciclo

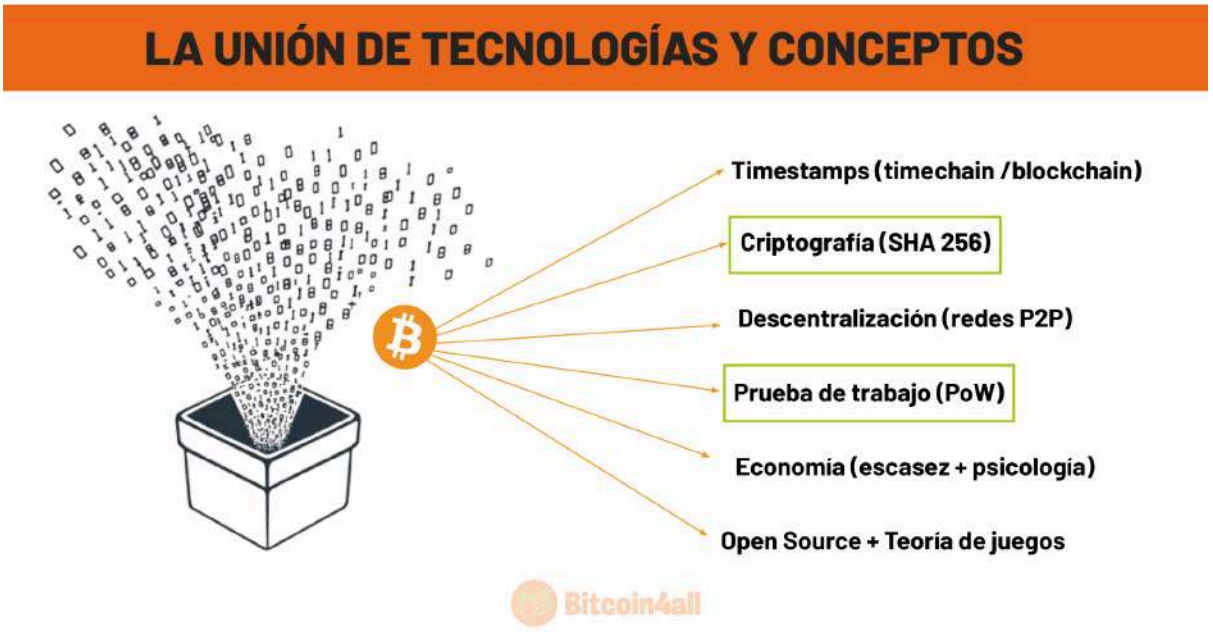
Bitcoin 4 All - Texto completo

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?
Parte II (minería, halving y ciclos)



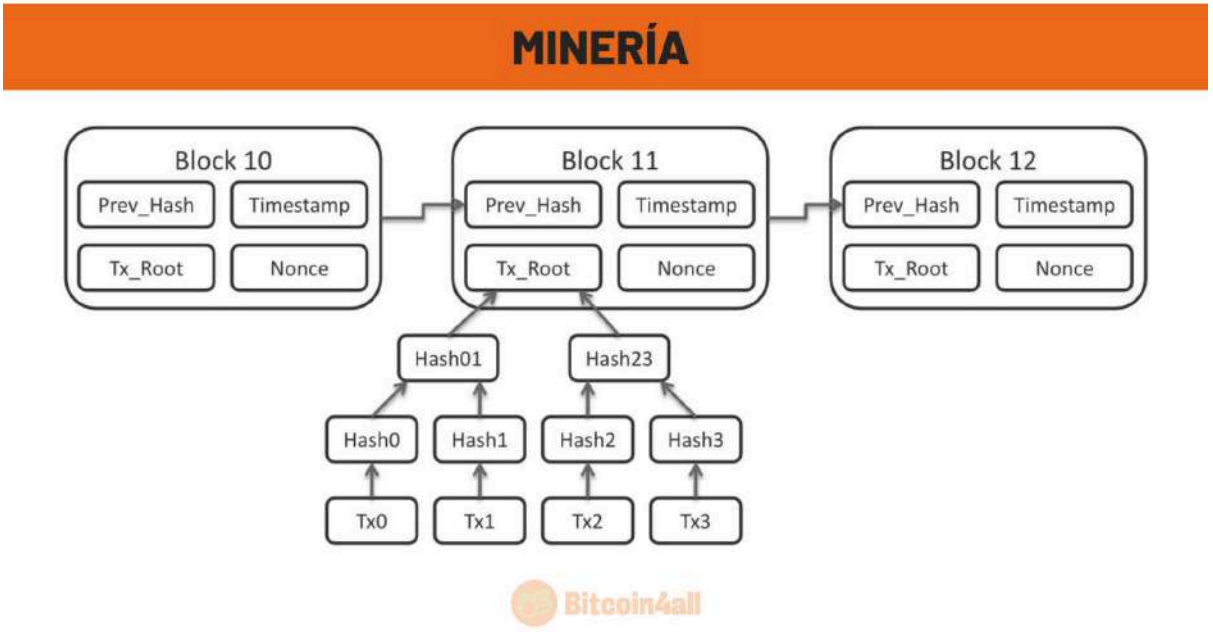
(slide 108) - Bitcoin 4 All

Ahora que has entendido cómo funciona la blockchain de Bitcoin y su necesidad de consenso de los participantes para la coordinación descentralizada, vamos a entender cómo la red se pone de acuerdo entre sí mediante un mecanismo llamado Prueba de Trabajo (PoW, del inglés "*Proof of Work*").

(slide 109) - Bitcoin 4 All

La minería de Bitcoin es una analogía del proceso de búsqueda de algo preciado, como el oro, salvo que en la red Bitcoin ese algo preciado es el hash de cada bloque. Con el oro, los mineros siguen cavando hasta que encuentran el metal precioso. Cuando lo hacen, tienen algo escaso y valioso en sus manos. El oro es escaso y, con el tiempo, es cada vez es más difícil y caro extraerlo, porque hay que excavar más profundamente en la tierra. Se necesitan equipos cada vez más modernos y eficaces para acceder a los yacimientos más profundos y complejos.

Algo muy parecido ocurre con Bitcoin. En la red Bitcoin, los mineros compiten entre sí, mediante ensayo y error, para ver quién llega antes al hash que cierra cada bloque de información.



(slide 110) - Bitcoin 4 All

¿Recuerdas que el bloque está formado por varios componentes? ¿El hash del bloque anterior, una marca de tiempo (el "*timestamp*") y todos los datos de la transacción?

Junto con esta información, también hay un dato llamado "*nonce*". Nonce significa "*number used only once*" – "número utilizado sólo una vez". Cuando los mineros utilizan potencia de cálculo para minar el bloque, significa que están, a una velocidad de cálculo absurda, intentando encontrar ese número que sólo puede ser utilizado una vez por la red. Es ese número el que todos los mineros compiten por encontrar.

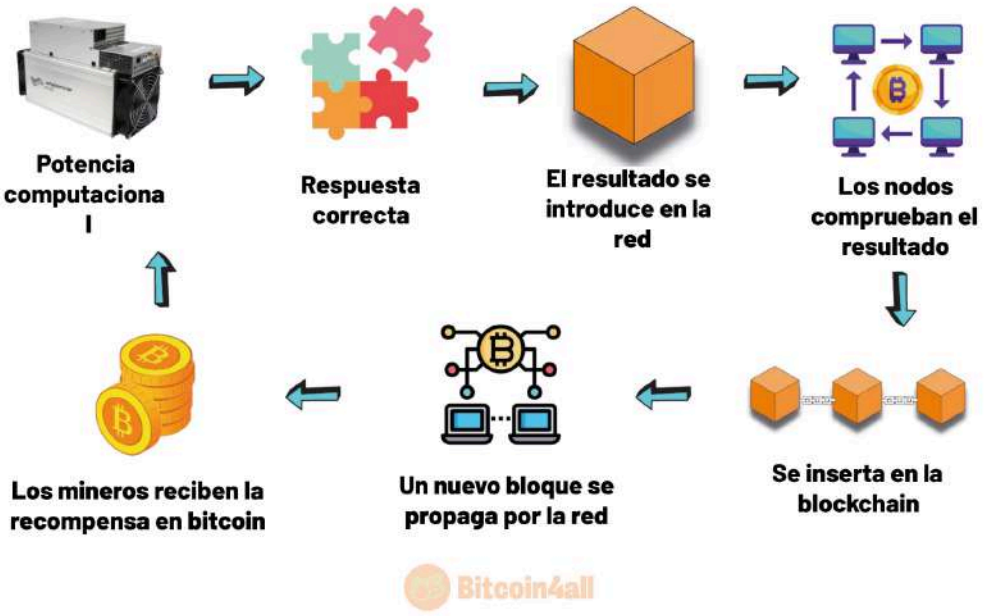
La cabecera del bloque contiene el hash que mezcla todos esos componentes: el hash del bloque anterior, la marca de tiempo ("*timestamp*"), la transacción raíz que resume todas las transacciones que entraron en el bloque y el nonce.

(slide 111) - Bitcoin 4 All

Una buena analogía de este proceso de minería es un rompecabezas. Así que en esta analogía la minería de bitcoins es como un puzzle, un juego, en el que cada 10 minutos los mineros tienen que encontrar la pieza que falta para completar el cuadro.

Todos buscan la pieza adecuada dentro de todas las posibilidades y quien la encuentra primero intenta encajarla en el cuadro. Cuando el minero encuentra la pieza que le falta, es muy fácil que todos se den cuenta de que ha encajado. Sólo hay que mirar la foto y ver si la pieza era correcta o no.

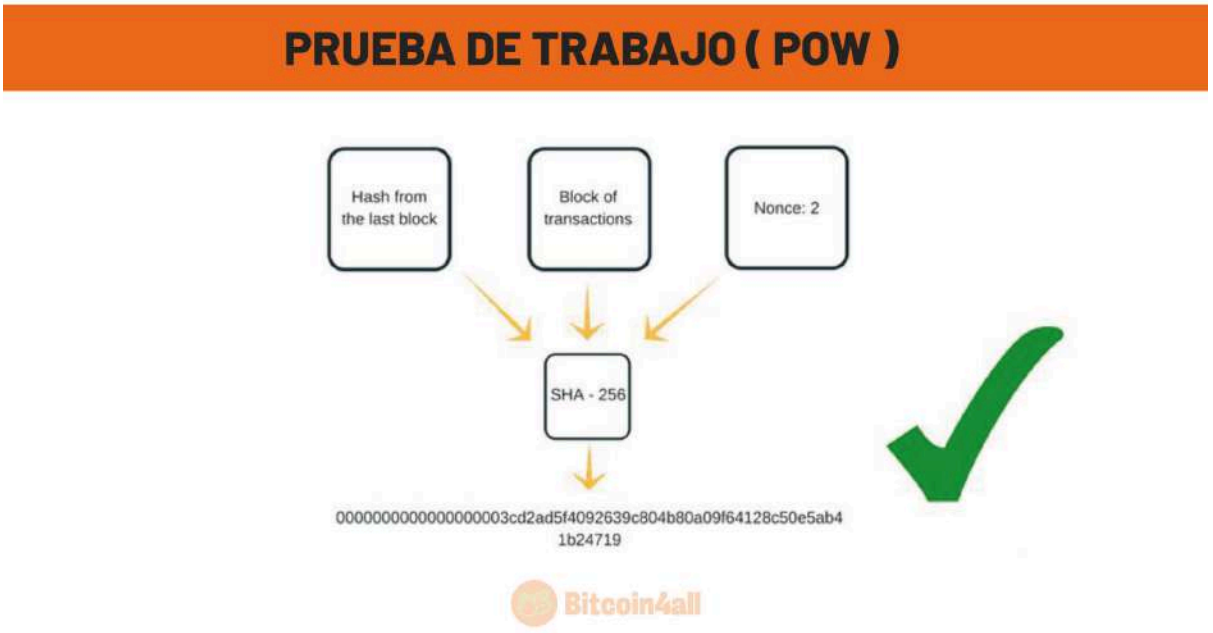
Eso significa que la minería es un proceso difícil de defraudar y, al mismo tiempo, muy fácil de verificar. Así como es difícil encontrar la pieza correcta en un rompecabezas gigante, es muy fácil comprobar si es la pieza que falta o no. Bitcoin es como un puzzle global en el que participa todo el mundo y se puede seguir los resultados en tiempo real.



(slide 112) - Bitcoin 4 All

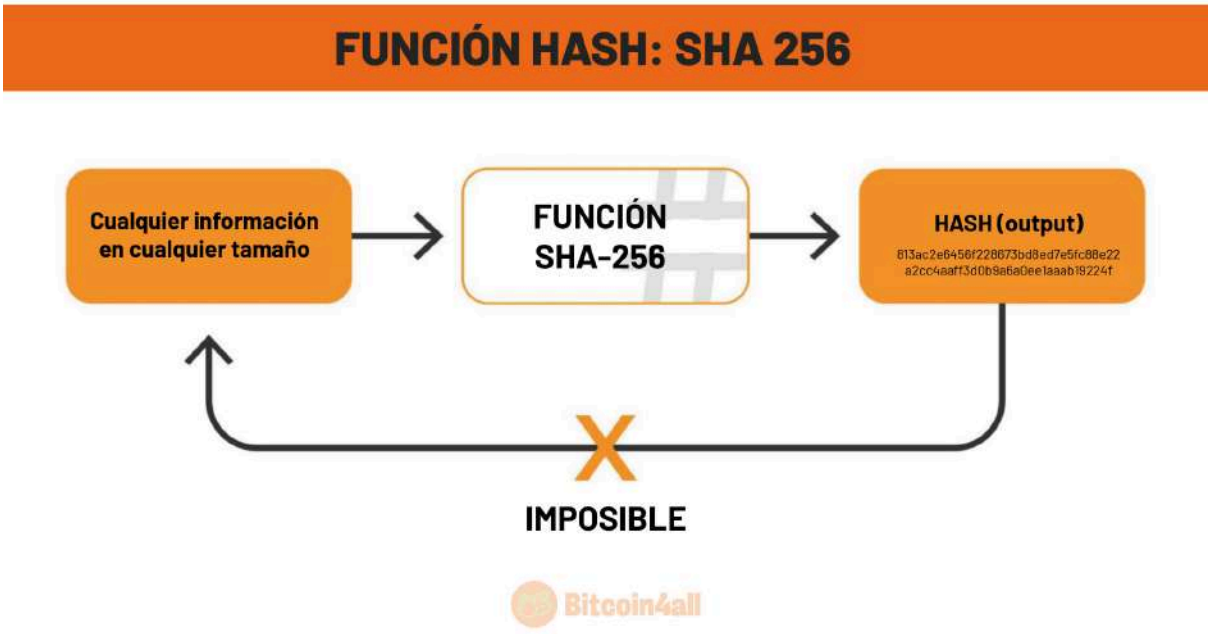
Todo el proceso de minería y consenso al registrar la blockchain de Bitcoin funciona así:

Los mineros utilizan la potencia computacional, comprando potentes máquinas con un enorme poder de cálculo para intentar encontrar el nonce del bloque lo más rápidamente posible. Cuando lo encuentran, crean el hash, lo muestran a la red, y los nodos comprueban que el bloque propuesto sigue las reglas. Si todo es correcto, el bloque se inserta en la cadena de bloques, se propaga por la red y todos los participantes insertan ese bloque en sus copias de la blockchain. Al final, los mineros reciben bitcoin como recompensa por completar su tarea.
Todo ese proceso se conoce como prueba de trabajo.



(slide 113) - Bitcoin 4 All

La prueba de trabajo significa que el minero ha seguido las reglas, ha encontrado el nonce, ha creado el hash del bloque y ha proporcionado un servicio computacional a la red. Cuando se encuentra toda la información del bloque, pasa por el proceso de encriptación de convertir la información en un puzzle criptográfico utilizando SHA-256. El resultado es ese número enorme de ahí abajo, que representa el hash del bloque, el resultado de todo el trabajo del minero.



(slide 114) - Bitcoin 4 All

Ese proceso no es exclusivo de Bitcoin, sino de cualquier cosa que pueda encriptarse, y SHA-256 es el algoritmo que lo hace. SHA-256 toma información de cualquier longitud y crea una secuencia de 256 bits: una serie de 256 ceros y unos. A partir de este enorme número lleno de ceros y unos, el algoritmo crea una secuencia hexadecimal formada por 64 dígitos entre letras y números, más fácil de escribir. En otras palabras, es fácil comprobar que la cifra es correcta, pero es prácticamente imposible falsificar la información que se ha cifrado.

Intentar hacer coincidir aleatoriamente un hash y romper el cifrado SHA-256 es prácticamente imposible. Implica un número absurdamente elevado de combinaciones posibles, ¡más números que el número de átomos del universo observable! Eso requeriría un número tan, pero tan grande de intentos que una computadora normal tardaría miles de millones de años en hacerlo.

¡Ahí es donde entra la historia de la computadora cuántica! La gente siempre nos pregunta si una computadora cuántica podría romper el cifrado de Bitcoin. Esa es una de las grandes esperanzas de los que odian Bitcoin, pero la verdad es que ninguna computadora cuántica podría probablemente matar a Bitcoin.

Debajo de esa lección dejaré un artículo que lo explica.

Vamos a ver un sitio web muy bueno. Es éste, llamado Code Beautify. Ese sitio te permite experimentar y convertir cualquier información en una función SHA-256.

Vamos a escribir Bitcoin4All aquí. Mira cómo cambia el código en el cuadro de abajo con cada letra, espacio o signo de puntuación que introduzcas. Eso es lo que le ocurre al hash del bloque de la red Bitcoin si se modifica alguna información. Fíjate también en lo rápido que fue. No hizo falta una gran potencia computacional para encontrar ese hash. Entonces, si es tan fácil crear un hash aquí en este sitio, ¿por qué se tarda 10 minutos en la red Bitcoin y ya no es posible minar desde la computadora de casa?

(slide 115) - Bitcoin 4 All

Eso tiene que ver con un mecanismo llamado ajuste de la dificultad.

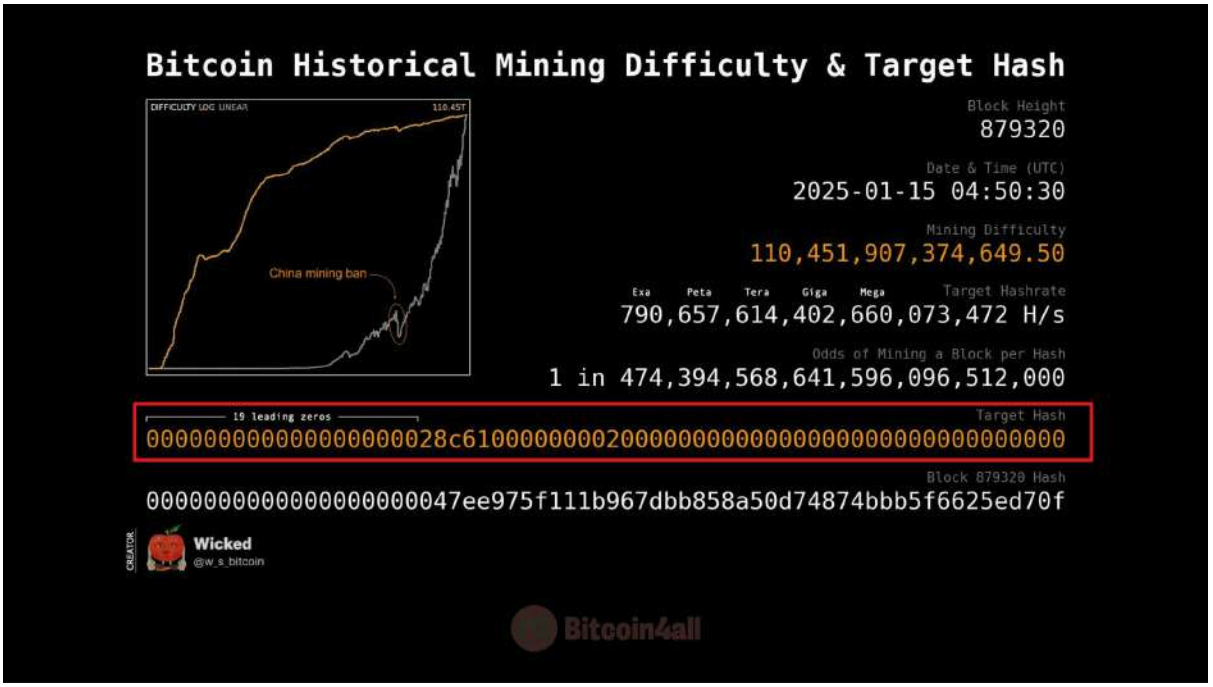
El ajuste de la dificultad tiene la función de regular la emisión de nuevos bitcoins. Ese ajuste es el que garantiza que el tiempo medio que se tarda en crear nuevos bloques y la recompensa que entrega la red sea de 10 minutos. Eso se debe a que cada 2016 bloques minados, unos 15 días de media, un algoritmo analiza la cantidad de potencia de cálculo de la red y aumenta o disminuye la dificultad de encontrar el hash del bloque.

Si el número de mineros aumenta de un momento a otro, la red se autorregulará para aumentar la dificultad de la minería con el fin de no acelerar el ritmo de creación de nuevos bloques y, en consecuencia, no acelerar el ritmo de creación de nuevos bitcoins.

(slide 116) - Bitcoin 4 All

Funciona así: a medida que más mineros se unen a la red y aumenta el hashrate (el ritmo al que se crean nuevos bloques), los mineros empiezan a encontrar bloques más fácilmente y el tiempo medio de minado entre un bloque y el siguiente se hace más rápido. La red se da cuenta de ello a través de sus algoritmos y aumenta la dificultad de la minería, con el resultado de que la velocidad a la que se crean nuevos bloques disminuye. Al fin y al cabo, a los mineros les resulta más difícil encontrar bloques, hasta que se estabiliza en una media de 10 minutos la frecuencia entre un bloque y el siguiente.

Así es como la red se regula a medida que aumenta la demanda, para que nunca pierda su previsibilidad.



(slide 117) - Bitcoin 4 All

Es posible saber el nivel de dificultad de minar cada bloque de acuerdo con el número de ceros que aparecen antes del número hash del bloque. Ese bloque, por ejemplo, tiene 24 ceros delante del código hash y se minó en octubre de 2022. Fue uno de los bloques más difíciles de minar en ese momento.

El objetivo del minero es montar un bloque cuyo código hash sea menor que el objetivo actual (penúltima línea en blanco). Cuanto más pequeño sea el objetivo, más difícil será encontrar un bloque válido. Cuantos más mineros haya en la red, más difícil será.

(slide 118) - Bitcoin 4 All

En otras palabras, cuantos más ceros encabecen un hash, más difícil será de minar: más tendrá que buscar el minero el nonce del bloque hasta que lo encuentre.

(slide 119) - Bitcoin 4 All

Debido a la configuración de la dificultad, la minería ha evolucionado y ya no es tan fácil minar desde la computadora de tu casa, es decir, desde una CPU. Hoy en día, Bitcoin se mina utilizando máquinas específicas llamadas ASICs. A medida que subía el precio de Bitcoin, acabó atrayendo a más y más gente, se empleó más potencia de cálculo en la red y con ello se aumentó el algoritmo de ajuste de dificultad para mantener una media de un bloque minado cada 10 minutos.

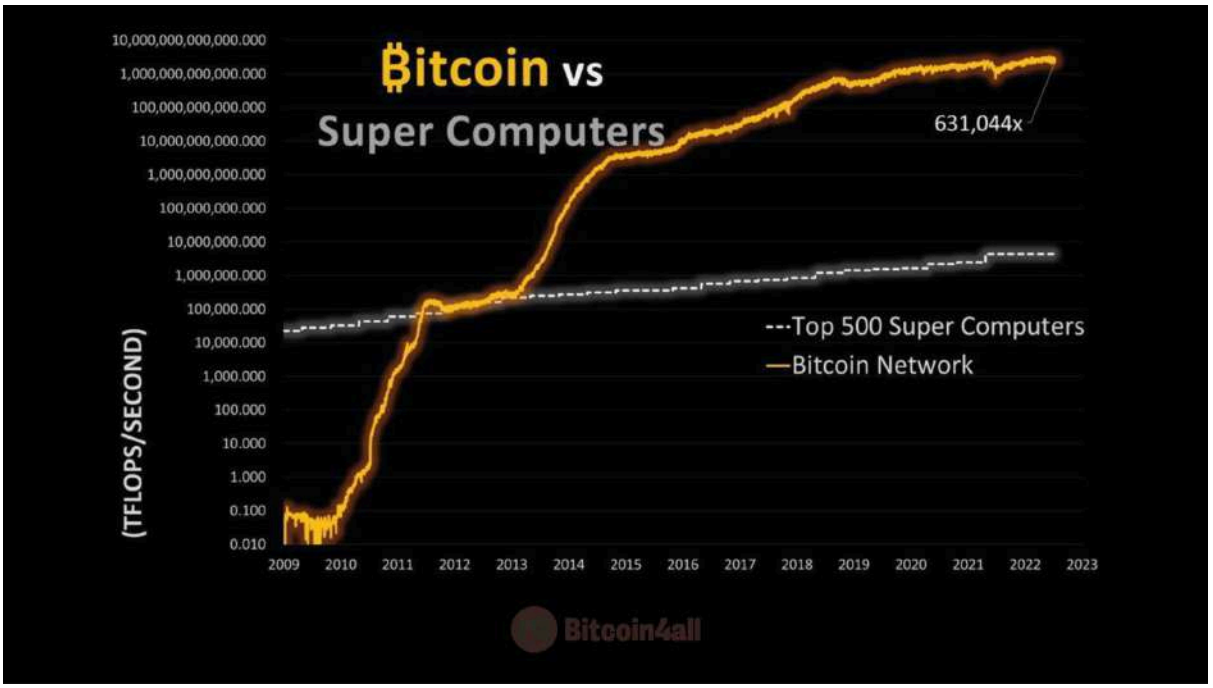
A medida que aumentaba la dificultad, los más expertos en tecnología empezaron a utilizar máquinas más potentes: las GPU, muy utilizadas en las computadoras para juegos. Bitcoin siguió atrayendo a más y más gente que quería minar, hasta que decidieron crear una máquina específica: los ASICs.

Ese tipo de máquina es mucho más potente y supera a las CPUs y GPUs en la velocidad de encontrar el hash del bloque. La minería se ha convertido en una industria gigantesca y dedicada que persigue implacablemente la eficiencia. En otras palabras, producir la mayor cantidad posible de bitcoins con la menor energía posible.

Por eso el precio no importa. Bitcoin podría alcanzar los 10.000 millones de dólares. La velocidad a la que se emiten nuevos bitcoins no cambia. Ni siquiera un aumento de la potencia del hashrate puede hacer que se emita más bitcoins del previsto en cada ciclo de reducción a la mitad. Incorporar más mineros a la red no produce más bitcoins, pero hace que la red sea más segura y descentralizada.

(slide 120) - Bitcoin 4 All

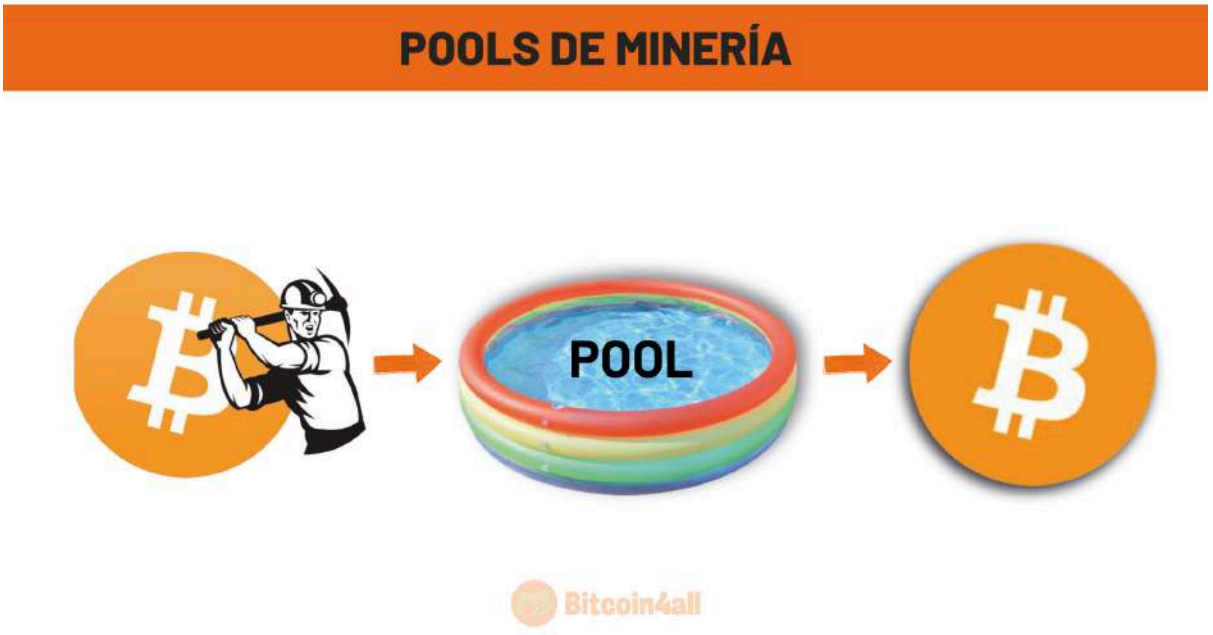
¿Y por qué ese mecanismo hace que la red sea más segura? Eso se debe a que cuanto mayor sea la potencia computacional, más difícil será atacar la red. En ese gráfico, la línea representa el hashrate, la potencia computacional, y los colores más rojos representan la dificultad de minar cada bloque. La dificultad y el hashrate han aumentado exponencialmente desde que Bitcoin empezó a circular. A medida que la línea se vuelve naranja, más difícil es minar un bloque. Cuanto mayor es la potencia computacional, más se ha adaptado la red para proteger las propiedades de Bitcoin. Por eso Bitcoin no tiene competidor en la minería: es el protocolo con más mineros distribuidos por todo el planeta y con más potencia computacional de todos.



(slide 121) - Bitcoin 4 All

Bitcoin es 631 veces más potente que las 500 mayores supercomputadoras del mundo juntas, representadas en la línea blanca, mientras Bitcoin se muestra en la línea naranja. Bitcoin tiene la red informática más resistente a los ataques y es 600 veces más fuerte que cualquier sistema informático o centro de datos centralizado.

Pero el avance de la minería no se ha detenido en los ASICs. Con el tiempo, incluso con una máquina superpotente, cada vez era más difícil encontrar bloques y los mineros acabaron agrupándose en los pools. Hacen una cooperacha con su potencia computacional para tener más posibilidades de encontrar bloques y compartir la recompensa.

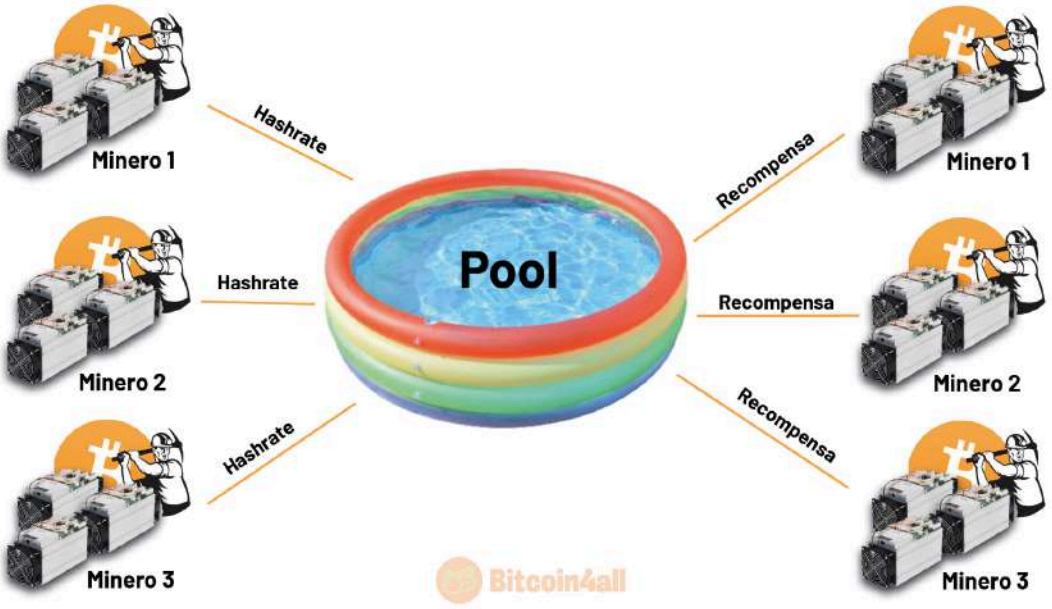


(slide 122) - Bitcoin 4 All

Los pools de minería funcionan entre el software de Bitcoin y los mineros, permitiendo a los mineros agrupar la potencia de cálculo de sus máquinas y tener más posibilidades de encontrar un bloque. Pool viene del inglés y significa tanto “conjunto” como “piscina”. Pools son una concentración de potencia computacional agrupada.

(slide 123) - Bitcoin 4 All

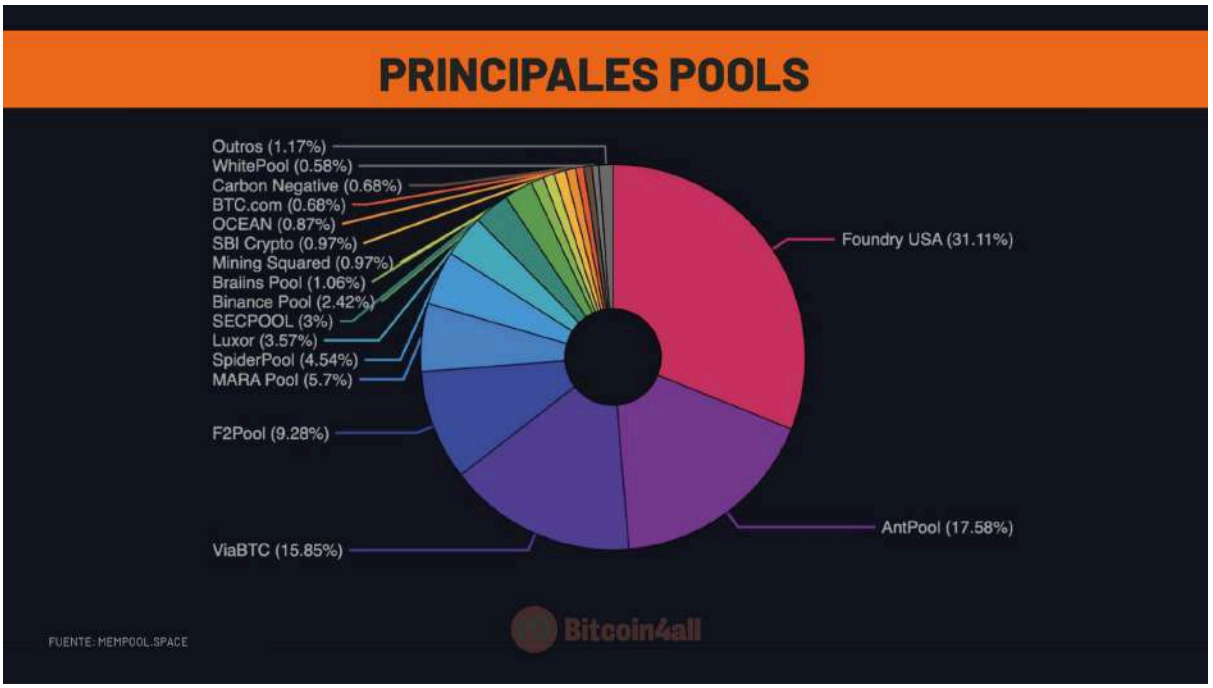
Para que te hagas una idea de lo difícil que es minar fuera de un pool, es decir, minar en solitario, una S19JPRO, que es una de las máquinas ASICs más modernas, tiene una probabilidad del 0,000000208% de minar un bloque de Bitcoin. Eso significa una posibilidad entre casi 4.800 millones de intentos a lo largo de toda la vida útil de la máquina, que dura una media de 5 a 8 años. Esa probabilidad seguirá disminuyendo con el tiempo, a medida que lleguen más mineros y el hashrate y la dificultad aumenten.



(slide 124) - Bitcoin 4 All

Por eso los pools son como una cooperacha de potencia computacional. Cuando alguien en el pool encuentra el bloque, todos comparten la recompensa en bitcoin en proporción a su

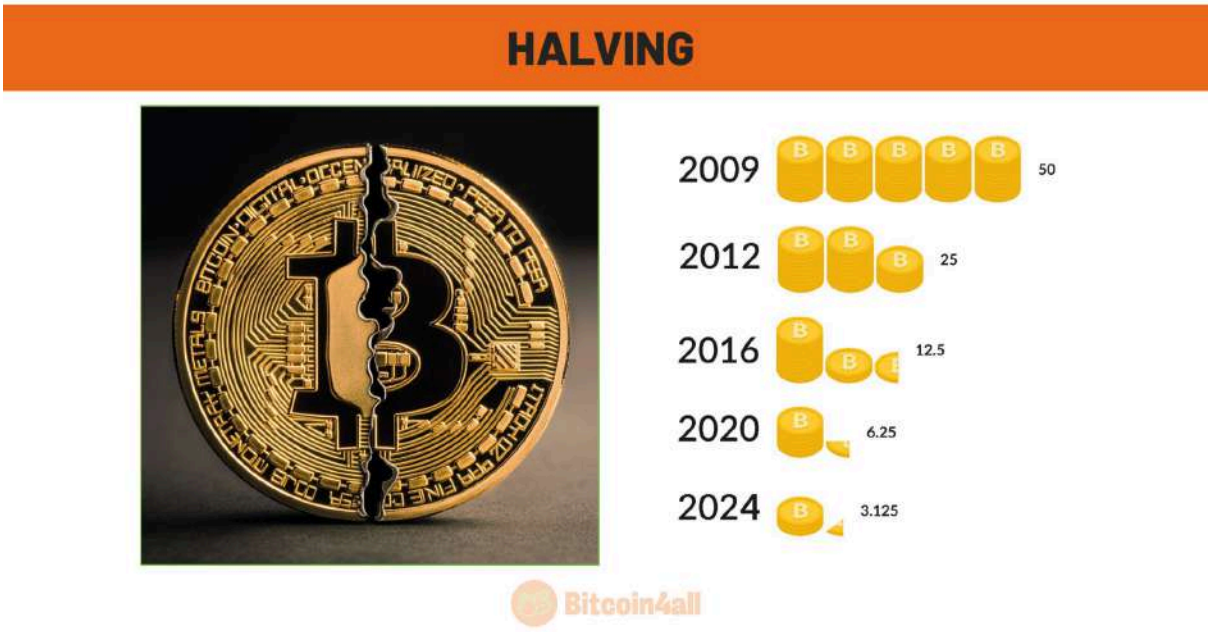
potencia de hash. De este modo, los mineros pueden obtener ingresos frecuentes en lugar de esperar a encontrar un bloque por su cuenta, lo que puede llevar años y no está cien por cien garantizado que ocurra.



(slide 125) - Bitcoin 4 All

Hoy en día la red Bitcoin tiene docenas de pools, pero cinco de ellos son los más grandes y agregan la mayor parte del hashrate: Foundry, Antpool, F2Pool, ViaBTC y Mara. Aunque mucha gente dice que eso sería un mecanismo de centralización, en realidad los mineros pueden abandonar un pool en cualquier momento e irse a otro, o incluso pueden minar en solitario si quieren probar suerte. En otras palabras, la concentración en esos cinco pools más grandes fue un movimiento natural del mercado de los propios mineros que querían estar en los pools con más probabilidades de encontrar bloques y compartir las recompensas. Los pools no dirigen la red, ya que son los nodos los que comprueban y deciden si los bloques minados son válidos o no.

Un otro punto muy importante en el funcionamiento de Bitcoin son los halvings, que tienen todo que ver con la minería. A medida que pasa el tiempo, Bitcoin es cada vez más escaso. La creciente escasez unida a la creciente demanda es lo que ha provocado los movimientos parabólicos al alza del precio del Bitcoin. Es el halving lo que hace que el Bitcoin se vuelva gradualmente más escaso mientras crea ciclos de revalorización que se han repetido.



(slide 126) - Bitcoin 4 All

Halving viene de la palabra "halfing" y significa "cortar por la mitad" en inglés. Eso significa que, por cada 210.000 bloques minados, de media cada 4 años, el protocolo reduce a la mitad la recompensa otorgada a los mineros.

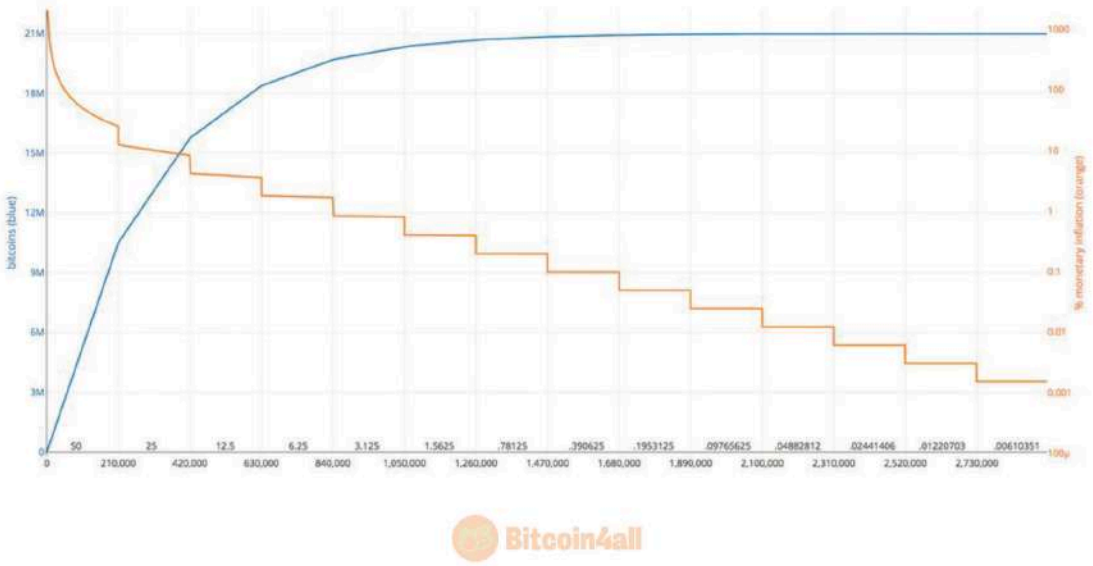
Halving	Fecha estimada	Altura del bloque	Recompensa por bloque (BTC)
0	N/A	0	50
1	28/11/2012	210.000	25
2	09/07/2016	420000	12,5
3	11/05/2020	630.000	6,25
4	2024	840000	3,125
5	2028	1050000	1,5625

(slide 127) - Bitcoin 4 All

El primer halving tuvo lugar el 28 de noviembre de 2012, al principio de la red. En aquel momento, la red Bitcoin producía 50 bitcoins por bloque de información procesado. En otras palabras, por cada 10 minutos de media en ese momento, los mineros recibían 50 bitcoins como recompensa. Con el halving de 2012, los mineros ganaban 25 bitcoins por bloque minado.

En 2016, tuvo lugar el segundo halving, en el bloque 420.000, y la emisión volvió a reducirse a la mitad. En lugar de recibir 25 bitcoins por bloque, cada minero pasó a recibir 12,5 bitcoins por bloque minado. Y el tercero halving tuvo lugar en 2020, el 11 de mayo, en el bloque 630.000, donde los mineros pasaron a recibir 6,25 bitcoins por bloque.

El último halving registrado, el cuarto, tuvo lugar en abril de 2024 en el bloque 840.000. El próximo será en 2028. Y lo bueno de todo esto es que sabemos de antemano qué bloque va a ser: en el bloque 1,50 millón. La nueva recompensa será de 1,5625 bitcoin para los mineros.



(slide 128) - Bitcoin 4 All

Esa imagen muestra cómo con cada paso de la línea naranja, es decir, con cada halving, Bitcoin se vuelve lentamente más escaso y se acerca al límite de suministro unitario de la línea azul.

Esa imagen es genial porque muestra cómo Bitcoin es transparente, programable y tiene una política monetaria predecible que no puede ampliarse ni modificarse. Es muy diferente de cualquier otro activo o moneda que cambie las reglas o las políticas monetarias en cualquier momento.

El último satoshi se acuñará en el año 2140 y será entonces cuando finalice la emisión de nuevos bitcoins. Las tarifas de red serán la única fuente de ingresos de los mineros para pagar los costes de funcionamiento.

Years	Years since Inception	Total # of Blocks	Block Reward (BTC)	Total Mined BTC	% of Total Mined
2008 - 2012	0 - 4	210,000	50.00000000	10,500,000.000	50.00000000%
2012 - 2016	4 - 8	420,000	25.00000000	15,750,000.000	75.00000000%
2016 - 2020	8 - 12	630,000	12.50000000	18,375,000.000	87.50000000%
2020 - 2024	12 - 16	840,000	6.25000000	19,687,500.000	93.75000000%
2024 - 2028	16 - 20	1,050,000	3.12500000	20,343,750.000	96.87500000%
2028 - 2032	20 - 24	1,260,000	1.56250000	20,671,875.000	98.43750000%
2032 - 2036	24 - 28	1,470,000	0.78125000	20,835,937.500	99.21875000%
2036 - 2040	28 - 32	1,680,000	0.39062500	20,917,968.750	99.60937500%
2040 - 2044	32 - 36	1,890,000	0.19531250	20,958,984.375	99.80468750%
2044 - 2048	36 - 40	2,100,000	0.09765625	20,979,492.188	99.90234375%
2048 - 2052	40 - 44	2,310,000	0.04882813	20,989,746.094	99.95117188%
2052 - 2056	44 - 48	2,520,000	0.02441406	20,994,873.047	99.97558594%
2056 - 2060	48 - 52	2,730,000	0.01220703	20,997,436.523	99.98779297%
2060 - 2064	52 - 56	2,940,000	0.00610352	20,998,718.262	99.99389648%
2064 - 2068	56 - 60	3,150,000	0.00305176	20,999,359.131	99.99694824%
2068 - 2072	60 - 64	3,360,000	0.00152588	20,999,679.565	99.99847412%
2072 - 2076	64 - 68	3,570,000	0.00076294	20,999,839.783	99.99923706%
2076 - 2080	68 - 72	3,780,000	0.00038147	20,999,919.891	99.99961853%
2080 - 2084	72 - 76	3,990,000	0.00019073	20,999,959.946	99.99980927%
2084 - 2088	76 - 80	4,200,000	0.00009537	20,999,979.973	99.99990463%
2088 - 2092	80 - 84	4,410,000	0.00004768	20,999,989.986	99.99995232%
2092 - 2096	84 - 88	4,620,000	0.00002384	20,999,994.993	99.99997616%
2096 - 2100	88 - 92	4,830,000	0.00001192	20,999,997.497	99.99998808%
2100 - 2104	92 - 96	5,040,000	0.00000596	20,999,998.748	99.99999404%
2104 - 2108	96 - 100	5,250,000	0.00000298	20,999,999.374	99.99999702%
2108 - 2112	100 - 104	5,460,000	0.00000149	20,999,999.687	99.99999851%
2112 - 2116	104 - 108	5,670,000	0.00000075	20,999,999.844	99.99999925%
2116 - 2120	108 - 112	5,880,000	0.00000037	20,999,999.922	99.99999963%
2120 - 2124	112 - 116	6,090,000	0.00000019	20,999,999.961	99.99999981%
2124 - 2128	116 - 120	6,300,000	0.00000009	20,999,999.980	99.99999991%
2128 - 2132	120 - 124	6,510,000	0.00000005	20,999,999.990	99.99999995%
2132 - 2136	124 - 128	6,720,000	0.00000002	20,999,999.995	99.99999998%
2136 - 2140	128 - 132	6,930,000	0.00000001	20,999,999.998	99.99999999%

(slide 129) - Bitcoin 4 All

Esa tabla de aquí es otra forma de mostrar lo mismo. La tabla muestra toda la política monetaria de Bitcoin, desde el primer satoshi y el primer halving hasta el último halving en 2140.

Esa tabla muestra que ya se ha emitido más del 90% de los bitcoins y que, para el año 2036, se habrá acuñado el 99% de todos los bitcoins. El resto, el 1% final, se creará entre 2036 y 2140. ¡Se tarda 110 años en extraer el 1% de la oferta de bitcoins!

El año 2030 es probablemente cuando la mayor fuente de ingresos de los mineros pasará a ser las tasas. En ese punto, la demanda de Bitcoin debe ser muy alta, hasta el punto de que las comisiones cobradas por los mineros sostengan su funcionamiento, incluyendo el mantenimiento de la máquina y los costes energéticos, y no tanto la recompensa por bloque.

(slide 130) - Bitcoin 4 All

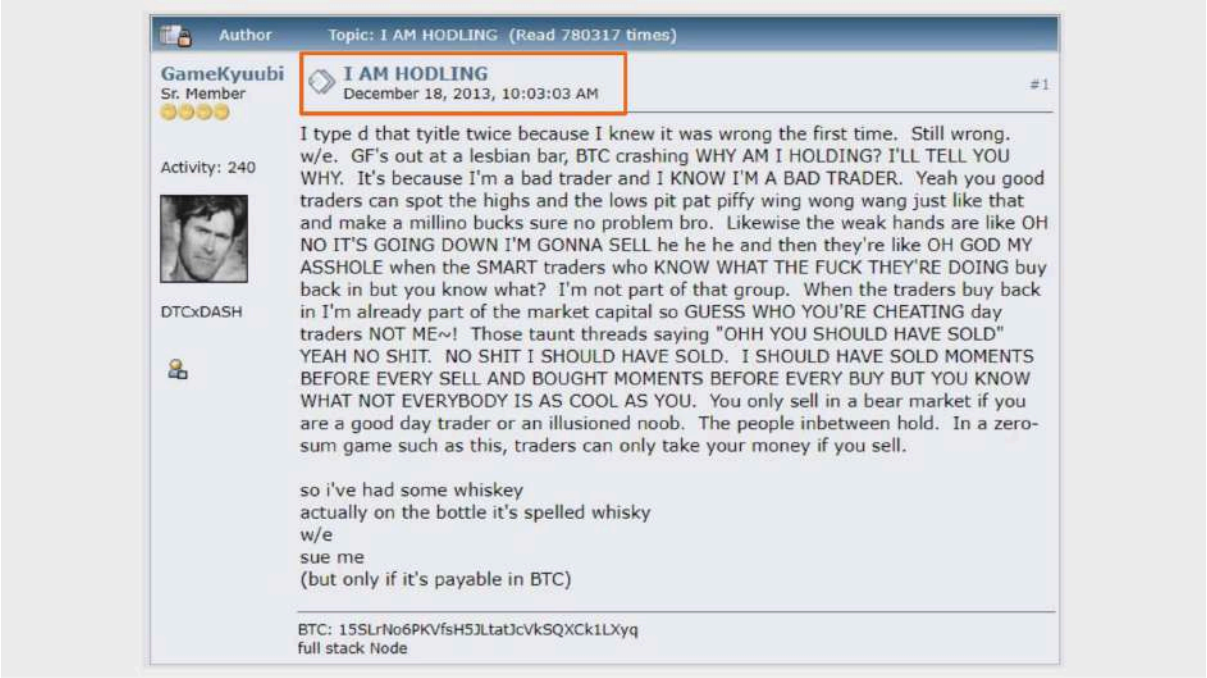
Cuando hablamos de 2140, surge el miedo a lo desconocido y las dudas: "¿Qué ocurre cuando se mina el último bitcoin?"

La respuesta es: nada. El gran cambio comienza mucho antes. En 2030, las tasas tenderán a ser la principal fuente de ingresos de los mineros. Cuando llegue 2140, los mineros probablemente recibirán mucho más en concepto de tasas que los pocos satoshis que ofrece la red, debido a la creciente escasez de la moneda, al aumento del precio del fiat y al mayor uso de la red.

¿Y por qué es tan importante el halving?

(slide 131) - Bitcoin 4 All

Los halvings crean un "shock de oferta": hay menos bitcoins disponibles mientras que la demanda sigue siendo la misma. Con cada halving, la cantidad de bitcoins creados por bloque se reduce a la mitad. Eso reduce la oferta, lo que hace subir el precio. Si mucha gente quiere comprar Bitcoin y no puedes crear más unidades, la única forma de convencer a los hodlers para que vendan es ofrecer un precio más alto.



(slide 132) - Bitcoin 4 All

Hodlers son bitcoiners que acumulan Bitcoin a largo plazo y no venden ni siquiera en las mayores caídas a corto plazo. El término *hodler* se convirtió en un meme porque un tipo en Bitcoin Talk, un famoso foro de Bitcoin, lo erro al escribir "*holder*" y la gente adoptó la jerga para diferenciarlo de la gente tradicional del mercado de valores. Esa imagen de la pantalla es una captura del post que dio nombre a los hodlers: bitcoiners que retienen firmemente sus bitcoins y no lo venden en absoluto.

La subida forma movimientos parabólicos, atrae la atención generalizada, Bitcoin aparece en las noticias y aumenta aún más la demanda. Es entonces cuando comienza la euforia estimulante del *bull run*.

Eso se debe a que la única forma de tener la misma liquidez para satisfacer a los nuevos compradores es aumentar la prima para que los que tienen Bitcoin cambien de opinión y quieran vender. Es la ley más simple de la economía: la ley de la oferta y la demanda. Si hay mucha demanda y se reduce la oferta, los precios suben. Como el número de Bitcoin está limitado a 21 millones de unidades y no hay forma de emitir más, cuando aumenta la demanda, la única forma de que la oferta satisfaga la demanda es que suba el precio.

Los halvings provocan choques de oferta que hacen que el Bitcoin suba hasta un nuevo avance del precio. Todo ese proceso crea movimientos cíclicos de apreciación y contracción hasta que se fija el nuevo precio.

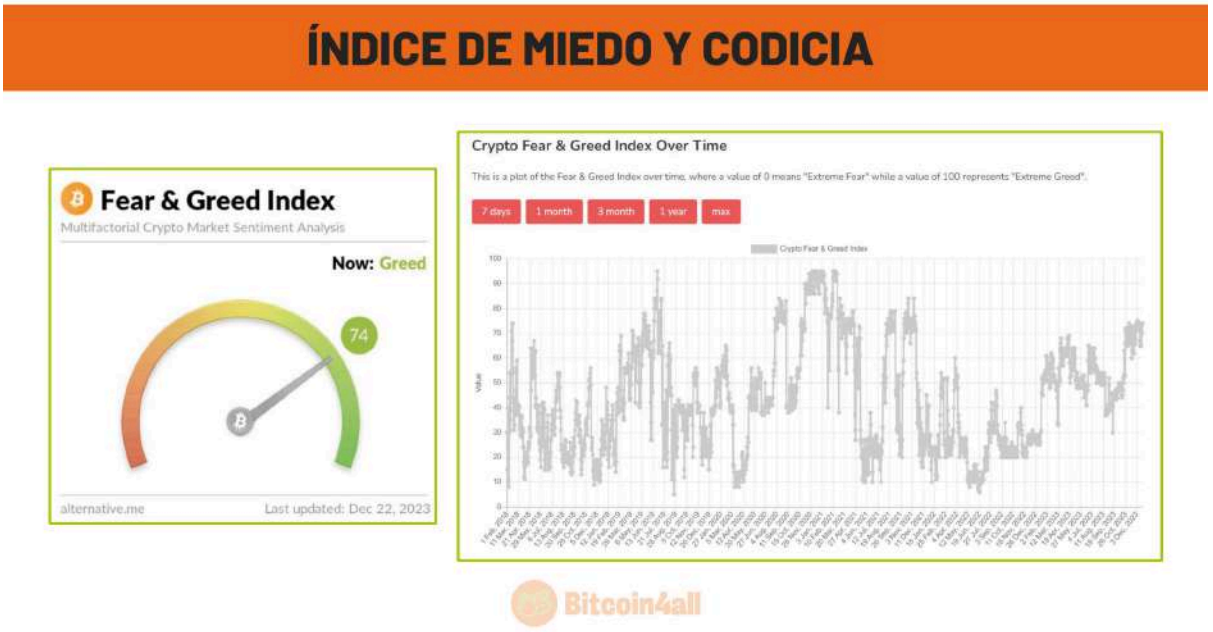
(slide 133) - Bitcoin 4 All

Los ciclos de Bitcoin constan de cuatro fases. La primera fase es el *bear*, cuando el mercado es bajista. Es cuando el precio cae bruscamente tras un periodo de máximos y los que llegaran en el mercado alcista se marchan. 2011, 2014, 2018 y 2022 fueron los años de Bitcoin en el *bear* (bajista). Es entonces cuando salen las únicas noticias negativas, y cualquiera que fuera turista en Bitcoin se marcha.

Después del *bear* viene una fase MUY agónica, que es la fase de acumulación. Es cuando el Bitcoin va solamente de lado durante todo un año. Nada ocurre, es puro aburrimiento y parece no acabar nunca.

La siguiente fase es la de expansión o crecimiento. Es el momento en que Bitcoin empieza a subir lentamente, como quien no quiere la cosa. Es la fase en la que los haters atacan porque no creen en una nueva subida y los bitcoiners empiezan a renovar sus esperanzas de que una nueva carrera alcista – *bull run* – está en el horizonte. 2012, 2016, 2020 y 2024 fueron años de expansión.

Y finalmente llega el *bull run*, el encierro. Es entonces cuando el Bitcoin alcanza el máximo del ciclo y corre como un toro desbocado al que nada puede frenar. ¡Esa fase es pura alegría y euforia y los haters desaparecen! Bitcoin está en el punto de mira del público, atrae la atención y alcanza un nuevo nivel de precios. Cuando pasa la euforia, llega la caída y se establece un nuevo suelo de precios. Y así todo vuelve al principio, a la fase bajista, de *bear*. Es una montaña rusa mental y emocional.



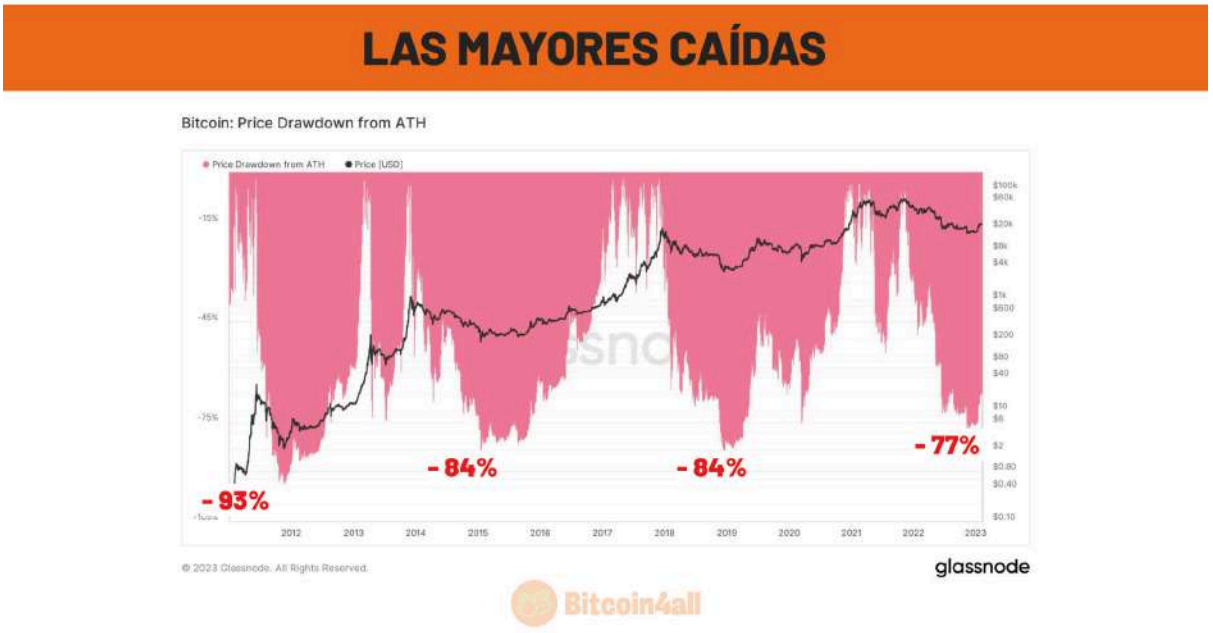
(slide 134) - Bitcoin 4 All

Tanto es así que se creó el índice de miedo y codicia para medir el estado emocional del mercado. En el índice, lo más cercano a 0 significa "Miedo Extremo", y lo más cercano a 100 representa "Codicia Extrema".

(slide 135) - Bitcoin 4 All

La gente suele querer que el Bitcoin se revalorice en línea recta, pero las mayores subidas tardaron un año en alcanzar el vértice del movimiento. Aquí he echado un vistazo más de cerca para analizar el precio de Bitcoin en los halvings. Desde el halving hasta el tope del ciclo ha tardado aproximadamente un año en alcanzar el ATH (*all time high*, máximo histórico), pero no ocurre en línea recta. El gráfico fluctúa mucho, pero con una media

ascendente del valor. Bitcoin se revalorizó un 11.000% tras el primer halving, un 2.500% tras el segundo y un 1.000% tras el tercero halving en 2020, cuando alcanzó el último ATH a 69.000 dólares. En 2024 tuvo lugar el cuarto halving, Bitcoin ya ha alcanzado los 100.000 dólares. A ver hasta dónde puede llegar el precio en este ciclo.



(slide 136) - Bitcoin 4 All

Pero todo lo que sube también baja. Aunque el Bitcoin ha experimentado grandes subidas de valor a lo largo de los años, también ha sufrido caídas.

En 2012 Bitcoin tuvo una caída brutal del 93%. Tras el primer halving cayó un 84%, en el segundo volvió a caer un 84% y en el último halving la caída fue del 77%, inferior a la de los *bears* anteriores. Eso significa que, con el tiempo, el Bitcoin se está volviendo menos volátil. Está lejos de ser una línea recta, por supuesto, pero ya podemos ver esa tendencia.

(slide 137) - Bitcoin 4 All

Lo que también puede observarse es que Bitcoin ha tenido valores mínimos cada vez más altos a lo largo de los ciclos. En 2012 un bitcoin valía menos de un dólar, en 2014 el mínimo ya era de diez dólares, en 2016 de cien dólares, en 2019 de mil dólares y en 2022 de diez mil dólares.

En otras palabras, aunque el Bitcoin caiga mucho, ha mantenido precios mínimos cada vez más altos a lo largo del tiempo. Pero ¿será siempre así? ¿Seguirá aumentando el valor de Bitcoin para siempre?

Este es el tema de la próxima lección. Ahora que ya sabes cómo funciona el Bitcoin y la historia de sus ciclos, es hora de comprender por qué su valor tiende a seguir creciendo a largo plazo. Hasta entonces.