How Bitcoin Works

Al estudiar la historia del dinero encontramos que el sistema económico actual predominante en el mundo tiene a la moneda fiduciaria (fiat) como protagonista. Particularmente es el dólar Estadounidense la moneda usada como reserva de valor junto con el oro físico.

Sin embargo el respaldo del dólar no guarda relación con la cantidad de oro en reserva. La emisión de estos papeles están a cargo de los bancos centrales (Reserva Federal en el caso) y son sus políticas las responsables de que una moneda sea más apreciada que otra: El peso Venezolano pierde su valor con respecto al dólar Americano porque, entre otras razones, se imprimen en mucha mayor cantidad.

El respaldo del dinero fiat hoy no es relación con una cantidad de oro en una reserva de un banco central. Lo que respalda al dinero fiat es la capacidad de los Estados en extraer renta de su población.

Un nuevo paradigma económico

Bitcoin es el culmen exitoso de un largo proceso planteado décadas antes por distintos economistas:

«Separar la economía del poder político»

> Friedrich Hayek en su libro La desnacionalización de la moneda de 1976, expone que en lugar de la emisión de una moneda específica por un gobierno nacional, uso que se impone a todos los miembros de su economía por la fuerza en la forma de moneda de curso legal, las empresas privadas deberían ser autorizadas a emitir sus propias formas de dinero y decidir cómo hacerlo por su propia cuenta. Hoy con Bitcoin (y otras monedas digitales) logran esa libre competencia escapando al espacio de control de los estados.

- Milton Friedman, ganador del premio Nobel de Economía de 1976, fue un estudioso de la dinámica del dinero. A pesar de ser un monetarista (propone que la emisión del dinero sea regulado por el estado) entendió que Internet podría ser el lugar donde existiría la plataforma para que el dinero electrónico funcione como efectivo.
  https://www.youtube.com/watch?v=IDykKZnBXEQ

Existen 3 espacios clásicos sobre los que la humanidad se desenvolvía hasta el siglo XX: tierra, mar y aire. Todos estos son controlados (con la lógica del monopolio de la violencia) por los estados, tanto para el cobro de impuestos o expropiaciones como para su protección. La fuerza militar tiene una especialización para cada una: Ejercito, Marina/Naval y Fuerza Aérea respectivamente.
En este siglo XXI existen otros dos espacios más donde se empieza a tener interacción humana libre: El ciberespacio y el espacio exterior.

- El ciberespacio es ese lugar no físico y sin límites donde existe una red de interconexión global. Mas allá de la infraestructura que representa Internet físicamente, el Ciberespacio es el lugar de interacción digital.
- El espacio (spatium) es aquel lugar más allá de la atmósfera terrestre. Hoy exploradas por empresas privadas.

Estos dos nuevos espacios no tienen Soberanía ni Jurisdicción. En un principio Internet y la exploración espacial eran solamente proyectos militares de estado, hoy su exploración y uso de ambos es también (y predominantemente) privada.

Bitcoin llega a ser el dinero de uso en el ciberespacio por excelencia, pues usa la infraestructura de comunicación de Internet. Tiene un único objetivo que se propuso en el paper que Satoshi Nakamoto (pseudónimo) publicó en 2008:
Bitcoin: A Peer-to-Peer Electronic Cash System

Cabe notar que Bitcoin nace con una filosofía económica detrás. Además de aplicar conceptos de la 'teoría de juegos' que sustentan un razonamiento de incentivos muy estructurado, rígido y regulado por protocolo y el código.

Características de Bitcoin

Bitcoin es una red de computadoras (nodos) que ejecutan un programa llamado Bitcoin-Core. Su activo (lo que funge como moneda) se llama bitcoin o btc, con b minúscula.

Tiene las siguientes características:

1. Las transacciones una vez que son ejecutadas no se pueden anular, cambiar o revertir. Funcionan 24/7.
2. Una vez que se solicita realizar una transacción mediante un nodo esta se propaga inmediatamente en toda la red no puede ser baneada, censurada o modificada por nadie.
3. Solamente el dueño de la clave privada puede aprobar una transacción. Cualquiera puede elevar transacciones (como una suerte de contador que hace cheques, solo tienen validez los que son firmados por el gerente) solo el propietario autoriza transferirlos.
4. No existe bitcoin falsificado. No necesitas conocer a la otra parte que te transfiere. Una transacción es valida si la puedes verificar en un bloque en cualquier nodo.
5. Las transacciones en Bitcoin no solicitan información personal (nombres, edad, género, etc.) es más, no necesitas ser un humano (un programa de computadora puede gestionar una clave privada). Eso no significa que sean anónimas. Las transacciones en Bitcoin son pseudónimas y transparentes para toda la red. Cualquier participante de la red puede ver toda transacción en todo momento.

Funcionamiento

Bitcoin aplica distintas tecnologías ampliamente conocidas que se usan (por separado) hace muchos años.

1. Huella digital HASH
   Particularmente Bitcoin hace uso de dos Hashes 'SHA256' y 'RIPEMD-160'.
2. Criptografía asimétrica o de clave pública.
   Bitcoin utiliza un estándar criptográfico basado en geometría algebraica de curva elíptica ECDSA. Se basa específicamente en el estándar 'secp256k1'.

3. Prueba de Trabajo POW.
   La prueba de trabajo tiene la función de normar el consenso en la red distribuida. Es el mecanismo que transforma la energía del mundo físico en efectivo electrónico. Siendo el centro de la seguridad en la red.
4. Blockchain.
   Blockchain es una forma de expresar una base de datos (al igual que sql, csv o excel) que hace uso del hash para relacionar bloques. Blockchain le otorga a Bitcoin ser tamper-evident. Esto significa que es evidente si alguien realiza una modificación en algún lugar pues el hash sería distinto.

Todas estas tecnologías juntas son la base que permite el funcionamiento de las transacciones en Bitcoin. Le otorgan en conjunto a Bitcoin una cualidad más: tamper-proof. No solo hace evidente que exista un cambio sino que hace virtualmente imposible modificar nada.

Incentivos en Bitcoin

Bitcoin se crea con una lógica de incentivos para el funcionamiento seguro e inmutable de la red.

1. Un bitcoin (1 btc) puede ser fraccionado. Así como 1 dólar se compone de 100 'centavos', 1 bitcoin se compone de cien millones 100 000 000 de 'satoshis' (sats).
2. Se van a emitir menos de 21 millones de bitcoins con el siguiente esquema:
   - ↳ Con cada bloque que se genera en la red se emite una cantidad nueva de bitcoin como recompensa al minero.
   - ↳ Se empieza con una recompensa de 50 btc por bloque, reduciéndose a la mitad cada 210'000 bloques(aproximadamente cada 4 años).
   - ↳ Las transacciones pagan además una comisión (fee) para ser procesadas al minero que generó el bloque. Comisión que no depende del monto a transferir sino del peso de la transacción (que puede pesar desde los cientos de bytes hasta 4 MB) medidos en satoshis/Byte. Mientras mayor sea el fee los mineros lo toman con más prioridad.

Con este script podemos calcular cuantos halvings existirán y cuanto btc se emitirá en total. Podemos saber con precisión el último bloque donde se emitirá bitcoin y estimar la fecha:

```python
from math import trunc
#la recompensa inicial son 50*10^8 sats (50 btc)
recompensa = 50 * 10**8
#un halv ocurre cada 210000 bloques
limite = 210000

btc = 0
halv = 0
blocks = 0
year = 2009


while(recompensa > 0):
   for i in range(0,limite):
      btc+=recompensa
      blocks+=1
   print('Halv: ',halv,end=' | ')
   print('Recompensa (sats): ',recompensa,end=' | ')
   print('Bitcoin emitido (btc): ',btc/10**8,end=' | ')
   print('Bloques emitidos: ',blocks,end=' | ')
   print('Año: '+str(year)+'-'+str(year+3) )
   recompensa=trunc(recompensa/2)
   year += 4
   halv += 1
   x.append(halv)
   y.append(btc/10**8)

print('btc total a emitir: ',btc/10**8)
```

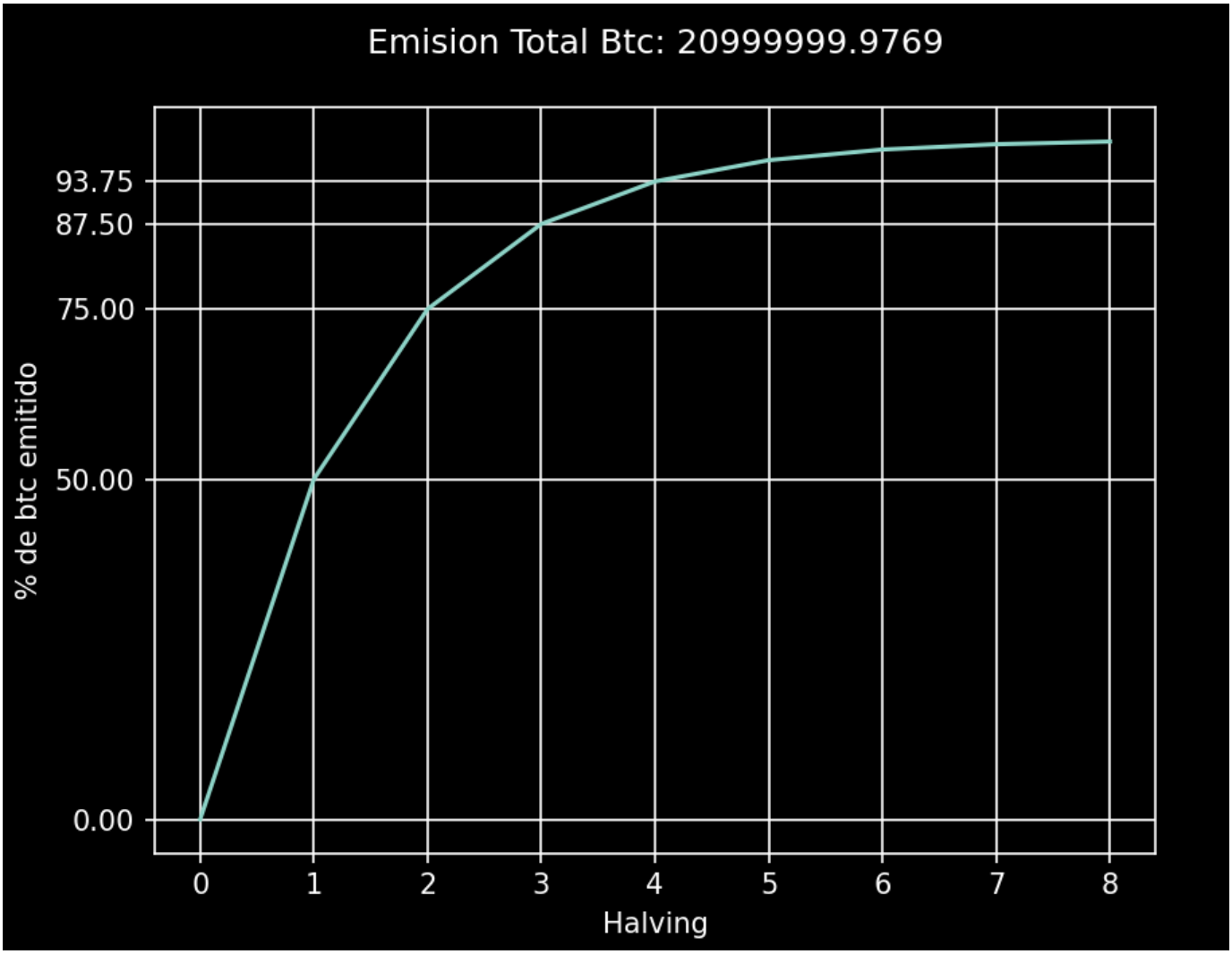
Donde el resultado es:

> **Note**
>
> btc total a emitir: 20999999.9769

```
Halv: 0 | Recompensa (sats): 5000000000 | Bitcoin emitido (btc):
10500000.0 | Bloques emitidos: 210000 | Año: 2009–2012

Halv: 1 | Recompensa (sats): 2500000000 | Bitcoin emitido (btc):
15750000.0 | Bloques emitidos: 420000 | Año: 2013–2016

Halv: 2 | Recompensa (sats): 1250000000 | Bitcoin emitido (btc):
18375000.0 | Bloques emitidos: 630000 | Año: 2017–2020

Halv: 3 | Recompensa (sats): 625000000 | Bitcoin emitido (btc):
19687500.0 | Bloques emitidos: 840000 | Año: 2021–2024
...
```

El límite de emisión estará por el bloque 6'930'000 en el año 2140. En ese momento la recompensa inicial de 5'000'000'000 sats se habrá dividido a la mitad 32 veces, llegando a la mínima unidad de 1 sat.

En el siguiente gráfico se muestra el comportamiento de la emisión. El primer halving minó ~50% de todos los bitcoins, en el segundo ~75%, en el tercero ~87.5%, etc.

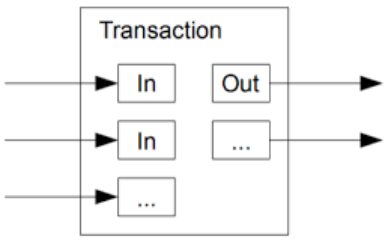


Transparencia de la Red.

Un residuo de realizar transacciones en Bitcoin es su registro en una base de datos contable que llamamos Blockchain. No existe una cuenta, ni un bloque de datos que almacene bitcoins para cada usuario como si fuera una caja fuerte de banco.

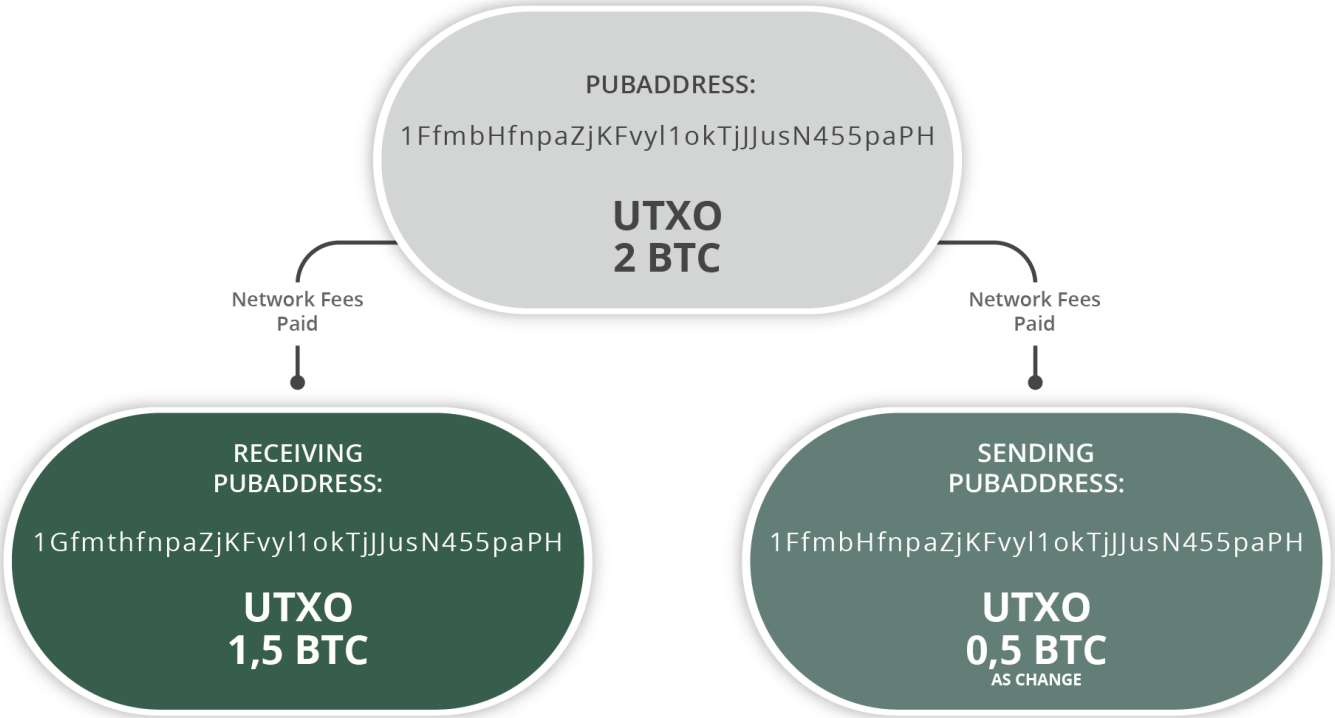
Lo que se almacena en la base de datos son las salidas de transacciones (UTXO) asociadas a una dirección de bitcoin.

Una transacción consta de entradas (in) y salidas (out).



Los UTXO se pueden pensar como monedas. Una vez que se generan bitcoins al crear un bloque se registra quien es el propietario. Cuando este propietario gasta estos bitcoins, en el historial se guarda la nueva dirección del nuevo propietario. En el ejemplo de la gráfica anterior note que el cambio es una nueva salida a la misma dirección.

Como se puede ver en la gráfica cada salida necesita una entrada previa. La única transacción que crea nuevos bitcoins es la recompensa de minero o 'coinbase', es decir, es la única que solo tiene salida. Por esta razón es imposible falsificar bitcoins. A lo mucho se puede intentar falsear la información de pago de UN UTXO.



Cuando decimos que una dirección de Bitcoin tiene una cantidad `x` de btc, nos referimos a la suma total de los UTXO que fueron enviadas a esa dirección.

El precio de hacer trampa

Crear un bloque falso cuesta una cantidad grande de energía (por el POW)

Potenciales puntos débiles

Bitcoin como toda tecnología no es 100% segura. Tiene ciertos puntos débiles que pueden significar un problema para su adopción.

1. Colisiones HASH-SHA256

El hash sha256 es un algoritmo que obtiene una huella digital a partir de un archivo. Una colisión ocurre cuando dos archivos distintos generan un mismo hash. Esto ya paso con la familia SHA-1 por parte de ingenieros de Google. Lograrlo en la familia SHA-2 por ahora es virtualmente imposible.

Sin embargo, de ser posible la colisión tenga en cuenta:

- La huella digital de un archivo se puede entender como la huella de un pulgar.
- Que dos archivos tenga una misma huella sería el equivalente a que un 'humano' de varias manos y extraña fisiología tenga una misma huella en un pulgar que una persona normal.

2. Ataque del 51%

Un ataque del 51% es algo que en el mismo bitcoin paper menciona como una vulnerabilidad a su propuesta de consenso en la red, la prueba de trabajo POW.

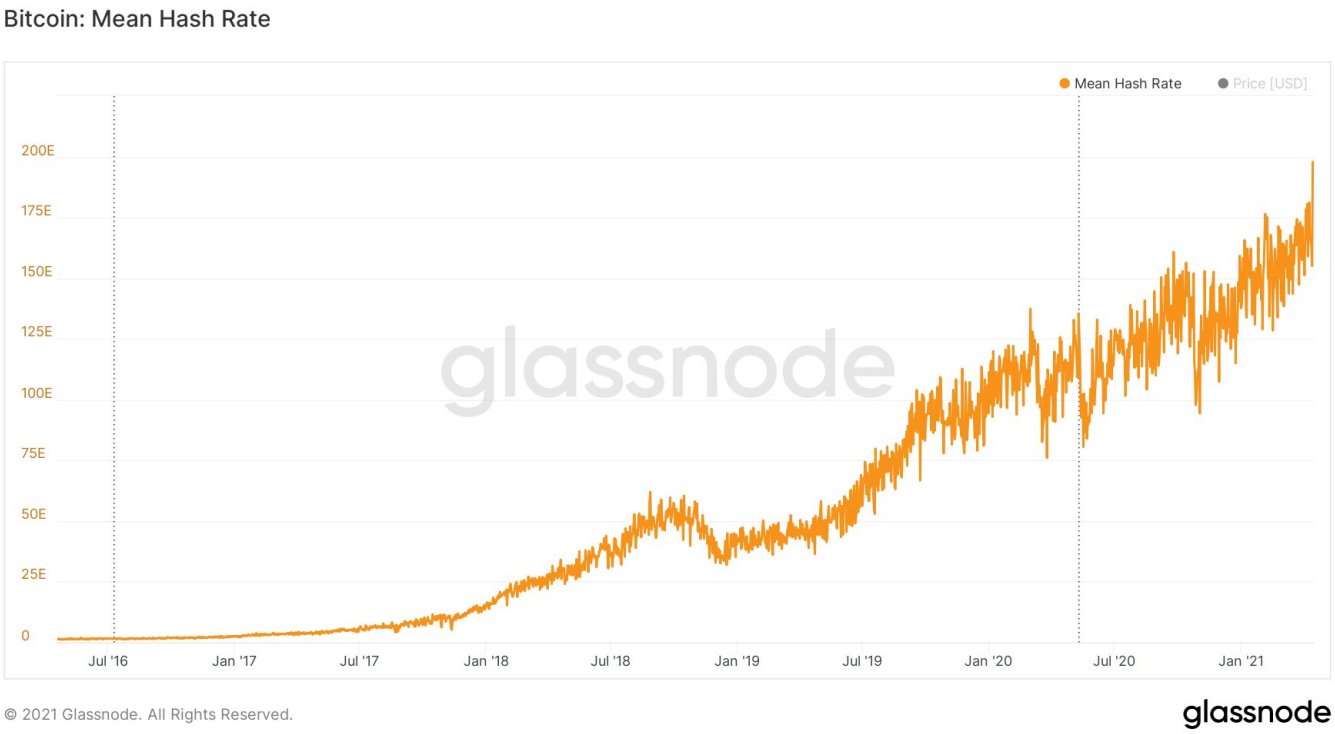
Bitcoin fue un proyecto que ha crecido y se ha desarrollado en bajo perfil durante su primer periodo. Año a año el poder de la red Bitcoin ha ido creciendo distribuyéndose en todo el mundo.

Reportes especializados arrojan cierta data sobre la descentralización del poder de hash rate mundial y como se distribuye geográficamente.

- 1. Estados Unidos: 37,8 %
- 2. China: 21,1%
- 3. Kazajstán: 13,2%

- 4. Canadá: 6.5%
- 5. Rusia: 4.7%
- 6. Alemania: 3,1%
- 7. Malasia: 2,5%
- 8. Irlanda: 2%
- 9. Tailandia: 0,96%
- 10. Noruega: 0,74%

Bitcoin ya cruzó un Umbral donde la misma disponibilidad de Hardware hace muy difícil tener dominancia en el mercado. El Hash Rate global se encuentra en su máximo histórico.



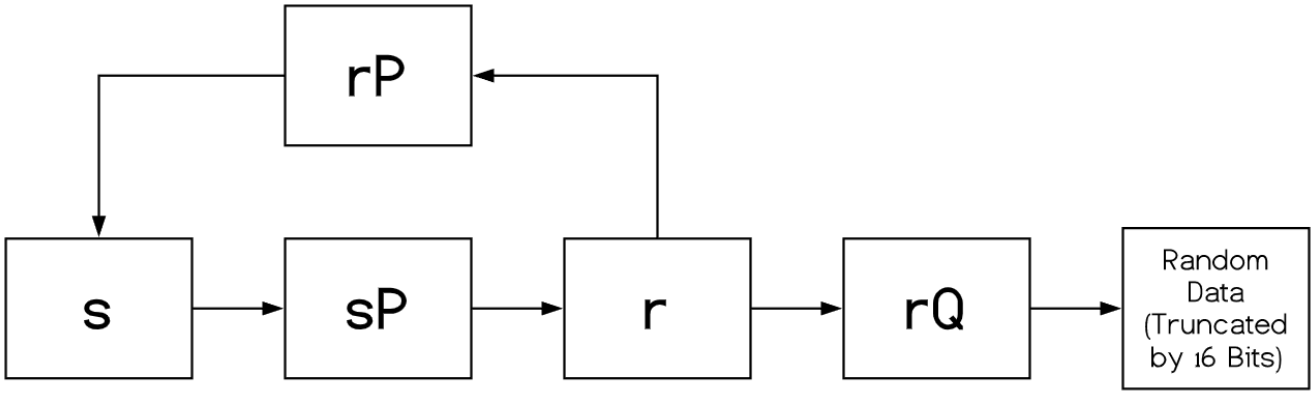
3. Backdoor Criptográfico

EC DRBG

Con el desarrollo de distintas técnicas y aplicaciones criptográficas se propusieron estandarizar herramientas que serían de uso masivo en Internet.

Una de estas herramientas era un generador randómico de números propuesto por el NIST y la NSA en los 90s:

'The Dual Elliptic Curve Deterministic Random Bit Generator'.



Sin entrar en mucho detalle se trata de un generador de números aleatorios aplicando curvas elípticas. Estos números se usaban como base para todo tipo de aplicaciones que usamos hoy en Internet (Navegadores Web con ssl, sistemas operativos win/unix, BlackBerry).

En 2004 se publica en ANSI X9.82 y en 2005 se publica en la ISO 18031.

En 2007, investigadores de Microsoft Shumov y Ferguson encuentran vulnerabilidades a este estándar y lo comparten en una crypto conferencia.

Si bien no se tiene confirmaciones oficiales y se lo toma como una especulación, en 2013 Snowden reveló la existencia de herramientas que podrían vulnerar el cifrado de Internet. El mismo 2013, RSA (Rivest, Shamir y Adleman) publica que deja de usar EC DRBG. En 2014 el NIST quita como algoritmo criptográfico estándar EC DRBG.

Bitcoin Secp256k1

Cuando se propuso el Paper de Bitcoin existían otros estándares más 'eficientes' y estudiados en la aplicación de cifrado mediante curva elíptica. Satoshi hace la elección en la familia 'Secp256k1' por una razón (pienso):
– Eficiencia.

Esta elección es notable, pues otra familia tenía mayor aceptación en el medio en esa época (2009): Secp256r1.

Ambas curvas son similares con al diferencia que los puntos generadores se obtienen de manera distinta. La familia Secp256 Con 'r' se generaron de manera aleatoria. Si bien podría tener alguna vulnerabilidad no se ha reportado.

En cambio la familia Secp256 con 'k' se llama así por la curva de Koblitz que está especialmente diseñada para multiplicaciones escalares más rápidas. Por lo tanto, las operaciones (de firma, verificación y generación de claves) en Secp256k1 son más rápidas que las de Secp256r1. Los parámetros de la curva de Koblitz están determinados matemáticamente, y hay pocas posibilidades de establecer tal puerta trasera.

4. Computación Cuántica

Los ordenadores se pueden entender como máquinas que realizan un procesamiento de Información. Este procesamiento puede ser mecánico, analógico/digital (electrónico) o cuántico.

Cada una de estas formas resuelve de forma particular ciertos problemas. Por ejemplo las computadoras mecánicas para predecir mareas.

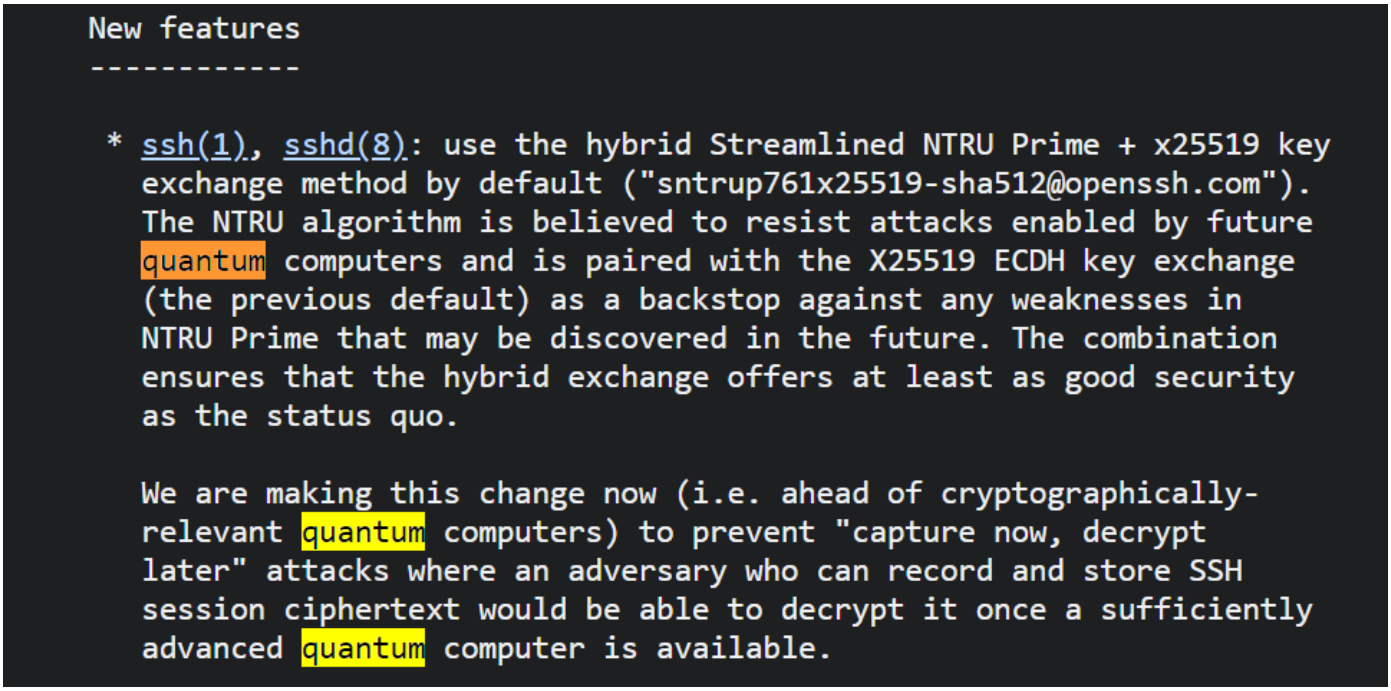
El calculo del HASH SHA256 se lleva de manera más eficiente en computadores analógicos (ASICS) que en digitales (GPU's u Ordenadores). Pero el software de Bitcoin Core funciona sólo sobre computadores digitales.

Las computadoras cuánticas tienen usos aún muy reducidos (no resuelven problemas en general) para algoritmos que aplican la matemática que modela procesos cuánticos. Se publican algoritmos que resuelven las técnicas de criptografía (RSA) pero aún no existe la capacidad computacional para romper cifrados que se usan hoy (más de 2000 bits). Además que la escalabilidad del hardware para computación cuántica no obedece a la ley de crecimiento exponencial cada dos años (Ley de Moore), es más, tiene el peor indicador de escalabilidad comparada con otras tecnologías.

Aún no se conoce ninguna propuesta o algoritmo cuántico que rompa el cifrado asimétrico por Curva Elíptica. De darse en un futuro (lejano) puede representar un tema que genere debate para actualizar el protocolo y hacerlo resistente a la computación cuántica. Otros

protocolos como SSH ya implementaron cambios para resistir algoritmos cuánticos que podrían romper su cifrado en un futuro.

https://www.openssh.com/releasenotes.html



```
New features
------------

 * ssh(1), sshd(8): use the hybrid Streamlined NTRU Prime + x25519 key
   exchange method by default ("sntrup761x25519-sha512@openssh.com").
   The NTRU algorithm is believed to resist attacks enabled by future
   quantum computers and is paired with the X25519 ECDH key exchange
   (the previous default) as a backstop against any weaknesses in
   NTRU Prime that may be discovered in the future. The combination
   ensures that the hybrid exchange offers at least as good security
   as the status quo.

   We are making this change now (i.e. ahead of cryptographically-
   relevant quantum computers) to prevent "capture now, decrypt
   later" attacks where an adversary who can record and store SSH
   session ciphertext would be able to decrypt it once a sufficiently
   advanced quantum computer is available.
```

5. Hacking The Code

El código de Bitcoin Core se encuentra libremente en Internet, por ejemplo se encuentra en este repositorio:

https://github.com/bitcoin/bitcoin

La totalidad del código esta disponible para que cualquier usuario pueda leerlo, cambiarlo o ejecutarlo. En un principio fue publicado únicamente por Satoshi Nakamoto. Hoy existe una comunidad global que realiza auditorias y estudios en el código proponiendo mejoras (BIP Bitcoin Improvement Propossal) y algunos (pocos) desarrolladores tienen a cargo el mantenimiento del software, de aceptar la propuesta de cambios. Precisamente son 6 personas que se sabe pueden firmar (con PGP) algún cambio en el código y publicarlo.

Para que exista un total efecto en toda la red, todos y cada uno de los nodos debe instalar de nuevo Bitcoin-Core con el parche reciente.

Por lo que suponiendo que una (o todas) de estas 6 personas que pueden hacer cambios usando sus firmas PGP en Bitcoin Core intenten un ataque malicioso (podríamos imaginar el extremo de una conspiración

global) es muy difícil que los nodos distribuidos en todo el mundo, acepten de buena gana hacer el cambio.

Realizar un cambio en Bitcoin Core puede llevar a resultados inesperados. Y pasar la barrera humana de implementarse en cada nodo es muy difícil.

Soft Fork

Un soft fork es una actualización en el código de Bitcoin Core que añade un cambio, pero sigue siendo compatible con una versión anterior.

Por ejemplo, la actualización de Bitcoin Core para agregar SegWit (Segregated Witness). Se activó a una altura de bloque 481'822 con una aceptación en la red de ~99.95%. Los nodos que no actualizaron para usar SegWit, aún pueden seguir operando normalmente.

Hard Fork

Un Hard Fork es un cambio en el código que vuelve incompatible la operación entre nodos con una versión anterior.

Se crea una nueva cadena de bloques y los nodos que se actualizan forman parte de otro nuevo blockchain. Esto podría darse de manera deseada (para crear otros proyectos como Bitcoin) como también ser un comportamiento no deseado (al elevar un cambio en el código de Bitcoin Core).

Existen varios hard forks de Bitcoin:

- 2014 Bitcoin XT – Proponía aumentar el tamaño de bloque de 1 MB a 8 MB. Ya no esta disponible.
- 2016 Bitcoin Classic – Intento de seguir con el proyecto Bitcoin XT. Hoy sigue existiendo.
- 2016 Bitcoin Unlimited – Propone un bloque de 16 MB. Sin aceptación popular.
- 2017 Bitcoin Cash – El hard fork que más éxito tiene propone no adoptar SegWit pero aumentar el tamaño de bloque a 8 MB.
- 2017 Bitcoin Gold – Este proyecto busca hacer que la minería de Bitcoin sea mucho más accesible.

6. Regreso al Patrón Oro

Una forma de tener un competidor a Bitcoin como dinero es que los estados decidan anclar su emisión monetaria a la existencia de Oro. Y que tenga libre movimiento tanto en portación como transferencia.

Esto supondría una coordinación controlada de muchos gobiernos distintos. Algo que (en una opinión personal del autor) no veo muy probable.

7. Destrucción de Internet

Bitcoin funciona sobre la infraestructura global de Internet. Los nodos se encuentran distribuidos en todo el mundo.

Tendría que existir una catástrofe sin precedentes que deje a todos los aparatos electrónicos inútiles en todo el Mundo. En caso de existir un ataque en escala global el último problema sería transmitir valor. Es un escenario muy fantasioso.

También cabe mencionar que existen nodos completos distribuidos en distintos satélites.

Se puede descargar todo el Blockchain usando una antena.