Hacer una transacción con Bitcoin es uno de esos pequeños placeres que nos trajo esta era moderna de internet. Poder enviar o recibir una cantidad de valor desde la comodidad de tu sala o habitación a cualquier parte del mundo, a cualquier hora, cualquier día de la semana sin la necesidad de un intermediario vigilando. Simplemente fascinante.

¿Parece de ciencia ficción, no es así? Pues yo creo que va más allá de eso.

Comparemos esto con una de las películas ambientadas en el futuro con una de las formas de pago más peculiares: *“El Precio del Mañana”*. Allí corre el año 2161, la moneda de cambio es el tiempo y para hacer una transacción tienes que hacer contacto con el antebrazo de la contraparte.

Aunque no podemos negar que eso se vería muy cool, lo cierto es que ya desde 2009 bitcoin es superior debido a su capacidad de hacer pagos *contactless*, algo impensable para alguien en 2011, año en que salió la película.

Pese a las diferencias entre ambas formas de pago, hay algo que sí comparten: el factor magia. *¿Acaso no sería algo mágico hacer una transacción con alguien con tan solo tocar su antebrazo?* *¿Que acaso no fue sorprendente la primera vez recibiste unos satoshis en tu wallet en apenas unos minutos?* Ambas experiencias reafirman la frase del escritor Arthur C. Clarke: *“Cualquier tecnología suficientemente avanzada es indistinguible de la magia.”*

Aunque nosotros no somos magos sino estudiantes que les apasiona la tecnología, hoy vamos a crear un truco: hoy vamos a convertir en conocimiento lo que para otros es indistinguible de la magia; hoy estudiaremos el proceso de una transacción en la **blockchain de bitcoin**.

**Ejecutando una transacción**

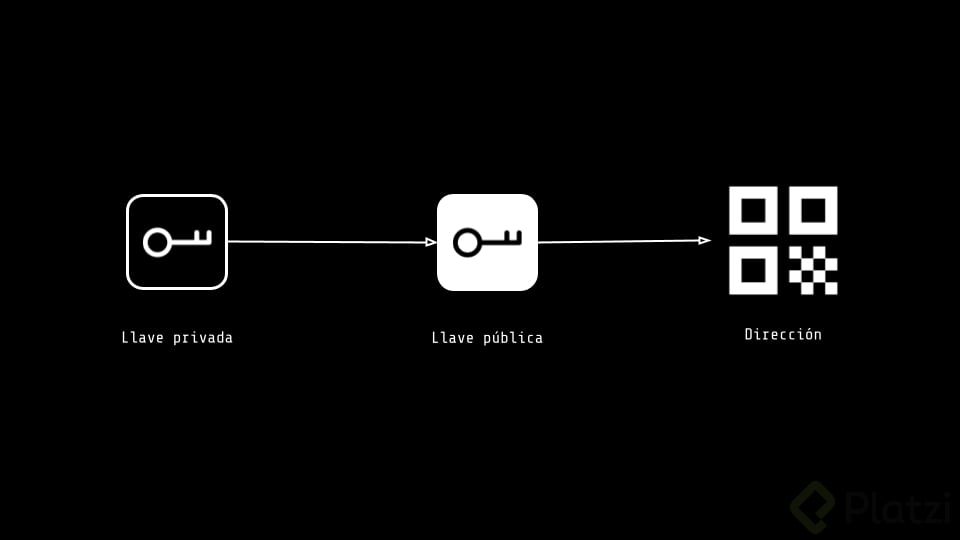
Comencemos explorando un paso a la vez y partiendo desde tu punto de vista; la ejecución de la transacción.

Imaginemos un escenario donde deseas realizar un pago en un restaurante que acepta Bitcoin. El que el monto a pagar es de 5 dls. Tomas tu celular, abres tu wallet, escaneas el código QR que viene con tu cuenta, verificas que todo sea correcto y presionas el botón de pagar. Tu ni siquiera lo notaste pero tu wallet hizo una serie de pasos por ti. Veamos cada uno de ellos.

Conoce más: [¿Qué es y cómo funciona Chivo Wallet?](https://platzi.com/clases/2378-bitcoin-salvador/39725-que-es-y-como-funciona-chivo-wallet/)

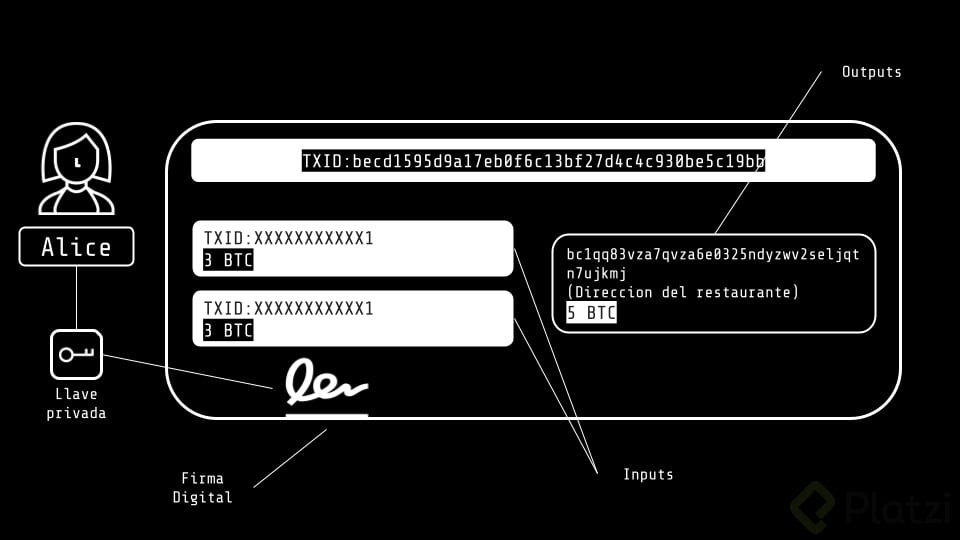
La primera funcionalidad de la que hiciste uso en tu wallet fue el almacenamiento de tu **Llave Privada**, llave con la que autorizaste tu transacción. Esta te fue dada la primera vez que la iniciaste en tu dispositivo móvil y para su respaldo se te otorgó una serie de 12 a 24 palabras conocidas como **Semilla Mnemotécnica**.

Esta llave privada fue la que generó una **Llave Pública**, que a su vez generó una **dirección** en la cual pudiste recibir los bitcoins pudiste gastar.



Lo siguiente que hizo tu wallet fue el armado de la transacción, la cual se compone de inputs y outputs, los cuales lleno de la siguiente manera:

Dentro de los **inputs** colocó una o más referencias a transacciones con outputs con saldo a tu favor dentro de la blockchain. A estos se les conoce como**UTXO’s** o *Unspent Transaction Outputs*. El monto acumulado en esta sección debe ser equivalente en bitcoin a 5 dlls o más. Por otro lado, en la parte de los **outputs** coloco la dirección del destinatario, el restaurante, y la cantidad a pagar.



¿Recuerdas que dijimos que el monto en los outputs debe ser superior a 5 dls? Esto es una regla general, ya que el saldo restante lo tomarán los mineros como la **comisión de la transacción**. Esto quiere decir que si el monto de los inputs suma un total de 6 dlls y el de los outputs 5, la comisión de la transacción será de 1 dólar.

Una vez que la wallet realizó lo anterior, solo esperó a tu confirmación con el botón de pagar y finalmente transmitió la transacción a un nodo. A partir de aquí no hay mucho que puedas hacer, solo esperar a que tu transacción entre un bloque lo más pronto posible. Veamos que sucede hasta que esto ocurre.

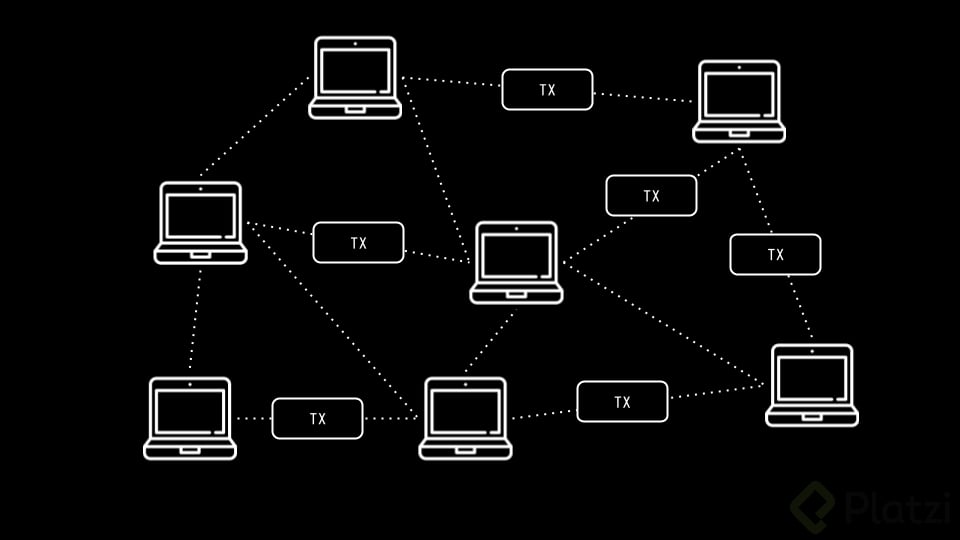
**El trabajo de un nodo**

En cuanto tu transacción es enviada es recibida por el nodo más cercano, es decir, al que tu wallet está conectado. El **nodo** es quien valida las transacciones y lleva el registro de toda la **blockchain** en memoria (más de 500 gb al momento de escribir esto), incluyendo la transacciones pendientes. Cada uno está conectado a su vez con otros nodos dentro de la red a través del protocolo TCP/IP.

La mayoría de las wallets mantienen sus propios nodos pero aun así te dejan la opción de conectar el tuyo propio, lo cual siempre es lo ideal.

En este caso, lo primero que hará el nodo receptor es validar la transacción, es decir, verifica que tu

**firma** es válida para gastar los inputs de la transacción y verificar que estos vienen de una *Coinbase Transaction*(este término lo definiremos en la sección de mineros). Si todo está correcto, mandará la transacción al\*\*\*Mempool\*\*\*, que es una especie de limbo de transacciones que no han sido incluidas en un bloque. Finalmente, la transacción es propagada hacia otros nodos para que realicen el mismo procedimiento.



Todos y cada uno de los más de 13,000 nodos que existen en la red de bitcoin deben de hacer el procedimiento anterior, hasta que todos tengan la transacción en el Mempool. Por ahora, la labor de los nodos ha terminado y a partir de aquí los mineros son los que entran en acción.

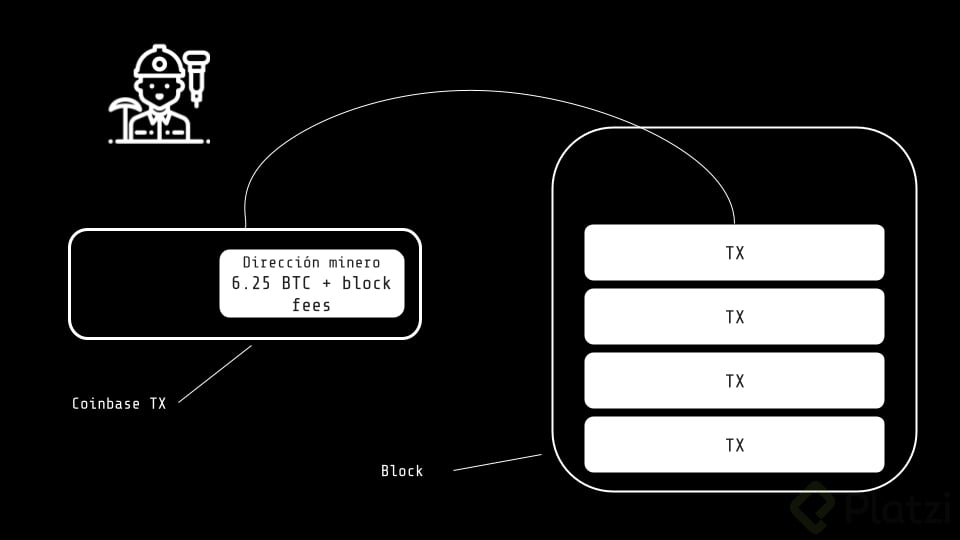
**La minería; dando seguridad a la red**

En definición, una persona que **mina** es todo aquel participante en la red de bitcoin que se encarga de **armar los bloques** y asegurar la red realizando la ***Prueba de Trabajo*** o Proof of Work. Veamos en qué consisten estas dos tareas.

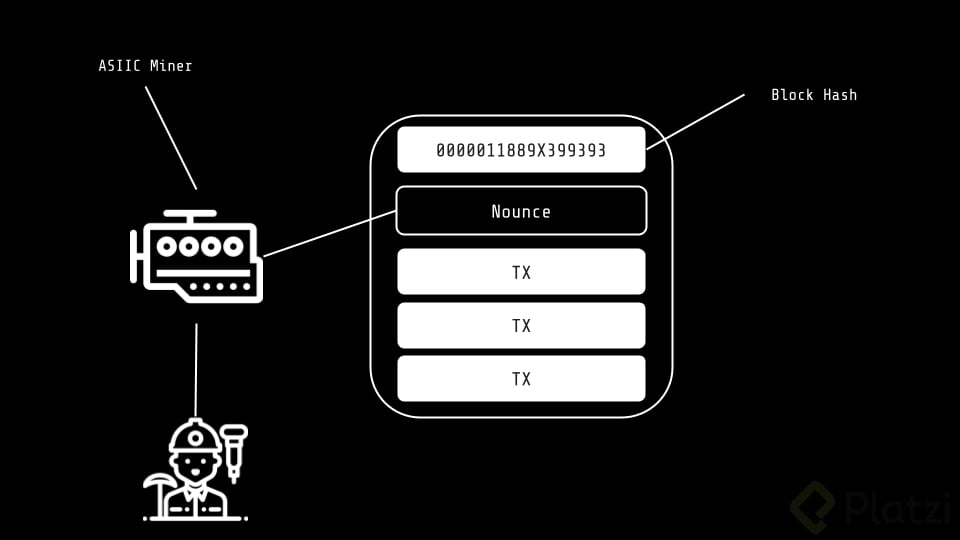
Una vez que tu transacción fue propagada por toda la red, los mineros, los cuales están conectados a un nodo, acomodan el mempool en forma de pila. Esta pila es ordenada de mayor a menor según el monto de comisión de la transacción. Esto quiere decir que las transacciones que tienen un mayor monto de comisión irán en la cima de la pila y formarán parte de un bloque de inmediato, por otro lado las transacciones con menor comisión irán detrás de estas.

Después que el mempool es ordenado, es hora de armar el bloque. Para llevar a cabo esta tarea, los mineros toman transacciones de la pila del mempool y las ponen en el bloque hasta que pese, máximo, **1 megabyte**. Posteriormente, el minero agregara una transacción extra: la **“Coinbase Transaction”**, un UTXO a su favor con las recompensas del bloque.

El monto de la CoinbaseTX está compuesto por dos cantidades, el *Subsidio del Bloque* y las *Comisiones del Bloque*. El **“Subsidio del Bloque”** corresponde a los bitcoins que son creados por default por la red cada vez que se crea un bloque. Actualmente este monto es de 6.5 bitcoins. Mientras tanto las “**Comisiones del Bloque**” son todas las comisiones de cada transacción dentro del bloque juntas.



Antes de comenzar a minar, el minero deberá agregar información adicional que servirá para identificar el bloque: el *hash del bloque anterior*, el *número del bloque*, la *raíz de merkle*, el *timestamp* y el *nonce*. A esta información se le conoce como **“Block Header”**. Una vez agregados estos datos, es hora de comenzar el proceso de minado.



**Minar** no es otra cosa que el proceso de ajustar el nounce del header y pasar el bloque por el **algoritmo de hash** **SHA-256** hasta que cumpla la dificultad que la blockchain exige para que este sea válido. La dificultad podemos medirla visualmente por el número de 0’ s que tiene un string dado por el algoritmo. Este string es conocido como **“Target Hash”.** Por tanto, para que un bloque sea válido lo único que tiene que hacer es tener una cantidad igual o mayor de 0 ’s al inicio de su hash. El primero en lograrlo puede transmitir su bloque y quedarse con su recompensa del mismo.

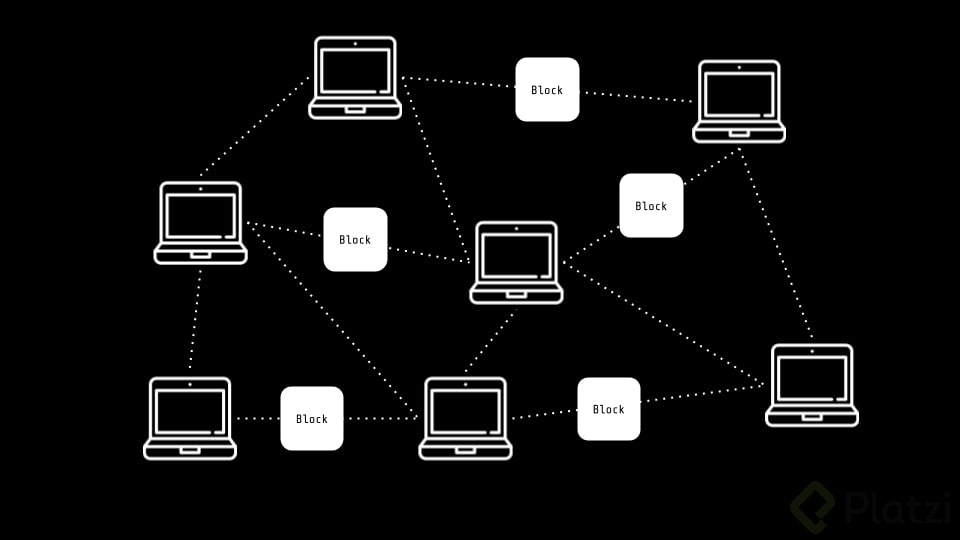
Target Hash:

$ bitcoin-cli getblocktemplate '{"rules": ["segwit"]}' | grep target

"target": "0000000000000000000e26320000000000000000000000000000000000000000",

Ya sé, suena sencillo, pero entre más 0 ’s tenga el Target Hash, más difícil es. Por ello, actualmente para lograr minar un bloque necesitas una granja de minería.

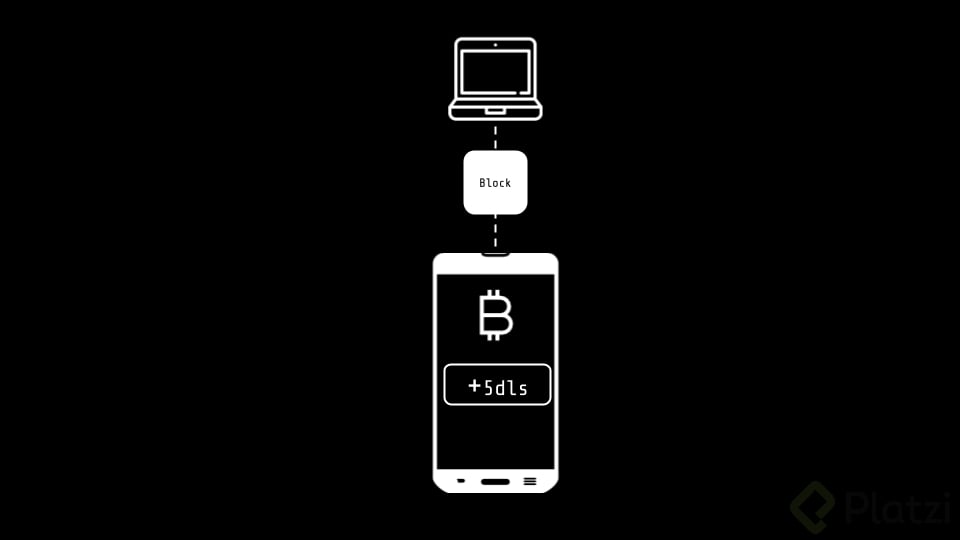
Para que el minero pueda reclamar sus recompensas del bloque este debe formar parte de la blockchain, por lo que debe transmitirlo apenas haya resuelto la Prueba de Trabajo. Esta transmisión se da a través del nodo donde obtuvo el mempool, el cual se encarga también de verificar las transacciones y el Target de dificultad del bloque. Si el bloque no presenta ninguna anomalía lo retransmite a los demás nodos, los cuales repiten el proceso de verificación.



Esta **propagación** dura apenas unos segundos por lo que llegará inmediatamente al nodo conectado a tu wallet.

**“Houston, hemos aterrizado”**

Mientras lo anterior sucedía, tu wallet estaba esperando una señal del nodo, hasta que finalmente, te manda una notificación: tu transacción tiene **1 confirmación**. Esto significa que fue incluida en el último bloque minado, por tanto se actualizo tu balance con 5 dolares menos y el de tu destinatario con 5 dolares mas.



Y listo, ahora ya puedes dejar el establecimiento pues la transacción ya está en la blockchain.

Ahora ya conoces los fundamentos y conceptos claves como *nodo*, *minero*, *mempool* o *wallet* dentro de blockchain plasmados en el contexto más común: una transacción. Con esto en mente ahora tienes una imagen mental de cómo funciona el algoritmo de bitcoin.

**Conclusión**

En Platzi además, tenemos una comunidad increíble de **Cryptocositas**. En dónde nuestra misión es aprender juntos día a día. Sin consejos de inversión, sin tomar el camino fácil, compartiendo con todos nuestro conocimiento y siendo parte de este ecosistema que va más allá del #hold o #tothemoon sino de la posibilidad de ser parte de una tecnología que está y va a revolucionar el mundo.

Si quieres unirte solo debes entrar [acá](https://t.me/joinchat/WPAsE3WGkKxHvTQr), seguir las reglas de la [comunidad](https://platzi.com/conducta/) y prepararte para nunca parar de aprender.

Recuerda que también tenemos el [Curso de Bitcoin y Blockchain](https://platzi.com/cursos/bitcoin-blockchain/) donde podrás aprender mucho más de esta criptomonedas y muchas más cosas sobre las diferentes blockchains.

Es muy probable que todavía tengas muchas dudas, por eso dejamelas en los comentarios y con gusto las responderé.