Last Update: jueves 10 noviembre 2022 18:32:15

Bitcoin

Bitcoin es un proyecto que busca solucionar un problema en concreto:

> «la transferencia de dinero electrónico de persona a persona (p2p)».

Dejando de lado qué es dinero/moneda y qué es valor/precio explicamos esta problema desde un punto de vista práctico.

Pagos en efectivo

Tradicionalmente para realizar la compra/venta usamos papel moneda como dólares o bolivianos. Al realizar un pago **solo se exige que los billetes o monedas se encuentren en buen estado y que obviamente no sean falsificados**. Estos billetes se diseñan y fabrican de manera de que no sean nada fáciles de falsificar y las autoridades castigan con cárcel (pues es un delito) a quienes traten de defraudar circulando billetes falsos. La gente en muchos países pagan impuestos que financian:

- A los policias e investigadores que tienen el trabajo de vigilar la existencia de falsificaciones.
- El material, diseño, fabricación del papel especial, impresión o acuñación y la reposición (si se daña) del billete/moneda circulante.

Cada billete tiene sus propias caracteristicas de seguridad que permiten verificar si son falsos de manera fácil:

- Bandas de un material especial que refleja la luz.

- Sellos que son visibles a contra-luz.
- Relieves en marcas.

Un ejemplo de empresas especializadas a las cuales distintos países recurren para aumentar la seguridad de sus billetes.

https://www.kinegram.com/en/protecting-banknotes/

Una vez que el pago en efectivo es aceptado no se necesita mayor información que el monto a pagar. La señora que vende dulces no tiene interés en saber el número de cuenta, nombre, dni.

La compra/venta directa y al contado es preferida por sobre otras formas de pago com aceptar el pago en cuotas (deuda), cheque u otros métodos financieros que involucra dar mayores datos (nombres, nro cuenta) para ser aceptado.

Sin embargo el riesgo de ser estafado por una falsificación, sufrir un hurto o dañar accidentalmente el dinero siempre existe. Bajo determinados contextos se puede acudir al ente que los emite (Bancos Centrales) para que puedan tomar una solución.

Pagos digitales

Tener dinero en efectivo y disponible todo el tiempo puede resultar problemático cómo cuando se maneja una cantidad grande, resulta poco práctico portarlo. La llegada de la tecnología permitío el uso de dinero electrónico en vez de dinero en efectivo para facilitar el movimiento económico.

El dinero deja de ser un papel o moneda físico y tangible para ser representado por un número digital en un ordenador. Internet permitió la interconexión de ordenadores en una red global pero no fue diseñada para ser una plataforma para desarrollar economía, por lo cual esta tuvo que adaptarse para funcionar sobre Internet.

La seguridad es un problema muy recurrente en Internet y el principal problema que se enfrenta una red de ordenadores de por ejemplo un banco, es ser infectado por un virus y convertirse en un punto silenciosamente malicioso.
La única forma que se tenía para solucionar este problema de

seguridad en Internet pasaba por entregar cada la decisión de cada acción a un ente único que lo regula.

Para solicitar el pago electrónico el banco solicita (todo automátizado en un cómodo software) toda la información vínculada como nombres, números, monto, saldos en cada cuenta, etc y la ejecuta si la considera procedente. Guardando y manteniendo un registro de cada movimiento.

Es una desventaja depender de un tercero (en este caso el banco) a cambio de la fácilidad de hacer un pago sin efectivo.
Por obvias razones el funcionamiento esta limitado por las caracteristicas de cada banco; limites de transferencia, costos de operación, horarios de atención, etc. El riesgo de sufrir un robo o tener un error puede mitigarse mediante este punto central que hace la verificación de cada movimiento. Este tiene el poder de bloquear una transacción, revertirla o confiscarla en cualquier momento.

Por lo cual la confianza en el uso de dinero electrónico esta ligada a la confianza en la institución bancaria que la gestiona: si tiene buenos sistemas de seguridad, si invierte en constantes y exhaustivas auditorias para encontrar errores, si tiene un seguro en caso de fallar, etc.

Un banco que tenga menos problemas de robos, hackings y funcione la mayor parte de tiempo tendrá mas usuarios. Estos compiten con otros servicios de intermediación como paypal o mercado libre que funcionan con la misma lógica de un punto central que decide cada movimiento.

BITCOIN LA INNOVACION

Bitcoin se propone como una solución alternativa de transferir dinero en un medio inseguro como Internet sin la necesidad de un punto central.

Al igual que en el ejemplo de una red de computadoras de un banco, que tenía un computador central con el poder de decidir sobre los demás ordenadores de otras sucursales que realizan las solicitudes, en bitcoin cada computadora de su red se considera un

banco completo. No existe una jerarquia ni diferencia entre ordenadores. No existe diferencia para la red que un nodo o punto sea una computadora básica (de recursos muy limitados) o un super ordenador. Para Bitcoin ambos tienen el mismo peso dentro de la red.

Entonces nace la pregunta:

> ¿Cómo evita bitcoin corromperse si pueden existir nodos maliciosos sin saber cúales explícitamente?

La solución que brinda Bitcoin representa una innovación disruptiva. Tomando distintas herramientas antes conocidas crea una nueva tecnología descentralizada y presente en cualquier lugar del mundo con una característica distintiva:

«Cada transacción es inmutable, una vez solicitado no se puede censurar y una vez ejecutada no se puede cambiar ni corregir ni anular ni devolver»

Para llevar a cabo esta característica, Bitcoin propone que cada computador que se una a esta red cumpla una serie de reglas para tener un concenso sin un punto central:

- Las transacciones se almacenan en texto plano dentro de "bloques" de 1 MB en promedio de tamaño.
- Los bloques deben tener una firma digital válida y esta se obtiene mediante un procedimiento computacional que se resuelve cada 10 min. en promedio. A este proceso se le llama minería y es una competencia entre todos los nodos que solucionan el procedimiento computacional para añadir nuevos bloques. Mientras más poder de procesamiento van teniendo los ordenadores y circuitos, la complejidad del procedimiento computacional aumenta (o disminuye) con ellos de manera que en promedio siempre demore los mismos 10 min. en producir un nuevo bloque.
- El premio por ganar esta competencia en generar nuevos bloques se paga con bitcoins. Inicialmente se entregaban 50 unidades por cada bloque con la promesa de ir reduciendo la mitad cada 4

años aproximadamente. En el año 2140 se calcula que la recompensa convergerá a cero y se terminen de emitir bitcoins.

- Desde el momento de la emisión del primer bloque en 2009 hasta el último con recompensa en 2140 llegarán a sumar 21 millones de bitcoins. No van a existir ni más ni menos.
- Cada ordenador debe validar todas las transacciones (comprobando su firma digital) y tener una copia verificada desde el primer bloque hasta el último actualizado. Esto significa que cada una de las transacciones es libre y pública para que cualquiera pueda verlo. Como una analogía, es como tener un registro de todas las manos por las que circuló una moneda desde el momento en que fue acuñada.
- Bitcoin utiliza 'direcciones' para mandar/recibir las monedas que ya se han emitido mediante mineria. Haciendo una analogía es como el correo cuando mandas una mail. Las direcciones son virtualmente infinitas y no exigen ningún requisito para tener una, la puede tener una persona (sin importar edad, sexo, etc), un programa y hasta una máquina.

El procedimiento computacional es un calculo simple de verificar pero muy dificil de obtener. Este se suele llamar "prueba de trabajo (PoW proof of work)" y es la forma en que se coordinan todos los participantes.

Finalmente,