“Blockchain: Registros, criptomonedas y usos comerciales”

INTRODUCCIÓN

… DE LAS CRIPTOMONEDAS AL BLOCKCHAIN …

Una **criptomoneda o criptodivisa** es definido como un medio digital de intercambio.

bitcoin

Litecoin

Ethereum

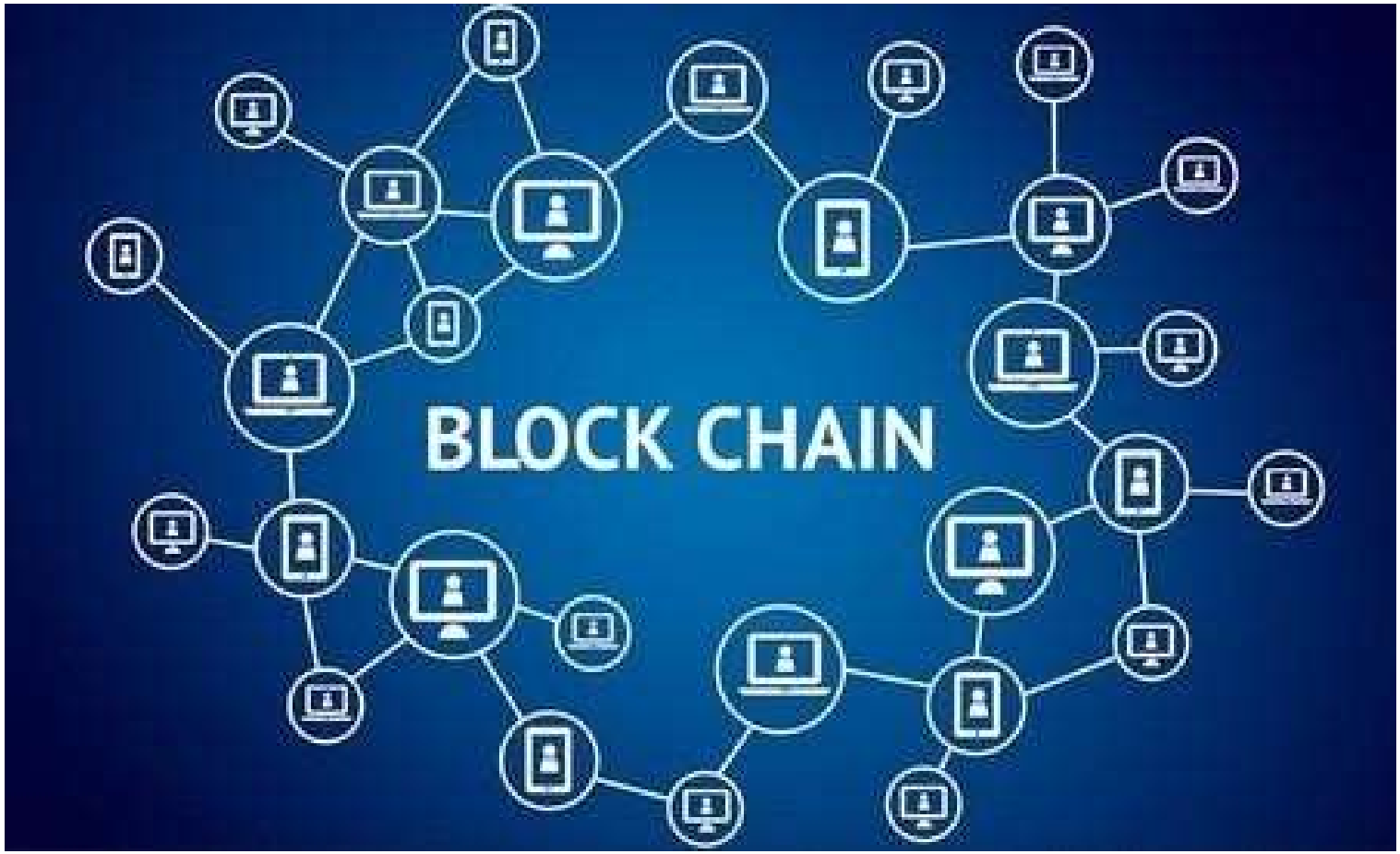
Ripple

EL ESTABLECIMIENTO DE UN LIBRO DE REGISTROS

Es necesario un

Libro de Registros mundial

¿CUÁL ES LA TECNOLOGÍA UTILIZADA EN LA REGISTRACIÓN DE LAS CRIPTOMONEDAS?

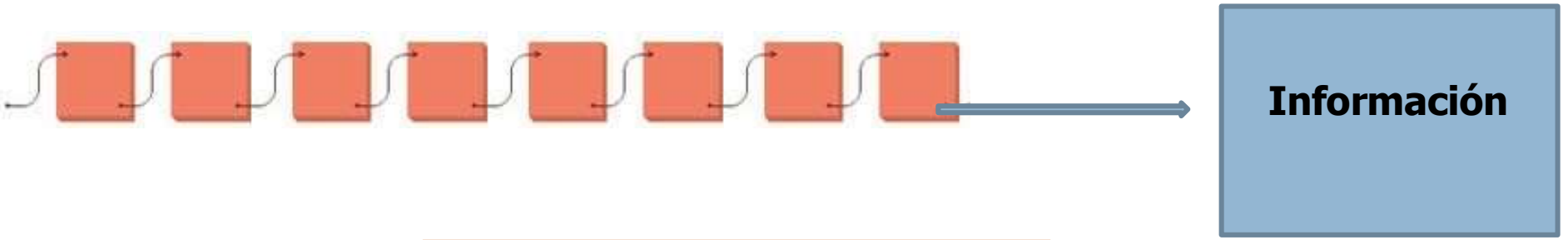


La “blockchain” o “cadena de bloques”.

CONCEPTO DE BLOCKCHAIN

La cadena de bloques es una base de datos que puede ser compartida por una gran cantidad de usuarios en forma peer-to-peer.

Permite almacenar información de forma inmutable y ordenada.



Es una Base de Datos pública.

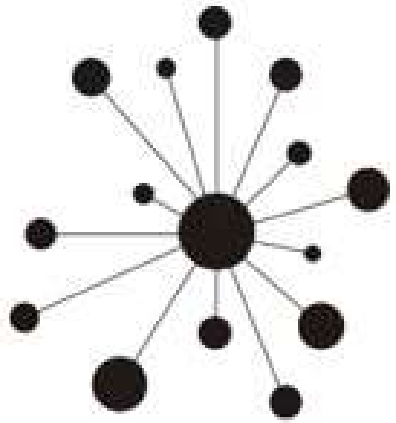
En el caso de bitcoin, la información añadida a la blockchain es pública y puede ser consultada en cualquier momento por cualquier usuario de la red.

CONCEPTO DE BLOCKCHAIN II

Es una Base de Datos descentralizada.

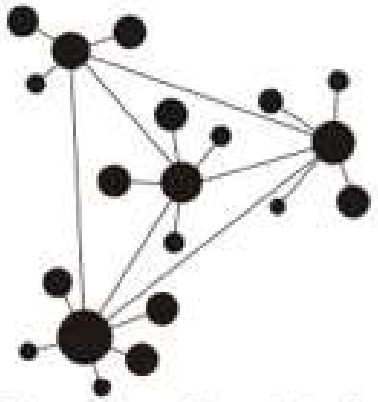
La información solo puede ser añadida a la cadena de bloques si existe un acuerdo entre la mayoría de las partes.

RED CENTRALIZADA



Todo pasa por un nexo central

RED DESCENTRALIZADA

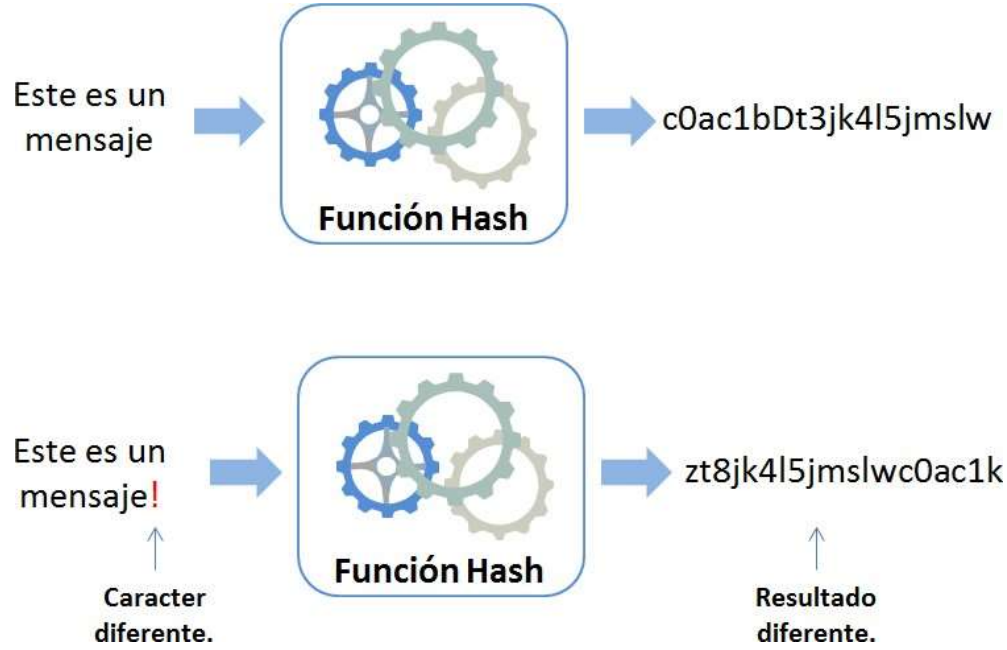


Hay varios nodos principales interconectados

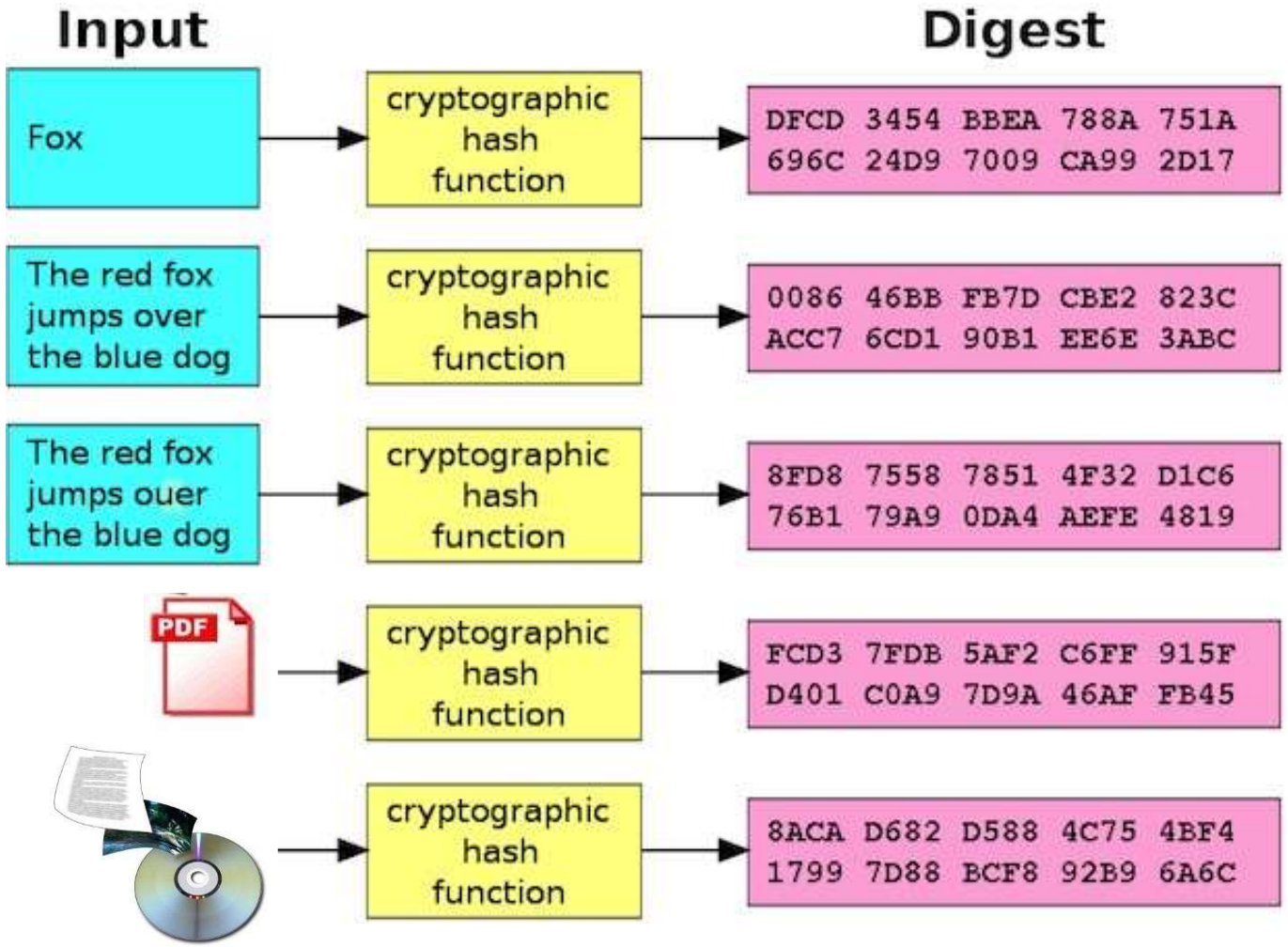
¿CÓMO SE BRINDA INTEGRIDAD EN LAS TRANSACCIONES?

PARA LA INTEGRIDAD DE LA INFORMACIÓN SE UTILIZA UNA FUNCIÓN DE HASH

Una función criptográfica hash es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

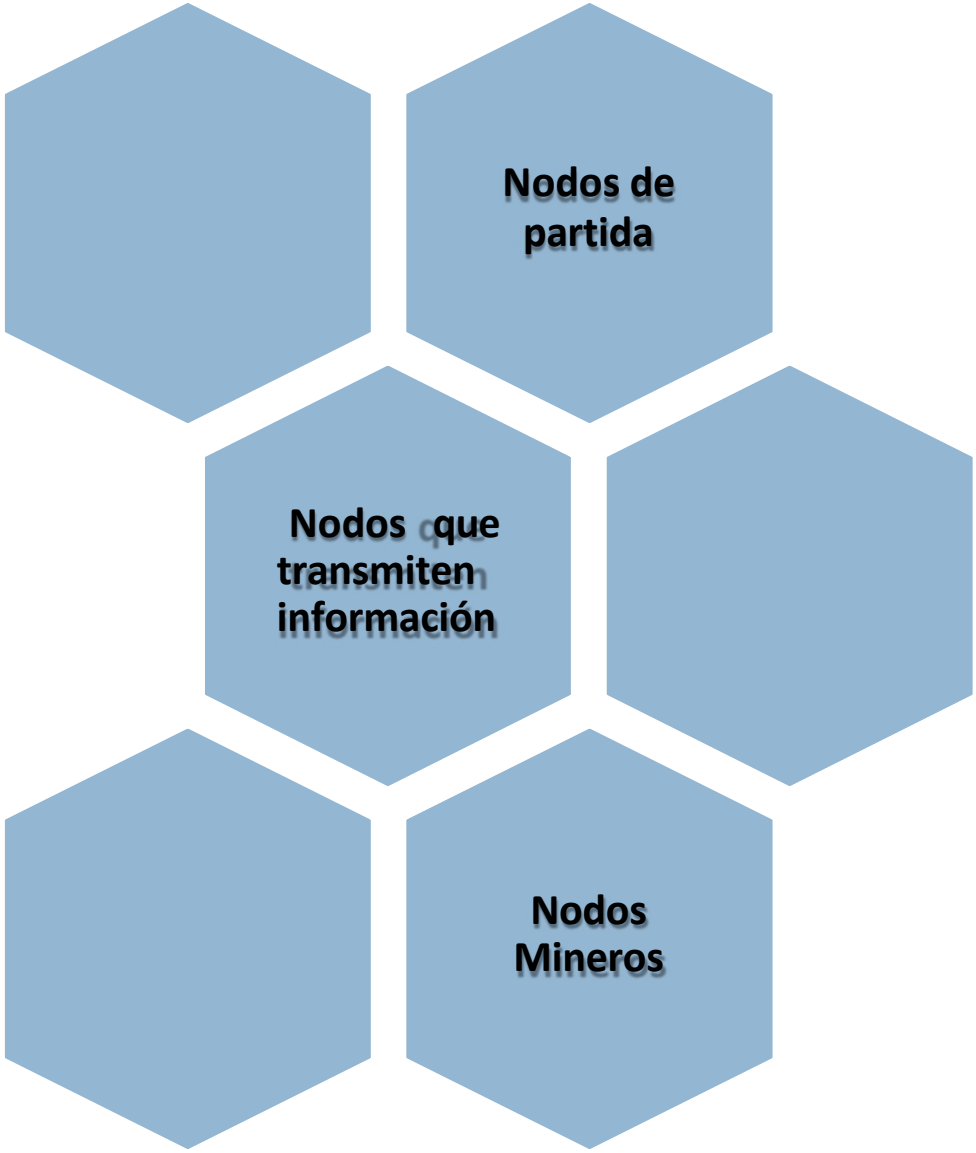


EJEMPLO DE FUNCIÓN DE HASH



BLOCKCHAIN: ¿QUIÉNES PARTICIPAN?

¿QUIÉNES PARTICIPAN?



NODO DE PARTIDA: USUARIOS FINALES

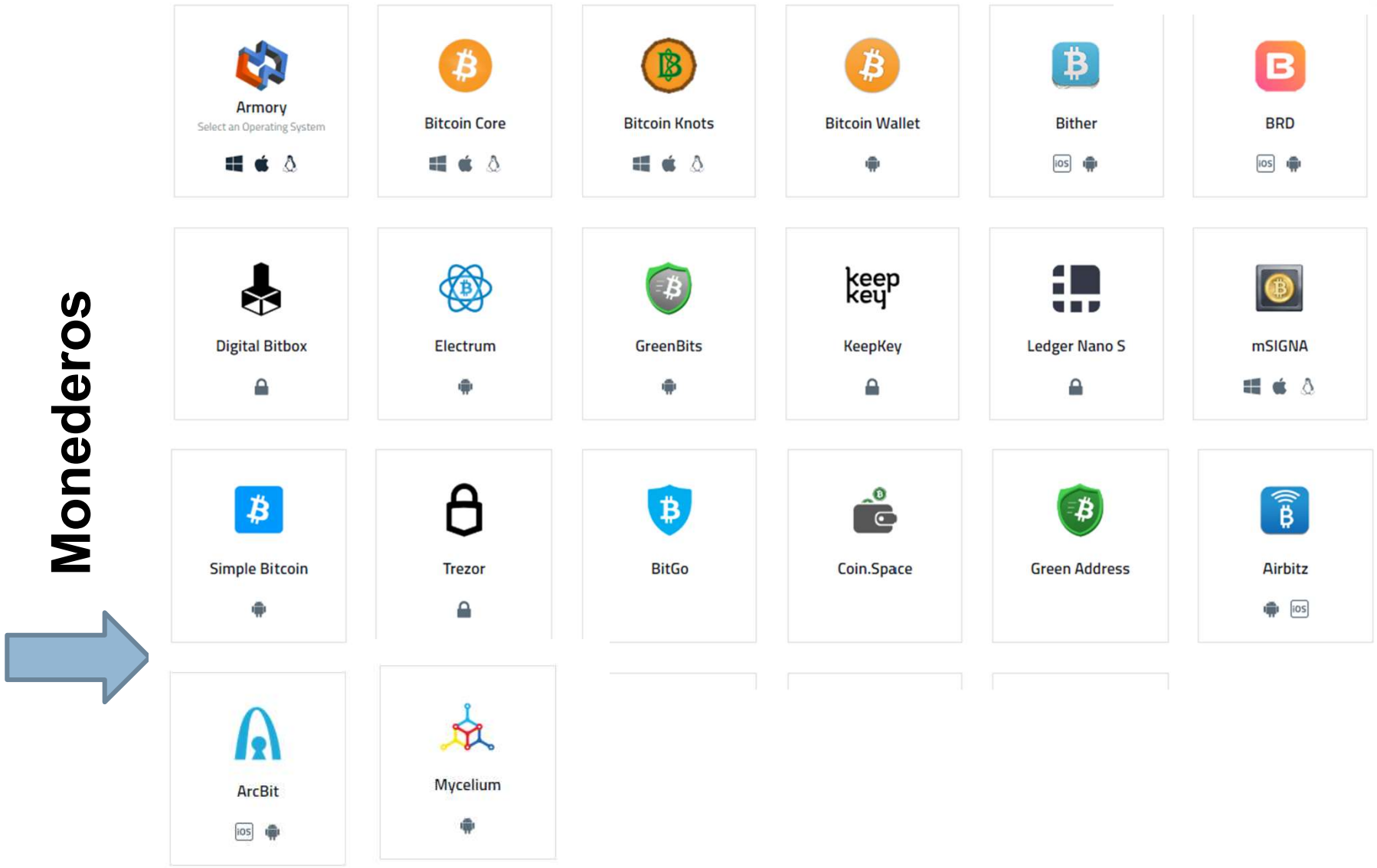
El broadcast node o un solo emisión, crea una transacción que transfiere sus monedas a la dirección Bitcoin.

Para transaccionar, cada usuario necesita un monedero de Bitcoin…

- Bitcoin no es 100% anónimo
-Los pagos de Bitcoin no son reversibles
-El Bitcoin no es una moneda oficial.

NODO DE PARTIDA: CUENTAS

Monederos

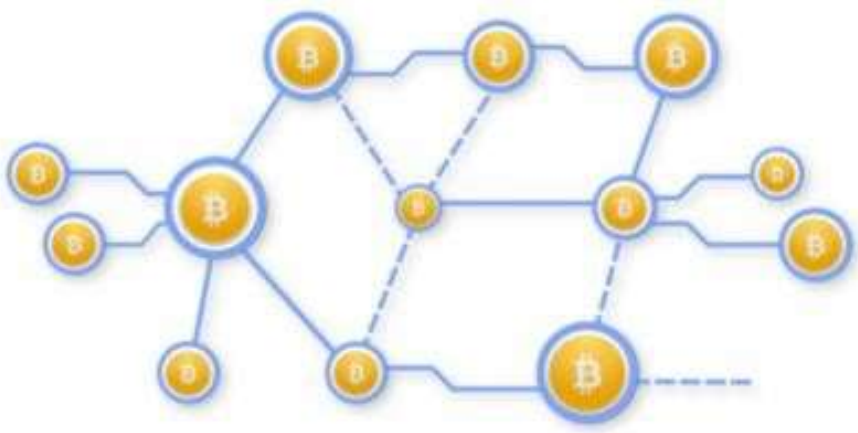


NODOS QUE TRANSMITEN (ALMACENAMIENTO)

Los nodos que transmiten o "Relay node" simplemente propagan esta transacción a otros nodos que también la transmiten, permitiendo que la transacción se replique rápidamente a todos los nodos.

Estos nodos comprueban que la transacción tiene el formato correcto, se asegura de que las firmas son válidas y busca en la versión más actualizada de la cadena de bloques (blockchain) para asegurarse y verificar que el dinero que se está transfiriendo está en la cuenta de origen de la transacción.

Los nodos mantienen copias constantemente actualizadas de la blockchain.



NODO DE MINERÍA

Si la transacción supera estos controles, llega en cuestión de segundos a todos los nodos de la red que realizan labores de minería.

Estos nodos mineros añaden esta transacción a un bloque preliminar, que tratarán de minar satisfactoriamente.

Los mineros trabajan 24 horas al día, siete días a la semana, para resolver problemas informáticos a cambio de una retribución en bitcoins.

BLOQUE

Información sobre las transacciones

NODOS DE MINERÍA MUNDIALES

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Mon Jun 18 2018 14:12:00 GMT-0300 (hora estándar de Argentina).

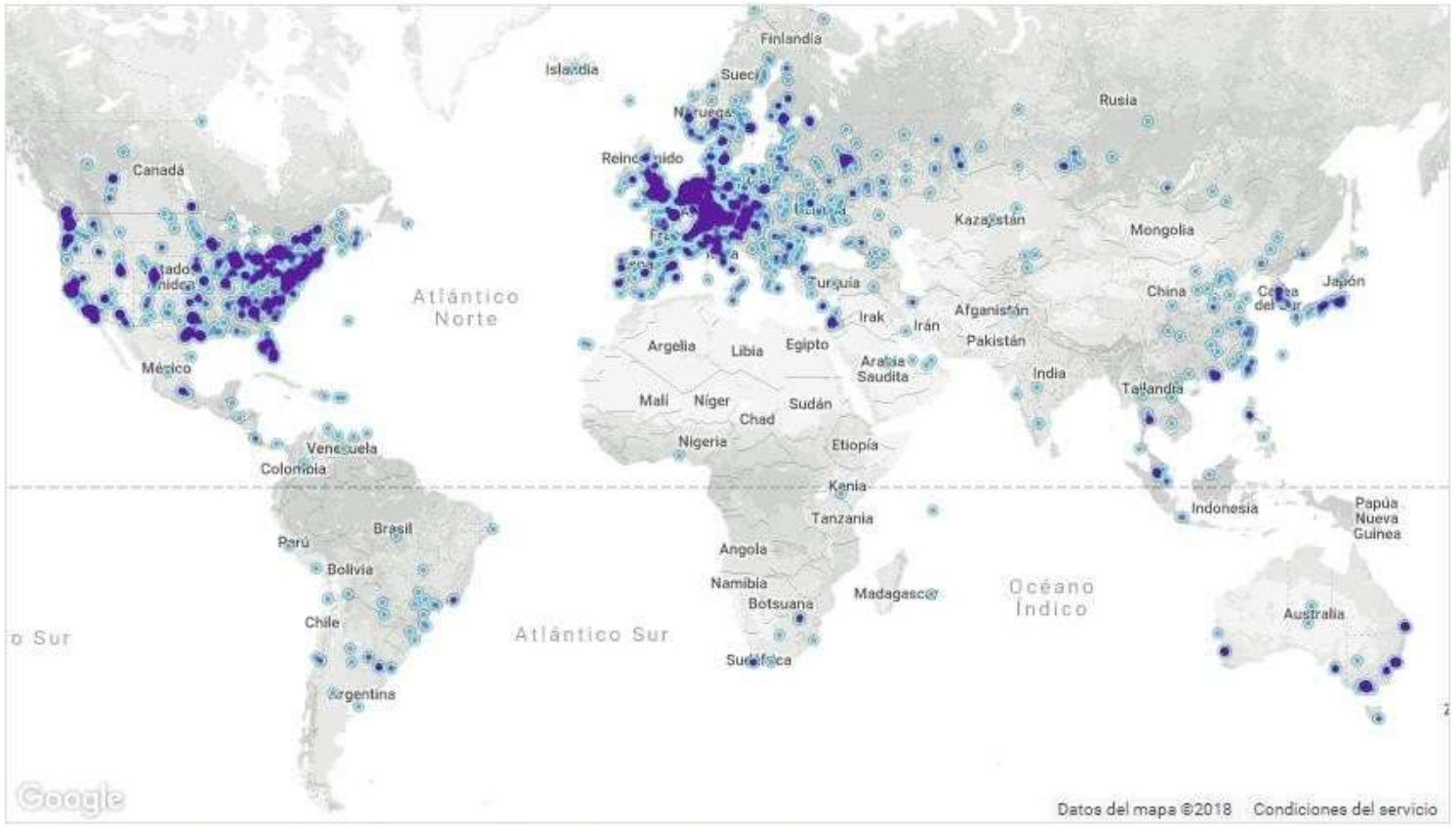
10033 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2491 (24.83%)
2	Germany	1765 (17.59%)
3	China	836 (8.33%)
4	France	670 (6.68%)
5	Netherlands	459 (4.57%)
6	n/a	373 (3.72%)
7	Canada	371 (3.70%)
8	Russian Federation	310 (3.09%)
9	United Kingdom	309 (3.08%)
10	Japan	224 (2.23%)

More (100) »



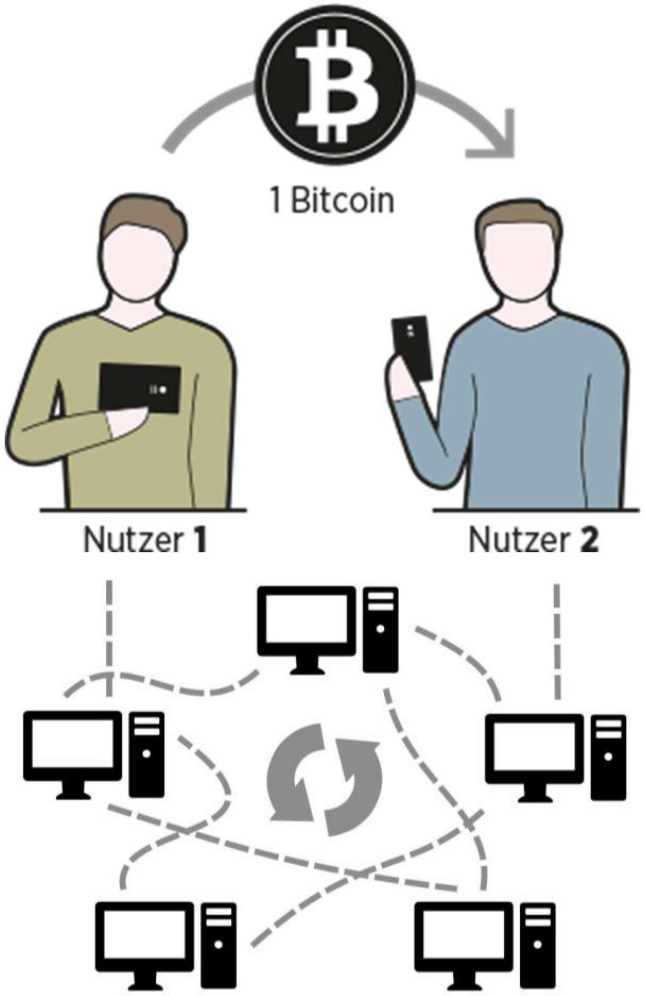
Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

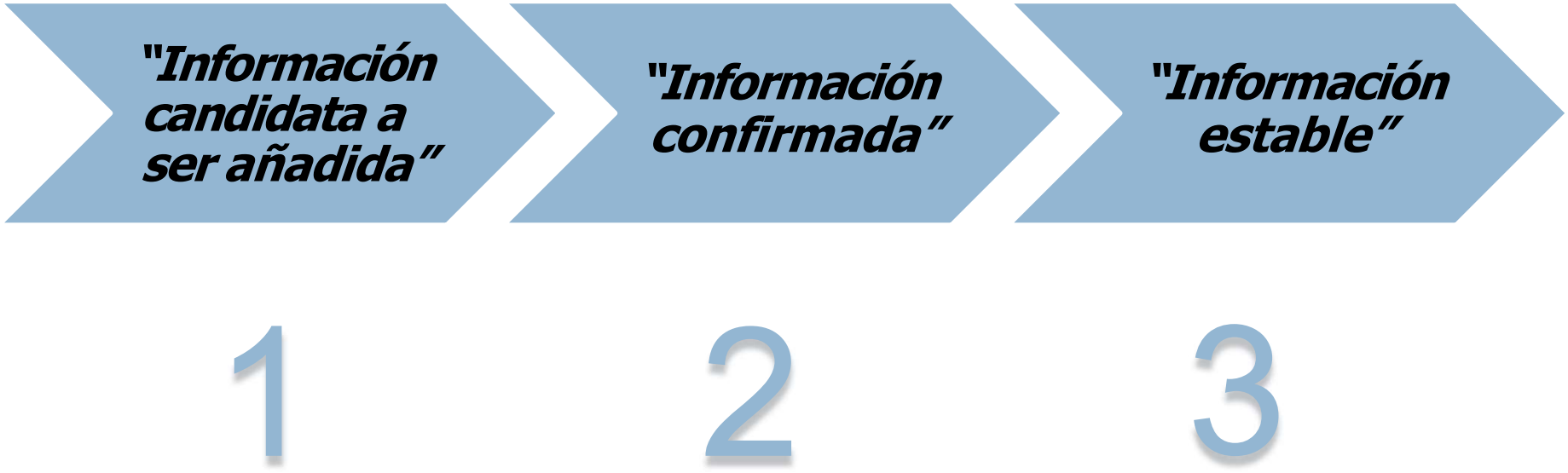
https://bitnodes.earn.com/

BLOCKCHAIN: ¿CÓMO SE REGISTRAN LAS TRANSACCIONES?

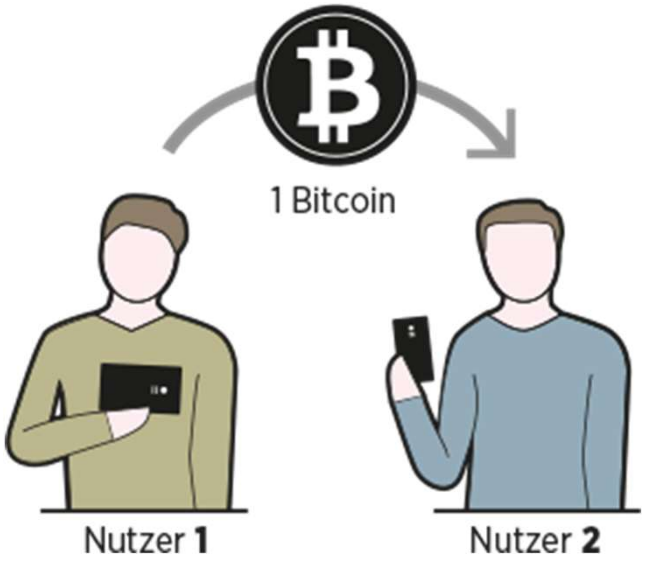
¿CÓMO SE REGISTRAN LAS TRANSACCIONES?



ESTADIOS DE UNA TRANSACCIÓN



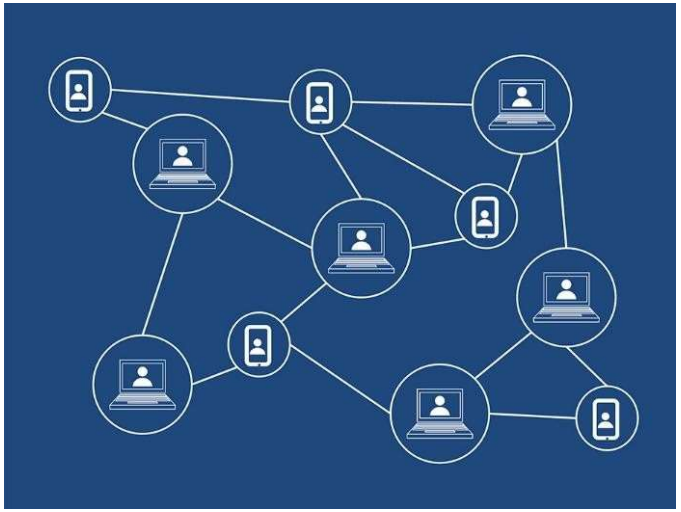
1



Información candidata a ser añadida

Es información que los nodos han enviado al resto de nodos mediante la red peer-to-peer pero que aún no ha sido validada en ningún bloque.

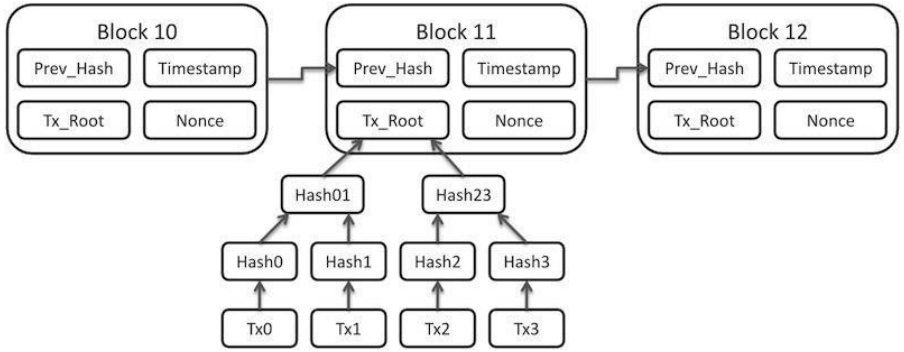
2



Información confirmada

Es la información validada por la red y se procede a añadirla al próximo bloque.

3



Información Estable

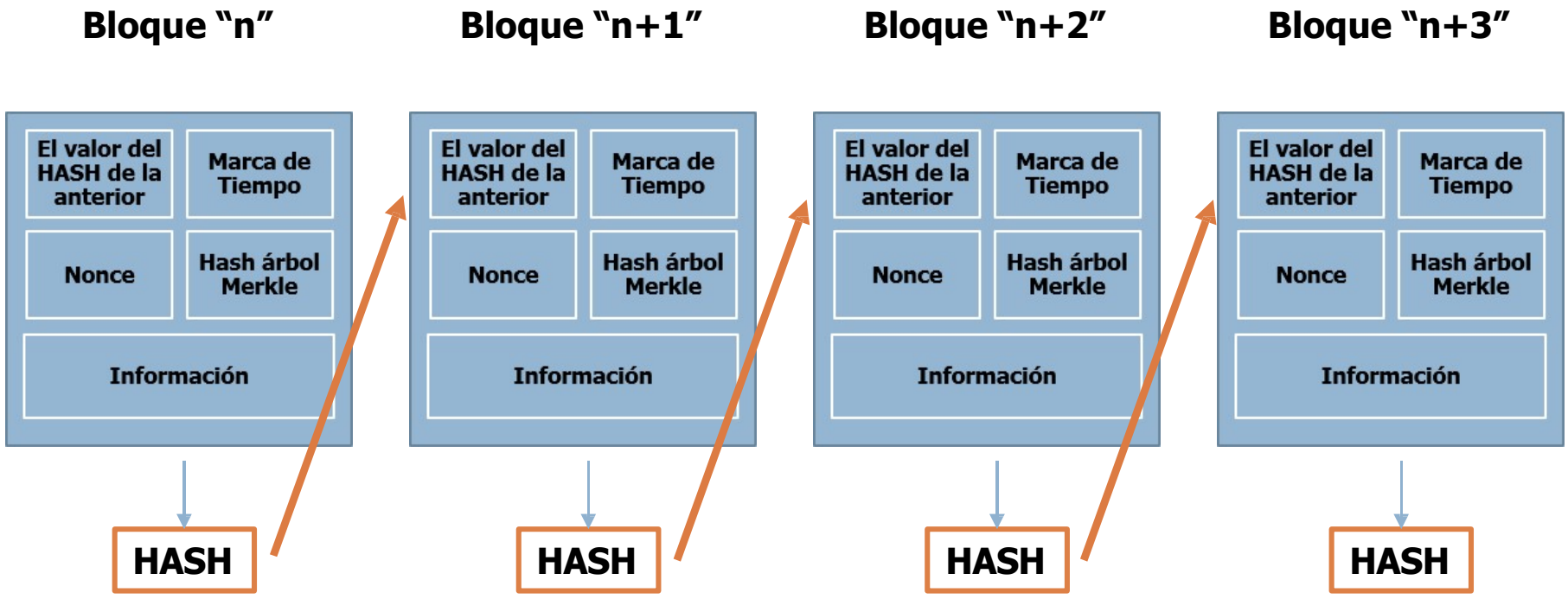
Es la información que forma parte de la blockchain de forma inmutable.

¿CÓMO SE COMPONEN LOS BLOQUES DE LA BLOCKCHAIN?

CONTENIDO UN BLOQUE

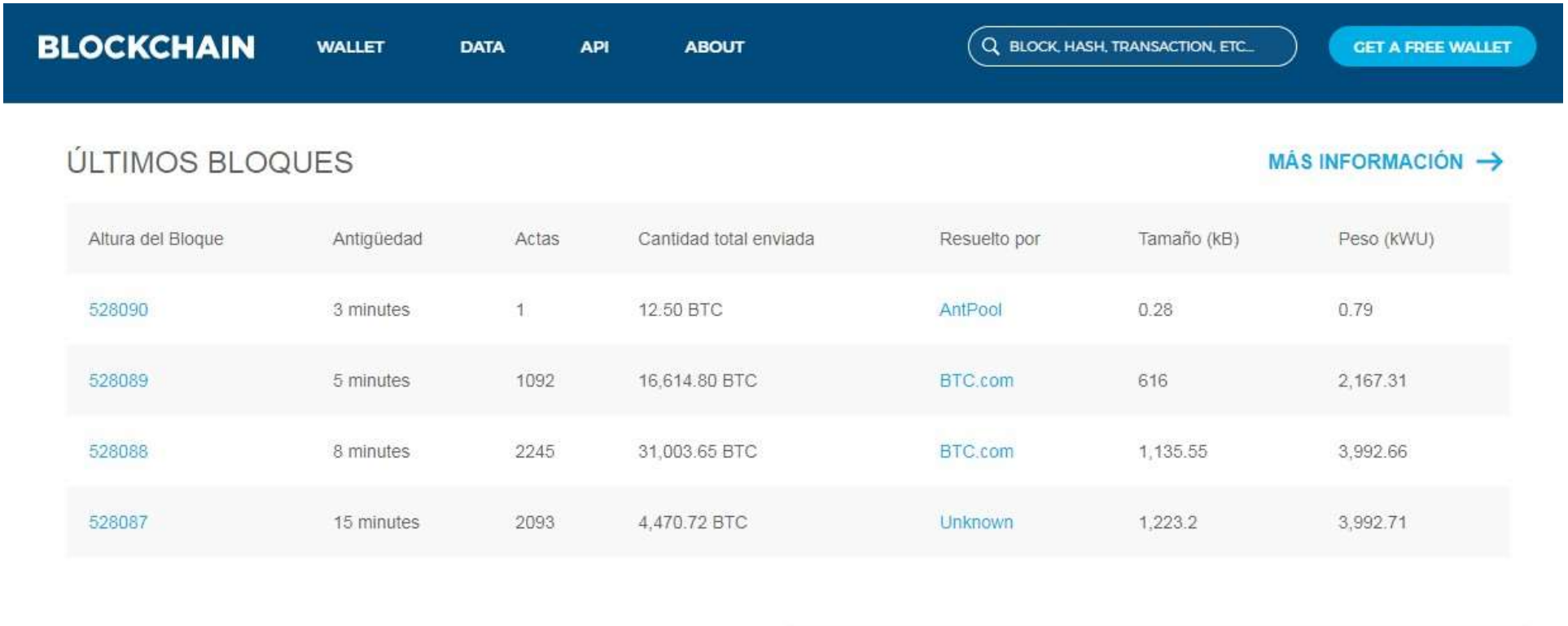
Fuente: LA BLOCKCHAIN: FUNDAMENTOS, APLICACIONES Y RELACIÓN CON OTRAS TECNOLOGÍAS DISRUPTIVAS . CARLOS DOLADER RETAMAL JOAN BEL ROIG JOSE LUÍS MUÑOZ TAPIA

¿CÓMO VALIDAMOS LA SECUENCIA?



¿QUIÉN PUEDE ACCEDER A LOS BLOQUES?

https://blockchain.info/



Bloques #528090

Resumen	
Número de Transacciones	1
Total de productos	12.5 BTC
Volumen Estimado de la Transacción	0 BTC
Comisiones de la Transacción	0 BTC
Altura	528090 (Cadena principal)
Fecha y Hora	2018-06-18 17:54:57
Hora de Recepción	2018-06-18 17:54:57
Resuelto por	AntPool
Dificultad	4,940,704,885,521.83
Bits	389609537
tamaño	0.285 kB
Peso	0.788 kWU
Versión	0x20000000
Mientras tanto	657436258
Recompensa del Bloque	12.5 BTC

Hashes	
Hash	0000000000000000002a882472c9f662433e361b39e4653477449209a1447142
Bloque Anterior	0000000000000000007bb28fc4f3b8038d0252ee9f67ddd152df4a1f9d0ee82
Bloque(s) siguiente(s)	
Raíz de Merkle	fc857ba54704e7bd5ddec9cf2c7f279c9d994b73d4c6b4c3dc161274fabd4ead

REPASO DE LA TECNOLOGÍA BOCKCHAIN

REPASO DE LA TECNOLOGÍA BLOCKCHAIN

BLOCKCHAIN: PRINCIPALES CARACTERÍSTICAS

Las principales características de la tecnología blockchain son:

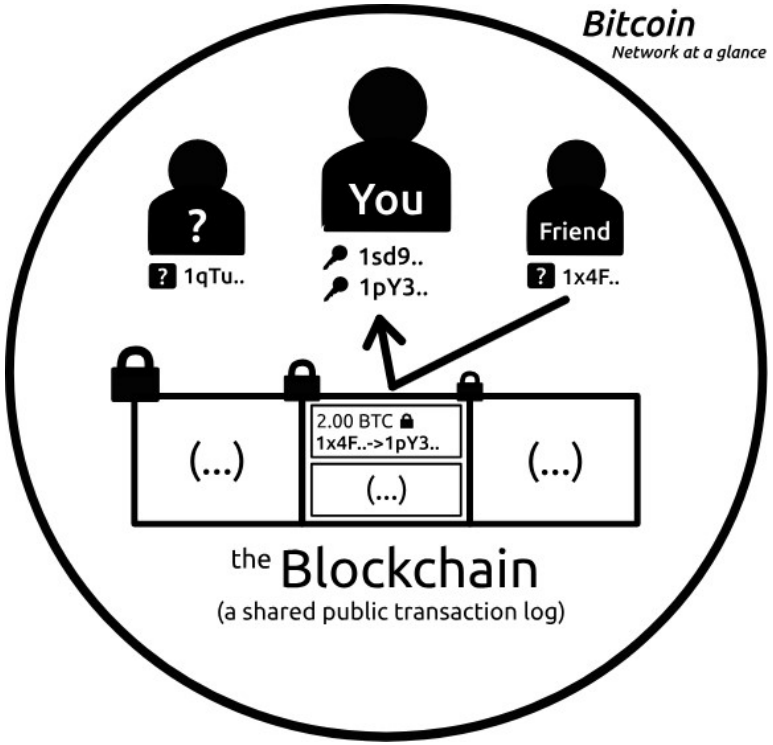
- Sistema **seguro** dado que su tecnología se basa en la criptografía de datos.
- La transacciones se concentran en **bloques**, y en estos bloques la información se almacena cronológicamente.
- Una vez aceptada, **la información no se puede borrar ni modificar**, por lo que se puede consultar en cualquier momento.
- Un blockchain **puede ser público o privado**, e incuso permitir ciertas consultas con un permiso.

¿EXISTE RIESGO DE FRAUDE?

De esta manera hackear la blockchain para introducir una transacción falsa o recurrir al doble gasto de las monedas resulta prácticamente imposible, pues se tendrían que modificar la mayoría de los nodos y violar la criptografía con la que se protegen los datos.

¿QUÉ OTROS USOS LE PODEMOS ASIGNAR A ESTA TECNOLOGÍA?

¿PARA QUÉ PODEMOS UTILIZAR ESTA TECNOLOGÍA?



Hashes de información

¿?