

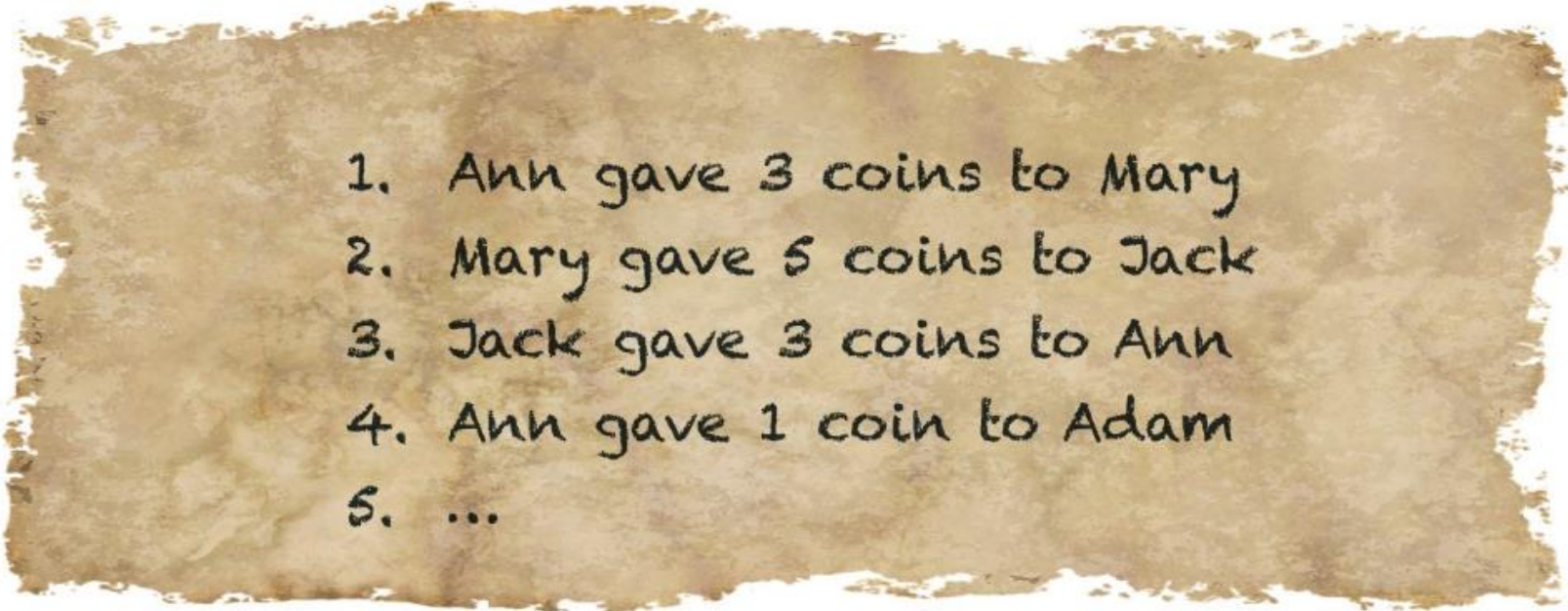
Blockchain

Un ejemplo de como funciona

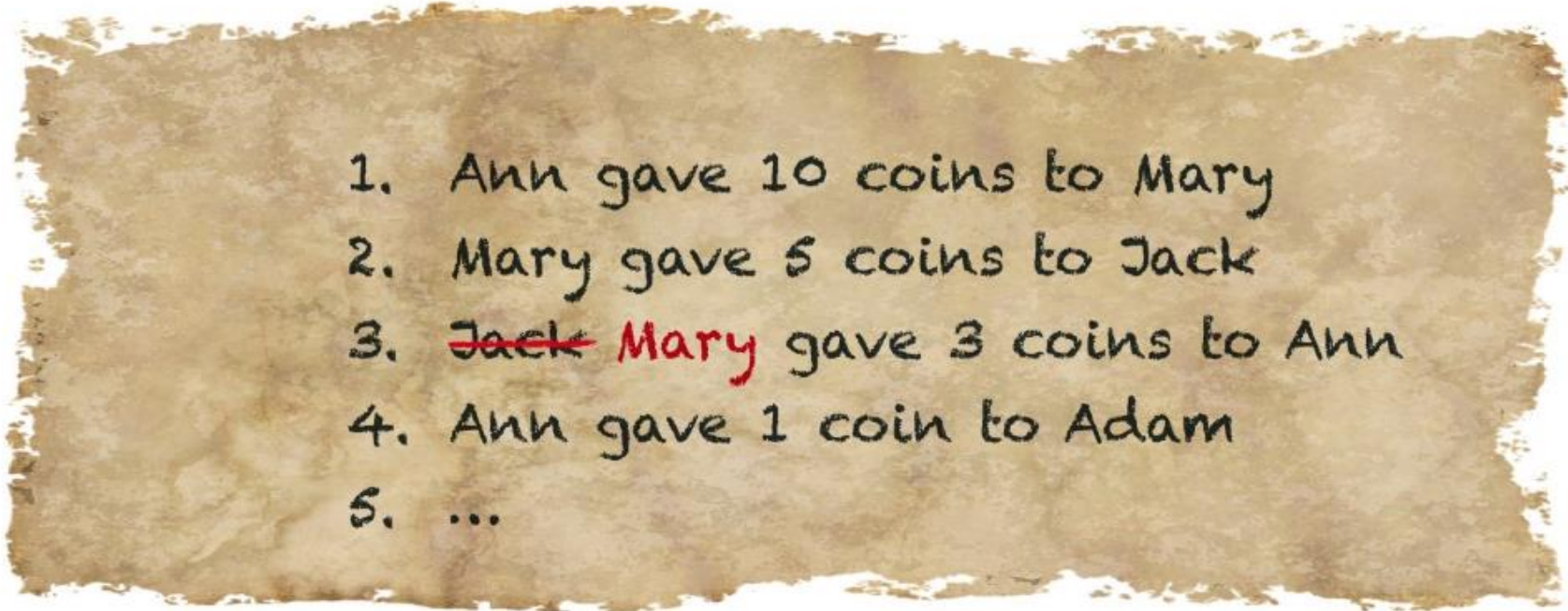
<https://es.cointelegraph.com/bitcoin-for-beginners/how-blockchain-technology-works-guide-for-beginners>

Hagamos una criptomoneda

- Un grupo de amigos decide hacer una criptomoneda
- Deben seguir un flujo de fondos , por lo que una persona llamada BOB , decidió llevar una lista con todas las transacciones.

- 
1. Ann gave 3 coins to Mary
 2. Mary gave 5 coins to Jack
 3. Jack gave 3 coins to Ann
 4. Ann gave 1 coin to Adam
 5. ...

- Uno de los amigos (JACK) decide modificar a su favor una transacción.

- 
1. Ann gave 10 coins to Mary
 2. Mary gave 5 coins to Jack
 3. ~~Jack~~ Mary gave 3 coins to Ann
 4. Ann gave 1 coin to Adam
 5. ...

- BOB notó que alguien había modificado su listado de transacciones y decidió implementar medidas de seguridad para que esto no sucediera.
- Implemento una contramedida que garantizara la integridad del listado de transacciones y pensó en una función hash

| Input | Output (Hash) |
|------------------------|--|
| Cat | 93g56gtf229hbno00r45sktrpbs59so9r3t7saer |
| A white cat is outside | js03bbstgo94r6s1z8mg05fgt3sba9tob32bsap7 |
| A white cat is inside | bbr19007go2tsi52bsi50o21nmiseas45on23mjn |
| A whiet cat is inside | 339n5sbk249nb9530gjdI04h92jg02jg9sm93hpz |
| A white cat is insid | 4bbj390osoh9djm395bksh94gf03sg034dfjh31x |

- Implemento una función hash después de cada registro de transacción

6. Ann gave 10 coins to Mary

cff4e860bd57c2bfb7c010927c3fbfee

7. Mary gave 5 coins to Jack

803c28370e9a16eb28a23d46d3ebe711

- JACK con el interés de beneficiarse, nuevamente altero una transacción a su favor y generó un nuevo código hash

6. Ann gave 10 coins to Mary

cff4e860bd57c2bfb7c010927c3f6fee

7. Mary gave ~~5~~ 8 coins to Jack

~~803c28370e9a16e628a23d46d3ebe711~~

4ae41f8cc3d4cc905f6b4c75ceab9da0

- BOB nuevamente detecto que alguien había alterado el registro y con la intención de garantizar confianza sobre la moneda que se había gestado, implemento nuevas contramedidas.
- Agrego un código hash después de cada registro. Este generado a partir del registro de transacción + el ultimo código hash

| Input | Hash |
|---|----------------------------------|
| Ann gave 10 coins to Mary | 8977e7c112aea5b0a62e9c5f3084a203 |
| Mary gave 5 coins to Jack 8977e7c112aea5b0a62e9c5f3084a203 | e37a8d1cc39ed9f54afadb6c6cafe639 |
| Mary gave 3 coins to Ann e37a8d1cc39ed9f54afadb6c6cafe639 | 5b9foe325f58766f5a2dfe7eec636f6d |
| Ann gave 1 coin to Adam 5b9foe325f58766f5a2dfe7eec636f6d | 55f28e65412b22aa3d6002bcf7d67201 |

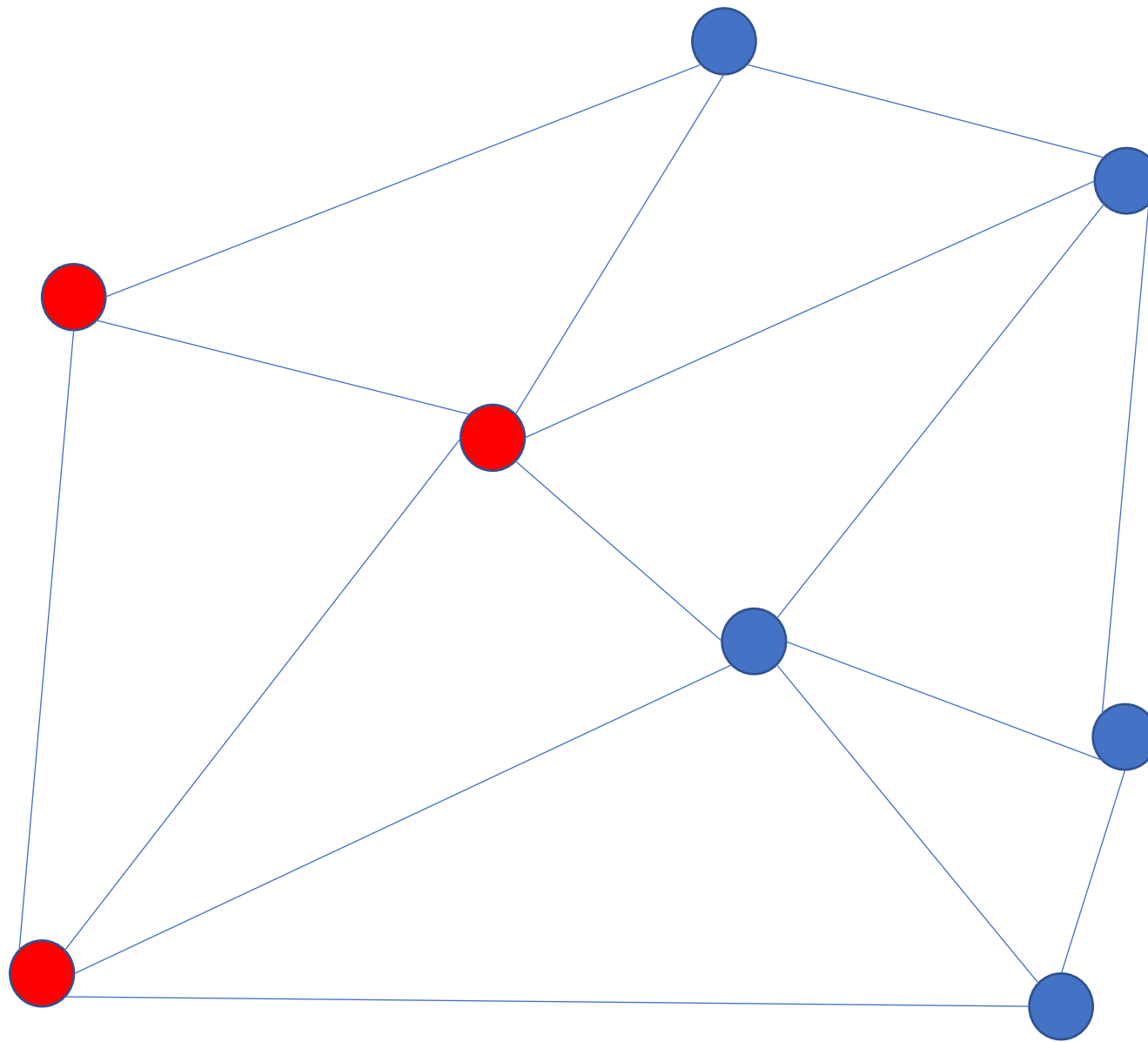
- Ahora!!! si alguien alterara alguno de los registros, para no dejar huellas, debía alterar todos los códigos hash generados.
- JACK muy interesado en seguir intentando de hacerse de mas dinero, se propuso tomarse el trabajo de modificar todos los hash.
- Como respuesta BOB decidió agregar un número después de cada registro (NONCE).
- El Nonce debe elegirse de modo que el hash generado termine en dos ceros.

- Ahora, para falsificar registros, JACK tendría que pasar horas y horas eligiendo Nonce para cada línea.
- Más importante aún, no sólo las personas, sino que las computadoras NO PUEDEN descifrar el Nonce rápidamente.

| Input | Hash |
|---|--|
| Ann gave 10 coins to Mary <u>451</u> | 219711e62645a21f2742ada2c6f2a900 <u> </u> |
| Mary gave 5 coins to Jack <u>13</u> 219711e62645a21f2742ada2c6f2a900 | 1cc4c07fa0757848b439e2361ce87d00 <u> </u> |
| Mary gave 3 coins to Ann <u>467</u> 1cc4c07fa0757848b439e2361ce87d00 | e43a132f4b67c65ba6914824a39b3900 <u> </u> |
| Ann gave 1 coin to Adam <u>56</u> e43a132f4b67c65ba6914824a39b3900 | 99012fe16897c19465941d5350afa900 <u> </u> |

- Bob con intención de dar un límite a la cantidad de transacciones decidió limitar a 5000 transacciones a lo que llamo bloque de transacciones.
- Además para dar mayor seguridad (disponibilidad, integridad y confidencialidad), implementó otra contramedida. Implemento copias del bloque en 5000 computadoras del mundo.
- A cada computadora se le llama NODO.
- Cuando se completan las 5000 transacciones se genera un nuevo bloque
- Para que una transacción entre en un bloque esta debe ser validada por el 51 % de los nodos.
- Es muy importante el orden en que entra la transacción
- Un secuencia de bloques se les llama BLOCKCHAIN

Nodos



- Que es una BILLETERA?
- La firma digital y su protagonismo en una transacción.