

BLOCKCHAIN & BITCOIN

MATIAS ANDRADE Y RODRIGO CONTRERAS



PROBLEMA?

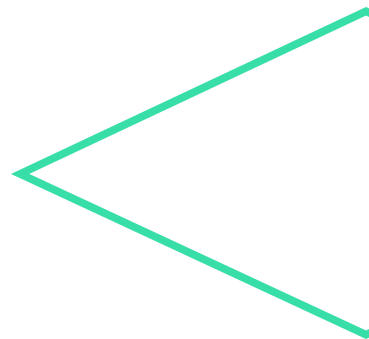
Confiar en terceros, double spending problem,
generales bizantinos.





BLOCKCHAIN?

Literalmente una cadena de bloques. Se puede
pensar como una lista ligada



ESTRUCTURA DE UN BLOQUE

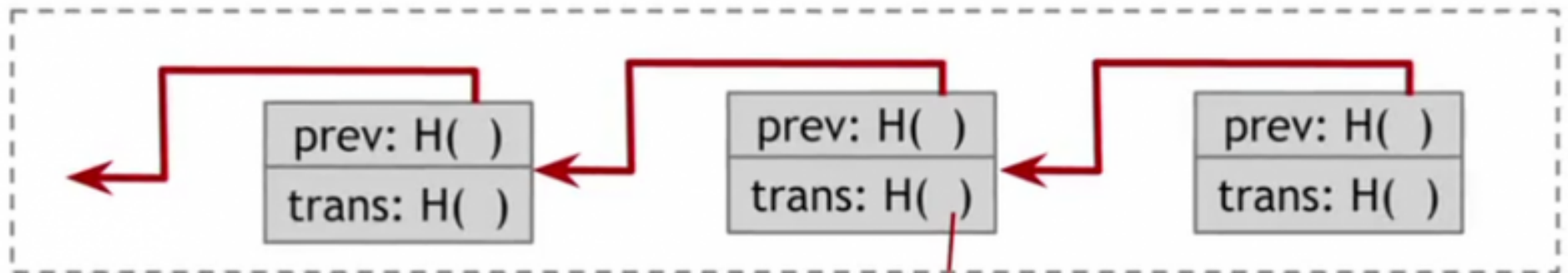
version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c81701000000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
...	

Block hash

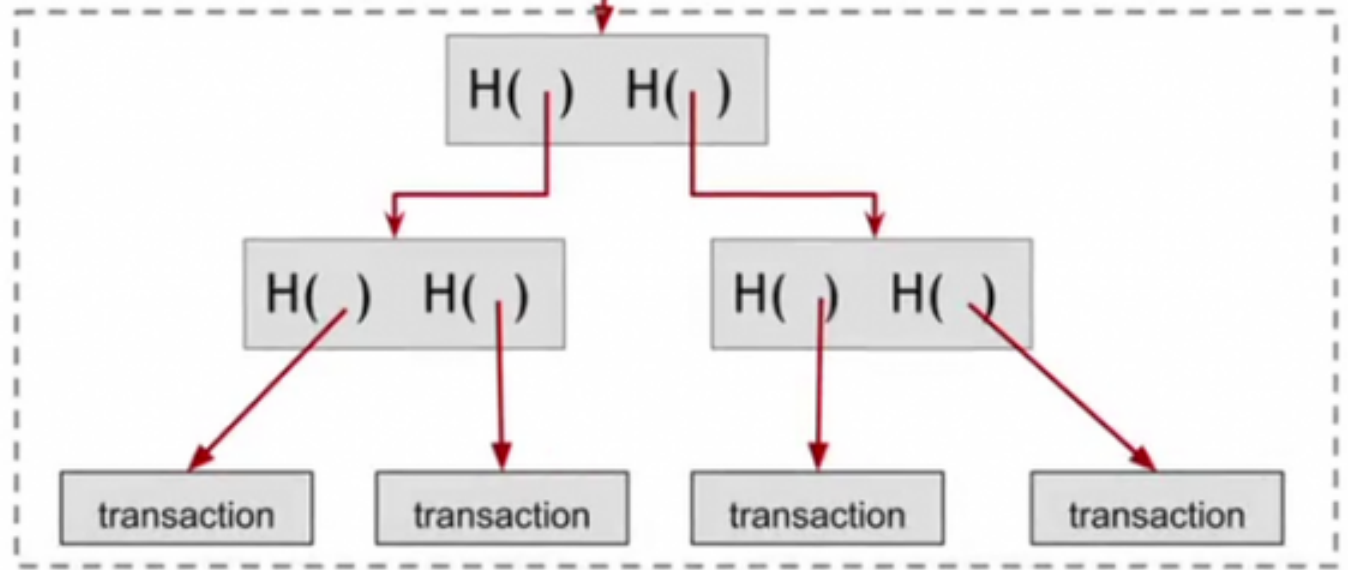
0000000000000000
e067a478024addfe
cdc93628978aa52d
91fabd4292982a50

MERKLE TREES

Hash chain of blocks



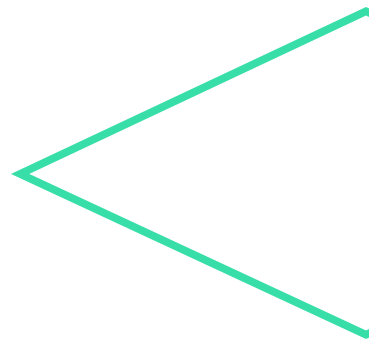
Hash tree (Merkle tree) of transactions in each block





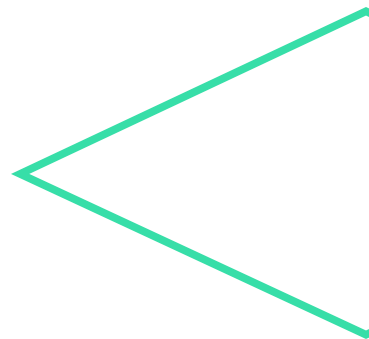
BITCOIN?

Red P2P descentralizada de pagos sin necesidad de intermediarios. Registra los pagos en un blockchain público.

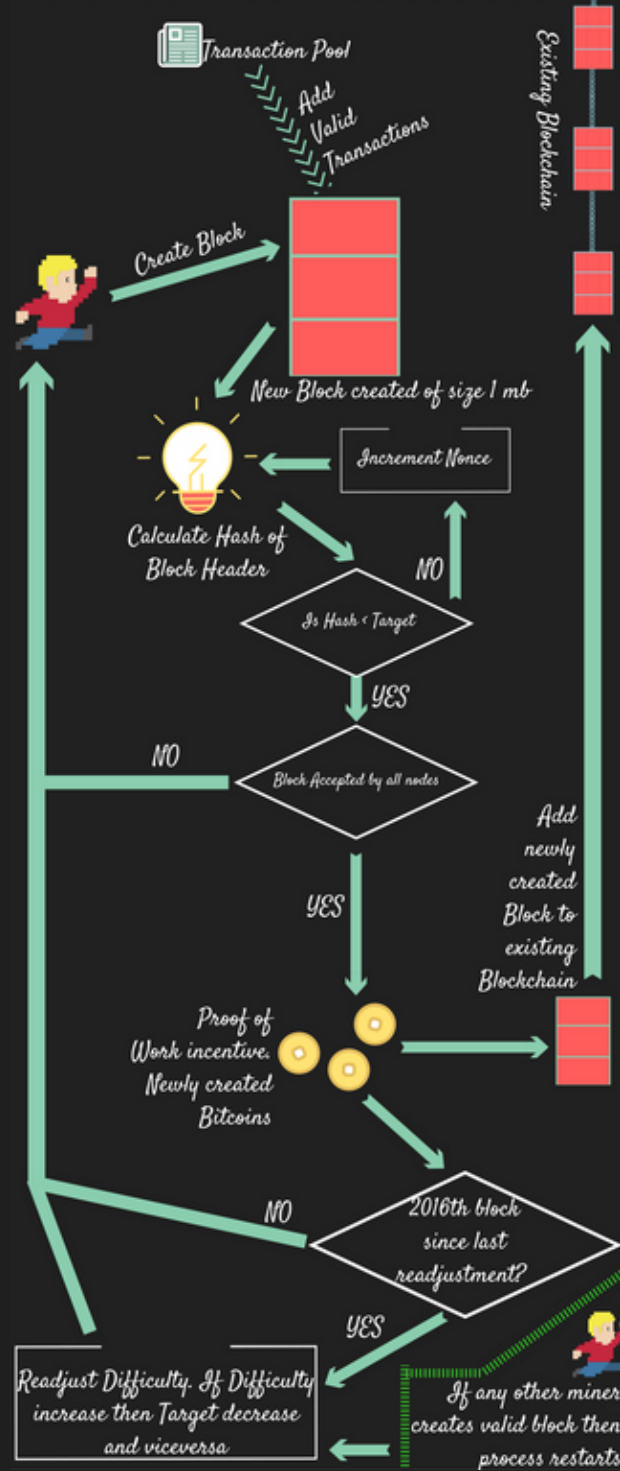
- 280,000 transacciones por día
 - Fee promedio de 0.00008205 BTC
 - Pool de 3,688 transacciones no confirmadas
 - Blockchain completo de 190 MB
- 



BITCOIN?

- Dificultad ajustable para mantener ritmo de 1 bloque cada 10 minutos
 - Mineros ganan por fees de la transacción y además premio fijo (decreciente)
 - Límite de 21 millones de monedas
 - Minado se anuncia con política del mejor esfuerzo
- 

BITCOIN MINING



PROCESO DE MINADO

According to Wikipedia, gesture-based systems accept input in the form of taps, swipes, and other ways of touching.

3 ALGORITMOS DE CONSENSO



PROOF OF WORK

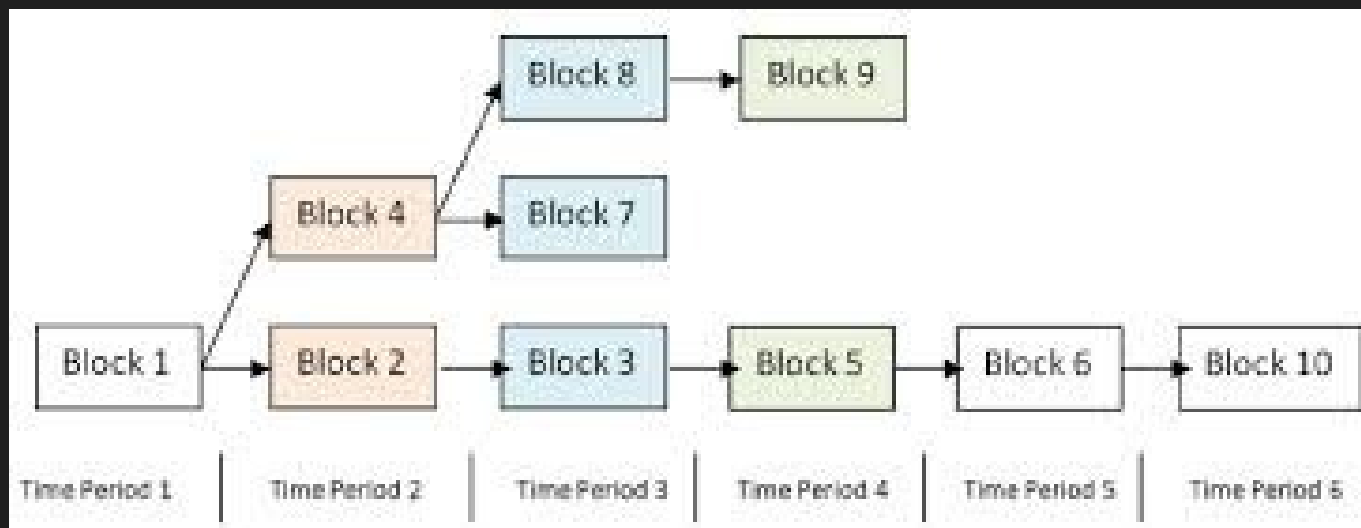


PROOF OF STAKE

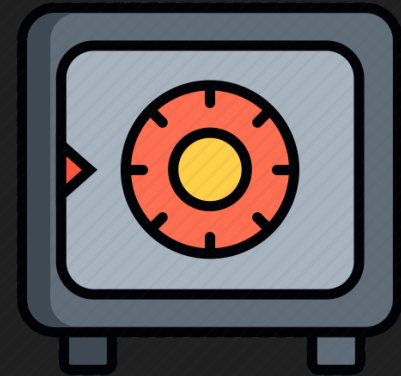
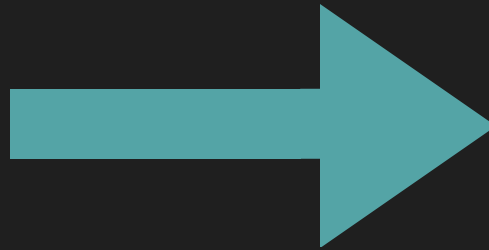


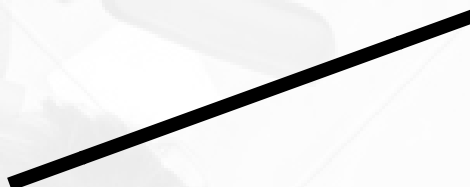
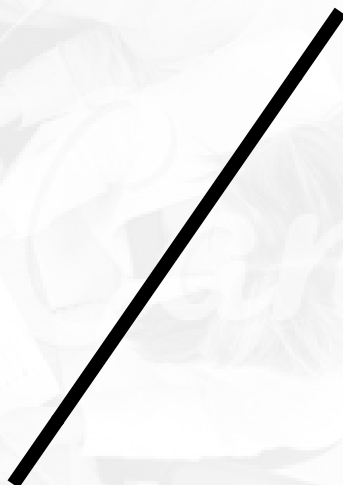
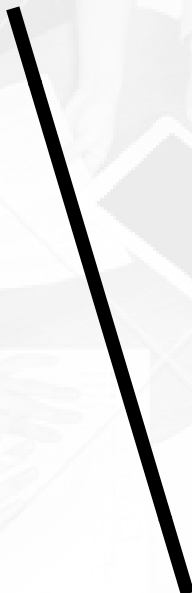
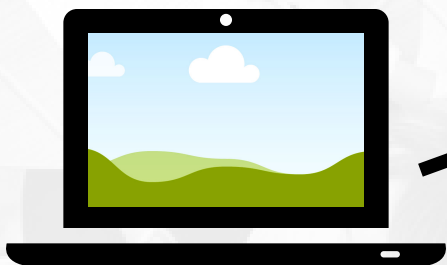
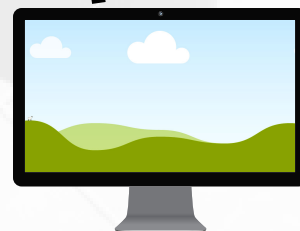
DELEGATED PROOF OF STAKE

PROOF OF WORK

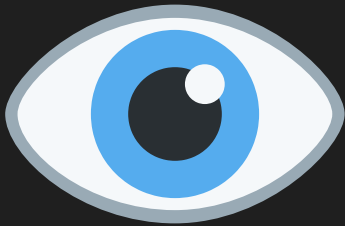


PROOF OF STAKE





DELEGATED PROOF OF STAKE

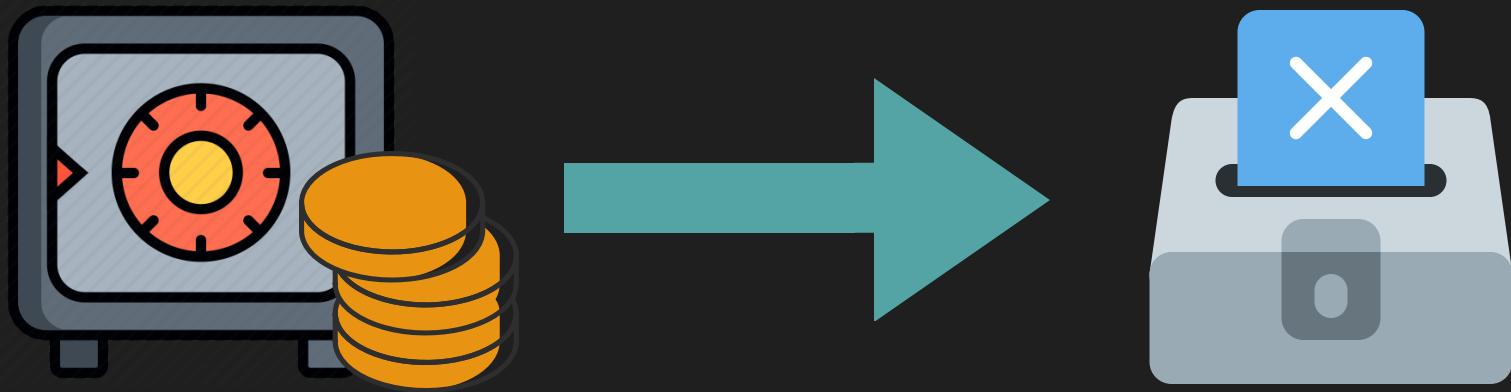


TESTIGOS



DELEGADOS

DELEGATED PROOF OF STAKE





¡GRACIAS!