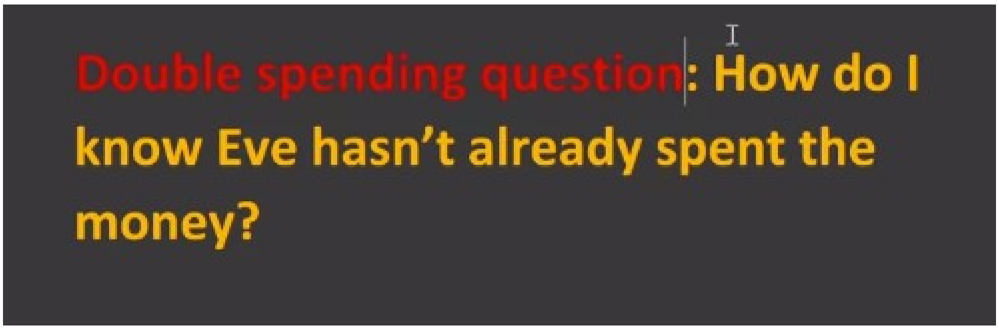
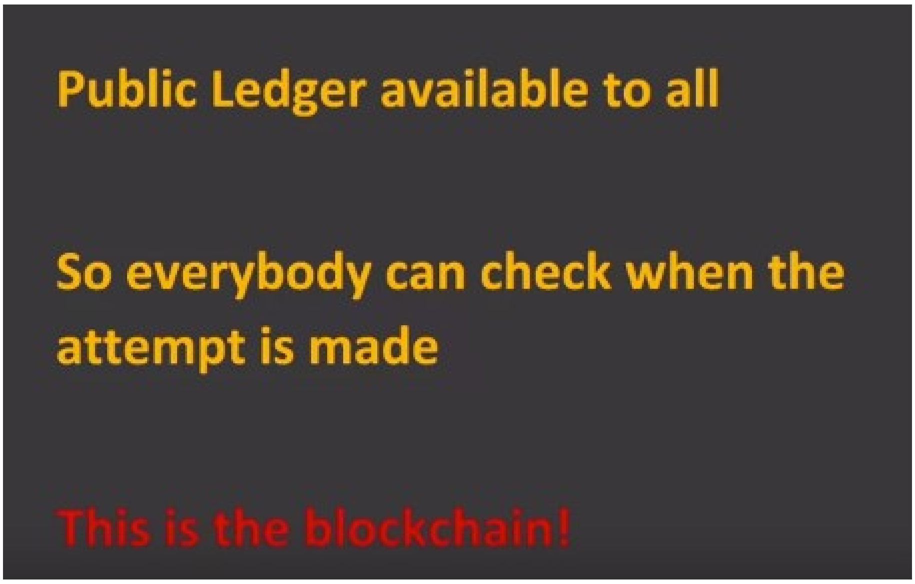
Week 14 – Double spending



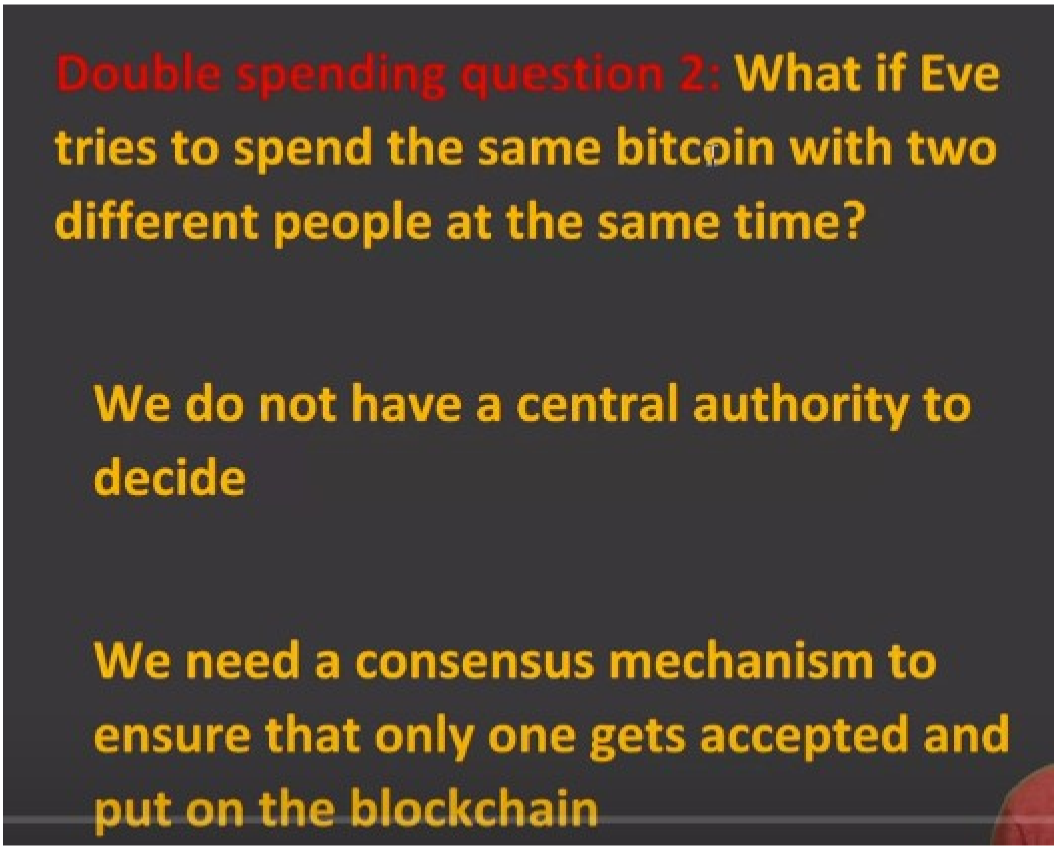
Double spending question: How do I know Eve hasn’t already spent the money?



Public Ledger available to all

So everybody can check when the attempt is made

This is the blockchain!



Double spending question 2: What if Eve tries to spend the same bitcoin with two different people at the same time?

We do not have a central authority to decide

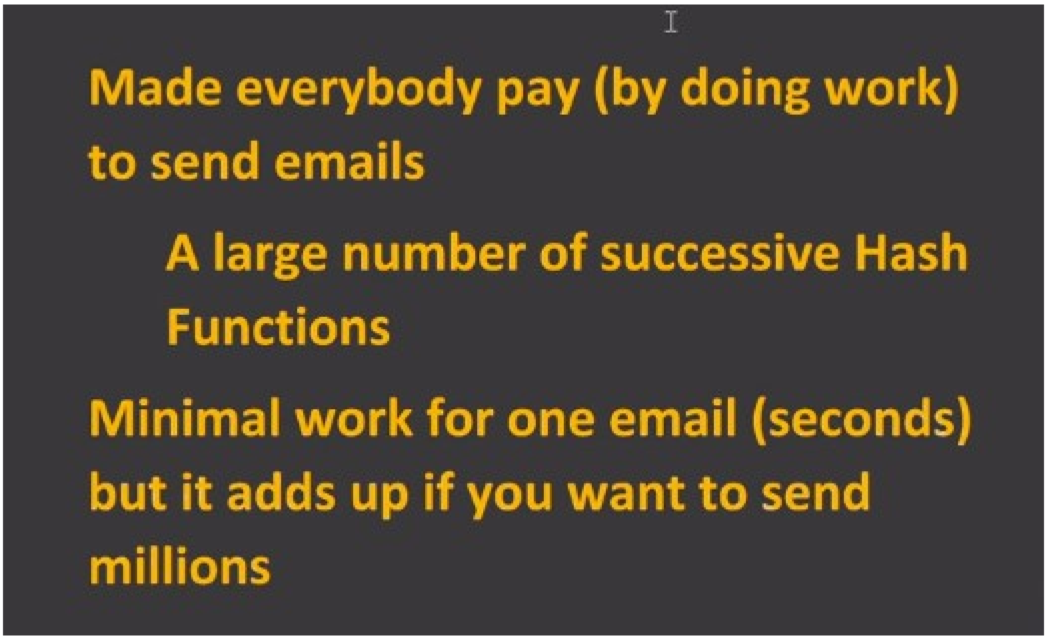
We need a consensus mechanism to ensure that only one gets accepted and put on the blockchain

The answer is based on proof of work

Idea adapted from Hashcash in 2002. (Denial of Service Attacks)

Hashcash

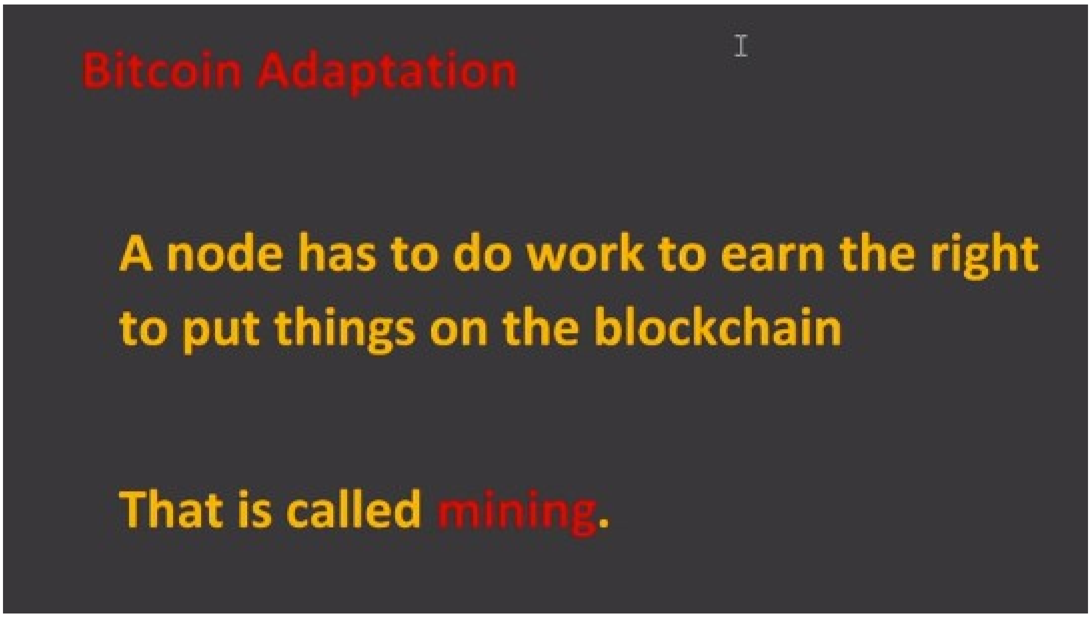
Wanted to stop spammers from sending millions of emails automatically



Made everybody pay (by doing work) to send emails

- A large number of successive Hash Functions

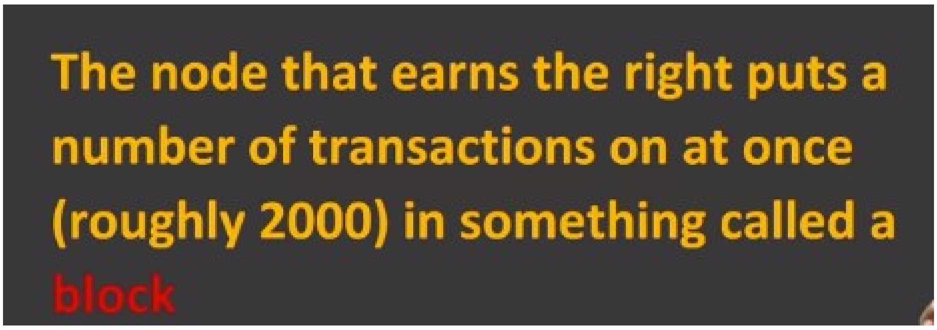
Minimal work for one email (seconds) but it adds up if you want to send millions



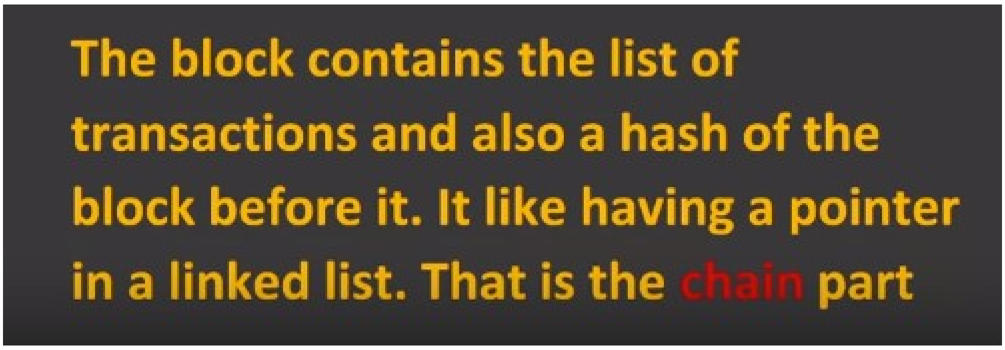
Bitcoin Adaptation

A node has to do work to earn the right to put things on the blockchain

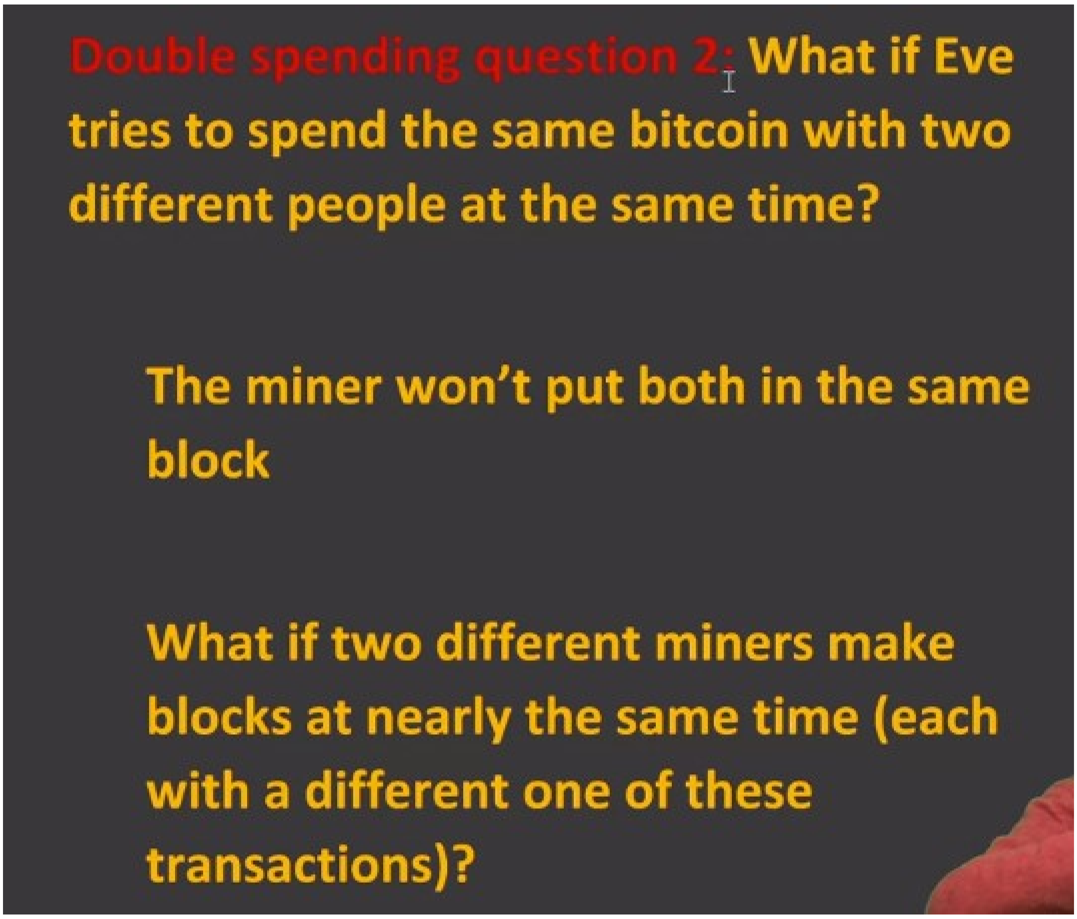
That is called mining.



The node that earns the right puts a number of transactions on at once (roughly 2000) in something called a block



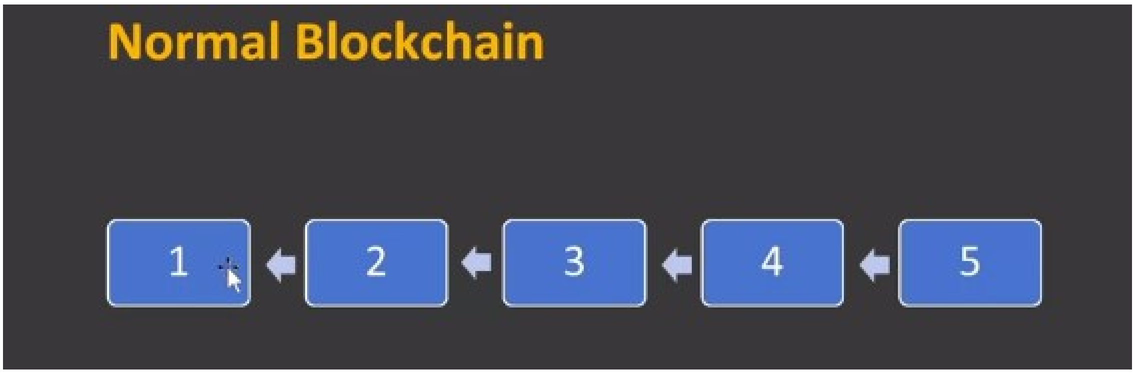
The block contains the list of transactions and also a hash of the block before it. It like having a pointer in a linked list. That is the chain part



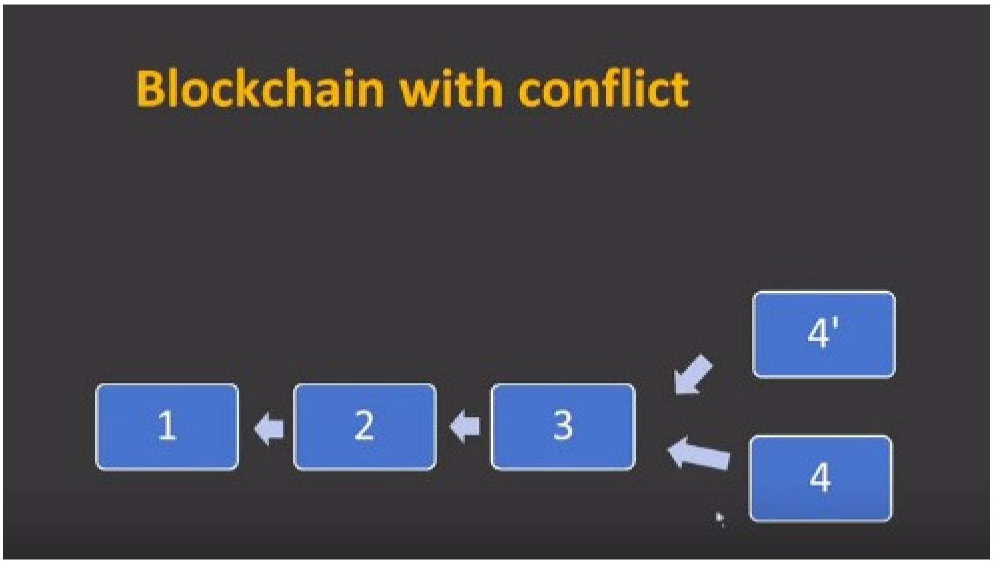
Double spending question 2: What if Eve tries to spend the same bitcoin with two different people at the same time?

The miner won't put both in the same block

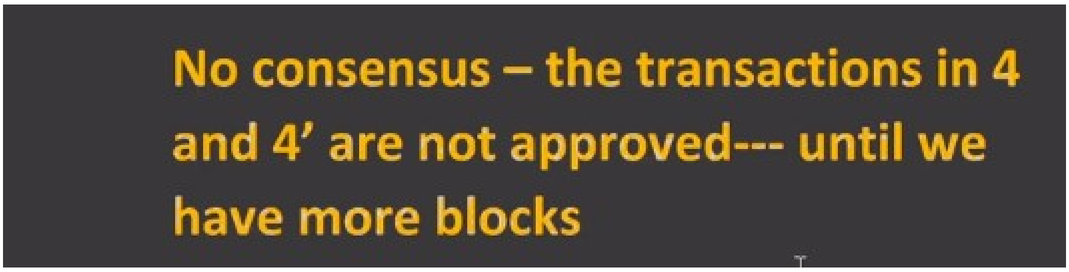
What if two different miners make blocks at nearly the same time (each with a different one of these transactions)?



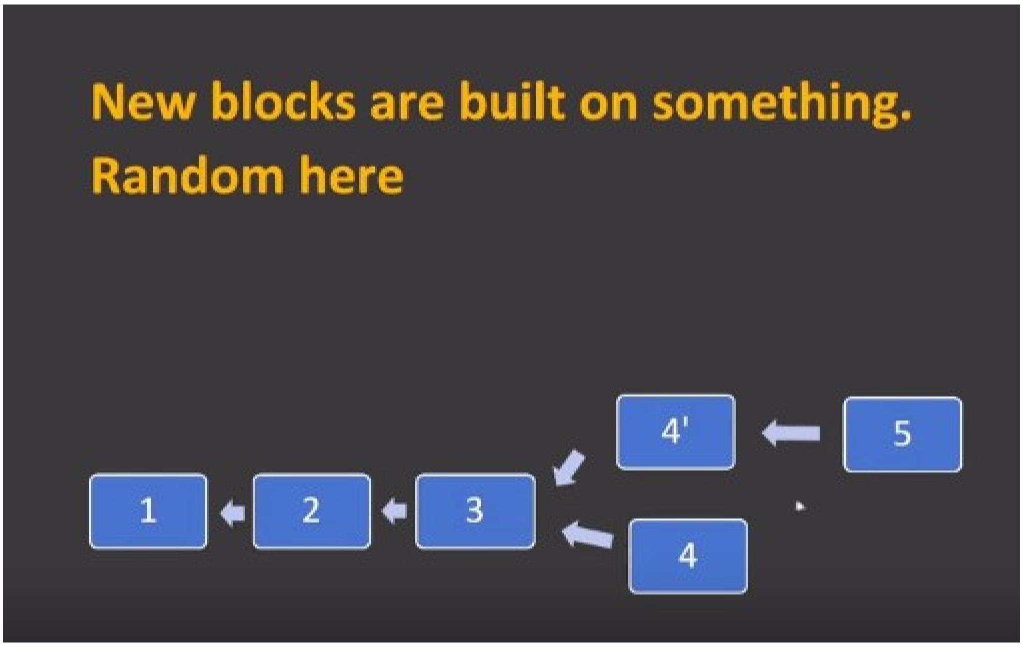
Normal Blockchain



Blockchain with conflict

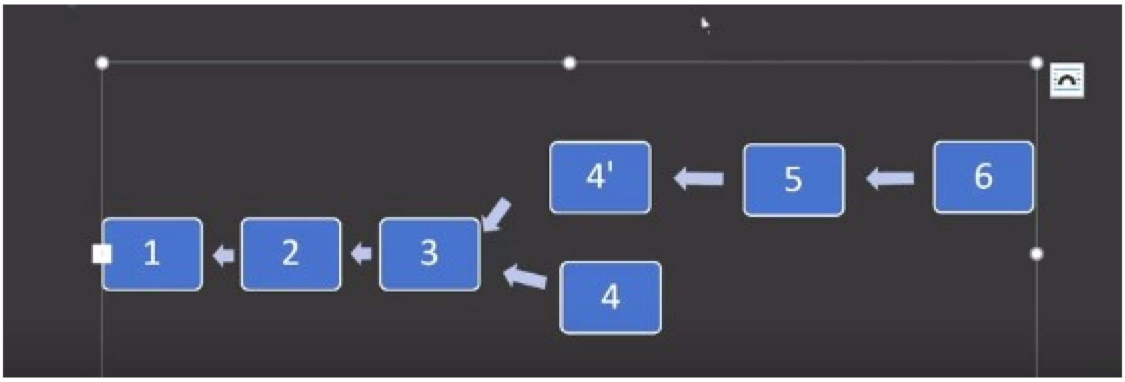


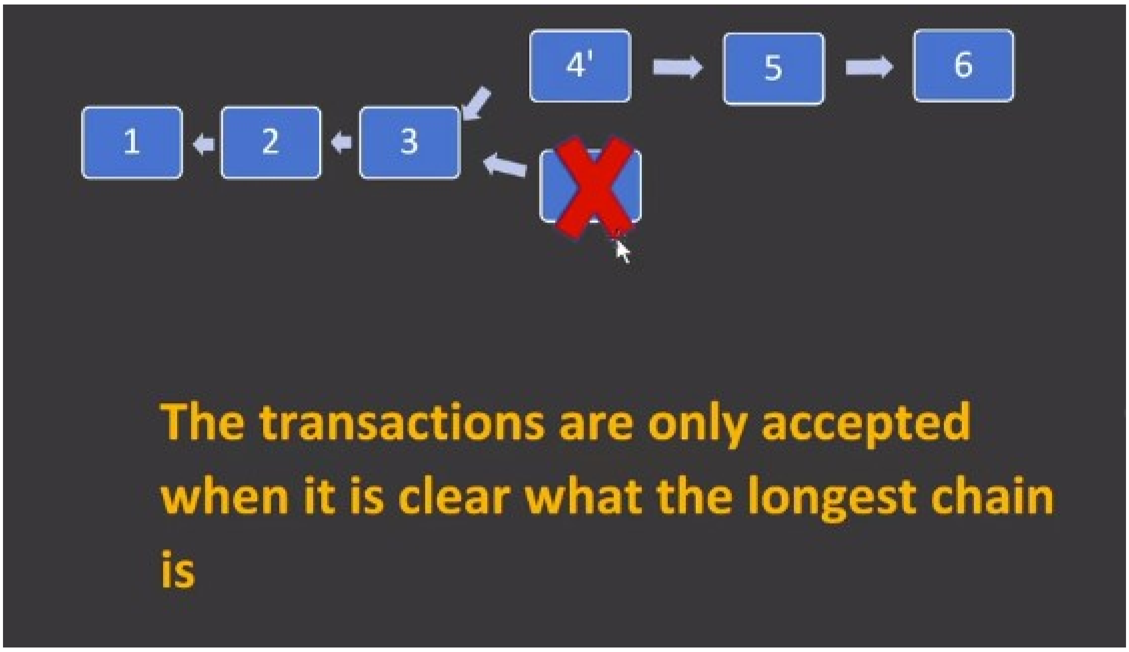
No consensus – the transactions in 4 and 4’ are not approved--- until we have more blocks



New blocks are built on something. Random here

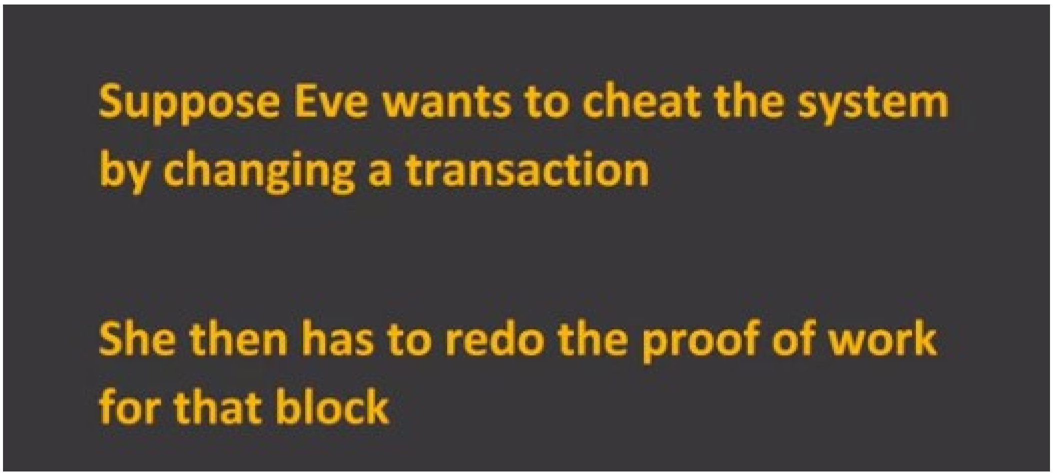
Next block definitely goes on the longest chain





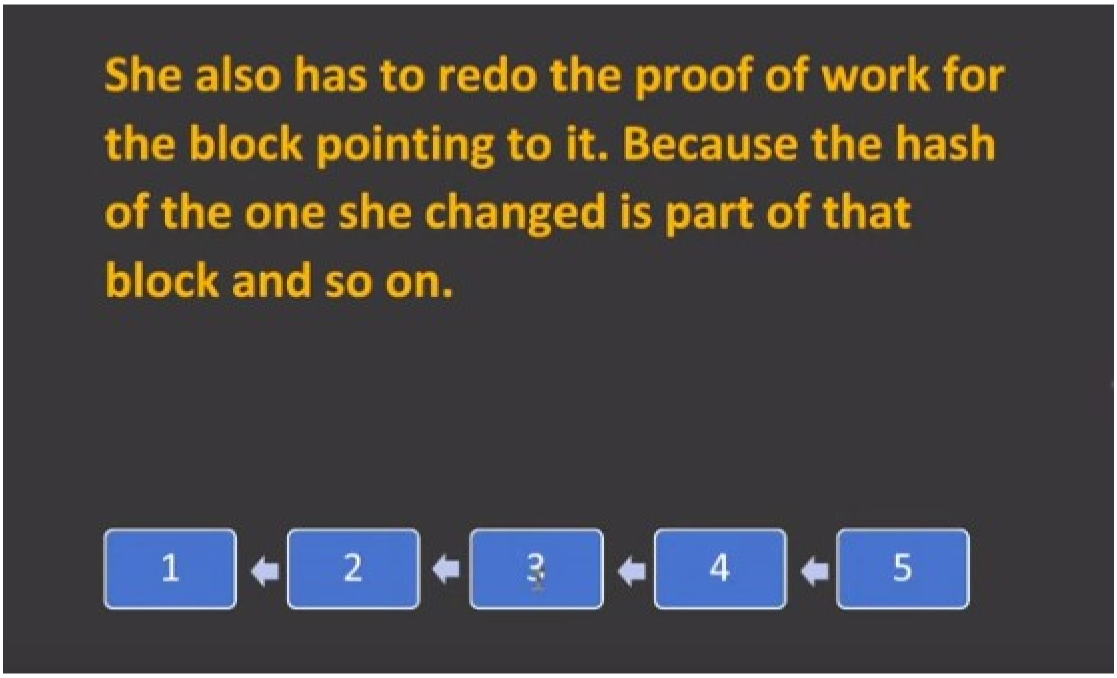
The transactions are only accepted when it is clear what the longest chain is

Immutability of the blockchain

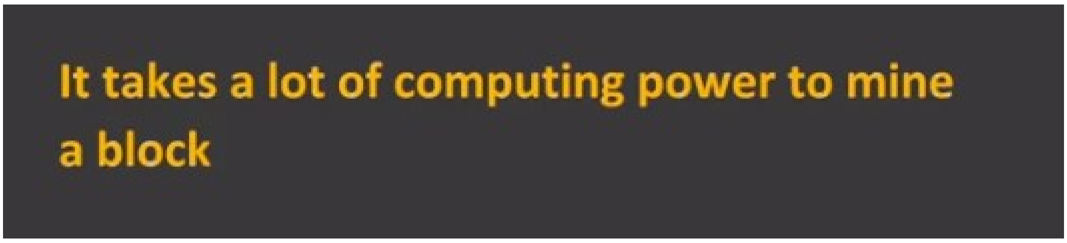


Suppose Eve wants to cheat the system by changing a transaction

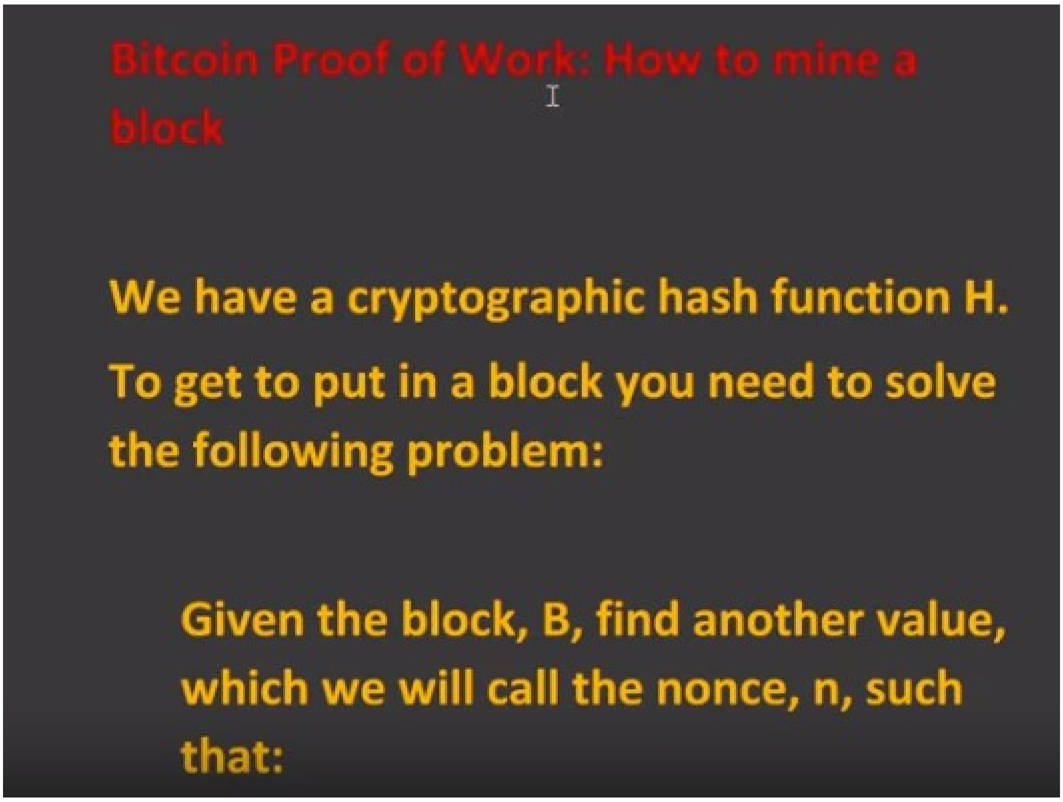
She then has to redo the proof of work for that block



She also has to redo the proof of work for the block pointing to it. Because the hash of the one she changed is part of that block and so on.



It takes a lot of computing power to mine a block

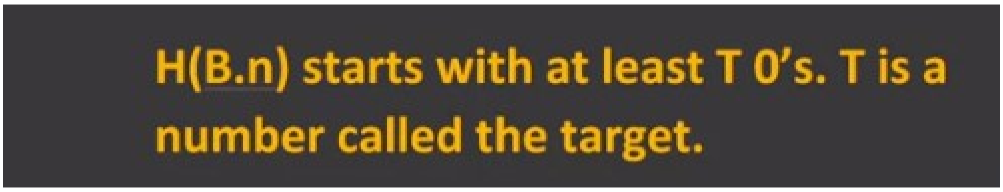


Bitcoin Proof of Work: How to mine a block

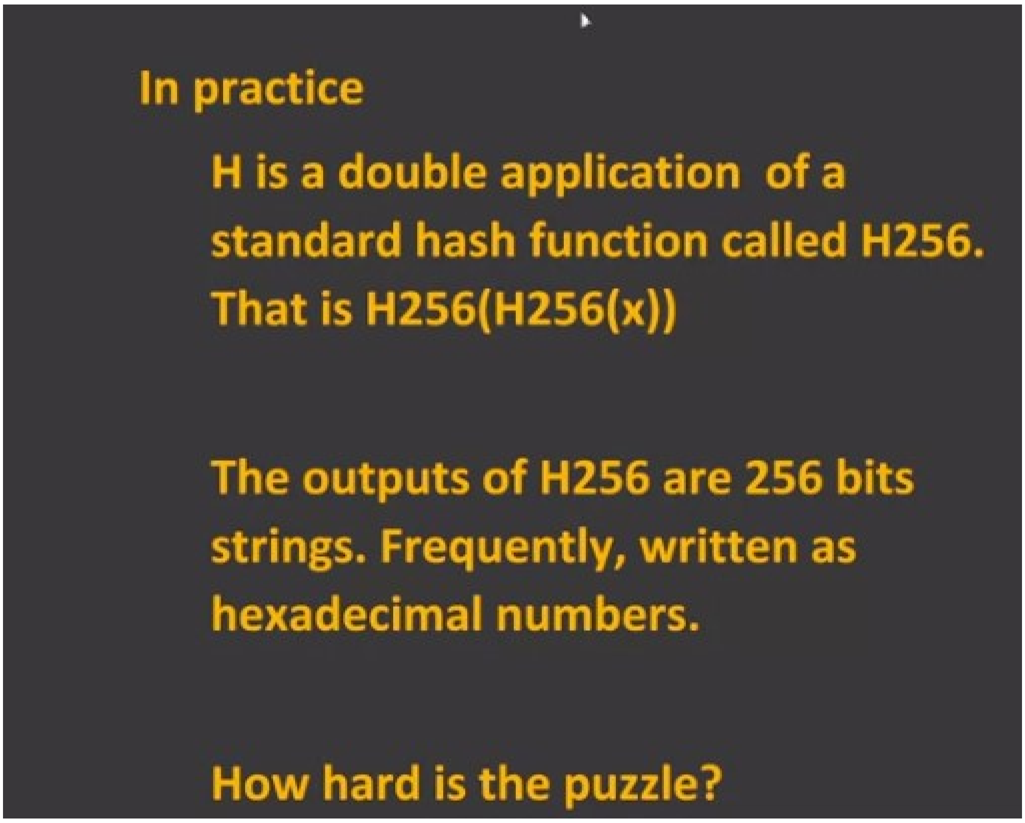
We have a cryptographic hash function H.

To get to put in a block you need to solve the following problem:

> Given the block, B, find another value, which we will call the nonce, n, such that:



H(B.n) starts with at least T 0's. T is a number called the target.

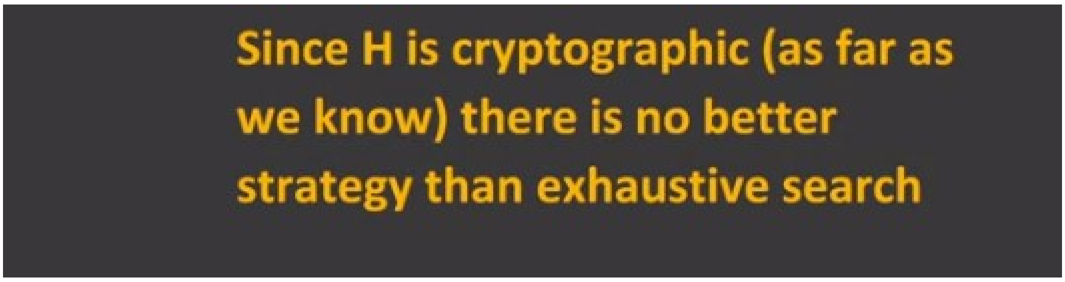


In practice

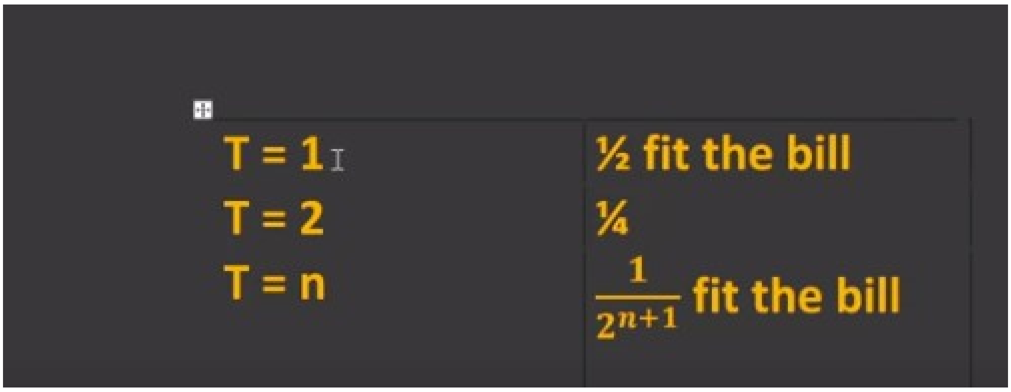
H is a double application of a standard hash function called H256. That is H256(H256(x))

The outputs of H256 are 256 bits strings. Frequently, written as hexadecimal numbers.

How hard is the puzzle?



Since H is cryptographic (as far as we know) there is no better strategy than exhaustive search



T = 1	½ fit the bill
T = 2	¼
T = n	$\frac{1}{2^{n+1}}$ fit the bill