Lecture 4: What is Bitcoin?

Hello and welcome to your fourth lecture, What is Bitcoin?

In this lecture you will learn:

- What is Bitcoin?
- What is a blockchain?
- How do transactions work?
- How does mining work?

We won't be going into any code, but we will dig into a lot of concepts in good detail! This lecture is a bit longer than some of the others but by the end you will be very familiar with Bitcoin.

So, what is Bitcoin? Bitcoin is the first and most popular cryptocurrency. It was founded by the anonymous Satoshi Nakamoto in 2009 and since then has launched a lot of innovation in blockchain technology which underpins its network.

So then what is the blockchain? The Bitcoin blockchain is a massive ledger of transactions. All transactions on the Bitcoin network get recorded on the chain.

The blockchain has "blocks" that get created at certain intervals. Each block contains some data.

Blockchains are "append only" which means they only get larger over time as new blocks get added.

As of July 2017, the full Bitcoin blockchain was about 126 GB

There are a number of implications of the Bitcoin blockchain.

Since every transaction gets recorded on chain with no encryption, transactions are transparent. Every person who runs a full Bitcoin node has a copy of every transaction. This allows anyone to independently verify any transaction.

Block explorers like blockchain.info allow you to view blockchain data without downloading the entire chain.

Every transaction on chain has a unique ID which can be searched and referenced.

Furthermore, since you can view every transaction, you can also see the balance and past transaction history of any address.

This is what a transaction looks like at a high level on the Bitcoin blockchain. There are some inputs and some outputs. You can have a single input go to multiple outputs or you can have multiple inputs go to a single output.

Bitcoin works using these inputs and outputs.

When you receive Bitcoin, you are receiving an input to your address

When you send Bitcoin, you are using outputs to your address to send an input to another address.

Transactions are how unspent outputs in your address are sent as an input to another address.

Your wallet balance is the sum of all unspent outputs to your address.

To send a transaction, you use your wallet's private key to sign a transaction with the desired outputs and an amount.

Signed transactions can only send the exact amount to the address specified and nothing else.

This is what keeps the network secure since you never have to expose your private key.

Wallet software handles the transaction signing for you and broadcasts only signed transactions. You can give signed transactions to anyone and transactions are what get stored in the blockchain.

So where does mining come into play with all of this? Well, mining is the process by which transactions get added to the blockchain. Mining also ensures that transactions are valid and that nobody is creating a fraudulent chain through proof of work. We will talk more about what that means.

Miners verify transactions, bundle transactions into blocks, then solve the proof of work.

The miner who solves the proof of work creates and issues the next valid block to the network. We will talk more about proof of work in the next slide.

After solving the proof of work, the miner gets an unspent output for themselves as a reward. Recall that unspent outputs are the equivalent of coins on the network.

The mining process ensures that nobody is trying to spend an invalid output. In other words, that they actually have the inputs required to create the outputs.

Miners run a lot of checks on transactions to ensure that they are valid.

This link has a full list of everything that miners check in case you are interested.

Proof of Work is a simple, yet powerful concept based on the idea that you have to prove that work was done which gives the Bitcoin network its security.

Proof of work uses a one-way hash function.

A one-way hash function has the property that given a "question", it always produces the same "answer", but given only the "answer", it is impossible to know what the "question" was.

Here is a visual representation of it.

First, you give a hash function some kind of input which could be the string “Dog”.

You feed that string into the specified hash function, which in this case is SHA-256 which is what the Bitcoin network uses. That string then turns into an output. That output is always the same if you give the function the same input. In other words, if you give the function “Dog” it will always produce the string “0eb1..etc”. Given that output string, you cannot tell that the string “Dog” was inputted.

Using the properties of a one-way hash function, Proof of Work is the process by which miners prove they did work.

Miners “ask questions” using this function extremely quickly trying to get a result from the function within certain parameters.

For example, perhaps only outputs where the first 7 digits are 0s are accepted by the network as a valid hash.

This is why when a new block is created, you know a lot of computational work was put into it.

So taking the example of 7 leading 0s, if you find the input which creates that hash, you will have “solved” the puzzle.

Furthermore, the “question” or input you give the function has to include the previous block’s “answer” which creates the “blockchain”

As part of your input you have to include the previous block’s hash

If you want to reverse a transaction that happened in the past, you will have to undo all the blocks that came after that transaction which means you need to have more computational power than the entire network combined.

So that was a lot of information all at once. We will go through a visualization of the same process to better understand it. Here we have 2 blocks that have been mined and their hashes. Note that these are real hashes from the Bitcoin network from blocks 1 and 2 and that everything in these examples are as accurate as possible.

Miners are currently searching for the third block.

Now we see that someone found the hash of the third block that fits the network parameters. As their proof of work, they provide that nonce value. Someone could verify that their proof is valid by executing the SHA256 function themselves.

If the network consensus is that the block is valid or in other words that a majority of the hashrate decides that the block is valid, then miners will begin searching for block #4 using the hash of block #3. Miners cannot start searching for block #4 until block #3 is found.

If block #3 is rejected for whatever reason, then miners will continue mining on block #2’s hash until a valid block comes along.

What is more likely, however, than an invalid block, is two competing chains with different valid blocks. Perhaps some miners are still looking for block #3 when they detect a longer chain which is already searching for block #5.

If block #3 was found on the alternate chain, then it will be “orphaned” as miners abandon the alternate chain for the main chain. The orphaned block could have been valid, but was not included since there was a different block #3 that took its place. The alternate chain dies off and miners move to the main chain.

Mining of some sort is essential for every blockchain based currency. Mining confirms transactions and allows value to be transferred. Mining secures the network ensuring no malicious parties attack the network. Mining also creates the blockchain which serves as the “repository of truth” and universal ledger of events on the network. Mining underpins the trustless consensus that allows Bitcoin and many other digital currencies to function.

And we made it to the end! We went very in depth in this lecture, but it will serve as an extremely useful starting point for analyzing coins and understanding the space. Many people in the space still do not understand at a fundamental level how Bitcoin works. Simply knowing the information this lecture puts you ahead of most people in the space. This concludes the fourth lecture, What is Bitcoin. Thanks and we hope you found this lecture helpful!

