**Lecture 6 Notes**

Slide 3

* If you are wondering what the “hash pointer” means, we will get there in a bit.
* As you may have guessed by now, this is what the structure of the blockchain is based on. A blockchain is basically a linked list. Let’s see what the blockchain structure looks like:
* The blockchain is a linked list that contains data and a hash pointer that points to its previous block, hence creating the chain.
* What is a hash pointer?
* **A hash pointer is similar to a pointer, but instead of just containing the address of the previous block it also contains the hash of the data inside the previous block**.

Slide 4

* This one small tweak is what makes blockchains so amazingly reliable and trailblazing.
* Imagine this for a second, a hacker attacks block 3 and tries to change the data. Because of the properties of hash functions, a slight change in data will change the hash drastically. This means that any slight changes made in block 3, will change the hash which is stored in block 2, now that in turn will change the data and the hash of block 2 which will result in changes in block 1 and so on and so forth. This will completely change the chain, which is impossible. This is exactly how blockchains attain immutability.
* So what does a block header look like?

Slide 6

**A block header contains:**

* Version: The block version number.
* Time: the current timestamp.
* Hash of the previous block.
* Nonce (more on this later).
* Hash of the Merkle Root.
* Right now, let’s focus on the Hash of the Merkle Root. But before that, we need to understand what a Merkle Tree is.

Slide 7

Markle tree

* The above diagram shows what a Merkle tree looks like. In a Merkle tree, each non-leaf node is the hash of the values of their child nodes.
* Leaf Node: The leaf nodes are the nodes in the lowest tier of the tree. So wrt the diagram above, the leaf nodes will be L1, L2, L3 and L4.
* Child Nodes: For a node, the nodes below its tier which are feeding into it are its child nodes. Wrt the diagram, the nodes labeled “Hash 0-0” and “Hash 0-1” are the child nodes of the node labeled “Hash 0”.
* Root Node: The single node on the highest tier labeled “Top Hash” is the root node.

Slide 8 & 9

**So, what does a Merkle Tree have to do with blockchains?**

* Each block contains thousands and thousands of transactions. It will be very time inefficient to store all the data inside each block as a series.
* Doing so will make finding any particular transaction extremely cumbersome and time-consuming.
* If you use a Merkle tree, however, you will greatly cut down the time required to find out whether a particular transaction belongs in that block or not.
* Now suppose I want to find out whether this data belongs in the block or not:
* Instead of going through the cumbersome process of looking at each individual hash and seeing whether it belongs to the data or not,
* I can simply track it down by following the trail of hashes leading up to the data:
* Doing this significantly reduces the time taken.

Slide 11

* Hashing in mining: The crypto puzzles.
* When we say “mining”, it basically means searching for a new block to be added in the blockchain.
* Miners from around the world are constantly working to make sure that the chain keeps on growing.
* Earlier it used to be easy for people to mine using just their laptops, but over time, people started forming mining pools to pool in their computer powers and mine more efficiently.
* This, however, could have been a problem.
* There is a cap for each cryptocurrency, eg. for bitcoin, it is just 21 million.
* There are only 21 million bitcoins out there.
* If the miners can carry on, at this rate, they will fish out all the bitcoins in existence.
* On top of that, there needs to be a specific time limit in between the creation of each blocks.
* For bitcoin, the time limit in between block creation is 10 mins.
* If the blocks could be created faster, it would result in:
* More collisions: More hash functions will be generated which will inevitably cause more collisions.
* More orphaned blocks: If a lot of miners are over mining, they will come up with new blocks simultaneously. This will result in or more blocks not getting to be part of the main chain and becoming orphan blocks.
* So, to restrict block creation, a specific difficulty level is set. Mining is like a game; you solve the puzzle and you get rewards.
* Setting difficulty makes that puzzle much harder to solve and hence more time-consuming.
* WRT bitcoins the difficulty target is a 64-character string (which is the same as a SHA-256 output) which begins with a bunch of zeroes.
* Several zeroes increases as the difficulty level increases.
* The difficulty level changes after every 2016th block.