Anthony Cicero

11/12/20

Guide to Blockchains

Contents

Disclaimer: This was written as a way to improve my understanding of blockchain technology. I am not an expert, and therefore there may be mistakes.

Intro

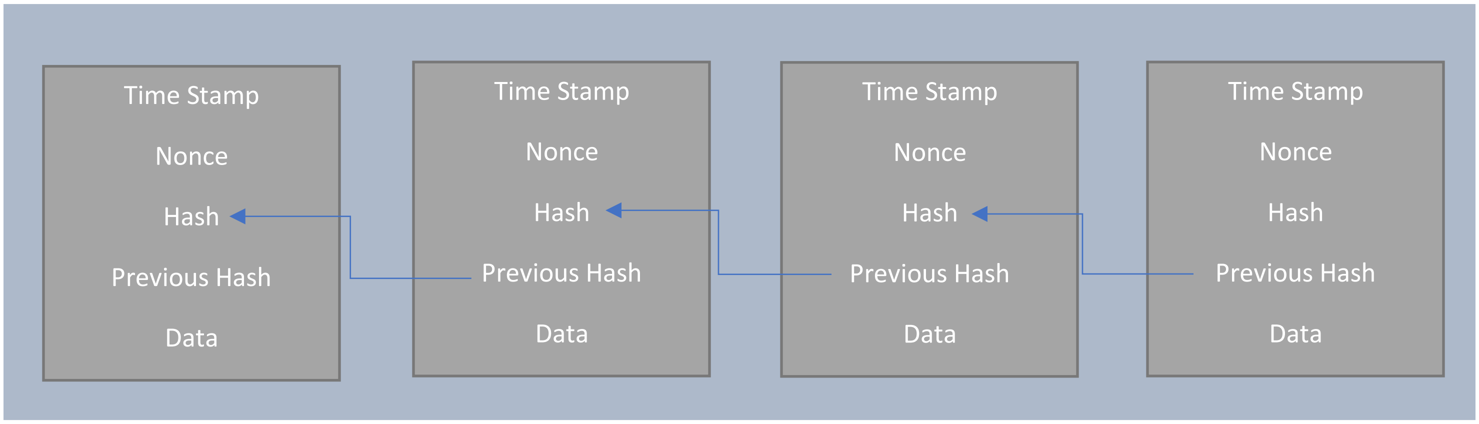
“Blockchains are just fancy linked lists” -Unkown

A blockchain is simply a list of blocks that are linked together with the use of hashes. Blockchains are notorious for being difficult to modify its data.

Blocks

Blocks are the data structure of blockchains. Each Block will contain the data we want to store in the blockchain, along with the components required to maintain the blockchain.

Below is an illustration of a blockchain made up of 4 basic blocks.



Blocks can be comprised of various different elements, but our basic block will consist of 5 components:

1. A **Time Stamp** (seconds since 1970-01-01T00:00 UTC)
2. A **Nonce** value (used for Proof of Work)
3. Some Type of **Data**
4. A **Hash** of the Block
5. The **Hash of the Previous Block** (The first block, called the Genesis block, will have a hash of 0x0)

Data is the information that we would like to store in the block chain.

A **Hash** is the output of an algorithm which maps input Data to a unique fixed length string. In our case, we will be using the SHA256 hashing algorithm, which will return a 256-bit hash value (represented as a 64-digit hexadecimal number).

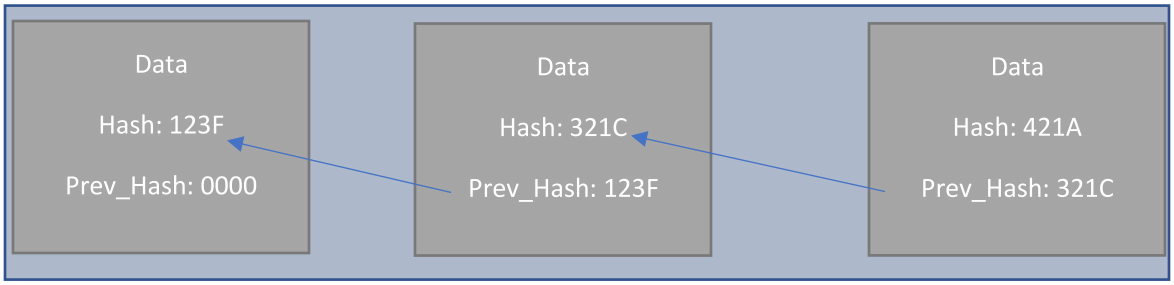
The **Previous Hash** is used to ensure the integrity of the blockchain. This is because if a blocks hash changes, all following blocks will become invalid.

The **Time Stamp** is the time (in seconds since 1970-01-01T00:00 UTC) that the block was added to the blockchain. Time stamps are used in order to add additional variation to the blocks hash, as well as making it more difficult to modify the blockchain. These two functions help to increase security of the blockchain.

The **Nonce** value stands for 'Number used once'. The Nonce is used for something called 'Proof of Work' which is the topic of Section 2.

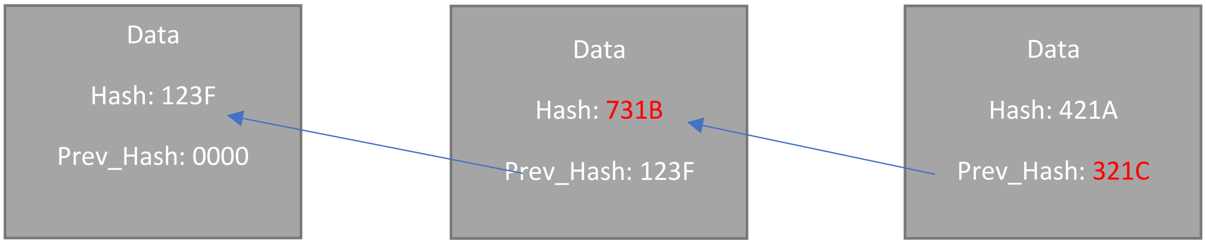
Below is an illustration of the how the Previous Hash is used to link together blocks:

Genesis Block   Block 2   Block 3



Let's say we change the data in Block 2. This will result in a different Hash.

Genesis Block   Block 2   Block 3



Anthony Cicero

Now the Previous Hash of Block 3 no longer matches the hash Block 2. This results in the blockchain being invalid. Therefore, in order for a block to be modified, each following block in the chain will also need to be modified. However, hashing alone does not provide enough protection to ensure the blockchain is not modified. Modern computers can calculate hashes fairly quickly, which is why a **Proof of Work** system is needed to make hashing more difficult.

To be Continued…