Understanding the Blockchain's Chain Of Blocks

Juliano Statdlober Follow
Feb 24 · 4 min read

There is a flood of information about Blockchain around us nowadays, countless books, articles, and videos, indeed. Many people read, write, and talk about it, but maybe only a few experts do understand the working principles behind the "chain of blocks." In my opinion, there are two significant types of content, either too shallow or too deep. In this article, I'll try to explain one of the core concepts of Blockchain plainly and understandably, even for those who are not technical experts.

First of all, before explaining the chain itself, there is another fundamental concept that requires explanation: ***hashing***.

> Hashing is a computing method to identify any dataset uniquely, whatever type of data it be, like image, audio ou text. Hashing generates a random sequence of bits unique to the file that is processed.

If we think of a computer image file, with millions or billions of bits, when a single bit is changed, so is the resulting hash. In computing, one typical use is comparing data, detecting if an image or a piece of text is changed, for instance. Another common use is for storing encrypted passwords in databases. A generated hash is readable by humans in something similar like this: "2e6e504eaf47df8e4c7c9d7109073a2e." Once data is hashed, there is no return. That means that it is not possible to convert hashed content back to the original format.

Well, we have learned so far that with hashing computing, we can uniquely identify a set of data. What's next?

What exactly is a chain of blocks?

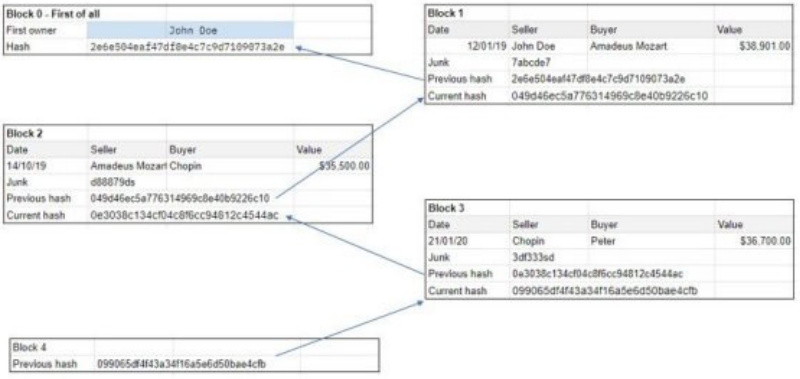
The first information that needs to be understood is that ***blocks are the units that store information in Blockchain***. In a typical Blockchain, blocks contain records of transactions, like money transfers, for example. It is important to stress out, however, that Blockchain is not only suitable for crypto coins, but to record many types of transactions, as transactions for control and transfer of any kinds of assets, as real state properties, cars, documents, etc

All data contained in a block is hashed and uniquely identified, as explained. The resulting hash represents the entire content itself, no matter which data is present. This resulting unique identification becomes the identifier hash of the block.

> Here is where the trick happens: the next block in the chain will keep that unique id from the previous one, and so on. Each block in the chain has its unique identifier and the identifier of the previous one.

There is another essential aspect in the recipe: each block's unique identifier contains the hash id of the previous one included as part of data, and therefore as its hash id.
Sounds confusing? Maybe it is. Perhaps this is why so many people pretend to understand Blockchain but do not.

Maybe it will be easier to understand with the help of the following figure. Let's assume a hypothetical simple chain with only five blocks.



As shown in the figure, each ID has a link to the previous. For example, refer to the current hash of Block 2: 0e3038c134cf04c8f6cc94812c4544ac; Block 3 has a reference for it as the previous ID.

At this moment, it is not relevant to worry about all other structures of Blockchain, as we are focusing solely on the chain structure. I intend to approach other concepts further. I think that it is crucial to understand the foundation first.

The topmost important take-away is, therefore, about how the chain works. You probably might be asking yourself, why is this important?

A key aspect of Blockchain is its ability to assure data integrity, or in other words, to detect if any data was changed. How does this work?
As mentioned, the computed hashing is the result of the data including the previous block's ID. First, let's review the original Block 2:

Block 2			
Date	Seller	Buyer	Value
14/10/19	Amadeus Mozart	Chopin	$35,500.00
Junk	d88879ds		
Previous hash	049d46ec5a776314969c8e40b9226c10		
Current hash	0e3038c134cf04c8f6cc94812c4544ac		

Now let's observe that changing only one dollar in the price will result in a completely different hash:

Block 2			
Date	Seller	Buyer	Value
14/10/19	Amadeus Mozart	Chopin	$35,501.00
Junk	d88879ds		
Previous hash	049d46ec5a776314969c8e40b9226c10		
Current hash	13c3e85349945034 1f9c59e78301ee3a		

According to this principle, any change in the data will result in different hash and imply that something was changed.

> More important is to stress out that, as each block's hash contains the previous one as its content, any change in one block will affect all subsequent blocks.

In other words, if a single change occurs in any block of a chain, all subsequent blocks will be affected and changed.
So we have the foundation concept that enables data integrity in Blockchain.
In further articles, I intend to explain other important concepts that may help a full understanding of this technology.

Originally published at https://www.datadriveninvestor.com on February 24, 2020.

Blockchain