Blockchain Data Structure

In this lesson, we well discuss the data structure of blockchain

WE'LL COVER THE FOLLOWING

What is blockchain?

In a blockchain system, data is stored in blocks of transactions. The most common definition is as follows:

> A timestamped log of transactions that is replicated on multiple peers.

Distributed Consensus

Now, some of these peers might be evil and intentionally report a tampered version of blockchain data. The entire network uses democracy to come to a consensus on the current state of data and any non-conformant or outlier peers are ignored/blocked.

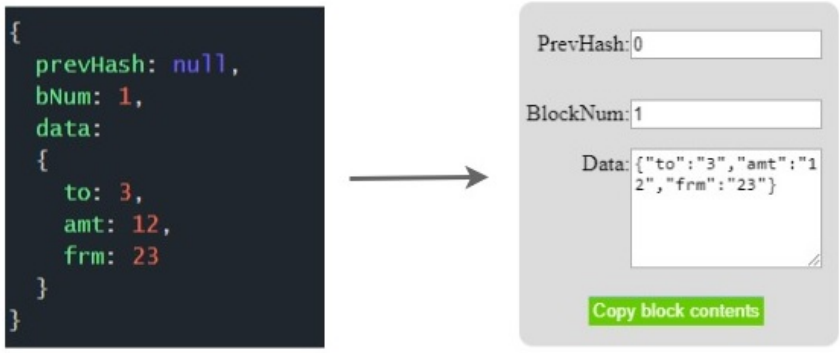
This means that in order for a blockchain network to be fair and valid, most of the nodes have to be fair. If 51% of the nodes are compromised the network is hacked. Since the networks are globally distributed, this is not a possibility.

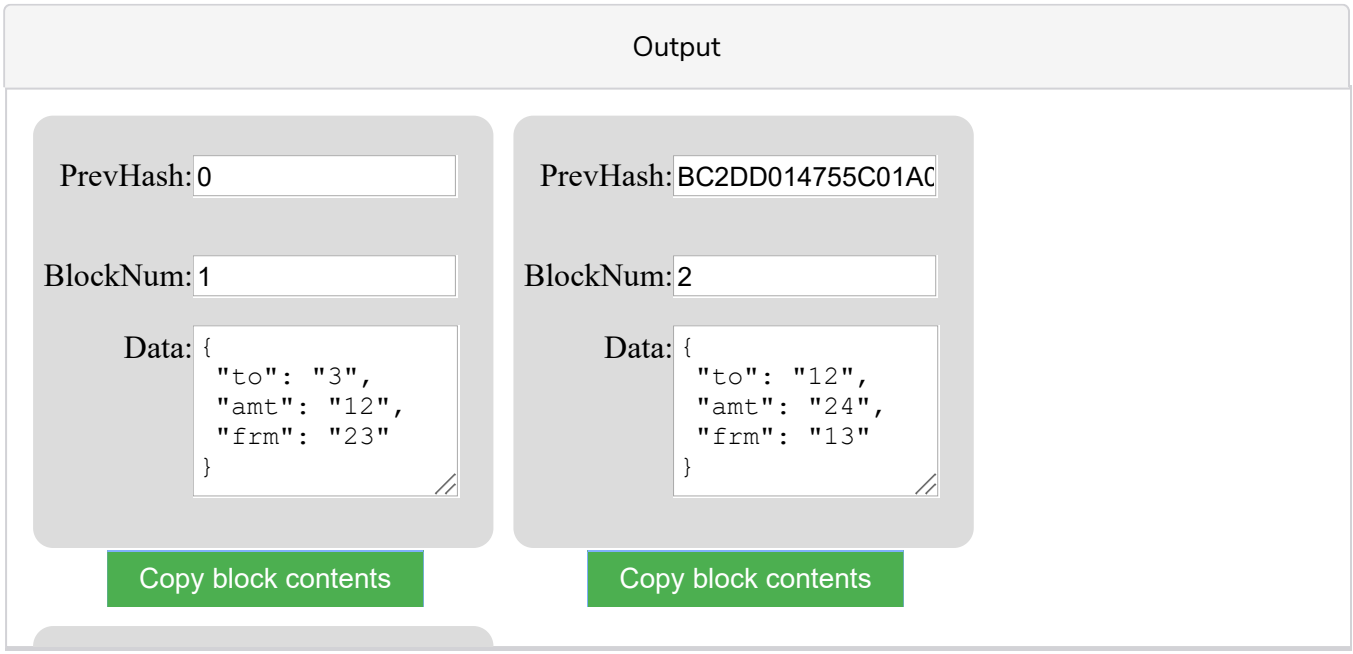
Data Storage in Blocks

Let’s see how blockchain stores data in blocks. Each block stores a data

blob(which is usually a list of transactions), its block number, and hash of the previous block:

Each block is represented by a json object here for better understanding:





Let's look at the previous block hash, referenced as "prevHash" in the above diagram.

When creating a new block, the hash of the previous block is calculated and added to the next block. Now if the previous block is altered later in time, the next block will be invalid as the prevHash stored in it will not match the actual hash of previous block.

Using one-way hash functions, the data in the blockchain is safeguarded from tampering.

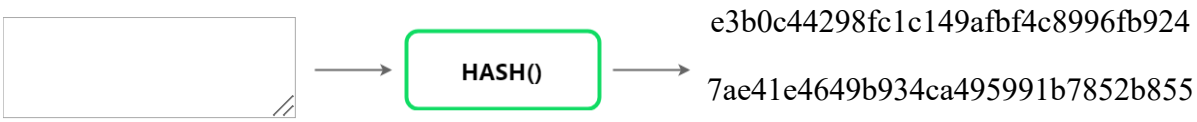
Activity:

Imagine that there are three more transactions to be recorded and a new block needs to be added to the block data structure shown above. What should be the value of PrevHash in new BlockNum 4.

Use the hashing widget below to help calculate your answer.

Check Answer View Hint

Output



Test Yourself

1 What does each block in a blockchain represent?

COMPLETED 0%

1 of 2

In the next lesson, we will see the blockchain playground.