**Lesson Plan – Creating Blockchain Class**

**Learning objectives -**

1. **Revise concepts of block hash creation from previous class**
2. **Creating Blockchain Class**

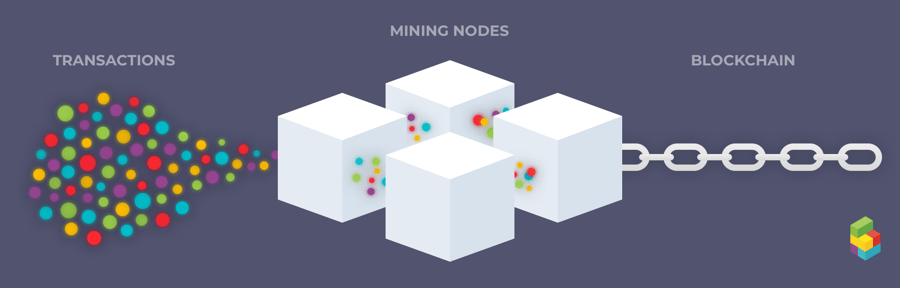
**Materials required -**

**repl.it login credentials**

**Gathering Blockchain Transactions**

The magic of blockchain is that it’s a secure digital ledger that records transactions in chronological order. In this exercise, we’ll explore how blockchain transactions are handled.

As transactions are carried out, they get placed in a special location called the *mempool* that collects all these unvalidated transactions. The latest transactions in the mempool are broadcasted to all blockchain participants.



Each participant collects these transactions into a new block. However, each block can only hold a limited number of transactions. Therefore, not all transactions can be added to a block at once.

Once a block is full, the next set of transactions will have to wait in the memory pool. At this point, the block is said to be unconfirmed, and the transactions inside the block are said to be invalidated.

Next, we’ll explore how blocks are added to the blockchain!

Note: Our course is explaining a very general approach to implementing blockchain technology. The way that the blockchain handles and verifies transactions can be customized to fit various applications, such as the oh so cute [Cryptokitties](https://www.cryptokitties.co/).

[**https://www.blocknative.com/blog/mempool-intro**](https://www.blocknative.com/blog/mempool-intro)

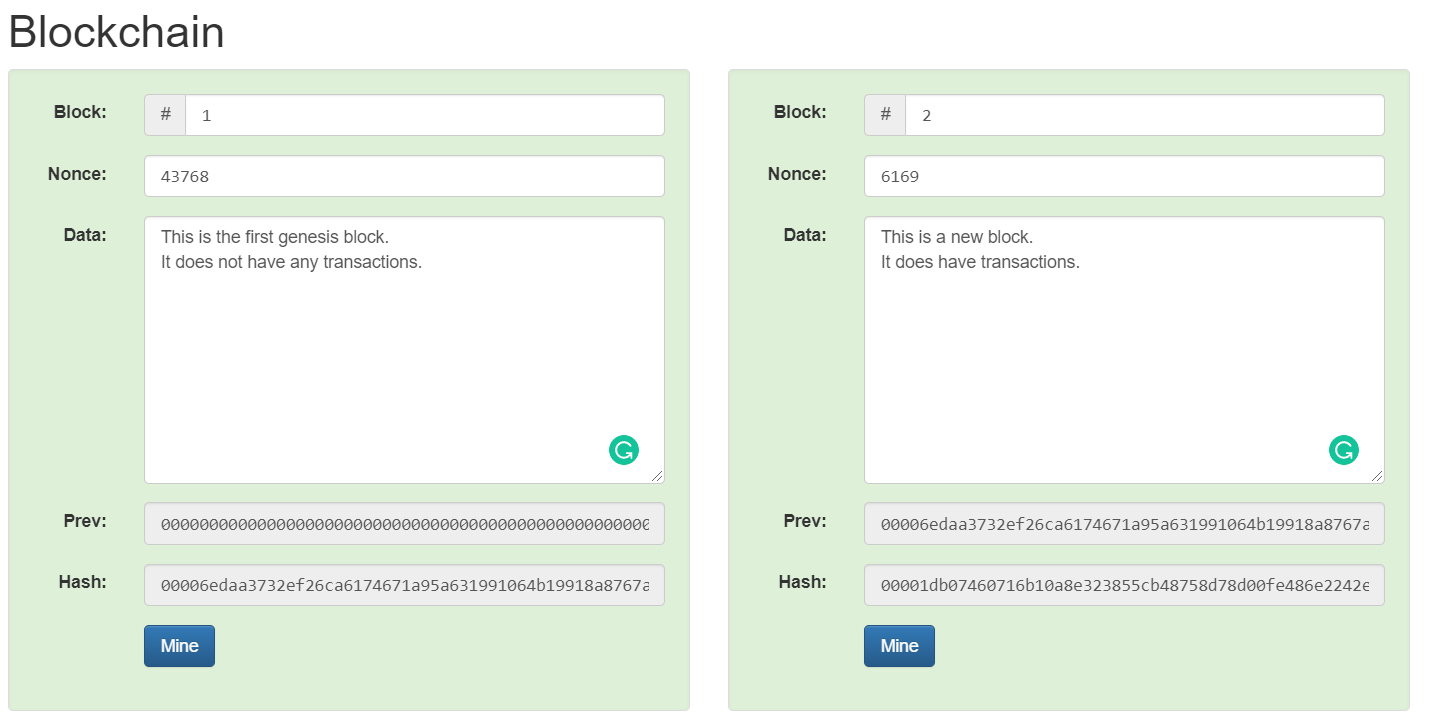
**Creating the Blockchain Class**

In a distributed blockchain, we would have specific nodes doing the mining. These nodes will be listening for new data or transactions being broadcasted in the network and will keep trying to find the nonce value that makes the block valid. When a miner finds this nonce value, it will broadcast the new block to the network. It is easy for all the other nodes in the network to verify if the block is valid because all they have to do is apply the hash function to the block with the given nonce. If the block starts with X number of zeroes, the block is valid.

A key rule of our distributed blockchain is that if a node receives two conflicting blocks, and both have valid hashes, it must trust the block with the longest history.

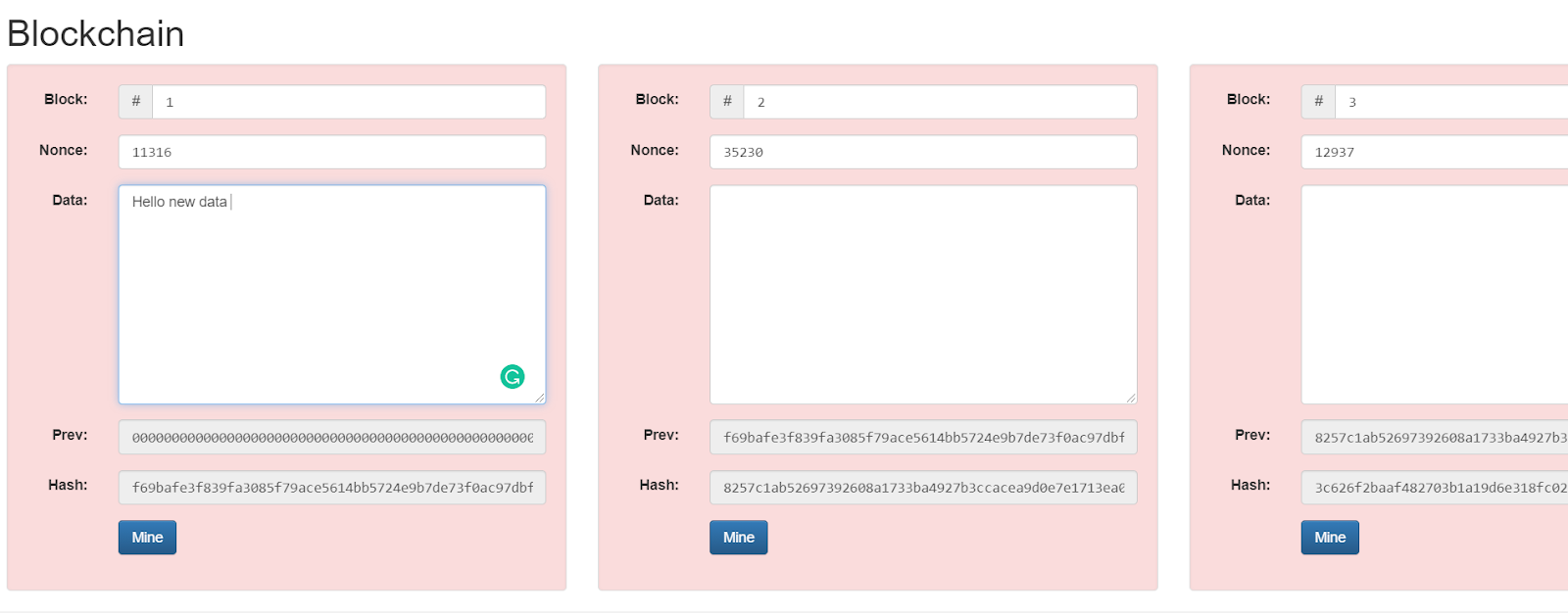
We can represent the blockchain as an object. We are using objects for our implementation, because they offer the flexibility to create specific attributes and methods. Representing it as an object also allows us to create blockchain instances for each computer participant.

Blockchain demo : <https://andersbrownworth.com/blockchain/blockchain>



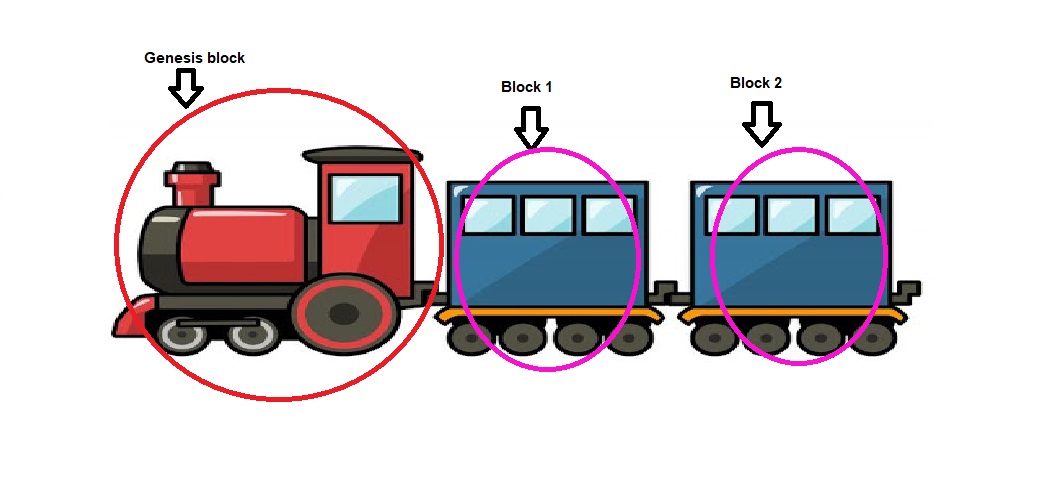
Block number 1 contains information such as Block, Nouce, Data, Prev (Previous hash) and Hash.

Similarly in block 2 have the same information.



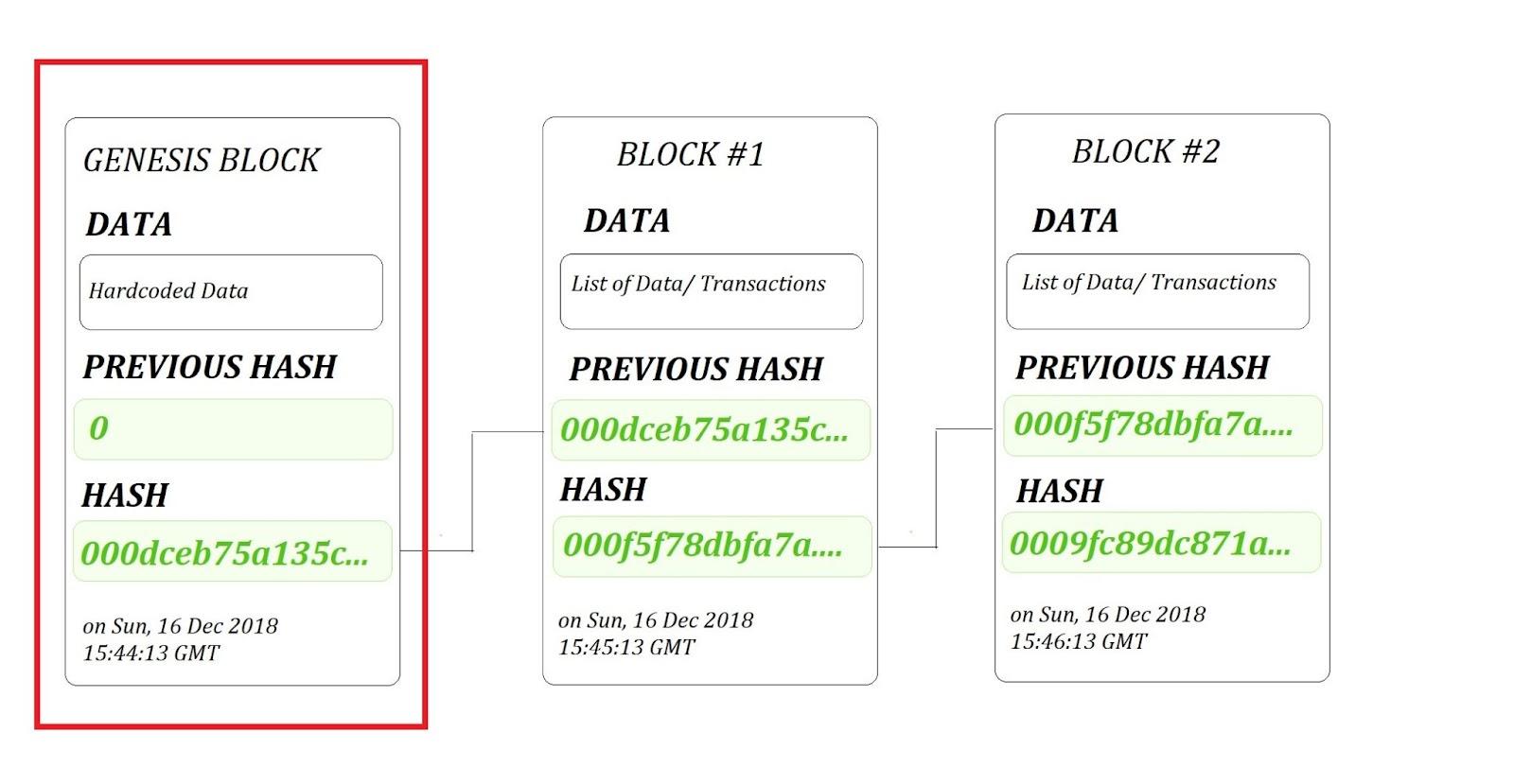
Here if we change any block data then the block turns red. Since the information which we are feeding in is not valid.

Blockchain is nothing but a transaction process where each new transaction gets added to the block and then it appears on the block.



Here you can see the engine is our genesis block and block 1 and block 2 are coaches of our train.

Let’s understand what we have in the Newly added block.



Here you can see we have the genesis block attached to block 1 and then block 1 is attached to block 2. You can see data in the BLOCKCHAIN #1 block is a list of data/Transactions . Which contains the name of the sender, name of recipient and amount of the transaction but the previous hash is not available but in the subsequent blocks the previous hash is updated with respect to the hash value of it’s previous block.

**Difference between hashing and Encoding :**

Encoding is the process where we transform original text format to new non-readable format. Just like hashing. But the difference between encoding and hashing is:

* Hashing is a one way procedure where we can't convert back the hash to a normal image.
* But in case of encoding we can convert back the hash to the original text. And the process of going back to the original text is now decoding.
* Decoding is the opposite of the encoding method where we get original text from encoded text.

**Key Terms:**

* **Transactions:** An exchange of value among participants on the blockchain network.
* **Participants:** Individuals accessing the blockchain network through computers to exchange value.
* **Unconfirmed:** Blocks and transactions that are yet to be verified.

Introducing the lesson/project including the concepts (Time - 45 min)

Activity link:

Link to Repl it Project :

<https://replit.com/@PriyankaJetLea1/Lesson5CreatingBlockchainclass>

**Homework –**

In this project, we want you to write a program to calculate the number of blocks present in the Blockchain and Print the Hash code of each Block present in Blockchain and verify the Current Hash code with the previous Hash Codes of the Block to verify the Transactions by using the below mentioned steps:

● Calculate Number of Blocks.

● Print the Hash of Each Block

● Verifying the Hashcode of

Current and Previous Block

**Solution link** : <https://replit.com/join/hhayinohrt-priyankajetlea1>