1. Kefa Kioge 22/00627 BBIT
2. George Ndegwa 22/00714 BBIT
3. Gitonga Victor Mutwiri 18/02659 BBIT
4. Edwin Kagiri Maina 22/08702 BIT
5. David Mugendi Nthuni 22/00381 BIT

GITHUB Link: <https://github.com/KefaKioge/Cryptocurrency-Project>

This document provides a more detailed explanation of the Cryptocurrency focusing on the functionalities of the Hadcoin blockchain and cryptocurrency.

**Functional Requirements:**

* **Block Creation:** The system allows the creation of new blocks on the blockchain. This involves functionalities like:
  + **Proof-of-Work (PoW):** The system implements a PoW mechanism to ensure slow block creation and deter malicious activities.
  + **Transaction inclusion:** The system allows adding new transactions to a pool waiting to be included in a block.
  + **Block validation:** The system must validate the integrity of new blocks before adding them to the chain. This includes verifying the PoW and ensuring proper linking between blocks.
* **Blockchain Management:**
  + **Chain retrieval:** The system allows retrieving the current state of the blockchain (all blocks).
  + **Chain validation:** The system provides functionality to check the validity of the entire blockchain based on defined consensus rules.
* **Transaction Management:**
  + **Transaction creation**: The system allows users to create new transactions specifying sender, receiver, and amount.
* **Network Management:**
  + **Node addition**: The system allows adding new nodes (computers running the blockchain software) to the network.
  + **Chain synchronization:** The system enables nodes to synchronize the blockchain with the longest valid chain identified in the network.

**Dependencies**

1. import datetime**:**
   * This line imports the datetime module from the Python standard library.
   * This module provides functionalities for working with dates and times. In the code, it's likely used to get the current timestamp when creating a new block (create\_block function) to record when the block was mined.
2. import hashlib**:**
   * This line imports the hashlib module from the Python standard library.
   * This module provides functions for various cryptographic hash algorithms. In the code, it's most likely used for the SHA-256 hashing function (hash function) to create a unique fingerprint for each block's data, ensuring data integrity and immutability.
3. import json**:**
   * This line imports the json module from the Python standard library.
   * This module provides functions for encoding and decoding JSON (JavaScript Object Notation) data format. In the code, used for:
     + Converting block data into a JSON string before hashing it (hash function).
     + Decoding JSON data received from API requests (e.g., adding transactions).
4. from flask import Flask, jsonify, request**:**
   * This line imports specific functions from the Flask web framework library.
   * Flask is a lightweight web framework for building web applications in Python. Here's what's imported:
     + Flask: This creates a Flask application instance used to define routes and handle requests.
     + jsonify: This function converts Python data structures (dictionaries, lists) to JSON format for sending responses through the web API.
     + request: This object provides access to information from the incoming web request, such as data sent from the user.
5. import requests**:**
   * This line imports the requests library, a popular external library for making HTTP requests in Python.
   * In the code, it's likely used in the replace\_chain function to:
     + Send HTTP GET requests to other nodes in the network to retrieve their blockchain information.
     + Compare the retrieved chains with the local chain to identify the longest valid chain.
6. from uuid import uuid4**:**
   * This line imports the uuid4 function from the uuid module (also part of the standard library).
   * The uuid module deals with generating Universally Unique Identifiers (UUIDs).
   * In the code, uuid4 is probably used to generate unique node addresses (node\_address) for each machine running the blockchain software, ensuring proper identification within the network.
7. from urllib.parse import urlparse**:**
   * This line imports the urlparse function from the urllib.parse module (standard library).
   * The urllib.parse module provides functions for parsing URLs into their components (scheme, hostname, port, etc.).
   * In the code, urlparse is likely used in the add\_node and replace\_chain functions to:
     + Extract relevant parts (like hostname) from the URLs of other nodes provided when connecting them to the network.

**Part 1 – The Blockchain Build:**

The Blockchain class is the heart of the Hadcoin system.

\_\_init\_\_(self)**:**

* + Initializes an empty list for the chain to store blocks.
  + Initializes an empty list for transactions that wait to be included in a block.
  + Creates the Genesis Block (block number 1) with a proof of work of 1 and a previous hash of '0' (as there's no preceding block).
  + Initializes an empty set named nodes to store the addresses of connected nodes in the network.

1. create\_block(self, proof, previous\_hash)**:**
   * This function creates a new block on the blockchain. It takes two arguments:
     + proof: The result of the Proof of Work (PoW) algorithm (explained later).
     + previous\_hash: The hash of the previous block for linking blocks together and maintaining chronological order.
   * The function creates a dictionary containing information about the new block, including:
     + index: The index (position) of the block in the chain (starts from 1).
     + timestamp: The current date and time when the block was created.
     + proof: The PoW result used in mining this block.
     + previous\_hash: The hash of the previous block.
     + transactions: A list of transactions included in this block.
   * After creating the block, it resets the transactions list (as they are now part of the block) and appends the new block to the chain list.
   * Finally, it returns the newly created block.
2. get\_previous\_block(self)**:**
   * This function simply returns the last block in the blockchain (chain) list. This block is used as a reference when creating a new block to link them together.
3. proof\_of\_work(self, previous\_proof)**:**
   * This function implements the Proof of Work (PoW) consensus mechanism, a critical concept in securing the blockchain.
   * It takes the previous\_proof (result from the prior block) as input.
   * The PoW process involves finding a number (called proof) that, when squared and subtracted by the previous proof squared, generates a hash value starting with a specific number of zeros (e.g., '0000' for 4 leading zeros in Hadcoin). This hashing function (SHA-256) is used to create a complex puzzle that requires significant computational power to solve.
   * The function iterates through different values of new\_proof until it finds one that satisfies the hash condition. This process slows down block creation and discourages malicious activities on the network.
   * Once a valid proof is found, the function returns it.
4. hash(self, block)**:**
   * This function takes a block (dictionary) as input.
   * It converts the block dictionary into a JSON string using the json.dumps function.
   * It then calculates the SHA-256 hash of the JSON-encoded block string.
   * The SHA-256 hash function is a cryptographic function that generates a unique and fixed-size alphanumeric string for any given data. This hash serves as a fingerprint of the block's content, ensuring data integrity.
   * The function returns the SHA-256 hash of the block.
5. is\_chain\_valid(self, chain)**:**
   * This function takes a blockchain (list of blocks) as input and validates its integrity according to the defined blockchain rules.
   * It iterates through each block in the chain, performing the following checks:
     + Checks if the current block's previous\_hash matches the hash of the previous block in the chain. This ensures the chronological order and tampering detection.
     + Retrieves the proof from the current block and the previous\_proof from the previous block.
     + Verifies if the current block's hash satisfies the PoW requirement (e.g., starts with '0000' in Hadcoin).
   * If any of the checks fail, the function returns False, indicating an invalid blockchain.
   * If all checks pass for all blocks in the chain, the function returns True, indicating a valid blockchain.
6. add\_transaction**:**
   * Appends a new transaction to the transactions list.
   * Returns the index of the block where the transaction will be added.
7. add\_node**:**
   * Adds a new node's address to the blockchain's nodes set, enabling communication between nodes.
8. replace\_chain**:**
   * Compares the local blockchain with other nodes' chains:
     + If a longer valid chain is found, replaces the local chain to maintain consistency.
     + Ensures consensus across the decentralized network.

**Part 2 - Mining and Web App:**

* **Flask App Creation:**
  + Uses the Flask framework to create a web application for interacting with the blockchain.
* **Node Address Generation:**
  + Uses uuid4 to generate a unique address for the node, used for identification within the network.
* **Blockchain Instance:**
  + Creates an instance of the Blockchain class to manage the blockchain data and functionalities.

**API Routes: Methods**

* mine\_block**:**
  + Performs the Proof-of-Work (PoW) consensus algorithm to mine a new block.
  + Adds a reward transaction to the miner (current node).
  + Creates the block and adds it to the blockchain.
  + Returns block information as a JSON response.
* get\_chain**:**
  + Returns the entire blockchain data as a JSON response.
* is\_valid**:**
  + Checks the validity of the blockchain using is\_chain\_valid and returns the result as a JSON response.
* add\_transaction**:**
  + Accepts a new transaction's details as JSON input.
  + Validates the transaction data.
  + Adds the transaction to the blockchain using add\_transaction.
  + Returns a confirmation message indicating the block where the transaction will be added.

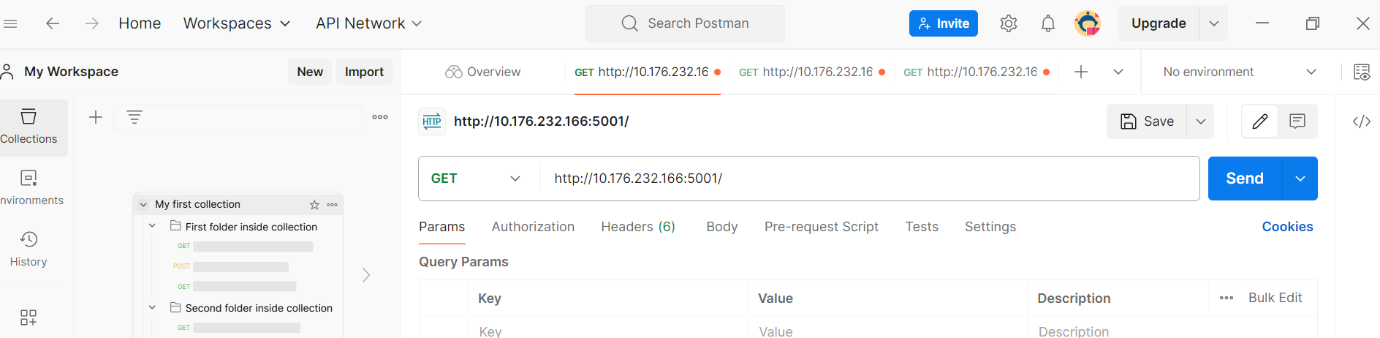
**Part 3 - Decentralization: Methods**

* connect\_node**:**
  + Accepts a list of new nodes as JSON input.
  + Connects the new nodes to the network using add\_node.
  + Returns a list of all connected nodes.
* replace\_chain**:**
  + Triggers the replace\_chain method to check for longer valid chains in the network.
  + Replaces the local chain if necessary to maintain consensus.
  + Returns the updated blockchain information as a JSON response.

**Running the App:**

* Starts the Flask web server on ports 5001, 5002 and 5003, making the blockchain accessible for interaction.

**Step 1: Open the three nodes in postman.**



Node 3

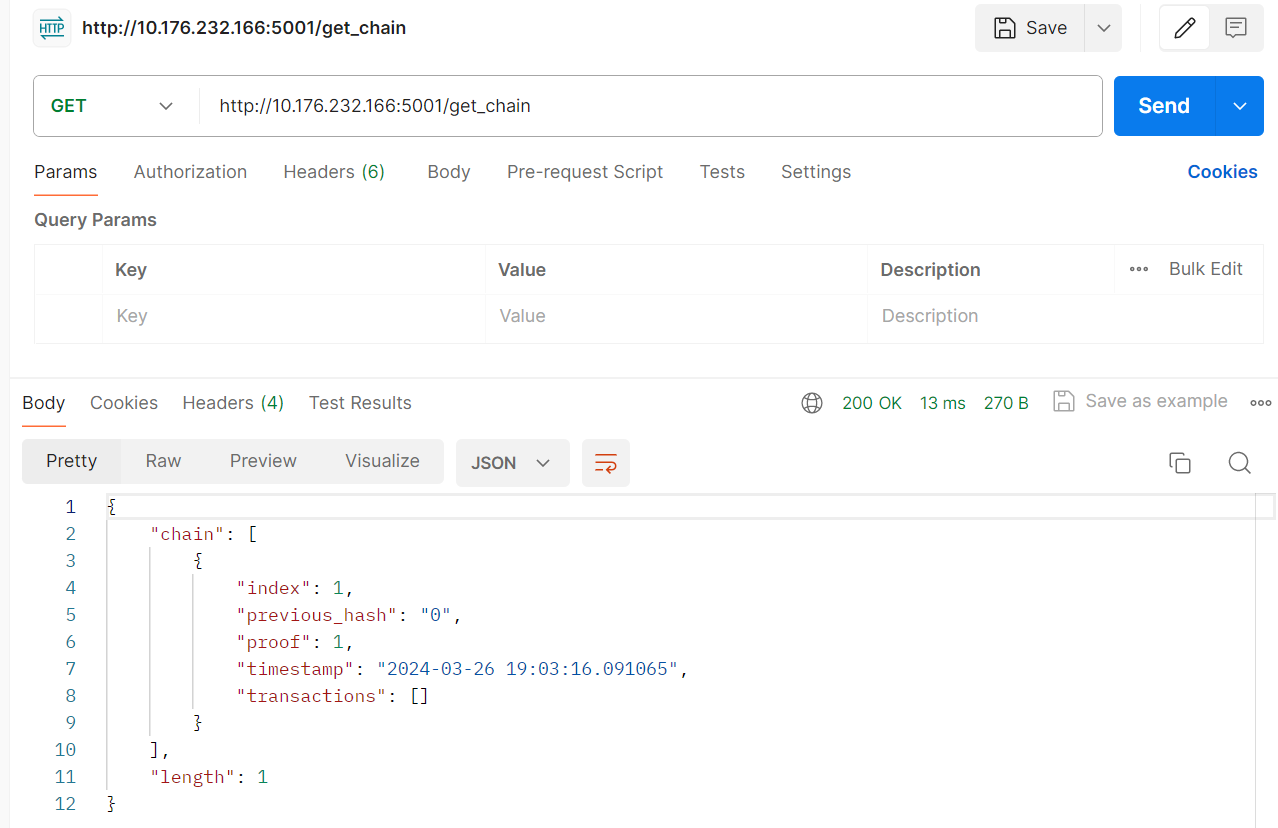
Node 3

Node 3

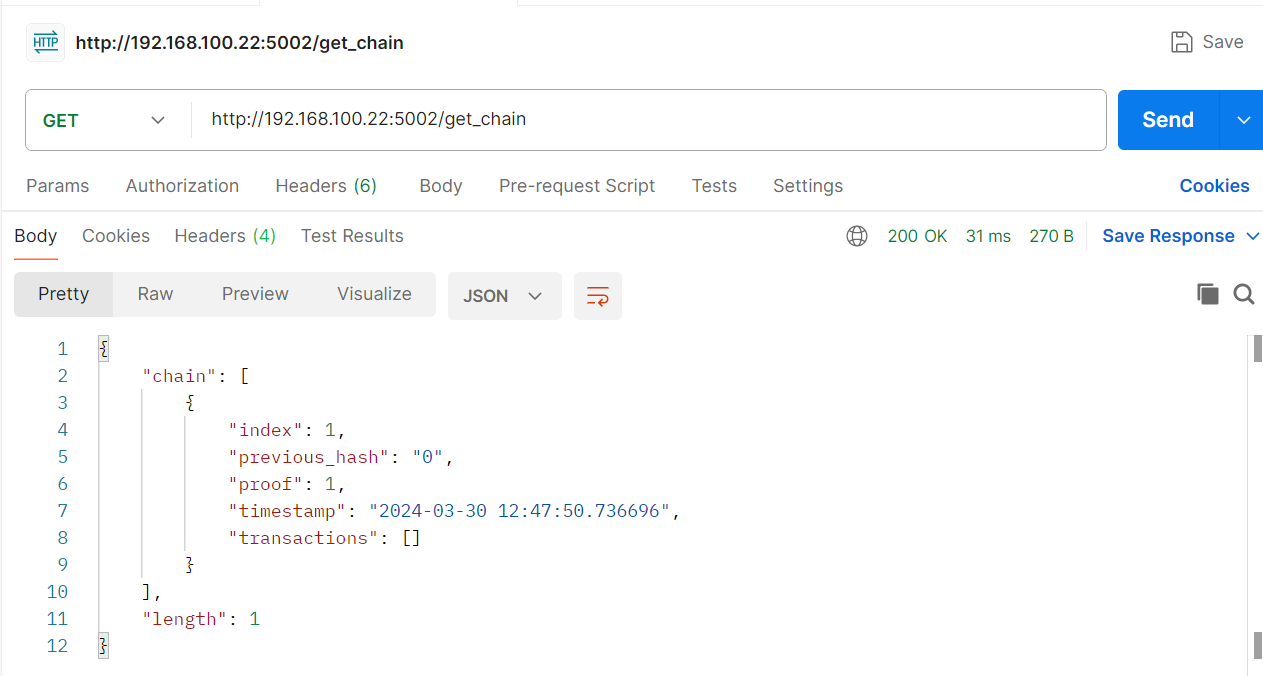
**Step 2: Create a Genesis block**

run the a “GET HTTP Method ” on the postman and run the python method “get\_chain” request in postman for each node. This creates the Genesis block.

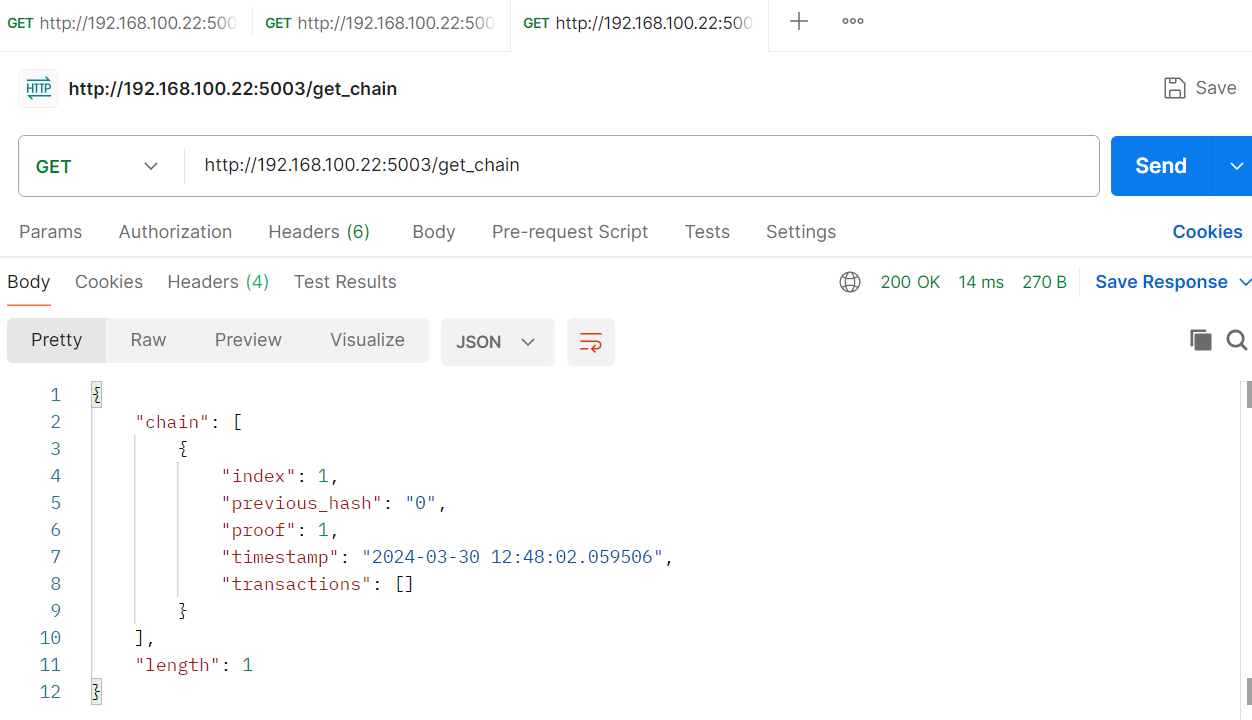
http://10.176.232.166:5001/get\_chain



<http://10.176.232.166:5002/get_chain>



http://10.176.232.166:5003/get\_chain



**Step 3: Connect all the Nodes**.

We will use a POST HTTP Method as follows:

Copy this python code, and paste it to all the nodes as follows:

Body > raw > select > json

Ensure to remove the line for the host node. Example for Node 1 remove this line: "http://127.0.0.1:5001", etc.

{

"nodes": ["http://127.0.0.1:5001",

"http://127.0.0.1:5002",

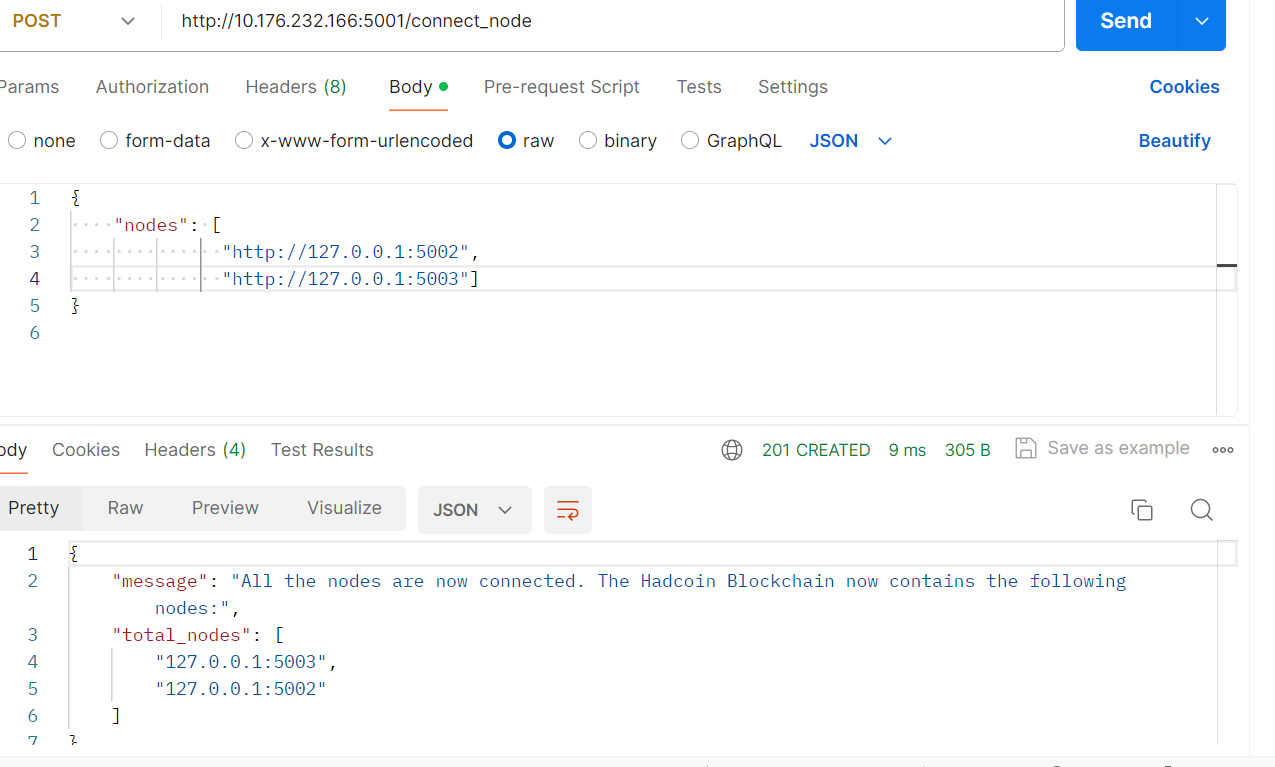
"http://127.0.0.1:5003"]

}

By using a “POST” request, run the following in Postman for every node.

Node 1: http://10.176.232.166:5001/connect\_node

* Node 1 connected



{

"nodes": [

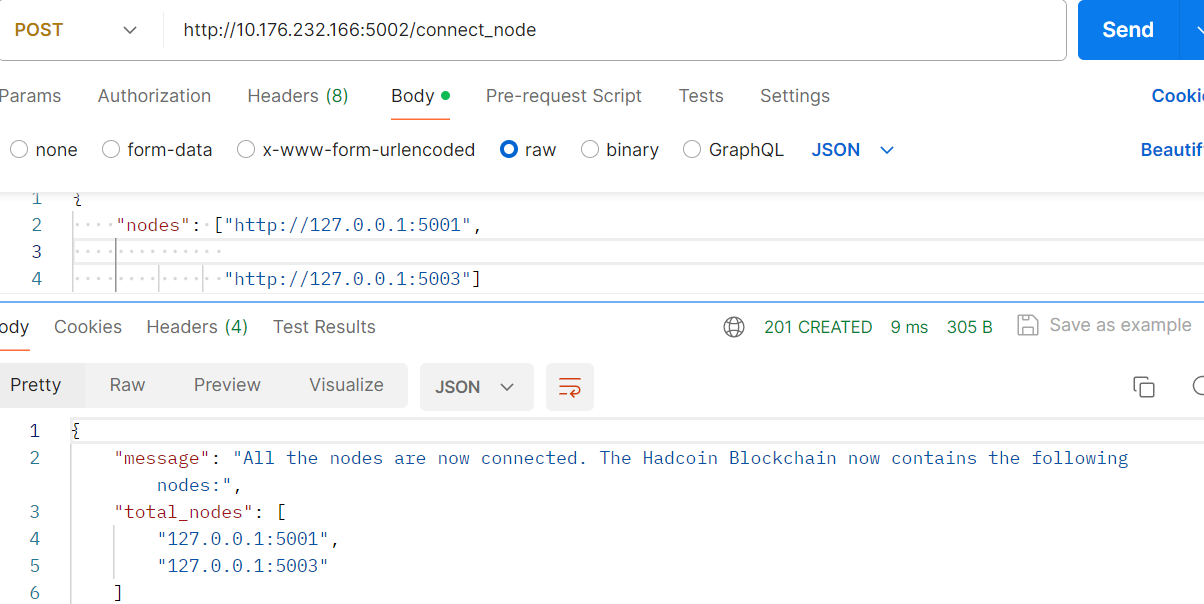
"http://127.0.0.1:5002",

"http://127.0.0.1:5003"]

}

Node 2: http://10.176.232.166:5002/connect\_node

* Node 2 connected



{

"nodes": [

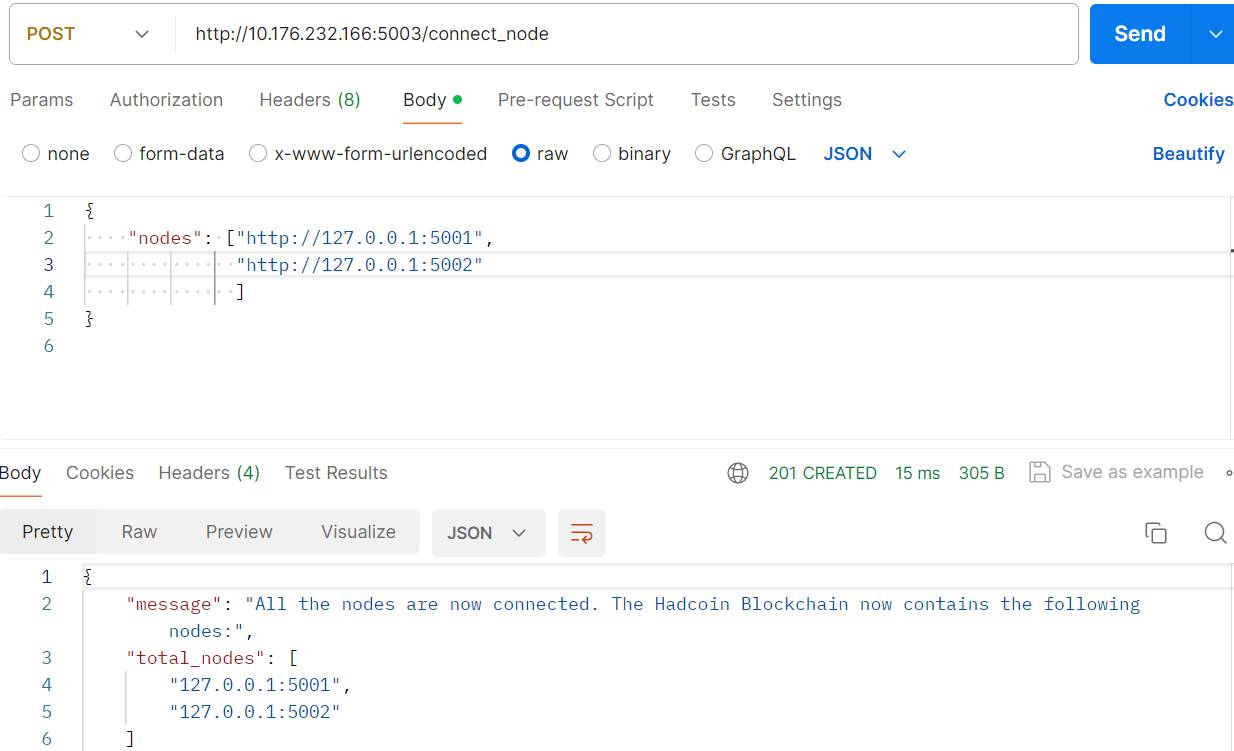
"http://127.0.0.1:5001",

"http://127.0.0.1:5003"]

}

Node 3: http://10.176.232.166:5003/connect\_node

* Node 3 connected



{

"nodes": [

"http://127.0.0.1:5001",

"http://127.0.0.1:5002"]

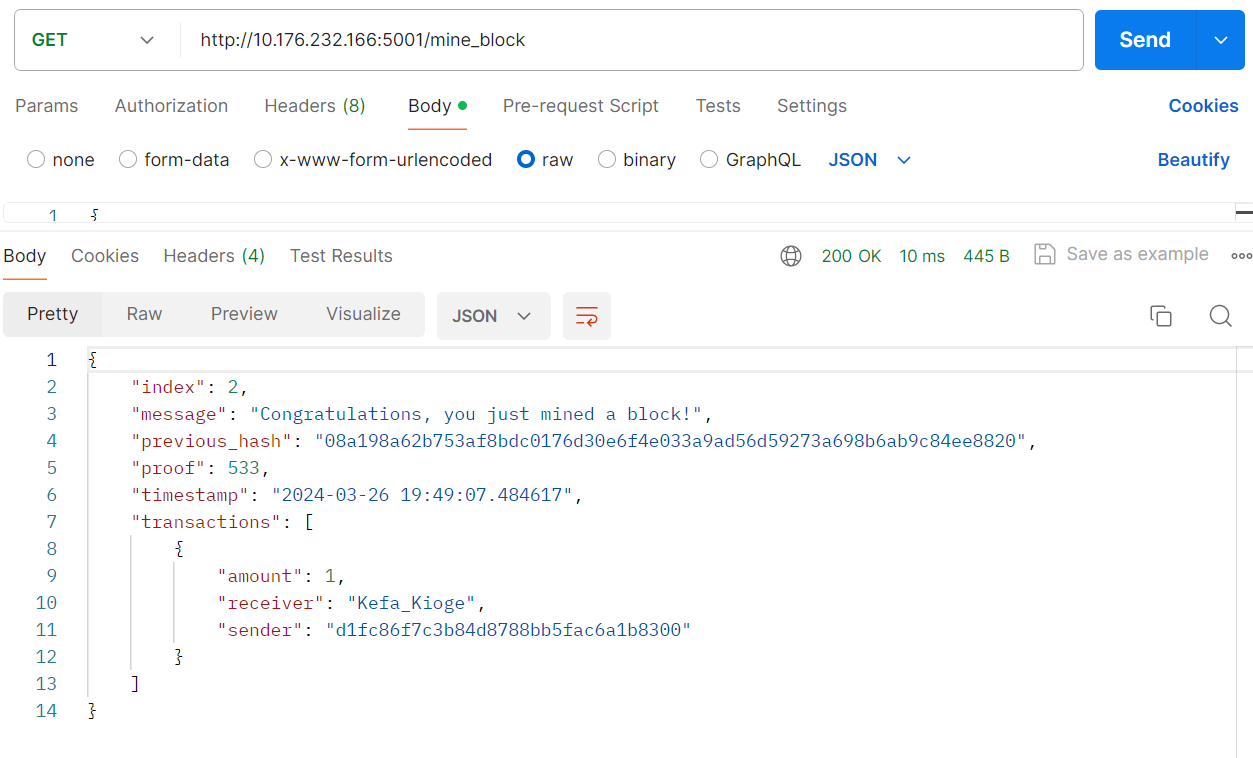
}

**Step 4: Mine a Block from Node 1**

Start by running a “GET” HTTP request and run a “mine\_block” function in node 1.

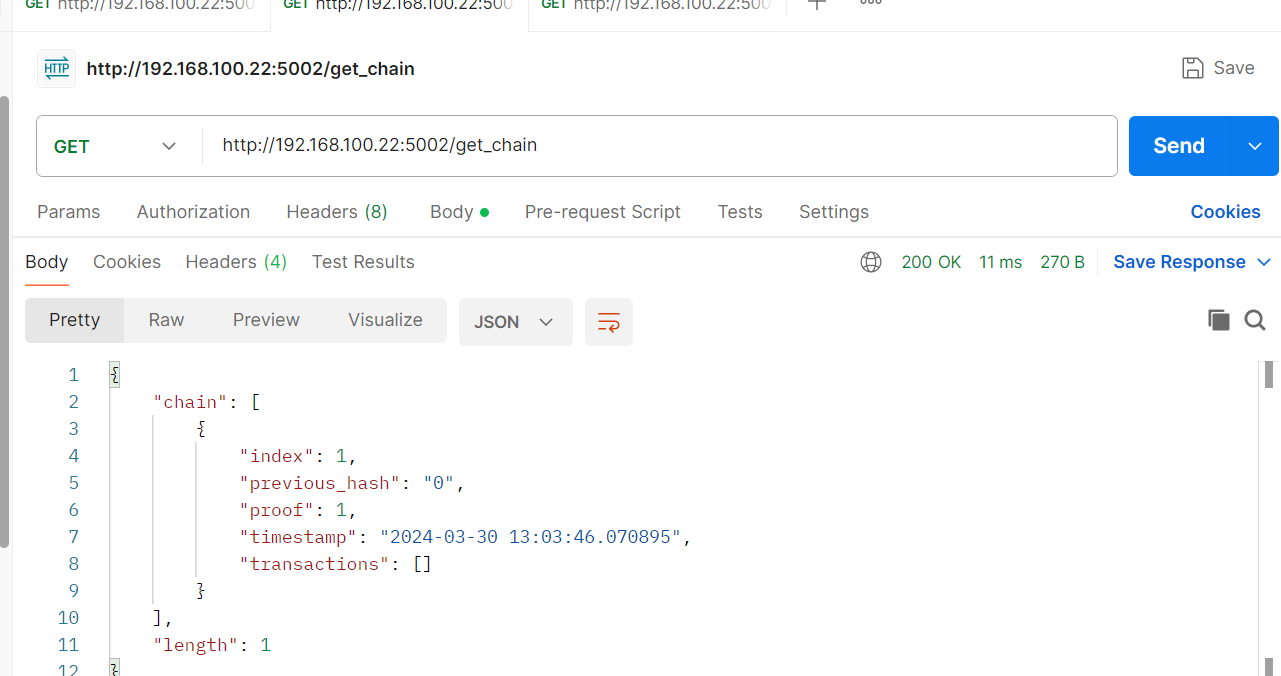
Mine a Block in Node 1

Node 1: http://10.176.232.166:5001/mine\_block



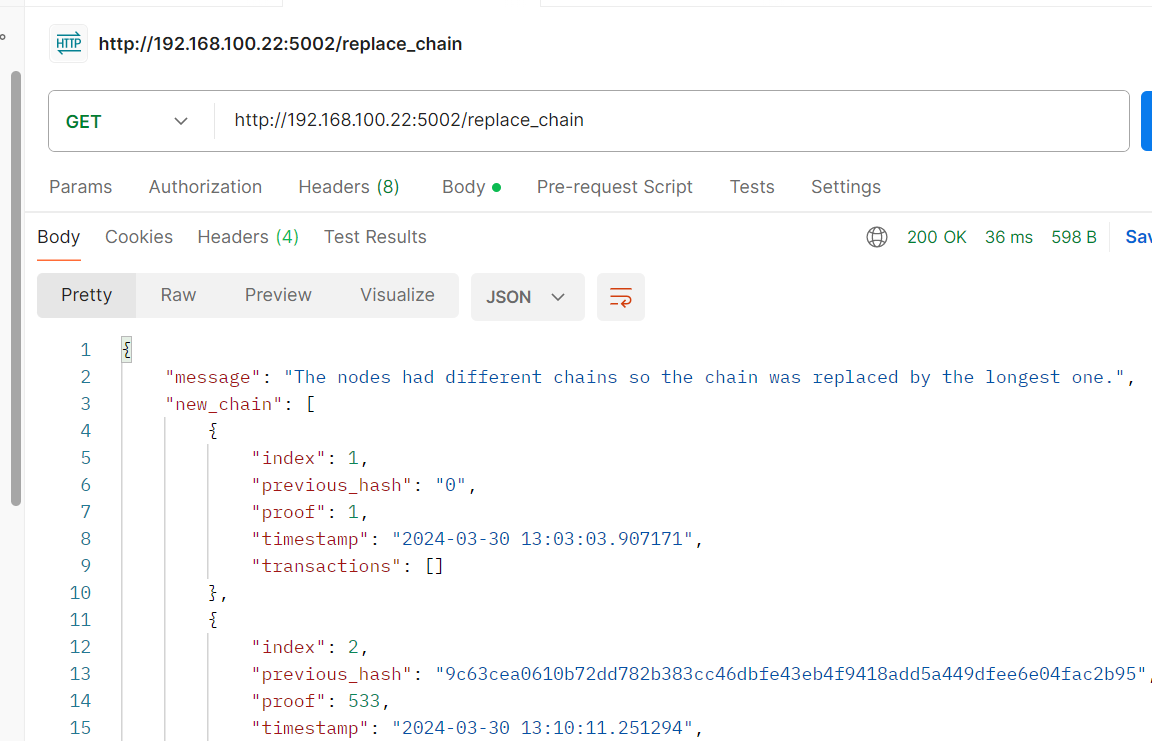
Note: At this point if you run the Get Command “get\_chain”, you will find no node has updated with the new blocks. Therefore we need to update all the nodes with the new mining transactions.

<http://192.168.100.22:5002/get_chain>



**Step 6: Create a Consensus by using replace\_chain command**

Node 2: http://10.176.232.166:5002/replace\_chain



**Step 7: We need to transfer some coins to George Ndegwa,**

We shall run a “POST” Command in postman and use method “add\_transaction”. Then using this python command. Replace the Json file with the below file. Indicate each of the particulars in the json file;

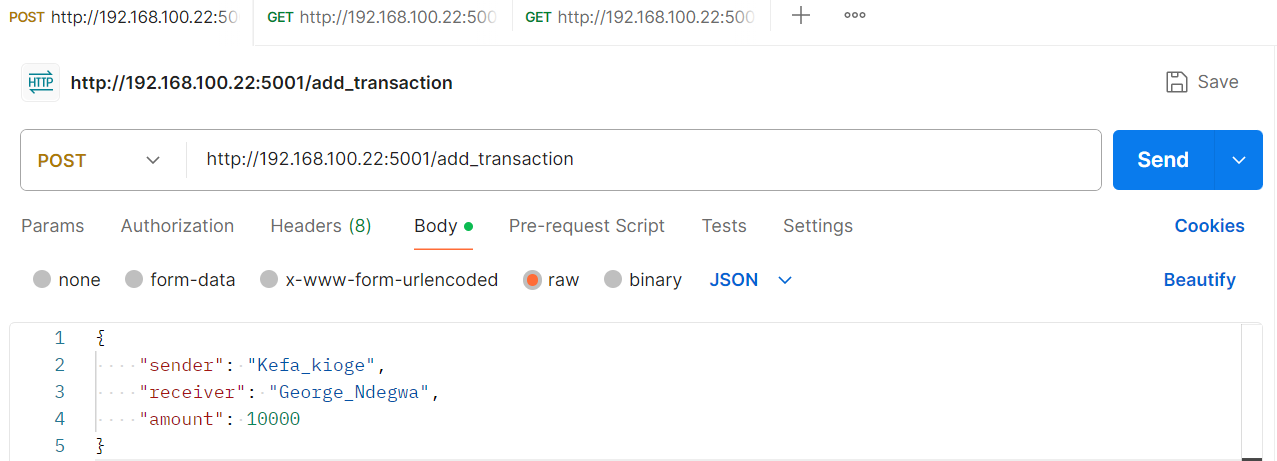
{

"sender": "",

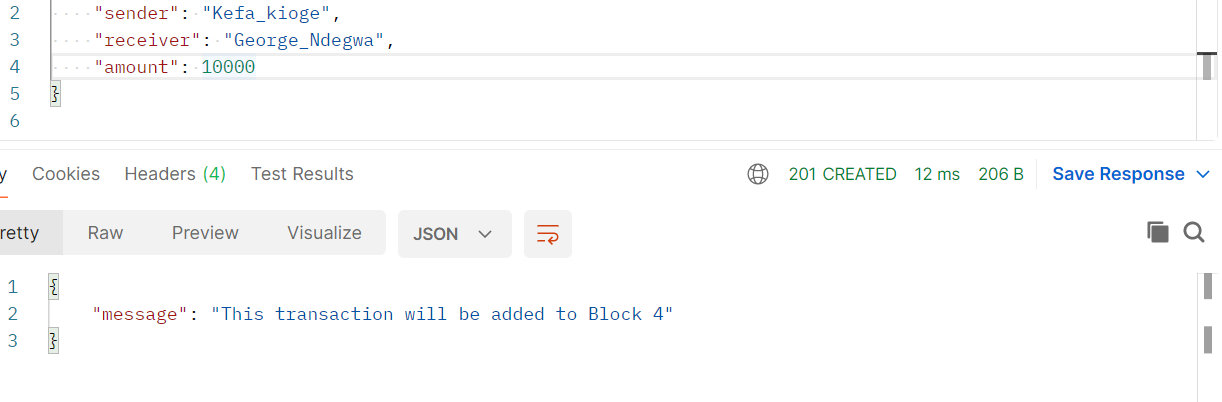
"receiver": "",

"amount":

}



The system gives you this message

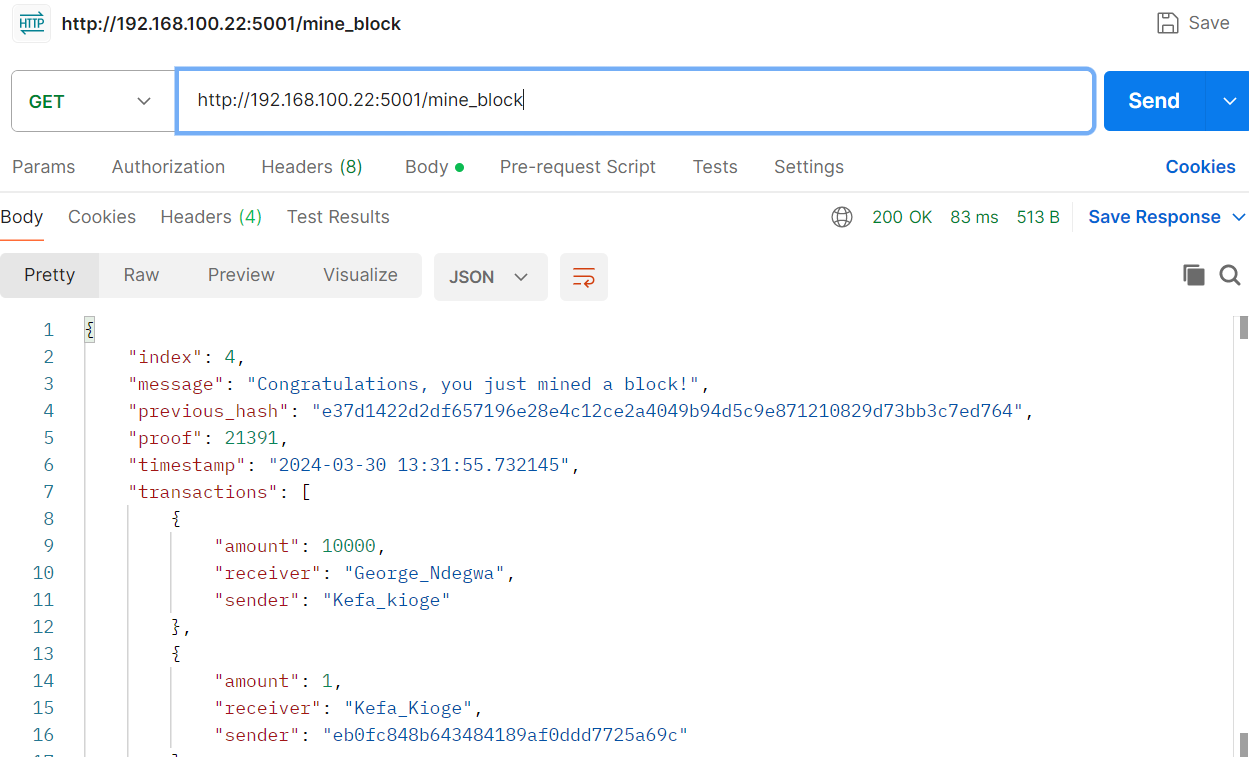


Now, Go to the run a “GET” Request in postman and run “mine\_block” in postman in node 5001:

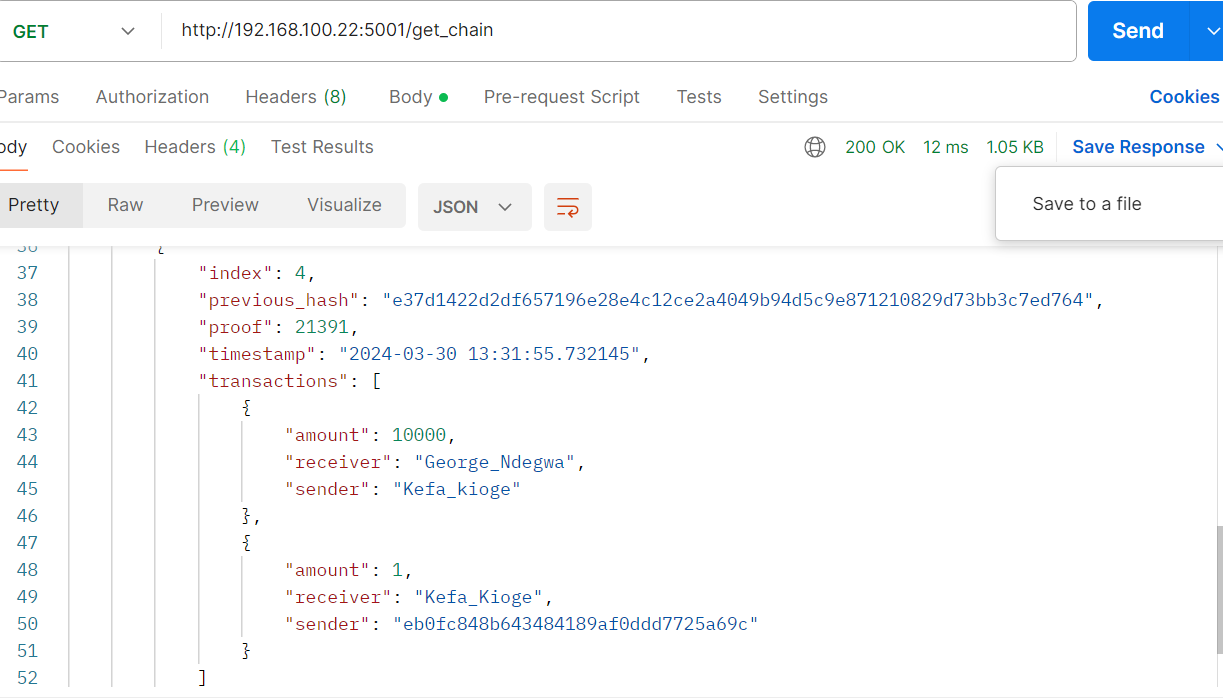
<http://192.168.100.22:5001/mine_block>

We shall get two new blocks

1. One block to myself that I have just mined , with one hadcoin and
2. From myself to George Ndegwa with 10000 coins.

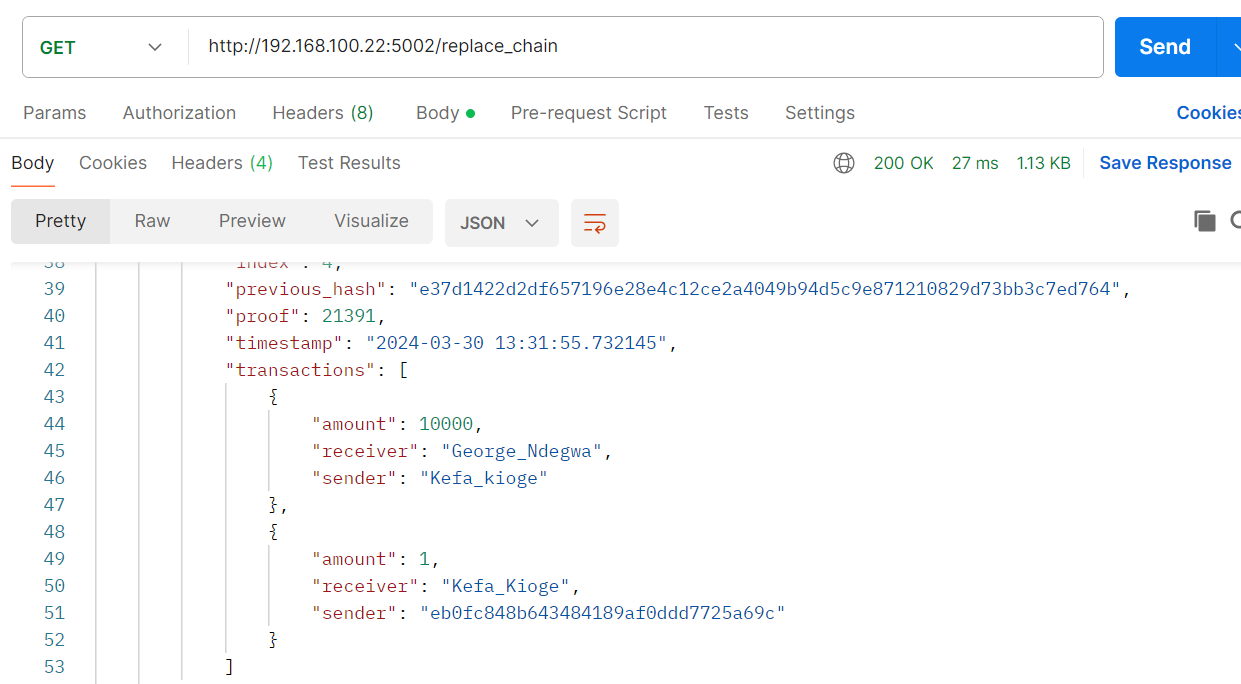


Lets have a look at our chain now by running “get\_chain” method. We get the two transactions above.

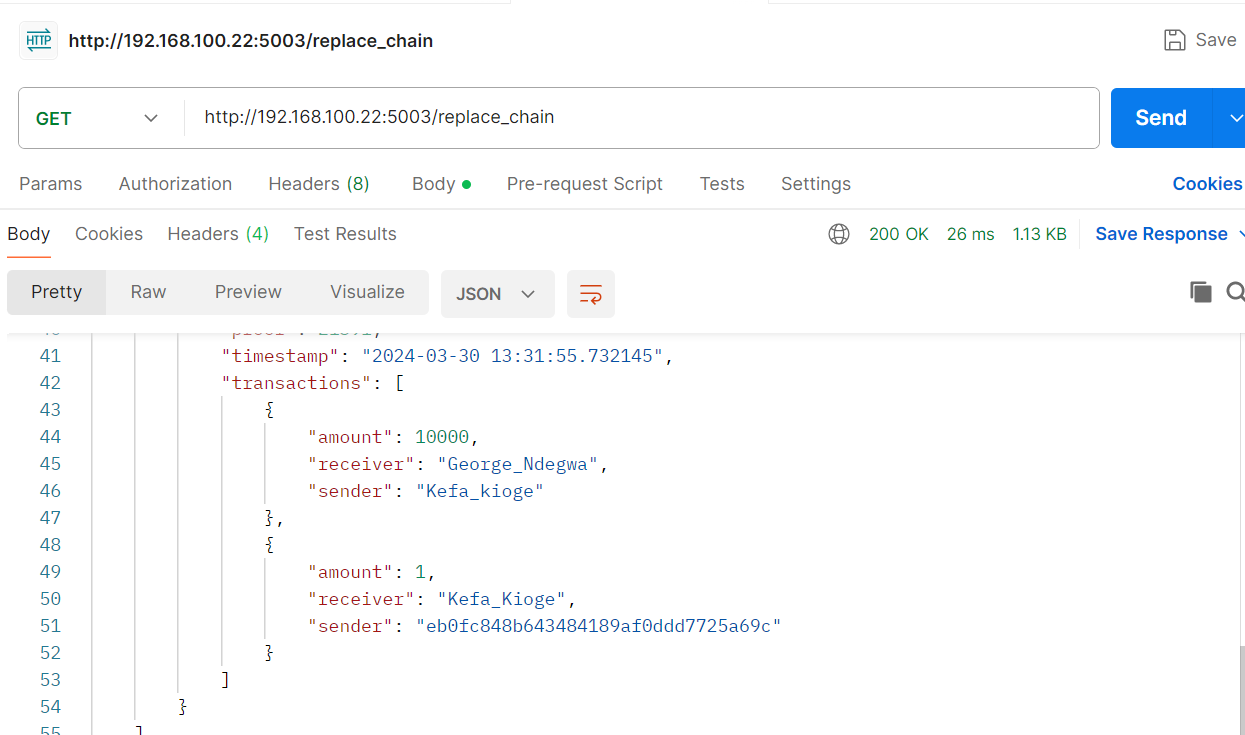


We need to update the chain in node 2 and node 3 by running the “GET “ Request “ for “replace\_chain” method in all the nodes:

Node2:



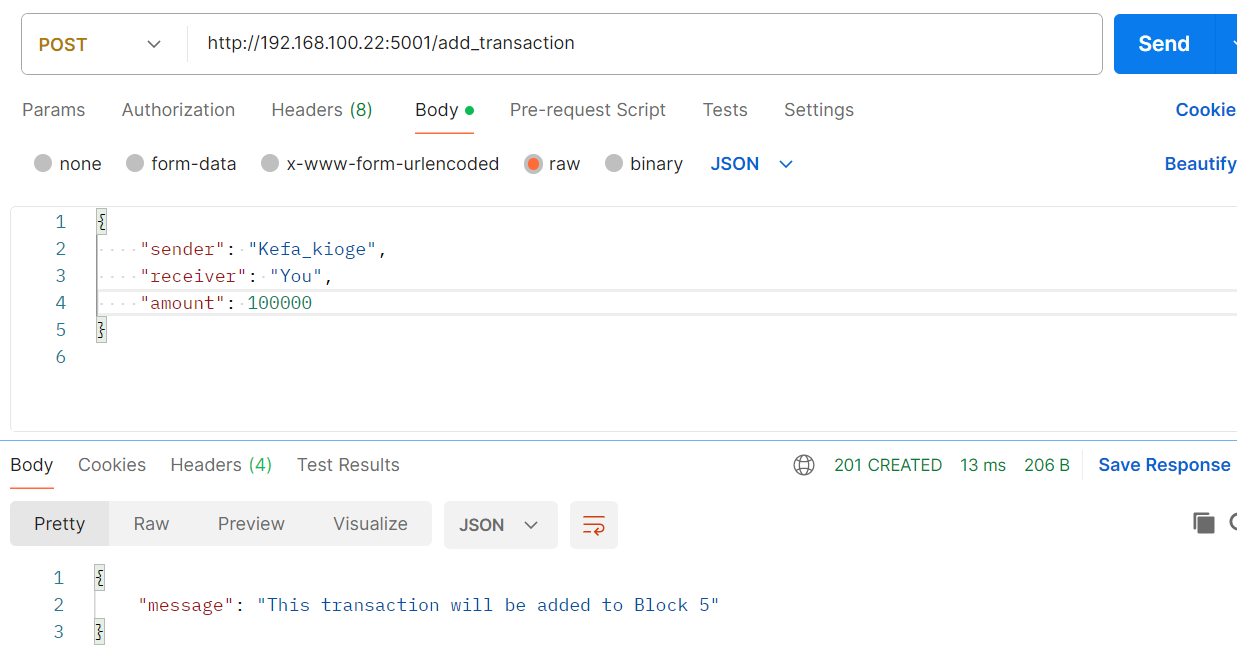
Node3:



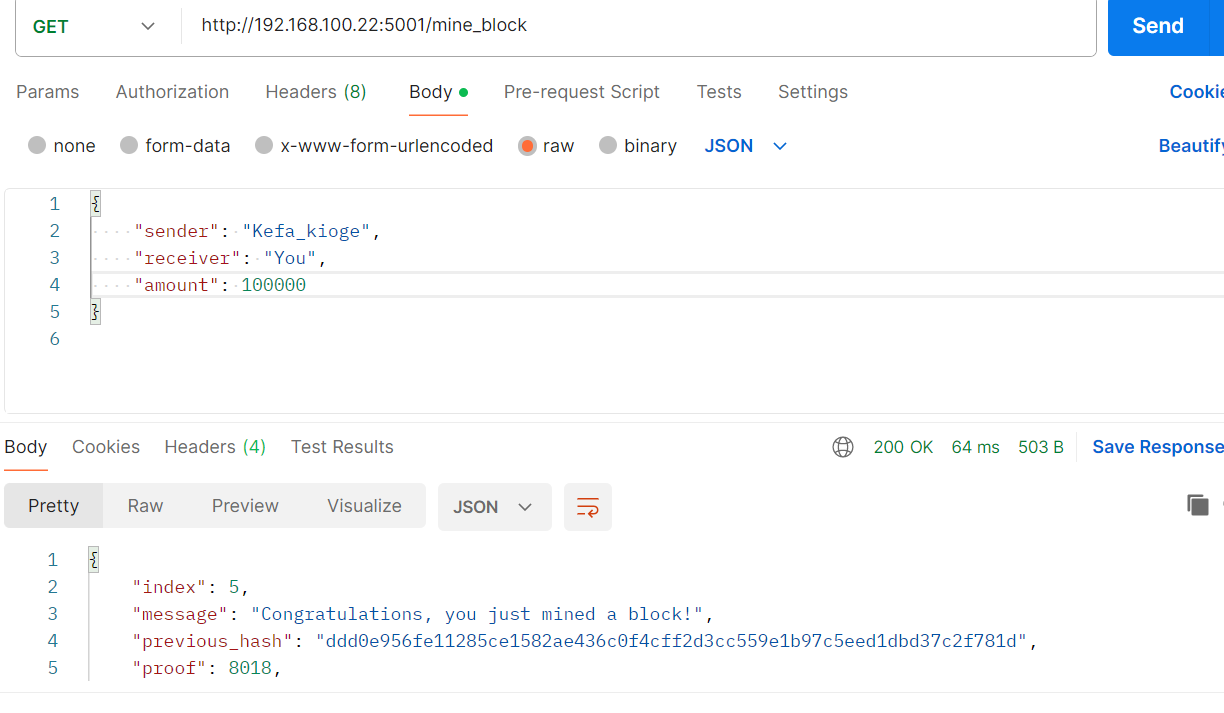
Now every node is updated.

Second Transaction:

Try sending 100, 000 Coins to you (node3)



We have to mine a new block to welcome this new transaction to block 5



Now run the <http://192.168.100.22:5001/replace_chain> in the other noderequest to update the block chain

