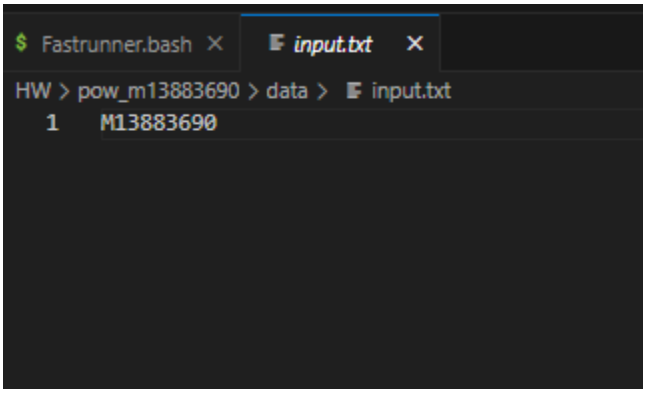
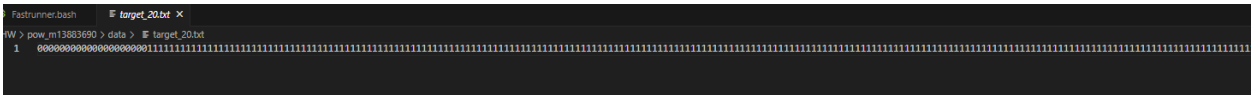
Project 4: Proof of Work

Report

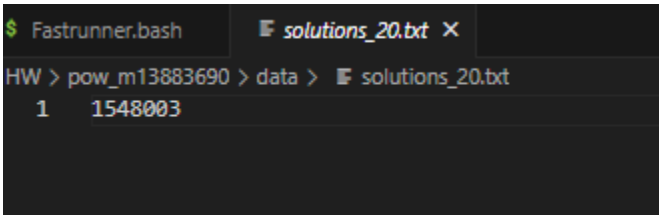
Mabon Ninan 1



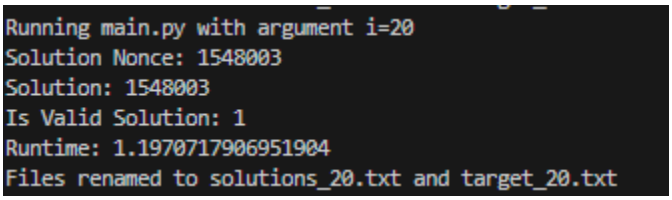
1. Target Generation Function:



2. Solution Generation Function



3. Verification Function:



4. Performance of POW:

Runtime Analysis:

Running main.py with argument i=16

Solution Nonce: 5948

Solution: 5948

Is Valid Solution: 1

Runtime: 0.004956245422363281

Files renamed to solutions_16.txt and target_16.txt

Running main.py with argument i=17

Solution Nonce: 5948

Solution: 5948

Is Valid Solution: 1

Runtime: 0.004708528518676758

Files renamed to solutions_17.txt and target_17.txt

Running main.py with argument i=18

Solution Nonce: 1417293

Solution: 1417293

Is Valid Solution: 1

Runtime: 1.095245122909546

Files renamed to solutions_18.txt and target_18.txt

Running main.py with argument i=19

Solution Nonce: 1417293

Solution: 1417293

Is Valid Solution: 1

Runtime: 1.095334768295288

Files renamed to solutions_19.txt and target_19.txt

Running main.py with argument i=20

Solution Nonce: 1548003

Solution: 1548003

Is Valid Solution: 1

Runtime: 1.1970717906951904

Files renamed to solutions_20.txt and target_20.txt

Running main.py with argument i=21

Solution Nonce: 3135790

Solution: 3135790

Is Valid Solution: 1

Runtime: 2.4319815635681152

Files renamed to solutions_21.txt and target_21.txt

Running main.py with argument i=22

Solution Nonce: 9618204

Solution: 9618204

Is Valid Solution: 1

Runtime: 7.426326274871826

Files renamed to solutions_22.txt and target_22.txt

Running main.py with argument i=23

Solution Nonce: 9618204

Solution: 9618204

Is Valid Solution: 1

Runtime: 7.391636848449707

Files renamed to solutions_23.txt and target_23.txt

Running main.py with argument i=24

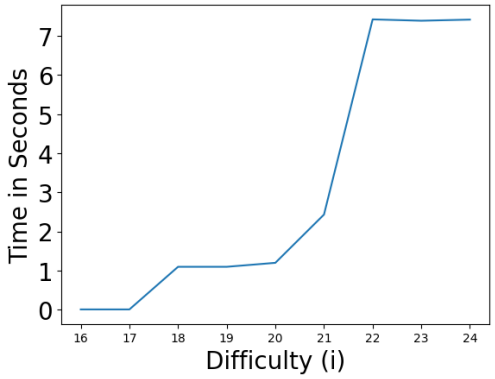
Solution Nonce: 9618204

Solution: 9618204

Is Valid Solution: 1

Runtime: 7.420438051223755

Files renamed to solutions_24.txt and target_24.txt



This project simulates Bitcoin mining by implementing the Proof of Work (POW) algorithm. The program computes a target based on the specified POW difficulty, generates a POW solution for a given input message and target, and verifies the validity of a solution using the SHA-256 hash function. The SHA-256 hash function ensures the cryptographic integrity of the mining process. Users can interact with the program by computing targets, mining for solutions, and verifying the authenticity of obtained solutions, gaining insights into the fundamental aspects of POW in cryptocurrency systems.

RUN CODE: bash Fastrunner.bash