Feras Alnehabi ID:443101183

CSC489 HW2

Blockchain Implementation

Description and Requirements:

Programming language used: Java

Libraries used: java.security.MessageDigest (for SHA-256 hashing)

java.time.Instant (for timestamp handling)

java.list (for linked list blockchain)

Program Requirements: Java JDK only (no external libraries required).

Implementation:

Block class:

Attributes:

index: Block's position.

previousHash: Hash of the previous block.

data: Transaction or message stored in the block.

timestamp: Time when the block was created.

hash: Computed hash of the block.

nonce: Used for proof-of-work.

miningTime: Time taken to mine the block.

next: Pointer to the next block.

Methods Implemented:

calculateHash(): Computes SHA-256 hash.

applySHA256(): Generates SHA-256 hash.

mineBlock(int difficulty): Implements proof-of-work and records mining time.

Blockchain Class:

Attributes:

head: First block (Genesis Block).

tail: Last block in the linked list.

difficulty: Number of leading zeros required in the hash.

Methods Implemented:

createGenesisBlock(): Initializes the blockchain with a genesis block.

addBlock(String data): Mines and adds a new block.

verifyChain(): Ensures blockchain integrity.

displayChain(): Prints blockchain details.

Main Class:

initializes a linked list-based blockchain.

Adds multiple blocks with different data.

Displays the blockchain structure.

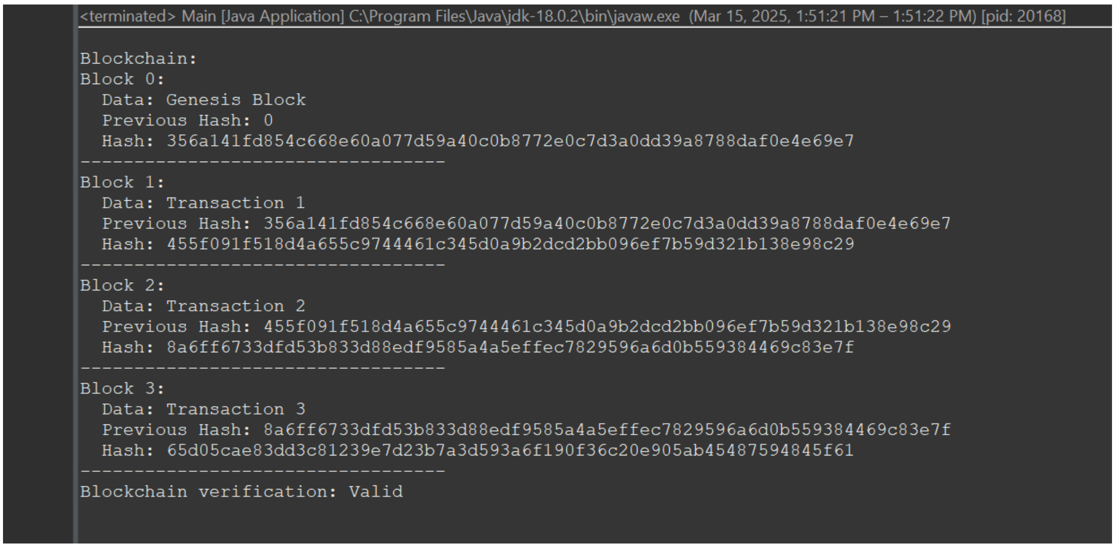
Verifies blockchain integrity.

Tampering test: Modifies a block to demonstrate integrity check failure.

Results:

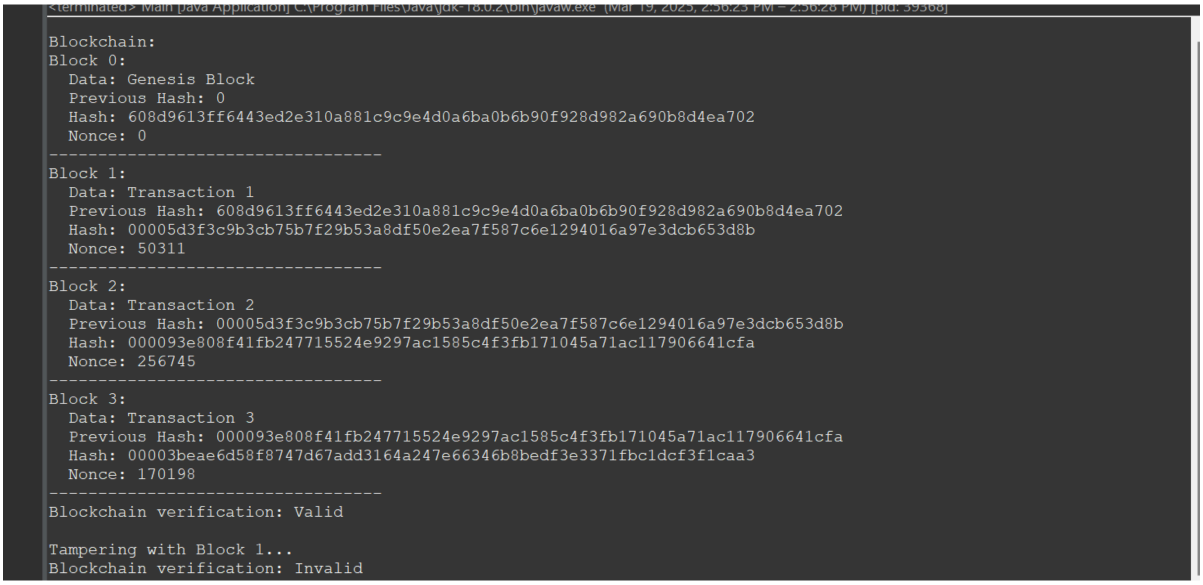
Part 1:

Results before tampering:



```
<terminated> Main [Java Application] C:\Program Files\Java\jdk-18.0.2\bin\javaw.exe  (Mar 15, 2025, 1:51:21 PM – 1:51:22 PM) [pid: 20168]

Blockchain:
Block 0:
  Data: Genesis Block
  Previous Hash: 0
  Hash: 356a141fd854c668e60a077d59a40c0b8772e0c7d3a0dd39a8788daf0e4e69e7
----------------------------------
Block 1:
  Data: Transaction 1
  Previous Hash: 356a141fd854c668e60a077d59a40c0b8772e0c7d3a0dd39a8788daf0e4e69e7
  Hash: 455f091f518d4a655c9744461c345d0a9b2dcd2bb096ef7b59d321b138e98c29
----------------------------------
Block 2:
  Data: Transaction 2
  Previous Hash: 455f091f518d4a655c9744461c345d0a9b2dcd2bb096ef7b59d321b138e98c29
  Hash: 8a6ff6733dfd53b833d88edf9585a4a5effec7829596a6d0b559384469c83e7f
----------------------------------
Block 3:
  Data: Transaction 3
  Previous Hash: 8a6ff6733dfd53b833d88edf9585a4a5effec7829596a6d0b559384469c83e7f
  Hash: 65d05cae83dd3c81239e7d23b7a3d593a6f190f36c20e905ab45487594845f61
----------------------------------
Blockchain verification: Valid
```

Results after tampering:

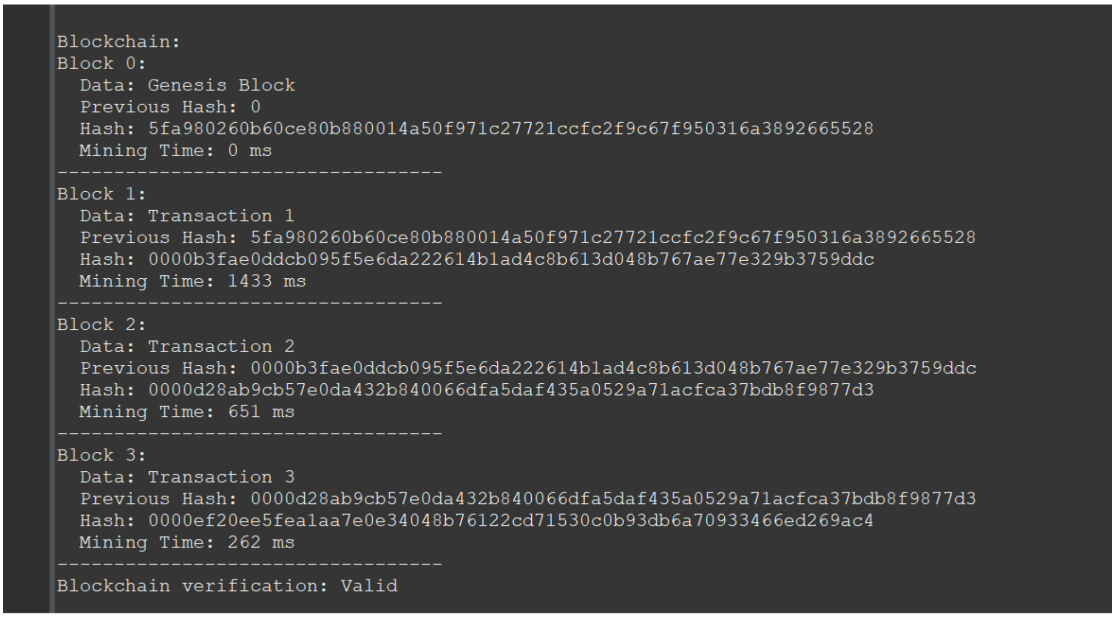


```
<terminated> Main [Java Application] C:\Program Files\Java\jdk-18.0.2\bin\javaw.exe  (Mar 19, 2025, 2:56:23 PM – 2:56:28 PM) [pid: 39368]

Blockchain:
Block 0:
  Data: Genesis Block
  Previous Hash: 0
  Hash: 608d9613ff6443ed2e310a881c9c9e4d0a6ba0b6b90f928d982a690b8d4ea702
  Nonce: 0
----------------------------------
Block 1:
  Data: Transaction 1
  Previous Hash: 608d9613ff6443ed2e310a881c9c9e4d0a6ba0b6b90f928d982a690b8d4ea702
  Hash: 00005d3f3c9b3cb75b7f29b53a8df50e2ea7f587c6e1294016a97e3dcb653d8b
  Nonce: 50311
----------------------------------
Block 2:
  Data: Transaction 2
  Previous Hash: 00005d3f3c9b3cb75b7f29b53a8df50e2ea7f587c6e1294016a97e3dcb653d8b
  Hash: 000093e808f41fb247715524e9297ac1585c4f3fb171045a71ac117906641cfa
  Nonce: 256745
----------------------------------
Block 3:
  Data: Transaction 3
  Previous Hash: 000093e808f41fb247715524e9297ac1585c4f3fb171045a71ac117906641cfa
  Hash: 00003beae6d58f8747d67add3164a247e66346b8bedf3e3371fbc1dcf3f1caa3
  Nonce: 170198
----------------------------------
Blockchain verification: Valid

Tampering with Block 1...
Blockchain verification: Invalid
```

Part 2:

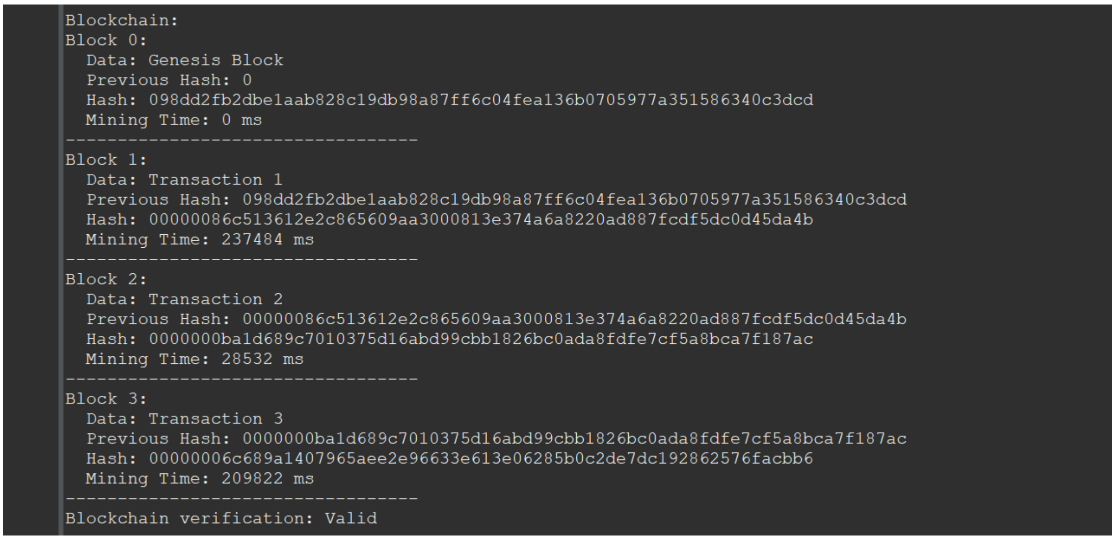
Implementation of proof of work mechanism with various difficulties:

Difficulty 4:



```
Blockchain:
Block 0:
  Data: Genesis Block
  Previous Hash: 0
  Hash: 5fa980260b60ce80b880014a50f971c27721ccfc2f9c67f950316a3892665528
  Mining Time: 0 ms
----------------------------------
Block 1:
  Data: Transaction 1
  Previous Hash: 5fa980260b60ce80b880014a50f971c27721ccfc2f9c67f950316a3892665528
  Hash: 0000b3fae0ddcb095f5e6da222614b1ad4c8b613d048b767ae77e329b3759ddc
  Mining Time: 1433 ms
----------------------------------
Block 2:
  Data: Transaction 2
  Previous Hash: 0000b3fae0ddcb095f5e6da222614b1ad4c8b613d048b767ae77e329b3759ddc
  Hash: 0000d28ab9cb57e0da432b840066dfa5daf435a0529a71acfca37bdb8f9877d3
  Mining Time: 651 ms
----------------------------------
Block 3:
  Data: Transaction 3
  Previous Hash: 0000d28ab9cb57e0da432b840066dfa5daf435a0529a71acfca37bdb8f9877d3
  Hash: 0000ef20ee5fea1aa7e0e34048b76122cd71530c0b93db6a70933466ed269ac4
  Mining Time: 262 ms
----------------------------------
Blockchain verification: Valid
```

Difficulty 6:



```
Blockchain:
Block 0:
  Data: Genesis Block
  Previous Hash: 0
  Hash: 098dd2fb2dbe1aab828c19db98a87ff6c04fea136b0705977a351586340c3dcd
  Mining Time: 0 ms
----------------------------------
Block 1:
  Data: Transaction 1
  Previous Hash: 098dd2fb2dbe1aab828c19db98a87ff6c04fea136b0705977a351586340c3dcd
  Hash: 00000086c513612e2c865609aa3000813e374a6a8220ad887fcdf5dc0d45da4b
  Mining Time: 237484 ms
----------------------------------
Block 2:
  Data: Transaction 2
  Previous Hash: 00000086c513612e2c865609aa3000813e374a6a8220ad887fcdf5dc0d45da4b
  Hash: 0000000ba1d689c7010375d16abd99cbb1826bc0ada8fdfe7cf5a8bca7f187ac
  Mining Time: 28532 ms
----------------------------------
Block 3:
  Data: Transaction 3
  Previous Hash: 0000000ba1d689c7010375d16abd99cbb1826bc0ada8fdfe7cf5a8bca7f187ac
  Hash: 00000006c689a1407965aee2e96633e613e06285b0c2de7dc192862576facbb6
  Mining Time: 209822 ms
----------------------------------
Blockchain verification: Valid
```

Difficulty 10: I ran the program for an hour and got no result