Module Code: CS3BC  
Assignment report Title: Blockchain Coursework Assignment  
Student Number: 30002734  
Date (when the work was completed): 12/05/2025  
Actual hrs spent for the assignment:  
Which Artificial Intelligence tools used (if applicable):

Part 1

The solution file BlockchainAssignment.sln was opened in Visual Studio, and BlockchainApp.cs was launched in the Windows Forms designer. A single-line TextBox, a Button and a large RichTextBox were added from the Toolbox. In the Properties panel, the TextBox was renamed to inputText, the Button to printButton with its Text property set to “Print,” and the RichTextBox to outputBox so that each control’s purpose was immediately clear. In the code view, the Print button’s Click event handler was generated automatically, and a single line of code was inserted to assign the contents of inputText to outputBox.Text. After resizing and anchoring the controls for a clean layout, the application was run, and the word “test” was entered into inputText before clicking Print. The same text appeared instantly in outputBox, confirming that control placement, naming conventions and event wiring were functioning correctly prior to implementing the blockchain logic.

Part 2

The core blockchain logic was implemented by creating two new classes, Block and Blockchain. In Block.cs, private fields for timestamp, index, previous hash and hash were declared. A parameterless constructor was provided for the genesis block that sets the timestamp to the current time, the index to zero and the previous hash to an empty string before calling CreateHash to compute its SHA-256 hash. The CreateHash method concatenates the index, timestamp and previous hash into a single string, runs it through the SHA256Managed hasher and formats the resulting byte array as a hexadecimal string to become the block’s hash. Overloaded constructors were also added to accept the last block so that new blocks automatically inherit the correct index and link back to their predecessor before computing their own hash.

In Blockchain.cs, a List of Block objects was declared and initialised in the constructor with a single new Block so that the chain always begins with the genesis block. A method named getBlockAsString was introduced to return the ToString representation of any block by index or to return an error message if the index is out of range. In the form’s constructor in BlockchainApp.cs, the existing UI controls were retained, and immediately after InitializeComponent, a new Blockchain object was instantiated. Calling getBlockAsString(0) replaced the initial console text with the details of the genesis block. When the application runs, it now displays the block index, timestamp, SHA-256 hash and previous hash (empty for block zero) in the RichTextBox, confirming that block creation and chaining behave as intended.

The appendix includes two images. The first shows the RichTextBox immediately after initialization with the “New blockchain initialised!” message. The second shows the running application displaying the full details of block zero in the RichTextBox.

Part 3

In the next phase, full wallet support and transaction creation were added to enable secure transfers of Assignment Coins. The application leverages the existing Wallet class, which implements ECDSA key‐pair generation and validation. Two new UI buttons, Generate Keys and Validate Keys, were placed beside text boxes labelled Public Key and Private Key. Clicking Generate Keys calls Wallet’s constructor, fills the Public Key field with the newly created public identifier and writes the matching private key into the Private Key field. Clicking Validate Keys then invokes Wallet.ValidatePrivateKey to confirm that the two values form a valid pair and displays “Keys are valid” or “Keys are invalid” in the main RichTextBox output.

With key management in place, a Transaction class was introduced to encapsulate everything needed for a blockchain transfer. Each transaction records a timestamp, sender address, recipient address, amount and fee. Its constructor concatenates those fields, runs the result through SHA-256 to produce a hash, and then calls Wallet.CreateSignature to sign that hash with the sender’s private key. This signature binds the transaction cryptographically to the sender and prevents tampering.

A Create Transaction button was added to the UI so that, once a valid key pair, recipient address, amount and fee are entered, clicking it constructs a new Transaction and writes its full details into the RichTextBox. This end-to-end flow ensures that every transaction is both authenticated and tamper-evident, laying the groundwork for the transaction pool and balance checks that follow.

In the appendix, the first screenshot will show the application after keys are generated and validated, with “Keys are valid” displayed in the output area. The second screenshot will show a completed transaction in the console, illustrating the timestamp, sender address, recipient address, amount, fee, transaction hash and digital signature.

Part 4

Part four extends the blockchain’s consensus by adding proof-of-work mining, transaction inclusion and miner rewards in the Block class. A new Mine method performs repeated SHA-256 hashing of the block header, which now includes index, timestamp, previous hash, Merkle root and a changing nonce, until the hash meets the difficulty target of four leading zeros. Each time the nonce is incremented, the CreateHash routine combines the header fields and computes the digest. As soon as Mine finds a valid hash, it returns, ensuring every block carries a verifiable proof of work.

When a block is constructed, it now accepts the previous block, the pending transactions list and the miner’s address. A reward transaction is generated that pays a base reward plus any collected fees, and all transactions are fed into a MerkleRoot method to produce the block’s Merkle root. Mine is then invoked to find the nonce and hash. Once mining completes, the block object holds its nonce, hash, Merkle root and the full sorted list of transactions so that every block records both its cryptographic proof and its contained transfers.

On the blockchain side, the transaction pool was introduced to hold pending transactions, and a GetPendingTransactions method was added to batch them in groups of five. A getLastBlock helper returns the current tip of the chain for linking new blocks. The Windows Forms interface gained three new buttons for Generate New Block, Print All and Print Pending Transactions. Generate New Block retrieves the next batch of transactions, calls the Block constructor to mine and link the new block, adds it to the chain and shows its details in the main output area. Print All lists every block in the chain, and Print Pending Transactions displays any transactions still waiting in the pool.

Part 5

Part five implements a complete validation layer to guarantee the blockchain’s integrity and the correctness of user balances. Two new static methods, ValidateHash and ValidateMerkleRoot, recompute each block’s SHA-256 hash (using its index, timestamp, prevHash, nonce and Merkle root) and rebuild the Merkle tree over its transactions to ensure nothing has been altered. In the UI a Full Blockchain Validation button now walks through every block from the second onward, checking that each block’s prevHash matches the actual hash of its predecessor, that its stored hash equals a fresh hash of its header, and that its stored Merkle root matches the recomputed root. If any of these checks fails, the app reports “Blockchain is invalid”; otherwise, it reports “Blockchain is valid.”

To tie balances back to the ledger, a GetBalance method was also added to the Blockchain class. It scans every confirmed transaction in every block, credits amounts where the given address is the recipient and debits the amount plus the fee where it is the sender and returns the net Assignment Coin balance. On the form, you can enter a public key and click Check Balance to display the computed balance in the main console area.

Part 6

In Task 6.1, a multithreaded mining mode was introduced to exploit all available CPU cores and drive down average block-find time. Each thread probes a distinct slice of the nonce space by stepping its nonce counter by the total thread count on every iteration. A shared cancellation flag, guarded by a simple lock, ensures that as soon as one thread finds a valid hash that meets the leading-zero difficulty target, all others stop immediately. A stopwatch measures the elapsed time for each mining run, and those results are written to the console area to compare single-threaded performance with multithreaded runs. The appendix shows comparisons of three multithreaded and three single-threaded blocks and their mining time. The mean block time over the three multithreaded blocks using 8 threads was 6.938 seconds, whereas for single threading, the mean was 39.999 seconds.

Task 6.2 adds an adaptive difficulty algorithm so that block creation stays close to a chosen target interval. After each block is mined, the application checks whether the mining time was faster or slower than the target time. If blocks are being found faster than the target, the difficulty is incremented by one; if too slow, it is decremented, never dropping below one. The current difficulty level is displayed in the UI alongside the mining controls and is logged with every block print-out. As shown in the appendix, as the difficulty increases, so does the mining time until it is longer than the target time, then both the difficulty and mining time decrease again.

TALK ABOUT SOME OTHER METHODS

Task 6.3 implements transaction selection preferences to explore different miner behaviours. A set of radio buttons in the form lets the user choose between three strategies, including greedy (highest-fee-first), altruistic (oldest-pending-first) or random selection. When “Generate New Block” is clicked, the code sorts the pending-transaction list according to the chosen strategy and then selects the required number of transactions for inclusion in the new block. This makes it easy to observe how each policy affects total fees collected and average transaction wait time. The appendix shows how each strategy chooses 5 transactions from the transaction pool.

MAYBE ADD LITTLE CODE SNIPPET

Part 7

In this final section, a proof-of-stake algorithm was implemented. When new blocks are created through mining, the blocks are “mined”, but when new blocks are created using proof of stake, the blocks are “forged”. Firstly, a “Forge New Block” button was added to the UI, which triggers the proof-of-stake algorithm. This starts by creating a dictionary of address-balance pairs by looking through every block in the chain and every transaction in each block to find all addresses that have either sent or received tokens. Then the getBalance function is called for each address, which populates the stakes dictionary.

These stakes are then used inside a new ValidatorPicker class to call Pick(), which shuffles the stakes dictionary, then generates a random value between 0 and the sum of all stakes. It steps through the list, cumulatively adding each address’s stake until the running total meets or exceeds the random sample; at that point, it returns that address as the chosen validator. The mining mode is determined and passed to GetPendingTransactions() to add the relevant transactions to the block.

A new block constructor was created specifically for proof of stake. The timestamp, index, previous block data, transaction list and Merkle Root are all set the same way as in

Appendix

Part 1

Application window with two textboxes and a button. The text is printed in the large text box from the small text box:

A screenshot of a computer

AI-generated content may be incorrect.

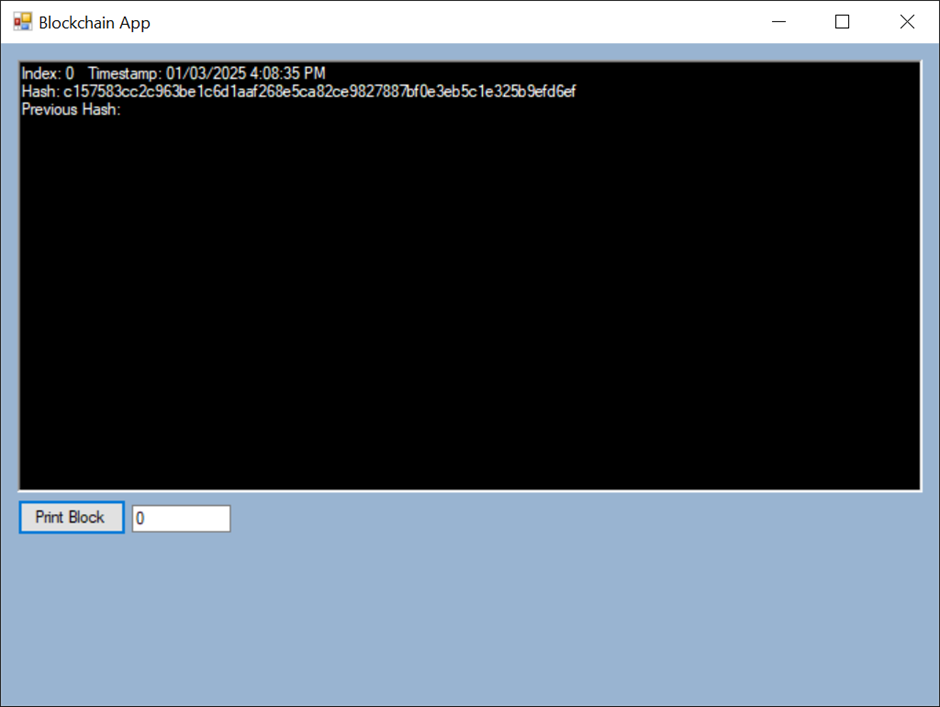
Part 2

New blockchain initialised message when starting the application:

A screenshot of a computer

AI-generated content may be incorrect.

Genesis block:



Part 3

Keys generated in the public and private key text boxes, then validated:

A screenshot of a computer

AI-generated content may be incorrect.

Transactions can be created, but they are not validated on the blockchain:A screenshot of a computer program

AI-generated content may be incorrect.

Part 4

New block and sent a transaction, which is pending:

A screenshot of a computer program

AI-generated content may be incorrect.

Both blocks are shown, with the transaction shown in the second block:A screenshot of a computer

AI-generated content may be incorrect.

Part 5

Keys generated with a transaction generated, giving the wallet tokens:

A screenshot of a computer

AI-generated content may be incorrect.

The transaction in the chain:

A screenshot of a computer

AI-generated content may be incorrect.

Blockchain being validated:

A screenshot of a computer

AI-generated content may be incorrect.

Part 6.1

Multithreaded block 1:

A screenshot of a computer

AI-generated content may be incorrect.

Multithreaded block 2:

A screenshot of a computer

AI-generated content may be incorrect.

Multithreaded block 3:

A screenshot of a computer

AI-generated content may be incorrect.

Single-threaded block 1:

A screenshot of a computer program

AI-generated content may be incorrect.

Single-threaded block 2:

A screenshot of a computer

AI-generated content may be incorrect.

Single-threaded block 3:

A screenshot of a computer

AI-generated content may be incorrect.

Part 6.2

|  |  |  |
| --- | --- | --- |
| Block Index | Difficulty | Mining Time |
| 0 | 4 | 0.211 |
| 1 | 5 | 6.487 |
| 2 | 6 | 24.768 |
| 3 | 5 | 14.148 |

Block 0:

A screenshot of a computer

AI-generated content may be incorrect.

Block 1:

A screenshot of a computer

AI-generated content may be incorrect.

Block 2:

A screenshot of a computer

AI-generated content may be incorrect.

Block 3:

A screenshot of a computer

AI-generated content may be incorrect.

Part 6.3

Three transactions in the pending list with fees from 1 to 3:

A screenshot of a computer

AI-generated content may be incorrect.

Four transactions in the pending list with fees from 4 to 7:

A screenshot of a computer

AI-generated content may be incorrect.

The next block was mined using greedy mining mode, containing the 5 highest fee transactions:

A screenshot of a computer

AI-generated content may be incorrect.

More transactions in the block:

A screenshot of a computer

AI-generated content may be incorrect.

End of block including mining reward transaction:

A screenshot of a computer

AI-generated content may be incorrect.

Using the same 7 transactions as before, we mine a new block using altruistic mode:

A screenshot of a computer

AI-generated content may be incorrect.

Next 3 transactions in the block:

A screenshot of a computer

AI-generated content may be incorrect.

End of block including the mining reward transaction:

A screenshot of a computer

AI-generated content may be incorrect.

Using the same transactions, now we use the random mode for transaction selection and mine a new block:

A screenshot of a computer

AI-generated content may be incorrect.

The next transactions (in random order of fees now):

A screenshot of a computer

AI-generated content may be incorrect.

End of block including mining reward transaction:

A screenshot of a computer

AI-generated content may be incorrect.