

SHA-256 in Action – Cryptographic Hashing   
  
**Objective/Aim:**  
  
 To understand and apply SHA-256 hashing on input data and observe the effects of cryptographic hashing in terms of data integrity and security.



**Apparatus/Software Used:**

* Laptop/PC
* PowerPoint/Word for documentation
* Blockchain demo

**Theory/Concept:**

**Blockchain Basics:**

* A blockchain is a chain of blocks where each block contains data, its own hash, and the hash of the previous block.
* Hashing ensures data integrity, as even a small change in data will completely change the hash value.

**Hashing:**

* A hash is a fixed-length string generated from input data using cryptographic hash functions (like SHA-256).
* It ensures immutability and data security in blockchain.

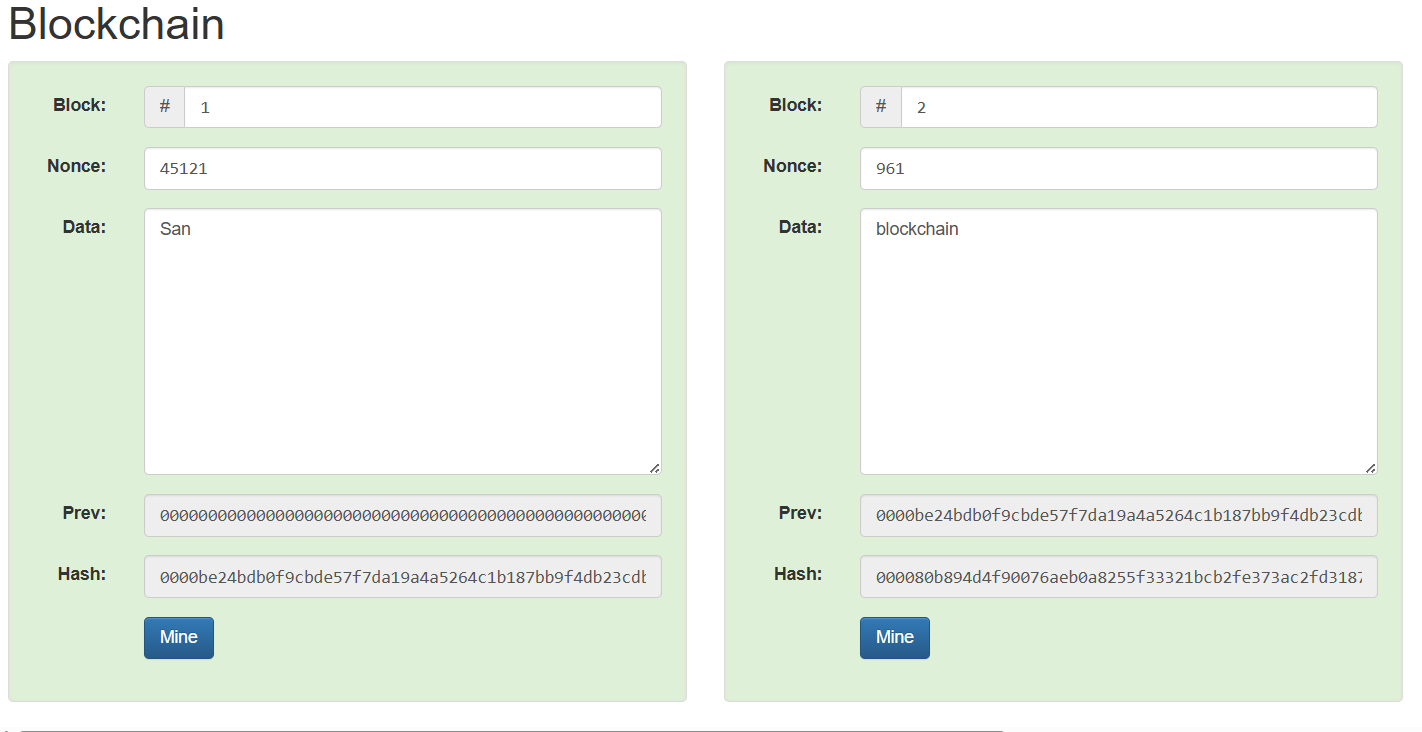
**Block Structure:**

* **Data:** Information stored in the block (e.g., transactions).
* **Previous Hash:** Links the current block to the previous block.
* **Current Hash:** Unique identifier of the block created by hashing block data.



**Procedure:**

* Open the Blockchain Demo website.
* Observe block structure: Data, Hash, Previous Hash, Nonce.
* Enter data in the first block and note the hash change.
* Add multiple blocks to create a chain.
* Modify data in any block and observe the chain breaks.
* Use “Mine” to fix invalid blocks by adjusting the nonce.
* Note how hashes link blocks and ensure chain integrity.



|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Observation Table:-**

|  |  |  |  |
| --- | --- | --- | --- |
| **Action** | **Input data** | **Hash output** | **observation** |
| Initial Block | First block | SHA256 hash | Unique hash generated |
| Second Block (Linking) | Second Block + Prev Hash | New SHA256 hash | Changes as previous hash changes |
| Data Modification | Change block data | New SHA256 hash | Hash completely changes |

**ASSESSMENT**