

 Mine It – Basic Proof-of-Work Simulation

**Objective/Aim:**  
  
 To simulate the **Proof-of-Work (PoW)** consensus mechanism and understand the fundamental principles of blockchain technology, including mining, cryptographic hashing, and the immutability of the chain.

**Apparatus/Software Used:**

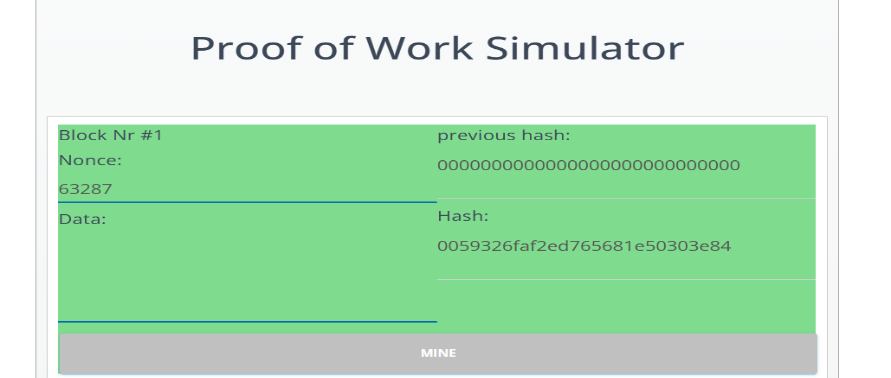
* Laptop/PC
* BRAVE
* A web-based **Proof of Work Simulator**.( https://blockchain-academy.hs-mittweida.de/2021/05/proof-of-work-simulator/)

**Theory/Concept:**

This simulator is Proof-of-Work (PoW), which validates transactions and creates new blocks. PoW is basically a computational puzzle. To add a block to the chain, miners need to find a specific number called a nonce. When this nonce is combined with the block's data and the previous block's hash, it generates a new hash that meets a strict difficulty requirement, like starting with several zeros. This process of finding the correct nonce is known as mining. It requires a lot of computational power through constant trial and error. The security of the blockchain comes directly from this effort. Because so much work is needed to solve the puzzle for one block, changing a historical block would mean re-doing the work for that block and all the blocks that come after it. This makes the ledger resistant to tampering.



**Procedure:**



### Mine the Genesis Block :-Data is entered into Block #1. Clicking "Mine" starts the search for a valid Nonce. Once found (e.g., 95597), the block is solved, its hash is generated 00f642ca..., and it turns green.



### 

### Extend the Chain :-The Hash from Block #1 automatically becomes the previous hash for Block #2. New data is added and Block #2 is mined. This process is repeated for Block #3,linking each new block to the one before it.

### Alter a Mined Block:-Change any data in a previously mined block (e.g., Block #3). The block's background instantly turns red, showing that the change has invalidated its original hash.

**Observation Table:**

Mining Success: Each block turns green upon being mined, confirming that a valid Nonce was found to produce a hash that meets the network's difficulty requirement (e.g., starting with "00").

Cryptographic Links: The Hash of each block is correctly passed on as the previous hash to the next, successfully creating a dependent chain.

Chain Invalidation: Altering data in any single mined block instantly invalidates its hash (turning it red) and breaks the chain. This causes all subsequent blocks to become invalid as well.