

 Hash Your First Block – Blockchain Basics and Setup  
  
**Objective/Aim:**  
  
 The objective is to understand the fundamental concept of cryptographic hashing in blockchain by practically setting up a basic blockchain environment and mining the initial block.

**Apparatus/Software Used:**

* Laptop/PC
* https://andersbrownworth.com/blockchain/block

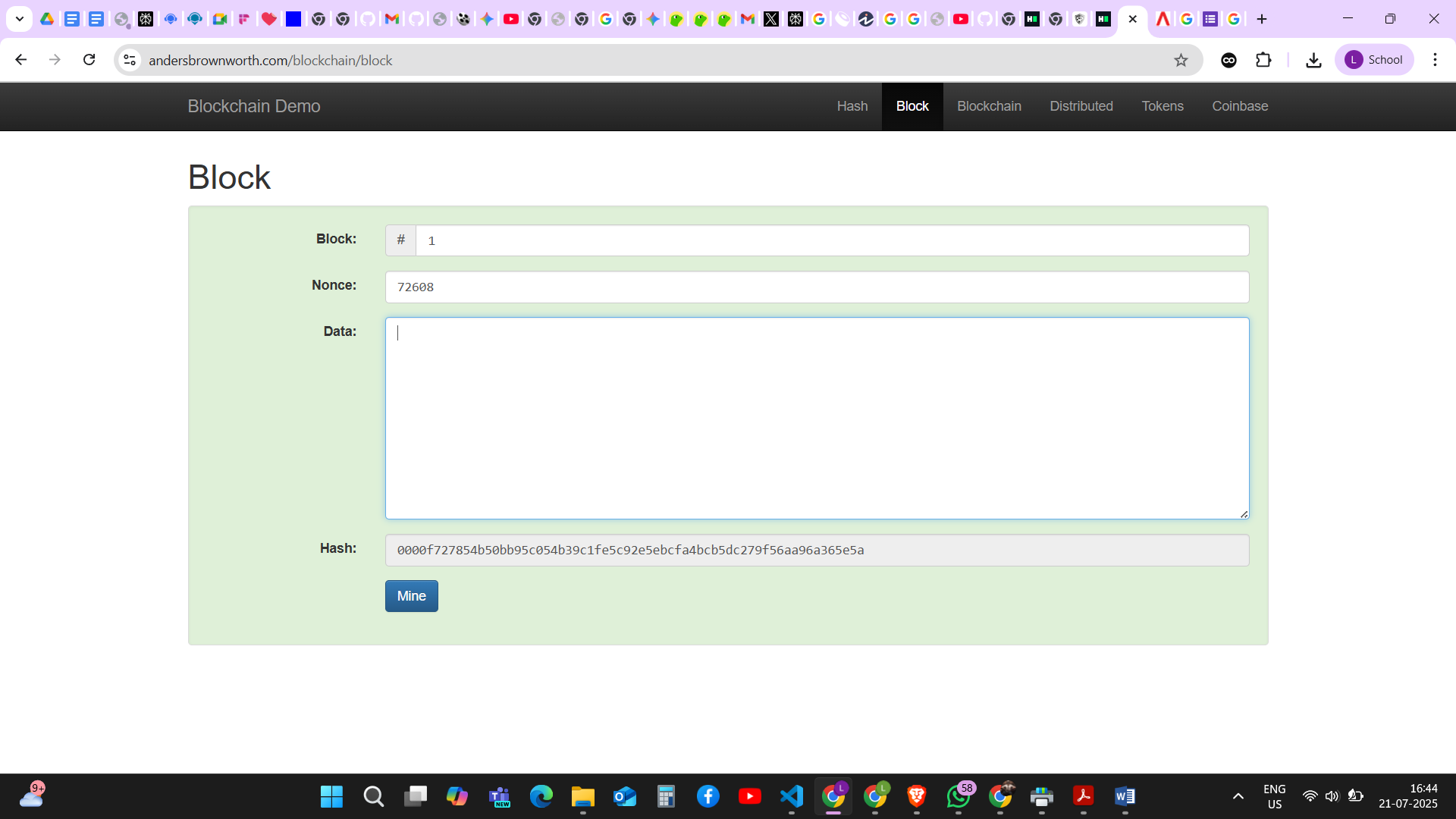
**Theory/Concept:**

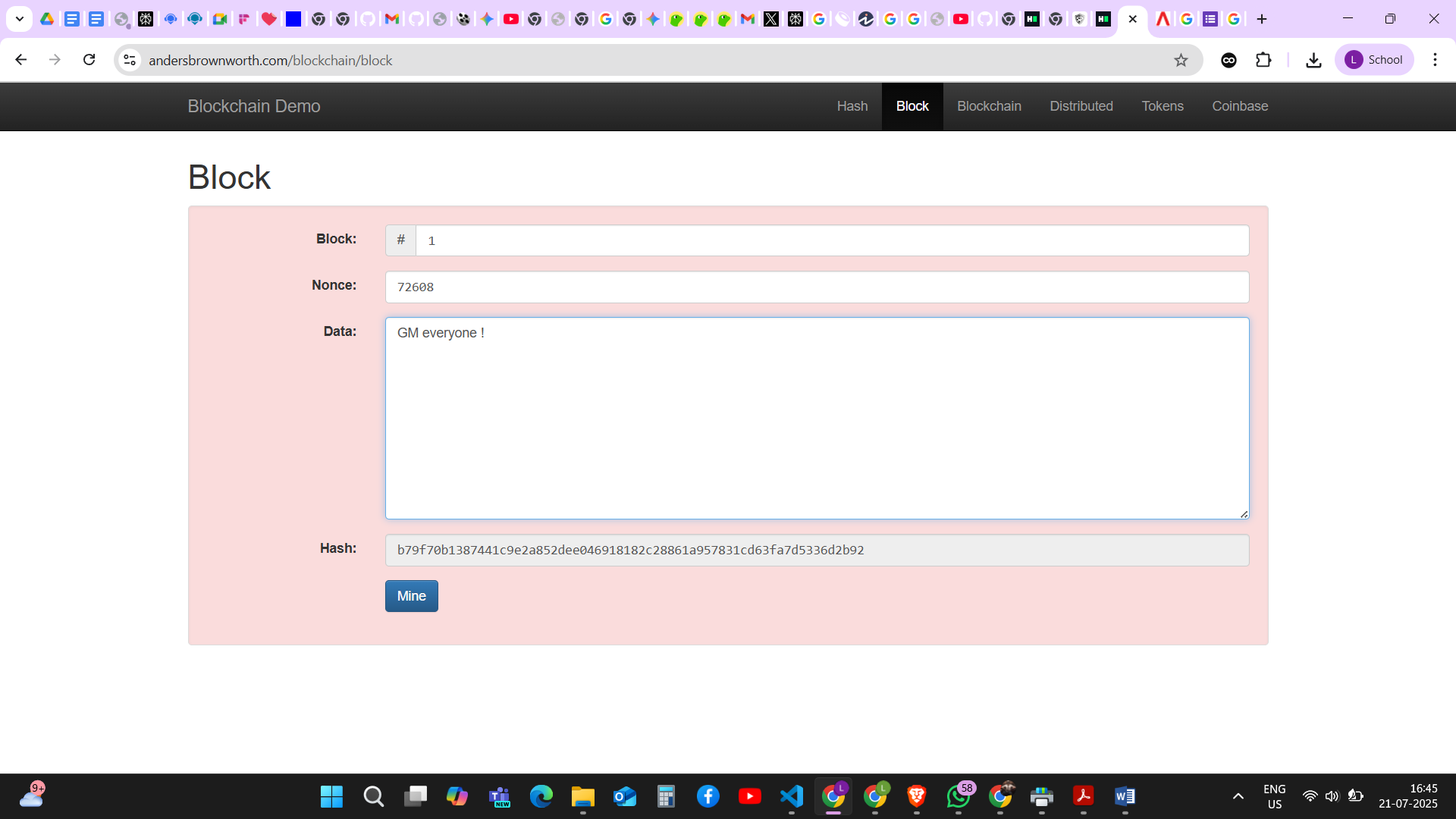
1. Cryptographic Hash Functions  
   These are algorithms creating a **unique, fixed-size digital fingerprint** for any data, making it computationally impossible to reverse or find two different inputs with the same output.
2. Blocks and Their Hashes  
   Each block includes the **cryptographic hash of the previous block**, forming an unbreakable, sequential chain and ensuring data integrity.
3. ImmutabilityDue to linked hashes, any alteration to a past block's data will **invalidate subsequent blocks**, making the blockchain inherently tamper-proof and secure.
4. Proof-of-Work (Mining)  
   In some blockchains, "mining" involves solving a complex puzzle to find a valid block hash, which **secures the network and prevents fraudulent activity** by requiring significant computational effort.

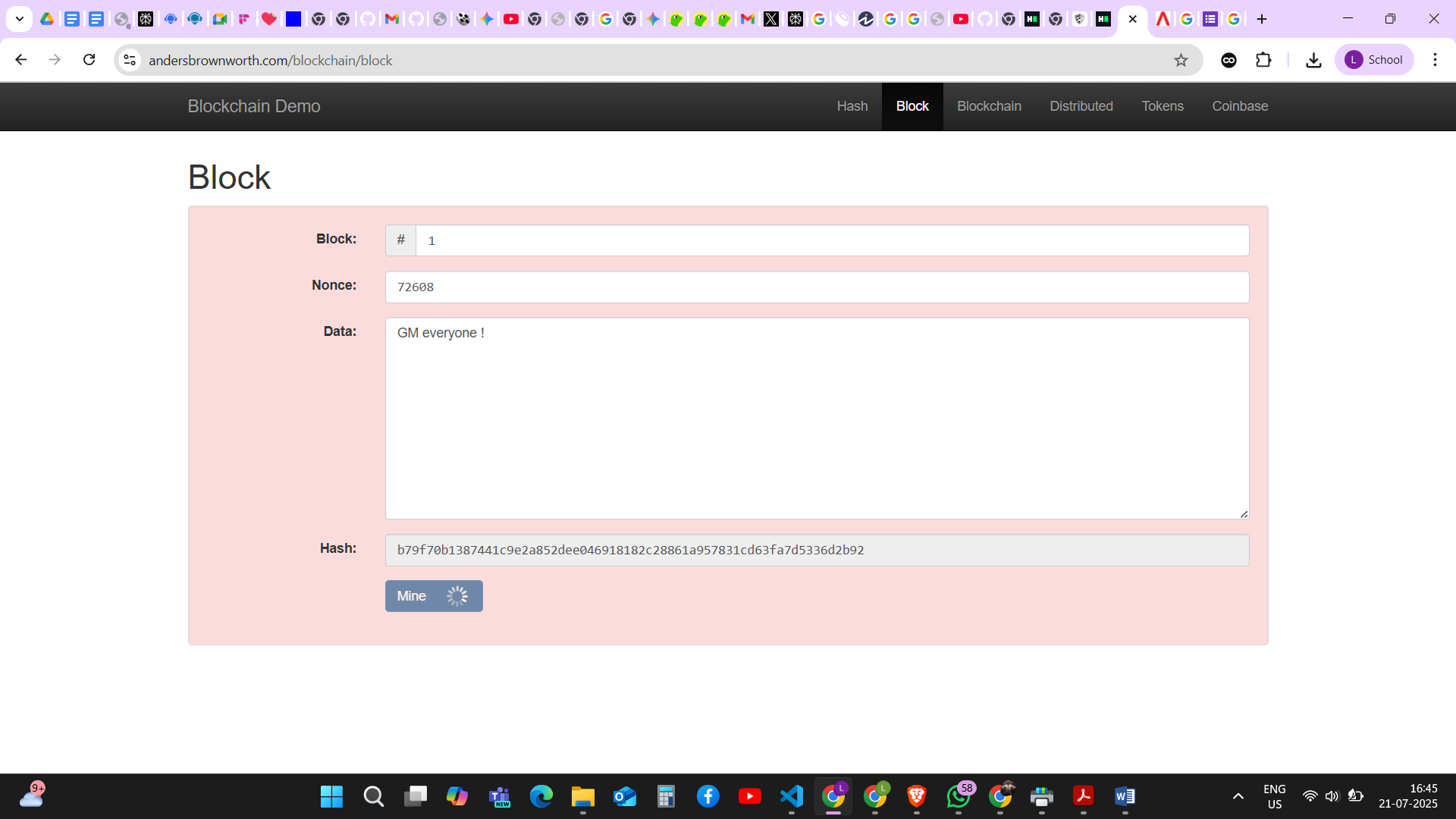


**Procedure:**

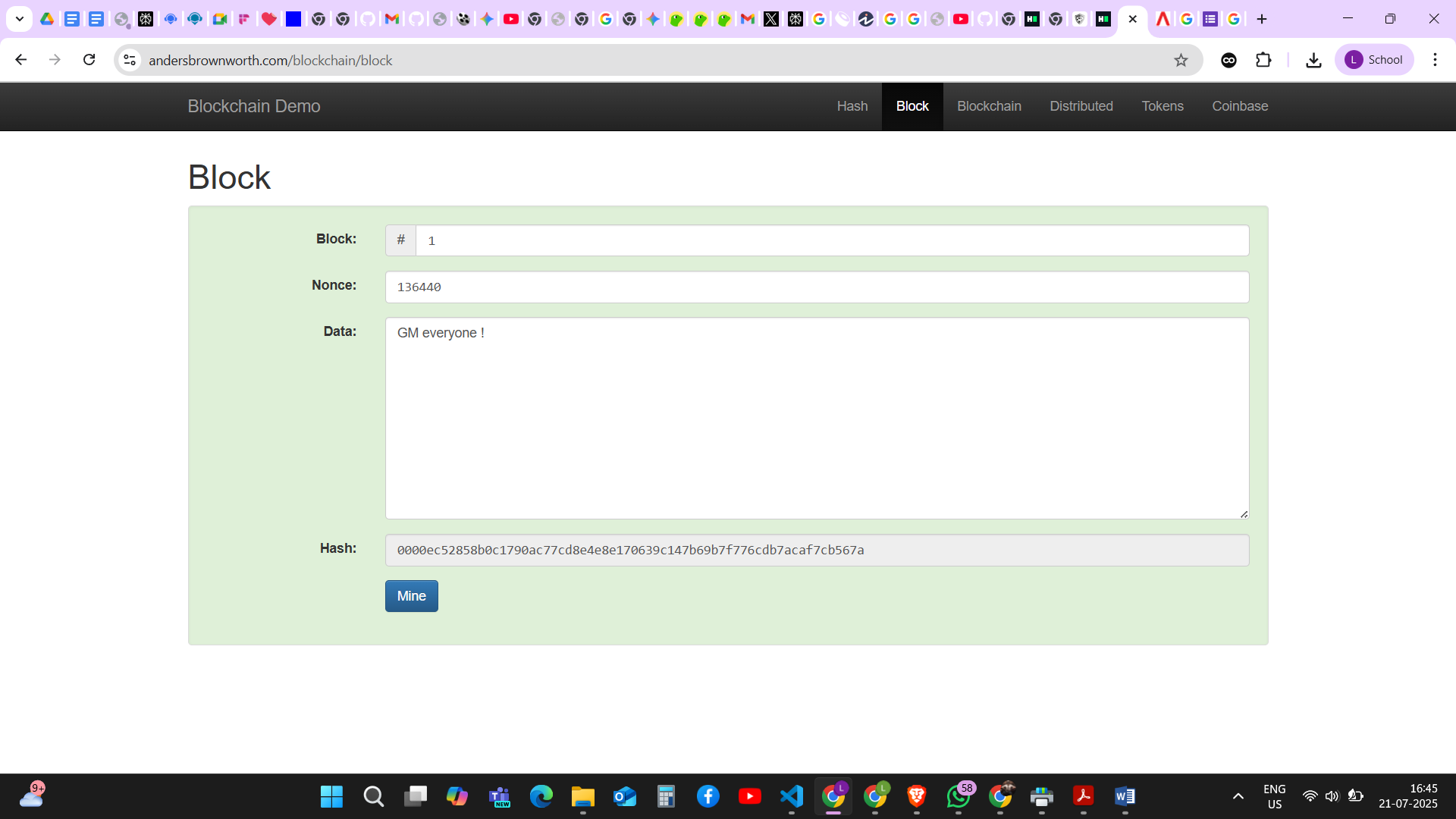
### Steps to Mine a Block on a Blockchain Demo

**Step 1: Observe the initial valid block.** The process begins with a valid block, as indicated by its green background. This is the "genesis block" or a previously mined block. The hash for this block starts with four leading zeros (0000f...), which satisfies the conditions for a valid block. The data field is initially empty.

 **Step 2: Add data to the block and observe the invalidation.** Text, in this case, "GM everyone!", is entered into the data field. Any change to the block's data immediately alters its hash. The new hash (b79f7...) no longer meets the validity condition (it doesn't start with four zeros), and the block's background turns red to show that it is now invalid.

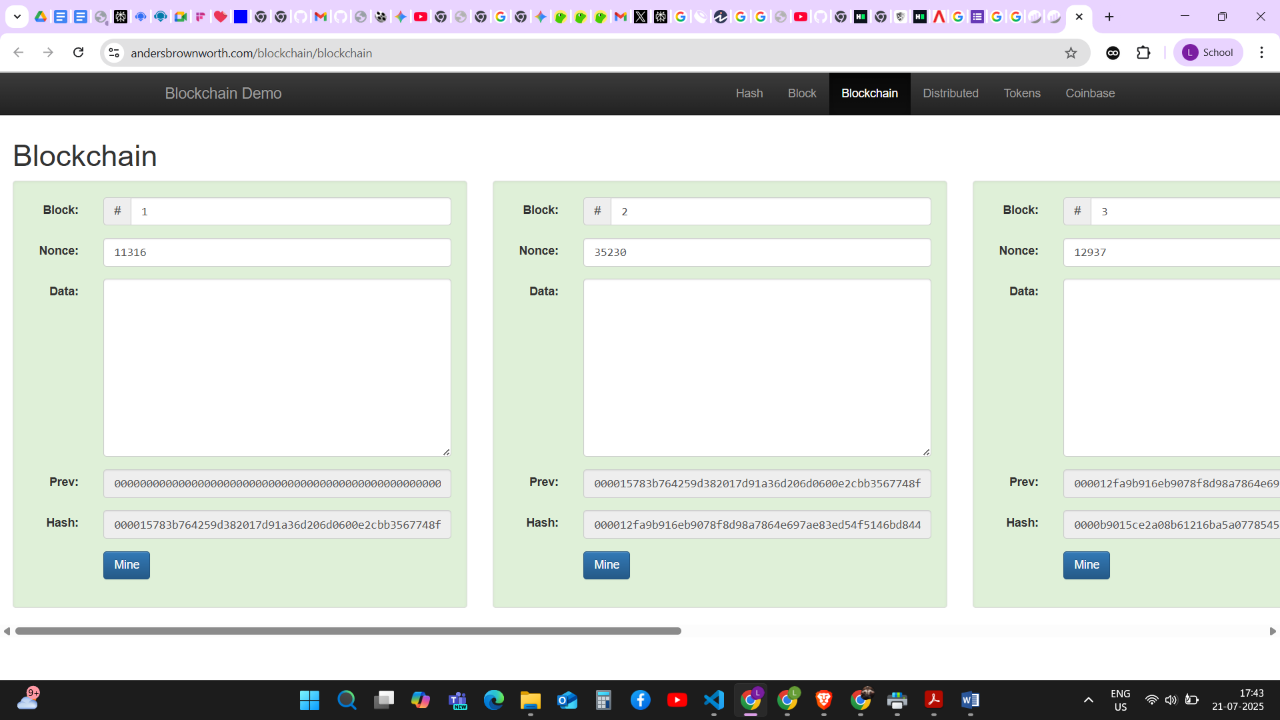
**Step 3: Initiate the mining process.** To make the block valid again with the new data, the "Mine" button is clicked. This starts the computational process of finding a new "nonce" (a number used once). The system will rapidly try different nonce values until it finds one that, when combined with the rest of the block's data, produces a valid hash.

**Step 4: A valid block is found through mining.** After the mining process is complete, the system has found a new nonce (136440). This new nonce results in a new, valid hash (0000ec...) that once again starts with four leading zeros. The block's background turns green, signifying that it has been successfully mined and is now a valid part of the blockchain.



**Observation**

#### The Initial Valid Chain

First, we see a complete and **valid** blockchain. Each block has a **hash** that starts with leading zeros, and the background of each block is green. Critically, Block #2's "**Prev**" field contains the exact hash of Block #1, and Block #3's "Prev" field matches the hash of Block #2. This creates a secure, cryptographic chain.

#### Tampering with a Block

Now, data is added to **Block #1**. The moment this new data is entered, the **hash** of Block #1 instantly changes. Because this new hash no longer starts with leading zeros, Block #1 becomes **invalid** (red).

This single change creates a domino effect:

* The "**Prev**" hash listed in Block #2 no longer matches the new hash of Block #1.
* This mismatch invalidates Block #2, which in turn invalidates Block #3. The entire chain is now broken and invalid.

#### The Chain is Valid Again

The entire blockchain is now secure and valid again, with the new data correctly incorporated. This process demonstrates that changing even a single piece of data in an earlier block requires a significant amount of computational work to re-validate all subsequent blocks, making the blockchain highly tamper-evident and secure.