Blockchain

## Summary

## This lab investigates the math and data structures that go into creating a block chain.  Bitcoin adds two additional features: proof of work and distributed consensus.

## Tools/Resources

Websites:

<https://andersbrownworth.com/blockchain/blockchain>

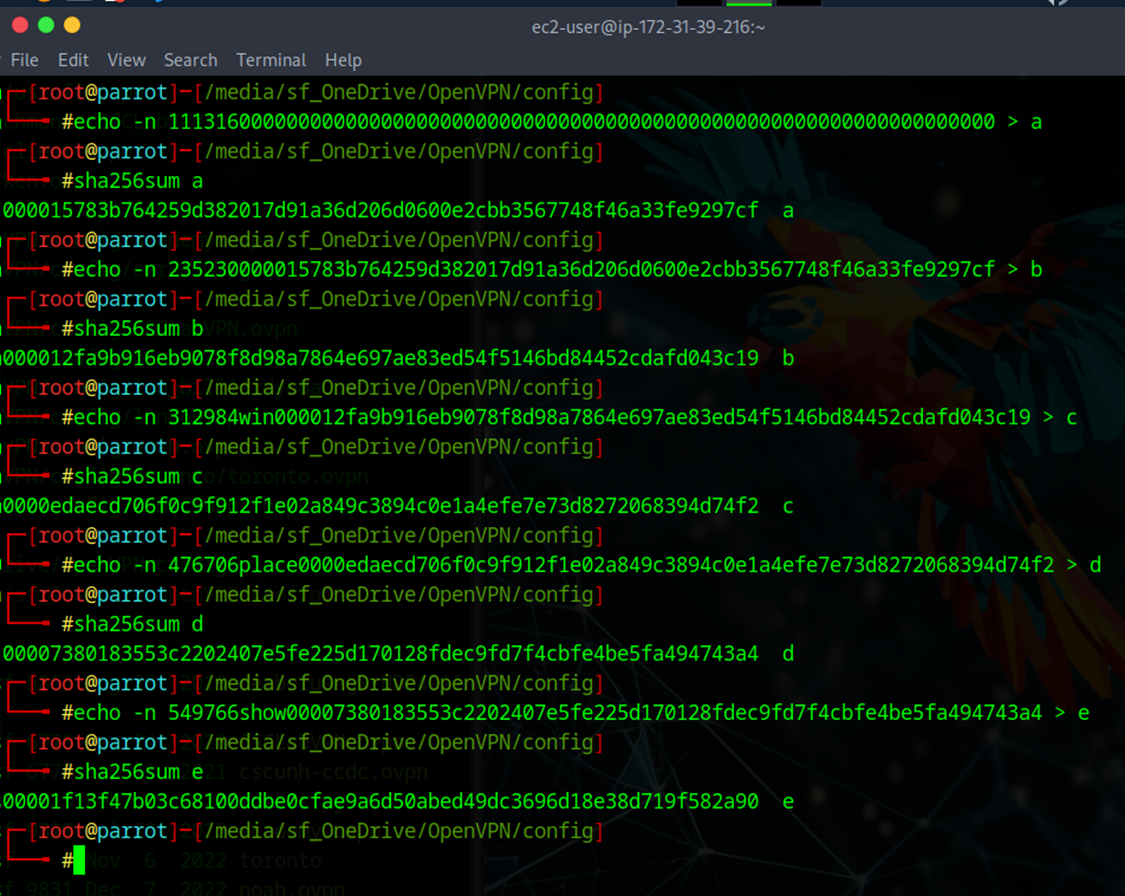
<https://gchq.github.io/CyberChef/>

## Tasks

* Peers: Decide who is going to be Peers A, B, and C
* Independently change a single transaction, mine until your peer is all green.
* Confirm the calculation is correct by computing your own SHA256 hash for the transaction you changed.
* Group: Exchange your transaction change with peers.
* Reconcile the changes make by your peers,
* Record the number of mine clicks until all green.  Remember all 3 peers need to agree on a final hash value (consensus).  Did everyone in your group need the same number of mine clicks?

## Submission

Upload to Canvas a docx or pdf containing the command line interaction for your group’s sha256 validation (all 5 blocks).  Your command shell will look something like:



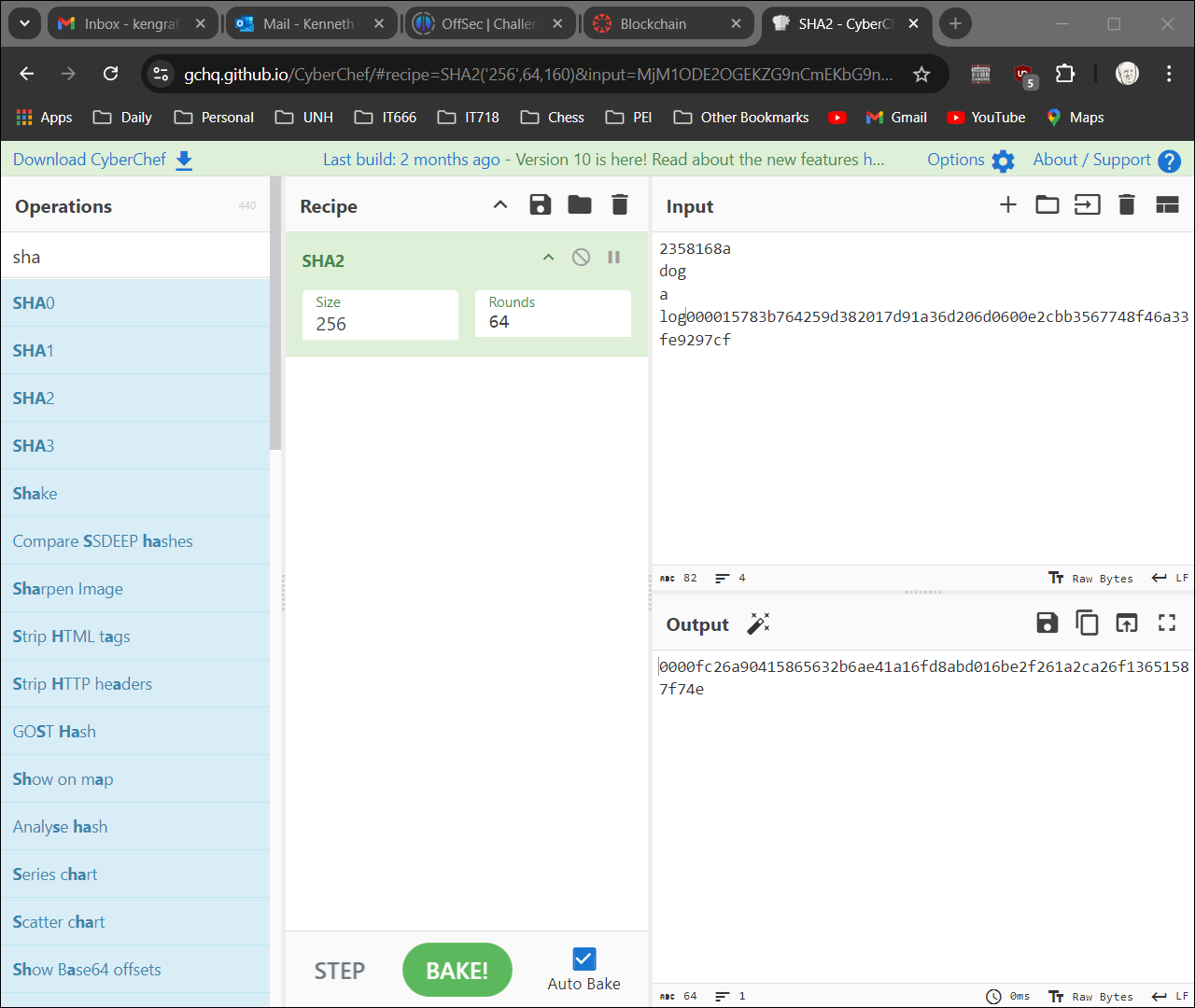
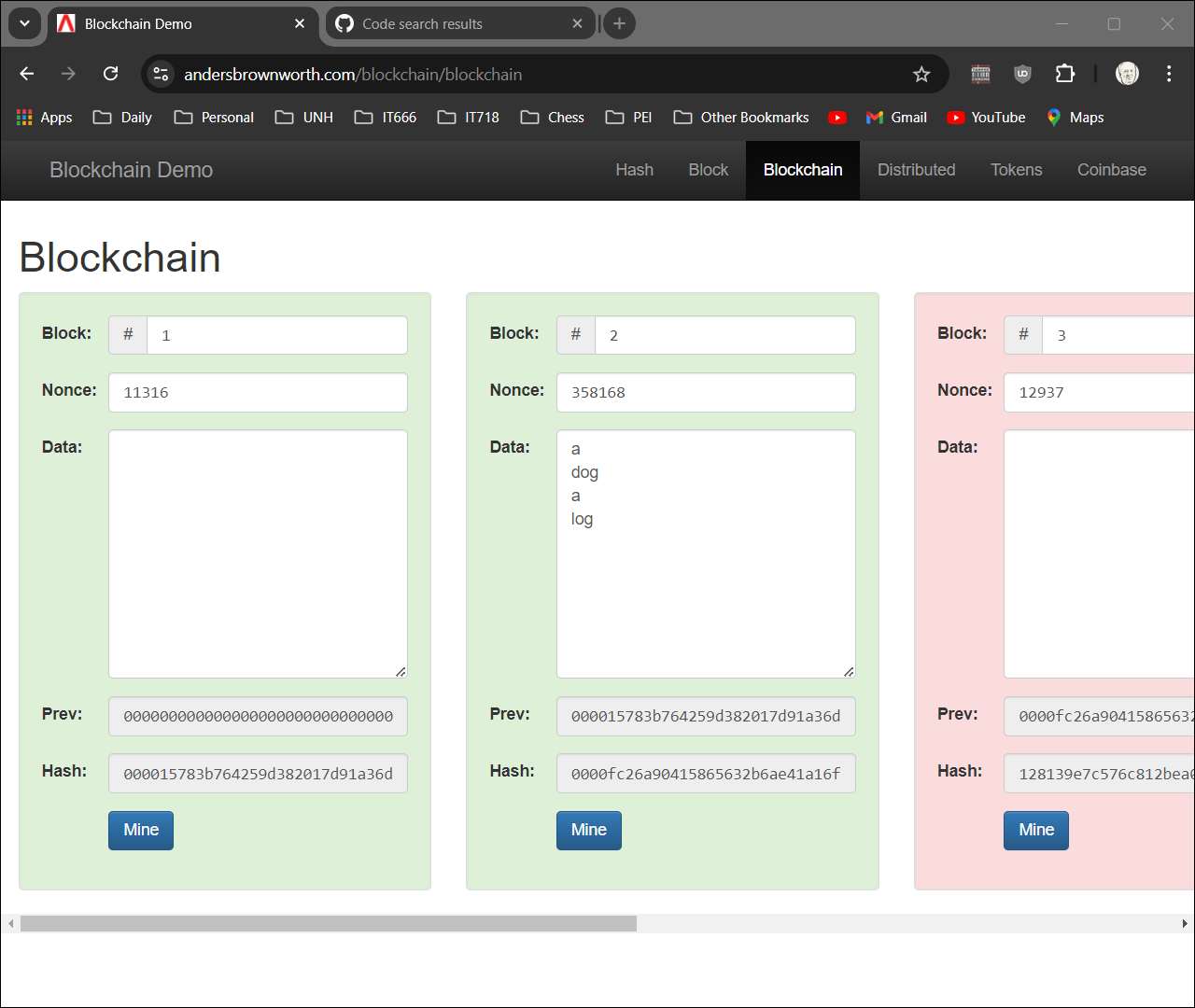
## Walkthrough

1. Open <https://andersbrownworth.com/blockchain/blockchain>
2. Prove you can calculate your own hashes using the data from the first block: block# + nonce + data + previous. CyberChef can also be used.

A screenshot of a computer

Description automatically generated

1. Add some message to the second block and click the “Mine” button. After a few seconds the site will calculate a new nonce so the hash value begins with “0000” and turns the block green again. Notice the other blocks are red. Why? Click the “Mine” button for the other red blocks. Does the order you click matter?
2. Validate your new message hashes correctly (whitespace matters) with either sha256sum or CyberChef



## Group exercise: Groups of 3.

Using the Distributed tab: <https://andersbrownworth.com/blockchain/distributed>

**Decide who is going to be Peers A,** B, and C

Independently change the data in one of the transactions for your peer. Count the number of mine clicks until your peer is all green.

**Group:**exchange your transaction change with the other peers.

Reconcile the changes make by your peers,

Count the number of mine clicks until all green.  Remember all 3 peers need to agree on a final hash value (consensus).

## Submission

Upload to Canvas a docx or pdf containing a screenshot showing your group’s sha256 validation

A screenshot of a computer

Description automatically generated

## Additional Thoughts

How are transactions stored in a bitcoin block? Merkle trees