Web3 Cohort by 100xDevs

Goal

To create a Cohort of people who are great at Blockchains, Web3.

My background in Web3

Detailed video - https://www.youtube.com/watch?v=gYK8azCYjnU

Started working in Sept 2022. Worked at ~3 companies since. Primarily worked at Wallets, Exchanges and Gambling websites.

Syllabus

Easy - https://blog.100xdevs.com/Web3-Client-side-9375f2aa571f4644aa45c3b5a5b6927c?pvs=25

Hard - https://blog.100xdevs.com/Web3-Contracts-ce3796e9db0e45708bc173f718b23392

TAs

Cohort Projects

1. https://github.com/code100x/stake - **Harkirat Singh**
2. https://github.com/code100x/tiplink - Led by **@cb7chaitanya**, mentored by Harkirat

If you want to propose a project, please build a v1 for the Superteam hackathon and we can sponsor it further

Cohort 3.0 Exclusive Hackathon

Link - https://earn.superteam.fun/listings/project/100xdevs-solana-mini-hackathon-1/

We’re doing an exclusive hackathon with $100 prize for the top 50 submissions

Focus on UX. Have a live link deployed.

Why blockchains?

Inflating currencies

Government has been printing currencies left right and center. This leads to increasing inflation, price of everything goes up.

Holding on to cash is a losers bet in the long run. Holding on to any asset (Gold, Stock, real estate) is better compared to currencies like USD, INR.

Fractional reserve Banking

Banks dont have your money. They lend out most of it.

If there is a bank run (everyone goes to the bank to withdraw their money), banks wont be able to pay everyone

Silicon valley collapsed in 2022. I was in the US when it happened. Most YC companies had their

How to create a new currency?

Right now, currencies can only be issued by central governments. You can’t create your own `Kirat coin` and ask users to use it.

Even if I do issue a `Kirat coin` , no one would use it, and for good reasons -

1. I can print any number of Kirat coins, making myself richer
2. I become the central mint and verification athority for the coin.
3. No one would (or should) trust me

Intro to hashing

Hashing is a process that transforms input data (of any size) into a fixed-size string of characters.

Hash functions have several important properties:

1. **Deterministic**: The same input will always produce the same output.
2. **Fast computation**: The hash value can be quickly computed for any given data.
3. **Pre-image resistance**: It should be computationally infeasible to reverse the hash function (i.e., find the original input given its hash output).
4. **Small changes in input produce large changes in output**: Even a tiny change in the input should drastically change the hash output.
5. **Collision resistance**: It should be computationally infeasible to find two different inputs that produce the same hash output.

Is this a hashing algorithm?

What if I try “hashing” a string by increasing each alphabet’s value by one. Do you think this follows all the rules we’ve written above?

SHA-256

Lets try out a famous hash function, SHA-256 here - https://emn178.github.io/online-tools/sha256.html

Node.js code for generating SHA-256

```
const crypto = require('crypto');

const input = "100xdevs";
const hash = crypto.createHash('sha256').update(input).digest('hex');

console.log(hash)
```

Intro to Proof of work

Assignment #1

What if I ask you the following question — Give me an input string that outputs a SHA-256 hash that starts with `00000` . **How will you do it?**

A: You will have to brute force until you find a value that starts with `00000`

▼ Node.js code

Copy

```
const crypto = require('crypto');

// Function to find an input string that produces a hash starting wi
function findHashWithPrefix(prefix) {
    let input = 0;
    while (true) {
        let inputStr = input.toString();
        let hash = crypto.createHash('sha256').update(inputStr).dige
        if (hash.startsWith(prefix)) {
            return { input: inputStr, hash: hash };
        }
        input++;
    }
}

// Find and print the input string and hash
const result = findHashWithPrefix('00000');
console.log(`Input: ${result.input}`);
console.log(`Hash: ${result.hash}`);
```

Assignment #2

What if I ask you that the `input string` should start with `100xdevs` ? How would the code change?

▼ Node.js code

Copy

```
const crypto = require('crypto');

// Function to find an input string that produces a hash starting wi
function findHashWithPrefix(prefix) {
    let input = 0;
    while (true) {
        let inputStr = "100xdevs" + input.toString();
        let hash = crypto.createHash('sha256').update(inputStr).dige
        if (hash.startsWith(prefix)) {
            return { input: inputStr, hash: hash };
        }
        input++;
    }
}

// Find and print the input string and hash
const result = findHashWithPrefix('00000');
console.log(`Input: ${result.input}`);
console.log(`Hash: ${result.hash}`);
```

Assignment #3

What if I ask you to `find` a nonce for the following input -

```
harkirat => Raman | Rs 100
Ram => Ankit | Rs 10
```

Copy

▼ Node.js code

```
const crypto = require('crypto');

// Function to find an input string that produces a hash starting wi
function findHashWithPrefix(prefix) {
    let input = 0;
    while (true) {
        let inputStr = `
harkirat => Raman | Rs 100
Ram => Ankit | Rs 10
` + input.toString();
        let hash = crypto.createHash('sha256').update(inputStr).dige
        if (hash.startsWith(prefix)) {
            return { input: inputStr, hash: hash };
        }
        input++;
    }
}

// Find and print the input string and hash
const result = findHashWithPrefix('00000');
```

Copy

```
console.log(`Input: ${result.input}`);
console.log(`Hash: ${result.hash}`);
```

Assignment #4

Lets explore https://andersbrownworth.com/blockchain/

Intro to Bitcoin

Bitcoin white paper was released in 2008 - https://bitcoin.org/bitcoin.pdf

1. Introduction

2. Transactions

3. Timestamp server

4. Proof of work

5. Network

6. Incentive