What we will Build

1. Perform a Proof of work to secure the blockchain
2. Create new blocks through a mining process
3. Create new, immutable, transactions
4. Validate the blockchain and all block data
5. Retrieve address/transaction/block data

Feature of our Blockchain Network

1. Create Api(Server) to intract with our blockchain from the internet
2. Upgrade API to a decentralized blockchain network, to host our blockchain
3. A consensus algorithm to make sure the data is legitimate and always synchronized
4. A Block Explorer, to explore the data in our blockchain through a user interface

What is a Blockchain?

An immutable , Distributed ledger

Ledger - A collection of financial account or transaction

Eg- Nik paid 30$ to Sid

John paid 80$ to Julia

Immutable - the ledger cannot be changed. Ever!

Distributed – not controlled by a single entity but instead run by normal everyday people.

Eg Facebook is centralized controlled by single

Node – each person contributed to the chain is called node and each node has the full updated copy of the ledger. So the ledger data is hosted synchronized across the network.

Industries Blockchain can improve

Financial services industries

Health care industries

Credit industries

Governments

Energy industries

Create a folder named Blockchain. Inside Blockchain folder create a dev folder and within that create two files called blockchain.js and test.js

Run npm init

Constructor function

A function that create a object and allow you to create a many instance of that class

Function User( firstName, lastName, age, gender){

this.firstName= firstName

this. lastName = lastName

this. age = age

this. gender = gender

}

var user1 = new User(‘John’, ‘Smith’, 26, ‘male’)

var user2 = new User(‘Julia, ‘Smith’, 25, ‘female)

if we add the property to the prototype of the constructor function then all the instance of the constructor function will have it.

User.proptotype.emailDomain=’@facebook.com’

Lets create Blockchain constructor function

What is proof-of-work?

Every blockchain is list of blocks and every single block has to be created and added to the chain. But before adding each block has to be legitimate (follow some rule and law) and correct txn and data should be inside it.

Every time we create a block we ensure it’s a legitimate block by mining it through proof of work

What Proof of work do?

“repeatedly hash block until it finds correct hash 🡺 ‘0000iuyiuyiuyiuyiuy” four zeros in the beginning

uses current block data for the hash but also the previousBlockHash

continuously changes nonce value until it find the correct hash

and return the nonce value that creates the correct hash

why hacking is tough

In order to generate the correct hash we need to run our hash block hundred of times and need lot of energy along with the currentBlockData and previousBlock.