**Deptt. Of Computer Science,**

**NIT Srinagar**

**Blockchain Development Internship Report**

Prepared by:

**Irfan Mehraj Wani**

**irfanwani347@gmail.com**

**+916005377974**

**August 05 , 2022**

**Chapter 0: Internship Description**

**Chapter 1: Blockchain**

**1.1: Introduction**

**1.2: How a Blockchain works**

**1.2.1: Understanding Hash and Hashing Functions**

**1.2.2: What is a Block?**

**1.2.3: Blockchain**

**1.2.4: Distributed Blockchain**

**1.2.5: Private key and Public key**

**1.3: Concensus**

**1.3.1: Proof of Work**

**1.3.2: Proof of stake**

**Internship Description**

This Internship was intented to teach me the basics of blockchain development. In this internship, i learned about blockchain, how it works and different components which make it to work and blockchain development (i.e, decentralized applications over a blockchain). I learned about different techlologies used to build an application over a blockchain. Some of them are;

Blockchain (what is it and how it works),

Ethereum blockchain, What it is and how to interact with it,

MetaMask,

smart contracts,

Solidity (A programming language to create smart contracts),

Deploying a smart contract and interacting with it,

setting a local blockchain using Ganache (ganache-cli),

Chainlink (providing data to the blockchain in a decentralized manner)

And so on...

**Chapter 1:** **Blockchain**

**1.1: Introduction**

A blockchain is a distributed database or ledger that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format.

Bitcoin was the first protocol to use this technology. This network is powered by cryptography. Blockchain brings in the concept of decentralisation where there is no intermediatory and there occur only peer to peer transactions in this system.

E.g, Ethereum uses blockchain to create decentralised applications, organisations etc.

Blockchain is a type of shared database that differs from a typical database in the way that it stores information; blockchains store data in blocks that are then linked together via cryptography.

As new data comes in, it is entered into a fresh block. Once the block is filled with data, it is chained onto the previous block, which makes the data chained together in chronological order.

Different types of information can be stored on a blockchain, but the most common use so far has been as a ledger for transactions.

In Bitcoin’s case, blockchain is used in a decentralized way so that no single person or group has control—rather, all users collectively retain control.

Decentralized blockchains are immutable, which means that the data entered is irreversible. For Bitcoin, this means that transactions are permanently recorded and viewable to anyone.

**1.2: How a Blockchain Works?**

The goal of blockchain is to allow digital information to be recorded and distributed, but not edited. In this way, a blockchain is the foundation for immutable ledgers, or records of transactions that cannot be altered, deleted, or destroyed. This is why blockchains are also known as a distributed ledger technology (DLT).

First proposed as a research project in 1991, the blockchain concept predated its first widespread application in use: Bitcoin, in 2009. In the years since, the use of blockchains has exploded via the creation of various cryptocurrencies, decentralized finance (DeFi) applications, non-fungible tokens (NFTs), and smart contracts.

**1.2.1: Understanding Hash and Hashing Functions**

Hash Function can be defined as a function which takes an input (some data) and applies some algorithm to produce an output of fixed length and the output is known as hash.

They are pseudo-random functions because, though they produce random outputs after we provide an input but the output always remains same with same input provided.

There are many examples of hash functions used these days in cryptography like, SHA256, SHA1, SHA2, Keccak256 (used by Ehtereum).

SHA256 is one of the most used hash functions these days. It takes an input of any length and produces an output of size 256 bits. In this

function, output has a size of 256 bits, i.e, it has 256 poisitions to be filled with either 0 or 1.

Thus total number of possible hashes which can be produced using this function is 2256 , thus making it nearly impossible to crack a hash.

There are only two ways to break a hashing algorithm;

1) Reverse Engineering the hash: One can reverse engineer the hashing algorithm (i.e, take the output andd retrace the path to the input) and extract the input from the output, but till date, no one has done this and seems impossible.

2) Brute Force: Another way to break a hash is to try different inputs until we get the desired hash thus giving us the desired input. Though this method doesn’t seem impossible but is very close to that as we already saw that there are a lot of possible hashes which makes it very difficult to guess that many hashes and it requires a lot of computational power.

Thus above two points justify the fact that hash functions are nearly impossible to crack making them secure, which is the reason they are used for managing passwords in databases and also in blockchain to validate a block.

E.g,

“superstrongpassword” if provided as an input string to SHA256 algorithm will produce a result as shown below;

9ca80cbce084b692e0b78adf4dc3f6b8883221d1fd59c86162c6f97bf4b75b8e

**1.2.2: What is a Block?**

Blocks are data structures within the blockchain database, where transaction data in a cryptocurrency blockchain are permanently recorded. A block records some or all of the most recent transactions not yet validated by the network. Once the data are validated, the block is closed. Then, a new block is created for new transactions to be entered into and validated.

A block is thus a permanent store of records that, once written, cannot be altered or removed.

A block is a place in a blockchain where information is stored and encrypted.

Blocks are identified by long numbers that include encrypted transaction information from previous blocks and new transaction information.

Blocks and the information within them must be verified by a network before new blocks can be created.

A block is represented by four parts;

1) Block Number: It is the number of the block in the blockchain.

2) Nonce: Stands for numbe used once, is a unique number assigned to a block which also represents the block. It acts as a solution to the block, as mining means finding a proper nonce which satisfies the condition for the hash (E.g, Hash should start with 4 zeroes).

3) Data: This represents the actual data to be stored in the block.

4) Hash: Hash is the output of the hash function where the first three (block number, nonce and data) collectively act as input.

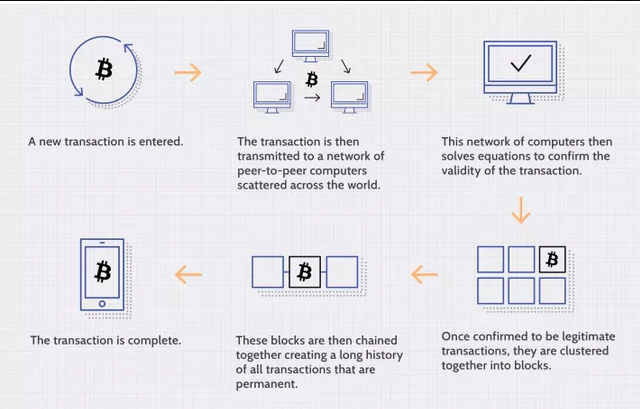
Besides these 4 components, when a block is in a blockchain, it also contains the hash of the previous block thus, getting connected to it, forming a chain, thus known as blockchain.

**1.2.3: Blockchain**

When multiple blocks are connected with each other where each block has the hash of previous block too, it is known as a blockchain.

First block in a block chain, which doesn’t have a previous hash, is known as Genesis Block.

Below is a diagram explaining the transaction process in a blockchain;



Simply put, a blockchain is a shared database or ledger. Pieces of data are stored in data structures known as blocks, and each node of the network has an exact replica of the entire database.

Security is ensured since if somebody tries to edit or delete an entry in one copy of the ledger, the majority will not reflect this change and it will be rejected.

**1.2.4: Distributed Blockchain**

When same blockchain is on different nodes in a network, it is known as Distributed Blockchain.

This reflects the decentralized nature of the blockchain as it is not controlled by a single node, but is present on every node in the network.

**1.2.5: Private key and Public key**

**Private Key**

A private key is a secret number that is used in cryptography and cryptocurrency.

A private key is a large, randomly-generated number with hundreds of digits. For simplicity, they are usually represented as strings of alphanumeric characters.

A cryptocurrency wallet consists of a set of public addresses and private keys. Anyone can deposit cryptocurrency in a public address, but funds cannot be removed from an address without the corresponding private key.

Private keys represent final control and ownership of cryptocurrency. It is vitally important to prevent one's private keys from being lost or compromised.

**Public Key**

A public key allows you to receive cryptocurrency transactions. It’s a cryptographic code that’s paired to a private key.

While anyone can send transactions to the public key, you need the private key to “unlock” them and prove that you are the owner of the cryptocurrency received in the transaction.

The public key that can receive transactions is usually an address, which is simply a shortened form of your public key.

Therefore, you can freely share your public key without worry.

Private key is used to generate public key using some algorithm.

Ethereum uses Elliptic Curve Digital Signature Algorithm (ECDSA) to generate public keys from private keys.

**1.3: Concensus**

A consensus mechanism refers to any number of methodologies used to achieve agreement, trust, and security across a decentralized computer network.

In the context of blockchains and cryptocurrencies, proof-of-work (PoW) and proof-of-stake (PoS) are two of the most prevalent consensus mechanisms.

Critics of Bitcoin miners have argued that PoW is overly energy-intensive, which has sparked the creation of new and more efficient mechanisms.