IT465 : Cryptocurrencies and Blockchain Technologies

Lab Assignment 2.

Name: Chinmayi C. Ramakrishna Date: 20.11.2021

Roll No: 181IT113

Q.1) Write about consensus algorithms in detail.

Proof of Work

The original consensus algorithm in a Blockchain network is called Proof-of-Work (PoW). This consensus method is used to validate transactions in the blocks and add them to the existing chain. This task is performed by miners. Miners compete against each other to solve a difficult mathematical puzzle. The miner to first complete the puzzle gets to add the block and is rewarded in return.

The main principle is the ability to solve a difficult mathematical puzzle and prove the solution with ease. This subsequently requires great computational power. Some of them are mentioned next.

1.

1) Hash function : this tells how to find the input knowing the output.

2) integer factorisation : this tells how to present a number as a multiplication of two other numbers.

3) guided tour puzzle protocol : if the server suspects a DoS attack, it requires a calculation of hash functions, for some nodes in a defined order. In this case, it's a 'how to find a chain of hash function values' problem.

The answer to the PoW problem or mathematical equation is called hash.

However, there are two problems involved.

1) As the network expands, the mathematical puzzle becomes more and more difficult. As a result, the hash power required increases. It is a computational intensive task leading to high power consumption.

2) The miners from mining pools can get undue advantage. This can lead to the very problem blockchain tries to solve : centralisation. With PoW, you will be much more likely to mine the next block if your mining

operation is scaled up. This gives richer miners an unfair advantage.

Proof of Burn

Proof of Burn (PoB) is a consensus technique that attempts to address the PoW system's high energy consumption issue.

PoB is generally referred to as a PoW system that does not waste energy.

Miners that deliver the money to an address that is verifiably unspendable in order to burn them. This procedure uses few resources (apart from the coins destroyed) and ensures that the network remains active and flexible. Miners may burn the native currency or an alternate chain's currency, such as Bitcoin, depending on the implementation. In exchange, users are given a reward in the blockchain's native currency token.

This network allows you to send transactions that burn your own bitcoin tokens. Besides mining / burning your block, other participants can add their transactions to yours. The purpose of all of this coin-burning activity is

to keep the network nimble, and both players are rewarded for their efforts.

By ensuring that cryptocurrencies are burned on a regular basis, the POB system prevents early adopters from being unfairly disadvantaged.

According to critics, proof-of-burn wastes resources in the same way that the resources required to manufacture the burned coins are wasted. Proof of Burn is similar to the Proof of Work consensus technique, in which individuals with a large number of currencies continue to accumulate even more coins.

Proof of Stake

Proof of Stake is the type of consensus mechanism used by blockchain networks to achieve distributed consensus.

It requires users to enter their ETH in order to become a network authentication. Authenticators are responsible for the same thing as miners in proof of work: ordering transactions and creating new blocks so that all nodes

agree on network status.

Proof of stake provides some benefits :-

1) energy efficiency
you do not need to use multiple energy blocks.

2) low entry barriers, reduced hardware requirements.

3) strong instability in a single placement

4) strong shard chain support

The validation process does not require the use of significant accounting power values, since validators are selected at random and do not compete. The only thing they need to do is create blocks when selected and verify the proposed blocks otherwise. This process is known as affirmation. Creators receive awards for raising new blocks and verifying them. If you testify to vicious blocks, you lose your stake.

Proof of Elapsed Time

Proof of Elapsed Time (PoET) is an Intel

5

corporation - developed consensus technique for determining new block winners and mining rights in permissioned blockchain networks.

PoET uses a lottery method that distributes the chance of winning evenly among network participants, ensuring that each node has an equal chance of winning.

For each node in the blockchain network, the PoET algorithm generates a random wait time, each node must go to sleep for that length.

The node that has the least wait time will be the first to win the block, allowing it to add a new block to the blockchain. The information is then broadcast to the entire network. The process is repeated for the discovery of the next block.

The PoET workflow is comparable to Bitcoin's proof of work (PoW), but it uses less energy since it allows a miner's processor to sleep and transition to other jobs for a predetermined amount of time, enhancing efficiency.

6

Proof of Activity.

Proof of Activity (PoA) is a combination of PoW and PoS.

In PoA, the mining process starts in the same way as the PoW process, with various miners trying to outdo each other with high computing power to get a new block. When a new block (or mine) is discovered, the system switches to PoS, with the newly discovered block containing only the miner's title and reward address.

Based on the details of the title, a new, a random group of verifiers from the block-chain network is selected, they need to confirm or sign a new block. If the author is the owner of most of the coins, the greater the chances of becoming a signer. Validators begin to sign the newly found block as soon as it is signed by all of them, and then it gains the status of a complete block, gets identified and added to the blockchain, and transactions begin to be recorded within it.

Decred (DCA) is most well-known cryptocurrency using PoA.

7

Proof of Weight

Proof of weight (PoWeight) is a blockchain consensus mechanism that gives users 'weight' based on how much crypto currency they carry. While a weighted harmonization approach is secure, it does not protect the network from double exposure attacks if the majority of users are honest.

Each time a blockchain transaction is made using the PoWeight consensus, the network establishes a committee made up of randomly selected network members and assigns 'weight' to each member which is minimal. The weight assigned is based on how much money they hold in the network.

Q2. What are the various attacks that are possible on Blockchain?

Finney attack.

It is a double duplicate destroyer that requires the miner's involvement when the block is dug. The risk of Finney's attack cannot be eliminated

8

no matter what safety precautions taken by the dealer, but some hash strength of the miners' force is needed and a certain sequence of events must occur. As in the case of a race attack, the seller or seller must consider the cost/ profit when he recieves payment with just one assurance when there is no assistance to the attacker.

Finney's attack works as follows: Suppose an attacker produces blocks from time to time. For each block he produces, he includes the transfer from address A to B, both of which he controls. To deceive you, when he makes a block, he does not spread it. Instead, you open your store web page and make a payment at your C address with A address. She is broadcasting her block now, and her transaction will come before your own.

2) Race attack

Race attack is just another "race" between two transactions that have been broadcast at almost the same time. The idea is to replace the original transaction with another refund in the fund you control, before the first job is written on the blockchain. The danger of being

vulnerable to a race attack or finney attack is when an unconfirmed transaction is accepted.

51% attack

when it comes to blockchains that use proof of work, 51% of attacks involve the attacker being able to gain of more than 50% of hashing power. By doing so, he or she is able to manipulate the data in the blockchain. First, they send a large amount of cryptocurrency to an exchange. Then, they convert it to another cryptocurrency and move the traded funds off the exchange to an address they own. Once completed, they reorganise the blockchain using this attack vector and "orphan" or "erase" their first transaction, leaving them with both the assets they traded with and the assets they traded for.

Eclipse attack

Eclipse attack involves a malicious character that seperates a particular user or node within a peer - to - peer (P2P) network. When performing an eclipse attack, the attacker attempts to redirect the user's internal and external connections directly away from the official neighbouring

10

nodes to the attacker-controlled nodes, and then closes the target in a completely different area from the actual network activity. By interfering with the current legal status of the blockchain ledger, an attacker could exploit a separate node in a variety of ways that could lead to the illicit transaction and prevent mining disruption. Because eclipse attacks are dependent on exploitation of neighboring target areas, how easily these attacks can be carried out depends largely on the basic structure of the targeted blockchain network.

Sybil attack

Sybil attack is a cyber security violation in which an attacker can create multiple fake identities that can act as nodes to flood a targeted network with the intent to disrupt or take over. Sybil attack uses the way official nodes build connections. Sybil attacks can be particularly dangerous if targeted to systems where new nodes are created and easily adapted.

DDoS attack

When they attack a blockchain network using DDOS attack, hackers aim to slow down the server

11

by using all of its processing resources for multiple applications. DDoS attackers aim to cut through the mines of network mines, e-wallets, crypto exchanges and other financial services. The blockchain can be hacked via DDoS attack in its system layer using a DDoS botnet.

In 2017, Bitfinex suffered a major DDoS attack. It was very difficult for the IOTA Foundation, which presented their IOTA token on their platform the day before Bitfinex informed users about the attack. Three years later, in February 2020, Bitfinex experienced another DDoS attack just a day after OKEx exchange cryptocurrency saw a similar attack.

Routing attack.

Routing attack can affect both individual nodes and the entire network. The idea of this robbery is to disrupt what is being done before your piers push you. It is almost impossible for other nodes to detect this disruption, ~~as~~ the hacker seperates the network into non communicable components.

Route attack actually involves two different attacks: partition attack, which seperates network

12

nodes into sipirate groups. Delay attack, which interrupts streaming messages and send them over the network.

DAO attack

The DAO is called the Decentralised Autonomous Organisation (DAO). DAOs are coded rules as smart contracts, which are also computer pro-grammes that assist, guarantee or enforce contract negotiations or performance or that make a subcontracter unnecessary. In simple terms, think of any ~~two~~ contracts between two parties that is translated into code, so it does not require an external action but automatically executes what has been agried upon.

The idea of DAO is that once introduced it can work based on its own smart contracts alone. DAO's smart contracts are based on Ethereum, a public blockchain (which is a distributed repository - for more information on the blockchain that is stored) a platform with a structured and basic ether (or ETH) transaction, cryptocurrency. ETH is a cryptocurrency similar to Bitcoin, but it is very popular as it offers a wide range of servces

13

and is therfore sometimes regarded as a major competitor to Bitcoin as the leading cryptocurrency.

Timejack attack

Timejacking uses the perceived vulnerability in managing the Bitcoin timestamp. During a timejacking attack, a hacker changes the node network timer and forces the side to accept another blockchain. This can be achieved if a malicious user adds multiple fake peers to a network with inaccurate timestamps. However, timejacking attacks can be prevented by limiting the reception time or using the node system time.

Q3) Write an example to create a Blockchain with Javascript.

```
const SHA256 = require("crypto-js/sha256");
class Block {
    constructor(hash, timestamp, data, lastHash=" "){
        this.hash = hash;
        this.data = data;
        this.timestamp= timestamp;
        this.lastHash = lastHash;
        this.hash= this.computeHash();
```

14

```
    this.nonce = 0;
}

computeHash(){
    return SHA256(
        this.hash + this.lastHash + this.timestamp +
        JSON.stringify(this.data) + this.nonce
    ).toString();
}

proofOfWork(difficulty){
    while(
        this.hash.substring(0, difficulty) != Array(
        difficulty +1).join("0")
    ){
        this.nonce++;
        this.hash= this.computeHash();
    }
}
}

class Blockchain {
    constructor(){
        this.blockchain = [this.genesisBlock()];
        this.difficulty = 4;
    }
    genesisBlock(){
        return new Block(0, "01/01/2020", "First Block", "0");
    }
```


15

```
findLastBlock(){
    return this.blockchain[this.blockchain.length-1];
}

addBlock(newBlock){
    newBlock.lastHash = this.findLastBlock().hash;
    newBlock.proofOfWork(this.difficulty);
    this.blockchain.push(newBlock);
}

checkChainValidity(){

    for(let i=1; i<this.blockchain.length; i++){
        const currentBlock= this.blockchain[i];
        const lastBlock= this.blockchain[i-1];

        if(currentBlock.hast!==currentBlak.computeHash())
        { return false; }
        if(currentBlock.lastHash !== lastBlock.nash)
            return false;
        return true;
    }
}

let coin = new Blockchain();

console.log("coin mining progressing...");
```


16

```
coin.addBlock(
    new Block(1, "08/10/2021", {
        sender: "Chinmayi C.R.",
        recipient: "Seema C.A.",
        quantity: 120
    })
);

coin.addBlock(
    new Block(2, "12/11/2021", {
        sender: "Mike Thomas",
        recipient: "Billy Manor",
        quantity: 100
    })
);

coin.addBlock(
    new Block(3, "28/04/2021", {
        sender: "Jenny Henry",
        recipient: "Kibutsuji",
        quantity: 50
    })
);

console.log(JSON.stringify(coin, null, 4));
```

17

Q4) Explain the importance of hyperledger with an example.

Hyperledger is a global business blockchain project that provides the required framework, standards and tools for building open source blockchains and related applications. Hyperledger projects include a variety of blockchain platforms that are commercially viable, in which network participants are known individually and as a result have a deep interest in participating in the compliance process. Using the components available under the hyperledger umbrella, an entity can use a variety of modular blockchain solutions and services to significantly improve the performance of their operations and efficiency of their business processes.

Examples.

Simbridge is the blockchain based digital asset exchange for institutional and authorised investors built on the open Source Hyperledger Fabric protocol. Simbridge's advanced technology utilises advanced security, consistency and state of the art authentication that guarantees without

18

blockchain and integrates with a highly efficient trading environment. The main advantages are better clarity, stronger security, greater accuracy, reduced costs and more efficient trading. Building on Hyperledger Fabric allows Symbridge to have a dedicated authentication network without sacrificing performance.

Public Mint, built on Hyperledger Besu, is an open blockchain integrated with API platform that allows fiat money to reap all the benefits of cryptocurrency, eliminating flexibility, and sophistication. Public Mint is the first fiat-native public blockchain that allows individuals, companies, applications and banks to engage in innovative and uncomplicated ways of making money. People and businesses from around the world are free to build all kinds of fiat-based apps and services over Public Mint, which is funded without the usual banking restrictions.

Q.5) Consider an example of health care and explain the importance of Blockchain.

The potential for blockchain technology to impact the healthcare sector extends beyond

the patient provider's paradigm as well. Blockchain solutions can ensure reliability and facilitate transparency in pharmaceutical product development, a process often extended under rigorous testing of data integrity or 'cleanliness'. If the data is not properly recorded, or worse, intentionally or haphazardly - all research, including billions of dollars and years, can be rendered completely useless. A government agency tasked with authorizing medicines and producing better patient health outcomes can easily and legibly track clinical research data with the blockchain technology.

Veridat is a U.S. company that developed these principles. This program uses the Bitcoin SV blockchain to bring integrity and data purity to the pharmaceutical industry. A long standing issue in medical research has been trust and transparency, with research and tests conducted on large volumes of data that could have a profound impact on the prospect of developing companies and patients. To deliver the best health outcomes, it's paramount to ensure the integrity, and reliability of that data. Transforming clinical research and trust to the field, Veridat utilises blockchain to synchronize clinical data.

20