|  |  |
| --- | --- |
| Logo UNIMAS | **UNIVERSITI MALAYSIA SARAWAK**  **Faculty of Computer Science and Information Technology** |

# Assignment/Report Cover Sheet

|  |  |  |  |
| --- | --- | --- | --- |
| Student Name (lecture group no) | Student Id Number | L. Group | Signature |
| NUR ASMA BINTI HASAN | 53104 | 01 |  |
| FATIN SHAHIRAH BINTI AMANZURIA | 55978 | 01 |  |
| SITI AMEERA BINTI AZAHAR | 57870 | 01 |  |
| AMIRA IZZATI SHAHILA BINTI AHMAD RIZAL | 55453 | 01 |  |
| MOHAMMAD FARHAAN IQBAL | 59404 | 01 |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subject Code: **TMN2073** | | Subject Name : **Computer Security** | | |
| Assignment Title : | **Project Report** | | Lecturer: | **Dr Adnan Shahid Khan** |
| Due Date : **21/5/2018, 4:00pm** | | | Date Submitted: **21/5/2018** | |

This cover sheet must be completed, signed and firmly attached to the front of the submission. All work must be submitted by the due date. If an extension of work is granted, an assignment extension acknowledgement slip must be signed by the lecturer/tutor and attached to assignment. Please note that is your responsibility to retain copies of your assignment.

|  |
| --- |
| ***Plagiarism and Collusion are methods of cheating that falls under Peraturan Akademik Universiti Malaysia Sarawak para 11: Etika Akademik***  **Plagiarism**  Plagiarism is the presentation of work which has been copied in whole or in part from another person’s work, or from any other source such as the internet, published books or periodicals without due acknowledgement given in the text.  **Collusion**  Collusion is the presentation of work that is the result in whole or in part of unauthorized collaboration with another person or persons.  Where there are reasonable grounds for believing that cheating has occurred, the only action that may be taken when plagiarism or collusion is detected is for the staff member not to mark the item of work and to report or refer the matter to the Dean. This may result in work being disallowed and given a fail grade or if the circumstances warrant, the matter may be referred to a Committee of inquiry for investigation. Such investigation may result in the matter being referred to the University Discipline Committee, **which** has the power to exclude a student. |

|  |
| --- |
| **Upon placing signature above, I certify that I have not plagiarized the work of others or participated in unauthorized collusion when preparing this assignment.**  **I also certify that I have taken proper case in safeguarding my work and have made all reasonable efforts to ensure that may work not be able to be copied.** |

|  |
| --- |
| **MARK :** |

**TABLE OF CONTENT**

CONTENT PAGE

1) BRIEF INTRODUCTION………………………………………………………………3

2) PROBLEM STATEMENT………………………………………………………………3

3) OBJECTIVE…………………………….……………………………………………….3

4) SIGNIFICANCE………………………………………………………………………...3

5) SUGGESTED SOLUTION………………………………………………………..…….4-5

6) PROVE YOUR SOLUTION IS CORRECT…………………………………………….6-12

7) REFERENCES…………………………………………………………………………..13

1. **BRIEF INTRODUCTION**

Our group being assigning to make decentralized chat using whisper protocol. Whisper is a communication protocol for DApps to communicate with each other.Whisper is designed for easy and efficient broadcasting, and also for low-level asynchronous communications. It is designed to be a building block in next generation of unstoppable DApps. All Whisper messages are supposed to be sent to every Whisper node, but only recipient has the key to decrypt it. Other means with this app we have a better way to send messages without having to trust a big network rather trust encryption.

1. **PROBLEM STATEMENT**

We have to trust a server and centralized system to send messages for example Facebook messages. All messages are saved and Facebook have all the rights over the messages like modify, delete and control over all the messages.

1. **OBJECTIVE**

To create a decentralized chat application without the present of centralized server where user has full control over the network which guards against temper and misuse of information.

1. **SIGNIFICANCE**

The application is much more secure between sender and receiver only. The processing time for each message is slower because of darkness.

1. **SUGGESTED SOLUTION**

We trying to create a decentralized chat app where there is no central server. That means no one can control the messages and we all control it at the same times.

With the power of proof of work on the blockchain we can easily guard against fake (impersonation) of messages. Means with this app we have a better way to send messages without having to trust a big network.

DApps that need to publish small amounts of information to each other and have the publication last some substantial amount of time. For example, a currency exchange DApp may use it to record an offer to sell some currency at a particular rate on an exchange. In this case, it may last anything between tens of minutes and days. The offer wouldn't be binding, merely a hint to get a potential deal started.

DApps that need to signal to each other in order to ultimately collaborate on a transaction. For example, a currency exchange DApp may use it to coordinate an offer prior to creating one (or two, depending on how the exchange is structured) transactions on the exchange.

DApps that need to provide non-real-time hinting or general communications between each other. E.g. a small chat-room app.

DApps that need to provide dark (plausible denial over perfect network traffic analysis) comms to two correspondents that know nothing of each other but a hash. This could be a DApp for a whistleblower to communicate to a known journalist exchange some small amount of verifiable material and arrange between themselves for some other protocol (Swarm, perhaps) to handle the bulk transfer.

In general, think transactions, but without the eventual archival, any necessity of being bound to what is said or automated execution & state change.

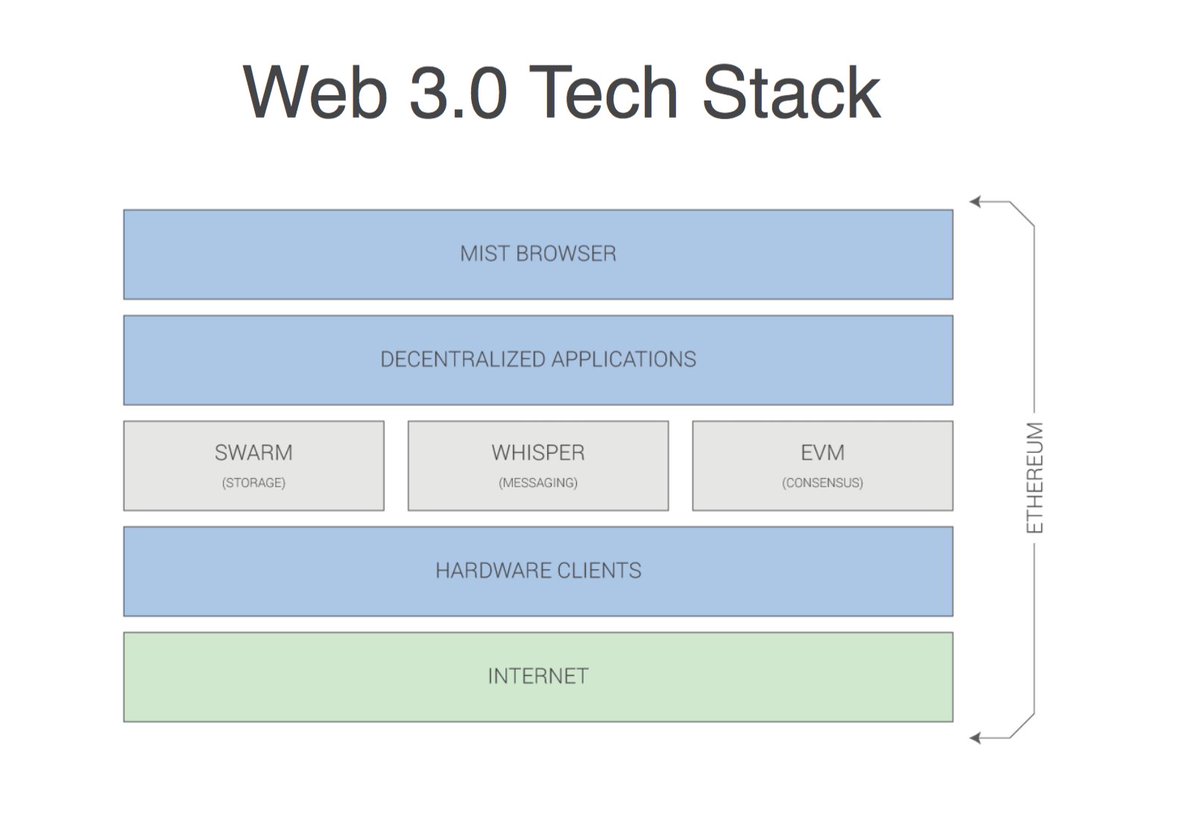


Figure 1. Web 3.0 – utilizing blockchain in web

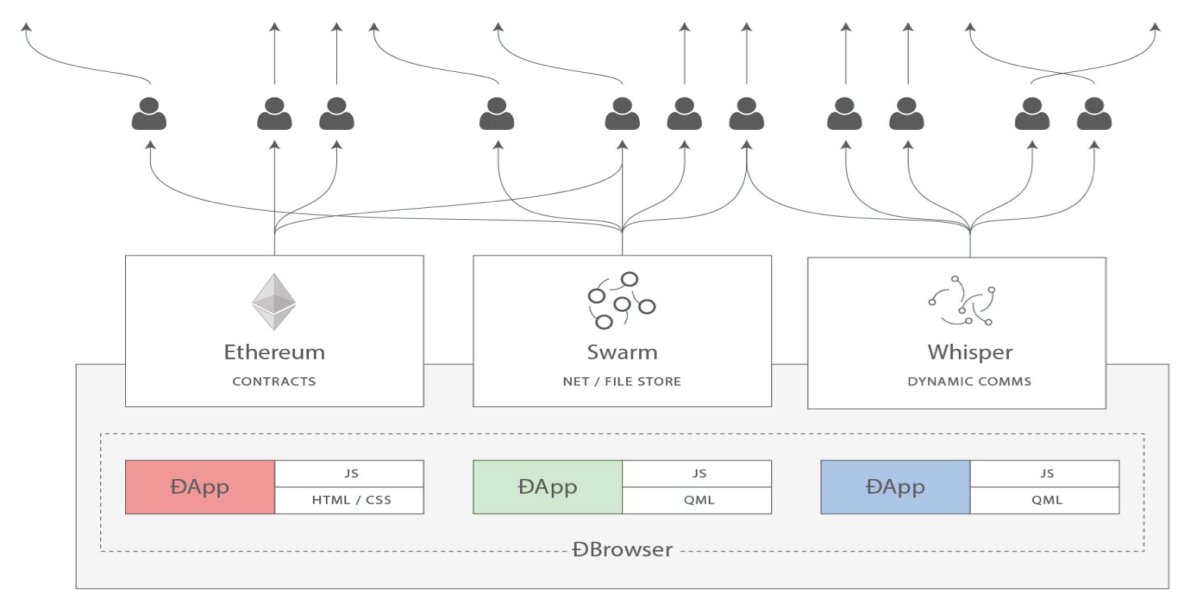


Figure 2.0 Whisper protocol acting on Ethereum network.

1. **PROVE YOUR SOLUTION IS CORRECT**

**<template>**

**<div>**

**<h1>Whisper Example Chat Application</h1>**

**<div v-if="!configured">**

**<input type="checkbox" v-model="asym" /> Asymmetric<br>**

**<asymmetric-key-config v-if="asym" :pub-key="asymPubKey" :key-id="asymKeyId"></asymmetric-key-config>**

**<symmetric-key-config v-else @update-sym-key="updateSymKey" :sym-key-id="symKeyId"></symmetric-key-config>**

**username: <input v-model="name" /><br>**

**<button @click="configWithKey" v-if="(asymKeyId || symKeyId) && name">Start</button>**

**</div>**

**<div v-else>**

**<div v-if="asym">**

**My publick key: {{asymPubKey}}**

**Recipient's public key: <input v-model="recipientPubKey" />**

**</div>**

**<div v-else>**

**Key: {{symKeyId}}**

**</div>**

**<p v-for="m of msgs">**

**<b>{{m.name}}</b>: {{m.text}}**

**</p>**

**Please type a message: <input v-model="text" @keyup.enter="sendMessage" />**

**<button @click="sendMessage">Send</button>**

**</div>**

**</div>**

**</template>**

**<script>**

**import Web3 from 'web3';**

**import SymmetricKeyConfig from './SymmetricKeyConfig.vue';**

**import AsymmetricKeyConfig from './AsymmetricKeyConfig.vue';**

**import {decodeFromHex, encodeToHex} from './hexutils';**

**const defaultRecipientPubKey = "0x04ffb2647c10767095de83d45c7c0f780e483fb2221a1431cb97a5c61becd3c22938abfe83dd6706fc1154485b80bc8fcd94aea61bf19dd3206f37d55191b9a9c4";**

**const defaultTopic = "0x5a4ea131";**

**export default {**

**data() {**

**this.web3 = new Web3(new Web3.providers.HttpProvider("http://localhost:8545"));**

**this.shh = this.web3.shh;**

**let data = {**

**msgs: [],**

**text: "",**

**symKeyId: null,**

**name: "",**

**asymKeyId: null,**

**sympw: "",**

**asym: true,**

**configured: false,**

**topic: defaultTopic,**

**recipientPubKey: defaultRecipientPubKey,**

**asymPubKey: ""**

**};**

**this.shh.newKeyPair().then(id => {**

**data.asymKeyId = id;**

**return this.shh.getPublicKey(id).then(pubKey => this.asymPubKey = pubKey).catch(console.log);**

**}).catch(console.log);**

**return data;**

**},**

**components: {AsymmetricKeyConfig, SymmetricKeyConfig},**

**methods: {**

**sendMessage() {**

**let msg = {**

**text: this.text,**

**name: this.name**

**};**

**this.msgs.push(msg);**

**let postData = {**

**ttl: 7,**

**topic: '0x07678231',**

**powTarget: 2.01,**

**powTime: 100,**

**payload: encodeToHex(JSON.stringify(msg)),**

**};**

**if (this.asym) {**

**postData.pubKey = this.recipientPubKey;**

**postData.sig = this.asymKeyId;**

**} else**

**postData.symKeyID = this.symKeyId;**

**this.shh.post(postData);**

**this.text = "";**

**},**

**updateSymKey(sympw) {**

**this.shh.generateSymKeyFromPassword(sympw).then(symKeyID => this.symKeyId = symKeyID)**

**},**

**configWithKey() {**

**// TODO use a form**

**if (!this.name || this.name.length == 0) {**

**alert("Please pick a username");**

**return;**

**}**

**let filter = {**

**topics: ['0xdeadbeef']**

**};**

**if (this.asym) {**

**if(!this.asymKeyId) {**

**alert("No valid asymmetric key");**

**return;**

**}**

**filter.privateKeyID = this.asymKeyId;**

**} else {**

**if (!this.symKeyId || this.symKeyId.length == 0) {**

**alert("please enter a pasword to generate a key!");**

**return;**

**}**

**filter.symKeyID = this.symKeyId;**

**}**

**this.msgFilter = this.shh.newMessageFilter(filter).then(filterId => {**

**setInterval(() => {**

**this.shh.getFilterMessages(filterId).then(messages => {**

**for (let msg of messages) {**

**let message = decodeFromHex(msg.payload);**

**this.msgs.push({**

**name: message.name,**

**text: message.text**

**});**

**}**

**});**

**}, 1000);**

**});**

**this.configured = true;**

**}**

**}**

**};**

**</script>**

1. **REFERENCES**

Cartwright, T.(2015, July 14).*Socket.io P2P*.https://socket.io/blog/socket-io-p2p/

Muneeb, M.(2017, December 19).*eChat:Decentralized Messenger On the*

*Blockchain*. Retrieved from https://me<dium.com/@mohammadmuneeb/echat-decentrali>zed-messengerab1a8954c953

Elliot, M.(2018, January 12). *Blockchain-Based Communication Platform Aims To Protects*

*Your Personal Message.* Retrieved from <https://cointelegraph.com/news/blockchain-based-> communication-platform-aims-to-protect-your-personal-messages

Irvin Steve Cardenes (2018, Apr 16) *Whisper*. Retrived from

<https://github.com/ethereum/wiki/wiki/Whisper>

Gluk256 (2017, May 10) *Whisper Overview*. Retrived from

https://github.com/ethereum/go-ethereum/wiki/Whisper-Overview