Building a decentralised forum

//Introduction

In the school, I have joined numerous project-based after-school clubs which needed to be collaboration and discussion. However, the platform for student to publish their idea and update their project progress has lots of advertisements and risks to privacy. To improve the current situation, I have decided to make a platform that enables teammates to discuss different topics. I would like to build a forum which benefits from the public scope of view and catching up on conversation easily. The forum will be present in a decentralised network model which means all data will be distributed, saved, and responded to from all nodes because it allows the chat data is saved securely by all the clients.

//Research on Blockchain

Blockchain in simple terms can be distributed database. Each similar data usage will be grouped together as a record. The distributed database known as blockchain will store a group of records which is named a block and organised in a linear structure and formed a chain structure. It is a concept that can be applied and implemented into different categories. The blockchain focuses on peer-to-peer network transmission. A computer on the internet can join the network as a node. When a new node is joined, it will sync with the data of other nodes and verify the data integrity by majority voting and storing the set of validated records. As result, all nodes will have their own copy of the database.

Majority voting is an error checking technique that was originally used in error checking in network data transmission where data is sent multiple times and the most seen pattern will consider as the correct data. Combined with blockchain technology, all different nodes will respond has their own blockchain database so the client can be checked and create a copy after the validation. Serialisation is also an important criterion for the formation of blockchain structure. Serialisation means the database keeps logs of changes and applies the change according to the time log. When it applies to the blockchain, a timestamp is added to the block for nodes to distinguish the linear order of the blockchain to make sure the hash stays the same.

The advantage of blockchain provided the counter-measurement of cyber security. Blockchain offers excellent transparency and permanent data protection. The data inside the block is hardly changeable because the hashing algorithm will generate another hash which is different from the original hash and so the system may use majority voting to decline the invalid update. Also, all changes are publicly viewable so people can

However, ethics and performance are the major against the blockchain. Because of its anonymity, illegal trading and payment will take place in cryptocurrency. It is difficult for police and government to track down. On the other side, blockchain needs computer resources to validate encrypt and prove the data integrity and maintain the data on the blockchain. These operation takes up power consumption and needs an endothermic reaction to cool down which contribute to the global warming issue. Due to the validation by receiving multiple same data at once. Network usage will be higher than usual database operation.

Blockchain requires encryption to secure the data of the blockchain. Encryption is a method that uses a hash function to scramble data known as plaintext into ciphertext. There are 2 types of encryption, symmetric and asymmetric key encryption. The difference between both is symmetric key encryption uses the same key for both encryption and decryption but asymmetric encryption doesn’t. Symmetric encryption is usually faster and more efficient due to shorter key length and simpler to execute. ECC is one of the asymmetric encryption it improved the RSA algorithm by using mathematic sequence - elliptic curves to provide shorter public and private keys for faster encryption and decryption.

The hash function is a mathematical function which converts a simple string (mixture of numerical and alphabetical values) as a key into a sequence of numbers as a hash value. A good hash function will return a unique hash value and return in a fixed length of the hash value. Operation and searching are very time efficient as the program only needed to search for the matched hash value.

//Existing Product

//Planning

Node.JS is used as the forum’s server backend application because it has multiple module extensions and is best for simultaneous website connection. Node.JS contain a module called Socket.io which uses WebSocket protocol to maintain the services. It is a completely different protocol that makes the best use of TCP/IP. It creates a connection between the server and the client and makes requests and responses. With this technology, the server network usage will be much lesser because one connection is needed. It also allows clients to broadcast new transactions as a comment in the forum in real time. Another reason for using node.js is because of the modularity of website content. The module in node.js library including ejs and pub view engine can render dynamic website content which is suitable for the forum because all topics and posts have different content and need to be dynamically rendered.

Before I start coding, risk assessment and planning will be done. There are 2 main safety risks. Firstly, a publicly published server has a risk of DDoS brutal attack. Hackers will use a large number of computers to send requests to the website server to make the server resources overload. Internal publishing websites could effectively minimise the risk of the attack. On the other hand, there is also a risk of users abusing the forum by creating a lot of topics and posts which affect the user experience of other users, cooldown will be used against the abuser.

To plan out the artefact project, I have breakdown the project into 2 main phases, the blockchain structure and network protocol usage. I have the Gantt timeline graph [appendix3] to show the progress of the coding part of the project.

I use the database to store the user detail as they are important data which contain data privacy so it is better to use a centralised database to store the password. I will use SQL query for user detail and login modification. However, the database server has system security too. Hackers could use SQL injection to put in a certain argument of SQL command to grant access to the system. To minimise the risk, I should use parameterised SQL commands, limit access to new hall students only and set up a user account with less privilege to the system administrator to secure the data.

//Technical solution

I have created a block [appendix 1], and transaction[appendix 2] class structure and imported them into the server. My idea is to create 3 different applications, the website server, the blockchain server and the blockchain node. The role of the blockchain server retrieves the network address from the node to provide a P2P connection, the blockchain client obviously is to stores blockchain data and responds to the request from the blockchain server and the website server is getting data from the blockchain server and display it onto the website.

However, I quickly found out it is impossible to do the small school-based project. As the blockchain node requires certain technical skills and storage space. I have re-design the block [appendix 4]and transaction[appendix 5] structure into a simpler, web-orientated script. Luckily, socket.io and crypto-algorithm provided a client version which can be run perfectly on the website without any installation on the computer. I use cookies and localStorage inside the browser which takes up at most 10 megabytes of computer storage. It is an ideal solution because it allows P2P via the browser itself and the website can verify the block in the browser and insert it into localStorage which creates a “distributed” database in website format

To be attractive to the user, I used Bootstrap 5 as the framework of the website CSS template in the pop-up window for login [appendix 10] and a button for the main page to provide a better user experience of using the forum. For the main search page [appendix 8], I use the layout of Google Search which makes the page simplest as possible. The page provides trending, search and random topic selections designed for all types of people whether casually browsing or specific topic discussion. On the other hand, modern simple grayscale colour has been used in the layout of the discussion section [appendix 9]. Also, the text area can be hidden to maximise work efficiency. In addition, the website is fully tailored to both desktop and mobile users.

There are several hinders while problem I have faced during my development is that there aren’t enough working clients to retrieve the data. Other nodes (website client) are needed to be online and stay active for the website to load data properly. Another problem is that the scope of the variable is not as wide as I think. The framework I have used for transmitting data between clients has refused to emit to other nodes which makes the peer-to-peer insist on server. A node in the server is always running and data transmission of P2P will pass through and store at the server temporarily as the solution of problem I have met while developing.

//Evaluation and conclusion

To prove the success of the website, I had 200 different visits to the forum[appendix 6] //in a time period //and received more than 20 responses[appendix 7] about my website. The overall ratings are above average show that the website runs well and the visits proved that the website server and handle a certain amount of access at the same time. The comment is notable the login progress could be simplified and the comment section could have more functionality like emoji and image insert and delete function should also be added into the forum. To improve the user experience, the “Single Sign On” Feature provided by the social media platform should be added as a feature of the forum.

Time management is the greatest drawback of my project. I spent too much time on the website UI and the research process which makes the whole project finish hastily without too much improvement and feedback. Although the drawback of ethics cannot be resolved because of the immutability of blockchain, I am satisfied with the final product so far. It is because my friends can use the forum to share their academic work and idea which align with my initial idea.