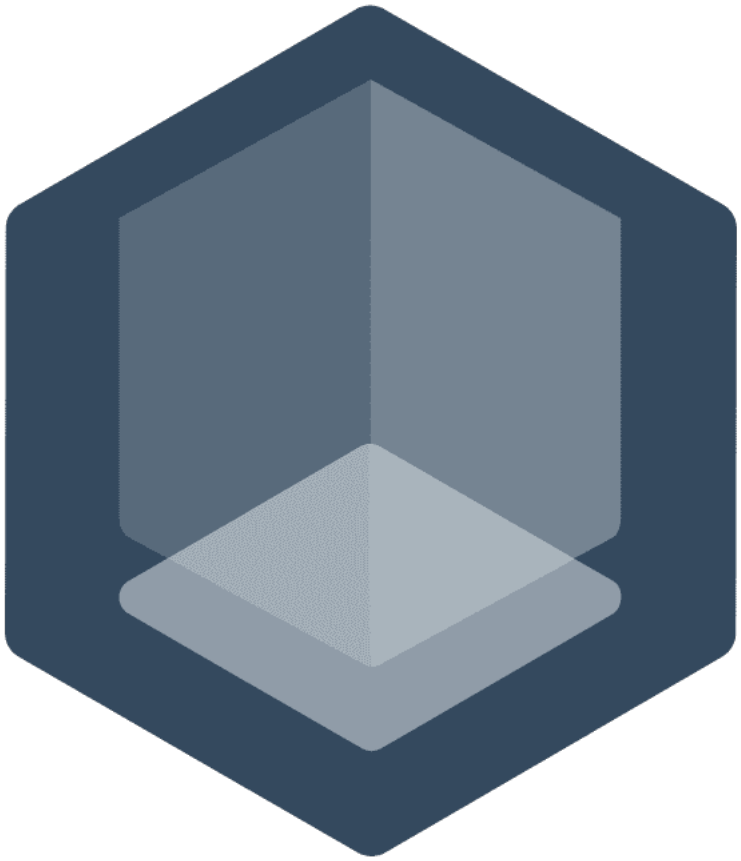

WeJure

A decentralized social network using blockchain and the interplanetary file system (IPFS)

1 Background

During this century, technology has advanced so much that it has become the driving force of the world. Some of the most notable inventions are smartphones, Wi-Fi, the World Wide Web. With such tools, people have been able to communicate with one another across the globe, access information with a touch of a finger, or receive entertainment almost anytime, anywhere.

In 1997, the first social media, Six Degrees was created, and since then, social medias have been evolving. The most dominant social media platforms in the current decade have been Facebook, YouTube, Twitter, and Instagram. According to a research (Deyan, 2022), people spend roughly 2.5 hours per day on social media in 2020.

Although social medias have brought huge benefits to the society, it still contains flaws. In the recent years, privacy has become a major concern. So far, social media platforms have been owned by their respective central organizations, meaning all the data as well as security are being handled by one single origination. As thus, concerns like free speech, privacy, and security have been raised in the past few years. A solution to such problems would be to implement the platform in a decentralized manner.

A decentralized application (dapp) refers to an application that runs on a peer-to-peer network instead of a client-server network. As data is distributed to every node in the network, no single authority has control over the network. One way to implement dapp is through the blockchain technology.

To form a block on the blockchain, transactions are clustered together and hashed. The hashing continues until the hash value satisfies the rules provided by the blockchain. Once succeeded, it is put as the new block on the blockchain of a node. This will then be broadcasted to all other nodes in the network, in which the block will be validated by the nodes. If the majority of the nodes considers the block to be valid, it will become the new block at every node in the network.

As the hash value of a block is based on its content, any changes would result in a different hash value. Since every block in the blockchain stores the hash value of the previous block, any changes to a block would result in a different hash value and thus would break the blockchain. In order to tamper with the blockchain, the attacker would first have to recalculate the hash value of the block as well as all others that succeed it, followed by taking control of over 51% of the network in order to have the tampered blockchain validated. As such, blockchains are considered very secure (Hayes, 2022).

Given the above reasons, a blockchain-based social media might be the solution to the rising concerns of privacy and security on social media.

2 Implementation

This project is intended to be used on the Ethereum blockchain. The reasons for choosing Ethereum are because it is one of the major blockchains, and it is also the earliest and most popular blockchain that implements smart contracts (Cryptopedia Staff, 2021)

The programming languages used in this project are ClojureScript, Solidity and a bit of HTML for the layout of the web app.

2.1 ClojureScript

ClojureScript is the main language used for this project. It is a compiler for Clojure that emits JavaScript code, which is one of the major languages used for web pages (ClojureScript, n.d.).

The framework used in this project is shadow-cljs and the libraries used are as follows:

2.1.1 Reagent

Reagent is an interface to React, a JavaScript (JS) library that allows its users to create HTML components using simple JS code. Its benefits include reusable components, easy creation of interactive components, and improved performance (Deshpande, 2021).

2.1.2 reagent-material-ui

This library is a wrapper for MUI: a very popular framework for React components.

2.1.3 web3.js

This JS library is used for interacting an Ethereum node.

2.2 Solidity

Solidity is the programming language used for implementing smart contracts: programs that are stored on the blockchain.

2.3 MetaMask

MetaMask is a browser extension that acts as a cryptocurrency wallet (MetaMask, n.d.). It simplifies the configurations needed to set up the web app as it handles the login, as well as the necessary validations needed for a transaction, like whether the user has sufficient coins to make a particular transaction.

2.4 Remix (Ethereum IDE)

The website was used to upload the smart contract to the Ethereum blockchain.

2.5 IPFS

The InterPlanetary File System is peer-to-peer file sharing network that can also be treated as a decentralized storage system.

As every data written to the blockchain comes with a fee, it would be costly and inefficient to upload every user data to the blockchain. Thus, IPFS was chosen to act as the storage system for this project.

The fees needed to upload a file to the IPFS network is decided by the node which provides the API. Infura, one of the API providers, has two plans: a free plan that provides 5GB of storage, and another plan which charges based on the file size. However, this gateway is currently free to use as it is in the beta stage.

3 Development

Since the blockchain is immutable, every change made to the smart contract would require a new copy to be uploaded, which comes with a fee. As such, it would costly if the smart contract was to be uploaded after every update.

Ganache is an Ethereum simulator used for development. Developers using this tool are given fake accounts with fake coins that can be used to make transactions. These transactions are then instantly mined by the program itself to form blocks on the local blockchain. With this tool, development becomes costless and efficient.

4 Limitations

Throughout the report, one major issue with the implementation of the decentralized social media has been repeatedly mentioned: a high cost. As every data uploaded to the blockchain comes with a fee, this undoubtedly discourages users to use the application. This is also the major reason that is preventing most Web2 applications from moving to Web3. Quoting Al-Naji (2021), it is believed that new blockchains are needed specifically for the implementation of decentralized applications in order to overcome these limitations.

Reference

Al-Naji, N. (2021, November 17). *Web 3 social media needs dedicated blockchains*. CoinDesk Latest Headlines RSS. Retrieved April 4, 2022, from https://www.coindesk.com/tech/2021/11/17/web-3-social-media-needs-dedicated-blockchains/

ClojureScript. (n.d.). Retrieved April 4, 2022, from https://clojurescript.org/

Cryptopedia Staff. (n.d.). *What is a crypto smart contract? how they work*. Gemini. Retrieved April 4, 2022, from https://www.gemini.com/cryptopedia/crypto-smart-contracts-explained#section-ethereum-the-first-mover

Deshpande, C. (2021, December 28). *The best guide to know what is react [updated]*. Simplilearn.com. Retrieved April 4, 2022, from https://www.simplilearn.com/tutorials/reactjs-tutorial/what-is-reactjs

Deyan, G. (n.d.). *How much time do people spend on social media in 2022?* Techjury. Retrieved April 4, 2022, from https://techjury.net/blog/time-spent-on-social-media/

Hayes, A. (2022, March 5). *Blockchain explained*. Investopedia. Retrieved April 4, 2022, from https://www.investopedia.com/terms/b/blockchain.asp

MetaMask. (n.d.). *The crypto wallet & gateway to web3 blockchain apps*. MetaMask. Retrieved April 4, 2022, from https://metamask.io/