CReDReP – Censorship Resitant Decentralized Review Platform

Shamna N V
Department of Computer Science and Engineering *(Professor)*
P A College of Engineering
Mangalore, India
shamna.cs@pace.edu.in

Shanen Tajjdeen Khazin
Department of Computer Science and Engineering *(Student)*
P A College of Engineering
Mangalore, India
shanen2000.k@gmail.com

Samah Shakir Ali
Department of Computer Science and Engineering *(Student)*
P A College of Engineering
Mangalore, India
samah.ilfath@gmail.com

Zeeshan Ashraf V O C
Department of Computer Science and Engineering *(Student)*
P A College of Engineering
Mangalore, India
zeeshanashrafvoc@gmail.com

Thahseen Majeed
Department of Computer Science and Engineering *(Student)*
P A College of Engineering
Mangalore, India
thahseen.majeed@gmail.com

***Abstract*— We see recently a widespread interest in decentralized networking in the personal computing space, that has become powerful enough to be nodes in a shared network and allow p2p operations to be carried out with the same level of reliability as specialized servers. With this, we want to illustrate how censorship resistant technologies like blockchain, combined with distributed file system protocol like IPFS can be used to create a product review platform that allows user interaction similar to that of a standard web applicaton and presents itself to be tamper-proof.**

I. INTRODUCTION

Blockchain is essentially a list of records linked together by cryptography. These records are managed in a public fashion by peer-to-peer networks with a distributed "ledger" of the records.

These records are unalterable without altering subsequent records, making data acquired permanent. This is one of the key reasons it was chosen for this project, as our goal is ultimately to build a "permanent record" of sort, of tamper-proof reviews. InterPlanetary File System (IPFS) is a protocol that seems similar to blockchain. It's quintessentially a file system protocol that's similar to BitTorrent, where peers on a network can request pieces of a file from the hundreds to thousand of other peers holding parts of it by referencing a Distributed Hash Table (DHT). The primary advantage of IPFS being that it's done on a global scale. These are two of the key technologies that will be utilized to build this decentralized application. The frontend will utilize React.js to allow user interaction. While using these key technologies, we aim to create a familiar interface for users that allow them to interact with the application just as you would with any web page

II. LITERATURE SURVEY

Review platforms giving your firm input on what your consumers really want, customer reviews may help your organisation better understand overall customer satisfaction. Blockchain is a decentralised data and transaction management system that was initially used in 2008 for the well-known Bitcoin cryptocurrency. The variety of possible uses for blockchain technology and the early stages of this research have sparked interest and publications in the area. Particularly from the standpoint of technological problems and constraints, the embedded potential of such technology to offer security, anonymity, and data integrity presents fascinating study fields. It was forecasted that the worldwide blockchain technology industry would reach 13.96 billion dollars in value by 2022 and expand at a compound annual growth rate of 42.8 percent over that time. The popular Bitcoin cryptocurrency was first used in 2008 as an example of blockchain, a decentralized data and transaction management system. The multitude of potential applications for blockchain technology as well as the preliminary research in the field have aroused curiosity and publications. The inherent potential of such technology to provide security, anonymity, and data integrity provides exciting research domains, particularly from the perspective of technological issues and restrictions. The financial systems that the general public is accustomed to dealing with on their regular days tend to be problematic, error-prone, and often extremely slow. Intermediaries are often needed to mediate the process and resolve conflicts. Of course, such actions generate stress and waste of time and money. In contrast, users find blockchain cheaper, more transparent and more effective. It is no wonder that an increasing number of financial services are using the blockchain system to introduce innovations such as smart bonds

and smart contracts. The former ones are automatically paid to the bond holders once certain pre-programmed terms are met. The latter ones are digital contracts that are self-executing and are maintained when the terms are met.

As mentioned by literary scholar Sundhararajan (2018) the main activities and resources of the blockchain technology are "decentralization" and "distrust." As a distributed accounting technology, a smart contract infrastructure platform and a disruptive computing paradigm, blockchain can effectively generate programmable currency, programmable financing and build a programmable society, which will have a far-reaching impact on the financial and other fields, and will lead to a new round of technological and application change.

This calls for a proposed system based on the novel yet reliable blockchain technology to take the place of a conventional platform based on the traditional client-server architecture, existing within a centralized infrastructure. With the guaranteed security and privacy benefits, there is a clear opportunity for these applications to shift to decentralized and p2p networks and leverage their user base to run such a platform while offering them value in the form of a service they can make use of.

III. System Architecture

The purpose of System Architecture is to depict a conceptual design with the intention of displaying key structure and behavior of system. This application consists of multiple components that work together to simulate a standard Client-Server setup. On the Client side we have the Web3 supported web browser connected to the client's wallet which acts as an Identity Provider, when an entry is made by the client onto the page, the browser contacts the smart contract that executes if all conditions are met. This in turn triggers an entry into the local Ethereum blockchain, and this entry is immediately reflected on the client's page.

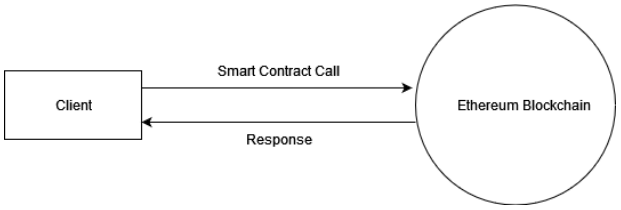

Figure 1: Context Level Dataflow Diagram

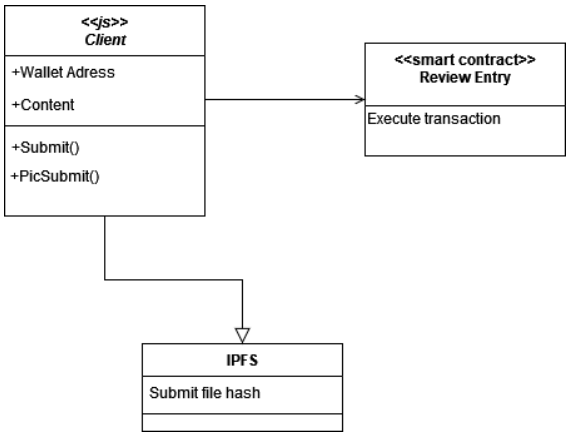

Figure 2: Dataflow Diagram

It's important to mention that the Ethereum blockchain, like most blockchains, uses a consensus mechanism for the purpose of coordinating transactions with other nodes, and keeping the network secure. The way Ethereum implements consensus is by using a proof-of-work (PoW) consensus protocol.

The application routes smart contract calls to be carried out on the client's wallet address, which is then carried out at the user's consent at the given wallet address. This is transaction is then carried out by other miners in the network who race to compute the block to be derived from the processing the transaction. To facilitate this, some minute amount of ETH shall be debited from the user's ETH wallet, in exchange for the proof of work provided by a fellow miner.

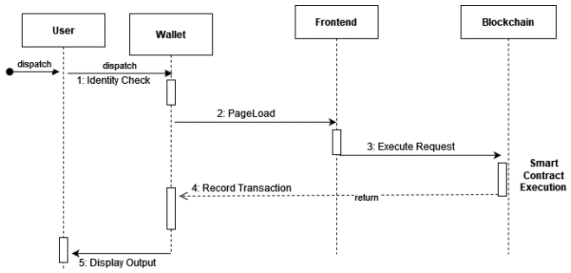

Figure 3: Sequence Diagram

On successful execution of the contract call, the appropriate response is fed back into the application, and is processed and displayed on the JavaScript based frontend.

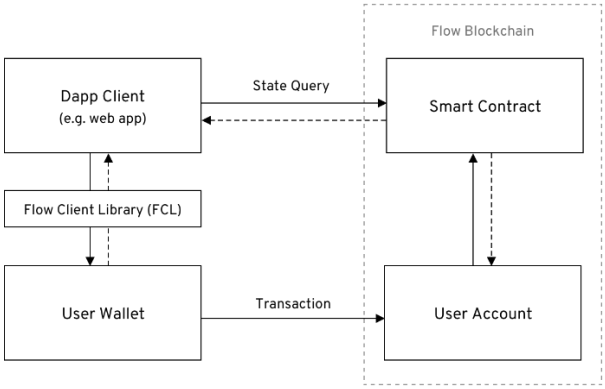

Figure 4: Product Architecture

IV. IMPLEMENTATION

Most of the client side is built to be similar to existing centralized Review platforms today to ensure a shorter adjustment period for the user in getting used to using our product. The user should be able to access CReDReP with ease as long as a popular browser with Web3 support is utilised. Ultimately this approach guarantees ample security and anonymity and can be advantageous to the end user.

The bulk of the application runs in Node.js environment. A self-hosted off mainnet Ethereum node is used to facilitate blockchain transactions executed via smart contracts. This is possible with the Ganache local blockchain application, part of the Truffle Suite framework. The frontend utilizes the popular React.js library for UI components. React is different from other libraries as it doesn't attempt to provide a complete "application framework." It is designed specifically for building user interfaces. Both design and development teams share the same language.

The backend is built using Ethereum smart contracts and the Solidity programming language. Ethereum core contributors invented Solidity with the purpose of designing Smart Contracts, which are basically computer programs made of lines of code that can be executed in the Blockchain. Solidity is a high-level, object-oriented language inspired by JavaScript, C++, Python and has syntax very similar to JavaScript. The client must use a Web3 supported browser, like chrome, paired with the MetaMask extension which acts as an identity provider of sorts.

Our project also uses a decentralized standard called IPFS as said above, which can be used to host content on a decentralized collection of nodes, in a semi-P2P fashion. We shall facilitate this by hosting an IPFS instance using the API of a popular aggregator available online.

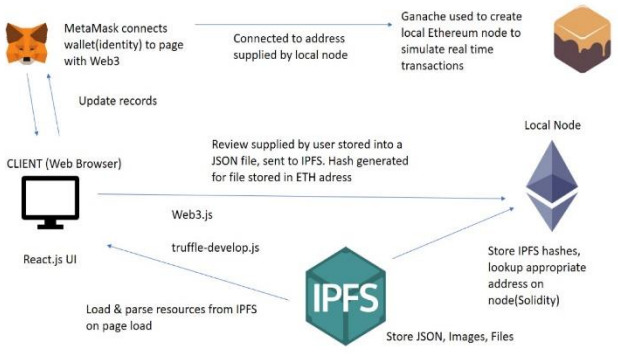

Figure 5: Decentralized Application Implementation

V. CONSTRAINTS

Utilising distributed systems comes with some caveats, we have to make sure to leverage a blockchain with incentivized nodes to ensure stability in functionality of application. Among these several others are as follows,

- Scalability: This problem poses to be a double-edged sword, on one hand the decentralized nature of nodes in a blockchain working in synchrony guarantees the ability accommodate traffic. But in the event the capacity causes congestion, smart contracts will see a large delay to undergo execution.
- Data is Immutable: Blockchains, in our case the Ethereum blockchain, was designed to be trustless. This means data added to the blockchain can't be altered under any circumstance. Hence, workarounds have to be made to circumvent this by referencing earlier data on input of newer data.
- Security limitations: Blockchains despite being more secure than many platforms that exist today, isn't exactly fireproof. There are possibilities of DDoS attacks and the infamous 51% attack that can deter security.
- Blockchains are still relatively new and have some way to go before being good as standardized alternatives. Also, users might not exactly be aware of the requirements needed to be set up to use a decentralize d app and hence must be educated on the same.

With the proposal to build a blockchain based review platform, the most reasonable approach must be taken to ensure wide compatibility. Hence, Ethereum smart contracts will be used to execute code on the backend. The login system used will use wallet addresses to guarantee unique users, with an extra personal information.

VI. CONCLUSION

This project was created with the intention to replace client server based traditional review platforms with a decentralized alternative. An alternative that aimed to be more secure and open by utilizing decentralized protocols and standards, didn't have a single entity as it's owner, and do all this while having a familiar user interface and overall experience for users, making it easier them to migrate from traditional platforms.

With the appropriate tools and the very well documented Ethereum platform, we were eventually able to accomplish this endeavor. There are obviously downsides to building an application of this nature, with one of the primary ones being it comes across an inconvenience to most users not familiar with web3 and implications.

Nevertheless, by building we have been inspired to continue on this path and see what other traditional applications can be bought to operate on the blockchain.

VII. FUTURE SCOPE

The application can be further made useful by implementing safeguards and implementing algorithms to judge reliability of information coming from a certain address using a variety of data points. As the case with blockchain, the larger the active users, the higher the stability and reliability to be expected. Hence, the key to successful decentralization of everyday solutions, is simply adoption.

VIII. REFERENCES

[1] Martens, Daniel; Maalej, Walid (2018). [ACM Press the 1st International Workshop - Gothenburg, Sweden (2018.05.27-2018.05.27)] Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain - WETSEB '18

[2] Salah, K.; Alfalasi, A.; Alfalasi, M. (2019). [IEEE IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) - Paris, France (2019.4.29-2019.5.2)] IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) - A Blockchain-based System for Online Consumer Reviews

[3] Xu, Quanqing; Song, Zhiwen; Mong Goh, Rick Siow; Li, Yongjun (2018). [IEEE 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS) - Singapore, Singapore (2018.12.11-2018.12.13)] 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS) - Building an Ethereum and IPFS-Based Decentralized Social Network System

[4] Harris, Christopher G. (2019). [IEEE 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) - Seoul, Korea (South) (2019.5.14-2019.5.17)] 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) - The Risks and Challenges of Implementing Ethereum Smart Contracts

[5] Gervais, Arthur; Karame, Ghassan O.; Wüst, Karl; Glykantzis, Vasileios; Ritzdorf, Hubert; Capkun, Srdjan (2016). [ACM Press the 2016 ACM SIGSAC Conference - Vienna, Austria (2016.10.24-2016.10.28)] Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16 - On the Security and Performance of Proof of Work Blockchains

[6] MJ , M. (2019). View of blockchain technology applications: A literature review: Brazilian Journal of Operations & Production Management. View of Blockchain technology applications: a literature review | Brazilian Journal of Operations: Production Management. Retrieved July 15, 2022, from https://bjopm.org.br/bjopm/article/view/585/882