Blockchain-based DeFi Crowdfunding Platform

Project Plan

Supervisor: Dr. Chow, Kam Pui
Student: Zhu Wendi (UID 3035638521)
# Table of Contents

1. Background ........................................................................................................................................... 3  
   1.1 Crowdfunding Market Introduction .............................................................................................. 3  
   1.2 Decentralized Finance .................................................................................................................... 3  
   1.3 Motivations ..................................................................................................................................... 4  
2. Objectives .............................................................................................................................................. 4  
   2.1 General Introduction ....................................................................................................................... 4  
   2.2 Feature Details ................................................................................................................................. 4  
      2.2.1 As Fundraisers ......................................................................................................................... 4  
      2.2.2 As Backers ............................................................................................................................... 5  
3. Methodology .......................................................................................................................................... 5  
   3.1 Blockchain and Smart Contract ....................................................................................................... 5  
      3.1.1 Ethereum ................................................................................................................................. 5  
      3.1.2 Ethereum Layer 2 .................................................................................................................... 6  
      3.1.3 Cosmos ................................................................................................................................... 6  
   3.2 Backend .......................................................................................................................................... 6  
   3.3 Frontend ........................................................................................................................................... 6  
4. Project Schedule and Milestones .............................................................................................................. 7  
5. References ............................................................................................................................................... 8
1. Background

1.1 Crowdfunding Market Introduction
Crowdfunding allows people to collect financial resources by getting a large number of people to each give a small amount of money, which can be seen as an open call to provide financial resources. Thanks to the diffusion nature of the Internet, people can easily post their ideas or specific statements on the platform to attract funds from others to support their activities. Crowdfunding mostly takes place on crowdfunding platforms (CFPs) [1]. Depending on the use of the fund and the purpose of the fundraising, crowdfunding activities can be divided into profitable and non-profitable fundraising.

Profitable crowdfunding (reward-based) can be used for some small-scale product development, which allows small companies and individuals to raise funds for their projects more efficiently. At the same time, users who participate in crowdfunding can be considered backers. The backers can be offered some incentives or rewards, such as early bird discount, an opportunity to pre-order the product and have a say in its development, or even own equity in an early or growth-stage company. Compared to bank loans, crowdfunding is more friendly to project sponsors because it does not require asset collateral, has no interest rate, and has a high fault tolerance rate. Additionally, backers have a closer connection to the project because they are also potential customers, which makes the products more in line with the demand. For small start-ups, crowdfunding may also offer more opportunities and flexibility than traditional financing or attracting investors to invest.

Nonprofit crowdfunding (donation-based) is a form of fundraising encouraging the public to invest in nonprofitable organizations (NPOs) or nonprofitable projects, usually for charitable purposes. It can be used for specific programs within the organization or a general donation to the cause. Today there are many third-party CFPs that provide publishing platforms and asset management for crowdfunding projects (such as Kickstarter, Indiegogo, Patreon, Mightycause, Donorbox, etc.). However, the traditional commercial model still has many drawbacks. For example, the platform may take a commission, different platforms have different standards and processes, and the funds could go opaque.

1.2 Decentralized Finance
Decentralized finance (DeFi) is a financial infrastructure based on blockchain. The transaction ledger is distributed on each decentralized node, and the entire blockchain is maintained by all nodes together. DeFi can offer financial instruments without relying on centralized organizations or intermediaries such as brokerages, exchanges, or banks using smart contracts on a blockchain. Each agreement is enforced by code, and legitimate state changes persist on a public blockchain, which can create an immutable and interoperable financial system with unprecedented transparency, equal access rights, and little need for custodians, central clearing houses, or escrow services [2].

DeFi revolves around decentralized applications (DApps), which are typically accessed through open-source software like browser extensions or applications [3]. Furthermore, DApps can be linked to the blockchain to let users operate with complex financial
services. There are numerous Defi projects that have a wide range of uses (for example, token issuance, automated coin exchange, decentralized lending platforms, decentralized derivatives, On-Chain Asset Management, etc.) [2].

1.3 Motivations
The decentralization of blockchain makes the circulation of assets more transparent and allows users around the world to cooperate without a centralized organization. Meanwhile, smart contracts can provide a collaborative environment that users can trust, making numerous decentralized financial projects possible. In addition, the Defi program allows for convenient cross-border projects where worldwide users can transact in the same environment without considering different legal environments. Defi can be seen as a solution for crowdfunding platforms based on the above features. With the constraints of smart contracts, the managing cost of the project will be lower and more transparent, and the flow of funds raised can be better monitored, while users have more direct control over the project, and users from different regions can be involved in the project more freely.

2. Objectives

2.1 General Introduction
This project aims to achieve a Blockchain-based DeFi Crowdfunding Platform, which allows organizations and individuals to raise tokens from users for a variety of purposes, including but not limited to: charity, investment projects, and funding for entrepreneurs and startups. The sole goal of the platform is to support crowdfunding projects and maintain funding pools, which makes the whole ecology of the platform purer. The smart contracts will be templatized so that anyone can easily publish their projects. The platform will encourage users to participate in the maintenance of the blockchain and publish relevant smart contracts. And users can be assigned voting power for each project/event accordingly, depending on how many tokens they hold, which allows them to participate in important decisions (e.g., review crowdfunding projects, decide on the management of the funding pool, approve the exchange of fiat currencies by the parties raising funds). The investor can follow the investee from the beginning to the end of the project, providing further support or limiting their economic activity. In a crowdfunding project, investees can raise funds in the form of crypto tokens by publishing specific fundraising projects. If the project violates the contract or does not meet the investor's (or donor's) expectations, then the remaining funds can be reduced or even returned, and if the investor (or donor) is satisfied with the project's progress, then the investee will receive the next tranche of funds.

2.2 Feature Details

2.2.1 As Fundraisers
1) Fundraisers can customize their own smart contract to publish the crowdfunding project. At the same time a funding pool will be created, and the fundraisers have limited authority over the pool (fundraisers can only divert tokens from the pool if
they meet the conditions in the contract). And fundraisers are advised to make explanation for the type (profitable/nonprofitable) and objectives of the fund.

2) The fundraising process can be divided into several (at least 1) phases. For each phase fundraisers need to clarify:
   a) Time period: Deadline of this phase.
   b) Minimal amount: If the received tokens do not reach a certain amount of limit at the end of this phase, then the tokens at that stage will be returned to senders.
   c) Maximal amount: If the received tokens have already reached the maximal amount during this phase, then the pool will stop receiving tokens for this phase (and may move the extra tokens to the next phase).
   d) Conditions for continuation: The fundraiser can only appropriate tokens from the pool if specific conditions are triggered, such as when the fundraiser have given the promised return or it is affirmed by a vote of investors.

2.2.2 As Backers
1) Users can freely transfer tokens between each other.
2) Users can browse all existing crowdfunding projects. Users can invest in a project by sending tokens to a specific pool of funds and become the backers of that project.
3) During each phase, backers can vote for project development. The voting power is generated by their contribution weight to the pool.

3. Methodology and Design

3.1 Blockchain and Smart Contract
Blockchain forms the base of the platform. The crowdfunding platform (CFP) will be based on the existing blockchain. And smart contracts will be written in Solidity, an OOP style smart contract programming language widely supported by different blockchain platforms. In the subsequent research and development process, I will further compare different blockchain development networks to select the suitable blockchain. The alternatives I am currently considering are listed below.

3.1.1 Ethereum
Ethereum was introduced in 2014 with a new proposition for building decentralized applications compared to the initial blockchain like Bitcoin. There is a single blockchain where people would be able to deploy any kind of program. Ethereum achieved this by using the Ethereum Virtual Machine (EVM), which can be viewed as a single, canonical computer [4]. This virtual machine was able to process smart contracts that any developer could deploy to the Ethereum blockchain in a permissionless way.
However, there are many limitations and drawbacks for constructing a platform directly based on Ethereum. First, decentralized applications built on top of Ethereum are inhibited by a shared rate of 15 transactions per second, and all applications are competing for the limited resources of a single blockchain. Second, the EVM optimizes for the average use case, which means it has relatively low
flexibility for developers. Third, each application is limited in sovereignty because they all share the same underlying environment. Forth, due to the high gas fee, low TPS and a growing number of transactions, this approach is costly and tedious [5]. Furthermore, as Ethereum just transitioned from Proof-of-Work (POW) to Proof-of-Stake (POS) in September 2022 (which is also called the Merge) [6], the entire structure and ecology of the blockchain are facing a huge change, and the applications may face some potential risks.

3.1.2 Ethereum Layer 2
Layer 2 (L2) is a collective term to describe a specific set of Ethereum scaling solutions. A layer 2 is a separate blockchain that extends Ethereum and inherits the security guarantees of Ethereum [7]. Layer 2s blockchain utilizes Ethereum for consensus and data availability and submit transactions to communicate with Ethereum, and ensure similar security. Moreover, by removing the transactions load from layer 1, layer 2 is more scalable. Typically, Ethereum layer 2 can have fewer gas fees and support more transactions per second (TPS). Currently, there are various layer 2s, such as Optimism, Arbitrum, Parastate, and Polygon.

3.1.3 Cosmos
Cosmos is a decentralized network of independent parallel blockchains, each powered by BFT (Byzantine Fault Tolerance) consensus algorithms like Tendermint consensus. Cosmos is highly suited to building application-specific blockchains, or app-chains [8]. Developers can customize blockchains from scratch that can natively interoperate with other blockchains (inter-blockchain communication). Also, developers can decide on the account model (account-based or UTXO), the state machine programming language, as well as a variety of other parameters of the blockchain, which is more flexible than Ethereum [8][9].

3.2 Backend
The backend of the platform is used for interfacing with both the blockchain as well as the applications. It will integrate the data from frontend and create the corresponding smart contracts and deploy them to the blockchain. At the same time, it can collect data on the blockchain and transmit it to the frontend. The backend is planned to be implemented using Django. Django is a high-level Python web framework that encourages rapid development and clean, pragmatic design and provides a lot of functionality out-of-box, like REST API support.

3.3 Frontend
The platform will be performed as a web application. Users can view their account and transfer tokens (considering security and simplicity, transactions and payments can rely on third-party e-wallet plugins). And can create their crowdfunding project by following the instructions. And can also invest in other projects on the blockchain. The frontend of the web application is planned to be implemented using React. React is an open-source JavaScript library for building user interfaces. It provides reusable components and has extensive community support and plugins, which can be used to provide a better user interface.
4. Project Schedule and Milestones

<table>
<thead>
<tr>
<th>Phase</th>
<th>Time</th>
<th>Task</th>
<th>Deliverable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inception</td>
<td>Sep 2022</td>
<td>Background research about the crowdfunding platform. 8h</td>
<td>2 Oct 2022</td>
</tr>
<tr>
<td></td>
<td>Oct 2022</td>
<td>Set up the project web page. 4h</td>
<td>Detailed Project Plan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Project Plan. 8h</td>
<td>Project web page</td>
</tr>
<tr>
<td>Elaboration</td>
<td>Oct 2022</td>
<td>Further research about blockchain development choice. 8h</td>
<td>22 Jan 2023</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Research on existing DeFi project architecture. 4h</td>
<td>Preliminary implementation</td>
</tr>
<tr>
<td></td>
<td>Nov 2022</td>
<td>Blockchain development (basic architecture). 32h</td>
<td>Detailed interim report</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Backend Architecture Design. 16h</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Learn about the React Framework. 16h</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dec 2022</td>
<td>Blockchain development (smart contract and fund pools customization). 40h</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Backend development. 16h</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Jan 2023</td>
<td>Connect backend to the blockchain. 40h</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Interim report. 8h</td>
<td></td>
</tr>
<tr>
<td>First presentation</td>
<td></td>
<td></td>
<td>9-13 Jan 2023</td>
</tr>
<tr>
<td>Construction</td>
<td>Feb 2023</td>
<td>Frontend development. 40h</td>
<td>18 Apr 2023</td>
</tr>
<tr>
<td></td>
<td>Mar 2023</td>
<td>Frontend development and tuning. 16h</td>
<td>Finalized tested implementation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deployment and testing. 16h</td>
<td>Final report</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Implement analytics. 16h</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Apr 2023</td>
<td>Deployment and testing. 16h</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Final report and presentation preparation. 40h</td>
<td></td>
</tr>
<tr>
<td>Final presentation</td>
<td></td>
<td></td>
<td>17-21 Apr 2023</td>
</tr>
<tr>
<td>Project exhibition</td>
<td></td>
<td></td>
<td>3 May 2023</td>
</tr>
</tbody>
</table>
5. References