UNIVERSITY OF THE WEST INDIES
Department of Computing
COMP 6001/6010–Research Methods
Semester I, 2021
Lecturer(s): Daniel Coore, Carl Beckford

Group Project

Due: Wednesday, Nov 30, 2022
(via Group Presentation)

Introduction

In this assignment, you will be critically analysing the prospects of an actual decentralised finance (DeFi) application, given the description of its parameters from its whitepaper. You may choose to take the role of a prospective investor, or a project team member, or perhaps an external interested party (e.g. a potential regulator). If you are familiar with blockchain technology and how decentralised finance applications work, you may skip the background section and proceed to read the details of the specific case study. The actual task for the assignment is given in the last section.

Background

A paper by the pseudonymous author Satoshi Nakamoto, published in 2009, presented the idea of *Bitcoin*(BTC) a decentralised digital currency that did not require a trusted third party, and could be supported in an entirely decentralised way by volunteers operating nodes of a network that would grant the currency its value. Central to the idea was that of the blockchain. A distributed ledger of transactions for the Bitcoin that all participating nodes in the network agree to, and is easy to verify, but takes significant computational effort to extend with new information. This makes the blockchain an effective mechanism for establishing consensus on "truth" without having a trusted third party to arbitrate.

An important development of this idea was that the blockchain could be used to store any type of information, not just currency[1] transactions. In particular, code and the data structures that it uses while running could also be stored on the block chain, provided that the execution model was public knowledge. This led to the idea of using the blockchain to support a *Smart Contract*, which is simply code written in a language specific to the block chain, made public and executed by nodes on the blockchain, so that the results of the execution could be recorded and preserved on the blockchain. The *Ethereum* blockchain (whose native coin is abbreviated ETH) was the first one to support smart contracts.

Liquidity Pools and Automated Market Makers

Two important developments of smart contracts are the related ideas of a *liquidity pool* and an *automated market maker* (AMM). A liquidity pool is a collection of tokens under control of a smart

[1]It is debatable whether cryptocurrency tokens are actually currency in the usual sense of the word; but for this assignment, we shall refer to them as such for simplicity

contract. They can be used to create a pool for lenders to deposit and earn interest from borrowers or as a source of tokens for future investments, or anything else one could imagine. The important feature is that the way the tokens are used is governed by the code of the smart contract.

One important example of a liquidity pool is an automated market maker (AMM). It consists of two (or sometimes more) currency tokens and maintains an invariant that the total value of each type of token is equal to the value of the other(s)[1]. This effectively provides a price conversion between them[2]. The liquidity pool supports adding and removing tokens in the right proportions to the pool, but very importantly, they support the ability to swap between the two tokens. So a user can provide an amount of one of the token pair, and receive, in exchange a fair amount of the other token in the pair.

As an example, say the tokens are called **X$** (we'll attach the '$' sign to remind us that these represent different currencies) and **Y$** and let x and y represent their respective quantities. Initially there are x_0 and y_0 of each token respectively, and we'll represent the state of the pool as (x_0, y_0). This means that x_0 **X$** tokens are worth the same as y_0 **Y$** tokens. So, this also means that we can put a price on **Y$** in terms of **X$**; specifically, it costs $\frac{x_0}{y_0}$ **X$** tokens to purchase 1 **Y$** coin. (If upon initialization, **X$** and **Y$** were considered equal value, then we would set $x_0 = y_0$ in the pool.) Note that if we wanted the price of **X$** in terms of **Y$** it would be the reciprocal of the price of **Y$** in terms of **X$**. Note that this price is actually a nominal price, the effective price will (usually) depend on the number of tokens that are actually exchanged relative to the number in the pool. The difference between the nominal price and the effective price is called *slippage*.

When a swap occurs, the number of tokens returned is determined by the formula built into the smart contract. The simplest formula (used by a DEX called UniSwap™) ensures that $xy = k$ for some constant k (this will be the formula that we will assume is true for whatever AMM is used for this assignment). Note that this means that at all times, the smart contract will try to ensure that the relative numbers of tokens respect this constraint. The new ratio of tokens determines the new (nominal) prices.

For example, suppose that the initial quantities of **X$** and **Y$** in the pool are (x_0, y_0) respectively, then it means that $k = x_0 y_0$, and the nominal price of **Y$** is x_0/y_0 **X$** tokens. Now, if a user supplies s **X$** tokens and receives r **Y$** coins in exchange, then the effective price would be s/r. Note that after the swap, the numbers of tokens would be $(x_1, y_1) = (x_0 + s, y_0 - r)$ and the invariant that $xy = k$ would mean that $(x_0 + s)(y_0 - r) = k$, so we can readily calculate r by transposing:

$$r = y_0 - \frac{k}{x_0 + s}$$

The new nominal price would be $\frac{x_0+s}{y_0-r}$. Although it might be a little confusing to try to follow these differences in price, it should be easy enough to see that since $x_1 > x_0$ and $y_1 < y_0$ then the new nominal price of x_1/y_1 is clearly larger than the previous nominal price. This makes sense since the previous swap gave up some **X$** in exchange for **Y$** representing a demand for **Y$**, and therefore the increase in its price is intuitive.

It is also clear that the change in price depends on both the amount of **Y$** purchased and the amount in the pool at the time of the purchase.

[2]The exact formulation of the notion of equivalence, and the mechanism for computing price is up to the implementation of the AMM in its smart contract

The Case

The name of the project is *Uniqo*. Details of it can be found in their whitepaper[2]. The creators claim that their token (UNIQO) is a unique product that offers its participants a reward of 1% per day on their deposits. It does this by *rebasing*, which just means that the smart contract implementing the token will report a gradually larger amount of the token when it is queried for the amount associated with a given wallet address. From a user's perspective, if a wallet holds 100 UNIQO tokens at a time t, then at time $t + 24$hrs that same wallet will hold 101 UNIQO tokens. The UNIQO tokens receive their value by being supplied from an AMM that pairs UNIQO tokens with BUSD tokens. The BUSD token is an example of a *stable coin*, which is a crypto token that is pegged to a fiat currency. In this case, 1 BUSD is worth 1 US dollar (usually to within 3 decimal places).

The project founders claim that the obvious problem of inflation of the token is solved through a combination of features. The first of them is called "Rebound" (their innovation), which will rebase the token if the inflation measured in the token, relative to a defined period, is ever above a threshold. In this case, the rebasing causes the number of UNIQO tokens to **decrease**. (The specific criteria for when a rebound is triggered are described in the whitepaper.) Note that the rebound feature affects the token count everywhere that it is held, not only in the liquidity pool that is controlling its price.

Another important inflation control mechanism is that they limit the amount that a wallet may sell within a 24 hour period. They refer to this as the *Daily Take Profit* (DTP). The DTP ratio is the ratio of the wallet that a holder may sell within a day. It ranges between 0.1% and 1% and depends on the fraction of the liquidity pool that is within the wallet (larger fractions are limited to smaller DTP ratios).

There are also other mechanisms, such as a tax on purchases and sales. Of the tax, a portion of the UNIQO tokens are *burned*. A token is said to be "burned" when it is transferred to an address from which it can never be retrieved. Such an address is usually defined by the smart contract supporting the token. The idea of burning a token is that it is removed from the liquidity pool, thereby increasing its price (and fighting inflation in the number of tokens).

At its launch, it was given an initial investment of US$1 million (in BUSD) to back its initial supply of 1 billion UNIQO tokens. (In other words, the AMM was seeded with 1 million BUSD and 1 billion UNIQO tokens upon launch of the project). It therefore had an initial price at launch of 0.001 BUSD per UNIQO token. Within 10 minutes, its price jumped to 0.0034 BUSD and after approximately 5 days, its price has moved to 0.0045 BUSD.

Notably, the whitepaper does not describe any specific plan for generating revenue other than from purchases. That is, the only mechanism for increasing the BUSD stable coin in the UNIQO liquidity pool is direct purchases of the UNIQO token. Although the project founders claim an intention to eventually invest the treausury in order to increase the store of BUSD, it appears they believe that new purchases alone can sustain the value of the UNIQO token over the long-term.

This leads to the question of whether the UNIQO token could be expected to retain value over the long-term. Given that it grows at a daily rate of 1%, are the project founders right to assume that new purchases are sufficient to support the value of the token, given all of the deflationary mechanisms that they have implemented? If you were asked by a friend or family member whether this is a viable project to invest in, what (quantified) advice could you provide?

Your Task

Given the description of the DeFi project, you are asked to analyse its viability for the long-term. Your analysis may be purely analytic where you might use continuous variables to represent discrete process changes, or discrete (where you use mathematical tools to analyse the discrete process) or computational (where you use code to simulate a model under your assumptions), or a combination of these. The objective of this exercise is to see how you model a problem, and subject it to analysis in order to gain some useful insight.

Specifically, you should present on the following:

1. What do you believe is a reasonable model for estimating the new subscribers? Your model should represent an expectation of the number of new subscribers over time. It should be quantified.
2. Based on the description of the project and your model of new subscribers, analyse the medium to long-term behaviour of the project. (In this context, medium to long term means (say) 6 months to several years.) Quantify your analysis:
   - If you believe that the price will increase and then decrease (or anything else), try to put time bounds on those changes
   - If you believe that the long-term behaviour depends on other factors not mentioned here, indicate what they are, and try to quantify their effects.
3. Based on your medium to long-term analysis, what recommendations would you make? These could be to:
   - potential investors (e.g. limits of investment, expected time to break even, estimation of risk, etc)
   - project founders (e.g. suggestions for revenue sources other than new subscriptions, minimum revenue required for sustainability, modifications to promised returns)
   - regulators (e.g. requirements to put on new projects, advice to investors, etc)

   You choose the role you would like to play here, but your recommendations should be based on the analysis previously presented and should be reasonably quantified. (Simply saying "Do this" or "Do not do that" is not good enough, unless you have proven an outcome that occurs under either **all** or **no** circumstances). You may make recommendations to more than one category of (potential) participant here.

In performing your analysis, you may make simplifying assumptions, so long as they are reasonable, or if they permit you to make useful categorical statements under certain conditions. In the end, the assessment of your presentations will be based on how reasonable your assumptions are, how well you have defended the elements of your model that you have captured, the degree to which you acknowledge or recognise the limitations of your model, and the soundness of your reasoning in your analysis and in drawing your conclusions.

Glossary

AMM	Automated Market Maker: a liquidity pool of a pair of tokens that establishes an exchange rate between the two.
(token) Burn	The transfer of a token to an irretrievable address, effectively removing it from circulation.
BUSD	An example of a stable coin: a cryptocurrency that is pegged to some fiat currency. In this case BUSD is pegged to the US dollar.
DEX	Decentralised exchange: a website where one can exchange one cryptocurrency for another; usually autonomously controlled.
Liquidity Pool	A store of tokens under control of a smart contract
Slippage	The term for the difference between the amount of an asset expected from a purchase and the amount actually received, usually expressed as a percentage.
Smart Contract	A program that is executed by the nodes that maintain a blockchain, and whose persistent state is maintained on the blockchain.

References

[1] FXCM Research Team. "Automated Market Makers: A Complete Guide." March 2022. `https://www.fxcm.com/markets/insights/automated-market-makers`

[2] The Uniqo develoment team. "Uniqo Documentation". `https://docs.uniqo.finance/`