Tutum DAO
&
Tutum stablecoin protocol

whitepaper

Konrad Wierzbik
konrad.wierzbik@epfl.ch

Łukasz Łakomy
lukasz.jan.lakomy@gmail.com

Abstract

In this article, we introduce the Tutum DAO and its stablecoin protocol. We start with a short introduction to stablecoins and their stabilization mechanisms, referring to already existing protocols. In detail, we discuss the stabilization mechanism used in our protocol. Then we present the idea of Tutum DAO itself and we introduce the Tutum share token with its tokenomics. Finally, we discuss the general structure of contracts that build an infrastructure of Tutum DAO and Tutum stablecoin.

1 Introduction

The need for stable assets in the crypto space is obvious. Users must have the possibility to possess stable assets on a blockchain. Thus, it is not a surprise that in the ten biggest by market cap cryptocurrencies, we find three[1] stablecoins pegged to USD: USDT, USDC, and BUSD. These stablecoins are however centralized and one needs to trust that their emitters behave correctly. Historically, there were many doubts about USDT which led to small price depegs. Even if these stablecoins get regularized by governments one won't be still 100% sure about them. As we know, the law in real life is not a machine code and can be stretched or omitted. In the context of milliards of dollars, one can be sure that this will happen. To answer these problems decentralized stablecoins have evolved in the market.

People often distinguish decentralized stablecoins into two groups: Collateral Debt Position (CDB) and Algorithmic stablecoins. In our opinion, this distinction is misleading as all decentralized stablecoins must have some algorithm that keeps their price pegged. Thus we follow the convention of dividing stablecoins into: fully collateralized, partly collateralized, and uncollateralized. The uncollateralized stablecoins have proven to be very unstable and susceptible to manipulation [2]. The same holds for partly collateralized stablecoins[3], however, as they are only partly uncollateralized the risks are much lower[4]. We believe that only the first two can be taken into account. The Tutum DAO stablecoin protocol will be stared up as fully collateralized with the possibility for future change into partly collateralized. In what follows, for simplicity, we assume that stablecoins are pegged to 1USD.

2 CBD stablecoin

CBD stablecoins are the most secure decentralized stablecoins (SC). They fulfill at least three needs of the market.

- Possession of decentralized stable asset;
- Leveraging collateral exposition;
- Exiting from cryptocurrencies to stable assets during bear market.

Notice that second and third points are somehow opposite. What we mean is that in the situation when collateral price is predicted to increase, people are rather going to take more loans, sell their stable assets and increase exposure to collateral. This creates downward SC price force. Opposite to situation when collateral price is going to fall, people will exit risky assets to stable assets and borrowers will be paying back their loans. This creates upward SC price force. These forces must be reacted with protocol stabilization mechanisms which creates counter price force. Before we discuss stabilization mechanisms let us introduce in more detail what CBD stablecoin is to unfamiliar reader.

2.1 Bank loan analogy for an unfamiliar reader

For those unfamiliar with CBD stablecoins, we describe its mechanism with a bank analogy. We start with a simple example which we modify step by step to get to CBD stablecoin.

Imagine a Bank that gives a loan in USD that is secured in gold. It means that if a person wants to take a loan in USD he/she must first deposit some value in gold. Of course, the credit value (CV) must not exceed the value of deposited gold (GV). Moreover, the value of credit must be lower than the value of deposited gold so the Bank is protected in case the gold to USD price falls. Thus the Minimum Collateral Coefficient (MCC) is introduced and the value of credit times the MCC must be lower than value of deposited gold:

$$CV \cdot MCC <= GV. \tag{1}$$

We can define Maximal Credit Value (MCV) as deposit value divided by Minimum Collateral Coefficient:

$$MCV = \frac{GV}{MCC}. \tag{2}$$

In case the gold value falls and the credit value exceeds maximal credit value (so-called under collateralization) the deposited gold is sold by the Bank in exchange for USD in order to protect itself from losses. This process is called liquidation.

Imagine now, that Bank decides to give credit not in USD but in their own currency called Gold-Backed Dollar GD. Giving credit Bank assumes that 1GD has a value of 1USD. The CV, GV, and MCV work the same. This time when liquidation takes place the gold is sold for GD and not USD.

Let's now replace the Bank with an unknown to us person, to decrease our institutional trust in this GD currency. Moreover, just for this example let's assume MCC to be equal to 120%. It means that to take credit of 1000GD that is worth in Banks opinion 1000USD we need to deposit at least 1200USD in gold. It is smart to deposit more gold

[1] Source: coingecko.com at 22 May 2022
[2] For example UST
[3] Example: Iron Finance
[4] A successful example is FRAX

to protect own self from liquidation in case of gold price changes. This is exactly what, let's say, Alice does. Precautionary she deposits 2000USD worth of gold and takes only 1000GD loan. She comes to Bob who wants to sell his old car for 1000USD with a ten 100GD bills. She explains to Bob how she got these ten bills after she gave some person 2000USD worth of gold. Bob surely will ask her if she has lost her mind. Who would give a stranger 2000USD in gold in exchange for nothing worth 10 bills...

Fortunately, in our case, the unknown person is not a person but a program running on some decentralized virtual machine and gold is replaced by cryptocurrency representing gold ownership or any other cryptocurrency. This time when Alice comes to Bob saying that she wants to buy Bob's car in exchange for a transfer of 1000GD on a given blockchain Bob became interested. Luckily for him, he can understand program code in detail. He verifies that the code has no bugs and that the value can not be stolen. He starts to believe that GD has some value backed by crypto gold that Alice took a loan against indeed. However, in Bob's opinion, 1GD is not worth 1USD but 0.9USD despite protocol (Bank) opinion. Alice agrees and she pays Bob 1000GD plus an extra 100USD. After a few months, Alice comes back to Bob and wants to buy back GD he still has. She says that the gold market is crushing and her deposit is at risk of liquidation, as its value is just above MCV. She wants to pay back her debt as soon as possible to secure the 20% of her extra deposit. Bob agrees to trade with her but this time, taking into account market situation, he asks 1.10USD per 1GD. Alice has no other option, as she doesn't want to lose 20% of extra deposit. She agrees.

To make GD to USD price pegged to 1USD per 1GD, the program must have stabilization mechanisms that will incentive the market to keep the price stable and pegged. As the price is all about supply and demand, the program must influence these to counteract market forces.

2.2 Stabilization mechanisms

Here we describe stabilization mechanisms that are used in the Tutum stablecoin protocol. Our priority is to keep the price close to 1USD and protect the borrowers from a situation in which during liquidation risk periods they must buy back stablecoin for a much higher price than 1USD. We point those mechanisms in order from the least controversial to the most.

2.2.1 Debt interest rates

The easiest, well known, mechanism to influence the supply and demand of stablecoin is by setting interest rates on debt.[5] When debt interest rates are increased borrowers are motivated to pay back their loans. To do so, they must buy back stablecoin from market and increase its price. On the contrary, if the loan interest rates are lowered, the more people should take it and the more supply of stablecoin should drag price down. Notice that as interest rates has no upper boundary and it is bounded from below by 0%. Thus this mechanism is good for keeping price pegged to 1USD from below but not from above. There is possibility of introducing negative interest rates on loan. It is when debt is decreasing with time. However, this leads to existence of stablecoins that are not backed by debt. Tutum DAO stablecoin protocol use negative interest rates combined with other mechanism 2.2.3 to prevent not backed stablecoins.

2.2.2 Variable Minimum Collateral Coefficient

In the event of a collateral market fall, there is a high liquidation risk. To counter it and protect borrowers the MCC can be temporally decreased. It reduces liquidation risks and makes it easier to take a new loan to increase stablecoin supply.

2.2.3 Interest rates for stablecoin

Introducing interest rates for stablecoin holders has opposite action than debt interest rates. Constantly increasing or decreasing holder balances by a given interest rates creates upward and downward force. Notice that increasing holder balances leads to existence of stablecoins that are not backed by debt. Thus increasing holder balances must be matched with increasing debts and decreasing holder balances must be matched with decreasing debt.

2.2.4 Transfer tax

This is a mechanism that should make price less prone to short spikes - to protect borrowers. In case when stablecoin price is trading significantly above 1USD the transfer tax is enabled. The fact of the tax being applied to a transfer depends on its receiver. If he has a debt position and not enough stablecoins to pay it back or is included in the tax-free list then the tax is considered as not applicable. By the definition, all swap contracts[6] are included in the tax-free list. Thus users selling stablecoin to swap contracts are never taxed and the users who buy stablecoins are taxed unless they have uncovered debt. The goal of this tax is to decrease buying pressure by adding additional transaction costs and in result to stop price from rallying even higher. For example, if the tax application is being triggered by the price of 1.01$ then depending on the current price (CP) the final tax percentage (TP) is

[5] Similarly in case of standard fiat currencies one says "money is cheap now" to say that interest rates on credit are low.
[6] Like Uniswap on ETH

calculated as follows:

$$\begin{cases} TP = \frac{CP-1.01}{CP} & for \quad CP > 1.01, \\ TP = 0 & otherwise \end{cases} \tag{3}$$

This mechanism comes from following reasoning. During market crash the demand on stablecoins is increasing drastically. Thus price of stablecoin can increase. We believe that borrowers, people who bring stablecoin to the market and provide market with stable asset during crisis, should not be hit twice. Once by the fact that collateral they own is losing value and secondly by the fact that they must pay more than 1USD for stablecoin to payback their loans. We believe that the second cost should be the burden on the market.

2.2.5 We will NOT use Anchor mechanism

The most controversial in our opinion is the anchor mechanism. It means allowing to mint stablecoin by depositing other stablecoin. In this way, the price of the former stablecoin is anchored to the latter stablecoin. For example, Maker DAO allows for minting one DAI for a 1.01GUSD[7]. In this way, the DAI price has a wall at 1.01GUSD.

We think that this mechanism is a negation of decentralized stablecoin. It moves responsibility for stability to different authorities and makes one stablecoin quality depend on another. First of all, in this way DAI is somehow dependent on centralized authority which emits GUSD. Second of all, this does not solve the USD peg problem. Of course, DAI will not exceed 1.01GUSD price, however, during the market crash, we observed stablecoins to depeg a little from USD. Tutum wants his stablecoin to be completely decentralized and pegged to USD not USDT, USDC, nor GUSD.

2.3 Stability measure parameter

We describe our stability measure mechanism on the example of pegged to 1USD Tutum stable Coin USDA and its collateral AZERO.

All mentioned stabilization mechanisms, except transfer tax, are controlled by the stability measure parameter. A stability measure parameter is an integer number with a base value of 0. Once per a given time the measurement takes place. It takes AZERO/USD and AZERO/USDA prices from oracle and calculates it ratio. This results in USDA/USD price. If its outcome is above the upper threshold, let's say 1.005USD (for the sake of this example), the stability measure parameter is increased by 1. If price is below the lower threshold, let's say 0.995USD, it is lowered by 1. When the price is in the threshold range it changes by 1 in the direction of 0. Based on the stability measure parameter the stabilization mechanisms are adjusted.

Let's give an example in form of a table 1. Having one vault with AZERO as collateral, base MCC = 200% and base interest rates 2.5%. It shows how MMC, debt interest rates, and stablecoin interest rates depend on stability measure parameter.

Table 1: Stability measure parameter to stability mechanism parameters table.

Stability measure parameter	**MMC**	**Debt interest rates**	**Stablecoin interest rates**
125..	175%	0% -0.2% per step	-10% -0.2% per step
75..125	175%	0%	0% → -10%
26..75	200% → 175%	0%	0%
1..25	200%	2.5% → 0%	0%
0	200%	2.5%	0%
-75..0	200%	2.5% → 10%	0%
..-75	200%	10% +0.2% pet step	0% + 0.2% per step

3 Tutum DAO

3.1 Tutum Shares

Tutum Shares (TTS) is governance token that also gives right to part of protocol income. It has unlimited supply, however the more TTS were minted the harder is it to mint new one. To mint TTS one have to generate income for the protocol by taking debt and paying interest rates or buy paying stablecoin interest rates. The income is generated in USDA which is then exchanged for other cryptocurrencies that are stored in treasury. The profit stored in treasury can be redeemed by burning TTS.

[7]Centralized stablecoin backed by USD emitted by Gemini exchange

3.1.1 Tokenomics

Initial supply of TTS is 10 milions.

- 1 milion early investors, public presale TBA
- 1 milion ICO
- 2 milions goes directly to early developers
- 2 milions is locked and linarly vested to the early developers through one year period
- 4 milion used as incentives to use the protocol, marketing, partnership. (The voice of TTS holders will be seriously taken into account)

All other TTS are minted by vault and stablecoin contract as they generate profit for protocol. For each 1USDA of generated profit, the amount user can mint depends on the Total Minted Amount (TMA) in the following way:

$$\frac{1}{2 \cdot \frac{TMA}{10000000}}$$

In the plots below we present some tokenomics properties.

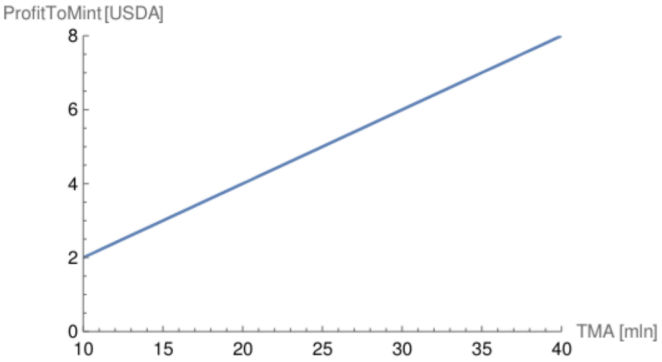

Figure 1: Amount of profit that must be generated by the user to let him mint one TST depending on Total Mintet Amount.

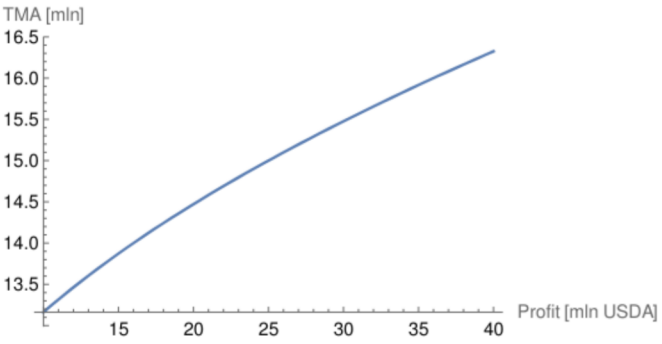

Figure 2: Total Minted Amount as a function of Total generated profit in USDA.

[8]If they accept them.

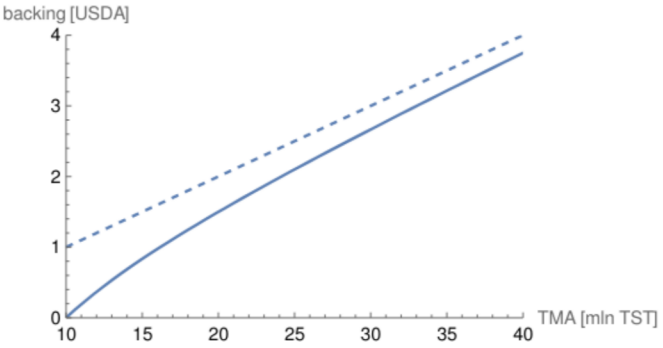

Figure 3: Predicted backing of each TST in generated income in USDA as a function of Total Minted Amount

3.1.2 Presale and ICO

We are going to run a presale in June. The presale amount is 1 million TTS and it is open for everyone. To take part in it one has to transfer a multiplication of 100 AZERO to a given address (not announced yet). After the presale period, the TTS will be distributed proportionally to the supplied amount of AZERO.

The ICO will take place once the functionality of a smart contract is available on the Aleph Zero blockchain. People will be able to buy TTS by interacting with ICO smart contract (more details in future).

The funds will be used for current development expenses (including 1000$ salary per month for full-time developers), running a validator node on Aleph Zero Blockchain, and supply of initial liquidity into the protocol.

From all presale participants, the one who buys the most of TTS will become one of seven multi-signature admins in the early stages of protocol. Moreover, all presale participants will choose another one of seven multi-signature admins.

3.2 The DAO way

The ultimate goal is to build a DAO similar to Maker DAO with TTS as a governance token. DAO will control the stablecoin protocol. This, however, is going to take place only a few months after launch.

In the beginning, the protocol and all the funds will be controlled by a multi-signature contract. We plan to have 7 administrators and at least 4 of them must agree to perform any operation. These 7 administrators positions will be distributed in the following way: 3 positions to early developers, 1 to an investor who buys the highest amount of TTS in presale, 1 to person chosen by pre-sale participants (based on bought TTS amount), and 2 to Aleph Zero foundation[8].

3.3 More on protocol profits

Tutum stablecoin protocol will generate profit. Most of it will be transferred to the treasury and will be backing TTS to increase its value. However some part of the income, with the agreement of DAO, could be spent on current DAO expenses.

Profit is generated in USDA and it is first stored in the Shares Profit Controller Contract. Before it is transferred to treasury USDA should be exchanged for another crypto asset. In the beginning, it will be AZERO, and later this can be changed in the governance process.

4 Contracts overview

For more details navigate to github repo : TODO link.

4.1 Stability Measure Parameters

Two contracts take part in supplying stability measurement parameter to the system:

Oracle Contract - Feeds price of AZERO/USD and AZERO/USDA.

Measurer Contract - Stores stability measure parameter and adjusts it based on oracle feeds.

4.2 Shares Contract

A PSP22 token with modified mint method as described in subsection 3.1.1. Access Control component to give MINTER role to the profit generators (VAULT, USDA) and BURNER role to treasury.

4.3 stablecoin

USDA stablecoin - PSP22 token with interest rates and tax parameters as described in 2.2.3 and 2.2.4. It is a profit generator and thus can mint Tutum shares. Access Control component to give MINTER role to Vault and Shares Profit Controller and BURNER role to Vault. Moreover, this contract stores total debt taken in USDA across all vaults. This is important in calculating transfer tax.

Vault - Stores deposits and mints USDA as a borrowed token. The most important interface functions are: deposit and withdraw collateral, borrow and pay back the loan, and buy risky vault (liquidation).

4.4 Controllers

Controller contracts allow anyone to update vault and USDA stabilization parameters to agree with the current stability measure parameter, as described in table 1.

Vault Controller - Based on stability measure parameter sets appropriate vault stabilization parameters

Stablecoin Controller - Based on stability measure parameter sets appropriate stablecoin parameters

Shares Profit Controller - Collects income from Vaults and USDA, distributes it to treasury and owner. Controls shares minting

5 Disclaimer

The Tutum DAO smart contracts are still in development. Therefore even though the general approach will not be changed, some parts of the specification may differ in the released version.

6 Comment

We have already planned to release additional functionalities/protocols governed by Tutum Dao. For now, we are not going to share them publicly as in our opinion they are quite innovative. However, we will share them with the biggest investors.