

# CS480001 / SEC532 - Blockchain: Security and Applications Homework 3

For the second homework, you have implemented an **exchange contract** to handle token registration and transfer functionalities. For this homework, we will continue to build upon the exchange contract and decentralize the governing process of the exchange.

As you all know, one of the biggest goals of the blockchain ecosystem is to level the power balance in the community. Our previous homework that allowed any user to register a token to our exchange contract respected this philosophy, however ignored to consider the registrar's credibility and the community's input in the decision process.

For such purposes, in this homework, you will implement a governance contract, where you will democratize the token registration process (partially 😊). The governance contract that you are going to implement will also abide by the ERC20 token standards. Unlike the previous tokens that you have created in the second homework (which were ambiguous and had no specific usage), the governance token will be used to vote for token registration proposals. This means, before adding any token to the exchange, the proposer must open a poll in the governance contract. Then the proposal is voted by the token holders of the governance contract (weighted). If the proposal constitutes a quorum, and there are more for votes than against, the proposed token is added to the exchange; if not the proposal is canceled. Technical details of the implementation are given below:

## Technical Details:


1. Only the governance contract is allowed to add tokens to the exchange contract.
2. A user(address) can propose to add a token to the exchange contract by creating a proposal in the governance contract if and only if the user has more than <threshold> amount of governance tokens. (threshold is arbitrary in the scope of this homework)
3. The voting process is weighted, meaning the amount of governance token that the user address has is linearly proportional to the number of votes that the user will cast.
4. A user can delegate their rights to vote to any other user.
5. Anyone can cancel the proposal if the proposer does not maintain its token balance above the threshold during voting.
6. For a proposal to pass, the quorum must reach 10% of the total amount of governance tokens, and the proposal must have more for votes than against.

- 7. After a proposal is successfully created in the governance contract, the voting period starts. The governance contract determines the voting period.
- 8. No votes that are cast out side of the voting period are not valid.
- 9. At the end of the voting period, anyone can cancel the proposal if it failed, and execute the proposal if it passed. In the scope of this homework passed proposals will register a token to the exchange contract.

If you want to read more on the idea of tokens, practical use cases of tokens, and technical details, please read:


ethereumbook/ethereumbook


The word "token" derives from the Old English "tācen," meaning a sign or symbol. It is commonly used to refer to privately issued special-purpose coin-like items of insignificant intrinsic


 <https://github.com/ethereumbook/ethereumbook/blob/devel/10tokens.asciidoc>


ethereumbook/  
ethereumbook


Mastering Ethereum, by Andreas M. Antonopoulos, Gavin Wood

 229  
Contributors

 22  
Issues

 9k  
Stars


 2k  
Forks



For more information on governance and how it is implemented in a real-life exchange, please check out the following links:

Uniswap

This document is a living document which represents the current process guidelines for developing and advancing Uniswap Governance Proposals. Several governance venues


 <https://uniswap.org/docs/v2/governance/process/>

Process

Uniswap | @Uniswap

Uniswap

Uniswap protocol is goverened and upgraded by UNI token holders, using three distinct components; the UNI token, governance module, and Timelock. Together, these contracts

 <https://uniswap.org/docs/v2/governance/governance-reference/>

Governance Reference

Uniswap | @Uniswap

**Deliverables:**

- 1. exchange.sol, governance.sol, and all the token contracts that you have created to test your implementation.
- 2. A one page report (**pdf**) explaining the fundamentals behind the governance process, and what do you need to improve further to establish a full-fledged governance pipeline.

**Submission:**

- Please compress all the .sol files and your report under <suid>-hw3.zip.

**Note:**

We provide token.sol and exchange.sol contracts for the ones that have an incorrect or missing implementation for the second homework.