TeleportDAO Whitepaper

Niusha Moshrefi Mahyar Daneshpajooh

September, 2021

Contents

1 Introduction

In 2008, Satoshi Nakamoto introduced Bitcoin to the world. Bitcoin has several advantages over traditional banking systems:

- **Decentralization**: In Bitcoin, the canonical chain is made when consensus is reached among miners via mining. No one has the power to "rewind" the canonical chain.
- **Anti-censorship**: No one can prevent a user from sending transactions to other users
- **More Resilient System**: Bitcoin consists of a distributed set of mining nodes that can join or leave the network without causing any disruption to the system. The system is made decentralized and permissionless, and there is no single point of failure.
- **Anonymity**: Users can send transactions in the network without revealing their real identity.

Although Bitcoin has the above unique properties, its application is limited to value transfer. Ethereum generalizes Bitcoin's idea of reaching consensus on balances of users to reaching consensus on the state of a code. Programmers can build any application and run it on the blockchain where miners reach consensus over the state of a running code. In the other words, Ethereum is a platform for decentralized applications (DApps). One of the applications that have attracted a lot of attention in recent years is decentralized exchange (DEX).

1.1 DEX

In traditional centralized exchanges (CEX), users deposit their assets to their CEX account, which is in full control of the CEX, and trade it on the exchange's database. However, using DEX, users exchange their assets directly on the blockchain. DEX has these advantages over CEX:

- **Anti-censorship**: A CEX can ban some users' trading activities or prevent them from depositing/withdrawing their assets. Since DEX is running on blockchain, users can make sure that no one can censor their trading activities.
- **Transparency**: CEX has the power of adding/removing trading pairs. In most cases, these processes are not transparent to the users. DEX's policy for adding/removing pairs is hard-coded in its protocol and the code is verifiable on the blockchain so that everyone can see a transparent token listing/delisting process.
- **Higher Security**: In CEX, users send their assets to the CEX's custodial address. If attackers gain access to the CEX's private key, they can access all users' assets that are in the custody of the CEX. In DEX, users have full control of their assets and there is no need for them to transfer their assets to a third party.

The biggest challenge of using DEX is its cost. Due to the scalability issues of the existing blockchains, the cost of recording data and executing programs on blockchains is high. In an order-book exchange, users submit buy order and sell order, then, the exchange matches these orders. A naive order-book implementation on a blockchain is not a cost-efficient solution. Automated Market Maker (AMM) is a solution that tackles the cost problem. An AMM DEX has a lower cost in comparison to an order-book-based DEX.

1.2 Interoperability

Interoperability solutions try to connect different blockchains. Using these solutions users can transfer assets and data across different blockchains. The need for interoperability comes from the fragmentation of the blockchain ecosystem:

1. Different blockchains differ in their main characteristics such as security, degree of decentralization, scalability, and privacy. There are tradeoffs between these characteristics, which means that no blockchain has all of these properties simultaneously.

2. Not all industries need the same level of security, privacy, scalability, and degree of decentralization. So, it is reasonable for each industry to have its unique blockchain with customized features. However, these blockchains may want to interact with other blockchains.

The following are the main categories of interoperability solutions:

- **HTLC**: Hash-Time-Lock-Contract (HTLC) is a solution for two users who want to exchange their assets on two different blockchains. One of the users generates a puzzle, shares it with the other user, and then both of them create HTLCs using this puzzle. When the first user reveals the puzzle's solution, both of them can claim their exchanged assets.

- **Custodians**: Custodians are a group of users who are in charge of verifying the correctness of transferred assets and data between chains.

- **Relay**: Relay is a smart-contract-based solution for the interoperability problem. Parties called relayers submit data from the source chain to the target chain, then, the relay contract checks the correctness of the submitted data.

Now, a question arises: can we leverage interoperability solutions to create a Cross-Chain Decentralized EXchange (CCDEX)? The answer is yes! TeleportDAO has done it. Before introducing TeleportDAO, let's see why CCDEX is important and what the challenges of implementing a CCDEX are.

1.3 Why Is CCDEX Important?

Let's explain the importance of a CCDEX through some examples. Suppose that Alice has tokenA on the source chain and she wants to exchange it for tokenB. Now, consider the following scenarios:

- Due to the congestion of the source network, the transaction fees are high. However, the target chain is not congested and transaction fees are low there.

- A DEX on some other chain offers a better price for the trading pair of A-B in comparison to the source chain's DEX.

- There exists no DEX on the source chain (source chain is a non-programmable blockchain such as Bitcoin, Dash, etc.)

- None of the DEXs of the source chain has the trading pair A-B, however, a DEX on some other chain has this trading pair.

- Alice wants to pay Bob for her purchase. Bob only accepts tokenB on some other chain as the payment.
- Alice wants to use some application that lives on another chain and accepts tokenB.

In all the above cases, a cross-chain exchange is needed.

1.4 What Are the Current Solutions for Cross-chain Exchange?

- **CEX-DEX**: One possible solution for a cross-chain exchange is using a CEX as an intermediary. In this case, a user sends tokenA to the CEX, exchanges it for tokenC, withdraws tokenC on the target chain, then, he exchanges tokenC for tokenB using a DEX on the target chain. This solution has three obvious disadvantages:
  1. A centralized entity (CEX) is involved in the process
  2. It creates a bad user experience: the user needs to perform four different actions (send, exchange, withdraw, exchange)
  3. It causes a lot of delays: depositing in and withdrawing out of an exchange is a slow process.
- **HTLC**: As we discussed before, HTLCs are used for exchanging assets on different chains. Before creating HTLCs on blockchains, users need to agree on the exchange rate. Using HTLC for a cross-chain exchange has the below downsides:
  1. When a user wants to perform a cross-chain exchange for a trading pair, he needs to find another user on the other chain who wants to perform the reverse cross-chain exchange for the same trading pair.
  2. Two users need to agree on the exchange rate beforehand.
  3. Wrapping is not possible using HTLC.
- **Wrap-DEX**: Another solution is to use existing wrapping products. Using these products, users can lock their assets on the source chain and receive an equal amount of assets on the target chain. Then, they can perform their action on the target chain. Although this solution is better than the above solutions, it has the below disadvantages:
  1. It has a bad UX because users first need to wrap their assets using the wrapping products and then exchange them on one of the DEXs living on the target chain.
  2. Current wrapping solutions are not efficient in terms of cost and speed. Moreover, some of the existing wrapping products rely on centralized parties.

1.5 What Are the Main Challenges of Implementing a CCDEX?

Since the cross-chain exchange is a complex process containing multiple steps and modules, many technical and user experience aspects should be considered while implementing it. Below, we address the 3 main challenges:

- **Cost**: Transferring data between chains and verifying them are costly processes. These costs can dissuade users from using a CCDEX.

- **Speed**: The data on the source chain should be finalized before being used on the target chain. Some blockchains like Bitcoin have a slow finalization time (60 mins). On the other hand, exchange users prefer to execute and settle their trades quickly.
- **UX**: Cross-chain exchange is a multi-step process that involves two blockchains. Sending transactions on two blockchains requires users to have a wallet with enough native coins on each chain. These requirements make the cross-chain exchange a complex process that is not suitable for average retail exchange users.

2 What Is TeleportDAO?

TeleportDAO is a CCDEX with three promising features: low cost, high speed, and full decentralization. Using TeleportDAO, a user can exchange his tokenA on the source chain for tokenB on the target chain instantly at a low cost. Moreover, users can transfer their assets between chains. This functionality is called wrapping: a user locks his tokenA on the source chain and receives an equal amount of wrapped-tokenA on the target chain. Wrapping is a two-way process: a user can move his assets back and forth among different chains. TeleportDAO's main contract lives on a programmable blockchain, but it can also connect this blockchain to any other blockchain - programmable or non-programmable. TeleportDAO has a native token called TDT (TeleportDAO Token), which is used for paying fees and rewards to TeleportDAO participants. TeleportDAO uses AMM as its price-discovery mechanism. Furthermore, TeleportDAO uses relay as its interoperability solution, which is the most secure and decentralized interoperability solution.

2.1 What Are the Main Advantages of TeleportDAO?

We summarize the advantages of TeleportDAO in the following:

- **Instant settlement**: Users can instantly transfer their assets from a source chain to the target chain. Also, they can instantly perform a cross-chain exchange between two chains.
- **Low-cost Relay**: The relay mechanism that we use in TeleportDAO is a low-cost and incentivized solution. It allows two blockchains to read data from each other.
- **Decentralized and Secure**: TeleportDAO is the combination of a relay and an AMM DEX, which makes it fully decentralized. Also, as the relayed data is verified by the smart contract, our protocol has blockchain-level security.
- **Universal Solution**: TeleportDAO protocol can be applied to a programmable blockchain or non-programmable blockchain.
- **Simple UX**: While designing TeleportDAO, we kept a very important objective in our minds: the whole process of cross-chain exchange and cross-chain transfer should be simple for users. Users only need to have the native token of the source chain to perform the cross-chain exchange.

3 System Architecture

In this section, we explain TeleportDAO's participants and its main components.

3.1 Participants

TeleportDAO has six main participants: relayer, Teleporter, liquidity pool provider, instant pool provider, fast pool provider and TDT holder. Relayers are in charge of transferring data from the source chain to the target chain. Teleporters facilitate cross-chain exchange and transfer for users. Liquidity pool providers and instant pool providers provide liquidity for exchange pools and instant pools. Finally, TDT holders participate in the TeleportDAO governance decisions. Below, we further explain the role of each party in the system.

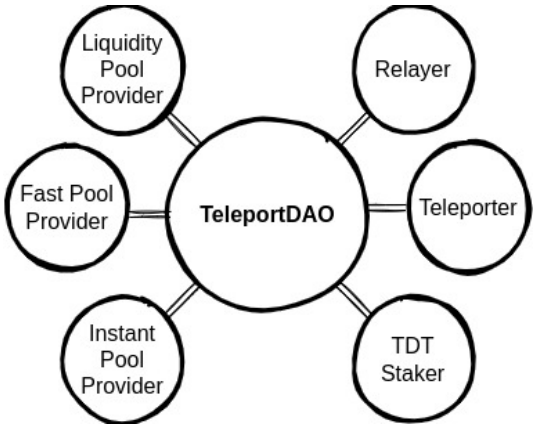

Figure 1: TeleportDAO participants

- **Relayers**: Relayers get data from the source chain and submit them to the target chain. Then, the relay contract checks the correctness of the submitted data and sends rewards to the relayer who has provided the valid data faster. Anyone can become a relayer in our system and compete to collect rewards. As long as one honest relayer exists in the system, users can perform cross-chain transfers and exchanges successfully.

- **Teleporter**: To create a better user experience, we introduce Teleporters. Teleporters are parties who transfer users' cross-chain transfer and exchange requests to the target chain. Users only need to have the native token of the source chain to perform cross-chain actions. Teleporters handle submitting the necessary transactions on the target chain and receive fees in return.

- **Instant Pool Providers**: These parties provide liquidity for instant pools. Instant pools are specific pools that enable instant features in the protocol. Anyone can become an instant pool provider in TeleportDAO and earn rewards in return.

- **Fast Pool Providers**: These parties provide liquidity for fast pools. Fast pools are specific pools that enable fast features in the protocol. Anyone can become an fast pool provider in TeleportDAO and earn rewards in return.

- **Liquidity Pool Providers**: These parties provide liquidity for liquidity pools of TeleportDAO. Anyone can become a liquidity pool provider in our system and collect exchange fees from users using that liquidity pool. All liquidity pool providers are required to put a small portion of their liquidity in the instant pools.

- **TDT Holders**: Users who hold TDT can participate in the governance of TeleportDAO.

Anyone can join the TeleportDAO protocol by playing any of the above roles.

3.2 Components

The main components of TeleportDAO are described as follows:

- **Blockchains**: The whole structure exists on at least two blockchains. One of them hosts the main contracts of TeleportDAO which we call "target chain" and the other blockchains are called "source chains". The target chain is programmable, however, source chains can be either programmable or non-programmable. The goal of TeleportDAO is to enable users to transfer or exchange their assets from a source chain to the target chain.
- **AMM DEX**: TeleportDAO AMM DEX lives on the target chain. It has two kinds of pools:
  - **Liquidity Pools**: In an AMM DEX, the relative price of tokenA to tokenB is calculated based on the amount of locked tokenA and locked tokenB in the liquidity pool of tokenA-tokenB trading pair. The amounts are calculated based on a constant product AMM scheme. Liquidity pool providers add liquidity to the liquidity pools to earn exchanging fees from them. In return, they receive LP tokens that indicate their share of the total collected fees.
  - **Instant Pools**: These pools enable instant exchange, instant transfer, fast exchange, and fast transfer in TeleportDAO. Each instant pool is created for a single token. Instant pool providers provide liquidity for these pools. They receive IP tokens that indicate their share of the total collected fees. To avoid liquidity issues, we allocate 10% of the provided liquidity from liquidity pool providers to get staked on instant pools.
- **Relay**: Relay is an interoperability solution that makes it possible to transfer assets and data from the source chain to the target chain. Relayers get block headers of the source chain and submit them on the target chain. Then relay, which is a smart contract on the target chain, checks the correctness of the submitted data. If a block header is validated by the relay, users can refer to it on the target chain for proving the validity of some finalized data on the source chain. As block headers include Merkle roots of all transactions and states, the relay can perform state or transaction inclusion verifications using Merkle proofs generated by a user. The simplest way to implement a relay is the SPV relay. In the SPV relay, the relay checks the validity of each submitted block header. However, checking the validity of each header has a considerable cost. In TeleportDAO, we apply LightSync, a light client solution that reduces the cost of relaying significantly.
- **Lock Pool**: In the case of having a programmable blockchain as a source chain, we use "Lock Pool Contract" and in the case of a non-programmable blockchain like Bitcoin, we use "Multisig Lock Pool":
  - **Lock Pool Contract**: Each lock pool contract is created for a single token. To perform the cross-chain transfer (exchange), the user locks the asset he wants to transfer (exchange), in the lock pool contract. After that, on the target chain, he provides proof of locking. Lock pool contracts assure that there exists an equal amount of locked assets on the source chain for every minted asset on the target chain.

– **Multisig Lock Pool**: Multisig lock pool plays a similar role to the lock pool contract in a non-programmable blockchain. Users lock their assets on the source chain by sending them to the multisig lock pool. The multisig holders are a group of users who have locked enough stake in TeleportDAO and mutually control the multisig lock pool contract. They take care of confirming burn requests and giving back users' locked assets on the source chain.
For transferring assets from the multisig lock pool to a user who has burned his wrapped tokens on the target chain, t valid signatures out of n signatures from multisig holders are sufficient. The signatures should be provided before a predetermined time has passed from sending the burn transaction by the user. Anyone (including the user himself) can report malicious acts of multisig holders to TeleportDAO by staking a small asset. This small amount of stake will be paid back in case of an honest report and gets slashed in case of a wrong report. The accused multisig holders should defend themselves by providing Merkle inclusion proof of the transaction that shows they have transferred the due amount. If a subgroup of t holders has signed such a transaction, they will provide the corresponding proof and all holders are clear. Otherwise, all the holders that have been unable to provide such proof will lose their stake on TeleportDAO as a penalty. The slashed amount will be paid to the user.

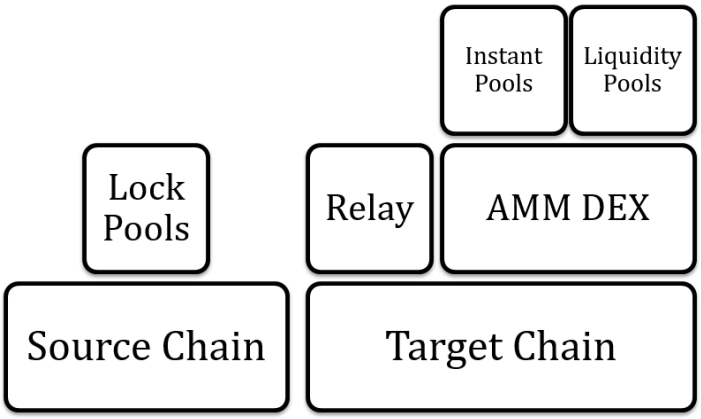

Figure 2: TeleportDAO components

4 How Does TeleportDAO Work?

4.1 Main Scenarios

- **Cross-chain Exchange**: Suppose that Alice wants to exchange amountA of her tokenA on the source chain and receive the amountB of tokenB on the target chain. First, she locks her tokenA on the source chain by sending them to the lockPool smart contract. Alice has to input the needed information for the exchange in a locking transaction. This information includes exchange tokens, the minimum amountB she expects to receive, the recipient address, etc. Note that most of the information is placed in the lock transaction by the UI automatically. Then, a Teleporter, who sees Alice's request on the source chain, submits her request on the

target chain. The inclusion and finality of the submitted transaction on the source chain are checked by the relay smart contract. After that, the AMM DEX executes Alice's request and sends the exchanged tokens to the recipient address on the desired chain. Alice has the option to receive the exchanged tokens on the source chain or target chain.

- **Wrap**: The wrapping process is similar to the exchange process. First, Alice locks her assets on the source chain. In the lock transaction, it can be determined that this is a transfer request or an exchange request. The Teleporter sends Alice's request to the target chain. After Alice's request gets verified and the smart contract makes sure that she has locked some amount of tokenA, the wrapped token smart contract gives Alice the same amount of wrapped-tokenA. Alice can get back her locked tokens on the source chain by burning her wrapped assets on the target chain.

- **Instant Exchange**: This feature is for users who want to perform their exchange in the shortest time. To perform instant actions, a user needs to lock TDT on the target chain. Suppose that Alice wants to exchange the amountA of her tokenA for some amountB of tokenB instantly. First, she needs to lock amountTDT of TDT on the target chain in a way that collateralRatio $\times$amountTDT$\times$PriceTDT is greater than amountA$\times$PriceA (collateralRatio is less than 1). Then, Alice sends her instant exchange request to the target chain. Alice's exchange request gets executed instantly and the exchanged tokenB gets transferred to her. Now, Alice has a limited time to lock amountA of tokenA in the lockPoolA smart contract on the source chain and provide the DEX contract with valid proof for that. If Alice doesn't provide the DEX with the corresponding proof in the predetermined time, the DEX will seize her locked TDT on the target chain as a penalty. The DEX exchanges a part of this amount of TDT to compensate for the exchanged amount of tokenA that has been spent during the process and sends the rest of it to the TeleportDAO treasury.

- **Instant Transfer**: The instant transfer is a special case of instant exchange. Here, Alice sends an instant transfer request for amountA of tokenA to the target chain. Provided that Alice has locked enough TDT on the target chain, the DEX accepts Alice's request and gives her amountA of tokenA from instantPoolA. Alice has a limited time to send the equivalent amount of tokenA to the lockPoolA contract on the source chain and provide the corresponding proof for the DEX on the target chain.

- **Fast transfer**: When a user wants to transfer an asset from the source chain to the target chain, first he locks the asset on the source chain. Then, he mints the wrapped asset on the target chain by providing proof for the inclusion of the lock transaction. If the source chain has a slow finality, it takes a long time for the user to be able to provide the inclusion proof for the lock transaction, so, the cross-chain transfer process will be slow. As an example, it takes about 60 minutes for data to get finalized in Bitcoin. The number of confirmation blocks "K" needed for a block to get finalized is called the finality parameter.
  In fast transfer, the user receives the wrapped asset on the target chain after his lock transaction gets buried under F ($<$ K) blocks. In other words, the user receives his transferred asset before his lock transaction becomes finalized on the source chain, reducing the waiting time for the user.
  As an example, suppose that Alice wants to transfer the amountA of tokenA from the source chain to the target chain. She locks this amount on the source chain. After this transaction

gets F confirmations, she sends the fast transfer request to the DEX contract. Leveraging the relay contract, the DEX contract checks whether the lock transaction has gotten F confirmations or not. If the condition is satisfied, the DEX contract sends an equivalent amount of tokenA from the instantPoolA on the target chain to Alice, extracting the fastFee. The fastFee is the fee that protocol gets from a user for the fast transfer service it provides. On the other hand, to compensate for the transferred amount from the instantPoolA, the locked amount on the source chain should be minted on the target chain and be sent to the instantPoolA. After the lock transaction gets finalized on the source chain, a Teleporter triggers the DEX contract to mint the wrapped tokens using the relay contract. The relay contract sends the minted tokens to the instantPoolA.
The above mechanism exposes instantProviders to a risk: since the lock transaction is not finalized when the tokens get transferred from the instantPoolA, there is a probability that the lock transaction gets reverted and the transferred amount from the pool does not get replaced. In this case, the instantProviders of instantPoolA lose their asset and Alice gains it.
To mitigate the above risk, we need to choose proper values for the below parameters:

- **fastFee**: A user who performs fast transfer should pay a fee to the instantProviders of instantPoolA.
- **fastLimit**: There is a limit on the amount that can be fast transferred in a single block of the source chain.

To determine the above parameters, first, we need to calculate the below parameters:

- **reversionProbability**: The probability of reversion of an F-confirmed transaction.
- **reversionCost**: The cost of reverting an F-confirmed block for an attacker.

The following conditions make, the fast transfer protocol secure:

1. The fastFee should be greater than reversionProbability*amountA: it motivates instantProviders to participate in the protocol.
2. The fastLimit should be less than the reversionCost: it demotivates attackers to revert an F-confirmed block as it won't be profitable for them to perform the attack.

Now a question arises: what are the differences between fast transfer and instant transfer? Why may a user prefer performing a fast transfer instead of an instant transfer? There are three main differences between fast transfer and instant transfer:

1. A user can perform a fast transfer without having any collateral on the target chain. However, for performing the instant transfer, the user needs to have enough collateral on the target chain.
2. The fast transfer is performed after the user's request gets F confirmations on the source chain. However, the user can perform instant transfer without the need to wait for any transaction confirmation on the source chain.
3. In instant transfer, the transferred amount is limited by the user's collateral on the target chain. In fast transfer, the transferred amount is limited by the fastLimit.

4.2 Fee and Reward Structure

Different parties of TeleportDAO need proper incentives to participate in the system. Below, we describe what fees users pay and how these fees are distributed between different participants. Whoever uses TDT, gets a discount on paying fees, however, there is no obligation for users to pay fees using TDT.

- **Relayer**: When a relayer submits a valid block header on the relay contract, the relay rewards him. The relay contract pays rewards from the relay treasury. If multiple relayers submit the same block header on the relay, the reward goes to the relayer who has submitted it first.
- **Liquidity Pool Providers**: Exchange fees of each trading pool are distributed among its liquidity pool providers proportional to their share in the pool. Users of trading pair tokenA-tokenB can pay the exchange fee in tokenA or TDT, so, the liquidity pool providers' rewards are in tokenA and TDT.
- **Teleporter**: Teleporters get fees for transmitting cross-chain exchange requests and wrap requests to the target chain. The cross-chain users can pay Teleporter fees in TDT or using the token that they want to exchange or wrap.
- **Instant Pool Provider**: They receive fees in return for providing liquidity for instant pools. Whenever a user performs an instant exchange, instant transfer, fast exchange, and fast transfer for tokenA, he needs to pay an instant fee in TDT or tokenA.
- **User**: users perform three kinds of actions: normal exchange, cross-chain exchange, and wrapping; cross-chain actions have the option of being instant or fast. The fees for each action are described below.
  - **Normal Exchange**: To exchange tokenA for tokenB, the user needs to pay the transaction fee as well as a small swap fee. The swap fee gets divided among liquidity pool providers of the tokenA-tokenB liquidity pool. The user can pay the swap fee in TDT or tokenA. Paying with the former has a discount for the user.
  - **Cross-chain Exchange**: To exchange tokenA on the source chain for tokenB on the target chain, a user needs to pay the accumulation of five fees: source chain's transaction fee, Teleporter fee, target chain's transaction fee, swap fee, and relay fee. The user can pay the last four fees in TDT or tokenA. Using TDT has a discount for the user.
  - **Wrapping**: To wrap tokenA on the source chain for wrapped-tokenA on the target chain, the user needs to pay the accumulation of four fees: source chain's transaction fee, Teleporter fee, target chain's transaction fee, and relay fee. The user can pay the last three fees in TDT or tokenA. Using TDT has a discount for the user.

4.3 Governance Model

When do we need governance? Decisions about the following subjects are made through the governance process:

- **Fees**: Relayers fees, Teleporters fees, and swap fees are determined by TDT holders' votes.

- **Adding/Removing Pair**: A new trading pair can be added or an existing one can be removed through the voting process.
- **Protocol Updates**: Protocols such as exchange protocol, relaying mechanism, etc. can be updated if their proposal is accepted

How does TeleportDAO governance work? Anyone can create a proposal regarding fees, adding and removing pairs, protocol updates, etc. For a proposal to get approved, the following conditions should be satisfied:

- In the first year of TeleportDAO deployment:
  - **Minimum participation**: 5% of total TDT holders
  - **Minimum vote**: 50% of voters
- After the first year of deployment:
  - **Minimum participation**: 10% of total TDT holders
  - **Minimum vote**: 50% of voters