Staking derivatives

Introduction

Staking derivatives is designed to enable SCRT staked to secure Secret Network to be used in other Secret Network applications such as DeFi, governance and games. Staking derivatives require delegators (holders) to stake their coins not directly to a validator, but stake coins to a secret contract, which then can delegate the coins to a list of validators based on the secret contract logic. The secret contract users interact with is called staking contract. Once delegators send token to the staking contract, the contract mints staking derivatives (dxSCRT) to the users. dxSCRT can then be used in any network application.

The primary goals of this effort is to ensure capital efficiency in the network.

Staking derivatives introduce concepts like validator pool, reward distribution logic, liquidity pool. Over time, these modules and concepts can evolve to a more permissionless product with decentralized governance.

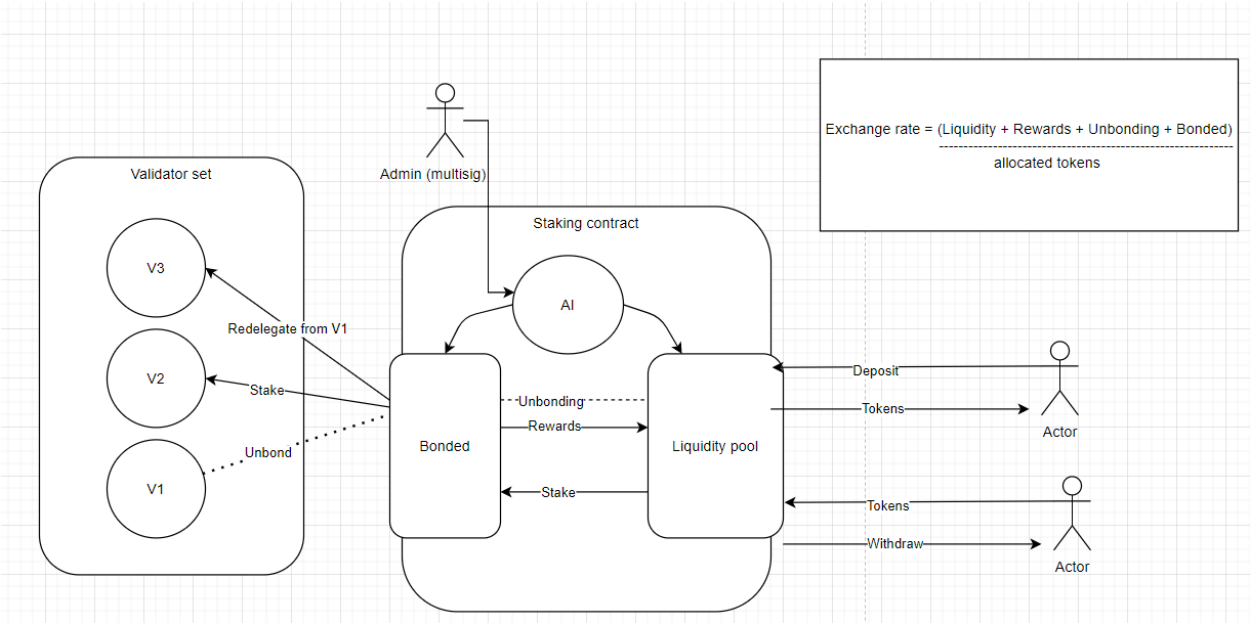
In addition, there also needs to be a fee users pay to create and burn staking derivatives. Initially staking derivatives can start with a fixed fee model. Over time, the product can introduce a constant function market maker (CFMM) to determine the price of liquid derivatives based on the size of the liquidity pool. *The higher the liquidity pool, the lower the fees. This ensures that SCRT is not disproportionately added to the liquidity pool vs. securing the network through staking.*

The advantages of dxSCRT are:

- Consumptive use for bonded SCRT, primarily in secretDeFi
- Automated re-delegation of network rewards by the staking contract
- Faster unbonding period (compared to 3 weeks), this is ensured by allocating some user tokens to a liquidity pool managed by the staking contract
- dxSCRT can be a privacy token - SNIP20. Users can buy dxSCRT for private staking.

Components

The components of staking derivatives contract include a validator set module that determines validator participation, staking module which handles bonded tokens and liquidity pool.



Validator set

Validator set contract determines the recipients of bonded SCRT in the staking contracts. Validators may be required to bond some SCRT in case they are slashed or slashed validators can be removed from the set.

- **Validator set** should be open to all validators, if there's a bond requirement it should not be prohibitive. *Potential idea that requires feedback:* **validators can add more deposit to receive a higher share of delegation from the staking derivatives contract.**
- **Distribution logic** of bonded SCRT among validators should either be uniform or based on validator deposits to the insurance pool. If Validator A bonds 30% of the insurance pool, Validator will receive 30% of the delegation in the pool.
- **Commission maximum** (the fees collected by validators) should be initially set to 10% and later *be subject to governance decisions going forward.*

Suggested MVP features for validator set

- Validator set is determined by an administrator. The smart contract administrator will add all interested validators to the contract
- Distribution logic is uniform. The pool of delegation is equally divided among n participants

Staking contract

Staking contract is the contract to which delegators will stake SCRT in order to receive dxSCRT and send dxSCRT in order to receive back SCRT. Staking contract has two components:

- ***Liquidity pool*** serves as a pool for delegators to have access to immediate liquidity.

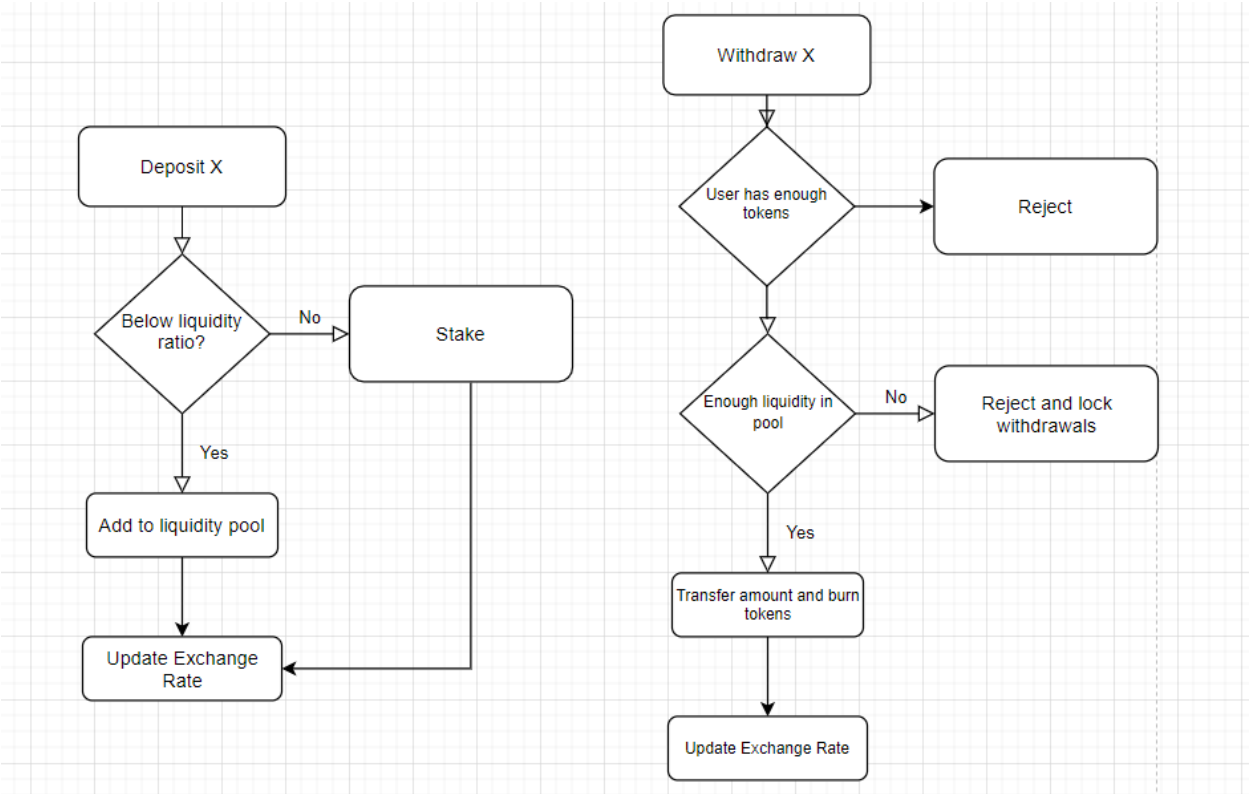
- ***Bonding pool*** represents the tokens that are delegated to the validators in the validator set based on the distribution logic described above

When a deposit is made to the staking contract x% of the funds go to the liquidity pool and (1-x)% of the funds get staked. This is a trade-off between staking rewards vs. access to liquidity. Higher liquidity ratio means lower delegation rewards for the users. *The liquidity ratio can either be set as a fixed number or can be determined as a function of supply and demand (like a CFMM).*

Staking contract can also have a fee model baked in. This would be the cost of minting a staking derivative. For example in MKR or Mirror, users pay a fee to mint tokens. The fee can also be tied to the concept of liquidity pool.

Suggested MVP features for staking contract

- Fixed fee model
- Fixed liquidity ratio
- No additional liquidity providers



Note: This diagram is slightly outdated

Liquidity pool

One advantage of the staking derivatives is to create faster liquidity while unbonding tokens, instead of the 3 week on-chain unbonding period. This is achieved by storing some of the tokens at the liquidity pool instead of delegating all tokens.

Liquidity ratio
At launch, the liquidity ratio is suggested to be set at a fixed rate (i.e. 20-25%). Liquidity ratio model can be replaced with a CFMM in future iterations

Liquidity providers (experimental idea, better suited for future iterations)
Users of dxSCRT and other network participants can provide liquidity to the pool. This would act as an insurance fund in case liquidity pool is depleted (there's a bank run). The liquidity providers to this insurance fund can collect fees for minting dxSCRT. *This is probably best left after the MVP.*

Bonded tokens

SCRT sent to the *staking contract* - *liquidity pool* requirements is delegated to the validator set based on distribution logic (i.e. share of stake provided by liquidity providers). Over time distribution logic should be determined by decentralized governance.