dPool: A Protocol for Pools of Staked Assets

Shaleen Jain (shaleen@jain.sh), Chakradhar (chakra5027@gmail.com)

v0.1.1 Draft

Feb 26, 2020

Abstract

In this paper we present a mechanism that allows users to delegate crypto assets of various dPoS blockchains by creating a pool of funds that is governed by a decentralized smart contract with pre-defined logic. The smart contract executes only when certain conditions are met allowing us to automate a lot of the manual processes and abstracts the protocol level details that are typical in the current staking and delegating ecosystem.
This creates an experience that is very similar to that offered by centralized custodian exchanges who provide staking rewards to their users by just holding their funds in their exchange wallets, yet completely decentralized and non-custodian by virtue of which our system is inherently more secure, distributed, eliminates legal and regulatory compliance and automates regular decision making and monitoring of network performance by employing optimised heuristics, game theoretic models, social consensus and governance.

Contents

1 Introduction

Till now the security and decentralization aspect of the blockchain networks has been in the hands of Network participants (Miners in the Bitcoin Blockchain) who typically provide the necessary infrastructure to run the network in return for incentives or rewards for their contributions.

Take Bitcoin as an example, the first computer or network of computers that found a hash with specific properties are rewarded with few Bitcoins roughly every 10 minutes. This is the proof that they have done the necessary work to verify all transactions in a block as valid and is allowed to add it to the blockchain. Committing a fraudulent transaction on the blockchain will require the party to have over half of the total hashrate of the entire network, this is known as the 51% attack. Since this process requires an immense amount of energy and computational usage, it is extremely hard for a malicious party to attack and make fraudulent transactions on the network. However this also hurts bitcoin blockchain as it is regarded as energy inefficient and harmful to the environment. Some other factors such concentration of miners in China which now hold a majority of computational power now is also the cause of concern, that is why networks have started to move from Pow to PoS, such as Ethereum which is proposed to be updated to PoS in 2020.

In a PoS network a group of validators takes turns proposing and voting on the next block, and the weight of each validator's vote depends on the size of its stake. When the validators discover a block which they think can be added to the blockchain, they will validate it by placing a bet on it. The validators will get a reward proportionate to their bets. Anyone who holds the blockchain's base cryptocurrency can become a validator by sending a special type of transaction to lock up their fund. Since this doesn't involve miners it is considered to be more energy efficient. DPoS is a further upgrade on PoS mechanism where the participants of the network have relatively more rights in the governance of the ecosystem of the network than in Pos.

With the rise of POS and DPOS systems there is a new breed of network participants evolved from Game-Theoretic models called Delegators. Most POS networks have a fixed number of validators with certain standards in order to reach a consensus quickly. Delegators can choose validators in order to stake the coins. This makes them participate in the governance process by choosing the right validators to perform operations in the network. Without delegators' help,

validators can not hold their position in the network as they need to have high stake in the network, i.e. Higher the number of staked tokens a validator holds, the higher it ranks, and less likely it would be to get deprived of the role of a validator.

1.1 The Pains of the Existing Staking Ecosystem

There is an increasing complexity in dealing with an ever-growing number of PoS blockchains with more than a few validators. We believe this is mainly due to lack of standardisation around a staking process and validator selection criteria.

- **Selecting a validator:** Right now every staking network has tens of validators. Delegators are perplexed to choose which validator they want to delegate their tokens towards. There are certain parameters outlined by different people to choose the validators but they need a lot of technical knowledge to understand the validator dynamics.

- **Lengthy process:** The process of staking a token varies from blockchain to blockchain with each having a different mechanisms and various bonding and unbonding requirements and periods and prerequisites. For a casual retail user doing this level of research for participating in networks security and consensus doesn't make sense unless they are ready to make a large investment.

- **Validator Performance Monitoring:** Keeping up with a chosen validators performance and network updates and/or changes is at this moment a very manual process with having to subscribe and follow many online forums and chat groups. Many users want to stake and forget.

- **Long lock-in periods:** With lock-in periods of over three to six months for some blockchains locking up native tokens by staking creates a trade-off for users between liquidity and earning rewards

- **No exit strategy**: In a clear bear market large institutional investors and even validators themselves wish to hedge their risk but are unable to do so due to the long lock-in periods or risk getting slashed by withdrawing earlier than the staking lock-in period expires.

1.2 Abstraction as a Solution

In software engineering and computer science, abstraction allows programmers to think on a certain level of complexity while hiding away details not relevant to the problem at hand. We use abstractions to prevent overloading the end user with details when they care more about higher level concepts. This lets developers focus user attention on what objects represent within their platforms, rather than the nuts and bolts.

In traditional finance, we have abstractions like the American stock market indexes (e.g. SP 500, DowJones Industrial Average (DJIA)) that represent hundreds or thousands of individual stocks. In the in-surance industry, we purchase policies comprised of a set of services in exchange for paying an insurance premium, without the need for fretting over individual coverage scenarios.

For cryptocurrencies, we can envision an abstract token or meta token, a single token representing a basket or portfolio of its underlying tokens [1]. That portfolio of the underlying token represented by a meta token can in-turn be representative of a smart-contract taking decisions to automate a lot of the tasks and act according to a predefined set of constraints.

1.3 Prior Art

A system like this has not been possible until now because no major PoS system live at this moment supports smart contract functionality which is critical for us. We believe the ideal blockchain for our use case while be one that has a delegated Proof of Stake consensus mechanism with a thriving validators and delgators ecosystem, smart contract capability with a mechanism to read the various on-chain and off-chain network statistics and optionally a provision of interoperability with other PoS blockchains allowing us to extend our application to chains as well.

The following are the blockchains we have identified that satisfy some or all of our above requirements:

- Polkadot
- Matic Network
- Skale Labs
- Cosmos with WASM runtime

Related Works:

The most notable prior attempt for creating a trustless staking pools is Rocketpool [2]. However their scope is only limited to the ethereum POS network and we haven't seen any proposal in their roadmap regarding the implementation of Validator indices that will keep the staking networks more decentralized. Other noteworthy projects like everett [3], stafi [4] & Stake DAO [5] have made considerable strides in making the staking tokens more liquid. As such, they are significant inspirations to the ideas put forth in this paper. But, we believe creating or focusing solely on liquidity for the staked tokens is not enough to bring more decentralization in the proof of stake networks.

2 dTokens

2.1 Overview

To solve the problem of liquidity in a PoS system that requires more than 50-60% coin staked to maintain network security we provide a wrapped token we call dTokens acting as a delegation receipt or a voucher acknowledging that a certain amount of tokens have been staked to a validator and are being used to secure the network. This allows us to then use the dTokens for additional use cases we describe in more detail below. However, just having a wrapped token to provide liquidity is not enough as it has no utility of its own and can very well lead to a fragmented market where there are ‘n’ wrapped tokens for ‘m’ staking tokens.

2.2 Introduction

A dToken is a rewards-bearing derivative token that is minted upon deposit and burned when redeemed. The dTokens carry the underlying value of the deposited amount plus the accrued rewards or minus the slashed amount from the validator, and can be safely stored, transferred or traded. While dPool will eventually interoperate across blockchains, dTokens are described in this document as smart contracts on the Ethereum blockchain that adhere to the ERC20 token standard. dTokens are very similar to the interest bearing cTokens by Compound Finance [6]

2.3 dToken Contracts

Each dToken contract of respective staked assets is structured as a smart contract that conforms to the ERC-20 token specification. Delegators balances will be represented as dToken balances. Delegators can mint dTokens by supplying assets to the market or redeem tokens for the underlying assets. The ratio between dTokens and the underlying asset increases overtime as interest is accrued by the asset when staking rewards are generated by the respective protocol. Examples of a dToken can be such as dMatic for Matic token of Matic network, dAtom for Atom tokens of cosmos, etc.

The conversion ratio of the token with the underlying asset depends on parameters like inflation/reward rate, slash ratio, bonding periods and the total tokens bonded by a validator.

$$conversionRatio = \frac{underlyingBalance + totalRewardsAccured - totalAmountSlashed}{dTokenSupply}$$

An initial conversionRation will be specified with contract creation of a dToken. Initial conversionRatio has to be large enough to account for the odd case of slashing as soon as the index has launched.

Two notable features of dTokens are that they are compounded as they earn the rewards and that their exchange rate is capable of falling if the underlying pool suffers a loss. This makes them well suited for risk management derivatives to be built on top.

Closing a dToken

Delegators are able to divest themselves of a dToken position in two ways: Redeeming the token with the underlying assets by sending the dToken to the burning address of the staking pool. When a dToken holder burns the token by sending it to the dToken contract, the assets they have staked will be deposited to their address after the end of the Bonding period of defined by the underlying assets blockchain protocol.

User flow

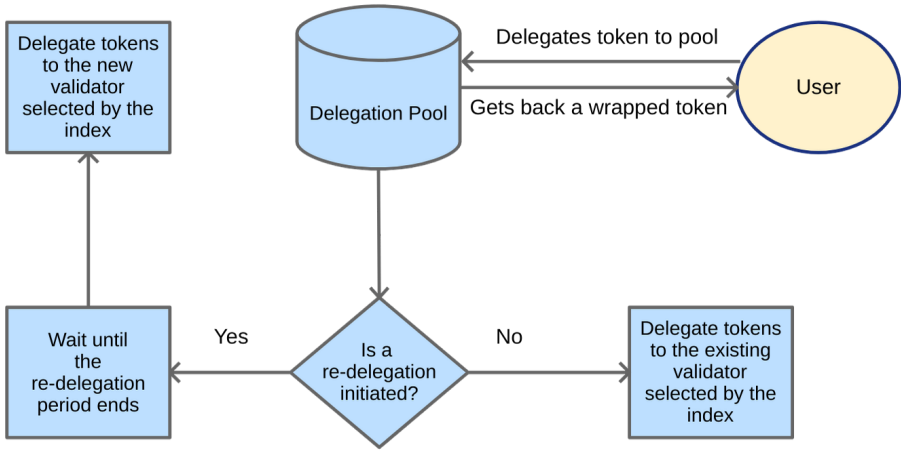

Figure 1: User delegation flow

2.4 Use Cases for dTokens

The Use cases of dTokens depends on the two types of participants in the ecosystem

1. **Network Participants (Validators & Delegators)**: Participate in validation process and were also primary asset holders who are looking for liquidity of their staked assets in order to mitigate risks from their staked assets
2. **Investors AKA Speculators**: These players are the ones who want to get exposure to staked assets without directly holding the underlying assets by speculating on derivate tokens like dToken via various margin lending and trading platforms

dTokens can be used as a building blocks for creating more sophisticated products. Some of the possible scenarios are:

- **Margin Lending**: Investors can speculate on a dToken that can represent a validator or a set of validator essentially speculating on their performance and reward output via margin trading platforms like dydx and syntetix
- **Liquidity:** Delegator and validators can get access to quick liquidity by providing dTokens as collateral to mint stablecoins via synthetic token protocols like syntetix and UMA protocol.
- **Total Return Swaps**: Holders and Validators can hedge their risk from price fluctuation through TRS (total return swap) mechanism where a third party pays them a fixed fee in order to claim future rewards accrued by them. For example: Alice creates an TRS on UAM protocol for a fixed duration like 3 or 6 months period. Bob will purchase the contract by paying an upfront fee to Alice to claim the total rewards accrued by dTokens for a given period of time.
- **Market Making**: They can earn trading fees by providing liquidity to DEXs like uniswap and Kyber.
- **Reverse Dutch Auction:** In Reverse Dutch Auction we offer up an asset for sale at some minimum price at which we think we could possibly sell the asset and periodically increase the price of the asset offered until there is a buyer. Such an auction contract can be used to sell any derivative token. The benefit of this auction is that it avoids the slippage and front-running that threatens the taker of sell orders for large amounts of the assets on DEXes.

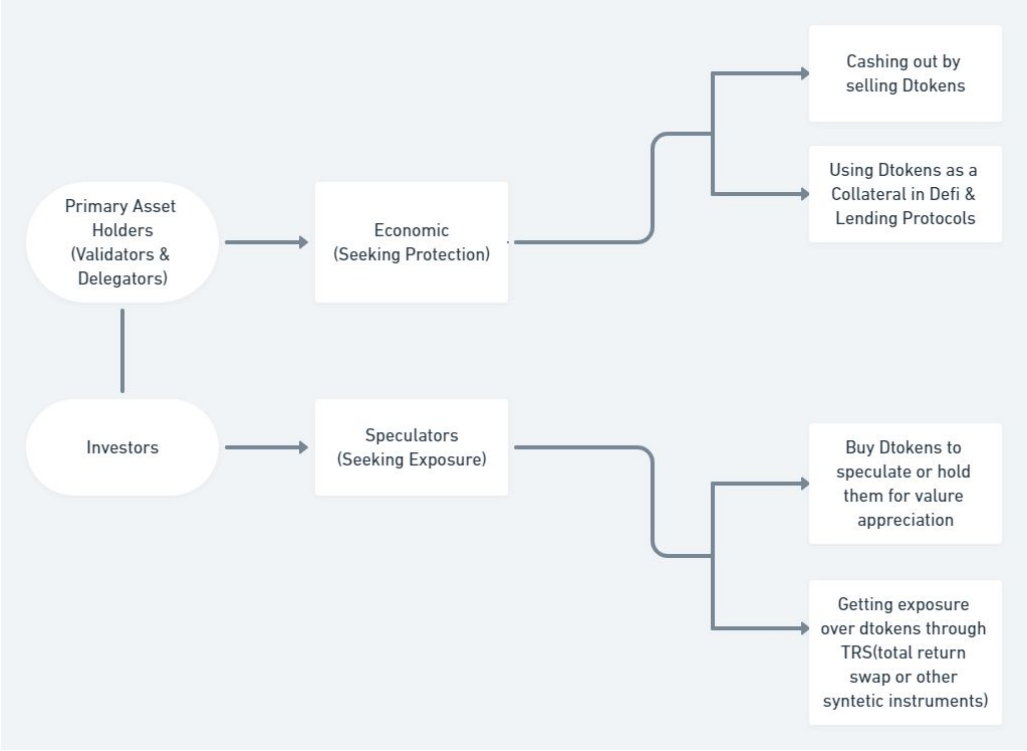

Figure 2: Possible use cases of a dToken

3 Validator indexes

3.1 Overview

Our goal with validator indexes is to provide benefits to the users by abstracting away the complexity of delegating their tokens which arise in terms of learning about the process and protocol requirements, knowing the criteria to select a validator, constantly monitoring the validator's performance and keeping up to date with network upgrades and how it might affect the delegation/staking mechanics. We provide this abstraction by the concept of indexes wherein we constantly measure and update a list of validators using a specific set of metrics leading to an ideal set of validators. At this point, we do not believe that we can judge validators by only one set of metrics therefore we provide multiple different indexes curated based on different sets of metrics leaving to the user which risk profile they wish to minimise by utilizing said indexes.

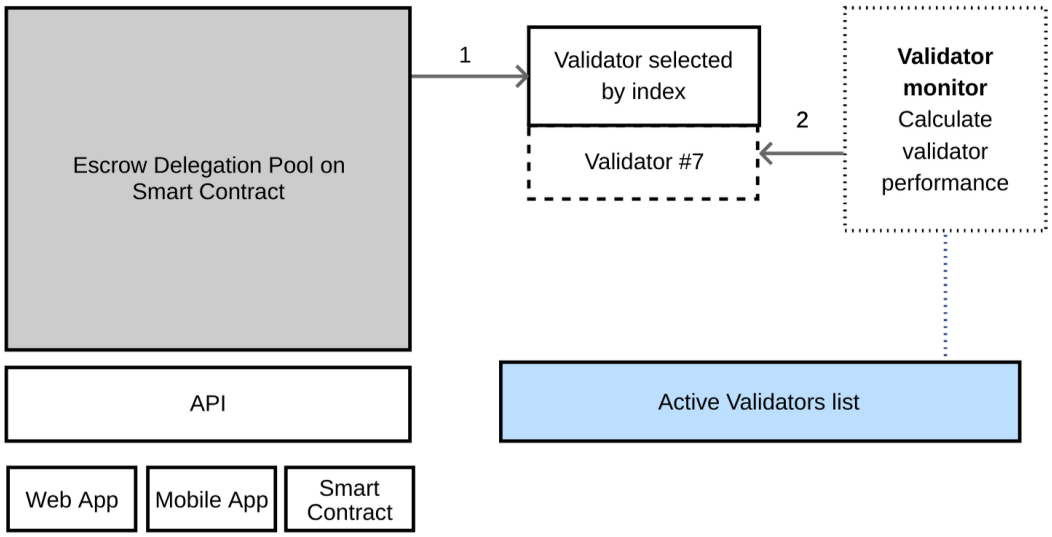

Figure 3: Process flow for delegation of tokens from pool

To bring more adoption and new investors to these staking networks we believe staking indexes will act as a gateway to bring more people to invest in these networks and eventually helping the network to be more decentralized and secured. Small validators will also benefit without reducing their hard earned commissions in order to attract delegations.

3.2 Concept

Reindexing period

This time period could be such as every delegation round period, every block, every new voting period, every staking lock-in and lock-out period, etc and is very specific to the underlying blockchain protocol.

Redelegation
After a reindexing period is over and results in a redelegation criteria being met it will trigger a redelegation over a set period of time known as redelegation period.
During redelegation the smart contract with automatically unbond tokens from existing validator for that specific index and redelegate those tokens to another validator according to the new index generated.

Redelegation Proposal Period
This period is a fixed period of time between 6 - 9 hours which gives the users of the particular index undergoing redelegation time to consider if the redelegation is valid and justifies the gas cost/fees. If the majority of the users conclude the redelegation is incorrect or should not happen for any reason and they can vote to stop the redelegation for that specific instance.

Redelegation Period
The redelegation period is the time required to unbond the delegators tokens from a previous validator and re-delegate to another validator. This period may vary from one blockchain to another.

3.3 Types of Implementation

Performance Index
A straight forward index is ranking the validator of the basis of their performance over a period of time (reindexing period) which can trigger a Redelegation.

How we measure metrics to calculate the performance of a validator will also be blockchain specific but examples include:

- Uptime
- throughput (request/s performance)
- Latency
- Reward rate
- Slashing history

The total performance score of a validator will take into account all these metrics.

Some chains such as Matic network will have a validator ranking system within the protocol making such an index very easy to implement. [7]

Need for different indexes

To enable a greater degree of decentralization among the staking networks we believe just by building a staking pool that runs on smart contracts is not enough. We have to make sure the assets should be allocated in chunks to different validators in order to avoid concentration of delegations to only a few validators.

Therefore we plan to come up with different indexes that provide other trade-offs between ease of selection and delegation decentralization. The indexes approach which was there in traditional finance will democratize pooled allocation to spread in different weightages to various validators.

We plan to continue researching on better indexes by market experimentation and user feedback but few of the indexes that we have come up in addition to performance index are:

- **Random chunked delegation index**
  Delegation amount is equally divided into “chunks” and then delegated to different randomly selected active validators.
- **Top 5 validators chunked delegation index**
  Delegation amount is equally divided into “chunks” and then delegated to the top 5 active validators.
- **Per validator index**
  Base case of just delegating directly to the validator but with the benefit of having an reward-bearing derivative token.
- **Minimum qualifying validator index**
  Base case of delegating directly to the validator along with constant monitoring of validator performance to avoid common cases of slashing conditions (such as signs leading to not enough uptime, etc).
- **Validator set index**
  A set of similar validators in terms of fees and reward cuts but tokens re-delegated between them based on various additional metrics.

We see the concept of indexes similar to token sets by SetProtocol [6] which offers various sets to users to choose and hedge their investment against since there cannot be a one size fits all approach.

4 Security

Users can trust our product only if we can guarantee the safety of their funds from hacks, bugs or even us. We can all agree that centralised exchanges are very susceptible to hacks and are an easy target due to them being a singular point of fund collection. Keeping with the ethos and principles of blockchain and the Bitcoin Ideology, we implement this system in a completely decentralised manner where only the code is law.

They achieve a high level of security by guaranteeing the following properties:

- **Non-custodial:** User funds will always be held in a non-custodial wallet or a non-custodial escrow smart contract
- **Explicit approval**: Tokens are only transferred from a users wallet by approval.
- **Minimum Escrow hold:** User funds are held in our escrow pool contract only until the funds are delegated to a validator and don't stay in our contracts for periods longer than a delegation period.

5 Governance

dPool will begin with centralized control of the protocol (such as choosing the re-delegation model per asset), and overtime, will transition to complete community stakeholder control via a DAO. The following rights in the protocol are controlled by the admin:

- The ability to list a new dToken market
- The ability to add a new index model
- The ability to update the index model per market
- The ability to update the oracle address
- The ability to choose a new admin, such as a DAO controlled by the community; because this DAO can itself choose a new admin, the administration has the ability to evolve over time, based on the decisions of the stakeholders

6 References

[1]: https://www.setprotocol.com/pdf/set_protocol_whitepaper.pdf
[2]: https://www.rocketpool.net/
[3]: https://everett.zone/
[4]: http://stafi.io/
[5]: Introducing Stake DAO by Stake Capital: claiming future yield revenue
[6]: https://compound.finance/documents/Compound.Whitepaper.pdf
[7]: https://docs.matic.network/staking/faqs/#how-can-a-new-validator-replace-an-existing-one