A Composable Solution to Risks and Delays in Unstaking Cryptocurrency in Proof-of-Stake Blockchains

Composable Foundation

Follow

--

Listen

Share

June 2023

Babylon, Composable Finance, and Stride

1 Abstract

Proof-of-Stake (PoS) consensus has become the norm for the vast majority of blockchains today, largely due to its energy efficiency compared to Proof-of-Work (PoW). Yet, to protect against malicious long-range attacks, PoS chains have established lengthy periods of time for blockchain users to unstake their funds, wherein these funds are unusable. This means users miss out on earnings opportunities and available liquidity for these tokens is reduced. To address this, liquid staking tokens (LST) were introduced, providing users with a liquid token representing staked funds that can be used during the staking period. However, these liquid staking tokens also have risks due to market depegs, and these risks increase with the length of the unstaking period.

Contributors to the decentralized finance (DeFi) organizationsBabylon, Composable Finance, and Stride are collaborating to introduce a solution that combines the benefits of liquid staking and cross-chain functionality while mitigating the risks associated with liquid staking. This collaboration is expected to reduce the systematic risks associated with liquid staking as it continues to grow in the DeFi space across multiple ecosystems.

2 Introduction

Overview and Benefits of Proof-of-Stake

The concept of a Proof-of-Stake (PoS) blockchain system was originally created by Sunny King and Scott Nadal in 2012, published in a paper[1] detailing what became the first PoS network, Peercoin[2]. This technology was developed as an alternative to the Proof-of-Work (PoW) consensus mechanism used by Bitcoin[3].

PoW ensures the security of the network and regulates the creation of blocks and the overall state of the blockchain by assigning the role of miners. Miners employ computer programs to make countless guesses to solve a challenging hash puzzle, with the winner being awarded the right to propose a block. Once the hash puzzle is solved, a block is verified and created, and the miner who discovered it is compensated in cryptocurrency. Despite its efficacy, this system has proven to be incredibly demanding in terms of computational requirements and energy consumption.

Proof-of-Stake was devised as a far more energy efficient means of securing a network and validating blocks. In lieu of miners, PoS involves validators who stake a network's native cryptocurrency by locking up these funds in a smart contract. When a new block is being created, validators are selected to publish the new block based on an algorithmic delegation based on how much the validator has locked up (i.e. staked). When a validator creates a block, they are also rewarded in crypto, similar to a miner in PoW. Individuals can delegate their staked funds to different validators to increase the validator's stake, therefore increasing the validator's chances and volume of block creation. Validators in turn give users staking rewards as a benefit to contributing to their stake and the validator's own earnings.

In the ten years since their ideation, Proof-of-Stake protocols have quickly become the norm in the blockchain space. There are notable exceptions such as Bitcoin which remains PoW since its inception, but virtually all new blockchains are PoS (such as the Cosmos Network[4], Polkadot[5], and Cardano[6]. The Ethereum Network[7] even made the switch from PoW to PoS with "The Merge" on September 15, 2022[8]).

There are many reasons for the rising popularity of PoS chains; a driving factor is the significantly lower energy consumption associated with PoS. For instance, Ethereum's Merge to PoS has reduced the chain's energy consumption by 99.9%, which is akin to the energy consumption of the entire country of Finland[9].

Limitations of Proof-of-Stake

Despite the energy savings of PoS networks, there are still limitations. For instance, token owners govern PoS systems, rather than nodes and miners in PoW. While this is more democratic in that it allows user-based governance, it also can increase centralization in the case of individuals owning large proportions of token supplies. Further, PoS chains are uniquely vulnerable to long-range attacks. While there are many protective steps against long-range attacks, they remain difficult to surmount.

To protect against long-range attacks, PoS chains require stakers to enter long lockup periods, where their tokens are slashable and non-transferrable. When a user wants to withdraw funds they have staked with a validator, it typically takes multiple weeks between these tokens being requested to be unstaked and the tokens actually being returned to the user, as illustrated in the table below.

Rather than a fixed unbonding time, the withdrawal period in Ethereum is decided by 2 variable processes: the validator exit process and the withdrawal process. Read more here.

During the unbonding period in PoS systems, users do not have access to their tokens. During this time, users are unable to receive staking rewards or participate in value-generating opportunities such as liquidity provisioning. This also poses the risk that the value of these tokens could significantly diminish during the unbonding period, rendering the user unable to try to sell their tokens before seeing their value plummet. This also reduces the available liquidity of this token. Overall, long unbonding periods introduce significant friction to PoS systems.

However, these lengthy unbonding periods serve a crucial purpose in protecting against long-range attacks[10], also referred to as alternative history

or history revision attacks. Such attacks occur when a malicious actor creates a branch off of the original blockchain that becomes longer than the true, canonical chain, thus overtaking it. These attacks are not feasible on PoW chains, as rewriting these blocks would require massive computational effort. Yet, on PoS networks, these attacks could happen through a number of different methods such as malicious actors forging block timestamps, joining forces to produce blocks on the branched chain, or using the keys of old validators (such as founders who have withdrawn their stake) to build a new chain branch.

To mitigate these attacks, social consensus is used on PoS chains. This involves new clients and validators to identify checkpoint blocks on a canonical chain using a trustworthy source like trusted websites or peers. This ensures that users are operating along the correct, canonical chain. However, this can take quite a bit of time, as it necessitates getting information from other sources or individuals. This is referred to as dismal latency, wherein it may take up to weeks for all trusted peers to agree on a checkpoint. To ensure that old validators cannot withdraw their stake and then create new branches of the chain before social consensus is reached (i.e. implementing a long-range attack), unbonding times on PoS networks are quite long.

This need for social consensus to mitigate long range attacks also has an impact on the functioning of IBC (Inter-Blockchain Communication). IBC works by the receiver chain maintaining a light client of the sender chain, and the light client is updated every time there is an IBC packet communicated. If an IBC connection has not been used for beyond the unbonding period of the sender chain, the receiver chain is susceptible to long range attacks in the sender chain, and the IBC connection needs to be shut down and restarted. This process essentially forces social consensus. In this context, a long unbonding period means that IBC connections can be maintained even with sporadic communication.

3 Liquid Staking

Overview of Liquid Staking

The concept of liquid staking was introduced[24] to provide token owners with a liquid token for the duration of their staking periods. In liquid staking, users can stake tokens as they normally would to PoS validators. Unlike traditional staking, when a user liquid stakes they are minted a token that represents this underlying stake that can be leveraged during staking.This provides users with flexibility and greater earning potential, as they can use these staked tokens freely, massively increasing the yield that a single token can earn

As a result, liquid staking and staked tokens have become quite popular. On Ethereum alone, there were 5,7100,300 liquid staked ETH, as of October 28, 2022[11]. Using the value of ETH at the time[12], this would be over $8.6 billion in total value of staked ETH, making Lido the largest DeFi protocol by TVL (total value locked).

Yet, liquid staking has limitations. For one, the stake underpinning a liquid staked token can be slashed or can still fall in value, meaning that the user will still have losses upon unstaking and that the staked token may also lose value. Further, liquid staking poses some network centralization risk, as liquid staking services can amass significant token volumes. For instance, LIDO[13] holds 4,798,754 ETH in its liquid staking protocol, which is 38.3% of the entire staked ETH token supply[14].

What is the impact of long stake unbonding periods on liquid staking protocols? In periods of deleveraging, such as the Three Arrows capital liquidation event, the price of LSTs (liquid staking tokens) can depeg against the underlying token. For example, leveraged stETH positions can be liquidated, which can lead to stETH selling, leading to further liquidations, which can cause a vicious cycle of cascading liquidations. Such a vicious cycle could harm the health of DeFi protocols, and in rare cases, the security of the network itself.

LST depegs present a profit opportunity for arbitrageurs willing to purchase, redeem and hold depegged staking tokens for the duration of the unbonding period. However, unbonding periods can be long (or even disallowed entirely), which increases the risk of holding the token during the unbonding period. In an efficient market, the magnitude of LST depegs should not exceed the price to short the underlying token over the duration of the unbonding period (if a depeg exceeded this price, an arbitrageur could short the token for the price to hedge exposure, and sell the difference once the unbonding has completed). Therefore, the longer the unbonding period, the greater the possible magnitude of a depeg. This enables a purely financial event like deleveraging to undermine the strategy tokens and subject liquidity providers to substantial loss.

Risks of Liquid Staking

The principal-agent problem is a situation in which the interests of the validator (the agents) are misaligned with the network participants (the principal). This occurs when the responsibility for block production and slashing is separated, leading some to question the validity of the PoS model. There is a concern that a validator who holds a large portion of liquid staked tokens may engage in unethical behavior, such as misbehavior and selling the tokens to avoid being slashed.

Leveraged staking poses its own set of risks, including the possibility of cascading liquidation and unbonding. By leveraging stake, a large number of underlying tokens may be unbonded by liquidators, which can reduce the stake rate. The practice of borrowing tokens against a staked position, such as stATOM, and then using those borrowed tokens to stake again, creates a cyclical process that increases risk. The more this process is repeated, the lower the collateralization ratio becomes, which makes the position more susceptible to liquidation from smaller price movements. In the event of a slash, the entire leveraged staking position could be liquidated, even all the way down to the initial staked amount.

Outsourcing Governance and Validator Set Selection to another chain presents its own set of challenges, particularly relevant within the context of the Cosmos ecosystem. For example, if Stride, with its own validator set, provides liquid staking to other chains, its validator set will now dictate the distribution of stATOM or stOSMO. This situation highlights the need for careful consideration and evaluation of the implications of outsourcing such critical components of a blockchain.

The Protocol Risk refers to the potential harm that could result from a significant security breach, such as the hypothetical scenario of a hack of a large LST protocol like Lido, which currently holds nearly 7 million staked ETH. This could lead to a catastrophic event and result in substantial consequences.

Babylon

Babylon[15] was created to bring Bitcoin security to enhance the security of PoS chains. One use case is to reduce the lengthy unbonding times in PoS chains in a manner that avoids the risks associated with both liquid staking and long-range attacks. Specifically, Babylon uses Bitcoin as a source of trust to checkpoint all the blocks on the PoS chains, instead of relying on social consensus. Since Bitcoin consensus requires hours while social consensus requires weeks, the unbonding time can be safely reduced from weeks to hours[16].

Stride

Stride[17] is the Cosmos liquid staking provider with the highest market share and first blockchain to use interchain accounts and interchain queries in production to build DeFi. Stride allows for cross-chain liquid staking, enabling users to stake tokens from any Cosmos chain through their protocol, minting users a staked version of their tokens. Currently, Stride supports liquid staking[18] for the Cosmos Hub (stATOM), Osmosis (stOSMO), Juno (stJUNO), and Stargaze (stSTARS) tokens among others.

Composable Finance

Composable Finance[19] is an organization building cross-ecosystem technology and infrastructure. This is being facilitated through Composable's Centauri[20], a bridge implementing the Inter-Blockchain Communication (IBC) Protocol[21] beyond Cosmos, connecting DotSama (Polkadot and Kusama[22]) to Cosmos sovereign chains, NEAR Protocol, ETH 2.0 and more. Through Centauri and its other offerings, Composable is interconnecting the expanse of the DeFi industry, with the aim of enabling any currency to be used on any chain.

4 Proposed Solution

Contributors to the Babylon, Composable Finance, and Stride projects are collaborating to create a solution to the current limitations in staking and unstaking in PoS blockchains. These three protocols are combining their technology to create an offering that allows the benefits of liquid staking, fast unbonding, and cross-chain operations to be merged. As a result, the advantageous field of liquid staking is made less risky, while also being further encouraged to grow across blockchain ecosystems.

In the immediate term, the token at the center of this offering is staked ATOM (stATOM), the staked version of the Cosmos Hub's native token, ATOM[23]. As Composable extends IBC to other ecosystems, stATOM will become available across more chains and ultimately the entire DeFi industry. This highlights the importance of Composable to the growing liquid staking sector. As it is expanding the functions and reach of staked tokens across the industry, Composable is taking responsibility for mitigating the risks associated with cross-ecosystem liquid staking.

In the current state of the market, liquid staking ATOM occurs as follows: users first bond their ATOM tokens through Stride in order to stake them, minting stATOM to the users in return. Users are freely able to use stATOM as always during the bonding period. Then, when users unbond, the stATOM is burned in order to return the user their ATOM. Yet, there is some inherent risk here since ATOM needs to be returned in 21 days, meaning users miss out on rewards. Further, in the event of a liquidity crunch, there may not be enough ATOM to go around, causing additional issues with this lengthy unbonding time.

Decreasing the duration of the unbonding period would mitigate the risks inherent in liquid staked ATOM, both for individual users and the broader ecosystem. As explained previously, a shorter unbonding period would lower the cost for arbitrageurs to purchase discounted stATOM and redeem it for ATOM, thereby reducing depeg risks and their severity. Thus, Babylon's proposals offer a promising solution to these challenges.

The risk of depegging increases when stATOM is bridged to other locations. However, with the Cross-chain Virtual Machine (XCVM), Stride users can manage depeg risk across various chains and ecosystems. For instance, a user deposits stATOM on Stride, transfers it to Picasso, and starts LPing on Pablo. If Babylon is live on the Cosmos Hub and the ATOM unbonding period is shortened, they can execute rapid ATOM withdrawals on Stride, all from a single program without the need to manually switch between multiple locations. This streamlined process reduces the complexity and risk associated with bridging and managing tokens across multiple ecosystems. This process can be replicated on any chain where stATOM is available, allowing users to skip the laborious steps of manual bridging and unbonding multiple times.

Overall, the joint solution from Babylon, Composable, and Stride offers improved flexibility and user experience for expanding liquid staking across multiple chains while minimizing the associated risks. This approach enables users to leverage liquid staked tokens (e.g., stATOM) across various ecosystems without imposing major undue risks on any individual ecosystem.

5 References

1. King, Sunny and Nadal, Scott. 2012. "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake". (https://decred.org/research/king2012.pdf).
2. "Peercoin". (https://www.peercoin.net/).
3. "Bitcoin". (https://bitcoin.org/en/).
4. "Cosmos Network". (https://cosmos.network/).
5. "Polkadot". (https://polkadot.network/).
6. "Cardano". (https://cardano.org/).
7. "Ethereum". (https://ethereum.org/en/).
8. "The Merge". (https://ethereum.org/en/upgrades/merge/#:~:text=The%20Merge%20was%20executed%20on,energy%20consumption%20by%20~99.95%25).
9. "Ethereum Energy Consumption Index". (https://digiconomist.net/ethereum-energy-consumption).
10. Deirmentzoglou, Evangelos; Papakyriakopoulos, Georgios, and Patsakis, Constantinos. 2019. "A Survey on Long-Range Attacks for Proof of Stake Protocols". doi: 10.1109/ACCESS.2019.2901858.
11. Lee, Martin and Furkan Gök, Hasan. 2022. "An On-Chain Look at Ethereum's LSD Landscape". (https://www.nansen.ai/research/an-on-chain-look-at-ethereums-liquid-staking-landscape).
12. "Ethereum Price". (https://ethereumprice.org/).
13. "LIDO". (https://lido.fi/).
14. "Ethereum Supply". (https://ycharts.com/indicators/ethereum_supply#:~:text=Ethereum%20Supply%20is%20at%20a,2.23%25%20from%20one%20year%20ago).
15. "Babylon Chain". (https://babylonchain.io/).
16. Nusret Tas, Ertem; Tse, David; Gai, Fangyu; Kannan, Sreeram; Maddah-Ali, Mohammed Ali and Yu, Fisher. 2022. "Bitcoin-Enhanced Proof-of-

Stake Security: Possibilities and Impossibilities". To appear in IEEE Symposium on Security and Privacy, 2023. (https://arxiv.org/pdf/2207.08392.pdf).

17. "Stride". (https://www.stride.zone/).
18. "Stride: The Liquid Staking Zone". (https://docs.stride.zone/docs).
19. "Composable Finance". (https://www.composable.finance/).
20. "Centauri". (https://docs.composable.finance/products/centauri-overview/).
21. "IBC Protocol". (https://tendermint.com/ibc/).
22. "Kusama". (https://kusama.network/).
23. Hart, Sam et al. 2022. "The Cosmos Hub". (https://gateway.pinata.cloud/ipfs/QmWXkzM74FCiERdZ1WrU33cqdStUK9dz1A8oEvYcnBAHeo).
24. Manian, Zaki and Sunny Aggarwal. (https://forum.cosmos.network/t/a-design-for-fungible-staking-derivatives/2441).