The bAsset Protocol: The Inter-Blockchain Financial Layer

Ryan Park, Jake Kim, Daniel SH Hong

June 2020

Abstract

While Proof-of-Stake (PoS) adoption continues to grow as a viable alternative to Proof-of-Work systems, the economic aspects of PoS remain an understudied area. For PoS systems to be sustainable in the long term, there needs to be a solution that repurposes staking as an attractive financial investment. In this paper, we propose a new asset class called **bAssets**. bAssets are shadow token representations of underlying staking positions, enabling utilization on decentralized financial applications. We show that such a system improves the economic efficiency of on-chain assets without harming the core incentives that make PoS protocols secure.

Table of Contents

List of Figures

I Introduction

Over a short period of time Proof-of-Stake (PoS) algorithms have grown in popularity, becoming a core component of many blockchains. [1] However, research on PoS has mostly been focused on algorithmic network security, while neglecting its economic implications.

PoS differs from traditional blockchain consensus algorithms (i.e. Proof-of-Work) in that token holders are able to gain income by locking up their capital rather than running physical mining hardware. Profits from locked-up capital are comparable to interest rates on investments in traditional finance. Interest rates tend to reflect all relevant market forces . This allows investors to be aware of the opportunity cost of their investment, leading to economic efficiencies.

PoS's economic inefficiencies are caused by the fact that rate of profit under PoS does not benefit economic circulation, unlike interest rates in traditional economics. This rate is crucial in maintaining the security of the network and thus is difficult to dynamically change based on market conditions. Therefore, a secondary financial layer must exist on top of PoS in order to solve this dilemma between capital inefficiency and network security.

We present bAssets - a decentralized protocol enabling the creation of liquid staking positions, which enable PoS ecosystems to bypass their limitations and increase their economic efficiency.

I.1 Prior Work

I.1.1 Proof-of-Stake (PoS)

PoS is a consensus algorithm, in which participants must lock up capital (tokens) in order to participate in the validation of on-chain network messages through a process known as staking. Under a standard PoS system, staking participants are incentivized to participate in network consensus through the distribution of staking rewards. To discourage malicious behavior, some PoS blockchains deduct staked tokens from malicious actors, an event also known as slashing. Additionally, an unstaking period, in which a certain amount of time is required for recovery of staked tokens, is introduced to prevent collusion between network validators. Finally, some PoS blockchains allow staking participants to delegate their stake to validators, who usually take a cut out of the rewards as a commission.

I.1.2 Decentralized Finance (DeFi)

DeFi refers to the ecosystem of smart contract-based decentralized applications (dApps) that primarily focus on finance. DeFi aims to create permissionless, trustless, and transparent financial products using blockchains [2]. For example, cryptocurrency users can use DeFi to mint stablecoins on MakerDAO [3], swap tokens on a decentralized system, such as Uniswap [4], or participate in money markets, like Compound [5].

II Problem Statement & Design Objectives

II.1 Problem Statement

As stated in the previous sections, vanilla PoS inevitably results in economic inefficiencies. In this section, we cover potential issues caused by fundamental dilemmas in PoS.

II.1.1 Staking Harms Ecosystem Development

While the ability to gain staking rewards is attractive for many investors, relying on reward mechanisms for network security means that PoS rewards have to compete with DeFi applications. For example, in order to stay competitive, staking DeFi lending platforms have to offer rates higher than the staking returns. This leads to capital inefficiency in money markets, by increasing the cost of borrowing tokens cost, reducing the propensity to borrow.

Additionally, staking also introduces an opportunity cost for locking up capital. Users are deterred from using applications that require tokens to be locked up, such as MakerDAO and interchain transfers, widely affecting the application ecosystem. Even if those applications were to stake a portion of their deposits with fractional reserve staking, they cannot stake all of their deposits without introducing secondary problems, such as the risk of bankruptcy.

II.1.2 PoS Security is Economically Inefficient

Tokens used in an application cannot be staked, and therefore, cannot contribute to network security. This is true even when applications carry out fractional reserve staking.

Moreover, the illiquidity of staked tokens means that market volatility directly affects network security. For example, individuals who value liquidity over staking can unstake a significant amount of tokens during periods of high market volatility, which negatively affects security under PoS.

II.1.3 PoS is not Market Friendly

Since staked tokens cannot be traded, their value cannot be properly reflected on the market. Therefore, under PoS, the value of the network is determined by those with less of a stake in the network. Additionally, the decentralized nature of networks may be heavily influenced by centralized exchanges, as they are required to maintain a significant number of unstaked tokens for liquidity purposes.

Furthermore, staking participants are directly exposed to price fluctuations during the unstaking period, becoming vulnerable to potential losses. This goes against the basic principles of PoS, as token holders are disincentivized from staking. This illiquidity also means the value of staked tokens cannot be invested in other applications, hindering the overall growth of the ecosystem.

II.2 Design Objectives

II.2.1 Decentralization

Whenever a significant value of assets is deposited for the generation of bAssets, any vulnerability within the system may become a single point of failure. Since staking positions securing underlying blockchains are managed by the bAsset protocol, a protocol failure may critically impact the network security of these chains. Thus, all processes involving the issuance and utilization of bAssets must be kept decentralized.

II.2.2 Fungibility

Each PoS validator has different commission rates and risk profiles. If bAssets do not account for these differences and each validator is given a unique bAsset, the overhead of having to interact with multiple tokens will negatively affect user experience. The liquidity of bAssets will be split among each bAsset type, further decreasing the usability of bAssets. Thus, to ensure a high degree of usability, bAssets must be made fungible regardless of the underlying staking position and validator.

II.2.3 Soft Peg with Native Token

The user experience of bAssets can be greatly improved by having a soft price peg between bAssets and native tokens. bAssets algorithmically follow the price of its underlying asset, similar to the way stablecoins follow the price of their respective fiat currencies.

II.2.4 Compatibility with Core Protocol Incentives

The bAsset protocol aims to preserve the core incentives of underlying blockchains. Incentives for positive behavior should not be affected, as disruptions could negatively affect, or even halt, network consensus. By implementing an insurance pool layer, the bAsset protocol financially motivates participants to support productive validators and punish the opposite. This mechanism provides an incentive for the creation of a healthy blockchain ecosystem and builds a symbiotic relationship with underlying blockchains.

III The bAsset Protocol

The bAsset protocol allows for the creation of bAssets, a liquid, tokenized form of a staking position.

III.1 Components

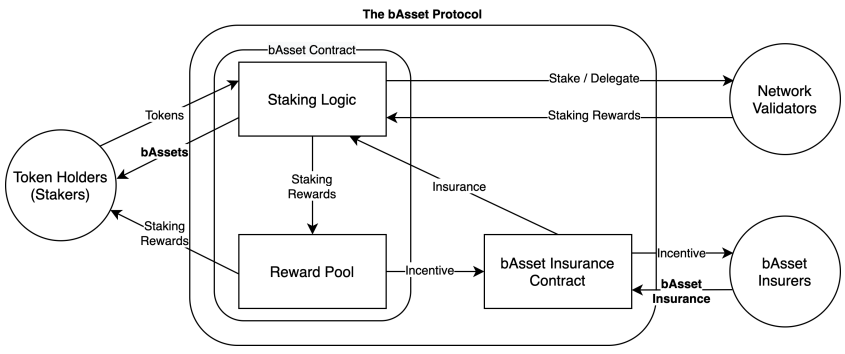

Fig. 1. Overview diagram of components in the bAsset protocol

III.1.1 bAssets

bAssets are tokenized representations of a staking position, which are soft-pegged to their respective underlying asset. bAssets are fungible regardless of which validator their staking positions are based on. bAssets each correspond to an underlying asset, and

thus staking rewards generated from them can only be claimed by the holder of bAssets through a reward distribution mechanism. Holders can reclaim underlying assets by reverting the bAsset minting process, after an unstaking period (e.g. 21 days for Cosmos) has passed.

III.1.2 bAsset Contract

The bAsset contract is responsible for the delegation of underlying assets, generating bAssets, and distributing generated staking rewards. A certain percentage of collected staking rewards is allocated to the bAsset insurance contract as an incentive.

III.1.3 bAsset Insurance Contract

The bAsset insurance contract provides protection against insolvency risks from events such as double-signing and downtime slashing. Funds in the bAsset insurance contract cover losses for respective scopes of liabilities (e.g. validators, nodes). While there is a risk of invested insurance funds being used to cover slashed assets and keep bAssets fungible, insurance participants can expect higher returns relative to vanilla staking rewards. In order to evenly distribute staked capital among participating validators, the contract may apply progressive taxation in addition to insurance incentives.

III.2 Mechanism

III.2.1 bAsset Generation

bAssets are issued when a user sends underlying assets to the bAsset contract, which then sends a staking transaction and opens a staking position. Users may select a validator to mint bAssets on. If no validator is chosen, then the contract stakes to the most over-insured validator, as they are more likely to perform better. Thus, the supply of bAssets issued is equivalent to the amount of assets staked - although this one-to-one peg may break in certain cases.

If bAsset insurance rates are low, the protocol can be adjusted to automatically transfer a portion of minted bAssets to the insurance contract to cover the underlying liquid staking position and slashing events.

III.2.2 Staking Reward Distribution

A bAsset holder can send a transaction that prompts the bAsset contract to send back a pro-rata share of the rewards accrued over the user's period of ownership. Additionally, transferring bAssets automatically triggers the rewards to be sent to the previous bAsset holder.

Moreover, since the bAsset contract cannot differentiate between natural persons and smart contracts, applications utilizing bAssets must claim staking rewards through a different mechanism.

III.2.3 Underlying Asset Redemption

Any bAsset can be converted back to its underlying asset when it is sent to the bAsset contract. When redemption is requested, the contract unstakes the underlying asset from the most under-insured (lowest-performing) validator, also on a one-to-one basis (which

may differ in specific situations). After an unstaking period, the redeemed assets are sent to the requester and the corresponding bAssets are burned.

III.2.4 Insurance Participation

The insurance mechanism works as a pool scheme to distinguish between scopes of liabilities. All bAsset holders are eligible to cover an insurance pool, incentivized by sharing a portion of bAsset staking rewards, which is then redistributed among insurers.

Each insurance pool, reflecting the different risk and reward profiles of validators, gives out insurance incentives on a pro-rata basis. Since each slashing event corresponds to a particular pool, the covered amount differs based on the performance of each pool.

III.2.5 Slashing Coverage

A slashing event automatically deducts its corresponding pool's balance and triggers a voting period to re-stake post-slashed assets. This enables steady income from bAssets, regardless of slashing events.

The previous insurers select validators to re-stake, with voting weight given in accordance with the proportion of covered assets. After the voting period, underlying assets are re-staked, with the amount being proportional to the number of votes.

However, there is a possibility where the corresponding insurance pool does not fully cover the slashing event. Ultimately, there is a possibility of bAsset under-collateralization breaking the protocol. In order to prevent these risks, the slashed amount gets subtracted from the total balance of the entire insurance pool on a prorated basis.

III.2.6 Peg Maintenance

Under most circumstances, bAssets and assets are exchanged one-to-one, with arbitrage opportunities preventing significant price deviation. However, slashing events with amounts beyond insurance coverage can cause this in-protocol peg to temporarily break, leading bAssets to be exchanged at a value below the original peg. In order to reinstate the peg to its pre-slash level, the protocol applies slippage to further mints and burns. Slippage profits are then used to increase the conversion rate on every trade. Redeeming bAssets has lower slippage than minting, minimizing additional loss to the value of bAssets.

The rate of slippage increases proportionally to the amount of deficit, and changes based on the following formula.

$$(slippageRate) = \left(1 - \frac{(depositedAssets)}{(bAssetSupply)}\right) \cdot (multiplier) \tag{1}$$

Therefore, at a bAsset supply of $\boldsymbol{S}$, a vanilla asset deposit of $\boldsymbol{D}$, and a multiplier value of $\boldsymbol{m}$, converting (minting and burning) $\boldsymbol{x}$ units of bAssets each follow the equations below:

$$assetsRequired(x) = \frac{S + x}{\left(\frac{S}{D} - 1\right)\left(\frac{S}{S+x}\right)^m + 1} - D \tag{2}$$

$$assetsGiven(x) = D - \frac{S - x}{\left(\frac{S}{D} - 1\right) \cdot \left(\frac{S-x}{S}\right)^m + 1} \tag{3}$$

IV Applications

The bAsset protocol provides liquidity to staking positions without harming the security of underlying blockchains. This allows several new types of applications to be developed on top of the protocol, with some possible examples listed below.

IV.1 A Primitive for Blockchain Finance

The utilization of bAssets offers the best of both staking and DeFi protocols. Users are able to take advantage of various financial applications without having to unstake their assets, improving capital utilization efficiency without compromising network security. As such, bAssets offer a diverse set of opportunities within both DeFi and PoS spaces.

IV.2 Price Volatility Hedging

A vanilla PoS protocol requires an unstaking period to redeem the underlying token for security reasons. Consequently, it lowers the incentive to stake due to price volatility risks during the unstaking period. bAssets allow staking participants to maintain their staking position in liquid form, enabling them to hedge their staked tokens effectively without time delays or fractional reserve staking.

IV.3 Leveraged Staking

With the addition of a money market built on top of bAssets, leveraging becomes possible. The money market is tweaked from traditional designs to share a portion of bAsset staking rewards with borrowers, who use bAssets as collateral to borrow stablecoins. Borrowers can then exchange borrowed stablecoins for more bAssets, increasing their exposure to the rate of staking rewards without needing to acquire additional capital. This incentivizes more tokens to be staked, increasing network security while growing network value with additional borrowed funds.

IV.4 Interchain Staking

A significant number of PoS validators and staking participants often support multiple networks at once. Similar to how bAssets allow staking leverages, a bAsset money market will allow staking participants to borrow stablecoins that can be converted to tokens on a different PoS blockchain. Thus, staking participants are able to stake in multiple chains at the same time without the need to acquire additional capital.

V Conclusion

In this paper, the authors have presented the bAsset protocol, a generalized protocol for creating liquid staking positions on PoS blockchains. bAssets are tokenized representations of a staking position, where holders of bAssets are eligible to claim the staking rewards generated by the underlying staking position. The bAsset protocol introduces a novel mechanism for incorporating liquidity in staking, enabling bAssets to become a primitive for blockchain finance. The protocol also opens applications such as hedging,

leveraged staking, and interchain staking. Through the introduction of the bAsset protocol, the authors believe that bAssets could pave the way for PoS networks to lay the foundation for the next financial ecosystem.

References

[1] Global Charts. (n.d.). Retrieved June 22, 2020, from https://www.stakingrewards.com/global-charts

[2] Binance Academy. (2019, September 30). *Decentralized Finance (DeFi) - Definition.* Retrieved June 22, 2020, from https://academy.binance.com/glossary/defi

[3] MakerDAO. "*The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System*" (**2020**). URL https://makerdao.com/en/whitepaper/

[4] H. Adams, N. Zinsmeister, D. Robinson. "*Uniswap v2 Core*" (**2020**). URL https://uniswap.org/whitepaper.pdf

[5] R. Leshner, G. Hayes. "*Compound: The Money Market Protocol*" (**2019**). URL https://compound.finance/documents/Compound.Whitepaper.pdf