An Efficient financial architecture for proof of stake blockchain infrastructure

Abstract

We propose a blockchain solution to financialize infrastructural assets for maximizing efficiency of consensus and boosting onchain application usage. We build a financial channel to turn on chain assets into flexible and tradable financial products. This paper compares the traditional financial product issues and the implications of staking assets in blockchain, examines the financial influence of staked assets on application usage. Through our financial channel, individuals can get mutual benefits from both staking rewards and the surplus generated from participation of onchain applications. Node operators can issue derivatives to sell staking assets with a time threshold. Thereby, this financial protocol allows users for the first time to earn significant premiums on staking and application at the same time. The issuance of underlying assets derivatives bring flexibility and financialization to the blockchain infrastructure.

Introduction

In City of capital, written by Bruce G. Carruthers, he compared the stock market to the engine of a nation. In just four decades, from 1672 to 1712, the United Kingdom developed from a country with middle-ranking economic and military power to one of the world leaders. This period also witnessed the growth and prosperity of the first stock exchange, London Stock Exchange. The primary purpose of the invention of the stock market was to transfer long-term treasury bonds to short-term profitable financial products. People activated this money-lending machine, which guaranteed financial support in the war. Following the same logic, proof of stake consensus was created to mitigate the drawbacks of proof of work. The total value of staked assets has increased from $741M to $4.7B with a total growth rate of 533%, and we expect it to increase further with new PoS networks emerging and existing blockchains migrating to PoS. However, proof of stake requires stakers to lock their assets on a chain for a certain amount of time, and it can't be linked to the secondary market which allows people to trade in the short term profitable financial markets.

All blockchains aim to create a database system that parties can jointly maintain and edit in a decentralized manner, with no individual party exercising central control. The decentralization of the operating system on blockchain affects agents' incentives and business practices in the economy. In a standard proof-of-stake system, the more people stake, the more tokens are taken out of circulation. This may seem good for the price of the token, but in many cases insufficient liquidity can get in the way of network growth.

Sufficient liquidity is necessary for capital to flow efficiently through a financial network. Illiquidity can act against demand because a relatively small increase in demand could cause a sharp increase in price, potentially to a point that exceeds the application utility buyer's maximum price preference. It can also affect the economics of the supply side by making it more expensive to exit the system if selling has too negative an effect on price. Movements in price due to buys and sells are called slippage, and too much of it is undesirable.

We intend to build a financial channel between protocol layer and application layer. Proof of stake token holders can deposit a native network coin into a staking contract and obtain a synthetic token which has equivalent value to the original network coin. With the synthetic token, a holder can trade in the secondary market and participate in onchain applications such as defi. While using the token freely, the holder essentially is claiming the staking reward from the underlying collateralized coin in the staking pool on the proof of stake chain. Conversely, for a node operator who is running a staking node with a large amount of staking assets, He can issue derivatives backed by his staked assets through staking auctions in our financial channel. The derivative is in the form of tokens and auction bidders can freely use the derivative tokens in applications or tradings.

Built on Polkadot, our financial channel lives on parachain and is developed by substrate and connected to parallel chains. The financial layer is an improved smart contract layer that integrates financial models. Running on polkadot blockchain, smart contracts can increase contractibility and facilitate the exchange of money and ownership of valuable things in a programmable and algorithmically automated way. Even in some situations where smart

contracts require the execution to be conducted by centralized parties, a decentralized consensus record reduces contracting and execution frictions. Smart contracts can improve contractibility and enforceability on certain contingencies.

Architecture

Staking derivative issuance:

We propose a staking auction mechanism where stakers can auction the staked assets and auction buyers can bid for a portion of the auction, which represents a portion of staked assets. Auction buyers can also participate in trenches to form staking backed derivatives. The governance will firstly verify the validity of staking parties and the amount of staked assets that are proposed to issue derivatives. The pricing of the derivative contracts are determined by issuers, but we have a framework to provide guidelines for issuers to set ask price. We first define features of staking contracts as follows:

Standard notations for each staking contract:

- Annual return rate in the staking: k%;
- Staking term: T;
- Time to maturity: τ;
- Contract size: C (without loss of generality, suppose $C = 1$);

- Current token price: S.

- Current value of the staking contract: $V = S * (1 + k\%)^{\tau/T}$.

If there are n contracts traded in the market, with all notations sub-labelled with i. Suppose $0 = \tau_0 < \tau_1 < \cdots < \tau_n$, then the (continuous-compounding) return rate of the token should be a piecewise constant r_i over time $[\tau_{i-1}], \tau_i)$. These return rates should satisfies

$$\begin{cases} e^{r_1 * \tau_1} = \frac{(1+k_1\%)^{\tau_1}}{V_1/S} \\ e^{r_1 * \tau_1} e^{r_2(\tau_2 - \tau_1)} = \frac{(1+k_2\%)^{\tau_2}}{V_1/S} \\ \vdots \\ e^{r_1 * \tau_1} e^{r_2(\tau_2 - \tau_1)} \cdots e^{r_n(\tau_n - \tau_{n-1})} = \frac{(1+k_n\%)^{\tau_n}}{V_n/S}. \end{cases} \quad (0.1)$$

So we have

$$\begin{cases} r_1 = \frac{1}{\tau_1}[\tau_1 \ln(1 + k_1\%) - \ln(V_1/S)] = \ln(1 + k_1\%) - \frac{\ln(V_1/S)}{\tau_1} \\ r_2 = \frac{1}{\tau_2 - \tau_1}[\tau_2 * \ln(1 + k_2\%) - \tau_1 * \ln(1 + k_1\%) - \ln(V_2/V_1)] \\ \vdots \\ r_n = \frac{1}{\tau_n - \tau_{n-1}}[\tau_n * \ln(1 + k_n\%) - \tau_{n-1} * \ln(1 + k_{n-1}\%) - \ln(V_n/V_{n-1})] \end{cases} \quad (0.2)$$

Now if we want to evaluate an staking contract with time to maturity and return rate k% then its value should be:

$$\begin{aligned} V &= e^{r_1 * \tau_1} e^{r_2(\tau_2 - \tau_1)} \cdots e^{r_i(\tau_i - \tau_{i-1})} e^{r_{i+1}(\tau - \tau_i)} \\ &= \frac{(1+k_i)^{\tau_i}}{V_i/S} * \left(e^{r_{i+1}(\tau_{i+1} - \tau_i)}\right)^{\frac{\tau - \tau_i}{\tau_{i+1} - \tau_i}} \\ &= \frac{(1+k_i)^{\tau_i}}{V_i/S} * \left(\frac{(1+k_{i+1})^{\tau_{i+1}}}{V_{i+1}/S} / \frac{(1+k_i)^{\tau_i}}{V_i/S}\right)^{\frac{\tau - \tau_i}{\tau_{i+1} - \tau_i}} \\ &= \frac{(1+k_i)^{\tau_i}}{V_i/S} * \left(\frac{(1+k_{i+1})^{\tau_{i+1}}}{(1+k_i)^{\tau_i}} \frac{V_i}{V_{i+1}}\right)^{\frac{\tau - \tau_i}{\tau_{i+1} - \tau_i}} \end{aligned}$$

With this pricing guidance, the issuer can evaluate the present price of their derivatives and open auction sale of staked assets.

Staking ETFs:

We also create a basket construction for staking rewards and it provides the easiest way to go long on the best proof of stake protocols. By holding one token, a holder can get exposure to the best return staking assets. The universal of potential PoS assets considered for inclusion into the basket are filtered based on market cap and daily volume. Assets are then ranked through factors such as staking ratio and reward ratio. Then our token basket consists of the top three tokens, market cap weighted and rebalanced monthly.

Consensus and protocols:

We use Polkadot based Proof of Stake consensus algorithm, which is a hybrid consensus model that separates block production from the final determination of the block. Our network has multiple types of nodes: diligence nodes, mining nodes, and Stake proxy nodes. Diligence nodes have the right to vote and recharge channels in addition to block generation. Also they will become block generation nodes when they meet the threshold of votes. The mining node generates blocks and are more appealing to votes. The Stake agent node is elected by the block generating node. Diligence nodes, mining nodes, and Stake proxy nodes must have the same network access environment and computing capabilities. Although Diligence nodes do not need to produce blocks, it is necessary to build real nodes to send heartbeat transactions. Nodes' block

production, missing blocks, dropped or other malicious behaviors will be punished. At the same time, the node's self-mortgage and the user's waiting for reward will be deducted. Stake agent nodes will get additional Stake revenue and violate the terms of the revenue contract and will be punished accordingly. The punishment funds will be transferred to the parliamentary fund, and a subsequent referendum will decide how to deal with it.

Node registration and application are open to all users. After the node server is set up, you can start running. We use a one-vote, one-vote model to prevent node conspiracy. All users can use BNC for node voting elections. The synchronization node and the block producer node need to pay the same cost to ensure the stable operation of the network, so the synchronization node and the block producer node will get the same benefits. The Stake agent node will be an important part of our multi-chain ecosystem, responsible for the production of the Stake income of our ecosystem. In addition to the block node's income, the Stake agent node will also receive the dividends generated by our Stake.

As an important part of our chain, the runtime environment is more low-level than smart contracts. The runtime environment consists of various runtime modules. The runtime modules include modules such as accounts, balances, staking, smart contracts, transition bridges, governance, and consensus. Modules can be independent of each other, while allowing modules to call each other. Most of the code logic of the chain runs in the runtime environment.

The runtime environment allows each runtime module to be upgraded independently, while an important feature of it is that there is no hard fork upgrade. When the existing blockchain system is upgraded, due to the inconsistent running versions of each node, there is a

risk of causing a hard fork of the entire chain, which seriously affects the healthy development of the entire ecosystem and the interests of nodes and users. We generate two versions each time the module is upgraded: Native and WASM. When the runtime environment determines that the version of the updated module is consistent with the current Native version, run the Native version code directly to get the fastest operating efficiency.

The assets locked by the user in the main chain through the cross-chain are multi-signed by the escrow contract, and the escrow contract is jointly managed by multiple witness nodes. Through the decentralized governance mechanism, the witness nodes are elected by the participants according to the voting share, and are rotated regularly. At the same time, when the assets held by the main chain escrow contract are too large, they can be split into multiple escrow contracts, and more trust node groups are introduced for custody to improve overall security.

Insurance and security:

By depositing our platform tokens, and specifying certain key parameters (e.g. underlying asset, strike price, expiry date, etc.), options writers are able to mint arbitrary fungible option tokens called oTokens. Selling those minted Tokens allows writers to earn premiums, thereby generating revenue on their collateral. Buyers can then purchase these oTokens, which trade on exchanges such as 0x or Uniswap, ensuring market liquidity. Beyond the primitive of fungible, freely tradable ERC20 option contracts enabled by this framework, in particular focusing on protective put strategies for deposit insurance (e.g. protecting users of tokenized money markets like Compound against hacks and liquidity crises), as well as protection against stablecoins like DAI crashing in value. We also consider cases wherein option sellers wishing to offer protection

can do so using a collateral type (such as ETH) which is different than the asset (such as USD) in which the strike price is denominated.

Financial Auditing:

The auditors' technology adoption exhibits strategic complementarity because the cost of auditing cross-auditor transactions decreases when more auditors adopt. When clients strongly value the benefit of misreporting even after taking into consideration the possibility of being detected, they would prefer to work with auditors not using blockchain, notwith- standing that the auditor using blockchain can offer a lower auditing fee. Consequently, when other auditors are not adopting, an auditor would not find it profitable to adopt because adoption would not only fail to attract more clients, but also could result in losing clients that the auditor would get with traditional auditing. Overall, three technological features of blockchain are conducive to the auditing process: (i) decentralization: the peer-to-peer design of blockchain eliminates the requirement of a trusted central party; (ii) encryption: the zero-knowledge proof method allows encrypted communication that preserves data privacy; (iii) immutability: once auditors request infor- mation through the federated blockchain, it is difficult for any auditors or outside hackers to intentionally revise or delete the information, unless they can revise information on a majority of nodes on the federated blockchain. We will build a decentralized financial auditing system to monitor the after auction activity of stakers who participate in the staking auction.

Economics

We have a native token for our financial channel. It serves to capture onchain value for our channel. The main functionalities of our tokens are as follows:

Services: We propose a token-locking reward model, which enables users to reward our protocol contributors by locking tokens, without needing to sacrifice their tokens. This process is similar to locking tokens: the principle is locked in a pool by a franchisee based on terms signed. Derivative issuers must negotiate a term, in terms of tokens needed and time length, allowing our financial channel to service as a public record of their agreement. Once terms have been established, the derivative issuer writes a transaction to the blockchain with the terms of their agreement. We refer to this transaction as the agreement transaction. Derivative issuers need to stake a certain amount of platform tokens to get permission for doing an auction.

ETF Issuance: we will allocate a pool of platform tokens to issue staking ETFs. Our newly issued token tracks a transparent, algorithmically managed basket of proof of stake assets. Rewards generated by the underlying assets tracked by our newly issued tokens are used to repurchase and burn.

Insurance: The concept of insurance comes from communities in the past who pooled their resources to protect each other from the risks they all faced. We realised we could build a mutual on a platform where individuals only need to trust the system, not everyone in it. The aim is to provide our members with more simple, transparent, accessible and cheaper financial protection against their risks. Our platform token will have a pool of insurance funds which

secure the onchain activities. We have staking derivative cover and it provides stakers and bidders against hacks in the value storing.

Buy back and burn: We will generate fee revenues from transactions and services in the operation of financial channels. All the revenue will be used to purchase back tokens and we will burn them as the benefit to all token holders.