EPOTTER | HASHKEY GROUP

EPotter Litepaper

A Leading
Liquid Node Validation Solution

Presented by the EPotter Team

21 September 2022

01 Proof-of-Stake

What is Proof-of-Stake?

Proof-of-Stake ("**PoS**") is one of the common consensus mechanisms used for blockchain networks. PoS blockchains motivate network participants to maintain the security and operation of an entire blockchain network with native crypto assets. Network participants need to commit their crypto assets as collateral to participate in the consensus process of the blockchain network through validator nodes. The collateral as a good-faith commitment will prevent validators from maliciously or irresponsibly processing transaction validation. In return, network participants will receive native crypto assets as node validation rewards.

In a PoS blockchain, validators are responsible for validating transactions, communicating between validator nodes, as well as maintaining and updating the blockchain ledger. Network participants can choose a trustworthy validator to which they will delegate their crypto assets, participate in the consensus process and receive node validation rewards in return. The amount of rewards depends on various factors, such as the issuance rate of the blockchain network, the total amount of assets participating in node validation, the performance of that validation node, and the validation service fee.

As of September 2022, there were approximately 100 PoS blockchains in the market with the total market value exceeding US$25 billion. The mainstream PoS blockchains include Cosmos, Polkadot, Tezos, Solana and NEAR. With the world's second largest blockchain network, Ethereum, upgraded to a PoS consensus mechanism ("**Ethereum 2.0 Upgrade**"), the market value of PoS blockchains has grown exponentially.

Why PoS?

PoS aims to solve the pain points of the Proof-of-Work ("**PoW**") consensus mechanism including slow transaction speeds and excessive energy consumption, reduce the network security cost and achieve a higher degree of decentralization.

PoS has the following advantages over PoW:

I. **Environmentally-friendly**

PoS network participants do not need to compete to solve the complex cryptographic puzzles using computational power, thus significantly reducing energy consumption.

II. **Low barrier to entry and more decentralized**

PoW blockchains require specialized hardware and chips for mining while PoS blockchains have lower technical requirements. This allows more validators to participate in PoS blockchains and achieve a higher degree of decentralization.

III. **Faster transactions**

PoS blockchains allow more validators to participate in the consensus process, hence increasing the transaction speed.

IV. **Lower network security cost**

In a PoW blockchain, miners usually bear a high operating cost due to the specialized technical requirement and they need higher mining rewards to cover the operating cost. While PoS blockchains have lower technical requirement, hence, the operating cost for validators are lower, implying lower network security costs.

02 Liquid Node Validation

Despite PoS blockchains having the above advantages over PoW blockchains, PoS blockchains still have some pain points. One of the most significant pain points is that there is no liquidity for delegated assets during the period of delegation. Moreover, most PoS blockchains have an unbonding period during which validators choose to exit the transaction validation process. For example, Polkadot has a 28-day unbonding period during which network participants will not receive node validation rewards. This means that the delegated assets cannot be traded or used for other financial activities during the unbonding period, which produces opportunity costs for network participants.

The pain points of PoS blockchains have led to a new business model - Liquid Node Validation.

What is Liquid Node Validation?

Liquid node validation will generate a liquid representation of the delegated assets ("**Liquid Node Validation Tokens**") on the blockchain network through on-chain protocols. The holders of Liquid Node Validation Tokens can continue to participate in node validation and earn rewards. In the meantime, Liquid Node Validation Tokens can be freely traded on the blockchain network, which allows network participants to enjoy the liquidity of delegated assets and participate in other financial activities with Liquid Node Validation Tokens to achieve additional rewards.

Market Landscape

There are two types of liquid node validation solutions in the market - non-custodial and custodial. Non-custodial solutions will use on-chain protocols (usually smart contracts) to generate Liquid Node Validation Tokens and manage the node validation process. Users' assets are managed in a trustless manner as all operations will be executed via protocols. All asset flows and relevant transaction data will be transparently recorded on-chain. On the other hand, custodial solutions are usually operated by institutions (usually centralized exchanges). They manage the node validation process and the generation of liquid node validation tokens in a centralized manner, hence, all asset flows and relevant transaction data are opaque.

Although there are already some liquid node validation solutions available in the market, there is still a great deal of room for liquid node validation to grow because the adoption of PoS blockchains is expected to continue to increase exponentially. Furthermore, not all liquid node validation solutions available in the current market

comply with the necessary regulatory regimes. This poses significant risks to network participants.

Fully decentralized liquid node validation solutions entirely rely on on-chain protocols and decentralized autonomous organization ("**DAO**") governance to manage users' assets and govern the operations of the project. However, when incidents occur in the context of a fully decentralized liquid node validation solution (e.g. bugs identified on the smart contracts), the DAO members have no obligation or responsibility to respond to such incidents. The DAO members can sell their DAO governance tokens and thus withdraw themselves from the DAO's governance.

The custodial solutions do not have transparent asset flows and it is not clear whether the service providers and the products are regulated. The liquid node validation tokens are not protected if the service provider loses the private keys, the wallets are hacked, the tokens are used inappropriately or the service provider behaves inappropriately.

To conclude, the HashKey Group considers that there is currently no decentralized Asia-based liquid node validation solution.

The Importance of Compliant Products

Decentralization, transparency, and trustlessness are the core value propositions of blockchain technology. The innovation of blockchain is undeniable, but the lack of regulation may pose various potential risks. It is not uncommon for projects to make money and then cease operations. Hence, compliance and regulation must be the future direction for industry development. Although regulators are trying to understand, learn about, and accept, this emerging technology, there is still a long way to go before achieving a balance between the blockchain development and compliance. There are very few fully institutional-level investment-grade liquid node validation products available in the current market. It is thus essential to provide a liquid node validation solution for the market.

03 EPotter

As PoS blockchains continue to grow, and the world's second largest blockchain network, Ethereum, has upgraded to PoS consensus mechanism, the HashKey Group would like to introduce a new liquid node validation solution to the market called EPotter.

Ethereum 2.0 Background

Since launch, the Ethereum blockchain has implemented a series of technology innovations, such as Ethereum Virtual Machine and smart contracts. These innovations have driven the rapid development of decentralized applications on the Ethereum blockchain. However, the PoW consensus mechanism results in the Ethereum blockchain having limited scalability. Hence, to enhance the scalability, the Ethereum blockchain officially launched the Ethereum 2.0 Upgrade in October 2020, which includes the transition to a new PoS consensus mechanism and sharding.

The Ethereum 2.0 Upgrade will enable:

- more participation to be introduced to the network through node validation, thus guaranteeing higher security;
- faster transaction speeds and higher network capacity; and
- more environmentally-friendly and sustainable transaction processing.

However, the Ethereum 2.0 Upgrade will be implemented in several phases.

Beacon Chain: The Beacon Chain is the new PoS consensus layer and was officially implemented in October 2020. Each validation node represents 32 ETH delegated to the Beacon Chain. The Ethereum PoW blockchain (Ethereum mainnet) will run parallel to the Beacon Chain in this phase to ensure data continuity.

The Merge: The original Ethereum mainnet has been merged with the Beacon Chain (the "**Merge**"). This has resulted in the PoW consensus mechanism being fully replaced with the PoS consensus mechanism.

The Merge was completed in September 2022. However, the transfer/withdrawal function of Ethereum 2.0 will be gradually open after the Merge. This is expected to be complete 6-12 months after the Merge.

Shard Chains: Shard chains will give the Ethereum blockchain more ability to store and access data. These are expected to be operational by the end of 2022.

With the Ethereum 2.0 Upgrade, it is expected that more ETH holders will participate in node validation to earn rewards. However, to participate in Ethereum node validation, ETH holders need to delegate at least 32 ETH and commit the technological and administrative resources to operate a validation node on the network. A user will not be able to undelegated delegated ETH or access accreted node validation rewards until the transfer/withdrawal function has been activated. This will only be done when the Shanghai Upgrade phase of the Merge has been completed.

If users choose to participate in Ethereum node valiation before the Ethereum 2.0 Upgrade is fully complete, their ETH have been delegated and cannot be used to participate in other financial activities such as liquidity mining, primary market investment, and lockdrops to achieve additional rewards. This leads to opportunity cost for ETH tokenholders and could make them reluctant to participate in Ethereum node validation at an early stage.

Moreover, liquidity will be an issue both before the Ethereum 2.0 Upgrade is complete but also during the unbonding period for most mainstream PoS blockchains.

In addition to the liquidity issue mentioned above, there is also an onerous technical requirement to participate in node validation. There will be penalties if the validation nodes are inactive or compromised. Therefore, professional validation services are needed for mainstream users to participate in the transaction validation process.

04 EPotter Introduction

Background

After years of operations, the EPotter team has accumulated extensive technical experience and insights with respect to blockchain technology development. EPotter has strong confidence in the Ethereum 2.0 Upgrade and is eager to provide support for Ethereum node validation and the Upgrade.

EPotter aims to solve the liquidity issue and high entry barriers for ETH holders in order to support the growth of Ethereum node validation. In the future, the ultimate goal of EPotter is to provide a liquid node validation solution for the mainstream PoS blockchains through leveraging the HashKey Group's ecosystem.

EPotter is responsible for developing, deploying, and maintaining the underlying protocols for Liquid Node Validation Tokens. Through EPotter, ETH holders can participate in node validation of the mainstream PoS blockchains in a regulated environment with professional validation service providers operating the validation nodes on behalf of users. Users can earn node validation rewards, and in the meantime, free up the liquidity of delegated assets and participate in other financial activities through Liquid Node Validation Tokens.

Purpose

EPotter will provide users with a transparent and secure liquid node validation solution with the following aims:

- providing a new method for decentralized liquid node validation solution offered to the market;
- facilitating traditional institutions to enter the blockchain world via EPotter's secure and convenient services;
- compatibility for mainstream PoS blockchains and helping users to maximize their capital efficiency;
- achieving 100% coverage for the potential slashing penalties to protect users' interests; and
- bridging the gap between compliance and blockchain technology development.

05 Project Design

Protocol Architecture

EPotter's liquid node validation solution aims to automate the node validation process and achieve transparency of asset flow through smart contracts. All relevant data is recorded on the blockchain, and the asset flows can be traced. The transparency of the node validation process is guaranteed by both technical and regulatory means to ensure users' assets will not be inappropriately used.

Users who have passed Know-Your-Client ("**KYC**") checks are allowed to interact with the EPotter smart contract. On behalf of users, the EPotter Smart Contract will interact with the PoS blockchain node validation contracts (e.g. Ethereum Deposit Contract), deposit users' native crypto assets to participate in node validation and assign the assets to validators.

Once the assets have been confirmed to participate in node validation, the EPotter Smart Contract will generate the corresponding Liquid Node Validation Tokens ("**epTokens**") based on the Conversion Rate (defined below). epTokens are liquid representations of users' delegated tokens, which allows users to participate in node validation and earn corresponding rewards, and in the meantime, enjoy the liquidity of delegated assets. The value of epTokens reflect the delegated assets and accreted node validation rewards. Users can hold or trade epTokens, or use epTokens to participate in other financial activities. Throughout the node validation process, EPotter does not take control of users' assets. All asset flows and relevant data are transparent on-chain.

There are two main components of EPotter's protocol architecture - the EPotter Smart Contract and the Validator Service.

- EPotter Smart Contract - built on top of the underlying PoS blockchain protocol. Functions include executing the interaction between users and the PoS blockchain node validation contracts (e.g. Ethereum Deposit Contract), the generation of epTokens and the calculation of the Conversion Rate.
- Validator Service – The assigned validators will run the transaction validation process on behalf of users.

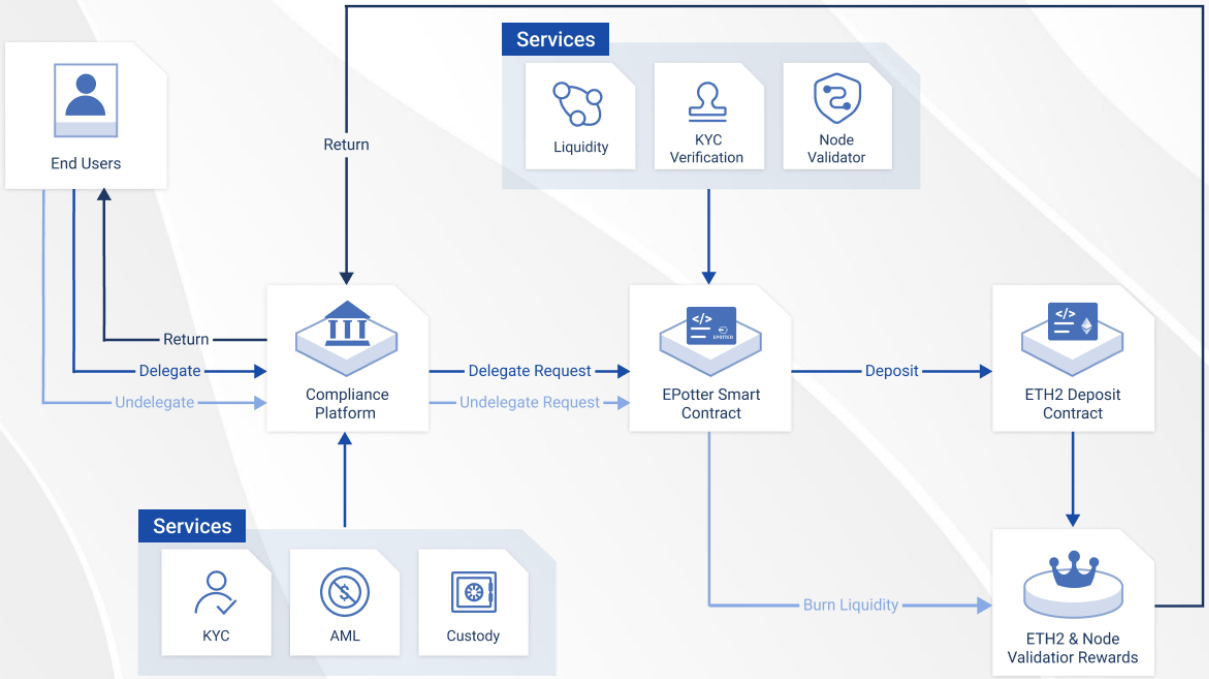

Figure 1: Product Architecture

EPotter Smart Contract

The EPotter Smart Contract contains a number of subcontracts such as enabling users to delegate native crypto assets for node validation, generating the corresponding epTokens, assigning their delegated assets to validators to run the transaction validation process and handling all necessary interactions with the PoS blockchain node validation contracts.

Subcontracts of the EPotter Smart Contract include:

- **epToken contract**: ERC20 Token contract for epTokens;
- **Swap contract**: EPotter core contract, responsible for the generation and destruction of epTokens, interaction with the PoS blockchain node validation contracts and validation node activation; and
- **KeyRegistry contract**: The information in relation to validation nodes is registered on-chain to ensure that it is transparent.

EPotter Smart Contracts are upgradeable, which allows for product iterations in the future. Although all contracts developed by EPotter will be audited before going live, it is still impossible to completely avoid the potential problems that may occur during operation. Therefore, the upgradable feature of EPotter Smart Contract ensures that the smart contracts can be updated in time when identifying any problems.

When assigning users' delegated assets to validators, the EPotter Smart Contract will automatically check the validators' status to ensure that the validation nodes are operated properly and are generating node validation rewards in order to maximise the value of epTokens.

All EPotter Smart Contracts will be audited by professional independent security auditor Xiamen SlowMist Technology Co., Ltd. to ensure security. The audit report will be disclosed to the public separately.

Validator Service

Stable transaction validation performance is crucial to secure users' assets and maximise the node validation rewards. EPotter will select reliable validators within the HashKey Group's ecosystem to provide transaction validation services with 100% coverage of any potential slashing penalties. This ensures that validators will strive to provide reliable transaction validation services to ensure the security of users' assets and minimize the potential slashing risks.

The validation keys related to validation nodes are generated by validators and submitted to the EPotter network. The EPotter Smart Contract will automatically assign validation nodes on behalf of users. Note that as the node validation requirements of PoS blockchains may vary, EPotter may adjust the product design based on their requirements.

For Ethereum node validation, withdrawal credentials are required to free up delegated assets and node validation rewards. The withdrawal credentials will be custodied by EPotter's licensed custodian partner. This means neither EPotter nor the validators have access to users' funds.

06 epToken Tokenomics

Benefits and Use Cases

The delegated assets on PoS blockchains are illiquid during the period when these are being delegated. Moreover, PoS blockchains such as Polkadot have a 28-day unbonding period. Ethereum does not allow withdrawal of delegated assets before the completion of the Ethereum 2.0 Upgrade. With EPotter, users can freely trade epTokens for their native crypto assets via secondary markets. Also, epTokens are compatible with the underlying blockchains. Hence, there could be a variety of use cases for epTokens in the future, such as lending or liquidity mining.

EPotter will first deploy its liquid node validation solution on Ethereum. Once the transfer/withdrawal functions of Ethereum 2.0 are available, the EPotter Smart Contract will be upgraded to allow users to unlock the delegated ETH and accreted node validation rewards using epTokens.

Node Validation Reward Calculation

When users delegate their native crypto assets on PoS blockchains and participate in node validation through EPotter, users will receive corresponding amount of epTokens at a Conversion Rate, which is calculated as follows:

$$Conversion\ Rate = \frac{Total\ Native\ Tokens\ delegated\ via\ EPotter + (Accreted\ Validation\ Rewards - Validation\ Service\ Fee)}{Total\ EPotter\ Liquid\ Node\ Validation\ Tokens\ Generated}$$

The Conversion Rate is updated every hour on the hour (Singapore time) via Oracle.

The epToken holders will earn node validation rewards through the increase of the epToken value. Therefore, the value of 1 epToken will always be greater than or equal to the value of 1 native token.

Fee Composition

Node Validation rewards are recorded and calculated by EPotter Smart Contract based on all validation nodes operated via EPotter and then reflected in the value of epTokens through Oracle. EPotter will receive 10% of all node validation rewards as a validation service fee and the remaining 90% will be paid to users.

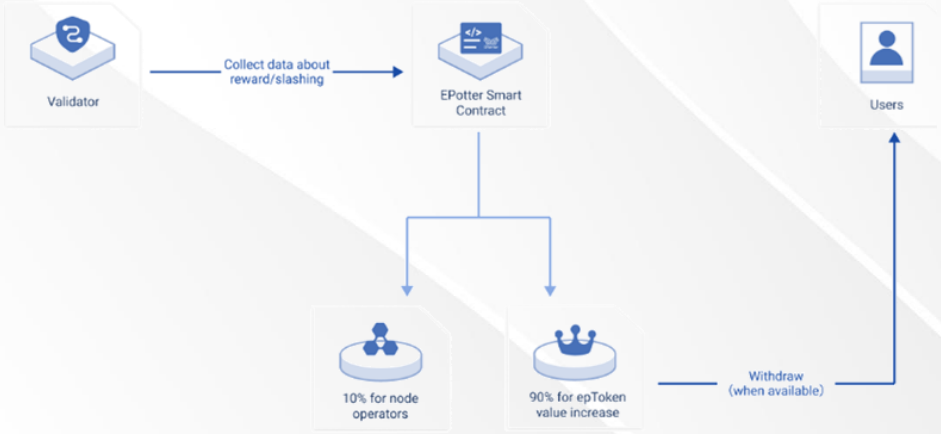

Figure 2: Fee allocation

07 Why EPotter

There are two types of liquid node validation solutions in the market - non-custodial and custodial. The non-custodial solutions are mainly operated as a decentralized project with DAO governance. The custodial solutions are mainly operated by centralized exchanges, however, most of them are not qualified to operate in a compliant manner, and do not transparently disclose the product-related information, which may pose a potential capital security risk.

EPotter has therefore fully considered the potential compliance and security issues and developed a liquid node validation solution for qualified investors.

The product design strictly complies with compliance requirements. EPotter, as a technical service provider for liquid node validation solutions, works with **independent law firms** to ensure that it operates in a legal manner. In addition, EPotter will work with licensed and regulated entities within the HashKey Group to provide safe and secure services such as custody services for users. On-chain smart contracts will also provide more transparency with respect to epTokens.

In addition, the epToken economic model focuses on value accumulation instead of balance growth. This means the node validation rewards earned by users do not increase the epToken balance. Instead, the value of epTokens will reflect the accumulation of node validation rewards. Compared with the balance growth model, when there are new node validation rewards, EPotter's users do not need to convert the node validation rewards into new epTokens and re-engage in other financial activities, which reduces transaction costs.

The product design is compatible with the mainstream PoS blockchains. EPotter will first deploy the liquid node validation solution on the Ethereum blockchain. In due course EPotter will expand the liquid node validation solutions to other mainstream PoS blockchains such as Cosmos, Polkadot, and Tezos.

08 Potential Risks

There are several potential risks in respect of epTokens and users should be aware of these potential risks before investing in them.

Smart Contract Security Risk

Despite EPotter Smart Contract being audited by a third-party auditor, there is no guarantee that the smart contracts will be vulnerability-free. Any code vulnerabilities or bugs could cause an entire smart contract or part of it to fail.

Ethereum 2.0 Upgrade Risk

The EPotter Smart Contract is built on the Ethereum blockchain, while Ethereum 2.0 is still under development and has not yet been fully upgraded. There is no guarantee that the Ethereum blockchain is error-free. Any problems associated with the Ethereum blockchain infrastructure could impact EPotter Smart Contract, lead to validator slashings and affect the epETH tokens' value. In addition, the adoption of Ethereum node validation may impact the node validation yield.

Private Key Management Risk

If a user deposits the epTokens in that user's self-custody wallet and loses that wallet's private key, the user will lose access to the epTokens and not be able to claim their delegated assets and node validation rewards. In this case, EPotter will not be responsible for the user's loss.

The private keys associated with the assets delegated by users via EPotter will be custodied by professional third-party custodians. EPotter has conducted rigorous background checks on, and technical reviews in respect of, them, however, the custodians might lose the private keys or be hacked, which may result in the loss of users' funds.

Validator Slashing Risk

Despite EPotter having strict criteria for validator selection, slashing events might still occur. To mitigate this risk, EPotter will offer a fully covered solution, which means EPotter will compensate users if any slashing events occur.

epToken Price Risk

A security auditor has been engaged to ensure that the epToken price is correctly calculated by the EPotter Smart Contract. However, the Conversion Rate might still deviate from the fair value depending on the market demand for epTokens.

Legal and Compliance Risk

As an emerging industry, future regulation of digital assets and blockchain technology is unpredictable. In the future, EPotter might be subject to oversight and scrutiny by regulators. EPotter will strive to meet compliance requirements to the maximum extent. In the event of policy changes, EPotter might be required by regulators to adjust the business model of its products, which might incur additional legal and operational costs. In the extreme scenario, regulators might request EPotter to cease operations.

Tax Risk

The taxation mechanisms on digital assets in various countries and regions are unclear. There may be taxation issues incurred through buying/selling/holding tokens and making profits from token trading.


EPOTTER | HASHKEY
GROUP