WEB3 SHIELD

Building the Insurance Layer for Web3!

WHITEPAPER

Last Updated - 31st March, 2025

www.web3shield.com

Notice and Disclaimer

PLEASE READ THE ENTIRETY OF THIS "NOTICE AND DISCLAIMER" SECTION CAREFULLY. NOTHING HEREIN CONSTITUTES LEGAL, FINANCIAL, BUSINESS OR TAX ADVICE AND YOU SHOULD CONSULT YOUR OWN LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S) BEFORE ENGAGING IN ANY ACTIVITY INCONNECTION HEREWITH. NEITHER WEB3SHIELD INC. (THE COMPANY), ANY OF THE PROJECT TEAM MEMBERS (THE WEB3SHIELD TEAM) WHO HAVE WORKED ON THE WEB3SHIELD ECOSYSTEM (AS DEFINED HEREIN) OR PROJECT TO DEVELOP THE WEB3SHIELD ECOSYSTEM IN ANY WAY WHATSOEVER, ANY DISTRIBUTOR/ VENDOR OF $SHLD TOKENS (THE DISTRIBUTOR), NOR ANY SERVICE PROVIDER SHALL BE LIABLE FOR ANY KIND OF DIRECT OR INDIRECT DAMAGE OR LOSS WHATSOEVER WHICH YOU MAY SUFFER IN CONNECTION WITH ACCESSING THIS WHITEPAPER, THE WEBSITE AT HTTPS://WEB3SHIELD.COM/ (THE WEBSITE) OR ANY OTHER WEBSITES OR MATERIALS PUBLISHED BY THE COMPANY.

Project purpose: You agree that you are acquiring $SHLD to participate in the Web3Shield ecosystem and to obtain services on the ecosystem thereon. The Company, the Distributor and their respective affiliates would develop and contribute to the underlying source code for the Web3Shield ecosystem. The Company is acting solely as an arms' length third party in relation to the $SHLD distribution, and not in the capacity as a financial advisor or fiduciary of any person with regard to the distribution of $SHLD.

Nature of the Whitepaper: The Whitepaper and the Website are intended for general informational purposes only and do not constitute a prospectus, an offer document, an offer of securities, a solicitation for investment, or any offer to sell any product, item, or asset (whether digital or otherwise). The information herein may not be exhaustive and does not imply any element of a contractual relationship. There is no assurance as to the accuracy or completeness of such information and no representation, warranty or undertaking is or purported to be provided as to the accuracy or completeness of such information. Where the Whitepaper or the Website includes information that has been obtained from third party sources, the Company, the Distributor, their respective affiliates and/or the Web3Shield team have not independently verified the accuracy or completeness of such information. Further, you acknowledge that circumstances may change and that the
Whitepaper or the Website may become outdated as a result; and neither the Company nor the Distributor is under any obligation to update or correct this document in connection therewith.

Token Documentation: Nothing in the Whitepaper or the Website constitutes any offer by the Company, the Distributor, or the Web3Shield team to sell any $SHLD (as defined herein) nor shall it or any part of it nor the fact of its presentation form the basis of, or be relied upon in connection with, any contract or investment decision. Nothing contained in the Whitepaper or the Website is or may be relied upon as a promise, representation or undertaking as to the future performance of the Web3Shield ecosystem. The agreement between the Distributor (or any third party) and you, in relation to any distribution or transfer of $SHLD, is to be governed only by the separate terms and conditions of such agreement.

The information set out in the Whitepaper and the Website is for community discussion only and is not legally binding. No person is bound to enter into any contract or binding legal commitment in relation to the acquisition of $SHLD, and no digital asset or other form of payment is to be accepted on the basis of the Whitepaper or the Website. The agreement for distribution of $SHLD and/or continued holding of $SHLD shall be governed by a separate set of Terms and Conditions or Token Distribution Agreement (as the case may be) setting out the terms of such distribution and/or continued holding of $SHLD (the Terms and Conditions), which shall be separately provided to you or made available on the Website. The Terms and Conditions must be read together with the Whitepaper. In the event of any inconsistencies between the Terms and Conditions and the Whitepaper or the Website, the Terms and Conditions shall prevail.

$SHLD token: In particular, it is highlighted that $SHLD:

(a) does not have any tangible or physical manifestation, and does not have any intrinsic value (nor does any person make any representation or give any commitment as to its value);

(b) is non-refundable and cannot be exchanged for cash (or its equivalent value in any other digital asset) or any payment obligation by the Company, the Distributor or any of their respective affiliates;

(c) does not represent or confer on the token holder any right of any form with respect to the Company, the Distributor (or any of their respective affiliates), or its revenues or assets, including without limitation any right to receive future dividends, revenue, shares, ownership right or stake, share or security, any voting, distribution, redemption, liquidation, proprietary (including all forms of intellectual property or licence rights), right to receive accounts, financial statements or other financial data, the right to requisition or participate in shareholder meetings, the right to nominate a director, or other financial or legal rights or equivalent rights, or intellectual property rights or any other form of participation in or relating to the Web3Shield ecosystem, the Company, the Distributor and/or their service providers;

(d) is not intended to represent any rights under a contract for differences or under any other contract the purpose or pretended purpose of which is to secure a profit or avoid a loss;

(e) is not intended to be a representation of money (including electronic money), security, commodity, bond, debt instrument, unit in a collective investment scheme or any other kind of financial instrument or investment;

(f) is not a loan to the Company, the Distributor or any of their respective affiliates, is not intended to represent a debt owed by the Company, the Distributor or any of their respective affiliates, and there is no expectation of profit; and

(g) does not provide the token holder with any ownership or other interest in the Company, the Distributor or any of their respective affiliates.

“ **Insurance** is the safety net for
decentralized dreams of Web3 ”

Web3Shield Economy Assumptions

With any industry as vast as 7 trillion dollars, innovation can not only transform and strengthen it but even make it future proof for challenges ahead. That's the story of the insurance industry with more than 12% CAGR (Compound Annual Growth Rate) projected for the next 3 years. However, most of insurance use-cases are kept orthodox and limited to a small set of verticals including life, health, vehicle, etc, hence, highly increasing the growth possibilities for innovation and expansion among new areas and verticals and specifically into web3.

Web3Shield Foundation, a One-Click Insurance provider for web3 is launching their $SHLD token in order to bring the much needed innovation in the Insurance industry and extending trusted insurance protocols and processes to web3 and crypto space. The $SHLD Token working as a unified token can work in different insurance protocols that are associated with the Web3Shield Ecosystem, currently being used in the genesis protocols & native ecosystem products :

- **EigenShield** : EigenLayer Restaking Insurance
- **BridgeShield** : Cross-Chain Insurance Protocol
- **BaseShield, SUIShield, TONShield** and other ecosystem native products

Product Suite

The $SHLD Token is built as a unique insurance utility token to be used for the entire Web3Shield suite of products and insurance protocols, which you can use to pay insurance premiums, buy advance policies, claim payouts, staking and validation of the system, governance, etc.

The Benefits

End Users/ Retail Users

1. Whenever end users are using a specific EigenLayer operator, Crypto Bridge, DApp, web3 protocol, or interact with any smart contract, they can opt-in for the One-Click Insurance by Web3Shield in order to insure their funds and wallets against slashing, hacks, exploits, technical faults, protocol issues, etc. They get to pay this insurance premium amount either in the token that they are paying gas fee in (mostly stable coins or chain native tokens) or they can pay the insurance premium via $SHLD token and they will be given a x% discount for premium payment or any other added incentives. So, if you have want to pay $10 as the insurance premium, when you put $SHLD token in the picture, you they will give you the $10 worth benefit, along with a x% cashback point in $SHLD Token.

2. On top of that, there are also additional incentives given in $SHLD Token for better engagement with the insurance protocols. Meaning, if some users are spending a significant amount of $SHLD tokens for premiums, they are eligible for loyalty rewards which will be given in $SHLD Tokens governed by the protocol automatically via airdrop or DTT or Direct Token Transfer. These tokens can be used to pay additional premium fee or buy more game policies or they can convert the same into fiat from their wallet and use it as per their requirement.

3. Thirdly, the $SHLD tokens can be used as a lock up token to stake (provide cover) to the protocol and earn rewards/APRs against the risk coverage provided. For example, the end users can play the role of reinsurer by holding/staking/locking their $SHLD tokens that will yield them reinsurer rewards, which in-turn can be used to pay for insurance premiums. This gives the user a freemium insurance model experience and helps them keep hodling their $SHLD tokens in future.

4. Lastly, a certain percentage of the total revenue done by web3shield by selling insurance policies, will go in buying back the $SHLD tokens back from the open market and burning them, hence creating a deflationary token model. Meaning, with increased product usage, revenue will increase and more tokens will keep on buring, hence the price of the token is organically increased with the product usage.

Business Partners/ B2B Users

Whenever a new web3 project joins web3shield ecosystem, they either have to operate on a revenue % sharing model with Web3Shield, to offer insurance options to their users or they have another option to stake/lock a certain lumpsum amount of $SHLD tokens to continue provide insurance services to their end users.
The staking model helps the projects to retain its complete revenue to itself, and helps Web3Shield to strengthen its decentralized network as it is equivalent to a validator joining the network by putting in some stake. As a result, Web3Shield ecosystem will become stronger and widely decentralized, hence, ensuring better trust from community and community members.
At the same time, the staked supply will help decrease the sell pressure on the token and a good leverage to the token price as well.

Product # 1

EigenShield : Eigenlayer Restaking Insurance

EigenShield : Eigenlayer Restaking Insurance

Overview

With the ever evolving web3 space, the need for innovation is almost inevitable. Aligning with the same ideology, EigenLayer launched a never heard before concept of **Restaking** on Ethereum blockchain in year 2023. Restaking refers to a mechanism that allows Ethereum validators to make their staked ETH more useful by committing to secure protocols or services other than the Ethereum network itself. This is done by extending Ethereum's robust security model, allowing the other protocols (dApps, services) to benefit from billions of dollars worth of staked ETH. In Eigenlayer's words, "Restaking enables staked ETH to be used as cryptoeconomic security for protocols other than Ethereum, in exchange for protocol fees and rewards."

As of July'2024, EigenLayer has over **$12 Billion in Total Value Locked**, and became one of the biggest protocols on top of ETH ecosystem wrt to TVL in almost a record time. However, as the protocol continues to grow and scale, the number and complexity of issues pertaining to it's security and fair operation has been on the rise. While a lot of people and market experts are still trying to understand the deeper details of the protocol, a lot of validators are worried about the safety of their stakes/ funds on Eigenlayer. There's been a lot of issues that are existent as black-boxes in the entire operational system of Eigenlayer, be it the risk of slashing, correct conduct by Operators, AVSs malfunctions, or be it a generalised risk of centralisation in the protocol as a whole.

To tackle all these issues, and let users be worry-free while using this protocol for restaking, Web3Shield has launched **EigenShield** that is the Restaking Insurance on the eigenlayer economy. It provides a **One-Click Insurance** option to end users, right at the time of performing any **Re-Staking Transaction** on any Operator or directly through EigenLayer's interface.

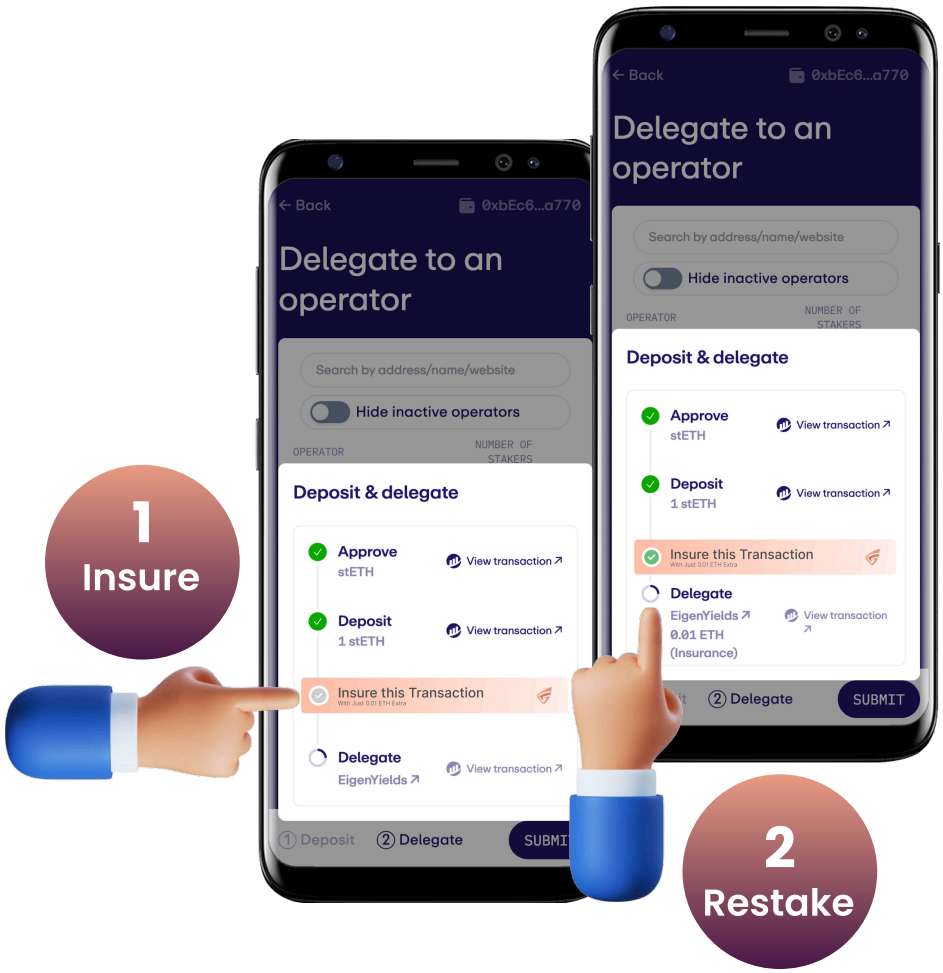
Web3Shield's EigenShield offers this Insurance capacity to the end users in a variety of ways via it's multiple distribution modes, including an Insurance Widget, browser extension, etc.

The Problem with EigenLayer

As the EigenLayer protocol continues to expand and provide ETH validators and stakers an option to earn a higher reward rates, a lot of issues, both significant and less-significant, starting to arise every single day. These include -

1. **Slashing Risk:** In the Eigenlayer ecosystem, the slashing risk is much higher as compared to the ETH ecosystem. Essentially, this means, that if a slashing event occurs, an EigenLayer Staker could possibly lose all its staked ETH, and incur a huge irreversible loss.
2. **Operator Misbehaving:** As itself stated by EigenLayer, the Operators are 3rd party entities in the eigen ecosystem. Hence, if an operator misbehaves or plays notorious, it can result in the stakers losing all of their funds. Also, notably, as the operator network on eigenlayer grows, this risk gets to be one of the biggest problems for eigen users.
3. **EigenLayer Centralization:** EigenLayer, as a whole, relies on a huge degree of centralization of re-staked assets into a few smart contracts. Such a concentration would mean that one successful penetration or exploitation by attackers/hackers could lead to failure in many significant parts of Ethereum's stake, and a dramatic risk to the entire ETH economy in general.
4. **AVS Malfunction:** Although AVSs are being registered systematically by EigenLayer itself, yet there is a significant risk associated with these. The responsibility to form and write the onboarding/integration conditions/rules in the AVS contract is by default assigned to the individual AVSs and not being managed by EigenLayer. Hence, any technical fault may end up causing a high turbulence in the eigen economy.
5. **Incorrect Yield Generation** : The risk of incorrect yield generation by an eigen Operator, or perhaps not delivering the assured yield to re-stakers is another problem that can worsen the state of the eigen economy.

In addition to above, another potential issue with EigenLayer is a **protocol-level risk**, that is, any individual AVS may be appropriately staked to the desired level of crypto-economic security. But if the same stake is restaked at several AVSs by the same validator, the cumulative gain from malicious behaviour may exceed the loss from slashing.



Our Solution - EigenShield

Web3Shield's EigenShield intends to bring a **One-Click Restaking Insurance** for EigenLayer and EigenLayer Operators. With a broader vision, EigenShield aims to secure and insure the entire EigenLayer economy by insuring the end users agains any black-swan events happending in the ecosystem. It intends to create a complete trustless system by leveraging the power of Insurance at a transaction level for end users.

This insurance can be opted-in by the user directly at the time of restaking their funds via any eigenlayer operator or interface. This gets to be possible by the virtue of our easy-to-integrate insurance SDK and widget, that integrates without disrupting any existing flow of the protocol.

Users, if opted for insurance, will receive back their funds safely even if an operator malfunctions, slashing occurs or if the protocol experience any hack or exploit at any level of operation. Hence, the process of re-staking becomes a no-brainer for the users, if clubbed well with One-Click Insurance offering.

The integration modes of Restaking Insurance is discussed in detail in further sections.

Restaking Insurance Expansion - Karak, Symbiotic and Others

The One-Click Restaking Insurance product is built in such a way that it is swift-to-integrate with any eigenlayer operator, interface or DApp built on top of EigenLayer. Additionally, the internal architecture is designed keeping in mind that the same solution can be **extended to other restaking protocols** including **Karak**, **Symbiotic**, etc.

Considering re-staking as a tech concept, has a lot of potential to grow and will definitely scale up as interesting protocols like Karak, Symbiotic, etc keep emerging out in the ecosystem. The **need for re-staking Insurance is massive** and the market is growing beyond thoughts. Hence, the near future plans for One-Click Re-Staking Insurance is to get extended to other restaking protocols and increase its market captualisation.

Please note - The architecture is discussed in detail in the further sections of this whitepaper.

Product # 2

BridgeShield : Cross-Chain Insurance Protocol

BridgeShield : Cross-Chain Crypto Bridge Insurance

Overview

In the dynamic and interconnected world of blockchain, cross-chain transactions have become a vital component of modern digital asset management. Web3Shield's Crypto Bridge Insurance product is designed to provide a safeguard in this critical area, offering users a seamless way to insure their transactions when bridging crypto from one chain to another. Recognizing the inherent complexities and potential vulnerabilities of cross-chain operations, our innovative insurance solution is more than a safety net; it's a commitment to user empowerment, transparency, and the continual growth of a secure and decentralized digital ecosystem. With Crypto Bridge Insurance, you bridge with confidence, knowing that Web3Shield is with you every step of the way.

Web3Shield's Crypto Bridge Insurance is revolutionizing the way users approach cross-chain transactions. With our one-click insurance service, users can effortlessly secure their assets as they bridge from one chain to another, mitigating concerns over potential vulnerabilities. Our streamlined process allows for a swift integration through an Insurance Facet contract and SDK, ensuring that the protection layer seamlessly incorporates into existing transaction flows. Through our offering, we aim to elevate user trust, enhance security, and foster a new age of confident decentralized interactions. Our dedication to providing this essential service is part of our broader commitment to driving global Web3 adoption, aligning with our mission to offer robust insurance, privacy, and security solutions for the decentralized digital landscape.

The Problem with Crypto Bridges

The decentralized world promises innovation and freedom but also brings its set of complexities and challenges. As Crypto Bridges become a crucial part of the digital asset ecosystem, several problems have arisen that hinder their widespread adoption and trust:

1. **Irrecoverable Loss of Funds:** In the digital realm, a single misstep or transaction error can lead to assets vanishing, a risk many deem overwhelming.
2. **Ever-Growing Bridge Hacks:** As technology advances, so do the methods of exploitation, making hacks inevitable, especially with the increasing volume on bridges.
3. **No Transaction Assurance:** Undertaking cross-chain transactions is fraught with anxiety for many, given the absence of guarantees for successful completions.
4. **Lack of Trust:** A cocktail of potential asset loss, mounting bridge vulnerabilities, and the uncertainty surrounding transactions culminates in a palpable trust deficit, hindering wider adoption.

These challenges not only impede the growth of Crypto Bridges but also undermine the broader promise of a secure, decentralized future. By addressing these concerns, we strive to create an environment where users can transact with confidence, knowing that their assets are protected.

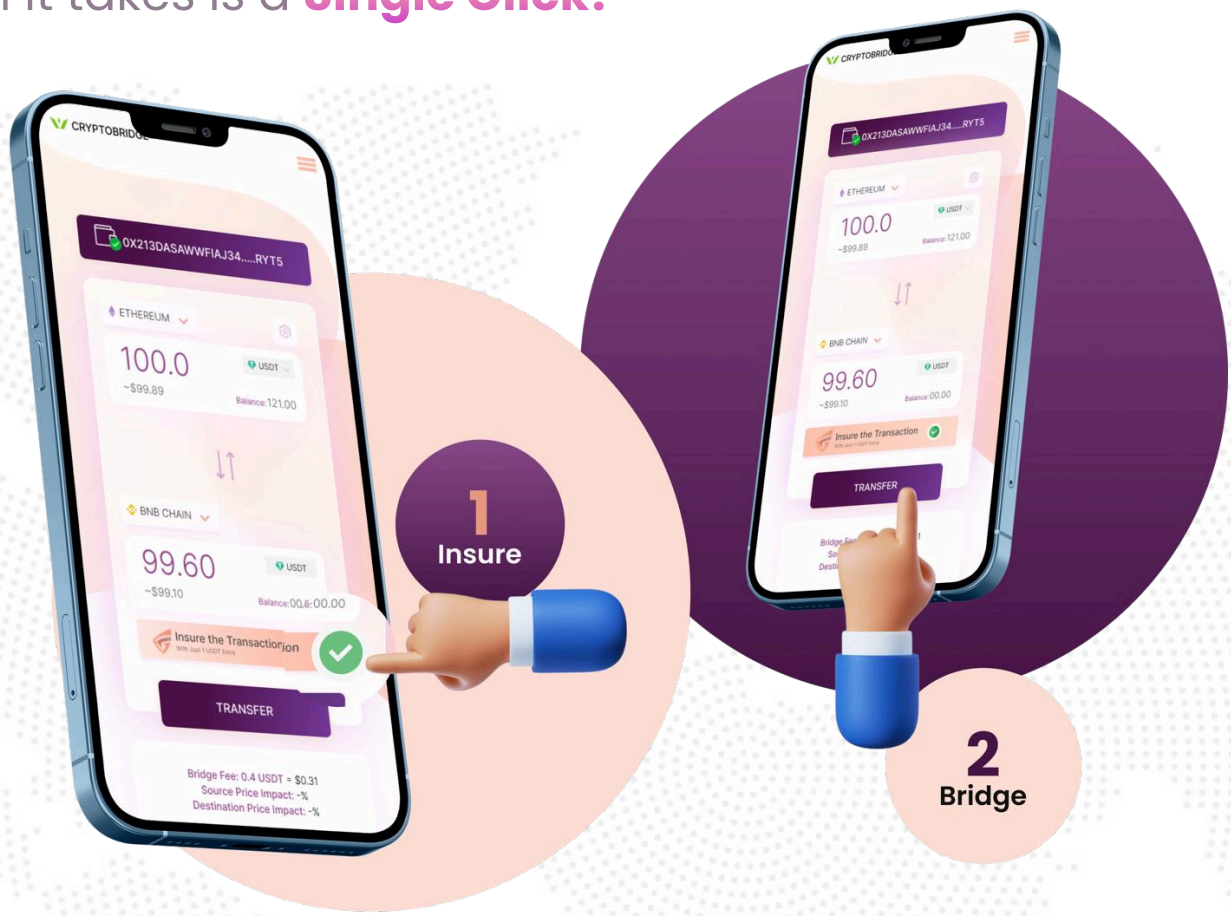
Our Solution

Web3Shield's Crypto Bridge Insurance is the definitive response to the challenges that have impeded the growth and trust in Crypto Bridges. With a vision to empower users and enhance their confidence, we offer a suite of features that enable bridges to offer users an extra layer of assurance, directly within the transaction flow.

One-click Insurance:

We believe in a user-centric approach where less is more. With our integration, users can simply select an insurance option during their bridging process. It's as straightforward as ticking a box.

All it takes is a **Single Click!**



Comprehensive Coverage

- Insured Bridge Transfers: We enable users to add insurance to their bridge transfers effortlessly, ensuring peace of mind as they navigate between chains.
- Atomic Coverage: Our solution integrates seamlessly into the bridging process, providing an unbroken, comprehensive coverage tailored to the individual transaction.

Integration

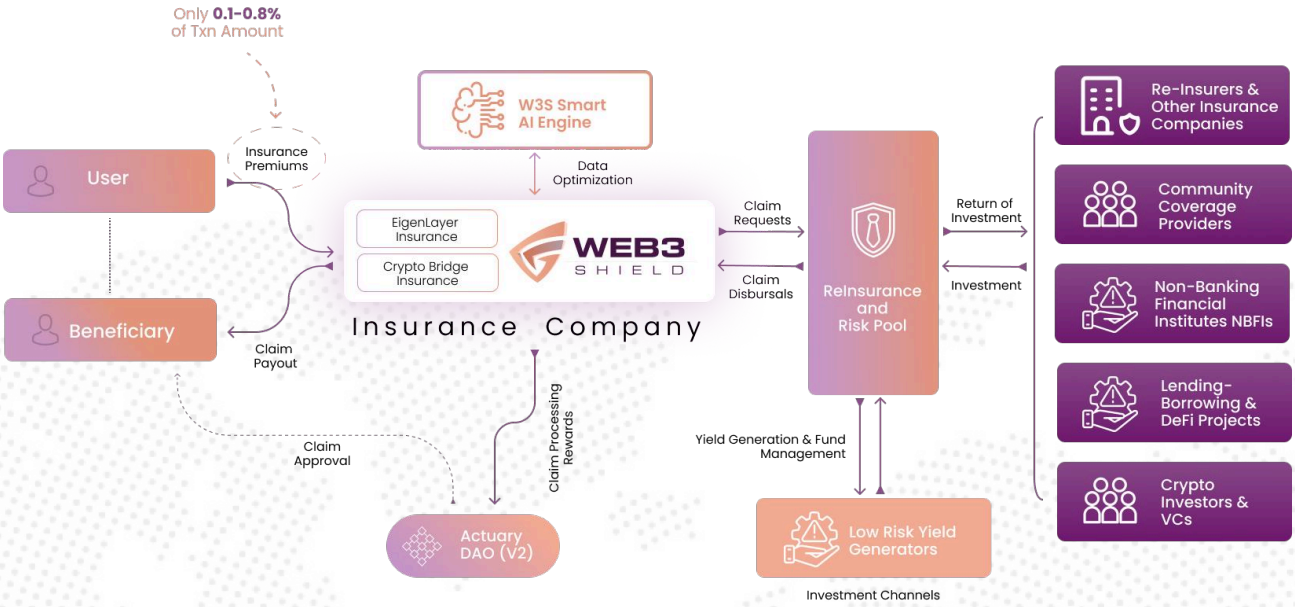
- Easy to Integrate SDK: Our Software Development Kit (SDK) is built for smooth and rapid integration, enabling bridges to offer our insurance solutions without hitches.
- Multichain Support: Web3Shield embraces the diverse world of blockchain, offering support across various chains, ensuring versatility for every bridge partner.

Our mission is not just to provide insurance but to weave trust into every transaction, fostering a safer and more reliable blockchain ecosystem.

Architecture

Web3Shield Architecture and Sytem Design

Architecture



In our insurance protocol, a variety of key players work seamlessly together, ensuring that users are provided with an unparalleled insurance experience on crypto bridges. Each actor plays a critical role, driving efficiency, safety, and trust.

1. **User:** The primary entity utilizing eigenlayer or crypto bridges, seeking to safeguard their assets against potential risks. They can effortlessly opt for insurance coverage during their transactions.

2. **Beneficiary:** Upon a validated and successful claim, a bridge user becomes a beneficiary, entitled to appropriate compensation commensurate with their loss.

3. **Actuary DAO:** A forward-looking approach to claim evaluation and policy review. The Actuary DAO will be a decentralized autonomous organization of expert actuaries who will collectively assess, verify, and manage insurance claims and policies. Their collective expertise ensures accuracy and fairness.

4. **Reinsurance Companies:** Established pillars in the insurance domain, these companies are brought onboard to underwrite and spread the inherent risks. They step in to cover larger losses and stabilize the insurance model, offering additional security to the bridge users.

5. **RiskPool :** The backbone of our insurance offering, the Risk Pool is a dedicated fund set aside to compensate successful claims. To optimize and grow the pool, external parties are invited to invest, drawn by the high-risk-high-reward model. Their investments amplify the pool's robustness and potential payout capacity.

6. **Yield Generation:** Financial prudence dictates not letting assets lie idle. The funds we hold, while waiting to cover potential claims, are invested in low-risk yield-generating platforms. This practice ensures the continuous growth of the fund, enabling us to cover larger claims while offering consistent returns to our investors.

7. **Community Coverage Providers:** Engaging the broader crypto community, these providers contribute to the risk pool, reinforcing its capacity to offer coverage while they earn steady rewards.

8. **Non-Banking Financial Institutes:** By broadening our collaboration with these institutes, we augment our risk pool's depth, ensuring a more extensive coverage umbrella for users.

9. **Re-insurers & Other Insurance Companies:** Diversifying our risk-sharing mechanisms, these entities strengthen the pool by redistributing risk and infusing capital, enhancing its reliability.

10. **Lending-Borrowing & DeFi Projects:** These platforms represent avenues where we judiciously reinvest our funds. By strategically allocating assets into these projects, we ensure stable returns for our risk pool investors, further bolstering the assurance provided to bridge users.

11. **Crypto Investors & VCs:** By tapping into their capital and strategic insight, we amplify our capacity to safeguard users' assets, making the ecosystem more resilient and user-centric.

For Cross Chain Insurance Protocol

Policy, Risk Assessment & Pricing

Policy

Overview

The purpose of this document is to illustrate the terms and conditions of the Insurance offered by Web3Shield.

General

Currently, Web3Shield offers Bridge insurance that is intended to reimburse for the loss of tokens while in transit from one chain to another.

Coverage / Covered Risks

When you use a crypto bridge to do transactions, your funds are exposed to a variety of risks. Web3Shield Insurance provides protection against the following claimable risk events:

- Loss of tokens in transit due to bridge malfunction, hack or vulnerability exploits of the covered Bridge.
- Loss of tokens in transit due to error in slippage reported by bridge and/or DEX for tokens received at bridge or DEX on destination chain.

Claims Process

After a loss event occurs, you must file a claim within the seven (7) days from the date of the loss event, any claim filed after this period shall not be covered.

Claim assessors (actuary DAO) will review, discuss, and vote to approve claims where proof of loss shows that the Cover Purchaser has suffered a loss of funds.

The details and results of the investigation, including the cover payout decision, will be produced in a report. If the claim is approved, funds will be made available to be claimed by the Cover Purchase Address.

For a detailed description of the Claims Assessment process see Claims Assessment section.

Proof Of Loss

When you insure a transaction with our Crypto Bridge Insurance and suffer a loss of funds, you can file a claim and claim assessors (actuary DAO) will review the claim submission to determine whether the claim is valid. To proceed with the claim request, proof of loss is required.

Proof of loss shall include, but is not limited to:

1. the Cover Purchase Address
2. the Source Chain Transaction ID/hash
3. the Policy ID
4. References to any relevant on-chain transactions
5. Official announcements / alerts / news of the occurrence of a hack
6. Any other evidence as deemed necessary

To proceed with the claim request, the claimant will be required to prove ownership of the affected address, allowing claim assessors to review the claim.

Some of the factors that claim assessors consider to determine whether to accept or reject a claim are (but not limited to):

1. If funds were deposited when the loss event occurred
2. If the claim was filed within the established period after the loss event occurred
3. If the Cover Purchaser suffered a loss of funds, and if so, the amount of funds that were lost
4. If the cover was active when the loss event occurred

Exclusions

- Policy purchased after the occurrence of exploitative events that have been made public will not be considered as eligible to make a claim.
- Any assets of widely blacklisted wallets and marked by illegality
- Any non-fungible token (NFTs)
- Any loss due to carelessness, misunderstanding, improper usage, omission or misuse by claimant
- There is clear evidence to suggest that the Cover Purchaser is being paid out by another insurance protocol/company (or any type of insurance provider) and the amount being paid out is, in aggregate, an amount in excess of the amount lost by the Cover Purchaser
- Loss due to movements in market price of asset
- Loss due to rug pulls
- Loss due to vulnerabilities, bugs or other issues made public prior to transaction execution
- Any event of token price depeg
- Loss due to changes or failures in safety or liveness properties of underlying blockchain
- Loss due to administrative, gas, transaction fees or expenses incurred in executing the transaction
- Loss due to collateral damage from claimable risk event:
  - Any consecutive losses due to the occurrence of the claimable risk event
  - Losses pertaining to other currencies and resulting consequences
  - Loss due to any additional or prior token approvals granted to a bridge exclusive of the approval granted for the bridging transaction
- The Loss Event took place outside of the Cover Period

Conditions

The cover purchaser may be compensated for his/her tokens lost during the covered bridge transaction where:

- The loss is related to the wallet address used to purchase the cover
- The loss occurred during the cover period
- A claim is submitted during the cover period or within 7 days after the cover expires
- Any recovery received by the Insured as compensation for his/her losses shall be excluded from the claim payments
- Claims without sufficient proof of loss and ownership are automatically deemed invalid and rejected
- Exploitative events on bridges will be announced on the respective discord channels (or any other social channels) and Web3Shield will stop issuing insurance policies for transactions on that bridge, any loss due to vulnerabilities, bugs or other issues made public prior to transaction execution are not covered

Termination

Web3Shield's obligation to reimburse the Cover Purchaser up to the value of any cover payout for any other compensation or loss recovery shall automatically terminate when one of the events below occurs:

- the occurrence of a claimable risk event;
- the termination of the covered bridge transaction.

In the event the cover is canceled due to the bridge transaction having been canceled and the cover purchaser's tokens remain unaffected, any contribution paid for the insurance (policy premium) by the cover purchaser shall not be refunded.

Misrepresentation / Fraud

A claim will be refused if it is made in any of these cases:

- if any Claim made is forged, fraudulent or exaggerated
- if any false declaration or statement is made
- If any claim is a duplicated claim
- if the claim is being made from a wallet address different from the cover purchase address
- If the ownership of the cover purchase address can't be proved or the cover purchaser has lost access to the cover purchase address

Definitions

- **Actuary DAO/Claim Assessors:** A decentralized group of actuary & underwriter professionals who assess a claim and its proof of loss to determine whether the claim is valid and therefore payable.
- **Claim**: A formal request submitted by a cover purchaser to receive compensation for losses suffered due to a claimable loss event. This request is subsequently evaluated by the Actuary DAO.
- **Claim Amount:** The amount requested as compensation following a claimable risk event.
- **Claimable Risk Event / Loss Event:** A specific incident resulting in the loss of assets during their transit.
- **Company Risk and Cover Pool:** A dedicated fund set aside to compensate successful claims.
- **Cover**: Coverage offered by Web3Shield in the event of a claimable risk event subject to the terms and conditions.
- **Cover Payout:** The compensation dispensed for a verified and approved claim to a cover purchaser.
- **Cover Period**: The specified duration during which the purchased insurance cover remains active and valid.

- **Crypto Bridge Insurance:** An insurance solution by Web3Shield, insuring assets against predefined risks within set terms and conditions.

- **Cover Purchaser** : The individual or entity identified as the authorized owner of the cover purchase address.

- **Cover Purchase Address** : The wallet address used for the transaction involved in paying the policy premium for Crypto Bridge Insurance.

- **Policy ID:** A distinct identifier allocated to each insurance policy issued.

- **Policy Premium:** The contribution paid for the insurance coverage.

- **Proof of Loss:** Essential documentation or information required when lodging a claim to confirm the legitimacy of the claimed loss event.

- **Rug pulls:** Deceptive tactics where a developer or project team entices investors/ users, only to abscond with their assets unexpectedly.

- **Slippage:** The difference between the expected price of a transaction and the executed price.

- **Transaction hash**: A unique alphanumeric identifier representing a specific on-chain transaction.

- **Transit**: A phase during which assets are considered in movement, starting from the initiation of a transaction on the source blockchain until its finalisation on the destination blockchain.

Disclaimer

As a decentralized protocol, Web3Shield operates outside the purview of traditional licensing and regulatory frameworks. Nonetheless, in the spirit of transparency and commitment to our stakeholders, Web3Shield will periodically disclose its audits and financial reports, or as necessitated by specific circumstances.

This cover is not a contract of insurance. It offers discretionary protection with the Claim Assessors / Actuary DAO having full and final discretion on claim and cover payout approval.

Completion of any cover payout is determined by sufficiency of assets in the Company's Risk & Cover Pool.

Pricing Model

Data Development Process

The data derived for modelling comes from DeFi Llama.

The severity data: past hacks and lost funds is reliably reported beginning in 2016. By the end of May 2023, the total amount of hacks recorded is 174. We have elected to use the 174 hacks for the calculations. It is important to mention that we are dealing with truncated data, specifically left truncated data, where there is no information recorded below the truncation point d. In our case the minimum amount lost recorded is d = 0.08 million USD.

For the frequency: daily TVL records per bridge since October 2020 are available. The first TVL record for each bridge occurs at different points in time. By the end of May 2023, 938 days were recorded, producing a total of 16634 daily TVL records. An extract of the Data Set is shown in the following figure.

Total daily sum	16219865396	16610444345	16146203157	16270397904	16726072929	16551323373	16656217295	16195142068	15712540066	15464611781	15527084029	15694604508	16622094994	17027388866
Protocol	**19/05/2022**	**20/05/2022**	**21/05/2022**	**22/05/2022**	**23/05/2022**	**24/05/2022**	**25/05/2022**	**26/05/2022**	**27/05/2022**	**28/05/2022**	**29/05/2022**	**30/05/2022**	**31/05/2022**	**01/06/2022**
WBTC	8116577719	8398549510	8083566374	8148821092	8396291313	8066423186	8184111876	8160384214	8050789732	7910657111	7982433218	8085901580	8681550246	8715762982
RenVM	295210443.1	309456836.9	299414111.4	304303664	314551603.3	305713768.6	315829865.9	314906639.7	304462976.1	299154626.7	305265494	310158646.5	325739150.2	325993294.1
hBTC	1129403771	1172388221	1145459545	1146940424	1178623430	1150174974	1157150691	1159099216	1141757349	1114672860	1132287520	1142770581	1228349772	1244171790
Strudel Finance	673177.83	700054.68	681019.8795	686605.2525	707084.9537	678646.096	690282.2898	689188.4876	683882.3832	666451.3648	677668.6557	689258.3047	734616.1882	741760.8112
Synapse	380256822.3	379543731.3	373804092	375193907	382499081	378577363.7	379650817.5	381288119.8	370601969.4	362305832.2	365618113.9	368580906.6	383439379.3	336570623.1
Portal	677439786.8	658755491.2	647414525.5	640818629.6	675004654.3	669418507.2	654348909.9	673046725.3	623084750.4	600034620.3	577463535.5	571875970.7	633037977.2	632306707.7
Allbridge	137376224.4	137680800.8	137159766.7	138315526.8	137828366	139594635.9	137474431.4	137938823.7	137372291.4	136526477.7	136933696.2	137123665.6	135900379.3	137805674.5
Multichain	3467391898	3484640646	3452077640	3467755536	3482662936	3459684362	3457534195	3015236958	2927886238	2927021090	2922460335	2923012278	2993812273	2987989166
JustCryptos	856836792	897575574	863176082	873644677	900117430	1131215694	1145452108	1149369054	1110515377	1096120172	1112482957	1126474946	1212458597	1219053208
cBridge	466069277.8	472424747.3	502001312.1	505298893.5	509442064.5	504723723.7	501838278.9	501395683.9	481566298.4	466936225.8	455178830.7	476523840.7	436742901.1	434381620.4
Wrapped BNB	83664965.3	87660802.67	87192494.95	89948071.14	91841442.52	91287077.39	94191747.95	93773751.09	86772292.04	86552133.82	87353976.19	87013452.24	92118909.18	92300192.13
Knit Finance	9511787.822	9521290.107	9502285.536	9511787.822	9511787.822	9521290.107	9501838.929	9502285.536	9511787.822	9521290.107	9511787.822	9511787.822	9501373.317	9502285.536
ChainPort	155985388	171187588	161933117	177172192	171395383	150706850	150342574	150573345	142298942	134581445	134530276	137862819	150387401	141761332
ioTube	50845384.19	53614244.37	54781579.46	58620427.66	63068667.08	58881139.23	60305201.15	60192517.7	55739774.98	55451950.09	55518413.82	57531210.66	60695462	59419207.09
Injective Bridge	10660412.38	10698188.23	10684210.02	10681775.18	10687682.4	10630739.55	10621412.01	10576381.66	10516611.86	10495506.59	10533147.36	10528172.7	10286408.35	10276356.62
deBridge	4493450.938	4513546.008	4564242.751	4558207.512	4541681.717	4526593.135	4490235.677	4521087.883	4014247.668	3971795.516	3982144.522	3940371.727	3882248.636	3876171.558
RelayChain	15635444.64	15926983.71	12693629.05	12801041.82	13076699.01	12693323.15	12644971.83	8704238.501	8579949.525	8245970.899	8276524.623	8098804.311	8409436.643	8369988.488
Octus Bridge	60860279.05	60920002.23	58659993.06	58929337.79	59433940.9	60392498.89	59346052.26	59697279.94	60155162.63	61254128.97	61230466.32	61783632.63	60936575.49	66476593.43
Terra Bridge	237449892.5	218806887.3	175006929.4	179461648.1	257277954.7	274539578.2	248843222.7	232647257.1	116243685.2	111797171.2	95642046.08	105613619.2	110059268.7	99748377.32
Hyphen	9284745.626	9537486.249	9483969.413	9619296.717	9733600.791	9626147.212	9604137.095	9460604.13	9066326.058	8949340.724	8985504.213	9038574.464	9791140.627	9868876.586
CENNZnet Bridge	173975.3638	180728.4951	177440.876	178906.1424	185036.4125	182153.3628	181538.0012	181792.3432	165663.1295	161632.216	166188.5382	167607.3608	197336.3413	208022.493
Nomad	54063758.52	56150898.7	56758581.56	57126036.91	57580870.32	57121269.23	57133408.86	57076367.46	57052774.68	56282735.84	57348261.73	57525098.65	60894337.93	61213216.47
Ad-Astra Bridge		10085.53462	10214.07461	10220.54715	10218.95859	5009852.531	4929498.514	4880536.931	3701983.786	3251212.679	3203923.157	2877682.882	13169804.44	19949487.88
Poly Network														409641931

Figure 1: Daily TVL per bridge

Pricing Model

Aggregate Loss Model

Web3Shield uses an actuary-based pricing model, works with a collective risk model that examines the aggregated losses. Aggregate loss distributions play an important role in the pricing of insurance coverages, they are calculated in terms of the underlying severity and frequency.

Probability distributions are obtained for the severity of individual losses and frequency. Using these two models, we carry out the necessary calculations to obtain the distribution of S (an aggregate loss model).

Frequency

From the Frequency modelling we obtain the probability of a given number of losses occurring during a specific period, this probability is calculated as a total probability based on the TVL and past bridge hack events.

Severity

The main challenge faced is forecasting the expected future claims experience, for that, we study the losses from past years. Severity modelling develops a model for the distribution of loss amounts based on data. We propose an inventory of standard parametric distributions that could be used to approximate the distribution for loss amount. They include, but are not limited to, the following families of distributions.

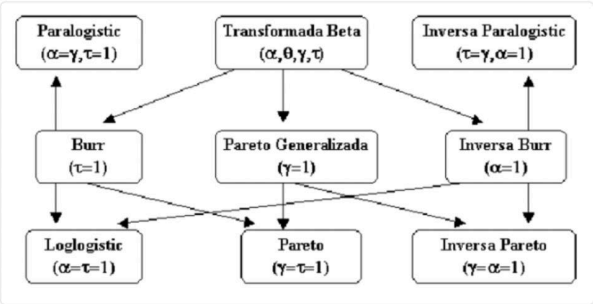


Figure 2: Transformed Beta Family

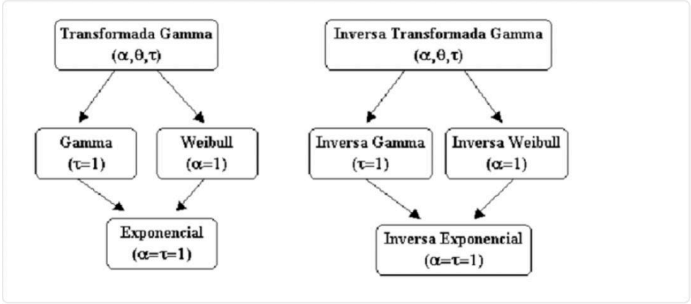


Figure 3: Transformed and Inverse Transformed Gamma Families

We proceed with a formal goodness-of-fit test, which is a statistical procedure that describes how well a distribution fits a set of observations by measuring the quantifiable compatibility between the estimated theoretical distributions against the empirical distributions of the sample data. Finally, we proceed with the model selection.

Risk Premiums

Once frequency and severity models have been estimated, Web3Shield formulates a base risk premium from the previous calculations.

Please note : Specific calculations and intricate details of our pricing model have been kept confidential for proprietary reasons and to prevent reverse engineering.

References

[1] Klugman, S.A., Panjer, H.H. and Willmot, G.E. (2012) Loss models: From data to decisions. Somerset: John Wiley and Sons.

[2] Total value hacked (USD) (no date) DefiLlama. Available at: https://defillama.com/hacks (Accessed: 25 May 2023).

[3] Bridge TVL Rankings (no date) DeFiLlama. Available at: https://defillama.com/protocols/Bridge (Accessed: 23 May 2023).

[4] Albright, Robert. (2020). Developing Aggregate Loss Models For Obscure Insurance Exposures. Retrieved from the University of Minnesota Digital Conservancy, https://hdl.handle.net/11299/217111.

[5] Taboga, M. (no date) Likelihood ratio test. Available at: https://www.statlect.com/fundamentals-ofstatis-tics/likelihoodratiotest#::text=The%20likelihood%20ratio%20(LR)%20test,a%20restriction%20on%20the%20parameter. (Accessed: 26 June 2023).

Risk Assessment

The security and reliability of crypto bridges are critical for user trust and confidence. For Web3Shield, this trust forms the foundation of our one-click insurance product. To ensure that this trust is well-founded, we have instituted a comprehensive risk assessment framework.

The risk assessment methodology presented in this section is adapted from the work of Joel John. To explore the original work in its entirety, please refer to "Assessing Blockchain Bridges".

This section introduces our approach to evaluating crypto bridges. Our methodology is rooted in high-level factors, which are essential determinants of a bridge's risk profile. Each factor comprises specific categories with their own allocated scores, resulting in a cumulative risk score for each bridge. This score informs our decisions on insurance terms and conditions for the respective bridge.
Our objective is to ensure transparency in our risk assessment process and provide our stakeholders, both bridge partners and users, with insights into the measures and standards we uphold.

Key Assessment Criteria

When assessing the viability and reliability of a bridge for integration with our one-click insurance product, we examine a set of core criteria. Each criterion gives us a snapshot of the bridge's overall quality, functionality, and trustworthiness:

- **Security**: How secure your parked assets are on a bridge
- **Performance**: The economic model behind a bridge-related transaction
- **Extractable value:** The possibility of flashbots or other intermediaries extracting a portion of the transaction
- **Connectivity**: The number of networks a bridge is connected to
- **Capability**: The extent of assets supported by a bridge

Security

The integrity of a crypto bridge, and consequently the confidence users place in it, hinges squarely on its security provisions. As we evaluate the safety standards of a bridge, it's essential to consider not just the overt mechanisms but also the underlying assumptions and contingencies.

The essential facets that shape a bridge's security framework:

1. **Degree of Liveness Assumption**: evaluates the duration a bridge has to dispute a potentially malicious transaction, with longer times indicating greater security vigilance.
2. **Validator Collusion**: assesses the risk of validators accessing user funds, with ideal systems ensuring no single validator has direct access to these assets.

3. **Measures for Worst Case Scenarios:** evaluate the provisions in place, including separate capital pools or token incentives, insurance coverage, etc. to compensate users post a potential hack.

4. **Soundness of Code:** assesses the combination of multiple audits and the capital allocated to bounties, encouraging thorough scrutiny by top minds for potential vulnerabilities.

Simply integrating Web3Shield's One-Click Insurance SDK enables bridges to increase their overall security rating!

Performance

In evaluating the efficiency of a bridge, we delve into various parameters that impact the user experience and financial feasibility. Let's dive into the intricacies that define a bridge's performance:

1. **Cost of bridging:** evaluates the scalability of fees, with special attention to the surges during cross-chain exchanges as asset volume increases.

2. **Liquidity Rebalancing Needs**: evaluates the efficiency of AMM pools in handling large exchanges, rewarding systems with stable, low-cost transactions, and penalizing those requiring frequent rebalancing or imposing high fees after minimal thresholds.

3. **Latency**: assesses bridge speed, favoring those completing transfers within 5 minutes and penalizing those taking more.

Extractable Value

Extractable value, though often overlooked, can have a profound impact on user experience and the overall security of assets. To shed light on its nuances, we've centered our attention on a few select metrics:

1. **MEV Leak**: evaluates the susceptibility of a bridge to transaction front-running, with bridges exhibiting robust protective measures against high-value MEV extractions scoring higher.

2. **Censorship resistance and position on the permission spectrum**: gauges a bridge's resilience against potential future sanctions, prioritizing permissionless and highly censorship-resistant platforms.

3. **Churn**: evaluates a bridge's capital efficiency by measuring the monthly capital flow in relation to its total value locked, highlighting bridges that optimize capital without excessive idle assets.

Connectivity

A bridge's versatility and reach in the vast blockchain ecosystem are often reflective of its adaptability and utility. Let's take a look at the metrics that define a bridge's connectivity:

1. **Types of Chains Supported**: evaluates a bridge's ability to interact with diverse networks and layers, ensuring they're not merely focused on popular EVM-based chains but offer varied asset flow.

2. **Number of Chains Supported**: measures the breadth of a bridge's connectivity, assessing not just the count but the seamless communication between these supported chains.

Web3Shield offers a chain-agnostic One-Click Insurance solution, enabling bridges to support their Security standard while maintaining Connectivity!

Capabilities

With Capabilities, we delve into the depth and variety of functions a bridge can perform, reflecting its utility in the decentralized space.

1. **ERC20 Support**: evaluates the bridge's capacity to handle multiple Ethereum/EVM based tokens.

2. **Contract Calls:** measures the bridge's capability to engage with smart contracts on destination chains, enabling advanced cross-chain interactions and operations.

We've delineated the crucial metrics that underpin the evaluation of bridges' risk profiles. Through a meticulous examination of security parameters, performance standards, extractable values, connectivity, and capabilities, we aim to offer an exhaustive and objective analysis. This framework will serve as the foundation for our one-click insurance product, ensuring that our offerings are grounded in a robust assessment.

Disclaimer

As a decentralized protocol, Web3Shield operates outside the purview of traditional licensing and regulatory frameworks. Nonetheless, in the spirit of transparency and commitment to our stakeholders, Web3Shield will periodically disclose its audits and financial reports, or as necessitated by specific circumstances.

This cover is not a contract of insurance. It offers discretionary protection with the Claim Assessors / Actuary DAO having full and final discretion on claim and cover payout approval.

Completion of any cover payout is determined by sufficiency of assets in the Company’s Risk & Cover Pool.

$SHLD - Utility Token

Web3Sheild Foundation & $SHLD Details

Web3Shield Foundation

Web3Shield Foundation will be building an interoperable token system with the help of the Unified $SHLD Tokens. So, whenever these tokens are used for any reason, the Web3Shield Foundation will be receiving a transaction fee. On top of that, as the demand for the tokens rise due to its ecosystem operations in insurance, the value of the token will rise, incentivizing the $SHLD hodlers.

Token function

The $SHLD token is used for insurance premium settlement, staking and loyalty token for the Web3Shield ecosystem and all its associated insurance protocols to come in future. The token facilitates additional functions as both deterrent to bad actors (via its staking function) and as a payment option, offering additional discounts to its users. List of token functions:

- Insurance Premium settlement
- Claims Payouts
- Staking upon registration (B2B)
- Reward claiming (Re-Insurance Pool Rewards)
- Governance
- Get users Attention and Financing of Risk/Reinsurance Pool.

Insurance Premium Settlement. Fees for opting for insurance for any transaction or a lumpsum wallet insurance can be settled either in Stable or native tokens or in the $SHLD token. However, all inurance policies bought with $SHLD will enjoy a x% discount on the premium amount or alternatively an x% of tokens as participation reward. Since all the web3 projects (initially eigen operators & crypto bridges) will enable the seamless use of $SHLD, we assume that eventually all premiums will be paid via $SHLD.

Staking upon Registration. New customers/web3 projects/crypto bridges of the web3shield's insurance widget will have the option to stake a floating amount of tokens (based on fixed USD equivalence). Those tokens will act as a guarantee of proper conduct and as an additional incentive token to give them a freemium insurance providing experience. Any project/bridge not acting in good faith will be at a risk of losing this deposit. In the meantime, those tokens will also provide double benefit to the rest of the platform users:

1. If the token value appreciates in value, users will be able to unstake part of their tokens (as long as they meet the fixed USD equivalence requirement) and sell them for a profit.
2. If the token value depreciates, users will be able to “sell their stake or asset” in the system at a slight discount to other users who wish to be a customer of web3shield, and instead opt for the revenues sharing option with Web3Shield.

Claims Payout. If a claim request arises due to any hack/issue, the claim payout will be paid to the users in the form of $SHLD tokens. If the user buys the policy using $SHLD tokens, an additional bonus in terms of $SHLD tokens will be provided to him along with the actual payout.

Reward Claiming (Re-Insurer Rewards). $SHLD will enable retail users to be able to stake any floating number of tokens or stable in the reinsurer risk pool, in order to earn a good APR from it. These staked tokens are kept in the pool and eventually increases the coverage capacity of the insurance provided by web3shield. Users can claim the rewards on their staked amounts visitng Web3Shield Dashboard.

User’s Attention and Financing. While not the main function of the $SHLD token, it still can be used as a pure medium of getting users attention to any web3 project by way of rewarding users in loyalty points.

Similarities and benchmarks. Conceptually the $SHLD token is very similar to the Binance coin (BNB), in the sense that it is used for the settling of fees and offers additional discounts to people opting to use it as a payment method. We will use this similarity when estimating token characteristics (such as velocity) further down in this document.

Important differences from the benchmark. While we will use BNB as a benchmark, it is important to also point out the differences between the two coins.

- In the B2B2 case, instead of burning, $SHLD will have a staking function, required upon customer registration.
- The $SHLD token may act as a payment token along with staking and loyalty on the Web3Shield platform.

Lost tokens. Inevitably some small % of tokens is going to be lost each year (lost private keys). We have done a conservative estimation of 0.5% of all tokens being lost per year. This is a conservative estimate, as studies have found that approximately 4 mn Bitcoins have been lost (approximately 25% of the available bitcoin supply as of 2017), over the course of 10 years[1]. Other estimates show this to be closer to 11% for provably lost coins[2].

Speculative action. In our assumptions, we have included a conservative 20% of all tokens held by speculators, taking them out of circulation. Web3Shield Foundation would initially fund the re-insurance risk pool with a specific amount of $SHLD and Stable Coins. Post this, X% of all transactional fees generated from revenue models listed in the Token function section referred earlier in the document would be diverted to the $SHLD re-insurance pool ensuring enough liquidity. The Foundation intends to gradually decrease the amount of tokens you get being a user(with early adopters getting the maximum rewards) but as $SHLD is a perpetually deflationary token, the rewards(in USD terms) would still keep on maintaining a peg above the USD threshold value over time. We also feel that the old and new members of the community should be rewarded more for investing in the project at an early stage and hence early contributers are provided with more reward tokens/ discounted tokens during the private sale of $SHLD Tokens.

[1] JEFF JOHN ROBERTS and NICOLAS RAPP (2017) Exclusive: Nearly 4 Million Bitcoins Lost Forever, New Study Says http://fortune.com/2017/11/25/lost-bitcoins/ [2] Coinmetrics: https://coinmetrics.substack.com/p/coin-metrics-state-of-the-network-d2e

$SHLD Staking

With $SHLD, one can also provide some liquidity into a pool and either get exclusive benefits within the associated projects like a discounted insurance policy or better/ easier claim payouts. In addition, as an $SHLD staker, you also can enjoy the rewards payout from the re-insurer rewards pool. However, as an early adopter to help provide liquidity, you become a significant stakeholder of the protocol.

The earnings that you'll receive from staking will be proportional to the amount of pool tokens you have staked versus the total amount of pool tokens staked. Unless you continue to provide liquidity, your holdings and corresponding cash flows will gradually be diluted.

Since the $SHLD users will be eligible to receive cash flows by staking their tokens, we can estimate an approximate expectation for the value of said cash flows.

Discounted Cash Flow Analysis (DCA) has been around for a while and has been established as one of the main evaluation methodologies of an investment based on its future cash flows. The purpose of DCF analysis is to estimate the money an investor would receive from an investment, adjusted for the time value of money[1]. While it has not widely been used in cryptocurrency atleast until start of 2021, our expectation is that with the increasing number of ILOs involving staking it is going to establish itself as the de-facto standard for any token with periodic cash flow payments on staking. The formula for calculating the net present value of a future cash flow goes as follows:

$$NPV = \frac{CF_1}{(1+r)^2} + \frac{CF_2}{(1+r)^2} + \ldots + \frac{CF_n}{(1+r)^n} + TV$$

Where:

I. 'NPV' is the net present value of the investment
II. 'CFn' is an expected future cash flow at period
III. 'r' is the discount rate, also referred to as the cost of capital
IV. 'TV' is the terminal value (or exit value) of the investment

In turn, **TV is evaluated as:**

[1] Investopedia, Discounted Cashflow Analysis - https://www.investopedia.com/terms/d/dcf.asp

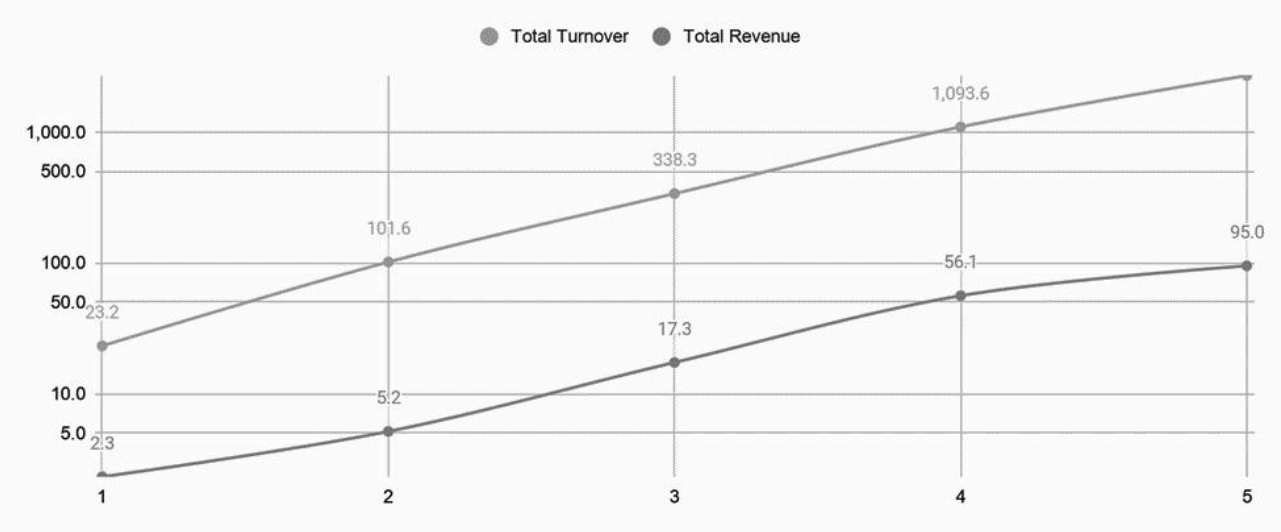
$$TV = \frac{CF_n \times (1+g)}{r-g} + \frac{A}{(1+r)^n}$$

With the two new elements being

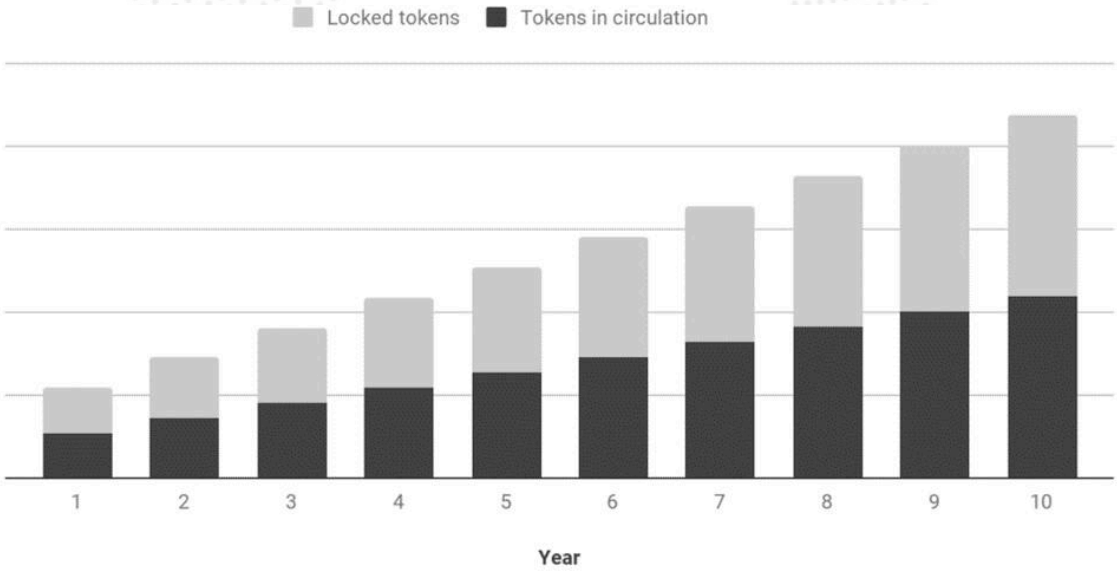
I. 'r' representing the expected long term growth rate of the underlying business.

II. 'A' representing any liquid assets available at the end of period

For our cash flow estimate, we are taking a very conservative approach, by looking at the Web3Shield Ecosystem and assuming that we will be able to reach the projected volume(as highlighted in Token Valuation sheet) within a 5 year period (while majority of other projects have reached their targets within 2-3 years)



Only users who stake/lock their $SHLD tokens in our staking contract will be eligible for receiving cash flows generated from the components of the ecosystem. At this point the exact number of users who will be willing to stake their tokens is unknown, but for the purpose of this calculation, we will assume that 50% of all circulating tokens will be locked at any given point in time.



ILO Financials & token generation event

Basics:

⌞Ticker:	SHLD
⌞ILO start date	TBD
⌞ILO end date:	TBD
⌞ILO Denomination currency:	USD
⌞Accepted currencies:	USDC, USDT
⌞Jurisdiction:	Panama
⌞Eligibility:	Subject to KYC and AML
⌞Compliance:	None
⌞ Token purchase contract:	SAFT
⌞ILO waves:	5

Token Generation Event Summary

⌞Sale type:	ILO
⌞Softcap:	TBD
⌞Hardcap:	TBD
⌞ILO Tokens:	TBD
⌞Remaining tokens post ILO:	burned
⌞ILO allocation:	30% (tentative)
⌞Initial Total Tokens:	TBD
⌞Token type:	Fixed supply
⌞Important notice:	Under SEC rules, this token is not a security but a Utility

*ILO tokens calculated under the assumptions of -

- **Stage 1 :** 10,000,000 SHLD sold @0.07 USD = 0.7 MM USD raised
- **Stage 2 :** TBD
- **Stage 3 :** TBD
- **Stage 4 :** TBD
- **Stage 5 :** TBD

Wave 1: Seed Round

Token price:	0.07 USD
Bonuses:	NA
Wave number of tokens available:	10,000,000 SHLD
Wave cap:	0.5 MM USD
Cumulative number of tokens available:	10,000,000 SHLD
Cumulative cap:	0.7 MM USD
Minimum investment:	25,000 USD
Maximum investment:	TBD
Wave start:	TBD
Wave end:	TBD

Token valuation

In this section, we will attempt to present a fair price estimate for the SHLD token, under the assumption of reaching hardcap and company revenue projections provided as-is.

Methodology. Probably the most widely used valuation methodology for utility tokens is the quantity theory of money[1] and more precisely the equation of exchange[2] . Several models[3] [4] based on those principles have been developed and widely accepted by the cryptocurrency community. In a nutshell, the equation of exchange is:

$$M \times V = P \times T \quad (1)$$

Where:

1. 'M' is the amount of money in circulation, within a specific system
2. 'V' is the velocity of money, or in other words: how often does money change hands within a predefined period (most commonly - annually)
3. 'P' is the price at which transactions are happening within the system
4. 'T' is the number of transactions for a predefined period (same period, as the velocity)
5. 'PXT' in this regard is essentially the total economic output of the system for the selected period, sometimes referred to as GDP of the system.

The above formula (1) is not directly applicable to cryptocurrencies (and a commonly encountered error), due to the fact that in a token/cryptocurrency economy, the two sides of the above equation are denominated in different units. When talking about the systems GDP, the expected Revenue in USD is generally used, on the other hand, the left-hand side of the equation is still denominated in the native token. We can solve this by introducing an additional parameter which represents the exchange rate between the token and USD (or any other FIAT currency based on the denomination of the system's GDP). The equation then becomes:

$$M_T \times E_{T/USD} \times V = P_{USD} \times T \quad (2)$$

This enables us to solve for (3) and get the expected token exchange rate (or token value), provided we can come up with adequate estimations for the other variables. From (2), we can solve for the token value as:

[1] Friedman M. (2008) Quantity Theory of Money. In: Palgrave Macmillan (eds) The New Palgrave Dictionary of Economics. Palgrave Macmillan, London https://link.springer.com/referenceworkentry/10.1057%2F978-1-349-95121-5_1640-2

[2] Bordo M.D. (1989) Equation of Exchange. In: Eatwell J., Milgate M., Newman P. (eds) Money. The New Palgrave. Palgrave Macmillan, London https://link.springer.com/chapter/10.1007/978-1-349-19804-7_17

[3] Chris Burniske (2017) Cryptoasset Valuations https://medium.com/@cburniske/cryptoasset-valuations-ac83479ffca7

[4] Brett Winton (2017) How to Value a Crypto-Asset—A Model https://medium.com/@wintonARK/how-to-value-a-crypto-asset-a-model-e0548e9b6e4e

$$E_{T/USD} = \frac{P_{USD} \times T}{M_T \times V} \quad (3)$$

However this begs the question - how do we estimate the staked TOKEN equivalent? Staking. Here, we refer back to the expanded equation of exchange (2) as follows:

$$M_T \times E_{T/USD} \times V = P_{USD} \times T \quad (4)$$

From here, we can represent the staked amount as a temporary reduction in the token supply, denominated in USD , converted to tokens, based on token price. Then we can subtract this amount from the total supply , as follows:

$$(M_T - \frac{S_{USD}}{E_{T/USD}}) \times E_{T/USD} \times V = P_{USD} \times T \quad (5)$$

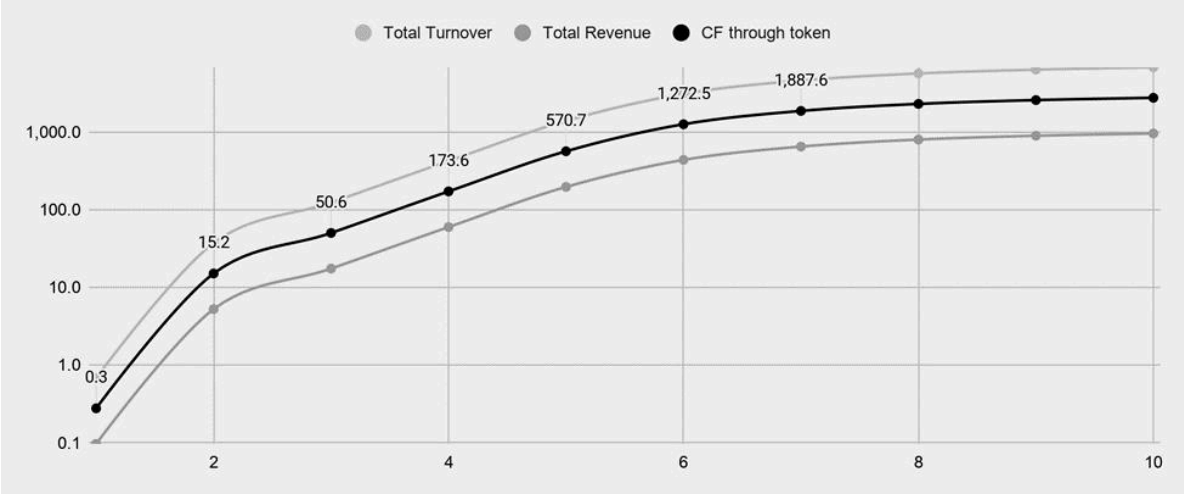
Following the same transformations, we did previously, we can simplify this equation to:

$$E_{T/USD} = \frac{P_{USD} \times T + S_{USD} \times V}{M_T \times V} \quad (6)$$

In other terms - the USD equivalent of any staked token amount can be represented as an increase in the GDP (or demand) for the token. This extra “demand” is not affected by velocity.

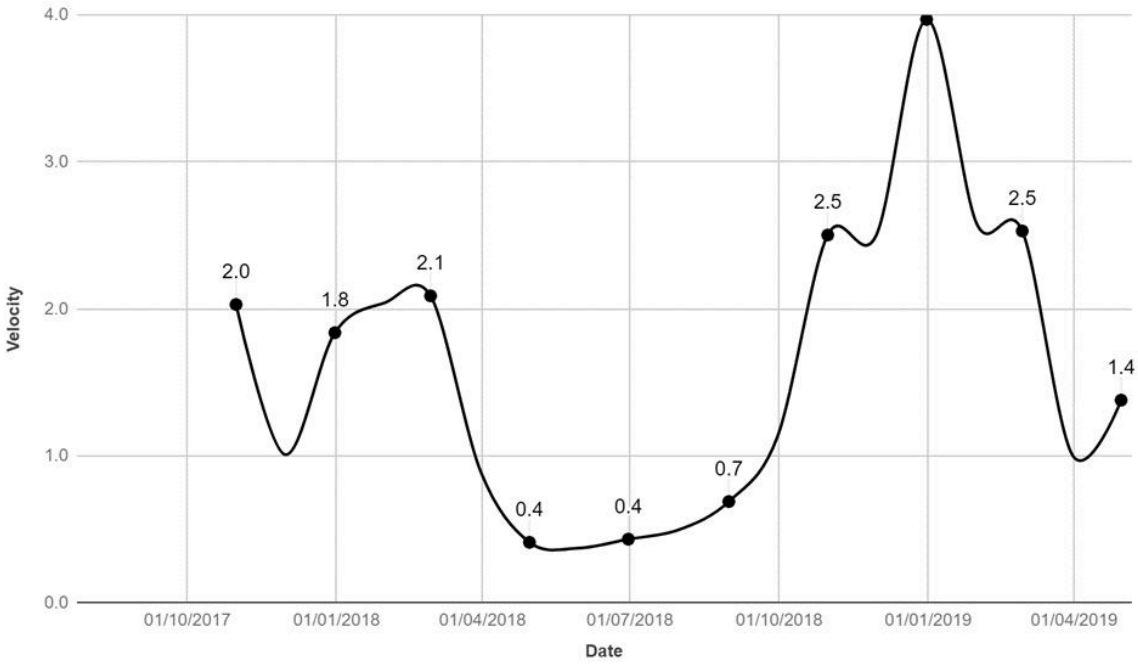
Having this in place, and having already estimated the USD equivalent of the staked tokens, based on the company's revenue projections, we can now estimate the actual circulation of tokens:

The GDP or Revenue of the system. This is based on the company's 5-year plan (upon successful ILO). The plan is based on the respective total addressable markets and assuming a very conservative 0.1% penetration of those markets within 10 years.



Projected company performance & growth, based on financial assumptions provided as-is by the company.

Token velocity. The token velocity is possibly the hardest and most sensitive assumption to make out of all. In order to get an adequate estimate of the expected velocity, we have used the Binance coin as benchmark (due to the similarities between BNB and $SHLD , as both are used for fee settlement and purchase of services on their respective platforms). We took a look at Binance's on-chain velocity (shown below). The reason to not include the off-chain velocity is that there has been multiple reports for exchanges reporting fake trade volumes[1], and as such, we do not think we can trust any exchange data at 100%.



BNB Velocity of On-Chain Transactions. Calculation is based on annualised 90 average transaction value.

Based on the above assumptions, and the outlined methodology, we can estimate the following figures:

Year	1	:	$0.35
Year	2	:	$0.99
Year	3	:	$2.34
Year	4	:	$4.96
Year	5	:	$9.25

[1] https://dashnews.org/report-majority-of-exchange-volume-is-fake-highlights-need-for-real-adoption/

It is important to point out that the fair price (scope of this document) aims to estimate the price of the $SHLD token solely based on its utility value. The actual price of the $SHLD token is likely to include a lot more speculative action (as with most financial assets) and will factor in, the expectation form investors for price appreciation as well as other uses of the $SHLD token which are not part of the original token design.

As Ray Dalio (American billionaire investor, founder of investment firm Bridgewater Associates, one of the world's largest hedge funds) recently said[1]:

“As you know, market pricing reflects expectations of the future; as such, it paints quite detailed pictures of what the consensus expectation of the future is. Then, the markets move as a function of how events transpire relative to those expectations. As a result, navigating markets well requires one to be more accurate about what is going to happen than the consensus view that is built into the price. That’s the game. ”

In other words, given that $SHLD token’s fundamental utility value is expected to appreciate above the ILO price, we do not expect that at any given point in time, the token will be traded below this price, unless the financial projections change.

[1] Ray Dalio (2019) Paradigm Shifts - https://economicprinciples.org/downloads/Paradigm-Shifts.pdf

www.web3shield.com
info@web3shield.com
www.linktr.ee/Web3Shield