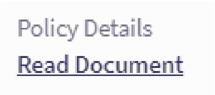
Unslashed General
Claims Acceptance Rule sets

This document details the acceptance criteria of claims submitted to Unslashed decentralized crypto-insurance protocol by insured Ethereum addresses.

This policy serves one main purpose:

Ensuring only valid claims submitted by insured addresses are accepted.

The jurors are expected to refer to the specificities of each individual cover policy (such as the name & address of the insurance tokens, the contracts & custodians covered and other coverage details) which are shared in the “Policy Details” section



Policy Details

Read Document

In case of any discrepancy between a specific cover policy and this general claims acceptance policy, the specific policy should be considered as the source of truth.

Who can submit a claim?

Any Ethereum address which owned the insurance token of the Unslashed Cover in question at least one block prior to the occurence of the event covered (as defined in each cover policy) then uses it to file a claim.

Claim Acceptance Criteria

Policy Period

The policy begins as soon as the insurance token of the Unslashed Cover in question is in the insured address (or held by any other authorized address or custodian as specified in the relevant cover policy)

The policy ends:

- at the expiry date as defined on the Unslashed User Interface and smart contracts; or

- as soon as the insured address doesn’t contain the aforementioned insurance token anymore.

Guidelines for claim acceptance

For “Smart Contract Integrity” covers

The claim will be accepted under this policy if:

- the loss is related to the Smart Contract Network described in the relevant cover policy; and
- the loss occurred due to an unauthorised, malicious or criminal act aiming at exploiting covered smart contracts’ code vulnerabilities; and/or loss occurred due to errors or omissions in code implementation, or unavailability or failure to access or process these covered smart contracts; and
- the loss occurred during the policy period.

For “Dollar Peg Stability” covers

As the covered stablecoin is pegged to the US dollar, it can happen that the covered stablecoin trades above or below peg.

The claim may be accepted under this policy if:

- the loss is related to covered stablecoin-US dollar peg, covered stablecoin trading below $0.95 on CMC, Coingecko or other sources; and
- the loss on covered stablecoin-US dollar peg results in a TWAP, based on market data extracted from reputable sources, below $0.95 in a two-week span at least; and
- the loss occurred during the policy period.

For “ETH 2.0 5% validator slashing” covers

An ETH2.0 validator is exposed to slashing penalties.
A slashing happens when a validator breaks the rules of the ETH 2.0 consensus, for example by double signing a slot. A penalty can also happen for going offline for a certain period of time.

A claim may be accepted under this policy if:

- the penalties have been accumulated for two months maximum; and
- the penalties amount to a maximum of 5% of the staked amount; and
- the penalties occurred during the policy period.

For “Wallet protection” covers for smart contract wallets

A claim may be accepted under this policy if:

- the loss is related to the Smart Contract Network described in the relevant cover policy; and
- the loss occurred due to an unauthorised, malicious or criminal act aiming at exploiting covered smart contracts' code vulnerabilities; and/or loss occurred due to errors or omissions in code implementation, or unavailability or failure to access or process these covered smart contracts; and
- the loss occurred during the policy period

Guidelines for claim rejection

For "Smart Contract Integrity" covers

A claim may be rejected if the loss:

- is due to the operation of a computer virus, a phishing attack, a hack or any other malicious activity where the smart contract continued to behave as intended; or
- is related to a hacked Smart Contract Network for which a hack or bug has been made public before the beginning of the policy period; or
- is due to a false business logic in the code which entailed a bug an arbitrageur was able to exploit; or
- is due to external inputs such as oracles - including price feed manipulation - or miner behavior, network congestion, etc. which didn't operate as intended but the covered Smart Contract Network continued to behave as intended; or
- is related to an attack vector which was communicated in protocol documentation; or
- is related to the act of breaking trust assumption, whether through decentralized governance or admin key abuse; or
- is related to a smart contract or set of smart contracts which was generated for the sole purpose of submitting a claim and getting cover, and not to be used by other users.

For "Dollar Peg Stability" covers

A claim may be rejected if the loss:

- is due to the operation of a computer virus, a phishing attack, a hack or any other malicious activity where the covered stablecoin smart contract continued to behave as intended; or
- is related to a hacked Smart Contract Network for which a hack or bug has been made public before the beginning of the policy period; or
- is due to a false business logic in the code which entailed a bug an arbitrageur was able to exploit; or
- is due to external inputs such as oracles - including price feed manipulation - or miner behavior, network congestion, etc. which didn't operate as intended but the covered stablecoin Smart Contract continued to behave as intended; or

- is related to an attack vector which was communicated in the covered stablecoin documentation; or
- is related to the act of breaking trust assumption, whether through decentralized governance or admin key abuse; or
- is related to a smart contract or set of smart contracts which was generated for the sole purpose of submitting a claim and getting cover, and not to be used by other users.

For “ETH 2.0 5% validator slashing” covers

A claim may be rejected if the penalties:

- have been accumulated for more than two month; or
- exceed a maximum of 5% of the staked ETH amount.

For “Wallet protection” covers for smart contract wallets

A claim may be rejected if the loss:

- is due to the operation of a computer virus, a phishing attack, a hack or any other malicious activity where the smart contract continued to behave as intended; or
- is related to a hacked Smart Contract Network for which a hack or bug has been made public before the beginning of the policy period; or
- is due to a false business logic in the code which entailed a bug an arbitrageur was able to exploit; or
- is due to external inputs such as oracles - including price feed manipulation - or miner behavior, network congestion, etc. which didn’t operate as intended but the covered Smart Contract Network continued to behave as intended; or
- is related to an attack vector which was communicated publicly including in protocol documentation prior to the event; or
- is related to the act of breaking trust assumption, whether through decentralized governance or admin key abuse; or
- is related to a smart contract or set of smart contracts which was generated for the sole purpose of submitting a claim and getting cover, and not to be used by other users.