Smart Contract Cover

This document sets out what events are covered and not covered by Nexus Mutual's Smart Contract Cover. It should also be used as a reference document by Nexus Mutual Claims Assessors when considering any Smart Contract Cover claim.

The document is deliberately kept high-level in order to allow for a pragmatic consideration of each individual claim by Claims Assessors.

These terms and conditions of Cover are held off-chain and interpreted by humans (Nexus Mutual Members). They are **not** part of the Nexus Mutual smart contract code.

All Cover is provided on a discretionary basis, with Nexus Mutual members having the final say on which claims are paid.

Cover

The Mutual may pay a claim under this Smart Contract Cover if:

- the designated smart contract address, or a directly related smart contract address in the case of a **smart contract system**, suffers a hack during the **cover period** that is a direct result of its smart contract code being used in an unintended way; and
- there is a **material loss of funds** from the smart contract, or **smart contract system**, due to the hack, with funds either:
  - moved to another address which the original owner or owners do not control; or
  - made permanently irrecoverable;

  and
- for covers where the cover period began after 21-Oct-2020 09:00:00 UTC, **cryptographic evidence** is provided that links the **impacted account** to the Covered Members account that is submitting the claim; and
- the Covered Member submits a claim during the cover period or within 35 days of the cover period ending.

Definitions

Cover amount means the amount of Cover specified by the Covered Member at purchase of Smart Contract Cover.

Cover period means the period of time, in days, that a Covered Member is protected under this Cover, chosen by the Covered Member when purchasing Cover and stated in the Member Smart Contract Data.

Cryptographic evidence means;

- where the Covered Members account is impacted directly, the submission of a claim will be taken as that evidence;
- where an account that is not a Covered Member is impacted;
  - a cryptographically signed message from the impacted account that references the Covered Members account address; or
  - the transaction hash of a zero value transaction from the impacted account to the Covered Members account; or

- other equivalent cryptographically signed evidence that links the impacted account to the Covered Members account.

Impacted Account means:

- an account which directly suffered a loss as a result of the hack; or
- where the cover holder is directly related to the team or individual who built or deployed the smart contract system, an account that either deployed the smart contract system or is otherwise publicly known as having built the system.

Loss of funds means the total funds lost caused by the hack not the loss of the individual Covered Member.

Material means:

- far exceeds gas related costs involved in operating the contract;
- the total funds lost are at least 20% of the **cover amount**.

Smart Contract System means a single smart contract or group of directly related smart contracts running on the public Ethereum network excluding any outside inputs to that system such as oracles, miners, the underlying Ethereum network and individuals or groups of individuals interacting with the system.

Exclusions

The Mutual does not provide Cover:

- for loss of funds due to phishing, private key security breaches, malware, exchange hacks or any other activity where the covered smart contract continues to act as intended;

- any claims if the smart contract or **smart contract system** was deployed primarily for the purpose of claiming on this Cover and not for real usage by customers;

- for any hacks occurring during the **cover period** if a hack occurred or a public bug disclosure was made for the designated smart contract address, or a directly related smart contract address in the case of a **smart contract system**, before the **cover period** began;

- for any events where inputs, that are external to the **smart contract system**, behave in an unintended way and the **smart contract system** continues to operate as intended, where inputs include but are not limited to; oracles, governance systems, incentive structures, miner behaviour and network congestion.

Cover Termination

Cover ends when:

- there has been a successful claim on the Cover; or
- the **cover period** specified at purchase has ended.

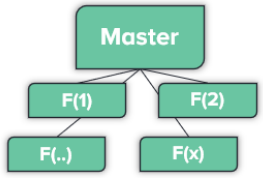
Smart Contract Systems

Most mainstream Ethereum applications are reasonably complex and so consist of a number of smart contracts all working together. The intention of Smart Contract Cover is to allow users to cover just one "lead" smart contract which represents cover against unintended uses of the whole system.

Some example cases for determining a "lead" contract are as follows:

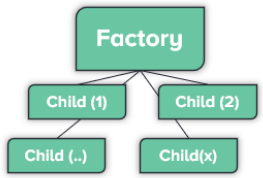
Product Structure with Smart Contract Systems

Case 1: Complex System



Eg: MakerDAO, Nexus, Augur

Case 2: Factory Contracts



Eg: Uniswap, Argent, Gnosis Multi-sig

Pricing / Quote	**Covered Member >** Chooses Master or Factory as the covered contract.
Risk Assessment	**Risk Assessor >** Stakes against Master or Factory
Claims	**Covered Member >** Gets paid on a bug/hack against either; a) Master or any of F(1), F(2), F(..), F(x); or b) Factory or any Child