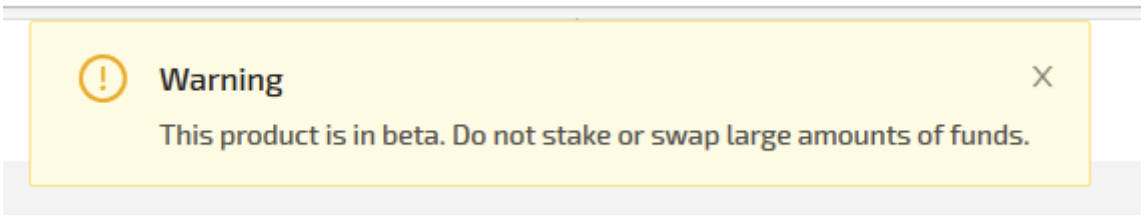
THORChain Chaosnet Risk Summary

A brief summary of Chaosnet risks, read this before using the network.

Kai Ansaari
Aug 27 · 10 min read



Chaosnet Risk Warning

- Chaosnet is a decentralized network, you are interacting with a network which is not within the control of the THORChain team.
- Chaosnet is an experiment in liquidity and security, it's high risk and not for use by new users.

- Chaosnet has mainnet assets at risk which act as an incentive to encourage attacks on the network by profit seeking actors. *All assets staked, bonded or being swapped are at risk of permanent loss.*

- By participating in Chaosnet you understand that you're taking full responsibility for any potential loss of assets; neither node operators nor THORChain team will be held accountable.

If you're still thinking about participating, read on…

Background

THORChain is a **decentralized liquidity network** which has been in active R&D for the past two years. THORChain enables cross-chain asset swaps in a permissionless & trustless setting via continuous liquidity pools.

The THORChain team have released their first live product on mainnet dubbed *'Chaosnet'* enabling BEP2 asset staking & swapping for the first time.

Chaosnet is designed to expose the network to scrutiny & attack in order to prove the security & economic incentives are correct; and to demonstrate the network is resilient, performant and overall fit-for-purpose.

The rationale for Chaosnet is based on game theory & behavioral economics *ie. without genuine incentives for all agents it's not possible to test the hypothesis or design assumptions underpinning the network.* Chaosnet is a vital step before THORChain's mainnet.

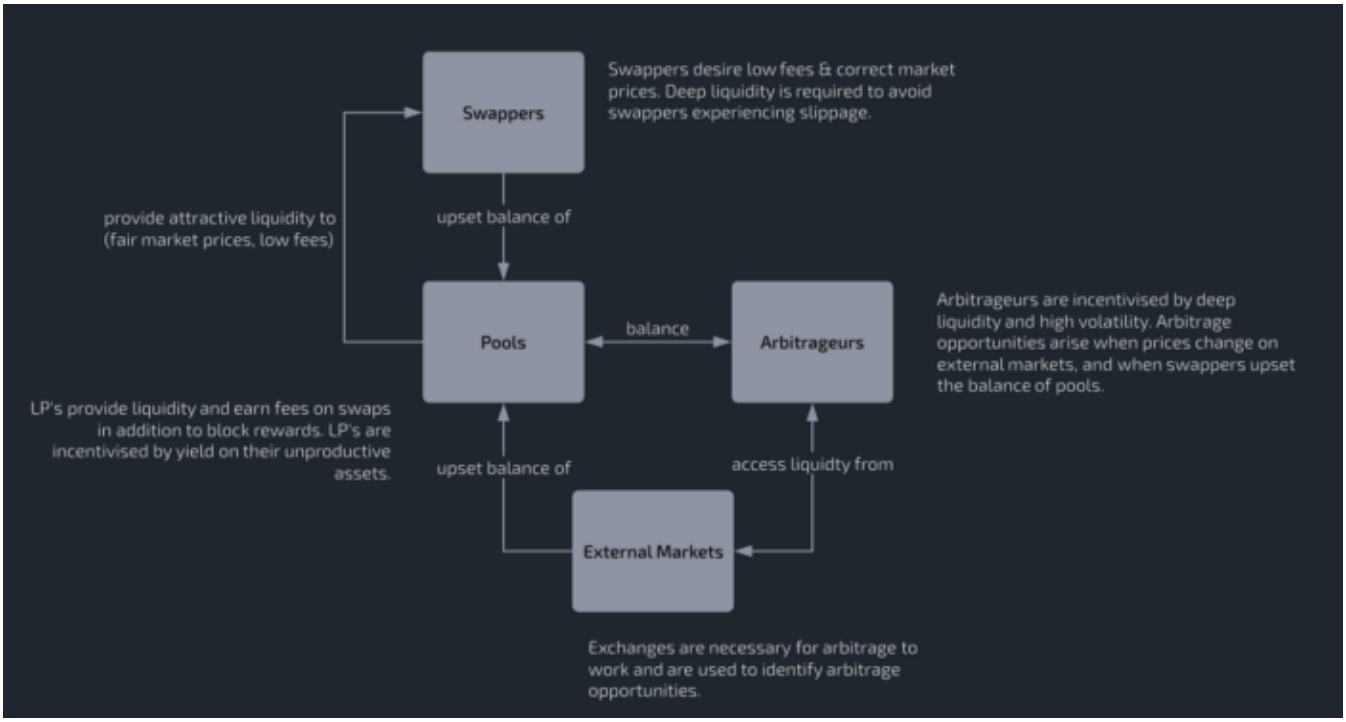
The following sections are designed to make the community aware of the key risks.

THORChain Overview

THORChain is an application specific blockchain built upon Tendermint BFT & Cosmos-SDK to facilitate decentralized, permissionless cross-chain staking & swapping via liquidity pools.

Primarily this is achieved using a constant product market maker (AMM) as mechanism for asset exchange; and Threshold Signature Scheme Cryptography (TSS) for securing assets in vaults & signing transactions.

Asset holders provide liquidity into pools by making on-chain transactions which swappers then take advantage of. THORChain uses one-way state pegs to observe events on connected chains and thus does not use two way pegs or representative assets.



Liquidity Providers (LPs) are incentivized to provide liquidity through block rewards and liquidity fees. **Swappers** are motivated to swap across pools by virtue of its deep liquidity, fair market prices & low fees; and owing to its permissionless and trustless nature. Since there are no external price oracles, **arbitrageurs** keep pools balanced to correct ratios in order to ensure assets are priced fairly.

The network is run by anonymous **nodes** (THORNodes) who run software to keep the network operational. Nodes facilitate staking and swapping via observation consensus, after which THORChain's state changes & becomes instantly final. Nodes also participate in multi-party computation to sign outgoing transactions using threshold signature schemes.

TLDR; THORChain is a decentralized liquidity network connecting blockchains together in a marketplace of liquidity. It's permissionless, trustless and manipulation resistant; and constitutes a paradigm shift in liquidity.

Chaosnet Objective

THORChain is live on mainnet and released to the public under the 'Chaosnet' designation. This comes with significant risk for ordinary users & power users alike.

There is a likelihood that use of Chaosnet and BEPSwap will result in loss of staked or bonded assets, as well as those being swapped.

Chaosnet is an experiment in digital asset liquidity and serves two key functions related to the security & economic design assumptions.

Persistent security bounty
Mainnet assets incentivize agents to attack the network for a potential reward.

Assets bonded & staked on the network therefore could be drained, stolen or irrevocably lost through malicious actors, disruptive node behavior or technical malfunction.

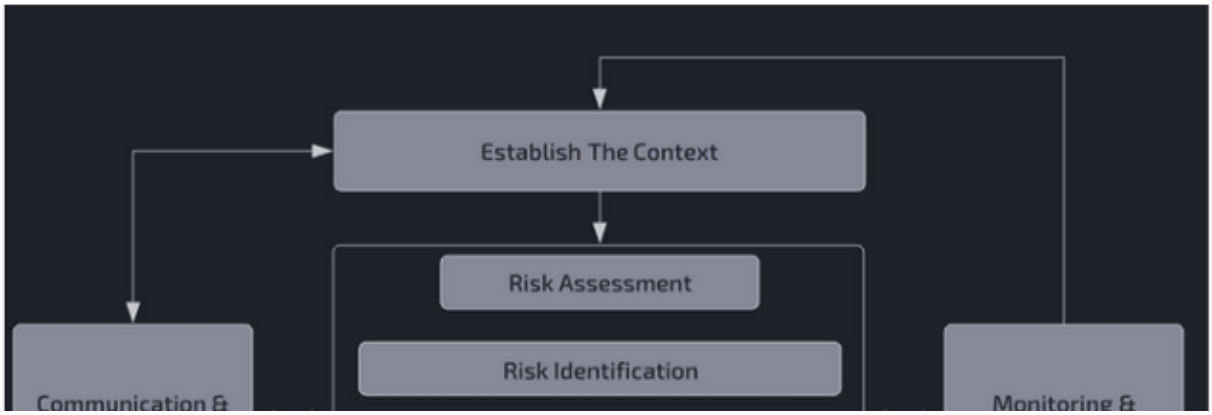
Live test of the economic model
Mainnet assets incentivize node operators to bond capital, LP's to pool liquidity, arbitrageurs to balance pools & swappers to access liquidity.

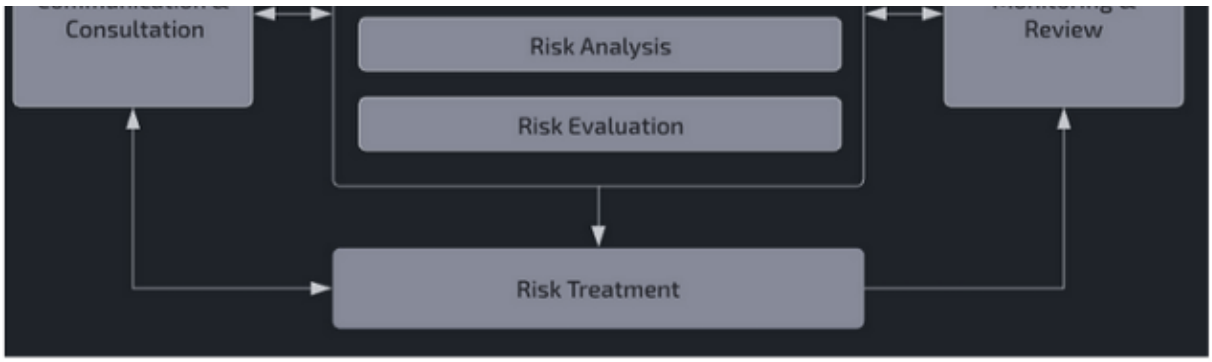
Liquidity may be lost or eroded temporarily or permanently due to the economic design of liquidity pools. This includes staking, swapping & arbitrage.

Key Risks

The THORChain team leverage industry standard risk management (eg. ISO3000) and quality frameworks (eg. ISO90001/ISO25010) in both project operations and product development processes in order to deliver high quality product and minimize risk.

This section covers only key risks from the risk management process and is not designed to be exhaustive. The team will constantly monitor & review risks as time goes by.





Risk Management Process — ISO3000:2009

THORChain is built on embryonic technology brought together in configurations never tested before. While the team have taken measures to minimize the likelihood of things going wrong, risks in crypto remain latent and difficult to identify & quantify .

Accordingly the risk profile for THORChain remains *relatively high* based on these unknown/unknowns.

The following key risk areas are put forward for consideration using generic linguistic scales based on qualitative risk analysis.

Nb. Impact scales are based on users not deploying more capital than they can afford to lose.

R0: Network Malfunction

Med Likelihood / Low Impact
Chaosnet is the first live test of the network in a real world scenario. While 5 testnets have proven the network to be resilient there may still be latent defects/bugs.

- There is the potential for the network to experience a p1 issue which would halt or bring down the network. In this situation users would be unable to withdraw liquidity, unbond or have their swaps fulfilled.

In all prior situations the network has been upgraded on the fly which provides some confidence that in the event of a serious defect/issue/malfunction, there is a serviceable solution for patching issues on the fly.

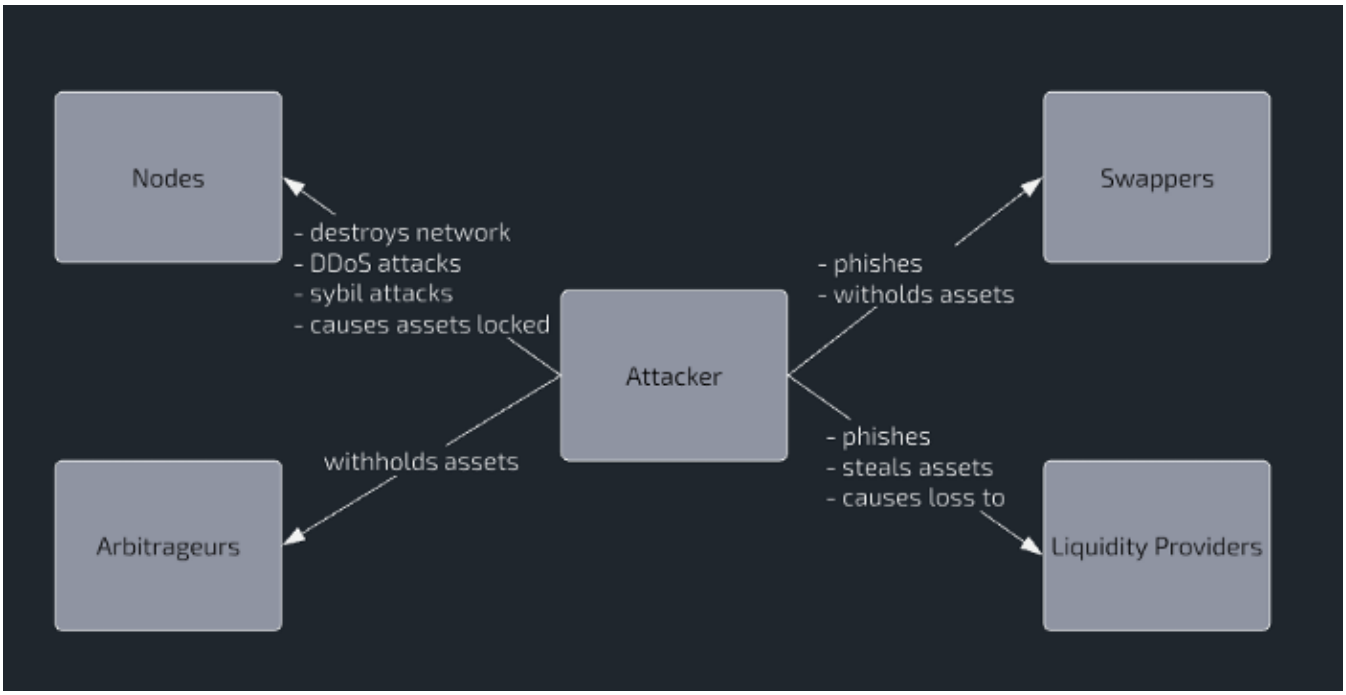
R1: Network attack / asset theft

Med Likelihood / Med Impact
Chaosnet is a decentralised, permissionless network based on game theory and using

complex & immature technology. There are likely many attack vectors which have not been identified during audits and testing.

- The network may be subjected to attack by irrational or profit seeking actors. Assets on the network may be totally drained/stolen including bonds, pooled liquidity and any assets in the process of being swapped.

Users should not bond, stake or swap more assets than they can afford to lose.



Key attack scenarios / impact

R2: Node operators may lose bond

Med Likelihood / Med Impact
Node operators bond capital to secure the network and underwrite staked capital. Operating a node is a serious business and comes with risk which is why rewards are extremely high.

- The network may be subjected to attack which would drain assets on the network.
- Nodes may be unreliable, malfunction or go down leading to nodes accruing slash points.
- In the event of a delegated yggrasil transaction being missed, the node may be slashed 1.5x the value of the transaction.

- A node operator may send a RUNE bond to an old bond address resulting in total loss of bond.
- A node operator may forget/lose access to their wallet with no means to access the returned bond when churned out.

Node operators should carefully consider the risks before becoming a THORNode operator.

R3: Liquidity Providers may lose assets

Med Likelihood / Med Impact
Liquidity Providers (aka Stakers) send assets to the network in order to "pool" them to earn fees on swaps and a share of the block rewards. LP's surrender these assets and own a share of the pool. LP's can withdraw their share of the pool by signing a transaction with their private key.

- The network may be subjected to attack which would drain pooled assets on the network. Nodes may be unreliable, malfunction or go down leading to loss of funds. It is possible for funds to be trapped in vaults forever.
- Pooled assets may experience impermanent loss if one asset moves strongly against another. The LP will then own more of one asset and less of the other.

R4: Swappers may lose their assets

Med Likelihood / Med Impact
Swappers send assets in order to swap them for other assets. eg. BNB > RUNE. Swappers pay fees and experience a slip based during this process.

- The network may be subjected to attack which would capture those assets and/or prevent the outgoing swap from being completed.
- Nodes may be unreliable, malfunction or go down leading to loss of funds during the swap process. It is possible for funds to be trapped in vaults forever.
- Pools may be imbalanced resulting in the swapper experiencing a high slip and therefore losing value on a swap.
- Swappers may not understand or have awareness while using BEPSwap and will approve swaps which are not advantageous to their position. Eg. wrong asset, high slip.

R5: Participants may expose their identity

Low Likelihood / High Impact
Participants in the network have many touch points with THORChain both technical & non-technical. eg. THORNodes, API's, interfaces, on-chain transactions, telegram, twitter etc.

- THORNodes expose themselves via public IP's which can be linked to their identity.
- Users of BEPSwap or other interfaces expose their public IP's which may be linked to their identity.
- On-chain transactions in/out of THORChain may be analysed by third parties and linked back to identities via on/off ramps.
- Communication with the team can be linked back to a users identity via social media accounts.

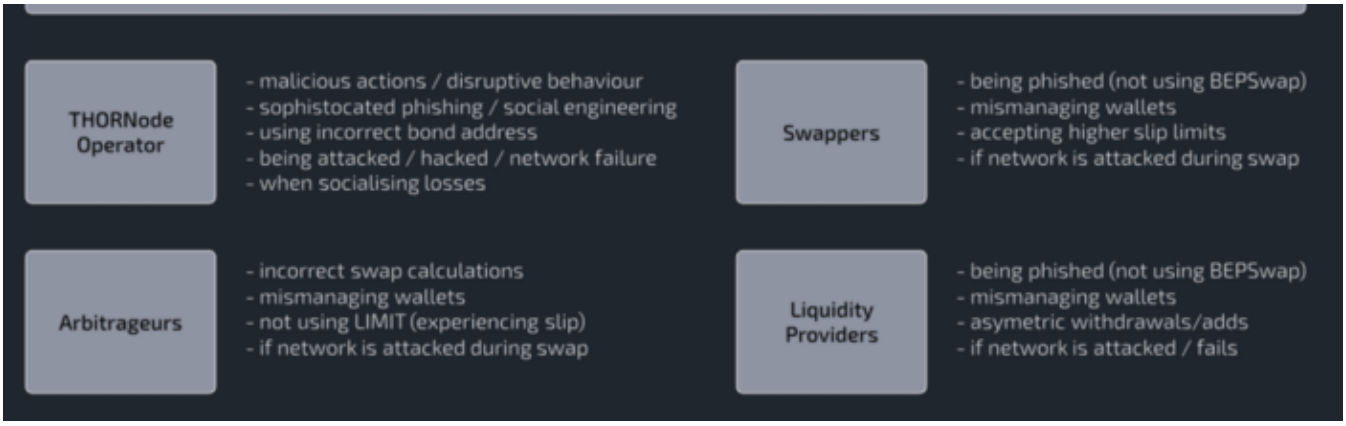
The risk of publicly identifiable information have privacy & security implications and may result in loss of digital assets, identity theft etc. This is entirely within the users sphere of influence. Interaction with THORChain should be done at your own risk.

R6: Phishing attacks

High Likelihood / High Impact
THORChain's code repositories are public with opensource licenses. It is trivial to fork the BEPSwap interface and trick users into using the malicious interface. Phishing is an extremely common scam and the team fully expect to see them spring up soon after launch.

- There is a high risk of fake BEPSwap interfaces being launched in order to steal assets from users. Domains will be registered for common domain mis-spellings, coordinated campaigns will be run to trick users into using malicious interfaces. Telegram, Discord and Twitter users will receive messages containing links to malicious interfaces.

Users should never click on any link to BEPSwap unless it's from the THORChain website, twitter, telegram or discord group. Users should also make small test transactions before staking or swapping and verify pool addresses with the THORChain team on telegram.



Mitigation Efforts

The following common mitigation strategies have been employed to reduce the risk profile for Chaosnet.

- **Audits:** Three external audits were completed. Certik (code quality), Kudelski (TSS implementation), Gauntlet Network (Multi agent simulation). The fourth audit commences soon (Infra/Security/Code) and will be completed during the operation of the network.
- **Public Testnets:** Multiple testnets have coordinated over the past two months involving community run nodes. Where defects/bugs were identified, the network was upgraded live without issue in cooperation with node operators. The current upgrade path remains viable.
- **Internal QA/QC:** The team has an effective quality assurance process which ensures all code is peer reviewed prior to being released. Unit test coverage exists for all code and CI/CD processes include integration testing. Functional testing and other forms of testing eg. regression testing, performance testing, pen testing are continually undertaken by the team. Several 'red teams' have been undertaken to attack the network & simulate live attack scenarios.
- **Economic Design:** The team has spent considerable time in R&D to validate & test the economic model so that key participants in the network will not suffer loss under normal circumstances. eg. Swapping / Staking. Returns for network participants is expected to be attractive and without loss.

Other avoidance and mitigation strategies have been and will continue to be employed to reduce the risk profile further. More information will be made available in future updates.

Contingent Response Strategy

During Chaosnet social media will be relied on heavily to provide updates about the network, including twitter, telegram and discord. The team will immediately disclose any issue affecting the network and will continue to update the community until resolution.

The team have responses planned for several scenarios, and in the event of a major issue request the community keep telegram chatter to a minimum so the team are able to communicate effectively and work with affected members to diagnose and resolve issues.

Should the network require an upgrade, the team will work with node operators to coordinate an emergency upgrade. In this situation the team rely on THORNode operators and therefore may experience a delay in getting the network back online. THORNode operators have been asked to monitor communication channels regularly for any emergency maintenance.

Responsible Disclosure

In the event you have discovered a vulnerability, contact the team immediately via twitter, telegram or discord. The team have allocated budget for security bounties and will reward those who uncover attack vectors at all levels of the technology stack. Links to socials can be found at the bottom of this blog.

Final Words

Chaosnet is an exciting moment in THORChain's history. Your participation is vital for product validation and will accelerate development toward multi-chain Chaosnet later this year.

In an ideal world the risks of using magical internet money in new DeFi products would be assumed & implied, but history has shown that's not the case. The team therefore asks the community to exercise caution during Chaosnet.

Community

To keep up to date, please monitor community channels, particularly Telegram and Twitter:

- **Twitter**: https://twitter.com/thorchain_org
- **Telegram Community**: https://t.me/thorchain_org
- **Telegram Announcements**: https://t.me/thorchain
- **Reddit**: https://reddit.com/r/thorchain
- **Github**: https://github.com/thorchain
- **Medium**: https://medium.com/thorchain