Third Wall Litepaper V0.3 (September 20th 2021)

By Ayla Goulding and Daniel Volkov

The Problem:

As of September 20th 2021, there are $173 billion in assets locked in DeFi protocols and over $1 billion has been stolen in smart contract hacks [1]. We believe DeFi protocol risk management will be necessary to onboard institutions and the next billion everyday users. DeFi needs an additional layer of protection, and that is what we are building at Third Wall.

Protocol	Blockchain	Value Lost
PolyNetwork	PolyNetwork	$600 Million
Parity	Ethereum	$160 Million
EasyFi	Ethereum	$59 Million
Uranium Finance	Binance Smart Chain	$57 Million
DAO	Ethereum	$50 Million
Parity	Ethereum	$30 Million
dForce	Ethereum	$25 Million
Pickle Finance	Ethereum	$20 Million
Yearn	Ethereum	$11 Million
Maker	Ethereum	$9 Million
bZx	Ethereum	$8 Million
Warp	Ethereum	$8 Million
Cover	Ethereum	$4 Million
Total		$1.1 Billion

Current risk management solutions are inadequate. At Third Wall, we strongly believe that our automated architecture will become the gold standard for DeFi coverage.

Current Landscape:

Alternative 1 -- Centralized Insurance Providers

Centralized insurance providers are a single entity that underwrites policies, validates incidents, and pays out claims. Centralized insurance providers have incentives to act against the best interests of their customers as they make more money when they payout fewer claims. Furthermore, they typically have a very tedious claims process.

Centralized insurance providers are also heavily regulated, which adds additional costs compared to decentralized alternatives. It is estimated that “35% of all

customer premiums are lost to frictions/overhead” in the centralized insurance world [2]. We are not aware of any centralized insurance provider that is currently offering DeFi insurance. However, even if they do enter the space, we believe they will remain a higher-cost product compared to on-chain alternatives that take advantage of frictionless blockchain technologies.

Alternative 2 -- On Chain Voting Systems

The majority of DeFi coverage sold today falls into this category. Nexus Mutual is the biggest player in on-chain voting insurance. We certainly commend Nexus Mutual for bringing insurance into the 21st century when they launched their on-chain coverage platform in 2019. By using the blockchain to validate and distribute claims, Nexus created a system which should be more efficient than centralized providers.

However, the problem with Nexus Mutual is a lack of objectivity. Nexus Mutual claims are assessed and validated by $NXM token holders. At the same time, $NXM stakers are also responsible for paying out claims. Because of this lack of objectivity, in the event of a hack where a lot of value was insured, there is no guarantee that $NXM holders would vote to pay out. So far Nexus has only had to pay out small amounts compared to the amount they insure.

Theoretically, these $NXM holders should consider the long-term interests of the protocol and try their best to pay out valid claims. But how can policyholders really be sure they will be fairly compensated in the event of a large hack? The only backstop is a nebulous vote from the Nexus “Advisory Board” threatening to burn staked $NXM if dishonest voting is detected.

This is how Nexus Mutual describes their approach in their whitepaper: “Designing incentive structures resilient to game theoretic attacks is very challenging. The approach described has a basic incentive structure at its core and then overlays timing windows and human intervention to prevent more extreme scenarios.” [3]

As DeFi matures and more traditional institutional investors come into this space, an anonymous, voting-based insurance solution will not be a convincing security model. Furthermore, Nexus’s voting mechanism also goes against the ethos of DeFi in some ways. In the ideal case, no party needs to trust any other one. Nexus Mutual and its clones are built on shaky ground, and the DeFi community needs a better alternative.

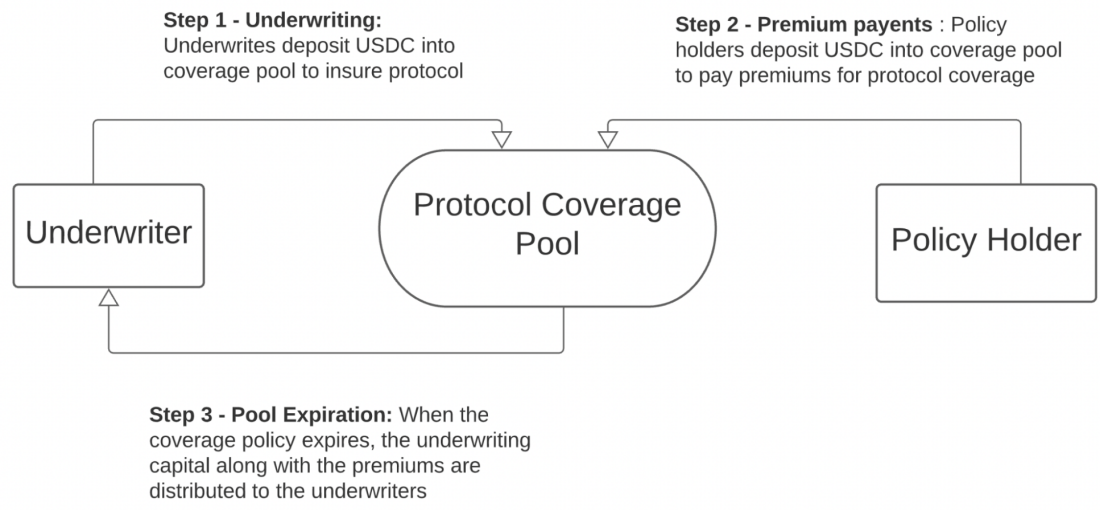
Third Wall

Third Wall is a decentralized risk-management protocol. Instead of relying on a centralized institution or a set of voters, Third Wall uses smart contracts to hold underwriter capital and pay out claims.

We plan to launch two different architectures (“Optionality” and “Automated Claims”), each of which may be more suited for protecting different protocols. We will start by launching “Optionality” and later launch “Automated Claims” based on market demand.

Third Wall Architecture: Shared Framework

Both architectures use a common base layer. In both, there is one pool for each coverage policy. Underwriters deposit capital in the pool and policyholders pay premiums to the pool.



At expiration, underwriters can withdraw premiums as well as their underwriting capital if it hasn't been claimed by policyholders in the event of a hack.

When you deposit into Compound or Aave or Alpha, you receive **redemption token** with the right to withdraw the underlying assets. For example, cUSDC is Compound's redemption token for USDC [4]. Redemption tokens are used in many DeFi protocols, including yield farming vaults and other money markets.

At launch, we will be taking a conservative approach. Underwriters will deposit base-level assets like USDC or WETH to underwrite coverage for these redemption tokens. Both architectures work the same way with any redemption token. However, the underlying asset will vary depending on the type of redemption token. Some examples:

Redemption Token:	Underwritten By:
cUSDC from Compound	USDC
aWETH from Aave	WETH
3CRV from Curve	USDC

Later we will allow underwriters to underwrite with productive assets, and enable the same assets to be used for underwriting multiple pools. These changes add risk to the protocol, but significantly improve underwriter returns while reducing premium costs for policyholders. These changes will be necessary if underwriters are to receive acceptable returns in the long-term.

Third Wall Architecture: "Optionality"

Third Wall's "Optionality" architecture is simpler and the most secure but is only compatible with protocols that utilize the redemption tokens we defined above. "Optionality" uses no claims processing components. Instead, we use something akin to a put option on redemption tokens to provide coverage.

Here is an example: Say we are looking to protect USDC deposits on Compound. To underwrite, underwriters deposit USDC into Third Wall's cUSDC coverage pool.

Anyone can purchase this Compound USDC coverage by paying premiums to the underwriter pool. In return, they get the right to trade their cUSDC for USDC from the underwriter's capital **at any time**. What you get with this architecture is the certainty of knowing you always have assets backing you up that you can claim at any time. This power allows any crypto user to use DeFi with absolute confidence.

The "Optionality" architecture is also highly scalable. Each time a coverage policy is created for a new protocol, or a protocol upgrades its code, new claims checker contracts would have to be written for "Automated Claims." But with "Optionality" one set of contracts will work to protect many different protocols.

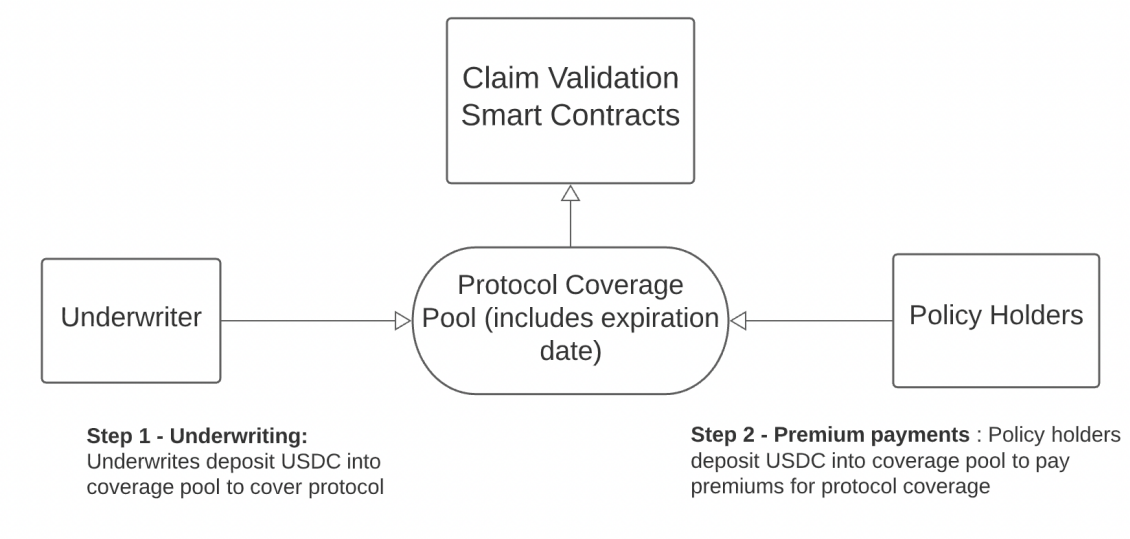
That means that our product has to be audited once and will work for many different protocols. This compares to the automated claims architecture, where a new audit has to be completed every time a new protocol is onboarded.

Third Wall Architecture: "Automated Claims"

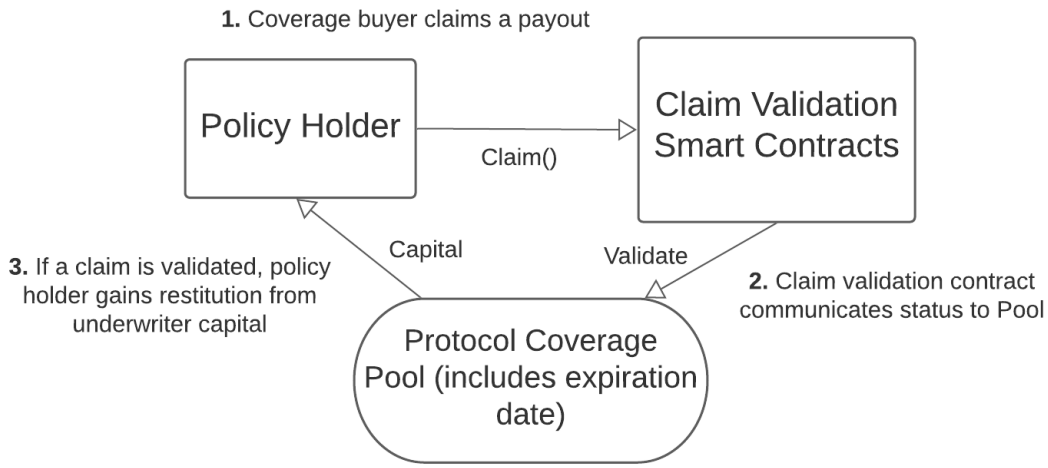
Our "Automated Claims" architecture will use smart contracts to check if certain conditions have been met to validate a claim, then automatically transfer funds from underwriters to policyholders when necessary. We will be working with DeFi protocols to craft simple and secure claim-checkers contracts that protect against the specific risks their communities are concerned about.

For example, we can cover Compound's USDC deposits by checking the redemption ratio of cUSDC. If there are fewer USDC backing each cUSDC, that indicates the cUSDC market has been hacked and USDC has been drained from Compound.

Another example -- we can provide coverage against DAI depegging from a baseline by checking a Uniswap TWAP (Oracle to capture data) to determine whether DAI has lost value relative to the baseline (i.e. by looking if DAI trades for less than 0.9 USDC).



If an exploit occurs, policyholders can call a claim() function which automatically checks on the state of the covered protocol and pays out funds if necessary.



Third Wall Governance Token

Down the line, we plan to introduce a Third Wall governance token. Holders will be able to vote on which coverage pools Third Wall will create. More details are forthcoming.

Conclusion

Protocol risk-management is a critical component of widespread DeFi adoption, allowing users to know their money is safe in the event of a hack. Providing the option to purchase coverage on a given protocol will enable many more conservative investors and institutions to feel safe using that protocol and DeFi in general.

Creating comprehensive coverage solutions may be one of the highest leverage opportunities to accelerate the transition to a decentralized financial system. This is why we are very excited to pursue this opportunity with our “Optionality” and “Automated Claims.” These architectures will simplify and de-risk the claims process, and will become the gold standard for protocol coverage.

Third Wall is focused on the long-term and building in the right way. That means building in public in a collaborative process with our community, and generously rewarding every single person that contributes to making the Third Wall a reality. We are inspired by the launches of projects like Uniswap, and want to see Third Wall become a fully decentralized cornerstone of the DeFi world.

References

[1] https://defillama.com/

[2] https://nexusmutual.io/assets/docs/nmx_white_paperv2_3.pdf

[3] https://nexusmutual.io/assets/docs/nmx_white_paperv2_3.pdf

[4] https://compound.finance/docs/ctokens