Reciprocally-Covered Assets:
A Peer-to-Peer Coverage Model for Decentralized Finance Assets

Robert M.C. Forster

October 27, 2021

Abstract

The decentralized finance industry is uniquely prone to financial losses through hacks, scams, and errors. The industry has responded to these threats by creating coverage protocols modeled after traditional insurance institutions to reimburse users in the case of lost assets. Proposed in this paper is a new model for coverage that uses the assets being covered as the underwriting funds for each other. This model emulates a traditional reciprocal inter-insurance exchange that uses assessable policies with no premiums paid upfront and that has no capital in reserve. It simplifies financial coverage to its most efficient form, drastically streamlining the user experience, removing the need for precise pricing in order to maintain solvency, ensuring supply grows with demand, and guaranteeing coverage costs exactly what it needs to cost.

1 Introduction

Blockchain technology's immutability, public nature, composability, and pseudo-anonymity provide the perfect conditions for funds being lost due to theft, scams, and error. With the advent of decentralized finance (DeFi)[1], these threats truly began to be realized. DeFi is an industry in which different aspects of the financial system–such as borrowing, lending, and trading–are replicated on blockchains in order to take advantage of the benefits of decentralization, and by nature it involves a large amount of capital. From September 2020 to September 2021, over $1.2 billion dollars was lost in DeFi hacks[2]. As the DeFi industry continues to grow, more and more funds will be at risk and more coverage will not only be desired but needed.

The current method of providing coverage to users against these threats is largely the same as with traditional institutions: underwriters provide funding, risk is assessed, a premium price is set for the coverage, and users purchase a coverage policy[3] [4] [5]. This method has proven successful to date but also has multiple shortcomings: the amount able to be covered depends on the underwriters' supply of capital, which will likely never allow for the full industry to be covered; leverage is required for underwriters to be adequately compensated, which introduces a risk of insolvency; and premium prices are exceedingly difficult to set given the data available and speed with which the industry is evolving.

2 Solution

2.1 Overview

Reciprocally-Covered Assets (RCAs) are a DeFi-native coverage method in which assets that are being covered simultaneously underwrite the other assets in the ecosystem. The system charges no premiums: payments are only made when loss occurs in one of the vaults of the ecosystem, at which point

[1] https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets

[2] https://rekt.news/leaderboard/

[3] https://documentation.unslashed.finance/

[4] https://docs.insurace.io/landing-page/

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

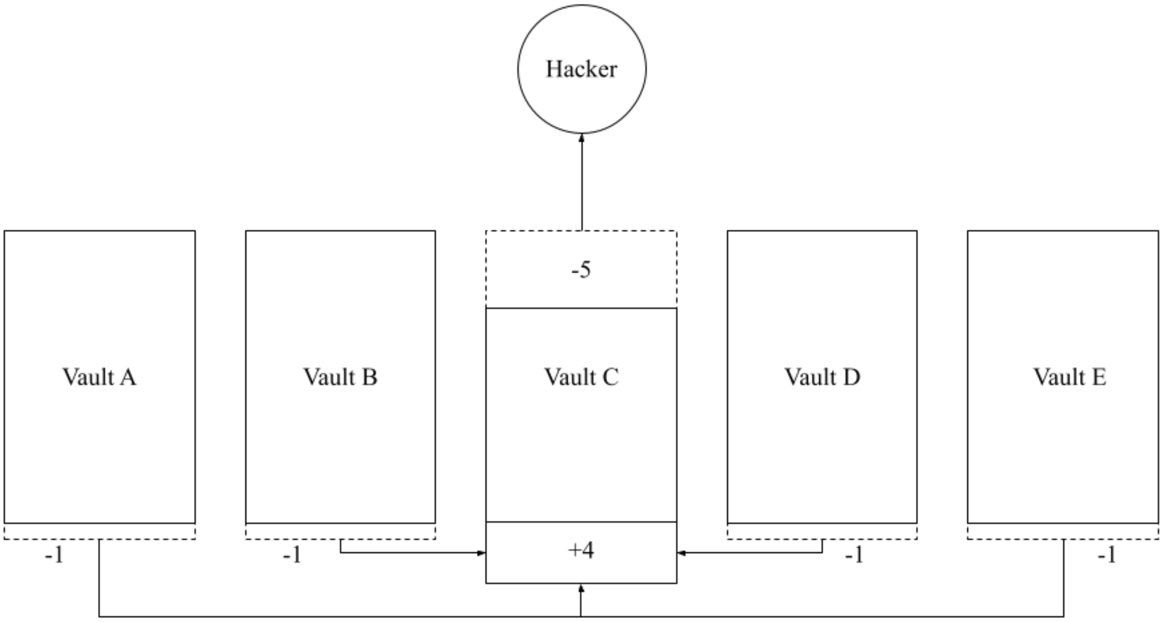

Figure 1: Functioning of a payout after a hack.

a small percentage of every vault is liquidated to compensate the affected vault.

RCAs act similarly to reciprocal inter-insurance exchanges[6] in which users/subscribers essentially cover each other against risk, although all policies are assessable with no premiums being paid in advance and there is no capital in reserve. They ease or remove all of the complications of traditional coverage: risk-based pricing, premiums, underwriting, supply problems, solvency, and more.

This method is only achievable in DeFi because it is exceedingly difficult for traditional finance to charge users retroactively in inconsistent and small amounts. With it, we create a system that always charges exactly what needs to be charged, never has coverage supply problems, never miscalculates risk, and is extremely resilient when the worst case scenarios occur.

RCAs are the first coverage method that is truly unique to DeFi, and the only coverage method with the ability to cover the total value in the sector.

2.2 User Experience

The user experience of RCAs is core to their success. To onboard, a user deposits their DeFi tokens (any token that may be at risk of losing value due to a hack, such as yield-bearing Yearn tokens[7] or liquidity provider Uniswap tokens[8]) into a vault and then, in return, receives tokens that represent their share of that specific vault. An example of this may be depositing yDAI tokens and receiving back arYDAI tokens, or depositing ETH:DAI UNI-V2 liquidity provider tokens and receiving back ETH:DAI arUNI-V2 tokens. This representative share is a reciprocally-covered asset that can be traded, sold, or redeemed for the underlying assets. It has coverage built into it: just by holding the asset, the user knows they will always have coverage for the value of their share of underlying tokens–no matter how much price changes.

This built-in coverage never expires, never requires premiums, and never needs to be updated.

[6] https://www.investopedia.com/terms/r/reciprocal-insurance-exchange.asp
[7] https://medium.com/yearn-state-of-the-vaults/the-vaults-at-yearn-9237905ffed3
[8] https://docs.uniswap.org/protocol/V2/concepts/core-concepts/pools

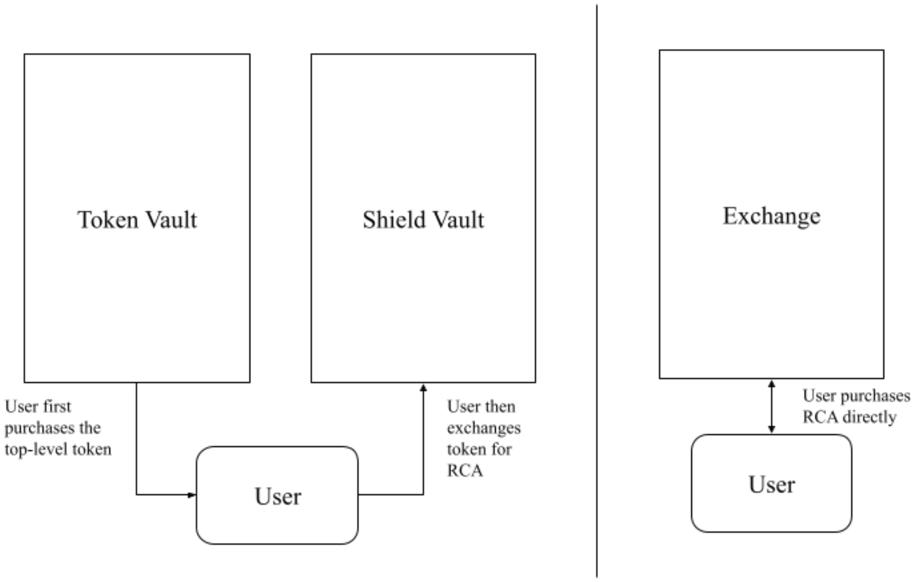
Token Vault
Shield Vault
Exchange
User first purchases the top-level token
User then exchanges token for RCA
User
User purchases RCA directly
User

Figure 2: Entering the RCA ecosystem.

Once the user enters the RCA ecosystem–whether by depositing the underlying asset or even just by purchasing the RCA on an exchange–they never again need to think about their coverage.

2.3 Costs

There are no upfront costs to reciprocally-covered assets. Payments are only ever made when a claimable event occurs, in which case small amounts of funds are liquidated from each vault to compensate the loss (denominated in Ether or a stablecoin[9]). This is similar to if they were a traditional insurance company that only offered assessable policies[10] (policies in which the company can retroactively charge customers extra if losses are greater than expected) and never charged premiums or had a capital reserve.

This method ensures users pay only exactly what needs to be paid: no more, no less, no profit for underwriters, and no worry of insolvency. The drawback of this method is that users may not know beforehand exactly what will be paid. As expanded upon in the Cost Data section below, past data and current analysis shows that it's very unlikely users will pay even 1% of the covered value per year for full coverage of their assets, although prospective users may be uncomfortable at the thought of this unknown and the system may need time to prove itself before gaining widespread adoption.

DeFi has not been around for long[11], so there is not much data available on the risks involved. However, not having adequate data is one area where RCAs shine because there is no risk in over- or under-charging users, but it's important to know the potential costs. In the simplest RCA system possible, the loss from each vault (L_i) will be determined by taking the same percent of funds from the value of the vault (V_i) as the total funds lost (TL) from the total value of all vaults (TVL).

$$L = V * \frac{TL}{TVL}$$

[9] https://www.investopedia.com/terms/s/stablecoin.asp
[10] https://www.investopedia.com/terms/a/assessable-policy.asp
[11] https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets

2.3.1 Cost Data

The best method to estimate costs of the system historically is to use data from payouts of coverage protocols compared to their total cover sold at the time. This is more accurate than simply using all DeFi hacks because it takes into account only protocols that have been deemed safe enough by underwriters to cover, which is a similar dataset to what RCAs would cover, although the full loss is still overestimated when taking into account that the actual loss is lower than the paid out loss.

We can examine Nexus Mutual's history for these numbers with the best historical data available. There were 2 claimable hacks that have occurred for Nexus Mutual[12]: one on the bZx protocol[13] and one on the Yearn protocol[14]. The bZx hack occurred in February of 2020 with a total payout of $33,640 USD[9]. The Yearn hack occurred in February 2021 with a total payout of $2,606,725[9]. $1,937,000 of the Yearn loss was confirmed to be not from actual loss because it was a payout to the Armor protocol which had a policy that simply relied on whether a hack occurred or not rather than requiring proof-of-loss. Every successful Nexus Mutual claim that has occurred to date was paid to a user whose policy did not require proof-of-loss[15] [9], so there's a high likelihood other claims did not compensate actual losses.

To determine the cost of these for the Nexus Mutual protocol we divide the loss (L) by the Nexus Mutual active cover amount at the time (ACA) then multiply by 100 to find the affected percent (C):

$$C = \frac{L}{ACA} * 100$$

At the time of the bZx hack, Nexus Mutual's active cover amount was $2,800,000[16], so the hack's total effect was 33,640 / 2,800,000, or 1.2% of the protocol funds. At the time of the Yearn hack, Nexus Mutual's active cover amount was $711,000,000 and the highest possible real losses was $669,725, so the hack's total effect was 669,725 / 711,000,000, or 0.09% of the protocol funds.

If the same scenarios occurred in an RCA system, the amount paid for the past year (October 2020 to October 2021) would have been–at most–0.09% for the average user. For the past 2.5 years (the amount of time since this coverage provider's launch[17]), the cost would have been–at most–1.29% for the average user. Considering both that RCAs will only ever payout actual amounts lost and that the bZx hack had a disproportionately large loss because of the small active cover amount at the time, it likely would have cost less.

We can also examine theoretical circumstances that may occur. For example, we can ascertain that in current times–if RCAs cover every single dollar in DeFi–for users to be charged 1% in the span of a year, $1 billion+ (estimate in this scenario because full DeFi TVL does not directly relate to liquid funds) would likely need to be stolen with none returned and protocols not reimbursing users.

2.3.2 Incorporating Risk

Detailed risk assessment is not technically required for reciprocally-covered assets to function, and they may begin with none at all. Since no premiums are charged for coverage, we can allow protocols to be covered with no specific risk assessment, with the figurative risk assessment being the initial process of the Armor DAO[18] allowing or disallowing the protocol.

[12] https://nexusmutual.gitbook.io/docs/claims-assessment/claims-history

[13] https://cointelegraph.com/news/decentralized-lending-protocol-bzx-hacked-twice-in-a-matter-of-days

[14] https://halborn.com/explained-the-yearn-v1-ydai-hack-feb-2021/

[15] https://forum.nexusmutual.io/t/add-proof-of-loss-requirement-to-cover-wording/131/19

[16] https://nexustracker.io/

[17] https://medium.com/nexus-mutual/weve-launched-2bc8ba1049f2

[18] https://en.wikipedia.org/wiki/Decentralized_autonomous_organization

As the RCA system expands and diversity increases, a certain amount of detailed risk assessment will be needed both for logistical reasons if the system is large (interacting with thousands of vaults for a small liquidation would be extremely undesirable), and to avoid adverse selection in which the system could become weighted toward protocols more likely to be hacked.

An example of risk of a protocol being taken into account in an RCA system is for protocols to be rated based on risk (using a variety of risk rating sources such as DeFiSafety[19]) then loss is to be paid back by removing a percent of funds from the riskiest to safest protocols. In this system, the riskiest protocols will have a certain amount of funds removed (based on a constant maximum percent) in almost every hack, whereas the safest protocols will only have funds removed once the hack is large enough.

For example, if we have 10 vaults with equal values rated from riskiest to safest, a hack occurs that affects 0.1% of the ecosystem, and the maximum percent that can be liquidated from each before moving onto the next is 0.5%, we will liquidate the maximum from the 2 riskiest vaults before the loss is fully compensated. If the hack affected more than 0.5% of the ecosystem, the liquidations would simply loop back around to the riskiest protocol and continue, so a hack affecting 0.75% of the ecosystem would end up liquidating 1% from each of the riskiest 5 protocols and 0.5% from each of the safest 5 protocols.

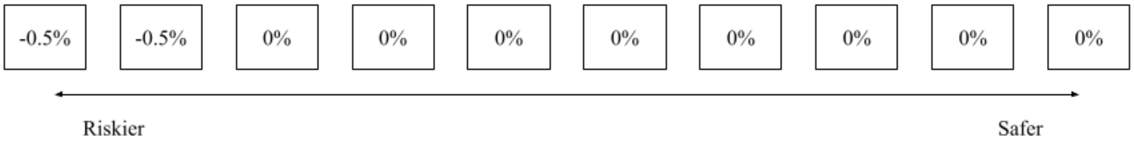

Figure 3: Example of vault losses based on risk rating.

To find the loss of a specific vault (L_i), we would sum the loss that previous vaults would have paid, then, if funds are still owed, take the minimum of either the total loss (TL) minus that sum, or the maximum loss percentage (M) of the value of the vault (V_i).

$$s_i = \sum_{k=0}^{i-1} V_k * M \text{ such that } i > 0, \text{ otherwise } s_i \equiv 0$$

$$L_i = \begin{cases} 0, & \text{if } s_i \geq TL \\ min\{TL - s_i \ , \ V_i * M\}, & \text{otherwise} \end{cases}$$

2.3.3 Protocol Profit

There are a few different ways for the Armor protocol to profit off of RCAs. The most obvious may be a small recurring fee of assets in the ecosystem such as 0.1% per year of the value of covered assets. Another viable method that also incorporates a disincentive to leaving the system would be to make RCAs free to mint, but charge a fee upon exiting the system.

Given that the size of the market is the entirety of DeFi, charging even minuscule fees could lead to an enormous amount of profit for the Armor protocol. The Armor protocol's DAO will have the ability to choose whether/when to implement fees for the system and which method to use, but while growing the protocol it is likely best to forego any fees in order to maximize growth.

[19] https://www.defisafety.com/

2.4 Stacked Risk

A DeFi asset may be exposed to "stacked risk" in which the risk profile may expand across a variety of underlying protocols rather than being isolated to one protocol. For example, if the asset is a token representing a share of a Yearn Finance vault[7], it may contain tokens from Curve Finance[20] that are then staked for a profit, simultaneously exposing a user to risk from Yearn code and Curve code.

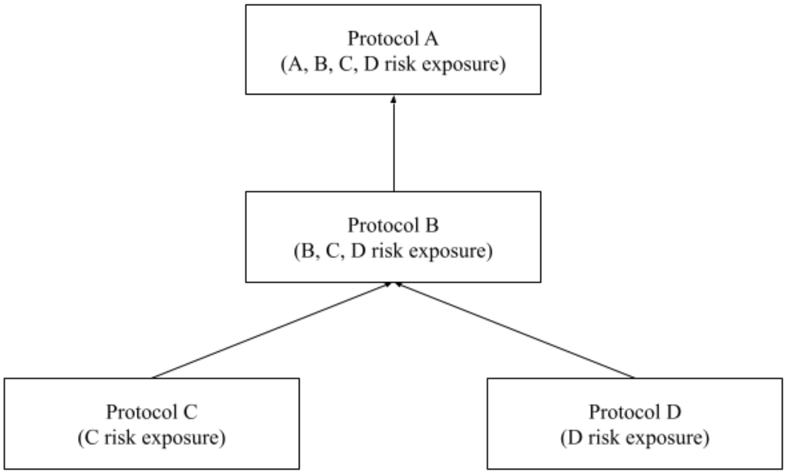

Figure 4: Example of protocols with stacked risk.

With DeFi coverage providers where a user purchases coverage for a specific protocol, they may not also be covered for events that occur on underlying protocols which would still lead to a loss of funds. Because RCA "underwriters" (users) cover every protocol in the system, the origin of the loss does not matter and there will be no additional work needed to ensure stacked risk is covered.

Stacked risk provides an interesting challenge because it can lead us to too much exposure to a certain protocol. For example, if we cover Protocol D in the above graphic separate from Protocol A and Protocol D itself is already at max capacity, any deposit into Protocol A would put the exposure to Protocol D above the maximum. Because of this, we should ensure the code for vaults with stacked risk raises the used capacities of underlying protocols in addition to top-level protocols.

2.5 Coverage Supply

A major bottleneck in the ability to provide coverage for the entire DeFi ecosystem for current coverage providers is the need for underwriters to provide capacity. More demand for coverage in a protocol does increase the incentive for underwriters to provide supply, but there must be free capital and the underwriters must make the calculations to determine whether the risk is worth the reward.

RCAs do not face any of these same problems because the supply of coverage is directly tied to the demand for coverage. The only limits in how much of a particular asset can be covered are the capacity limits of each protocol that ensure risk is diversified. With demand being the factor that increases supply, RCAs can technically cover every dollar in DeFi with no need for underwriters or profit incentive (as long as there's adequate diversity in the DeFi industry at large).

While actual capacity limit of a single protocol (CL_i) can be decided and adjusted by the community as RCAs evolve, they may first begin as simple as deciding no more than a maximum percentage (MP) of 10% of TVL (TVL) that can be attributed to a single protocol. Oracles will be used to block deposits after that amount is reached.

[20] https://curve.fi/

$$CL_i = TVL * \frac{MP}{100}$$

Capacity limits of each protocol are extremely important in the mitigation of losses for users. As diversity of the system and total value locked increases, the effect of a single hack on the ecosystem decreases. Although this will need to be fleshed out through more assessment, other factors that can be incorporated later may take into account the number of pools a protocol has, the uniqueness of different pools or parts of an ecosystem, and more.

Because these capacity limits are based on the total value locked in the ecosystem, when new deposits are made into it, the capacity limit of all individual vaults rises. If CLI_i is the capacity limit increase for any vault, D is the amount of the deposit, and TP is the total percentage any one protocol can be of the total value locked, coverage increases at:

$$CLI_i = D * \frac{TP}{100}$$

This means that if each protocol has a maximum percentage of 10% of the full ecosystem value and a user deposits $10 of value into one protocol, the capacity limit for every protocol is raised by $1 of value.

2.6 Claims

Covered events are events that will trigger payouts for users. These may include hacks pertaining to smart contract code, rug pulls by owners, errors in centralized security, and more. The final decision based on what will be covered will be made by the DAO and can be adjusted at any time. The events that we will cover will depend on data gathered over the course of the system regarding increases in costs based on what is to be covered.

If a covered event occurs, the claims process will then be initiated without any input needed by the user. First, RCA deposits and withdrawals will be temporarily frozen to ensure users cannot leave the ecosystem before liquidation, assets across vaults will be liquidated in small amounts to receive compensation for the affected vaults, claims payouts will occur by sending affected vaults Ether (or a fiat-denominated stablecoin), then users may withdraw the payout according to the share of the vault they hold.

Claims are particularly easy to verify in this system because all losses are from the vault of assets rather than from individuals. We can immediately ascertain exactly what was lost from the vault, and begin repaying the vault (and therefore holders of the reciprocally-covered asset) depending on how much was lost. The DAO will then vote on the amounts that need to be repaid to each affected vault, and allow liquidation of tokens from the other vaults to complete the payout.

To determine final value of a vault (V_{i_2}) after a hack using the simplest RCA system (no risk ratings), we multiply the old value of the vault (V_{i_1}) by the new total value locked of the RCA ecosystem (TVL_1) divided by the old total value locked (TVL_2).

$$V_{i_2} = V_{i_1} * \frac{TVL_2}{TVL_1}$$

There is no system necessary to vote whether an individual's claim is valid, no need to verify loss of a user, and no need to decide exactly how much a user should be compensated.

A very important aspect of claims is also who votes on whether they're valid. With RCA systems, Armor token holders will vote on whether claims are valid and the full ecosystem will take part in paying out those claims, resulting in the only incentive for token holders to be to ensure the system works as intended, and payouts always being made for valid claims. This avoids mixed incentives and possible scenarios in which large claims may not be paid out simply because of the potential loss for claims assessors.

2.6.1 Solvency

Solvency is an enormous benefit to RCA systems as risk is, in essence, fully-backed. This, of course, is not completely accurate because the users suffering from a loss will not receive 100% of their loss back. Figure 6 demonstrates what happens if 25% of the entire RCA ecosystem (100% of Vault B and 100% of Vault E) is hacked all at once. Everyone who got hacked will be compensated–contrary to many coverage providers who may be insolvent with a hack of this magnitude–but the compensation will only be 75% of the value stolen, as affected vaults will only be repaid an amount that matches the losses of other vaults.

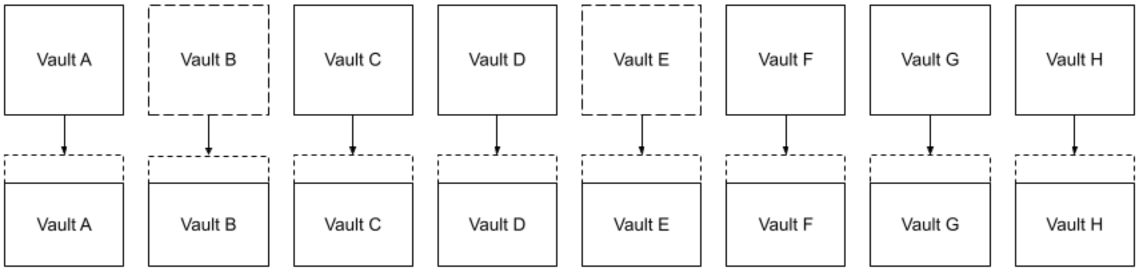

Figure 5: RCA solvency in the event of a 25% of all TVL hack.

To make adequate profit for the risk taken while charging reasonable premiums, other coverage providers will generally leverage their capital pool. This may mean, for example, that $1 of capital covers $10 of risk. Because of this, a situation in which multiple very costly claimable events occur in a short timeframe may make a coverage provider insolvent and not able to pay users for their loss. While the same situation would be damaging to holders of RCAs because they would be charged over 10% of their funds, losses would still be able to be repaid.

3 Transition

Armor's transition to fully reciprocally-covered assets will likely take a long time; the reason for this being that the diversity of the ecosystem is a crucial aspect of its safety. Not only does this require greater adoption of the RCA system, but also greater adoption of DeFi in general, which will lead to funds being less concentrated in a small number of protocols. There will also likely be skepticism that must be overcome through the success of RCAs.

Currently, Armor's Shield Vaults[21] provide the perfect starting point for an RCA system. The vaults already use wrapped tokens in the way that an RCA system will, and they already use partial coverage. Partial coverage works by fully covering only a fraction of the assets in the vault, which are spread across many pools in a protocol, allowing users a much lower cost while maintaining similar safety when taking into account the small likelihood of a protocol having every pool hacked at once. The technical development needed to incorporate RCAs into Armor's current shield vault system is

[21] https://armorfi.gitbook.io/armor/armor-v2/arshield-armored-vaults

minimal.

Armor will continue to use Shield Vaults that are partially covered by a third-party underwriter, add RCA capabilities, then begin to lower the percent of coverage fees paid to the underwriter. A hybrid system like this will still give great benefits in coverage capacity, cost, and stacked risk coverage while we move toward our final destination.

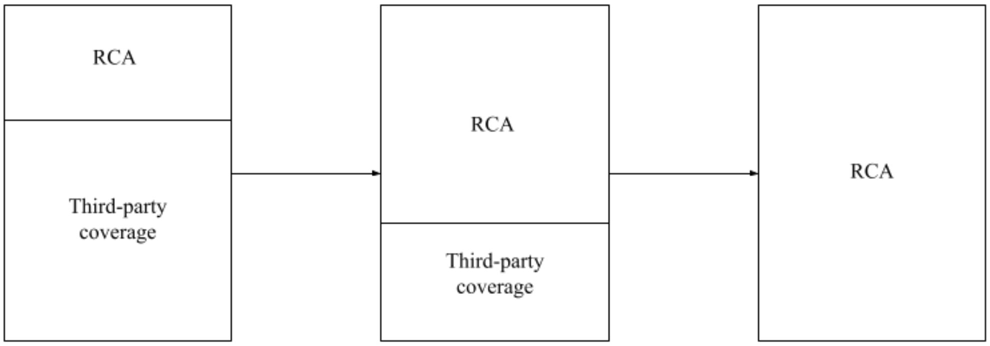

Figure 6: Armor's transition process to RCAs.

3.1 Security

While RCAs can cover each other in the case of a vulnerability within Armor itself if the vulnerability affects only a limited number of vaults, the security of Armor's smart contracts is extremely important to keep in mind during and after our transition. Because the system has the potential to hold all of DeFi's value within it, a vulnerability in Armor's code could be disastrous for the ecosystem. To avoid this, we must both make the contract code and design as simple as possible and put an incredible focus on security during their development, launch, and operation through audits before and throughout operation, consistently advertised and very high-paying bug bounties, and live monitoring of contracts. In addition to RCAs providing protection for each other in most cases, purchasing coverage for Armor from an unrelated protocol or even from an off-chain provider for a small portion of the system's value will be another helpful layer of security.

4 Expansion

RCAs are designed to be able to cover every dollar invested in decentralized finance. To do this, after its initial creation, RCA development will be focused on expanding the diversity of the system while maintaining safety. They should not cover protocols without heavy due diligence, but each extra protocol that is covered provides more coverage for the rest and a lower portion paid by each user when a claimable event occurs. A DeFi safety rating rubric will be created that aggregates scores from existing DeFi safety rating platforms to determine whether a protocol is safe enough to cover in terms of code quality, focus on security, transparency, team, history, and more; this will initially be used to provide a binary answer as to whether the protocol will be included, then can be used for more detailed risk assessment.

Because diversity is key, RCAs will quickly move to covering risk on blockchains other than its initial blockchain, the Ethereum Mainnet. The process for this is simple as nothing is holding them to a single blockchain. If a hack occurs anywhere, all other vaults—regardless of the blockchain they're on—can have small amounts withdrawn to pay someone out, then those amounts will be transferred to the affected vault on whichever chain.

The ideal vision of the RCA system is for users to be able to purchase any RCA directly from an exchange or protocol without ever interacting with the underlying token. This is a vision in which

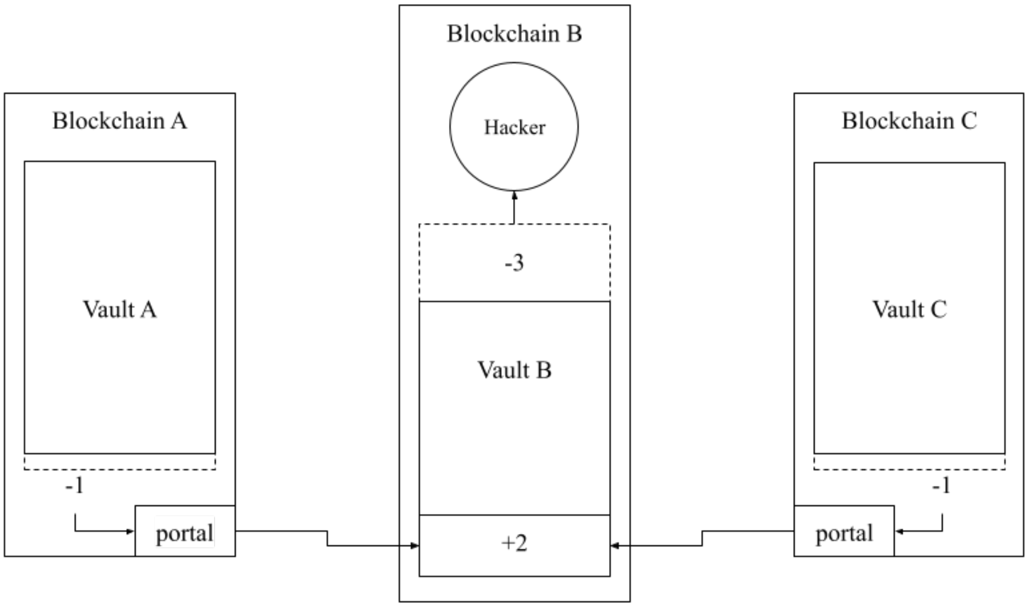

Figure 7: RCAs securing each other across blockchains.

users are perpetually covered against the risks of DeFi without a second thought–or even first thought.

5 Conclusion

The popularization of DeFi has brought about enormous risk of stolen and lost capital. Current coverage providers give protection against these risks but have shortcomings such as usability, over- or under-priced premiums, supply constraints, perverse incentives for claims assessors, and potential for insolvency. The reciprocally-covered asset model provides a simple solution to all of these problems: it always charges the exact amount necessary (from past data, much less than charged by other providers), the supply is directly tied to demand, its claims assessors are not the party that is at risk of losing funds, and there's much less risk of insolvency than other systems. It's a completely DeFi-native model that makes covering your *ass*ets simple, cheap, safe, and accessible.