Eonian Savings Account Litepaper

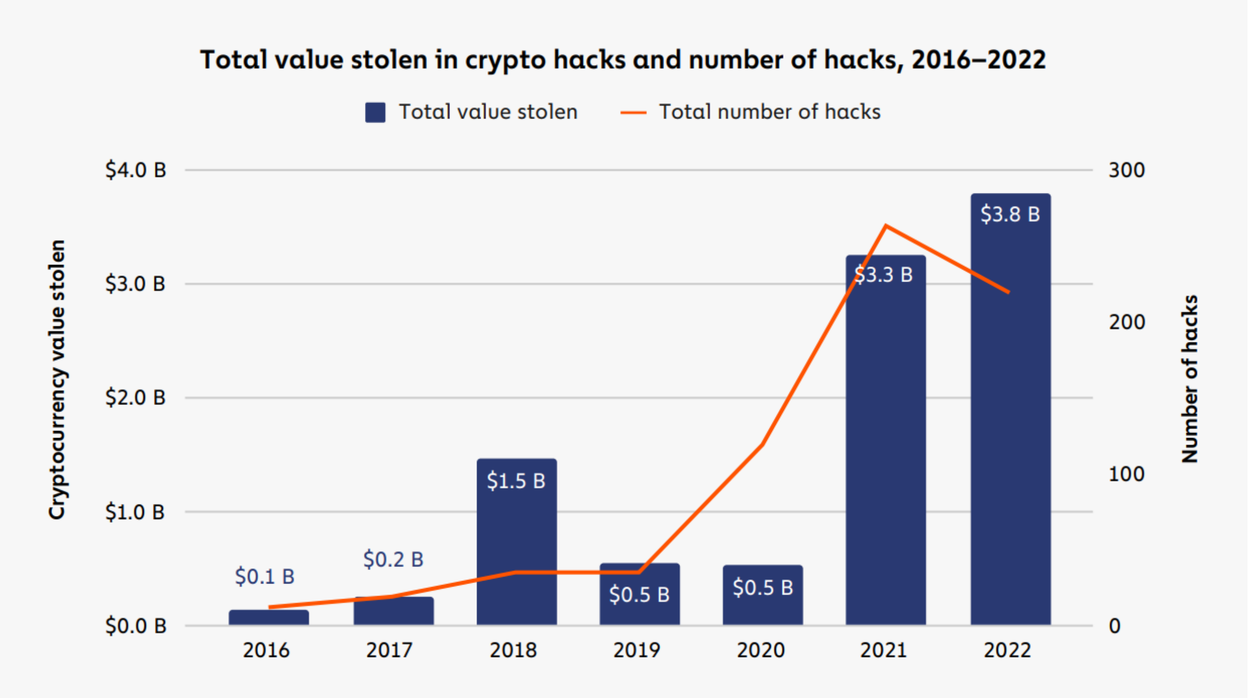
Made by the Eonian Team.

Introduction

Cryptocurrency adoption is surging, but with increased adoption comes increased risk. Cybercriminals stole a staggering $3.8 billion in cryptocurrency in 2022, representing a 15% increase over the previous year, according to a report from Chainalysis. In these assets, the percentage of money received by wallet hacks is on the rise every year. The Eonian Savings Account aims to be the bulwark against such threats, providing zero-fee insurance for your assets with the added perk of returns on your savings.

The Problem

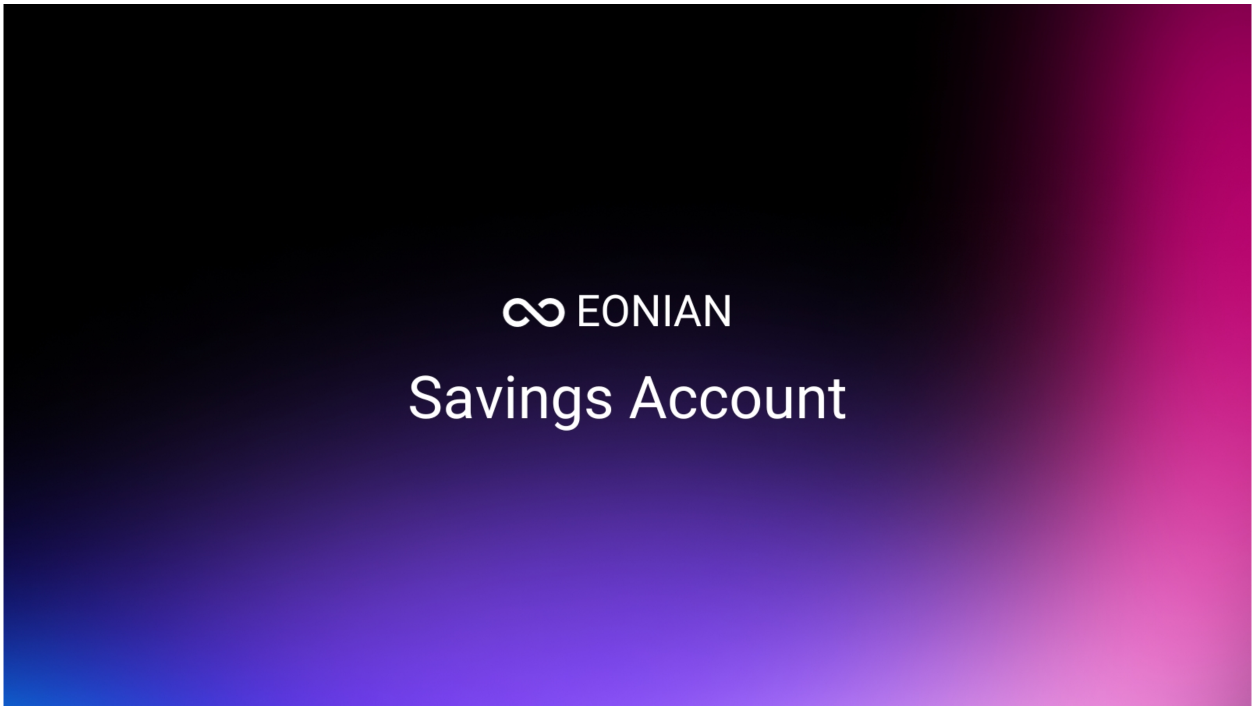
Crypto wallets, despite being known as one of the safer options for crypto storage, are not immune to hacks. There have been many cases where assets lying dormant in wallets for years were stolen without any interaction from the owner. This is supplemented by the large-scale hacks involving popular wallets like MetaMask and TrustWallet.



Only in 2022 alone did crypto hack revenue hit $3.8 billion. Almost all of it is coming from DeFi and crypto wallet hacks. But the problem with wallet hacks is actually more critical than with DeFi protocols and contains not in the risk of hacks itself but rather in the response from wallet developers.

Biggest DeFi protocols, when hacked, often attempt to reimburse users by utilizing insurance, loans, bonds, or the project budget itself. Wallet providers, in contrast, frequently eschew responsibility. They usually try to blame users for losing the key and disagree with making any reimbursements.

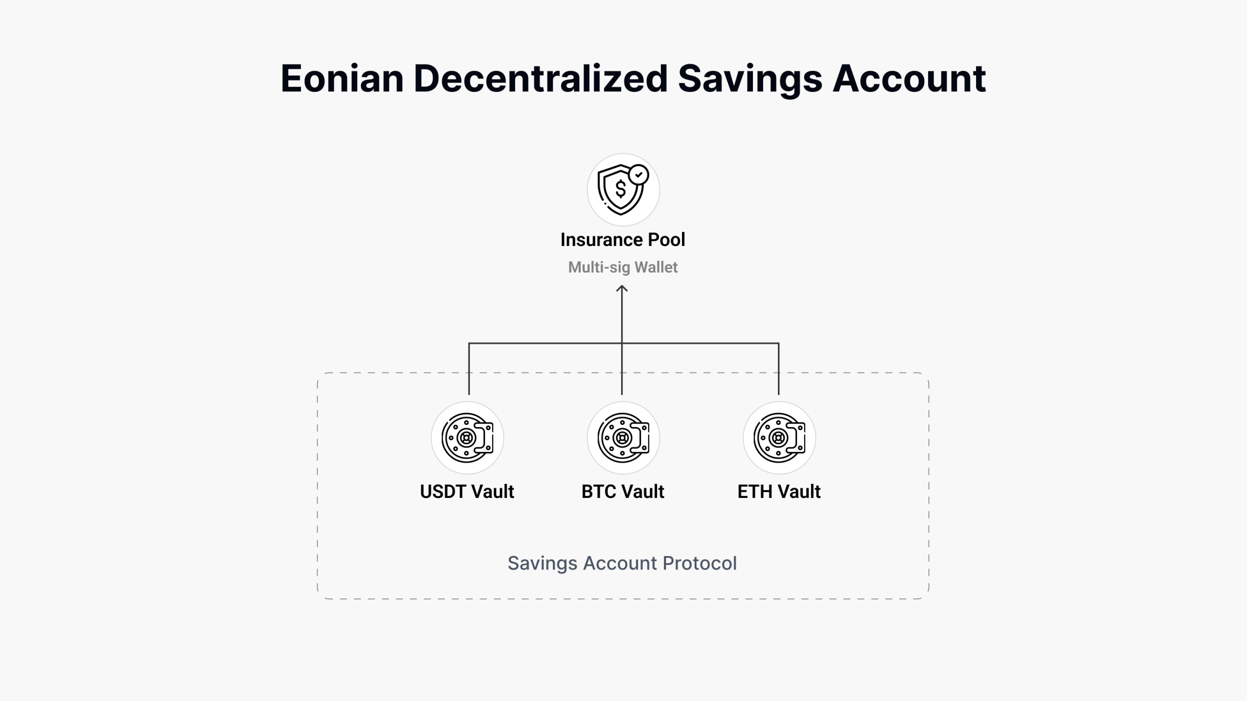
The grim reality is that, in many wallet hack cases, wallet developers, despite being aware of the situation, have neither taken responsibility nor made amends to return the stolen funds or at least develop proof that they will not be hacked again. This situation underscores a dire need for asset protection.



The Solution

The Eonian Decentralized Savings Account offers an innovative solution to this pervasive issue. The protocol provides insurance against technical hacks of hot, cold, and hardware wallets. Distinctively, if your assets are maliciously withdrawn or if you lose your private key, Eonian ensures that your funds are returned. At its core, the solution functions via smart contract protocol. Based on similar smart contracts technology, working tokens like USDT and WETH.

You can think of our decentralized savings account as a bank savings account but on the chain. Assets stored there will be used in a similar way as in a bank but fully automated and independent from any human operations through smart contracts. These smart contracts will provide liquidity (in other terms, give “loans”) to different protocols and use revenue from these protocols to fill the insurance pool and pay users’ premiums for holding their assets in the savings account.



The main difference of the savings account protocol protection system is the user email, serving as a 2FA channel. This email allows users to lock or recover access to assets in the unfortunate event of a hack or lost access. Through this email, the user can provide a new wallet address to which we can send reimbursement or transfer money from an old wallet that is no longer accessible.

Benefits and Features

Eonian Savings Account stands out with its plethora of features:

- **Safety First -** Diversification and monitoring are used to drastically decrease the risk of potential hacks.
- **Zero Fees -** Enjoy the luxury of no fees for insurance, deposits, or withdrawals.
- **Simplicity -** There are no registrations or complicated procedures. Simply, as long as you keep your assets in our savings account, you will receive insurance and premiums automatically.
- **Flexibility -** Unwrap your assets anytime without any time locks and limits.
- **Rewards -** Benefit from up to a 10% APY premium on insured assets in the Vaults.

- **Backup Plan -** If you lose access to your wallet, the protocol facilitates fund recovery using your email.
- **Wallet and protocol hack insurance -** In simple words, we return your money when someone steals it from your wallet. That's as simple as it is. But you can read the complete list of cases that we cover there.

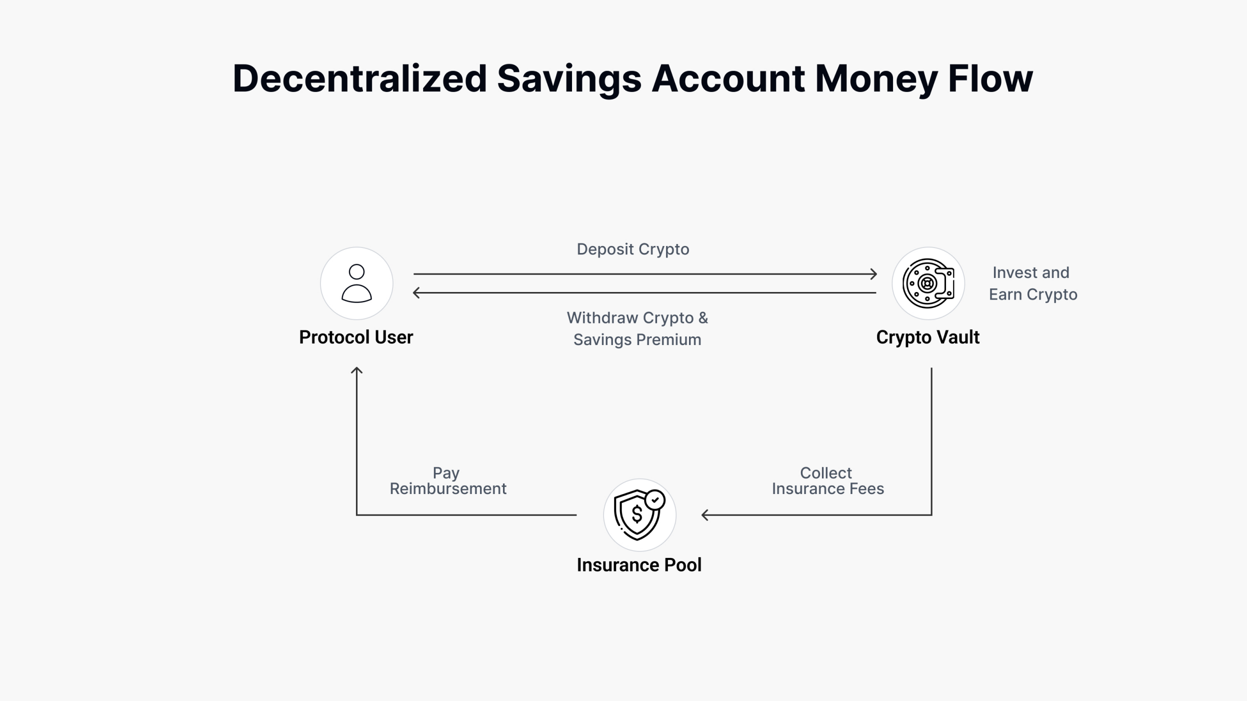
Use Cases

Here are some scenarios where users can derive immense value from Eonian:

- **Hacked Wallet Recovery -** In case the user's wallet key gets stolen, and all assets are rapidly withdrawn. The user can notify the Eonian team. We will verify the user's identity, lock the assets from hackers during an investigation, and repay the stolen funds to the user at the end.
- **Lost Key Assistance -** If the user misplaces their wallet key, locking their assets. Eonian allows the user to recover access to their funds by liaising through email, ensuring the safe transfer of assets to a new address.
- **Passive Income Generation -** Any trader can use Eonian as a safe vault for their BTC and ETH holdings intended for long-term investments. By merely holding their assets in Eonian's Vaults, the trader enjoys an additional yearly return on static assets that, otherways, cannot be invested anywhere.

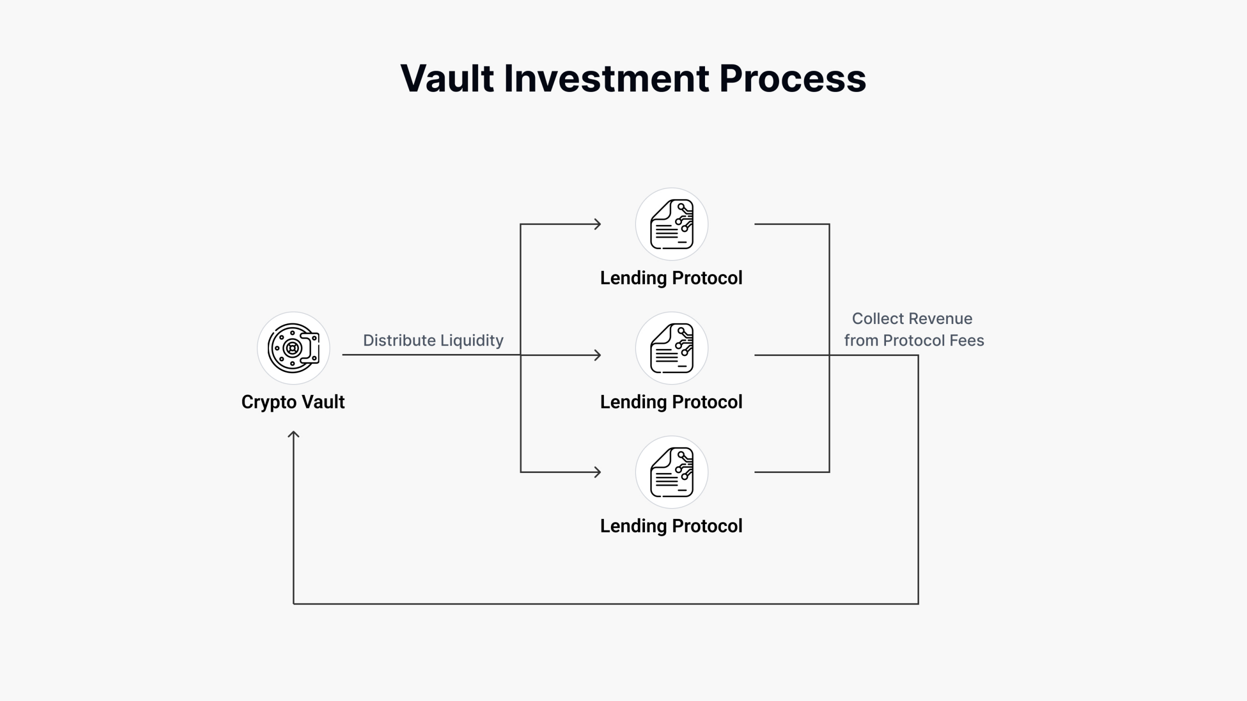
How Solution Works

Our decentralized savings account protocol allows you to save your tokens inside of the Vault smart contract. The Vault, in response, gives you an insured version of your coins, which equals 1-to-1 your original coins. They represent your ownership of assets. You can unwrap them back or send them to another wallet at any moment without any fees or locks from our side.



While you holding these coins, they grow in relation to your original coins. This means that the longer you hold them, the higher the amount you will be able to withdraw. This passive investment opportunity is called a savings premium.

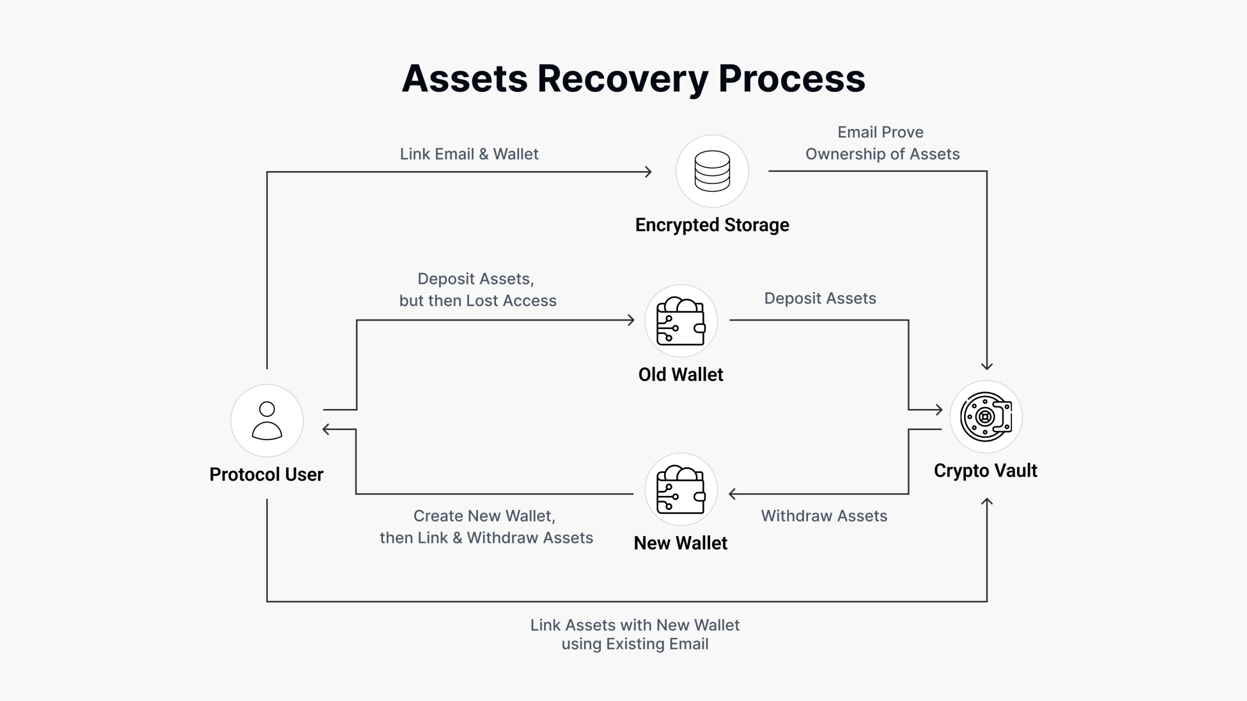
While you hold your assets in Vault, they will be distributed between different lending protocols. These protocols give fully collateralized loans to crypto users. In exchange for these loans, users pay fees, which are then collected by our Vauls. This revenue is distributed back between the insurance pool and our protocol users.



This works as a collective security system. The revenue of total protocol liquidity that our protocol generates allows us to decrease risks and pay reimbursement for each of our protocol users in case of a hack.

When you will make your first deposit, dApp will ask you to provide an email. It will be used to restore access or confirm your identity in case of a wallet hack. If someone steals your private key or, in another way, steals your assets, you will be able to contact us from this email. We will lock your assets to save them from hackers. When the investigation is finished, you will create a new wallet that you can trust. We will transfer your existing assets and make reimbursements for what is lost.

You can read more info about the claim process here.



The Insurance Pool

Our protocol maintains an insurance pool from which we can pay users' compensation in case of a hack. This insurance pool is bootstrapped from protocol founders' money, showcasing our trust in the solution's safety. Insurance from this pool is paid from the revenue of the protocol, not by users directly.

The revenue mainly comes from the investment of assets, which is covered by insurance. At this stage, the protocol works as a traditional yield aggregator. Assets invested in different lending protocols and DEXes, where they earn returns from fees of these protocols. Nevertheless, our protocol works a little bit differently from other yield aggregators. While they prioritize returns on investment, our protocol invests in a way that decreases the risk of investment. It distributes assets between multiple protocols, which decreases the risk of losing all assets in case of a one-protocol hack.

Our protocol and protocols in which we invest are also covered by insurance, which results in much lower investment risks.

To maintain the stability of the pool size, we have in place three strategies:

- We can dynamically adjust the amount of premium that we pay to users. This increases the amount of profits that go directly to the insurance pool.

- We can dynamically decrease the coverage percentage size to influence the demand in our savings account. As a result, it will decrease the new liquidity flow and give the protocol time to grow the insurance pool size until it is able to cover more money.
- In the future, we will also provide liquidity providers the ability to invest directly in the insurance pool. They will be able to earn high APY as a reward for covering the risks for regular holders.

Savings Premium

The majority of revenue generated from investment protocols is used to pay and fill the insurance pool, but when the insurance pool is bigger than the need to cover users' assets, the revenue is redistributed back to users as a savings premium. This allows users to not only save their assets but also grow them while they are holding them.

This savings premium is dynamically adjusted based on the amount of liquidity in the Vault, the insurance pool, and the market risk situation.

> 💡 Our early-access users and beta testers get a higher premium as a reward for their involvement.

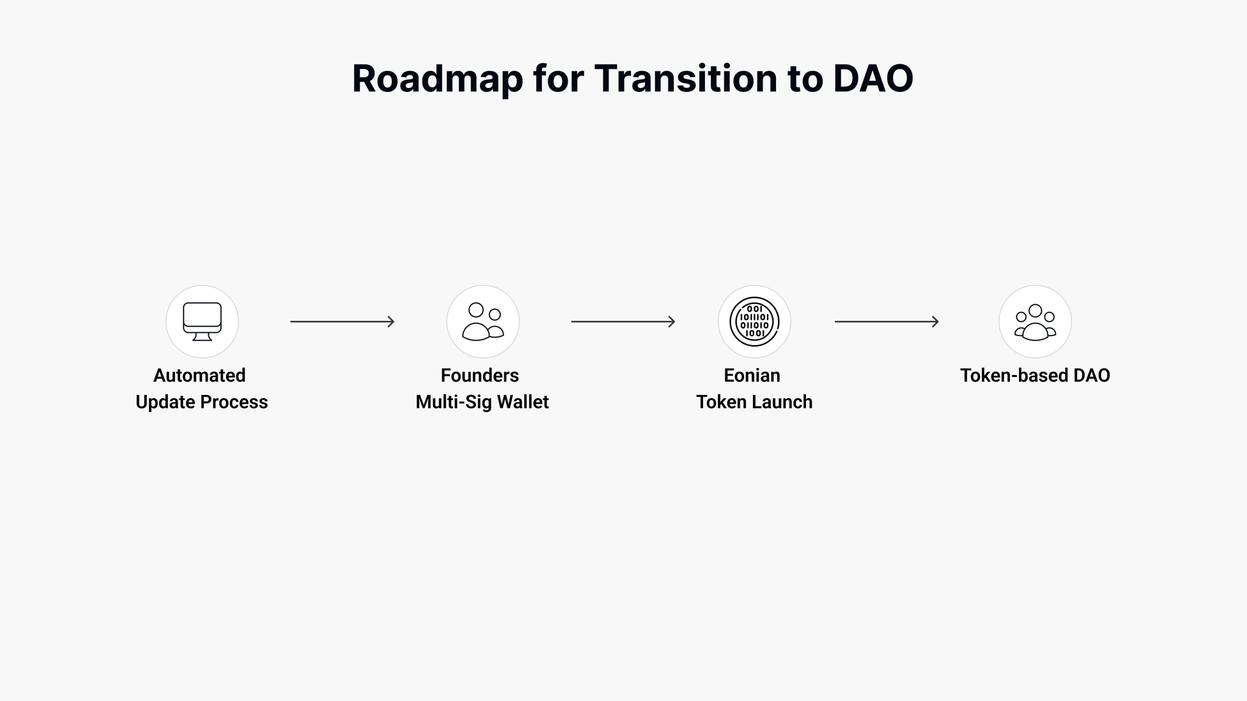
Assets Recovery

One integral part of any wallet is the private key. But there exists a hard problem where to save it. If the key is stored only locally on the device, it guarantees increased security and a lower risk of hack. But if the device is lost, access is lost with it. On the other hand, it is possible to save a key on the server or encrypt and store it on another chain. Some wallets even provide this solution directly. But all of them introduce the risk of private keys being stolen on the server or unencrypted on the chain. And give access to some middleman who can accidentally lose or use this key.

We allow the user to store their key locally on the device. But in case the user loses the device, he is still able to recover access to assets in our protocol by creating a new wallet and then contacting us through the receiver's email. This email works as a 2FA channel, which will be used to target us on which wallet we must move user assets to give access back to these assets.

In the future, we will introduce additional channels, like messengers and phones, to make this recovery process even more convenient. But even one email paired with a wallet can provide a higher level of safety and reliability than a hardware wallet.

Governance and Trust



We recognize the importance of trust and proper governance in any decentralized solution. We developed a long-term plan to transition the governance of the protocol to the users and community of the protocol. This DAO model will operate on the basis of the project’s token, which will be distributed across users, the community, investors, and the development team. This token main utility is to provide voting rights in the insurance claim dispute process and protocol changes voting.

In complex cases where the nature of the hack is ambiguous, this dispute process will include voting and investigation from the community and other protocol users. This way of governance will ensure transparency and fairness in each dispute since all participants are interested in producing the fairest result. There are the main sides of the decision process:

- Users - they are interested in making honest decisions, as on one side, they can be in the same situation next time. On the other hand, each payment can decrease the insurance pool size, which balances the amount of payments that users can accept.

- Investors, the team, and the community - all of them will have a vesting period for their tokens after payments. This forces them to accept only fair dispute results, as each of them can directly influence token price and, as a result, their own capital.

We plan to release the project token and develop DAO after the release of the protocol. Until this moment, we will gradually develop and release different features that increase the safety and decentralization of the protocol.

- At the release stage, the protocol will operate via a multisig wallet, requiring the majority of the founders' approval for any transactions for protocol updates or reimbursements.
- Additionally, we will set a timelock contract on all transactions for reimbursements for 7 days. These transactions will automatically be posted in our Discord channel, where you can subscribe to receive notifications. This way allows you to be sure that the development team cannot at one moment take all the money from the protocol. About any payments, you will know in advance and have 7 days to withdraw all money from protocol.

Dispute Process

In case of an unclear insurance claim, the user will be able to initiate a dispute process. During the dispute process, the team will try to collect evidence for one or another resolution. We already have contacts with firms that investigate hacks in DeFi. We can involve them in large and complex cases. They are usually able to trace any money movement on the chain and have contacts with local police offices in place. This way allows us to trace the majority of hacks and get evidence for resolution.

Traditional insurance companies usually have on-site detectives who investigate complex cases for them. In our situation, we plan to build a community of detectives who will work on investigations of different cases on the chain. They will receive a reward for finding any evidence for unclear cases. This way will allow us to ensure trust and safety for all sides while increasing the speed and effectiveness of the dispute process.

At the current moment, disputes are resolved by the team. Voting for dispute resolution is made through a multisig wallet and requires a majority of founders' approval. In the future, this process will include DAO voting, mainly represented by protocol users and investors, which allows for a decrease in conflict of interest and guarantees honest voting. All participants of the voting will receive a reward, no matter the result of the process. This way, we can increase participation and, as a result, a more fair voting process.

You can read more info about the insurance claim process here.

Security

Security is paramount for Eonian. The protocol's multifaceted security approach includes:

- **SecOps and Secure SDLC -** We take a security-first approach to ensure that all of our contracts are safe to use. We use enterprise-level software security practices such as SecOps and Secure SDLC, which have already shown great results in the Web2 world but have been overlooked by many Web3 developers.
- **Continuous Monitoring -** We don't stop at the audit of the protocol. Security is not a point where you can stop working. We monitor new breaches and hacks in DeFi to quickly react and fix vulnerabilities where others may be failing. You can see the list of vulnerabilities that we collected and monitor there.
- **Rigorous Testing -** We use code review, automated testing, and code coverage reports. We investigate and will build a solution for automated code analysis for vulnerabilities.
- **Attack Analysis -** We collected more than 40 smart contract vulnerabilities and different hack cases. During development, we are making vector attack analyses using these vulnerabilities to find ways the hackers can attack our protocol.
- **Attack Simulations -** We are working on instruments to test protocol by making possible attack simulations on the blockchain before deploying new changes for the mainnet.
- **Multi-layer Testing -** We test our protocol on three different levels: Preview (On testnet), Development (on mainnet, but only accessible to the main team), and Staging (On Mainnet, but accessible to the team and dedicated alpha testers). You can read about it there.
- **Insurance Pool -** At the current moment, our insurance pool is mainly bootstrapped on founders’ money. It means that in case of any issue or hack, we will first who

lose money as we will be forced to repay users their losses. This way, we want to show how much we trust our solution and how much we are motivated to keep the safety of the solution at the highest level. The pool is stored separately from the main protocol. This ensures we will be able to repay users' money even if the Eonian protocol is compromised.

- **Next-generation security system -** We are working on protocol monitoring on blockchain. It will monitor not only our protocol but also the protocols in which we move liquidity. At any moment, monitoring will be able to provide the current state of money flow and the health state's overall investment system. It will also use the mempool of the blockchain to monitor future transactions and to understand when there will be possible hacks or issues, which can result in money loss. By using such information, we will be able to automatically send withdrawal transactions before bad transactions are committed and save all money from vulnerable protocols.
- **Security Audits -** We make independent vertical audits of all protocols in which our protocol invests. Unlike standard audits, which primarily focus on code, vertical audits offer a holistic examination. This includes not only the code but also the operational mechanisms, administrative roles, upgrade paths, and, critically, the team behind the protocol. You can see the list of audits there.
- **Circuit Breakers** - If our protocol detects significant losses, it automatically pauses itself and withdraws all money to prevent further damage. You can read about it there.

Roadmap

Research & Development

2022-2023

During the last few years, we have been working on safety investigations and developments in DeFi. You can see publications of the majority of our researches there. We have prepared a proper base for the development of our solution.

Closed Beta Test

Q4 2023

Soon, we plan to launch a closed beta test of our savings account. You can already join the waitlist for our closed beta test there. During the closed beta test, we will provide increased APY for all participants as a reward for their contribution.

Alpha Test Launch

August 2023

In August, we launched the alpha test of our yield aggregator, which has already generated returns on investments for many users. This testing allowed us to test and improve our yield aggregator protocol, which can now work as the proper foundation of our decentralized savings account protocol.

Open Beta Test and Release V1

Q1-Q2 2024

During the beginning of the 2024 year, we plan to launch an open beta test with a later release that will allow anyone to use our application.

Token Launch

Q3-Q4 2024

At the end of the 2024 year, we will launch our token which will work as a foundation for the DAO.

Team Founders

The Eonian team founders are a synergistic blend of experience and expertise:

- **Vladislav Goncharov (CEO) -** Team lead and architect with more than 8 years in the software industry. Worked on big data, machine learning, fraud prevention, and financial systems.
- **Sergey Soloview (CTO) -** A Full-Stack engineer with more than 10 years in the software industry. He worked as an ML/Data Science researcher and mobile/web developer.
- **Artem Bukharin (CPO) -** His credentials include 3 years in entrepreneurship and marketing, alongside 4 years as a Senior Product Manager in a startup studio.

Economic Model

The full model will be described later in the whitepaper, but there is shown a high-level overview of the protocol economic model.

The overall economic model is quite simple. We replicated a traditional bank's business model while adjusting it for the crypto market. To make it work on a chain, we combined the insurance business model with the BDS (Business Development Companies) investment process. In simple words, we give protocols (businesses in traditional terms) loans while maintaining overall assets health through insurance and paying users percentage from these loans as a premium. In a similar way, working savings accounts in traditional banks. With only a few exceptions:

- Banks work not only with businesses but also give loans to regular clients. While on a chain all users are mainly anonymous, client loans can be represented only through collateral lending. This solution is already pretty well implemented by many old protocols like Compound and Aave. There is no reason to replicate it. Instead, we are building on top of them and providing liquidity to such protocols.
- Banks' liquidity flow and overall health state are unclear at any moment, but on-chain, we can trace the protocol's whole liquidity at any moment. This makes our solution even more transparent and safer than traditional banks, by definition.
- A most important difference with banks is that for the majority of protocols, we can withdraw tokens at any moment. This not only allows the implementation of safer solutions but also requires changes in risk management in comparison to traditional banks. They usually take a long time to investigate the client before giving him a loan. We, on the other hand, must make such an analysis not only initially but also in each block (almost each second). The model requires monitoring of all investment protocols and redistribution of liquidity as often as possible to increase returns and decrease risks.

Risks and Revenue Analysis

There, we will take a look at the most simplified risk model version. It does not cover all risks but is close enough to a real model to form result expectations.

On the one hand, we provide insurance for multiple people and support many different types of wallets. The chances that all wallets of all people will be hacked are very low. At the same time, the chance that at least one will be hacked is relatively high. It means that at any moment, we need to have an insurance pool that fully covers the average wallet hack amount for all of our users.

There are currently not many statistics directed to wallet hacks on average due to the complexity of differentiating wallet hacks from key losses. But we can base the average amounts on top of the last 5 years of transaction volume received by wallet hacks in relation to the whole transaction volume from illegal actions. According to Chainalisis, it is around 0.2 - 2%.

In such cases, we can expect, on average yearly 2% of wallets will be hacked. For 1000 users, it gives us 20 users hacked per year. Additionally, we currently plan to support the top 20 wallets. For the same 1000 users and with normal distribution, it results in around 50 users being hacked in case of a full wallet hack independently from the user. In other words, from 2% to 5% of protocol users, on average, will be hacked. If we assume that, on average, all users will have a similar amount deposited, then yearly, we will need to cover around 2%-5% of TVL.

Additionally, we need to cover our vaults and investment protocols with insurance from the same pool. We expect to have at least 10 Vaults with 3-5 protocols per Vault. It gives us an expectation of losing around 2% of TVL in case of one protocol hack. With the earlier security measures described, we expect very low chances of protocol hacking. But even in such cases, in total, with wallet hacks, it will require us to maintain no more than 4%-7% of TVL in the insurance pool.

To support the full money flow, we need to have a minimum of 7% of TVL in the insurance pool at any moment. But we can expect that insurance cases do not happen in a normal distribution. They usually tend to happen in short periods of time in big amounts. This requires us to have some buffer to be able to cover picks of reimbursements. For simplicity, we will assume that the reserve part of insurance is the same size as the minimal insurance pool size. So, we need to have 7%-14% of TVL in the insurance pool at any moment.

On average, yield aggregators generate around 5% APY. Our investment strategies historically generate from 5% to 15% APY. This gives us from -2% to 13% returns per year after all hacks are covered. (Cases with abnormal distribution will be described in the whitepaper).

This means that the insurance pool, after all covers, will be able to receive from -14% to 92% APY as insurance payments and support itself in a balanced state on average.

Revenue Distribution

Revenue generated from protocol investment strategies is distributed dynamically and in multiple destinations, but they can be described into three main groups:

- The majority of revenue will be used to support the insurance pool as insurance fees. This means that the exact percentage of distribution will be dynamically adjusted based on liquidity pool size and overall asset size, which it must cover. At the initial stage, the percent will be set to 60% of the revenue.
- If the insurance pool is big enough to support full Vaults assets, revenue will be distributed to holders. This distribution allows us to pay a premium on assets that they are holding in protocol. At the initial stage, the percentage will be set to 20% of the revenue.
- The remaining 20% of the revenue will be taken as a protocol fee and will be used to pay dividends for project token holders, buy out project tokens from the market, and support other protocol operations. At the initial stage, while we do not have tokens, this part of the revenue will also be redirected to the insurance pool. Resulting in a total of 80% of revenue at the start going to the insurance pool.

Future Outlook

While the insurance pool can maintain positive returns and grow by itself over time, it may not be enough in case of the rapid growth of protocol TVL. To cover such cases, in the future, we will be able to provide access to an insurance pool for liquidity providers more tailored to risks. They will be able to invest in a liquidity pool and receive part of the revenue that it generates.

This way, the insurance pool/TVL ratio can be balanced by regular market conditions of supply and demand.

FAQs

How Do Protocols Work?

Protocols function as smart contracts, programs that operate on a blockchain. Tokens like USDT and WETH also work as smart contracts.

What is the difference between CEX and protocol?

Protocols operate in a decentralized manner. Even if the protocol team is not available, the users will still be able to continue working with the protocol without any issues. Also, usually, the development team does not have access to users' assets, and it can only make updates to the protocol. Meanwhile, in CEXes, all money is in full control of the company, and they can lock users at any moment or go bankrupt.

Why is Eonian safer than wallets?

Eonian provides insurance to return user money, while wallets do not return money if it is stolen.

What if Eonian's investment protocols get hacked?

Eonian's rigorous audit and monitoring system minimizes this risk. But if such happens, we have an insurance pool from which we will be able to pay money back.

How does Eonian's insurance against wallet hacks work?

The savings account protocol provides insurance against technical hacks of hot, cold, and hardware wallets. Distinctively, if your assets are maliciously withdrawn or if you lose your private key, Eonian ensures that your funds are returned.

An integral component of the protection system is the user's email, serving as a 2FA channel. It aids in direct communication and swift asset recovery in the unfortunate event of a hack or lost access. Through this email, the user can provide a new wallet address to which we can send reimbursement or transfer money from a wallet that is no longer accessible.

You can think of our decentralized savings account as a bank savings account but on the chain. Assets stored there will be used in a similar way as in a bank but fully automated and independent from any human operations through smart contracts. These smart contracts will invest (in other terms, give "loans") to different protocols and use revenue from these protocols to fill the insurance pool and pay users' premiums for holding their assets in the savings account.

The short overview of the process of getting insurance payment works this way:

- The user deposits tokens that he wants to save in our Vault using his wallet and links his email, which will be used for recovery. At this point, all deposited assets are automatically covered.

- Our Vault invests tokens in different lending protocols to earn fees from them. These fees are used to fill the insurance pool, and some parts are shared with a user account.
- When the user noticed that his wallet was hacked, he contacted us using his email to start the recovery process. If assets have not yet been withdrawn by hackers from Vault, we lock them to send them later, when the user will create a new wallet.
- If assets were withdrawn, we start the investigation process. Big wallet hacks, which start to be more common, are easy to identify, so we will be able to pay reimbursement very fast.
- In rare cases, when it is hard to understand the reason for the hack, we can start the dispute process, which will result in voting by our DAO. This DAO includes the same users that hold assets in Eonian, so they are most interested in correct results. You can read more there:
- After that, we pay reimbursement from our insurance pool to a new wallet, which the user will create and provide as an email.

You can get more info about covered cases in our insurance coverage policy:

How does insurance compare to existing solutions in the market?

Despite the fact that crypto wallet and DeFi hacks are growing significantly each year, there are still not many insurance protocols in crypto. Also, all of them currently have one common flaw: they are all centralized. So, if you currently want to decrease risks while investing in crypto, you need to be ready to trust some central entity, which is usually the main thing that people want to avoid when going to crypto. This already sounds silly.

On top of that, all of them require paying some fee, in percent of your invested assets. The insurance solutions in crypto are split into two categories:

- The first category is insurance for tokens invested in some DeFi protocols. After he provides liquidity to some protocol like Uniswap or Compound, the user needs to deposit his liquidity tokens to the insurance protocol. This protocol, in the best case, takes some percent of profit, or, in the worst case, some percent of total assets. It is not only complex but requires you to trust some company whose insurance pool size you cannot see.

- The second category provides insurance to wallets directly. There is usually no possibility of staying anonymous or making it autonomous. All known companies in this area operate fully off-chain. So, their fee, insurance pool size, and success coverage cases are unknown.

We are different from all of them, firstly because our protocol is decentralized and transparent. You can check the insurance pool size and total covered liquidity directly on the blockchain at any moment. On top of that, you can vote for coverage cases and control how protocol evolves through DAO. There is currently no one, who has been able to develop a decentralized insurance protocol.

Secondly, our protocol covers both sides of the equation: the wallet and DeFi protocols together. We cover wallets from profits that generate DeFi protocols in which our Vaults invest. Additionally, we cover these DeFi protocols with insurance. So even if they are hacked, you still do not lose money. This way, we can monitor and audit protocols independently, and, as a result, diversify investment between them in the most secure way, in real-time.

Thirdly, we do not take any fees from users' money. Deposit, withdraw, or assets that you hold do not encounter any fees. So you can just save and forget about money till the moment when they need you. On top of that, we pay a premium on money that the user saves in protocol, so you can even earn passively with us.

More info on hacks amount: https://www.chainalysis.com/blog/2022-biggest-year-ever-for-crypto-hacking/

How is Eonian's insurance pool funded?

This insurance pool is bootstrapped from protocol founders' money, showcasing our trust in the solution's safety. In the future, any liquidity provider will be able to invest in it to receive returns from insurance fees. Insurance from this pool is paid from the revenue of the protocol, not by users directly.

The revenue mainly comes from the investment of assets, which is covered by insurance. At this stage, the protocol works as a traditional yield aggregator. Assets invested in different lending protocols and DEXes, where they earn returns from fees of these protocols. Nevertheless, our protocol works a little bit differently from other yield aggregators. While they prioritize returns on investment, our protocol invests in a way that decreases the risk of investment. It distributes assets between multiple protocols, which decreases the risk of losing all assets in case of a one-protocol hack.

Our protocol and protocols in which we invest are also covered by insurance, which results in much lower investment risks.

The majority of revenue generated from investment protocols is used to pay and fill the insurance pool, but when the insurance pool is bigger than the need to cover users' assets, the revenue is redistributed back to users as a premium. This allows users to not only save their assets but also grow them while they are holding them.

What measures ensure insurance pool sustainability?

You can read more about the economic model behind the insurance pool there:

But in short, our insurance pool model generally works similarly to traditional banks. They earn money from giving loans and pay from profits in case of losses or other issues. So, even on a high level, you can see that it is a very sustainable model. But crypto still has some differences.

At the current moment, the amount of wallet hacks is between 0.2-2% per year, and with our diversification of investments between protocols, we can expect between 0.5-2% of TVL loss because of DeFi hacks. Also, on average, yield aggregators generate around 5% APY. Our investment strategies historically generate from 5% to 15% APY.

These numbers show that after all covers, we can expect that the insurance pool will grow from -14% to 92% per year. So, even in the case of abnormal growth in hacks during the year and low APY on the DeFi market, we will be able to pay users money. But to maintain the stability of the pool size, we have in place three strategies:

- We can adjust the amount of premium that we pay to users dynamically, to increase the amount of profits that go directly to the insurance pool.
- We can dynamically decrease the coverage percent size, to make for people less interested in saving money in Vaults. As a result, it will decrease the new liquidity flow and give the protocol time to grow the insurance pool size until it is able to cover new money.
- In the future, we will also provide liquidity providers the ability to invest directly in the insurance pool. They will be able to earn high APY as a reward for covering the

risks for regular holders.

Technical Architecture

The main information for technical architecture will be provided in the whitepaper, but there, you can see a general overview.

Eonian Savings Account operates using a specialized protocol crafted meticulously to serve the dual purpose of insuring user assets against hacks and facilitating their growth. At its core, the protocol integrates the mechanics of a proven yield aggregator optimized for our specific use case.

The Yield Aggregator

A yield aggregator is a protocol that automates the process of seeking the highest returns on investments within the DeFi ecosystem. It does so by strategically allocating assets across various lending and liquidity platforms. For Eonian, this mechanism is pivotal in generating revenue and insurance payments.

The aggregator continually scans the DeFi landscape, redirecting assets between lending protocols like Compound, Aave, and various DEXes. The objective is twofold: maximize return on investment while diversifying to minimize risks. In the case of Eonian, it mainly targeted minimizing risks and impermanent losses through diversification and proper investment planning.

Revenue Distribution

The revenue generated through the yield aggregator undergoes a structured distribution:

Insurance Pool

A significant portion is directed towards the Insurance Pool. This pool is crucial, acting as a safety net, ready to compensate users in the unfortunate event of a covered hack. It's noteworthy that the insurance pool's architecture currently rests on a multisig wallet setup, developed by the renowned and trusted provider, SafeWallet. This design ensures both security and transparency in fund management.

The exact percent of revenue distribution to the insurance pool will be dynamically adjusted based on liquidity pool size and overall assets size, which it must cover.

User Premiums & Protocol Maintenance

After allocation to the Insurance Pool, the remaining revenue caters to operational costs, user premiums, and other protocol-specific rewards and incentives. As our ecosystem grows, we anticipate these revenue streams to play a more substantial role in protocol sustainability and user engagement.

Insurance Pool Future Development

While our current setup leverages SafeWallet's multi-sig model, our vision for the Insurance Pool is expansive. In the foreseeable future, we aim to democratize the pool by allowing individual participants to provide liquidity. Such a move will not only increase the pool's robustness but will also integrate a community-driven approach, letting multiple stakeholders actively contribute and benefit from the protocol's growth. Such an insurance pool provider will be able to earn part of the payments that are paid for insurance coverage.

Conclusion and Future Outlook

We believe that DeFi and crypto, in general, are struggling to replace traditional finances not because of not enough high returns but because of the lack of safety that traditional finances can provide. On the other side, DeFi can become an even safer solution than TradFi, given the technological features of blockchain, like decentralization and transparency, that banks usually lack.

We replicated the banking core solution and adjusted it for the on-chain operation to potentially create a platform where a new decentralized bank can be built. This way, we can elevate overall DeFi safety by providing insurance for different protocols and savings core to smart contract wallets.

Developed by the Eonian Team. For more information, visit Eonian.