HACKLESS

Multi-service security platform for DeFi protocols

WHITEPAPER

v. 2.0 September 2022

CONTENTS

INTRODUCTION

01 The Hackless platform is being designed to bolster security of DeFi protocols by offering a comprehensive package of monitoring tools, analytics and security services. Hackless offers a complex and reliable toolkit that helps boost a DeFi protocol's security from hacks and malicious attacks. The platform's services are aimed at helping developers both to detect a potential hack attack and save funds in case a protocol is attacked.

02 The platform combines security features to provide DeFi protocols with a multi-sided protection. A DeFi protocol will greatly benefit by extensive ongoing monitoring features with dynamic analysis of transactions, mempool tracking, transactions and funds flow analysis models, tools for safe funds migrations and an alert system, among other features.

03 Hackless works at the infrastructure level of EVM-compatible blockchains and unites several elements from the blockchain ecosystem in order to strengthen the smart contract's security from the lowest levels of the blockchain ecosystem.

PROBLEMS TO SOLVE

Smart contract development, in general, and DeFi protocols launch in particular, involve handling a large number of possible vulnerabilities and ways that could compromise the code. Almost every big protocol from EVM-based chains struggles with possible exploits and the security of user funds due to vulnerabilities that exist since Ethereum was created. However, progress has been made, numerous security tools and static analysers have been created, the newest approaches in testing and best practices of Solidity development have appeared, and professional teams of smart contracts auditors have formed.

Nevertheless, progress is ongoing, therefore exploiters and hackers are attempting to find new ways of breaking smart contract security and finding vulnerabilities, which are threats to the funds of users. Exploiters are able to use a huge amount of computable power, create a bunch of monitoring scripts, work with transactions directly in the mempool, and even work with miners and miners' pools. As a result, DeFi protocols struggle to deal with new types of attacks at the infrastructure level. Moreover, handling such issues without good defence mechanisms is quite difficult and requires a significant amount of resources – both financial and in terms of development, not to speak of the time required.

PROBLEMS TO SOLVE

Furthermore, if a hack attack has already taken place, and a protocol is under attack, there is almost nothing that can be done, except to pause all operations. Consequently, all funds are locked and become inaccessible. Since the protocol is already under the close eye of the hacker and is constantly monitored, there is no way to free the funds and migrate to a new version.

It is also important to remember that all these problems usually appear because of the technical advantage that exploiters possess. In most cases, it is more important to prevent an attack before it happens. To achieve this, reliable and constant monitoring of incoming transactions and advanced analysis is necessary. However, this still remains a problem because it also requires the approach based on the infrastructure layer of Ethereum.

So, in a few words, the DeFi protocol may face several problems:

Probability of exploitation at the infrastructure layer – from well-known frontrunning to advanced techniques

Lack of monitoring and analytics that would help prevent attacks

Lack of early alerts for the under-attack mode

Locking of funds in case of under-attack mode

Hackless aims to offer a solution for all these problems.

PROBLEMS TO SOLVE

The main goal of the Hackless platform is to provide a robust security layer between the Ethereum (or other EVM-compatible blockchains in the future) infrastructure layer and DeFi protocol. Hackless aims to resolve the aforementioned problems by means of the following actions.

- Provide a safe infrastructure for the preparation of private transactions and private mining
- Provide dynamic checking services for constant monitoring of mempool and incoming transactions
- Provide a safe solution for fund migrations from the attacked DeFi protocol
- Provide analytics models for detection of fraudulent and dangerous transactions in order to prevent the attack before it begins
- Provide alert systems
- Ongoing cooperation with the teams of auditors for combining security measures on both the smart contracts side and the infrastructure side.

The Hackless platform aims at becoming a security provider for DeFi protocols with a complex approach involving ongoing monitoring, prevention of attacks, as well as providing safe solutions for under-attack protocols.

KEY FEATURES

Cryptographically protected operations

Advanced analytics against fraudulent transactions

Quick and safe migration of funds and liquidity

Ongoing protection of DeFi protocols

Early detection of suspicious activity

Boosted security of smart contract infrastructure

These are the core features that create the basis of Hackless as a comprehensive security platform. We strive to add new features regularly to meet the needs of the ever-evolving DeFi universe.

PLATFORM PRODUCTS

As a security platform, Hackless provides multiple services to ensure complex security of a protected protocol.

SafeMigrate

The first-to-market service which ensures that funds can be successfully migrated by the user from a paused DeFi protocol. It is the core application and the first solution developed by the Hackless platform. It includes the application to get signed transactions from users and protocol owners, and private mining services to ensure the execution of the transactions within one block. Therefore, even if the protocol is under attack, funds can be migrated to a newer and safer version of the protocol.

Watchdog

It includes on-going services for checking and validating transactions directed to a protocol in order to locate fraudulent transactions and prevent an attack on a protocol with an in-time pause or migration transaction feature. This requires on-going mempool monitoring, signed pause transaction, transaction analysis services and the alert system – all components are accessible within the Hackless platform. The core application will allow DeFi project teams to feel more secure as alerts will be received long before an exploiter is able to launch an attack.

Mancer – **Security analysis module**

This is one of the key components of the Watchdog service and it offers a set of frequently updated models, which are applied to the set of transactions in order to find fraudulent or suspicious ones. Based on modern machine learning algorithms and models, it helps the Watchdog service to detect potential exploitative events.

Guardian – **Alerts system**

One of the key components of the Watchdog service that provides the call-back to the DeFi protocol in case a dangerous transaction has been noticed or if an unusual flow was detected. The next level of the alert system is stop-transactions – previously signed by the owner a paused transactions, which can be executed right at the moment a suspicious activity is detected in the protocol. It creates a safe switch, which prevents the protocol from being exploited.

PLATFORM PRODUCTS

Warehouse – **Analytics system**

This component of the Watchdog service provides complex analytics for collected data from the protocol. This allows for a check on the visualised state of the system, the checked transactions, fund flows and other additional data which can be collected during monitoring. These modules are useful, for instance, for the tracking systems during the post-mortem investigations of the hacked protocol.

Conductor – **Private mining provider**

One of the key services offered by the Hackless platform. It provides transactions to the private mining pool in order to ensure that the attacker will not be able to detect countermeasures directed against the exploit. This feature will be expanded in the future to include other EVM-based networks such as Polygon, BSC, Fantom, Avalanche, etc.

HacklessLib – **Solidity security libs**

A side-product of the Hackless platform based on the security measures and recommendations collected from the experience of platform engineers. Based on regular contact with the teams of auditors and own smart contracts safe restrictions, HacklessLib will be a valuable addition to the standard OpenZeppelin library.

Hackless services for individual DeFi users

At Hackless, we're sure that for an individual DeFi investor asset protection is as important as ownership and investment. With so many hacks taking place, individual protection will greatly add to the overall industry security level and offer more confidence in keeping investments safe across a huge number of decentralised projects.

This being said, an individual user can also access Hackless security services:

- Stake Warden – an individual subscription for boosted protection of stakes, deposits and other DeFi operations
- Conductor – a MEV-powered service used for designing individual solutions for migrating assets from a hacked digital wallet

PLATFORM PRODUCTS

Stake Warden

This can enhance the safety of the funds which they provide on third-party protocols outside the Hackless ecosystem. As a user stakes their tokens and provides a signed transaction for the required action (unstake funds, withdraw them back to a user's wallet, repay loan, make a SafeMigrate request, etc.), the Watchdog service continuously monitors third-party protocols. In case any suspicious activity is detected, Watchdog sends an immediate alert to the Hackless platform and notifies the user. If there is a possibility of a hacker attack, SafeMigrate claims the funds of users and migrates them securely (or executes other tx provided by the user).

Conductor for everyone

This service can help if an account is hacked, private key is compromised, or if the user still has a great deal of valuable assets that get stuck in the wallet.

Here are some instances when Conductor can be applied:

- You have NFTs on the wallet, either set for an auction or are simply being held – both evaluated or unevaluated – which you wish to move to a safe place.
- Non-liquid assets – some "land" tokens from the NFT game, some items or creatures from the play2earn game, some in-game tokens or any other assets which cannot be sold in DEX. Now you need to migrate them to a safe place.
- You participate in a staking or vesting program of the token, which is not tradeable yet. As a result, you need to change the participating account or migrate already unlocked tokens.
- You have some funds staked or deposited or lent funds and you have a bit of time while the hacker is still guessing. Therefore, you need help to claim rewards, unstake utility tokens, and withdraw your deposit from the vault or any DeFi protocol.
- You have positions opened in order books, in lending protocols or other financial instruments, in turn requiring help to close the position and withdraw funds to a safe place.

* For all these cases Hackless team will prepare an individual solution for each DeFi participant. At the moment, we're doing it through a custom solution within Conductor. And once the use case gains traction and is established as part of Hackless services, the team will make it a part of Stake Warden with an easy-to-use interface. Over time the variety of cases accessible for the user via Stake Warden will only grow and include more standard DeFi operations.

EXPANSION PLANS

Beside the core features offered by the Hackless platform, we have a vision of the platform's further development. We see immense potential and scope for further development since there is no limit in terms of improving security.

We plan on expanding the list of supported EVM-based chains. Hackless starts from the Ethereum – and will apply all features in this regard. Nevertheless, core applications may be expanded to other chains.

Connection of analytics for non-EVM chains. Several modules and applications from the Watchdog service can be applied to almost every blockchain, therefore, they are the first candidates for the expansion.

Services to improve fund security. Migration of funds to a new version of the protocol is not the only possible case requiring protection. Safe swaps, safe deposits, flashloan resistance – all of these are actual cases facing issues of a lack of security.

MEV services support for other EVM-based networks (Polygon, Fantom, BSC, Avalanche).

Dynamic analysis. Expansion of analysis to check not only the single protocol, but the entire connected ecosystem with a shift from analysis to prediction.

DAO expansion to integrate it with Hackless services for subscribed protocols as an additional layer of security.

DAO voting-based pause mechanics for subscribed protocols. It is additionally secured by the service of signatures collection in order to ensure the honesty of participants.

All of these are distant plans of the Hackless platform. Nevertheless, they are valuable and in demand, and are therefore added to our features list.

EXPANSION PLANS

Keeper approach

Hackless services can be outsourced to a set of nodes, which are incentivised to perform client operations and process front-running transactions based on a protocol configuration in a manner that is trust-minimised and decentralised.

Hackless Keeper will stake HKLS tokens in order to participate in task distribution process. This stake will be also used for penalty in case of false-positive scenarios.

A regular user will have to create a configuration task and pass signed transactions via trusted channel to Hackless Keeper network in order to use Hackless Keeper Protocol. User should stake HKLS tokens which can be later withdrawn by Keeper in case of a successful task processing.

Depending on the staked HKLS amount, different concurrent Keepers will do mempool simulation and transaction processing.

TOKENOMICS

The Hackless platform maintains its own utility token – HKLS. The token is used as an internal asset to gain access to the platform's core features.

Token utility

1. Subscription

Users provide the necessary amount of HKLS tokens and stake them on the platform. The amount is locked for the chosen period of time – several days, several weeks, several months or a year. The amount (recalculated on a daily basis) decreases if the term becomes longer. The longer the subscription period, the less tokens are locked. During the 'lock period' tokens are linearly burnt – returned to the treasury in order to be recirculated later through the rewards system. Nevertheless, users can freely unlock the amount of tokens left without incurring additional fees – only the actually used amount is charged. Also, the first users of the platform will not have a burn rate in order to stimulate the usage.

2. Tiers for access

Subscription services have several tiers in order to provide flexibility of services and meet users' needs. The Hackless platform will offer tiers for providing combinations of the Watchdog service core components: alerts, several levels of analytics, stop-transactions, data for analysis accumulation, etc. Users will be able to combine any services they require and not lock extra tokens.

3. Private mining services

The Hackless platform works as a provider of private transactions in order to ensure that the attacker will not be able to detect countermeasures directed against the exploiter. Therefore, these transactions are charged in the platform native protocol with the ability to deposit sufficient amount of tokens for prolonged usage of the service. The service has the ability to be expanded into other EVM-compatible chains (Polygon, BSC, Fantom, Avalanche, etc.).

Token utility

4. DAO

The HKLS utility token also works as a governance token. It gives the user voting power for the DAO, where the main proposals for the platform's developmental direction will be offered. By holding HKLS tokens and using it for voting, users will add more security to the platform.

5. Decentralised Security Council Stake

The service applicable for HKLS token holders allows them to stake the token in order to take part in the governance of a certain smart contract agreed for a particular service. Hackless platform and the guarded protocol incentivise councillors to stake the HKLS token. In the response, they should secure the protocol by monitoring and pausing the contract in case of an attack. To ensure the honesty of the councillors, their stake and rewards are locked for several periods, or until new councillors are selected.

6. Insurance deposit

There is a special kind of security insurance deposit for users, which allows users to stake HKLS tokens in order to secure funds deposited in a DeFi protocol. A user provides a signed transaction for the secure migration of deposited funds and HKLS insurance deposit. Subsequently, the user gets a custom instance of the Watchdog service, which searches for unusual activity on the target protocol on an individual basis for the user. Once suspicious activity is detected, the Hackless platform migrates user's funds to their reserve address through the SafeMigrate service. Therefore, the user gets individual Watchdog instance with safe funds migrations for any kind of DeFi service in exchange for the insurance deposit of HKLS tokens (which are burnt in case of usage).

7. Token utility for individual users

Each HKLS token holder can get maximum value by staking their HKLS tokens. As a user stakes HKLS tokens, they:

- Receive voting power in the DAO.
- Get incentivised by receiving tokens from Hackless partners.
- Get access to the Hackless security services which greatly enhance he safety of the funds of all users outside the Hackless ecosystem.

TOKENOMICS

Token utility

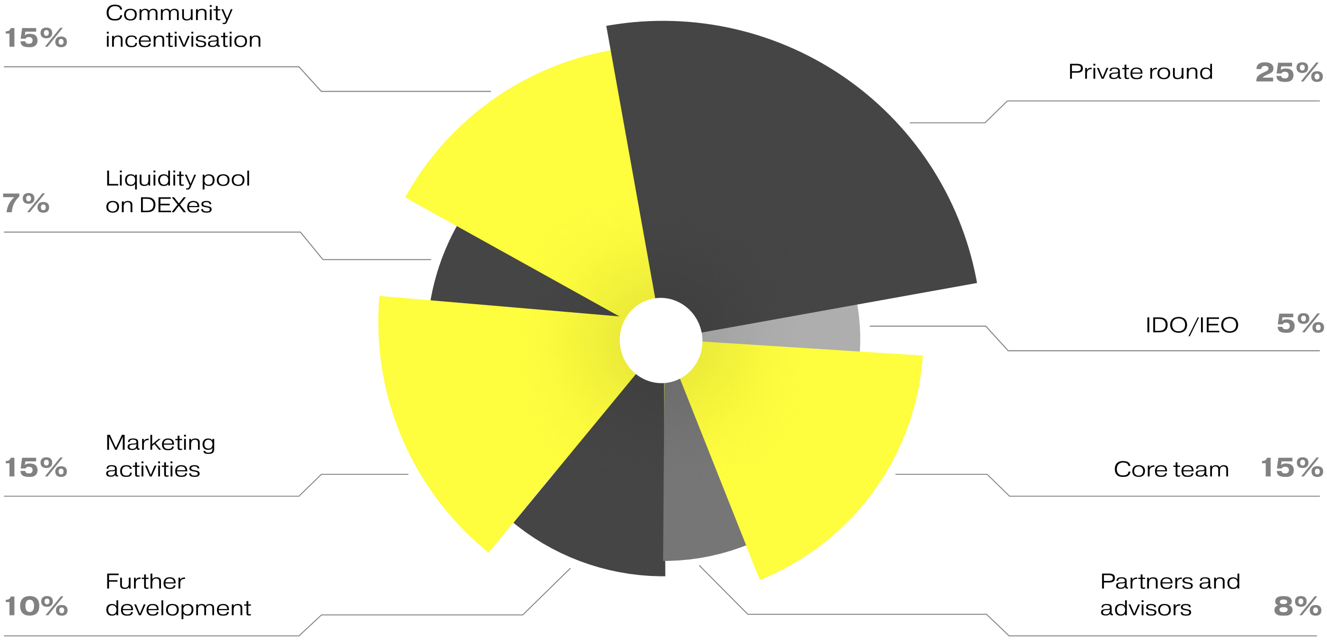
An individual user can secure their assets with Hackless in the following ways:

1. Provide an action on a third-party protocol. For example – stake tokens, make a deposit or even take a loan on a lending platform.
2. Stake HKLS tokens on our platform to get individual subscriptions on the set of services.
3. Provide a signed transaction for the required action: unstake funds, withdraw them back to a user's wallet, repay or even liquidate loan, transfer to a safe location or even make a SafeMigrate request.
4. Watchdog continuously monitors third-party protocols. In case any suspicious activity is detected (rapid TVL decrease, suspicious transactions, etc.), Watchdog sends an immediate alert to the Hackless platform and notifies the user.
5. In case there is a possibility of a hacker attack, SafeMigrate claims the funds of users and migrates them securely (or executes other tx provided by the user).
6. In a scenario where a protocol owner pauses the smart contract, Watchdog monitors its mempool and once the smart contract is unpaused, SafeMigrate claims the funds of users immediately.
7. Staked HKLS tokens are charged for the provided security services. The longer these tokens are staked, the less users will be charged.

The Hackless platform does not have access to the funds of users since the provided signed transaction only allows our protocol to return assets to a user's wallet. This way, we enable the highest possible trustless security for the funds of individual users on other DeFi protocols. A user gets access to the individual migration request or other transactions available for private execution, as well as an individual alarm and instances of Watchdog service.

TOKEN DISTRIBUTION

The initial HKLS distribution is 20 million tokens. This number includes all of the categories of token recipients in the distribution schedule.



Private round 25%

All private round participants will have a 3-month cliff before the linear 12-month vesting period starts. 10% of tokens are unlocked immediately which allows initial usage of the platform and participation in further staking programs.

IDO/IEO 5%

Strategic round is hosted on the Hackless platform within native smart contracts. All participants have a 3-month cliff before the 12-month vesting period. 10% of tokens are unlocked immediately to allow participants to use core services of the platform from the moment of their launch and to take part in staking programs.

Core team 15%

Core team is incentivised with tokens for the future development and expansion of the platform. In order to provide fair incentivisation, team tokens are locked for 12 months before the 18-month vesting period starts.

TOKEN DISTRIBUTION

Partners and advisors —— **8%**

Incentivisation program to encourage external advisors and partners to enroll in the platform's development and growth. To prevent the oversaturation, 3% of tokens will be available initially on the market, the rest of the tokens have a 6-month lock before the 18-month linear market entry.

Further development —— **10%**

Incentivisation for the dev-team and external contributors (in the form of grants for example). To prevent the oversaturation of the market, these tokens have a 6-month cliff before 18-month linear market entry.

Marketing activities —— **15%**

The marketing activities tokens have a 3-month cliff (just by the time the first product is ready) and 18-months linear market entry.

Liquidity pool on DEXes —— **7%**

To provide the sufficient amount of tokens for circulation on decentralised markets, initially 15% of the tokens will be available, but liquidity will be spread among several DEX platforms, so liquidity will be provided as the tokens are added to the platforms. The rest of the tokens have a 1-month cliff before 6-month market entry.

Community incentivisation —— **15%**

Launch of several staking programs, liquidity providers and early participants incentivisation. In order to encourage token holders, we decided to provide incentivisation programs at an early stage. Therefore, 2% of tokens will be available initially, after a 1-month cliff the rest will be linearly released during the next 30 months.

TOKEN CIRCULATION SUPPLY

The chart below shows the allocation of HKLS tokens and increase in circulating supply as tokens unlock.

	Purpose	Supply, HKLS	Supply, %	TGE unlock, %	Lock-up cliff	Vesting*
■	Private round	5MLN	25%	10%	3 months	12 months
■	IDO/IEO	1MLN	5%	100%	35% each month	35% each month
■	Core team	3MLN	15%	0%	12 months	18 months
■	Partners & Advisors	1,6MLN	8%	3%	6 months	18 months
■	Further development	2MLN	10%	0%	6 months	18 months
■	Marketing activities	3MLN	15%	0%	3 months	18 months
■	Liquidity pool on DEXes	1,4MLN	7%	15%	1 month	6 months
■	Community incentivisation	3MLN	15%	2%	1 month	30 months
	TOTAL:	**20MLN**	**100%**			

*linear vesting starts after the cliff

HACKLESS

Get armed with Hackless to
protect your DeFi protocol