Whitepaper



CRYP2NOVA

Version 1.0

2019

Archived copy · cryp2nova.com

1. What is Hacken 2
1.1 Hacken History 2
1.2 Hacken Business to Business (B2B) products 3
1.2.1 Hackenproof 3
1.2.2 Security Assessment & Incident Response 3
1.2.3 Blockchain Security Consulting 4
1.2.4 CryptoExchange Ranks - CER 5
1.2.5 Cyber School & White Hat community development 6
1.3 Hacken B2B key goals in 2020 7
1.4 ICO use of proceeds 8

2. What is HackenAI 9
2.1 Problem 9
2.2 Market Opportunity 10
2.3 HackenAI Solution 10
2.3.1 Cyber Boot Camp 11
2.3.2 Password manager 12
2.3.3 Two-factor authentication (OTP generation) 13
2.3.4 Compromised accounts monitoring 13
2.3.5 Secure storage 13
2.3.6 VPN service 14
2.3.7 NonCustodial Crypto Wallet 14
2.3.8 Digital Asset Viewer/Tracker 14
2.3.9 Cybersec Marketplace 14
2.3.10 CER 15
2.3.11 News and industry alerts 15
2.3.12 Others 15
2.4 Tech Implementation 15
2.5 Security 17
2.6 Technical Roadmap 19
2.7 Competitors Analysis 20
2.8 Go to market strategy 22

3. What is HAI 23
3.1 Why VeChain? 23
3.2 HAI transaction model 23
3.3 Tokenomics 25
3.4 HAI as a key element for HackenAI user base growth 28
3.5 HKN Migration 29
3.6 HAI Distribution 29
3.7 Use of Proceeds 30
3.8 HAI Roadmap 31

4. Legal 32

5. Team 33

6. Combined Roadmap 34

7. Summary 35

LEGAL DISCLAIMER 35
Warning About the Token 36
Sales restrictions 36
Warnings 36

Archived copy · cryp2nova.com

1. What is Hacken

1.1 Hacken History

Hacken, founded in August 2017 by cybersecurity experts, Big 4 professionals, and white hat hackers, is a cybersecurity ecosystem. The ecosystem development budgets were formed from the HKN token generation event that occurred in October - November 2017.

Since late 2017, we have been developing an ecosystem that:

- Ensures continued high-quality protection from major cyber risks for our clients
- Contributes to the development of an ethical hackers community through education and client connection
- Simplifies knowledge on cryptocurrency exchange cyber risks

We are focused on securing tech infrastructure from cybercriminals through our:

Experienced Team:
50 years of combined experience in protecting clients of all sizes and industries including banking, manufacturing, transportation, and e-commerce.

Strong R&D and Knowledge Base:
Highly professional in-house experts regularly strengthen their skills by analyzing the latest hacking methods shared within the HackenProof community of 2,000+ cybersecurity researchers.

Education & Network:
Hacken CyberSchool and the HackIT conference have developed a large international community of tech-savvy practitioners who deal with varying levels of cybersecurity issues.

Partnerships:
Hacken is cooperating with industry leaders such as CoinMarketCap, Bitfury, and Etherscan to promote cybersecurity, accountability, and transparency of the blockchain and IT industry.

Public Research:
Increasing brand awareness driven by unique research materials published in influential media such as *TechCrunch* and *Forbes*.

With more than 200 blockchain clients served over the last two years, Hacken has become the leader of the blockchain security industry, the biggest cryptocurrency exchange auditor, and a trusted brand in traditional enterprise cybersecurity.

Archived copy · cryp2nova.com

1.2 Hacken Business to Business (B2B) products

1.2.1 Hackenproof

https://hackenproof.com

HACKENPROOF is a bug bounty platform that helps businesses protect their digital assets, the personal data of customers, and their reputation through crowdsourced security.

By combining a “crowd” of cybersecurity researchers (white hat hackers) with the HackenProof platform, we deliver services that traditional cybersecurity firms cannot. Conventional cybersecurity companies are constrained by the size of their teams, as the amount of time and skill available is limited. A bug bounty platform solves this issue since hundreds of security researchers test products on a continuous basis. This approach allows vulnerabilities to be identified more efficiently and thus prevent possible cyber threats.

The HackenProof platform brings together a large number of expert white hat hackers from all over the world, specializing in finding vulnerabilities in various technologies such as web, mobile, hardware/IoT, and especially in Blockchain applications and smart contracts.

The core of the HackenProof platform is ethical cooperation between cybersecurity professionals and responsible IT companies that care about the security of their products. We ensure responsible and coordinated vulnerability disclosure and encourage white hat hackers to protect modern businesses.

Bug Bounty Platform Advantages

1. Unlike conventional cybersecurity firms, the bug bounty platform attracts a crowd of highly skilled cybersecurity researchers with various backgrounds to find product vulnerabilities.

2. The bug bounty platform provides transparent reporting, 24/7 analytics, and information on the current status of your bug bounty program.

3. The platform handles all operational issues - validating submitted bugs, communicating with the white hat hackers, and organizing other operational activities.

Due to the responsible decision to run a bug bounty at Hackenproof, white hat hackers identified high and critical vulnerabilities before the black hat did at more than 40 products. Tech teams were able to timely fix them and companies didn’t experience any financial losses.

1.2.2 Security Assessment & Incident Response

https://hacken.io/services/#security-assessment

Hacken delivers a wide range of professional services to protect systems, networks, and software applications from cyber attacks and human-based errors for businesses operating in the digital world. Our inhouse specialists design the best-in-class solutions, focusing on the specific needs of the client.

Archived copy · cryp2nova.com

Hacken Services Portfolio:

1. Offensive Testing & Defensive Services

- Web application penetration testing (“pentest”)
- Mobile application pentesting
- Social engineering testing

2. Incident Response & Brand Protection

- Cybersecurity forensics
- Malware analysis
- Phishing response

3. Hardware Security

- IoT and Crypto wallets

4. Managed Services

- DS\IPS\NGFW design\maintenance
- Anti-DDOS\Waf design\maintenance

5. Security Operations

- Security architecture consultancy
- Security hardening

1.2.3 Blockchain Security Consulting

https://hacken.io/services/#blockchain-security

From 2017-2019, Hacken performed 150+ security audits for blockchain companies, establishing it as a trusted partner and industry leader. Hacken also manages blockchain security industry players cooperation through various public and private cybersecurity groups and communities.

Our professional team of consultants performs smart contract audits, DApp security reviews, and blockchain protocol reviews in accordance with our internal methodology and industry best practices. Hacken provides security consulting services across multiple different blockchain protocols, including VeChainThor, Ethereum, Tron, EOS, and more.

Smart Contract Audit
The Hacken team analyzes smart contract functionality and administers necessary checks against all known vulnerabilities. A security audit includes a manual codebase audit by Hacken consultants, an automated tools security audit, and a brief analysis of the smart contracts functionality.

DApp Security Review
A decentralized application (DApp) operates its backend code on a decentralized peer-to-peer network.

Archived copy · cryp2nova.com

A Hacken DApp security review focuses on the client and server-side security issues for the DApp. The review also consists of a smart contract audit for the back-end and "smart" penetration testing (“pentest”) for the front-end. A smart pentest checks for any potential server misconfigurations and Cross-Site Scripting (XSS). For DApps with rich server logic (database, registration forms etc.), a full pentest is recommended.

Blockchain Protocol Security
Cybersecurity is often not a priority during the development of innovative and original protocols. However, after accumulating considerable sums of money, blockchain protocols are susceptible to becoming targets of hacking attacks. Hacken offers blockchain protocol security which includes three sub-services: a protocol model security review, a tokenomics review, and a protocol implementation security analysis.

1.2.4 CryptoExchange Ranks - CER

https://cer.live

CER is the first digital assets auditor that systematizes and publishes data on crypto exchanges to protect traders from fraudsters.

CER has worked on numerous transparency researches and investigations that have impacted the industry maturity. They were republished by most of the biggest tech and crypto media.

CER is widely known for its trusted rankings:

- Top 100 cryptocurrency exchange cybersecurity ranking
- Cryptocurrency exchange hot and cold wallets balance ranking

CERtified
Hacken helps cryptocurrency exchanges build long-term successful relationships with their customers by setting up the highest cybersecurity standards through the CERtification compliance process.

Cybersecurity CERtificate
While blockchain technology facilitated freedom in executing financial operations, it also attracted thousands of black hat hackers. The main threat is the irreversibility of hacked or misspent crypto assets. Once an exchange is hacked, it is extremely unlikely that any compromised digital assets can be reversed, as most blockchains are immutable. Users of the exchanges have the right to know if the platform is compliant with cybersecurity best practices.

As a cybersecurity leader, Hacken has created industry-leading cybersecurity standards for cryptocurrency exchanges. The CER cybersecurity certificate is an Exchange 2.0 compliance standard, which signifies that a cryptocurrency exchange can be trusted.

Cryptoexchange security assessment methodology was developed based on vast experience.

Certification covers areas such as the building and maintenance of a secure network, protection of clients data as well as provides effective cybersecurity threat protection measures.

Archived copy · cryp2nova.com

Proof of Funds CERtificate
Trade volume has already been deemed an unreliable metric for cryptocurrency exchange's ranking. Traders and Crypto projects are no longer using the trade volume metric while making decisions on which exchange to choose.

Today the key metric for a trader is transparency of operations and mitigation insolvency risks for exchange.

The first step for industry maturity is to develop an accountability standard for exchanges to report the balances of crypto that they are holding on their traders' behalf.

Proof of funds CERtificate is the first and leading initiative for hot and cold wallet's data aggregation.

1.2.5 Cyber School & White Hat community development

https://cyberschool.tech

Cyber School is a training course for juniors/rookies to become middle-level cybersecurity specialists.

We transferred our experience from running a number of offline hacking events to create a cybersecurity training program, the most comprehensive one available in Eastern Europe. It runs for five months and includes:

- High-level understanding of TCP/IP protocol and OSI Seven Layer Model
- Windows and/or Unix-based systems/architectures and related security, LAN/WAN technologies
- Solid understanding of information technology and information security

White Hat Hackers Community Development
In 2017 and 2018, Hacken organized a global cybersecurity forum HackIT that gathers leading companies and prominent names from the industry, as well as top ethical hackers.

In 2019, Hacken co-hosted Blockshow Asia 2019 in Singapore as a privacy and cybersecurity partner. BlockShow one of the biggest conferences in the blockchain industry, considered by many as a "flagship event".

From 2019 and onwards, Hacken is supporting various cybersecurity conferences and white hat community events with an essential focus on the Onsight Bug Bounty Marathon **Hacken Cup**.

About Hacken Cup
The Hacken Cup is a short timeframe bug bounty event custom-tailored to a client's needs. Hacken brings together top white hat hackers to perform an onsite bug bounty marathon for select clients. White hat hackers from all over the world look for vulnerabilities, immediately reporting their findings on the spot. Triage teams validate reports allowing the security team is able to tackle found issues right away.

Archived copy · cryp2nova.com

Past Events

Hacken Cup 2018

25 hackers 4 companies 60 reports
https://www.youtube.com/watch?v=NDLdGEGCQOE

Hacken Cup 2017

25 hackers 3 companies 102 reports
https://www.youtube.com/watch?v=O2XZmRFwNaM&t=21s

1.3 Hacken B2B key goals in 2020

HACKEN PRODUCT/SERVICE LINE	BUSINESS DEVELOPMENT	PRODUCT DEVELOPMENT
Hackenproof	**Grow White Hat Hackers Community to 5,000 researchers**	SaaS bug bounty solution for small internet companies
Security Assessment & Incident Response	Open business development office in Singapore	**Automated scanner for cybersecurity threats**
Blockchain Security Consulting	**Establish a Blockchain Security Alliance**	DApps security research
CER	CERtificates legitimacy through cooperation with traditional economy regulators	**Vulnerability disclosure programs aggregator for cryptocurrency exchanges**
Cyber School & White Hat community development	**Hold Hacken Cup 3 in Singapore**	Online cybersecurity education course

CRYP2NOVA

Archived copy · cryp2nova.com

1.4 ICO use of proceeds

In autumn of 2017, Hacken issued HKN token as part of community building and fundraising event for ecosystem development. A total of 4 million of HKN tokens were sold reaching Limited milestone that reflected the following ecosystem element's development:

HACKEN ECOSYSTEM ELEMENT	RAISED FUNDS ALLOCATION
HackenProof Marketplace	60%
HackIT Conference	15%
Hacken Accelerator	25%

During the HKN generation event, Hacken received 252 BTC, 5,359 ETH and 1,240USD in exchange for 4mln HKNs. Raised funds were released and converted on a monthly basis, according to development budgets. The average BTC conversion rate was $5,237 and $211 for ETH, resulting in a $2.45 MM USD ecosystem development budget.

Raised funds allocation

HACKEN ECOSYSTEM ELEMENT	HACKENPROOF MARKETPLACE	HACKIT CONFERENCE	HACKEN ACCELERATOR (CER & CYBER SCHOOL)
Budgets according to Hacken Ecosystem WP 2017	**60%**	**15%**	**25%**
Cybersecurity team	-2.4%	-1.0%	0.0%
Product development costs	-1.6%	-0.3%	0.0%
Marketing & Business development	-2.9%	-1.2%	0.0%
Administration costs	-0.8%	-0.4%	0.0%
2018, net of revenues:			
Cybersecurity team	-6.9%	-3.1%	-2.3%
Product development costs	-5.3%	-0.7%	-9.8%
Marketing & Business development	-7.3%	-3.9%	-4.5%
Administration costs	-3.1%	-0.9%	-1.2%
2019 actual + budget, net of revenues:			
Cybersecurity team	-3.3%	-0.7%	-1.5%
Product development costs	-1.8%	-0.3%	-2.4%
Marketing & Business development	-2.9%	-1.3%	-1.2%
Administration costs	-1.4%	-0.2%	-0.8%
Reserve for 2020 and onwards	**20.1%**	**1.0%**	**1.2%**

Hacken community and HKN holders are the key creators of the Hacken ecosystem. Hacken management and its team are very thankful for this opportunity to work on a lifetime project and develop something inspiring.

Archived copy · cryp2nova.com

2. What is HackenAI

The creation of HackenAI is our reward and effort to pay back the Hacken community for their trust and support. All gained experienced, partnerships, expertise in cybersecurity, and tokenomics are now in one single application. We believe it will disrupt the personal cybersecurity market.

2.1 Problem

cybercare = healthcare

Preventative measures go along way in healthcare and cybersecurity. However, many individuals don't invest in preventative measures to improve their health or their cybersecurity protocols. Typically, we only visit doctors when there's a problem or seek professional IT help after an attack.

Healthcare and cyber protection require a preventive approach. But many still disregard their personal cybersecurity because:

- They believe that cybersecurity is too complicated and don't want to spend time it out
- There is a misconception that antivirus software solve all problems
- There is a lack of educational material regarding personal cybersecurity
- Most people think that they are safe just because they are small targets, that is why they are the perfect victims
- Lack of sense of urgency because they haven't been hacked yet or don't personally know any hacking victims

Rise of digital assets

For many years, banks and governments have been responsible for the security of assets. As blockchain technology adoption grows and systems become more decentralized, users must take personal control over their data. Software alone does not provide a sufficient level of cybersecurity, and security ignorance is no longer an option. The risk of a cybersecurity attack on an individual user who is their own crypto asset custodian is increasingly higher due to the irreversibility of hacked or misspent crypto assets.

Digital assets are now getting a lot of attention, as the transition into a more digital reality begins. However, even since the early days of the internet, it was almost impossible to prevent digital fraud and other criminal activity. With the introduction of blockchain technology, some strides forward have been made, however, we still have to deal with the huge problem of securing all of our digital assets.

In the world of cryptocurrencies, the main threat is the irreversibility of hacked or misspent crypto assets. Once an exchange is hacked, it is extremely unlikely that any compromised digital assets can be recovered, as most blockchains are immutable.

Today, individuals' digital assets are the easiest targets for black hat hackers. As a result, we see:

- Social media phishing attacks as the main gateway to crypto account access
- The takeover of individual accounts through leaked databases and 2FA resets
- Increase in successful SIM swap attacks
- Bitcoin clipboard steals

Archived copy · cryp2nova.com

Cyber threats as a stoppage factor for crypto mass adoption

While cryptocurrencies will inevitably become a standard asset class, there will be a delay in adoption as hacks and security threats continue to dominate the headlines of the mainstream media. According to the *Deloitte 2019 Global Blockchain Survey*, 29% of enterprise-level respondents see security threats as major organizational barriers to institutional blockchain tech investors, along with regulatory issues at 30%, and legacy system retrofitting/replacement also at 30%.

2.2 Market Opportunity

Just like antiviruses software has helped to protect almost every computer since the ’90s, users in the new digital era need cybersecurity assistance to form a preventive shield from new and growing cybersecurity threats. With all of these threats constantly on the minds of both current investors and sideline investors, there is an increased demand for products that put these fears to rest. More specifically, there is a need for:

- Cyber-Hygiene Education - Interactive online training for both non-tech professionals and tech staff to hone their cybersecurity skills. This can include the basics such as rotating your password once in a while, not clicking on suspicious-looking emails, and other simple practices that can increase security. Armed with this knowledge, people will be better prepared to manage anything hackers throw against them.

- Preventing Breaches and Intrusions - This will include tips companies implement to better safeguard against hacks. Defending against SQL injections, authentication bypasses, IDORs, local file inclusions, and so many other threats is critical. In fact, there are countless threats out there that are unknown to most

- Cyber Security Incident Response - By the time you realize that you’ve been hacked, it's already too late. Furthermore, you need to know which actions to take if in the event of a hack or suspicious activity surrounding your accounts. Thus, people must know about all cyber breaches as soon as possible to safeguard their assets and protect their personal information.

At Hacken, we believe that for a personal cybersecurity application to get mass adopted, it has to solve cybersecurity issues in the most simple and convenient manner:

- Simple starting pack with a quick practical knowledge win
- Focus on UI/UX. Simplicity and embedded gamification throughout the user journey
- Multifunctionality. All needed cybersecurity tools in one “swiss army application”
- Proof of virality. The app should have been easy to peach to a friend with and without financial incentives

2.3 HackenAI Solution

Right now, everybody is looking for a solution that will provide them with some peace of mind without having any expert cybersecurity knowledge. Fortunately, there is a product that does exactly this: HackenAI.

Archived copy · cryp2nova.com

HackenAI is a revolutionary, 360° cybersecurity companion product that incentivizes users to learn good cybersecurity habits. Powered by the native HAI token, HackenAI takes ownership of user cybersecurity by consistently watching all potential threats and malpractices, and immediately prompts users with timely, detailed information. It even suggests steps to take in mitigating the risks of exploitation.

For early adopters and users who were not involved in any cybersecurity activities, they start with a dashboard of practical educational modules they'll need to complete in order to achieve a 99.9% level of protection against known cybersecurity threats. HackenAI will drive users through notifications and clear guidance and will keep a positive track for everyday practical knowledge wins.

2.3.1 Cyber Boot Camp

CyberBootCamp is a user's personal guide in the world of cybersecurity. With our constantly updated educational material, the user will learn the basics of personal cybersecurity in a simple and gamified way. At the time of the first release, the HackenAI CyberBootCamp will consist of six modules. Each module consists of the theoretical lessons, the practice, and the final test.

After successfully passing the CyberBootCamp, users will be rewarded with HAI tokens in equivalent to a one month subscription fee for the HackenAI app. After completing the BootCamp, the user will receive additional tradeable HAI tokens and cybersecurity expert status.

The CyberBootCamp will consist of:

module 1 Accounts Management. In this module, users will learn how to create a strong password, what passwords they should avoid, and how to minimize risks of being hacked using weak passwords. Also, users will check their accounts for compromised data leakages and learn how to use 2FA-authentication in the safest way. After passing this module, the user will gain access to and learn how to efficiently set up the HackenAI password manager and will be allowed to subscribe to a dark web monitoring service.

module 2 Anti-phishing. Users will learn what websites to avoid in order not to be caught by phishers. Useful life hacks on how to recognise phishing sites will be presented in this Boot Camp. As a part of a social engineering test, users will receive actual phishing exploits to his or her linked emails without any warnings. This module is one of the most important for users because phishing attacks are becoming more common and in most cases it's quite difficult to distinguish phishing services.

module 3 Privacy. During the third module, users will gain crucial knowledge about important privacy settings of his or her social media accounts and hardware devices. Users will learn how to determine whether an application that collects data might be compromised, what permission(s) they should deny while installing new applications, and how to set up the privacy settings to keep the personal data secured.

Archived copy · cryp2nova.com

module 4 Data Protection Rules. In this module, users will learn basic principles about how to protect his or her personal data on the internet. It includes best practices for how to store data securely, basic encryption methods, and critical backups.

module 5 Digital Assets Security. This module was created in collaboration with white hat hackers and will be extremely useful for digital asset users. We have consolidated all trusted knowledge about secure storing of private keys, secure trading practices, cryptocurrency exchanges API policies, operating software crypto wallets, hardware wallet usage, and much more.

module 6 Essentials. In the last module, users will learn how to use global DNS, when it's necessary to use a VPN, what antivirus software to trust, and essential information about available cybersecurity tools.

2.3.2 Password Manager

Massive phishing scams, data breaches, and identity theft are often in the headlines, and people are understandably worried. It's not just government employees who are vulnerable, but all of us. For example, *64% of Americans* have personally experienced a major data breach. Yet this is a global problem. In 2018, there were four billion internet users, and cybercrime cost the world $3 trillion. By 2021, there will be six billion Internet users, and the cost of cybercrime is expected to rise to $6 trillion per year. One of the biggest problems is password storage. A significant amount of cybercrimes were committed via password theft. Most of the users don't pay much attention to the security of their passwords because of:

- Lack of understanding of the risks and consequences of being hacked
- Pre-existing safety nets in legacy systems
- Little Knowledge of best cybersecurity practices

As a result, people are starting to care about their cybersecurity too late, in most cases only after being hacked. HackenAI Password Manager can help. The main purpose of the HackenAI Password Manager is the secure storage of a user's passwords and other critical personal data. By passing the Boot Camp, users learns how to set up the password manager correctly and use it on a daily basis.

All users' data is kept only on their hardware devices. In one click, users can backup passwords using cutting-edge encryption and store it in HackenAI secure storage and/or on the VeChainThor blockchain. If the user needs to sync it with another device or restore it on a lost smartphone, the user can do it by decrypting the last sync, which is stored secure storage or VeChainThor blockchain by entering seed phrase (12 words) and passing additional authentication layers. To protect against sim swap attacks, the Password Manager will not make use of phone numbers for authentication. For quick access to data in an application or on device, users use local passwords (may be different on each device).

Archived copy · cryp2nova.com

The basic functionality of the Password Manager will include:

- Primary functions
  - Import Items (passwords) from external password storages
  - Export Items to CSV
  - Manually add items
  - Copy username/password/OTP/url
  - Open (launch website in new tab of the browser)
  - Generating password (when form is filing and in the separate menu)
  - Automatic password capturing (when form sent)
  - Password strength alerts (One password in multiply Items, worst passwords, short passwords, bad passwords fired in the internet, password monitoring)
  - Forms autofilling
- Sharing Items with other people
- Reporting about Items and storage health
- Select identity for session
- Encrypted storage for seed phrase printscreens
- Private keys and profiles storage
- Secure notes storage
- Emergency contact

2.3.3 Two-factor authentication (OTP generation)

With HackenAI two-factor authentication, users can add their online accounts to the application to generate one-time passwords. Similar to apps such as Google Authenticator, HackenAI has the ability to backup data in secure storage. This is a must-have feature for users who care about their personal cybersecurity.

2.3.4 Compromised accounts monitoring

Using HackenAI, continuous monitoring of accounts for compromises is possible. Usually it is enough to search by email using the API of third-party services or third-party databases. On the other hand, a separate service is responsible for this, which checks the passwords through the databases of leaked data and gives the results to client application. Data is checked by the date of compromise and the date of the last password change. If the date of the last password change is unknown, then we consider the data compromised and notify the user about it.

2.3.5 Secure storage

Data secure storage is used to save user data, such as notes, screenshots, private keys, credit card data, and so on. This data is stored as securely as passwords, and the user can share it without transmitting it in clear text format through insecure channels.

Archived copy · cryp2nova.com

2.3.6 VPN service

A premium VPN service will be available for HackenAI paid subscribers. VPN secures the private network, using encryption and other security mechanisms to ensure that only authorized users can access it and that the data cannot be intercepted. This type of network is designed to provide a secure, encrypted tunnel to transmit the data between the remote user and the company network. It can also be leveraged for personal needs for securing network data. Hacken VPN protects users from unwanted advertisements and snoopers that track you across the web.

2.3.7 NonCustodial Crypto Wallet

A non-custodial multi-network crypto wallet, that at launch, will support the following currencies: Bitcoin, Ethereum, VeChainThor (VET), VIP-180 (VTHO, HAI), ERC-20, BEP-2. More blockchains to be added later. The main purpose for the crypto wallet is a secure storage of the currencies and making use of the staking options for HAI.

2.3.8 Digital Asset Viewer/Tracker

Most crypto users employ different exchanges for trading crypto. This is done because there is no single exchange that trades all the tokens. There are several solutions for manual input of the assets and a few that are building a one-stop trading terminal.

In our digital assets tracker, we don't make any bidding or other actions through exchanges API. We strongly recommend using read-only API credentials for adding to our application

Few of the most famouscyber attacks were committed using the "stupid trade" technique through API. The Hacken team sees API's as a backdoor window, and in most cases, the weakest point of exchanges security.

Using the Digital Asset Tracker, you can:

- Connect all exchanges accounts and import all assets data every time while login
- Connect wallets and add them to the consolidate crypto statement
- Track performance of their crypto assets
- Monitor performance of their trading bots
- View the average buy prices
- See the trading profitability chart
- Export the consolidated statement
- Add assets to the Watchlist
- Configure custom triggers for alerts

2.3.9 Cybersec Marketplace

With HackenAI, users will benefit from having access to third-party cybersecurity services and products on a marketplace. The marketplace will include the ability to purchase anti-viruses, cloud protection services, performance boosters, etc. Purchases on the marketplace will be done in HAI.

Archived copy · cryp2nova.com

2.3.10 CER

The Crypto exchanges ranking module is going to be integrated in HackenAI. Users will be able to check up to date information about all crypto exchanges including their security and solvency.

2.3.11 News and industry alerts

The Hacken analytical center continuously releases cybersecurity research, crypto-fraud investigations, and white hat hacking insights. We inform users of any new data leakages and explain in simple words what happened in a timely manner. In addition, we ensure that HackenAI users are aware of unethical and fraudulent crypto companies.

2.3.12 Others

Additional features that will be developed in later HackenAI releases are:

1. **PROXY SERVICE** (for Browser extensions)
2. **DISABLING TRACKERS** (for Browser extensions)
3. **SECURE BROWSER** (for mobile apps)

2.4 Tech Implementation

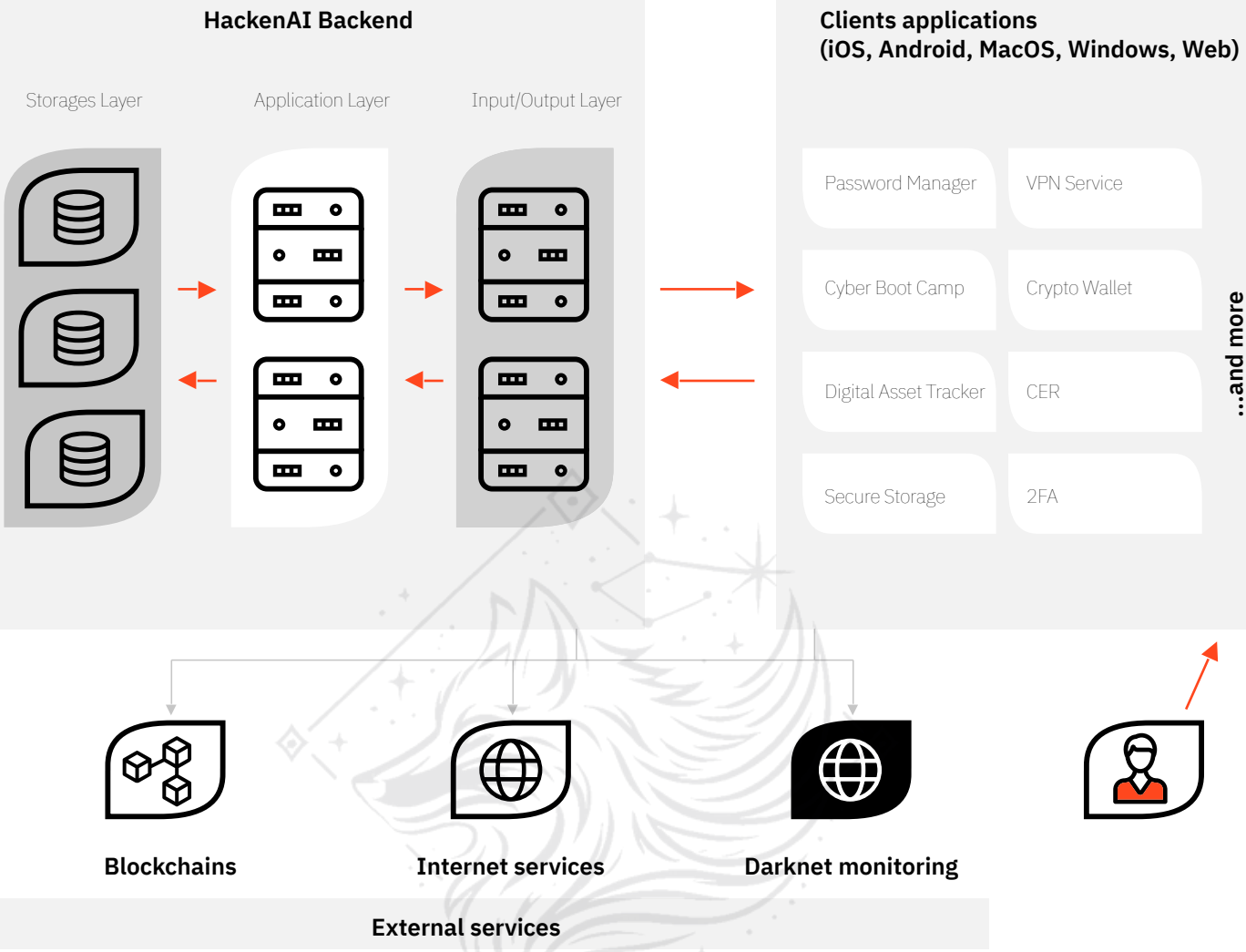
Hacken is a scope of client-server applications. Clients applications are available on:

- Mobile applications for iOS and Android
- Desktop applications for Windows and macOS
- Web version
- Extensions for most popular web-browsers.

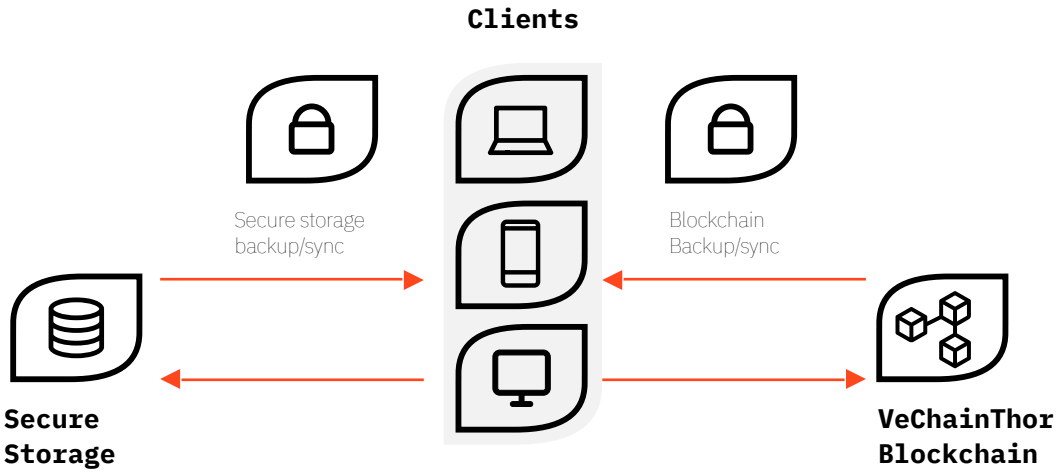
All operations with user's data are performed on client-side. The backend doesn't have any access to decrypted user's data or keys to decrypt data.

On the backend application level, HackenAI has a microservice architecture. The microservice architecture allows for easy scaling and the ability to quickly add functionality.

Archived copy · cryp2nova.com



By default, the user's data is stored in secure data storage, but users can enable data storing on the VechainThor blockchain. In blockchain, data is publicly available but not personalized and encrypted. The advantage of saving data on the blockchain is that it is immutable and is always available with internet access.



HackenAI's syncing feature allows automatic sharing of data and settings between all user devices.

Archived copy · cryp2nova.com

2.5 Security

The most important part of technical implementation is data security. HackenAI uses the latest and best data protection practices. All critical data is well protected.

Protecting user data
All data is protected with at least three security keys:

- User Seed phrase
  · Generated by application
  · Never stored on HackenAI servers
  · Used Only to generate private keys for deciphering sync data and crypto-assets access
  · Never transfers over the internet

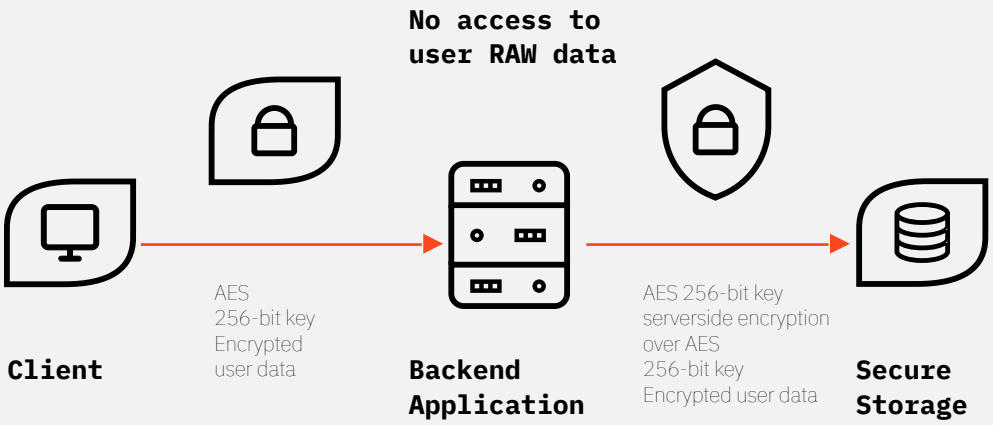
- Local password
  · Set up by the user
  · Used for access to data on authorized devices
  · Never stored on HackenAI servers.
  · Never transfers over the internet

- User device key
  · Auto-generated for each device
  · Used for authentication

Local access to data
Access to local data requires a local password, which is only known by the user. Local password can be different for various devices with the same account. It is used to generate the AES 256-bit key for ciphering and deciphering keys (global) to decrypt user data. 256-bit key generation is done with the following inputs: local password, generated 32-byte salt (cryptography), and randomly chosen 16-byte initialization vector.

Server data protection
On the server-side, HackenAI cyphers all user data when storing it. This encryption is done on the user device, and we don't have any keys for deciphering data. Only the user with private keys can decrypt all data.

Archived copy · cryp2nova.com



Communication security
Communication between clients and servers are secured with SSL/TLS. All data transmitted by the internet is already encrypted on the user's device.

Communication between browser or browser extension and HackenAI application is secured by AES256.

For authentication, HackenAI uses zero-knowledge solution.

Data sharing
Users can share their data with other users. HackenAI even in the data sharing process doesn't have access to raw data.

For data sharing purposes, HackenAI uses asymmetric encryption. When user account registered application creates a unique pair of public and private keys. The private key stored in the user's personal data storage. The public key sends to HackenAI servers.

When users want to share data:

- user1 asks user2's public key
- user1 generates a unique key for sharing data (sharing object key)
- user1 encrypts sharing object key by user2's public key
- user1 sends encrypted sharing object key to HackenAI servers
- user1 encrypts data (password, note, or more) with sharing object key
- user1 sends encrypted data to HackenAI servers
- user2 receives notification about data sharing from user2
- user2 manually accepts data sharing in application
- user2 receives encrypted object key and encrypted data
- user2 decrypts object key by own private key and then decrypts by object key sharing data

Archived copy · cryp2nova.com

Account recovery
For account recovery or adding a new device, the user simply needs to enter their recovery seed phrase, generated on registration. When the seed phrase is inputted, it transforms into the primary 256-bit key. This key is used to derive keys for deciphering data is downloaded from HackenAI storage.

Account recovery by guardians
HackenAI offers a recovery mechanism by guardians (people you trust). Guardians must be registered in HackenAI. If a user wants to share their private key with his or her trustees, he can specify the guardian's user emails. All potential guardians must approve the user's request. If a potential guardian is not registered in HackenAI yet, they can register then approve the request. The user chooses the number of guardians and minimum required number of guardian responses with key parts. After all guardians approve the requests, the user's client sends parts of their private key to the trustees' client.

If the user loses their seed phrase and local password (or loses their device), they can make a request to recoverer the keys through their guardians. When a minimum required number of guardians responds to the request, the user gets access to his account.

Bug bounty
The private bug bounty program with top white hat hackers will run for all unpublished HackenAI releases.

After each application update release, we will announce public bug bounties with extensively higher than market remunerations.

We will open source most critical parts of our source code to ensure the highest security standards.

2.6 Technical Roadmap

CRYP2NOVA

Q4 2019

- HackenAI development began

Q1 2020 (HACKENAI MVP LAUNCH)

Client platforms:
- iOS and Android applications

Functional:
- Passwords manager
- Cyber BootCamp
- NonCustodial Crypto Wallet (HAI)
- Guardians access recovery
- Referral system
- Compromised accounts monitoring

Archived copy · cryp2nova.com

Q2 2020

Client platforms:
- Desktop applications: MacOS and Windows
- Web browser extensions

Functional:
- Secure storage (Notes, Keys, and more)
- Digital assets tracker with exchange integrations and monitoring of most popular blockchains
- Import/export data from password storages and managers
- Adding more cryptocurrencies support to wallet
- Two-factor authentication (OTP generation)

Q3 2020

Client platforms:
- HackenAI Web version

Functional:
- Items sharing
- Emergency contact
- External service for top-up balance
- DEX integration
- CER crypto exchanges monitoring service
- Cybersec Marketplace

Q4 2020

Functional:
- Identity manager for password manager
- Passwords changer for most popular web services
- Dark web monitoring
- Blockchain data backup

AFTER IMPLEMENTATION

Functional:
- VPN service
- Proxy and identity hide for web browser extensions
- Blockchain data backup

2.7 Competitors Analysis

Prior to HackenAI, there was NO crypto-specific cybersecurity protection and prevention software on the market for individual use. The following companies offer a fraction of our app's functionality.

Archived copy · cryp2nova.com

Our main competitors are:

LASTPASS – a freemium password manager that stores encrypted passwords online. A user's content in LastPass, including passwords and secure notes, is protected by one master password. The content is synchronized to any device in which LastPass software or app extensions are used. Information is encrypted with AES-256 encryption with PBKDF2 SHA-256, salted hashes, and the ability to increase password iterations value. Encryption and decryption take place at the device level.

The most known incident with LastPass occurred in 2015. It was a breach of user data, include user emails, password hashes, server per user salts and authentication hashes. Other incidents (2016, March 20, 2017, March 25, 2017 and 2019) concerned browser extensions vulnerabilities on the client-side. It could lead to a leak of user credentials.

1PASSWORD – a password manager developed by AgileBits Inc. It provides a place for users to store various passwords, software licenses, and other sensitive information in a virtual vault that is locked with a PBKDF2-guarded master password. By default, this encrypted vault is stored on the company's servers for a monthly fee.

DASHLANE – a cross-platform premium password manager and digital wallet application available on macOS, Windows, iOS, and Android. Dashlane uses a Freemium pricing model, which includes both a free tier and a premium subscription. Over time, more features were introduced to the product such as: multi-factor authentication, automatic form filling, password generating, digital wallet, security breach alert, and VPN.

KEEPASS – a free and open-source password manager. KeePass supports a number of plugins. It has a password generator and synchronization functionality, supports two-factor authentication, and has a Secure Desktop mode. It can use a two-channel auto-type obfuscation feature to offer additional protection against keyloggers. KeePass can import from over 30 other most commonly used password managers.

Name	Founded	Country	Users (min)	Delievery form	Prise	Decryption key	Backup Sync	Security health	Password manager	Crypto storage	Digital assets tracker	Research database	Cryptocurrency sites scoring and alerts
hoi	2017		N/A	Local installation	Xxx months free	Seed phrase	Cloud + Block-chain	+	+	+	+	+	+
LastPass	2008		13,5	Cloud-based	Free or $36.00 (yearly)	Master password	Cloud	+	+	-	-	+	-
1Password	2005		15	Local installation	$3-5 (monthly)	Master password	Cloud	+	+	-	-	+	-
dashlane	2009		10	Local installation	Free or $4,99/$9,99 (monthly)	Master password	Cloud	+	+	-	-	+	-
KeePass	2003		20	Local installation	Free/Open Source	Master password	Cloud	+	+	-	-	-	-
TREZOR	2018		1	Local installation+ Hardware	Free for Trezor owners	Hardware token	Cloud	-	+	+	-	-	-
Blockfolio	2014		5	Local installation	free	N/A	Cloud	-	-	-	+	+	-
DELTA	2017		21	Local installation	free or $7 (monthly)	N/A	Cloud	-	-	-	+	+	-

Archived copy · cryp2nova.com

2.8 Go-to-market strategy

Priority markets

The market potential for personal cybersecurity is vastly untapped. The first priority market for HackenAI is the VeChain community with 60,000 current VET holders. The second priority market will be crypto users who do not use password managers. They are low-hanging fruit for black hat hackers, that's why we intend to reach them before the bad actors do. The next priority market will be primarily, the English-speaking userbase who are aware of the burgeoning crypto space but are afraid to enter due to cybersecurity risks.

Total Addresseble Market, 2018-2019 Statistics

	English Speaking (aproximate)	Non-English Speaking (aproximate)	Total (aproximate)
Global Intenet Users (GUI)	1,109,000,000	3,281,000,000	4,390,000,000
Global Password Manager Users	32,000,000	28,000,000	60,000,000
% Password Managers Penetration to GUI	2.89%	0.85%	1.37%
Global Cryptocurrency Users	27,000,000	15,000,000	42,000,000
% Cryptocurrencies Penetration to GUI	2.43%	0.46%	0.96%

HackenAI Penetration Goals to Target Audience

Target Audience / Assumption	0.5%	2%	5%	35%
VET holders	300	1,200	3,000	21,000
To Password Manager Users	300,000	1,200,000	3,000,000	N/A
To Cryptocurrency Users	210,000	840,000	2,100,000	N/A

The password manager market has more than *60 million users*, offering a wide range of opportunities for user acquisition campaigns in the existing market. We believe that the combination of both existing password manager's market and emerging the VeChain and crypto market will be a driving force of HackenAI's go-to-market strategy.

Daily usage

HackenAI has the probability to be used daily for cybersecurity and digital assets tracking purposes, password management, dark web monitoring, and other features. Personal cybersecurity will become a new trend of the cyber era, and we believe HackenAI will take the lead in this market.

Archived copy · cryp2nova.com

3. What is HAI

HAI is a VIP180 token, minted on the VeChainThor Blockchain.

HAI will be used as a utility token to power most activities performed within the HackenAI Platform. Holders of HAI will receive benefits from both HackenAI Platform, as well as our white hat community and B2B business activity.

3.1 Why VeChain?

For the past year, our team has evaluated migration options to all major blockchain platforms. We have reviewed the VeChainThor blockchain, and without a doubt, it is the best available option for us in the blockchain market for the following reasons:

- **SECURITY.** Hacken was a security auditor of the VeChainThor blockchain protocol. VeChainThor's Proof of Authority consensus is one of the most secure methods to protect its users from currently known hacker attacks.

- **TECHNOLOGY.** Unlike any other blockchain, VeChainThor's **Multi-Party Payment (MPP) and Multi-Task Transaction (MTT)** bring greater accessibility and will be important enablers of mass adoption. MPP is incredibly important for a smooth user experience, key for mass user adoption of blockchain technology. MPP allows for HackenAI to sponsor ausers' transactions, making it more user-friendly for an audience that may not be blockchain-savvy enough to calculate the amount of gas they need in their wallet.

- **ENTERPRISE ADOPTION.** DNV GL, PWC, Deloitte, and many other corporations are actively working together with VeChain in pursuit of blockchain mass adoption. Hacken shares a similar enterprise client strategy. We understand that it takes a lot of professionalism and trustworthiness for enterprises of that caliber to lend their name.

- **VALUES AND ETHICAL PRINCIPLES.** It's no secret that most of the Hacken and VeChain core team have professional experience with Deloitte and PwC. We share the same values and ethical principles, allowing us to collaborate effectively.

- **VECHAIN ECOSYSTEM.** VeChain has an active community of projects built on the VeChainThor blockchain, like OceanEx, 8Hours, Plair, Safe Haven, and more.

3.2 HAI transaction model

As HAI is a VIP180 token on VeChainThor, transaction fees on the VeChainThor blockchain must be paid using VTHO in accordance to the VeChainThor transactional model. On the user-level, VTHO is generated by holding VET or can be purchased at open market. However, HackenAI will implement MPP to mitigate the need for users to hold VTHO to access our services by sponsoring their transaction fees. This will increase the rate of adoption.

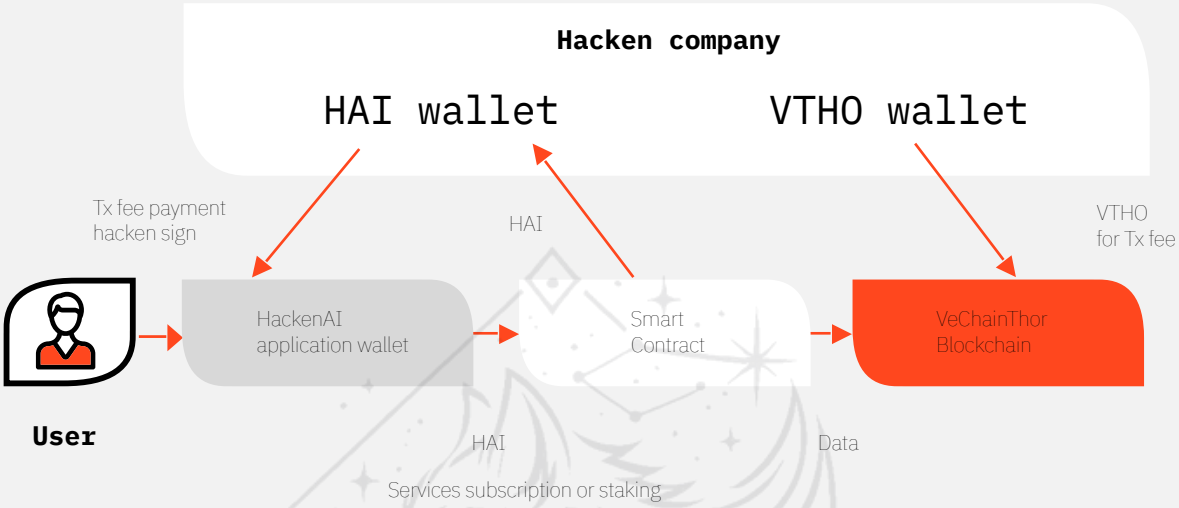
Archived copy · cryp2nova.com

Payments for services

For user convenience, we have designed HackenAI to operate on a single token model (HAI token). We will implement transaction fee payment delegating for HackenAI services.

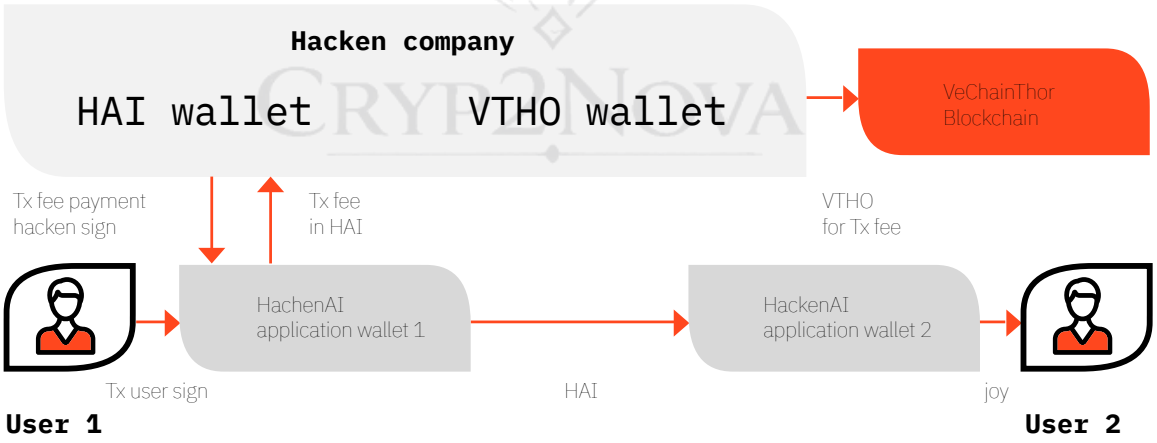
When the user wants to pay for services, or make staking, he or she makes payment in HAI, and Hacken pays transaction fee for this payment.

For these purposes, Hacken makes Smart Contract, and then use VIP-191 protocol or MPP with MTT.



P2P payments

For sending HAI from one user to another, the company needs to use VIP-191 protocol. When the user sends a transaction, he or she pays the transaction fee in HAI to Hacken, and Hacken pays it in VTHO to the blockchain. Users should not think about VTHO to pay for GAS. The user works with only one token.



VechainThor blockchain valuable transactions

According to this single token model concept, Hacken is responsible for paying for all VTHO any HAI transactions within Vechain Blockchain.

Hacken accumulates VTHO from:

- VET staking
- HAI/VTHO trading pair at an exchange

Archived copy · cryp2nova.com

According to our cooperation agreement, the Vechain Foundation contributes to Hacken ecosystem development **20%** from monthly total VTHO received from HAI transactions sent from HackenAI wallet. This contribution is proportionally distributed between HAI fourth level staking partners.

The number of HAI valuable transactions within VechainThor Blockchain will grow in line with the HackenAI user base.

3.3 Tokenomics

HackenAI's mission is to improve individual's cybersecurity knowledge through education, a variety of tools gathered in one app, and incentification. HackenAI is free to install and to use the first six months after the successful completion of all CyberBootCamp modules.

Revenue model
For the purpose of sustainable HackenAI development and HAI demand growth, we will require monthly subscription payments for all HackenAI modules activation. Subscription fees will be introduced at HackenAI Beta release. At Beta release, subscription fees will be paid in HAI only and is variable depending on HAI market price. Users are charged with an advanced monthly payment every first day of the month. VTHO costs for transaction are included in the monthly subscription fee.

Later HackenAI releases will introduce an embedded decentralized exchange module, which will allow users to pay fiat and other cryptocurrencies for the HackenAI subscription fee. Paid funds are used to automatically buy the required amount of HAI and send them to the Hacken corporate account to complete the subscription payment cycle.

ways to get HAI (supply)

- Educational mining (bonus for passing CyberBootCamp and other future cybersecurity tasks)
- Earn at Hackenproof bug bounty platform
- Swap HKN tokens
- Referral bonus scheme
- Buy at an exchange

ways to use HAI (demand)

- HackenAI subscription fee
- Hacken B2B services payment
- 3rd party products purchase from HackenAI cybersecurity marketplace
- Staking program
- Corporate governance

Educational mining and gamification
Today there is no standalone solution that can protect you from all new security threats that appear every day. Cybersecurity is a process, and HackenAI ensures that users are aware of all new cybersecurity issues through permanent education. HackenAI will communicate this through notifications and tasks to users to perform cybersecurity improvements.

Archived copy · cryp2nova.com

HackenAI will reward users for the following activity within the platform:

- Educational cybersecurity tasks completion
- Crypto exchanges cybersecurity reviews
- Cybersecurity research content
- Daily platform usage
- Creative marketing content

HAI Staker Program

The HackenAI staking program has two main goals:

- Bring actual value to partners in the form of free cybersecurity services
- Build partnership network for HackenAI promotion

There are four staking hierarchy levels based on the amount of benefits included:

1. Researcher staking
2. Expert staking
3. Architect staking
4. Ethical hacker stacking

REQUIREMENTS:	1st level Researcher	2nd level Expert	3rd level Architect	4th level Ethical hacker
CyberBootCamp completion	no	yes	yes	yes
KYC	N/A	N/A	yes	yes
HAI staking, USD equivalent	100	400	2,500	10,000
Staking length	6 months	6 months	6 months	6 months
INCENTIVES:				
HackenAI subscription	free during staking period	Lifetime free subscription	Lifetime free subscription for 5 users	Lifetime free subscription for 50 users
Referral bonus	tradable equivalent in HAI tokens of 1 months subscription fee for one referred user	tradable equivalent in HAI tokens of 1 months subscription fee for one referred user	tradable equivalent in HAI tokens of 2 months subscription fee for one referred user & tradable equivalent in HAI tokens of 1 month subscription fee for second level referral	tradable equivalent in HAI tokens of 3 months subscription fee for one referred user & tradable equivalent in HAI tokens of 2 month subscription fee for second level referral
Hacken B2B partnership program	N/A	N/A	Hacken cybersecurity services and products exclusive partnership program	Hacken cybersecurity services and products exclusive partnership program
Governance Mechanisms	N/A	N/A	N/A	Token, product, and community roadmap planning voting
Yield	N/A	N/A	N/A	Share from monthly VTHO turnover in HAI ecosystem

CRYP2NOVA

Archived copy · cryp2nova.com

If HAI's price appreciates during the staking period, the user can re-apply to the same staking level at a new increased HAI price at the end of the staking period. Released differences can be immediately traded.

If HAI's price depreciates during the staking period, users can re-apply to the same staking level with no additional collateral needed.

HAI Staker program rules can be changed after reaching 100,000 subscribers milestone.

Tokenomics was designed in tight cooperation with *Economics Design*.

Referral bonus program

To accelerate the rate of adoption, we will introduce a referral bonus program for all of our users. Pitching HackenAI is easy, since it solves everyone's real-life problems.

Each user can earn HAI through referrals. HAI equivalent of a one month subscription is paid to regular HackenAI users for each referred graduate of the CyberBootCamp.

The higher the user staking level, the bigger the remuneration for the same referral job. Below is an illustration of six month referral earnings to different staking levels:

STAKING LEVEL	Direct referrals, users	2nd level referrals, users	Referral bonus for direct referral, equivalent in monthly subscriptions	Referral bonus for 2nd level referral, equivalent in monthly subscriptions	Total referral earning, USD equivalent in HAI
4th level Ethical hacker	50	1000	3	2	2150
3rd level Architect	50	1000	2	1	1100
2nd level Expert	50	1000	2	0	100
1st level Researcher	50	1000	1	0	50

Archived copy · cryp2nova.com

Corporate governance
Fourth level HAI Staker program membership allows users to participate in HackenAI tactical and strategic development. Ethical Hacker Stakers join a planning group, that would design a roadmap for the following decisions:

- HackenAI modules development
- Regional expansion
- Community building
- Cryptocurrency exchanges listing
- Partnerships

3.4 HAI as a key element for HackenAI user base growth

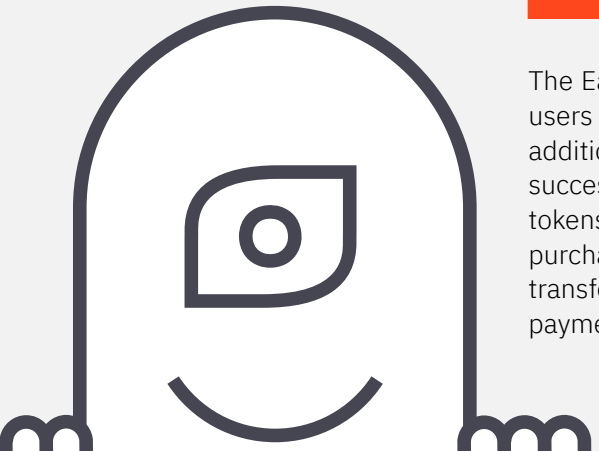
HackenAI is fully powered by HAI token that is an essential part of the application. When the App is installed, the user experience starts with an educational CyberBootCamp. Users receive their first HAI tokens as a reward for successful completion of BootCamp modules. If all tests are passed the user will get enough tokens to use all HackenAI functions six months for free. For most of HackenAI users, HAI token will be their first digital asset.

A key success factor of every application's initial launch is word of mouth. Every Hacken community member knows that demand for HAI will grow if they tell their friends about it and its benefits HackenAI. The core team has created an effective elevator pitch that our initial community can leverage in spreading the word:

"Hey, check your email in HackenAI's leaks database for compromised passwords!"

"Hey, check your microphone settings and find out what apps are listening to us now!"

"Hey, as a reward for becoming more secure, you could earn HAI tokens!"



The Early Adopter Advocacy and Referral Marketing Strategy will give users the ability to pitch the app to their friends and be rewarded with additional HAI. When the App is installed, and CyberBootCamp is successfully passed, both users will receive a reward in the form of HAI tokens that they will be able to use to cover subscription fees as well as purchasing any of HackenAI's products. The inner wallet will allow the transfer of HAI token between and the ability to use it as a form of payment.

Archived copy · cryp2nova.com

3.5 HKN Migration

Hacken Ecosystem ERC20 token HKN will migrate from the Ethereum Blockchain to the VeChainThor blockchain. During this process, the current HKN tokens will be converted to HAI tokens minted on the VeChainThor Blockchain as a VIP180 token.

After much deliberation and analysis with internal and external partners, the token swap ratio for our HKN holders is finalized as **1:15 (1 ERC20 HKN token = 15 VIP180 HAI tokens).**

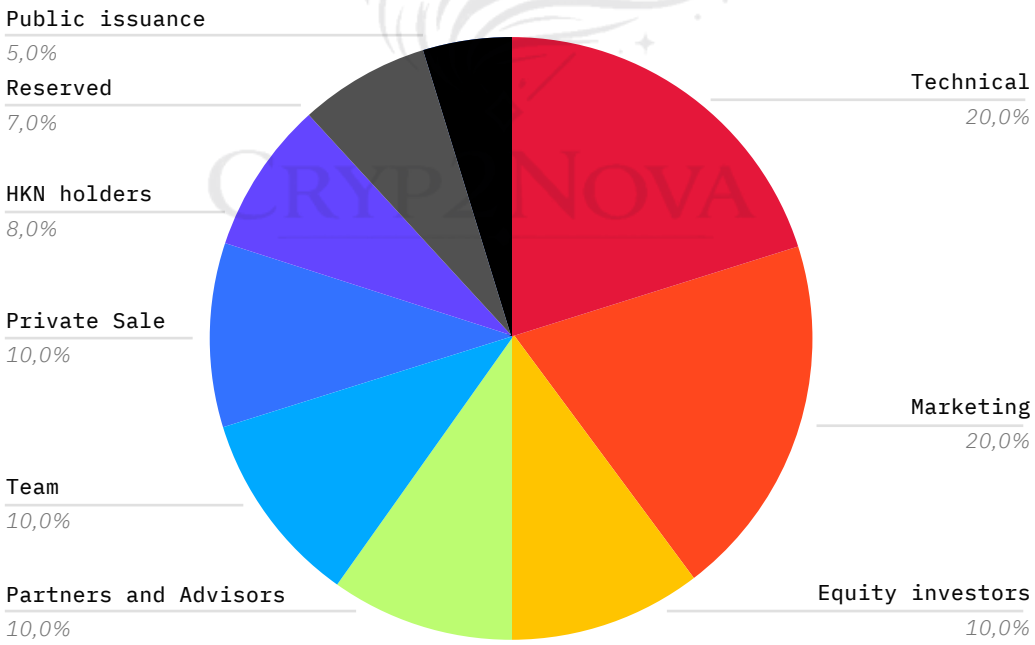
The swap ratio was determined based on a combination of several factors, taking into consideration the best interests of the community.

The HKN to HAI token swap is planned for early 2020, which will also depend on several moving factors such as the private token presale, limited sale to VeChain X-Nodes, ITO and exchange listings. The old ERC20 HKN token will still be tradeable on our listed exchanges until further notice.

3.6 HAI Distribution

HAI distribution and lock-up model primary's goals are:

- ensure the Hacken Ecosystem is sustainable for long-term development
- protect HAI holders from pump & dump
- HAI demand/supply effective management



Archived copy · cryp2nova.com

Teams, partners, advisors, and equity holders have token lock-ups that depend on the user base number. First lock-up milestone - 100,000 paid HackenAI subscribers.

The HAI marketing budget is going to be used mainly for user acquisition campaigns.

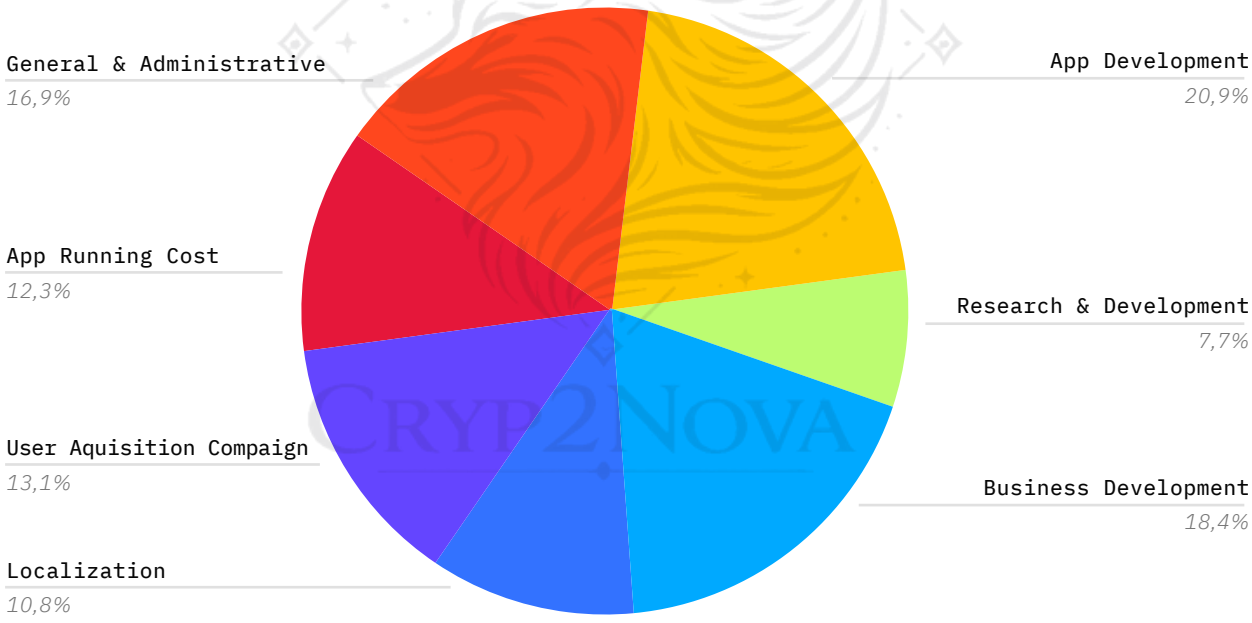
The HAI budget for technical development would be unlocked according to development needs, after major application releases and synced with HAI listings at top exchanges.

Hacken will release semi-annual reports that will disclose key numbers of token usage. Major decisions on marketing and development budgets will be voted on by major Hacken stakeholders, including fourth level stakers.

3.7 Use of Proceeds

At presale round, Hacken is raising 2 mln USD that will form a sufficient budget for 1.5 years of application development and marketing. The key milestone is to reach 100,000 paid subscribers, which is our break even, according to the financial plan.

The main financial plan capital expenditures are as follows:



Use of Private Token Sale Proceeds will go towards:

- 1,5 year of product development expenses
- 1,5 year for global business development expenses
- Global key markets localisation and operations
- User acquisition marketing campaigns
- Key Hires
- Partnership Staking program business development activities

Archived copy · cryp2nova.com

3.8 HAI Roadmap

Based on our tokenomics, we are not planning to issue all tokens at one time. First limited HAI offering is going to be announced through official Hacken social media channels and is planned in Q4 2019. Only 7.5% of tokens will be at circulation supply at first listing.

The HKN swap and first HAI/BTC trading pair will be introduced at the same time in Q1 2020.

Reserving a major part of tokens gives us a wide range of opportunities for the future app development without any limitations.

Archived copy · cryp2nova.com

4. Legal

Hacken OU is an Estonian Private Limited Company. According to various studies, Estonia is among the top seven countries regarding favorability of establishing a business and conducting ITOs and IEOs. In addition to a favorable regulatory framework, it is easier and cheaper to start and run a business in Estonia than in many other “ITO friendly” countries, such as Singapore, Switzerland, USA, Malta etc. Estonia also has a history of supporting start-ups and new technological business ideas, which can be used in favor of a new business.

The Initial Token Offering of HAI utility token is conducted according to consumer protection rules and the Advertising Act, for which the promotion of the product or service must be in line with its characteristics and the Law of Obligations Act that establishes the contractual conditions and obligations to which tokens that offer access to a product.

CRYP2NOVA

Archived copy · cryp2nova.com

5. Team

The Team behind HackenAI: Industry Veterans in Blockchain Cybersecurity

DMITRIY BUDORIN

CEO

Dmitriy Budorin is co-founder and CEO at Hacken, leading blockchain cybersecurity consulting company, and CER, crypto exchanges ranking and certification platform. Today Dmitriy is a worldwide expert in cryptocurrency exchanges security and transparency. Previously he was a top-level executive in Ukraine's military defense industry. As an ACCA, his other achievements include an eight-year career at Deloitte in financial and IT audit.

ANDRII MATIUKHIN

CTO

Andrii is a highly qualified cybersecurity expert with 14 years of success and experience in the industry. He is a certified expert in several areas and has more than 10 certificates of competence. His role at Hacken is to provide technological leadership in developing, integrating, and supporting the ecosystem.

EVGENIA BROSHEVAN

HackenProof Managing Lead

Evgenia is a co-founder of Hacken and CEO of HackenProof. In her role, she unites the efforts of bug hunters, internal security team, as well as sales and product teams to provide security excellence for responsible business.

PAVEL RADCHUK

Blockchain Security Lead

Pavel is the Blockchain Security Lead at Hacken. Pavel has managed 100+ consulting projects including smart contract audit and blockchain protocol security review. He is the main organizer of #blockchainhackers meetups - networking events for all people interested in blockchain security. Pavlo is true builder, who participated (and won) in several hackathons, developed several programming languages, and has strong application security background.

IVAN NAUMENKO

HackenAI Product Manager

Ivan is a product manager with deep knowledge in cybersecurity, adtech, and mobile app development. Ivan has more than 10 years of experience in product and project management.

NAZAR KHALAVKA

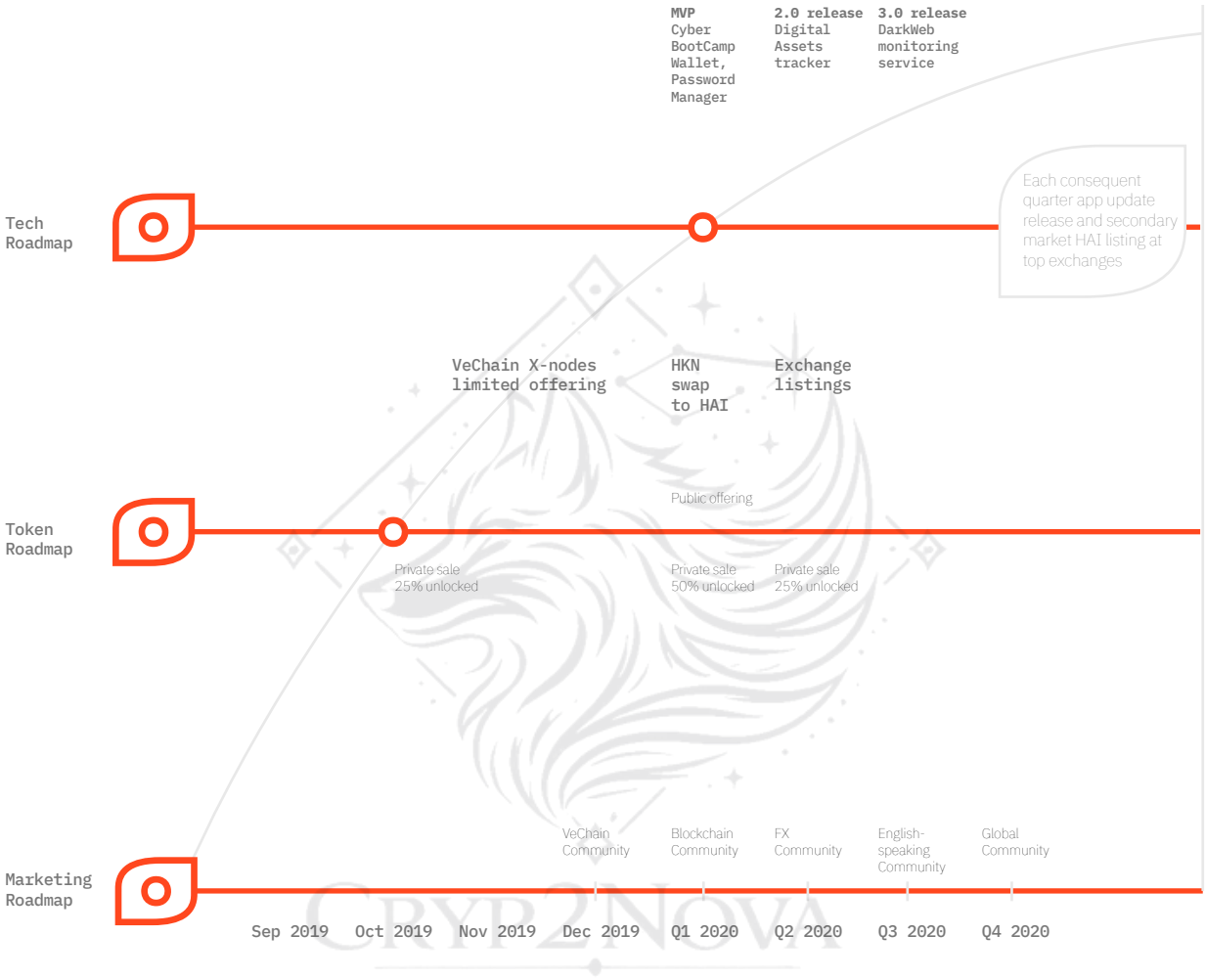
Project Manager

Nazar is a qualified project manager with more than five years of experience in finance, venture capital, and startup management. Nazar has extensive experience building startups from scratch and is an important part of the team.

Archived copy · cryp2nova.com

6. Combined Roadmap

Working on the HackenAI app, our team has synchronized technical, marketing and token development roadmaps.



The next big step will be the MVP release of the app that is expected to be in the first quarter of 2020. This event will be synchronized with the HKN swap and HAI/BTC trading pair introduction at major cryptocurrency exchanges.

Each consequent quarter, app update releases will be accompanied with the secondary market HAI listing at top cryptocurrency exchanges. Using this token distribution model, we can leverage the supply side of maintaining the constant demand for HAI token.

Fourth level Ethical Hacker Stakers would be involved in the decision making process for application, marketing, and token development.

Teams, partners, advisors, and equity shareholder tokens are locked until certain user base milestone levels are met.

Archived copy · cryp2nova.com

7. Summary

With HAI, we have created the ecosystem where both stakeholders and end users are benefiting from the HackenAI application user base growth. The HackenAI app and the HAI token are going to revolutionize mobile application market in the near future. We will see more and more unicorn apps that are shifting their growing value from equity investors to application users. There is no doubt that there is a need and niche for cybersecurity lifetime companion HackenAI. Let's usher in its success together.

LEGAL DISCLAIMER

Participating in an Initial Token Offering (ITO) is a high-risk activity. By participating in this ITO, the purchaser understands and accepts the risks that economic results are not guaranteed. Finally, the purchaser declares being aware of the legal uncertainty of this type of transaction and to have conducted their own legal due diligence according to applicable laws.

The purchaser also acknowledges the technological and economic uncertainty of the project presented in this White Paper. As such, Hacken (the "Company") is absolved of any legal action resulting from failure, nonperformance, or non-implementation of the project. The HackenAI utility token (HAI) gives users the ability to utilize HackenAI application services and token value is not guaranteed.

The Company's only obligation is to distribute the HAI token under the conditions defined in the white paper and no other rights are transferred upon the ITO.

During the ITO, the company may not be held liable for any of the following:

- Use of the service that is not compliant with the applicable terms;
- Any error, malfunction, malicious action, or violation of the White Paper's terms by the user, a third party, or service controlled by a third party;
- All direct or indirect damages that may occur during the operation: cryptocurrency losses, profits or financial losses, or other damages whatsoever in the type;
- The loss of control, for any reason, of a user's login credentials resulting in the fraudulent use of the tokens (i.e lost credentials, hacking, unwanted disclosure or technical failure, etc.).
- The temporary or permanent suspension of the service, whatever the cause, and especially due to a request from the public authorities, judicial authority, or any third party;
- Computer failure resulting in loss of data, including content in case of impact;
- The professional activity of users;
- Lack of compatibility between the service specificity and the customers' requirements;
- Generally, all damage whose cause does not depend on the company: Internet network outage, failure specific to the user's equipment, etc.

Archived copy · cryp2nova.com

Warning About the Token

According to Estonian and European regulation, the HAI token is a cryptographic utility token usable on the VeChain blockchain allowing access to the functionalities of the HackenAI application suite.

The HAI token is not a security or a financial instrument within the meaning of the Markets in Financial Instruments Directive (MiFID II) of the European Parliament (2014/65/ EU) or within the meaning of the article L211-1 and followings of the Estonian Monetary and Financial Code.

Participating in an ITO is a high-risk activity. This ITO in particular is only aimed at experienced professionals who are experienced with blockchain technology, cryptocurrency trading and trading with other market instruments. By participating in this ITO, the purchaser is aware and accepts the risks related to security, the potential lack of technical and economic results and the total or partial loss of its capital. Finally, the purchaser declares being aware of the legal uncertainty of this type of transaction and to have conducted his own legal guidance according to the applicable law to which he subscribes. Indeed, the token grants no financial (income, capital or dividend) or voting rights in the company. The token is a crypto-asset issued by HackenAI through the ITO and used by the members of the HackenAI application and community.

Sales restrictions

The participation in the ITO is strictly reserved for natural or legal persons acting within the scope of their professional activity. Especially, the professional purchaser claims to have a good knowledge of Blockchain technologies and cryptocurrency. Any natural person acting on a non-professional basis as a simple consumer within the meaning of EU Directive 2011/83/EU relating to consumer rights are excluded from the ITO. It is the responsibility of each purchaser to determine its non-professional status and, in doing so, to refrain from participating in any way in the ITO. Due to national legislation, participants from the following countries are not allowed to participate in the ITO: “US Person”, Canada, South Korea, Singapore and China. This prohibition applies to all types of people (moral, physical, agent, etc.) and to any indirect participation (via a proxy, a name loan, etc.). By participating in the ITO, the purchaser agrees to the legal disclaimer and, especially, that they respect the above provisions.

Warnings

ITOs are high-risk operations because of their experimental nature. Moreover, the market or markets on which these tokens are traded do not offer the same guarantees that are generally applicable to conventional financial markets.

Archived copy · cryp2nova.com

By participating in this operation, participants declare to understand and assume the following risks:

- **THE LACK OF REGULATION:** the purchaser agrees not to benefit from any guarantees associated with IPOs on regulated financial markets or other regulated financial investments;

- **CAPITAL LOSS:** the purchaser accepts the risk of a total or partial capital loss with cryptocurrency or with the token;
- **VOLATILITY OR MARKET RISK:** the token value, just like that of cryptocurrencies in general, can be extremely volatile and subject to significant, and largely unforeseeable fluctuations.

Archived copy · cryp2nova.com