



---

# HACKEN

# Ecosystem

August 2017

White paper. Version 1

# Table of Contents

## Summary

## Introduction

What is the Hacken Ecosystem?

How Does Hacken Make Use of Blockchain?

Why Yet Another Cybersecurity Marketplace?

## The Hacken Token

HKN Sale

Token Distribution

Milestones

Roadmap

The "Burning" Principle

Escrow and Audit

Disclaimers

## HackenProof

## Unreported Zero-Day Remuneration Platform

## Hacken Accelerator

## Cybersecurity Analytics Center

## HackIT Conference

Capture the Flag Competition

"Battle of Hackers"

Cyberdetective OSINT Challenge

HackIT Cup

## Who Are We?

## Why Does It Matter?

Addendum. Brief Analysis of Existing Vulnerability

Research Crowdsourcing Businesses

# Summary

This white paper explains key business components of the Hacken Ecosystem. **It also details the sale of Hacken tokens, which will start at 00:00 EET on October 12, 2017 and will end at 00:00 EET on November 11, 2017.** The paper also explains the subsequent roadmap for building the Hacken Ecosystem, should the token sale reach its target milestones.

The Hacken Ecosystem is a community driven business organization that will result from this token sale and will be incorporated in a number of jurisdictions Worldwide. It consists of the HackenProof bug bounty marketplace, Unreported Zero-Day Remuneration Platform, Hacken Cybersecurity Startups Incubator, Cybersecurity Analytics Center and HackIT Conference.

Hacken (HKN) is an ERC20 token, which is the only payment tool allowed in the Hacken Ecosystem. Buying Hackens today, will allow one to receive high quality cybersecurity services in the future, at an attractive price.

Please bear in mind, that all the financial data and legal documentation related to this token sale are available separately from this white paper upon request.

# Introduction

\$32M stolen from Parity and \$7.4M from Coindash in 2017, \$72M from Bitfinex in 2016, \$5.1M from Bitstamp in 2015, \$65M from Mt. Gox in 2014. These are gruesome fiat equivalents lost to hackers by various cryptocurrency infrastructure projects.

According to Tyler Moore of Tulsa's Tandy School of Computer Science, since bitcoin's inception in 2009 to March 2015, around 33% of all bitcoin exchanges during that period were hacked. Cryptocurrencies certainly are not the only businesses distressed by hackers. US President Donald Trump, himself a subject of a recent cybersecurity controversy, stated that cybertheft is the fastest growing crime in the United States by far.

This presidential concern is followed by big money. The United States will invest over \$19B in cybersecurity as a part of the 2017 Federal Budget. This figure is up from the \$14B budgeted in 2016, by the Obama Administration.

Unfortunately, there is not enough talent to make use of these enormous financial resources. According to CyberSeek there are more than 348,000 open cybersecurity positions in 2017, and this number will be up to 1.8M by 2022. Combined with an unaccounted for number of blackhat hackers, employed on the opposite side of the firewall, these statistics demand a swift response.

Until recently, Eastern Europe, and Ukraine in particular, had been a safe haven for various controversial online operations. Boasting enormous numbers of highly qualified math and computer science university graduates, the country's economy still has little to offer these people. Nevertheless, Ukrainian founders were behind such Silicon Valley unicorns as PayPal, WhatsApp and even the very WiFi technology you are likely using right now.

We think Ukraine can become the next European cybersecurity hub. Boosting expertise in this area is now a matter of the country's survival, given Petya.A, the forced power grid blackout of 2015, and other state-sponsored cyber attacks sure to be inflicted. However, the emergence of this vibrant cybersecurity industry should be facilitated by a resourceful and ethical expert community.

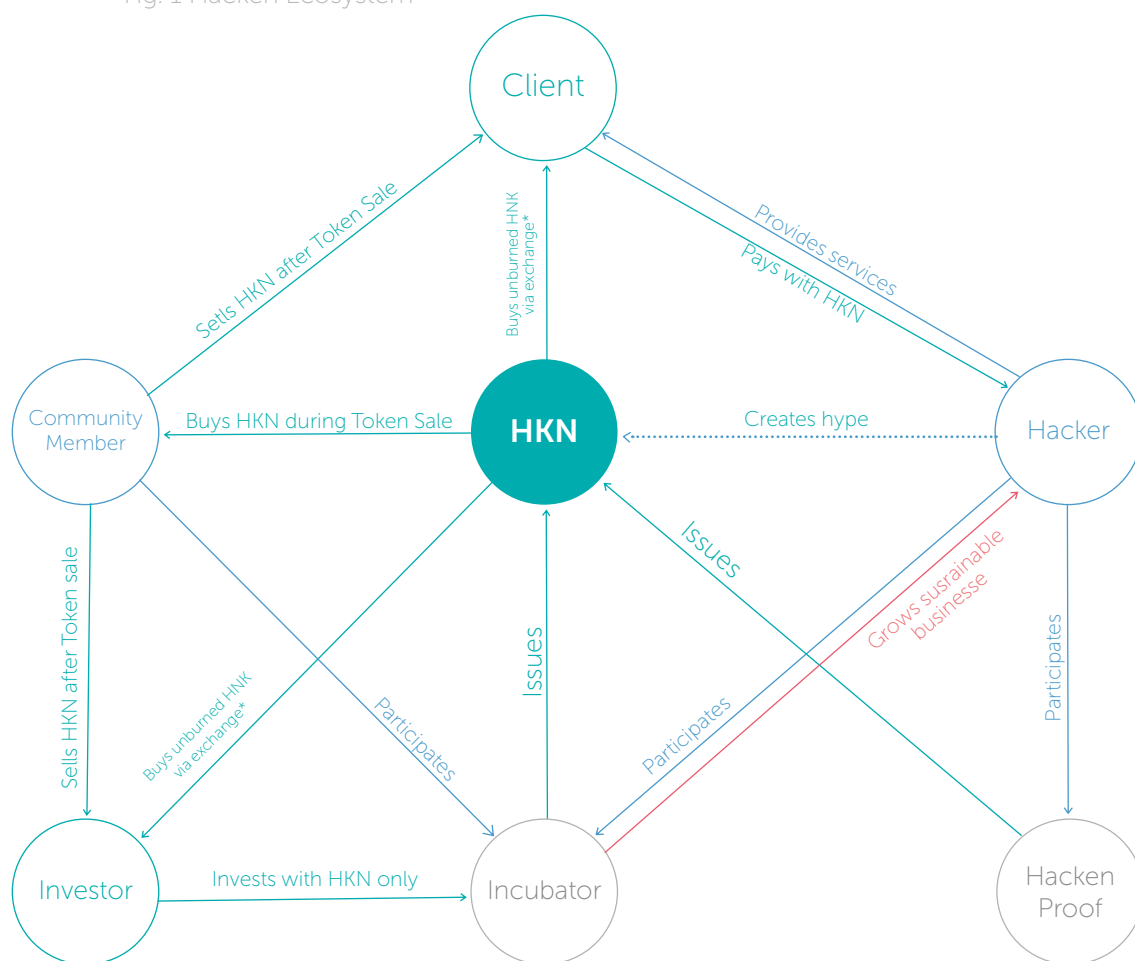
Our goal at Hacken is to lay down such a framework by creating a stable means of income and financial incentives for its members. In the long run, your participation in the Hacken Ecosystem will make sure the next generation of local computer whiz kids will be on your side of the firewall.

# What is the Hacken Ecosystem?

Our ecosystem consists of a token — the Hacken, and a constellation of businesses providing services, which can be received only by using Hacken as a payment instrument. The amount of Hackens is finite, limited to 20 million tokens that will be distributed during the pre-sale and the main token sale.

The businesses comprising the Hacken Ecosystem are the HackenProof bug bounty marketplace, Unreported Zero-Day Remuneration Platform, Hacken Cybersecurity Startups Incubator, Cybersecurity Analytics Center and HackIT Conference. Each element of this ecosystem is further described in a separate section of this paper.

Fig. 1 Hacken Ecosystem



\*See the section on [the «Burning» principle](#)

The big idea behind Hacken is that it turns each owner of Hackens into a community member. Because Hacken is a specialized software utility token, being primarily focused on cybersecurity professionals and projects, it will also bring these people together by providing incentives for doing business with one another and for investment in cybersecurity startups. These people will need to communicate and interact with each other in order to make use of their Hackens. The more vibrant the community is, the more value it delivers to each member.

While our ecosystem has solid business plan and product roadmap, it is not only about business. Our aim is also to grow and support HackIT — the largest international cybersecurity conference in Ukraine.

The cybersecurity business is very much about expertise, ethics and persistent training. By supporting HackIT, we want to ensure that we give back to the community which empowers our platform.

A great illustration of our core values is the story of Oleksii Matiiasevych — Ukrainian cybersecurity professional, EDCC architect at Ambisafe and our technology advisor in this token sale.

Only this last Summer, on July 19, 2017, Oleksii discovered a critical vulnerability in the code of the Parity Ethereum wallet. There was no time for discussion, as Oleksii showed evidence of an ongoing hacker attack that resulted in the compromise of hundreds of Ethereum wallets. He ended up transferring \$1,402,996.09 worth of Ethers from the compromised wallets to the ones he secured and controlled. Oleksii then contacted the White Hat Group which took charge of locating and returning all the coins to their rightful owners.

The ultimate goal of our ecosystem, is to create a generation of hackers to whom what Oleksii did is entirely normal, the only acceptable life scenario.

# How Does Hacken Make Use of Blockchain?

## Proof of Vulnerability Testing

When clients sign the bug bounty program agreement, our team creates a relevant blockchain block containing data about the product, the terms of service agreement and a timestamp. The next block of the chain, which is specific to this client, will contain information on vulnerabilities, discovered during our security research.

After clients resolve the vulnerabilities that were discovered during the bug bounty research, HackenProof experts conduct a post-research audit. We then discuss our findings with the clients and advise any additional measures which need to be taken. Should the findings of the audit be satisfactory to both parties, our team and the clients, we form the next block in the chain, which contains information about the issues that were resolved.

At the end, clients receive a HackenProof Vulnerabilities and Countermeasures Certificate, containing a report on all the vulnerabilities discovered and resolved with a timestamp for each event. Clients can then adjust their Blockchain sharing preferences and publish the certificate to the public, customers, investors or to whomever they designate.

## Cryptocurrency

Besides use of the blockchain in cybersecurity, this token sale also features an interesting financial innovation in the area of cryptocurrencies. That is our "burning" principle, which we explain in a [separate section](#) of this paper.



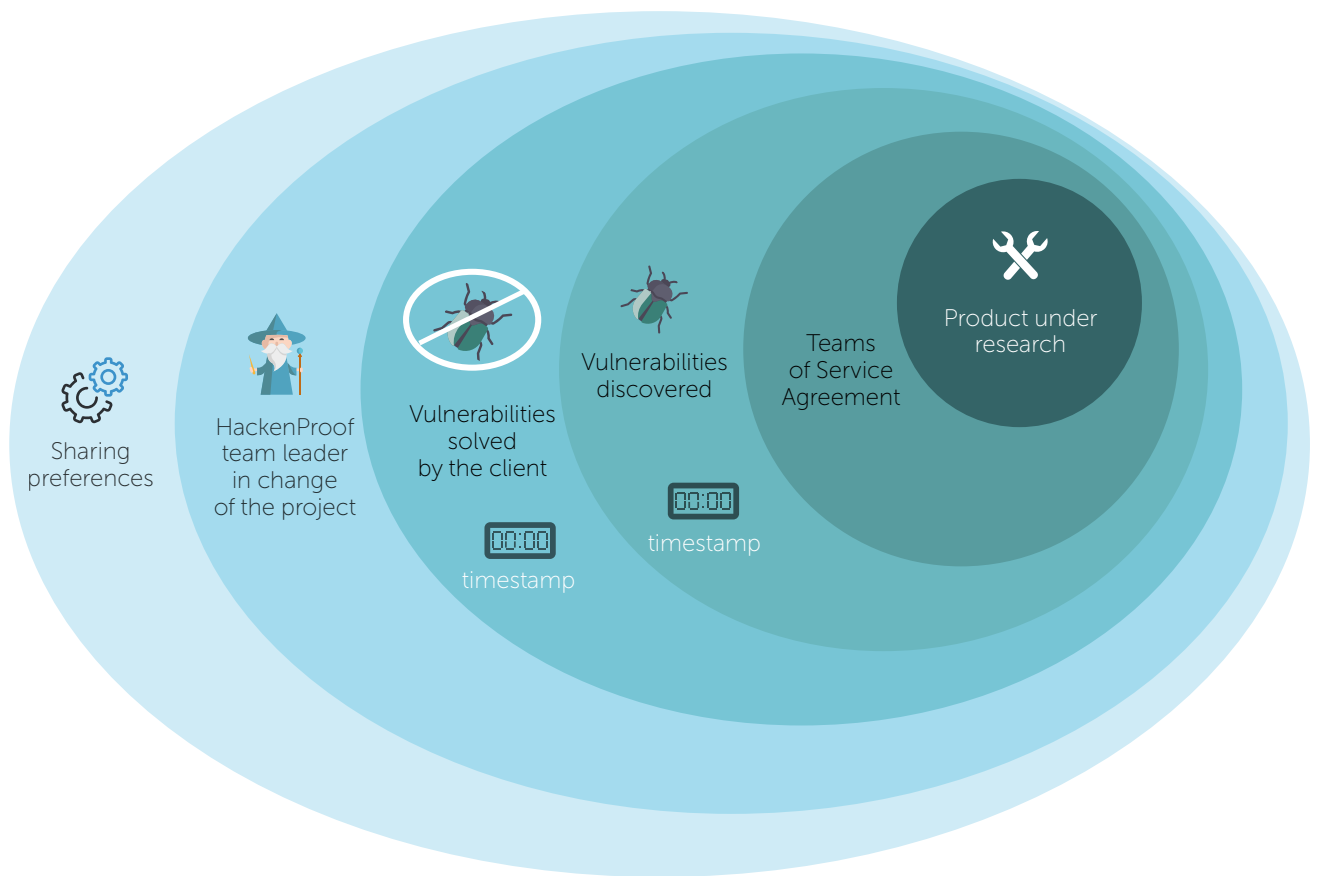


Fig. 2 HackenProof Vulnerabilities and Countermeasures Certificate

## Why Yet Another Cybersecurity Marketplace?

As you can see from our brief market analysis in the Addendum to this paper, or from your own personal observations, there are already at least four existing bug bounty and penetration testing services. Each of these has a growing customer base and investor support ranging from several to 74M US dollars. So the obvious question is: does the market really need yet another one?

### **We think it does. Here are the reasons why:**

- 1 / Currently the supply fails to meet the demand in the area of penetration testing and bug bounty programs.

Recently Mazda sponsored a CTF contest in Las Vegas, in which the winner received a truck. After Jeep, Tesla and Nissan LEAF hacks, the automotive industry is desperate for highly qualified bounty hunters and penetration testers. In our situation, that translates to: no, four existing services are painfully not enough. There is still a blue ocean of niche and general purpose cybersecurity communities.

- 2 / A cybersecurity ecosystem that is custom-tailored for blockchain. Being blockchain entrepreneurs ourselves, we understand this technology, its nuances, risks and its community better than most of the current cybersecurity establishment. Reading about blockchain in the Wall Street Journal, discussing it with colleagues over a cup of coffee and investing a few thousand dollars in Bitcoin just for fun, is one thing. Basing your entire business cash flow and core certification technology on blockchain is something entirely different.
- 3 / Did we forget the SME? Small and medium enterprises cannot afford the benefits of the enterprise penetration testing and bug bounty programs. This does not mean they don't need one. In the current cybersecurity environment, being a small business means very limited access to the perks of modern computer security infrastructure. We will provide SMEs with simple and convenient online tools to organize and run bug bounty and penetration testing campaigns.
- 4 / Same time zone, same cultural values. Hacken will be among the first movers in the European market of bug bounty marketplaces. Currently this market is dominated by Silicon Valley based providers. This is perfectly understandable, but San Francisco and Bay Area are not the only place in the World where good software and hardware projects are created. There is still enough demand for services based in other parts of the World and providing good value for the money.

---

# The Hacken Token

For millennia immeasurable, money had been an efficient, yet not the main driver, in uniting human organizations and driving their subsequent growth and development. Hacken is no exception. The distributed nature of blockchain enables us to promptly create a new token and imbue it with the best qualities of a modern currency. The smart contracts technology enables us to add an additional layer to Hacken and create economic incentives for the cybersecurity community to unite and cooperate in an ethical and legitimate manner.

Hacken is the only currency accepted inside our ecosystem. Any new orders via HackenProof, Unreported Zero-Day Remuneration Platform, Cybersecurity Analytics Center or new investments via Hacken Accelerator must be made in Hackens. This will reward community members who get paid in Hackens, by providing positive liquidity and low volatility.

Please note: Hackens are not intended to be a digital currency, commodity or any other kind of financial instrument, do not represent any share, stake or security or equivalent rights, including, but not limited to, any right to receive future revenue shares and intellectual property rights, and do not represent any ownership right.

# HKN Sale

Besides use of the blockchain in cybersecurity, this token sale also features an interesting financial innovation in the area of cryptocurrencies. That is our “burning” principle, which we explain in a separate section of this paper.

|                                                |                                                                         |     |
|------------------------------------------------|-------------------------------------------------------------------------|-----|
| <b>Total supply</b>                            | 20M Hackens<br>1.3M @presale (1M + 30% bonus)<br>18.7M @main token sale |     |
| <b>Symbol</b>                                  | HKN                                                                     |     |
| <b>Minimum sale-in</b>                         | 1 ETH                                                                   |     |
| <b>Max cap</b>                                 | 20M. No future emissions planned                                        |     |
| <b>Initial fiat equivalent</b>                 | 1 HKN = 1 USD                                                           |     |
| <b>Currencies accepted</b>                     | BTC, ETH, DASH, LTC, USD, EUR, TaaS                                     |     |
| <b>Length of Token Sale</b>                    | end of October, 2017 — end of November, 2017                            |     |
| <b>Escrow</b>                                  | on average 80% of the funds raised are kept in an escrow account        |     |
| <b>* Bonus Program for the main token sale</b> | 1 — 4 hours                                                             | 25% |
|                                                | 1 — 2 days                                                              | 20% |
|                                                | 3 — 7 days                                                              | 15% |
|                                                | 1 — 2 weeks                                                             | 10% |

Fig. 3 Token Sale Details

# Token Distribution

|                                         |            |
|-----------------------------------------|------------|
| <b>Open sale</b>                        | <b>80%</b> |
| <b>Team remuneration</b>                | <b>10%</b> |
| <b>Advisors</b>                         | <b>7%</b>  |
| <b>Token Sale Bounty,<br/>of which:</b> | <b>3%</b>  |
| Community manager                       | 1%         |
| Blog posts                              | 0.80%      |
| BitcoinTalk Signature                   | 0.30%      |
| BitcoinTalk Translation                 | 0.30%      |
| BitcoinTalk Thread                      | 0.20%      |
| Tweets                                  | 0.20%      |
| Facebook posts                          | 0.20%      |

Fig. 4 Token Distribution Chart

# Milestones

| Commitment                                         | Minimum Milestone | Limited Milestone | Target Milestone | Advanced Milestone | Maximum Milestone |
|----------------------------------------------------|-------------------|-------------------|------------------|--------------------|-------------------|
| Tokens sold                                        | 1.5M              | 4M                | 10M              | 18M                | 20M               |
| HackIT Conference                                  | 15%               | 10%               | 5%               | 5%                 | 5%                |
| HackenProof Marketplace                            | 85%               | 60%               | 65%              | 40%                | 40%               |
| Cybersecurity products acceleration and incubation | —                 | 30%               | 25%              | 15%                | 15%               |
| Cyber security big data analytics platform         | —                 | —                 | 5%               | 10%                | 10%               |
| Unreported zero-day auction platform               | —                 | —                 | —                | 30%                | 30%               |

Fig. 5 Milestones

# Roadmap

| Project / Distribution of Resources | 2017 Q4    | 2018 Q1   | 2018 Q2    | 2018 Q3    | 2018 Q4 | 2019  | 2020 |
|-------------------------------------|------------|-----------|------------|------------|---------|-------|------|
| HackIT Conference                   | —          | —         | —          | <b>35%</b> | —       | 33%   | 32%  |
| HackenProof Marketplace             | <b>10%</b> | 20%       | 10%        | 10%        | 10%     | 25%   | 15%  |
| Hacken Accelerator                  | 5%         | 5%        | <b>10%</b> | 10%        | 15%     | 30%   | 25%  |
| Zero-day Platform                   | <b>5%</b>  | 5%        | 10%        | <b>15%</b> | 15%     | 25%   | 25%  |
| Analytics Center                    | 2.5%       | <b>5%</b> | 5%         | 7.5%       | 7.5%    | 37.5% | 35%  |

Fig. 6 Roadmap

## Launch periods:

HackenProof Marketplace — Q4 2017

Analytics Center — Q1 2018

Hacken Accelerator — Q4 2017

Zero-day Platform — Q3 2018

HackIT Conference — Q3 2018, new competitions and speaking panels at HackIT 2018 will be supported by Hacken

## The «Burning» Principle

We invented the “burning” principle for this token sale for regulatory reasons that might otherwise prevent customers residing in some jurisdictions from participating. We also believe that “burning” will expedite the growth of liquidity, and lessen the volatility risks for Hacken. It is important for all owners of Hacken to understand that “burning” affects only the platform fees, thus reducing the amount of Hackens which we, the founders of the platform, not our customers or clients, own.

What happens to the other 50% of our service margin that is not burned? The managing company of the Hacken Ecosystem will accumulate these Hackens until their amount reaches 1% of the total amount of Hackens in circulation.

Upon this event we will make 24 hours announcement, and then sell 1% of the amount accumulated at the moment of the event (i.e. 0.01% of the total amount of Hackens as of the moment of the event) via the major cryptocurrency exchanges. The sale will take place at 14:00 EET on the day following the day of the announcement. The list of exchanges will be provided to the public at the time of occurrence of the first such sale. We reserve the right to amend the list of exchanges in the future.

| Project           | The "Burning" Principle                                                                                                                                                                                                                            | Notice                            | Timing                                          |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|-------------------------------------------------|
| HackenProof       | 50% of the platform service margin for each transaction. Currently the estimated average margin for HackenProof services is 30% per transaction, meaning 15% of each transaction amount involving services of HackenProof is going to be 'burned'. | 24 hours before the burn          | Daily at 12:00 PM EET                           |
| Accelerator       | 50% of the accelerator margin during the startup exit. For obvious reasons it is difficult to estimate the exact exit margin right now. We expect the investment replicators to be within a range of 10x and higher.                               |                                   |                                                 |
| Zero-Day Platform | 50% of the yearly profit achieved by Hacken managing company from both operations. The amount of profit will be calculated on the basis of the financial reporting audited by a reputable international auditor.                                   | One calendar week before the burn | Yearly, after the audit of financial statements |
| Analytics Center  |                                                                                                                                                                                                                                                    |                                   |                                                 |

The "burning" will change the settled exchange rate of Hackens v. other crypto or fiat currencies. We need this to keep a decent price tag for vulnerability search services, attract more hackers to the platform, as well as ensure the stable and efficient maintenance of our Ecosystem. All the burning data will be transparent and available to the public via our website.

## Escrow and Audit

The escrow agents are involved in the process of guarding and managing the assets of investors. Their function is to monitor the use of the collected funds according to the roadmap described in this paper.

The escrow agents can veto the transaction by applying a cryptographic key to the project's HKN wallet, which we use to accumulate funds from investors.



The escrow account providers will be Juscutum and one of the Big 4 audit companies selected via tender managed by the Public Board of Trustees of the Hacken Ecosystem. Juscutum is a Ukrainian law firm based in Kyiv and providing legal support for blockchain businesses. For the HackenProof and HackIT Conference, 70% of the raised funds will be kept at Escrow. An escrow account will be established for 100% of the budgeted R&D costs for the Zero-day Platform, Hacken Accelerator and Cybersecurity Analytics Center.

The yearly audit of the financial statements of the legal entities comprising the Hacken Ecosystem will be conducted by an internationally recognized audit organisation, selected via tender managed by the Public Board of Trustees of the Hacken Ecosystem.

## Disclaimers

This document as well as any other documentation or information supplied together with, do not constitute an offer or solicitation to sell shares or securities. None of the information presented is intended to form part of, and should not be deemed a basis for any investment decision.

The Hacken Ecosystem does not provide investment advice or counsel or solicitation for investment in any security and shall not be construed in that way. This document does not constitute or form part of, and should not be construed as, any offer for sale or subscription of, or any invitation to offer to buy or subscribe for, any securities or other financial instruments.

# HackenProof

HackenProof is a bug bounty marketplace platform created by white hat hackers and the blockchain community based on the principle of fair share. This is a place where the two communities can cooperate and support each other. The purposes of this cooperation are high quality penetration testing and vulnerability reports for a premium fee paid to community members submitting these reports.

## How Does It Work?

- 1 / Customers sign up for the bounty hunting program, choose a defined program policy, decide on invitations and rewards and set the level of bounty payment.
- 2 / Our experts help customers setup and customise their program, and manage it if need be.
- 3 / After the scope of the security assessment is established our team invites the Hacken community to participate in the assessment. Hundreds of white hats evaluate the customer's code for vulnerabilities and bugs.
- 4 / Community members submit and prioritize vulnerabilities. Their reports are checked for relevance and originality.
- 5 / Community members receive a fee for discovering valuable vulnerabilities.
- 6 / The customer can additionally order advice from the Hacken security solution architects team to develop countermeasures if needs be.
- 7 / The customer gets a Vulnerabilities Certificate, attesting that her software was examined and tested by the Hacken community. Optionally, there can be a separate Countermeasures section in the Certificate, listing all the issues discovered and patched by the client.

## Money Back Guarantee

Some time after the initial launch we will implement the money back guarantee. For an additional fee the client will be able to purchase our services with a 'money back' option.

Therefore, if a client discovers a major vulnerability, which was not covered by HackenProof Vulnerabilities and Countermeasures Certificate after this certificate was issued, then client can claim back the fee paid to us. The expert examination of whether the discovered vulnerability exists and whether this is a 'major' vulnerability will be conducted by a third party, predetermined by the contract between the client and HackenProof.

## Key Features

**Invite only or public** — the public visibility level of your bug bounty program can be configured depending on your objectives.

**Self managed or dedicated** — your program can be customised depending on your budget and level of expertise.

**Customer self-service portal with rich scope of flexibility.** You can run a wizard to define and start your program, a bot will then check the reports and eliminate duplicates. You can then adjust the payments to offer bonuses for the most valuable discoveries.

**Customizable and sealed testing environment empowered** by VDI, VPN and PAM solutions, allowing researchers participating in the campaign to better understand the client's infrastructure without causing any harm or drama.

# Unreported Zero-Day Remuneration Platform

**We will create a remuneration fund for unreported zero-day vulnerabilities.** Hacken will support bright technology experts, by financially rewarding their original and previously undisclosed zero-day research.

We understand the legal and ethical risks involved, but our vision is that zero-day discoveries must have a transparent and publicly accountable remuneration channel, otherwise they will end up in the wrong hands. Currently the major risk is that many elements of the self-initiated zero-day research methodology are considered illegal in many jurisdictions. Such regulatory attitude slows down the development of verified remuneration channels and of zero-day research itself.

Regulatory inconsistencies lead to the risks of criminal prosecution of white hat experts openly doing their research for the benefit of humanity, while black hat hackers usually escape any punishment, doing dirty work for illegal cartels or rogue state actors. The reason for this, is a lack of effective digital discovery and evidence gathering mechanisms by local law enforcement agencies or, in the case of illegal state-sponsored hacking, direct government support and financing of the black hat hacking operations.

We will establish ethical and anonymous business processes for talented individuals researching zero-day vulnerabilities. The plan is to

invest a substantial amount of funds raised during this token sale in the research of regulatory and legislative framework in major jurisdictions, in particular — Europe. The ultimate goal is to create a transparent regulatory environment for our fund before it starts operations.

We would like to run special discounts for our community members to become subscribers of our Zero-Day Platform. However, it is important for Hacken community members to understand that for ethical and regulatory reasons, their participation in this token sale does not automatically grant them access to the Zero-Day Platform.

The public Board of Trustees of the Zero-Day Remuneration Platform will draft the access rules and perform the screening process. This Board will be created within one year after the token sale, if we reach the milestone which enables the Zero-Day Remuneration Platform. See the Hacken Token section for more details. The Board will consist of the most respected and experienced members of our community.

# Hacken Accelerator

**It is great when your employees decide to start their own business.**

That is an indicator that their current employment is enriching, inspiring and empowering.

In the 2000s Google started incentivising employees to 'moonlight' and develop their own projects and products. More recently it resulted in the emergence of Google Ventures, one of the most respected and innovative venture capital funds worldwide.

Being business owners in the cybersecurity field ourselves, we see the huge openness and potential of the Eastern European cybersecurity market. Frankly, it needs more high quality players and more innovative business models.

The biggest current problem is a lack of skills in attracting reliable investors and building a transparent corporate structure among Eastern Europeans who decide to start their own cybersecurity businesses. This results in a limited amount of substantial deals in our part of the world.

Without big exists, there are less angels ready to support early stage startups. Consecutively, the early mistakes and resulting failures traumatise young founders, driving them away from the very idea of launching their own business. We believe Hacken can break this vicious circle, by building a solid reputation among investors and business owners and then vouching for the best and most reliable members of our community. We will by then know whom they are, not only from their pitch decks and LinkedIn profiles, but from their real life projects and the everyday stress of deadlines and business KPIs.

After selecting these soon-to-be entrepreneurs, we will beef up their knowledge. By inviting our best clients and community members who already run their own businesses, they will be inspired and grow the next generation of cybersecurity leaders.

## **Investor Benefits**

- 1 / We co-finance the projects and share the risks with investors. Hacken will invest in up to 25% of the equity of startups that we accelerate.
- 2 / The Hacken marketing platform and our marketing team will be available to train accelerator participants, jointly develop the market entry strategy and help them successfully execute it.
- 3 / Hacken Analytics Center will help participants of the acceleration program to research competition and relevant customer segments and develop a unique customer value proposition.

# Cybersecurity Analytics Center

We are going to create a team of analysts, who will perform fundamental cybersecurity research, as well as monitor and audit existing and upcoming cybersecurity products.

Our team will then provide outstaffed corporate cybersecurity research, expert clearance and independent research and comparison of these products.

The basic newsletter of the Center will be in the open access via the Hacken website and social media. All the in-depth analytics will be available based on a subscription and via direct acquisition.

## Areas of Research

- Blockchain security, vulnerabilities and countermeasures;
- Classification, comparison and market research of cybersecurity products;
- Cryptography, secure communications and data protection;
- Big data analytics and visualisation in cybersecurity.

## Team

The Center will be lead by a well known CTF formation and their international advisors. The primary task of the team will be to develop an infrastructure and framework for researching and analysing 30+ different types of cybersecurity products.

We also plan to institute a permanent internship program with the Center for students from Ukraine and abroad. The most likely source of the talent will be finalists and winners of the HackIT Conference.



# HackIT Conference

Hackit is an annual international forum on cybersecurity held in Kharkiv, Ukraine.

The first HackIT Conference gathered 450 participants from two countries, the second had 650 participants from six countries. Besides the traditional speaking panels featuring local and international experts, HackIT runs a number of specialized cybersecurity competitions, which are free for everyone to participate.

## Capture the Flag Competition

HackIT CTF will take place on August 25 —27 of this year. Hackers will compete in 8 categories: Web, Misc, Joy, Crypto, PWN, Reverse, Forensics, Stego. In 2016, the event gathered more than 5,000 unique online participants from 1062 teams coming from 93 countries. The winner of the event, the DCUA team from Ukraine later became the best team of 2016 Worldwide according the CTF Time Rating.

## «Battle» of Hackers

The selection round for this competition occurs in the first half of the conference day and the final takes place during its second half. During the selection round, each participant has 30 minutes to solve the maximum number of cybersecurity assignments and earn points. Finalists who earned the maximum points then take the podium to perform real time cybersecurity problem solving. Their computer screens are broadcasted to the audience, and their performance is covered live by a cybersports TV anchor.

# Cyberdetective OSINT Challenge

This competition is run via a dedicated website and it starts several weeks before the conference. Participants receive a set of problems requiring to perform online open source intelligence researches in the most popular social networks, messaging applications and search engines. The winners get souvenirs and free tickets to the conference.

## HackIT Cup

This competition gathers the 30 brightest hackers from all over the World who became winners of HackIT CTF. The participating peers will sharpen their skills and develop an even stronger community.

They will be also offered a chance to participate in a private bug bounty program with instant payments. This year the vulnerability reports will be presented to the clients on board of Antonov 225 Mriya, the largest airplane in the world.

## Hacken at HackIT

At HackIT 2018 and ongoing conferences all tickets sales are going to be in Hacken only.



## HackIT Conference Quick Facts

- 1 / HackIT is community-driven event endorsed by local OWASP and DEF CON groups;
- 2 / The conference featured keynotes by industry leaders, including CheckPoint, EY, Samsung, Cyphort and GlobalLogic;
- 3 / Besides the conference HackIT features three online competitions: CTF, Battle of Hackers and Cyberdetective OSINT Challenge;
- 4 / More than 5,000 participants from 93 countries took part in HackIT CTF 2016;
- 5 / HackIT CTF 2016 winners, DCUA team, went on to become the best CTF team of 2016, according to CTftime.org.

# Who Are We?

We all were involved in various cybersecurity projects for the majority of our careers.

We long have seen Ukraine as a country of huge potential in the area of cybersecurity. Recent state-sponsored cyberattacks on the country's infrastructure led us to believe that our time had come.

Dmytro is ACCA, he worked for Deloitte for 8 years in various accounting, audit and project management positions. Currently, he is one of the top executives within Ukraine's military defence industry after its large scale reform was launched by the government in 2014-2015. While at Deloitte, Dmytro became the winner of the Deloitte CIS Audit Challenge with his audit of a Big Data SAP solution which was widely implemented in CIS offices, and in fact substantially increased project efficiency.



**Dmytro Budorin**

is the CFO and the Lead Manager of Hacken



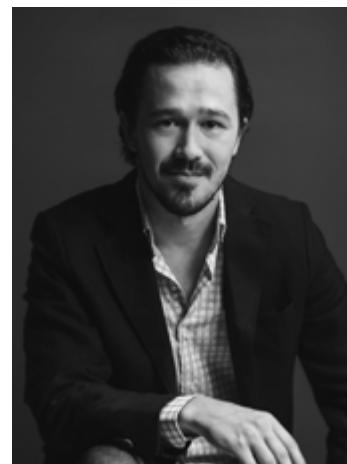
**Mykyta Knysh**

is the Community Director at Hacken

Mykyta specializes in cybersecurity training for various government institutions of Ukraine.

He is the CEO of ProtectMaster, one of Ukraine's oldest and reputable cybersecurity firms. Mykyta is a cybersecurity advisor to the Administration of the President of Ukraine and co-founder of HackIT Conference.

Andrii has 13 years of successful career in cybersecurity. He worked for corporate customers, integrators and successfully drove complex technical solutions for a dozen projects in several countries for corporations, government agencies, banks and even the International Olympic Games Committee. He is a certified expert in a number of technologies, including such vendors as CheckPoint, Cisco and Juniper Networks. His role in project is to provide technology leadership for developing, integrating, and supporting the HackenProof platform.



**Andrii Matiukhin**

is the CTO of Hacken



**Dr. Yegor Aushev**

is the COO of Hacken.

Yegor holds a Ph.D. in High Energy Physics from DESY, Hamburg. He is the author of 22 scientific papers in this field.

Since 2015, Yegor is the CEO of Information Security Group — a boutique cybersecurity firm providing penetration testing, data protection services and information security audit.

**Vladimir Taratushka**

Computer geek since 6 years old, started hacking in games, later - commercial software.

Studied informational and economical security. Was involved in online moneymaking with mobile payment content providers and CPA networks. Mined bitcoins since 27\$ price, was top10 at Eligius mining pool. Built a distributed affiliate mining network. Web developing company founder, Co-Founder HackIT conference. Selling and buying software exploits and 0-days.



---

# Why Does It Matter?

It is not news that cybersecurity is currently hot and so are cryptocurrencies. Nor is it anymore surprising to the World that Eastern Europe had currently become a testing range for state-sponsored cyber warfare.

Currently Ukraine is a notorious illustration of how traditional institutions failed to protect those for which they were created. The partial excuse here is our unreformed post-Soviet mentality, which was not ready for exponential digital threats of a World that is flat.

At the same time, during these recent turbulent years we observed a phenomenon that is totally new to our part of the World — a civic cyberactivism. Ordinary people: university professors, business consultants, attorneys and bankers united their efforts to build the country's collective cyberdefence system. We already saw this three years ago in the wake of Ukraine's military conflict that happened in the real space.

Such grassroots activism not only provides hope, but can also lead to a number of successful business cases. After all, the Western firewalls failed as well in 2015-2017, despite having better institutional culture, a well-established system of training, and most importantly, larger defense budgets which cannot be compared to the ones of Eastern Europe.

Cryptocurrencies play a vital role in enabling huge, distributed and transparent cyberdefense budgets formed by individual backers. They allow for bypassing the traditional institutional network, which in this case, might reach the target only when it is already too late.

This token sale, if successful, will enable us not only to build a sound regional cyberdefense system, but one which will also adjust itself to the challenges that will undoubtedly appear within the next decade. It might also launch a movement, that in several years will become an important factor in deterring and countering international cybercrime, including the ones that are state-sponsored.

Our experiment at Hacken starts with the obvious business model: a bug bounty and crowdsourced penetration testing platform. While some similar platforms already exist, we believe there is still a lot of land under the sun, as we explained in a separate section of this paper.

We then plan to unfold the ecosystem into two of our most risky adventures: the Zero-day Fund for buying critical vulnerabilities out of the grey market and the Accelerator for cybersecurity startups. Yes, currently there are too many startups with the word 'cyber' in their pitch deck. In this case, think not of a business opportunist, but of a local self-educated engineer with limited command of English (as of now), yet with a head full of bright ideas which might bring about the next WiFi or PayPal. We know such people exist in our neck of woods. We know mentors, who will help them to ramp their ideas up to a commercial level.

The Zero-day Fund might not initially seem related to the Accelerator, but it most definitely is. In order to drive smart Eastern Europeans away from dubious sources of income, we will first offer to legitimize their work by acquiring vulnerabilities they discover and making sure such vulnerabilities are disclosed to the rightful parties, primarily — the vendors. We will then offer a viable alternative to hacking, which in time will certainly become increasingly mundane. The alternative we are promoting is launching a legitimate business and halting being dependant on the Don who pays for petty dirty jobs.

Finally, while taking the best talent from the existing ecosystem, we want to make sure to give back. This effort is our support of HackIT Conference and creation of Cybersecurity Analytics Center.

HackIT already serves as a storefront for the profession. It is an inspiration for future generations and a place of knowledge exchange between established and aspiring cybersecurity professionals. The Center will then employ and support those people, who don't feel like starting their own business and are more inclined towards an academic and research career, moving forward the fundamental science of cybersecurity.


There are more projects to come, and they are already in our roadmap and on our radar. However, we realise that the existing milestones are already very ambitious and will require our full commitment at least for several years. So we better do what must be done first, and then "we will live on and we will see", as the common Ukrainian expression goes.

We hope this paper provided solid arguments and detailed information and ultimately convinced you to participate in our Hacken sale. If so, welcome to the Hacken Ecosystem and we'll see you soon as our respected community member and client. If not, we will be happy to provide you with additional assistance and more details at [info@hacken.io](mailto:info@hacken.io) or via our Twitter [@Hacken\\_Mrktplc](https://twitter.com/Hacken_Mrktplc).

# Addendum. Brief Analysis of Existing Vulnerability Research Crowdsourcing Businesses

| Feature                                                    | Bugrowd                                 | HackerOne                           | Synack                     | Cobalt    | HackenProof                                                                                                          |
|------------------------------------------------------------|-----------------------------------------|-------------------------------------|----------------------------|-----------|----------------------------------------------------------------------------------------------------------------------|
| 1. Country                                                 | US                                      | US / the Netherlands                | USA                        | USA       | Estonia / Ukraine                                                                                                    |
| 2. Market segment                                          | Mass market                             | Mass market                         | Corporate                  | Corporate | Hybrid                                                                                                               |
| 3. Penetration testing program                             | No                                      | No                                  | Yes                        | Yes       | Yes                                                                                                                  |
| 3.1. Subscription model                                    | No                                      | No                                  | Yes                        | Yes       | Yes                                                                                                                  |
| 4. Consulting <sup>1</sup>                                 | Yes                                     | Yes                                 | Yes                        | Yes       | Yes                                                                                                                  |
| 5. Private bug bounty                                      | Yes                                     | Yes                                 | No                         | No        | Yes                                                                                                                  |
| 5.1 List of top researchers <sup>2</sup>                   | Yes                                     | Yes                                 | No                         | No        | Yes                                                                                                                  |
| 5.2 Hands on bug bounties program development <sup>3</sup> | Yes                                     | Yes                                 | No                         | No        | Yes                                                                                                                  |
| 5.3 Managed platform <sup>4</sup>                          | Yes                                     | Yes                                 | No                         | No        | Yes                                                                                                                  |
| 6. Time based bug bounties (on demand) <sup>5</sup>        | Yes                                     | Yes                                 | No                         | No        | Yes                                                                                                                  |
| 7. Public bug bounties                                     | Yes                                     | Yes                                 | No                         | No        | Yes                                                                                                                  |
| 8. Money back                                              | No                                      | No                                  | No                         | No        | Yes                                                                                                                  |
| 9. Extended features                                       | Proprietary VPN technology <sup>6</sup> | Automated elimination of duplicates | Hydra scanner <sup>7</sup> | N/A       | a. Smart portal <sup>8</sup><br>b. Customization wizard for bounty program<br>c. Automated elimination of duplicates |



- 
- <sup>1</sup> High touch features, including the ability to have an expert provide debriefs on severely exploitable vulnerabilities.
  - <sup>2</sup> Researchers are allowed access to private bug bounties programs.
  - <sup>3</sup> In addition to hosting a platform to manage customer's program.
  - <sup>4</sup> In resource-constrained environments, customer may wish to outsource parts of her program.
  - <sup>5</sup> These types of bounty programs are typically of shorter duration and have a capped expenditure, which means you can limit your costs associated with scope content and thereby rival traditional outsourced penetration tests.
  - <sup>6</sup> Allows researchers to view specific program content through their portal.
  - <sup>7</sup> Advanced vulnerability intelligence platform for automating routine processes.
  - <sup>8</sup> Virtual desktop infrastructure for on-site bug bounty campaign. Virtual private network for on-site bug bounty company. Privileged account security solution for on-site bug bounty company;

---

# List of Figures and Tables

The Hacken Ecosystem

The HackenProof Vulnerabilities and Countermeasures Certificate

Token Sale Details

Token Distribution Chart

Milestones

Roadmap

The “Burning” Principle

HackIT Conference: Quick Facts

Existing Bounty Programs