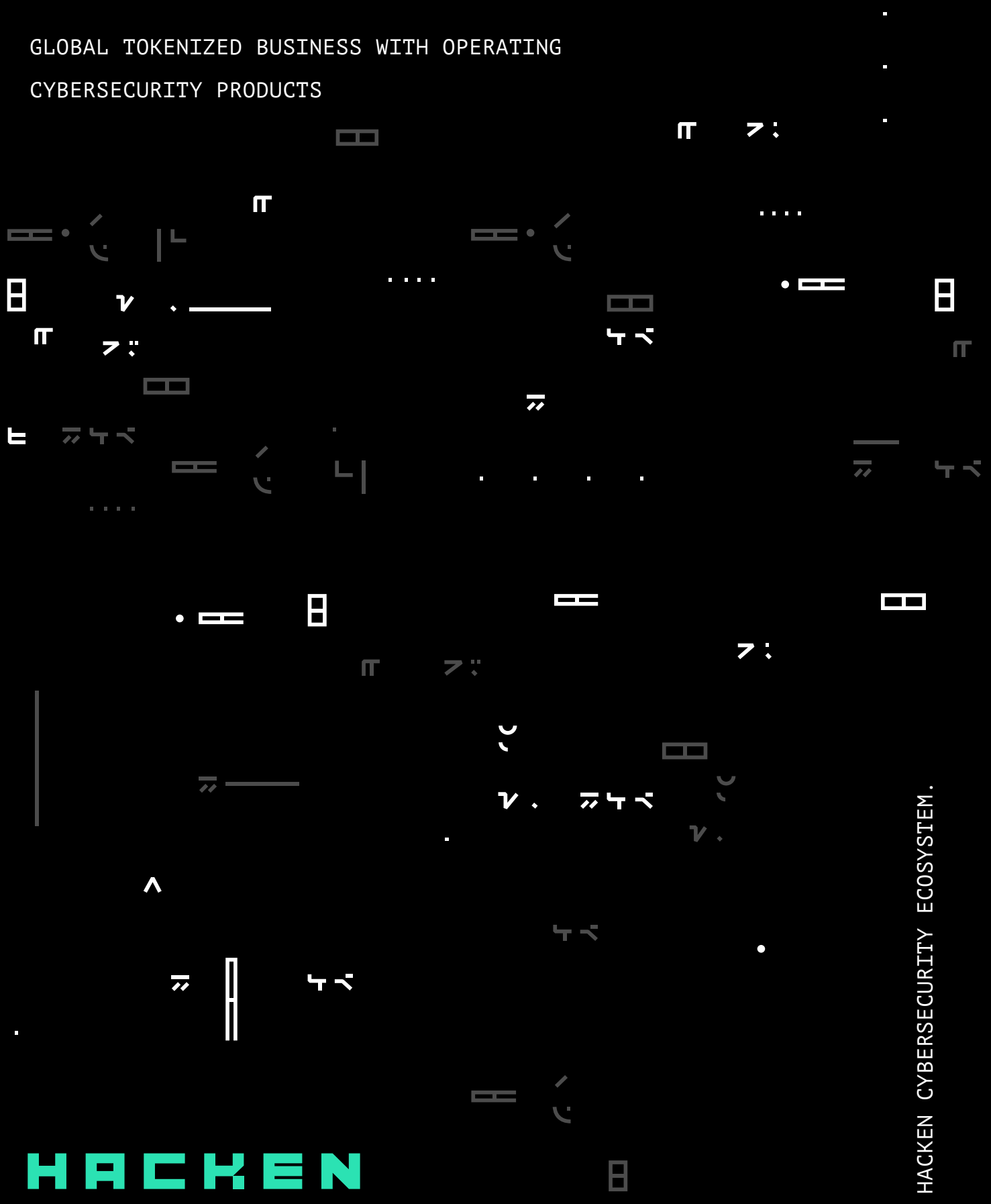
white paper version 2.0

GLOBAL TOKENIZED BUSINESS WITH OPERATING CYBERSECURITY PRODUCTS



HACKEN

HACKEN CYBERSECURITY ECOSYSTEM.

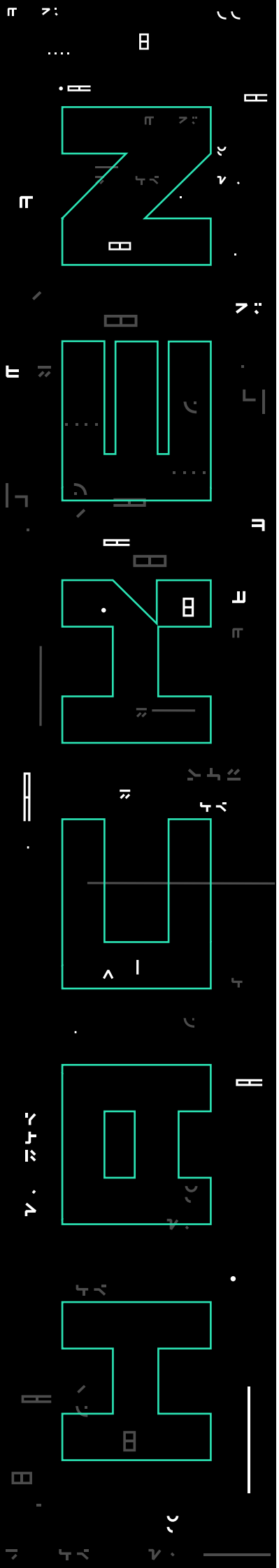
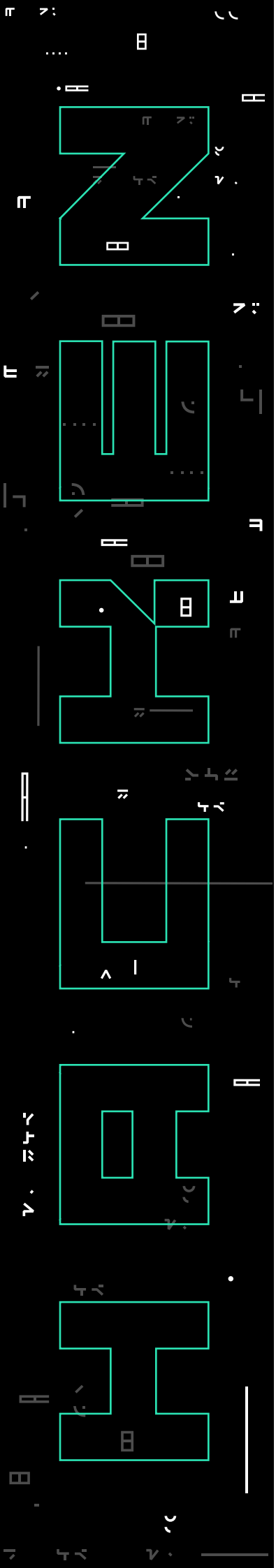


TABLE OF CONTENTS



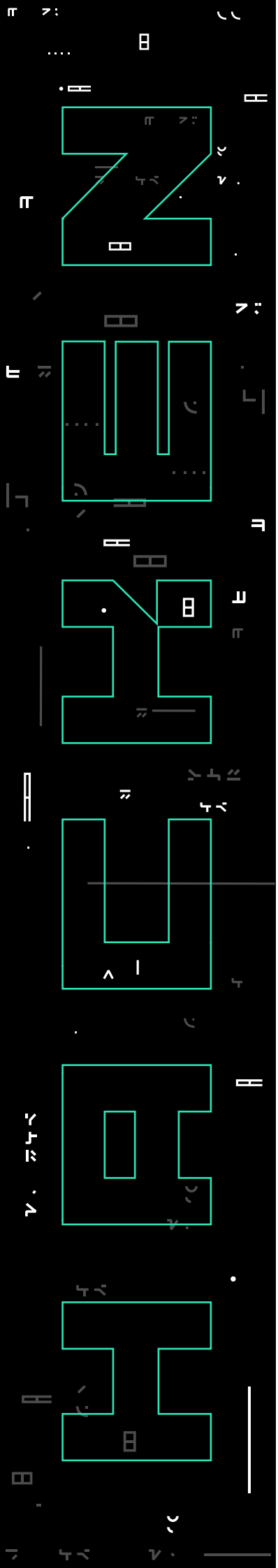
SUMMARY

This white paper explains the key business components of Hacken Ecosystem. It also details the recent initial coin offering (ICO) of Hacken token that took place in the autumn of 2017. Further, the document lays out the growth prospects of Hacken Ecosystem.

Hacken Ecosystem is a community-driven business organization with several jurisdictions worldwide. It consists of Hacken Hub (penetration testing, smart contract audit, and anti-phishing services), HackenProof bug bounty platform, Crypto Exchange Ranks (CER), and HackIT Conference.

HKN, an ERC20 token, is the only payment method allowed within Hacken Ecosystem. Buying HKNs early allows token holders to receive high-quality cybersecurity services in the future at an attractive price.

Financial data and legal documentation on HKN token sale are available as a separate attachment upon request.

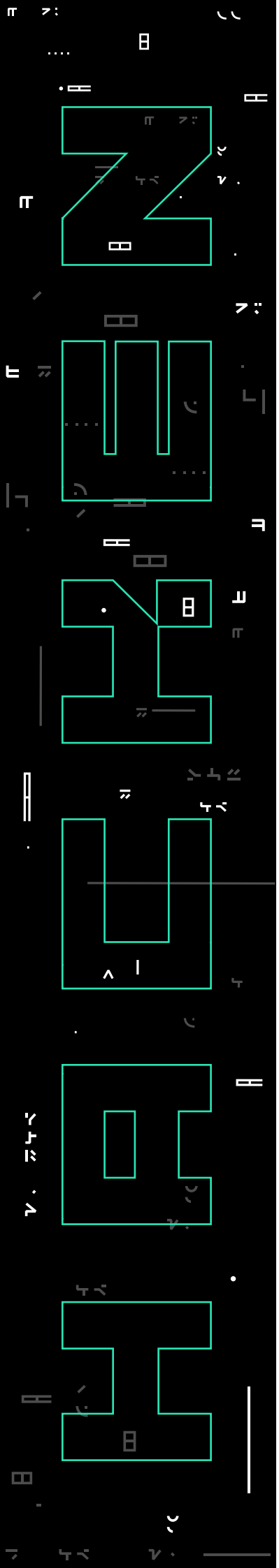


DISCLAIMERS

This document and any related documentation do not constitute an offer or solicitation to sell shares or securities. The information provided here is not intended to be a basis for any investment decision(s).

Hacken Ecosystem does not provide investment advice, counsel, or solicitation for investment in any particular security and shall not be construed in such ways. This document does not constitute and should not be construed as an offer for sale or subscription. Neither it is an invitation to offer or buy any securities or other financial instruments.

.



INTRODUCTION

$530M was stolen from Coincheck and $170M from BitGrail in 2018, $32M stolen from Parity and $7.4M from Coindash in 2017, $72M from Bitfinex in 2016, $5.1M from Bitstamp in 2015, $460M from Mt. Gox in 2014. These are daunting fiat equivalents lost to evil hackers due to various cryptocurrency infrastructure vulnerabilities.

According to Tyler Moore of Tulsa's Tandy School of Computer Science, since Bitcoin's inception in 2009, up until March 2015, around 33% of all bitcoin exchanges were hacked. Cryptocurrencies certainly are not the only businesses distressed by malevolent hackers. According to President Trump, for instance, cybertheft is the fastest growing crime in the United States by far.

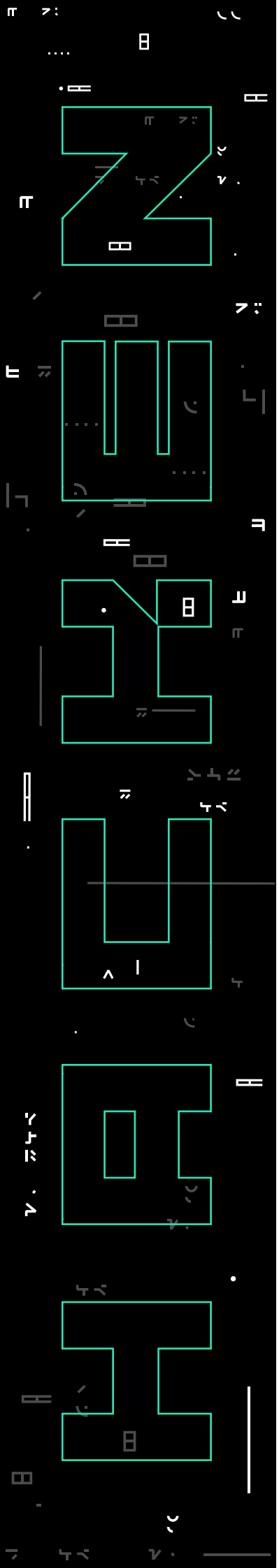
This presidential concern was followed by big money. The United States invested over $19B in cybersecurity as a part of the 2017 Federal Budget. This shows an increase from the $14B figure – the amount of funds in the budget allocated for cybersecurity by the Obama Administration in 2016.

Unfortunately, there is not enough talent to make use of these enormous financial resources. According to CyberSeek, there were more than 348,000 open cybersecurity positions in 2017, and this number is projected to rise to 1.8M by 2022. When one observes the growing number of evil hackers, one wonders why so many positions in the sphere are vacant.

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 still has little to offer to these people. Nevertheless, Ukrainian entrepreneurs behind such Silicon Valley unicorns as PayPal, WhatsApp messenger, and even the very WiFi technology you are likely using right now.

Ukraine also has a long history of a somewhat complicated relationship with Blockchain. While Bitcoin has never been officially recognized as a legitimate payment tool by local authorities, Ukrainian startups and experts stand among global leaders in the Blockchain revolution.

The story of BitFury proves the point. Established in 2011 in



Kyiv, BitFury controlled around 9.5% of the entire Bitcoin processing power as of January 2017, an achievement made possible due to customized mining chipsets developed by BitFury hardware engineers.

BitFury also secured a number of unique B2G partnerships, including the novel project allowing to secure land titles via blockchain. For instance, BitFury launched a joint project in cooperation with the government of Georgia.

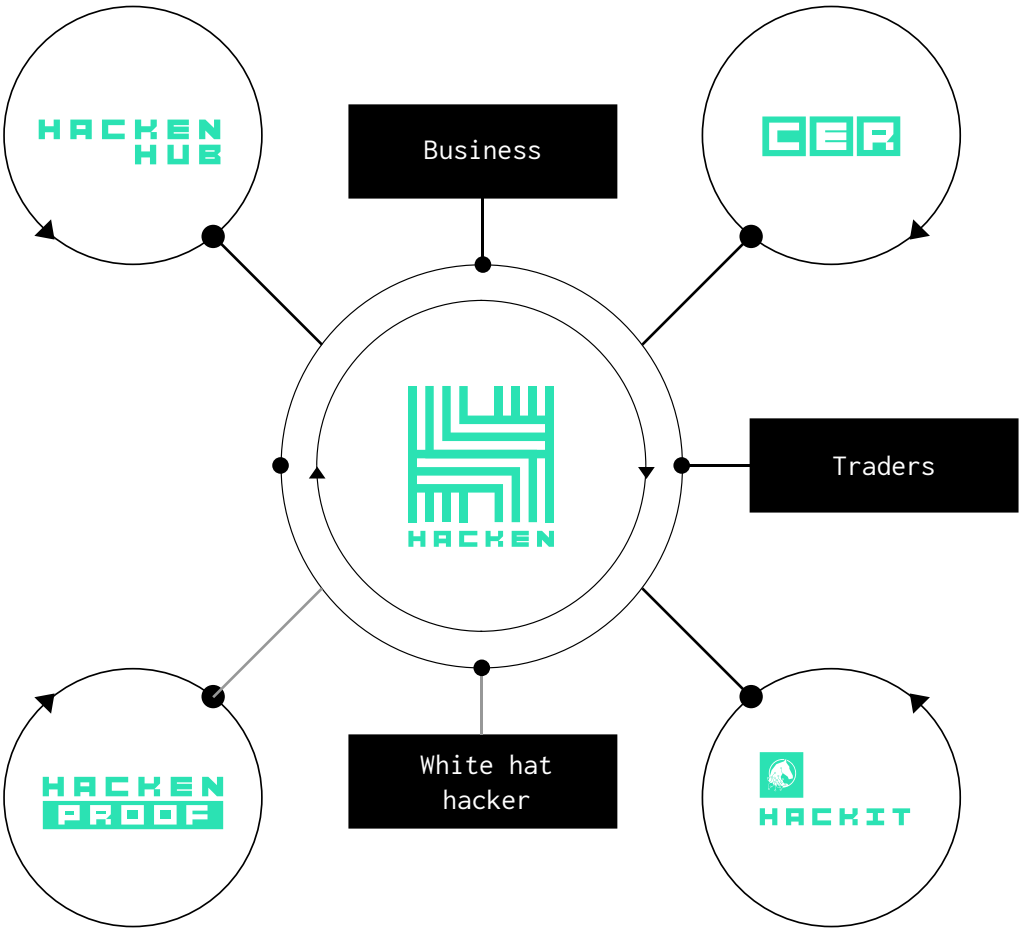
Since Ukraine has the potential to establish itself as a European cybersecurity hub, boosting expertise in this area is of utmost importance. The value of the Ukrainian currency (hryvnia) fell following the 2014 military conflict with Russia and booming Blockchain industry will contribute to the economy of the country.

The emergence of this new vibrant industry should be facilitated by a resourceful and ethical company with expertise in cybersecurity. This is where we come into the game, meet Hacken!

Our priority is to highlight the importance of the white hat cybersecurity community for the IT infrastructure of the world. To do so, we offer a stable means of income for our clients and financial incentives for our members. In the long run, your participation in Hacken Ecosystem will help to ensure that the next generation of secure computer whiz kids will be on your side of the firewall.

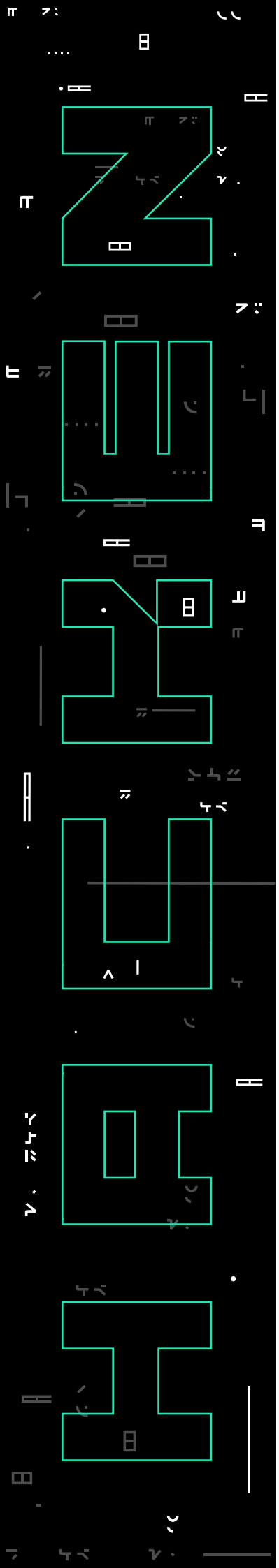
WHAT IS THE HACKEN ECOSYSTEM?

Hacken Ecosystem consists of Hacken token (HKN) and a constellation of cybersecurity services. The total supply of HKNs is finite, limited to 5.6 million tokens. This number will decrease over time because the team performs routine token burns. These burns increase liquidity and decrease volatility of the HKN token.



The businesses that comprise Hacken Ecosystem are Hacken Hub (penetration testing service, smart contract auditing, and anti-phishing services), HackenProof bug bounty platform, Crypto Exchange Ranks (CER), and the annual HackIT Conference. This document contains detailed descriptions of the four areas.

Community values are of primary importance to Hacken – we encourage HKN token holders to get involved through social media and to participate in the life of the company. HKN is a specialized software utility token that employs cybersecurity professionals and offers a project-based approach. The people



holding HKN need to communicate with each other in order to make use of their HKNs. Our vibrant community enriches the experience of each member and contributes to the security of their daily Internet activities.

While Hacken Ecosystem has a detailed business plan, our focus goes beyond profit. One of our goals is to grow and support various community events and meetups in Europe and beyond. Towards this end, we organize our very own international cybersecurity conference — HackIT.

The cybersecurity industry requires expertise, ethics, and persistent training. To empower our platform, we ensure that we give back to the community. We feel that setting up HackIT every year is a great way to do this. It helps to engage the cybersecurity industry worldwide through friendly competition, education, and entertainment.

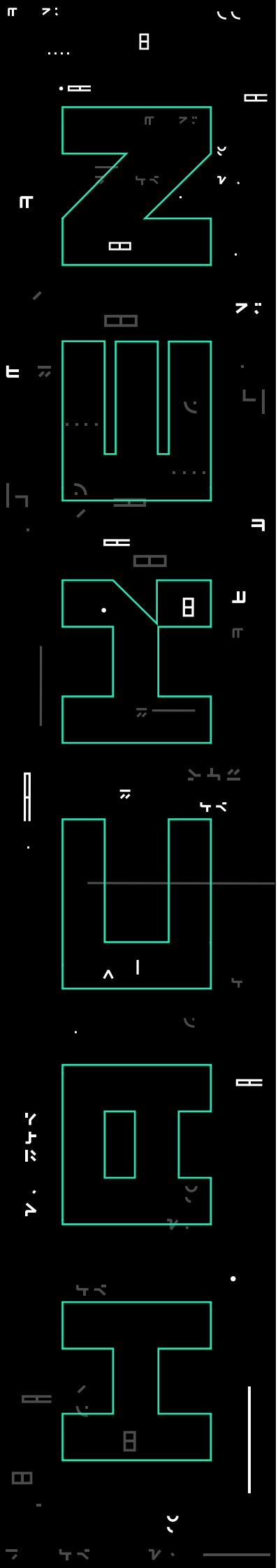
A great illustration of our core values is the story of Oleksii Matiiasevych— a Ukrainian cybersecurity professional, EDCC architect at Ambisafe, and technology advisor for the Hacken team.

On July 19, 2017, Oleksii discovered a critical vulnerability in the code of the Parity Ethereum wallet. There was no time to delay, as Oleksii found evidence of an ongoing attack that compromised hundreds of Ethereum wallets. He ended up “saving” $1,402,996.09 worth of Ethereum and transferred the money from the compromised wallets to the secure ones. Oleksii then contacted White Hat Group — they took charge of locating and returning the coins to their rightful owners.

Later, on May 22, 2018, Oleksii Matiiasevych helped to prevent a massive crisis in a large crypto marketplace by identifying a vulnerability that the top 8 cryptocurrency exchanges were susceptible to.

At Hacken we support Oleksii’s standpoint, his policy is the only acceptable course of action in such situations.

Being white hat hackers, we adhere to the ethics of computer hacking what implies providing expert security assessment to ensure comprehensive protection of a company’s information systems. Hacken specialists reflect appropriate goals, possess necessary knowledge and skills, as well as desire to make the web safe again.

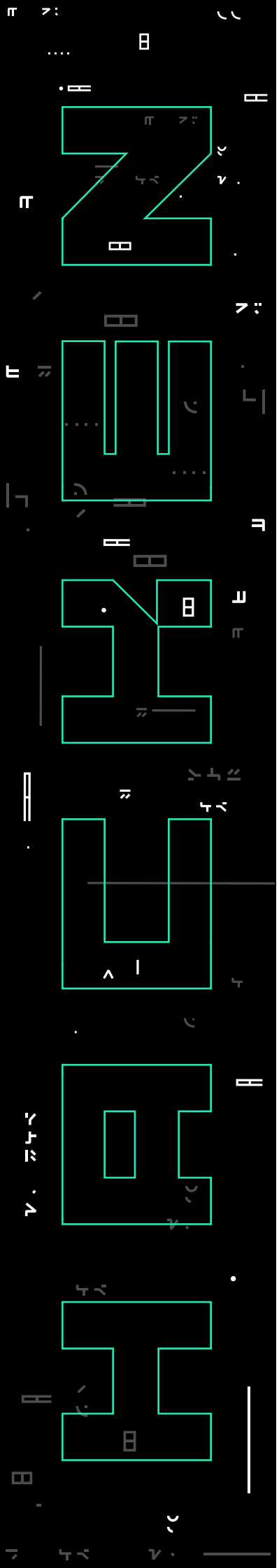


THE HACKEN TOKEN

For many millennia, money has been an efficient tool that unites organizations and drives their subsequent growth and development. Hacken is no exception. The distributed nature of Blockchain has enabled us to engineer the HKN token so that it has the best qualities of a modern cryptocurrency. Smart contract technology enables us to add an additional layer to Hacken by creating economic incentives and engaging the cybersecurity community to promote ethical crypto use.

HKN is the only currency accepted within the Hacken Ecosystem. Any services via HackenProof, Hacken Hub, or advanced subscription to our CER analytics must be purchased in HKNs. This will reward community members who get paid in HKNs by providing positive liquidity and low volatility.

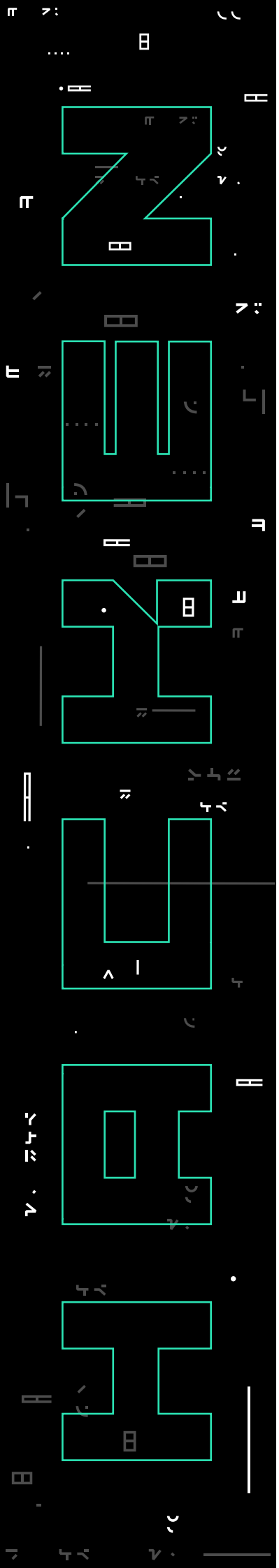
Please note: HKN is not intended to be a digital currency, commodity, or any other kind of financial instrument. It does not grant any share, stake, security, or equivalent ownership rights including any right to receive future revenue shares and intellectual property rights.



HKN Token Sale Information

Besides employing Blockchain in cybersecurity, HKN token also implements another interesting financial innovation in the area of tokenomics - the “burning” principle which we explain in a separate section of this paper.

TOTAL SUPPLY	20M Hackens 1.3M @presale (1M + 30% bonus) 18.7M @main token sale
SYMBOL	HKN
MINIMUM SALE-IN	1 ETH
MAX CAP	5.6M. No future emissions planned
INITIAL FIAT EQUIVALENT	1 HKN = 1 USD
CURRENCIES ACCEPTED	BTC, ETH, DASH, LTC, USD, EUR, TaaS
LENGTH OF TOKEN SALE	One month
ESCROW	On average 80% of the funds raised are kept in an escrow account
***BONUS PROGRAM FOR THE MAIN TOKEN SALE**	1 – 4 hours 25% 1 – 2 days 20% 3 – 7 days 15% 1 – 2 weeks 10%

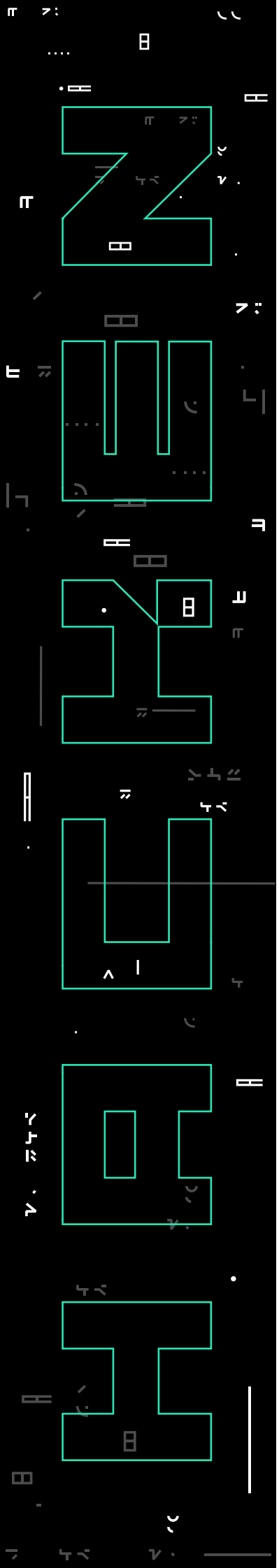


Token Distribution during ICO:

OPEN SALE	80%
TEAM REMUNERATION	10%
ADVISORS	7%
COMMUNITY MANAGER	1%
VOLUNTEERS BOUNTIES	2%

Token Distribution:

THE TOTAL AMOUNT OF HKNS CONTRIBUTED	5.6m HKNs
FUNDS RAISED	252 BTC, 5359 ETH, and $1240
TOKENS RESERVED FOR HKN CORE ACTIVITIES	560 000 HKN
TOKENS RESERVED FOR ADVISORY BOARD AND PARTNERS	392 000 HKN
TOKEN HOLDERS	3688



Launch periods:

2018

Q1

HackenProof Platform

Q2

CER

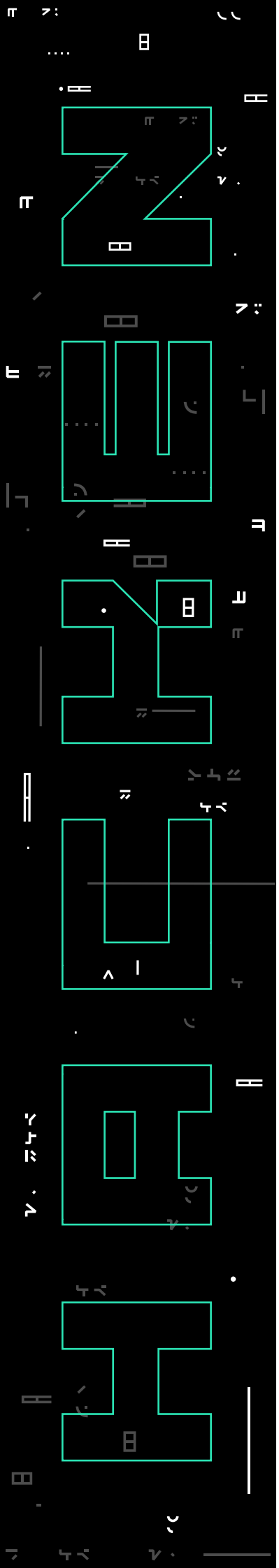
Q3

HackIT Conference
New competitions and speaking panels at HackIT 2018 will be supported by Hacken

Q4

Hacken Marketplace

2019



THE «BURNING» PRINCIPLE

When creating the HKN token, we developed our very own “burning” principle. We believe that “burning” will expedite the growth of liquidity and lessen the volatility risks for Hacken token holders over time. It is important for all owners of Hacken to understand that “burning” applies to platform fees only - this reduces the amount of HKNs owned by the founders of the platform; not its customers or security researchers.

The burning of HKNs is not integrated into the main smart contract of Hacken on the Ethereum Network. We want to ensure that the HKN token transactions between investors and exchanges will not trigger the burning mechanism. The burning principle will be applied only to the “product” transactions; in other words, to all HKN transfers related to the services of Hacken Ecosystem.

Every Hacken service transaction is divided into 3 parts.

The first part is the 70% of the net value of HKNs transferred. This amount is immediately delivered to the wallet of the final recipient. For instance, HackenProof bug bounty payment in HKNs goes to white hat hackers who submit vulnerabilities. In case of a service purchase (e.g. anti-phishing or smart contract audit), this amount of HKNs is considered company’s revenue.

Of the remaining 30% of the transaction, 15% of tokens represent a team fee. It is applied to all services and payments - should that be HackenProof or other Hacken services.

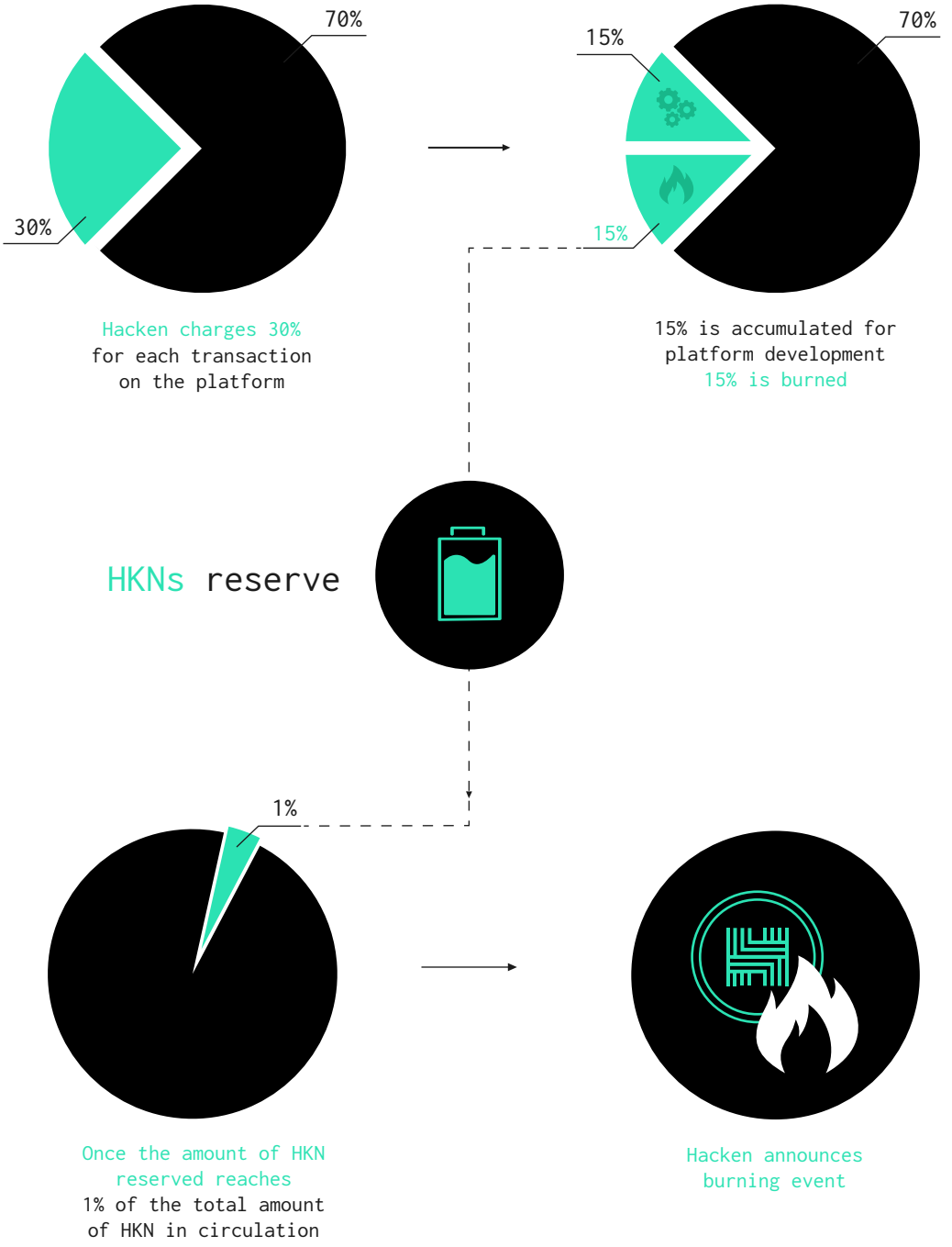
The other 15% goes towards the token burn event. These tokens are transferred to the HKN reserve. Once the amount of HKNs in the reserve is equal to 1% of total supply, the team will sell 1% of the tokens (i.e. 0.01% of the total amount of Hackens as of the moment of the event) via major cryptocurrency exchanges.

We will announce the event on social media with a 24-hour notice.

The sale will take place at 14:00 EET on the day following the day of the announcement. Hacken will provide the list of exchanges to the public at the time of the event. We reserve the right to amend the list of exchanges in the future.

The “burning” will influence the exchange rate of Hackens vs

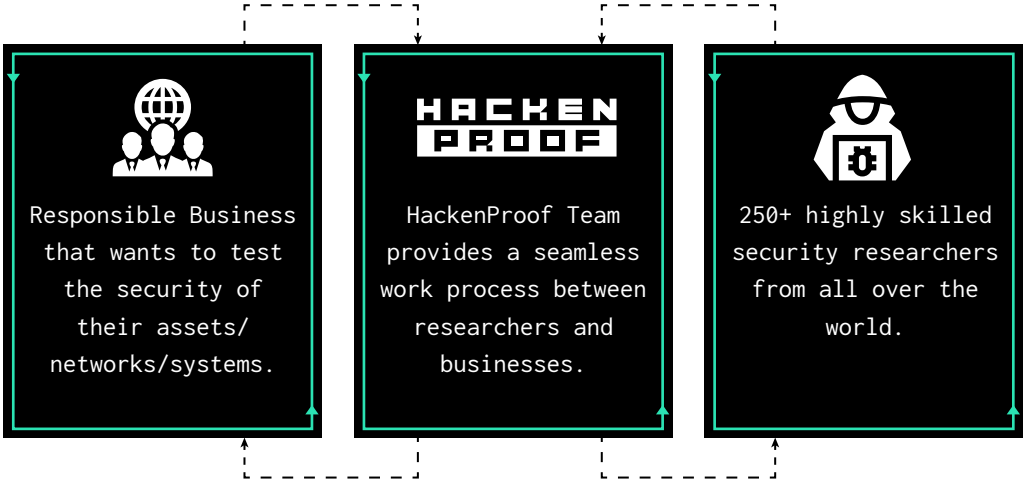
other crypto or fiat currencies. This allows Hacken to maintain a decent price tag for vulnerability search services, attract more white hat hackers to the platform, and ensure stable and efficient maintenance of our Ecosystem. All the burning data will be transparent and available to the public via our website.



HACKENPROOF

HackenProof is a Bug Bounty Platform that helps businesses to protect their digital assets, personal data of customers, and their reputation through crowdsourced security.

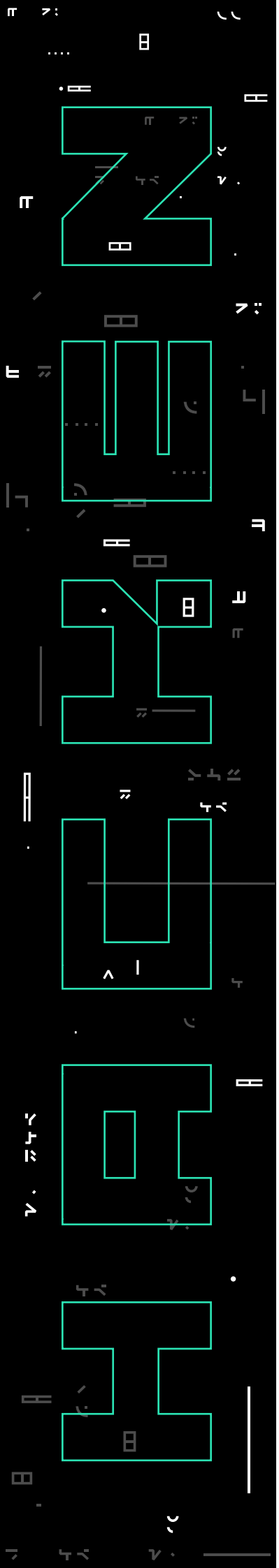
By combining a “crowd” of cybersecurity researchers (white hat hackers) and HackenProof platform, we deliver the quality of service that cannot be matched by traditional cybersecurity firms. Conventional cybersecurity services are constrained by the size of their teams: the amount of time and skill employees have as a group. Bug bounty platform solves this issue – hundreds of security researchers will test your product on a continuous basis. This approach allows to identify vulnerabilities more efficiently and to prevent possible cyber threats.



The HackenProof platform has gathered a great number of skilled white hat hackers from all over the world that specialize in finding vulnerabilities in the 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 who care about the security of their products. We ensure responsible and coordinated vulnerability disclosure and encourage white hat hackers to protect modern businesses.

Any actions that may potentially damage the systems of a client are pre-negotiated and necessitate customer’s consent. This process of customization is transparent and thoroughly planned in advance. Throughout the assessment, businesses receive frequent detailed reports from security researchers.



A tokenized platform is decentralized among the community. Receiving remuneration in HKNs, white hats are one of the significant constituents representing the beneficiaries of the platform. HKN's price directly depends on the quality of the services provided, the number of secured clients, and the overall size of the white hat community.

Bug bounty platform advantages

Unlike conventional cybersecurity firms, bug bounty platform attracts a crowd of highly skilled cybersecurity researchers with various backgrounds to find product vulnerabilities.
Bug bounty platform provides transparent reporting, 24/7 analytics, and information on the current status of your bug bounty program.
The platform handles all operational issues – validating submitted bugs, communicating with white hats, and organizing other operational activities.

How Does It Work?

1 / Customers sign up for the bug bounty program, choose program type (private or public), determine the number of white hat hackers and their skill set, and decide on reward parameters.

2 / Our security team helps customers set up and manage their program(s).

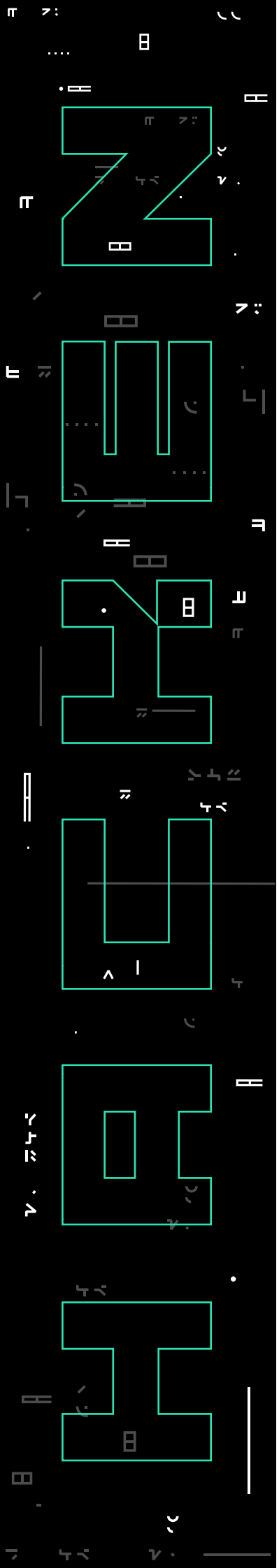
3 / After the scope of the security assessment is established, our team invites the HackenProof community to participate in the bug bounty program. Hundreds of white hats evaluate customer’s code in search of vulnerabilities.

4 / Community members submit detailed reports of all vulnerabilities they discover. Their reports are checked for accuracy, relevance, and originality.

5 / White hats receive bounties for discovering valid vulnerabilities.

6 / Customer may order additional professional advice from the Hacken Security Solution team.

HackenProof Roadmap



APR. 31

Vulnerability public disclosure feature

Flexible automated payouts

JUN. 30

Implementation of Hackenproof Widget for submitting

JUL. 31

Enabling Integrations with third parties via API

AUG. 30

Group researches and teamwork mechanism implementation

Endorse and feedback module release

SEP. 30

Beta version

OCT. 30

Source code proof programs

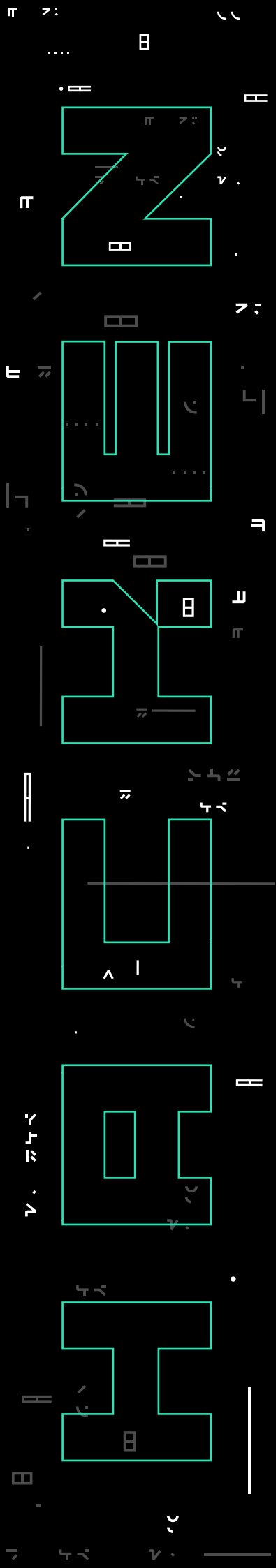
SEP. 30

Adding Company Scoreboard

Smart profile filling

DEC. 30

Decentralized review protocol MVP Release



CER

Crypto Exchange Ranks does analysis, scoring, and benchmarking of exchanges – the platform will ease the process of finding a relevant crypto exchange.

CER provides 24/7 analysis of data from all major crypto exchanges. The information is thoroughly analyzed via advanced economic and mathematic models, artificial intelligence, machine learning, linguistic programming, and a detailed cybersecurity assessment. The processed data is used as input for a multi-factor scoring model in order to produce the most precise estimations.

As a result, CER clients receive accurate and up-to-date ratings of trading platforms – this information significantly enhances the decision-making processes when it comes to exchanges.

Problems that are going to be resolved

- Liquidity;
- Quotations clarity;
- Kitchen-cheating;
- Arbitrage trading;
- KYC and AML process;
- Legal compliance & legitimacy;
- Withdrawal process and limits (counterparty risks);
- Public opinion sensitivity;
- Technical and cybersecurity sustainability.

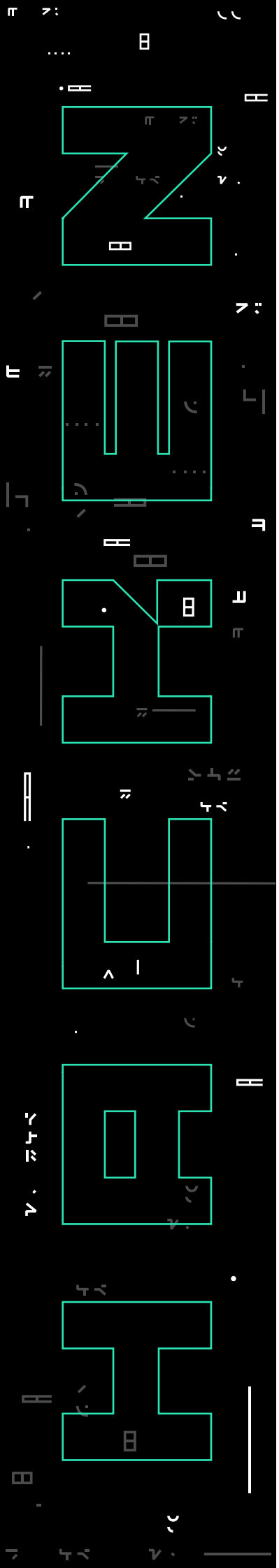
Specialists that are working at CER

We have 5 main directions:

- Economic and mathematic modeling in risk assessment.
- -Artificial Intelligence and machine learning algorithmization.
- Cybersecurity (Hacken).
- NLP (Neuro-linguistic programming).
- HFT (High-Frequency Trading).

Target Audience

Individual investors, institutional investors, traders (HFT), crypto exchanges, independent governmental agencies, and traditional financial institutions. By the latter, we mean establishments, such as pension capital funds, which do not have direct exposure to cryptocurrency and require tools to analyze risks.



HACKEN HUB

Hacken Hub provides a wide range of cybersecurity services. We employ experts from across the world to provide customized cybersecurity solutions for all kinds of businesses.

Anti-Phishing Service

Specialists from Hacken apply filters to detect phishing messages and then compare the specified URI codes to the ones cataloged in a growing database of known malicious URIs. Another way Hacken detects phishing sites is by determining features of their behavior and blocking them automatically every time users come across them.

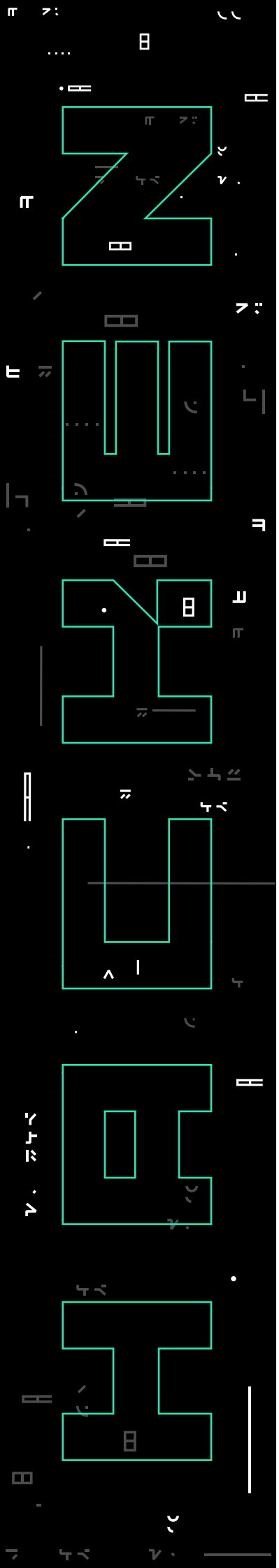
Our anti-phishing services also offer educational materials – they teach users to recognize phishing emails and dangerous sites, protect their computer and mobile devices, choose secure passwords, and block fraudulent Google ads and fake social media accounts that violate user's brand name and success for nefarious ends.

Besides, one of our most recent antiphishing services is AntiPhishing Bot. Phishers and fake channels are the reason why we developed the bot for Telegram because this messaging service is one of the most popular communication channels in the crypto and real worlds. Among its most popular and useful features are blocking links in 2 modes, anti-admin phishing, statistics monitoring, and wallet recognition.

Smart Contract Audit

A tiny error or defect in the logic of a smart contract may lead to the enormous financial loss.

The external audit ensures that your smart contract works as you expect: it detects vulnerabilities in the contract and double-checks the logic of your program. Hacken tests the code of a smart contract and suggests solutions for the detected issues. Our methodology includes testing reentrancy attacks, access control, and many more.



Here are some key benefits of doing Smart Contract audit with Hacken:

- A detailed report
- Reliability when it comes to tight deadlines
- Fixed and transparent pricing
- Appropriate and easily interpretable audit metrics
- Analysis and testing by at least two independent researchers.

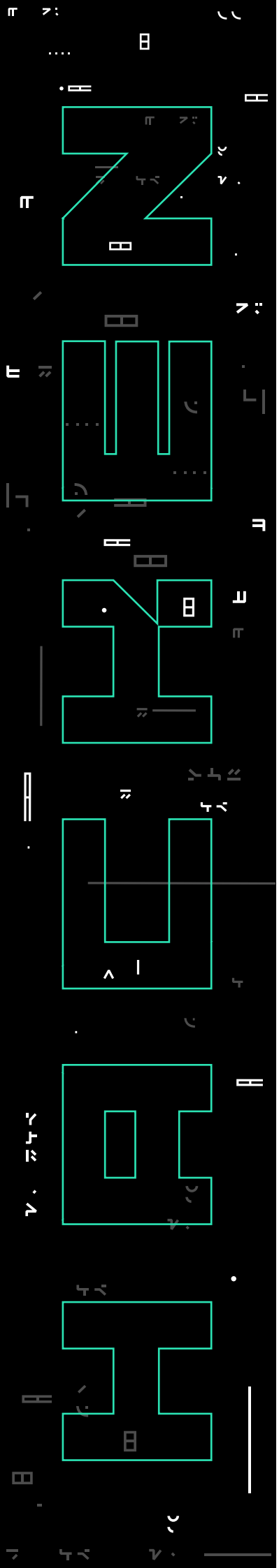
Penetration Testing

Penetration testing has become of utmost importance for companies that operate in the digital world.

Security testing for web and mobile applications is performed to find all possible vulnerabilities in applications. Hacken provides clients with black-, grey- and whitebox penetration testing. Our professionals have substantial experience across different technology stacks and platforms.

Here are some key benefits of doing Smart Contract audit with Hacken:

- A detailed report
- Reliability when it comes to tight deadlines
- Fixed and transparent pricing
- Methodology description



HACKIT CONFERENCE

HackIT is an annual international forum on cybersecurity held in Ukraine.

In 2015, the first HackIT conference took place. It gathered 450 participants from two countries. Next year, 650 participants from six countries attended HackIT. About 700 people attended the conference last year. In 2018, HackIt will be held for the fourth time and more than 1200 attendees are expected to come.

The conference offers speaking panels featuring local and international experts, as well as specialized cybersecurity competitions, which are free for everyone to participate.

Capture the Flag Competition

Hackers compete in 8 categories online: Web, Misc, Joy, Crypto, PWN, Reverse, Forensics, and Stego. Thousands of hackers worldwide take part in the CTF competition to test their skills and win money rewards and tickets to HackIT.

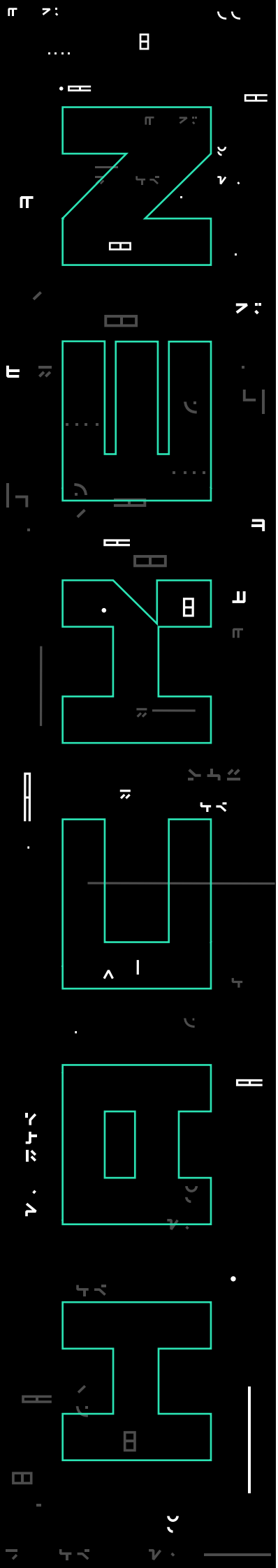
HackIT Cup

HackIT Cup – an onsite Bug Bounty Marathon. It is a real challenge for the best white hat hackers gathered under one roof: the participant who finds the highest number of vulnerabilities in the digital assets of a customer wins the competition.

For the first time, this competition gathered the 30 brightest hackers from all over the world and offered them a chance to participate in a private bug bounty program with instant payments. The participators sharpened their skills and showed dedication to community values of white hats. In 2017, on the board of Antonov 225 Mriya, one of the largest airplanes in the world, Steve Wozniak greeted these very researchers.

«Battle» of Hackers

The selection round for this competition occurs during the first half of the conference day. During the selection round, each participant has 30 minutes to solve the maximum number of tasks to earn points. During the second half of the first conference day, finalists of the selection round 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.



HackIT Conference Quick Facts

1) HackIT is a community-driven event endorsed by the local OWASP and DEF COIN groups

2) The past conferences featured keynote addresses by industry leaders: CheckPoint, EY, Samsung, Cyphort, and GlobalLogic

3) HackIT also 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, the DCUA team, went on to become the best CTF team (according to CTFtime.org).

6) HackIT 2018 will aim to bridge Europe and Asia. It will last for 5 days and will include 2 workshop days, 2 days of speaking panels, and a trip to Chornobyl.

ABOUT US

All members of our team have been involved in various cybersecurity projects for the majority of their careers.

For a long time, we have seen the huge potential of Ukraine in the area of cybersecurity. Recent state-sponsored cyber attacks on the infrastructure of the country led us to believe that our time had come.

CEO

Dmytro Budorin

Dmytro is ACCA; he worked in Deloitte for 8 years in various audit, ERP implementation, and project management positions. While at Deloitte, Dmytro won the Deloitte CIS Audit Challenge with his audit of a Big Data SAP solution, which CIS offices widely implemented. As of late, he has been one of the top executives in Ukraine's military defense industry. At Hacken, Dmytro takes a leading role: he is responsible for all managerial decisions and implementation of Hacken’s long-term and short-term strategic goals.

CSO

Mykyta Knysh

Mykyta is Hacken’s Chief Security Officer; he specializes in cybersecurity training for various governmental institutions of Ukraine. He was a non-regular consultant at the Administration of the President of Ukraine and is now a former officer of security services of Ukraine. Mykyta managed his own successful business in the field of cybersecurity and co-founded HackIT conference. His role is to provide operational security services to the clients.

CTO

Andrii Matiukhin

Andrii has 13 years of successful experience in cybersecurity and implementation of technologies: he worked with such vendors as CheckPoint, Cisco, and Juniper Networks. Andrii successfully put forward complex technical solutions for more than a dozen projects in several countries for corporations, government agencies, banks, and even the International Olympic Games Committee. His role at Hacken is to provide technological leadership, coordinate existing services, and support the interaction between business units within Hacken Ecosystem.

Business Development Director

Dr. Yegor Aushev

Yegor holds a Ph.D. in High Energy Physics from DESY, Hamburg. He is the author of 22 scientific papers in the field. Since 2015, Yegor has been the CEO of Information Security Group – a boutique cybersecurity firm offering penetration testing, data protection services, and information security audit. Currently, Yegor is working on entering new markets for Hacken Ecosystem and opening new offices overseas. Moreover, Yegor is also responsible for Government Relations.

CFO

Oleg Zverlin

Oleg worked at Deloitte for more than 11 years in various management positions. He is a finance professional with extensive hands-on experience in financial analysis and corporate finance: M&A transaction services, business valuation, financial modeling, business plan development for strategic and financial investors. He worked in Ukraine, the UK, and CIS countries. At Hacken, Oleg oversees company's finances: liquidity management, financial planning, and controlling. Further, he maintains the financial health of Hacken Ecosystem.

HackIt Lead Manager

Vladimir Taratushka

Vladimir studied Informational Security and has a degree in Economical Security. This hereditary coder started hacking in games as early as 6 and later switched to commercial software. His background leads him into the crypto world, and Vladimir started mining BTC when the currency was valued at just $27. He built a distributed mining network, founded a web developing company, co-founded HackIT cybersecurity conference and ProtectMaster - an information security services company.

COO

Andrey Polyansky

Andrey is a highly qualified manager with more than 18 years of experience in the finance industry. He developed his expertise via a banking career in large international groups in Ukraine. Andrey received an MBA degree and was accredited as ICU's executive coach. At Hacken, he is responsible for the management of company's operations, HR, and procedures related to the efficiency of business development.

CMO

Ivan Hotsko

Ivan started his career with the b2b startup Precoro. He then worked as a multi-regional SEO specialist for TemplateMonster, one of the world's biggest website template marketplaces. A certified inbound and sales marketer, Ivan focuses on demand, leads, and customer generation. His primary responsibility is to generate revenue by increasing ROI through digital marketing operations.

Crypto Exchange Rating Product Manager

Shestakov Dmytro

Dmytro has almost 12 years of experience in the field of investment management and strategy development; he holds an MBA degree in banking and finance. Dmytro headed Investment and Innovations at one of the largest governmental enterprises in the defense industry of Ukraine. Moreover, Dmytro has worked as a Vice-President for Strategy and Development at Ukrainian Interbank Currency Exchange. As a CER Product Manager, he conducts market researches, generates product requirements, and represents products according to time-integrated plans.

HackenProof Product Manager

Evgenya Borshevan

Before joining Hacken, Evgenia was in charge of one of the largest cybersecurity conferences in Eastern Europe – HackIT. She has taken part in numerous scientific security conferences and summer schools in Europe. Last but not least, she holds a master's degree in cybersecurity and the title of a Certified Ethical Hacker. Evgenia is a co-founder of Hacken and performs several tasks as HackenProof Product Manager: she unites the efforts of all security researchers, internal security team, sales, and product teams to provide security excellence for responsible businesses.

Brand Director

Marichka Voitovich

Marichka implemented marketing and rebranding strategies for the first Ukrainian weapon supplier and presented the company at military exhibitions. She created a set of catalogs for all Ukrainian weapons. Marichka is in charge of the brand promotion of Hacken Ecosystem. She cultivates the image of the Hacken brand all over the world during international conferences.

Demand Generation Director

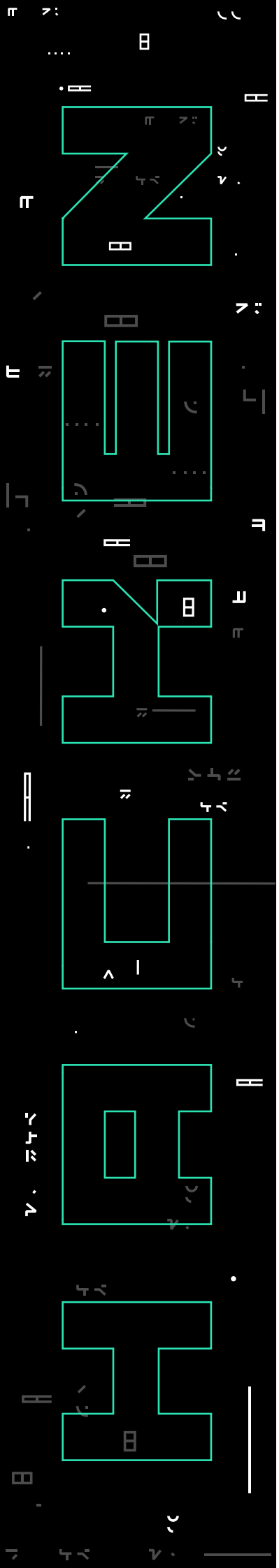
Hleb Myrko

Hleb started his career as a co-founder of an educational project focused on the African and Asian markets. Simultaneously, he worked for UvoCorp as a writing mentor and corporate trainer. Hleb has a Master's Degree in Management and Economics, and he is a certified inbound marketer. At Hacken, he is responsible for generating demand on each strategic direction of the Hacken Ecosystem operations including HKN token, HackenProof, CER, Hub Services, and HackIT Conference.

Growth Hacker

Ilya Alypov

Ilya is a certified inbound marketing specialist. He specializes in the development of web solutions for small and medium businesses. Further, he focuses on the organization of confluences, product development, data-driven marketing, and design. His role in the project is to design and build a scalable and stable growth machine.



WHY DOES ANY OF THIS MATTER?

It’s neither surprising that cybersecurity is a thriving industry, nor that the reason for that is Eastern Europe becoming a test site for state-sponsored cyber warfare.

Recently, Blockchain has also come under attack and became a test site for various penetration and hacking techniques (as we mentioned in the Introduction section). The more Blockchain projects emerge, the more black hat hackers focus their attention on this industry.

During these recent turbulent years, we observed a phenomenon that is totally new to Eastern Europe – civic cyberactivism. Most different Ukrainian citizens - university professors, business consultants, attorneys, and bankers united their efforts to build a collective cyber defense system for the country.

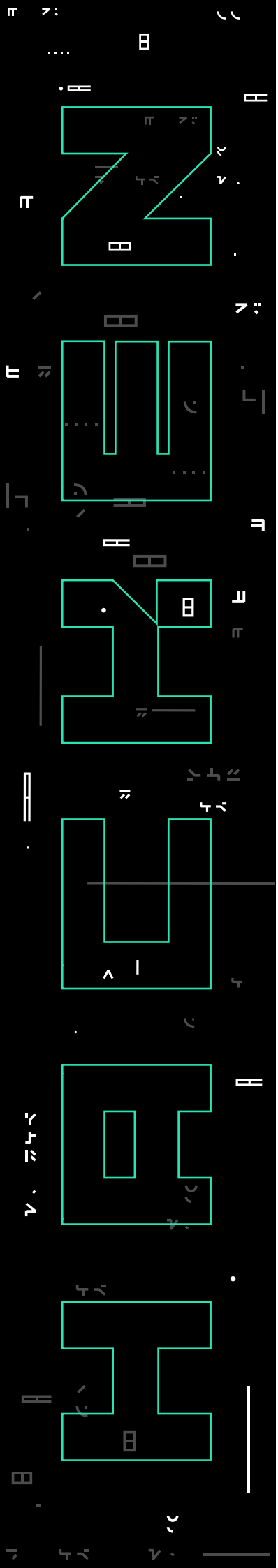
Cyberactivism is a positive development that may lead to a number of favorable projects and initiatives. After all, despite a superior institutional culture, proper training, and larger budgets, Western firewalls failed in recent years.

Cryptocurrencies play a vital role in enabling huge, distributed, and transparent cyberdefense budgets form a decentralized network of individual backers.

That is why the HKN token sale was a major success! It enabled us to build a sound regional cyber defense system that adjusts to meet potential in years to come. Ultimately, it is intended to launch a movement that will focus on countering international cybercrime and cooperate with different governmental institutions to develop cybersecurity standards.

Hacken has a straightforward business model: a wide range of cybersecurity services including a Bug Bounty Platform – HackenProof – and crypto security and analytics center –CER.

We look for the best talents in existing cybersecurity ecosystems and give back to the community. This latter effort is our support of HackIT Conference and assistance to the global community via the services of Hacken Hub.



CONTACT US

We hope that this document provided solid arguments and detailed information about Hacken's importance to the global fintech industry. We welcome you to the Hacken Ecosystem! We are happy to provide you with assistance and more details at info@hacken.io or via our Telegram Group https://t.me/hacken_en.

Visit Hacken's (HKN) official channels:

- Official Website;
- Hub Hacken;
- HackenProof;
- Crypto Exchange Ranks.

Follow Hacken's (HKN) official social media accounts:

- Telegram;
- Twitter;
- Facebook;
- Reddit;