New security standards for Token Offerings

NOBOBOX

NOBOBOX revolutionizes cryptocurrency shopping by providing freedom for consumers and increased profits for vendors

FinTech

- Headquartered in Liechtenstein
- Developed a smart contract according to ERC20 standards
- Enlisted Kaspersky Lab to conduct a Smart Contract Review
- Launched Token Sales on February 10, 2019

NOBOBOX creates a completely new shopping experience with innovative services. Customers have the choice whether they want to pay with crypto or fiat money, and merchants choose which currency to accept.

NOBOBOX offers solutions for both consumers and retailers. The NOBOCARD hybrid provides a seamless experience to customers regardless of the payment format they use: fiat, crypto or credit. Registration on nobobox.com lets buyers mix up currencies in their NOBOWALLET and pay with the currency that suits them best. The PLUG'N'PAY solution can be integrated into online stores and allows merchants to receive payments in the currencies of their choice.

"We believe that by bringing in NOBOCARD and PLUG'N'PAY we are providing an absolutely new level of freedom to use cryptocurrency like any other payment option when shopping. We are creating an excellent opportunity for investors to jump on a blockbuster in the crypto economy", - says Chief Marketing Officer at NOBOBOX, Helene Stil.

"Security should become an essential element of every ICO project and Kaspersky Lab with their 21 years of cybersecurity expertise is a perfect fit for this role. We wholeheartedly recommend the Kaspersky Smart Contract Review service to any company planning an ICO."

Helene Stil, Chief Marketing Officer at NOBOBOX.

Challenge

"On the 10 th of February 2019 we began selling our tokens, NBX. During preparations we thought about more than just the technical requirements for entering the market. There already have been numerous ICOs on the market, where companies just run with the idea, compose a glossy whitepaper, raise funds and snatch at the profits without laying any serious groundwork or developing for the long-term. This approach makes it difficult for anyone who is offering a sound project and a real investment opportunity," continues Helene Stil.

"Of course, the security, transparency and trustworthiness we offer to our investors is absolutely key. We set the soft and hard cap, and if we don't reach the soft cap all our investors will get their money back.

The smart contract business logic is described in the ICO Whitepaper and we were looking for additional verification. Naturally, we thought of having a 3rd party **security assessment of Smart Contract**", Helene carries on, "we had to be absolutely sure that neither design flaws nor vulnerabilities or undocumented features inside the NOBOBOX Smart Contract affect the execution and success of our project."

TRUST
A security assessment of smart code reassures investors that the company is results-driven

SECURITY
An additional verification layer ensures better protection for investors' funds from money-draining bugs

TRANSPARENCY
Having a cybersecurity partner in place adds to a trustworthy reputation for entrepreneurs

EXPERTISE
21 years of cybersecurity expertise boosts any startup project in the crypto currency field

"The shocking story of The DAO Hack when 70mln dollars were stolen due to a critical money-draining bug in the Smart Contract, pushed the businesses planning ICOs to seriously consider external assessments of the Smart Contract code they have developed", sums up Vitaly Mzokov, Head of Verification, Growth Center at Kaspersky Lab. "Assessments have become the "must have" process when a company hires external developers".

Kaspersky Lab Solution

Helene describes the decision-making process: "We were looking for a reliable partner for a Smart Code review, since once the Initial Token Sale (ITS) begins and the Smart Contract is published, making any changes is a complicated task and leads to unnecessary risks. Kaspersky Lab made our short list quickly thanks to their excellent reputation on the security market. We considered several offers and chose Kaspersky Lab after appraising their 21 years of expertise in the cybersecurity field and their proven experience in discovering the most advanced threats including those in the blockchain-based industry."

The Smart Contract Review took 5 days and included the technical assessment of the code and an examination for design flaws and vulnerabilities. The process also involved verifying the consistency between the logic described in the NOBOBOX ICO whitepaper and the logic implemented in the actual source code.

"We received a report from Kaspersky Lab experts containing their findings and their recommendations. Luckily, there were no critical or money-draining bugs found. The discovered issues included some unintentional errors, but since they could badly impact our investors' trust, we are glad they have all been found and resolved", Helene concludes.

The Smart Contract Review entailed Kaspersky Lab conducting a second review after all corrections to the code were made. The security experts re-checked everything and gave it a "green light".

70 million USD

The most expensive money-draining bug ever found in a Smart Contract

1 week

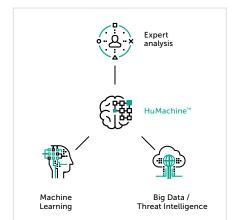Time required for a Kaspersky Smart Contract Review

Why all ICO projects need a Cybersecurity partner

"We consider our partnership with Kaspersky Lab essential for NOBOBOX business. We conduct all our operations in cyberspace, so is vital to have a partner with outstanding expertise in cybersecurity on our side," Helene Stil went on to say.

"We are impressed with Kaspersky Lab's rigorous standards and attention to every detail, as well as their quick and professional communications. We always felt a reliable presence as we were working with Kaspersky Lab and we are glad to promote our partnership and impress our reliability on investors."

"Security should become an essential element of every ICO project and Kaspersky Lab with their 21 years of cybersecurity expertise is a perfect fit for this role. We wholeheartedly recommend the Kaspersky Smart Contract Review service to any company planning an ICO," notes Helene.

Helene Stil concludes: "Across the crypto business it is truly important to have a cybersecurity partner in place as there are multiple security concerns about crypto. Having an established partner with long-term experience in the cybersecurity field ensures an extra advantage to the reputable ICO company. We plan to cooperate with Kaspersky Lab in the future to safeguard the security and transparency of all of our future products."

Expert analysis

HuMachine™

Machine Learning

Big Data / Threat Intelligence