Tael

Smart contract audit as a baseline requirement for token listing

2019

kaspersky BRING ON THE FUTURE

Kaspersky Smart Contract Audit

Tael introduces a blockchain-based solution to fight counterfeit goods in China.

www.taelpay.com

RetailTech

- Based in China, with operations in Australia, Japan, Singapore, and Europe
- Founded in 2015
- Listed on Binance
- Passed **Kaspersky Smart Contract Audit**

We decided to go a different way and choose a major cybersecurity vendor whose name is globally recognized. Kaspersky easily fit our vendor profile requirements. They have 20 years of experience in the cybersecurity field, a team of world-renowned experts, and solutions designed to protect against threats acting in the blockchain and crypto world."

Alex Busarov,
Co-founder & CEO, Tael

People are excited about blockchain solutions for consumer markets. Tael, with its blockchain-based anti-counterfeit solution, breaks into the Chinese market to become an essential tool for young parents concerned about the quality of their infant formula and other sensitive goods, such as cosmetics, nutrition, and health supplements.

Consumers are not the only ones who care about the authenticity of the products they buy in the local supermarket. Manufacturers and retailers suffer a lot from counterfeit goods. Not only does it impact their income but it also jeopardizes customer loyalty.

"The Tael solution consists of two blockchain layers: the first one, based on Hyperledger Fabric, is responsible for handling the NFC anti-counterfeit label algorithm and the earning of loyalty points with each consumer authentication 'touch'. The second layer utilizes the Ethereum blockchain, allowing easy integration into exchanges and providing simple storage options for token holders." – explains Alex Busarov, co-founder and CEO of Tael

"Thanks to retail giants like Rakuten adopting new technology and becoming our partner, we are able to offer an extensive selection of authentic, high-demand imported products to tens thousands of our users. Consumers are able to verify the origin of products regardless of whether they purchase it online or offline."

Alex Busarov sums up: "Our solution demonstrates growing levels of adoption and real-world usage, a fixed amount of tokens issued, and a constantly growing base of token holders interested not only in trading operations but in safe purchases."

Security is a baseline for token listing

"When it comes to blockchain technology and crypto operations, you definitely have to think about securing your solution and digital assets from cybercriminals looking for easy profits." - Alex Busarov turns the conversation back to security needs.

"When we talked to exchanges about listing our tokens, many of them had the same request: make sure you audit your smart contract code to confirm its security for exchange users. We approached the top exchanges and they were unequivocal: a baseline requirement is a 3rd party audit of the smart contract code." - says Alex Busarov.

41,389
Tael token holders worldwide

265
products from **90** different brands are available in the Tael Ecosystem

18x (1800%)
Tael customer base growth rate in 2019

Pavel Pokrovsky, Blockchain Security Group Manager from Kaspersky, summarizes: "Exchanges care about their reputation and do not want to put themselves at risk with new tokens that could be a potential attack vector. During the last 3 years, exchanges have suffered a lot from cyber fraud. Now they have implemented procedures to assess the reliability of the partners they work with."

"So, we found ourselves looking for a reliable vendor who would be able to review and assess the Tael smart contract and reassure its level of security for us, our community, and crypto exchange users." – sums up Alex Busarov.

One for all

"When communicating with exchanges about listing our token, we received recommendations for smart contract audit companies from each exchange. However, often the company recommended by one exchange was completely unknown to the others.

We decided to take a different route and choose a major cybersecurity vendor whose name is globally recognized. Kaspersky easily fit our vendor profile requirements. They have 20 years of experience in the cybersecurity field, a team of world-renowned experts, and solutions designed to protect against threats acting in the blockchain and crypto world." – shares Alex Busarov.

Pavel Pokrovsky explains: "Smart contracts and blockchain code can contain bugs or even major backdoors. These can be an entry point for threat actors."

A smart contract contains algorithms that determine how each step of a transaction is performed. **Kaspersky Smart Contract Audit** includes identification of security vulnerabilities, design flaws, and undocumented features within the smart contract code that could lead to exploitation.

The review also includes verifying the consistency between the logic described in the whitepaper and the logic implemented in the actual source code.

TRUST
Security assessment is a baseline requirement to enter the world's top crypto exchanges

SECURITY
Kaspersky Smart Contract Audit secures Tael's commitment to their community

PROTECTION
Auditing smart contracts protects community funds from draining away

"Exchanges care about their reputation and do not want to put themselves at risk with new tokens that could be a potential attack vector. During the last 3 years, exchanges have suffered a lot from cyber fraud. Now they have implemented procedures to assess the reliability of the partners they work with."

Pavel Pokrovsky,
Blockchain Security Group Manager, Kaspersky

Performed by malware experts, the audit results in a report on detected issues and recommendations on how to mitigate them. After the code owners correct the issues, the security experts re-check everything before giving the final code a 'green light'.

Secure blockchain

We developed our blockchain-based solution to ensure the authenticity of imported goods and sensitive products in areas where counterfeits are a persistent issue. For their part, Kaspersky secures vital elements of our blockchain-based solution. We both work to secure our customers and that creates a good foundation for a partnership: both teams understand how important security and safety are for their respective clients." - summarized Alex Busarov.

2017 and 2018 were the years when cyber fraud grew exponentially in the crypto world. Nowadays, fintech companies have to pay significantly more attention to security during the development stage and implement risk prevention procedures in each step of crypto currency introduction to the market, from the initial coin offering to listing and trading tokens.

We are glad to observe security awareness growing in the crypto world. An additional effort to reassure the security of token offering literally pays for itself. Smart contract audits require little resources but save the company not just financial assets, but also intangibles such as reputation and the trust of customers that cost a lot", - concluded Pavel Pokrovsky.

Kaspersky Smart Contract Audit

Identification of security vulnerabilities, design flaws and undocumented features

www.kaspersky.com/blockchain

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com

kaspersky **BRING ON THE FUTURE**