Blockchain Security related solutions

Kaspersky® Smart Contract Review

Make sure your Smart Contract is written in secure manner, follows best practices and implements business logic as outlined in your project Whitepapers.

Kaspersky® Incident Response

The overall aim of Incident Response is to reduce the impact of a security breach or an attack on your IT environment. The service covers the entire incident investigation cycle.

Kaspersky® Educational Services

Cybersecurity education is the critical tool for enterprises faced with an increasing volume of constantly evolving threats.

Kaspersky® Penetration Testing

Penetration testing is a practical demonstration of possible attack scenarios where a malicious actor may attempt to bypass security controls in your corporate network to obtain high privileges in important systems.

Kaspersky® Application Security Assessment

Uncover vulnerabilities in applications of any kind, from large cloud-based solutions to embedded and mobile apps.

Kaspersky® DDoS Protection

Total DDoS attack protection and mitigation solution that takes care of every stage to defend your business. From continuous analysis of all of your online traffic, through to alerting you about the possible presence of an attack.

Kaspersky® Anti Targeted Attack

This platform combines the latest technologies and global analytics in order to detection and respond promptly to targeted attacks, counteracting the attack at all stages of its lifecycle in your system.

Kaspersky® Anti-Phishing Feeds

This service actively tracks and alerts you in real time to the appearance of phishing sites targeting your brand, and provides you with relevant, accurate and detailed ongoing reporting about phishing or fraudulent activity.

Kaspersky® Fraud Prevention

Powered by a complex range of advanced technologies with Machine Learning the service is applied for proactive detection of sophisticated fraud schemes across web and mobile channels.

www.kaspersky.com

Kaspersky Lab
Enterprise Cybersecurity: www.kaspersky.com/enterprise
Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com/

#blockchainsecurity

Kaspersky for Business

KASPERSKY lab

Blockchain Security

The ultimate solution package for securing blockchain-based technologies

Blockchain-based technology is becoming increasingly popular and is now used to solve a wide range of tasks. And it's not all about cryptocurrencies. Its many applications make blockchain technology a key element in establishing business processes that can even be applied in manufacturing.

Blockchain technology is present in IoT networks, workflow management systems, crypto-currencies and numerous other fields. It is now an essential component and state-of-the-art standard for a whole host of businesses.

However, being a security-driven measure, blockchain technology itself can be exposed to various risks. Given the fact that blockchains contain sensitive information about the assets and infrastructure of specific users and enterprises, providing comprehensive protection is critically important.

Ensure complex security for your blockchain applications

Incident Response
Instant reaction to intrusions, identity compromise and security breaches.

Application Security Assessment
Code review, detection of threats related to smart contracts and platform drawbacks.

Education & Awareness
Learn how to react when your blockchain application is at risk and how to prevent security incidents.

Protection Against Fraud & Phishing
Mitigate the risk of phishing and data leakage caused by malicious activity.

Continue reading to learn how Kaspersky Lab can protect your blockchain-based business from cyber-threats

The benefits of decentralization:

Centralized security systems can be broken by attacking just one central node. In the past few years, hundreds of millions of individual identities have been compromised due to cyberattacks:

- Facebook (2018) – 87 million profiles (source: The Guardian)
- LinkedIn (2016) – 167 million account details (source: Telegraph)
- eBay (2014) – 145 million profiles (source: Reuters)
- JPMorgan Chase (2014) – 83 million accounts (source: The Guardian)

In 2017, the WannaCry malware infected 300,000 computers all over the world. The damage was estimated to be around $1 billion. (source: Telegraph)

Decentralized networks are vulnerable too:

- In June 2016, the DAO (Decentralized Autonomous Organization) refund mechanism was exploited. An Ethereum-based smart contract of two steps was able to return Ethereum to the investor. Then it took the tokens from an investor's wallet. The hacker repeated the first step which wasn't added to the blockchain until he gained $79.6 million. Developers decided to rewrite the history – it was a very dirty fix. (source: Business Insider)
- In December 2017, the large Bitcoin mining marketplace called NiceHash lost $60 million following a hack. (source: bitcoin.com)

Are you in?

The fact you're reading this means you're interested in protecting your blockchain-based application or network. This is a crucial part of a cybersecurity strategy for many enterprises.

Large distributed systems have always required multi-layered protection. Blockchain technology appears to be both a modern infrastructure solution and remedy. It provides automated workflow functionality as well as protection.

Why blockchain?

You probably already know all about the advantages of blockchain technology – first and foremost, its high level of security and reliability.

Decentralization

A blockchain usually consists of a distributed P2P network. The endpoints – nodes – replicate the data within the system. This architecture prevents complete system failure as there is no single point with full responsibility.This approach protects a blockchain from hacking by forcing a potential intruder to pass every node's security barrier in order to gain access to the system and data.

Cryptography

The data is only accessible through a set of private and public keys. The credibility of transactions is ensured by complex cryptography. This makes the system sufficiently tamper-proof.

Consensus protocols

System changes are only allowed with the consent of the holders of major stakes in blockchain power or assets. This is called a consensus protocol. Stakeholders agree on a decision to add new transactions to the blockchain, preventing any unwarranted violations.

Seems to be secure, but is it?

There are lots of risks you may not notice or don't know how to respond to

Smart contract vulnerabilities

Smart contracts and the blockchain application code may contain bugs or even major backdoors. Each of these can be an entry point for hackers. There's often a threat of code injections and insecure data storage or transfer. The application can be exposed to the risk of client-server communication flaws.

Website Vulnerabilities / DDoS threats

ICO hubs and crypto assets exchange websites can be exposed to the risk of DDoS attacks and breaches.

Phishing

Social engineering, fraud and phishing remain potential threats even to highly protected systems such as blockchains, as scammers can elicit users' login credentials or personal information.

Decentralized applications vulnerabilities

Decentralized applications (dApps) have caused a paradigm shift in software development. They are, by design, immune to the numerous security issues that affect traditional applications. But since they are written by humans, they introduce new vulnerabilities that hackers are eager to exploit.

Lack of operational security and cyber-hygiene

In some cases, if over 50% of the blockchain power is controlled by the attackers, they will be able to verify fraudulent transactions.

You have to take action to provide additional security for your blockchain-based projects, would it be Enterprise Blockchain, Crypto-Exchange or any Token Offering project

- Keys should only be provided to trusted users who have passed an internal verification;
- Access to the blockchain has to be well encrypted and protected from outsiders;
- Network participants have to use as much security layers as possible: login, password, public and private keys, certificates;
- Blockchains and smart contracts must not contain malicious code;
- Client-server or P2P communications have to be secured against the siphoning off of data transfers;
- Each user has to be informed of the action plan in the event of an attack;
- Each user needs to be familiar with the precautions to take to prevent leakages;
- Access to the various components of the blockchain should be strictly differentiated in accordance with the user level.

Now you can see how vulnerable your blockchain project may be and how important it is to provide comprehensive security

Discover the wide range of solutions from Kaspersky Lab for blockchain-based projects

Blockchain technology can be applied in many different areas, including IoT, banking, and e-government. But the roots and the primary demand are still in the field of crypto assets.

The technology provides complex security for ICOs and crypto exchanges – areas where finances are concentrated and risks are high.

Token Offering such as ICO (Initial Coin Offering) or STO (Secure Token Offering) is a procedure to attract investments through selling company tokens. A crypto asset exchange is where users trade and buy cryptocurrencies. Both ICOs/STOs and crypto exchanges take place in cyberspace and are vulnerable to cyberthreats.

Crypto exchanges and all Token Sales require specific cyberprotection

We can provide that		
Blockchain App Security	Token Offering Security	Crypto Exchange Security
Blockchain-based networks are used in a wide range of fields. Even though the technology itself is secure, blockchains also need protecting. The risks of bugs, targeted attacks or unauthorized access can be eliminated by: • Instant incident response • Code review • Fraud and phishing protection • User education	Based primarily on combined technology, ICOs/STOs need code protection as well as web protection: • Fraud and phishing protection • Incident investigation • Smart contract reviews and reports • Website security monitoring • Cyber-Hygiene Education • Testing for breaches • Project code review • DDoS protection	Crypto asset exchanges require constant protection and monitoring: • Fraud and phishing protection • Incident investigation • Website security monitoring • Cyber-Hygiene Education • Testing for breaches • Targeted attack prevention • DDoS protection • Quarterly security reports • Regular code review