INSOLAR

Hands-on experience in security assessment for an enterprise blockchain

2020

kaspersky BRING ON THE FUTURE

Kaspersky Enterprise Blockchain Security

Insolar introduces a next-generation distributed ledger platform to drive blockchain adoption amongst Fortune Global 500. It powers shared processes and trusted data exchange while ensuring data consistency, transparency and security.

www.insolar.io

IT

- Headquartered in Switzerland, with offices in USA, UK, Canada and Russia
- Founded in 2017
- Passed **Kaspersky Blockchain Application Security Assessment**

"We engaged Kaspersky, an independent, best-in-class cybersecurity expert, to evaluate our code during the final stages of development. Together, we uncovered and resolved issues that might have affected Insolar Blockchain Platform's security and reliability. Now, we are confident that the platform's performance will meet the strict requirements of Fortune Global 500 customers."

Andrey Zhulin, CEO at Insolar

Insolar Blockchain Platform is a DLT solution that enables enterprises to build and run dApps – decentralized business applications. These applications kick off new performance levels and transparency for crucial transactional business workflows such as supply chain management, production management, and electric utilities value chains. A modular structure and preconfigured networks reduce development cycles and do not require specialized in-house blockchain professionals.

It is still Day 1 of the enterprise blockchain era. In-house development is extremely complex and costly. The most advanced market players prefer to use blockchain or DLT platforms. They build out their business logic and applications on top of external resources. This in turn, drives the commercial adoption of these new technologies.

Andrey Zhulin, CEO at Insolar explains: "Every blockchain is characterized by a consensus algorithm, which is an effective and secure method to ensure the correctness of the data recorded and to protect it from fraud and manipulation."

Insolar presents a DLT platform with an innovative approach to the formation of consensus mechanisms.

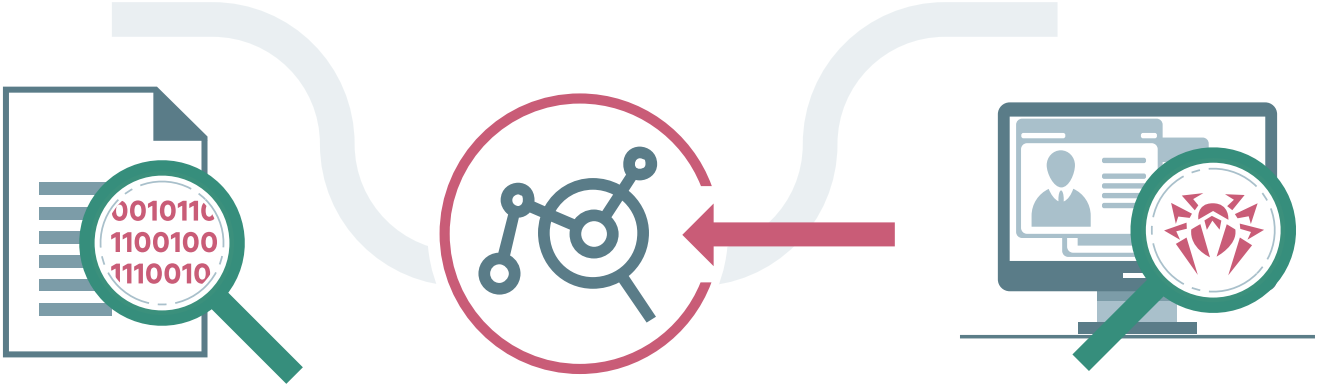
"Insolar Blockchain Platform separates consensus into two layers: network and business," Andrey continues. "Such an approach enables flexible business logic implementation using standard components, in addition to providing an adjustable algorithm for validating transactions."

"The solution focuses on business needs and provides flexibility for each data operation. Our approach is based on separating network consensus (when nodes agree on the work state using a BFT-like protocol) from business logic to create a risk versus value balance for enterprise customers. A so-called Dynamic Consensus protocol flexibly manages numbers of validators and validation algorithms," Andrey explains.

Significant advances in regulatory compliance, enhanced validation for the most valuable transactions, and interoperability with other blockchains for better data management set the Insolar solution apart from existing blockchain offerings for business.

"Designed as a hybrid system, Insolar allows customers to choose between using either just a public blockchain, just a private blockchain or hybridizing them. In order to simplify development and reduce time-to-market, Insolar customers and partners can take advantage of preconfigured networks, prefabricated elements and tools, built-in smart contracts and other components for quick development of decentralized applications for their business," the CEO of Insolar added.

Blockchain Application Security Assessment



“When it comes to decentralized applications for business, the attacks associated with them point to privileged users or insiders. Security assessments help prevent possible insider threats for future platform users. Insolar demonstrated a security attitude that proves their security promise to customers and partners is serious. This practice is worth noting and replicating.”

Pavel Pokrovsky, Blockchain Security Group Manager at Kaspersky

ASSURANCE
Kaspersky Application Security Assessment is a value-add element of a security strategy designed to reassure businesses and customers alike

SECURITY
Applying security measures to individual components safeguards the overall solution from security breaches

RELIABILITY
Application security assessments mitigate the risks of platform failure caused by incorrect logic or code errors

Challenge

Blockchain ensures record immutability but does not guarantee immunity to cyberthreats. If attackers decide to target an enterprise blockchain, the consequences can be dramatic for the network’s participants. Disruptions to supplies, manufacturing and maintenance, and other adverse effects can threaten businesses, as well as consumer convenience and safety. Attacks against a blockchain are most likely to succeed when directed at the supporting applications and infrastructure.

“One of the key advantages of Insolar Blockchain Platform for our customers is the security of their data and processes when managed through Insolar-based applications,” noted Andrey Zhulin. “We evaluate user data security from two aspects: regulatory compliance and protection from leakage. We implement security controls throughout the development process and while setting up the infrastructure for the network.

In order to systematically analyze the security risks associated with applications, we identified a need to invite independent cybersecurity experts with considerable experience in the application security assessment field.”

Solution

“We appointed the Kaspersky team to assess the security of the wallet application and its ecosystem,” Andrey Zhulin went on to say. “We based our choice on a comparison of information security vendor offerings. Kaspersky’s global recognition and reputation made it our first choice. We were also pleased to find that the price met our budgetary expectations”.

The security assessment included several steps: code review, a network

penetration test and a web application penetration test. The assessment uncovered an issue that impacted network infrastructure availability. This issue was swiftly resolved under the guidance of Kaspersky's expert team.

"We engaged Kaspersky, an independent, best-in-class cybersecurity expert, to evaluate our code during the final stages of development. Together, we uncovered and resolved issues that might have affected Insolar Blockchain Platform's security and reliability. Now, we are confident that the platform's performance will meet the strict requirements of Fortune Global 500 customers," concluded Andrey Zhulin.

"When it comes to decentralized applications for business, the attacks associated with them point to privileged users or insiders. According to an OpinionMatter survey, 95% of IT leaders acknowledged that insider security threats are a danger for their organization," points out Pavel Pokrovsky, Blockchain Security Group Manager at Kaspersky. "Insider refers not only to malicious internal actors actively seeking to do harm but also to internal victims of phishing attacks who become gateways for external threat actors. Security assessments help prevent possible insider threats for future platform users."

Good practices are worth keeping

"Insolar demonstrated a security attitude that proves their security promise to customers and partners is serious. This practice is worth noting and replicating," underlined Pavel Pokrovsky.

"Vulnerabilities can appear during the application lifecycle, software updates or insecure re-configuration. Interruption of platform availability is not the only possible outcome. Code errors or design flaws can expose businesses to attacks such as: syphoning of confidential data, tampering with data or systems or fraudulent activities.

Every application that works on top of a blockchain network should be subject to security assessments as well as penetration testing. Of course, conventional security controls should not be ignored either.

These next-generation technologies are going to revolutionize business workflows in the coming years. The blockchain itself is immutable and tamperproof, but the applications that leverage the network pose challenges at every level. We strongly recommend assessing solutions built around blockchain technologies to mitigate cyber-risks and ensure that all necessary security measures are in place," concluded Pavel Pokrovsky.