How to boost business with a blockchain securely

2019

Enterprise Blockchain Security

kaspersky

Learn more at kaspersky.com
#kasperskyblockchain

Getting blockchained? Great!

Enterprise Blockchain Landscape
There are three key points of vulnerability that can be exploited to gain unauthorized access to data, conduct unverified transactions, or penetrate a corporate network: blockchain applications, smart contracts and the network infrastructure. Blockchain applications are used to access data on a blockchain. Besides certain business functionality, they must also provide strong user authentication and authorization features.

Source: IDC Worldwide Blockchain 2018-22 Forecast

A blockchain, or distributed ledger technology (DLT), provides a number of unique benefits that are extremely useful for business processes in enterprises:

- **Resilience to fraudulent data manipulation**
- **Trusted infrastructure for business transactions**
- **Easy and efficient data auditing**

Major Fortune 500 companies, from retail and finance to manufacturing and airlines, are exploring blockchain technology for its benefits in business operations and security. Blockchain technology helps companies reduce costs, streamline business processes, improve product and customer data tracking and security and reduce instances of fraud and counterfeiting. For example, blockchain technology reduces indirect costs in supply chain processes, makes financial processes easy to audit and less costly, and improves trust in public registries (e.g. medical records).

So, blockchain technology appears to be an efficient and secure way to implement sensitive business processes.

Feeling truly safe now? – Not really...

To reap the benefits of blockchain technology, companies need to introduce new software applications as well as new IT infrastructure – servers, databases, network connections, etc. And this is where risks can appear.

Smart contracts (aka chaincode) are sets of business logic implemented in a programmatic form. Smart contracts 'trigger' a business transaction if the required business conditions (also recorded on the blockchain) are met. For example, parties can agree on the delivery of goods and services, or specific terms upon which funds can be automatically released or penalty charges applied. Smart contracts must act as documented, behave deterministically and contain no undeclared functions.

There are blockchain-specific aspects to the development of both applications and smart contracts that a developer must take into account, and which may also be subject to malicious manipulations.

- For example, take retail companies looking to track goods from vendor to customer. This implies using chaincode and multiple network connections from parties beyond a single corporate network. In such a structure, the integrity and business logic of the chaincode and security of the participating nodes will be of key importance for the reliable operation of the entire process and the trustful results it produces.
  a. Errors in the chaincode can lead to non-deterministic behavior of nodes and to data being completely discredited.
  b. Security flaws in network infrastructure can be exploited by advanced persistent threats (APTs) in order to drain sensitive commercial data.
- Shipping companies seek to employ blockchain technology to make their supply chain management systems more transparent and trusted. As part of the process, they actively use smart contracts and blockchain applications, operating on a distributed network.
  c. Unauthorized access to data via the blockchain applications may result in data manipulations and compromise several entities.
  d. Non-deterministic behavior of the smart contracts will produce inconsistent results in the business process.
  e. Endpoint security flaws can make the corporate networks of the participating parties vulnerable to attacks.
- Financial organizations see DLT as a means to reduce transaction costs, onboard crypto-backed customers and improve transparency and auditability. They actively pursue R&D and strive to get maximum use of blockchain benefits. In the desire to make the most of the technology, it's crucial to implement every piece of the ecosystem in a secure way.
  f. Insufficient user authentication in blockchain applications may lead to unauthorized financial transactions.
  g. Errors or malicious manipulations in the chaincode may cause incoherent behavior of nodes and unpredictable results, while misconfiguration may lead to data manipulation and unapproved transactions.

The biggest issue with blockchain-based processes is that once launched, they are very difficult to amend if there are any operational problems. That's why it's critically important to comprehensively test your blockchain solution with a trusted auditor.

The Kaspersky Enterprise Blockchain Security service

Kaspersky has developed the Enterprise Blockchain Security service to mitigate the risks of attacks on blockchain applications, smart contracts and blockchain infrastructure.

Blockchain Application Security Assessment

Kaspersky's acknowledged, top-grade expertise in cryptography and reverse engineering are crucial for trusted in-depth analysis. A successful security audit report is confirmation that the MVP/concept of project is safe. The Security Assessment helps in getting approval for project implementation. The service includes a comprehensive audit of application source code, a database (e.g. CouchDB) audit, a message broker (e.g. Kafka) audit and black/grey box testing.

Chaincode Audit

A successful chaincode audit confirms the blockchain business logic behaves as documented and has no known vulnerabilities or undeclared features. This is important for successful implementation and future operation of the system.

Endpoint Protection

Kaspersky's endpoint protection solution secures the entire system at the device level. The service functionality, including Host Intrusion Prevention, cloud-enabled anomaly detection, as well as web, device and application controls, reduces your attack surface and helps keep corporate resources under control, even outside your IT perimeter.

An Application Security Assessment is performed by Kaspersky experts who provide security services to such major vendors as Oracle, Google, Apple, Facebook, PayPal and others. The assessment is performed manually, following the 'four-eyes principle' and in strict adherence to international standards and best practices, including:

- Web Application Security Consortium (WASC) Threat Classification
- Open Web Application Security Project (OWASP) Testing Guide

During the Chaincode Audit we ensure that the chaincode:

- Does not have undeclared features.
- Does not have known vulnerabilities.
- Documentation and code comments match logic and behavior.
- Complies with business logic requirements, matches initial values, etc.
- Implements and adheres to the existing chaincode interfaces.
- Follows best practices.

Our team of experts review the source code line-by-line, documenting any issues they discover.

The Kaspersky Enterprise Blockchain team has deep, practical knowledge of the field that covers different platforms, programming languages, cryptography, reverse engineering frameworks, vulnerabilities and attack methods.

How it works

NDA

Under a service agreement with strict NDA conditions

Code

Customer provides Kaspersky with the source code of the application/chaincode

List of vulnerabilities

Analytical report is created based on audit results, with a list of vulnerabilities and recommendations on how to fix them

Modifications

After amendments are made, Kaspersky can re-audit the application and chaincode

Stamp of protection

Put the Kaspersky logo on your corporate website as proof your business is secure

Key service advantages:

- Kaspersky Enterprise Blockchain Security is designed specifically for private blockchain needs
- Our comprehensive service guarantees flawless operation of applications, smart contracts and network infrastructure
- Security audit report and recommendations from Kaspersky's world-renowned experts in the information security field
- 24/7 premium support available.

Blockchain technology in a nutshell

A blockchain, or distributed ledger technology (DLT), creates a decentralized, immutable ledger of records. If data has been stored on it, it cannot be subsequently changed or deleted. In DLT, a database is duplicated on all the participants' computers; there is no central database server.

The writing of data on a blockchain is called a 'transaction'. All transactions add some data to a blockchain and are accessible by all participants (provided they have access rights).

Blockchain technology establishes a trusted infrastructure between its participants, removing the need for other trusted intermediaries to conduct transactions.

As there is no central database to hack, blockchain technology provides protection against unauthorized intervention or fraudulent data manipulation.

Blockchain technology facilitates the execution of some business logic by means of smart contracts (aka chaincode). Basically, when the necessary business conditions are met, a smart contract is executed and a programmed transaction is performed.

Blockchains differ by type: public vs private. Each type can be permissionless (anyone can access the blockchain) or permissioned (users are granted special permission to access it).

Private permissioned blockchain platforms are most commonly used as **enterprise blockchains**.

Protect your blockchain infrastructure with Kaspersky Enterprise Blockchain Security

www.kas.pr/dlt

kebs@kaspersky.com

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tommorow.

Know more at kaspersky.com/transparency

Proven.
Transparent.
Independent.