Blockchain Node Risk Management
# Table of Content

<table>
<thead>
<tr>
<th>Key points</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Illustrative data on blockchain node incidents</td>
<td>6</td>
</tr>
<tr>
<td>The Blockchain Node Risk Management solution</td>
<td>9</td>
</tr>
<tr>
<td>Conclusion</td>
<td>12</td>
</tr>
<tr>
<td>Contact Us</td>
<td>13</td>
</tr>
</tbody>
</table>
Blockchain infrastructure opens a wide attack surface for anyone who wants to abuse the trust between distributed ledger applications.

Ensuring the security of blockchain nodes using traditional approaches is often time-consuming and resource-intensive without providing adequate guarantees.

Blockchain infrastructure security falls apart from modern agile development and IT operation frameworks.

The risks associated with node compromise are unacceptably high and have the potential to devastate a business.

Blockchain security competencies are rare, cooperation between different parts of enterprise on blockchain security is complicated.

Implementation of “zero trust” model is painful or unfeasible for the blockchain enterprise architecture in most cases.

Blockchain node security posture ensures effective and efficient protection of blockchain infrastructure. It enables organizations for “zero trust”, DevSecOps, Infrastructure as a Code/GitOps operations style, cooperation between IT, IS, Risk and Audit departments on blockchain security.
Introduction

The last decade has seen a remarkable evolution of blockchain technologies, transitioning from its roots in cryptocurrency supported by a small community of computer enthusiasts to encompassing sophisticated enterprise contracts, DLT applications, and layer two protocols. This enabled organizations to quickly share digital assets, make united decisions and protect them from being tampered with. Blockchain and Cloud, AI, and IoT technologies make innovative products possible and open new markets.

At the core of this complex system is the blockchain node software. It does the following primary tasks:

- establishes communications with other nodes (often called peers);
- keeps track of past transactions in the local database;
- makes an agreement with the rest of the world about the state of this database;
- executes scripts embedded inside trades;
- provides the interface for software on upper layers (wallets, oracles, etc.).

The public and accessible nature of the blockchain infrastructure opens a wide attack surface for anyone who wants to abuse the trust between DLT applications. Nearly everyone with a minimum skill can send the transaction, attempt to invoke a smart contract function, or apply resources to affect the consensus algorithms. While each architecture layer has its own threats and security controls, we must recognize the value of the lowest peer-to-peer layer (p2p) implemented in the node software. A malicious attacker can cause significant damage by exploiting node-related weaknesses.
Like any other software, managing blockchain nodes demands specialized expertise and effort. This knowledge is often concentrated within the IT department, with only a few individuals possessing a comprehensive understanding of the risks and requirements involved. Negligence can rapidly compromise the availability, performance, and integrity of a node, potentially jeopardizing the entire business within hours. As the industry expands, it becomes increasingly important for other organizational stakeholders, such as security specialists, risk managers, and auditors, to pay greater attention to blockchain infrastructure.

These stakeholders need a simple and efficient way to evaluate the state of blockchain nodes and report their findings to upper management. However, in many cases, this is unachievable without cultivating blockchain expertise in other departments. This approach can consume valuable time and organizational resources, as the expertise outside the IT department might be utilized only sporadically throughout the year, making it an impractical allocation of security, risk, and auditor labor.

Often assurance engagements could be more effective and efficient as they require many manual tasks to collect the node status and configuration, verify it against best practices, raise the findings in front of IT, wait for the remediation, and loop through the verification phase again. The broad involvement of high-profile specialists in such routine tasks can lead to demotivation and unsatisfactory results. It distracts the work of blockchain administrators as well, as they need to break away from their main responsibilities and assist the assurance team.

But not only that, but effective verification against best practices also concerns the blockchain pioneering organizations. The concept of “zero trust” already lies in their security strategies. The nodes and any system interacting with them need continuous validation from the cooperative party. The traditional security model of implicit trust is too risky, as an attacker with the ability to compromise one node gains unrestricted capabilities to attack other participants of the blockchain. While the requirement for zero trust is clear and well documented even in the national security standards (e.g., NIST), the material solution is still an open question, and the irregularity in the application of security measures continues to preserve.

These stakeholders need a simple and efficient way to evaluate the state of blockchain nodes and report their findings to upper management. However, in many cases, this is unachievable without cultivating blockchain expertise in other departments. This approach can consume valuable time and organizational resources, as the expertise outside the IT department might be utilized only sporadically throughout the year, making it an impractical allocation of security, risk, and auditor labor.

To paint a more accurate picture, it is essential to consider the overall immaturity of security tools and their insufficient customization for blockchain P2P security needs. Conventional servers and workstations typically have monitoring agents installed to detect malicious activity. However, blockchain node administrators are often hesitant to install additional software for two main reasons: potential performance impacts and the risk of introducing untested, incompatible changes that could jeopardize the availability and integrity of the blockchain database.

As a result, the core of crypto technology infrastructure, which demands the highest level of protection, faces a significant deficiency in logical and administrative controls.

Building a Resilient Blockchain Ecosystem: The Role of Security Specialists, Risk Managers, and Auditors.


Illustrative data on blockchain node incidents

To support our perspective, we can highlight several notable incidents and their consequences related to blockchain node compromises, including one of the largest hacks in history. On March 29, 2022, Axie Infinity’s Ronin Network reported in a blog post that it lost approximately $615 million in USDC (a U.S. dollar-pegged stablecoin) and Ethereum. Axie Infinity is a popular blockchain game that allows users to earn money as they play. The attack took place on March 23, when the perpetrators exploited hacked private keys to create fraudulent withdrawals, according to the blog post. It also mentioned that other key validator nodes were compromised.

READ MORE »
Another impressive incident related to the validation node compromise is a $100M hack of the Harmony Bridge. The attacker took advantage of the low number of validator node verification requirements and used two validator nodes to steal millions of dollars in assets.
According to Web3 Hack Statistics, the total amount of money hacked during 2022.

$3.32B

Number of hacks

376
The Blockchain Node Risk Management solution

Our blockchain risk management solution addresses the issues described above:

- High risks for publicly facing nodes.
- Ineffective assurance process.
- Inability to integrate blockchain infrastructure into enterprise security architecture.
- The lack of proper asset and configuration management.
- Weak cooperation between different enterprise units in the area of blockchain security.
We aim to address the needs of various organizational stakeholders by incorporating the following principles:

**Blockchain-native architecture**

We interact with your organization’s nodes in the same way as all other peer nodes. By doing so, we eliminate risks associated with agent-based security architectures that could impact node performance or stability. By emulating the blockchain node protocol, we can observe low-level details of its behavior and report any deviations and associated threats. This native architecture allows us to inherit blockchain scalability and minimize integration efforts. With our solution, you can quickly gain unprecedented insights into your nodes with just one click!

**Cloud and container-friendly approach**

For those who prefer a seamless experience, our cloud integration supports all popular providers and container orchestrators. You can easily grant our cloud tool access to inventory and discover all blockchain nodes in your tenant through a straightforward workflow. Continuous cloud monitoring will notify you about the appearance of new nodes and automatically run a predefined integration script to onboard them.
Automated administrative workflows and runbooks within our portal

You can use one of our standard processes for asset, configuration, incident, change, problem, vulnerability, and risk management or customize them to fit your existing IT and IS management framework. Auditors, IT managers, security specialists, administrators, business owners, and even third-party vendors can collaborate efficiently through our solution. Achieving compliance with ISO27001, HIPAA, COPPA, and SOC has never been easier in this area than with our innovative solution.

DevOps-enabling APIs

In today's IT landscape, where many organizations are adopting Infrastructure as Code (IaC) or GitOps-style operational models, any solution must be capable of participating in these processes. Our tool offers extensive APIs that allow you to fine-tune every aspect of its functionality or provide node security data to any consumer. To make life easier for DevOps specialists, we will publish a comprehensive set of SDKs, plugins, and providers for major IaC frameworks. Onboarding a security tool for management has never been simpler, thanks to a text file.

Built for SOAR (Security Orchestration, Automation, and Response) and “zero trust”

Enterprise security teams often use a wide variety of tools, such as SIEM, access policy brokers, threat intelligence, log management, PKI (Public Key Infrastructure), and many others. Integrating a new system for seamless collaboration within the SOAR ensemble typically requires significant effort, which can sometimes overshadow the benefits of risk mitigation. We’ve designed our solution with enterprise security architecture in mind, offering software hooks and guidance for quick integration with existing security tools and processes.
Conclusion

Blockchain technologies have transformed and will continue to revolutionize how organizations conduct digital business and address security concerns. These technologies enable the exchange and transformation of digital assets, with the P2P layer and blockchain node software at the core of this capability. While numerous approaches exist to secure node environments, our solution offers a simpler, more reliable, and in-depth alternative.

The Blockchain Node Security Posture provides several unique benefits to organizations utilizing distributed ledger technology (DLT) applications:

- Enhanced protection by eliminating uncertainty and revealing critical vulnerabilities associated with blockchain node software.
- Cost and time savings through automated administrative processes, cloud-native functionality, seamless integration with SOAR and „zero trust“ tools, as well as support for Infrastructure as Code (IaC) and GitOps-style operations.
- Increased maturity and improved collaboration between IT, information security, risk management, vendor management, audit, and business owner representatives.
- Faster time to market blockchain products, as the time for making security decisions drastically decreases.
- Easier compliance for key regulations and management frameworks with our standard templates and workflows.

With the Blockchain Node Security Posture, organizations can more efficiently and effectively protect their blockchain node environments.
Upgrade your blockchain security today!
Try our Blockchain Node Security Posture solution
and unlock a new level of protection.

GET STARTED WITH A SCHEDULED DEMO

Contact Us

Calendly
calendly.com/itrustinc

Email Address
Sales@iTrustInc.com

LinkedIn
linkedin.com/company/itrust-inc

Website
iTrustInc.com