BlocWatch

THE IMPORTANCE OF BLOCKCHAIN MONITORING

MONITOR | ANALYZE | VALIDATE | SECURE

Distributed Ledger Technology (DLT) and blockchain is bringing countless opportunities to businesses around the globe. Public, private, and permissioned blockchains provide organizations with new ways to manage their supply chains, contracts, payments, identity, and resources. In fact, Gartner research predicts that blockchain will support the annual global movement and tracking of $2 trillion of goods and services by 2023.

The driving force behind this revolution is the realization that blockchain brings organizations greater transparency and security, all while reducing costs and increasing the speed of doing business. However, as with all new technologies, there are risks that accompany these new opportunities. Specifically, as adopters place more and more of the valuable business processes on blockchain technology, they will also need greater visibility into the systems. They will need assurance around both operational and security metrics as they look to protect their business processes and investments.

This paper discusses key considerations that blockchain adopters should assess and also provides ideas around the critical aspects of monitoring that all users should incorporate into their blockchain environments.

Topics:

1. Identify and mitigate suspicious behavior
2. Receive real-time alerts for critical issues
3. Create and access auditable records
4. Analyze blockchain data and events
5. Ensure the security and health of the blockchain

1. Identify and mitigate suspicious behavior:

Identifying and mitigating suspicious behavior should be the first job for blockchain teams. Large implementations encompass millions or even billions of dollars in transactions in a single day. Plainly, tracking these transactions and ensuring their validity is not an option, it is a business necessity.

And, although blockchain technology is designed to provide secure transactions with an immutable record, there are still a number of ways that network security and policy violations could occur. Hackers are still going to attack enterprise chains. Endpoints and nodes within the chain still remain vulnerable. When thinking about these issues, users should retain visibility into activity and pay specific attention to events such as:

- Increases in failed transactions
- Changes to access controls and permissions
- Multiple failed login attempts
- Unauthorized new users
- Sudden spikes or drops in transaction volume
- Transaction times that fall outside of normal business hours

These are the types of events that warrant greater attention. Of course, not all will be malicious, but having a systematic process to identify and investigate each should be built into every implementation.

2. Receive real-time alerts for critical issues:

Blockchain creates trust, but a single bad actor can break that confidence. Given the complexity of systems and volume of transactions, it could be days, weeks, or months before an anomaly is detected and resolved. Security researchers have shown that single breaches often result in millions of dollars of cost, and breaches become more expensive and create more disruption the longer that they persist.

Ideally, the implementation will incorporate automated alerting to help mitigate this risk. Again, we all know that even systems with "the best" security get hacked. Therefore, blockchain administrators should look to build multiple layers of security along with automated fail safes.

3. Create and access auditable records:

In the event of an audit, raw blockchain data can be difficult to understand. Auditors need to know what information is important, and businesses want the issue resolved in a timely and cost-effective manner.

BlocWatch creates a record that an auditor can understand. This third-party tool collects transaction data in a way that ensures privacy is protected. You have the power to choose what data is collected and determine which information is most important to your chain health. This record saves time and significantly reduces the costs associated with the audit.

4. Analyze blockchain data and events:

It would be impossible to keep up with all blockchain activity at all times. You need an at-a-glance view of vital statistics so that you get the full picture of what's happening.

Monitoring a blockchain means that you need a comprehensive view of transaction volume, contract usage, validation speeds, and overall chain health. The streamlined BlocWatch dashboard brings you actionable insights so that you can see transactions in real-time, view alerts, and take action where needed.

5. Ensure the security and health of the blockchain:

In a PwC survey of global organizations, 84% of executives said that their companies are "actively involved" with blockchain technology to some degree.

Blockchain adoption is a promising solution for businesses of all kinds, but it also represents a significant investment.

BlocWatch provides you with tools to monitor blockchain performance and ensure chain health. The out-of-the-box dashboards and reports enable you to investigate and diagnose issues related to asset inventory, contract usage, transaction volume, validation speeds, node health, and more. Additional tools from BlocWatch allow you to verify and endorse blockchain transactions to provide assurance to all blockchain participants of the accuracy and legitimacy of endorsed transactions.

BlocWatch helps you take the guesswork out of managing your blockchain network. Comprehensive monitoring services enable you to manage both public and private blockchains. The application leverages machine learning to identify suspicious activity, monitor transactions, and track smart contract performance across both cloud and on-premise environments.

Contact the Experts at BlocWatch

Visit www.blocwatch.com to schedule a live demo with our experts and we will demonstrate how BlocWatch can bring your blockchain platform to the next level.

CLICK HERE TO SCHEDULE A DEMO

BLOCWATCH