Vendor Vignette

Splunk for Blockchain

Founded 2003 | HQ San Francisco, CA | 6,000 employees (approx.) | $2.36B revenue (2019)

Splunk's move in the blockchain arena is important because – though core blockchains themselves are highly secure – today there is little visibility into the infrastructure and broader operating environments running blockchain networks. Splunk offers an alternative to this opaqueness and, as far as we know, the first true blockchain monitoring system on the market.

The Company

Splunk was co-founded by Michael Baum, Robert Das, and Erik Swan in 2003 and is headquartered in San Francisco. The current CEO is Doug Merritt. After raising $40 million over three rounds of investment, the company IPO'd on the NASDAQ (SPLK) in 2012 and has made 16 acquisitions over the years. With revenues of $2.36 billion for 2019, Splunk continued to grow in 2020.

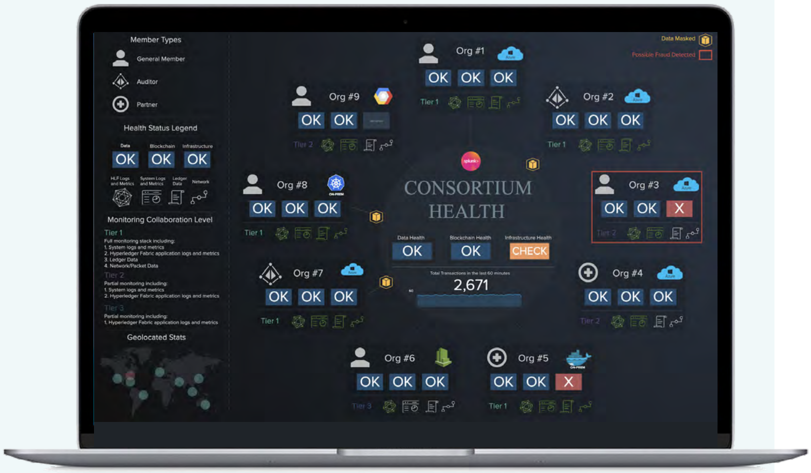
Splunk is best known for its machine data analysis tools; indeed, it is one of the few firms that specialize in making machine level data accessible and is widely used for application management, security, and data analytics. In 2020, Splunk quietly released enhancements to support enterprise blockchains and provide the same level of insight to blockchain networks as it does to more common enterprise application infrastructures. This capability, Splunk for Blockchain, is the focus of this report.

The Technology

To understand Splunk's blockchain story, it's important to understand what Splunk as a whole does. In simple terms, Splunk provides IT system security threat detection and monitoring and application performance monitoring for both on-premises operational systems and cloud native applications running on modern architectures. These are systems that collect, index, search, and translate all the machine data and log files that run across your network – be they on premises, in the cloud, or hybrid – thus providing a single location to analyze, read, and act upon the information. In slightly more technical terms, what Splunk does is to capture and index big data, then coordinate and correlate it into a user interface/dashboard that can generate reports, trigger alerts, and create data visualizations. These are used to keep core systems running, predict potential issues before they occur, and improve the security and risk postures in managing business-critical applications.

Splunk's entry into the blockchain market, then, is not through building blockchains but through doing what it does best, providing real-time or near-real-time visibility (observability) into the underlying mechanisms and infrastructure that blockchains run upon. All blockchains by default are multi-party systems, with multiple nodes (tens or even thousands) running distributed ledgers. This means that there will be a lot of often diverse infrastructure to support those ledger activities. The Splunk for Blockchain platform provides a unified environment to observe, monitor, and analyze all the data across the distributed stack: in short, an extension of what it already does in non-blockchain environments.

Figure 1
Splunk for Blockchain Unified Interface



Tier 1
Full monitoring stack including:
1. System logs and metrics
2. Hyperledger Fabric application logs and metrics
3. Ledger Data
4. Network/Packet Data

Tier 2
Partial monitoring including:
1. System logs and metrics
2. Hyperledger Fabric application logs and metrics

Tier 3
Partial monitoring including:
1. Hyperledger Fabric application logs and metrics

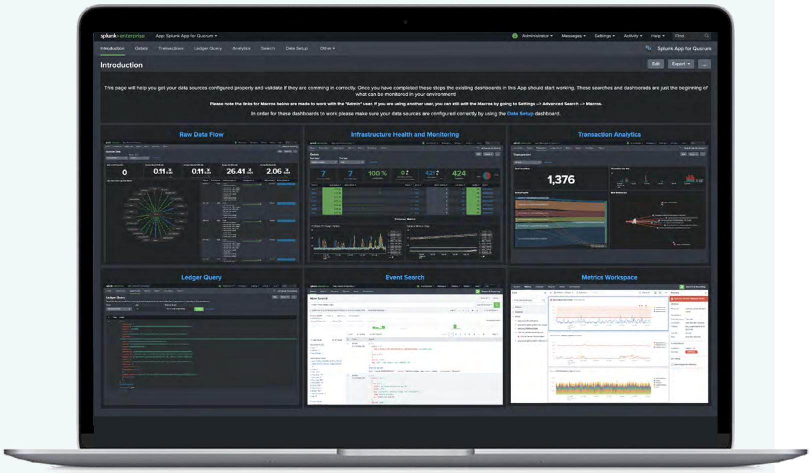
When we think about blockchain data, it is natural to think about hashes stored on the blockchain along with some associated metadata. But the infrastructure running the blockchain itself also generates a lot of machine data. Splunk for Blockchain brings all this blockchain and network data together in one place so that the business, IT ops, or security can observe what is happening across the network and respond to any changes, irregularities, or breaches (see Figure 1). In other words, Splunk for Blockchain provides a unified interface that shows and provides access to everything from blockchain node performance to security protocols across a consortium's entire infrastructure. It provides full observability in one place of the blockchain network's data across multi-party systems, be it on premises, running differing security protocols, running in the cloud, in a container, or on an aging server. This is laudable and a great first step. Though this may seem like an obvious requirement, it should be noted that very few blockchains today are able to provide this level of monitoring; in fact, it is the Achilles heel of many enterprise blockchain implementations.

Enterprise blockchains are by their nature multi-party systems. Even within a single consortium, some members may be running managed services while others run their own nodes, multiple containers, and servers on premises or in third-party cloud systems. In practical terms, this means multiple different components, speeds, tolerances, security protocols, and structures are in play. In terms of monitoring, at best each member will have its own logging and monitoring system. They know what is happening on their system, their node, their copy of the ledger, but have very limited visibility, or no visibility at all, into the blockchain's overall state of health. It's a single, though distributed, ledger running across multiple closed silos. That's problematic enough, but when, for example, smart contracts are deployed to add consensus-driven automation and decision-making to the blockchain, the complexity increases.

To be clear, Splunk for Blockchain does not offer a means for interoperability across blockchains. What it offers is the means to drill down into exactly what is happening, when and where, across a blockchain or even across different blockchains. For example, you can search for a particular hash and see where it is running on different blockchains, including layer 2. You can drill down when something goes wrong and see exactly what happened, where, and why, so that it can be remedied. Again, this may seem like an obvious requirement, but most blockchains today cannot do such troubleshooting quickly and accurately.

In summary, Splunk for Blockchain provides a monitoring system for enterprise blockchains with optimized connectors and an interface to show what is running across the entire network, and specifically what each element is currently doing. It's a unified system that can be used by IT operations management and security – those responsible for keeping the network and all the nodes running. It's a system that has been optimized for blockchains specifically, to give full end-to-end observability through indexing chain events. In practical terms, this means that when a node falls over, fails to connect, or has been compromised, that is visible in real time. Without Splunk for Blockchain (or another similar system), only the owner of that node would have that information. With Splunk for Blockchain, you centralize the management and monitoring of the network and can share that capability (if you want to) securely across all of the participants, thus providing the means to stabilize and manage often unstable and unpredictable complex blockchain environments.

Figure 2
Splunk for Blockchain Monitoring System



Introduction

This page will help you get your data sources configured properly and validate if they are comming in correctly. Once you have completed these steps the existing dashboards in this App should start working. These searches and dashborads are just the beginning of what can be monitored in your environment!

Please note the links for Macros below are made to work with the "Admin" user. If you are using another user, you can still edit the Macros by going to Settings --> Advanced Search --> Macros.

In order for these dashboards to work please make sure your data sources are configured correctly by using the Data Setup dashboard.

Splunk for Blockchain is relatively new to the market and is a blockchain-agnostic Version 1 system, a core foundational monitoring system. We expect further enhancements and features to be added throughout 2021 as it is deployed more widely and Splunk receives feedback from users regarding their priorities and needs.

Our Opinion

Splunk's move in the blockchain arena is important because, though core blockchains themselves are highly secure, today there is little visibility into the infrastructure and broader operating environments running blockchain networks. To be clear, most enterprise blockchains are secure and able to scale effectively, but stability is an ongoing concern, particularly as these networks run across patchwork quilts of infrastructure components. As of today, as long as the network is running (bear in mind it has a lot of tolerance, as it is distributed) little attention is given to how it is truly performing. But as enterprise blockchains roll out in earnest, that will no longer work. Splunk for Blockchain offers an alternative to this opaqueness and, as far as we know, the first true blockchain monitoring system on the market.

Advice to Buyers

The focus of enterprise blockchain builders has naturally been on securing and optimizing the blockchain itself. However, no matter how efficiently you secure the ledger, it runs on a much broader system into which you have little or no unified visibility. If a transaction fails, most times you will not know why. As enterprise blockchain gains momentum, this will have to be addressed and the need to orchestrate and have secure and layered (permissioned) visibility into the entire network will become critical. At the time of writing, to the best of our knowledge Splunk is the only provider of a service offering this visibility and monitoring. Therefore, whether you are a consortium or blockchain service provider you will want to look at Splunk for Blockchain as a way to manage and provide stability to your blockchain.

SOAR Analysis

Strengths

- Deep expertise in system monitoring
- High brand awareness and industry credibility

Aspirations

- Become the *de facto* system monitor for enterprise blockchain
- Add further layers of depth and breadth to its blockchain monitoring system

Opportunities

- Partner with consortiums in building out networks
- Partner with blockchain vendors and service providers

Results

- First to market blockchain monitoring system
- Multiple early deployments

About Deep Analysis

Deep Analysis is an advisory firm that helps organizations understand and address the challenges of innovative and disruptive technologies in the enterprise software marketplace.

Its work is built on decades of experience in advising and consulting to global technology firms large and small, from SAP, Oracle, and HP to countless start-ups.

Led by Alan Pelz-Sharpe, the firm focuses on Information Management and the business application of Cloud, Artificial Intelligence, and Blockchain. Deep Analysis recently published the book "Practical Artificial Intelligence: An Enterprise Playbook," co-authored by Alan and Kashyap Kompella, outlining strategies for organizations to avoid pitfalls and successfully deploy AI.

Deep Analysis works with technology vendors to improve their understanding and provide actionable guidance on current and future market opportunities.

Yet, unlike traditional analyst firms, Deep Analysis takes a buyer-centric approach to its research and understands real-world buyer and market needs versus the “echo chamber” of the technology industry.

Contact us:

info@deep-analysis.net
+1 978 877 7915