HYPERLEDGER FOUNDATION

Case Study:

Splunk correlates data across all datasets—including Hyperledger Fabric

---

Splunk's open-source code helps companies gain visibility into their Hyperledger Fabric infrastructure and ledger data without needing to build custom tools

Goals

- Get to production faster and more securely through a better understanding of data
- Reduce time to resolutions by combining different data
- Gain better observability into siloed data

Large organizations have always struggled to get visibility into their data. Frequently, data comes in many sources and formats while also being siloed across the organization. DLTs add ledger data and metadata to the mix.

Similarly, consortiums need to interoperate with each other. Yet organizations often use disparate tools for logs, metrics and tracing. All these are deployed on different clouds or on-prem. Then they build their own tools to take data from the ledgers and put it into a SQL database. Consortiums may include competitors who don't trust one another, so they don't want to share data. But, if no one shares data, it can be challenging to determine if an organization has a problem or if it lies in the network.

Splunk, a company focused on removing barriers between data and action, has enabled customers to have complete monitoring and observability into their own data by bringing it all into one place, regardless of format.

Splunk is now offering open source solutions allowing the ingestion of ledger data and corresponding metadata while correlating with other data sources. Not only the blocks and transactions but also chaincode events. In a nutshell, Splunk has created a solution that allows any organization to answer any question, from security to observability. This is the launch of a new era in Fabric networks, where silos between organizations, infrastructure providers, and data sources are eliminated.

Evolving to address customer needs on Hyperledger Fabric

Splunk's customers include 92 Fortune 100 companies. Before choosing a blockchain platform, it wanted to know what its customers were already using. And many of them used Hyperledger Fabric.

"The ecosystem of Hyperledger is enterprise-friendly," says Nate McKervey, Head of Blockchain and DLT at Splunk. "It makes sense for Splunk to enable enterprises to turn data into doing when it comes to distributed ledger data, just like Splunk does for other data.

Bringing DLT data in wasn't simple, but, because of Splunk's origins, it wasn't too difficult, either.

Splunk already ingests data without caring about structure, schema, or format. This feature saved the company the trouble of formatting Hyperledger Fabric data before ingestion.

That flexibility allowed developers to send data to Splunk and then figure out what to do with it. "It was really more of a question of what else can we collect besides the ledger data to help our customers ask any question they have," says McKervey.

And to find out those questions, they asked their customers.

Blocks and transaction data allowed users to analyze and correlate that data with other data they had in Splunk. "Our customers said, 'That's great. But we need more than that.

We want chaincode events,'" explains McKervey.

"When metrics were introduced, we needed to get metrics into Splunk. More recently, it's been private data collection," says McKervey.

Initially, the platform focused on uses from an IT perspective. If there are issues, can users drill down and figure out problems with less downtime? The company wanted users to feel confident going into production with Hyperledger Fabric.

Then its focus shifted to security. Customers wanted to know what else they could do to secure their infrastructure. Keeping it up and running was important, but so was making sure nothing would compromise their Hyperledger Fabric environment.

One of those interested customers was S&P Global.

Protecting crucial, powerful data assets

S&P Global delivers data, research, and credit ratings, among other things, to governments, companies, and individuals. Its Ratings division provides independent data and insight to the marketplace.

In 2019 it was entering a new region. S&P took this opportunity to explore modern technologies and new ways of doing business. It decided to build a content management solution from scratch with innovative technology and security.

"Our solution is essentially a blockchain based content management system," explains Mark Wang, Global Head of Cloud Architecture at S&P Global Ratings. S&P securely stores and shares files with different stakeholders. These might be regulators, external entities, and internal users. But this content includes critical and sensitive information. So the solution needed to provide permanency for records, and it needed to protect the security of these crucial, powerful data assets

"As a credit rating agency, we're heavily regulated. We want to be multi-cloud. We need to satisfy regional data localization requirements. And data security is highly critical," Wang says. "We needed a secure solution that's tamper proof and immutable."

For over a decade, S&P had been using Splunk for its infrastructure monitoring. "Everything we deploy has an automation with Splunk," says Wang. At a Splunk conference in 2019, S&P saw the Hyperledger Fabric-based applications Splunk was developing. "We saw enormous potential for some of our emerging use cases," says Wang. "Since we already had the platform, it made perfect sense to leverage it with Hyperledger Fabric."

It also helped that Hyperledger Fabric is a private permission blockchain and is enterprise ready.

S&P could now get user interactions and metadata—like who uploaded documents or modified documents and when. S&P developed applications to retrieve that metadata and present it to the user for document searches. This opened up possibilities for providing an audit trail.

“Say a regulator comes to us and needs a complete audit trail of how a document that impacted the market was generated,” explains Wang. “They need to know who modified it, who saw it, things like that. We can put together all those pieces and connect those dots with the data the logger is capturing from the chain network.”

“The Splunk integration with Hyperledger Fabric lets us see the actual business transaction and be able to index and search that data.”

— Mark Wang, Global Head of Cloud Architecture, Information Technology, *S&P Global Ratings*

S&P uses Splunk for three primary areas. The first is infrastructure monitoring on the operations of different components. The company wants to make sure the system stays healthy and the right teams are alerted if there’s an issue. The second is visibility into the events happening within the blockchain network. And third is business activity monitoring, which includes searching for document metadata.

“That’s where the Splunk integration with Hyperledger Fabric is so helpful,” says Wang. “We can see the actual business transaction and be able to index and search that data.”

Users can access the system through an internet user interface to perform searches. With just a keyword, Splunk looks back at the metadata lists such as document name, version history, and other associated metadata that goes along with that object. Then it pulls back the results.

All of this happens securely, which was one of the biggest reasons S&P invested and built on a blockchain platform.

An additional benefit is that Splunk’s out-of-the-box solution didn’t require S&P to hire developers to create something from scratch. It’s also low maintenance. Because of the automation S&P has built, the company didn’t need to bring on more Splunk engineers.

Partnering improves both platforms—and the Hyperledger Fabric Community

The partnership sped up S&P's use cases, but it also helped Splunk enhance its product.

S&P adopted the latest versions of Hyperledger Fabric, which pushed Splunk to update its codebase to be compatible with it.

"Then we had an AHA moment...imagine if every single company adopting Hyperledger Fabric needed this data? They'd have to go figure out a solution—update their code or add new capabilities. Why not just have one open source solution?" says McKervey.

Splunk is committed to open source as a core contributor to CNCF projects such as OpenTelemetry, contributing to Hyperledger projects, the Baseline protocol, the Enterprise Ethereum Alliance and more. "'Open' is one of our core values," explains McKervey. "We want to be known in the ecosystem as a contributor, not a proprietary closed stack set of solutions."

S&P also contributed code that it had asked for regarding private data collection.

"We had an AHA moment...imagine if every single company adopting Hyperledger Fabric needed this data? They'd have to go figure out a solution—update their code or add new capabilities. Why not just have one open-source solution?"

— Nate McKervey, Head of Blockchain and DLT, *Splunk*

What's next

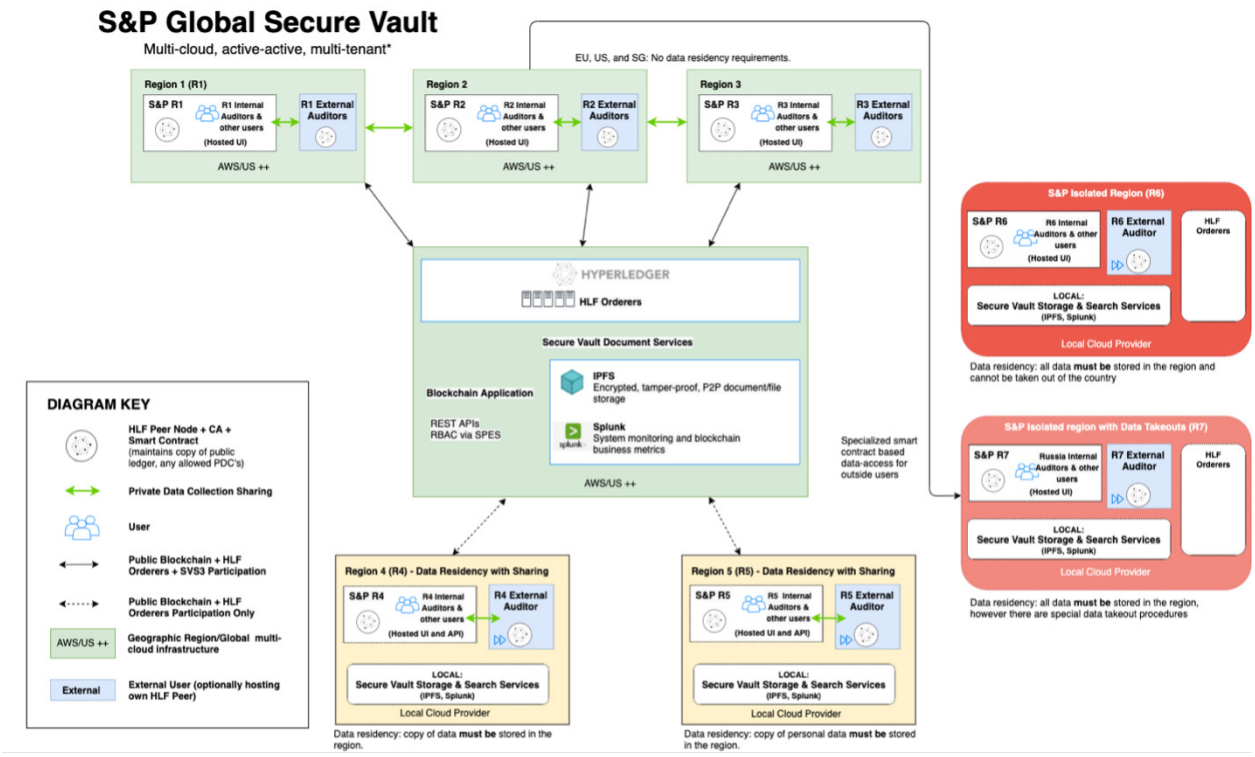
What started out as a regional solution for S&P now promises to be a global solution. "It's multi-cloud, multi-tenant, and secure. It can scale to multiple regions and multiple participants," explains Wang. "We want to make it global and put in other requirements in terms of data retention, data privacy and data localization."

S&P is also improving performance speed, which is slower than they want it to be, especially for write operations. Here, again, Splunk is there to help fine-tune and optimize the system. "We've put in a trace ID so we can see timing," says Wang. "We look at performance tests and benchmarks."

Other areas S&P wants to expand are auditing and security, which will support regulators, internal auditors and business stakeholders.

As for Splunk, it will continue to make it easier for customers to get their logs, metrics, traces, and ledger data all in one place. “We want to help customers turn data into doing as fast as possible,” says McKervey.

System graphic



About Splunk

Splunk is the world's first Data-to-Everything™ Platform designed to remove the barriers between data and action, so that everyone thrives in the Data Age. We're empowering IT, DevOps, and security teams to transform their organizations with data from any source and on any timescale.

With more than 7,500+ employees in 27 offices worldwide, we're building a future where data provides clarity, elevates discussion and accelerates progress for innovators in IT, security, DevOps and more. To learn more, visit https://www.splunk.com/

splunk>

About S&P

For over 160 years, S&P Global has been turning information into insights, providing essential intelligence that accelerates progress in our ever-changing world. We deliver data, research, credit ratings, benchmarks and ESG solutions that governments, companies and individuals depend on to make decisions with conviction.

All over the world, in every corner of the globe, over 23,000 employees are focused on the real-time information that is vital to the world of business. To learn more, visit https://www.spglobal.com/en/

S&P Global

About Hyperledger Foundation

Hyperledger Foundation was founded in 2015 to bring transparency and efficiency to the enterprise market by fostering a thriving ecosystem around open source blockchain software technologies. As a project of the Linux Foundation, Hyperledger Foundation coordinates a community of member and non member organizations, individual contributors and software developers building enterprise-grade platforms, libraries, tools and solutions for multi-party systems using blockchain, distributed ledger, and related technologies. Members include industry-leading organizations in finance, banking, healthcare, supply chains, manufacturing, technology and beyond. All Hyperledger code is built publicly and available under the Apache license. To learn more, visit: https://www.hyperledger.org/

HYPERLEDGER FOUNDATION