Brought to you by Informa Tech

OMDIA

Publication date:
29 Nov 2022
Author:
Rik Turner, Principal Analyst, Emerging Technologies

On the Radar: RKVST offers supply chain trust, anchored in the blockchain

Summary

Catalyst

RKVST offers technology that underpins supply chain integrity, transparency, and trust. Its cloud-based platform, which it delivers in software-as-a-service (SaaS) mode, is anchored in blockchain technology, and establishes the provenance of any asset, with an immutable record of all changes made to it throughout its life. It also enables governance by ensuring that the appropriate data reaches the right destination within an organization, and in a timely fashion.

Omdia view

Supply chain security is a major concern in our globalized economy, so verifiable data on assets in a chain has become vital. And as the world is becoming increasingly digital, knowledge of software supply chains is now critically important from a security perspective.

RKVST plays in both the physical and digital supply chains with its blockchain-based technology, which positions it to benefit from developments in both worlds.

Why put RKVST on your radar?

RKVST is worth including on a list of potential suppliers of services that enable trust and transparency in any type of supply chain. Given its partner-friendly approach to entering new verticals, it should also be on the radar of vendors providing any type of technology for compiling, managing, and exchanging lists of assets for inclusion in an inventory.

Blockchain technology has gained prominence over the last decade thanks to its use in underpinning many cryptocurrencies, particularly Bitcoin, which launched officially in 2009.

It was clear from the outset that the underlying technology had multiple other applications – essentially anywhere that digital trust needed to be established and grounded in immutable data, (a.k.a. a single source of truth). Furthermore, the distributed nature of blockchain meant that no single central authority needed to be trusted to curate the information held on it. Even the operator of a platform could not change any of the data without that change being recorded in the system.

In cybersecurity, the blockchain can underpin identity management

Technology companies have therefore set to finding areas in which to apply blockchain. In the world of digital security, for instance, an obvious area is identity management. With business-to-consumer (B2C) interactions increasingly moving to online channels, the ability to store identity information in an immutable fashion and check against it in every session is clearly of value. Furthermore, with the impact on the workplace of the COVID-19 pandemic driving ever more knowledge workers into the remote working paradigm, even business-to-employee (B2E) connections can benefit from such a tamper-proof identity management capability.

In trade and e-commerce, supply chain management can benefit

While identity management has been the great beneficiary of blockchain in the world of cybersecurity, in the domains of e-commerce and trade finance a natural target for the application of this technology is supply chain management. Global supply chains have become the norm over the last half-century, empowered by an ever-larger fleet of giant container ships and communication networks that can carry ever more data, at ever greater speeds.

However, with the ease of procurement and reduction in costs of globalization have come issues of trust, as the current scandal around child deaths in The Gambia from cough syrup manufactured in India has graphically demonstrated. Even short of such tragic examples, consumer activism in the advanced economies now demands to know whether products from the developing world have been sourced in a sustainable and eco-friendly fashion, and there is a need to guarantee that providers that had a clean bill of environmental health last year, or even last month, continue to meet all the necessary requirements now.

As such, supply chain integrity is in the spotlight as never before, and the need to underpin it with technology that provides an audit trail based on irrefutable evidence has thrown a spotlight on the blockchain as a suitable candidate. The immutable nature of the data held in the blockchain's distributed ledger technology (DLT) makes it a natural contender for this role.

Product/service overview

RKVST is a leading exponent of this blockchain-based approach to the problem of reliable supply chain information, regardless of whether the assets are physical (e.g., building materials) or virtual (such as application code).

Given that the majority of its customers require brownfield rather than greenfield deployments of its technology, RKVST's Zero Trust Fabric enables such organizations to evolve toward a zero-trust architecture for their supply chain management. It does this by augmenting legacy systems with zero-trust features and functionality.

RKVST effectively sets up a safe "bridge" for critical informationto flow between organizations and across boundaries, in a secure and verifiable manner. As such, the vendor argues, it can enable digital transformation and bring efficiency to supply chain operations by promoting data visibility between supply chain partners, while leaving existing private operations alone.

All data flowing through the Zero Trust Fabric is protected with provenance, governance, and immutability, which make it reliable and trustworthy for ingestion into a customer's applications and processes.In addition to the real-time visibility of information from partners, the Zero Trust Fabric maintains a complete tamperproof lifecycle history of all data objects in the system, creating an evidential stream of reliable information for digital operations, fitting in with existing audit and regulatory processes.

Company information

Background

RKVST was founded as Jitsuin in 2018 by its president Krishna Anne, chief product officer Jon Geater, and VP of business development, Rob Brown. Anne was previously CEO of Secure Thingz and led its acquisition by IAR Systems (in early 2018). He has also held executive roles at Rambus, Broadcom, AMD, and MIPS. Geater held senior global technical roles at Thales e-Security, Trustonic, ARM, and nCipher, where he built chip-to-cloud solutions for mobile, IoT, payments, and smart cities. Brown was IoT Marketing Director at Trustonic and, before that, Director of Marketing for the Secure Services Division at ARM.

The company's CEO, who joined a few months after its foundation, is Rusty Cumpston, who was previously a founder and CEO at SWIM.AI and Sensity Systems.

Jitsuin rebranded in March 2022, adopting the name of its flagship platform for blockchain data assurance and sharing. RKVST has raised a total of $13.5m, most recently announcing a $7.5m Series A round led by Ridgeline Partners, with participation by Acadia Woods, Cyber Mentor Fund, and Long Run Capital, in September 2022.

Current position

Given that it can underscore a variety of use cases, a large part of RKVST's go-to-market strategy involves technology partners that take it into quite different applications of its technology. It has a growing ecosystem of partners focused on improving supply chain visibility and security:

- Software Composition Analysis (SCA) tool vendors Bytesafe, Meterian, and SOOS enable developers to automate the publishing of software artifacts for their customers by connecting to RKVST using the tools already in use and enabling business owners to control data privacy.
- Finite State, Netrise, and RevEng can publish software artifacts by reversing software binaries, enabling either a publisher to perform a final verification check on packages or software users to discover what is inside packages.
- Security Orchestration and Automated Response (SOAR) platform Revelstoke can ingest software artifacts from the software supply chain to help security operations centers respond to vulnerabilities.

Additionally, RKVST's API/SDK can be used directly for custom integrations. Example projects include the following:

- For zero-trust IoT access, it integrates with Device Authority for traceability of device software provenance in SBOMs, advanced composition analysis, and IoT risk reduction
- For transparency in carbon offset equivalents in the aviation industry it integrates with SATAVIA

- In nuclear waste handling, it works with Digital Catapult, a UK non-profit focused on advanced digital technologies, and Sellafield Ltd on creating a trusted and secure record for tracking hazardous waste and materials throughout the waste handling lifecycle
- For strong regulatory oversight of “skeleton keys” for electronic door locks in the business access management arena, it partnered with Wavestone.

RKVST has also won awards in various technology challenges, such as the Siemens Global Challenge where they demonstrated a way to transform the industrial drive business so that customers could shift to opex “motion-as-a-service”, where they pay for how much movement is delivered, rather than capex tied up in assets.

RKVST currently has around 180 users registered for its platform, with around 50 that it describes as active. At the moment, the vendor offers its technology in two distinct tiers in a classic freemium model, with the first being RKVST Free and the second RKVST Team, which is subscription based and starts at $499 a month.

The competitive landscape for RKVST’s technology comprises various other platforms, focused on supply chain integrity and based on the blockchain. These can be vertically focused offerings such as TradeLens, Everledger, or the Food Trust platform from IBM, or pure technology enablement offerings such as Circulor, Vendia, or ImmuDB.

Future plans

RKVST will continue with its freemium mode, where customers can start out on the free version of its product and progress to a paid version as they perceive the benefits of the technology and need to apply it to more assets. It now plans to extend its portfolio – first with a high-end offering called RKVST Enterprise, which it describes as a white-glove service, then with an intermediate one called RKVST Business.

The company considers the provision of these multiple service levels to be essential to the delivery of supply chain transparency because they enable both large and small players to contribute to the same “single source of truth.” On the operational/non-functional side, therefore, the RKVST roadmap includes innovations in the delivery of a single platform that can address the needs of enterprise IT departments and small business at the same time.

On the feature/functional side, RKVST maintains a strict focus on solving problems of access to high-integrity digital evidence in cross-border supply chain operations, rooted in assertions and attestations of “who did what, and when.” Future plans include improvements to the quality and granularity of all dimensions of “who did what, and when,” such as more options for strong digital identity and more ways of assessing trustworthy time. Tools for collecting, validating, and verifying this evidence in a clean-room context will also continue to evolve.

Because of RKVST’s partner ecosystem go-to-market strategy, the roadmap also includes a number of interoperability standards that make application integrations easier and more powerful; for example, supply chain integrity, transparency, and trust (SCITT), and associated standards in the Internet Engineering Task Force (IETF).

Key facts

Table 1: Data sheet: RKVST

Product/service name	RKVST Zero Trust Fabric	**Product classification**	Supply chain trust, integrity, and transparency enablement
Version number	Not applicable due to SaaS delivery mode	**Release date**	1: First generation: February 2019 Second generation: March 2020 Third generation: March 2022
Industries covered	All with a supply chain or critical operations focus.	**Geographies covered**	All, but predominantly US and UK
Relevant company sizes	All	**Licensing options**	Freemium Saas or (in rare large user cases) enterprise private deployment.
URL	https://rkvst.com	**Routes to market**	Partner integrations for off-the-shelf; systems integrators for custom projects.
Company headquarters	Silicon Valley, California, US, and Cambridge, UK	**Number of employees**	22 currently, but planning to grow this year

Source: Omdia

Analyst comment

Organizations need reliable information on their supply chains, including the ones they use for software (both their own application development and the third-party software they use across their business, such as SolarWinds). That reliability can be enabled by DLT, so blockchain-based platforms such as those that RKVST develops have a considerable addressable market.

There are already a number of other companies with such technology, including tech heavyweights like IBM and Oracle, but the potential market is so large and diverse that there is almost certainly room for smaller players such as RKVST, particularly given its partner-friendly approach to the development of new use cases for its platform.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Further reading

Supply Chain Regulations (June 2021)

Blockchain's role in IoT: opportunities, use cases, and service provider strategies (July 2020)

Author

Rik Turner, Senior Principal Analyst, Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com