Digital Systems & Technology

DevOps & Blockchain: Powering Rapid Software Delivery in Regulated Environments

As IT organizations push forward with DevOps tools that automate application development and maintenance processes, they can lose sight of the key "who, what, where and when" variables that surround software releases, thus elevating the possibility of noncompliance with a host of regulatory mandates. By embracing blockchain, they can create a tamperproof way of ensuring regulatory compliance while extending their embrace of IT service automation.

Executive Summary

As digital overturns the value propositions of business models across the globe, enterprises need to stay one step ahead of technology's unrelenting progress to remain relevant. Businesses rely on enterprise IT to run business better, and IT teams across the world are embracing DevOps[1] to automate and accelerate application delivery and support.

The global DevOps platform market is expected to grow at a CAGR of 22.5%, reaching a total value of approximately $12.9 billion by 2024, according to researcher Ameri Research.[2] Regulated industries such as banking and financial services, as well as healthcare and life sciences, account for more than 50% of the projected DevOps market. These industries have

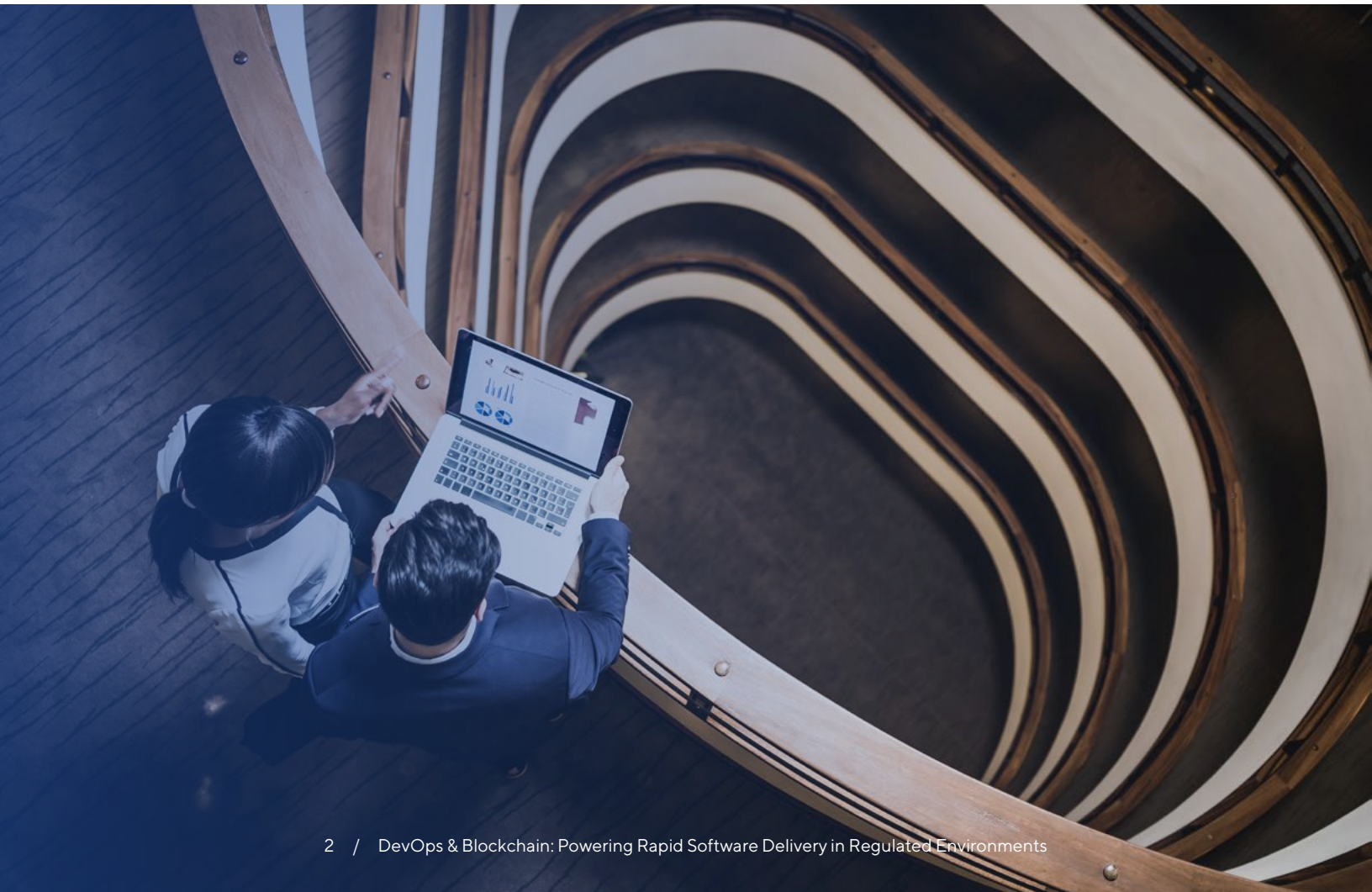
Cognizant

significant regulatory compliance challenges as their applications must meet mandates such as HIPAA,[3] Sarbanes Oxley (SOX),[4] GAMP 5[5] and numerous mandates laid out by the U.S. Federal Drug Administration (FDA).[6]

Based on our estimates, the demand for DevOps in regulated industries is expected to accelerate the CAGR projection cited above. The aforementioned regulatory bodies mandate a stringent process for business processes including application delivery and support. Process compliance is validated by a series of audits that verify the level of compliance measured via tracing of the quality standards adopted by regulated companies.

In our view, the traceability of a software release (the who/what/when concerning changes made) will no longer be present — or obvious — when IT organizations use the automated constructs enabled by DevOps. This could lead to noncompliance. As a result, many enterprises are grappling with the paradox of DevOps automation versus increased government scrutiny; eventually, they need to consider a Faustian bargain of trading off speed for statutory compliance.

Emerging technologies such as blockchain — which entails both distributed ledger and strong cryptography — offer competitive solutions for diverse business challenges that involve numerous stakeholders. This white paper presents a solution that uses blockchain technology to solve regulatory challenges in DevOps adoption. The solution is available as a feature in our product Cognizant OneDevOps™ Insights,[7] which helps organizations measure progress in software delivery through dashboards and metrics.



Regulatory impediments for DevOps adoption

As IT organizations adopt DevOps, friction often emerges between IT and the audit department. The cost of auditing increases as the software development lifecycle (SDLC) progresses, because noncompliance identified at later phases of SDLC will result in significant rework, and often significant penalties, for the offending company. Hence, it is vital that appropriate controls are in place during every phase of the SDLC and that auditability is reported in a tamperproof way.

DevOps processes challenge the traditional way of thinking about audit, controls, security and risk. IT and audit should be able to find cooperative ways of working so financial processes and controls are in alignment with IT's efforts to accelerate product rollouts using DevOps principles.

The conventional approach requires auditors to review enterprise IT systems and report business risks (BR) associated with automated processes (or DevOps). Business or IT then comes up with an appropriate control strategy (CS) to mitigate the risk and provides evidence of how effectively the control strategy is being followed or adopted. Figure 1 portrays several BR instances identified by an auditor and the appropriate CS and process evidence.[8]

Fitting risk with controls

Business Risk	Control Strategy	Process Evidence
▪ An internal actor abuses privileges (provided or developed) to commit fraud to the organization and/or its customers.	▪ All code is validated through defined controls prior to production deployment to prevent developers from inserting "back doors" or vulnerabilities into production.	▪ Static code analysis based on a well-defined coding standard. ▪ Change history for the coding standards document (for at least the last five changes). ▪ Build statistics for last six months showing details of broken builds due to static code analysis violations.
▪ Code is deployed into production that causes an outage, service impairment or data errors.	▪ All code is validated prior to production deployment to ensure the service runs correctly in production and interruptions can be fixed quickly.	▪ Comprehensive quality management process that clearly defines test cases. ▪ Change history for at least the last five changes made to the test cases. ▪ Test report statistics for the last six months showing the details of the test executions.
▪ An external actor gains unauthorized access to production or preproduction environments (e.g., database, OS, networking) and installs malicious code or changes/ steals data.	▪ Unauthorized access is prevented, detected and corrected through the regular review of access credentials and system configurations based on the published SLA for each element of the environment.	▪ Well-defined role-based access system implemented across all the stages of software development. ▪ Clear event and access logs for access controls for all tools and higher environments.

Figure 1

Quick Take

Regulatory Compliance's Toll on App Dev

Audits play a vital role in certifying enterprises are ready for business. Specific statutory bodies regulate each industry — for instance, fintech needs to comply with SOX, whereas healthcare needs to abide by HIPAA[9] and GAMP 5. The compliances are structural, and not prescriptive, in nature. For instance, GAMP 5 mandates regular quality checks during application development which may include engineering practices like test-driven development (TDD),[10] peer reviews and a comprehensive quality management system; however, it does not define the intrinsic details of activities and validations.

Each enterprise has the flexibility to define its software development and support processes that broadly comply with the respective guidelines while adherence is reviewed in an audit. The following are the three broad categories of information reviewed during an audit:

- **Segregation of duties:** An audit trail of the system of records that holds complete information of the role-based access control system so one person alone cannot make changes to software in production.
- **Traceability:** An audit trail of the system of records that traces an artifact across the software delivery pipeline. For instance, the end-to-end traceability of user stories, commits, build numbers, etc. through production deployments.
- **Chain of custody:** An audit trail of the system of records that holds complete information of the state and ownership of the software asset across the software delivery pipeline. For instance, who were the developers and approvers associated with the changes across the development phases of the software?

An internal survey conducted across our regulated projects show the impact of audits (internal as well as external) on application delivery. The top four areas and their pain points are depicted in Figure 2.

Top-four regulatory compliance pain points during an audit

All the below areas and pain points hamper DevOps automation and make audits both time-consuming and process-heavy.

1. AUTOMATION

Exists only for lower environments

Lack of traceability

2. PROCESS

Well-defined; however, manual

Checklist-based

3. DATA

Scattered evidences

Manual collation

4. CULTURE

Show and tell

Often reactive

Source: Cognizant
Figure 2

Blockchain as an application delivery backbone

Application delivery in regulated industries must comply with a host of compliance guidelines, which makes enterprise automation and DevOps transformation extremely challenging. A solution that enables organizations to run DevOps automation alongside existing controls on the software delivery process and provides enough evidence of traceability, segregation of duties, and chain of custody in a clear and tamper-resistant way is the need of the hour.

A blockchain primer

Blockchain technology is piloted across enterprises to solve issues with trust, security, immutability and traceability across all the parties involved in a business transaction. Blockchain's technology infrastructure allows multiple stakeholders to share a common truth in an immutable and decentralized manner via a distributed ledger. The issues of trust, security, immutability and traceability are addressed by blockchain components such as smart contracts, digital signatures and cryptography.

Blockchain's evolution into DevOps

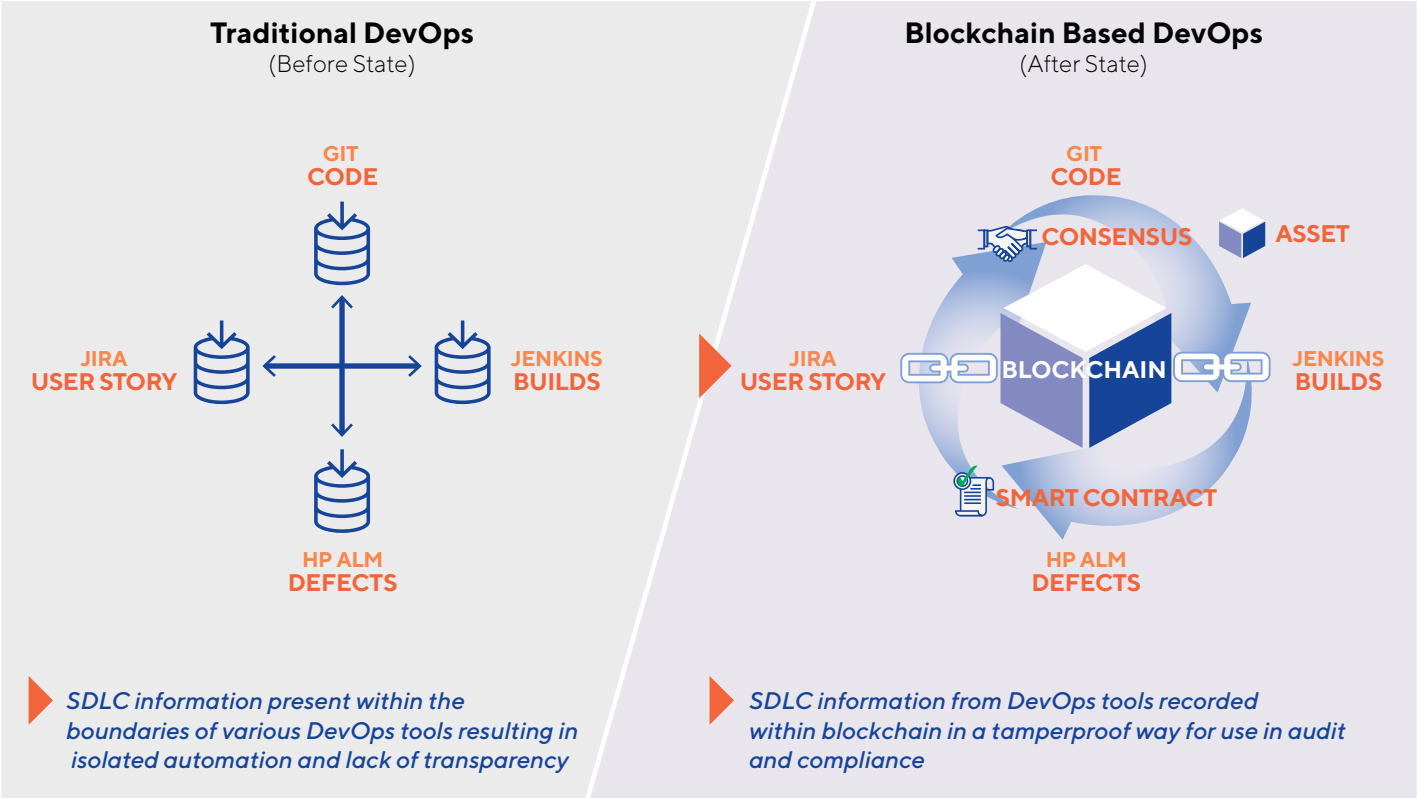


Figure 3

The transfer of an asset from one stage of the SDLC to another is recorded within the blockchain infrastructure. For instance, all the events and states of a software asset (i.e., user story or requirement, code commits, build versions, packages, deployments, tests and defects) are linked to each other and stored inside the blockchain infrastructure. The details for each of the transactions — including the person who made the change, the exact time stamp and the associated metadata — are also archived in a tamperproof fashion.

This information serves as the source of truth for auditors for reviewing the process associated with software development. All the associated transactions are recorded within blockchain infrastructure for the respective phase of software development.

A blockchain-based enterprise DevOps solution can both accelerate application delivery and comply with regulatory requirements, where the risk-based controls and processes are clearly enforced and recorded in a private permissioned blockchain network such as Hyperledger Fabric.[11]

Our solution is built around a private permissioned distributed ledger such as Hyperledger Fabric that serves as the backbone of the enterprise DevOps ecosystem — typically, an integrated system of SDLC and information technology service

Our solution is built around a private permissioned distributed ledger such as Hyperledger Fabric that serves as the backbone of the enterprise DevOps ecosystem — typically, an integrated system of SDLC and information technology service management tools.

How DevOps capabilities are extended via blockchain

DevOps application delivery pipeline

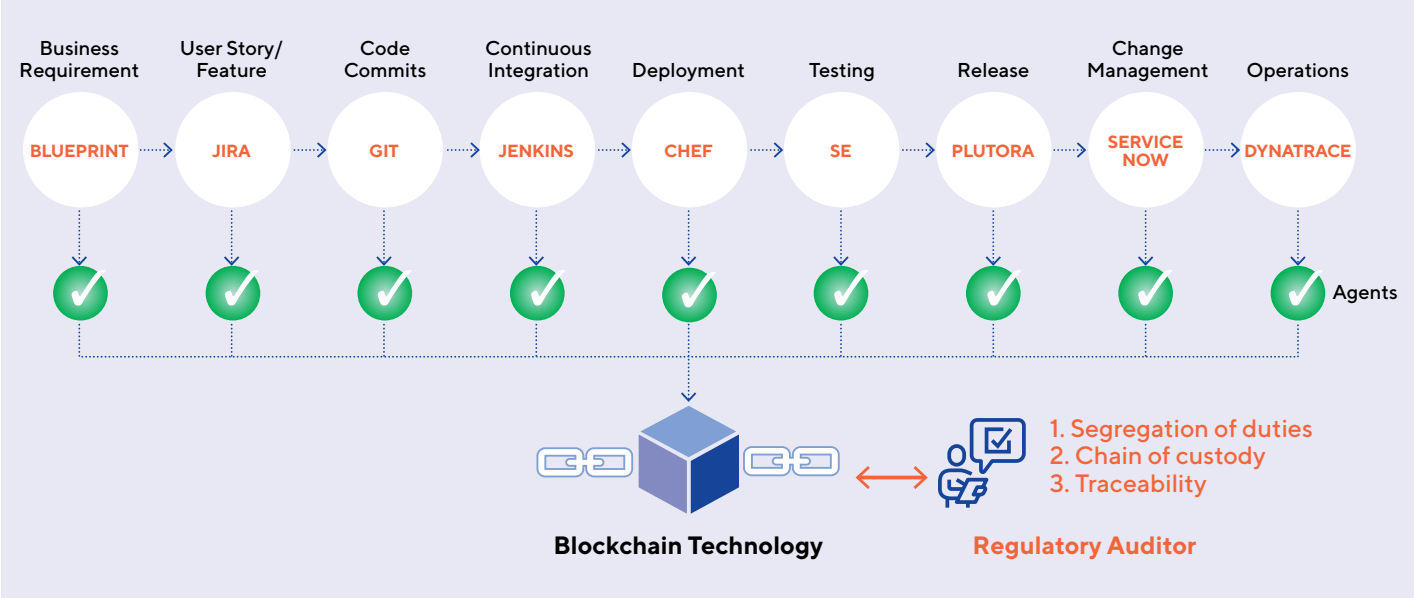


Figure 4

management (ITSM) tools (see Figure 4). The DevOps implementation would typically comprise subsystems of continuous integration, continuous delivery, release management and environment management. Each subsystem may have manual or automated processes for validating application quality such as static code analysis, unit testing, code coverage, regression testing, etc.

In a typical DevOps implementation, each of the SDLC and ITSM tools are integrated with each other such that the construct of a delivery pipeline allows seamless movement of code across the build, deploy, test and release stages of the application lifecycle. The blockchain implementation for a DevOps ecosystem will comprise the following components:

- **Agents:** Data collectors that focus on assembling data for specific events from respective SDLC tools. All information about a change in state of an asset inside a tool will be queried by the agents and will be sent to the blockchain for validation and archiving. For instance, agents that work with application lifecycle management (ALM) and source code management (SCM) tools collect metadata for stories and commits for state changes.
- **Event handler:** The data from the agents is parsed and processed prior to being archived on the blockchain. The event handler invokes an appropriate smart contract based on the data collected by the agent. For instance, data from ALM and SCM tools is parsed; the event handler then invokes the respective smart contracts to record the information to the blockchain infrastructure.
- **Smart contracts:** Definitions of the policies and processes that require adherence for a specific regulatory guideline are codified inside smart contracts. These constitute the decentralized business logic that validates and archives the data within the blockchain infrastructure
- **Query component:** This is the subsystem that focuses on querying information from the blockchain. It takes input such as asset details (e.g., user story identifier, code commit number, etc.), queries the blockchain and returns all the transactions associated with details such as who, what, when and how. The information retrieved is presented in the user interface where auditors and regulatory authorities can review adherence.
- **Auditor view:** The regulatory authorities will have a view of the following:
  - **Segregation of duties:** This means a clear view of the personas who made changes. For instance, implementation of role-based access control across the SDLC and ITSM to prevent one person from making changes to systems in production.
  - **Traceability:** The ability to look at the software asset's trace events associated with any particular change request or change of state.
  - **Chain of custody:** The ability to look at detailed drill-down information on each state or phase of the software asset shown inside the traceability function that addresses the questions what, when and how.
- **DevOps ecosystem:** This refers to the SDLC and ITSM tool chains that are integrated to facilitate the automated code movement and deployment across various environments.

Based on our assessment for a large banking customer, where DevOps practices were not applied for preproduction and production due to stronger regulatory compliance requirements and audits, for a product release that takes 90 days, 50% of the time was spent on manual release activities and record-keeping. This includes time spent on environments, deployments and approvals. A solution such as blockchain-based DevOps can bring down the release timelines by 70%, while more effectively enabling regulatory compliance.

Blockchain-enabled DevOps transformation

Accelerated DevOps

A DevOps implementation backed by blockchain technology can serve as a backbone for enterprise IT, which can release an application to production faster, resolve issues quicker and improve the user experience without compromising on quality and auditability.

Based on our assessment for a large banking customer, where DevOps practices were not applied for preproduction and production due to stronger regulatory compliance requirements and audits, for a product release that takes 90 days, 50% of the time was spent on manual release activities and record-keeping. This includes time spent on environments, deployments and approvals. A solution such as blockchain-based DevOps can bring down the release timelines by 70%, while more effectively enabling regulatory compliance.

Transparency & traceability

All the events associated with an artifact (e.g., a requirement, user story or defect) in application delivery are recorded as they occurred within blockchain infrastructure as a transparent and tamperproof system of records. The system of records will serve as a complete audit trail associated with the artifact along with its digital imprints ensuring compliance.

Cultural shift: A departure from sample-based audits

The ability to record the transfer of a software asset inside blockchain from one stage of development to another allows real-time, comprehensive audits without sampling. Due to the practical complexities in accessing, analyzing and reviewing data along with evidence, auditors restrict reviews of sampled data sets and specific periods. With this feature, the following results can be expected:

- Audit preparation time will be reduced by one-third due to all the information being recorded as an immutable source within blockchain.
- The number of stakeholders involved in the audit process will be reduced due to automation.
- Automation will reduce manual error and the audit trail recorded inside the blockchain, which further improves the transparency of the audit process.

Looking forward

Blockchain technology opens up a new model of operating DevOps by defining compliance as code. The entire application delivery lifecycle could be codified as smart contracts through various DevOps tools such as Git, Jenkins, Jira and HP ALM. Smart contracts would validate the entry and exit points of the various stages of the application delivery pipeline, shifting IT away from proprietary checks inside specific tools. Since the quality gates and validations are abstracted away from the DevOps tools, this helps IT to accommodate process changes with greater agility and confidence.

Enterprises understand that audits are a routine part of doing business, and they anticipate greater challenges in complying with regulatory standards that are updated to accommodate changing socioeconomic and geopolitical developments. Given blockchain's growing maturity as an enterprise infrastructure, we recommend that IT leaders review their existing application delivery and DevOps processes and consider embracing distributed ledger technology to enable a more proactive and automated approach to regulatory compliance.

Blockchain-technology-driven DevOps will help IT organizations to release software at the will of the business, secure in the knowledge that regulatory procedures are being met with confidence and accuracy.

Blockchain technology opens up a new model of operating DevOps by defining compliance as code. The entire application delivery lifecycle could be codified as smart contracts through various DevOps tools such as Git, Jenkins, Jira and HP ALM. Smart contracts would validate the entry and exit points of the various stages of the application delivery pipeline, shifting IT away from proprietary checks inside specific tools.

Endnotes

1 DevOps is a software development methodology that aims to accelerate the software delivery process by means of collaboration between the development and operations teams through automation. See https://en.wikipedia.org/wiki/DevOps.

2 DevOps Platform Market Outlook To 2024, Ameri Research, May 3, 2017, www.ameriresearch.com/devops-platform-market-outlook-2024/

3 www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

4 www.investopedia.com/terms/s/sarbanesoxleyact.asp

5 https://ispe.org/sites/default/files/publications/guidance-documents/ISPE-GAMP5-table-content.pdf.

6 www.fda.gov/media/73141/download

7 https://onedevops.atlassian.net/wiki/spaces/OI/overview

8 DevOps Audit Defense Toolkit is a community-built process framework for DevOps and Compliance, written by James DeLuccia, IV, Jeff Gallimore, Gene Kim, and Byron Miller.

9 www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

10 http://agiledata.org/essays/tdd.html.

11 Hyperledger Fabric is an enterprise grade permissioned distributed ledger platform for a broad set of industry use cases; www.hyperledger.org/projects/fabric.

About the authors

Karthikeyan Vedagiri

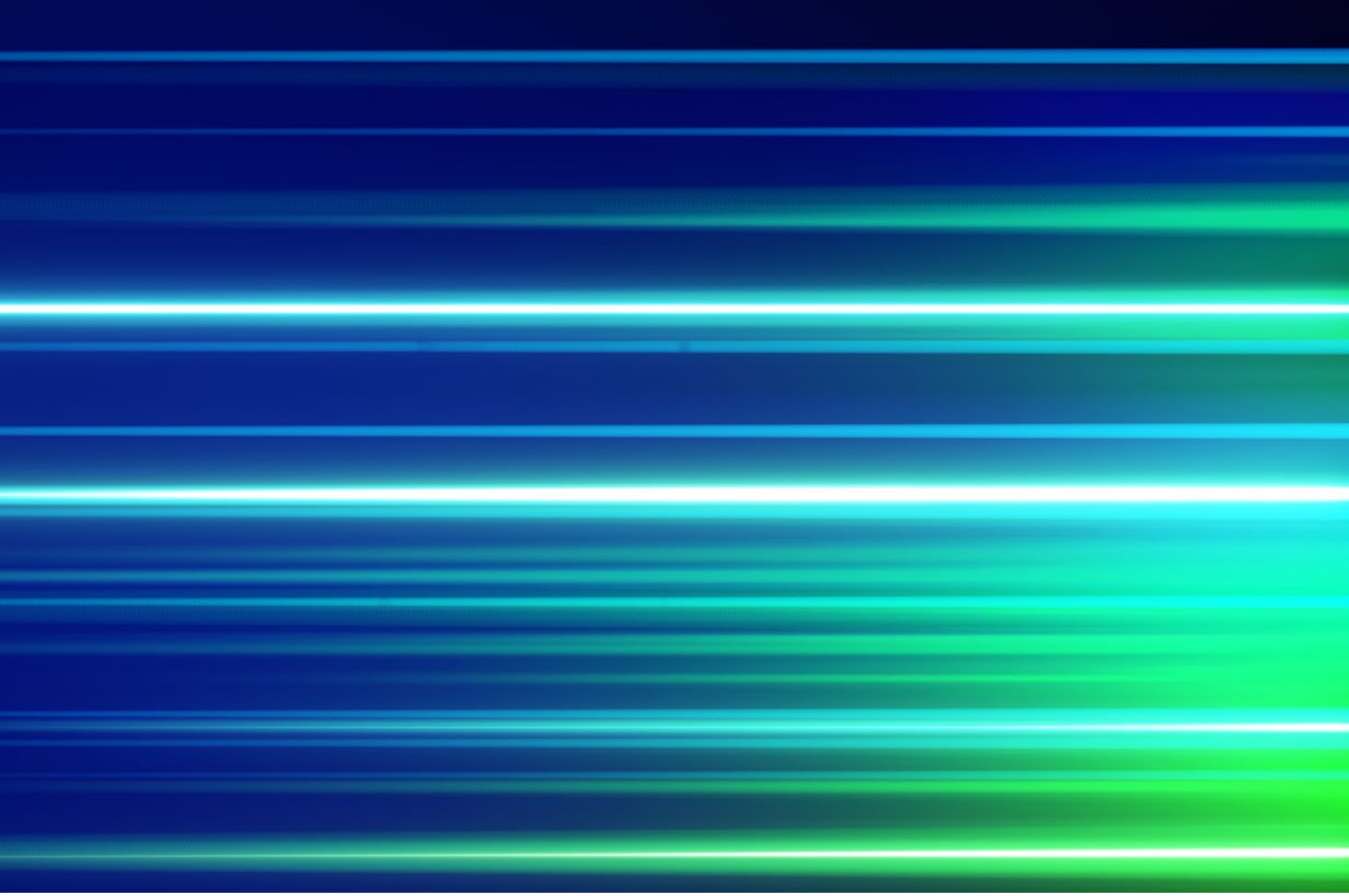
Associate Director, Digital Engineering Practice, Cognizant

Karthikeyan Vedagiri is an Associate Director, Projects, within Cognizant's Digital Engineering Practice, where he focuses on the development of products and accelerators for Cognizant OneDevOps™. He has more than 15 years of experience in product engineering and quality assurance and specializes in design and architecture of test automation frameworks, deployment pipelines and DevOps platforms for emerging technologies such as cloud, container and platform as a service (PaaS). Karthikeyan has a bachelor's degree in engineering, with specialization in electronics and communication, from Madras University, Tamil Nadu, India. He can be reached at Karthikeyan.Vedagiri@cognizant.com | www.linkedin.com/in/karthikeyan-vedagiri/.

Rajkumar Chandrasekaran

Chief Architect, Digital Engineering Practice, Cognizant

Rajkumar Chandrasekaran is a Chief Architect within Cognizant's Digital Engineering Practice. He has 17 years of experience in the field of large-scale application development and has played varied roles, from application architecting through reengineering of applications. Rajkumar is currently architecting Cognizant's OneDevOps™ platform and is responsible for product development in the DevOps space. He has a bachelor's degree in engineering, with specialization in computer science, from MS University, Tamil Nadu, India. Rajkumar can be reached at Rajkumar.Chandrasekaran@cognizant.com | www.linkedin.com/in/rajkumar-chandrasekaran-98309012/.



About Cognizant Digital Engineering

Cognizant's Digital Engineering team designs, engineers and delivers digital products and experiences that drive digital-first business models. It offers the most comprehensive engineering expertise and client-centric methodology for sustainable innovation. The Cognizant Digital Engineering team was named in the HFS Research Winner's Circle in Software Product Engineering for its consulting capability, deep client relationships and strong partnership ecosystem for software product engineering.

About Cognizant

Cognizant (Nasdaq-100: CTSH) is one of the world's leading professional services companies, transforming clients' business, operating and technology models for the digital era. Our unique industry-based, consultative approach helps clients envision, build and run more innovative and efficient businesses. Headquartered in the U.S., Cognizant is ranked 193 on the Fortune 500 and is consistently listed among the most admired companies in the world. Learn how Cognizant helps clients lead with digital at www.cognizant.com or follow us @Cognizant.

Cognizant

World Headquarters

500 Frank W. Burr Blvd.
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277

European Headquarters

1 Kingdom Street
Paddington Central
London W2 6BD England
Phone: +44 (0) 20 7297 7600
Fax: +44 (0) 20 7121 0102

India Operations Headquarters

#5/535 Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060

Codex 4008