CAG: Compliance Adherence and Governance in Software Delivery Using Blockchain

Submitted by grigby1 on Fri, 04/03/2020 - 12:04pm

Title	CAG: Compliance Adherence and Governance in Software Delivery Using Blockchain
Publication Type	Conference Paper
Year of Publication	2019
Authors	Singi, Kapil, Kaulgud, Vikrant, Bose, R.P. Jagadeesh Chandra, Podder, Sanjay
Conference Name	2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)
Date Published	May 2019
Publisher	IEEE
ISBN Number	978-1-7281-2257-1
Keywords	auditing, blockchain, blockchain technologies, building software, client industry, Collaboration, compliance adherence and governance, compliance specifications, contracts, copyright issues, Crowd Sourcing, cryptocurrencies, decentralized CAG, development activities, disparate sources, distributed teams, economic challenges, extraordinary amounts, functional specifications, geographically distributed teams, Global Software Development, legislation, level agreements, Libraries, License verification, Licenses, litigations, metadata , noncomplaint license software, nonconformant behavior, open source components, open-source software components, Policy Based Governance, pubcrawl, public domain software, SDLC, security risks, smart contracts, Software, software delivery, software development life cycle, software development management, software engineering, standard compliances, technical challenges, vulnerability assessment

Abstract

The software development life cycle (SDLC) starts with business and functional specifications signed with a client. In addition to this, the specifications also capture policy / procedure / contractual / regulatory / legislation / standard compliances with respect to a given client industry. The SDLC must adhere to service level agreements (SLAs) while being compliant to development activities, processes, tools, frameworks, and reuse of open-source software components. In today's world, global software development happens across geographically distributed (autonomous) teams consuming extraordinary amounts of open source components drawn from a variety of disparate sources. Although this is helping organizations deal with technical and economic challenges, it is also increasing unintended risks, e.g., use of a non-complaint license software might lead to copyright issues and litigations, use of a library with vulnerabilities pose security risks etc. Mitigation of such risks and remedial measures is a challenge due to lack of visibility and transparency of activities across these distributed teams as they mostly operate in silos. We believe a unified model that non-invasively monitors and analyzes the activities of distributed teams will help a long way in building software that adhere to various compliances. In this paper, we propose a decentralized CAG - Compliance Adherence and Governance framework using blockchain technologies. Our framework (i) enables the capturing of required data points based on compliance specifications, (ii) analyzes the events for non-conformant behavior through smart contracts, (iii) provides real-time alerts, and (iv) records and maintains an immutable audit trail of various activities.

URL https://ieeexplore.ieee.org/document/8823885
DOI 10.1109/WETSEB.2019.00011
Citation Key singi_cag_2019

auditing blockchain blockchain technologies building software client industry collaboration compliance adherence and governance compliance specifications contracts copyright issues Crowd Sourcing cryptocurrencies decentralized CAG development activities disparate sources distributed teams economic challenges extraordinary amounts functional specifications geographically distributed teams Global Software Development legislation level agreements Libraries License verification Licenses litigations metadata noncomplaint license software nonconformant behavior open source components open-source software components Policy Based Governance pubcrawl public domain software SDLC security risks smart contracts Software software delivery software development life cycle software development management software engineering standard compliances technical challenges vulnerability assessment