Uma Abordagem de Auditoria Contínua com Blockchain para Gerenciamento de Mudanças em TI

Carlos Fraga[1] **, Antônio Abelém**[2] **, Vinícius Borges**[3] **,**
Billy Pinheiro[4] **, Weverton Cordeiro**[1]

[1] Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Caixa Postal 15.064 – 91.501-970 – Porto Alegre – RS – Brazil

[2]Instituto de Ciências Exatas e Naturais – Universidade Federal do Pará (UFPA)
Caixa Postal 479 – 66.075-110 - Belém – PA – Brazil

[3]Instituto de Informática – Universidade Federal de Goiás (UFG)
Caixa Postal 131 – 74.690-900 - Goiânia – GO – Brazil

[4]Amachains – Espaço Inovação – Parque de Ciência e Tecnologia Guamá (PCT Guamá)
66.075-750 – Belém – PA – Brazil

{carlos.fraga,weverton.cordeiro}@inf.ufrgs.br, abelem@ufpa.br,
vinicius@inf.ufg.br, billy@amachains.com

Abstract. *Information Technology (IT) changes are a critical part of the day-to-day operations of most modern organizations, and poor change delivery can pose severe risks to business continuity. In this context, frameworks like COBIT seek to provide guidance for best practices and procedures for proper IT change management, and shareholders often resort to auditing to ensure change delivery following defined procedures. To this end, third-party audit companies perform periodic inspections of the target IT system, log of changes deployed, etc. However, the sheer volume of changes, ever-increasing change complexity, and automation make it challenging to deliver change auditing between inspection events. To tackle this issue, we propose in this paper a blockchain-based approach for continued IT change auditing. In summary, we instrumented a change orchestration framework with a solution for certifying each change deployed in the target system through blockchain. The chain of IT changes in between inspection events is then used to ensure that only certified changes were deployed in the infrastructure.*

Resumo. *As mudanças na Tecnologia da Informação (TI) são uma parte crítica das operações diárias da maioria das organizações modernas, e uma entrega deficiente das mudanças pode representar riscos graves para a continuidade dos negócios. Neste contexto, frameworks como o COBIT procuram fornecer orientação para as melhores práticas e procedimentos para uma gestão adequada das mudanças de TI, e os acionistas recorrem frequentemente à auditoria para garantir a entrega das mudanças seguindo os procedimentos definidos. Para esse fim, empresas de auditoria terceirizadas realizam inspeções periódicas dos sistemas de TI alvo, dos logs de mudanças implantadas, etc. No entanto, o grande volume de alterações, a complexidade cada vez maior das alterações e a automação tornam um desafio fornecer auditoria de mudanças*

entre as inspeções. Para resolver esse problema, propomos neste artigo uma abordagem baseada em blockchain para auditoria contínua de mudanças de TI. Em resumo, instrumentamos um framework de orquestração de mudanças com uma solução para certificar cada mudança implantada no sistema alvo por meio de blockchain. A cadeia de mudanças entre os eventos de inspeção é então usada para garantir que apenas mudanças certificadas foram implantadas na infraestrutura.

1. Introdução

Em um mundo cada vez mais dinâmico e em constante evolução, mudanças em sistemas e infraestruturas de Tecnologia de Informação (TI) são cruciais para o sucesso de empresas e organizações. Tais mudanças, se não forem bem planejadas e geridas, podem implicar em falhas sistêmicas, vulnerabilidades de segurança e, em casos extremos, indisponibilidades do serviço, com perdas financeiras, de imagem e de credibilidade [Pandey and Mishra 2014].

A gestão de mudanças em TI, conforme orientada por *frameworks* como *ITIL* [Axelos 2019] e *COBIT* [Isaca 2018], visa maximizar o número de mudanças bem sucedidas através da avaliação de riscos, da autorização e da gestão temporal. Recentemente, diversos processos vêm sendo adotados para a automatização dessas mudanças [Axelos 2019][Isaca 2018][Mahimkar et al. 2021]. Além disso, as preocupações com segurança, com boas práticas e com a certificação dos roteiros de mudanças têm sido incorporadas a esses processos, os quais elevam o nível de confiança das organizações nos processos de gestão de mudanças, segurança, etc. [Mohan and Othmane 2016].

Para as auditorias de TI, a verificação de processos, de ferramentas, de procedimentos, de políticas, de ambientes tecnológicos e de seus ativos é de importante relevância para aferir a adequação (*compliance*) de organizações às metodologias, aos padrões, às diretrizes e às boas práticas estabelecidas. Nesse contexto, as auditorias independentes prestam um serviço de investigação e acreditação para organizações, útil para relações de parceria com outras organizações, com governos, sociedade, etc. [Gantz 2013].

Para os fins de auditoria, o estado atual dos sistemas e da infraestrutura de TI da organização auditada é analisado em intervalos de tempo variados sendo, o mais comum, a inspeção anual [Gantz 2013]. No entanto, o grande volume de mudanças, a complexidade cada vez maior das mudanças e a crescente automação [Han et al. 2022] impõem desafios para a certificação de mudanças realizadas entre inspeções. Por exemplo, suponha uma organização que passou por duas inspeções de auditoria: em 30-12-2022 e em 30-12-2023. A análise da "foto" dos sistemas e da infraestrutura de TI no momento de cada auditoria, embora permita certificar tais elementos naqueles momentos, não garante que todas as mudanças realizadas entre 30-12-2022 e 30-12-2023 foram necessariamente certificadas, isto é, seguiram os procedimentos pré-determinados e aprovados pela organização. A partir desse exemplo, nota-se a dificuldade em verificar e assegurar a conformidade, ao longo do tempo, das mudanças realizadas [Han et al. 2022][Aditya et al. 2018]. Há, ainda, uma dificuldade para as auditorias analisarem o estado dos sistemas e das infraestruturas quando não estão presencialmente na organização auditada ou quando não possuem evidências históricas desses estados disponíveis [Zheng et al. 2018].

Para suprir essas lacunas, o presente artigo apresenta uma abordagem para audi-

toria contínua de gestão de mudanças de TI via *blockchain*. A abordagem baseia-se na instrumentação de um *framework* de orquestração de mudanças com uma solução para certificar, via *blockchain*, cada operação de mudança implantada nos sistemas. A cadeia de mudanças feitas entre inspeções é, então, usada para indicar se apenas mudanças certificadas foram implantadas desde a última inspeção. Dessa forma, a abordagem proposta visa dar visibilidade à sequência de eventos de mudanças feitas na TI para os fins de auditoria; tal aumenta a acurácia e a assertividade dos pareceres das auditorias e, portanto, a confiabilidade do processo de gestão de mudanças na organização. O código fonte do nosso protótipo de prova de conceito e os *scripts* para experimentação encontram-se disponíveis publicamente para os pesquisadores interessados em reproduzir os experimentos e verificar os resultados alcançados [Fraga 2023].

O restante do artigo está organizado como segue. A Seção 2 revisa alguns dos principais trabalhos relacionados à área. A Seção 3 detalha o problema em análise. A Seção 4 detalha a abordagem de auditoria contínua proposta no presente artigo. A Seção 5 discorre sobre a avaliação experimental conduzida, enquanto que as Seções 6 e 7 apresentam, respectivamente, discussões sobre o estudo e trabalhos futuros, e a conclusão.

2. Trabalhos Relacionados

[Byrnes et al. 2018] resumem a história da auditoria nos Estados Unidos, desde a Revolução Industrial até os dias atuais, fazendo uma análise sobre os conceitos da auditoria tradicional, da auditoria automatizada e da chamada auditoria do futuro. Os autores alertam que, para a plena adoção da auditoria do futuro, os auditores, os reguladores e os criadores de padrões precisarão implementar melhorias e/ou ajustes importantes nos seguintes temas: mudanças no cronograma e na frequência da auditoria; maior educação em tecnologia e métodos análiticos; adoção de exame populacional completo em vez de amostragem; reexame de conceitos - como materialidade e independência - e obrigatoriedade do fornecimento do padrão de dados de auditoria.

Nessa mesma linha, [Chan and Vasarhelyi 2018] mostram que o paradigma de auditoria contínua trouxe inovação para a prática tradicional de auditoria, por meio de sete dimensões: (i) auditorias contínuas ou mais frequentes; (ii) modelo de auditoria proativa; (iii) automação de procedimentos de auditoria; (iv) evolução do trabalho e papel dos auditores; (v) mudança na natureza, tempo, e extensão da auditoria; (vi) uso de modelagem de dados e dados analíticos para monitoramento e testes, e (vii) mudança na natureza e tempo dos relatórios de auditoria. Adicionalmente, os autores afirmam que a auditoria contínua consiste em quatro etapas: a) automação de procedimentos de auditoria; b) modelagem de dados e desenvolvimento de *benchmark*; c) análise de dados; e d) relatórios. Na visão dos autores, cada vez mais praticantes e acadêmicos estão adotando o conceito de auditoria contínua, o que culminará com a adoção progressiva dessa prática, em detrimento das práticas tradicionais de auditoria.

Ambos os estudos de [Byrnes et al. 2018] e [Chan and Vasarhelyi 2018] focam, majoritariamente, em auditoria financeira. No entanto, argumentamos que o tema auditoria extrapola essa área, e os mesmos conceitos se aplicam à auditoria de TI. Além disso, o assunto é realidade presente das organizações nos dias atuais, mesmo que o número de publicações recentes focadas em auditoria de TI não seja expressivo. Apesar disso, a literatura é rica em investigações sobre mudanças em TI. [Zaydi and Nassereddine 2021]

discutem a importância da gestão de mudanças, analisando aspectos de segurança nesse processo. Através de seu estudo, propuseram um algoritmo de aprendizado de máquina (AM) para prever mudanças que causam incidentes em TI. Entendemos que o estudo avança sobre uma importante temática, como a prevenção de incidentes na gestão de mudanças de TI. No entanto, não há - explicitamente - uma discussão sobre como essas mudanças podem ser analisadas por uma empresa auditora, nem como algoritmos de AM podem ser auditados ou beneficiar processos de auditoria.

Mais recentemente, [Mahimkar et al. 2021] propuseram um *framework* para gerenciamento de mudanças que permite composição de processos de mudanças, planejamento e otimização, verificação do impacto e tradução de mudanças expressas em mais alto nível para um conjunto de operações que as implementam. No entanto, a auditoria das mudanças realizadas pelo *framework* ficou fora do escopo do artigo.

[Rysbekov 2022] conduziu pesquisas com engenheiros *DevOps* para entender a viabilidade do uso de conformidade contínua nas organizações. A conclusão foi de que há espaço para integrar processos de conformidade com pipelines de desenvolvimento. Porém, seu estudo não propõe uma ferramenta que enderece as necessidades de auditorias e se limita a sugerir aspectos de funcionalidades que podem ser desenvolvidas e/ou exploradas em uma solução de conformidade contínua.

Além dos trabalhos acima, outras investigações têm sido realizadas envolvendo *blockchain* e auditoria. [De Castro et al. 2022] estuda uma arquitetura, baseada em *blockchain*, para a auditoria de operações de tratamento de dados, conforme as regulamentações das leis LGPD no Brasil e *GDPR* na União Europeia. [Vries 2022] estuda a detecção de anomalias durante auditorias de TI. Dentre suas sugestões, está a analise completa de uma população de dados, e não apenas a análise de amostras. [Marques et al. 2022] apresentam uma solução baseada em *blockchain* para implementar um *log* distribuído e auditável com dados enviados a partir de coletores autorizados e customizados. [Hashem et al. 2023] estudaram como a *blockchain* pode afetar a qualidade de um processo de auditoria. Dentre suas conclusões, vale citar o ganho de tempo e eficiência para auditorias, a análise de população - em vez de amostra - e a configuração de um processo de auditoria contínuo. [Macedo and Campista 2020] propõem o uso de *blockchain* para aumentar a auditabilidade e rastreabilidade de operações de redes móveis.

[Chatziamanetoglou and Rantos 2023] propoem um modelo teórico de gestão de configuração a partir do uso da blockchain. Apesar de verificarmos diversos objetivos e funções em comum com nosso estudo, os autores não conduziram uma prova de conceito ou protótipo que exercitasse o modelo proposto. Na conclusão os autores indicam a importância de novas pesquisas explorarem essa teoria na prática, atentando para o requisito de performance. Apesar dos avanços observados, nota-se uma lacuna persistente em soluções que possam oferecer auditoria contínua em gerenciamento de mudanças.

Assim sendo, o presente artigo busca detalhar os avanços na abordagem de [Fraga et al. 2024]. Nas próximas seções apresentamos uma solução, acompanhada de um protótipo como prova de conceito [Fraga 2023], para esse fim.

3. Contextualização e Definição do Problema

Durante um evento de auditoria de TI terceirizada em uma organização, os processos de gestão de mudanças são analisados. O estado dos sistemas e da infraestrutura são verifi-

cados para diferentes checagens de segurança e melhores práticas processuais, eventualmente sugeridas e definidas por políticas e *frameworks* de conformidade [Moeller 2010]. Os insumos utilizados nessas análises geralmente são fornecidos pela própria organização auditada e podem ser alvo de adulterações para mascarar ou esconder informações que seriam verificadas como indício de não conformidade pelos auditores. Além disso, há um trabalho manual de coleta e compartilhamento dessas informações que acarretam maior tempo para a conclusão do evento de auditoria. Em qualquer caso, o processo de auditoria é limitado, pois não analisa a conformidade de mudanças executadas entre inspeções.

A seguir descrevemos um processo que exemplifica, de forma resumida, os passos de uma auditoria de TI terceirizada na sua interação com a organização auditada [Moeller 2010]. Após a contratação da empresa de auditoria por parte da organização, há o agendamento da primeira visita de inspeção. Na data agendada, a empresa auditora dá início ao processo de auditoria, capturando o estado atual dos sistemas e da infraestrutura, analisando esse estado e emitindo seu parecer de conformidade. Ao término desse processo, avalia-se se o contrato com a organização segue vigente para que, em outro momento, uma nova visita/inspeção seja agendada. Do contrário, a auditoria não é realizada novamente.

Nesse cenário, exemplificamos um problema que pode ocorrer nessa abordagem não contínua de auditoria. Suponha duas inspeções de auditoria, realizadas nas datas D_1 e D_2. S_1 determina o estado dos sistemas e da infraestrutura de TI auditado em D_1 e S_2 o estado auditado em D_2. Suponha também que, após D_1 e antes de D_2, foram executadas as mudanças M_1, M_2, M_3 e M_4, com cada mudança causando um efeito no estado atual dos sistemas e da infraestrutura. Sem auditoria contínua, a empresa de auditoria não é capaz de certificar que os estados intermediários gerados por cada mudança também são conformes (*compliants*).

4. Nossa Proposta: Auditoria Contínua de Mudanças em TI via *Blockchain*

Com a abordagem proposta para auditoria contínua, além de confirmar que S_1 e S_2 são conformes (*compliants*), também atestaria-se que o estado S_2 pode ser alcançado a partir de S_1 aplicando os efeitos das mudanças M_1, M_2, M_3 e M_4 executadas. Matematicamente, teria-se: $S_{n+1} = S_n + \sum_{i=1}^{k} s(M_i, S_i)$ onde *s(M_i, S_i)* é a função que define os efeitos da mudança M_i sobre o estado intermediário S_i e *k* é o número de mudanças executadas. A não satisfação dessa igualdade significaria que alguma mudança não certificada/registrada foi executada entre inspeções, cabendo à auditoria evidenciar esse fato. Portanto, como principais contribuições do presente artigo, objetivamos o aperfeiçoamento do processo de auditoria de mudanças em TI para auditoria contínua via: (i) redução do esforço manual de coleta de evidências para auditoria; (ii) garantia da integridade dos dados coletados; (iii) capacidade de inclusão de processos diversos de verificação para fins de auditoria nos processos de mudança; e (iv) verificação da integridade dos sistemas e da infraestrutura a cada mudança executada.

4.1. Coleta Automática de Evidências

Visando uma redução do esforço de coleta de evidências, nossa abordagem propõe que as auditorias de TI incorporem uma aplicação de coleta de evidências de execuções de mudanças, aqui denominado agente da auditoria. Esse agente seria capaz de se integrar, de maneira simples, aos processos de mudança das organizações. Além disso, esse

agente armazenaria essas informações em um repositório acessível aos interessados na informação – no caso, à auditoria terceirizada e à própria organização auditada.

A definição das informações que serão coletadas dos sistemas e da infraestrutura é de responsabilidade da auditoria e precisa ser definido/configurado no agente da auditoria. Um exemplo de modelo de informações que pode ser usado é o *Common Information Model*[1] *(CIM)*, mantido pela *Distributed Management Task Force (DMTF)*. Segundo a *DMTF*, esse modelo fornece uma definição comum de informações de gerenciamento para sistemas, redes, aplicativos e serviços, além de permitir extensões de fornecedores.

O agente de coleta automatizada precisaria ser disponibilizado para as organizações auditadas, de modo que estas o incluam em seus processos e ferramentas responsáveis pelas execuções de mudanças. Além disso, a auditoria deve fazer um controle de assinaturas das versões do agente de coleta, de modo que seja possível, a partir do seu uso, garantir acesso das organizações auditadas ao repositório de dados (para fins de escrita) somente a partir de versões homologadas.

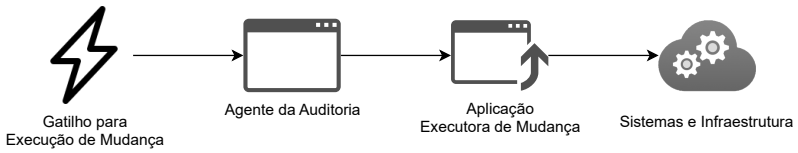

Figura 1. Esquema de exemplo de uso do agente da auditoria.

A Figura 1 ilustra um esquema de execução de mudanças com auditoria. A figura descreve o processo de mudança a partir do gatilho para execução da mesma, por ex., a configuração de um *cluster* em um *datacenter* ou a instalação de uma plataforma de *software*. Esse gatilho executa o agente da auditoria que coleta as evidências da mudança a ser executada. O agente é configurado/instalado para invocar o sistema que orquestra as mudanças na organização, isto é, a aplicação executora de mudança (por ex., *Jenkins*[2], *Kubernetes*[3], *Ubuntu Package Management System*[4]). Assim, será possível acionar a aplicação executora através do agente da auditoria. Toda a evidência gerada pela aplicação executora será então coletada pela agente e enviada para um repositório de dados.

O agente da auditoria deve possuir a capacidade de verificar sua própria assinatura de modo que, em seu fluxo transacional, ocorra uma validação que garanta que a versão do agente em execução seja uma versão válida e autêntica da auditoria. Além disso, o agente deverá calcular as assinaturas das aplicações executoras de mudança e eventuais artefatos (em formato de arquivo) necessários para a execução da mudança. Por exemplo, se a aplicação cliente for configurada com a ferramenta *Terraform*[5], um arquivo de extensão "*.tf*" pode ser considerado um artefato dessa ferramenta.

[1]https://www.dmtf.org/standards/cim
[2]https://www.jenkins.io
[3]https://kubernetes.io
[4]https://ubuntu.com/server/docs/package-management
[5]https://www.terraform.io

4.2. Integridade das Evidências

Empregamos a tecnologia *blockchain* para garantir a integridade das evidências geradas pela organização para a auditoria. O *blockchain* desempenha um papel fundamental como repositório de dados devido a sua característica de completa transparência transacional entre os membros da rede. A partir da tecnologia citada, as partes interessadas nas informações se tornam pares na rede e são capazes de receber todos os dados armazenados no repositório compartilhado. Assim, as partes podem verificar a autenticidade das informações, bem como a integridade, a partir das chaves públicas dos demais pares da rede e das assinaturas das transações na cadeia de blocos da rede.

Além disso, a *blockchain* utilizada como repositório de dados em um agente confiável da auditoria, como a citada na Seção 4.1, garante que toda a evidência gerada por aplicações executoras de mudanças nos sistemas e na infraestrutura integradas à ela seja confiável. Logo, a mesma estaria imune a adulteração por parte de qualquer parte mal intencionada em comprometer a acurácia e a assertividade da análise da auditoria.

Também é possível definir um maior nível de segurança e restrição para o processo de mudança de TI, caso a organização assim o exija. Com isso, qualquer mudança só será autorizada se as ferramentas usadas para orquestrá-la tenham sido previamente comunicadas e homologadas pela auditoria. Isso pode ser feito, via *blockchain*, armazenando-se as informações dessas ferramentas homologadas e dos artefatos de insumo e executando-se *smart contracts* para aferir se uma dada ferramenta já foi homologada e, portanto, pode ser autorizada para uso na mudança.

4.3. Verificação Contínua de Mudanças

Assim que o agente da auditoria está configurado e instalado junto às aplicações executoras de mudanças (como sugerido na Seção 4.1), ele permite que a auditoria verifique os sistemas e a infraestrutura para diferentes fins de conformidade. Por ex., quanto às mudanças de instalação de *software*, a auditoria pode avaliar as aplicações e as bibliotecas instaladas antes e depois da mudança. Através de uma comparação desses dois estados, ao final da mudança, pode-se avaliar como ela impactou essa lista de aplicações instaladas.

As informações da diferença de estados mencionadas acima, juntamente com a identificação do aplicativo de execução de mudança, os artefatos envolvidos e o resultado da execução, podem ser armazenados no *blockchain*. Assim, tem-se um histórico completo das mudanças executadas e dos estados intermediários dos sistemas e da infraestrutura antes e depois de cada mudança (tal como necessário para satisfazer o formalismo matemático descrito na Seção 4).

4.4. Integridade dos Sistemas e da Infraestrutura entre Eventos de Auditoria

Considerando que o evento de inspeção é comumente realizado uma vez por ano, é importante verificar o estado atual dos sistemas e da infraestrutura auditada e garantir que, entre esses eventos anuais, os sistemas e a infraestrutura não passem por estados de não conformidade. Em nossa abordagem, é possível que a auditoria verifique o estado atual dos sistemas e da infraestrutura e compare-o com o resultado de uma simulação dos efeitos da sequência de mudanças realizadas no período e gravadas na *blockchain*. Ou seja, o estado dos sistemas e da infraestrutura capturado pela auditoria no último evento de

inspeção pode ser submetido à aplicação das diferenças de estado constantes em cada mudança gravada na *blockchain*. Ao final da última mudança, basta verificar se a assinatura correspondente do estado dos sistemas e da infraestrutura simulada equivale à assinatura do estado observado na inspeção atual. Dessa forma, é possível garantir que os sistemas e a infraestrutura estejam em conformidade durante o período compreendido entre os eventos de auditoria. Assim, caracteriza-se um aspecto de auditoria automática e/ou contínua, pois passa-se a considerar, nos pareceres dos auditores, a integridade confiável dos sistemas e da infraestrutura durante todo o período auditado.

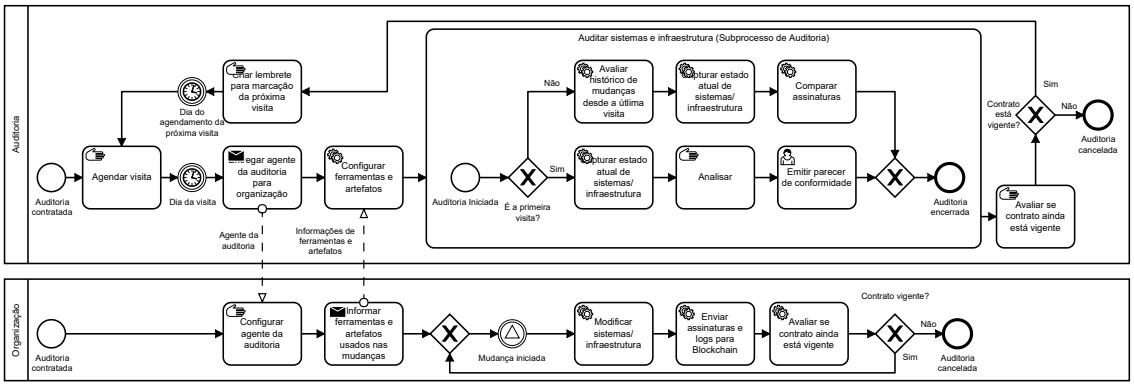

Figura 2. Exemplo de processo de auditoria terceirizada com a abordagem proposta.

A Figura 2 exemplifica o processo de auditoria de TI terceirizada com a aplicação da abordagem proposta neste artigo. Nessa abordagem, a participação da organização é fundamental para a obtenção dos ganhos esperados, a partir da configuração e utilização do agente da auditoria nos processos de mudanças. Já na Figura 3 mostramos, em um esquema simples, toda a abordagem com um exemplo ilustrativo de uso.

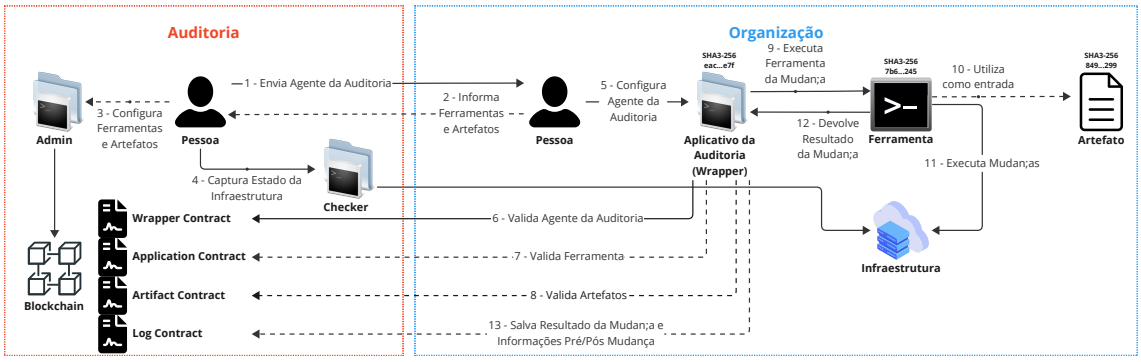

Figura 3. Esquema de exemplo de uso da abordagem proposta.

Ao término da execução da mudança, a ferramenta executora devolve seu resultado para a aplicação cliente da auditoria, que fará o armazenamento do resultado junto das informações pré e pós mudança na *blockchain*, evidenciados no esquema pelos passos doze e treze da Figura 3.

5. Avaliação Experimental

Para avaliarmos a proposta deste trabalho, implementamos uma prova de conceito através do desenvolvimento do agente da auditoria e da configuração de uma rede *blockchain*.

Adicionalmente, construímos alguns fluxos de mudança para simular o uso da solução em um ambiente de TI de uma organização auditada. O objetivo é avaliar qualitativamente a capacidade da solução em (i) viabilizar a coleta automática de evidências de mudanças de TI, (ii) garantir a integridade dos dados coletados, (iii) permitir a inclusão de processos diversos de verificação - para fins de auditoria - nos processos de mudança da organização e (iv) verificar a integridade dos estados intermediários dos sistemas e da infraestrutura entre eventos de auditoria e após cada mudança.

5.1. Protótipo de Prova de Conceito

Para implementar a abordagem proposta, construímos cinco projetos diferentes na linguagem de programação *Java* e centralizamos em um repositório público de código no *GitHub*[6]. Os comandos e *scripts* para executar cada projeto também estão disponíveis.

Projeto *Chaincode*. Esse projeto concentra todos os subprojetos de contratos inteligentes para *blockchain* que são utilizados no contexto do presente artigo: (i) o *Wrapper Chaincode* que mantém a assinatura válida do agente da auditoria; (ii) o *App Chaincode* que mantém as informações das ferramentas usadas pelas organizações auditadas; (iii) o *Artifact Chaincode* que mantém as informações dos artefatos usados pelas organizações auditadas; e (iv) o *Log Chaincode* que mantém as informações de execução de mudanças das organizações auditadas. Além disso, todos os projetos de *smart contracts* foram construídos para serem usados em uma rede *blockchain* permissionada da infraestrutura do *Hyperledger Fabric*[7].

Projeto *Admin*. Este projeto possui uma aplicação para uso exclusivo da auditoria, no qual é possível interagir com os *smart contracts* dos projetos *Wrapper Chaincode*, *App Chaincode* e *Artifact Chaincode*. Nele, uma pessoa da auditoria pode consultar e alterar o *hash* válido do agente distribuído para as organizações auditadas, a lista de aplicações executoras de mudança homologadas e seus artefatos homologados.

Projeto *Wrapper*. O projeto *Wrapper* possui uma agente da auditoria criado para uso das organizações auditadas por essa auditoria. Através dele, a auditoria pode introduzir verificações pré e pós mudanças de TI que estejam sendo realizadas com o uso do agente. Durante uma mudança da organização, o agente executa os procedimentos pré-mudança. Logo em seguida, este executa a aplicação da organização responsável pela execução da mudança e, após o término da mudança, o agente executa os procedimentos pós-mudança. Por fim, o agente concentra todas as informações das execuções feitas por ele mesmo e pela aplicação executora da organização e as envia para a *blockchain* através do *smart contract Log Chaincode*. As informações salvas são: 1) da linha de comando responsável por invocar a aplicação executora da organização; 2) da aplicação executora (nome, localização na máquina e *hash*); 3) dos eventuais artefatos utilizados pela aplicação executora (nome, localização na máquina, *hash* e conteúdo); 4) do resultado dos procedimentos pré-mudança; 5) do resultado da mudança; e 6) do resultado dos procedimentos pós-mudança executados.

Projeto *Samples*. Este projeto concentra algumas ferramentas e artefatos utilizados para os fins da pesquisa deste artigo. Como ferramenta, criamos uma aplicação simples que

[6]O protótipo de prova de conceito, os scripts para execução dos experimentos e os artefatos produzidos como resultados da avaliação realizada estão disponíveis publicamente no GitHub [Fraga 2023]

[7]https://www.hyperledger.org

executa comandos *shell*, conforme descrito no artefato de insumo. Como artefatos, criamos diversos arquivos com a extensão "*.workflow*", contendo comandos de exemplo que podem ser utilizados em uma mudança. Por exemplo, podemos destacar dois dos fluxos criados no contexto do presente artigo: a instalação de pacote/aplicação na máquina e a criação de *cluster Kubernetes* em um provedor de serviços de nuvem.

Projeto *Checker*. Este projeto possui uma aplicação criada exclusivamente para a auditoria. Nele, é possível fazer análises nos sistemas e na infraestrutura da organização, em eventos de auditoria anuais, além de fazer verificações de conformidade. Essa verificação é feita comparando o estado atual dos sistemas e da infraestrutura com os estados anteriores registrados pela auditoria ou com os armazenados na *blockchain* ao longo das mudanças executadas.

5.2. Testes de Verificação do Protótipo

Para testar as aplicações e a abordagem proposta, definimos um cenário de uso por uma organização auditada que realiza algumas mudanças de TI em seus sistemas e em sua infraestrutura entre os eventos da auditoria. Essas mudanças para fins de testes se baseiam na instalação ou desinstalação de componentes de *software* na máquina alvo da mudança. Os testes foram conduzidos no sistema operacional *GNU/Linux*, no entanto, espera-se que tal prova de conceito seja bem sucedida em outros sistemas operacionais compatíveis com *Java*.

Primeiramente, precisamos configurar a rede *blockchain* permissionada *Hyperledger Fabric*. Para isso, utilizamos a ferramenta *Minifabric*, que fornece algumas funcionalidades para construção e gestão de uma rede *Hyperledger Fabric*, comumente usada em estudos e testes. Como segundo passo, configuramos nossos *smart contracts* do projeto *Chaincode* na rede *blockchain* criada através do *Minifabric*. A figura 4 mostra a topologia da rede configurada com dois nós pares (*peers*) de cada organização (auditoria e organização auditada), além de três nós ordenadores da auditoria e os quatro *smart contracts* criados em nossa abordagem.

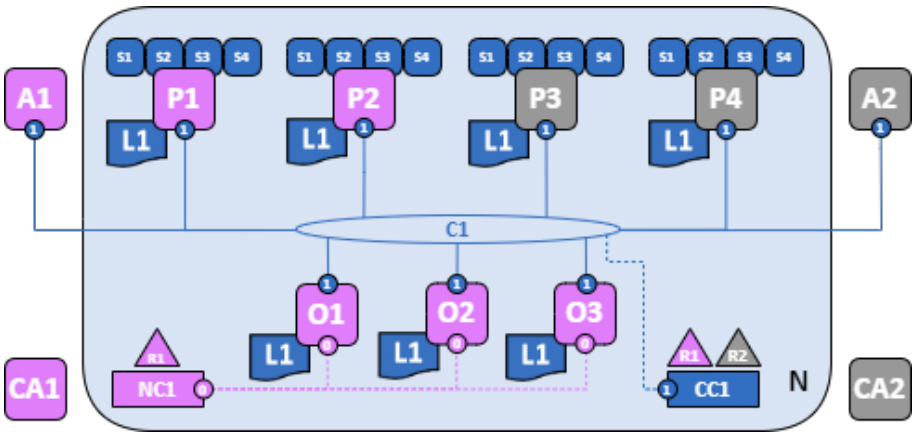

Figura 4. Topologia da rede *blockchain* utilizada nos testes do protótipo.

Após isso, com o aplicativo do projeto *Admin*, configuramos a identidade (par de chaves) a ser usada para interagir com a rede *blockchain*, no caso, a da auditoria, de modo que preparamos o aplicativo para utilizar os *smart contracts* existentes na rede. Com

isso, configuramos os *smart contracts* para armazenar a assinatura da versão do agente da auditoria (*Wrapper*), do aplicativo executor de mudanças e dos artefatos de fluxos de mudanças (*Samples*), todos em formato de *hash SHA3-256*.

Nesse estágio, já podemos iniciar as aferições de uma primeira visita da auditoria à organização e o processo de execução de mudanças de TI com o uso do agente da auditoria. Para tal, configuramos no aplicativo do projeto *Checker*, a identidade da auditoria para uso da rede *blockchain* e executamos uma ação de verificação do estado atual dos sistemas e da infraestrutura – no caso, a leitura da listagem completa de pacotes e aplicativos instalados na máquina que será alvo das mudanças de testes. Cabe ressaltar que a auditoria pode definir diferentes ações para serem conduzidas em suas inspeções anuais à organização.

Nesse momento, preparamos um *script* para simular a execução paralela de 25 mudanças de TI. Todas elas foram executadas através do aplicativo cliente da auditoria e do aplicativo executor de mudanças da organização. Com isso, pudemos avaliar a capacidade da nossa abordagem de utilizar uma rede *blockchain* para um cenário de mudanças concorrentes. Ao executar o *script*, foi possível monitorar a rede através da ferramenta *Hyperledger Explorer*, na qual se verificou todas as 25 transações de mudanças sendo processadas corretamente.

Por fim, simulando uma segunda visita da auditoria à organização, utilizamos o aplicativo do projeto *Checker* para avaliar as assinaturas na primeira e segunda inspeções. Mais especificamente, é verificado se a assinatura do estado atual dos sistemas e da infraestrutura corresponde à assinatura do estado resultante da simulação de todas as mudanças registradas na *blockchain* sobre o estado obtido na inspeção anterior (ou seja, analisando a validade das mudanças conforme o formalismo matemático da Seção 4).

5.3. Avaliação Experimental

A partir do uso do agente da auditoria como *software* iniciador do aplicativo executor das mudanças, e do armazenamento das informações relacionadas à mudança na *blockchain*, verificou-se qualitativamente uma redução do esforço manual de pessoas da organização ou da auditoria na obtenção de evidências de mudanças realizadas. Em relação ao custo computacional, verificou-se um *overhead* insignificante da execução do agente de auditoria contínua e do armazenamento na *blockchain*. Nesse caso, considera-se que o principal custo computacional está relacionado ao espaço em disco para armazenamento da própria *blockchain* – que fica a cargo da empresa de auditoria.

Do ponto de vista de integridade dos dados coletados, considerando que o agente da auditoria está presente na máquina da aplicação executora de mudanças, é correto afirmar que as informações recebidas pelo agente da auditoria são íntegras. Tal ocorre pois não há intermediação entre o processo do agente e do aplicativo executor e, portanto, as informações correspondem ao que de fato o aplicativo executor informa como saída de informações.

Além disso, o próprio agente da auditoria está conectado à *blockchain* para armazenamento das informações através da invocação do *smart contract Log Chaincode*. Assim sendo, podemos afirmar que o dado permanece íntegro do agente da auditoria até a rede *blockchain*, considerando que o protocolo utilizado pelo aplicativo com a *block-*

chain é o *gRPC (Google RPC)*[8] sobre HTTPS. Outrossim, a *blockchain* permissionada e suas características de integridade dos dados – através do sequenciamento e assinatura de transações em blocos distribuídos entre participantes da rede (chamado de *peers*) – também contribuem para a reafirmação da integridade das informações de mudanças de TI das organizações auditadas.

Verificamos que o agente da auditoria, uma vez integrado aos processos de execução de mudanças, permite que a auditoria realize verificações nos sistemas e na infraestrutura a cada mudança realizada, seja na etapa pré-mudança, seja na etapa pós-mudança. Pode ainda se beneficiar do que os dados desses dois momentos podem viabilizar, como as diferenças dos sistemas e da infraestrutura entre esses dois momentos. Com isso, a auditoria não apenas adquire uma capacidade de inclusão de processos diversos de verificação de conformidade em mudanças de TI, mas também torna-se capaz de elevar seus processos a um nível de auditoria contínua. Isso ocorre em virtude de que essas verificações seguem sendo realizadas a despeito da presença ou formalidade de uma visita de inspeção da auditoria.

Por fim, foi possível verificar que o estado dos sistemas e da infraestrutura nas inspeções da auditoria estava válido perante o que ela havia levantado de informações desde sua última visita, considerando os subsequentes estados dos sistemas e da infraestrutura a cada mudança de TI executada no período até então. Com isso, a auditoria se torna capaz de emitir pareceres de conformidade, para todo o período entre as inspeções, com maior grau de confiabilidade, pois deixa-se de avaliar apenas amostras do estado dos sistemas e da infraestrutura, e passa-se a verificar todo o histórico do período avaliado.

6. Discussão e Trabalhos Futuros

Uma premissa fundamental para a abordagem de auditoria contínua proposta é a colaboração por parte da organização auditada. Isso ocorre porque é essencial instalar, configurar e utilizar um agente da auditoria nos processos e ferramentas de mudanças de TI da organização. Considerando os benefícios para ambas as partes no cenário de adoção da abordagem proposta, e considerando que as organizações necessitam ser auditadas em algum nível durante suas relações comerciais, entende-se que existem as condições necessárias para viabilizar esta colaboração.

Em relação aos experimentos realizados, as aplicações de prova de conceito dessa abordagem foram concebidas e testadas exclusivamente em *Java* e sistema operacional *GNU/Linux*. De qualquer forma, as empresas de auditorias podem criar aplicações como estas em outras linguagens, observando outros sistemas operacionais ou ambientes, eliminando essa limitação da abordagem/solução proposta.

Do mesmo modo, entendemos que há oportunidades de pesquisa relacionadas à elevação dos níveis de segurança da abordagem proposta a partir do uso de *Hardware Security Modules* [Mavrovouniotis and Ganley 2014] nas máquinas nós da rede *blockchain*. Assim, a chave privada da organização ficaria inacessível no sistema de arquivos da organização.

Analisando os projetos da prova de conceito dessa estudo, temos oportunidades de exploração de um maior nível de auditoria contínua, através de proposições/evoluções do

[8]https://grpc.io

projeto *Checker*, de modo que se busque formas de remover ou de reduzir a necessidade de visitas frequentes da auditoria à organização auditada. Por fim, há espaço de avanços também na ideia base do projeto *Wrapper*, de modo que as organizações também possam utilizar dessa ferramenta de forma integrada a da auditoria, para executar verificações de seu próprio interesse em seus próprios sistemas e em sua infraestrutura, ainda no âmbito da segurança da informação.

7. Conclusão

Mudanças em sistemas e infraestruturas de tecnologia de informação são uma constante imprescindível para as organizações que dependem fortemente de TI. Dependendo das organizações, elas podem se deparar com processos de auditoria em suas relações comerciais e regulatórias. Porém, geralmente, essas auditorias ocorrem anualmente e envolvem trabalho manual de coleta de evidências e análises focadas em amostras.

Visando explorar soluções que pudessem garantir a conformidade de organizações auditadas entre eventos de auditoria, no que se refere às mudanças de TI executadas, este artigo apresenta uma abordagem de auditoria contínua para gestão de mudanças em TI usando *blockchain*. Almejamos responder quatro tópicos através dessa abordagem: (i) a redução do esforço manual de coleta de evidências para auditoria; (ii) a garantia da integridade dos dados coletados para a auditoria; (iii) a capacidade de inclusão de processos diversos de verificação para fins de auditoria nos processos de mudança da organização; e (iv) a verificação da integridade de sistemas e da infraestrutura entre eventos de auditoria.

Após implementação e testes de uma prova de conceito utilizando uma *blockchain* permissionada (*Hyperledger Fabric*), concluímos que a abordagem proposta endereça as hipóteses e as necessidades levantadas. Ela permite que organizações auditadas tenham menos esforço e preocupações na atividade de levantamento e no registro de evidências de suas mudanças de TI. Também a auditoria se beneficia de um ambiente mais confiável de evidências para análise, além da possível incorporação de verificações automatizadas nesse processo. Além disso, entendemos que esse estudo oferece uma linha de pesquisa importante para futuros pesquisadores no que tange à evolução da auditoria de TI para um modelo mais contínuo de análise de conformidade.

Referências

Aditya, B. R., Ferdiana, R., and Santosa, P. I. (2018). Toward modern it audit- current issues and literature review. *Proceedings of the 4th ICST 2018*, 1:1–6.

Axelos (2019). *ITIL Foundation*. The Stationery Office, 4th edition.

Byrnes, P. E., Al-Awadhi, A., Gullvist, B., Brown-Liburd, H., Teeter, R., Warren, J. D., and Vasarhelyi, M. (2018). Evolution of auditing: From the traditional approach to the future audit. *Continuous Auditing: Theory and Application*, pages 285–297.

Chan, D. Y. and Vasarhelyi, M. A. (2018). Innovation and practice of continuous auditing1. *Continuous Auditing: Theory and Application*, pages 271–283.

Chatziamanetoglou, D. and Rantos, K. (2023). Blockchain-based security configuration management for ict systems. *Electronics*, 12(8).

De Castro, M., Pereira, M., and Castro, M. (2022). Uma arquitetura baseada em blockchain para auditoria de conformidade com regulamentos de proteção de dados. In *Anais do XXII SBSeg 2022*, pages 390–395.

Fraga, C. (2023). Protótipo: Uma abordagem de auditoria contínua com blockchain para gerenciamento de mudanças em ti. Disponível em https://github.com/contaudit/contaudit.

Fraga, C., Abelém, A., Borges, V., Pinheiro, B., and Cordeiro, W. (2024). A blockchain-based approach for continuous auditing in it change management. In *NOMS 2024-2024 IEEE/IFIP Network Operations and Management Symposium*.

Gantz, S. D. (2013). *The Basics of IT Audit: Purposes, Processes, and Practical Information*. Syngress.

Han, H., Fei, S., Yan, Z., and Zhou, X. (2022). A survey on blockchain-based integrity auditing for cloud data. *Digital Communications and Networks*.

Hashem, R., Mubarak, A.-R., and Abu-Musa, A. (2023). The impact of blockchain technology on audit process quality: An empirical study on the banking sector. *International Journal of Auditing and Accounting Studies*, 5(1):87–118.

Isaca (2018). *COBIT 2019 Framework: Introduction and Methodology*. Isaca.

Macedo, L. and Campista, M. (2020). Tecnologia blockchain para auditoria em redes móveis. In *Anais do XXXVIII SBRC 2020*, pages 798–811.

Mahimkar, A., De Andrade, C. E., Sinha, R., and Rana, G. (2021). A composition framework for change management. *Proceedings of the ACM SIGCOMM 2021 Conference*, pages 788–806.

Marques, M., Simplicio, M., and Miers, C. (2022). Event2ledger: Container traceability using docker swarm and consortium hyperledger blockchain. In *Anais do XXII SBSeg 2022*, pages 103–110.

Mavrovouniotis, S. and Ganley, M. (2014). *Hardware Security Modules*. Springer.

Moeller, R. (2010). *IT Audit, Control, and Security*. Wiley.

Mohan, V. and Othmane, L. B. (2016). Secdevops: Is it a marketing buzzword? mapping research on security in devops. *Proceedings of the 11th International Conference on ARES 2016*, pages 542–547.

Pandey, A. and Mishra, S. (2014). Understanding it change management challenges at a financial firm. *Proceedings of the ISECON 2014*, pages 1–10.

Rysbekov, A. (2022). Continuous compliance: Devops approach to compliance and change management. Master's thesis, University of Oslo, Oslo, Norway.

Vries, T. d. (2022). Anomaly detection in it audit: The possibilities and potential in the domain of it audit. Master's thesis, University of Turku, Amsterdam, Netherlands.

Zaydi, M. and Nassereddine, B. (2021). A machine learning based secure change management. *Studies in Computational Intelligence*, 919:505–519.

Zheng, Z., Xie, S., Dai, H. N., Chen, X., and Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4):352–375.