UNIVERSIDADE FEEVALE

DIOVANE BARBIERI GABRIEL

TRILHAS DE AUDITORIA COM BLOCKCHAIN: UMA ANÁLISE DE DESEMPENHO OPERACIONAL

(Título Provisório)

Anteprojeto de Trabalho de Conclusão

Novo Hamburgo
2020

DIOVANE BARBIERI GABRIEL

TRILHAS DE AUDITORIA COM BLOCKCHAIN: UMA ANÁLISE DE DESEMPENHO OPERACIONAL

(Título Provisório)

Anteprojeto de Trabalho de Conclusão de Curso, apresentado como requisito parcial à obtenção do grau de Bacharel em Sistemas de Informação pela Universidade Feevale

Orientador: Prof. Dra. Adriana Neves dos Reis

Novo Hamburgo
2020

RESUMO

A informação tem se tornado cada vez mais um recurso valioso dentro das organizações, e para proteger e garantir a sua integridade, conceitos antigos de trilhas de auditoria têm sido aprimorados, e novas técnicas de segurança estão sendo criadas à medida que novas tecnologias vão surgindo. Pensando nisso autores da atualidade criaram novas abordagens utilizando a crescente tecnologia do *blockchain* que permite que informações sejam armazenadas em seu interior de forma que não possam mais ser alteradas. Desta forma é possível utilizar o conceito convencional de trilha de auditoria, a partir da geração de *logs*, e gravá-los no interior do *blockchain*, ganhando a propriedade da imutabilidade e separando as informações do dispositivo titular do sistema, pois um registro de *log*, armazenado no mesmo equipamento, é igualmente vulnerável. Sendo assim, este trabalho tem como objetivo implementar uma alternativa própria para utilização do *blockchain* para trilha de auditoria, e assim fazer experimentos comparativos buscando analisar o desempenho e operacionalidade de diferentes abordagens propostas.

Palavras-chave: *Blockchain*. *Log*. Trilha de auditoria. Análise.

SUMÁRIO

MOTIVAÇÃO

Cada vez mais a informação torna-se um recurso crítico dentro das organizações. O crescente número de dispositivos e computadores conectando todos os tipos de usuários por todo mundo, faz com que cada vez mais dados sejam processados em menores períodos de tempo. Para ser capaz de entender o que implica a segurança de um computador, é necessário compreender os termos exposição, vulnerabilidade e risco (BOSWORTH; KABAY, 2002).

A vulnerabilidade é um ponto fraco em sistema computacional ou nos meios que o cercam que pode comprometer a segurança. Um risco, dentro da computação, é a probabilidade de um evento ocasionar uma perda de qualquer natureza, como por exemplo, perdas financeiras e de pessoal, perda de reputação e clientes, incapacidade de operar normalmente ou completamente durante um período de tempo, incapacidade de crescimento, e violação de leis e regras governamentais (BOSWORTH; KABAY, 2002). Em casos onde a propriedade do dispositivo é diferente da propriedade dos segredos contidos dentro do mesmo, é essencial que existam formas e mecanismos de auditoria que possam identificar e determinar qualquer tentativa de fraude (SCHNEIER; KELSEY, 1999).

Precauções especiais devem ser tomadas a fim de validar a integridade e assegurar que dados críticos sejam devidamente protegidos. A principal medida a ser tomada para evitar esse tipo de perda é a auditoria. O papel da auditoria inclui recomendar iniciativas que minimizem, ou preferencialmente, eliminem vulnerabilidade e riscos, garantir que os devidos controles de segurança estejam em vigor, determinar se os dispositivos de auditoria e segurança são válidos, e verificar se os parâmetros, trilhas de auditorias e mecanismos de segurança estão funcionando da forma devida (BOSWORTH; KABAY, 2002).

Em sistemas computacionais, ações relacionadas às operações do usuário e controle de aceso devem ser mantidas em arquivos de *log* seguros para detecção de violações e intrusões ou para objetivos relacionados à auditoria do sistema (XU et al, 2005). Nos arquivos de *log* é comum que sejam armazenados uma grande quantidade de informações sigilosas. Sendo assim, é de extrema importância garantir que, em caso de violações do sistema, tais *logs* não sejam comprometidos e que a violação possa ser detectada (XU et al, 2005). No caso de um atacante experiente, o primeiro objetivo será obter acesso ao sistema de *log* de auditoria para que seja possível apagar qualquer vestígio que sinalize o ataque, e manter o modus operandi em segredo perante aos administradores do sistema, mantendo assim esse método disponível para ataques futuros (BELLARE; YEE, 1997).

Considerando os cenários citados, é importante destacar que em casos onde os arquivos de *logs* são armazenados no mesmo dispositivo da aplicação, em situações de ataques as duas informações podem estar igualmente vulneráveis e poderão ser comprometidas. Pensando nisso novas formas de assegurar a integridade dos dados e dos *logs* estão sendo elaboradas, como é a abordagem proposta por Rosco Kalis e Adam Belloum (2018), que utiliza da geração de *hash* dos *logs* gerados pela trilha de auditoria, para enviar ao *blockchain*. Desta forma, estes dados ficarão completamente isolados e independentes do sistema principal.

Com a tradução literal de *blockchain* tem-se o que podemos chamar de "cadeia de blocos" ou "corrente de blocos", o que justamente sugere seu funcionamento. De acordo com Galen et al. (2018), *blockchain* trata-se de um livro de registros de transações públicas, seguro e digital. Um *blockchain* é fundamentalmente um banco de dados distribuído em um registro público, com todos os eventos e transações digitais realizadas e compartilhadas entre todos os seus participantes (CROSBY et al., 2016). Caso algum desses participantes tente adulterar algum bloco, este último será descartado, pois será comparado ao restante dos participantes. Desta forma, para que seja possível a adulteração de informações do *blockchain*, seria preciso um ataque que atingisse ao mesmo tempo mais de 50% dos participantes, "o que é operacionalmente impossível". (SANT'ANA, 2018, p. 4).

Além do conceito básico do *blockchain* é importante também conhecer e entender o conceito de *Smart Contracts*, ou no português, "Contratos Inteligentes". Contratos inteligentes são uma forma de fazer cumprir digitalmente um contrato ou acordo entre partes através de um código computacional (KALIS; BELLOUM, 2018). Kalis e Bellum (2018) seguem dizendo que este conceito é anterior ao *blockchain* mais de uma década, mas apenas quando o *blockchain* foi implementado finalmente foi possível implementar esses contratos sem a necessidade de um terceiro confiável para execução do contrato.

Ethereum trata-se de uma plataforma descentralizada que implementa *blockchain* e oferece a capacidade de publicar contratos inteligentes em seu *blockchain*, que pode ser executado pelo *Ethereum Virtual Machine* (EVM) (KALIS; BELLOUM, 2018). Ao publicar esses contratos para o Ethereum *blockchain*, todas as partes envolvidas podem inspecionar facilmente o contrato e terão a garantia de que o contrato execute exatamente como especificado (KALIS; BELLOUM, 2018).

A proposta de Kalis e Belloum (2018) consiste em armazenar parâmetros durante a interação do usuário, e ao final, o método de publicação é chamado, para enviar o

identificador *hash* de auditoria para o contrato inteligente Ethereum. Este método é executado de forma assíncrona, para que o resto do aplicativo possa continuar em execução, enquanto a transação é executada no *blockchain*.

Como trata-se de processamento assíncrono, pois pode levar algum tempo até que a transação seja executada e aceita no *blockchain*, em situação de falha ou interrupção da aplicação durante o processo de auditoria, uma entrada de auditoria incompleta poderia ser gravada no banco de dados, enquanto nada é enviado para o *blockchain*, o que invalidaria a trilha de auditoria. Outro ponto negativo observado no método utilizado, é que quando cinco ou mais transações estão sendo processadas simultaneamente ocasionam falha. Isso geralmente não é um problema para aplicativos menores, mas pode definitivamente impactar aplicativos maiores (KALIS; BELLOUM, 2018).

Partindo deste contexto, o presente trabalho visa desenvolver uma implementação própria de trilha de auditoria utilizando *blockchain*, permitindo aplicar experimentos de comparação e análise relativos à proposta de Kalis e Bellum para avaliar na prática como tais implementações se comportam em determinados cenários de baixa e grande demanda computacional, podendo assim determinar a viabilidade destas aplicações. Isto também motivado pelo escasso número de discussões sobre o tema na literatura científica.

OBJETIVOS

Objetivo geral

Aplicar a tecnologia do *blockchain*, para armazenamento de informações que sirvam de lastro para autenticar a integridade de dados através de trilhas de auditoria, tendo como base o conceito convencional de geração de *logs*. Além disso, espera-se contribuir com resultados extraídos de experimentos comparativos entre diferentes implementações que utilizam desta tecnologia, para determinar melhores e piores opções em diferentes cenários, de acordo com o contexto aplicado.

Objetivos específicos

- Implementar uma solução própria para armazenamento de informações de *log* no *blockchain*.
- Criar experimentos comparativos medindo performance entre diferentes propostas de implementação.
- Evidenciar vantagens e desvantagens de cada implementação nos diferentes cenários.
- Formular recomendações sobre as diferentes propostas de implementação, de acordo com diferentes contextos.

METODOLOGIA

Este trabalho do ponto de vista de sua natureza, enquadra-se como experimental, pois consiste, especialmente, em aplicar os itens de sob influência de determinadas variáveis, em situações conhecidas e controladas, para então visualizar os resultados produzidos pelo experimento sobre o objeto (GIL, 2008).

Partindo desta metodologia, este trabalho consiste em aplicar experimentos práticos sobre uma implementação própria para envio de informações de trilha de auditoria para o *blockchain*. Da mesma forma, utilizará outra implementação sugerida por Kalis e Belloum (2018), aplicando os mesmos testes e variáveis, a fim de analisar o seu desempenho, de forma comparativa. Com os resultados obtidos será possível identificar qual proposta demonstra o melhor resultado, e formular recomendações de qual melhor se aplica em sistemas com maior ou menor demanda de transações. Para executar as práticas de experimento, este trabalho terá como base o procedimento abaixo descrito, como sugerido por Turrioni e Mello (2012):

a) Planejamento do experimento;

b) Operacionalização das variáveis;

c) Estabelecimento das relações causais;

d) Definição das técnicas de análise dos dados do experimento;

e) Especificação da unidade de análise ou montagem do banco de ensaio;

f) Especificação do tempo para condução do experimento;

g) Projeto do experimento;

h) Realização do experimento e coleta de dados;

i) Análise estatística;

j) Análise dos resultados;

k) Conclusão;

l) Redação e publicação dos resultados.

Dessa forma será possível apresentar todo o processo de forma padronizada, objetiva e clara.

CRONOGRAMA

Trabalho de Conclusão I

Etapa	Meses				
	Ago	Set	Out	Nov	Dez
Anteprojeto					
Definir as tecnologias a serem utilizadas na implementação própria					
Implementar proposta própria para envio de trilhas de auditoria ao *blockchain*					
Replicar implementação proposta por Kalis e Belloum (2018) para trilhas de auditoria utilizando *blockchain*.					
Redigir TCC 1					
Entregar TCC 1					

Trabalho de Conclusão II

Etapa	Meses				
	Fev	Mar	Abr	Mai	Jun
Determinar procedimentos dos experimentos					
Aplicar experimentos em ambas implementações					
Analisar os resultados dos experimentos					
Identificar os melhores resultados e melhores aplicações					
Redigir TCC 2					
Entregar TCC 2					

BIBLIOGRAFIA

BELLARE, Mihir; YEE, Bennet. **Forward integrity for secure audit logs**. Technical report, Computer Science and Engineering Department, University of California at San Diego, 1997.

BOSWORTH, Seymour; KABAY, Michel E. (Ed.). **Computer security handbook**. John Wiley & Sons, 2002.

CROSBY, Michael et al. **Blockchain technology: Beyond bitcoin**. Applied Innovation, v. 2, n. 6-10, p. 71, 2016.

GALEN, Doug et al. **Blockchain for social impact**: moving beyond the hype. Center for Social Innovation, RippleWorks. https://www.gsb.stanford. edu/sites/gsb/files/publication-pdf/study-blockchain-impact-moving-beyond-hype_0.pdf, 2018.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. Editora Atlas SA, 2008.

KALIS, Rosco; BELLOUM, Adam. **Validating data integrity with blockchain**. In: 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom). IEEE, 2018. p. 272-277.

SANT'ANA, Rafael Ribeiro Péret de, **REVOLUÇÃO BLOCKCHAIN: Os contratos inteligentes.** Pontifícia Universidade Católica de Minas Gerais (PUC), 2018.

SCHNEIER, Bruce; KELSEY, John. **Secure audit logs to support computer forensics**. ACM Transactions on Information and System Security (TISSEC), v. 2, n. 2, p. 159-176, 1999.

TURRIONI, João Batista; MELLO, Carlos Henrique Pereira. **Metodologia de pesquisa em engenharia de produção**. Programa de Pós-Graduação em Engenharia de Produção da Universidade Federal de Itajubá. Itajubá: UNIFEI, 2012.

XU, Wensheng; CHADWICK, David W.; OTENKO, Sassa. **A PKI based secure audit web server**. IASTED Communications, Network and Information and CNIS, 2005.