Disponibilização Segura, Automática e Confiável de Dados Proprietários utilizando Corrente de Blocos

Gustavo F. Camilo, Miguel Elias M. Campista,
Luís Henrique M. K. Costa, Otto Carlos M. B. Duarte*

[1]Grupo de Teleinformática e Automação (GTA)
Universidade Federal do Rio de Janeiro (UFRJ)

Resumo. *A Lei Geral de Proteção de Dados Pessoais (LGPD) determina o respeito à privacidade como fundamental para a proteção de dados proprietários no Brasil, garantindo o poder de controle dos cidadãos sobre os próprios dados. Entretanto, sistemas atuais de compartilhamento e comercialização de dados delegam a confiança a serviços centralizados, restringindo este controle. Este projeto propôs um sistema seguro, ágil e eficaz para a comercialização de dados automatizada, distribuída e transparente entre múltiplos domínios administrativos utilizando corrente de blocos (blockchain), contratos inteligentes, reputação e confiança. O sistema proposto utiliza a tecnologia de corrente de blocos para garantir o armazenamento seguro e distribuído das permissões de acesso dos usuários, devolvendo ao proprietário o controle sobre os próprios dados. Um protótipo do sistema proposto foi desenvolvido utilizando a plataforma de código-aberto Hyperledger Fabric para a implementação de contratos inteligentes e de uma rede de corrente de blocos. Os resultados de avaliação de desempenho mostram que o sistema proposto provê segurança e privacidade na comercialização de dados entre domínios de maneira distribuída, ágil e eficaz, atendendo simultaneamente mais de 200 requisições por segundo e punindo efetivamente o comportamento malicioso.*

1. Introdução

A centralização de soluções para compartilhamento de dados restringe o poder do usuário sobre os próprios dados. Esta centralização afeta fortemente os proprietários de dados, que: (i) transferem o controle sobre os próprios dados para o provedor de serviço; (ii) são obrigados a assinar termos de serviço que comprometem a própria privacidade ou a privacidade dos seus dados e (iii) devem pagar altas taxas ao provedor de serviço para utilizar o sistema. Como os dados são geralmente armazenados em claro, i.e., não-criptografados, o comprometimento desses serviços centralizados por um atacante pode acarretar no vazamento de dados privados de milhões de pessoas. Recentemente, um vazamento de dados resultou na exposição dos dados de mais de 200 milhões de brasileiros [Canaltech 2022, g1.com 2022]. A centralização da confiança em um serviço também cria um ponto único de falhas. Essa característica torna o sistema suscetível a ataques de negação de serviço (*Denial of Service* - DoS), que geram indisponibilidade ao usuário final. Dessa maneira, faz-se necessário um sistema distribuído e seguro para o compartilhamento de dados e que entregue o poder de decisão de volta ao usuário proprietário.

*In memoriam.

Este trabalho de iniciação científica propôs um sistema baseado na tecnologia de corrente de blocos para garantir o compartilhamento seguro, distribuído e automático de dados em cenários com múltiplos domínios administrativos sem confiança mútua e interconectados. O sistema proposto utiliza a tecnologia de corrente de blocos (*blockchain*), estrutura de dados imutável e distribuída [Nakamoto 2008], para o armazenamento das permissões de acesso, permitindo que usuários proprietários mantenham controle sobre quem possui acesso aos dados proprietários. O armazenamento somente dos metadados e não dos dados na corrente de blocos previne que a corrente de blocos não cresça a uma alta taxa e torna o sistema mais simples [Andersen et al. 2017]. Além disso, o sistema proposto utiliza a tecnologia de contratos inteligentes, códigos auto-executáveis na corrente de blocos, para estabelecimento e atualizações de permissões de acesso de maneira automática e distribuída de acordo com regras definidas pelo usuário. O trabalho também aproveita a robustez da corrente de blocos a ataques de gasto duplo para permitir a recompensa segura a usuários proprietários em compartilhar seus dados. Por fim, o trabalho implementa um protótipo da arquitetura proposta usando a plataforma de código-aberto Hyperledger Fabric [Androulaki et al. 2018] para a corrente de blocos, o controlador Ryu e o emulador de redes Mininet [Lantz et al. 2010]. Os resultados da avaliação de desempenho mostram que o sistema proposto atende de maneira rápida às requisições de acesso de centenas de usuários em cenários reais, atingindo vazão de transação maior que a de comércios eletrônicos a nível nacional.

A utilização da tecnologia de corrente de blocos assegura a imutabilidade dos registros da transferência de ativos. Entretanto, a corrente de blocos sozinha não é suficiente para garantir a entrega de dados armazenados fora da corrente (*off-chain*) e tampouco atesta a qualidade deles. Usuários maliciosos podem aproveitar essa vulnerabilidade para efetuar ataques e anunciar dados falsos ou não entregar dados adquiridos por compradores honestos. Assim, o trabalho também propôs e desenvolveu um sistema de reputação e confiança (*Trust and Reputation System* - TRS) confiável, imutável e distribuído utilizando os contratos inteligentes. Participantes honestos podem facilmente verificar a reputação de outros usuários do sistema de maneira rápida verificando informações publicamente disponíveis na corrente de blocos. O sistema de reputação desenvolvido se baseia nos conceitos de reputação e confiança do cotidiano para simular comportamento próximo ao encontrado na vida real. Resultados de avaliação de desempenho de um protótipo desenvolvido mostram que o sistema proposto é eficaz na detecção e punição de comportamento malicioso dos vendedores, reduzindo os danos causados por atacantes.

O restante do artigo está organizado da seguinte forma. A Seção 1.1 apresenta o impacto da pesquisa desenvolvida. A Seção 2 detalha o sistema proposto, descrevendo a aquitetura proposta e o sistema de reputação desenvolvido. A Seção 3 apresenta os resultados obtidos de um protótipo desenvolvido do sistema. Por fim, a Seção 4 conclui o artigo.

1.1. Impacto

O trabalho de iniciação científica aqui descrito recebeu o prêmio de Melhor Trabalho em Sessão de Apresentação do Centro de Tecnologia com a apresentação intitulada “Um Sistema Distribuído para o Compartilhamento Seguro e Automático de Dados através de Corrente de Blocos” na XLII Jornada Giulio Massarani de Iniciação Científica, Tecnológica, Artística e Cultural (JICTAC 2020) da Universidade Federal do Rio de Ja-

neiro em maio de 2021. Além disso, este trabalho também gerou uma menção honrosa no III Workshop em Blockchain: Teoria, Tecnologias e Aplicações do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos [Camilo et al. 2020a]. Um protótipo da proposta foi desenvolvido e disponibilizado publicamente no repositório do laboratório: `https://github.com/GTA-UFRJ-team/blockchain-marketplace`. Por fim, este trabalho serviu de base para o Projeto de Graduação do autor intitulado "Compartilhamento Seguro, Distribuído e Automático de Dados através de Corrente de Blocos" e gerou as seguintes quatro publicações em conferências nacionais e internacionais [Camilo et al. 2020a, Camilo et al. 2020b, Camilo et al. 2021, Camilo et al. 2020c]:

- **Camilo, G. F.**, Rebello, G. A. F., de Souza, L. A. C., Duarte, O. C. M. B. - "AutAvailChain: Automatic and Secure Data Availability through Blockchain", em IEEE Global Communications Conference (GLOBECOM 2020), Taipei, Taiwan, Dezembro 2020. **Classificação A1 pelo Qualis da CAPES**.
- **Camilo, G. F.**, Rebello, G. A. F., Souza, L. A. C., Duarte, O. C. M. B. - "AutAvailChain: Disponibilização Segura, Controlada e Automática de Dados IoT usando Corrente de Blocos", em III Workshop em Blockchain: Teoria, Tecnologias e Aplicações do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (WBlockchain SBRC 2020), Rio de Janeiro, Brasil, Dezembro 2020. **Menção Honrosa**.
- **Camilo, G. F.**, Rebello, G. A. F., Souza, L. A. C., Duarte, O. C. M. B., "A Secure Personal-Data Trading System Based on Blockchain, Trust, and Reputation", em 3rd IEEE International Conference on Blockchain (Blockchain 2020), Rhodes, Grécia, Novembro 2020.
- **Camilo, G. F.**, Rebello, G. A. F., Souza, L. A. C., Duarte, O. C. M. B., "Um Sistema Seguro de Comercialização de Dados Pessoais Sensíveis baseado em Reputação, Confiança e Corrente de Blocos", em XX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg 2020), Petrópolis, Brasil, Outubro 2020.

Além dos trabalhos citados acima, o autor participou no desenvolvimento de mais de 10 artigos publicados em conferência nacionais e internacionais. As seguintes publicações que o autor participou ajudaram a formar a base de conhecimento na área do trabalho desenvolvido:

- Rebello, G. A. F., **Camilo, G. F.**, Guimarães, L. C. B., de Souza, L. A. C., Thomaz, G. A., Duarte, O. C. M. B. - "A Security and Performance Analysis of Proof-based Consensus Protocols", in Annals of Telecommunications, 2021. (Accepted for publication)
- Souza, L. A. C., Rebello, G. A. F., **Camilo, G. F.**, Guimarães, L. C. B., Duarte, O. C. M. B., "DFedForest: Decentralized Federated Forest", em 3rd IEEE International Conference on Blockchain (Blockchain-2020), Rhodes, Grécia, Novembro 2020.
- Rebello, G. A. F., **Camilo, G. F.**, Guimarães, L. C. B., Souza, L. A. C., Duarte, O. C. M. B., "On the Security and Performance of Proof-based Consensus Protocols", em 4th Conference on Cloud and Internet of Things (CIoT 2020), Niterói, Brasil, Outubro 2020
- Rebello, G. A. F., **Camilo, G. F.**, Guimarães, L. C. B., Souza, L. A. C., Duarte, O. C. M. B., "Security and Performance Analysis of Quorum-based Block-

chain Consensus Protocols", Relatório Técnico, Programa de Engenharia Elétrica, COPPE/UFRJ, 2020.

- Rebello, G. A. F., **Camilo, G. F.**, Silva, L. G. C., Guimarães, L. C. B., Souza, L. A. C., Alvarenga, I. D. e Duarte, O. C. M. B. - "Provendo uma Infraestrutura de Software Fatiada, Isolada e Segura de Funções Virtuais através da Tecnologia de Corrente de Blocos", em II Workshop em Blockchain: Teoria, Tecnologias e Aplicações (WBlockchain SBRC 2019), Gramado, Brasil, Maio 2019. **Prêmio de melhor artigo**.

2. Compartilhando Dados de Maneira Segura

O sistema proposto busca automatizar as atualizações de permissão de acesso, uma vez que a atualização manual de permissões requer a constante disponibilidade do usuário proprietário. Para garantir essa automatização, o sistema utiliza a tecnologia de contratos inteligentes aliada a controladores de redes definidas por *software* (*Software Defined Networking* - SDN). O cenário da proposta considera o compartilhamento entre grandes centros de dados que oferecem serviços de armazenamento em nuvem interconectados através da tecnologia SDN. Dessa maneira, a atualização das permissões de acesso consiste em dois níveis. No primeiro nível, os contratos inteligentes analisam as requisições de acesso para validar uma solicitação de acesso com base em uma política previamente determinada. Caso o usuário cumpra a política definida, o contrato atualiza a permissão de acesso do usuário aos dados de maneira automática e sem necessidade de intermediário e publica a atualização na corrente de blocos. No segundo nível, o controlador SDN recebe a requisição de acesso do usuário à máquina que armazena os dados e verifica na corrente de blocos se o usuário possui permissão de acesso.

Para estabelecer a interação entre as tecnologias utilizadas, o trabalho propôs uma arquitetura dividida em dois módulos principais, como mostra a Figura 1. O Módulo de Corrente de Blocos armazena um registro das permissões de acesso de um usuário a um recurso, registra os anúncios e demandas de aquisição de dados no sistema. Este módulo contém a estrutura da corrente de blocos [Nakamoto 2008], que armazena os contratos inteligentes e registra de maneira imutável o histórico de transações emitidas no sistema. No contexto de controle de acesso e comercialização de dados proposto, as transações consistem em operações de requisições de acesso ou compra e venda de dados dos usuários. Essas operações são registradas publicamente na corrente de blocos, garantindo que os proprietários mantenham os dados sob controle.

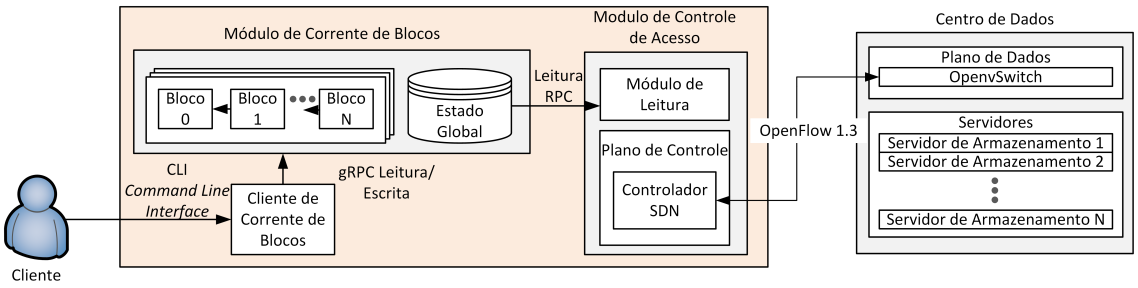


Figura 1. Arquitetura do sistema proposto. O cliente comprador (vendedor) anuncia dados próprios (adquire dados) através da corrente de blocos.

O Módulo de Controle de Acesso gerencia as permissões de acesso a um recurso a nível de rede e é composto pelo controlador SDN e pelo módulo de leitura. O módulo de leitura lê a corrente de blocos através de chamadas de procedimentos remotos (RPC - *Remote Procedure Call*) e repassa as informações adquiridas para o plano de controle. O controlador armazena quais usuários têm acesso ao servidor de armazenamento em uma tabela que relaciona as permissões aos endereços IP de origem e destino. Ao receber uma nova requisição, o plano de controle atualiza as permissões de acesso armazenadas localmente, permitindo que os usuários possam se conectar ao servidor que armazena os dados previamente adquiridos através da corrente de blocos. Caso um usuário sem permissão tente estabelecer conexão ao servidor, o controlador verifica na corrente de blocos através do módulo de leitura se as permissões concedidas foram atualizadas. Caso estejam desatualizadas, o controlador atualiza a versão local das permissões dos servidores, atendendo as transações a serem processadas.

O trabalho aproveita as características de robustez da corrente de blocos contra ataques a gastos duplos para estabelecer um mercado de dados, em que os proprietários e interessados podem anunciar e procurar por dados. Assim, o sistema define dois tipos de usuários: vendedores e compradores. Vendedores são proprietários de dados que escolhem por comercializar os seus dados e pedem uma recompensa por eles. Compradores interessados podem efetuar buscas por anúncios da corrente de blocos para adquirir dados. Apesar da separação em dois tipos de usuários, um participante pode assumir os dois papéis, tanto anunciando seus dados, como comprando dados de outros proprietários.

Vendedores e compradores utilizam três tipos de transação propostos pelo trabalho que são armazenadas na corrente de blocos e garantem a comercialização segura de dados. Vendedores emitem transações de anúncio para divulgar publicamente o tipo de dados que possui e o preço deles. Como a transação de anúncio é armazenada publicamente na corrente de blocos, compradores podem facilmente encontrar anúncios que os interessem e comprar utilizando uma transação de compra. A transação de compra referencia a transação de anúncio para facilitar a verificação de pagamento por um contrato inteligente e registra o endereço do comprador para que o controlador SDN atualize as permissões de acesso. Por fim, este trabalho assume que os dados são armazenados de maneira criptografada para evitar vazamento a terceiros não autorizados. Assim, faz-se necessária uma etapa adicional em que o vendedor emite automaticamente uma transação de resposta contendo a chave para decifrar os dados criptografada com a chave pública do comprador para garantia de confidencialidade.

2.1. Reputação e Confiança

A corrente de blocos sozinha não garante a entrega de dados armazenados fora da corrente (*off-chain*) e tampouco a qualidade deles. Vendedores maliciosos podem efetuar ataques anunciando dados falsos ou simplesmente falhando em entregar dados honestamente adquiridos. Este trabalho também propôs um sistema de reputação e confiança (*Trust and Reputation System* - TRS) que permite que compradores possam ter uma noção prévia do produto oferecido e das intenções do vendedor baseado em avaliações de outros compradores na rede. O TRS desenvolvido utiliza métodos matemáticos para modelar a evolução da confiança e reputação de um vendedor no sistema baseado em interações da vida real. Assim, o modelo utilizado garante que a confiança de um comprador em um vendedor aumente gradualmente com interações positivas e diminua drasticamente

com qualquer interação negativa. Na confiança do vendedor, o modelo ainda considera que as interações recentes são mais relevantes que as interações do passado para permitir possíveis alterações no comportamento de um vendedor. O modelo utiliza uma função de envelhecimento adaptativa para implementar o esquecimento gradual de interações passadas, expressa por:

$$I_n = \sum_{i=1}^{n} \beta^{(n-i)} \delta_i, \tag{1}$$

em que β é o fator de esquecimento, n é o total de interações ocorridas e δ_i é o valor associado a cada interação. Se a interação i for positiva, $\delta_i = \delta_+ > 0$. Caso contrário, $\delta_i = \delta_- < 0$. Utilizando $|\delta_-| \gg |\delta_+|$, as interações negativas pesam mais do que as interações positivas e o modelo é capaz de simular a confiança igual a da vida real.

O trabalho desenvolvido optou por adotar um fator de esquecimento que se adapta de acordo com a probabilidade de o vendedor agir honestamente [Sun et al. 2008]. Essa abordagem busca assimilar o modelo com interações reais, em que interações recentes são mais significativas que interações passadas. Para modelar a probabilidade de um vendedor agir honestamente, este trabalho utiliza uma distribuição β com probabilidade *a priori* de $\frac{1}{2}$. A atualização da distribuição é calculada a cada nova interação através de inferência Bayesiana e utiliza o valor esperado $E[p] = \frac{\delta_+ + 1}{\delta_+ + \delta_- + 2} = \beta$ da nova distribuição para estimar a probabilidade de o vendedor agir honestamente naquele momento. O trabalho optou pelo fator de esquecimento adaptativo devido à sua robustez contra ataques de dissimulação. Neste tipo de ataque, um vendedor malicioso comporta-se bem apenas o suficiente para recuperar sua reputação na rede e voltar a agir maliciosamente. O fator de esquecimento adaptativo garante que, se a probabilidade do vendedor ser honesto é alta, i.e. $E[p] \to 1$, o sistema leva mais tempo para esquecer o passado do vendedor, recompensando-o por suas boas ações. Por outro lado, ações maliciosas do vendedor levam à baixa probabilidade de ser honesto, i.e. $E[p] \to 0$, e suas ações passadas honestas são rapidamente esquecidas e, assim, o peso de suas ações maliciosas recentes sobre a reputação é maior. Após calcular I_n, o modelo calcula o novo valor da confiança de um comprador i em um vendedor j utilizando a função de Gompertz, como mostra a Equação 2. Na equação, a, b e c são constantes que representam a assíntota, o parâmetro de deslocamento ao longo do eixo x e a taxa de crescimento da confiança, respectivamente. O trabalho optou pela função de Gompertz dada sua característica de aumentar gradualmente, simulando a confiança na vida real, e ao fácil ajuste do seu formato através das constantes a, b e c. Assim, a confiança de um comprador i em um vendedor j pode ser expressa por:

$$s_{ij} = a \exp(-b \exp(-cI_n)). \tag{2}$$

Assim, como as transações de compra e venda de dados, o trabalho define mais uma transação, a transação de avaliação, para que compradores possam avaliar um produto adquirido. O armazenamento da transação de avaliação na corrente de blocos garante que todos os participantes da rede tenham acesso às avaliações e a tecnologia de contratos inteligentes garante que o cálculo correto da reputação de maneira distribuída.

3. Avaliação de Desempenho

Um protótipo da proposta foi desenvolvido utilizando a plataforma de código aberto Hyperledger Fabric 2.0 [Androulaki et al. 2018] para a corrente de blocos, o emulador de rede virtual Mininet [Lantz et al. 2010] e o controlador de redes definidas por *software* Ryu[1]. O Hyperledger Fabric é uma plataforma de código-aberto que permite o desenvolvimento de redes de corrente de blocos permissionadas entre organizações. O aspecto organizacional do Hyperledger é adequado ao cenário da proposta, que considera múltiplos domínios administrativos interconectados. Apesar do protótipo utilizar o Hyperledger Fabric, o sistema proposto é agnóstico a uma corrente de blocos específica e pode ser implementado em outras plataformas que suportam contratos inteligentes. Os resultados apresentam intervalo de confiança de 95%.

Um contrato inteligente escrito em linguagem Go é executado em todos os pares, eliminando uma entidade centralizada de confiança e implementando as lógicas de transação descritas na seção anterior, além de um sistema de *tokens* e contas de organizações. Esses *tokens* funcionam como moedas que as organizações podem usar para a comercialização de dados. O valor real desses *tokens* pode ser acordado fora da corrente (*off-chain*) entre as organizações.

O primeiro cenário de teste do protótipo foi implementado de maneira distribuída em dois computadores, que simulam duas organizações que participam da corrente de blocos: um Intel i7-8700 CPU 3.40 GHz com 32 GB de RAM executa a Organização 1; um Intel i7-7700 CPU 3.60 GHz com 64 GB de RAM executa a Organização 2. Três Intel Xeon E5-2609v4 CPU 1.70 GHz com 8 GB de RAM foram adicionados ao cenário anterior como Organizações 3, 4 e 5. O experimento avalia a vazão de transações variando o número de clientes que emitem 50 e 500 transações na Organização 1, que é a única organização que emite transações. A Figura 2 apresenta o resultado com um número crescente de clientes em três computadores para verificar a escalabilidade do sistema proposto. A taxa de transação atinge um pico de cerca de 243 transações por segundo, o que é o suficiente para atender de maneira eficiente um cenário de mercado a nível nacional[2]. A figura também mostra uma tendência de crescimento no valor dessa taxa, o que expõe que o resultado ainda não atingiu o máximo de vazão suportada no processamento das requisições. O resultado prova que, mesmo quando o número de organizações aumenta em um cenário próximo ao real, o sistema atende de maneira rápida e eficiente a centenas de requisições por segundo.

O segundo experimento avaliou o tempo de acesso aos dados após a confirmação da compra na corrente de blocos. O experimento consiste em criar uma rede Mininet com três hospedeiros (*hosts*), um comutador (*switch*) e um controlador SDN. O hospedeiro h_1 simula um servidor que armazena os dados à venda que foram anunciados na corrente de blocos. Um cliente comprador emite uma transação de compra passando o endereço IP do hospedeiro h_2, que faz uma requisição a h_1 e espera a resposta. O tempo da primeira requisição é maior porque o controlador verifica e processa as transações pendentes da fila. A média do tempo de resposta obtida é de $0,473$ segundos, valor adicional des-

[1]Disponível em https://osrg.github.io/ryu/

[2]MercadoPago apresentou 227 milhões de vendas no terceiro trimestre de 2019. Disponível em: https://ideias.mercadolivre.com.br/sobre-mercado-livre/mercado-livre-cresce-368-em-vendas-e-atinge-us-76-bilhoes-em-volume-de-pagamentos-com-mercado-pago-no-3o-tri/

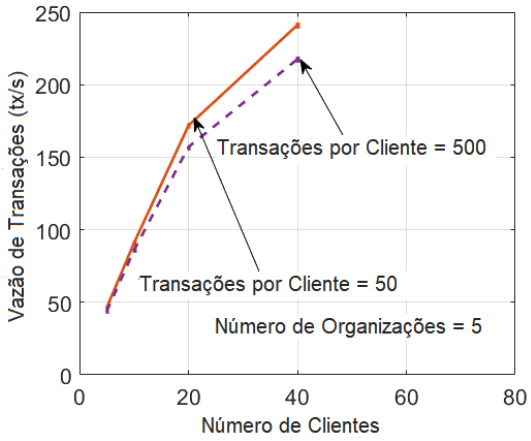


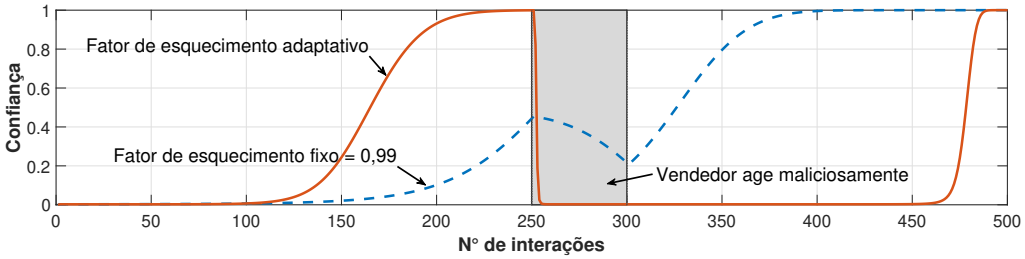
Figura 2. Vazão de transações com um número crescente de clientes em cinco organizações executando em múltiplas máquinas. Cada cliente emite um número de transações de anúncio e o tempo decorrido para a emissão é medido para o cálculo da vazão.

prezível para o usuário final. Esse resultado comprova que o tempo de acesso aos dados adquiridos é rápido e imperceptível, atendendo satisfatoriamente a interação com o cliente comprador.

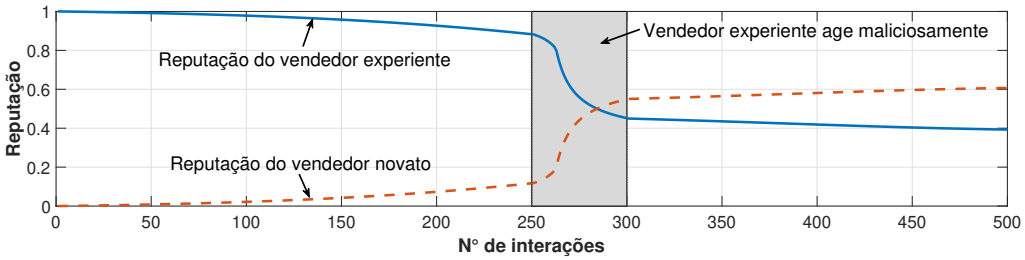
3.1. Sistema de Reputação e Confiança

O modelo proposto para o sistema de reputação e confiança foi simulado com auxílio do *software* MATLAB. O primeiro experimento do TRS avalia a efetividade da utilização de um fator de esquecimento adaptativo em quando comparado a um fator de esquecimento fixo para mitigar ataques de dissimulação. Os ataques de dissimulação são comuns em sistemas de reputação e confiança e ocorrem quando um usuário alterna seu comportamento entre honesto e malicioso para prejudicar outros sem ser detectado. A Figura 3(a) mostra as três fases do ataque. Nas primeiras interações, entre 0 e 250, o vendedor age honestamente para ganhar confiança dos usuários do sistema. Assim, o vendedor é recompensado pelo fator de esquecimento adaptativo, uma vez que não houve qualquer ação maliciosa. Entretanto, durante as interações 251 e 300, o vendedor se aproveita da confiança construída para agir maliciosamente. Enquanto o fator de esquecimento fixo resulta em uma queda gradual da confiança, o fator de esquecimento adaptativo pune rapidamente o vendedor nas primeiras ações maliciosas até chegar à confiança nula. Nas interações 301 e 500, o vendedor volta a se comportar honestamente para recuperar sua confiança. No entanto, o fator de esquecimento adaptativo faz o atacante continuar com confiança nula e precisar de mais interações para recuperá-la novamente. O experimento demonstra que, com o fator de esquecimento adaptativo, o sistema pune atacantes de forma mais eficiente e previne possíveis danos a diversos compradores.

O segundo experimento do TRS avalia a evolução da reputação de um vendedor novato ao entrar em um sistema onde os demais vendedores já possuem alta reputação. A Figura 3(b) mostra o caso em que um vendedor novato realiza duas vezes mais vendas positivas que um vendedor experiente. Na primeira fase, o vendedor novato começa com reputação nula e a aumenta gradualmente conforme recebe mais interações positivas que o vendedor experiente. Nesse caso, o vendedor experiente, apesar de ainda possuir



(a) Evolução da confiança de um vendedor para fatores de esquecimento fixo e adaptativo durante um ataque de dissimulação. O fator de esquecimento adaptativo recompensa vendedores que sempre foram honestos e pune fortemente vendedores maliciosos, entre 250 e 300.



(b) Evolução da reputação de um vendedor novato que recebe o dobro de avaliações positivas que um vendedor experiente. Ao agir maliciosamente, no intervalo de 250 a 300, o vendedor experiente perde reputação rapidamente e é ultrapassado pelo vendedor novato.

Figura 3. Evolução da confiança e reputação de vendedores.

reputação significativamente maior, deve aumentar suas vendas positivas para competir com o vendedor novato ou será lentamente ultrapassado. No entanto, na segunda fase o vendedor experiente decide agir maliciosamente anunciando dados de baixa qualidade apenas para alavancar seu número de vendas. Com as interações negativas resultantes, os compradores punem o vendedor experiente, que perde ainda mais reputação e é rapidamente ultrapassado pelo vendedor novato. Por fim, na terceira fase, o vendedor experiente retorna à situação da primeira fase. Porém, apesar de estar no sistema há mais tempo, sua reputação é menor que a do vendedor novato. O experimento demonstra que, assim como na vida real, o sistema beneficia vendedores experientes e exige que os novatos possuam um diferencial. O vendedor experiente não pode se basear apenas na experiência para preservar sua reputação, pois será rapidamente ultrapassado pelo vendedor novato.

4. Conclusão

O trabalho de iniciação desenvolvido apresentou uma arquitetura que utiliza a tecnologia de corrente de blocos para garantir a comercialização segura, automática e distribuída de dados proprietários entre usuários do sistema. Ao armazenar as permissões de acesso de maneira transparente e distribuída, o sistema desenvolvido permite que usuários mantenham controle sobre quem possui acesso a seus dados. A corrente de blocos sozinha, no entanto, não garante a entrega de dados adquiridos e tampouco atesta a qualidade dos dados anunciados. Para isso, o trabalho desenvolvido também propôs um sistema de reputação e confiança de usuários e da qualidade dos dados. O esquema de reputação desenvolvido foi modelado matematicamente para simular interações reais. Um protótipo do sistema proposto foi implementado e disponibilizado publicamente. A avaliação de desempenho do protótipo mostra que o sistema proposto atende facilmente a demanda de

comercialização no cenário nacional, atendendo a mais de 200 requisições simultaneamente. Além disso, os resultados do sistema de reputação e confiança proposto comprovam a eficiência do modelo proposto em identificar corretamente atos maliciosos, sendo eles devidamente punidos com perda significativa de reputação.

Referências

Andersen, M. P., Kolb, J., Chen, K., Fierro, G., Culler, D. E., and Popa, R. A. (2017). WAVE: A decentralized authorization system for IoT via blockchain smart contracts. *University of California at Berkeley, Tech. Rep*.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., et al. (2018). Hyperledger fabric: A distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference*, page 30. ACM.

Camilo, G., Rebello, G. A., de Souza, L. A., and Duarte, O. C. (2020a). AutAvailChain: Disponibilização Segura, Controlada e Automática de Dados IoT usando Corrente de Blocos. In *Anais do III Workshop em Blockchain: Teoria, Tecnologia e Aplicações*, pages 1–14, Porto Alegre, RS, Brasil. SBC.

Camilo, G., Souza, L., and Duarte, O. (2021). Um sistema seguro e distribuído para o provisionamento de funções virtuais de rede como serviço através de corrente de blocos. In *Anais do XXXIX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 770–783, Porto Alegre, RS, Brasil. SBC.

Camilo, G. F., Rebello, G. A. F., de Souza, L. A. C., and Duarte, O. C. M. B. (2020b). Autavailchain: Automatic and secure data availability through blockchain. In *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, pages 1–6.

Camilo, G. F., Rebello, G. A. F., de Souza, L. A. C., and Duarte, O. C. M. B. (2020c). A secure personal-data trading system based on blockchain, trust, and reputation. In *2020 IEEE International Conference on Blockchain (Blockchain)*, pages 379–384.

Canaltech (2022). Vazamento da Nvidia expôs dados de 71,3 mil funcionários. `https://canaltech.com.br/seguranca/vazamento-da-nvidia-expos-dados-de-713-mil-funcionarios-210683/`. Acessado em 6 de março de 2022.

g1.com (2022). Megavazamentos de dados expõem informações de 223 milhões de números de CPF. `https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/01/25/vazamentos-de-dados-expoem-informacoes-de-223-milhoes-de-numeros-de-cpf.ghtml`. Acessado em 6 de março de 2022.

Lantz, B., Heller, B., and McKeown, N. (2010). A network in a laptop: Rapid prototyping for software-defined networks. In *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*, Hotnets-IX, New York, NY, USA.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Disponível em https://bitcoin.org/bitcoin.pdf. Acessado em 15 de abril de 2020.

Sun, Y., Han, Z., and Liu, K. R. (2008). Defense of trust management vulnerabilities in distributed networks. *IEEE Communications Magazine*, 46(2):112–119.