Fortalecendo a Privacidade na Autenticação em Redes Virtuais Privadas: Uma Proposta de Pesquisa explorando Blockchain e Prova de Conhecimento Zero

Elimar Ximenes[1], **Emerson B. Tomaz**[1] **e Allysson Allex Araújo**[2]

[1]Universidade Federal do Ceará (UFC) – *Campus* de Crateús
Crateús, Ceará – Brasil

[2]Universidade Federal do Cariri (UFCA) – Centro de Ciências e Tecnologia
Juazeiro do Norte, Ceará – Brasil

elimarximenes@alu.ufc.br, emerson@crateus.ufc.br,
allysson.araujo@ufca.edu.br

Abstract. *With the advancement of Information Systems, data privacy has become a central concern. Virtual Private Networks (VPNs), although widely used, present vulnerabilities related to traditional authentication methods (username and password) and the use of traceable payment methods, such as credit cards. This ongoing research proposes an architecture for anonymous authentication in VPNs, based on blockchain and Zero-Knowledge Proofs (ZKP), which allows user identity to be validated without exposing it, while cryptocurrency payments eliminate identifiable data. The solution aims to offer greater security, privacy, and anonymity, being relevant, for example, for citizens in contexts of surveillance and censorship.*

Resumo. *Com o avanço dos Sistemas de Informação, a privacidade de dados tornou-se uma preocupação central. As Redes Virtuais Privadas (em inglês, Virtual Private Networks ou VPNs), embora amplamente utilizadas, apresentam vulnerabilidades relacionadas à autenticação tradicional (usuário e senha) e ao uso de meios de pagamento rastreáveis, como cartões de crédito. Esta pesquisa em andamento propõe uma arquitetura de autenticação anônima para VPNs baseada em blockchain e Prova de Conhecimento Zero (ZKP), que permite validar a identidade do usuário sem expô-la, enquanto pagamentos com criptomoedas eliminam dados identificáveis. A solução busca oferecer maior segurança, privacidade e anonimato, sendo relevante, por exemplo, para cidadãos em contextos de vigilância e censura.*

1. Introdução

Com o crescimento do uso de tecnologias digitais e plataformas online, as preocupações com a privacidade e o uso de dados têm se intensificado como um requisito importante na área de Sistemas de Informação (SI) [Perdices et al. 2023]. A privacidade digital diz respeito ao direito dos indivíduos de controlar a coleta, uso e divulgação de seus dados pessoais em ambientes digitais, bem como à capacidade de navegar e interagir em espaços virtuais sem vigilância indesejada [Acquisti et al. 2020].

No cotidiano, os usuários enfrentam riscos como vazamentos de informações, roubo de identidade e uso indevido de dados sensíveis. Em contextos de regimes autoritários, essas preocupações tornam-se ainda mais críticas, pois há um agravamento

devido à vigilância e censura governamental. Estudos indicam que tais regimes frequentemente monitoram e restringem a Internet, o que resulta em auto-censura e limitações à liberdade de expressão [Robinson and Tannenberg 2019, Ong 2019].

Uma das ferramentas amplamente utilizadas para mitigar essas ameaças são as Redes Virtuais Privadas (em inglês, *Virtual Private Networks* ou VPNs). As VPNs oferecem uma camada adicional de segurança ao mascarar o endereço *Internet Protocol* (IP) do usuário, criptografar o tráfego de rede e implementar autenticação para proteger a privacidade e confidencialidade dos dados [Cameron et al. 2005]. No entanto, não é possível afirmar que sua proteção é infalível. Em regimes autoritários, por exemplo, o uso de VPNs pode ser monitorado, restringido ou mesmo proibido. Além disso, falhas de segurança, vazamentos de dados e ordens judiciais abusivas podem comprometer a privacidade dos usuários [Schaub 2024, Nardi 2024]. Até mesmo o método de pagamento da VPN pode representar um risco, pois o uso de um cartão de crédito, por exemplo, pode expor a identidade do usuário, o que pode acarretar graves consequências em Estados autoritários.

Recentemente, pesquisadores têm buscado aprimorar a segurança, privacidade e anonimato em VPNs. Bakker (2023) propôs a integração do aplicativo IRMA com o WireGuard para autenticação anônima, mas deixou de abordar a obtenção dos parâmetros de autenticação e a privacidade nos pagamentos. Outros trabalhos, como os de Praveena *et al.* (2024) e Jin *et al.* (2016), exploraram, respectivamente, autenticação multifator e o uso de localização geográfica para maior segurança, porém sem considerar o anonimato ou propor alternativas aos métodos de pagamento tradicionais, que geralmente estão vinculados à identidade do usuário. Apesar de relevantes, essas propostas não contemplam uma perspectiva que assegure a privacidade, desde o pagamento até a autenticação.

Esses desafios ressaltam a urgência de soluções inovadoras que proporcionem maior proteção e anonimato aos usuários. Diante desse contexto, este trabalho propõe uma abordagem baseada em Prova de Conhecimento Zero (em inglês, *Zero-Knowledge Proof* ou ZKP) e *blockchain*. A adoção do ZKP se justifica pela possibilidade de validar a legitimidade do usuário sem expor sua identidade [Robert et al. 2022]. Por sua vez, a utilização da *blockchain* se destaca por sua capacidade de garantir descentralização e segurança de dados, além de viabilizar o uso de criptomoedas e contratos inteligentes, eliminando a rastreabilidade associada aos métodos de pagamento tradicionais. À luz dessa motivação, este projeto de pesquisa em andamento visa propor e avaliar uma arquitetura para preservação da privacidade na autenticação de serviços de VPN, utilizando ZKP e integrando *blockchain* para garantir segurança e anonimato no processo de pagamento. Como parte desse arcabouço geral, este artigo apresenta o escopo metodológico adotado para alcançar esse objetivo, a arquitetura proposta e evidências preliminares sobre a viabilidade do uso do protocolo ZKP no que se refere à escalabilidade.

Este estudo visa contribuir para a área de SI ao propor uma nova abordagem de autenticação anônima baseada em *Blockchain* e ZKP, fortalecendo a privacidade dos usuários em serviços de VPN. Diferentemente das soluções tradicionais, que frequentemente dependem de entidades centralizadas e podem expor metadados sensíveis, a arquitetura apresentada possibilita uma autenticação segura e pagamento descentralizado, reduzindo os riscos de rastreamento e censura. Essa perspectiva converge, por exemplo, com o desafio *Systemic and Socially Aware Perspective for Information Systems* discutido no I GranDSI-BR [Boscarioli et al. 2017], ao integrar segurança técnica à proteção de di-

reitos fundamentais, como privacidade e liberdade, alinhando o desenvolvimento técnico de SI às demandas sociais, humanas e políticas.

2. Procedimentos Metodológicos

Este estudo se caracteriza como uma pesquisa de natureza aplicada cujo objetivo é desenvolver uma arquitetura de autenticação anônima para serviços de VPN. A pesquisa se enquadra no tipo descritiva com uma abordagem quali-quantitativa. Para alcançar o referido objetivo, adotamos uma abordagem metodológica baseada em *Design Science Research* (DSR), a qual resultará em dois artefatos: (1) **Modelo**, uma representação abstrata que descreve a estrutura, os principais componentes (*blockchain*, servidor VPN e cliente VPN), suas interações e protocolos; e (2) **Instanciação**, uma implementação concreta da arquitetura proposta, apresentada como prova de conceito em um ambiente simulado.

Assim, nesta pesquisa, seguimos um percurso metodológico de seis etapas para execução da DSR, conforme sugerido por Peffers *et al.* (2007). As etapas 1 e 2, relativas ao problema e objetivos foram concluídas, a etapa 3 parcialmente, e as demais estão sendo desenvolvidas de forma iterativa. A seguir, será descrito cada etapa da DSR. Na **Etapa 1** (Conscientização do Problema), realizamos um levantamento bibliográfico que identificou dois principais problemas: o registro de dados de pagamento identificáveis por provedores de VPN e a dependência de autenticação baseada em usuário/senha. Na **Etapa 2** (Definição de Objetivos), com base nos problemas identificados, concluímos que a *blockchain* poderia eliminar o registro de dados de pagamento identificáveis por meio de criptomoedas e contratos inteligentes, enquanto o protocolo ZKP evitaria a exposição de dados de identificação. Assim, o objetivo deste estudo é desenvolver e avaliar uma arquitetura de autenticação anônima para VPNs, utilizando *blockchain* e ZKP. Na **Etapa 3** (*Design* e Desenvolvimento), tem-se a criação de uma arquitetura modular, integrando *blockchain*, cliente VPN e servidor VPN, conectados por um protocolo de autenticação anônima baseado em ZKP. O *Design* priorizou a privacidade, minimizando a exposição dos dados pessoais dos usuários, sendo organizado em duas fases: *configuração* (contratação do serviço) e *autenticação* (acesso do usuário). Na **Etapa 4** (Demonstração), a validação ocorrerá por meio de uma simulação computacional, testando a eficácia e viabilidade em um ambiente controlado, com *blockchain*, servidor VPN e cliente VPN. Na **Etapa 5** (Avaliação), serão realizadas análises qualitativas e quantitativas. A análise qualitativa examinará a resistência a ataques, como *Man-in-the-Middle* (MitM) e *replay*, por meio de sua replicação com o *sniffer* Wireshark, além de uma avaliação formal e uma análise crítica da proposta, considerando suas limitações. Já a análise quantitativa medirá o desempenho com base nos tempos de execução das operações (autenticação via ZKP e confirmação das transações na *blockchain*), nos custos das taxas de transação (*gas fees*) da *blockchain* e na escalabilidade da solução. Na **Etapa 6** (Comunicação dos resultados), a disseminação do conhecimento será realizada por três canais principais: TCC, Artigo Científicos e, posteriormente, a disponibilização do código-fonte e documentação em um repositório no GitHub.

3. Resultados Preliminares: Modelo Proposto e Análises Iniciais

Nossa proposta se fundamenta em dois pilares: (1) o uso de criptomoedas e contratos inteligentes para anonimizar as transações financeiras; (2) o protocolo ZKP para autenticação anônima, assegurando a segurança do *login* sem comprometer a privacidade. A Figura

1 ilustra a arquitetura proposta, incluindo seus componentes e o fluxo de operação. A proposta é apresentada de forma ampla, destacando as três entidades principais: *blockchain*, Cliente VPN e Servidor VPN, além de suas interações. A parte numerada de 1 a 9 detalha a *fase de configuração*, enquanto a *fase de autenticação*, representada pela parte 10 intitulada "autenticar", descreve a execução do protocolo ZKP em três rodadas entre o Cliente e o Servidor VPN. A seguir, cada fase será explanada detalhadamente.

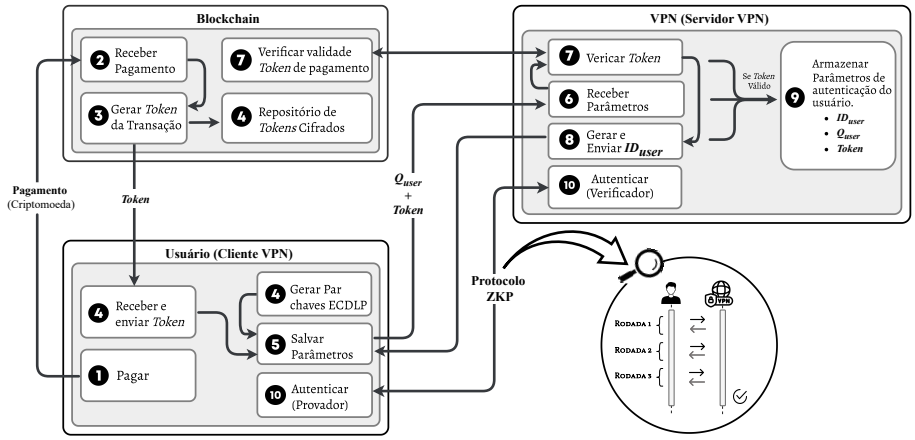

Figura 1. Visão geral da arquitetura.

Na ***fase de configuração***, o processo é iniciado pelo usuário, que realiza uma solicitação de registro na aplicação Cliente VPN e autoriza o pagamento de uma quantia em criptomoeda por meio de sua *Wallet*. Após a confirmação do pagamento, a *blockchain* gera um *token* de identificação da transação, que é armazenado de forma cifrada na *blockchain* com a chave pública da VPN e também enviado ao usuário por um canal seguro *Transport Layer Security* (TLS) para evitar ataques como *Man-in-the-Middle* (MitM). O usuário, então, cria um par de chaves ECDLP, sendo a chave pública Q_{user} e a chave privada k_{user}, e envia Q_{user}, junto com o *token*, ao Servidor VPN via TLS. O servidor valida o *token* na *blockchain*, e, se válido, associa o *token* ao ID_{user} gerado, armazenando as informações e retornando o ID_{user} ao usuário. Após isso, o processo é concluído, e o usuário já pode acessar o serviço.

Na ***fase de autenticação***, o protocolo ZKP foi implementado com base em curvas elípticas, podendo também ser fundamentado em outros problemas matemáticos da classe NP. O protocolo foi projetado para garantir segurança e anonimato, com o Cliente VPN atuando como *provador* e a VPN como *verificador*, adotando três rodadas com o mesmo processo para reduzir a chance de acerto aleatório por parte de um provador desonesto, mantendo, ainda assim, a eficiência computacional. Na primeira rodada, o Cliente VPN calcula um ponto compartilhado na curva elíptica, A_1, selecionando um número inteiro aleatório $v_1 \in \mathbb{F}_p$, tal que $A_1 = v_1 \cdot G$, em que $\mathbb{F}_p$ é um campo finito e G é o ponto gerador da curva. Em seguida, o ponto A_1 e o identificador ID_{user} são enviados ao Servidor VPN. O Servidor VPN, ao receber esses valores, gera um desafio σ_1 utilizando a função *hash* $\sigma_1 = H(G \parallel Q_u \parallel A_1 \parallel ID_{user})$, em que Q_u é a chave pública do usuário. Este desafio é enviado de volta ao Cliente VPN, que calcula a resposta π_1 com a equação $\pi_1 = v_1 + \sigma_1 \cdot k_u \pmod p$, utilizando sua informação privada v_1, o desafio σ_1 e sua chave privada k_u. O valor de π_1 é então enviado ao Servidor VPN.

Para verificar se a prova apresentada pelo Cliente VPN é válida, o Servidor VPN

calcula um novo ponto P_1, tal que $P_1 = \pi_1 \cdot G - \sigma_1 \cdot Q_u$. Se $P_1 = A_1$, a prova é considerada válida, e o usuário passa para a segunda rodada. Caso contrário, a autenticação falha e o processo não prossegue para as rodadas subsequentes. Esse processo é repetido em mais duas rodadas, garantindo robustez na autenticação e minimizando riscos de ataques. A Figura 2 ilustra o fluxo completo das três rodadas do protocolo ZKP.

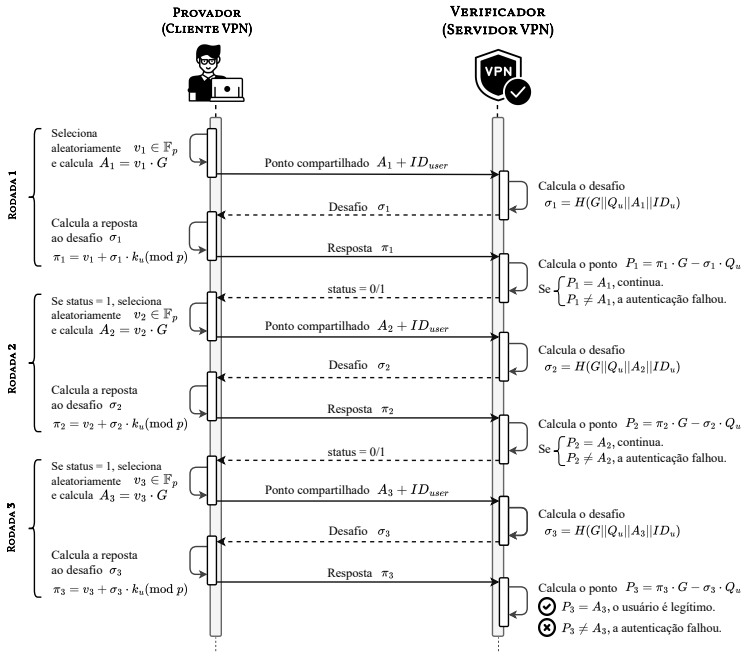

Figura 2. Fase de autenticação: execução do protocolo ZKP.

Para uma análise inicial da viabilidade do protocolo ZKP no contexto de escalabilidade, foram seguidos os procedimentos da *fase de autenticação* em uma máquina virtual Ubuntu 20.04 LTS na Google Cloud, com 16 GB de RAM, 16 vCPUs e 50 GB de armazenamento, localizada nos Estados Unidos. Inicialmente, o tempo de autenticação para um único usuário foi de aproximadamente 2,26 segundos. Para testar múltiplos usuários, foram simulados cenários com 20, 40, 60, 80 e 100 usuários utilizando *threads*. A Figura 3 mostra que o tempo de autenticação aumenta linearmente com o número de usuários, sem sobrecarga considerável, evidenciando de forma preliminar a viabilidade do protocolo em cenários de maior demanda.

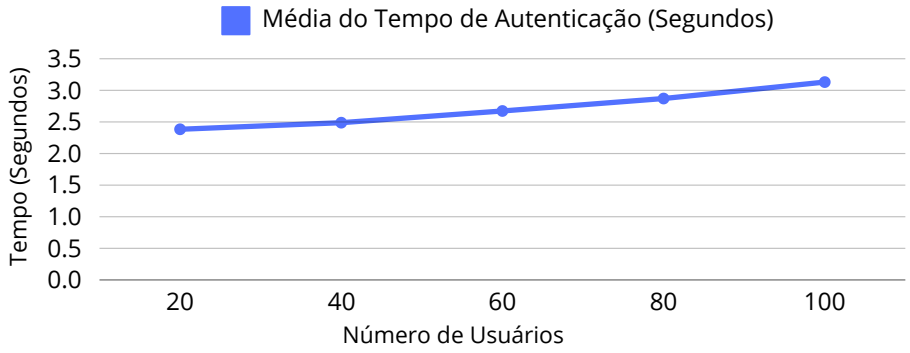

Figura 3. Média do Tempo de Autenticação por Número de Usuários

4. Considerações Finais, Contribuições para SI e Próximos Passos

Este estudo em andamento propõe uma arquitetura para fortalecer a privacidade e a segurança dos usuários de VPNs, visando mitigar riscos associados à vigilância estatal, ataques cibernéticos e ordens judiciais abusivas. A arquitetura proposta tem o potencial de evitar a exposição de dados pessoais em vazamentos, sejam eles acidentais ou maliciosos, o que é especialmente relevante em regimes autoritários e em serviços de VPN vulneráveis. Essa abordagem tem impacto social importante, por exemplo, para jornalistas, ativistas e cidadãos em contextos opressivos, que dependem de ferramentas confiáveis para proteger sua identidade online. Além disso, este trabalho pode contribuir no contexto de SI ao discutir novas direções sociotécnicas para o desenvolvimento de tecnologias que conciliam privacidade e autenticação, além de promover o equilíbrio entre esses fatores, instigando, assim, a produção de novos conhecimentos. Nos próximos passos desta pesquisa, será realizado mais um ciclo das etapas 3, 4 e 5, com foco na conclusão da implementação e na avaliação completa prevista nos procedimentos metodológicos.

Referências

Acquisti, A., Brandimarte, L., and Loewenstein, G. (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology*, 30(4):736–758.

Bakker, J. A. (2023). Irmaguard: Anonymous but authenticated vpn. Dissertação (mestrado em engenharia de software), Department of Computer Science.

Boscarioli, C., de Araujo, R. M., Maciel, R. S., Neto, V. V. G., Oquendo, F., Nakagawa, E. Y., Berrnardini, F. C., Viterbo, J., Vianna, D., Martins, C. B., et al. (2017). I GranDSI-BR: Grand research challenges in information systems in Brazil 2016-2026.

Cameron, R., Cantrell, C., Killion, D., Russell, K., and Tam, K. (2005). Vpn theory and usage - chapter 11. In Cameron, R., Cantrell, C., Killion, D., Russell, K., and Tam, K., editors, *Configuring NetScreen Firewalls*, pages 439–474. Syngress, Burlington.

Jin, Y., Tomoishi, M., and Matsuura, S. (2016). Enhancement of vpn authentication using gps information with geo-privacy protection. In *2016 25th Int. Conf. Comput. Commun. Netw.(ICCCN)*, pages 1–6. IEEE.

Nardi, C. (2024). Global affairs investigating 'malicious' hack after vpn compromised for over one month. *National Post*. Accessed: March 24, 2024.

Ong, E. (2019). Online repression and self-censorship: Evidence from southeast asia. *Government and Opposition*, 56:141 – 162.

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, 24.

Perdices, D., de Vergara, J. E. L., González, I., and de Pedro, L. (2023). Web browsing privacy in the deep learning era: Beyond vpns and encryption. *Computer Networks*, 220:109471.

Praveena, N., Jackson, B., Varalakshmi, S., Maheswari, G. U., et al. (2024). A secure multi-factor authentication system using elgamal bakers map function in virtual private network. In *2024 Third International Conference on Distributed Computing and Electrical Circuits and Electronics*, pages 01–07. IEEE.

Robert, L., Miyahara, D., Lafourcade, P., and Mizuki, T. (2022). Card-based zkp for connectivity: applications to nurikabe, hitori, and heyawake. *New Generation Computing*, 40(1):149–171.

Robinson, D. and Tannenberg, M. (2019). Self-censorship of regime support in authoritarian states: Evidence from list experiments in china. *Research Politics*, 6.

Schaub, S. (2024). VPNs and the fight against government censorship. *TechRadar*. Access: June 19, 2024.