Gestão Segura e Escalável de Identidades através de Múltiplas Corrente de Blocos

Lucas Airam C. de Souza, Gustavo F. Camilo, Gabriel Antônio F. Rebello, Miguel Elias M. Campista, Luís Henrique M. K. Costa

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

Resumo. *A identificação dos cidadãos é essencial para liberar o acesso a serviços básicos como saúde e educação. Entretanto, sistemas tradicionais de gestão de identidade adotam abordagens pouco escaláveis ou prejudiciais à segurança e à privacidade do usuário. Este artigo apresenta a proposta de um sistema de gestão de identidade baseado na interoperabilidade de correntes de blocos. No sistema, cada domínio mantém uma corrente de blocos para gerir a identidade de seus usuários. Além disso, o trabalho analisa a técnica de troca de informações entre correntes de blocos para implantar o conceito de "traga a sua própria identidade". Dessa forma, o sistema mitiga problemas de escalabilidade e garante aos usuários o controle sobre os seus dados. O trabalho desenvolvido é parte do projeto fomentado pela Rede Nacional de Ensino e Pesquisa, "Gestão de Identidade com Troca de Informações entre Correntes de Blocos".*

1. Introdução

A identidade é um dos bens mais preciosos do cidadão. Somente a partir de documentos que comprovam sua identidade, as pessoas conseguem obter acesso a direitos básicos, como voto, educação, saúde e moradia, além de acesso a serviços e emprego. Apesar da extrema relevância para o bem-estar geral, aproximadamente 1 bilhão de pessoas no mundo não possuem acesso a qualquer forma de prova de identidade atualmente [Pangestu et al. 2022]. Essa defasagem de registro acontece principalmente porque os processos de geração de documentos são altamente burocráticos e centralizados, criando empecilhos que aumentam os gastos e dificultam o acesso para parte da população. A centralização do gerenciamento de identidade afeta também os cidadãos que possuem registros, que confiam seus dados em armazenamentos governamentais centralizados. Isso gera um ponto único de falha, implicando em múltiplas vulnerabilidades de segurança para os dados dos usuários, que passam a estar sujeitos, por exemplo, a vazamento de informações e indisponibilidade devido a ataques de negação de serviço (*Denial of Service* - DoS). Mesmo esquemas de gerenciamento de identidades federados, que permitem o reaproveitamento de identidades, não são completamente descentralizados, portanto, são vulneráveis em pontos únicos de falha. Dessa forma, garantir uma maneira segura e desburocratizada de criação e prova de identidade é essencial para reverter essa situação.

A tecnologia de corrente de blocos (*blockchain*) se apresenta como uma alternativa que pode ser utilizada para criar identificações descentralizadas (*Decentralized Identifiers* - DID) digitais simples e acessíveis em relação aos processos burocráticos comuns. Apesar do uso de corrente de blocos, as identidades podem ser limitadas em um provedor de serviços como a Amazon ou Google. Dessa forma, cada identidade criada possui validade apenas no domínio do seu provedor de serviços de criação, sendo desconhecida por outros domínios. Assim, a cada

Este trabalho foi realizado com recursos do CNPq, CAPES, FAPERJ, FAPESP e RNP (E-26/203.211/2017, E-26/202.689/2018; 15/24494-8, 18/23292-0, 2015/24485-9 e 2014/50937-1.)

novo serviço de que um usuário deseja usufruir, é necessário o cadastro e memorização das informações de acesso. Esse gerenciamento centralizado produz um desafio para os usuários, que acumulam dados ou devem memorizar informações necessárias para autenticação. Além disso, a dificuldade de memorização das informações para autenticação e acesso aos serviços motiva os usuários a tomarem medidas prejudiciais à segurança, como a reutilização de dados, armazenamento de informações em texto em claro e em locais inseguros. Dessa forma, a implementação de um sistema de identidade baseado em corrente de blocos que requer dos usuários o armazenamento de poucas informações para acessar diversos serviços é conveniente. Para atender a este cenário, o sistema de gestão de identidade é composto por uma corrente de blocos primária, que foca a troca de informações entre os domínios participantes, e múltiplas correntes de blocos secundárias, administrada por cada um dos domínios.

Este artigo propõe uma arquitetura que aplica o conceito de "traga sua própria identidade" (*Bring Your Own Identity* - BYOI) através da troca de informações entre correntes de blocos. O sistema possui dois tipos de correntes de blocos: secundária e primária. As correntes de blocos secundárias armazenam metadados de identidades dos clientes [Dunphy e Petitcolas 2018]. Assim, quando um cliente cria uma conta no domínio A, o mesmo armazena os dados do cliente em seu próprio servidor e inclui o *hash* das informações cadastradas na corrente de blocos. Dessa forma, a proposta garante ao usuário a integridade no registro de suas informações e que seus dados não são públicos na corrente de blocos, reduzindo o custo de armazenamento de informações e mitigando problemas de privacidade. Caso o usuário queira se cadastrar em outro domínio, o domínio B emite uma transação à corrente de blocos primária com uma requisição assinada pelo usuário. Os domínios monitoram a corrente de blocos primária e verificam que uma transação foi emitida com o seu identificador como destino. Os domínios podem verificar a assinatura do usuário e autenticar o pedido. O processo de criação de uma identidade prevê que o usuário registra um conjunto de permissões sobre quais informações o domínio pode compartilhar com terceiros. Essas permissões podem ser asseguradas de maneira distribuída a partir de contratos inteligentes.

2. Trabalhos Relacionados

A mudança de paradigma trazida pela Web 3.0 torna necessária a existência de sistemas capazes de prover e gerenciar identidades de forma descentralizada. Assim, há um número crescente de sistemas e plataformas propostos para atender a esses requisitos, entre os quais destacam-se Sovrin, uPort e ChainID.

Sovrin [Reed et al. 2016] é uma plataforma para criação de identidades digitais. Pioneira entre os sistemas de identidades digitais, a plataforma Sovrin contribuiu para o surgimento de diversas propostas após a doação de seu código-fonte como parte do projeto Hyperledger Indy. uPort [Naik e Jenkins 2020] é um sistema de gestão de identidade descentralizado desenvolvido sobre a plataforma Ethereum. O sistema é desenvolvido através de um contrato inteligente, sendo de fácil uso e implantação. ChainID [Queiroz et al. 2021] é uma plataforma para gestão de identidades descentralizadas através da tecnologia de corrente de blocos. A proposta apresenta o uso da infraestrutura de identidades digitais em diversos fluxos de oferta de serviços, de forma segura e transparente.

As propostas anteriores visam um cenário com uma única corrente de blocos para a gestão de identidades. A proposta atual prevê o uso de múltiplas correntes de blocos, classificadas como corrente de blocos primária ou corrente de blocos secundária. As correntes de blocos secundárias são permissionadas e privadas, administradas pelos domínios provedores de serviços, enquanto a corrente de blocos primária é mantida de forma pública para consultas em

eventuais disputas. Dessa forma, o sistema é escalável, pois os domínios realizam a maioria das operações em paralelo e de forma independente, e economiza espaço de armazenamento, porque os serviços só precisam ter acesso a informações essenciais para seu funcionamento.

3. Arquitetura Proposta

O cenário da proposta compreende múltiplos domínios administrativos concorrentes, como Facebook e Google, que gerenciam identidade dos usuários que utilizam seus sistemas. A Figura 1 ilustra a arquitetura proposta para o sistema. As correntes de blocos fornecem algumas propriedades, como imutabilidade, transparência e descentralização, necessárias para a garantia de segurança em um cenário com diversos participantes sem confiança mútua [Queiroz et al. 2021]. Esta arquitetura permite uma alta escalabilidade, uma vez que cada domínio armazena dados somente de seu interesse, e privacidade, já que um domínio possui informações somente de seus clientes, sem acesso às informações de outras correntes de blocos secundárias.

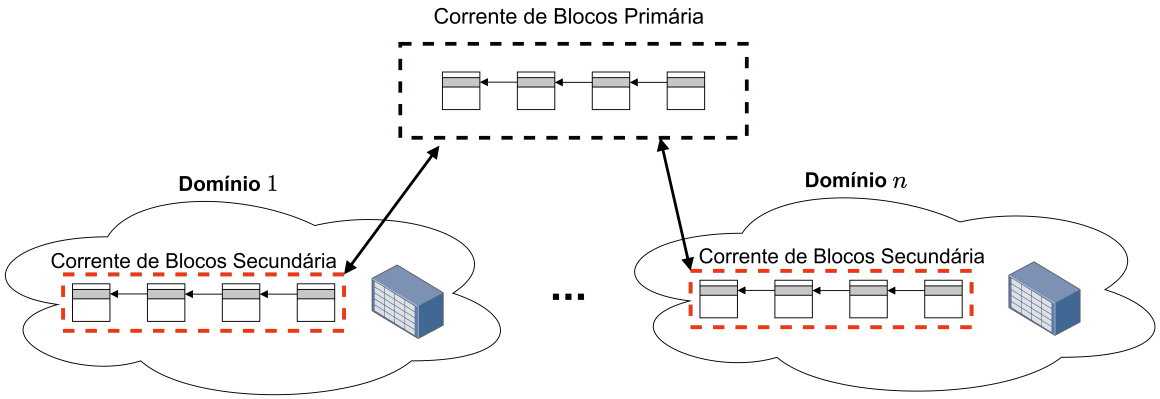

Figura 1: Arquitetura proposta para o sistema de gerenciamento de identidades.

A corrente de blocos primária é responsável por registrar as requisições de informações de identidades entre domínios. A corrente de blocos primária realiza as operações necessárias para garantir a interoperabilidade entre as correntes de blocos e transferência de informações requisitadas por domínios distintos.

As correntes de blocos secundárias são responsáveis por registrar informações dos usuários nos domínios provedores de serviços. Estas correntes são administradas pelos domínios, que podem escolher mecanismos de consenso e parâmetros de blocos mais rápidos e eficientes, além de registrar permissões e registro de seus clientes, sem revelar informações a outros domínios. Cada domínio possui total autonomia para gerenciar as próprias correntes de blocos, podendo privilegiar diferentes aspectos de acordo com suas preferências e demandas. As informações de registro de identidade são armazenadas para garantir transparência aos clientes. Para garantir a privacidade dos clientes, dados pessoais são armazenados fora da corrente. O registro, no entanto, apresenta o *hash* destes dados de maneira pública, provendo integridade da informação armazenada.

O objetivo dessa arquitetura com uma corrente de blocos por domínio é mitigar os problemas de escalabilidade do número de usuários, evitando a existência de uma única corrente de blocos responsável pelo armazenamento de todos os dados. A escalabilidade é alcançada através da paralelização do gerenciamento de identidades por domínios diferentes em correntes de blocos secundárias distintas. Entretanto, há um compromisso para o usuário quanto ao modelo de segurança incorporado pela corrente de blocos secundária de seu provedor de serviço.

Enquanto sistemas com uma única corrente de blocos mantêm maior resiliência quanto aos participantes maliciosos, correntes de blocos secundárias permissionadas com poucos participantes são mais vulneráveis. Além disso, as correntes de blocos públicas devem ser armazenadas por todos os participantes, apresentando uma sobrecarga. A proposta atual mitiga essa sobrecarga dividindo a informação em múltiplas correntes de blocos, assim os participantes armazenam apenas as informações contidas em correntes de blocos de seu interesse.

4. Conclusão e Trabalhos Futuros

Este artigo propõe um sistema de gestão de identidades baseado no paradigma "traga a sua própria identidade". O sistema usufrui dos benefícios da tecnologia de corrente de blocos para criação de identidades de forma descentralizada através de uma solução escalável com múltiplas correntes de blocos. Como trabalhos futuros, será implementada uma prova de conceito para a avaliação da proposta.

Referências

Dunphy, P. e Petitcolas, F. A. (2018). A First Look at Identity Management Schemes on the Blockchain. *IEEE Security & Privacy*, 16(4):20–29.

Naik, N. e Jenkins, P. (2020). uPort Open-Source Identity Management System: An Assessment of Self-Sovereign Identity and User-Centric Data Platform Built on Blockchain. Em *2020 IEEE International Symposium on Systems Engineering (ISSE)*, páginas 1–7. IEEE.

Pangestu, M. et al. (2022). ID4D Data: Global Identification Challenge by the Numbers. Relatório técnico, The World Bank.

Queiroz, S., Greve, F., Sampaio, L. N. e Marques, E. (2021). Plataforma para Gestão de Identidades Descentralizadas Baseada em Blockchain. Em *Anais do XXI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, páginas 29–42. SBC.

Reed, D., Law, J. e Hardman, D. (2016). The Technical Foundations of Sovrin. *The Technical Foundations of Sovrin*.