Governança Digital que se Explica: Interação Segura com Regras Programáveis

Bruno Evaristo[1,2], **Jeffson Celeiro**[1,2], **Antônio Abelém**[2]

[1] Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPQD)
Campinas – SP – Brasil

[2]Universidade Federal do Pará (UFPA)
Belém – PA – Brasil

elderb,jcsousa@cpqd.com.br, abelem@ufpa.br

Abstract. Introduction*: The work proposes explainable digital governance based on blockchain, smart contracts, and decentralized identity.* ***Objectives****: aiming for transparency, security, and trust.* ***Methodology****: combines DIDs and VCs, with off-chain data and on-chain metadata to ensure privacy and interoperability.* ***Expected results****: Validate the architecture in real-world scenarios, enhancing privacy and flexibility with zero-knowledge proofs and DIDComm.*
Keywords *Machine-readable governance, decentralized digital identity, Blockchain.*

Resumo. Introdução*: O trabalho propõe uma governança digital explicável baseada em blockchain, contratos inteligentes e identidade descentralizada,* ***Objetivos****: visando transparência, segurança e confiança.* ***Metodologia****: combina DIDs e VCs, com dados off-chain e metadados on-chain para garantir privacidade e interoperabilidade.* ***Resultados Esperados****: validar a arquitetura em cenários reais, ampliando privacidade e flexibilidade com provas de conhecimento zero e DIDComm.*
Palavras-Chave *Governança legível por máquina, identidade digital descentralizada, Blockchain.*

1. Introdução

A crescente complexidade dos sistemas digitais tem ampliado a distância entre os usuários e as regras que regem suas interações nesses ambientes. Embora a digitalização traga benefícios como automação e conectividade, ela também impõe desafios relacionados à transparência, à confiança e à compreensão dos mecanismos que controlam o acesso, a identidade e as decisões. Neste cenário, torna-se urgente desenvolver modelos de governança digital que sejam não apenas tecnicamente robustos, mas também compreensíveis e acessíveis aos seus usuários [de Souza et al. 2022].

Este trabalho em carácter inicial, propõe uma abordagem de governança digital explicável, em que regras programáveis são formalizadas em formatos legíveis por máquina e vinculadas a mecanismos de identidade digital descentralizada. A proposta integra contratos inteligentes operando em redes blockchain com tecnologias de autenticação baseadas em carteiras digitais, permitindo que os próprios usuários

visualizem as regras em vigor, acompanhem decisões e compreendam os critérios aplicados em tempo real.

Ao colocar o ser humano no centro da governança digital, a arquitetura favorece interações mais seguras, auditáveis e transparentes, promovendo uma relação de confiança entre usuários e sistemas automatizados. Essa estrutura busca alinhar inovação tecnológica com princípios fundamentais da Interação Humano-Computador, como visibilidade do sistema, feedback imediato e autonomia do usuário.

2. Metodologia

A metodologia combina blockchain, identidade descentralizada e linguagens formais para estruturar uma governança digital programável e centrada no usuário. Primeiro, definiu-se um modelo lógico de governança legível por máquina, com regras em contratos inteligentes interoperáveis entre diferentes blockchains. Em seguida, foi criado um fluxo de autenticação e autorização com Identificadores Descentralizados(DIDs) e Credenciais Verificáveis(VCs), permitindo que o usuário submeta credenciais de forma segura, tenha permissões avaliadas automaticamente e receba feedback em tempo real por meio de uma interface explicável.

Na arquitetura proposta, dados sensíveis e lógica condicional são mantidos off-chain, garantindo privacidade, enquanto os metadados e os registros de verificação são armazenados on-chain, assegurando imutabilidade e auditabilidade. A separação clara entre esses componentes favorece a escalabilidade do sistema e facilita a explicação das decisões de acesso ou negação ao próprio usuário, promovendo uma experiência mais transparente, compreensível e confiável.

3. Proposta e Fluxo de Funcionamento Prático

A gestão eficaz requer governança estruturada, mas enfrenta desafios como definição de direitos, resolução de conflitos, confiança e adaptação regulatória [Grover et al. 2021]. A governança legível por máquina e a identidade descentralizada transformam esse cenário ao introduzir descentralização, automação e verificabilidade, permitindo decisões e relações de confiança mais transparentes e auditáveis por meio de regras programáveis [Evaristo et al. 2025].

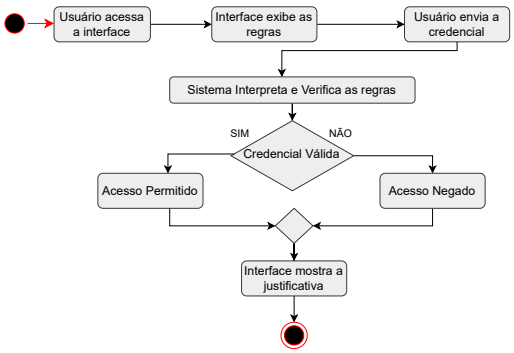

Figura 1. Fluxo de Interação na Governança Digital Explicável.

o modelo proposto não se limita a promover a interoperabilidade entre sistemas, mas também se estrutura como um meio de comunicação agnóstico e seguro, ou

seja, capaz de operar de forma independente de plataformas proprietárias, protocolos específicos ou infraestruturas descentralizadas, minimizando assim pontos únicos de falha e vetores de ataque. Além disso, define regras explícitas para a emissão e verificação de credenciais, fundamentadas em princípios de IDD, o que permite que o controle da identidade permaneça sob domínio do usuário, reduzindo riscos relacionados a acesso não autorizado, falsificação de identidade e vazamento de informações sensíveis como definido no fluxo da Figura 1.

Já na Figura 2, representa o fluxo de interação em um sistema de governança digital descentralizada que prioriza a explicabilidade e a segurança, conforme os princípios de Interação Humano-Computador. O processo tem início quando o usuário acessa uma aplicação ou serviço por meio de uma interface digital que expõe, de forma clara e visual, as regras programáveis que serão aplicadas à sua credencial. Esse primeiro contato com o sistema é fundamental para garantir a visibilidade do funcionamento e promover a compreensão do que está sendo solicitado, porque está sendo solicitado e como a informação será processada.

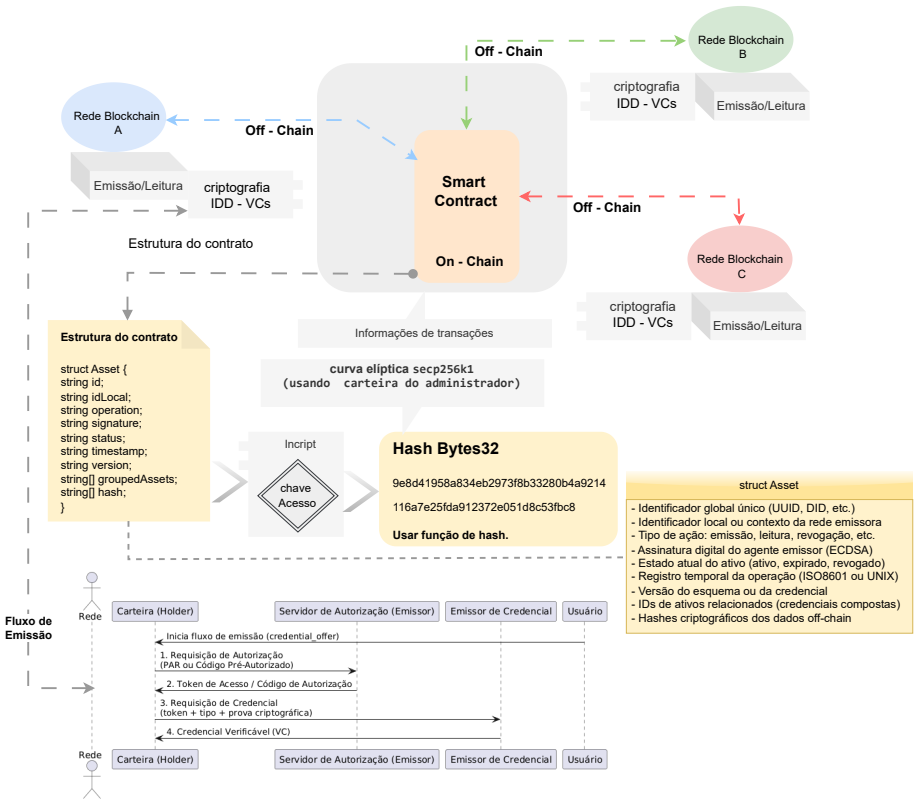

Figura 2. Fluxo de Comunicação entre as redes.

O usuário envia sua credencial verificável por uma carteira digital (DID), que é processada por um validador ao identificar a operação (emissão, leitura ou revogação), interpretar metadados padronizados e aplicar regras em contratos inteligentes. A verificação combina dados on-chain (estrutura e assinatura) e off-chain (informações criptografadas e hashes), garantindo segurança, integridade e privacidade.

Durante o processo, o contrato inteligente, implantado em múltiplas blockchains

interoperáveis, é consultado para confirmar a validade, status e assinatura da credencial, utilizando criptografia baseada em curva elíptica (secp256k1). O sistema realiza essa operação sem exigir ação ou conhecimento técnico do usuário, mantendo a interação fluida e compreensível. Após a validação, o sistema gera um feedback automático e visível, informando claramente se a credencial foi aceita ou recusada e por qual motivo, reforçando a confiança e a autonomia do usuário sobre seus próprios dados.

A arquitetura integra blockchain, contratos inteligentes e identidade descentralizada para automatizar a verificação e tornar a governança digital mais transparente e compreensível. Sob a ótica da IHC, prioriza transparência, feedback imediato, menor carga cognitiva e centralidade do usuário, favorecendo uma experiência digital confiável, ética e segura.

4. Conclusão e trabalhos futuros

Este trabalho apresentou uma estrutura em carácter de pesquisa inicial de governança digital explicável, que combina regras legíveis por máquina, identidade descentralizada e contratos inteligentes em redes blockchain interoperáveis. A proposta permite que usuários interajam com o sistema de forma segura, compreensível e auditável, promovendo autonomia e confiança. Como continuidade, pretende-se validar a arquitetura em cenários reais e incorporar mecanismos como provas de conhecimento zero e DIDComm, ampliando a privacidade e a flexibilidade nas interações em ecossistemas descentralizados.

5. Cuidados Éticos

Este estudo seguiu as Resoluções CNS nº 466/2012, nº 510/2016, nº 674/2022 e Norma Operacional 001/2013, com aprovação do Comitê de Ética em Pesquisa sob CAAE (omitido para revisão); as pessoas participantes assinaram TCLE, tendo garantidos anonimato, confidencialidade dos dados e direito de desistência a qualquer momento.

6. Agradecimentos

Agradecemos o apoio institucional e financeiro do Projeto ILIADA, em parceria com o CPQD (Termo de Parceria nº TPA/184/SOFTEX/CPQD), essencial para o desenvolvimento das atividades de pesquisa, inovação e validação tecnológica.

Referências

de Souza, F., Formigoni Filho, J. R., Marino, F. C. H., e Sampaio, A. S. (2022). Autenticaçao segura de pessoas com carteira digital: um estudo no cpqd. In *Simpósio Brasileiro sobre Fatores Humanos em Sistemas Computacionais (IHC)*, pages 48–55. SBC.

Evaristo, B., Celeiro, J., Veloso, A., e Abelém, A. (2025). Modelo de governança baseada em regras legíveis por máquina voltada a aplicações de identidade digital descentralizada. In *Colóquio em Blockchain e Web Descentralizada (CBlockchain)*, pages 55–60. SBC.

Grover, B. A., Chaudhary, B., Rajput, N. K., e Dukiya, O. (2021). Blockchain and governance: theory, applications and challenges. *Blockchain for Business: How It Works and Creates Value*, pages 113–139.