Estrutura de governança orientada por regras programáveis com suporte de identidade digital descentralizada

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 e abelem@ufpa.br

Resumo. *Com o avanço da era digital, técnicas tradicionais de gestão de identidades se mostram cada vez mais complexas e pouco confiáveis. Para superar esses desafios, surgem novos modelos, como a governança legível por máquinas e a identidade descentralizada, que empregam tecnologias como blockchain e criptografia. Este trabalho visa propor uma camada de autenticação baseada nesses modelos, garantindo que as regras de governança sejam precisamente codificadas de maneira agnóstica, favorecendo escalabilidade, reconhecimento legal e reduzindo vulnerabilidades de diferentes redes descentralizadas.*

1. Introdução

O conceito de governança envolve regras, procedimentos e mecanismos que guiam e supervisionam uma organização ou sistema, abrangendo decisões, responsabilidades e prestação de contas. Aplicado à tecnologia, visa especialmente garantir a interoperabilidade e conformidade entre sistemas [Tan et al. 2022]. Este trabalho foca especificamente na Governança Legível por Máquina (*Machine Readable Governance* - MRG), ou governança ”on chain”, um conceito recente baseado em blockchain, contratos inteligentes e identidade digital descentralizada (IDD) [ind 2021].

O objetivo é codificar regras de governança em formatos que possam ser automaticamente executados por sistemas computacionais, eliminando a necessidade de intervenção humana constante. Utilizando identidades descentralizadas, a governança ”on chain”assegura que regras e condições definidas sejam automaticamente cumpridas nas operações e transações [ind 2022]. Quando sistemas distintos compartilham padrões semânticos na codificação dessas regras, a interoperabilidade torna-se possível, permitindo integrar diferentes aplicações em ecossistemas descentralizados mais amplos.

A integração da blockchain com tecnologias de registro distribuído (DLT) e identidade descentralizada proporciona uma solução avançada para a gestão e proteção de dados pessoais, permitindo maior privacidade e controle por parte dos usuários sobre suas informações. Dessa forma, reduz-se a dependência de intermediários e fortalece-se a segurança dos dados [Queiroz et al. 2021].

O objetivo central deste trabalho é projetar e implementar uma estrutura de governança automatizada, transparente e orientada ao usuário, capaz de oferecer uma camada confiável de controle e gerenciamento para indivíduos ou entidades. Para tal, propõe-se a formalização de regras em linguagens legíveis por máquina, com suporte a

interpretação dinâmica e adaptável a diferentes redes descentralizdas. A solução inclui a incorporação de uma camada de verificação de identidade baseada em mecanismos de identidade digital descentralizada (DID), visando assegurar a confidencialidade, integridade e proteção dos dados pessoais. A arquitetura proposta também viabilizar a interoperabilidade entre credenciais verificáveis (Verifiable Credentials – VCs) e identificadores descentralizados (DIDs), promovendo a compatibilidade entre múltiplas redes.

2. Proposta e Fluxo de Funcionamento Prático

A gestão eficaz de organizações e sistemas requer uma governança bem estruturada, que assegure decisões responsáveis e uso ético dos recursos. Contudo, ela enfrenta desafios como a definição clara de direitos e deveres, resolução de conflitos, construção de confiança entre as partes e adaptação ágil a mudanças regulatórias e comerciais [Grover et al. 2021]. A governança legível por máquina e a identidade descentralizada, representam uma transformação significativa na concepção e gestão da governança e identidade no ambiente digital. Essas abordagens introduzem novos paradigmas baseados em descentralização, automação e verificabilidade, permitindo que decisões e relações de confiança sejam operacionalizadas de forma transparente e auditável por meio de regras programáveis [ind 2022].

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 na Figura 1.

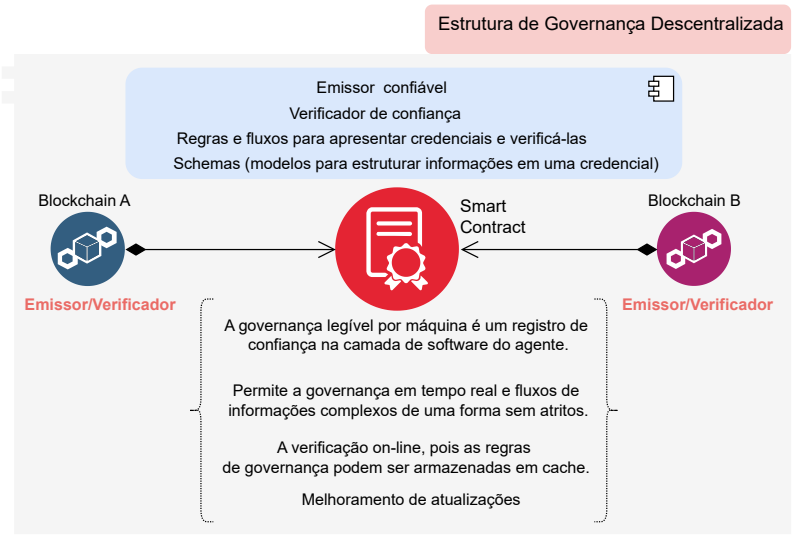

Figura 1. Arquitetura Teórica da Proposta

Já na Figura 2, apresenta uma arquitetura técnica voltada à emissão e leitura de credenciais verificáveis (VCs) em um ecossistema baseado em múltiplas redes blockchain interoperáveis. Nela, observa-se a separação clara entre componentes executados on-chain, ou seja, diretamente nos contratos inteligentes das blockchains A, B e C, e elementos off-chain, que são processados fora da cadeia de blocos, geralmente por agentes externos ou aplicações integradas.

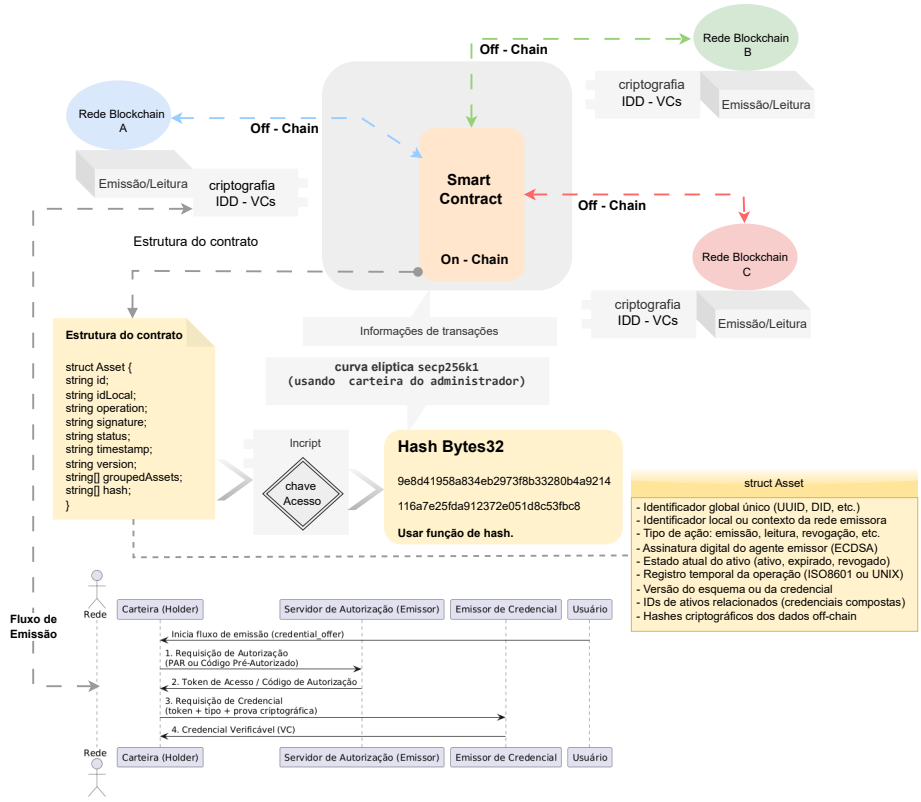

Figura 2. Fluxo de Comunicação entre as redes

Cada rede blockchain representada (A, B e C) funciona como um domínio autônomo de confiança, capaz de operar de forma independente, mas padronizada. Todas elas compartilham a mesma lógica de contratos inteligentes, que registram metadados de transações sobre ativos digitais — neste caso, credenciais verificáveis associadas a usuários. As transações são formalizadas por meio da estrutura de dados Asset, que encapsula informações como identificadores globais e locais, tipo de operação (emissão, leitura, revogação), assinatura digital, status da credencial, carimbo temporal, versão da estrutura e hashes criptográficos dos dados sensíveis que permanecem armazenados off-chain.

A assinatura digital registrada no campo signature é produzida com base no algoritmo ECDSA, utilizando a curva elíptica *secp256k1*, especialmente em sistemas baseados em blockchain e identidade descentralizada [Kuntz 2022]. Com o uso de carteiras criptográficas vinculadas a administradores e agentes autorizados. O uso dessas técnicas assegura as propriedades clássicas da segurança da informação: confidencialidade, integridade, autenticidade e não repúdio, além de possibilitar auditorias confiáveis.

A lógica do sistema opera como um mecanismo híbrido: os dados sensíveis e a lógica condicional são processados fora da blockchain (off-chain), enquanto os contratos inteligentes armazenam informações verificáveis, imutáveis e auditáveis (on-chain). Essa separação favorece escalabilidade, preservação da privacidade e eficiência computacional. Além disso, a arquitetura suporta governança distribuída, já que diferentes redes podem operar com suas próprias regras, mas respeitando um esquema comum de dados e validação. Dessa forma, o modelo viabiliza interoperabilidade entre blocos institucionais ou governamentais distintos, com segurança criptográfica e rastreabilidade garantida por meio da blockchain.

3. Conclusão e trabalhos futuros

Este trabalho propôs uma estrutura de governança automatizada orientada à governança legível por máquina, integrada a mecanismos de identidade digital descentralizada (IDD) e à execução de regras automatizadas por meio de contratos inteligentes operando em redes blockchain interoperáveis. A proposta parte do princípio de que regras formais podem ser representadas, versionadas e executadas de maneira transparente, verificável e auditável, reduzindo a intervenção humana e promovendo maior confiabilidade nos processos de validação e tomada de decisão entre agentes distribuídos.

Como continuidade, pretende-se avaliar a estrutura de governança em cenários reais, considerando desempenho, interoperabilidade e robustez da governança. Pretende-se ainda incorporar governança dinâmica e suporte a autenticação delegada, com verificação seletiva baseada em zero-knowledge proofs e DIDComm, ampliando a privacidade, autonomia e conformidade dos usuários em ecossistemas descentralizados.

4. Agradecimentos

Agradecemos ao apoio institucional e financeiro recebido no âmbito do Projeto ILIADA, desenvolvido em parceria com o CPQD, no contexto do Termo de Parceria nº TPA/184/SOFTEX/CPQD. Esta colaboração foi fundamental para o desenvolvimento das atividades de pesquisa, inovação e validação tecnológica aqui apresentadas.

Referências

[ind 2021] (2021). Trust registry or machine readable governance?

[ind 2022] (2022). Machine readable governance is the key to scaling decentralized trust.

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

[Kuntz 2022] Kuntz, J. (2022). *Blockchain Ethereum: Fundamentos de arquitetura, desenvolvimento de contratos e aplicações*. Casa do Código.

[Queiroz et al. 2021] Queiroz, S., Greve, F., Sampaio, L. N., and Marques, E. (2021). Plataforma para gestão de identidades descentralizadas baseada em blockchain. In *Anais do XXI Simpósio Brasileiro em Segurança da Informaçao e de Sistemas Computacionais*, pages 29–42. SBC.

[Tan et al. 2022] Tan, E., Mahula, S., and Crompvoets, J. (2022). Blockchain governance in the public sector: A conceptual framework for public management. *Government Information Quarterly*, 39(1):101625.