

# Modelo de governança baseada em regras legíveis por máquina voltada a aplicações de identidade digital descentralizada

Bruno Evaristo<sup>1,2</sup>, Jeffson Celeiro<sup>1,2</sup>, Alan Veloso<sup>2</sup>, Antônio Abelém<sup>2</sup>

<sup>1</sup> Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPQD)  
Campinas – SP – Brasil

<sup>2</sup>Universidade Federal do Pará (UFPA)  
Belém – PA – Brasil

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

**Abstract.** *With the advance of the digital age, traditional identity management techniques have become increasingly complex and unreliable. To overcome these challenges, new models are emerging, such as machine-readable governance and decentralized identity, which employ technologies such as blockchain and cryptography. This work aims to propose an authentication layer based on these models, ensuring that governance rules are precisely encoded in an agnostic way, favoring scalability, legally recognizable and reducing the vulnerabilities of different decentralized networks.*

**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 [Tan et al. 2022]. Aplicado à tecnologia, visa especialmente garantir a interoperabilidade e conformidade entre sistemas [FERREIRA 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 desenvolver um ecossistema automatizado, transparente e centrado no usuário, proporcionando uma camada confiável de controle para indivíduos ou organizações. Para isso, será necessário traduzir as regras em uma linguagem legível por máquinas, mantendo flexibilidade interpretativa. Também será implementada uma camada de verificação de identidade para assegurar proteção e privacidade de dados pessoais. Essa abordagem fomenta a interoperabilidade entre credenciais verificáveis (VCs) e identificadores descentralizados (DIDs).

Este trabalho está estruturado da seguinte forma: Os Seção 2 que expõem projetos e iniciativas relacionadas a proposta do artigo, A Seção 3 destaca a proposta geral do desenvolvimento do trabalho e fluxo de funcionamento prático e por fim a Seção 4, que expõe a conclusão inicial seguindo de desafios para o avanço do trabalho.

## **2. Trabalhos Relacionados**

Existem inúmeros trabalhos que tratam do termo governança descentralizada vinculado ao termo identidade digital descentralizada (IDD), que levam em consideração uma estrutura participativa, com uma abordagem agnóstica, o que é o caso do projeto Alastria, O Alastria é um consórcio sem fins lucrativos que desenvolve uma infraestrutura blockchain pública e permissionada na Espanha, com o objetivo de promover transações legalmente válidas e respeitar os regulamentos europeus [Alastria Consortium 2024]. Outro exemplo, é a iniciativa European Blockchain Services Infrastructure (EBSI), uma estrutura de governança colaborativa e descentralizada permite que a EBSI forneça serviços públicos transfronteiriços seguros e eficientes, alinhados com os valores e regulamentações europeias [European Commission 2024b].

Outra iniciativa de regulamentação de modelos de governança descentralizado é o eIDAS 2.0 é uma atualização do regulamento europeu que visa aprimorar a identificação eletrônica e os serviços de confiança para transações digitais na União Europeia e amplia o escopo do regulamento original, incluindo o setor privado e promovendo a interoperabilidade entre os Estados-Membros [European Commission 2024a]. Outra iniciativa recente é o que a IEEE tem se dedicado ao desenvolvimento de padrões e diretrizes para a governança de blockchain, o modelo de governança 4P+I é uma estrutura analítica desenvolvida para avaliar e orientar a governança de sistemas blockchain, considerando cinco dimensões principais [mod 2024].

E por fim, foi verificado também a LACChain, O LACChain é uma iniciativa liderada pelo Laboratório de Inovação do Banco Interamericano de Desenvolvimento (IDB Lab) que visa desenvolver o ecossistema blockchain na América Latina e no Caribe, esse modelo de governança permite que forneça uma infraestrutura blockchain pública permissionada que respeita a soberania dos países participantes, promovendo uma plataforma tecnológica avançada e colaborativa na região [Allende López et al. 2020].

### 3. Proposta

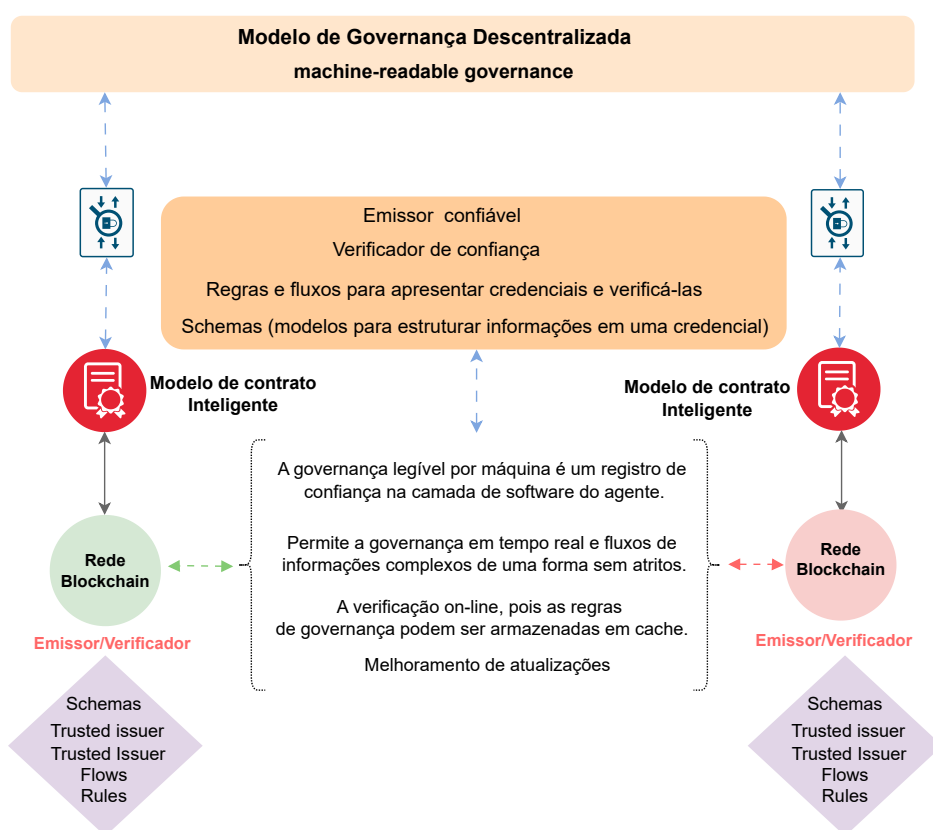
A administração de qualquer organização ou sistema exige uma governança eficaz e bem estruturada, para garantir que as decisões sejam tomadas com eficiência e responsabilidade, bem como promover o uso ético e equitativo dos recursos. No entanto, o tema da governança apresenta complexidades e desafios, tais como a delimitação inequívoca de direitos e deveres, a adequada resolução de conflitos, o estabelecimento da confiança entre as partes e a capacidade de ajustar de forma ágil suas regras em resposta a desafios internos e externos, tais como alterações no quadro regulatório vigente ou novos desafios comerciais [Grover et al. 2021]. A governança legível por máquina e a identidade descentralizada são temas recentes, surgidos com o advento das DLTs (*Distributed Ledger Technologies*). Eles representam uma mudança profunda na forma como concebemos e gerimos a governança e a identidade no espaço digital [ind 2020]. No entanto, a integração desses dois conceitos apresenta vários desafios, descritos na Figura 1:



**Figura 1. Desafios de Integração entre MRG e IDD**

A codificação da governança legível por máquinas enfrenta desafios como a complexidade em transformar regras específicas em código claro, imutabilidade de erros no blockchain e dificuldades de interoperabilidade entre plataformas. Também envolve riscos para a privacidade dos usuários e desafios logísticos e culturais na transição da governança tradicional para sistemas automatizados. Adicionalmente, a escalabilidade das tecnologias blockchain, as limitações jurídicas e regulatórias existentes, preocupações de segurança, dificuldades na verificação de dados externos à blockchain, e o risco da má gestão das chaves pelos usuários são questões críticas. Por fim, surgem desafios sociais e éticos relacionados à inclusão e justiça na definição e alteração dessas regras automatizadas.

Esses desafios não são intransponíveis, mas destacam que a implementação da governança legível por máquina com identidade descentralizada precisa ser abordada com cuidado, considerando não apenas as vantagens técnicas, mas também as implicações sociais, éticas e legais. E, no que trata de interoperabilidade, o tema da segurança surge inevitavelmente. É nesse contexto que se coloca o uso de identidade digital descentralizada, associado a provas de credenciais emitidas sob as regras de uma estrutura de governança interoperável. Isso possibilita, por exemplo, a comunicação entre uma instituição X e uma instituição Y, em que se aceitem ou se rejeitem categorias inteiras de prova sem que seja necessário rastrear os DIDs e as práticas comerciais encontrados em cada emissor individual.



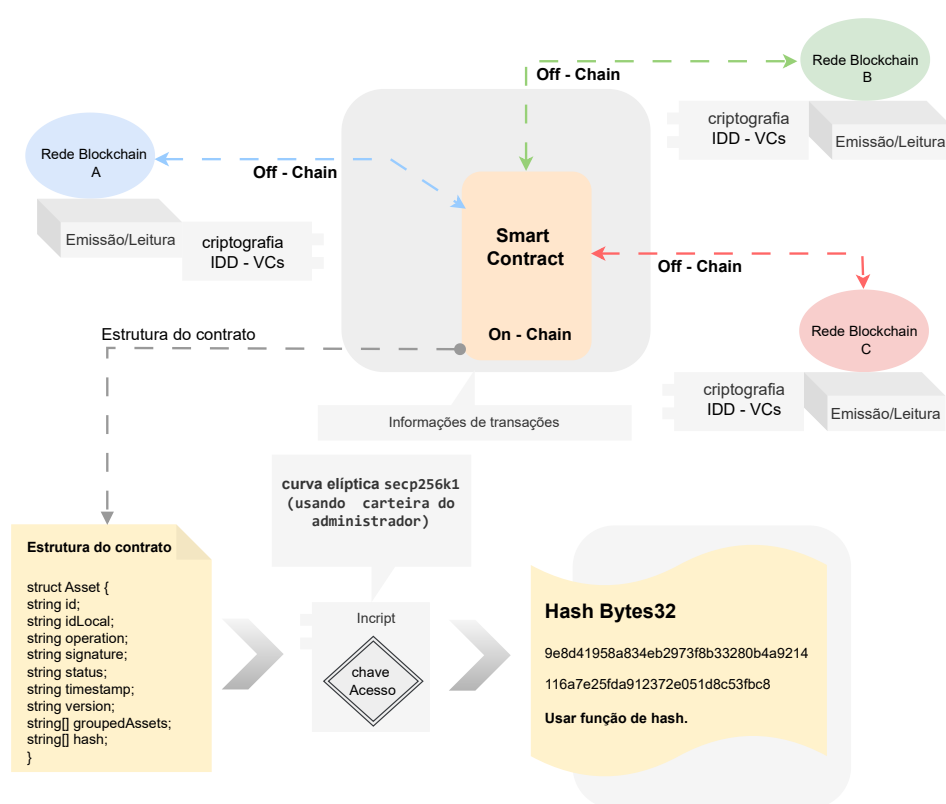
**Figura 2. Arquitetura Teórica da Proposta**

A Figura 2 mostra bem como o modelo visa ser um meio de comunicação agnóstico, fazendo com que se tenha a real interoperabilidade descentralizada, utilizando esquemas de atributos e regras de emissão e verificação, utilizando técnicas de IDD inseridas de maneira Off-chain e critérios definidos via contratos inteligentes de forma On-chain, para a execução final de comunicação de redes distribuídas distintas.

### 3.1. Fluxo de Funcionamento Prático

O contexto inicialmente proposto combina fundamentos teóricos e ferramentas técnicas contidos na Figura 3. Por exemplo, considera-se o processo inicial de emissão e leitura

de informações específicas (X ou Y) usando diferentes blockchains (A, B ou C). Inicialmente, a informação é criptografada e vinculada a uma credencial verificável (VC) ou a um identificador descentralizado (DID) público, sendo então armazenada em um contrato inteligente (on-chain). O sistema verifica para qual rede blockchain a informação será encaminhada, agindo como um intermediário ou broker de acordo com o modelo de governança previamente estabelecido. Ao chegar à rede de destino, a informação é descriptografada em um ambiente off-chain, validando-se as credenciais inicialmente associadas e garantindo que a chave utilizada está correta. Um mecanismo adicional de segurança assegura que uma rede não autorizada não tenha acesso à chave necessária, garantindo privacidade e segurança na comunicação entre as redes envolvidas.



**Figura 3. Fluxo de Comunicação entre as redes**

#### 4. Conclusão e trabalhos futuros

A ideia geral é disponibilizar uma estrutura Agnóstica, baseada em governança legível por máquina, a qual fornecerá uma camada interoperável de governança, a fim de, fornecer um padrão de comunicação entre diversas redes e aplicações. Como é um trabalho a Passo inicial, existem mais dúvidas que respostas, nisso é pretendido alguns objetivos iniciais, como: investigar as formas de governança introduzidas por blockchains baseadas em contratos inteligentes e mecanismos registros por meio de identidade digita, a elaboração de uma estrutura que forneça uma camada de fato interoperável de integração, onde seja possível ler as regras (contratos inteligentes) de uma linguagem que as máquinas possam interpretar, através do uso de inteligência artificial baseado no registro de credenciais

verificáveis e por fim, A realização de uma avaliação experimental da estrutura implementada comparando com abordagens convencionais, e expondo ganhos de comunicação entre redes descentralizada.

## 5. Agradecimentos

Os autores reconhecem o apoio dado a este trabalho pelo MCTI-Ministério da Ciência, Tecnologia e Inovação, com recursos financeiros do FUNTTEL e administrados pela FI-NEP, no âmbito, especificamente, do projeto TECSEG - Desenvolvimento de tecnologias e metodologia de avaliação e investigação de segurança para redes e aplicações de governo digital, contrato 01.21.0163.01, Referência 1196/21.

## Referências

- [ind 2020] (2020). Machine-readable governance theory, code, and the future.
- [ind 2021] (2021). Trust registry or machine readable governance?
- [ind 2022] (2022). Machine readable governance is the key to scaling decentralized trust.
- [mod 2024] (2024). Framework do modelo de governança 4p+i aplicado aos alvos de governança blockchain. <https://blockchain.ieee.org/standards>.
- [Alastria Consortium 2024] Alastria Consortium (2024). Alastria blockchain ecosystem. <https://alastria.io>. Acesso em: 26 mar. 2025.
- [Allende López et al. 2020] Allende López, M., Pardo, A., and Da Silva, M. (2020). LAC-Chain Framework for Permissioned Public Blockchain Networks: From Blockchain Technology to Blockchain Networks. Technical report, Inter-American Development Bank.
- [European Commission 2024a] European Commission (2024a). eidas 2.0: European digital identity framework. <https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation>.
- [European Commission 2024b] European Commission (2024b). European blockchain services infrastructure (ebsi). <https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/>. Acesso em: 26 mar. 2025.
- [FERREIRA 2022] FERREIRA, R. G. (2022). Governança de blockchain e seus componentes/ferramentas: um estudo sobre o estado-da-arte. B.S. thesis.
- [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.
- [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 Informação e de Sistemas Computacionais*, pages 29–42. SBC.
- [Tan et al. 2022] Tan, E., Mahula, S., and Cropvoets, J. (2022). Blockchain governance in the public sector: A conceptual framework for public management. *Government Information Quarterly*, 39(1):101625.