Preservação da Confiabilidade de Registros Digitais Assinados

TRUSTER Preservation Model

José Alexandre C. Vasco
Neide De Sordi

OBSERVATÓRIO NACIONAL DE BLOCKCHAIN

Sumário

23 de janeiro de 2026

Parte 1 - TRUSTCHAIN E CONFIANÇA DIGITAL

- **O Problema:** Expiração de certificados e perda da validade jurídica de longo prazo.
- **A Solução**: Arquitetura TrustChain (Projeto InterPARES Trust) baseada em DLT.
- **Inovação:** Registro imutável via TRUSTER VIP para garantir autenticidade perene.
- **Impacto:** Eliminação de revalidações periódicas e de infraestruturas centralizadas.

Parte 2 - : ADERÊNCIA A REQUISITOS E VIABILIDADE NO BRASIL

- **Normas**: Conformidade com os modelos e-Arq Brasil e MoReq-Jus .
- **Ecossistema:** Integração com RDC-Arq e Cadeia de Custódia Digital (CCDA) .
- **Estratégia:** Blindagem de ativos digitais críticos contra a obsolescência tecnológica.
- **Futuro:** Mitigação do risco quântico na preservação digital sistémica .

A contribuição brasileira

A Rede Cariniana de Preservação Digital do Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict), criada para garantir o acesso contínuo e de longo prazo a documentos eletrônicos.

Rede DRÍADE - Rede de Estudos e Práticas em Preservação Digital, grupo de Pesquisa registrado no CNPq, é parte das iniciativas da Rede Cariniana. A Driade reúne pesquisadores e instituições nacionais e internacionais para desenvolver, compartilhar e implementar conhecimentos e metodologias voltados à preservação digital.

O TRUSTER Preservation Model foi traduzido em 2025 no âmbito do PreservIA, Comitê da Rede Driade que estuda a utilização da IA na preservação digital.

^

23 de janeiro de 2026

TrustChain

O Projeto TRUSTER Preservation Model explora os desafios críticos e soluções para garantir a validade a longo prazo de documentos com assinaturas digitais, carimbos de tempo e selos digitais. Este problema afeta especialmente organizações que produzem milhões de documentos assinados digitalmente, cujos certificados expiram após um período relativamente curto.

↓INTERPARES TRUST

O relatório do projeto InterPARES Trust (ITrust) foi a quinta fase do International Research on Permanent Authentic Records in Electronic Systems Project, desenvolvido entre 2013 e 2019, com foco em preservação da confiabilidade da informação digital através da tecnologia blockchain.

23 de janeiro de 2026

O Problema da Preservação Digital

Desafios atuais na manutenção da validade jurídica a longo prazo de documentos assinados digitalmente, comprometendo a confiabilidade dos registros eletrônicos de órgãos públicos e instituições.

Limitações Técnicas

Registros digitais assinados têm validade limitada devido à expiração dos expiração dos certificados digitais e à obsolescência tecnológica, afetando afetando milhões de documentos críticos em órgãos governamentais, governamentais, instituições financeiras e hospitais.

Impactos Jurídicos

A verificação de assinaturas torna-se inviável após a expiração de certificados ou o desaparecimento da autoridade certificadora, gerando gerando riscos legais e custos elevados com soluções tradicionais como a como a reassinatura periódica.

23 de janeiro de 2026

Soluções Tradicionais

Abordagens existentes para preservação de registros digitais assinados e suas limitações suas limitações fundamentais que motivaram a busca por uma solução inovadora baseada inovadora baseada em blockchain.

Abordagens Existentes

Abordagem 1: Preservar assinaturas digitais originais e originais e toda a infraestrutura necessária, resultando resultando em custos operacionais elevados.

Abordagem 2: Eliminar assinaturas após validação, preservando apenas o conteúdo com menor custo, mas destruindo evidências de autenticidade.

Abordagem 3: Registrar rastros das assinaturas como como metadados, gerando dependência de terceiros e terceiros e perda do status de fonte primária de autenticidade.

Limitações Críticas

As soluções tradicionais apresentam problemas fundamentais: necessidade de revalidações periódicas (reassinaturas), dependência de terceiros confiáveis, custos crescentes e perda gradual de autenticidade ao longo do tempo.

Tais limitações demonstram a necessidade de uma quarta abordagem inovadora: a utilização de blockchain para garantir a preservação permanente da validade.

23 de janeiro de 2026

Estudos de Caso Reais

Validação do modelo TRUSTER através de três estudos de caso realizados entre 2016-2017, com parceiros institucionais na Europa, focando em registros com assinaturas digitais expiradas e seus desafios de preservação.

FINA (Croácia)

Sistema **e-Regos** de fundos de aposentadoria foi desativado e transferido para FINA. Os registros possuíam assinaturas qualificadas e carimbos de tempo, mas não podiam mais ser validados porque as CRLs e cadeias de certificados não foram preservadas.

TechEd (Croácia)

Registros do sistema **e-Tax** da Administração Tributária continham assinaturas XML e carimbos de tempo de 2006 que não eram mais passíveis de validação devido à expiração e não preservação das CRLs, além da ausência de metadados sobre validade das assinaturas.

Enigio Time (Suécia)

Registros médicos e administrativos da região de Skåne apresentavam documentos críticos assinados digitalmente, mas a validade não era verificada no momento do arquivamento, com informações salvas apenas como metadados, sem estratégia de comprovação futura.

Constatações dos Estudos

23 de janeiro de 2026

Análise dos resultados obtidos nos três estudos de caso demonstrou pontos críticos nos processos de processos de preservação digital e validou a necessidade de uma solução baseada em blockchain. blockchain.

+ **Ausência de Preservação**

Identificada insuficiência de ações de preservação preservação digital específicas para registros registros assinados digitalmente, resultando em resultando em documentos críticos com assinaturas não validáveis.

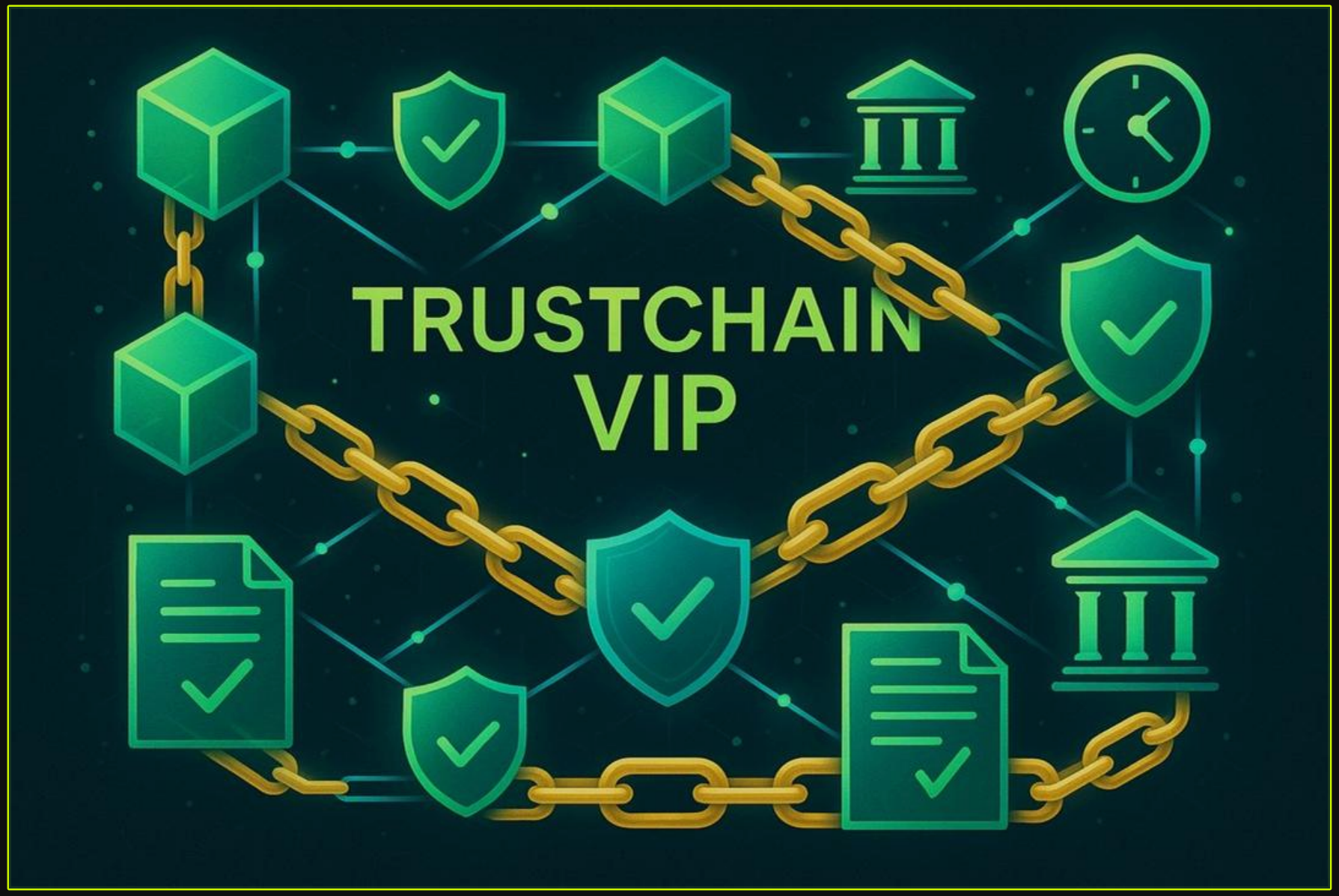
+ **Riscos Institucionais**

Constatados significativos riscos legais e operacionais devido à expiração de certificados digitais e à falta de preservação das CRLs, comprometendo a autenticidade a longo prazo.

+ **Validação da Proposta**

Os estudos confirmaram a necessidade urgente de urgente de uma solução como o TrustChain, que que preserve permanentemente a informação de informação de validade sem depender de reassinaturas periódicas.

23 de janeiro de 2026
2026



23 de janeiro de 2026

TrustChain VIP

(Validity Information Preservation)

Uma solução inovadora que utiliza **blockchain** para registrar a validade de assinaturas digitais em uma blockchain, eliminando a necessidade de reassinaturas periódicas e preservando permanentemente a prova de autenticidade.

O **TRUSTER VIP** (Validity Information Preservation) representa uma quarta abordagem para a preservação digital confiável a longo prazo.

23 de janeiro de 2026

Como Funciona o TrustChain

O TrustChain é uma rede blockchain semiaberta que armazena apenas o hash do documento documento assinado digitalmente, preservando a prova de autenticidade sem depender de uma depender de uma única fonte de confiança, eliminando a necessidade de resignaturas periódicas. resignaturas periódicas.

Validação Distribuída

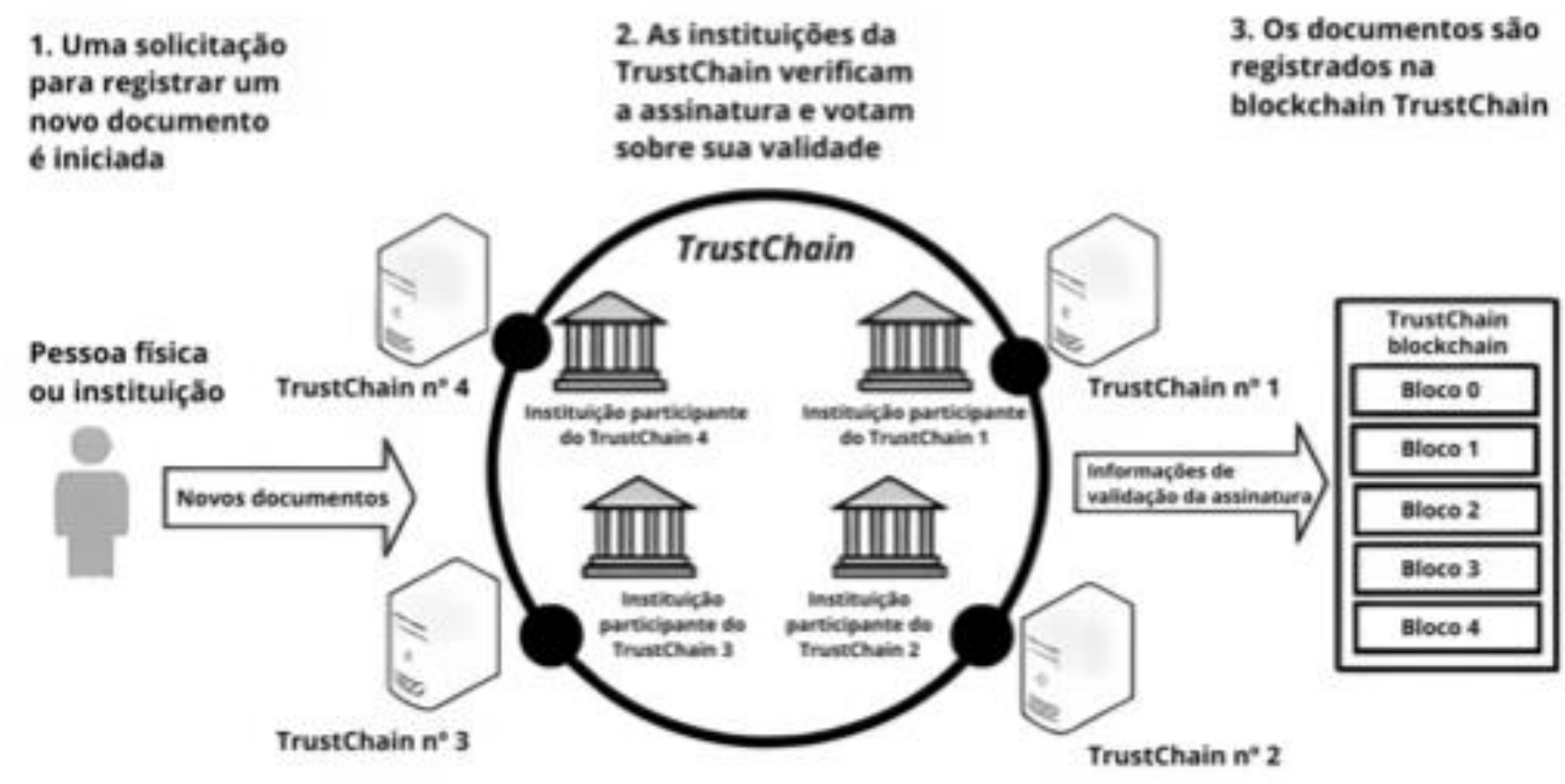
Múltiplas instituições autorizadas inserem e validam registros na rede. Mecanismo de votação votação entre nós participantes para validar blocos blocos antes da inclusão na cadeia. A arquitetura de arquitetura de confiança distribuída elimina dependência de autoridades certificadoras individuais e aumenta a resiliência contra fraudes, fraudes, **já que seria necessário comprometer múltiplos nós para inserir registros fraudulentos**.

Registro e Preservação

O sistema armazena o hash do documento junto com metadados essenciais e timestamp, não o documento em si. Complementa sistemas de gestão documental existentes, não os substitui. O formato dos registros é baseado em JSON, incluindo dados sobre a autoridade certificadora e referências do documento original.

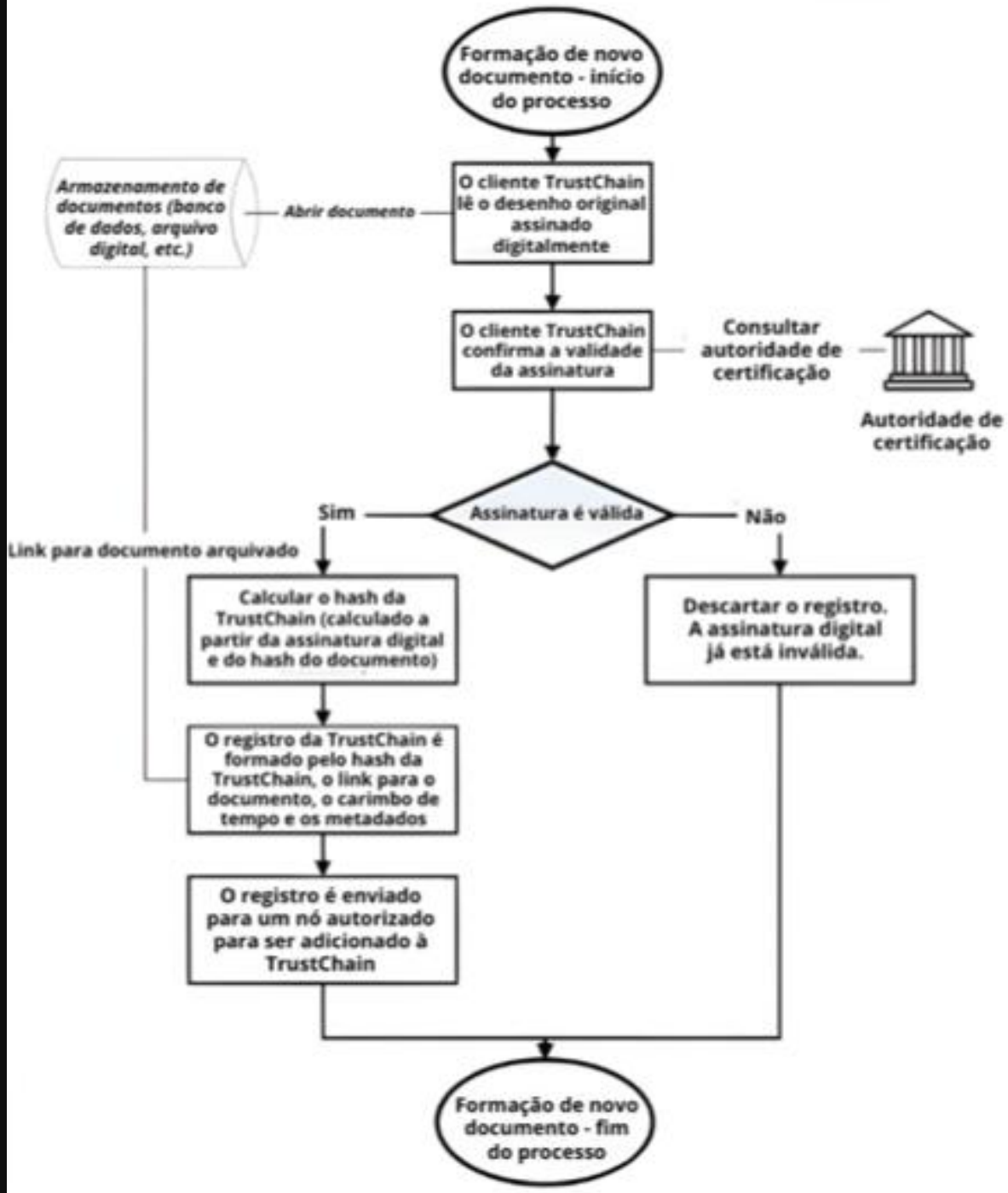
Conceito de TrustChain

23 de janeiro de 2026



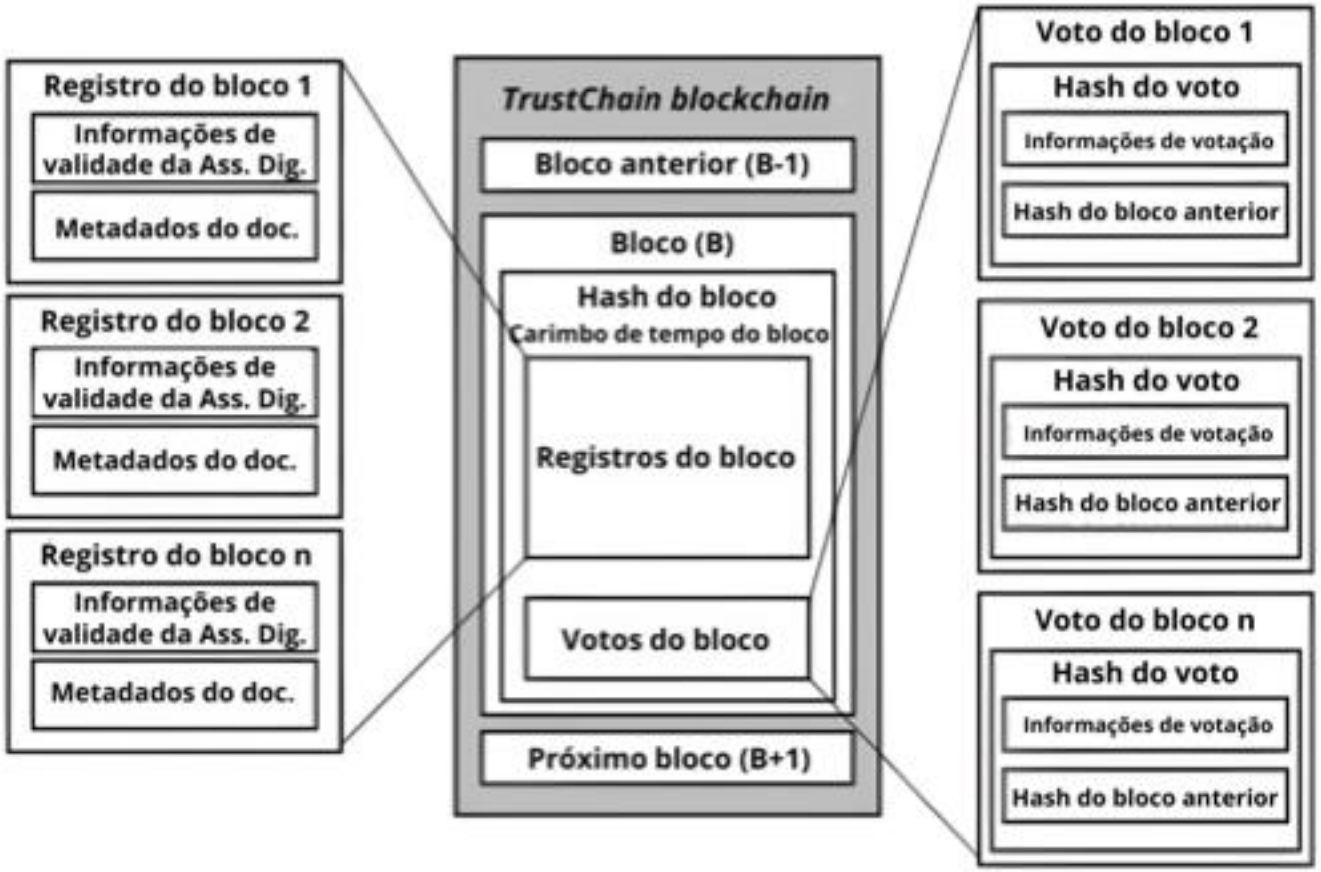
23 de janeiro de 2026

Registro de um documento no TrustChain



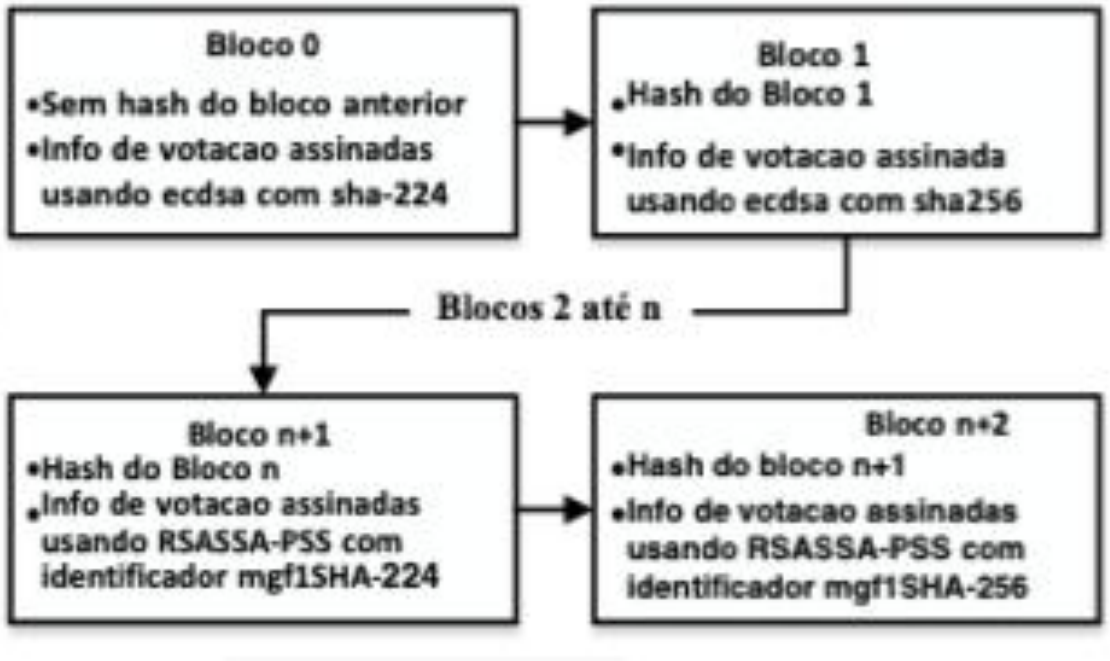
Estrutura de blockchain no TrustChain

23 de janeiro de 2026



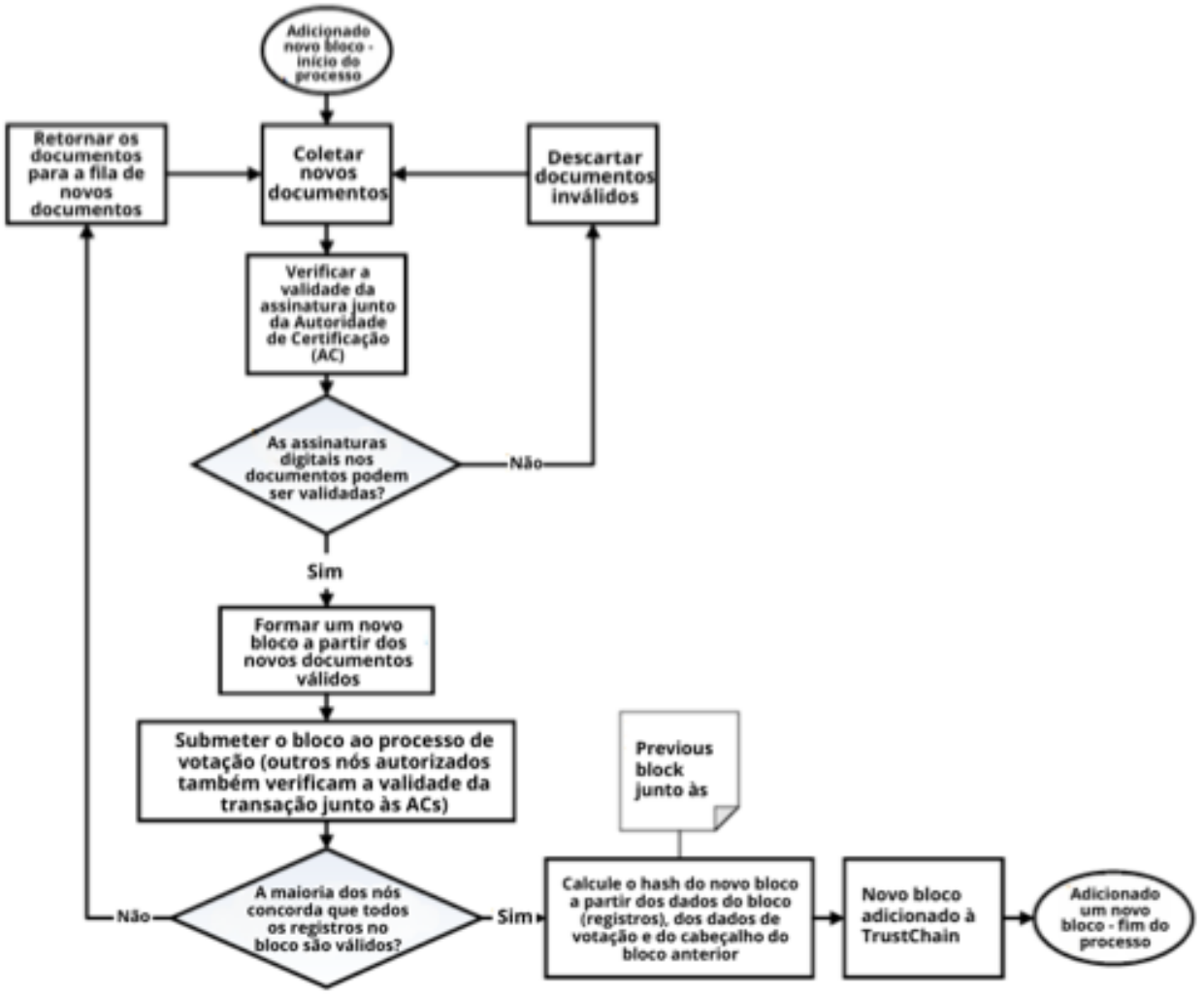
Mudanças no algoritmo de voto

23 de janeiro de 2026



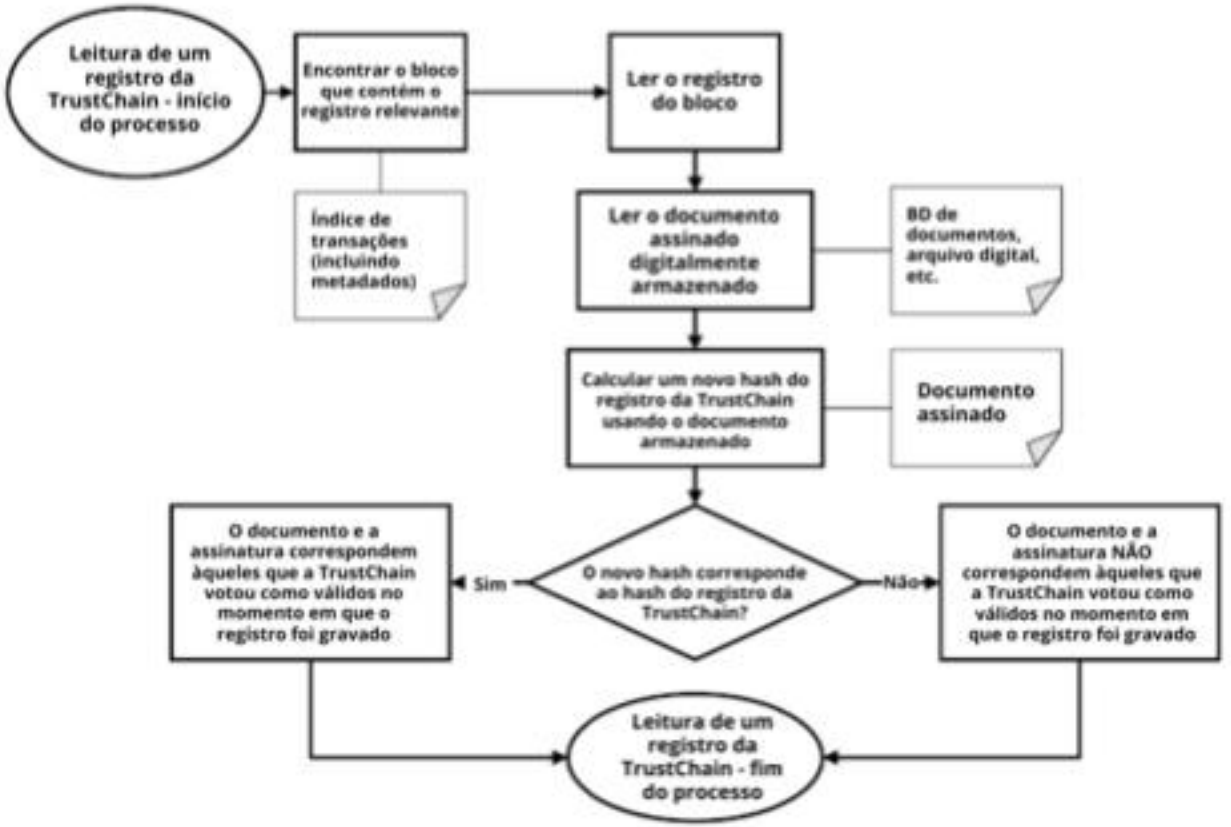
Adicionando um novo bloco ao TrustChain

23 de janeiro de 2026



Lendo um registro do TrustChain

23 de janeiro de 2026



23 de janeiro de 2026

Vantagens

O modelo TrustChain oferece soluções inovadoras para os desafios de preservação digital de registros assinados, proporcionando confiabilidade e sustentabilidade a longo prazo.

- \+ Fornece evidências robustas de que a assinatura era válida no momento do registro e de que não houve adulteração
- \+ Elimina a necessidade de reassinaturas periódicas ou carimbos de tempo adicionais
- \+ Aprimora a validação de registros para preservação a longo prazo
- \+ Não depende de uma única entidade confiável, distribuindo a confiança entre instituições participantes

Desenvolvimentos Futuros & Impacto

23 de janeiro de 2026

+ Evolução Técnica

Novas implementações em desenvolvimento incluem TrustChain-H para preservação eficiente de hashes, TrustChain-C para armazenamento otimizado de intervalos de validade, e integração de carimbos de tempo qualificados em cada bloco da cadeia.

+ Impacto Institucional

O modelo TRUSTER representa uma abordagem inovadora para a arquivologia digital, oferecendo uma solução sustentável para o desafio da preservação de longo prazo e validade legal de documentos assinados, com potencial transformador para instituições públicas e privadas.

+ Segurança Aprimorada

Implementação de esquemas de chave transitória aumentará a resiliência contra ameaças futuras de computação quântica, garantindo que o modelo permaneça seguro mesmo diante da evolução tecnológica.

23 de janeiro de 2026

Aplicações do TRUSTER Preservation Model

ADERÊNCIA A REQUISITOS: como a arquitetura **TrustChain** atende aos modelos de requisitos de sistemas de gestão de documentos **e-ARQ Brasil e MoReq-Jus e do Modelo OAIS/RDC-Arq de preservação digital.**

VIABILIDADE: análise da compatibilidade do **TrustChain** com o ecossistema digital brasileiro (cases: **ICP-Brasil e Diploma Digital).**

RISCOS FUTUROS: o principal desafio de longo prazo: o risco quântico e o posicionamento do **TrustChain** como arquitetura resiliente preparada para a **Criptografia Pós-Quântica (PQC).**

AUTENTICIDADE: FUNDAMENTO ARQUIVÍSTICO

Custódia ininterrupta – Garantia da validade probatória e histórica de um documento

CADEIA DE CUSTÓDIA – Requisito que assegura a **autenticidade e a presunção de prova** de um registro desde sua criação até a destinação final.

CADEIA DE PRESERVAÇÃO (CoP) - InterPARES Conjunto de estratégias e atividades técnicas para garantir autenticidade ao longo do ciclo de vida.

TRUSTCHAIN COMO COMPLEMENTO DA CoP
Registra prova de autenticidade em DLT
Garante perenidade independente de sistemas centralizados

TrustChain vs ChainGUARD - Convergências

Aspecto	TrustChain	ChainGUARD
Foco	Cadeia de **preservação** de documentos arquivísticos digitais	Cadeia de **custódia** de vestígios digitais em investigações criminais
Objetivo	Autenticidade e confiabilidade de longo prazo	Integridade e rastreabilidade durante **investigações e processos judiciais**
Tecnologia	Blockchain + hashes criptográficos + metadados de preservação + políticas arquivísticas de preservação	Blockchain + **banco imutável** off-chain + hashes criptográficos + assinaturas digitais
Público	Arquivos, repositórios digitais, patrimônio cultural	Polícia, perícia forense, Ministério Público, Judiciário
Ciclo de vida	Todo o ciclo (ênfase no **longo prazo** e preservação permanente)	Coleta → movimentação → uso processual (foco no **curto/médio prazo**)

TrustChain - foca em **PRESERVAÇÃO** (guarda longa). O **ChainGuard** - foca nos registros da **PERÍCIA** (curto prazo).
Os Vestígios digitais são documentos que precisam de preservação digital permanente.

TrustChain & Modelo OAIS: Complementaridade Estratégica

O Dilema da Preservação: A migração de formatos (ex: PDF/A → X) é necessária para a legibilidade futura (RDC-Arq), mas ela invalida a assinatura digital original.

A Solução TrustChain: Foca na preservação da prova. Registra a validade da assinatura no momento da ingestão, antes que a migração ocorra.

Integração com o Modelo OAIS (ISO 14721):
Fornece PDI (Informação de Descrição de Preservação) externo ao repositório.
Uso de DLT (Blockchain) assegura proveniência e fixidez imutáveis.

Diferencial: A prova de autenticidade sobrevive à obsolescência tecnológica e a eventuais falhas do repositório centralizado.

ISO/TR 24332:2025 | Padronização da Gestão Documental com Blockchain

Integra Blockchain e DLT à gestão documental, promovendo interoperabilidade e preservação de registros autoritativos autênticos.

ASPECTO	TRUSTCHAIN (TRUSTER)	ISO/TR 24332:2025
Natureza	Modelo técnico/protótipo	Norma orientadora
Foco	Validade de assinaturas digitais	Registros autoritativos (documentos arquivísticos).
Tecnologia central	Blockchain semiaberta, multi-institucional	Blockchain/DLT (diversos modelos)
Participação	Ingestão restrita, acesso aberto	Vários modelos possíveis
Metadados	ISAD(G), JSON, interoperabilidade	Reforça importância dos metadados
Governança	Votação entre nós institucionais	Apresenta conceitos, mas não prescreve
Compatibilidade	Complementar a sistemas arquivísticos	Compatível com múltiplos sistemas
Permanência dos registros	Permanente, sem revalidação periódica	Recomenda permanência e integridade

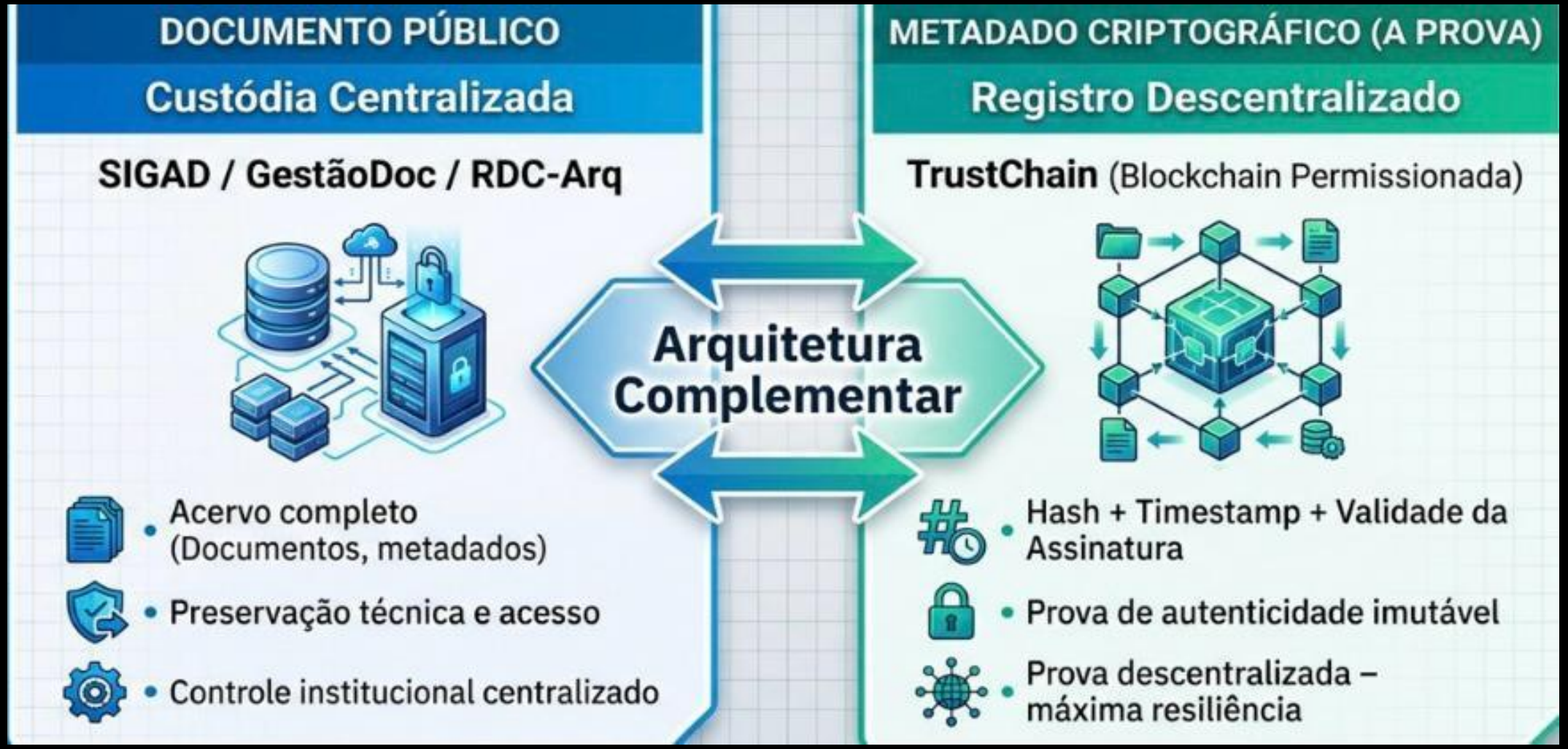
Compatibilidade com os modelos de requisitos e-ARQ Brasil e MoReq-Jus

- **Os Modelos de requisitos para sistemas de gestão de documentos e-ARQ Brasil, aprovado pelo Conarq e MoReq-Jus, – aprovado pelo CNJ estabelecem os requisitos e metadados que esses sistemas devem atender.**

- **O TrustChain** – garantia do registro imutável da **prova de autenticidade c**omplementar e essencial aos modelos de requisitos nacionais para **garantir a validade e autenticidade da assinatura digital a longo prazo**, superando o risco de obsolescência do certificado.

- **Resultado da análise:** 100% de aderência aos requisitos obrigatórios

Sistemas de gestão e preservação de documentos e o TrustChain - Complementariedade



Requisito	e-ARQ Brasil (V2.) / MoReq-Jus (2ª Edição)	Valor Agregado : TrustChain
Verificar validade na captura	**7.5.3 / 11.6.1.3 (O**): Exige a verificação da assinatura digital no momento da captura.	A validação inicial do sistema alimenta a Blockchain com um dado verificável.
Registro de validade (Metadado)	**7.5.4 / 11.6.1.4 (O) (RNF) :** Exige o registro do status de validade e data/hora como metadado. R.NF.S.7.1.3	O registro na blockchain torna este metadado inalterável, cumprindo o requisito de permanência da prova.
Código de Integridade (Hash)	**RCA4.1.23 (RF)/ RSE11.7.1/73 (O):** Atribuição de código hash para manutenção da Fixidez.	O TrustChain armazena o hash do documento, garantindo a integridade (Fixidez) por meio de um mecanismo externo, a prova de falhas.
Carimbo de Tempo Confiável	**7.6.1 / 11.7.1 (O) (RNF):** Acesso a relógios e carimbador de tempo confiáveis.	**Timestamp intrínseco:** O TrustChain fornece um timestamp inerente ao bloco, distribuído e seguro, atendendo diretamente a esta obrigação.

TrustChain: Elimina a complexidade na Gestão da Lista de Certificados Revogados (LCR)

- **Os modelos de requisitos e-ARQ Brasil e MoReq-Jus exigem a custódia e a consulta constante às LCR de cada Autoridade Certificadora.**
- **Em qualquer sistema, a Infraestrutura de Chaves Públicas (PKI) exige a custódia (perpétua e inviável) de LCRS.**

Eixo	Ação do TrustChain (A Solução Cripto-Ágil)	Ganho Estratégicos
Simplificação Operacional	TrustChain realiza a complexa consulta à LCR de todas as ACs **apenas** no momento da validação inicial da assinatura.	Os sistemas são **liberados** da tarefa cara de armazenar e gerenciar dezenas de listas históricas de diferentes ACs.
Prova de Validade Perene	O sistema registra o **status de validade** resultante dessa consulta em um único metadado imutável: **TRUSTER VIP** na Blockchain.	O TrustChain garante a conformidade tornando a prova perene e imune ao colapso do sistema de custódia das LCR .

Uso e potencial do TrustChain - ICP-Brasil

O ITI já utiliza a tecnologia blockchain no sistema de carimbo de tempo da ICP-Brasil desde 2021.
Em 2025, o ITI oficializou o uso da blockchain para certificar data e hora em documentos oficiais.

O TrustChain é a extensão lógica dessa política para o problema do Longo Prazo: se o blockchain é robusto para garantir segurança e rastreabilidade na emissão do carimbo de tempo (Curto Prazo), é também a aplicação ideal para o Longo Prazo.

TrustChain não substituiria procedimentos na ICP-Brasil e nem interferiria no trabalho diário ou na fiscalização e auditoria. Ele poderia assumir o desafio após a validade do certificado expirar.

Complementariedade: O TrustChain usa o mesmo princípio de imutabilidade já endossado pelo ITI para criar a Prova de Validade Perene.

A ICP-Brasil demonstra que a tecnologia Blockchain é confiável; o TrustChain pode estender essa confiança validada para todo o ciclo de preservação do documento público.

eIDAS 2.0 - REGULAMENTO (UE) 2024/1183
MUDANÇA DE PARADIGMA REGULATÓRIO:

- **PRESERVAÇÃO DIGITAL = SERVIÇO DE CONFIANÇA REGULAMENTADO → Provedores certificados DEVEM garantir validade perene de assinaturas**

- **ESPECIFICAÇÃO CEN/TS 18170:2025**: **requisitos funcionais para garantir preservação, integridade e confiança**

- **DLT OFICIALMENTE RECONHECIDA →** Tecnologias de Registro Distribuído integradas à infraestrutura de confiança da UE → Blockchain = solução legítima para serviços de preservação como prova de integridade e temporalidade. O arquivamento digital deve ser auditável e perene.

: UE reconhece que PKI tradicional é INSUFICIENTE para preservação

O TrustChain antecipa esta evolução global ao oferecer uma camada de preservação baseada em evidências, superando as limitações da PKI tradicional.

↓

CONVERGÊNCIA BRASILEIRA: Lei 14.063/20 (assinatura eletrônica) inspirada no eIDAS

ASSINATURA CADASTRADA (login/senha) e o TrustChain

- **Os modelos de requisitos e a legislação classificam a autenticação por login e senha com nível de segurança inferior ao da certificação digital.**
- **TrustChain eleva confiabilidade de sistema já consolidado sem exigir migração para certificação digital**

Pontos Críticos

Aspecto	Fragilidade SIGAD/GestãoDoc	Solução TrustChain
Não Repúdio Jurídico	A assinatura cadastrada não confere presunção legal de autoria com o mesmo rigor da ICP-Brasil, sendo mais contestável em juízo.	Registra o hash do evento em DLT, conferindo prova criptográfica inegável de que a ação ocorreu, elevando a confiança do metadado de autenticação.
Risco para a custódia	A validade da prova depende inteiramente da integridade do banco de dados central do SIGAD, que é um ponto único de falha.	Registra o Timestamp Intrínseco e o hash na DLT, garantindo que o metadado permaneça íntegro, mesmo que o sistema central falhe ou seja desativado.
Segurança da Ação (risco de fraude)	A chave é vulnerável a roubo, e a autoria pode ser repudiada. O log da ação é vulnerável à adulteração.	Garante a imutabilidade do registro da ação. O log de auditoria é protegido pela DLT, impedindo que a fraude ou o repúdio sejam encobertos.

CASO DE USO: DIPLOMA DIGITAL (MEC/RNP)

- **CONTEXTO**: Portaria MEC nº 554/2019: Instituição do Diploma Digital RNP: Infraestrutura de registro e validação Desafio: Validade de longo prazo (50+ anos)
- **FRAGILIDADES ATUAIS:** Certificados ICP-Brasil: Validade 1-5 anos Instituição emissora pode encerrar atividades Necessidade de revalidação periódica TRUSTCHAIN COMO SOLUÇÃO: Registro da validade do diploma
- **NO MOMENTO DA EMISSÃO ↓ TRUSTER VIP (**Blockchain): Prova imutável ↓ Validação independente de: • Validade do certificado emissor • Existência da instituição • Revalidações periódicas
- **IMPACTO:** Diploma com validade probatória perene = Segurança jurídica para estudantes e instituições

AMEAÇA QUÂNTICA E A RESILIÊNCIA DO TRUSTCHAIN

O documento que assinamos com validade legal hoje terá valor probatório daqui a 20 ou 50 anos, quando o hardware quântico estiver maduro?

ALGORITMO DE SHOR: Quebra criptografia de chave pública (RSA, ECC)
Computadores quânticos em 10-20 anos

ATAQUE HNDL (Harvest Now, Decrypt Later):
Documentos capturados HOJE
Decifrados no FUTURO quando hardware quântico estiver disponível → Repúdio de autoria/assinatura

SOLUÇÃO CRIPTO-ÁGIL DO TRUSTCHAIN:

- O TrustChain registra o EVENTO de validação: "Esta assinatura ERA VÁLIDA em 23/01/2026".
- A prova é registrada em DLT (independente do algoritmo).
- Quando a PQC (Criptografia Pós-Quântica) estiver madura, a migração transparente da prova para um novo algoritmo MANTÉM o valor probatório perene.
- RESULTADO: A prova sobrevive à obsolescência.

|Obrigado

José Alexandre Vasco |
Vasco.jose@fgv.edu.br

Neide De Sordi
nsordi@gmail.com