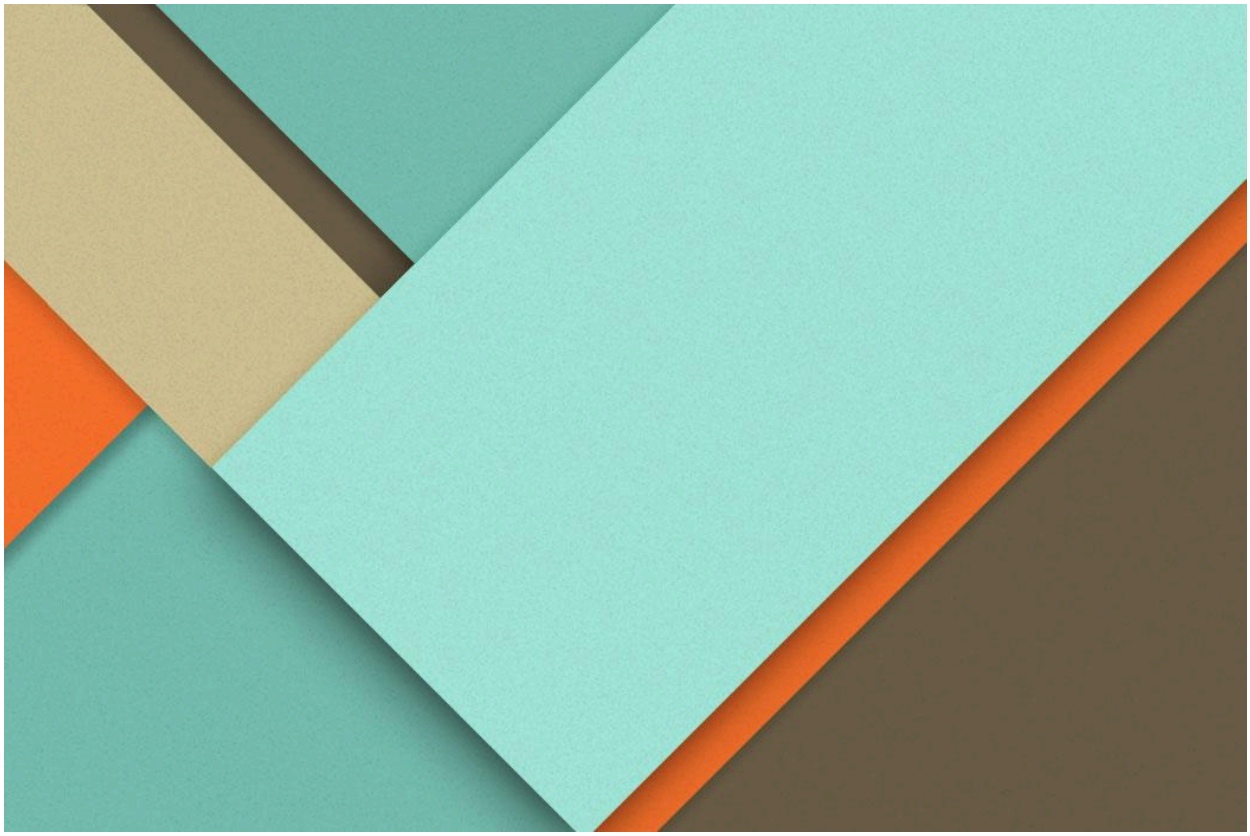

DataTrust-CA, Alqueire DataCenter, against the DIGITAL CRIMES

03.07.2025

—

Mario Caseiro
MCL Desenvolvimento de Software LTDA - Sintaxes Tecnologia
Rua Galeazzo Alessi 70, conj 111
São Paulo, SP 04305-050

Memorando Oficial: Proposta para uma Infraestrutura Nacional de Confiança Digital

Assunto: Proposta para uma Infraestrutura Nacional de Confiança Digital: Integrando DataTrust CA, Corda DLT Fork e Data Centers Alqueire para Segurança Aprimorada e Oportunidade Econômica

Para: Autoridades Governamentais (e.g., Banco Central do Brasil, Ministério da Fazenda, Ministério da Ciência, Tecnologia e Inovação), Partes Interessadas Chave do Setor Privado (Instituições Financeiras, Empresas de Tecnologia) De: [Seu Nome/Título - e.g., Mario Caseiro, Diretor de Tecnologia / Arquiteto Chefe, FAP Consulting & MCL Desenvolvimento de Software] Data: 3 de julho de 2025

I. Introdução e Sumário Executivo: Assegurando o Futuro Digital do Brasil

A rápida adoção de instrumentos financeiros digitais no Brasil, em particular o Pix, ressalta tanto um progresso imenso quanto vulnerabilidades críticas em nossa infraestrutura digital nacional. O recente incidente, com o roubo reportado de 1 bilhão de Reais de contas Pix interbancárias, serve como um lembrete vívido e alarmante de que os protocolos de segurança existentes, como TLS/SSL, embora vitais para canais de comunicação seguros, não garantem inerentemente a integridade dos dados de transação em sua camada mais profunda e crítica – o próprio *payload*. Atores maliciosos podem explorar essa lacuna ao alterar parâmetros sensíveis antes ou depois que os dados sejam criptografados para transporte, resultando em perdas financeiras significativas e erosão da confiança pública.

Este memorando delineia uma iniciativa estratégica inovadora para transformar fundamentalmente o cenário da segurança digital do Brasil. Propomos o estabelecimento de uma robusta infraestrutura nacional de confiança digital centrada em três pilares interconectados: DataTrust CA, um conceito revolucionário para a certificação da integridade de dados; uma DLT (*Distributed Ledger Technology*) permissionada de nível estatal e *fork* do Corda da R3, garantindo registros de transações imutáveis e confidenciais; e uma rede distribuída de Alqueire Data Centers *Tier IV*, fornecendo a segurança física fundamental e resiliência. Esta solução abrangente não apenas aborda as vulnerabilidades atuais, mas também cria uma oportunidade de negócio sem precedentes para o governo alavancar sua própria infraestrutura confiável para entrar e liderar o mercado de alta tecnologia.

II. O Desafio: Preenchendo a Lacuna da Confiança Digital

A economia digital prospera na confiança, mas essa confiança é constantemente desafiada por ameaças cibernéticas em evolução. Enquanto o *Transport Layer Security* (TLS/SSL) efetivamente criptografa dados em trânsito e autentica identidades de servidores, ele opera na camada de rede. Isso deixa uma vulnerabilidade crítica na camada de *application*: parâmetros de dados sensíveis dentro de transações digitais (como aqueles incorporados em links de pagamento Pix) podem ser manipulados antes da assinatura criptográfica pelo remetente ou após a descriptografia pelo destinatário sem quebrar a sessão TLS. Esse "ponto cego" nas estruturas de segurança existentes permite fraudes sofisticadas, como evidenciado pelo recente incidente Pix em larga escala.

O paradigma atual, onde a dependência principal é colocada na segurança do canal, é insuficiente para a escala e criticidade das transações digitais modernas. Uma nova abordagem é urgentemente necessária – uma que mude de uma suposição de canais seguros para uma garantia verificável da integridade do conteúdo, garantindo que o *payload* dos dados em si seja autêntico, inalterado e confiável de ponta a ponta.

III. DataTrust CA: O Novo Paradigma da Certificação de Integridade de Dados

O DataTrust CA (Autoridade Certificadora) representa essa mudança fundamental. Ao contrário da PKI (*Public Key Infrastructure*) tradicional focada na identidade e segurança de transporte, o DataTrust CA é concebido como uma nova classe de entidade certificadora dedicada à validação da integridade de *payloads* de dados na camada de *application*.

A metodologia central do DataTrust CA envolve:

- **Canonicalização de Dados e *Hashing* SHA-256: Antes de qualquer transmissão de dados, os parâmetros de transação sensíveis são primeiro canonicalizados (padronizados) e então submetidos a um algoritmo de *hashing* SHA-256 criptograficamente seguro. Isso cria uma impressão digital única e de tamanho fixo dos dados.**
- **Criptografia ECC e Certificação: Este *hash*, juntamente com o *payload* dos dados (serializado eficientemente usando formatos compactos como MessagePack), é então criptografado usando ECC (*Elliptic Curve Cryptography*). O ECC é escolhido por sua alta segurança com tamanhos de chave menores, crítico para desempenho e escalabilidade em sistemas de alto volume como o**

Pix. O DataTrust CA então certifica este *payload* criptograficamente seguro, fornecendo uma atestação de sua integridade e autenticidade.

- **Integridade Ponta a Ponta: Este processo garante que, se um único parâmetro dentro do *payload* dos dados for alterado, a assinatura criptográfica será invalidada, e a transação será imediatamente rejeitada, acionando um alerta. Isso fecha fundamentalmente a lacuna de segurança explorada por muitos esquemas de fraude atuais.**

Ao implementar o DataTrust CA, o Brasil estabelece uma robusta camada criptográfica que garante a fidelidade e a não corrupção das informações digitais, promovendo uma nova era de confiança verificável em nossa infraestrutura digital nacional.

IV. Corda DLT Fork: Um Ledger Soberano e Seguro para Registros Imutáveis

Para complementar as capacidades de certificação do DataTrust CA, propomos o desenvolvimento de uma DLT de nível estatal, *open-source*, baseada em um *fork* do Corda da R3 consortium. O Corda é uma plataforma *blockchain* permissionada comprovada, amplamente adotada no setor financeiro globalmente. Seu design suporta inerentemente altos níveis de privacidade e confidencialidade, o que é primordial para dados financeiros e governamentais sensíveis.

As principais características desta DLT proposta incluem:

- ***Blockchain* Permissionada: A DLT seria controlada e operada por uma entidade confiável, como o Banco Central do Brasil (BACEN), garantindo supervisão regulatória e estabilidade. Essa natureza permissionada permite um controle rigoroso sobre as identidades dos participantes e a governança da rede.**
- ***Blockchain* Criptografada: O próprio *blockchain* abrigaria registros de transações onde os *payloads* são serializados em MessagePack, criptografados com ECC, e certificados pelo DataTrust CA. Isso garante que, embora a integridade dos dados seja registrada de forma imutável no *ledger*, o conteúdo sensível da transação permanece criptografado e acessível apenas às partes legítimas da transação (gerador e destinatário) que possuem as chaves ECC únicas.**
- **Registros Imutáveis e Verificáveis: Esta DLT serve como um registro irrefutável e auditável de todas as transações certificadas pelo DataTrust CA. Ela fornece prova definitiva da integridade dos dados, permitindo verificação instantânea por instituições autorizadas e simplificando significativamente os processos de auditoria.**

- **Adaptação e Soberania: O *forking* do Corda permite um desenvolvimento sob medida para atender aos requisitos regulatórios, de segurança e operacionais específicos do Brasil, garantindo a soberania digital sobre este *ledger* crítico. Além disso, as parcerias existentes da R3 com entidades como a CIP (Câmara Interbancária de Pagamentos) e a Rede Brasileira de Sistemas Financeiros Nacionais (*Blockchain Network*) demonstram a compatibilidade e relevância do Corda dentro do ecossistema financeiro nacional.**

Esta camada DLT cria um mecanismo seguro, transparente (quando autorizado) e altamente eficiente para gerenciar ativos digitais, desde dinheiro M1 até documentos oficiais, proporcionando um nível de confiança sem precedentes nas trocas digitais.

V. Alqueire Data Centers: A Fundação da Soberania e Resiliência Digital

Todo o ecossistema digital seguro – compreendendo as operações do DataTrust CA e a DLT Corda de nível estatal – exige uma infraestrutura física igualmente robusta e resiliente. Propomos o desenvolvimento de Alqueire Data Centers: uma rede de instalações *Tier IV* estrategicamente distribuídas por todo o Brasil, especificamente dentro de cada unidade da federação, e idealmente co-localizadas perto de usinas hidrelétricas para garantir fontes de energia sustentáveis, redundantes e seguras.

Os Alqueire Data Centers são meticulosamente projetados para serem um baluarte de segurança e resiliência, aderindo aos mais altos padrões globais (*Tier IV*) para *uptime*, redundância e tolerância a falhas. Seu propósito principal é:

- **Garantir Integridade Inquestionável: Fornecer o ambiente fisicamente seguro necessário para a operação contínua e ininterrupta do *blockchain* DataTrust CA, processando bilhões de transações com segurança.**
- **Proteger Chaves Privadas: Crucialmente, esses *data centers* são projetados para proteger as chaves privadas do DataTrust CA, que são primordiais para a integridade criptográfica de todo o sistema. Segurança física em várias camadas, controles ambientais avançados e sistemas sofisticados de monitoramento garantirão sua proteção.**
- ***High Availability* e Escalabilidade: O design *Tier IV* garante o máximo *uptime* e a capacidade de escalar as operações para atender às crescentes demandas de uma economia digital nacional.**

Além de servir como a base para a confiança digital nacional, os Alqueire Data Centers são concebidos com um modelo operacional duplo que apresenta uma oportunidade de negócio única para o governo:

1. **Data Centers Operacionais Estatais: Um dos dois Alqueire Data Centers em cada unidade federativa seria dedicado exclusivamente à hospedagem do *core* da DLT e serviços relacionados para operações governamentais. Isso inclui o gerenciamento de transações de dinheiro M1 digital, a segurança de documentos oficiais e o fornecimento de um *ledger* confiável para todas as trocas digitais em nível estadual. Isso garante o controle governamental direto sobre seus ativos e infraestrutura digitais críticos.**
2. **Serviços de Ledger de Alta Segurança para o Setor Privado: O segundo Alqueire Data Center em cada par seria dedicado à comercialização de serviços de *blockchain* privado de alta segurança e confiança para empresas. Alavancando a mesma infraestrutura *Tier IV*, capacidades de certificação DataTrust CA e robusta tecnologia DLT, o governo pode oferecer segurança, integridade e confidencialidade incomparáveis para transações digitais do setor privado. Isso cria uma nova e significativa fonte de receita, posiciona o governo como um provedor de serviços digitais de ponta e altamente seguros, e fomenta a inovação dentro do setor privado ao fornecer uma plataforma confiável.**

Uma adição crítica e inovadora a esta arquitetura reside na troca física das chaves ECC emparelhadas (*pair-to-pair*). Esta medida, que reforça a segurança fora da camada digital, ocorreria em infraestruturas governamentais previamente dedicadas à recepção de pessoas para trabalhos ou necessidades estatais, e para instituições bancárias, garantindo um ponto de contato físico e seguro para o intercâmbio de um dos ativos mais críticos do sistema. Este processo garante que a *key* ECC só seja fisicamente entregue e pareada, impedindo qualquer interceptação digital na fase de *key exchange*, elevando o nível de segurança a um patamar sem precedentes.

VI. Sinergia e Oportunidade de Negócio Transformadora para o Governo

A integração sinérgica do DataTrust CA, do *fork* do Corda DLT e dos Alqueire Data Centers distribuídos cria um ecossistema holístico para a confiança digital que é incomparável globalmente. Esta iniciativa oferece benefícios profundos e uma oportunidade de negócio transformadora para o governo brasileiro:

- **Segurança Nacional Aprimorada e Confiança: Ao estabelecer um padrão ouro para a integridade e autenticidade dos dados, o Brasil pode reduzir**

drasticamente a fraude digital (como exemplificado pelo recente incidente Pix), proteger seus cidadãos e reforçar a confiança em sua economia digital e sistemas financeiros.

- **Soberania e Resiliência Digital: O controle direto desta infraestrutura digital crítica, da certificação ao *ledger* e à hospedagem física, concede ao Brasil total soberania digital. Isso reduz a dependência de entidades externas para a segurança digital central, garantindo a resiliência nacional contra ameaças cibernéticas e mudanças geopolíticas.**
- **Novas Fontes de Receita e Liderança Econômica: A comercialização de serviços de *blockchain* privado de alta segurança através dos Alqueire Data Centers abre um mercado lucrativo. O governo, ao se tornar um provedor de soluções de *ledger* de nível empresarial, certificadas e imutáveis, pode gerar receita substancial, diversificar seu portfólio econômico e estimular o crescimento de um setor de alta tecnologia no Brasil.**
- **Posicionamento como Líder Tecnológico Global: Esta iniciativa posiciona o Brasil na vanguarda da segurança digital e da inovação DLT. Ao desenvolver, implantar e comercializar ativamente uma infraestrutura digital tão avançada e confiável, o Brasil demonstra seu compromisso com a tecnologia de ponta e sua capacidade de liderar na economia digital global. Isso eleva a posição tecnológica da nação e atrai mais investimentos e talentos.**
- **Colaboração Público-Privada: Esta estrutura naturalmente encoraja a colaboração entre autoridades governamentais, instituições financeiras e empresas de tecnologia, promovendo uma abordagem unificada para a segurança digital e a inovação.**

VII. Chamada à Ação

Chegou o momento para uma abordagem proativa e transformadora em relação à segurança digital. As vulnerabilidades expostas nos sistemas atuais exigem uma solução abrangente e integrada que não apenas proteja, mas também crie novo valor econômico.

Respeitosamente solicitamos o apoio e a colaboração das autoridades governamentais e líderes do setor privado para avançar esta iniciativa estratégica. Estamos preparados para apresentar um plano de pré-projeto detalhado, alavancando as especificações técnicas e *insights* arquitetônicos desenvolvidos, para garantir os recursos humanos e financeiros necessários para concretizar esta visão. Este é um investimento não apenas em tecnologia, mas na segurança duradoura, prosperidade e futuro digital do Brasil.

Atenciosamente,

Mario Cintra Leite de Oliveira Caseiro

São Paulo, 03 julho de 2025

Documento assinado digitalmente
gov.br
MARIO CINTRA LEITE DE OLIVEIRA CASEIRO
Data: 03/07/2025 16:08:15-0300
Verifique em https://validar.iti.gov.br