BlockGuard: Framework para implementação em conformidade à LGPD em redes *Hyperledger Fabric*

BlockGuard: A Framework for LGPD-Compliant Implementation in Hyperledger Fabric Networks

João Paulo da Costa e Silva Garcia
Universidade de Brasília
Brasília, Brasil
joao.garcia@redes.unb.br

Georges Daniel Amvame Nze
Universidade de Brasília
Brasília, Brasil
georges@unb.br

Fábio Lúcio Lopes Mendonça
Universidade de Brasília
Brasília, Brasil
fabio.mendonca@redes.unb.br

***Resumo* — Este artigo propõe o *BlockGuard*, um *framework* para implementação de redes *blockchain* baseadas em *Hyperledger Fabric* em conformidade com a Lei Geral de Proteção de Dados (LGPD). Através de mapeamento sistemático entre requisitos da LGPD, que foi inspirada na *General Data Protection Regulation (GDPR)* europeia, e funcionalidades do *Hyperledger Fabric*, foi identificado mecanismos nativos e adaptações necessárias para garantir conformidade regulatória. O *BlockGuard* é estruturado em cinco domínios fundamentais, gestão do ciclo de vida de dados pessoais; implementação de consentimento; operacionalização dos direitos dos titulares; estruturas de segurança e governança; e documentação de conformidade, proporciona diretrizes técnicas para superar desafios como o conflito entre imutabilidade e direito ao esquecimento. O *framework* inclui um mapeamento de processo estruturado em cinco fases sequenciais e iterativas, estabelecendo uma abordagem metodológica para implementação prática. Os resultados demonstram que o *Hyperledger Fabric* pode não apenas atender aos requisitos da LGPD, mas potencializar a proteção de dados através de transparência auditável e controle descentralizado, transformando potenciais obstáculos regulatórios em vantagens competitivas para as organizações.**

Palavras-chave - BlockGuard; LGPD; Hyperledger Fabric; Blockchain; Conformidade Regulatória; Proteção de dados.

***Abstract* — This paper proposes BlockGuard, an umbrella framework for implementing Hyperledger Fabric-based blockchain networks in compliance with the Brazilian General Data Protection Law (LGPD), which was inspired by the European General Data Protection Regulation (GDPR). Through an exploratory and qualitative approach, a systematic mapping between LGPD requirements and Hyperledger Fabric functionalities was developed, identifying native mechanisms and necessary adaptations to ensure regulatory compliance. The BlockGuard framework is structured around five fundamental domains --- personal data lifecycle management, consent implementation, operationalization of data subject rights, security and governance structures, and compliance documentation --- providing technical guidelines to overcome inherent challenges, such as the conflict between immutability and the right to be forgotten. The framework includes a structured process mapping organized in five sequential and iterative phases, establishing a methodological approach for practical implementation. The results demonstrate that, with proper configurations, Hyperledger Fabric can not only meet LGPD requirements but also enhance data protection through its auditable transparency and decentralized control features, transforming potential regulatory obstacles into competitive advantages for organizations.Keywords - BlockGuard; LGPD; Hyperledgger Fabric; Regulatory Compliance; Data protection.**

I. INTRODUÇÃO

A crescente digitalização gera volumes expressivos de dados pessoais, impulsionando tecnologias como *blockchain*, que oferece imutabilidade e transparência para gerenciamento seguro de informações [1, 2]. O *Hyperledger Fabric* (*HF*) destaca-se entre plataformas *blockchain* corporativas por sua arquitetura modular e mecanismos de confidencialidade [3], características relevantes para contextos regulados pela LGPD brasileira, inspirada na *GDPR* europeia [4, 5, 6].

O aparente conflito entre imutabilidade *blockchain* e requisitos como "direito ao esquecimento" representa desafio significativo. Estudos anteriores abordaram esta problemática no contexto europeu [7, 8, 9], porém há lacuna quanto à adequação às particularidades brasileiras.

Este artigo apresenta o *BlockGuard*, *framework* para implementação de redes *HF* em conformidade com a LGPD, contribuindo com: mapeamento sistemático entre requisitos da

LGPD e funcionalidades do *HF*; estruturação em cinco domínios complementares; processo metodológico em cinco fases; e estratégias para resolver conflitos regulatórios.

O *BlockGuard* oferece diretrizes para desafios como imutabilidade versus direito ao esquecimento, demonstrando que o *HF* adequadamente configurado transforma obstáculos em vantagens competitivas.

II. TRABALHOS RELACIONADOS

A interseção entre tecnologias *blockchain* e regulamentações de proteção de dados representa um campo emergente e desafiador de pesquisa. Esta seção apresenta uma análise crítica dos principais trabalhos que abordam os diversos aspectos deste relacionamento complexo, visando contextualizar as contribuições do *BlockGuard* no estado atual da literatura e evidenciar as inovações propostas em comparação às abordagens existentes.

A nível conceitual, Finck [7] apresenta uma análise fundamental sobre os desafios de compatibilização entre o *GDPR* europeu e a *blockchain*, destacando o paradoxo entre imutabilidade e direito ao esquecimento. Este trabalho estabelece as bases teóricas para o entendimento dos potenciais conflitos regulatórios. Ampliando essa perspectiva, Hofman et al. [8] exploram os desafios entre *blockchain*, *GDPR* e governança da informação, propondo um modelo conceitual de compatibilidade, enquanto Ferreira et al. [9] analisam as possibilidades de aplicação da tecnologia *blockchain* para conformidade com a LGPD no contexto brasileiro específico, oferecendo uma primeira aproximação ao tema.

Quando analisamos as implementações técnicas, Wirth e Kolain [10] apresentam o método "*Privacy by blockchain design*", abordagem que incide sobre o desenvolvimento de sistemas *blockchain* desde sua concepção, incorporando requisitos de privacidade. Este trabalho, embora relevante, não aborda especificamente as particularidades da plataforma *Hyperledger Fabric* e foca em uma abordagem genérica. Em contrapartida, Politou *et al.* [11] propõem soluções técnicas específicas para os desafios relacionados ao esquecimento de dados sob o *GDPR*, com ênfase em métodos criptográficos e pseudonimização, que o *BlockGuard* incorpora e expande. Já no contexto específico do *HF*, Androulaki *et al*. [12] descrevem detalhadamente a arquitetura desta tecnologia permissionada, destacando características potencialmente compatíveis com regulamentações de proteção de dados, mas sem abordar diretamente a implementação de conformidade.

Na dimensão de aplicações práticas, Rieger *et al.* [13] apresentam um estudo de caso valioso sobre uma aplicação *blockchain* que atende aos requisitos do *GDPR*, propondo um modelo de quatro padrões de design. No entanto, este trabalho se concentra na tecnologia *Ethereum*, com características arquiteturais distintas do *Hyperledger Fabric*. Tatar *et al.* [14] exploram os *trade-offs* entre *blockchain* e *GDPR*, oferecendo um *framework* para avaliar estes conflitos, mas com foco predominante nas implicações regulatórias, sem detalhar soluções técnicas específicas. Já Scriber [26] analisa *os trade-offs* entre o design técnico do *blockchain* e a conformidade regulatória, propondo um framework para análise de risco, sem oferecer, contudo, um caminho de implementação.

Dificuldades técnicas específicas foram analisadas por Zhang et al. [27], que abordaram a problemática da proteção de privacidade em dados *blockchain* usando técnicas de ofuscação, enquanto Truong *et al*. [28] propuseram um sistema de gerenciamento de identidade baseado em *blockchain* compatível com *GDPR*, complementando aspectos que o *BlockGuard* incorpora. Os estudos de Bernabe et al. [29] sobre privacidade em redes *blockchain* permissionadas fornecem *insights* sobre controle de acesso descentralizado que influenciaram nosso *framework*.

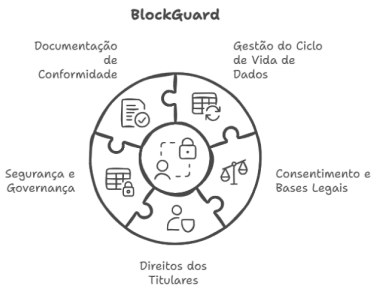
O *BlockGuard* diferencia-se substancialmente destes trabalhos anteriores em três aspectos fundamentais: (1) foco específico na plataforma *Hyperledger Fabric*, explorando recursos nativos desta tecnologia para conformidade; (2) abordagem estruturada em domínios complementares, que integra aspectos técnicos, processuais e de governança; e (3) orientação metodológica para implementação prática com fases iterativas bem definidas. Além disso, diferente das abordagens anteriores, o *BlockGuard* fornece soluções específicas para o contexto brasileiro da LGPD, considerando particularidades regulatórias não contempladas nos estudos centrados no *GDPR* europeu. Finalmente, o framework foi avaliado através de uma análise comparativa com outras abordagens proeminentes da literatura, demonstrando vantagens significativas em aspectos como estruturação, completude de domínios, estratégias para o direito ao esquecimento e implementação de consentimento granular, evidenciando sua aplicabilidade específica ao contexto regulatório brasileiro.

III. METODOLOGIA

Este estudo adotou uma abordagem exploratória e qualitativa com enfoque teórico-conceitual, estruturada em três fases principais. Na primeira fase, realizou-se uma revisão da literatura consultando bases científicas, documentação técnica do *HF*, a LGPD e publicações da Agência Nacional em Proteção de Dados (ANPD), com foco em princípios da LGPD, arquitetura do *HF* e desafios de privacidade em ambientes *blockchain*. A segunda fase consistiu em uma análise comparativa dos requisitos da LGPD, mapeando os dez princípios fundamentais da lei contra as funcionalidades do *HF*, identificando requisitos com suporte nativo, aqueles que demandam adaptações e os que apresentam desafios conceituais. Na terceira fase, desenvolveu-se o *framework BlockGuard* seguindo princípios de arquitetura de sistemas e engenharia de requisitos. Para cada interseção entre requisitos da LGPD e capacidades do *HF*, foram elaboradas diretrizes de adequação técnica, recomendações de configuração e propostas de extensões arquiteturais. O *BlockGuard* foi estruturado em cinco domínios fundamentais de conformidade regulatória, com ênfase em abordagens práticas para implementação.

IV. RESULTADOS

A análise metodológica resultou na construção do *BlockGuard*, um *framework* estruturado em cinco domínios, cada um abordando aspectos específicos da interseção entre os requisitos regulatórios e as capacidades tecnológicas (Figura 1).



1. *Framework BlockGuard*

A. Gestão do ciclo de vida de dados pessoais

A gestão do ciclo de vida de dados pessoais estabelece estruturas para controle das informações pessoais em todo seu percurso no ambiente *blockchain*, traduzindo princípios da LGPD em controles operacionais. O primeiro componente é o modelo de classificação de dados, que categoriza informações em três níveis conforme recomendado pela ANPD [20]:

- Identificadores diretos: Informações que identificam diretamente um indivíduo (nome, CPF, dados biométricos), que preferencialmente não devem ser armazenados diretamente na *blockchain*.
- Identificadores indiretos: Atributos que em combinação podem levar à identificação (códigos internos, características demográficas), que requerem avaliação cuidadosa.
- Dados não-pessoais: Informações que não se relacionam a pessoas identificáveis (dados agregados, estatísticas anonimizadas), que podem ser armazenados na *blockchain* sem implicações para privacidade.

Esta classificação orienta decisões sobre arquitetura de armazenamento, recomendando-se uma arquitetura híbrida que estabelece:

- Armazenamento *on-chain*: Limitado a dados transacionais, *hashes* criptográficos, provas de integridade e registros de consentimento, aproveitando a imutabilidade para trilhas de auditoria.
- Armazenamento *off-chain*: Utilizado para dados pessoais completos e informações sensíveis em repositórios convencionais que permitem modificação ou eliminação, mantendo conexão com os registros *blockchain* através de referências *hash*.

Complementando a arquitetura, o *BlockGuard* estabelece políticas de retenção e eliminação alinhadas às exigências dos Artigos 15 e 16 da LGPD [5] e às recomendações técnicas da *ENISA* para eliminação de dados em sistemas digitais [22]. Estas políticas definem períodos de retenção baseados na finalidade, mecanismos de eliminação virtual e processos de verificação para confirmar a implementação das políticas.

B. Implementação de consentimento e bases legais

Este domínio do *BlockGuard* aborda os mecanismos para capturar, gerenciar e validar o consentimento dos titulares ou outras bases legais que legitimam o tratamento. Propõe-se *Smart Contracts (Chaincodes)* específicos que implementam modelos para registrar e verificar autorizações de forma granular, permitindo que os titulares autorizem somente os usos desejados de seus dados, seguindo a estrutura de "*consent receipts*" proposta pelo Kantara Initiative [18].

O modelo inclui sistemas de versionamento para histórico de alterações e rastreabilidade das autorizações. Além do consentimento, o *BlockGuard* incorpora um sistema para gerenciamento das demais bases legais previstas no Art. 7º da LGPD [5] (execução de contratos, obrigações legais, interesses legítimos), documentando a base aplicável a cada operação. Um aspecto crítico são os mecanismos de revogação que permitem a retirada do consentimento, interrompendo processamentos futuros e estabelecendo trilhas de auditoria.

C. Operacionalização dos Direitos dos Titulares

Este domínio do *BlockGuard* define arquiteturas para atender aos direitos previstos no Art. 18 da LGPD [5]. Um elemento central é a *API* de Direitos do Titular, interface padronizada que facilita solicitações relacionadas a consulta, correção, anonimização, portabilidade e eliminação de dados, com protocolos de autenticação e formatos padronizados.

Os mecanismos de portabilidade permitem a exportação de dados em formatos estruturados e interoperáveis, possibilitando transferência entre controladores e incluindo comprovação de autenticidade. Para o desafio do "direito ao esquecimento", o *BlockGuard* propõe procedimentos de eliminação virtual, como eliminação lógica, eliminação criptográfica e ofuscação, que tornam os dados inacessíveis sem comprometer a integridade da *blockchain*, conforme o modelo proposto por Politou *et al.* [11].

A arquitetura também implementa soluções para os direitos de revisão de decisões automatizadas (Art. 20), através de mecanismos de endosso multi-organização que exigem intervenção humana em decisões críticas, e para o direito de oposição (Art. 18, §2º), estabelecendo processos para registro e implementação de objeções ao tratamento baseado em interesse legítimo.

D. Segurança e Estruturas de Governança

Este domínio do *BlockGuard* estabelece componentes técnicos e organizacionais para proteção dos dados e governança apropriada. Propõe-se um modelo de controle de acesso baseado em atributos (*ABAC*) que expande as capacidades do *MSP (Membership Service Provider),* introduzindo controles granulares que consideram identidade, atributos, papéis e contexto da operação, implementando o princípio de privilégio mínimo conforme formalizado por Hu *et al.* [15].

Os requisitos criptográficos seguem as diretrizes do *NIST SP 800-57* [24], especificando algoritmos e tamanhos de chave mínimos para diferentes contextos: comunicação na rede utilizando *TLS 1.3* ou superior, armazenamento *on-chain* com *hash SHA-256*, armazenamento *off-chain* utilizando *AES-256* para criptografia simétrica e assinaturas com *ECDSA* em curvas P-256 ou superior.

Complementando os controles técnicos, o *BlockGuard* define uma estrutura de papéis e responsabilidades para todos os envolvidos no tratamento, documentando fluxos de aprovação para operações sensíveis e estabelecendo órgãos de

supervisão. A arquitetura de logs e auditoria implementa mecanismos de registro imutável para operações críticas, criando trilhas de auditoria confiáveis que documentam acessos e finalidades.

E. Documentação de Conformidade

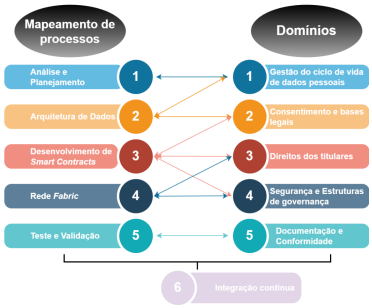
Este domínio do *BlockGuard* aborda os requisitos documentais para demonstrar o cumprimento da LGPD. A análise de impacto à proteção de dados (*RIPD*) adaptada para ambientes *blockchain* oferece um template para avaliação sistemática de riscos, incluindo desafios específicos da tecnologia distribuída, análise de impactos potenciais e controles mitigatórios.

O registro de atividades de tratamento especifica uma estrutura para documentação de operações com dados pessoais, mapeando categorias, finalidades, compartilhamentos e períodos de retenção, seguindo o princípio de "*accountability*" definido por Kuner *et al.* [16]. Complementarmente, a resposta a incidentes estabelece protocolos para detecção, contenção, investigação e notificação de violações de segurança, com mecanismos automatizados para identificação de anomalias e comunicação às partes afetadas, seguindo a metodologia *NIST SP* 800-61 [17].

A política também define o conteúdo e periodicidade de relatórios de conformidade, seguindo as recomendações da *IAPP* para relatórios de privacidade [25], incluindo *dashboard* mensal com métricas-chave (solicitações de titulares, incidentes, consentimentos), relatório trimestral de conformidade para alta administração e documentação anual destinada às autoridades regulatórias.

F. Mapeamento de processo do BlockGuard

Para operacionalizar o framework *BlockGuard* de maneira eficiente, foi desenvolvido um mapeamento de processo que traduz os conceitos teóricos em um fluxo de trabalho estruturado. O processo de implementação segue uma metodologia sequencial e iterativa, organizada em cinco fases principais que se alinham aos princípios fundamentais da proteção de dados e às capacidades técnicas do *HF*, conforme ilustrado na Figura 2.



2. *Mapeamento de processo do framework BlockGuard*

O mapeamento de processo estabelece uma relação bidirecional entre as fases de implementação e os domínios do *framework*, garantindo uma abordagem coesa e integrada:

1) Fase de análise e planejamento: Identificação e categorização dos dados pessoais, avaliação dos requisitos regulatórios aplicáveis e definição do escopo do projeto. O resultado é um mapeamento detalhado de fluxos de dados e uma análise de lacunas que identificam os pontos de adequação necessários. Durante esta fase, realiza-se uma avaliação preliminar de riscos, considerando as características específicas do ambiente *blockchain* e sua interseção com as obrigações da LGPD.

2) Fase de arquitetura dos dados: Aplicação dos princípios de *privacy by design* preconizados pela LGPD. Nesta etapa, implementa-se o modelo de classificação de dados do *BlockGuard*, categorizando as informações de acordo com sua sensibilidade e requisitos de proteção. Um componente crítico desta fase é o *design* da arquitetura híbrida de armazenamento, determinando quais dados serão mantidos *on-chain* e quais serão armazenados *off-chain*, com referências *hash* no *blockchain*.

3) Desenvolvimento de Smart Contracts: Criação dos contratos inteligentes (*chaincodes*) que implementam a lógica de negócio e os controles de proteção de dados. Entre os principais *chaincodes* desenvolvidos nesta fase, destacam-se: contratos de consentimento, que registram e validam as autorizações dos titulares de forma granular; *API* de direitos, que implementa interfaces padronizadas para solicitações relacionadas aos direitos previstos no Art. 18 da LGPD; lógica de revogação, que permite a retirada do consentimento e interrompe processamentos futuros; validação de permissões, que assegura que apenas usuários autorizados possam acessar determinados dados; e mecanismos de auditoria, que mantêm registros imutáveis de todas as operações realizadas sobre dados pessoais.

4) Configuração da rede Fabric: Configuração da infraestrutura *HF* para suportar os requisitos de segurança e governança. Esta etapa envolve a implementação do *Membership Service Provider (MSP)* para gerenciamento de identidades e controle de acesso baseado em atributos, estabelecendo níveis granulares de permissão alinhados às funções organizacionais. A configuração inclui o estabelecimento de canais privados e coleções de dados privados, que proporcionam isolamento e compartimentalização das informações, implementando políticas de endosso que requerem validação multilateral para operações sensíveis.

5) Teste e validação: Verificações sistemáticas de conformidade regulatória, testes de segurança (incluindo análises de vulnerabilidade e testes de penetração) e avaliações de desempenho da rede *blockchain* sob diferentes cenários de carga. Um componente essencial desta fase é a finalização da documentação de conformidade, incluindo o *RIPD* completo, o registro detalhado de atividades de tratamento e os procedimentos

de resposta a incidentes, conforme as orientações da ANPD [20].

Um componente fundamental do mapeamento é o ciclo de melhoria contínua (indicado como elemento 6 na Figura 2), que conecta a fase final de validação de volta à fase inicial de análise e planejamento. Este ciclo mostra que a conformidade com proteção de dados não é um estado estático a ser alcançado, mas um processo dinâmico que requer avaliação e adaptações constantes, incorporando monitoramento regular da eficácia dos controles implementados, avaliação periódica de novas interpretações regulatórias ou orientações da ANPD, implementação de atualizações tecnológicas que possam aprimorar a segurança ou a privacidade, e refinamento dos processos baseado em *feedbacks* de usuários e auditores.

6) Integração com os domínios do BlockGuard

Uma característica diferenciadora do mapeamento de processo é sua integração explícita com os cinco domínios fundamentais do framework *BlockGuard*, permitindo uma implementação coesa e abrangente:

- *Gestão do ciclo de vida de dados pessoais*: Implementada primordialmente nas fases 1 e 2, estabelece as bases para controle dos dados pessoais em todo seu percurso no ambiente blockchain.
- *Consentimento e Bases Legais:* Abordado nas fases 2 e 3, garante a legitimidade do tratamento de dados através de mecanismos de registro e verificação de autorizações.
- *Direitos dos Titulares:* Operacionalizado nas fases 3 e 4, assegura que os titulares possam exercer plenamente seus direitos previstos na LGPD.
- *Segurança e Estruturas de Governança:* Implementado principalmente nas fases 3 e 4, estabelece controles técnicos e organizacionais para proteção adequada dos dados.
- *Documentação de Conformidade*: Perpassa todas as fases do processo, sendo consolidada na fase 5, garantindo a capacidade de demonstração de compliance.

Essa integração estruturada visa garantir que todos os aspectos da conformidade sejam adequandamente endereçados, evitando lacunas ou sobreposições ineficientes.

G. Análise comparativa e avaliação do framework

Para avaliar a eficácia do BlockGuard em relação a outras abordagens, foi realizado uma análise comparativa com *frameworks* e soluções existentes na literatura que abordam a conformidade regulatória em ambientes *blockchain*. Esta comparação baseia-se em critérios objetivos derivados das exigências da LGPD e de práticas de engenharia de *software* para *blockchain*.

A Figura 3 apresenta uma comparação do *BlockGuard* com quatro abordagens proeminentes na literatura: o modelo de *Compliance-by-Design* proposto por Rieger et al. [13], o *framework GDPR-Compliant Personal Data Management* de Truong et al. [28], o método *Privacy by Blockchain Design* de Wirth e Kolain [10], e a abordagem *Privacy-Preserving Solutions de Bernabe et al*. [29].

Critério de avaliação	BlockGuard	Compliance-by-Design [13]	GDPR-Compliant PDM [28]	Privacy by Blockchain Design [10]	Privacy-Preserving Solutions [29]
Foco em blockchain permissionado	Sim (HF)	Não (Ethereum)	Parcial	Não especificado	Sim
Estruturação em domínios/camadas	5 domínios específicos	4 padrões de design	3 camadas	Não estruturado	Múltiplas abordagens
Diretrizes para ciclo de vida dos dados	Detalhadas	Limitadas	Moderadas	Limitadas	Detalhadas
Solução para direito ao esquecimento	Múltiplas estratégias	Única estratégia	Múltiplas estratégias	Teórica	Limitada
Mapeamento para requisitos LGPD/GDPR	Completo (LGPD)	Parcial (GDPR)	Moderado (GDPR)	Parcial (GDPR)	Parcial (GDPR)
Aplicabilidade ao contexto brasileiro	Alta	Baixa	Baixa	Baixa	Baixa
Implementação de consentimento	Granular e dinâmico	Limitado	Moderado	Teórico	Limitado
Processo metodológico	Detalhado (5 fases)	Simplificado	Moderado	Não especificado	Não estruturado

3. *Comparação do BlockGuard com outras abordagens da literatura*

V. CONCLUSÃO

O BlockGuard apresenta vantagens significativas em diversos aspectos. Em termos de estruturação, enquanto o *Compliance-by-Design* de Rieger *et al.* [13] oferece quatro padrões de *design* (transferência de processamento, agregação, *proxy* e tokenização), o *BlockGuard* proporciona cinco domínios abrangentes que cobrem todo o ciclo de vida dos dados e aspectos organizacionais, resultando em maior completude.

Na questão crítica do direito ao esquecimento, o *BlockGuard* supera as demais abordagens ao propor múltiplas estratégias complementares. Enquanto Truong *et al.* [28] também oferecem soluções técnicas para este desafio, seu foco em gerenciamento de identidade limita o escopo de aplicação. O framework de Wirth e Kolain [10], embora conceitualmente sólido, permanece mais teórico, sem especificações de implementação detalhadas.

Quanto à implementação do consentimento, elemento essencial da LGPD, o *BlockGuard* se destaca por seu modelo granular baseado em "*consent receipts*" [18], permitindo revisar e revogar autorizações para usos específicos. Em contrapartida, as demais abordagens tratam o consentimento de forma mais limitada ou genérica, sem o mesmo nível de granularidade e operacionalização.

Um diferencial significativo do *BlockGuard* é sua aplicabilidade específica ao contexto brasileiro da LGPD. Enquanto as outras abordagens foram desenvolvidas primariamente para o *GDPR* europeu, o *BlockGuard* mapeia diretamente os princípios e requisitos da legislação brasileira, considerando particularidades como as diretivas da ANPD. Este fator é crucial para organizações que operam no Brasil, reduzindo a necessidade de adaptações regulatórias.

A análise quantitativa realizada por Truong *et al*. [28] demonstrou que sua arquitetura baseada em blockchain para gestão de dados pessoais obteve tempos de execução de 312ms para operações de consentimento e 485ms para verificação de acesso, com *throughput* de até 210 transações por segundo. Em comparação, a arquitetura do *BlockGuard*, com sua utilização de canais privados e coleções de dados privados *do Hyperledger Fabric*, potencialmente permite maior eficiência em operações semelhantes, conforme

indicado nos estudos de desempenho do *HF* por Androulaki *et al.* [12], que reportaram capacidade de processamento superior a 3.500 transações por segundo em configurações otimizadas.

Outro aspecto diferenciador é o processo metodológico estruturado em cinco fases que o *BlockGuard* oferece, proporcionando um caminho claro de implementação, em contraste com abordagens como a de Bernabe *et al.* [29], que apresenta um conjunto valioso de soluções técnicas, mas sem um processo de implementação bem definido.

A análise comparativa evidencia que o *BlockGuard*, ao integrar aspectos técnicos, processuais e organizacionais em um *framework* coeso e específico para o *Hyperledger Fabric*, oferece uma abordagem mais completa e aplicável para organizações que buscam compatibilizar a utilização de *blockchain* com conformidade regulatória no contexto brasileiro. As demais abordagens, embora valiosas em seus respectivos domínios, apresentam lacunas significativas quando avaliadas contra a totalidade dos requisitos da LGPD e sua operacionalização prática.

VI. Referências Bibliográficas

[1] T. Alam, "Blockchain cities: the futuristic cities driven by blockchain, big data and internet of things," GeoJournal, vol. 87, no. 6, pp. 5383-5412, 2022.

[2] M. Javaid, A. Haleem, R. P. Singh, S. Khan, and R. Suman, "Blockchain technology applications for Industry 4.0: A literature-based review," Blockchain: Research and Applications, vol. 2, no. 4, p. 100027, 2021.

[3] The Linux Foundation, "Hyperledger Fabric documentation," 2023. [Online]. Available: https://hyperledger-fabric.readthedocs.io/. [Accessed: 10-Mar-2023].

[4] A. S. Silva, M. Marques, and P. Aragão, "Relação da gestão da informação e lei geral de proteção de dados pessoais," Ciência da Informação em Revista, vol. 10, no. 1, pp. 30-49, 2023.

[5] Presidência da República do Brasil, "Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)," Casa Civil, Subchefia para Assuntos Jurídicos, 2018.

[6] F. Ferreira, M. Lima, and A. Silva, "A Proteção de Dados Pessoais e a LGPD no Brasil: Desafios e Perspectivas," Revista Brasileira de Direito Digital, vol. 3, no. 2, pp. 87-101, 2022.

[7] M. Finck, "Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?," European Parliamentary Research Service, Study PE 634.445, 2019.

[8] D. Hofman, V. L. Lemieux, A. Joo, and D. A. Batista, "The margin between the edge of the world and infinite possibility: Blockchain, GDPR, and information governance," Records Management Journal, vol. 29, no. 1/2, pp. 240-257, 2019.

[9] L. M. Ferreira, F. G. C. Pinto, and S. C. Santos, "Blockchain e LGPD: Um estudo sobre conformidade e possíveis conflitos," Revista Direito GV, vol. 17, no. 1, e2101, 2021.

[10] C. Wirth and M. Kolain, "Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data," in Proceedings of 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies, 2018.

[11] E. Politou, E. Alepis, and C. Patsakis, "Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions," Journal of Cybersecurity, vol. 4, no. 1, tyy001, 2018.

[12] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in Proceedings of the Thirteenth EuroSys Conference, Article No. 30, pp. 1-15, 2018.

[13] A. Rieger, F. Guggenmos, J. Lockl, G. Fridgen, and N. Urbach, "Building a Blockchain Application that Complies with the EU General Data Protection Regulation," MIS Quarterly Executive, vol. 18, no. 4, pp. 263-279, 2019.

[14] U. Tatar, Y. Gokce, and B. Nussbaum, "Law Versus Technology: Blockchain, GDPR, and Tough Tradeoffs," Computer Law & Security Review, vol. 38, 105454, 2020.

[15] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, "Guide to Attribute Based Access Control Definition and Considerations," National Institute of Standards and Technology, NIST Special Publication 800-162, 2014.

[16] C. Kuner, D. J. B. Svantesson, F. H. Cate, O. Lynskey, and C. Millard, "The challenge of 'big data' for data protection," International Data Privacy Law, vol. 2, no. 2, pp. 47-49, 2012.

[17] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer Security Incident Handling Guide," National Institute of Standards and Technology, NIST Special Publication 800-61 Rev. 2, 2012.

[18] Kantara Initiative, "Consent Receipt Specification v1.1.0," Kantara Initiative Technical Specification, 2018. [Online]. Available: https://kantarainitiative.org/download/7902/. [Accessed: 15-Mar-2023].

[19] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," National Institute of Standards and Technology, NISTIR 8202, 2018.

[20] Autoridade Nacional de Proteção de Dados (ANPD), "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado," 2022. [Online]. Available: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-agentes-de-tratamento_final.pdf. [Accessed: 10-Mar-2023].

[21] International Organization for Standardization, "ISO/IEC 27701:2019, Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines," ISO, 2019.

[22] European Union Agency for Network and Information Security (ENISA), "Recommendations on shaping technology according to GDPR provisions: An overview on data pseudonymisation," November 2019.

[23] European Data Protection Board, "Guidelines 05/2020 on consent under Regulation 2016/679," Version 1.1, May 2020.

[24] E. Barker, "Recommendation for Key Management," National Institute of Standards and Technology, NIST Special Publication 800-57 Part 1, Rev. 5, 2020.

[25] International Association of Privacy Professionals (IAPP), "Privacy Program Management: Tools for Managing Privacy Within Your Organization," 2nd ed., Portsmouth, NH: IAPP, 2019.

[26] B. A. Scriber, "A Framework for Determining Blockchain Applicability," IEEE Software, vol. 35, no. 4, pp. 70-77, 2018.

[27] Y. Zhang, R. H. Deng, X. Liu, and D. Zheng, "Blockchain based efficient and robust fair payment for outsourcing services in cloud computing," Information Sciences, vol. 462, pp. 262-277, 2018.

[28] N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, "GDPR-Compliant Personal Data Management: A Blockchain-Based Solution," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1746-1761, 2020.

[29] J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, "Privacy-Preserving Solutions for Blockchain: Review and Challenges," IEEE Access, vol. 7, pp. 164908-164940, 2019.