Prontuário Eletrônico do Paciente baseado em *Blockchain*: Uma Análise das Potencialidades e Desafios à Luz dos Requisitos da SBIS e LGPD

Pamella Soares[1], Allysson Allex Araújo[2], Raphael Saraiva[1], Jerffeson Souza[1] George Sousa[3] e Lúcia Duarte[3]

[1] Programa de Pós-Graduação em Ciência da Computação (PPGCC)
Universidade Estadual do Ceará (UECE) – Fortaleza, Ceará - Brasil

[2]Grupo de Estudos em Sistemas de Informação e Inovação Digital (GESID)
Universidade Federal do Ceará (UFC) – Crateús, Ceará – Brasil

[3]Programa de Pós-graduação em Cuidados Clínicos em Enfermagem e Saúde (PPCCLIS)
Universidade Estadual do Ceará (UECE) – Fortaleza, Ceará - Brasil

{pamella.soares,raphael.saraiva,george.jo}@aluno.uece.br,
allysson.araujo@crateus.ufc.br, {jerffeson.souza,maria.duarte}@uece.br

Resumo. *A tecnologia blockchain tem se mostrado proeminente em sua integração com Prontuário Eletrônico do Paciente (PEP) por permitir o registro de eventos digitais de forma transparente, segura, resiliente e compartilhado entre diferentes entidades. Entretanto, apesar de promissora, essa integração apresenta desafios ao considerar a adequação às normas, cultura e regulamentos institucionais. Por sua vez, a fim de se alinhar adequadamente, o PEP precisa ser devidamente certificado por entidades credenciadas e, adicionalmente, garantir privacidade aos dados do paciente. Considerando tal problemática, esta pesquisa tem como objetivo, realizar um mapeamento preliminar das potencialidades e desafios relacionados aos requisitos e princípios estabelecidos pela Sociedade Brasileira de Informática em Saúde e pela Lei Geral de Proteção de Dados. Dessa forma, pretende-se contribuir ao promover a discussão e a cooperação entre academia, governo e mercado no contexto de projetos de software relacionados à integração de blockchain e PEP.*

1. Introdução

O Prontuário Eletrônico do Paciente (PEP) é uma estrutura que descreve e registra eventos e serviços médicos realizados aos pacientes ao longo de sua vida (incluindo procedimentos, prescrições e exames executados por profissionais) de forma a facilitar a tomada de decisões para definir os devidos tratamentos e processos [Possari 2005]. Nesse sentido, um ponto crítico a ser observado é a segurança da informação, visto que os dados do paciente devem receber tratamento adequado a fim de preservar a privacidade [De Muylder et al. 2019]. Considerando tais particularidades, o usufruto de *blockchain* no contexto de PEP tem se posicionado como proeminente tendo em vista a capacidade única de registro imutável de eventos digitais de forma transparente, segura e resiliente. Em suma, o *blockchain* funciona como um livro-razão distribuído, onde o registro, a verificação, o armazenamento, a manutenção e a transmissão de dados são baseados numa arquitetura distribuída protegida por criptografia, cuja governança e confiança

mútua entre os nós da rede é estabelecida de forma descentralizada através de algoritmos de consenso [Beck et al. 2017]. Catalisado por tal ascensão tecnológica, tem-se a consolidação das Aplicações Descentralizadas as quais possibilitam o desenvolvimento de programas que se comunicam com a *blockchain* e cuja lógica de negócios é descrita a partir de contratos inteligentes (CIs) [Xu et al. 2019].

A adoção de *blockchain*, embora promissora, ainda apresenta desafios que envolvem fatores institucionais relacionados às normas e culturas das organizações, regulamentos e leis existentes, e a governança [Janssen et al. 2020]. No Brasil, para que um sistema de informática em saúde seja certificado, por exemplo, necessita-se que os requisitos de segurança, estrutura, conteúdo e funcionalidades estejam em conformidade com os critérios especificados pelo manual de certificação da Sociedade Brasileira de Informática em Saúde (SBIS). Por sua vez, deve-se criar medidas de segurança, técnicas e administrativas adequadas para proteger os dados sensíveis de acessos não autorizados pelos titulares, baseando-se nos princípios da Lei Geral de Proteção de Dados (LGPD). Assim, para que uma organização atenda de forma contínua e sustentável aos princípios da LGPD, faz-se necessário analisar todas as áreas de negócios, incluindo processos, pessoal e tecnologia [Garcia et al. 2020]. Todavia, apesar da existência de guias técnicos de implantação da LGPD e de manuais da SBIS, este último, específico para sistemas de saúde, ainda se identifica uma carência quanto ao alinhamento e discussão específica do atendimento de tais normas ao utilizar *blockchain* na implementação de PEPs.

Portanto, o presente trabalho visa identificar e avaliar as potencialidades e os desafios no desenvolvimento de PEPs baseado em *blockchain* por meio de uma análise documental no manual de certificação da SBIS e na LGPD. Respectivamente, esta avaliação considera os requisitos para certificação de PEPs, assim como os princípios de privacidade dos dados sensíveis. O processo de análise dos documentos foi baseado em [Bowen 2009] de modo que os textos relevantes foram reunidos e um esquema organização e gestão desenvolvido. Em seguida, foram feitos resumos e anotações dos originais e a avaliação a autenticidade dos documentos, assim como o devido entendimento de conceitos básicos e, finalmente, a exploração do conteúdo. Dessa forma, tem-se como contribuição prover um mapeamento preliminar relacionando as potencialidades e desafios atreladas ao uso de *blockchain* em PEP de forma alinhada ao arcabouço regimental brasileiro (quanto à SBIS e LGPD) e, consequentemente, fomentar a discussão e cooperação entre a academia, governo e mercado no contexto de projetos de software com essa natureza.

2. Análise preliminar dos requisitos advindos da SBIS e LGPD

Conforme sintetizado na Figura 1, organizou-se em 4 grupos o subconjunto de potenciais requisitos e princípios (oriundos da SBIS e LGPD) impactados pela adoção de *blockchain*. Para cada grupo, tem-se uma possível estratégia de *design* para introduzir o uso de *blockchain* o qual reflete, por sua vez, diferentes potencialidades e desafios.

Quanto às potencialidades do **Grupo 1**, constatam-se requisitos sobre *identificação e autenticação de pessoas, autorização e controle de acesso à diferentes 'atores' da solução* solicitados pela SBIS, cujas regras de negócio que podem ser implementadas nas estruturas de dados do contrato inteligente (CI). Dependendo da lógica, pode-se identificar as partes que interagem com a solução a fim de impedir o acesso de terceiros não-autorizados pelo paciente. Logo, o paciente poderá gerenciar o controle de

acesso de forma segura e possuirá registros gravados em *blockchain* com as respectivas entidades de saúde habilitadas, semelhante ocorre para *confidencialidade e consentimento* sugeridas pela LGPD e, consequentemente, influenciam no *direito de acesso*, *direito à informação* por parte do paciente e na *identificação dos responsáveis pelo tratamento* dos dados. Além disso, pode-se atender a anonimização por meio de estratégias *off-chain* visando preservar a *privacidade* de dados sensíveis. Essa técnica armazena em *blockchain* apenas o *hash* ou ponteiros advindos de banco de dados (BD) tradicional e/ou distribuído, os quais conterão as informações completas liberadas apenas se o paciente permitir. A forma como cada dado será armazenado pode impactar na modelagem arquitetural a qual, inicialmente, pode ser composta por camadas de armazenamento *on-chain* e *off-chain*.

	Requisitos da SBIS	Ref.	Princípios da LGPD	Ref.	Estratégias de *design*
Grupo 1	Identificação e autenticação de pessoas	NGS1.02	Anonimização	Art. 5º (3)(11); Art. 12º	Regra de acesso por meio da manipulação de estruturas de dados implementadas nos CIs.
	Autorização e controle de acesso	NGS1.04	Confidencialidade e Consentimento	Art. 5º (VII); Art. 8º Art. 46º	
	Privacidade	NGS1.12	Direito de acesso | Direito à informação | Identificação dos responsáveis pelo tratamento	Art. 18º	Estratégia *off-chain* para privacidade de dados sensíveis.
	Atores	FUNC.18			
Grupo 2	Disponibilidade do RES	NGS1.05	Integridade	Art. 6º (IV)(VII)	Réplicas dos dados em cada nó da rede.
	Segurança de Dados	NGS1.07			Armazenamento de *hash* imutável e auditável.
Grupo 3	Dados clínicos	ESTR.04	Limitação de armazenamento	Art. 15º	Estratégia *off-chain* para armazenamento dos dados brutos.
	Gerais	SGED.01	Minimização de dados pessoais	Art. 6º (1)(2)(3)	
			Direito ao esquecimento	Art. 5º (XIV)	
Grupo 4	Problemas/condições de saúde e outras questões	FUNC.02			Imutabilidade e operações *append-only*.
	Médico-legal	FUNC.17			

Figura 1. Potenciais subconjuntos de requisitos da SBIS e de princípios da LGPD.

Em relação às possibilidades do **Grupo 2**, conforme o conceito de disponibilidade pela SBIS, deve-se possibilitar a restauração de cópias de segurança com informações suficientes para restauração. A descentralização da *blockchain* e a persistência dos dados apresentam-se relevantes visto que os vários nós da rede se conectam entre si e, assim, mantêm as réplicas das informações de maneira distribuída, as quais podem ser acessadas mesmo se um ou mais nós estiverem desativados. Adicionalmente, um sub-requisito da SBIS (e também requerido pela LGPD) sobre disponibilidade é a integridade dos dados, a qual dispõe que a informação não deva ser alterada ou excluída sem autorização prévia de alguém autorizado. Isto posto, a estrutura implementada no CI pode guardar a impressão digital criptográfica (*hash*) exclusiva de um documento armazenado inicialmente. A partir disso, pode-se verificar a integridade dos dados comparando o *hash* computado (a saída de execução do algoritmo) a um valor de *hash* conhecido, esperado e inalterado. Assim, torna-se possível demonstrar se uma mídia foi modificada ou adulterada pois, quando há alteração, o valor *hash* computado modifica-se. Há de se ressaltar que a imutabilidade dos dados no *blockchain* proporciona a não exclusão e alteração de transações já submetidas, o que garante que ações de correção ou edição preservem os dados.

O **Grupo 3** refere-se, em suma, à estruturação e conteúdo dos *dados clínicos*. Os principais ativos a serem inseridos e visualizados contêm várias informações e métodos relacionados aos exames e procedimentos realizados, e são compilados em arquivos de diferentes formatos. Porém, depara-se ainda com o desafio de escalabilidade em *blockchain* para armazenar, por exemplo, um arquivo de mídia. Considera-se, portanto, o uso de estratégia *off-chain* para armazenamento de informações brutas em BD terceirizado,

semelhante ao que foi apresentado para o Grupo 1. A técnica de armazenar apenas o *hash* do arquivo em *blockchain* contempla o fato de que deve-se restringir a quantidade de dados a serem apresentados a depender do propósito de uso, influenciando no princípio de *limitação de armazenamento* e *minimização de dados pessoais*. Ressalta-se que um dos princípios básicos de leis que visam proteger dados sensíveis é o *direito ao esquecimento*. Porém, como a principal característica da *blockchain* é a imutabilidade das informações, não é possível excluir ou alterar dados que já foram armazenados. Esse desafio gera controvérsia quanto ao uso de *blockchain* e este direito, haja vista que o dado deve ser apagado quando houver solicitação do titular. Para mitigar esse conflito, a estratégia *off-chain* faz com que os dados completos armazenados em BDs terceiros sejam removidos facilmente. Já na *blockchain*, as referências das partes e o *hash* das informações brutas não terão mais capacidade de referenciar qualquer informação fora da *blockchain*.

As potencialidades concernentes apenas à SBIS no **Grupo 4** refletem a demanda que se tenha um entendimento cronológico e integral sobre a saúde durante a vida do paciente. Considera-se que *blockchain* possibilita o armazenamento com registro de tempo. Além disso, realiza apenas operações *append-only*. Dessa forma, as transações históricas, que são apenas anexadas, não podem ser excluídas ou modificadas sem invalidar a cadeia de *hashes*. Tal funcionalidade pode proporcionar a rastreabilidade de informações.

Por meio deste estudo preliminar, compartilha-se, com acadêmicos e profissionais envolvidos com *e-health*, um mapeamento de potencialidades e desafios ao integrar a tecnologia *blockchain* para PEP. Assim, oportuniza-se o debate sobre o uso de *blockchain* no contexto de PEP de forma alicerçada nos requisitos da SBIS e princípios da LGPD.

Referências

Beck, R., Avital, M., Rossi, M., and Thatcher, J. B. (2017). Blockchain technology in business and information systems research.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative research journal*.

De Muylder, C. F., de Oliveira, J. G., Batista, C. L., and Marques, R. M. (2019). Segurança da informação ea área da saúde: a convergência dos temas ea intensidade das publicações científicas. *Revista de Gestão em Sistemas de Saúde*, 8(2).

Garcia, L. R., Aguilera-Fernandes, E., Gonçalves, R. A. M., and Pereira-Barretto, M. R. (2020). *Lei Geral de Proteção de Dados (LGPD): Guia de implantação*. Editora Blucher.

Janssen, M., Weerakkody, V., Ismagilova, E., Sivarajah, U., and Irani, Z. (2020). A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. *International Journal of Information Management*, 50:302–309.

Possari, J. F. (2005). Prontuário do paciente e os registros de enfermagem. In *Prontuário do paciente e os registros de enfermagem*, pages 246–246.

Xu, X., Weber, I., and Staples, M. (2019). Blockchain patterns. In *Architecture for Blockchain Applications*, pages 113–148. Springer.